UNIT -1

NETWORK HARDWARE

The two dimensions of network hardware are:

1) Transmission technology
2) Scale

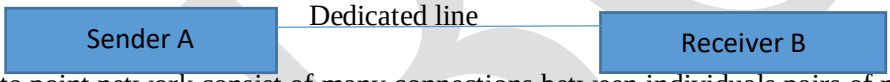
1. Transmission Technology

There are two types of transmission technology are: 1) Broadcast links and 2) Point – to – Point links.

1. Broadcast links

- Broadcast network have a single communication channel that is shared by all the machines on the network.
- packets can sent by any machine are received by all the others.
- When a packet with this code is transmitted, it is received and processes by every machine on the network. This mode of operation is called broadcasting

2. Point – to –point links



- Point – to point network consist of many connections between individuals pairs of machines.
- Often multiple routes; choose the shortest path to send the packets.
- Point – to –Point transmission with one sender and one receiver is sometimes called unicasting.

1.2.2.Scale

The types of networks are classified in their scale are shown below:

Inter process distance	Processors located in same	Example
1m	Square Meter	Personal Area Network
10m	Room	LAN
100m	Building	LAN
1km	Campus	LAN
10km	City	MAN
100km	Country	WAN
1000km	Continent	WAN
10,000km	Planet	Internet

3. Types of Networks

1) Local Area Network

2) Metropolitan Area Network

3) Wide Area Network

4) Wireless Area Network

5) Home Network

6) Internetwork

1) Local Area Network (LAN)

- LANs are privately owned networks within a single building or campus of up to a few kilometers in size.
- They are widely used to connect personal computer and workstation in company offices and factories to share resources and exchange information.
- The characteristics are
  - Size
  - Transmission technology
  - Topology
- Various topologies are possible for broadcast LANs. They are 1) Bus and 2) Ring

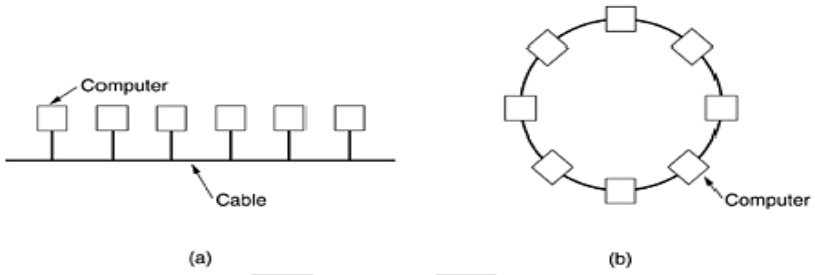


Fig: Two broadcast networks. (a) Bus (b) Ring

Bus Network

- In a bus network, one machine is the master and is allowed to transmit.
- All other machines are required to refrain from sending.

Ring Network

- In a ring network, each bit propagates around on its own, not waiting for the packet to which it belongs.
- Each bit is a ring can takes the time to transmit a few bits, often before the complete packet has even been transmitted.

2) Metropolitan Area Network (MAN)

- MAN covers a city.
- There were locally designed ad-hoc systems.
- Entire channels designed for cables only.
- The cable channels were highly specialized, such as all news, all sports, all cooking, all gardening and so on.

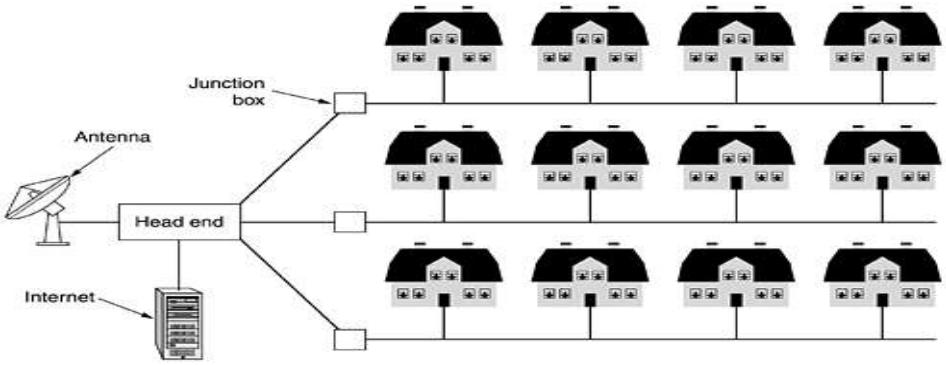


Fig: A metropolitan area network based on cable TV

- ✓ The best example is the cable television network.

3) Wide Area Networks (WAN)

- WAN spans a large geographical area.
- It contains a collection of machines intended for running user programs. These machines are called hosts.
- The hosts are connected by a communication subnet or subnet.
- The subnet is operated by Telephone Company or Internet Service Provider.
- The subnet is to carry message from host to host.
- The subnet consists of two distinct components
  1) Transmission Technology
  2) Switching Elements.
- Transmission lines move bits between machines.
- They can be made of copper wire, optical, fiber or even radio links.
- Switching elements are specialized computers that connect two or three transmission links.
- These switching elements are called Routers.

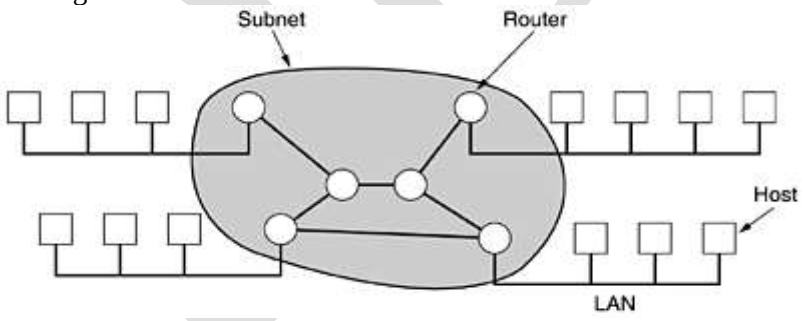


Fig: Relation between hosts on LANs and the subnet

- Each host is connected to a LAN on which a router is present and a host can be connected directly to the router.
- A collection of communication lines and routers from the subnet.
- A collection of routers and communication lines that moved packets from the source host to the destination host.
- When a packet is sent from one router to another via one or more intermediate routers, the packet is received at each intermediate router, stored there until the required output line is free, and then forward.
- This is called a store- and – forward or packet – switched subnet.

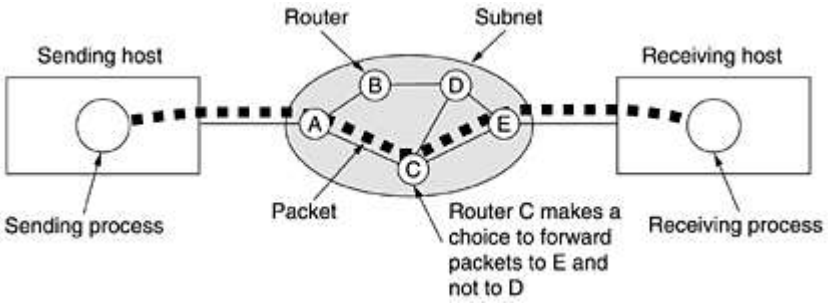


Fig: A stream of packets from sender to receiver

- When a process on some host has sent a message to receiving process on some other host, the sending host first cuts the message into packets, each one bearing its number in the sequence.
- Choose the shortest path and sends a packets from source to destination host.

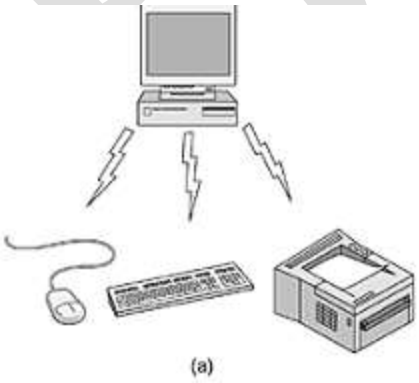
4) Wireless Networks

Wireless Networks can be divided into:

i) System Interconnected ii) Wireless LANs and iii) Wireless WANs

i) System Interconnected

- ✓ System interconnected is all interconnecting the components of a computer using short-range radio.
- ✓ Every computer has a monitor, Keyboard, mouse, and printer connected to the main units by cables.
- ✓ Some companies got together to design a short-range wireless network called Bluetooth to connect these components without wires.



✓ **Fig: a) Bluetooth configuration.**

Bluetooth also allows digital cameras, headsets, scanners, and other devices to connect to a computer within the range. No cables, no driver installation, just put them down, turn them on and they work.

ii) Wireless LANs

- ✓ Every computer has a radio modem and antenna with which it can communicate with other systems.
- ✓ If the systems are close enough, they can communicate directly with one another in a peer - to – peer configuration. The standard wireless LANs called IEEE 802.11

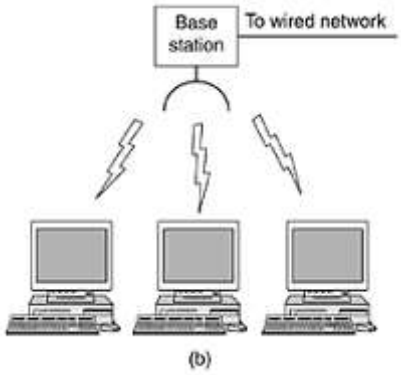


Fig: (b) Wireless LAN

iii) Wireless WANs

The radio network used for cellular telephones is an example for low-bandwidth wireless systems. These wireless systems have three generations are:

i) First generation was analog and for voice only.
ii) Second generation was digital and for voice only.
iii) Third generation is digital and is for both voice and data.

5) Home Networks

Every device in the home will be capable of communicating with every other device and all of them will be accessible over the internet. Some categories are:

1) Computer (Desktop PC, Notebook PC, PDA, Shared Peripherals)

2) Entertainment (TV, DVD, VCR, camcorder, camera, stereo, MP3)

3) Telecommunications (telephone, mobile telephone, intercom, fax)

4) Appliances (microwave, refrigerator, clock, furnace, airco, lights)

5) Telemetry (utility meter, smoke/burglar alarm, thermostat, babycam)

6) InterNetworks

- A collection of interconnected networks is called an Internetwork or internet.
- A common form of internet is a collection of LANs connected by a WAN.
- Subnet makes the collection of routers and communication lines owned by the network operator.
- A combination of subnet and its hosts forms a network.
- An Internetwork is formed when distinct networks are interconnected.
- Connecting a LAN and a WAN or connecting two LANs forms an internet.

Network Software

Network software encompasses a broad range of software used for design, implementation, and operation and monitoring of computer networks. Traditional networks were hardware based with software embedded.

Functions of Network Software

1. Helps to set up and install computer networks

2. Enables users to have access to network resources in a seamless manner
3. Allows administrations to add or remove users from the network
4. Helps to define locations of data storage and allows users to access that data
5. Helps administrators and security system to protect the network from data breaches, unauthorized access and attacks on a network
6. Enables network virtualizations

Methods of Network Software

1) Protocol Hierarchies

2) Design issues for the layers

3) Connection-oriented and Connectionless services

4) Service primitives

5) The relationship of services to protocols

1) Protocol Hierarchies

- ✓ Networks are organized as a stack of layers or levels, each one built upon the one below it.
- ✓ The number of layers, the name of each layer, the contents of each layers and the function of each layer differ from network to network.
- ✓ The purpose of each layer is to services to the higher layers.
- ✓ **A protocol is an agreement between the communicating parties on how communication is to proceed**.
  A five-layer network is illustrated:

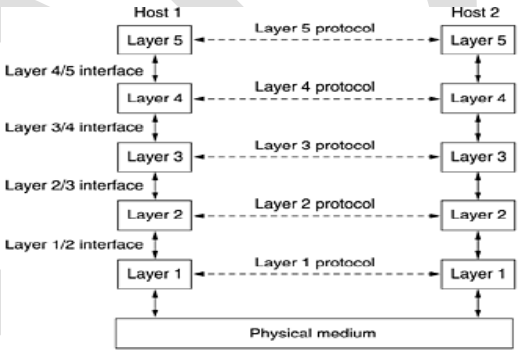


Fig: Layers, protocols, and interfaces

- The entities comprising the corresponding layers on different machines are called peers.
- No data are directly transferred from layer n on one machine to layer n on another machine.
- Each layer passes data and control information to the layer immediately below it, until the lowest layer is reached.
- Below layer is the physical medium through which actual communication occurs.
- Between each pair of adjacent layers is an interface.
- A set of layer and protocols is called a network architecture. A list of protocols used by a certain systems. One protocol per layer is called protocol stack.

2) Design Issues for the layers

- ✓ Design issues that occur in computer networks are present in several layers. Every layer needs a mechanism for identifying senders and receiver. Network has many computers.
- ✓ They have rules for data transfer. In some systems, data only travels in one direction, in others, data can go both ways.
- ✓ Error control is an important issue because physical communication circuits are not perfect. The receiver must have some way of telling the sender which message has been correctly received and which has not.
- ✓ Some kinds of feedback from the receiver to the sender, either directly or indirectly, about the receiver's current situation. This subject called flow control.

3) Connection-oriented and Connectionless services

- ✓ Connection-oriented service is modeled after the telephone system. To talk to someone, you pick up the phone, dial the number, talk and then hang up.
- ✓ To use a connection –oriented network service, the service users first establish a connection, user the connection, and then release the connection.
- ✓ Connection-less service is modeled after the postal system. Each message carries the full destination address, and each one is routed through the system independent of all the others.
- ✓ Each service can be characterized by a quality of service. There are six different types of services are:

	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
	Unreliable connection	Digitized voice
Connection-less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

Fig: Six different types of services

4) Service primitives

A service is specified by a set of primitives available to a user process to access the service. The five service primitives for implementing a simple connection –oriented services are:

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

Fig: Five service primitives for implementing a simple connection-oriented service

These primitive might be used as follows:

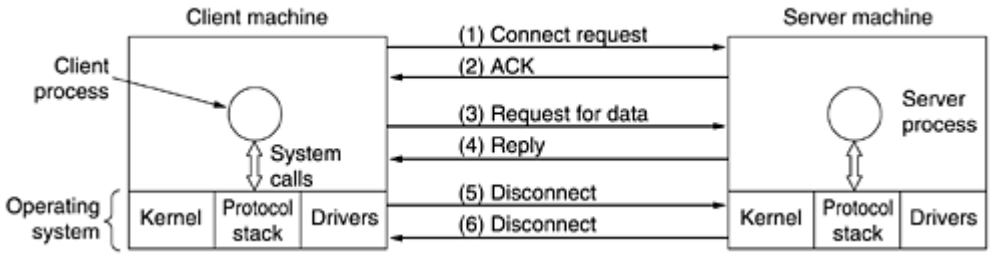


Fig: Packets sent in a simple client-server interaction on a connection-oriented network

- The server executes LISTEN to indicate that it is prepared to accept incoming connections. The connection is to make it a blocking system call.
- The client process executes CONNECT to establish a connection with the server.
- The servers to execute RECEIVE to prepare to accept the first request. The RECEIVE call blocks the server.
- The client machine asks the request for data to the server.
- The server reply the request asks from the client as an acknowledgement.
- SEND is to sends a message from client to server.
- The client sends the DISCONNECT to the server, they reply DICONNECT to client.

5) The relationship of services to protocols

- A service is a set of primitives that a layer provides to the layer above it.
- A Protocol is a set of rules governing the format and meaning of the packets, or messages that are exchanged by the peer entities within a layer.
- Service relate to the interface between layers.
- Protocol relate to the packets send between peer entities on different machines.
- A service is an object-oriented language or an abstract data type.
- A protocol relates to implementation of the service and is not visible to the user of the service.
- Service primitive SEND PACKET with the user providing a pointer to a fully assembled packet.
- All changes to the protocol were immediately visible to the users.

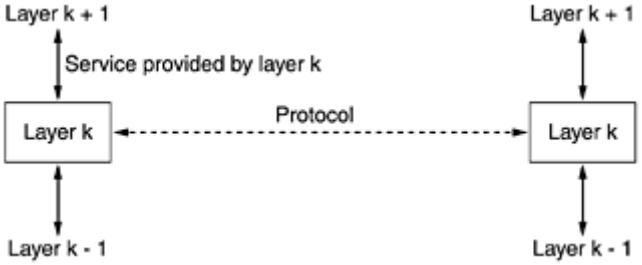


Fig: The relationship between a service and a protocol

Reference Model

In computer networks, reference models give a conceptual framework that standardizes communication between heterogeneous networks.

- ✓ The OSI model is based on a proposed developed by the International Standards Organization (ISO) towards international standardization of the protocols used in the various layers.
- ✓ The model is called ISO- OSI (Open Systems Interconnected) reference model because it deals with connecting open system.

The principles of seven layers are:

1) A layer should be created where a different abstraction is needed.

2) Each layer should perform a well-defined function.

3) The function of each layer should be chosen with an eye.

4) The layer boundaries should be chosen to minimize the information flow across the interfaces.

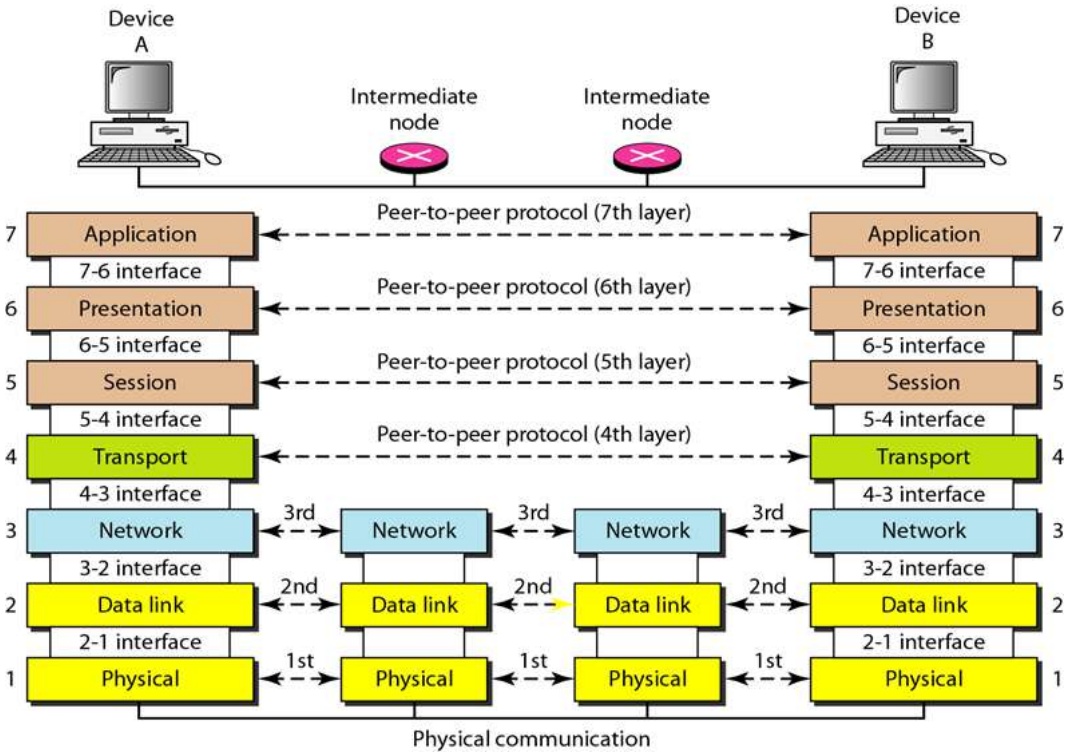
5) The number of layers should be large enough.

The two popular reference models are:

1. OSI Model
2. TCP/IP Protocol Suite

OSI Reference Model

OSI or Open System Interconnection model was developed by International Standards Organization (ISO). It gives a layered networking framework that conceptualizes how communication should be done between heterogeneous systems. It has seven interconnected layers. The seven layers of the OSI Model are a physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer. The hierarchy is depicted in the following figure:



`

Fig. OSI Reference Model

The working of the layer is as follows when the data is send from one device to another on the network. When the formatted data unit passes through the physical layer, it is changed into an electronic signal and transported along a physical link.

1. Physical Layer

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits.** When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

The functions of the physical layer are :

1. **Physical characteristics of interfaces and medium**
   It defines the characteristics of the interface between the devices and transmission medium. It also defines the type of transmission medium.
2. **Representation of bits**
   A stream of bits is encoded into signals. It defines the type of encoding.
3. **Bit synchronization**
   The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
4. **Bit rate control**
   The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
5. **Physical topologies**
   Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topology.
6. **Transmission mode**
   Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.
7. **Line Configuration**
   The connection of devices to the media as point to point or multipoint configuration.

2.Data Link Layer

The data link layer if responsible for moving frames from one hop to the next. Layer is also called as node to node delivery layer. The responsibilities are as follows

1. **Framing**
   The DDL divides the stream of bits received from the network layer into manageable data units called frames.
2. **Physical Addressing**
   It adds a header to the frame to define the sender and\or receiver of the frame.
3. **Flow control**
   The data link layer imposes a flow control mechanism to avoid overflowing the receiver.
4. **Error Control**
   It adds reliability by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames by adding the trailer to the end of the frame.
5. **Access Control**
   It determines which device has control over the link at any given time, when two or more devices are connected to the same link.

3.**Network Layer**

The Network layer is responsible for the delivery of individual packets from the source host to the destination host. The other responsibilities are

1. **Logical Addressing**
   When a packet passes the network boundary, the network layer adds the logical addresses of the sender and receiver.
2. **Routing**
   When independent networks or links are connected to create internetworks, the connecting devices route or switch the packets to their final destination.

4.Transport Layer

The transport layer is responsible for the delivery of a message from one process to another. Also called as end to end delivery layer. Other responsibilities of the transport layer include the following;

1.Serivce-point addressing

The transport layer gets the entire message to the correct process on the destination system by adding a type of address called a service-point address (or port address).

2.Segmentation and reassembly

A message is divided into transmittable segments, with each segment containing a sequence number. These numbers are used to reassemble the message at the destination and to identify and replace packets that were lost in transmission.

3. Connection control

In a connectionless service each segment is treated as independent packet and in connection oriented service each segment is treated as dependent packet. After all the data are transferred, the connection is terminated.

4.Flow control

Flow control is performed from end to end rather than across a single link.

5.Error control

At this layer the error control is performed in a process-to-process rather than across a single link.

5.Session Layer

The session layer is responsible for dialog control and synchronization. Specific responsibilities of the session layer include the following

1. **Dialog Control**
   The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half duplex or full duplex mode.
2. **Synchronisation**
   The session layer allows a process to add checkpoints, or synchronization points, to a stream of data.

6.Presentation Layer

The presentation layer is responsible for translation, compression and encryption. Specific responsibilities of the presentation layer include

1. **Translation**
   The presentation layer is responsible for the interoperability between different encoding methods. It translates from one method to another method of code.
2. **Encryption**
   To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends

the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.

3. **Compression**

   Data compression reduces the number of bits contained in the information. Data compression is important in the transmission of multimedia such as text, audio and video.

7.**Application Layer**

The application layer is responsible for providing services to the user. The layer responsibilities are

1. **Network Virtual Terminal**

   A network virtual terminal is a software version of a physical terminal nad it allows a user to log on to a remote host.

2. **File Transfer, Access and Management**

   This application allows a user to access files in a remote host, to retrieve files from a remote computer for use in the local computer and to manage or control files in a remote computer locally.

3. **Mail Services**

   This application provides the basis for e-mail forwarding and storage.

4. **Directory Services**

   This application provides distributed database sources and access for global information about various objects and services.

GUIDED TRANSMISSION MEDIA

A transmission medium can be broadly defined as anything that can carry information from a source to a destination. In data communications the definition of the information and the transmission medium is more specific.

The transmission medium is usually free space, metallic cable, or fiber-optic cable. The information is usually a signal that is the result of a conversion of data from another form.

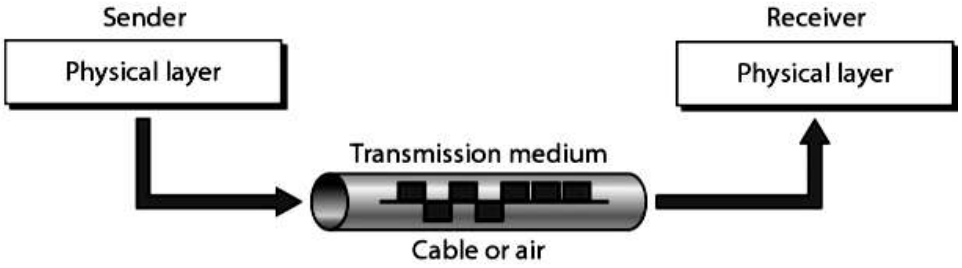
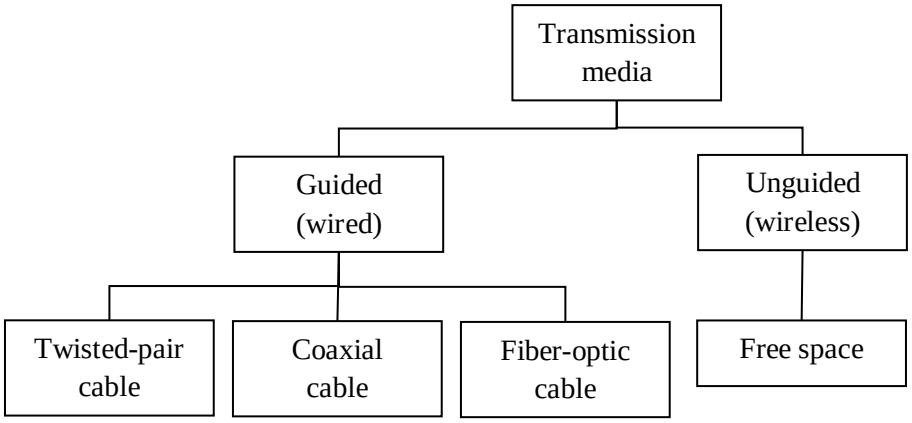


FIGURE TRANSMISSION MEDIUM

Transmission media can be divided into two broad categories: Guided medium and unguided medium.



Guided Media

Guided media provide a conduit from one device to another. A signal traveling along any of these media is directed and contained by the physical limits of the medium.

Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current.

Optical fiber is a cable that accepts and transports signals in the form of light.

1 MAGNETIC MEDIA

The most familiar way of transporting data from one computer to another is to write them onto magnetic tape or removable media and then physically transport the tape or disks to the destination machine, their they can be read them back again.

This method is more cost effective in high bandwidth applications. An industry-standard Ultrium tape can hold 800 gigabytes. A box 60 × 60 × 60 cm can hold about 1000 of these tapes, for a total capacity of 800 terabytes, or 6400 terabits.

2 TWISTED-PAIR CABLE

Twisting makes it probable that both wires are equally affected by external influences. The number of twists per unit of length has some effect on the quality of the cable.

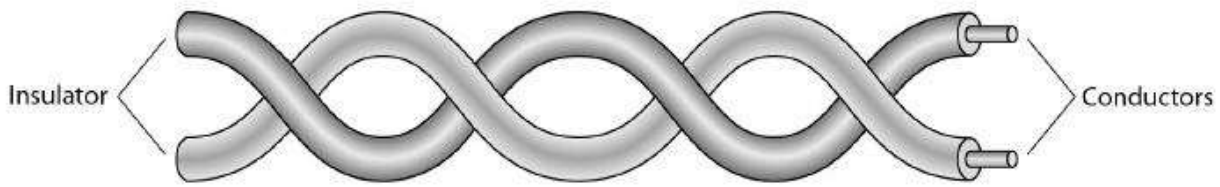


FIGURE TWISTED-PAIR CABLE

Unshielded Versus Shielded Twisted-Pair Cable

The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP). IBM has also produced a version of twisted-pair cable for its use called shielded twisted-pair (STP).

STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors. Metal casing improves the quality of cable by preventing the penetration of noise or crosstalk.

Connectors

The most common UTP connector is RJ45 (RJ stands for registered jack). The RJ45 is a keyed connector, meaning the connector can be inserted in only one way.

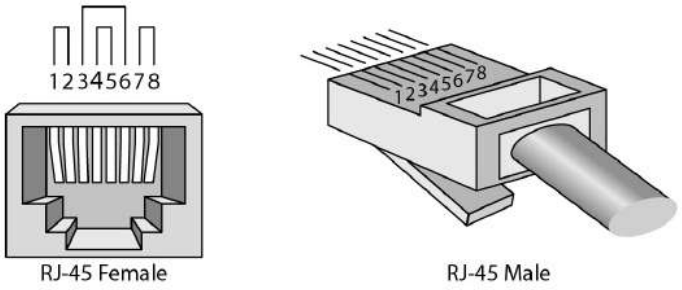


FIGURE UTP CONNECTOR

Applications

a) Twisted-pair cables are used in telephone lines to provide voice and data channels.
b) Local-area networks, such as 10Base-T and 100Base-T, also use twisted-pair cables.

Performance

A twisted-pair cable can pass a wide range of frequencies. With increasing frequency, the attenuation, measured in decibels per kilometer (dB/km), sharply increases with frequencies above 100 kHz which is described in figure 2.8. Gauge is a measure of the thickness of the wire.

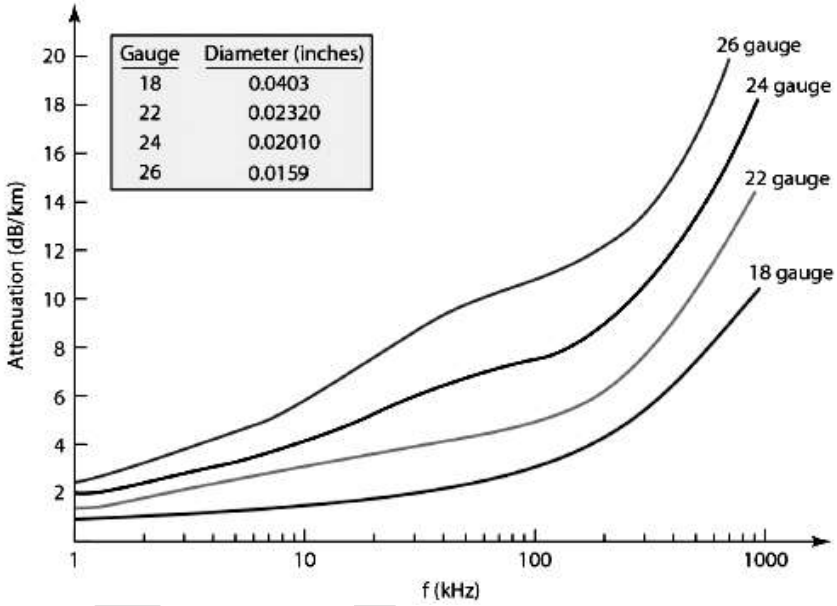


FIGURE UTP CABLE - PERFORMANCE

3 COAXIAL CABLE

Coaxial cable carries signals of higher frequency ranges. Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two.

The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit.

This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.

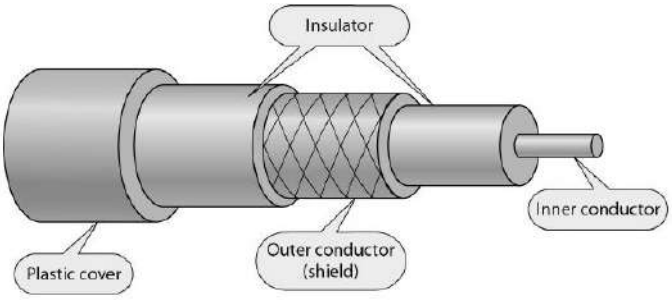


FIGURE COAXIAL CABLE

Coaxial Cable Standards

Coaxial cables are categorized by their radio government (RG) ratings. Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and type of the inner insulator,

the construction of the shield, and the size and type of the outer casing. Each cable defined by an RG rating is adapted for a specialized function.

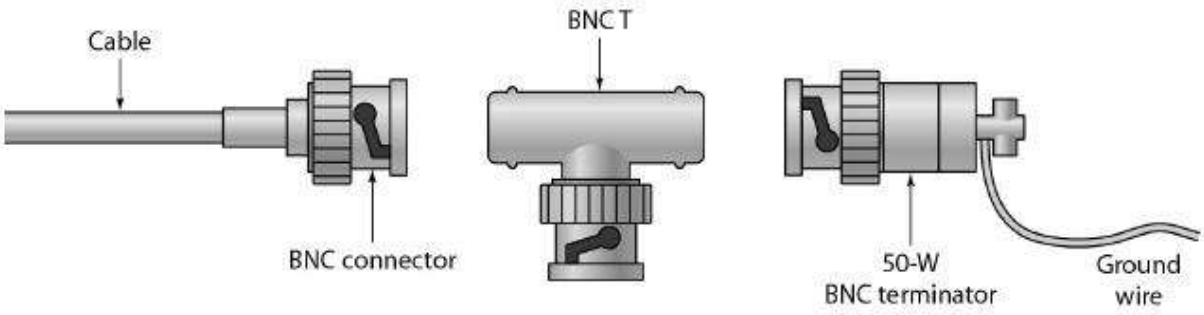
Category	Impedance	Use
RG – 59	75Ω	Cable TV
RG – 58	50Ω	Thin Ethernet
RG – 11	50Ω	Thick Ethernet

TABLE CATEGORIES OF COAXIAL CABLES

Coaxial Cable Connectors

To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayone-Neill-Concelman (BNe) connector. Three popular types of connectors:

a) **BNC connector** - used to connect the end of the cable to a device, such as a TV set.
b) **BNC T connector** - The BNC T connector is used in Ethernet networks to branch out a connection to a computer or other device
c) **BNC terminator** - The BNC terminator is used at the end of the cable to prevent the reflection of the signal.



(a) BNC Connector (b) BNCT Connector (c) BNC Terminator

FIGURE .BNC CONNECTORS

Applications of the coaxial cable

a) Cable TV
b) Telecommunication
c) Traditional Ethernet LANs

Performance of the coaxial cable

The attenuation is much higher in coaxial cables than in twisted-pair cable. Although coaxial cable has a much higher bandwidth, the signal weakens rapidly and requires the frequent use of repeaters.

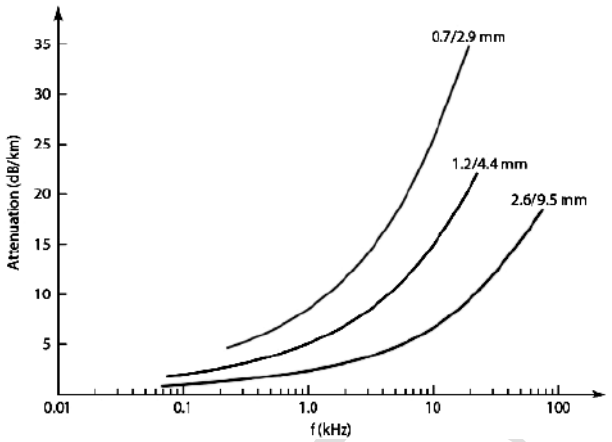
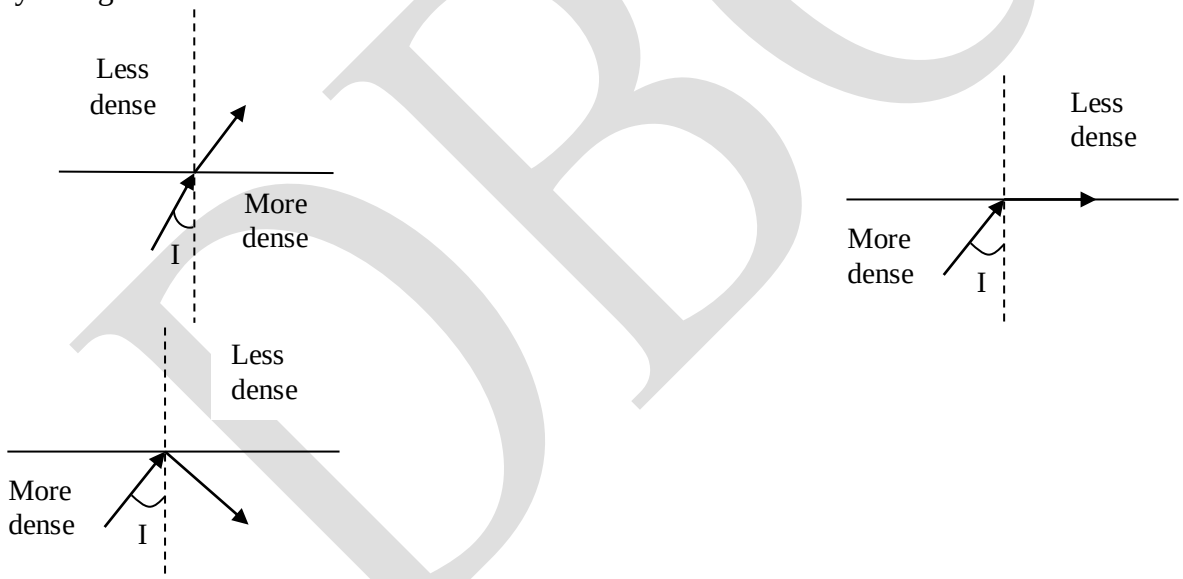


FIGURE. PERFORMANCE OF THE COAXIAL CABLE

4. FIBER-OPTIC CABLE

`A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. Light travels in a straight line as long as it is moving through a single uniform substance.

If a ray of light traveling through one substance suddenly enters another substance the ray changes direction.



I < Critical angle, refraction I = Critical angle, refraction I > Critical angle, refraction

FIGURE BENDING OF LIGHT RAY

Bending Of Light

a) If the angle of incidence is less than the critical angle, the ray refracts and moves closer to the surface.
b) If the angle of incidence is equal to the critical angle, the light bends along the interface.
c) If the angle of incidence is greater than the critical angle, the ray reflects and travels again in the denser substance.

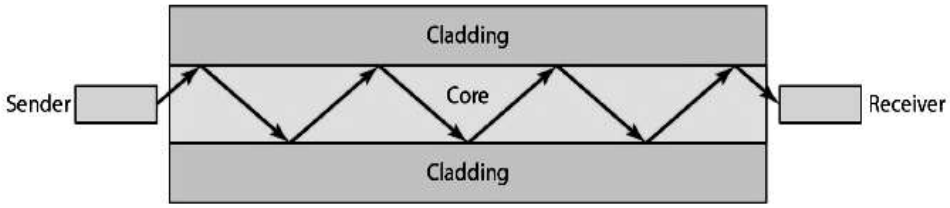
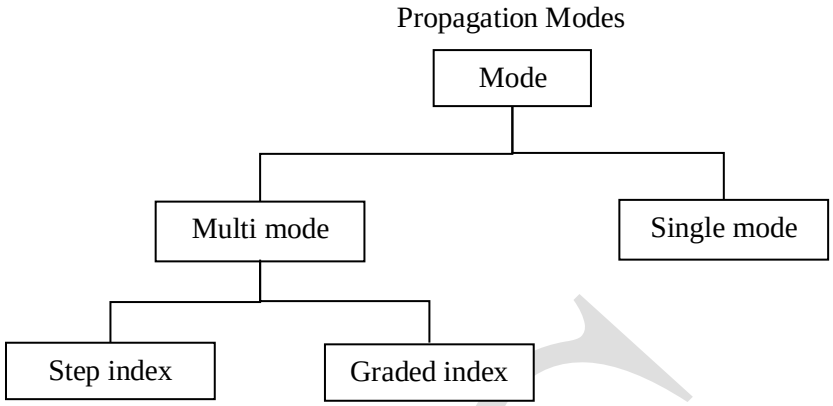


FIGURE. OPTICAL FIBER

Propagation modes

If the angle of incidence is less than the critical angle, the ray refracts and moves closer to the surface.



(i) **Multimode fiber:** Multiple beams from a light source move through the core in different paths. Multimode can be implemented in two forms step-index and graded-index.

(a) ***Multimode step-index fiber:***

(b) ***Multimode graded-index fiber***

(ii) **Single mode:** Single-mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal. The single mode fiber itself is manufactured with a much smaller diameter than that of multimode fiber.

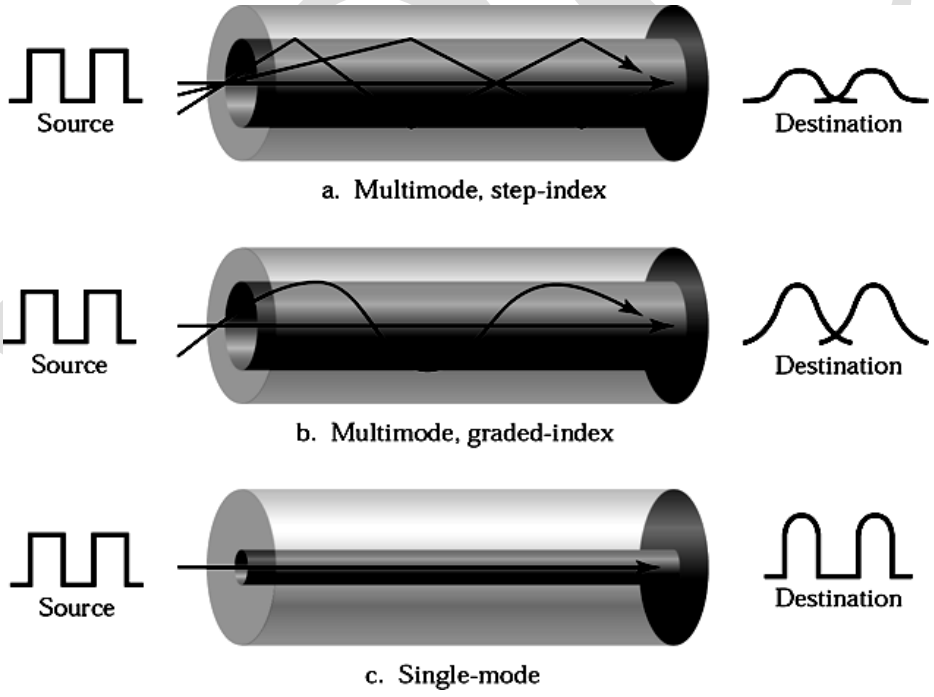


FIGURE. OPTICAL FIBER- PROPAGATION MODES

. The fiber is at the center of the cable, and it consists of cladding and core.

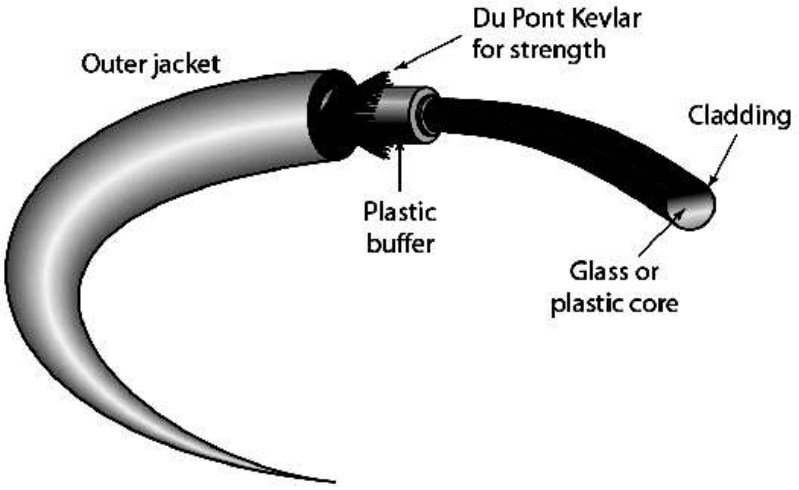


FIGURE. FIBER CONSTRUCTION

Fiber-Optic Cable Connectors

a) The subscriber channel (SC) connector is used for cable TV. It uses a push/pull locking system.
b) The straight-tip (ST) connector is used for connecting cable to networking devices. It uses a bayonet locking system. It is more reliable than SC.
c) MT-RJ is a connector that is the same size as RJ45, used in fast Ethernet

Advantages of Optical Fiber

a) Higher bandwidth
b) Less signal attenuation
c) Immunity to electromagnetic interference
d) Resistance to corrosive materials
e) Light weight
f) Greater immunity to tapping

Disadvantages

a) Installation and maintenance
b) Unidirectional light propagation
C) Cost

WIRELESS TRANSMISSION (Unguided Media)

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication.

Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.

The part of the electromagnetic spectrum, ranging from 3 kHz to 900 THz, is used for wireless communication. Unguided signals can travel from the source to destination in several ways;

i) **Ground propagation:** Radio waves travel through the lowest portion of the atmosphere.
ii) S**ky propagation:** Higher frequency radio waves radiate upward into the ionosphere and they are reflected back to earth.
iii) L**ine-of-sight propagation:** Very high frequency signals are transmitted in straight lines directly from antenna to antenna

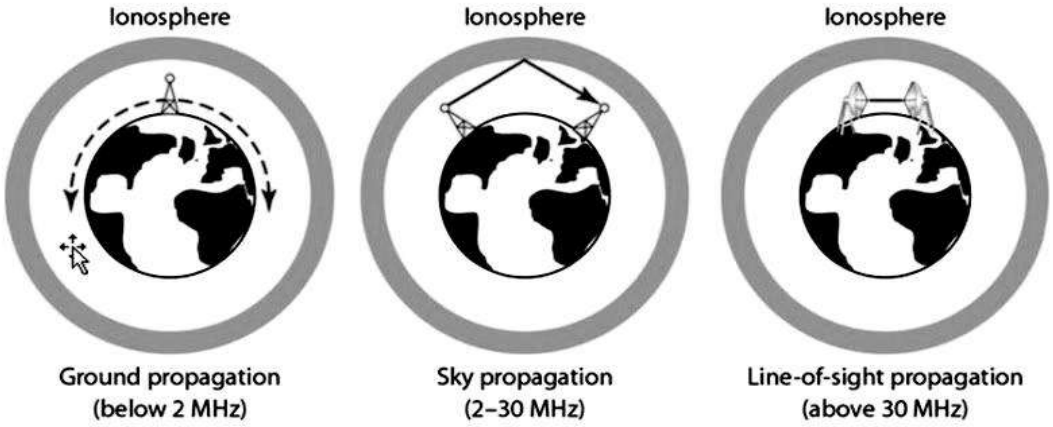


FIGURE 1 TRAVELLING MODES OF WIRELESS SIGNALS

We can divide wireless transmission into 3 broad groups. They are,

i) The electromagnetic spectrum
ii) Radio transmission
ii) Microwave transmission
iii) Infrared transmission
iv) Light transmission

1 THE ELECTROMAGNETIC SPECTRUM

When electrons move, they create electromagnetic waves that can propagate through space. The number of oscillations per second of a wave is called its **frequency (f)** and is measured in **Hz**.

The distance between two consecutive maxima or minima is called the **wavelength (λ)** and it is measured in meters. .

In a vacuum, all electromagnetic waves travel at the same speed regardless of their frequency. This speed is called the **speed of light (*c*)** and it is approximately 3 × 108 m/sec.

In copper or fiber the speed slows to about 2/3 of this value and becomes slightly frequency dependent. No object or signal can ever move faster than light. The fundamental relation between *f*, λ, and *c* (in a vacuum) is

$$\lambda f = c$$

When λ is in meters and *f* is in MHz then

$$\lambda f \approx 300$$

The electromagnetic spectrum is shown in figure 2. The radio, microwave, infrared, and visible light portions of the spectrum can all be used for transmitting information by modulating the amplitude, frequency, or phase of the waves. Ultraviolet light, X-rays, and gamma rays would be even better, due to their higher frequencies.

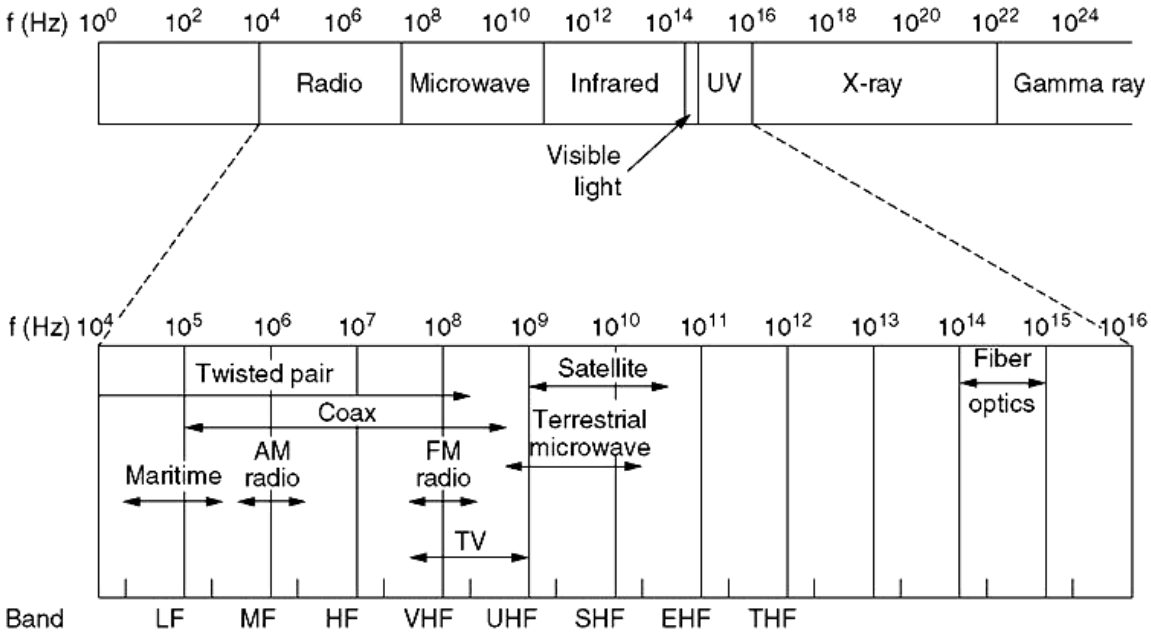


FIGURE 2 THE ELECTROMAGNETIC SPECTRUM

The bands listed at the bottom of figure 2 are the official ITU names and are based on the wavelengths. Here, the LF band goes from 1 km to 10 km.

terms LF, MF, and HF refer to Low, Medium, and High Frequency, respectively. The amount of information that an electromagnetic wave can carry depends on the received power and is proportional to its bandwidth.

In some applications, a wider band is used with three variations namely

i. Frequency hopping spread spectrum

The transmitter hops from frequency to frequency hundreds of times per second. It is popular for military communication. It also offers good resistance to multipath fading and narrowband interference.

This technique is used in Bluetooth and older versions of 802.11.

ii. Direct sequence spread spectrum

It uses a code sequence to spread the data signal over a wider frequency band. These signals can be given different codes by using a method called ***CDMA (Code Division Multiple Access)***. This method forms the basis of ***3G mobile phone networks*** and is also used in ***GPS (Global Positioning System)***.

iii. Ultra-Wideband communication (UWB)

UWB sends a series of rapid pulses, varying their positions to communicate information. The rapid transitions lead to a signal that is spread thinly over a very wide frequency band.

UWB is defined as signals with a bandwidth of at least 500 MHz or at least 20% of the center frequency of their frequency band.

2 RADIO TRANSMISSION

Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves. They are omnidirectional.

When an antenna transmits radio waves, they are propagated in all directions, means that the sending and receiving antennas do not have to be aligned.

A sending antenna sends waves that can be received by any receiving antenna. Radio waves with low and medium frequencies can penetrate walls. Radio waves are used for multi-communication (TV, radio, paging systems).

Disadvantages of Radio waves

a) Penetrate the walls
b) Omnidirectional

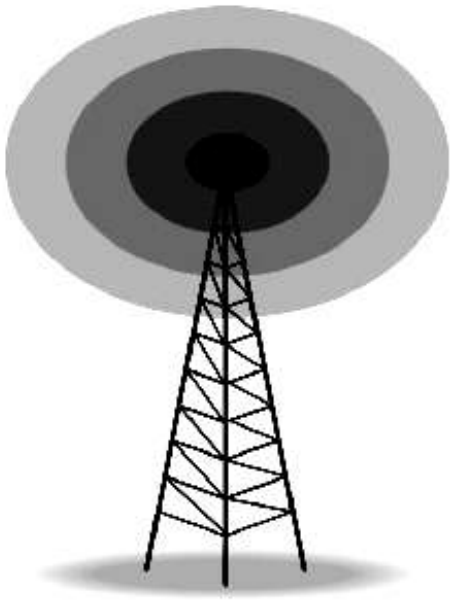


FIGURE. OMNIDIRECTIONAL ANTENNA

3 MICROWAVE TRANSMISSION

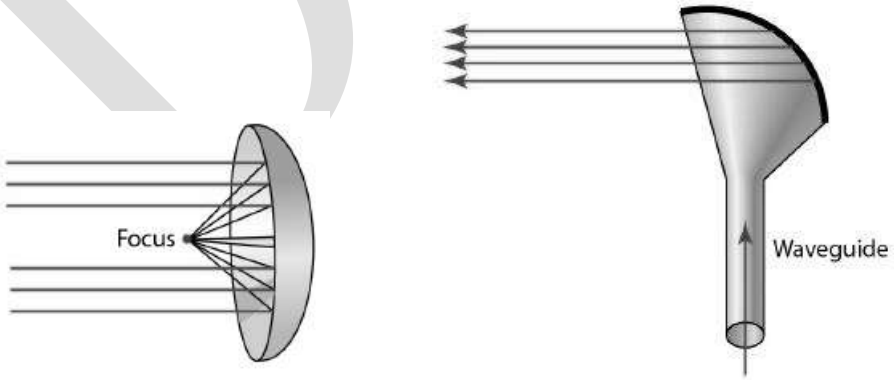
Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves. Microwaves are unidirectional Microwave propagation is line-of-sight

Use of certain portions of the band requires permission from authorities. Microwaves are using 2 types of antennas, they are

i) ***The parabolic dish****:* The parabolic dish focuses all incoming waves into a single point.
ii) ***The horn:*** A horn antenna looks like a gigantic scoop. Outgoing transmissions are broadcast up a stem and deflected outward in a series of narrow parallel beams by the curved head.

Applications

a) Cellular telephones
b) Satellite n/w
c) WLAN's



(a) Dish antenna (b) Horn antenna

FIGURE UNIDIRECTIONAL ANTENNAS

4 INFRARED TRANSMISSION

Infrared waves are having the frequencies from 300 GHz to 400 THz. Since, Infrared waves having high frequencies they cannot penetrate walls.

Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation. Unguided infrared waves are widely used for short-range communication.

The remote controls used for televisions, VCRs, and stereos all use infrared communication.

They are relatively directional, cheap and easy to build. The major drawback of a infrared waves is that they do not pass through solid objects.

Due to this property, an infrared system in one room of a building will not interfere with a similar system in adjacent rooms or buildings.

The security features of infrared system are better than that of radio systems.

5 LIGHT TRANSMISSION

A modern application is to connect the LANs in two buildings via lasers mounted on their rooftops. So each building needs its own laser and its own photo detector.

Lasers are unidirectional with high bandwidth and low cost. It is also easy to install and does not require an FCC (Federal Communications Commission) license.

The laser's strength a very narrow beam is its weakness but 1mm wide beam at a target 1mm wide 500 meters away requires.

A disadvantage is that laser beams cannot penetrate rain or thick fog, but they normally work well on sunny days.

Convection currents can interfere with laser communication systems. A bidirectional system with two lasers is shown in figure 2.20.

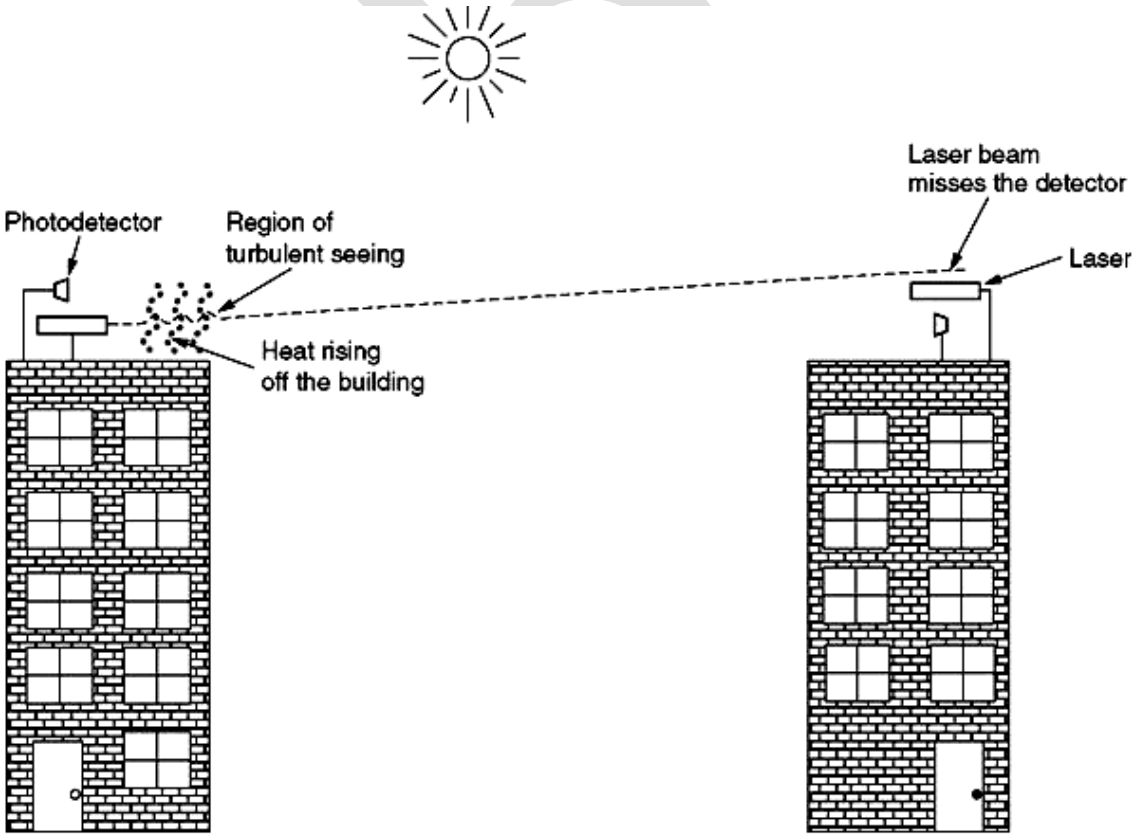


FIGURE A BIDIRECTIONAL SYSTEM WITH TWO LASERS

Differences between the guided and unguided media

Guided media	Unguided media
Signal energy propagates within the guided media	Signal energy propagates through air
Suitable for point-to-point communication	Suitable for broadcasting
Signals appears in the form of voltage	Signals appears in the form of electromagnetic waves
Ex: Twisted pair, Co-axial, Fiber optics	Ex: Radio wave, Micro wave, Infrared

PUBLIC SWITCHED TELEPHONE NETWORK

The ***PSTN (Public Switched Telephone Network)*** was designed for transmitting the human voice in a more-or-less recognizable form. The PSTN is highly suitable for computer-computer communication.

- ✓ When the distances are large or there are many computers on the cables have to pass through a public road or other public right of way, the costs of running private cables are usually prohibitive.
- ✓ The network designers must rely on the existing telecommunication facilities. These facilities especially the PSTN (Public Switched Telephone Network).

1.STRUCTURE OF THE TELEPHONE SYSTEMS

- ✓ If the telephone owner wanted to talk to a other telephone owners, separate wires had to be string to all n houses.
- ✓ Within a year, the cities were covered with wires passing over houses and trees in a wild jumble.
- ✓ It became immediately obvious that the model of connecting every telephone to every other telephone, as shown (Fig: a) was not going to work.

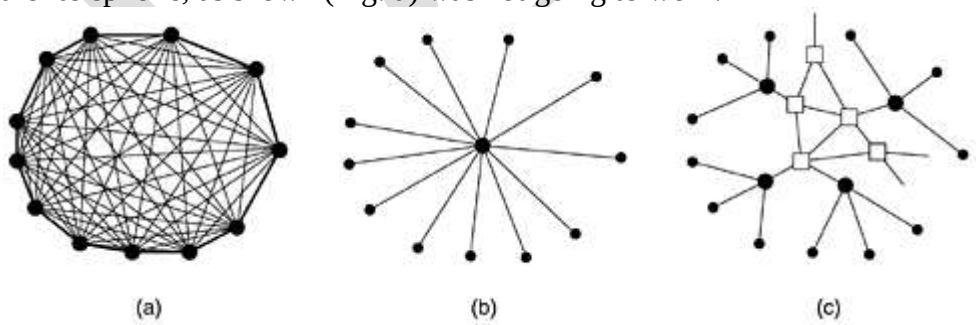


Fig: (a) Fully-interconnected network. (b) Centralized switch. (c) Two-level hierarchy

- ✓ To make a call, the customer would crank the phone to make a ringing sound in the telephone company office to attract the attention of an operator,
- ✓ The switching offices were singing up everywhere and people wanted to make long-distance calls between cities, begin to connect the switching offices.
- ✓ To connect every switching office to every other switching office by means of a wire between them quickly became unmanageable, so second-level switching offices were invented.

- ✓ After a while multiple second-level offices were needed as illustrated (Fig: c).
- ✓ The three major parts of the telephone system were in place: the switching offices, the wires between the customers and the switching offices and the long-distance connection between the switching offices.
- ✓ Each telephone has two copper wires coming out of it that go directly to the telephone company's nearest end office
- ✓ The distance is typically 1 to 10 km, being shorter in cities than in rural areas. The two-wire connections between each subscriber's telephone and the end office are known in the trade as the local loop.
- ✓ If a subscriber attached to a given end office call another subscriber attached to the same end office, the switching mechanism between the two local loops. This connection remains intact for the duration of the call.
- ✓ A telephone network consists only of telephones, end offices and toll offices as shown:

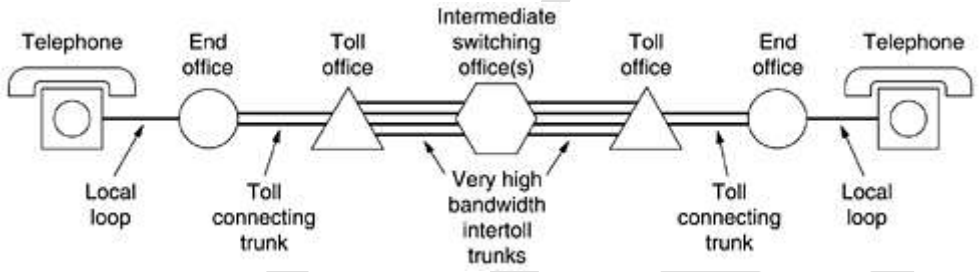


Fig: A typical circuit route for a medium-distance call

- ✓ If the caller and callee do not have a toll office in common, the path will have to be established somewhere higher up in the hierarchy.
- ✓ Primary, sectional and regional exchanges communicate with each other via high bandwidth inter toll trunks (also called inter office trunks).
- ✓ The number of different kinds of switching centers and their topology.

The telephone system consists of three major components:

1. Local loops (analog twisted pairs going into houses and business)

2. Trunks (digital fiber optics connecting the switching offices)

3. Switching offices (where calls are moved from one trunk to another)

2. MODEM

- ✓ The square waves used in digital signals have a wide frequency spectrum and subject to strong attenuation and delay distortion.
- ✓ These effects make base band (DC) signaling unsuitable except at slow speeds and over short distances.
- ✓ To get around the problems associated with DC signaling, especially on telephone lines, AC signaling is used.
- ✓ A continuous tone in the 1000 to 2000 Hz range called a sine wave carrier is introduced.
- ✓ Its amplitude, frequency, or phase can be modulated to transmit information.

- ✓ In amplitude modulation, two different amplitudes are to represent 0 and 1 respectively.
- ✓ In frequency modulation, also known as frequency shift keying, two (or more) different tones are used.
- ✓ In the simplest form of phase modulation, the carrier wave is systematically shifted 0 or 180 degrees at uniformly speed intervals.
- ✓ A better scheme is to use shifts of 45, 135, 225 or 315 degrees to transmit 2 bits of information per time interval.

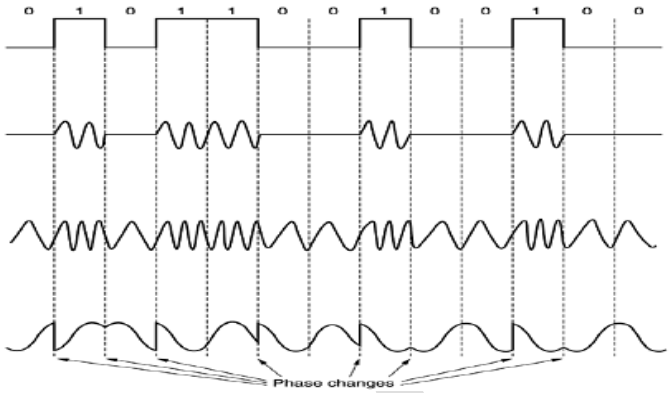


Fig: (a) A binary signal. (b) Amplitude modulation. (c) Frequency modulation. (d) Phase modulation

A device that accepts a serial stream of bits as input and produces a carrier modulated by one of these methods is called a modem (for modulation – demodulation).

- ✓ The modem is inserted between the (digital) computer and the (analog) telephone system.
- ✓ All modern modems allow traffic in both directions at the same time. A connection that allows traffic in both directions simultaneously is called full duplex.
- ✓ A two-lane road is full duplex.
- ✓ A connection that allows traffic either way, but only one way at a time is called half duplex. A connection that allows traffic only one way is called simplex. A one-way street is simplex.

3. TRUNKS AND MULTIPLEXING

- ✓ To install and maintain a high-bandwidth trunk as a low-bandwidth trunk between two switching offices.
- ✓ Telephone companies have developed elaborate schemes for multiplexing many conversations over a single physical trunk.
- ✓ These multiplexing schemes can be divided into two basic categories:
    1. FDM (Frequency Division Multiplexing)
    2. TDM (Time Division Multiplexing)
    3. WDM(Wave Division Multiplexing)
- ✓ In FDM, the frequency spectrum is divided into frequency bands, with each user having exclusive possession of some band.
- ✓ In TDM, the users take turns, each one periodically getting the entire bandwidth for a little burst of time.

1.Frequency Division Multiplexing

- ✓ The three voice-grade telephone channels are multiplexed using FDM. Filters limit the usable bandwidth to about 3100 Hz per voice-grade channel.

- ✓ When many channels are multiplexed together, 4000 Hz is allocated to each channel to keep them well separated.
- ✓ First the voice channels are raised in frequency, each by a different amount.
- ✓ Then they can be combined because no two channels now occupy the same portion of the spectrum.
- ✓ There are gaps between the channels, there is some overlap between adjacent channels because the filters do not have sharp edges.
- ✓ This overlaps means that a strong spike at the edge of one channel will be felt in the adjacent one as non-thermal noise.

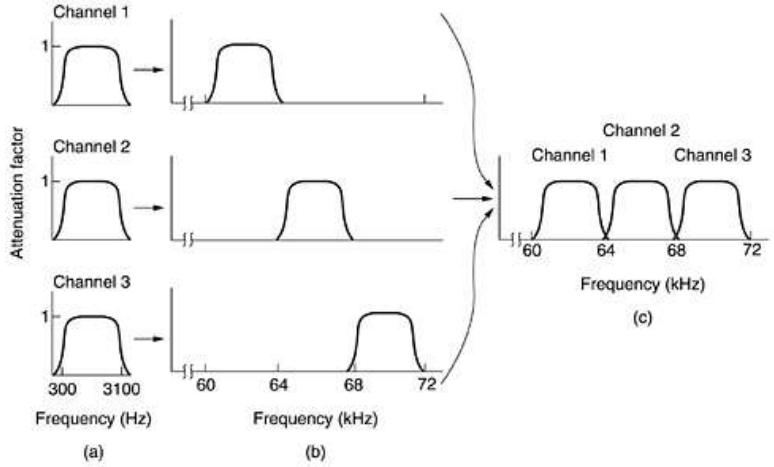


Fig: Frequency division multiplexing.

(a) The original bandwidths. (b) The bandwidths raised in frequency. (c) The multiplexed channel

- ✓ A widespread standard is twelve 4000-Hz voice channels multiplexed into the 60 to 108 KHz band. This unit is called a group.
- ✓ Five groups can be multiplexed to form a super group. The next unit is the master group, which are five super groups or ten super groups.

2.Wavelength Division Multiplexing

- ✓ For fiber optic channels, a variation of frequency division multiplexing is used. It is called WDM (Wavelength Division Multiplexing).
- ✓ Four fibers come together at an optical combiner, each with its energy present at a different wavelength.
- ✓ The four beams are combined onto a single shared fiber for transmission to a distant destination.
- ✓ At the far end, the beam is split up over a many fibers as there were on the input side.
- ✓ Each output fiber contains a short, specially constructed core that filters out all but one wavelength.
- ✓ The resulting signals can be routed to their destination or recombined in different ways for additional multiplexed transport.

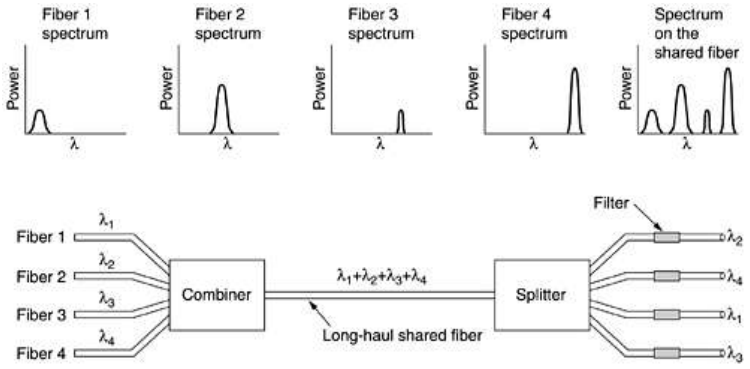


Fig: Wavelength division multiplexing

- ✓ As long as each channel has its own frequency range and all the ranges and disjoint, they can be multiplexed together on the long haul fiber.
- ✓ The only difference with electrical FDM is that an optical system using a diffraction grating is completely passive and thus highly reliable.

3. Time Division Multiplexing

- ✓ TDM can be handled entirely by digital electronics. It can only be used for digital data.
- ✓ The local loops produce analog signal a conversion is needed from analog to digital in the end office, where all the individual local loops come together to be combined onto outgoing trunks.
- ✓ How multiple analog voice signals are digitalized and combined onto a single outgoing digital analog.
- ✓ The analog signals are digitalized in the end office by a device called codec (coder-decoder).
- ✓ At a lower sampling rate, information would be lost, at a higher one, no extra information would be gained. This technique is called PCM (Pulse Code Modulation).

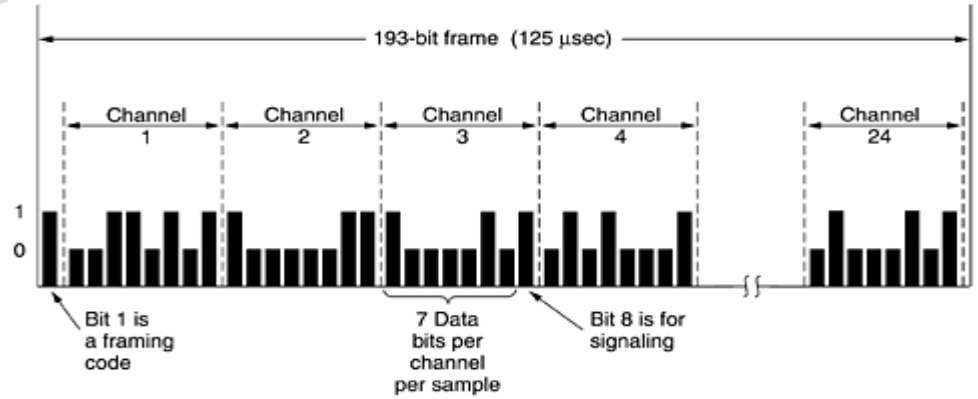


Fig: The T1 carrier (1.544 Mbps).

- ✓ The T1 carrier consists of 24 voice channels multiplexed together.
- ✓ The analog signals are sampled on a round-robin basis with the resulting analog stream being fed to the codec rather than having 24 separate codec and then merging the digital output.
- ✓ Each of the 24 channels, in turn gets to insert 8 bits into output stream.
- ✓ Seven bits are data and one is for control yielding 7*8000=56,000 bps of data, and 1*8000=8000 bps of signaling information per channel.

- ✓ A frame consists of 24*8=192 bits plus one extra bit for framing, yielding 193 bits every 125 □sec. This gives a gross data rate of 1.544 mbps. The 193rd bit is used for frame synchronization.

4. SWITCHING

The phone system is divided into two parts:

1. Outside plant (the local loops and trunks, since they are physically outside the switching office)
2. Inside plant (the switches), which are inside the switching offices.

The different switching techniques are:

1) Circuit Switching

2) Message Switching

3) packet switching.

1) Circuit Switching

When the computer places a telephone call, the switching equipment within the telephone system seeks out a physical path all the way from your telephone to the receiver's telephone. This technique is called Circuit Switching.

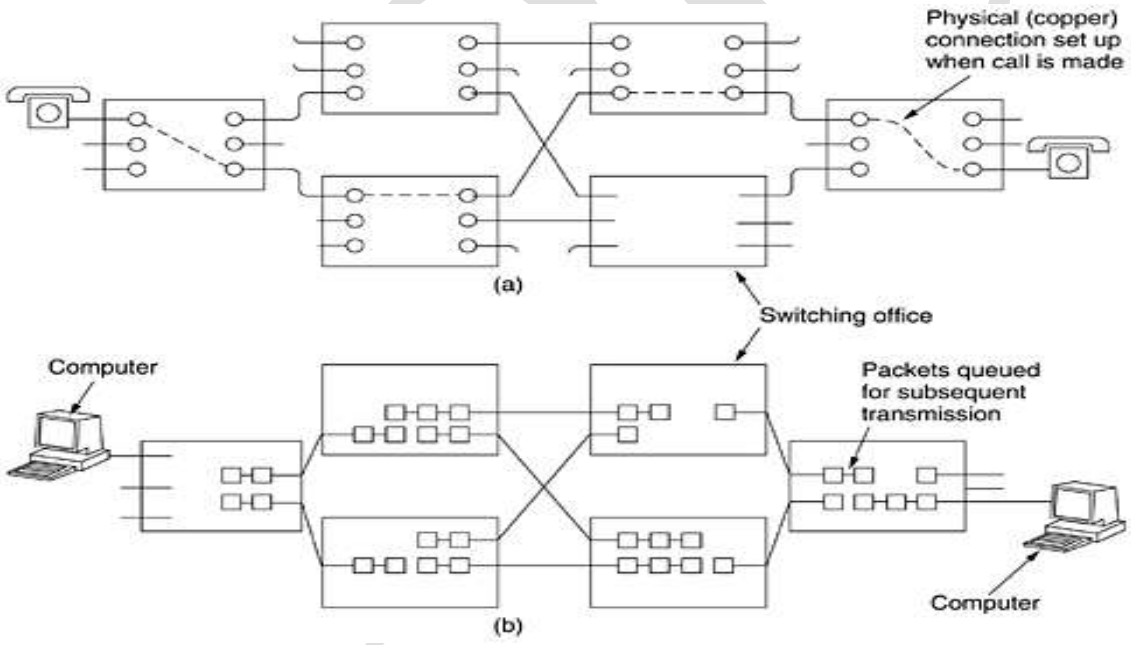


Fig: (a) Circuit switching. (b) Packet switching

- ✓ Each of the six rectangles represents a carrier switching office (end office, toll office, etc.).
- ✓ Each office has three incoming lines and three outgoing lines.
- ✓ When a call passes through a switching office, a physical connection is established between the line on which the call came in and one of the output links as shown by the dotted lines.
- ✓ The alternative to circuit switching is packet switching as shown fig(b).
- ✓ Individual packets are sent as need be, with no dedicated path being set up in advance.
- ✓ It is up to each packet to find its way to the destination on its own.

- ✓ An important property of circuit switching is needed to set up an end-to-end path before any data can be sent.
- ✓ The elapsed time between the end of dialing and the start of ringing can easily be 10 sec, more on long-distance or international calls.

2.Message Switching

When this form of switching is used, no physical path is established in advance between sender and receiver. Instead, when the sender has a block of data to be sent,

it is stored in the first switching office (i.e., router) and then forwarded later, one hop at a time. Each block is received in its entirely inspected for error, and then retransmitted.

A network using this technique is called a store-and –forward network.

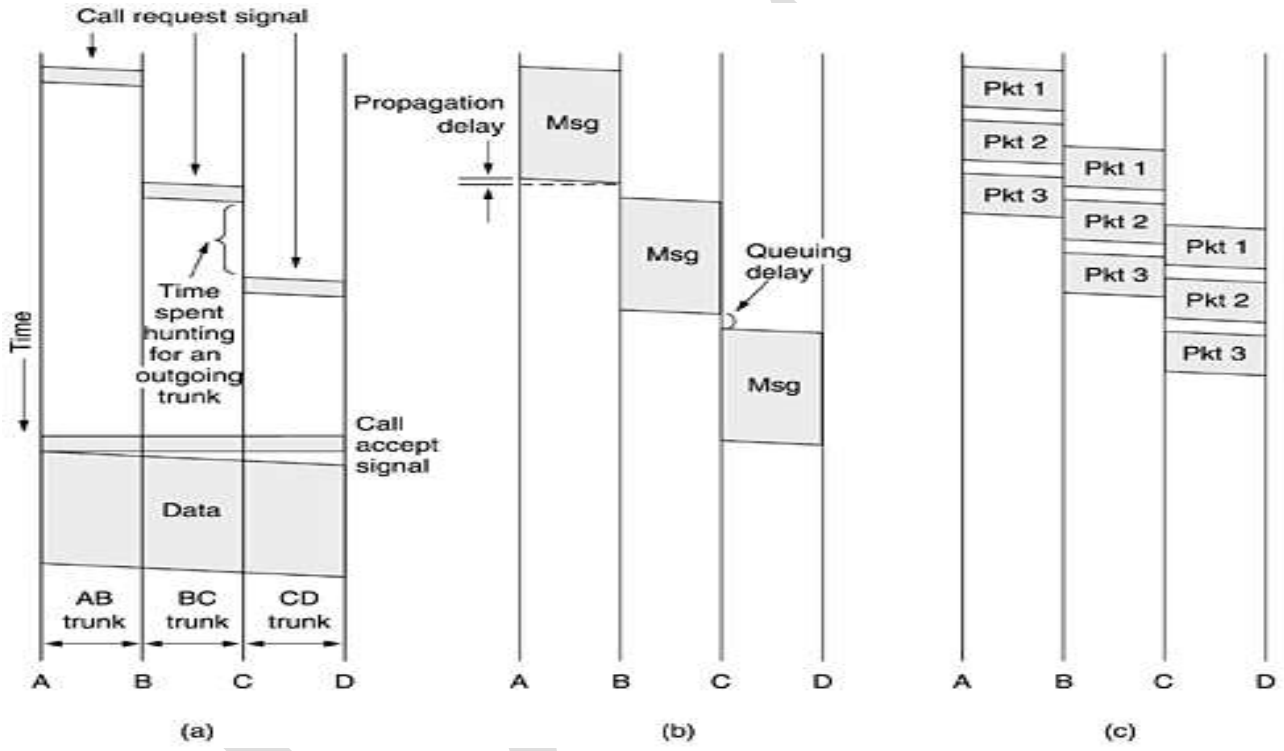


Fig: Timing of events in (a) circuit switching, (b) message switching, (c) packet switching

3.Packet Switching

- ✓ With message switching there is no limit at all on block size, which means that routers must have disks to buffer long blocks.
- ✓ It also means that a single block can tie up a router – router line for minutes, rendering message switching useless for interactive traffic.
- ✓ The packet switching was invented packet-switching networks place a tight upper limit on block size, allowing packets to be buffered in router main memory instead of m disk.
- ✓ The packet switching over message switching as shown fig b and fig c.
- ✓ The first packet of a multi-packet message can be forwarded before the second one has fully arrived, reducing delay and improving throughput.
- ✓ Computer networks are usually packet switched, occasionally circuit switched, put never message switched.

Difference between circuit switching and packet switching

Item	Circuit switching	Packet switching
Call setup	required	Not needed
Dedicated physical path	Yes	No
Each packet follows the same route	Yes	No
Packets arrives in order	Yes	No
Is a switch crash fatal	Yes	No
Bandwidth available	fixed	Dynamic
Time of possible congestion	At setup time	On every packet
Potentially wasted bandwidth	Yes	No
Store-and-forward transmission	No	Yes
Transparency	Yes	No
Charging	Per minute	Per packet

THE MOBILE TELEPHONE SYSTEM

The mobile phone system is used for wide area voice and data communication. Cellular network or telephony is a ***radio-based technology***.

The radio waves are electromagnetic waves propagated by ***antennas.*** Most signals are in the 850 MHz, 900 MHz, 1800 MHz, and 1900 MHz frequency bands. Mobile phones are sometimes called as ***cell phones*** which have gone through five distinct generations. They are;

- 1G (First Generation) − They were standards for analog voice mobile phone communications.
- 2G (Second Generation) − They were standards for digital voice mobile phone communications.
- 3G (Third Generation) − These standards were for communications in form of both digital voice as well as digital data.
- 4G (Fourth Generation) − 4G standards provide mobile broadband internet access in addition to digital voice and data.
- 5G (Fifth Generation) − It is the next step of mobile communication standards beyond 4G which currently under development.

1. FIRST-GENERATION (1G) MOBILE PHONES: ANALOG VOICE

Mobile radiotelephones were used periodically for maritime and military communication during the early decades of the 20th century. In 1946, the car-based telephones were introduced.

This system used a single large transmitter and had a single channel, used for both sending and receiving. To talk, the user had to push a button that enabled the transmitter and disabled the receiver. Such systems are known as ***push-to-talk systems***.

In the 1960s, ***IMTS (Improved Mobile Telephone System)*** was installed. It used a high powered (200-watt) transmitter and had two frequencies, one for sending and one for receiving. , Thus the push-to-talk button was replaced by IMTS. IMTS supported 23 channels spread out from 150 MHz to 450 MHz.

Advanced Mobile Phone System

In 1982, ***AMPS (Advanced Mobile Phone System)*** was invented by Bell Labs and first installed in the United States. In all mobile phone systems, a geographic region is divided up into **cells** with an ***antenna*** control by a cell office in each cell.

The idea of frequency reuse is illustrated in figure 5. In figure 5, the cells are all the same size and they are grouped in units of seven cells.

Each letter indicates a group of frequencies and for each frequency set there is a buffer about two cells wide where that frequency is not reused. This will provide a good separation and low interference.

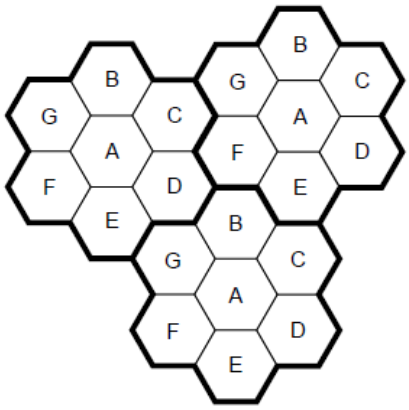


FIGURE 5 FREQUENCIES ARE NOT REUSED IN ADJACENT CELLS

When the number of users has grown then the system may get overloaded. At this point the power can be reduced and the overloaded cells will split into smaller ***microcells*** to permit more frequency reuse, as shown in figure 6.

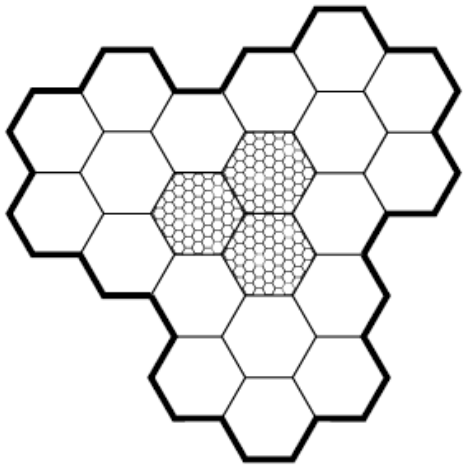


FIGURE 6 SMALLER CELLS WITH MORE USERS

At the center of each cell is a base station to which all the telephones in the cell transmit. The base station consists of a computer and transmitter/receiver connected to an antenna. In a small system, all the base stations are connected to a single device called an ***MSC (Mobile Switching Center)*** *or* ***MTSO (MobileTelephone Switching Office)***. In a larger

one, several MSCs may be needed and all of which are connected to a second-level MSC, and so on.

Handoff

the telephone is informed of its new boss and if a call is in progress, it will be asked to switch to a new channel. This process is called a ***handoff*** and it takes about 300 msec. Here, the channel assignment is done by the MSC.

Channels

AMPS use FDM to separate the channels. The system uses 832 full-duplex channels, each consisting of a pair of simplex channels. This arrangement is known as ***FDD (Frequency Division Duplex)***.

The 832 channels are divided into four categories namely;

a) ***Control channels*** (base to mobile) are used to manage the system
b) ***Paging channels*** (base to mobile) are used to alert mobile users to calls for them
c) ***Access channels*** (bidirectional) are used for call setup and channel assignment
d) ***Data channels*** (bidirectional) are used to carry voice, fax, or data.

Call Management

Each mobile telephone in AMPS has a ***32-bit serial number*** and a ***10-digit telephone number*** in its programmable read-only memory. The telephone number is represented as a 3-digit area code in 10 bits and a 7-digit subscriber number in 24 bits.

When a phone is switched on, it scans a preprogrammed list of 21 control channels to find the most powerful signal. The phone then broadcasts its 32-bit serial number and 34-bit telephone number.

In AMPS, this packet is sent multiple times in digital form with an error-correcting code.

2.SECOND-GENERATION (2G) MOBILE PHONES: DIGITAL VOICE

2G is the Second-Generation wireless cell phones, based on digital technologies and in early 1990's. 2G provided services such as text message, picture messages and MMS.

2G has greater security for both sender and receiver. All text messages are digitally encrypted, which allows for the transfer of data in such a way that only intended receiver can receive and read it.

2G system uses digital mobile access technology such as ***TDMA and CDMA***. TDMA divides signal in time slots while as CDMA allocates each user a special code to communicate over a multiplex physical channel. An example for different TDMA technologies is ***GSM, PDC, iDEN and iS-136***. GSM was first 2G System. An example for CDMA technology is ***IS-95.***

Several digital systems were developed, and three have been widely deployed. ***DAMPS (Digital Advanced Mobile Phone System)*** is a digital version of AMPS which uses TDM to place multiple calls on the same frequency channel. ***GSM (Global System for Mobile communications)*** is based on a mix of FDM and TDM. ***CDMA (Code Division Multiple Access)*** is based on neither FDM nor TDM. The CDMA technology has become the basis for 3G systems.

GSM (THE GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS)

GSM (Global System for Mobile Communications) is a second-generation digital mobile telephone standard using a variation of Time Division Multiple Access (TDMA).

It is the most widely used of the three digital wireless telephone technologies namely CDMA (Code Division Multiple Access), GSM and TDMA. GSM ***digitizes and compresses voice data***, then sends it down a channel with two other streams of user data, each in its own time slot.

It operates at either the 900, 1800 or 1,900MHz frequency bands. GSM was initially developed as pan-European collaboration, intended to enable mobile roaming between member countries. .

The mobile itself is divided into the handset and a removable chip with subscriber and account information. This chip is also called as a **SIM card (Subscriber Identity Module).** The GSM architecture is shown in figure 2.51.

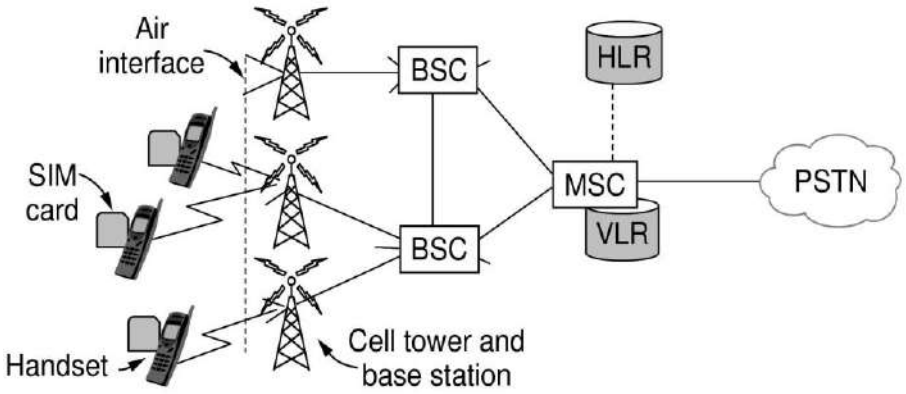


FIGURE 7 THE GSM ARCHITECTURE

The GSM technical specifications define the different entities that form the GSM network by defining their functions and interface requirements. There are four main areas of GSM Network;

i. Mobile station (MS)
ii. Network and Switching Subsystem (NSS)
iii. Operation and Support Subsystem (OSS)
iv. Base-station subsystem (BSS)

The mobile talks to cell base stations over an **air interface.** The cell base stations are connected to a ***BSC (Base Station Controller)*** that controls the radio resources of cells and handles handoff. The BSC in turn is connected to an MSC that routes calls and connects to the PSTN (Public Switched Telephone Network).

To route calls, the MSC needs to know where mobiles can currently be found. It maintains a database of nearby mobiles that are associated with the cells it manages. This database is called the ***VLR (Visitor Location Register).***

There is also a database called the ***HLR (Home Location Register)*** in the mobile network that gives the last known location of each mobile. This database is used to route incoming calls to the right locations. Both databases must be kept up to date as mobiles move from cell to cell.

The air interface

GSM runs on a range of frequencies including 900, 1800, and 1900 MHz. More spectrums are allocated to support a larger number of users. GSM is a frequency division duplex cellular system, it means that each mobile transmits on one frequency and receives on another, higher frequency. In GSM a single frequency pair is split by time-division multiplexing into timeslots to share between multiple mobiles.

A 200-kHz channel of GSM is shown in figure 8. In this figure a GSM system operating in the 900-MHz region has 124 pairs of simplex channels.

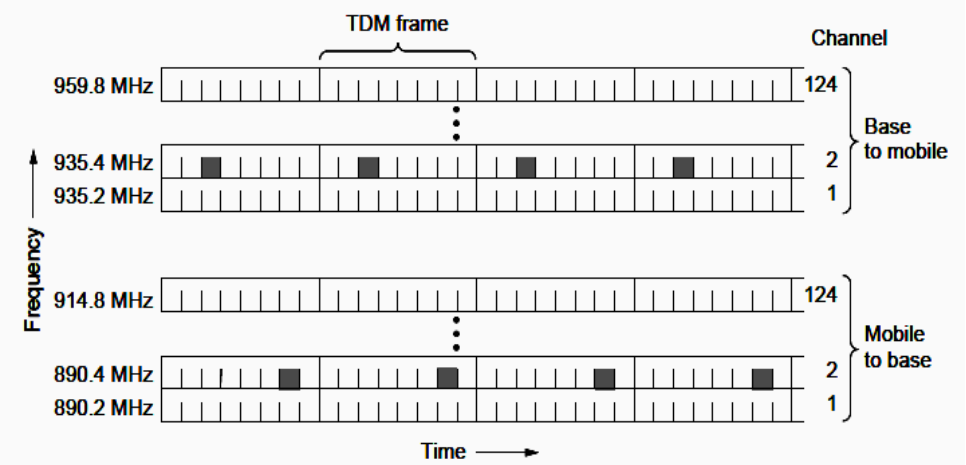


FIGURE 8 GSM CHANNEL

Each TDM slot shown in figure 8 has a specific structure and groups of TDM slots form multiframes. A simplified version of this hierarchy structure is shown in figure 8. Here,

a) Each TDM slot consists of a ***148-bit data frame*** that occupies the channel for ***577 µsec***.
b) Each data frame starts and ends with ***three 0 bits*** for frame description purposes.
c) It also contains ***two 57-bit information fields***, each one having a ***control bit*** that indicates whether the following information field is for ***voice or data***.
d) Between the information fields is a ***26-bit Sync*** field that is used by the receiver to ***synchronize to the sender's frame boundaries***.
e) A data frame is transmitted in 547 µsec, but a transmitter is only allowed to send one data frame every 4.615 msec since it is sharing the channel with seven other stations
f) The figure 2.53 shown that, eight data frames make up a TDM frame and 26 TDM frames make up a 120-msec multiframe.
g) Out of these 26 TDM frames, slot 12 is used for control and slot 25 is reserved for future use. So, only 24 are available for user traffic.

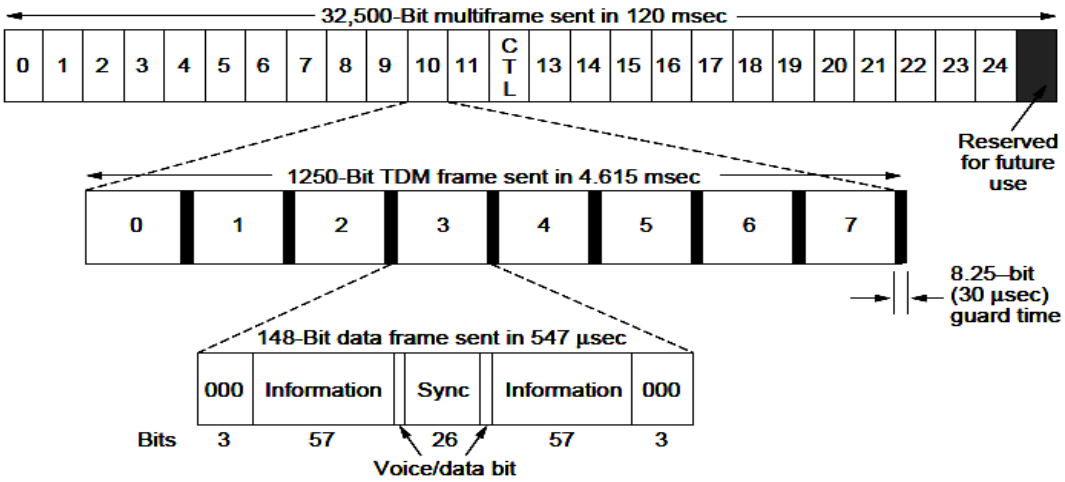


FIGURE A PORTION OF THE GSM FRAMING STRUCTURE

In addition to the 26-slot multiframe a 51-slot multiframe is also used. Some of the slots in 51-slot multiframe are used to hold several ***control channels*** to manage the system. The following control channels are used in GSM;

1) The ***broadcast control channel*** is a continuous stream of output from the base station containing its identity and the channel status. All mobile stations monitor their signal strength to see when they have moved into a new cell.

2) The ***dedicated control channel*** is used for location updating, registration, and call setup. Each BSC maintains a database of mobile stations in the VLR. And the information needed for the maintenance of the VLR database is sent on the dedicated control channel.
3) The ***common control channel*** is split up into three logical subchannels. They are
   a) The ***paging channel*** used by the base station to announce incoming calls.
   b) The ***random access channel*** allows users to request a slot on the dedicated control channel.
   c) The ***access grant channel*** is used indicate the assignment of the requested slot

3.THIRD-GENERATION (3G) MOBILE PHONES: DIGITAL VOICE AND DATA

The third generation of mobile phones is used to communicate both digital voice *and* data. The International Telecommunications Union (ITU) defined the third generation (3G) of mobile telephony standards IMT-2000 to facilitate growth, increase bandwidth and support more diverse applications. The following factors forced the industry to develop third generation (3G) mobile phones;

i. The data traffic already exceeds voice traffic on the fixed network and is growing exponentially, whereas voice traffic is essentially flat. Many industry experts expect data traffic to dominate voice on mobile devices as well soon.
ii. The telephone, entertainment and computer industries have all gone digital and are rapidly converging.
iii. Many people are searching for lightweight, portable devices that act as a telephone, music player, video player, email terminal, Web interface, gaming machine and more, all with worldwide wireless connectivity to the Internet at high bandwidth.

IMT-2000 defines a set of technical requirements for the realization of such targets, which can be summarized as follows;

i. High data rates (144 kbps in all environments and 2 Mbps in low-mobility and indoor environments)
ii. Symmetrical and asymmetrical data transmission
iii. Circuit-switched and packet-switched-based services
iv. Speech quality comparable to wire-line quality
v. Improved spectral efficiency
vi. Several simultaneous services to end users for multimedia services
vii. Seamless incorporation of second-generation cellular systems
viii. Global roaming

ITU predict a single worldwide technology for IMT-2000, so manufacturers could build a single device that could be sold and used anywhere in the world. ***The number 2000 stand for three things***;

i. The year it was supposed to go into service
ii. The frequency it was supposed to operate at (in MHz)
iii. The bandwidth the service should have (in kbps).

3G Standards and Access Technologies

As mentioned before, there are several different radio access technologies defined within ITU, based on either CDMA or TDMA technology. An organization called ***3rd Generation Partnership Project (3GPP)*** has continued that work by defining a mobile system that fulfills the IMT-2000 standard. This system is called ***Universal Mobile Telecommunications System (UMTS)***. After trying to establish a single 3G standard, ITU finally approved a family of three 3G standards, which are part of the 3G framework known as IMT-2000;

i. W-CDMA
ii. CDMA2000
iii. TD-SCDMA

The two most popular IMT proposals are ***WCDMA (Wideband CDMA)*** *or* ***UMTS (Universal Mobile Telecommunications System)*** and ***CDMA2000.*** The WCDMA was proposed by Ericsson and CDMA2000 was proposed by Qualcomm. The WCDMA uses 5-MHz channels and CDMA2000 uses 1.25-MHz channels.

3G W-CDMA (UMTS)

WCDMA is based on direct sequence code division multiple access (DS-CDMA) technology in which user information bits are spread over a wide bandwidth by multiplying the user data with the spreading code. The chip rate of the spreading sequence is 3.84 Mcps. Here, the WCDMA system deployment is used together with the 5-MHz carrier spacing.

3G CDMA2000

The code division multiple access 2000 is the natural evolution of IS-95 (cdmaOne). It includes additional functionality that increases its ***spectral efficiency and data rate capability***. CDMA is a mobile digital radio technology where channels are defined with codes. .

This standard is being developed by Telecommunications Industry Association (TIA) of US and is standardized by 3GPP2. The main CDMA2000 standards are;

i. CDMA2000 1xRTT,
ii. CDMA2000 1xEV
iii. CDMA2000 EV-DV

Advantages of CDMA

i. CDMA can improve capacity by taking advantage of small periods when some transmitters are silent.
ii. With CDMA, each cell uses the same frequencies by mounting multiple directional antennas (or) sectored antennas.
iii. CDMA facilitates soft handoff, in which the mobile is acquired by the new base station before the previous one signs off.

UNIT – II

DATA LINK LAYER

The main job of the data link layer is to make the communication on the physical link reliable and efficient. The data link layer uses the services of the physical layer to send and receive bits over communication channels. The data link layer provides the following functions;

i. Providing a well-defined service interface to the network layer
ii. Dealing with transmission errors
iii. Regulating the flow of data so that slow receivers are not swamped by fast senders

The data link layer achieves these goals by takes the packets it gets from the network layer and encapsulates them into ***frames*** for transmission. Each frame contains ***a frame***

header, a frame trailer and a payload field for holding the packet. The frame format is illustrated in figure 2.1. Frame management forms the heart of what the data link layer does.

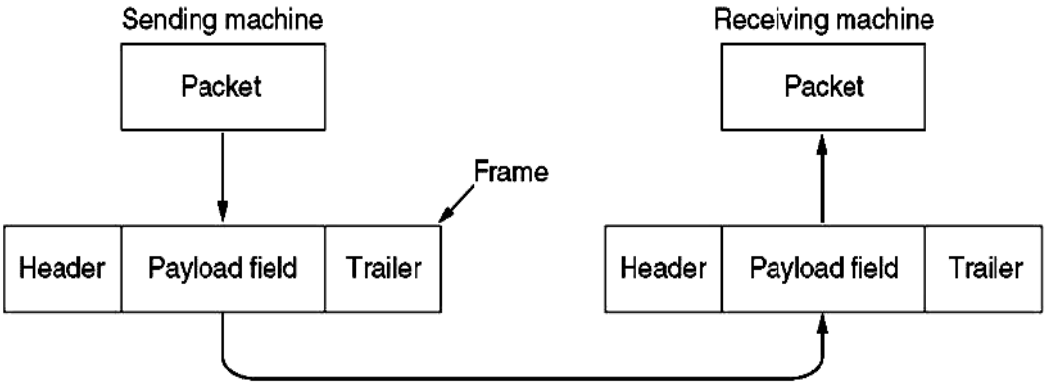


FIGURE 2.1 RELATIONSHIP BETWEEN PACKETS AND FRAMES

DATA LINK LAYER DESIGN ISSUES

1. SERVICES PROVIDED TO THE NETWORK LAYER

The function of the data link layer is to provide services to the network layer. The principal service is transferring data from the network layer on the source machine to the network layer on the destination machine.

. This communication is illustrated in figure 2.2. But the actual transmission follows the different path as shown in figure 2.3.

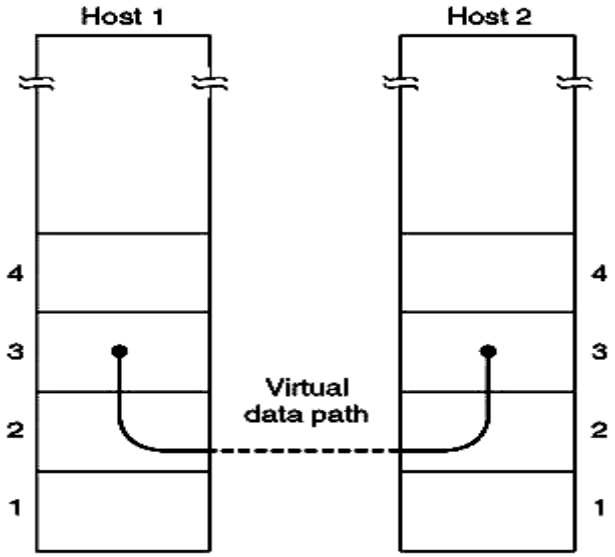


FIGURE 2.2 VIRTUAL COMMUNICATION

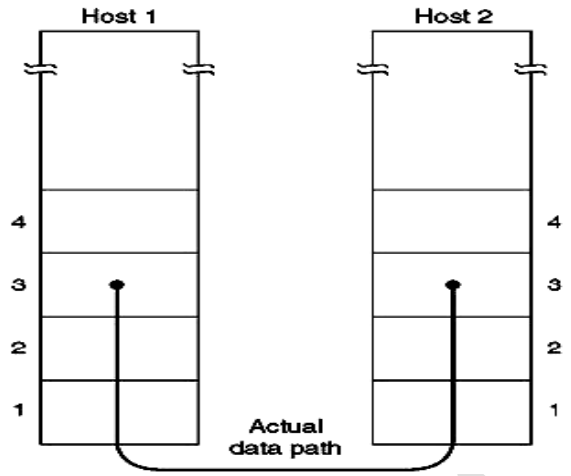


FIGURE 2.3 ACTUAL COMMUNICATION

The data link layer can be designed to offer various services. The actual services offered by the data link layer may vary from protocol to protocol. Three reasonable possibilities are;

i. Unacknowledged connectionless service
ii. Acknowledged connectionless service
iii. Acknowledged connection-oriented service

i) Unacknowledged connectionless service

In an unacknowledged connectionless service, the source machine send independent frames to the destination machine ***without getting any acknowledgement*** from the destination machine. Ethernet is a good example that provides this class of service.

ii) Acknowledged connectionless service

The acknowledged connectionless service is used to provide high reliability. Here, ***no logical connection is used but each frame sent is individually acknowledged.*** In this method, the sender knows whether a frame has arrived correctly or been lost

iii) Connection-oriented service

In this service, the source and destination machines establish a connection before any data are transferred. Each frame sent over the connection is numbered, and the data link layer guarantees that each frame sent is indeed received.

In an acknowledged connectionless service, a frame may be sent and received several times due to the acknowledgement loss which leads to bandwidth wastage. When connection-oriented service is used, transfers go through three distinct phases.

i. The connection is established. The variables and counters required at both the sides are initialized to keep track of frames. The value of the variables are used to predict the frames to be received and or not.
ii. One or more frames are transmitted.
iii. The connection is released, freeing up the variables, buffers, and other resources used to maintain the connection.

2.FRAMING

To provide service to the network layer, the data link layer must use the service provided to it by the physical layer. The physical layer accepts a raw bit stream and attempt to deliver it to the destination.

It is a responsibility of the data link layer to detect and correct errors.

Translation of physical layer's raw bits into larger aggregate (or) discrete units called frames. Here, beginning and end of the data are marked to recognize the frame. The data link layer will break up the bit stream into discrete ***frames*** and compute a short token called a ***checksum***

Breaking up the bit stream into frames is more difficult. The following four methods are available to break the bit streams;

i. Byte count
ii. Flag bytes with byte stuffing
iii. Flag bits with bit stuffing
iv. Physical layer coding violations

i) Byte count

This method uses a field in the header to specify the number of bytes in the frame. When the data link layer at the destination sees the byte count it knows how many bytes follow and consequently where the end of the frame is.

This technique is shown in figure. Here, four small example frames of sizes 5, 5, 8, and 8 bytes, respectively were taken.

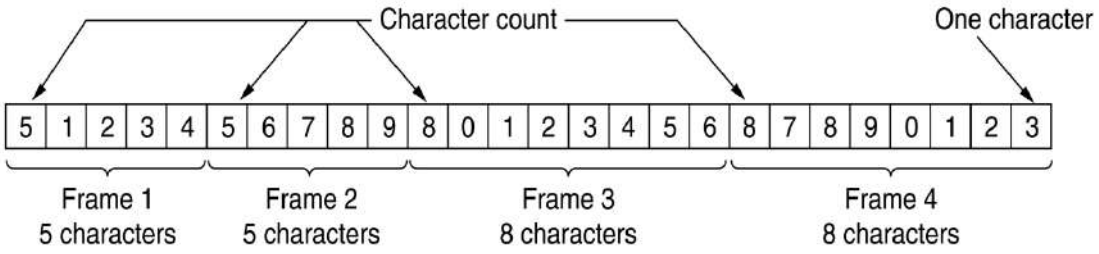


FIGURE A BYTE STREAM WITHOUT ERROR

The trouble with this algorithm is that the count can be confused by a transmission error. For example, if the byte count of 5 in the second frame of figure 2.5 becomes a 7 due to a single bit flip,

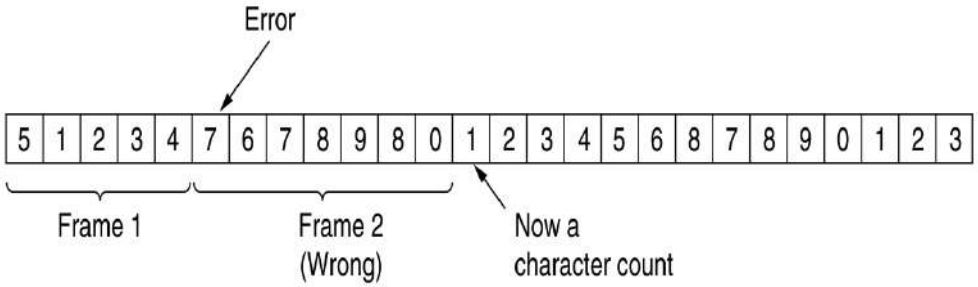


FIGURE 2.5 A BYTE STREAM WITH ERROR

ii) Flag bytes with byte stuffing

In this method, start and end of frame are recognized with the help of ***flag bytes.*** Each frames starts and ends with a flag byte.

Two consecutive flag bytes indicate the end of one frame and start of the next one. The flag bytes used in this method is named as ***ESC flag byte***. .

Figure illustrates the four examples of byte sequences before and after stuffing.

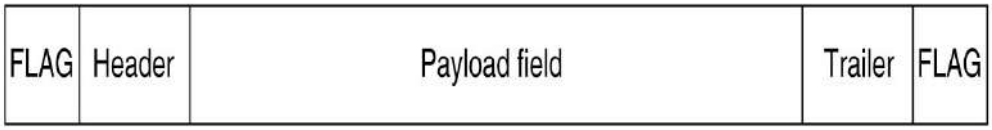


FIGURE 2.6 A FRAME DELIMITED BY FLAG BYTES

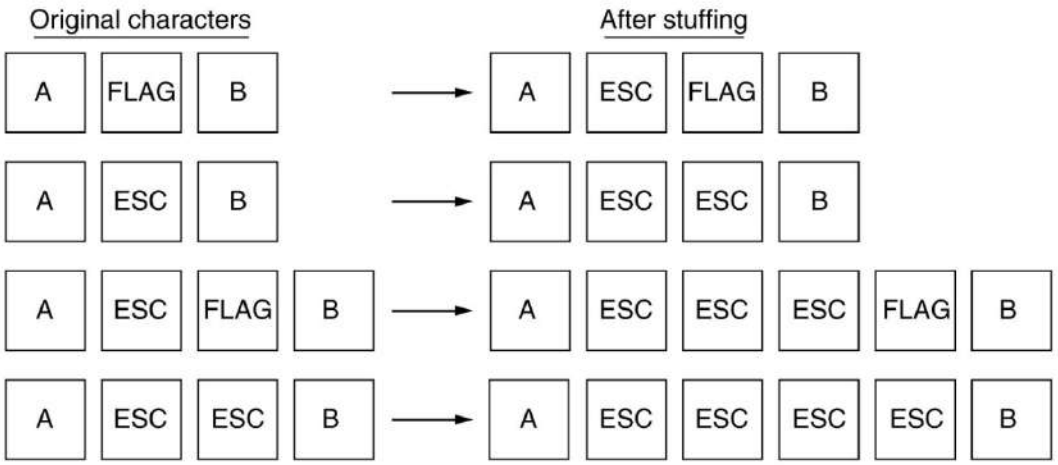


FIGURE 2.7 EXAMPLE BYTE SEQUENCES BEFORE AND AFTER STUFFING

iii) Flag bits with bit stuffing

It allows frame to contain arbitrary number of bits and arbitrary character size. The frames are separated by separating flag. Each frame begins and ends with a special bit pattern, ***01111110*** called a ***flag byte***.

When five consecutive l's are encountered in the data, it automatically stuffs a '0' bit into the outgoing bit stream. In this method, frames contain a random number of bits and allow character codes with a random number of bits per character.

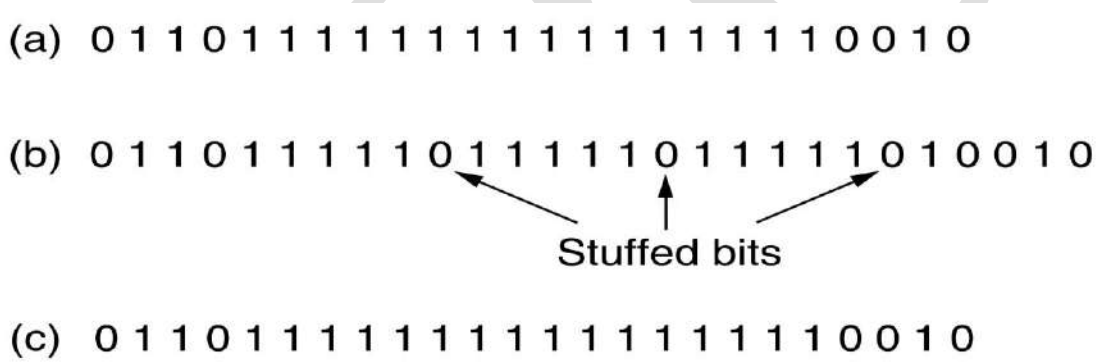


FIGURE 2.8 BIT STUFFING

iv) Physical layer coding violations

The final framing method is physical layer coding violations and is applicable to networks in which the encoding on the physical medium contains some redundancy. In such cases normally, a 1 bit is a high-low pair and a 0 bit is a low-high pair.

The combinations of low-low and high-high which are not used for data and it may be used for marking frame boundaries. Here, the redundancy means that some signals will not occur in regular data.

3. ERROR CONTROL

The way to ensure reliable delivery is to provide the sender with some feedback about what is happening at the other end of the line. The protocol calls for the receiver to send back special control frames bearing positive or negative acknowledgements about the incoming frames.

If the sender receives a positive acknowledgement about a frame, it ensures that the frame has arrived safely. On the other hand, a negative acknowledgement means that something has gone wrong, and the frame must be transmitted again.

It is generally necessary to assign sequence numbers to outgoing frames, so that the receiver can distinguish retransmissions from originals.

The checksums may be of two types. They are;

i. **Error detecting**: Receiver can only detect the error in the frame and inform the sender about it.
ii. **Error detecting and correcting**: The receiver can not only detect the error but also correct it.

4. FLOW CONTROL

One more design issue occurs in the data link layer is, when a sender wants to transmit the frames faster than the receiver can accept them. This situation can occur when the sender is running on a fast, powerful computer and the receiver is running on a slow, low-end machine. At this moment, the transmission is error free but the receiver is unable to handle the frames as fast as they arrive and will lose some. In this situation, two approaches are commonly used. They are,

(i) **Feedback-based flow control:** The receiver sends back information to the sender giving it permission to send more data or at least telling the sender how the receiver is doing.
(ii) **Rate-based flow control:** The protocol has a built-in mechanism that limits the rate at which senders may transmit data, without using feedback from the receiver.

5. AUTOMATIC REPEAT REQUEST (ARQ):

- In this scheme, the information word is coded with adequate redundant bits so as to enable detection of errors at the receiving end.
- If an error is detected, the receiver asks the sender to retransmit the particular information word.
- This system is useful where the expected errors are burst in nature or error rate of the channel is low, i.e. the channel is fairly reliable.

There are functionalities of ARQ protocol,

- Transmission of frames
- Error checking at the receiver end.
- Acknowledgement
- Negative if error is detected (NAK)
- Positive if error is detected (ACK)
- Retransmission of acknowledgement is negative (NAK)
- There are some techniques of ARQ protocol,
    1. Stop and wait
    2. Sliding Window

6.LINK MANAGEMENT FUNCTION

The transfer of data between two devices executes through various phases. These phases are

1) Connect phase
2) Link establishment phase
3) Actual data transfer phase
4) Termination phase
5) Clearing of connection phase

ERROR DETECTION AND CORRECTION

Network must be able to transfer data from one device to another with complete accuracy. Data can be corrupted during transmission. For reliable communication, errors are detected and corrected.

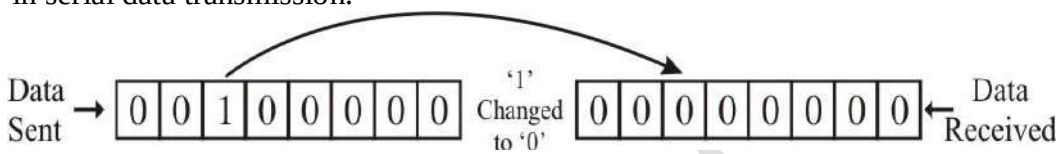
1.Types of Errors

Whenever electromagnetic signal flows from one point to another, it is subjected to unpredictable interference from heat, magnetism and other forms of electricity. This interference can change the shape on timing of the signal. There are two types of errors,

i. Single-Bit Error
ii. Burst Error

i) Single-Bit Error

In a single-bit error, only 1 bit in the data unit has changed. Single bit error can happen if we are sending data using parallel transmission. Single bit error is produced very rarely in serial data transmission.



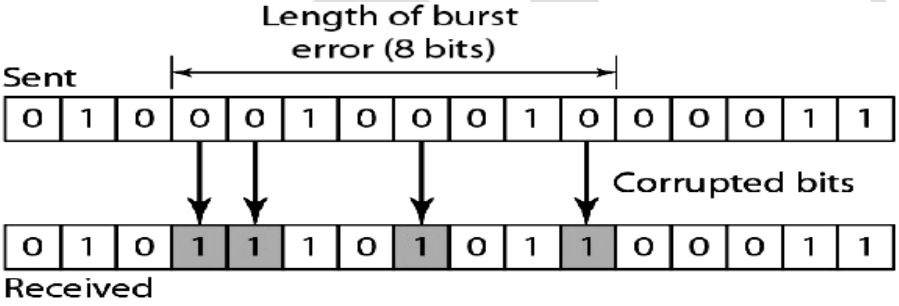
SINGLE-BIT ERROR

Example

The data rate is 1Mbps. For a single bit error, possibility is 1/1,000,000 (or) 1 Microseconds.

ii) Burst Error

A burst error means that 2 or more bits in the data unit have changed. Burst error will be produced by serial transmission. Number of bits affected in burst error will depend on the data transmission rate and duration of noise.



BURST ERROR OF LENGTH 8

2. Redundancy

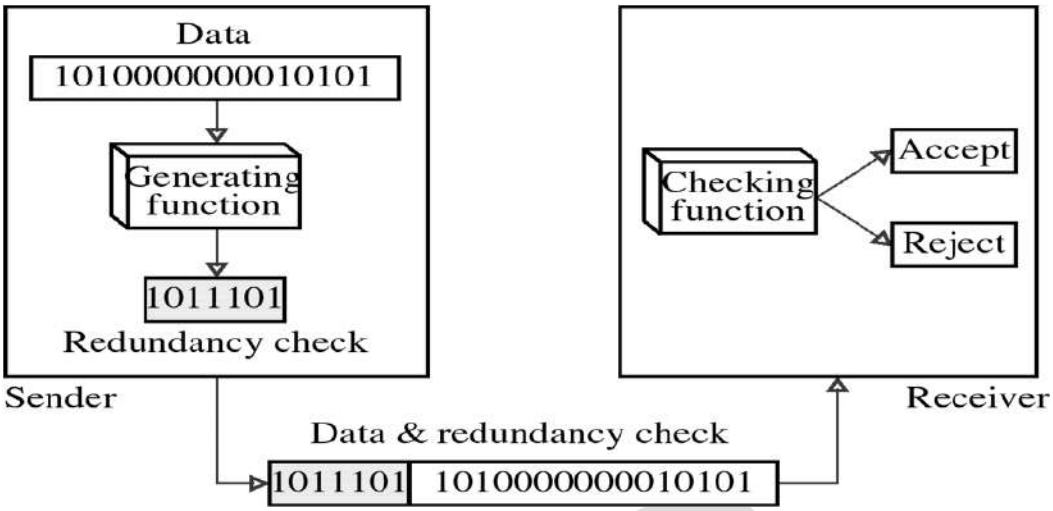
An early error detection mechanism would send every data unit twice. The receiving device would then be able to do a bit-by-bit comparison between the two versions of data. Any discrepancy would indicate an error. Any error will found the necessary correction mechanism should take place.

Disadvantages

i. Transmission time is double.
ii. Time taken for bit-by-bit comparison is high

To overcome this drawback, instead of repairing the entire data stream, a shorter group of bits (redundant) may be appended to the end of each data unit. The technique involving the addition of extra bits to the data unit is called redundancy.

These redundant bits are added by the sender and removed by the receiver. Their presence allows the receiver to detect or correct corrupted bits. By suitably appending the required parity (either odd or even parity) may be obtained. In the appended unit, if the total number of 1s is even then it is called even parity and if the total number of 1s is odd then it is called odd parity.



3. ERROR DETECTING CODES

Four types of error detecting codes are common in data communications. They are;

i. Vertical redundancy check (VRC)
ii. Longitudinal redundancy check(LRC)
iii. Cyclic redundancy check (CRC)
iv. Checksum

i) Vertical redundancy check (VRC)

- Most common and least expensive mechanism.
- VRC is also called as parity check method.
- Redundant bits or parity bit is appended to every data unit so that the total number of 1's in the data unit becomes even.
- Some systems may use odd parity checking.
- It can detect only the single bit error.

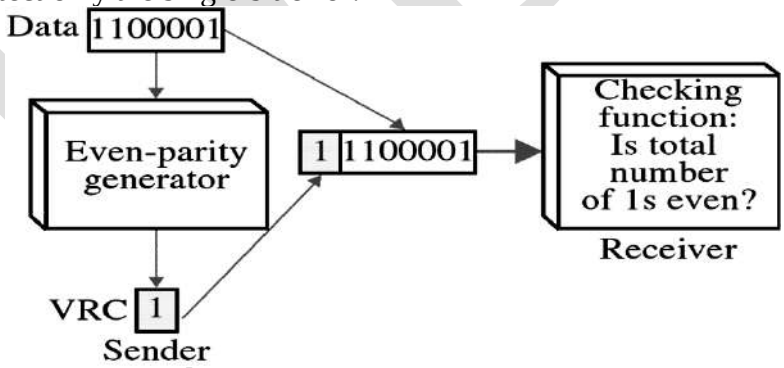


FIGURE 2.12 VERTICAL REDUNDANCY CHECK

ii) Longitudinal redundancy check (LRC)

- In LRC block of bit is organized in to a table.
- For example 32 bit data unit is arranged as four rows and eight columns.
- Check the parity bit for each column and create a new row of eight bits which are the parity bits for the whole block.
- Original data with eight parity bits are transferred to the receiver.

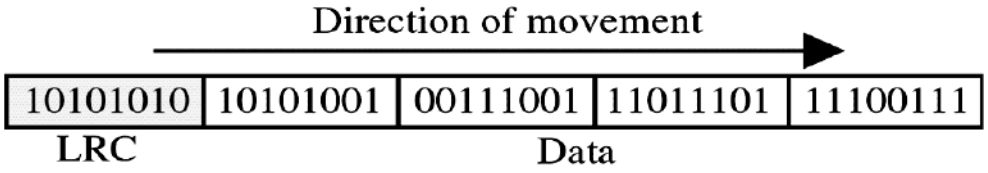


FIGURE 2.13 LONGITUDINAL REDUNDANCY CHECK

iii) Cyclic redundancy check (CRC)

- Unlike VRC and LCR, CRC method is working based on division.

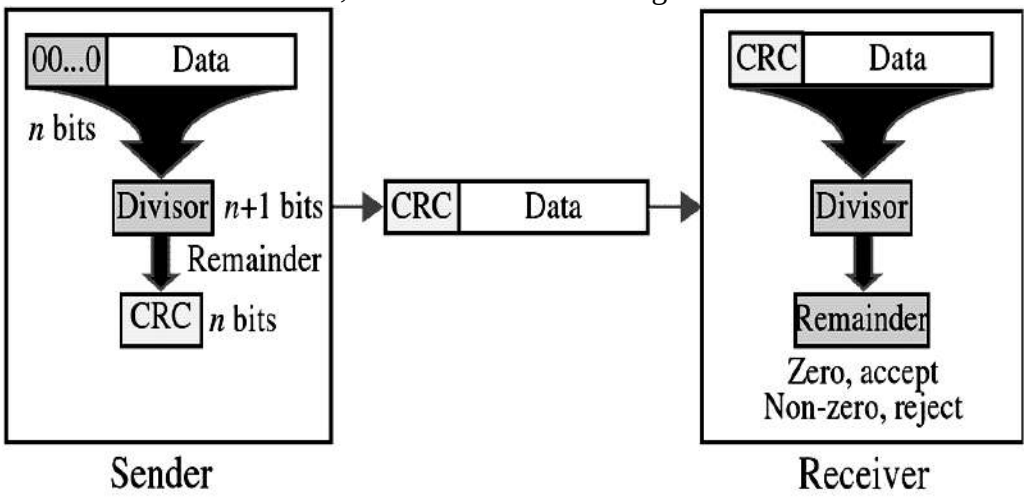


FIGURE 2.14 CYCLIC REDUNDANCY CHECK

CRC generator

- CRC generator uses modulo-2 division.

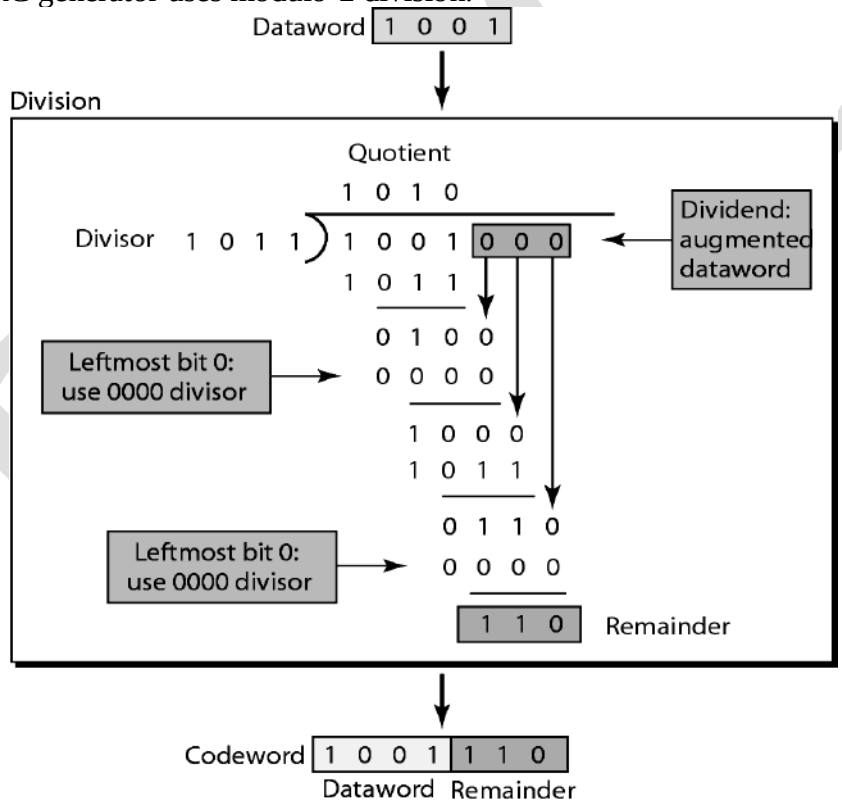


FIGURE 2.15 CRC GENERATOR

CRC Checker

- The CRC checker functions exactly like the CRC generator
- After receiving the data appended with the CRC, the checker does the same modulo-2 division.
- If the remainder is all 0's the CRC is dropped and the data accepted. Otherwise the data will be discarded (It should be resent by the sender).

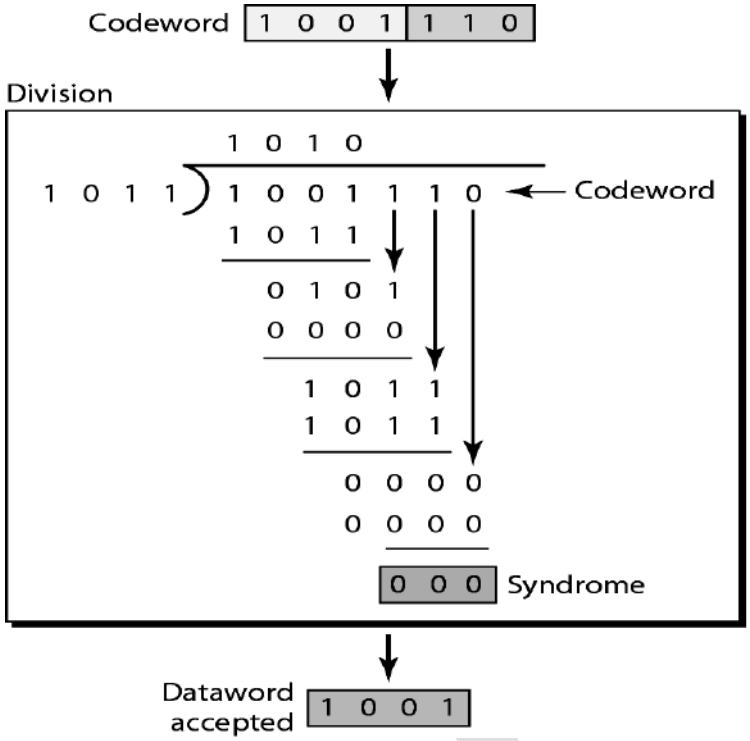


FIGURE 2.16 CRC CHECKER

Polynomials

- It is a more common representation of data than binary form
- Easy to analyze
- Divisor is commonly called generator polynomial

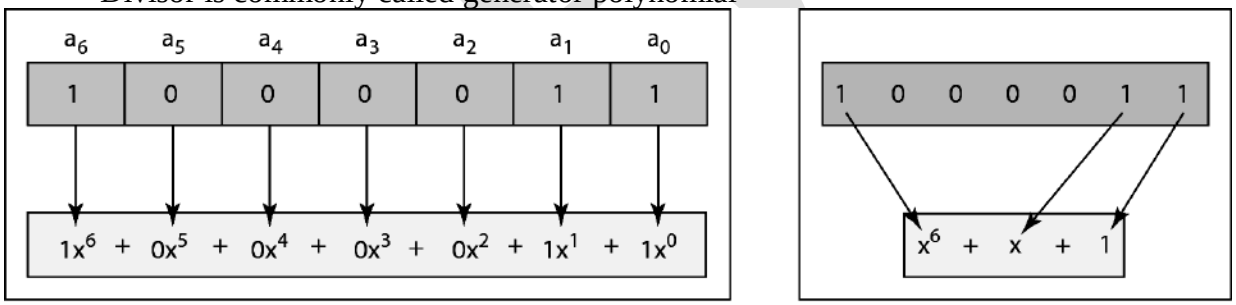


FIGURE 2.17 POLYNOMIAL REPRESENTATION

Properties of polynomials

i. It should not be divisible by x.
ii. It should be divisible by x+1.

CRC-12

$x^{12} + x^{11} + x^3 + x + 1$

CRC-16

$x^{16} + x^{15} + x^2 + 1$

CRC-ITU

$x^{16} + x^{12} + x^5 + 1$

CRC-32

$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

FIGURE 2.18 STANDARD POLYNOMIALS

iv) Checksum

- It is the error detection mechanism used by the higher layer protocols.
- Checksum is working on the redundancy concept.

Checksum Generator

- The data unit is divided into K sections, each of n Bits
- All sections are added together using one's complement to get the sum.
- The sum is then complemented and becomes the checksum.
- The check sum is sent with the data
- If the sum of the data segment is T, the checksum will be –T.

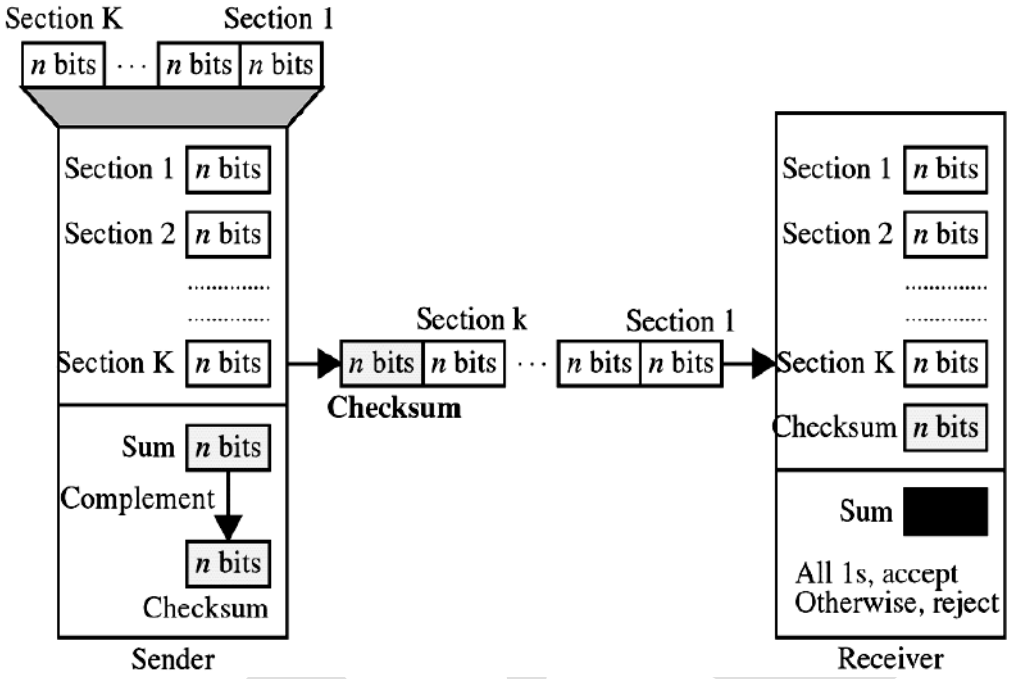


FIGURE 2.19 CHECK SUM GENERATOR AND CHECKER

Checksum checker

- The unit is divided into k sections, each of n bits.
- All sections are added together using one's complement to get the sum.
- The sum is complemented.
- If the result is zero, the data are accepted: otherwise, they are rejected.

Performance

- The checksum detects all errors involving an odd number of bits.
- It detects most errors involving an even number of bits.
- If one or more bits of a segment are damaged and the corresponding bit or bits of opposite value in a second segment are also damaged, the sums of those columns will not change and the receiver will not detect a problem.

4. ERROR CORRECTION

It can be handled in two ways:

i. Receiver can have the sender retransmit the entire data unit.
ii. The receiver can use an error-correcting code, which automatically corrects certain errors.

Single-bit error correction

- To correct an error, the receiver reverses the value of the altered bit. To do so, it must know which bit is in error.
- Number of redundancy bits can be calculated as follows.
  Let data bits = m
  Redundancy bits = r
  ∴ Total message sent = m+r
- The value of r must satisfy the following relation:
  $2^r \geq m+r+1$

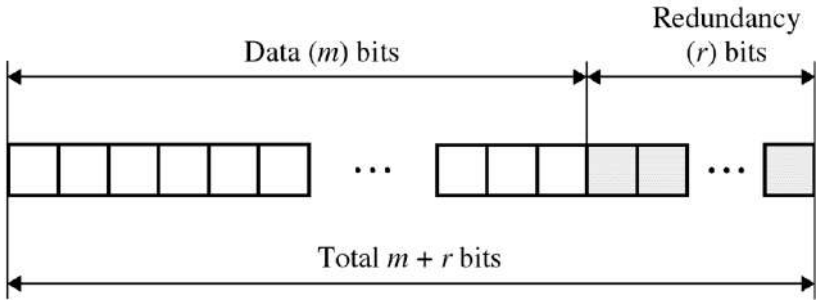


FIGURE 2.20 REDUNDANCY BITS

Number of data bits k	Number of redundancy bit r	Total bits k + r
1	2	3
2	2	5
3	3	6
4	3	7
5	4	9

TABLE 2.1 REDUNDANCY BIT CALCULATION

Hamming Code

- Hamming code is used to positioning the redundancy bits.
- For example

  If m =7 then r=4;

  So total number of bits = 7+4

  = 11
- The redundancy bits are r1, r2, r3 and r4.
- The position of the redundancy bits will be

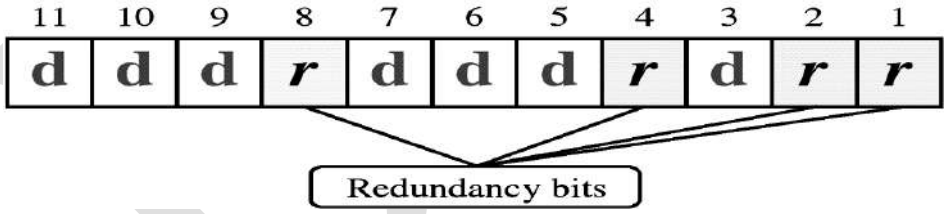
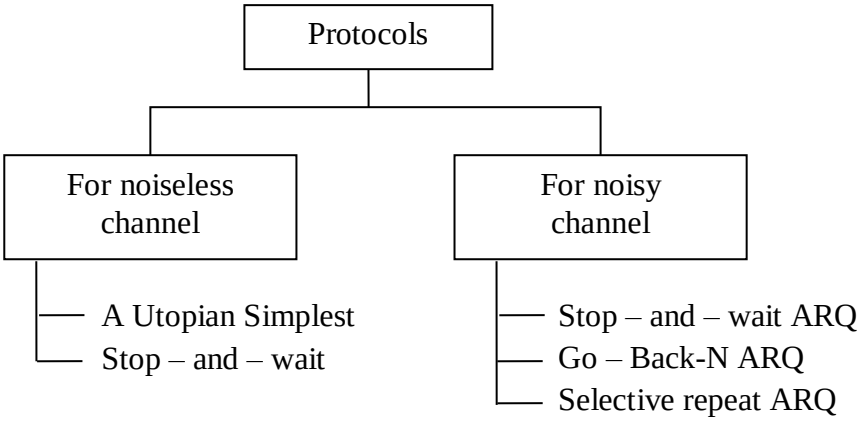


FIGURE 2.21 POSITION OF THE REDUNDANCY BITS

ELEMENTARY DATA LINK PROTOCOLS

- The specific set of rules and procedure for carrying out data link control function is called data link protocol.
- A data link protocol specific format of frame, contents of fields and sequencing.
- Some data link protocols are listed below;
  1. High level Data Link Control (HDLC)
  2. Binary synchronous Data Link Control (BISYNC)
  3. Synchronous Data Link Control (SYNC)



- **Noiseless Channel**

An ideal channel is a channel in which no frames are lost, duplicated, or corrupted. Two protocols were introduced for this type of channel. The first is a protocol that does not use flow control; the second is the one that does.

- **Noisy Channel**

Consider the normal situation of a communication channel that makes errors. Frames may be either damaged or lost completely.

An Unrestricted simplex protocol

- ✓ Data are transmitted in one direction only. Both the transmitting and receiving network layers are always ready to proceed.
- ✓ The protocol consists of two distinct procedures a sender and a receiver. The sender runs in the data link layer of the source machine, and the receiver runs in the data link layer of the destination machine.

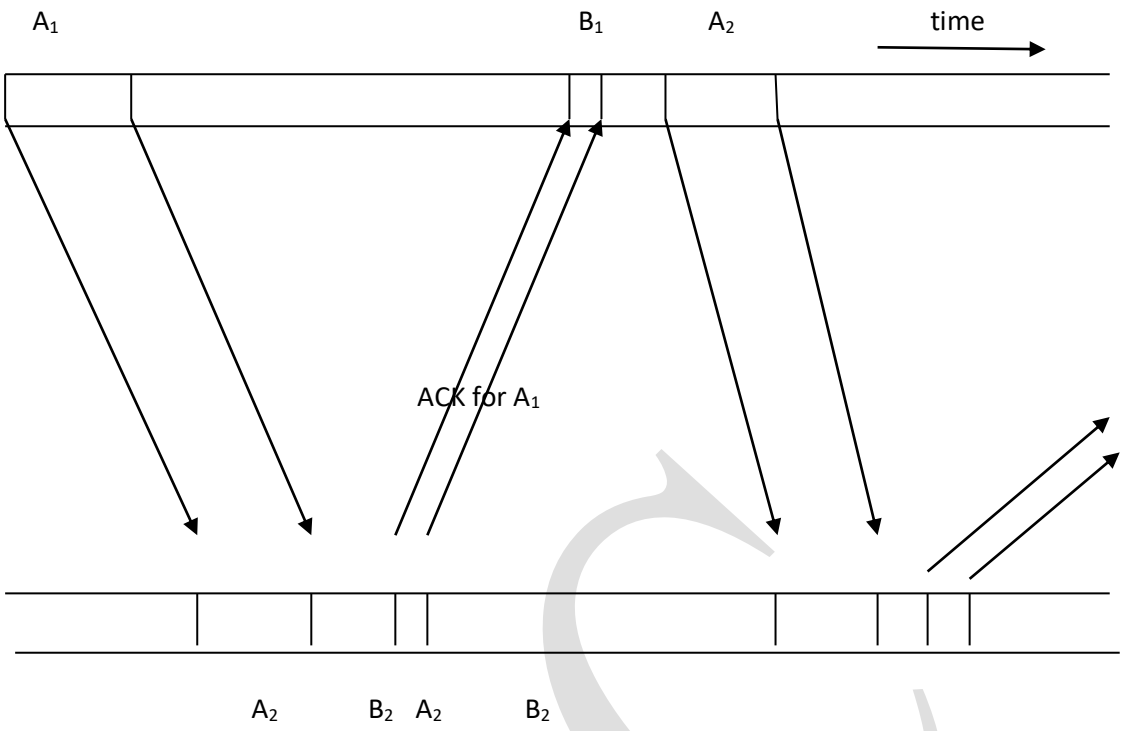
The body of the loop consists of three actions:

- ➔ Fetch a packet from the network layer,
- ➔ Construct an outbound frame using the variable
- ➔ Send the frame on its way.

A simplex stop and wait protocol

- ✓ The simplest retransmission protocol is stop and wait ARQ.
- ✓ Transmitter (Station A) Sends a frame over the communication line and then waits for a positive or negative acknowledgment from the receiver (Station B).
- ✓ If no errors occurred in the transmission, station B sends positive ACK, to Station A.
- ✓ The transmitter can now start to send next frame.
- ✓ If the frame is received at station B with error, then a NAK, is sent to the station A, in this case station A must retransmits the old packet in a new frame.
- ✓ There is also the possibility that information frames and ACK s can be lost.
- ✓ To account for this, the sender is equipped with a timer.
- ✓ If no recognizable ACK is received when the timer expires at the end of time out interval, then same frame send again.

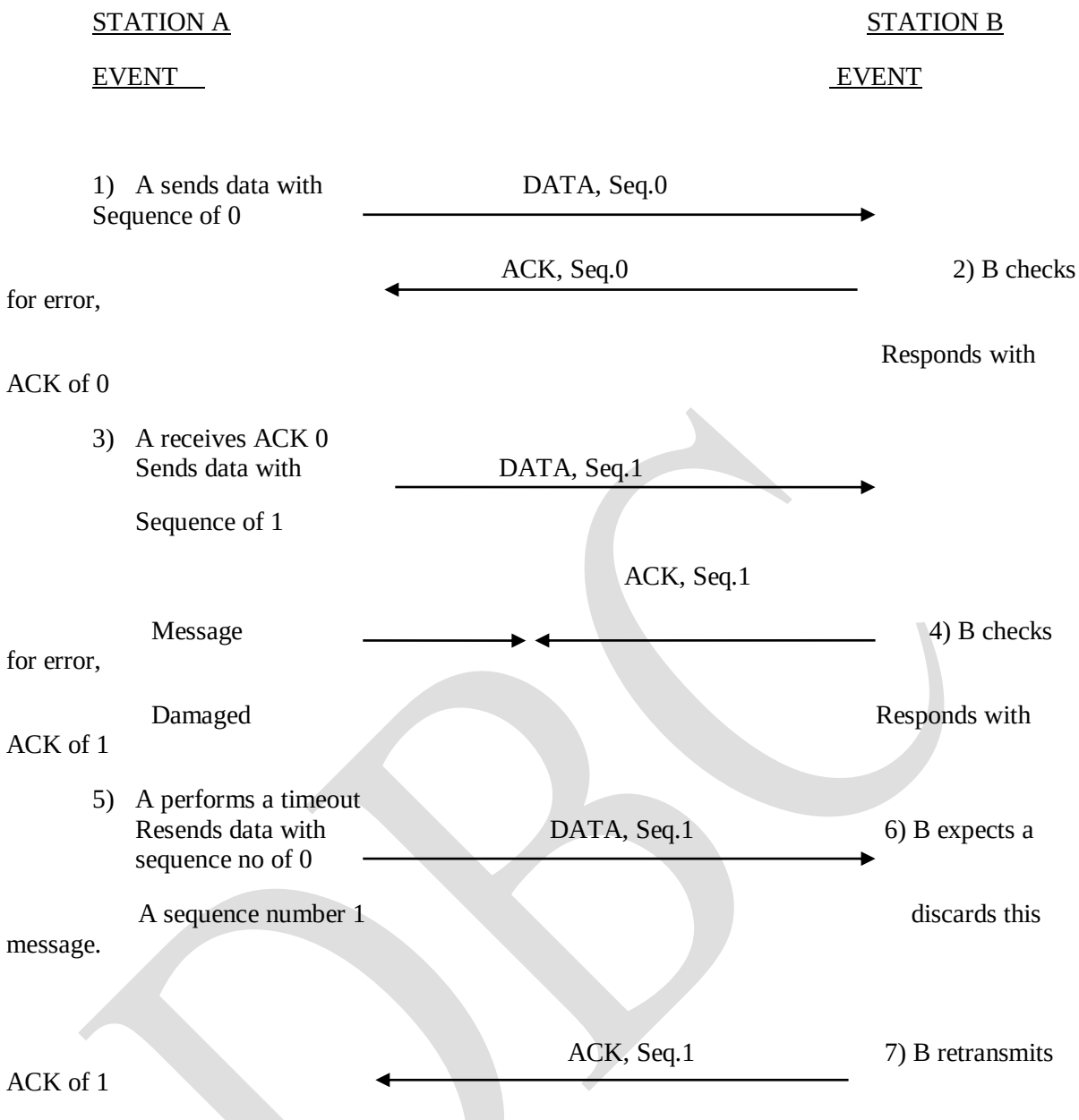
Station A



Station B

A simplex protocol for a noisy channel

- ✓ In a noisy communication channel if a frame is damaged in transmit; the receiver hardware will detect this when it computes the checksum.
- ✓ If a damaged frame is received, it will be discarded and transmitter will retransmit the same frame after receiving a proper ACK.
- ✓ If the ACK frame gets lost and data link layer on A eventually times out. Not having received an ACK, it assumes that its data frame was lost or damaged and sends the frame containing packet 1 again.
- ✓ This duplicate frame also arrives at data link layer on B, thus part of file will be duplicate and protocol is said to be failed.
- ✓ A typical approach to solve this problem is the provision for a sequence number in the header of the message.
- ✓ The sequence can then check for the sequence number to determine if the message is a duplicate.
- ✓ Since only message is transmitted at any time.
- ✓ The sending and receiving station need only 1 bit alternating sequence of 0 or 1 to maintain the relationship of the transmitted message and its ACK / NAK.



SLIDING WINDOW PROTOCOLS

- In sliding window protocol multiple data frames can be transmitted continuously without waiting for ACK, of individual data frames. This protocol is call **sliding windows.**
- Because of the method used to synchronize the sending sequence numbers in the headers with the appropriate ACK.
- The transmitting station maintains a sending window that delineates the no of messages with their sequence number.
- The receiver station maintains a receiving window that performs complementary functions.
- These two sides use the window to co ordinate the flow of message between each other.
- Each data frame carries sequence number for identification. The number of frames in a window is called its size.
- A copy of transmitted frame is retained in the window till it is acknowledged.
  1. STOP-AND WAIT ARQ.
  2. GO-BACK-N ARQ.
  3. SELECTIVE-REPEAT ARQ.

1.STOP-AND- WAIT ARQ

- This is the simplest flow and error control mechanism. It has the following features.
- The sending devise keeps the copy of the last frame transmitted until it receives an acknowledgement for that frame. Keeping a copy allows the sender to re- transmit lost or damaged frames until they are received correctly.
- Both data and acknowledgement frames are numbered alternately 0 and 1. A data frame 0 is acknowledged by an ACK 1.
- A damaged or lost frame is treated in the same manner by the receiver. If the receiver detects an error in the received frame, it simply discards the frame and sends no acknowledgement.
- The sender has a control variable, which we call S, that holds the number of recently sent frame. The receiver has a control variable, which we call R that holds the number of the next frame expected.
- The sender starts a timer when it sends a frame. If an ACK is not received within an allotted time period the sender assumes that the frame was lost or damaged and resends it.
- The receivers send only positive ACK for frames received safe and sound; it is silent about the frames damaged or lost.

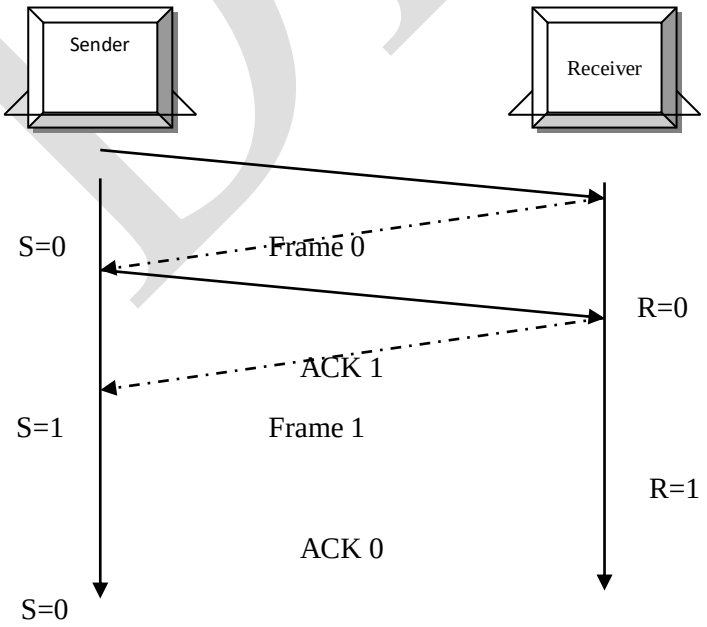
Operations:

The possible operations are

- Normal operation
- Lost frame
- ACK lost
- Delayed ACK.

Normal operation

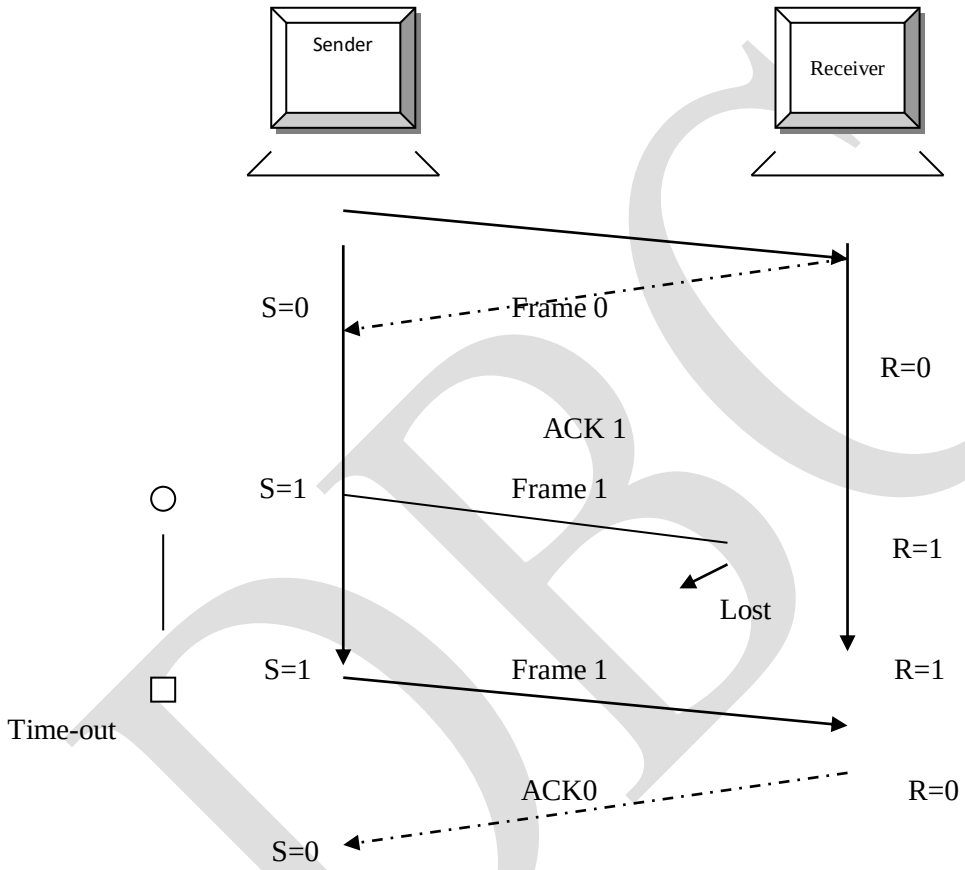
- The sender sends frame 0 and wait to receive ACK 1. when ACK 1 is received it sends frame 1 and then waits to receive ACK 0, and so on.
- The ACK must be received before the time out that is set expires. The following figure shows successful frame transmission.



Time Time

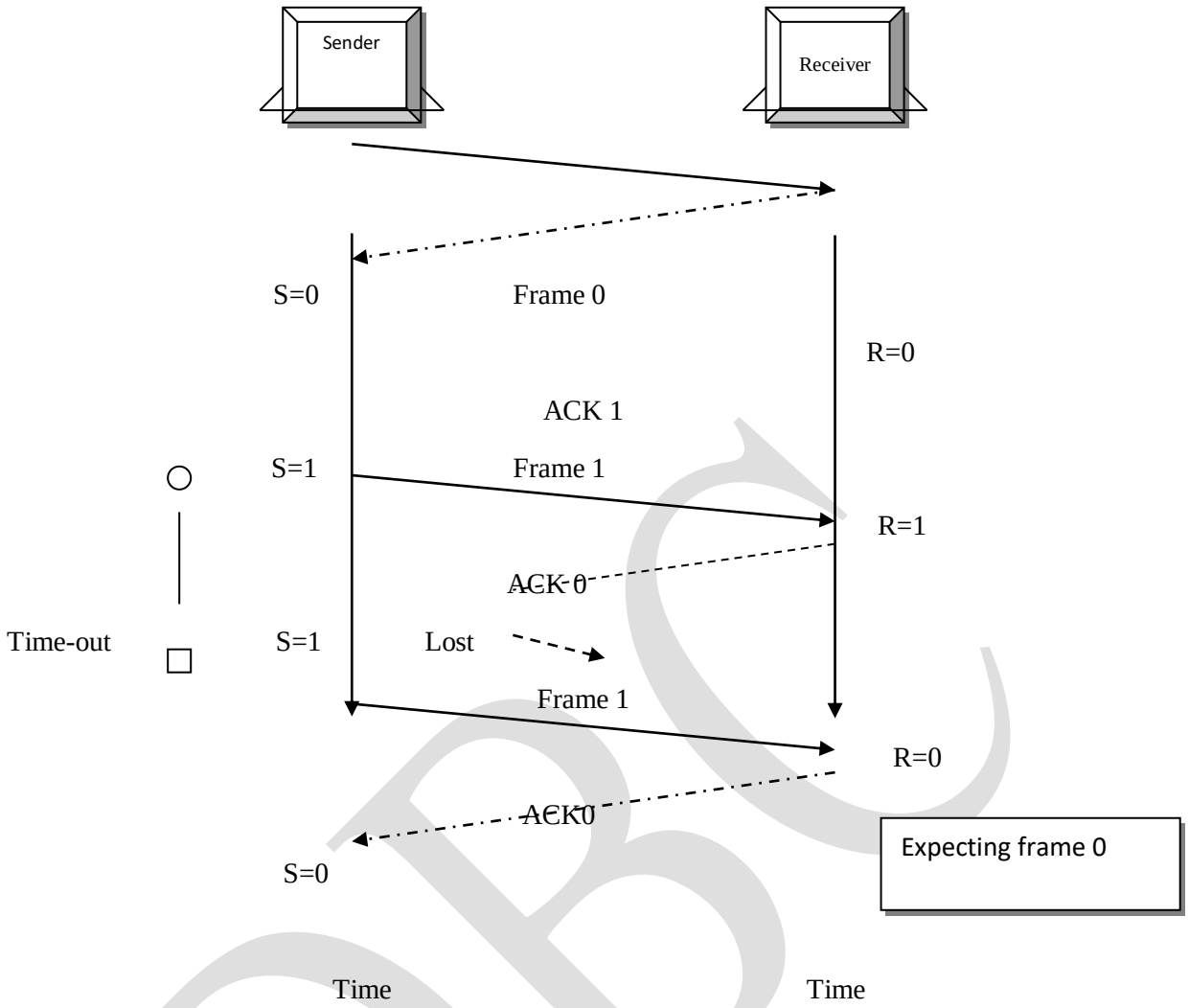
Lost or damaged acknowledgement

- When the receiver receives the damaged frame it discards it, which essentially means the frame is lost.
- The receiver remains silent about a lost frame and keeps its value of R.
- For example in the following figure the sender transmits frame 1, but it is lost. The receiver does nothing, retaining the value of R (1). After the timer at the sender site expires, another copy of frame 1 is sent.



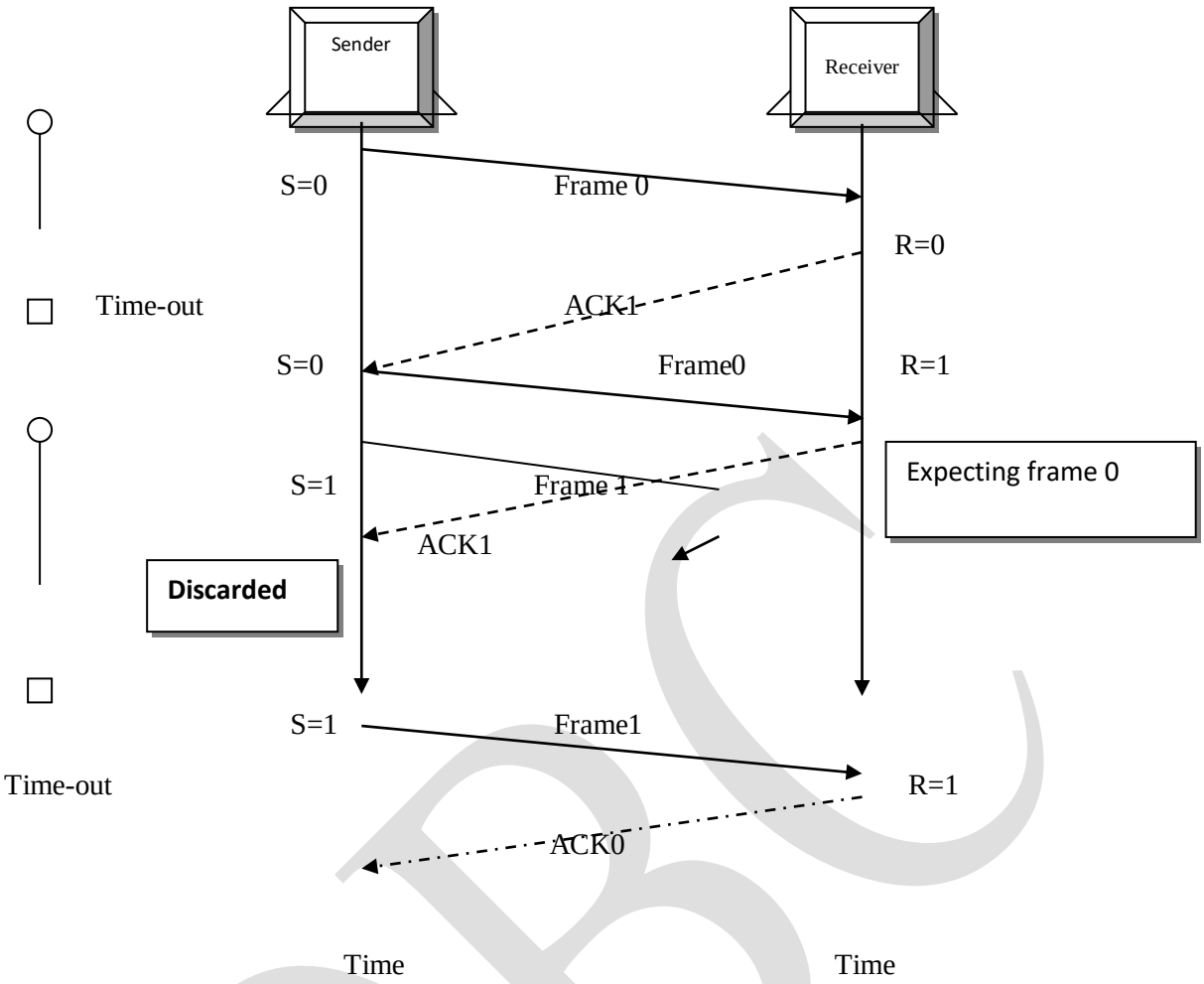
Lost acknowledgement

- A lost or damaged ACK is handle in the same by the sender; if the sender receives a damaged ACK, it discards it.
- The following figure shows a lost ACK 0.the waiting sender does not know if frame 1 has been received. When the timer for frame 1 expires the sender retransmits frame 1.
- Note that the receiver has already received frame 1 and is expecting to receive frame 0. Therefore, its silently discards the second copy of frame 1.



Delayed acknowledgement

- An ACK can be delayed at the receiver or by some problem with the link. The following figure shows the delay of ACK 1; it ids received after the timer for frame 0 as already expired.
- The sender has already retransmitted a copy of frame 0. The receiver expects frame 1 so its simply discards the duplicate frame 0.
- The sender has now received two ACK's, one that was delayed and one that was sent after the duplicate frame 0 arrived. The second ACK 1 is discarded.

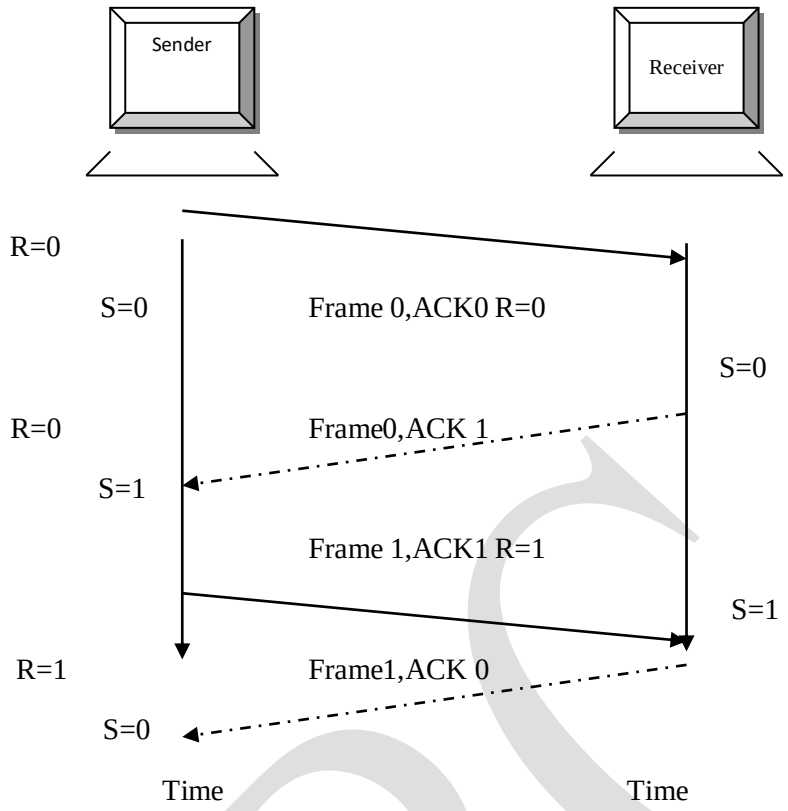


BIDIRECTIONAL TRANSMISSION

The stop – and – wait mechanism is unidirectional. We can have bi-directional transmission if the two parties have two separate channels for full duplex communication or share the same channel for off duplex transmission. In this case, each party needs both S and R variables to track frames sent and expected.

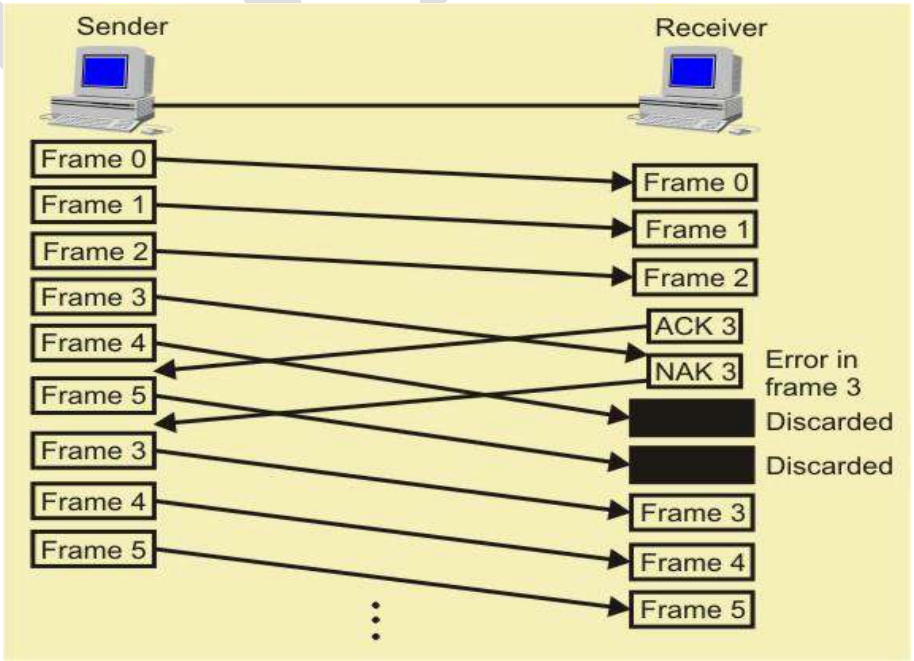
PIGGYBACKING

It's a method to combine a data frame with an ACK. In following figure both the sender and the receiver have data to send. Instead of sending separate data and ACK frames. It can save bandwidth because the overhead from a data frame and an ACK frame can be combined into just one frame



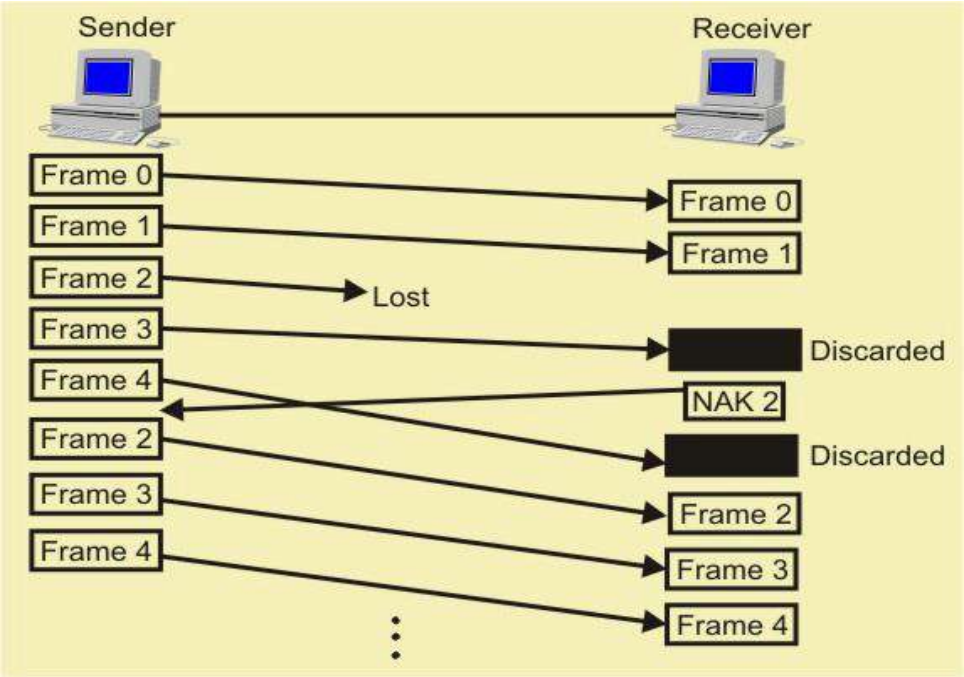
2 .Go-back-N ARQ

- The most popular ARQ protocol is the go-back-N ARQ, where the sender sends the frames continuously without waiting for acknowledgement.That is why it is also called as *continuous ARQ*.
- As the receiver receives the frames, it keeps on sending ACKs or a NACK, in case a frame is incorrectly received. When the sender receives a NACK, it retransmits the frame in error plus all the succeeding frames.



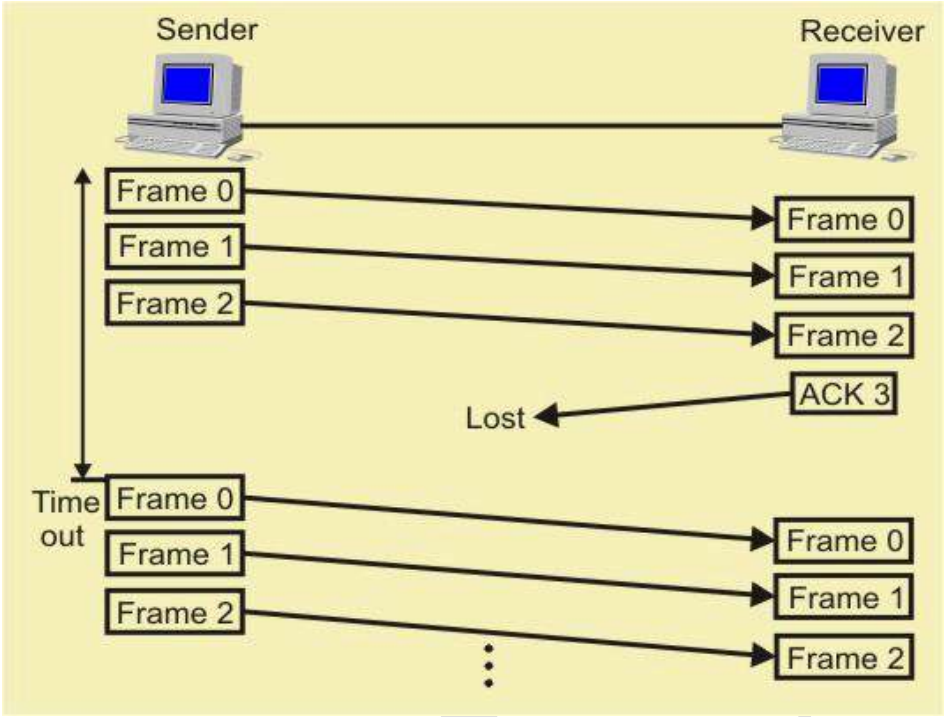
Frames in error in go-Back-N ARQ

- Hence, the name of the protocol is go-back-N ARQ. If a frame is lost, the receiver sends NAK after receiving the next frame .



Lost Frames in Go-Back-N ARQ

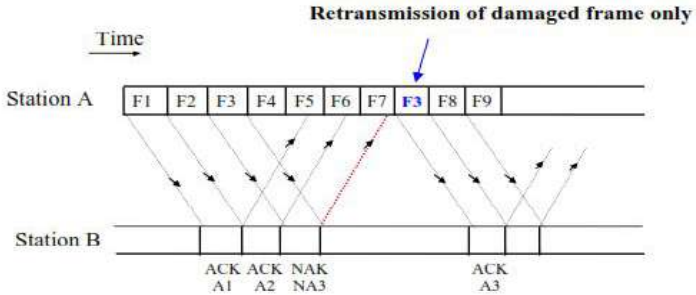
- In case there is long delay before sending the NAK, the sender will resend the lost frame after its timer times out.
- If the ACK frame sent by the receiver is lost, the sender resends the frames after its timer times out.



Lost ACK in Go-Back-N ARQ

3.Selective-Repeat ARQ

- The selective-repetitive ARQ scheme retransmits only those for which NAKs are received or for which timer has expired.



Selective-repeat Reject

- This is the most efficient among the ARQ schemes, but the sender must be more complex so that it can send out-of-order frames.

The receiver also must have storage space to store the post- NAK frames and processing power to reinsert frames in proper sequence.

Unit – III

Network Layer

Layer-3 in the OSI model is called Network layer. Network layer manages options pertaining to host and network addressing, managing sub-networks, and internetworking. Network layer takes the responsibility for routing packets from source to destination within or outside a subnet.

Network Layer Design Issues

Network layer takes the responsibilities as follows

1. Store and forward switching
2. Services provided to the transport layer
3. Implementation of connectionless service
4. Implementation of connection-oriented service
5. Comparison of virtual-circuit and datagram subnets

1) Store and Forward Switching:

- ✓The major components of the system are the carrier's equipment (routers connected by transmission lines)shown inside the shaded oval and the customers' equipment, shown outside the oval.
- ✓Host H1 is directly connected to one of the carrier's routers, A, by a leased line.
- ✓H2 is on a LAN with a router, F, owned and operated by the customer.
- ✓We have shown F as being outside the oval because it does not belong to the carrier, but in terms of construction, software and protocols, it is probably no different from the carrier's routers.

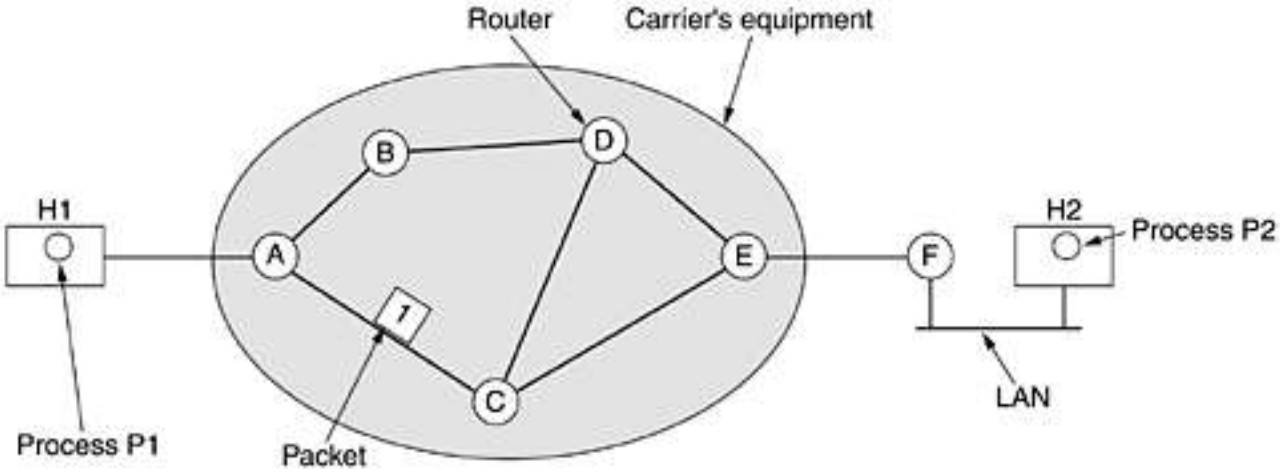


Fig: The environment of the network layer protocols

- A host with a packet to send transmits it to the nearest router, either on its own LAN or over a point-to-point link to the carrier.
- The packet is stored there until it has fully arrived so the checksum can be verified.
- Then it is forwarded to the next router along the path until it reaches the destination host, where it is delivered. This mechanism is store-and-forward packet switching.

2) Services provided to the transport layer:

- The network layer provides services to the transport layer at the network layer / transport layer interface.

The network layer services have been designed with the following:

1) The services should be independent of the router technology.

2) The transport layer should be shielded from the number, type and topology of the routers present.

3) The network addresses made available to the transport layer should use a uniform numbering plan, even across LANs and WANs.

- Each packet must carry the full destination address because each packet sent is carried independently of its predecessor.
- The subnet should provide a reliable, connection-oriented service.
- In this view, quality of service is the dominant factor and without connections in the subnet, quality of service is very difficult to achieve, especially for real-time traffic such as voice and video.
- The Internet offers connectionless network-layer service and ATM network offers connection-oriented network-layer service.

3) Implementation of connectionless service:

The types of service are: 1) Connectionless 2) Connection-oriented.

- If connectionless service is offered, packets are injected into the subnet individually and rounded independently of each other.
- No advance setup is needed. The packets are frequently called datagram (in analogy with telegrams) and the subnet is called a **datagram subnet.**
- If connection-oriented service is used, a path from the source router to the destination router must be established before any data packets can be sent.
- This connection is called a **VC (Virtual circuit),** in analogy with the physical circuits set up by the telephone system and the subnet is **called a virtual circuit subnet**.
- The network layer has to break it into four packets 1,2,3 and 4 and sends each of them in turn to route A using some point-to-point protocol, for example, PPP.
- Every router has an internal table telling it where to send packets for each possible destination. Each table entry is a pair consisting of a destination and the outgoing line to use for that destination.

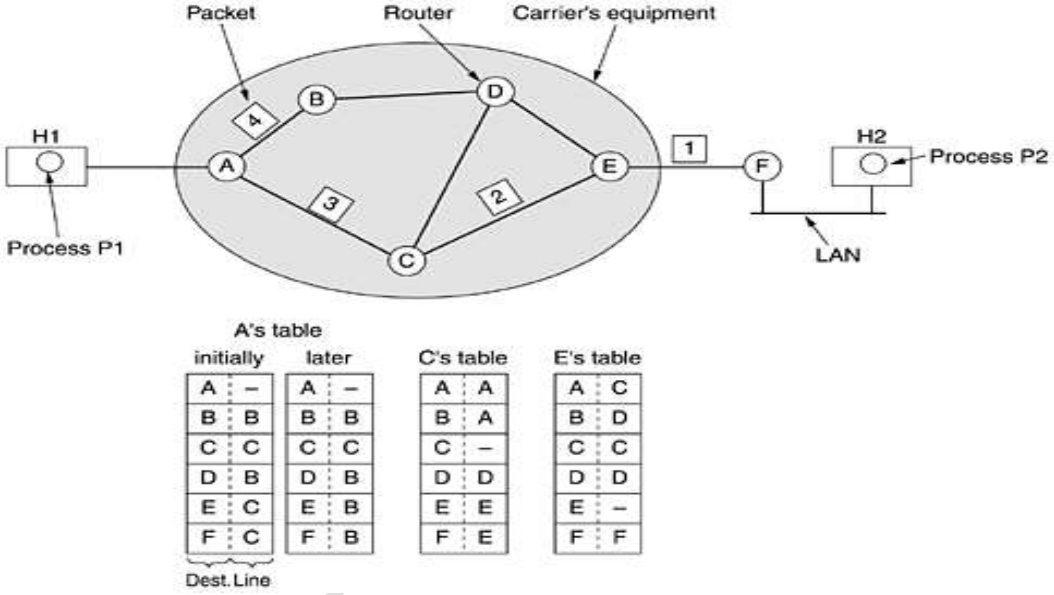


Fig: Routing within a datagram subnet.

Let us assume that the message is four times longer than the maximum packet size

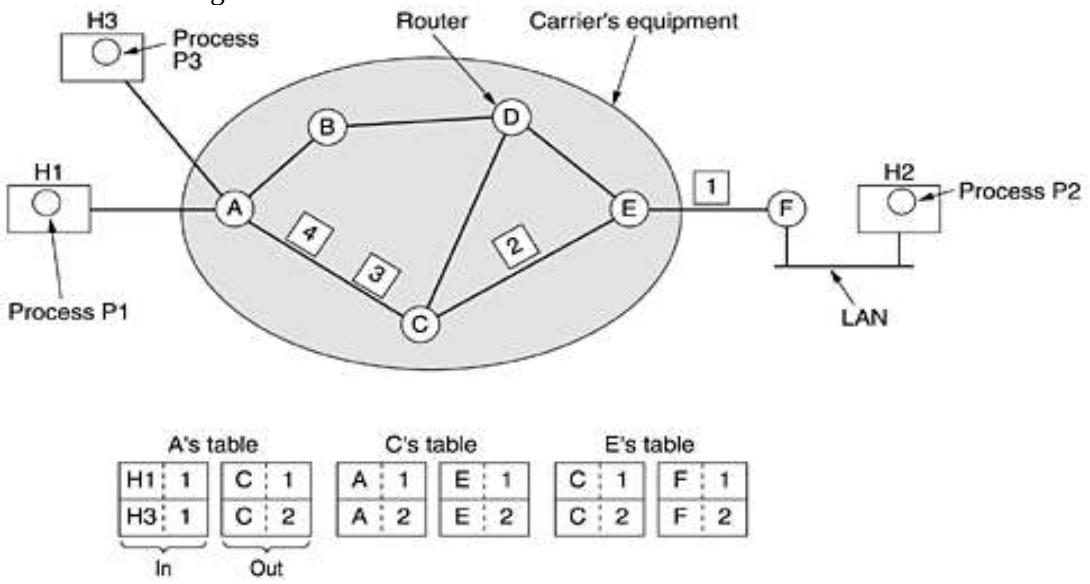
✓Only directly-connected lines can be used.

✓The algorithm that manages the tables and makes the routing decisions is called the routing algorithm.

4) Implementation of connection-oriented service:

- ✓ When a connection is established, a route from the source machine to the destination machine is chosen as part of the connection setup and stored in tables inside the routers.
- ✓ That route is used for all traffic following over the connection, exactly the same way that the telephone system works.

- ✓ When the connection is released, the virtual circuit is also terminated.
- ✓ With connection-oriented service, each packet carries an identifies telling which virtual circuit it belongs to.



5) Comparison of virtual-circuit and datagram subnets:

Issue	Datagram Subnet	Virtual-circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State Information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up, all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VC that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated for each VC.
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC.

Routing Algorithms

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

1. **Non-Adaptive**
2. **Adaptive**

- Non-adaptive algorithms do not base their routing decisions on measurements or estimates of the current traffic and topology.

- The choice of the route to use to get from I to J (for all I and J) is computed in advance, off-line and downloaded to the routers, when the routers when the network is booted. This procedure is sometimes called **static routing.**
- Adaptive algorithms change their routing decisions to reflect changes in the topology, and usually the traffic as well. This procedure is called **dynamic routing.**

1.The optimality principle

- ✓ One can make a general statement about optional routes without regard to network topology as traffic. This statement is known as the optimality principle.
- ✓ It states that if router J is on the optimal path from router I to router k, then the optimal path from J to K also falls along the same route.

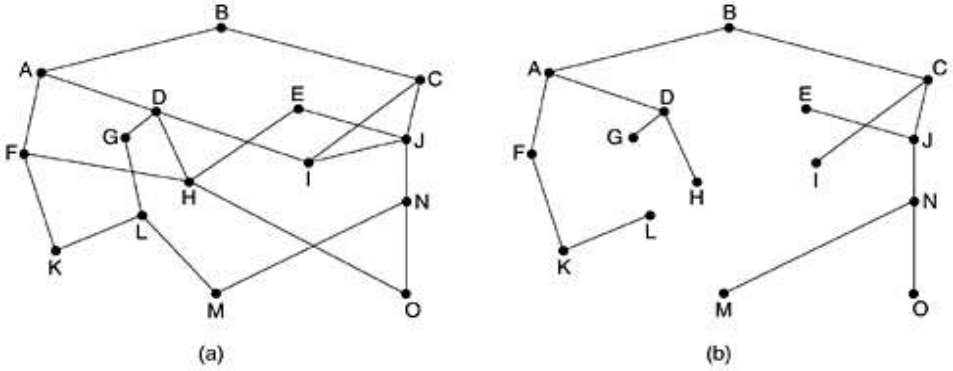


Fig: (a) A subnet. (b) A sink tree for router B

- ✓ The set of optimal routes from all sources to a given destination from a tree rooted at the destination. Such a tree is called a **sink tree.**

2.The shortest path routing:

To build a graph of the subnet, with each node of the graph representing a router and each arc of the graph is representing a communication line (often called a line).

- ✓ To choose a route between a given pair of routers, the algorithm just finds the shortest path between them on the graph.
- ✓ To illustrate how the labeling algorithm works, look at the weighted, undirected graph, where the weights represent, for example, distance, we want to find the shortest path from A to D.
- ✓ We start out by marking node A as permanent, indicated by a filled-in circle.

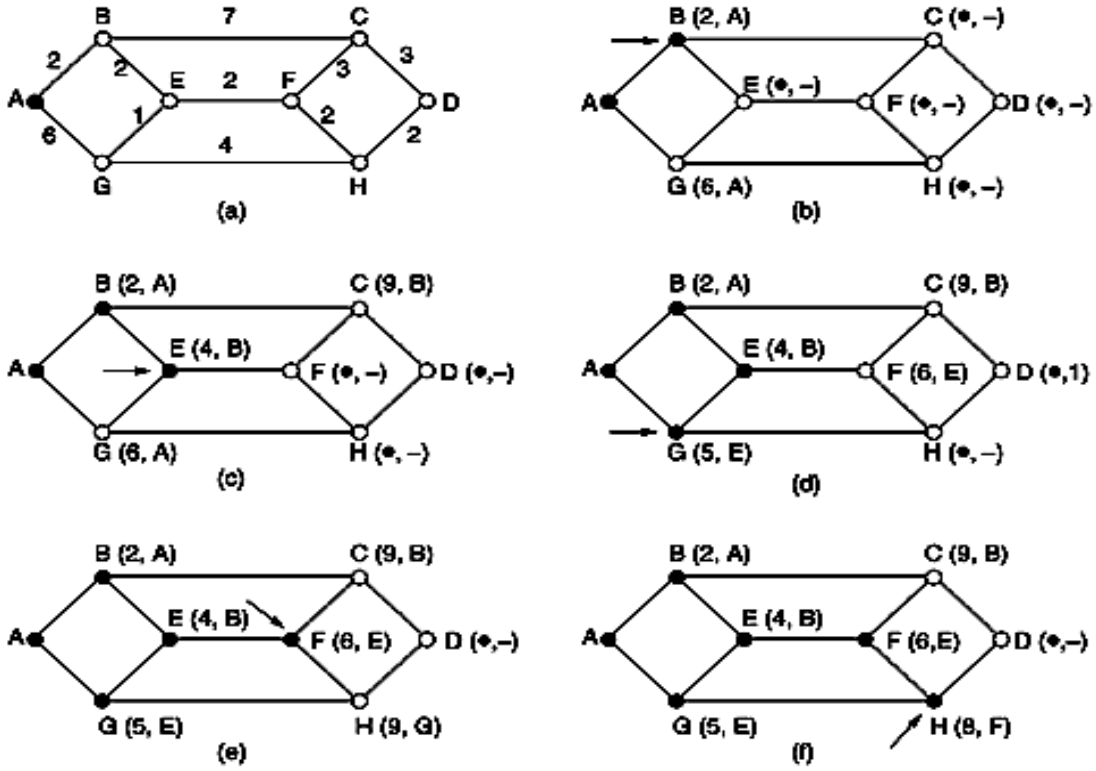


Fig: The first five steps used in computing the shortest path from A **to** D**. The arrows indicate the working node.**

- ✓ Each of the nodes adjacent to A (the working node), relabeling each one with the distance to A.
- ✓ Whenever a node is relabeled, we also label it with the node from which the probe was made so that we can reconstruct the final path later.
- ✓ Having examined each of the nodes adjacent to A, we examine all the tentatively labeled nodes in the whole graph and make the one with the smallest label permanent, as shown in fig (b).
- ✓ This one becomes the new working node.
- ✓ We now start at B and examine all nodes adjacent to it. If the sum of the label on B and the distance from B to the node being considered is less than the label on that node, we have a shorter path, so the node is relabeled, if it is shortest path.
- ✓ After all the nodes adjacent to the working node have been inspected and the tentative labels changed if possible, the entire graph is searched for the tentatively-labeled node with the smallest value.
- ✓ This node is made permanent and becomes the working node for the next round.

3.The flooding:

- ✓ The static algorithm is flooding, in which every incoming packet is sent out on every outgoing line except the one it arrived on.
- ✓ Flooding obviously generates vast numbers of 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.
- ✓ To achieve this goal is to have the source router put a sequence number in each packet it receives from its hosts.
- ✓ Each router then needs a list per source router telling which sequence numbers originating at that source have already been seen.
- ✓ If an incoming packet is on the list, it is not flooded.
- ✓ For example, it can be used in military applications, distributed applications and wireless networks.

4.The distance vector routing:

- ✓ Distance vector routing algorithm operate by having each router maintain a table (i.e. a vector) giving the best known distance to each destination and which line to use to get there. These tables are updated by exchanging information with the neighbors.
- ✓The distance vector routing algorithm is sometimes called the distributed Bellman-Ford routing algorithm and the Ford-Fulkerson algorithm. It was the original ARPANET routing algorithm.
- ✓In distance vector routing, each router maintains a 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 that destination and an estimate of the time or distance to that destination.
- ✓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 simply examines each queue. If the metric is delay, the router can measure it directly with special ECHO packets that the receiver just timestamps and sends back as fast as it can.

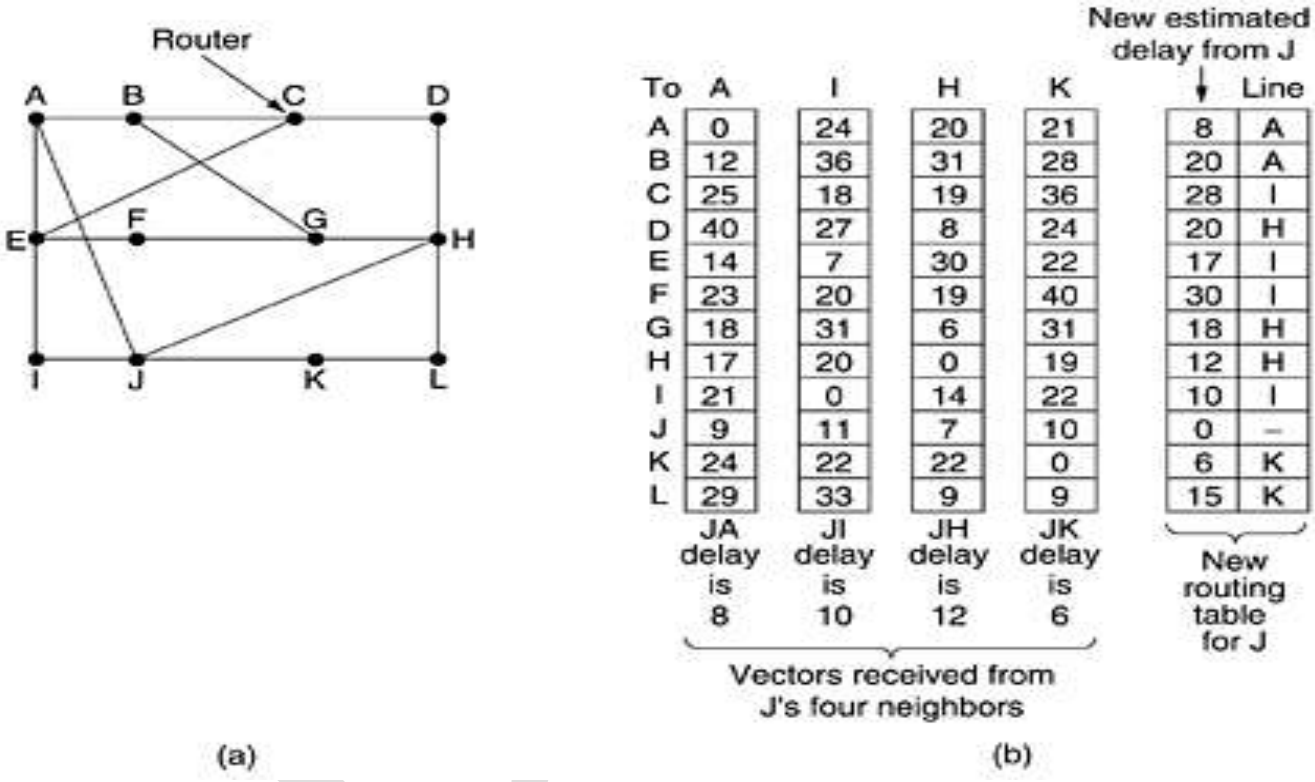


Fig: (a) A subnet. (b) Input from A**,** I**,** H**,** K**, and the new routing table for** J**.**

The fig(a) shows a subnet. The first four columns of part (b) show the delay vector received from the neighbours of router J. A claims to have 12-msec delay to B, a 25-msec delay to C, a 40-msec delay to D, etc. Suppose that j has measured or estimated its delay to its neighbours, A, I, H and K as 8, 10, 12 and 6-msec, respectively.

4.The link state routing:

The link state routing is simple and has five parts. Each router has:

1. Discover its neighbors and learn this network addresses.
2. Measure the delay or cost to each of its neighbors.
3. Construct a packet telling all it has just learned.
4. Send this packet to all other routers.
5. Compute the shortest path to every other router.

1.Learning about the neighbors:

When a router is booted, its first task is to learn who its neighbors. By sending a special HELLO packet on each point-to-point line. The router on the other end is expected to send back a

reply telling who it is. The three routers are all connected to F, it is essential that it can determine whether all three mean the same F.

When two or more routers are connected by a LAN, the situation is slightly more complicated. Fig(a) illustrates a LAN to which three routers A, C, and F, are directly connected. Each of these routers is connected to one or more additional routers, as shown.

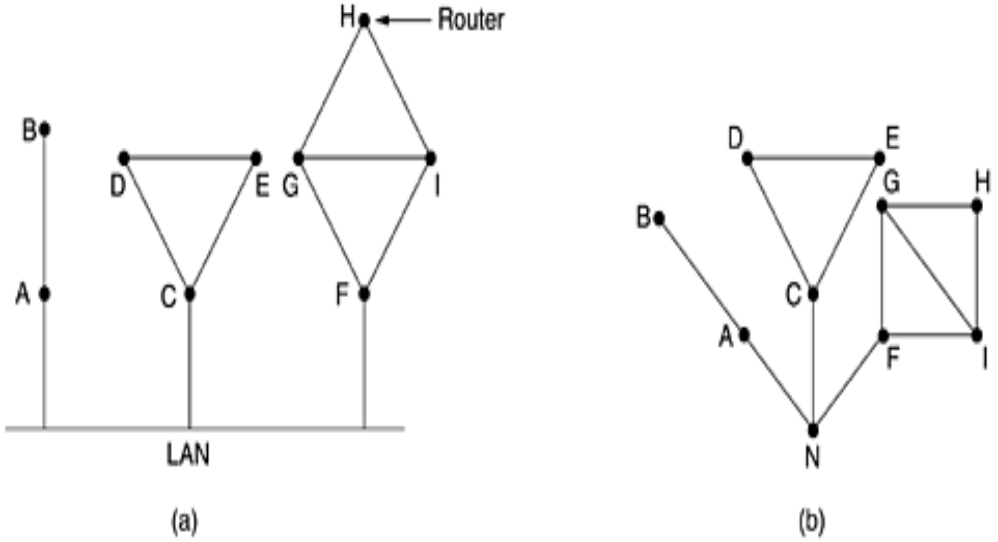


Fig: (a) Nine routers and a LAN. (b) A graph model of (a).

2. Measuring line cost:

The most direct way to determine this delay is to send over the line a special ECHO packet that the other side id required to send back immediately. By measuring the round-trip time and dividing it by two, the sending router can get a reasonable estimate of the delay.

Consider the subnet of fig 5.12, which is divided into two parts, East and West, connected by two lines CF and EI.

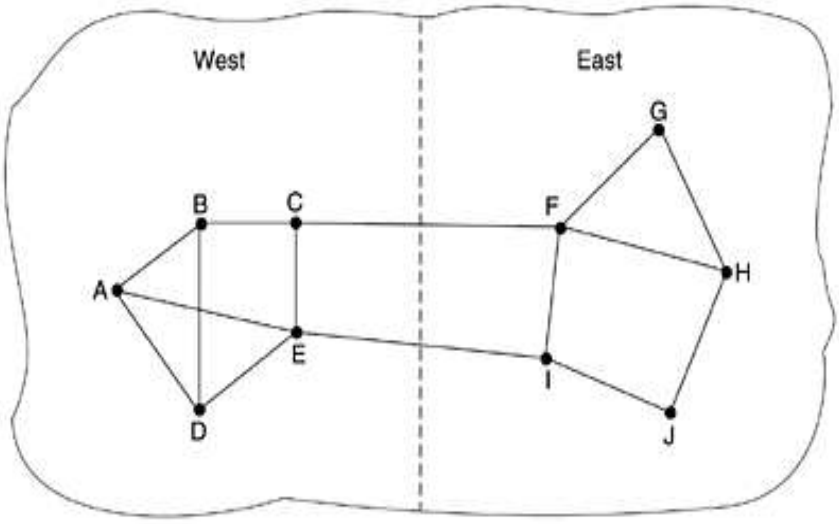


Fig: A subnet in which the East and West parts are connected by two lines.

3. Building link state packets:

The packet starts with the identity of the sender, followed by a sequence number and age, and a list of neighbors. For each neighbors, the delay to that neighbors is given. An example subnet is

given in fig(a) with delays shown as labels on the links. The corresponding link state packets for all six routers are shown in fig(b).

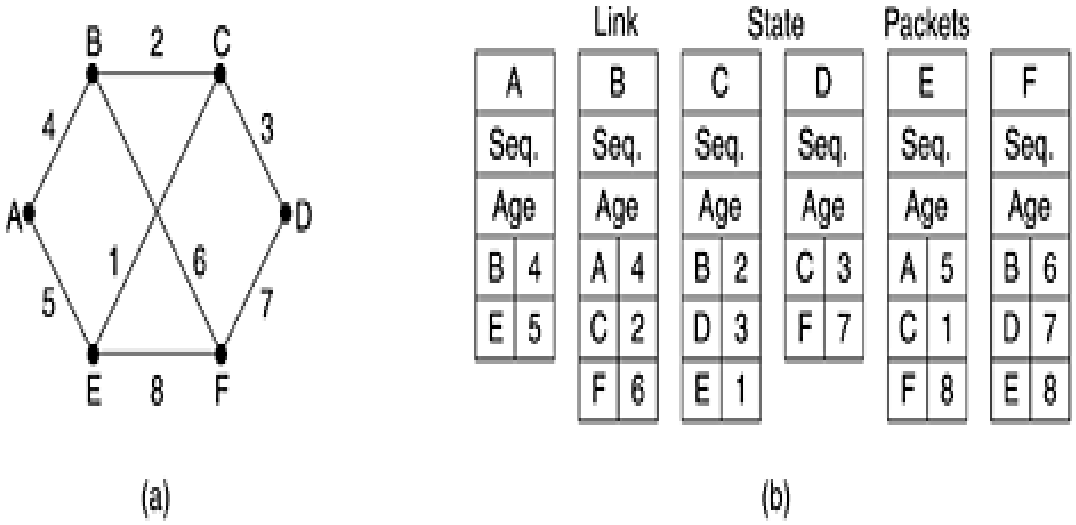


Fig: (a) A subnet. (b) The link state packets for this subnet

4. Distributing the link state packets:

The packets are distributed and installed, the routers getting the first ones will change their routes. The different routers may be using different versions of the topology, which can lead to inconsistencies, loops, unreachable machines and other problems.

The fundamental idea is to use flooding to distribute the link state packets. To keep the flood in check, each packet contains a sequence number that is incremented for each new packet sent. Routers keep track of all the (source router, sequence) pairs they see. When a new link state packet comes in, it is checked against the list of packets already seen. If it is new, it is forwarded on all lines except the one it arrived on. If it is a duplicate, it is discarded.

5. Computing the new routes:

Once a router has accumulated a full set of link state packets, it can construct the entire subnet graph because every link is represented. Every link is, in fact, represented twice, once for each direction. For a subnet with n routers, each of which has k neighbors, the memory required to store the input data is proportional for kn. For large subnets, this can be a problem.

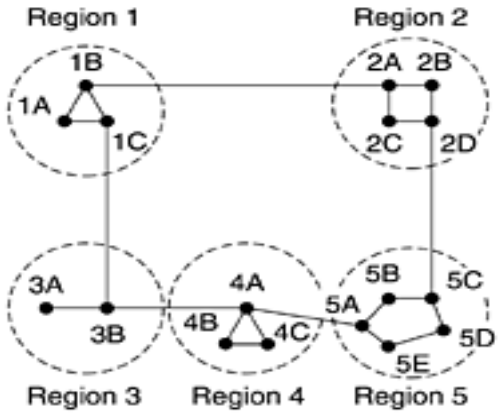
6.The Hierarchical routing.

- ✓ As network grow in size, the router routing tables grows.
- ✓ The router memory consumed by ever-increasing tables, but more CPU time is needed to scan them and more bandwidth is needed to send status reports about them.
- ✓ Every router to have an entry for every other router, so the routing will have to be done hierarchically.
- ✓ In hierarchical routing, the route packets to destinations within its own region, but knowing nothing about the internal structure of other regions.
- ✓ When different networks are interconnected, each one as a separate region in order to free the routers in one network from the topological structure of the other ones.
- ✓ For huge networks, a two-level hierarchy may be insufficient, it may be necessary to group the regions into clusters, the clusters into zones, the zones into groups, and so on.
- ✓ Fig. gives a quantitative example of routing in a two-level hierarchy with five regions. The full routing table for routers 1A has 17 entries, as fig (b).

- ✓ When routing is done hierarchically, as fig(c), there are entries for all the local routers as before, but all other regions have been condensed into a single router, so all traffic for region 2 goes via the 1B-2A line, but the rest of the remote traffic goes via the 1C-3B line.
- ✓ Hierarchical routing has reduced the table from 17 to 7 entries.

For example, the best route from 1A to 5C is via region 2, but with hierarchical routing all traffic to region 5 goes via region 3, because that is better for most destinations in region 5.

For example, consider a subnet with 720 routers. If there is no hierarchy, each router needs 720 routing table entries. If the subnet is partitioned into 24 regions of 30 routers each, each router needs 30 local entries plus 23 remote entries for a total of 53 entries. If a three-level hierarchy is chosen, with eight clusters, each containing a regions of 10 routers, each router needs 10 entries for local routers, 8 entries for routing to other regions within its own cluster, and 7 entries for distant clusters, for a total of 25 entries.



(a)

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	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

(b)

Hierarchical table for 1A

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

(c)

Fig: Hierarchical routing

7.The broadcasting routing.

Sending a packet to all destinations simultaneously is called *broadcasting*.

- ✓ The first method, which requires no special features from the subnet is for the source to simply send a distinct packet to each destination. It is also *called multi-destination routing*.
- ✓ When a packet arrives at a router, the router checks all the destinations to determine the set of output lines that will be needed.
- ✓ Multi-destination routing is like separately addressed packets, except that when several packets must follow the same route, one of them pays full fare and the rest ride free.
- ✓ The router forwards copies of it onto all lines except the one it arrived on.
- ✓ The broadcast packet arrived on a line other than the preferred one for reaching the source; the packet is discarded as a likely duplicate.

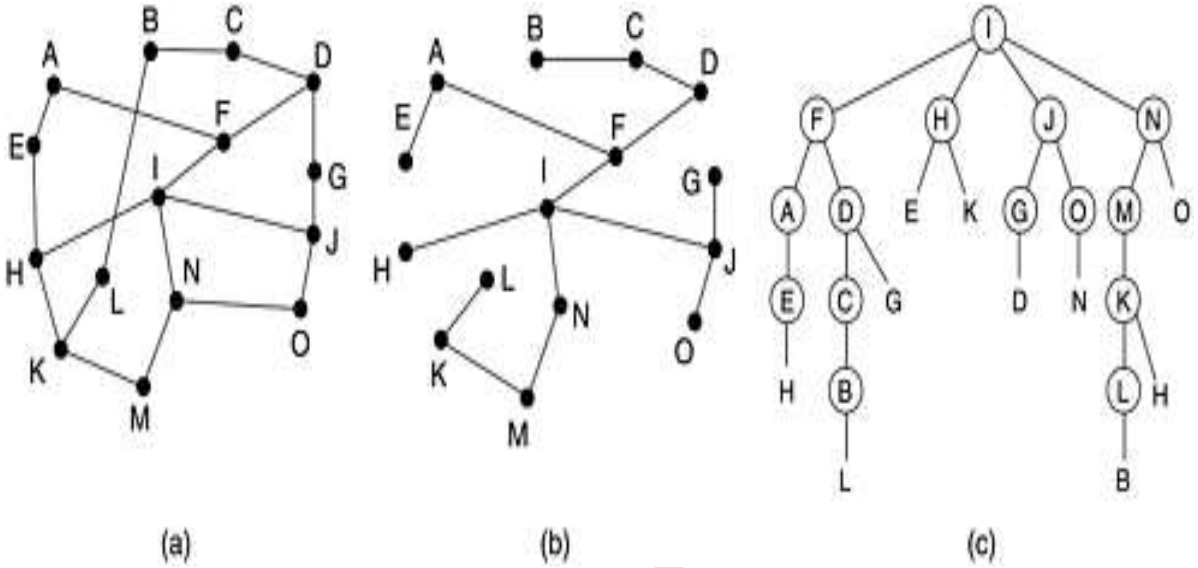


Fig: Reverse path forwarding. (a) A subnet. (b) A sink tree. (c) The tree built by reverse path forwarding

- ✓On the first hop, I send packets to F, H, J, and N, as indicated by the second row of the tree.
- ✓Each of these packets arrives on the preferred path to I (assuming that the preferred path falls along the sink tree) and indicated by a circle around the letter.
- ✓On the second hop, eight packets are generated, two by each of the routers that received a packet on the first hop.

.

8.The multicast routing.

- ✓ One process to send a message to all the other member of the group.
- ✓ Sending a message to a group is 4
- ✓ In multicast routing, each router computes a spanning tree covering all other routers. For example, in fig (a) we have two groups, 1 and 2. Some routers are attached to hosts that belong to one or both of these groups.
- ✓ A spanning tree for the leftmost router is shown in fig (b). 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 of the group. Fig (c) shows the pruned spanning tree for group 1. Fig (d) shows the pruned spanning tree for group 2. Multicast packets are forwarded only along the appropriate spanning tree.

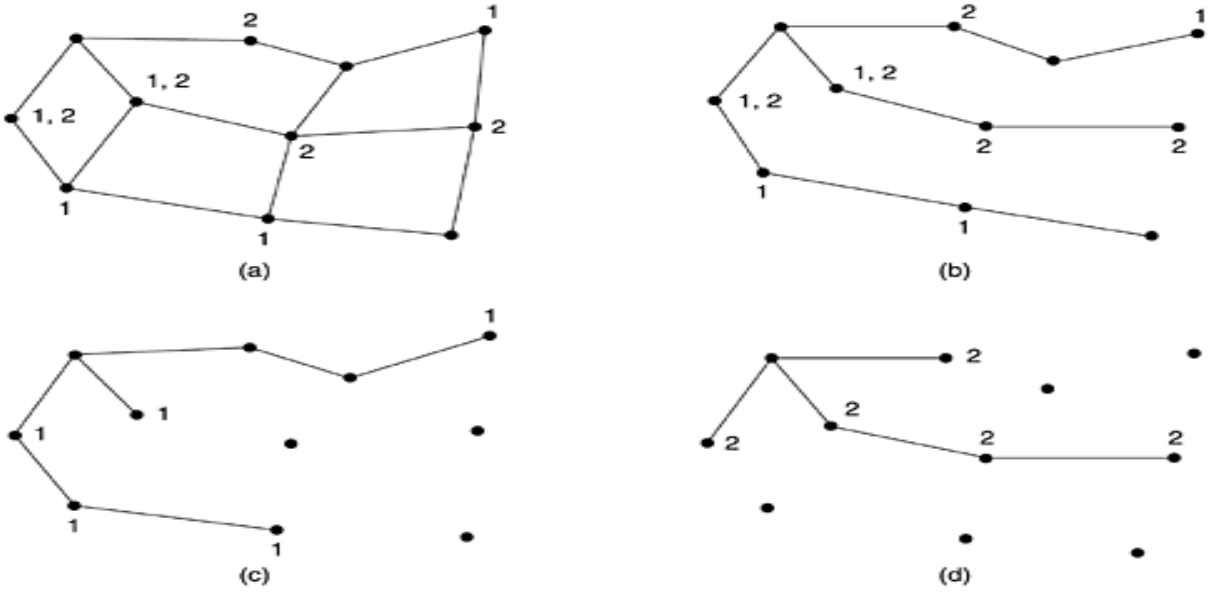


Fig: (a) A network. (b) A spanning tree for the leftmost router. (c) A multicast tree for group 1. (d) A multicast tree for group 2.

Disadvantages:

- ✓ Suppose that a network has n groups, each with an average of m members.
- ✓ For each group m pruned spanning trees must be stored for a total of mn trees
- ✓ When many large groups exists, considerable storage is needed to store all the trees.

The routing for mobile hosts:

We have a WAN consisting of routers and hosts. Connected to the WAN are LANs, MANs and wireless cells.

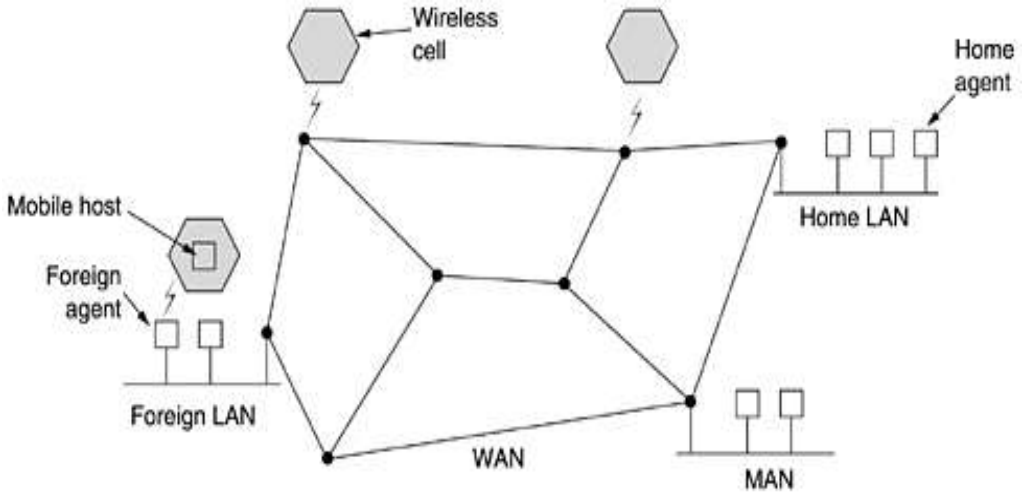


Fig: A WAN to which LANs, MANs, and wireless cells are attached

Hosts that never move are said to be stationary. They are connected to the network by copper wires or fiber optics.

Kind of hosts:

(i) Migratory host

It basically stationary hosts who move from one fixed site to another from time to time but use the network only when they are physically connected to it.

(ii) Roaming host:

Roaming host actually compute on the run and want to maintain in their connections as they move around.

- ✓In fig. the world is divided up into small units called as areas, area is typically a LAN or wireless cell.
- ✓Each area has one or more foreign agent which are processes that keep track of all mobile host visiting the area.
- ✓In addition each area has a home agent which keeps track of hosts whose home is in the area, but who are currently visiting another area.
- ✓If new host enters into the area, the computer should register itself with the foreign agent there.
- ✓Foreign agents announcing its address to mobile host, if not the mobile hosts can broadcast a packet for asking any foreign agent is there.
- ✓The mobile host registers with the foreign agent, the foreign agent contacts the mobile hosts home agent to inform about the mobile host to register.
- ✓The home agent examines the security information and sent acknowledgement to the foreign agent, the foreign agent makes an entry in its table and inform the mobile host that is now registered.

CONGESTION CONTROL ALGORITHMS

Congestion control Algorithm:

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

As traffic increases too far, the routers are no longer able to cope and they begin losing packets.

At very high trafffic, performance collapses completely and almost no packets are delivered.

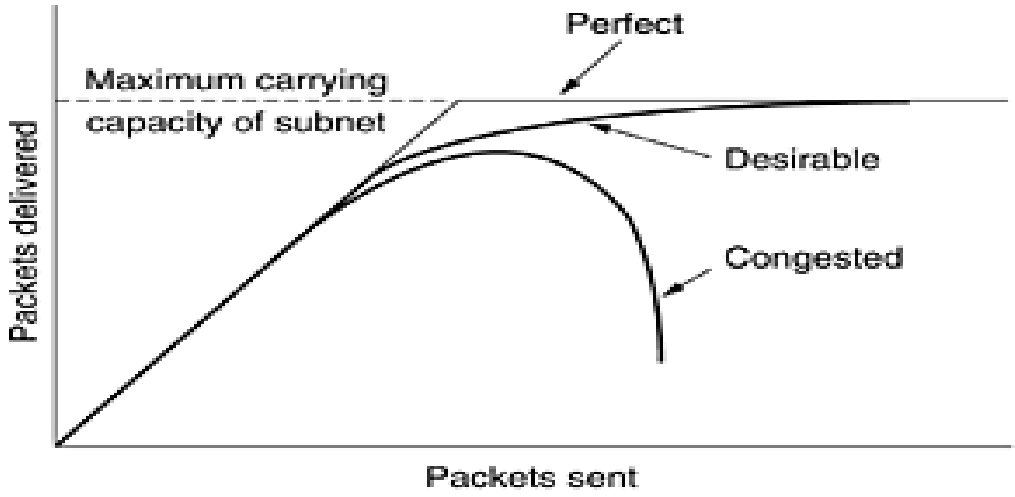


Fig: When too much traffic is offered, congestion sets in and performance degrades sharply

Congestion can be brought on by several factors:

- If all of a sudden, streams of packets begin arriving on three or four input lines and all need the same output line, a queue will build up. If there is insufficient memory to hold all of them, packets will be lost.
- Slow processors can also cause congestion. If the routers' CPUs are slow at performing the bookkeeping tasks required of them (queuing buffers, updating tables, etc.), queues can build up, even though there is excess line capacity.
- Low-bandwidth lines can also cause congestion. Upgrading the lines but not changing the processors, or vice versa, often helps a little, but frequently just shifts the bottleneck.

1.General Principles of congestion control:

This approach leads to dividing all solutions into two groups:

Open loop and closed loop.

- ✓ Open loop solutions attempts to solve the problem by good design.
- ✓ 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.
- ✓ 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.**

The closed loop algorithms are also divided into two subcategories:

Explicit feedback versus implicit feedback.

In explicit feedback algorithms, packets are sent back from the point of congestion to warn the source.

In implicit algorithms, the source deduces the existence of congestion by making local observations, such as the time needed for acknowledgements to come back.

2.Congestion prevention policies:

Layer	**Policies**
Transport	Retransmission Policy Out-of-order caching policy Acknowledgement policy Flow control policy Timeout determination
Network	virtual circuits versus datagram inside the subnet packet queuing and service policy packet discard policy routing algorithm packet lifetime management
Data link	Retransmission Policy Out-of-order caching policy Acknowledgement policy Flow control policy

- ✓**Retransmission policy** is concerned with how fast a sender times out and what it transmit upon time out.
- ✓Retransmitting all outstanding packets using go back N will put a heavier load on the system than will a leisurely sender that uses selective repeat.
- ✓**Out-of order packets** will have to be transmitted again later, creating extra load.
- ✓**Acknowledgement policy** also affects congestion if each packet is acknowledged immediately, the acknowledgement packets generate extra traffic.
- ✓A tight **flow control** scheme reduces the data rate and thus helps fight congestion.
- ✓**In network layer congestion occurred** in both but algorithm work only with virtual-circuit subnets.
- ✓**In packet queuing** the ordering of packets are processed whether routers have one queue per input line, one queue per output line or both.
- ✓**Discard policy** is the rule telling which packets is dropped when there is no space.
- ✓**A good routing algorithm** can help to avoid congestion and bad one can send too much traffic over already congested lines.
- ✓**Packet lifetime management** deals, how long a packet works long time or too short, if short before reaching destination time out including retransmission.
- ✓The same issues in the transport layer is also occurred in data link layer.

3.Virtual-Circuit subnets:

- ✓It is widely used to keep congestion that has already started from getting worse is **admission control.**
- ✓Once congestion has been signaled, no more virtual circuits are set up until the problem has gone away.
- ✓Attempts to set up new transport layer connections fail.
- ✓While this approach is crude, it is simple and easy to carry out. In the telephone system, when a switch gets overloaded, it also policies admission control by not giving dial tones.

For example, consider the subnet of fig(a) in which two routers are congested.

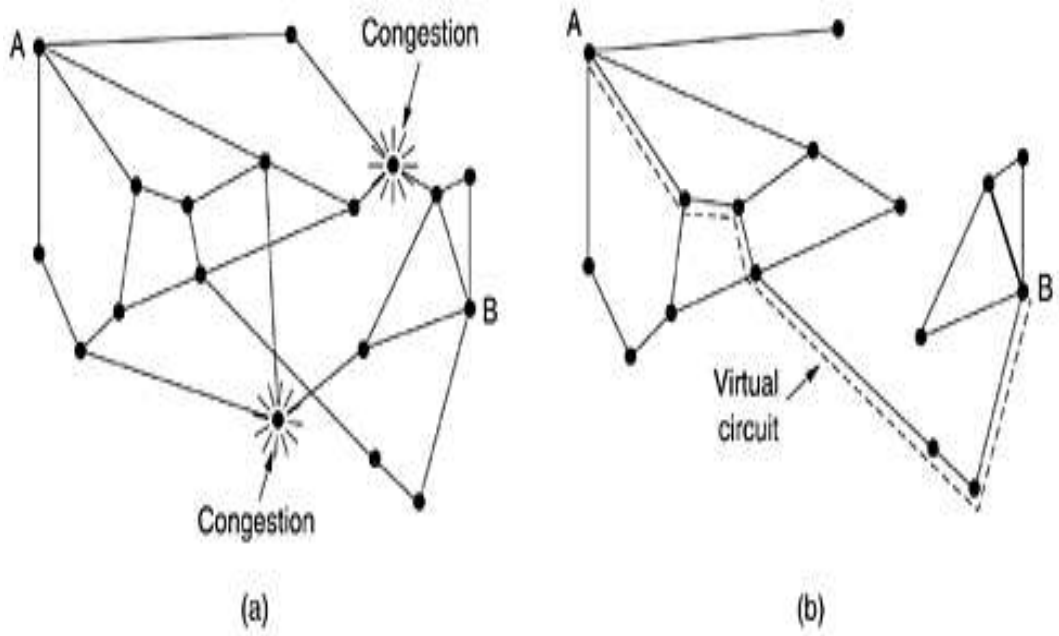


Fig: a) A congested subnet. (b) A redrawn subnet that eliminates the congestion. A virtual circuit from A **to** B **is also shown.**

- ✓ Suppose that a host attached to router A wants to set up a connection to a host attached to router B.
- ✓ This connection would pass through one of the congested routers.
- ✓ To avoid this situation, we can redraw the subnet as shown in fig(b), omitting the congested routers and all of their lines.
- ✓ The dashed line shows a possible route for the virtual that avoids the congested routers.

4.Datagram subnets:

Each router can easily monitor the utilization of its output and other resources. For example, it can associate with each line a real variable, u, whose value, between 0.0 and 1.0, reflects the recent utilization of that line. To maintain a good estimate of u, a sample of the instantaneous line utilization, f (either 0 or 1), can be made periodically and u updated according to

$$U_{new}=qu_{old}+(1-a)f$$

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

The warning bit:

The old DECNET architecture signaled the warning state by setting a special bit in the packet's header.

So does frame delay. When the packet arrived at its destination, the transport entity copied the bit into the next acknowledgement sent back to the source. The source then cut back on traffic.

Choke Packets:

The router sends a choke packet back to the source host, giving it the destination found in the packet.

When the source host gets the choke packet, it is required to reduce the traffic sent to the specified destination by X percent.

Hop-by-Hop choke packets:

At high speeds or over long distances, sending a choke packet to the source hosts does not work well because the reaction is so slow.

For example, a host in San Francisco (router A in fig) that is sending traffic to a host in New York host (router D in fig.) at 155 mbps. If the New York host begins to run out of buffers, it will take about 30 msec for a choke packet to get back to San Francisco to tell it to slow down.

5.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.
- ✓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.

6.Jitter Control:

- ✓For application such as audio and video streaming, it does not matter much if the packets take 20 msec or 30 msec to be delivered, as long as the transmit time is constant.
- ✓The variation in the packet arrival times is **called jitter**.
- ✓High jitter, for example, having some packets taking 20 msec and others taking 30 msec to arrive will give an uneven quality to the sound or movie.

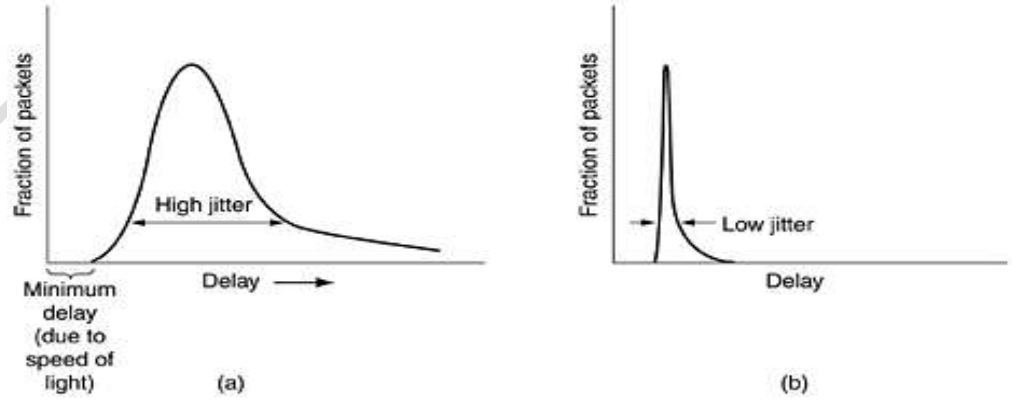


Fig:(a) High jitter. (b) Low jitter

Quality of Service

1) Requirements:

A stream of packets from a source to a destination **is called a flow**. In a connection-oriented network, all the packets belonging to a flow follow the same route; in a connectionless network, they may follow different routes. The needs of each flow can be characterized by **four primary parameters: reliability, delay, jitter and bandwidth**. Together these determine **the QoS (Quality of Service) the flow requires**.

Several applications and their requirements are listed below:

- ✓The first four applications have stringent requirements on reliability.
- ✓This goal is usually achieved by check summing each packet and verifying the checksum at the destination.
- ✓The four final (audio/video) applications can tolerate errors, so no checksums are computed or verified.
- ✓File transfer applications, including e-mail and video are not delay sensitive. Interactive applications, such as web surfing and remote login, are more delay sensitive.
- ✓Real-time applications, such as telephony and videoconferencing have strict delay requirements playing audio or video files from a server does not require low delay.

ATM networks classify flows in four broad categories with respect to their QoS demands as follows:

1) Constant bit rate (e.g., telephony)
2) Real-time variable at rate (e.g., compressed video conferencing)
3) Non-real-time variable bit rate (e.g., watching a movie over the Internet)
4) Available bit rate (e.g., File transfer)

2) Techniques for achieving good quality of service:

Some of the techniques system designers use to achieve QoS:

Overprovisioning:

An easy solution is to provide so much router capacity, buffer space and bandwidth that the packets just fly through easily. The trouble with this solution is that it is expensive.

Buffering:

In fig, we see stream a packets being delivered with substantial jitter. Packet 1 is sent from the server at t=0 sec and arrives at the client at t=1 sec. Packet 2 undergoes more delay and takes 2 sec to arrive. As the packets arrive, they are buffered on the client machine.

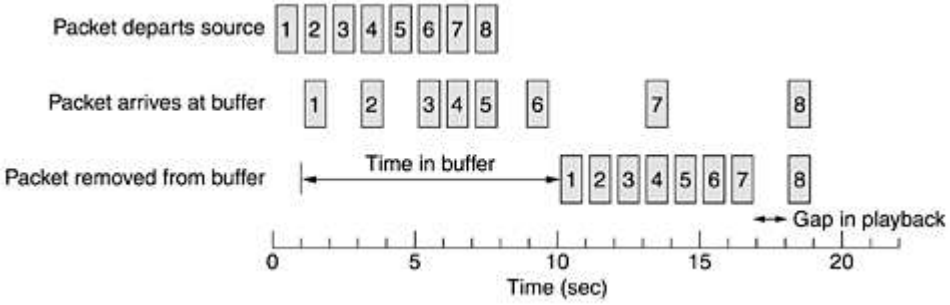


Fig: Smoothing the output stream by buffering packets.

At t=0 sec, playback begins. At this time, packets 1through 6 have been buffered so that they can be removed from the buffer at uniform intervals for smooth play. Packet 8 has been delayed so much that it is not available when its play slot comes up, so playback must stop until it arrives, creating an annoying gap in the music or movie.

Traffic Shaping:

- ✓ The source outputs the packets with a uniform spacing between them, but in other cases, they may be emitted irregularly, which may cause congestion to occur in the network.
- ✓ Nonuniform output is common if the server is handling many streams at once, and it also allows other actions, such as fast forward and rewind, uses authentication, and so on.
- ✓ We used here (buffering) is not always possible, for example, with videoconferencing. However, if something could be done to make the server (and hosts in general) transmit at a uniform rate, quality of service would be better.

- ✓ With a technique, traffic shaping, which smooth out the traffic on the server side, rather than on the client side.
- ✓ Traffic shaping is about regulating the average rate of data transmission. In contrast, the sliding window protocols, the amount of data in transit at once, not the rate at which it is sent.
- ✓ When a connection is set up, the user and the subnet (i.e., the customer and the carrier) agree on a certain traffic pattern (i.e., shape) for that circuit. Sometimes is called **a service level agreement.**

The leaky bucket algorithm:

- ✓ Imagine a bucket with a small hole in the bottom, as illustrated in fig (a). No matter the rate at which water enters the bucket, the overflow is at a constant rate, p.
- ✓ When there is any water in the bucket and zero when the bucket is empty. Once the bucket is full, any additional water entering it spills over the sides and is lost.
- ✓ The same idea can be applied to packets, as shown in Fig (b). Each host is connected to the network by an interface containing a leaky bucket, a finite interval queue.
- ✓ If a packet arrives at the queue when it is full, the packet is discarded. This arrangement can be built into the hardware interface or stimulated by the host operating system.
- ✓ It was first proposed by Turner (1986) and is called the leaky bucket algorithm.

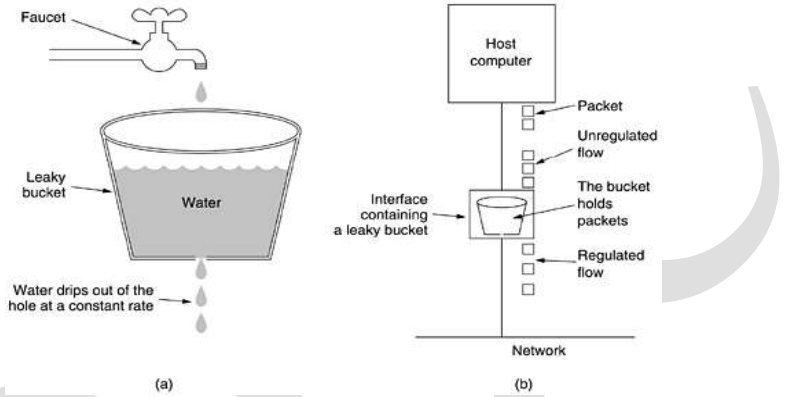


Fig: (a) A leaky bucket with water. (b) A leaky bucket with packets

- ✓ 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).
- ✓ The byte-counting leaky bucket is implemented almost the same way. At each tick, a counter is initialized to n.
- ✓ If the first packet on the queue has fewer bytes than the current value of the counter, it is transmitted, and the counter is decremented by that number of bytes.
- ✓ Additional packets may also be sent, as long as the counter is high enough.
- ✓ When the counter drops below the length of the next packet on the queue, transmission stops until the next tick, at which time the residual byte count is reset and the flow can continue.

The token bucket algorithm:

- ✓ In fig (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 fig (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 token bucket algorithm does allow saving, upto the maximum size of the bucket n.
- ✓ This property means that burst of upto n packets can be sent at once, allowing some bushiness in thin the output stream and giving faster response to sudden burst of input.
- ✓ A host can make the host stop sending when the rules say it must. Telling a router to stop sending while its input keeps pouring in may result in lost data.

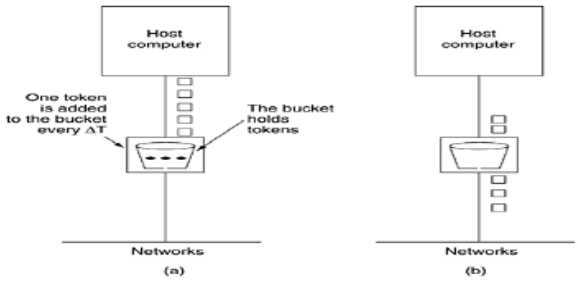


Fig: The token bucket algorithm. (a) Before. (b) After

- ✓ The implementation of the basic token bucket algorithm is just a variable that counts token. The counter is incremented by one every ΔT and decremented by one whenever a packet is sent.
- ✓ When the counter hits zero, no packets may be sent. In the byte-count variant, the counter is incremented by k bytes ΔT and decremented by the length of each packet sent.

INTERNETWORKING

The Internetworking:

When two or more networks are connected to from an Internet.

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

1.How network differ:

- ✓ Networks can differ in many ways.
- ✓ Packets sent from source to destination it travel many intermediate foreign networks before reach to destination.
    - ✓ Protocol conversion are required to handle the situations such as
    - ✓ reordering,
    - ✓ Address Conversions,
    - ✓ different packet sizes used by different networks,
    - ✓ quality of services,
    - ✓ multicasting,
    - ✓ security
    - ✓ service offered etc.

2.How networks can be connected:

- ✓ Networks can be interconnected by different devices such as repeaters, hubs, bridges and switches, routers etc.
- ✓ Each one used in different layers to transmit from one network to another.
- ✓ A router that can handle multiple protocols is called a multiprotocol router.
- ✓ Gateways are used in transport layer.
- ✓ In network layer interconnections represented as:

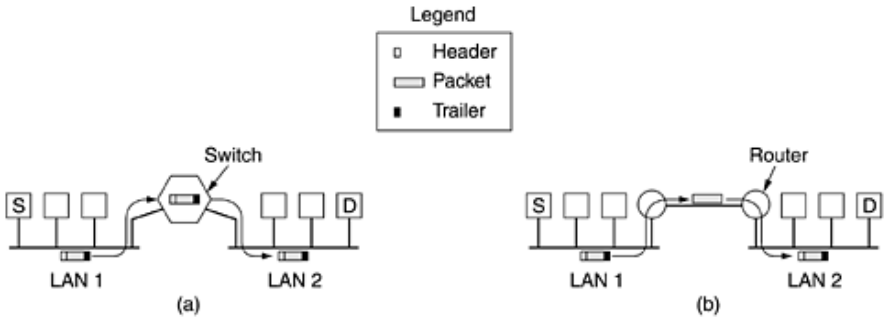


Fig: (a) Two Ethernets connected by a switch. (b) Two Ethernets connected by routers.

- ✓By using switches it just receives and sends to the particular destination.
- ✓In other internetworking, the pair of routers used instead of a switch.
- ✓The router examines the address in the packets based on this address, it decides to send the packet to the remote router.

3.Concatenated Virtual Circuits:

Two styles of internetworking are possible:

- ✓ A connection-oriented concatenation of virtual-circuit subnets and a datagram internet style.
- ✓ A connection to a host in a distant network is set up in a way similar to the way connections are normally established.
- ✓ The subnet sees that the destination is remote and builds a virtual circuit to the router nearest the destination network.
- ✓ The gateway records the existence of the virtual circuit in its tables and proceeds to build another virtual circuit to a router in the next subnet until it has been received.

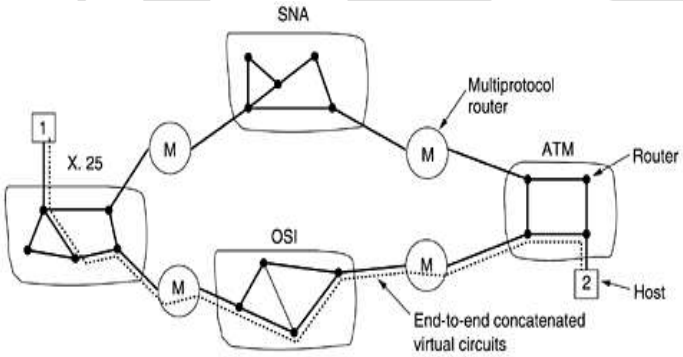


Fig: Internetworking using concatenated virtual circuits

4.Connectionless Internetworking:

- ✓ In fig datagram's from host 1 to host 2 are shown taking different routes through the Internetwork.
- ✓ 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.
- ✓ There is no guarantee that the packets arrive at the destination in order, assuming that they arrive at all.

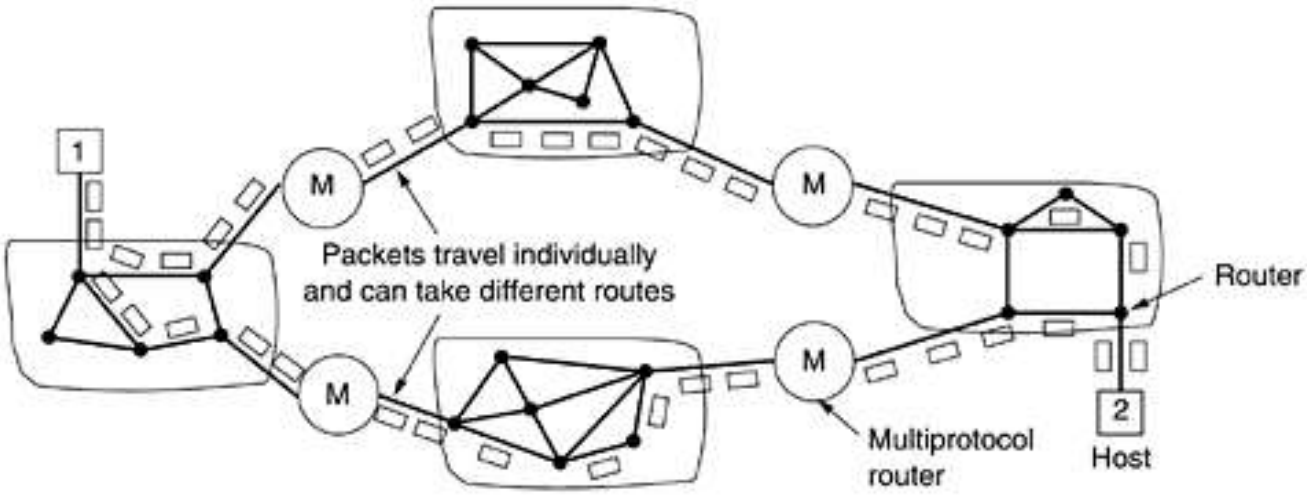


Fig: A connectionless internet

Advantages:

- ✓The virtual circuit model using a single subnet, buffers can be reserved in advance, sequencing can be guaranteed, short headers can be used etc.

Disadvantages:

- ✓Table space required in the routers for each open connections.
- ✓The datagram approach is much pretty than virtual circuit.
- ✓Various adaptive routing algorithms are possible in an internet.

5.Tunneling:

- ✓In making two different networks interwork is exceedingly difficult.
- ✓As an example, think of an international bank with a TCP/IP based Ethernet in Paris, a TCP/IP based Ethernet in London, and a non-IP wide area network (e.g., ATM) in between, as shown in fig.
- ✓The solution to this problem is a technique **called tunneling**.
- ✓To send an IP packet to host 2, host 1 constructs the packet containing the IP address of host 2, inserts it into an Ethernet frame addressed to the **pair's multi-protocol route**r, and puts it on the Ethernet.

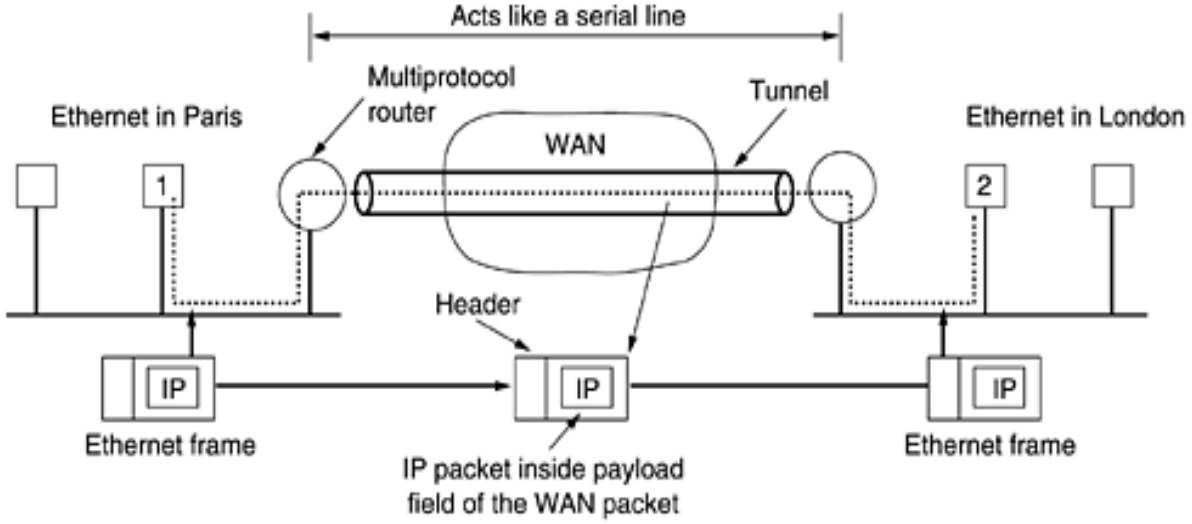


Fig: Tunneling a packet from Paris to London

6.Internetworking Routing:

- ✓ Routing through an internetworking is similar to routing within a single subnet, but with some added complications.
- ✓ Consider, for example, the internetwork of fig(a) in which five networks are connected by six routers.
- ✓ Making a graph model of this situation is complicated by the fact that every router can directly access (i.e., send packets to) every other router connected to any network to which it is connected.
- ✓ For example, B in fig (a) can directly access A and C via network 2 and also D via network 3. This leads to the graph of fig (b).

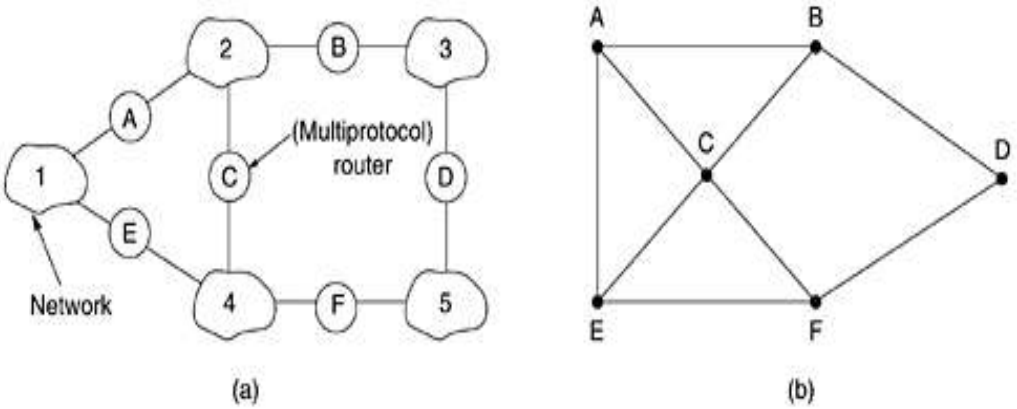


Fig: (a) An internetwork. (b) A graph of the internetwork

- ✓ Once the graph has been constructed, known routing algorithms, such as the distance vector and line state algorithm, can be applied to the set of multi-protocol routers.

7.Fragmentation:

✓Each network imposes some maximum size on its packets.

These limits have various causes, among them:

1) Hardware (e.g., the size of an Ethernet frame)
2) Operating system (e.g., all buffer are 512 bytes)
3) Protocols (e.g., the number of bits in the packet length field)
4) Compliance with some (inter)national standard
5) Desire to reduce error-induced retransmission to some level.
6) Desire to prevent one packet from occupying the channel too long.

The only solution to the problem is to allow gateways to break up packets into fragments, sending each fragment as a separate Internet packet.

- ✓The first strategy is to make fragmentation caused by a "small packet" network transparent to any subsequence networks through which the packet must pass on its way to the ultimate destination.
- ✓In this approach, the small packet network has gateways that interface to other networks.
- ✓ATM networks, for example, have special hardware to provide transparent fragmentation of packets into cells and then reassembly of cells into packets.
- ✓The other fragmentation strategy is to refrain from recombining fragments at any intermediate gateways.

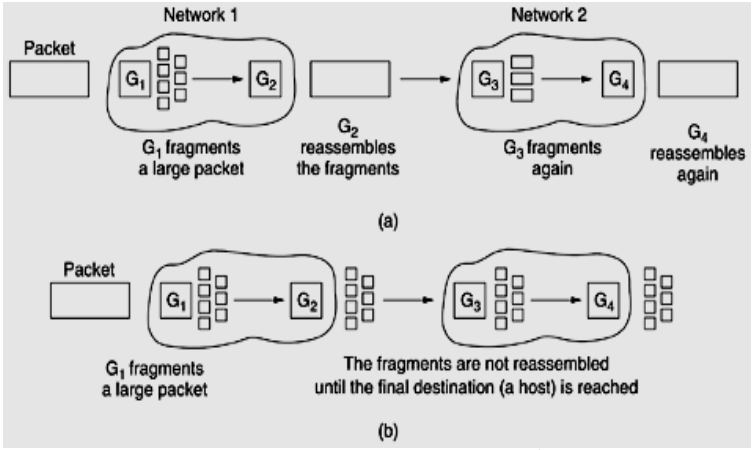


Fig: (a) Transparent fragmentation. (b) Nontransparent fragmentation

Two opposing strategies exist for recombining the fragments back into the original packet.

- ✓Once a packet has been fragmented, each fragment is treated as though it were an original packet.
- ✓All fragments are passed through the exit gateway. Recombination occurs only at the destination host IP works this way.

UNIT – IV

Transport Layer and services

1.The services provided in the upper layer in transport layer

- The transport layer makes use of the services provided by the network layer. The hardware and/or software within the transport layer that does the work are **called the transport entity.**
- The transport entity can be located in the operating system kernel, in a separate user process, in a library package bound into network applications, or conceivably on the network interface card.
- The relationship of the network, transport and application layers is shown in fig.

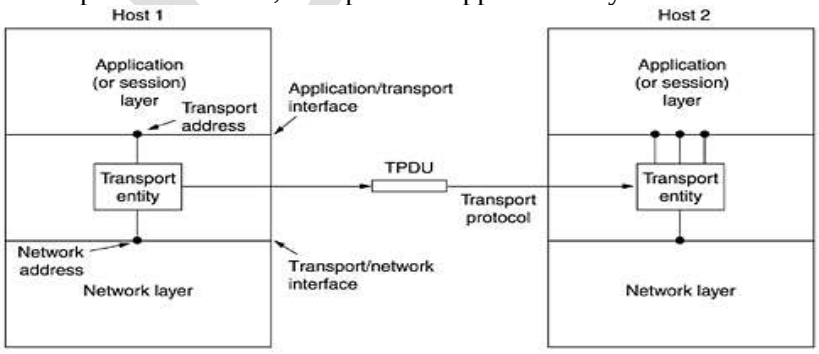


Fig: The network, transport, and application layers

- There are two types of network service, connection-oriented and connectionless. There are also two types of transport service.
- The connection-oriented transport service is similar to the connection-oriented network service in many ways.

- Connections have three phases: **establishment, data transfer and release**.
- Addressing and flow control are similar in both layers.
- The connectionless transport service is also very similar to the connectionless network service.

2. Transport service primitives

- To allow users to access the transport service, the transport layer must layer provide some operations to applications programs, that is, the transport service interface?
- Each transport service has its own interface. The transport service is similar to the network service, but there are also some important differences.
- The main difference is that the network service is intended to model the service offered by real networks. Real networks can lose packets, so the network service is generally unreliable.
- The (connection-oriented) transport layer service is reliable. Real networks are not error-free, but that is preciously the purpose of the transport layer – to provide a reliable service on top of an unreliable network.
- Consider two processes connected by pipes in UNIX. They assume the connection between them is perfect.
- They do not want to know about acknowledgements, lost packets, congestion, or anything like that. What they want is a 100 percent reliable connection. Process A puts data into one end of the pipe, and process B takes it out of the other.
- A second difference between the network service and transport service is that the services are intended for. The network service is used only by the transport entities. Few users write their own transport entities, and thus few users or programs ever see the bare network services.
- Consider the five primitives listed in fig. This transport interface is truly bare bones, but it gives the essential flavor of what a connection-oriented transport interface has to do.
- It allows application programs to establish, use, and then release connections, which is sufficient for many applications.

Primitive	**Packet Sent**	**Meaning**
LISTEN	(None)	Block until some process tries to connect
CONNECT	CONNECTION REQUEST	Actively attempt to establish a connection
SEND	DATA	Send Information
RECEIVE	(None)	Block until a DATA packet arrives
DISCONNECT	DISCONNECT REQUEST	This side wants to release the connection

Fig: The primitives for a simple transport service

- Consider an application with a server and a number of remote clients. To start with, the server executes a LISTEN primitive, typically by calling a library procedure that makes a system call to block the server until a client turns up.
- When a client wants to talk to the server, it executes a CONNECT primitive.
- The transport entity carries out this primitive by blocking the caller and sending a packet to the server.
- Encapsulated in the payload of this packet is a transport layer message for the server's transport entity.
- TPDU (Transport Protocol Data Unit) for messages sent from transport entity to transport entity.
- TPDUs (exchanged by the transport layer) are contained in packets (exchanged by the network layer). Packets are contained in frames (exchanged by the data link layer). When a frame arrives, the data link layer processes the frame header and passes the contents of the frame payload field up to the network entity.
- The network entity processes the packet header and passes the contents of the packet payload up to the transport entity.

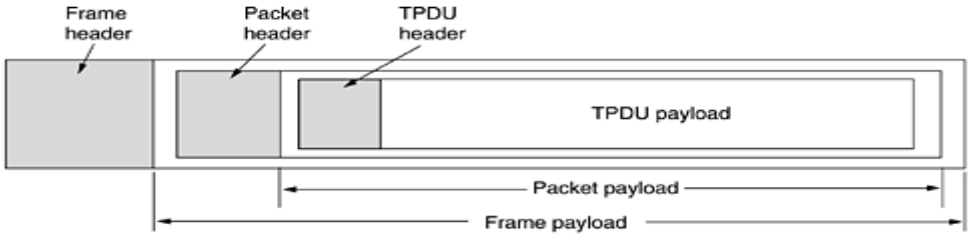


Fig: Nesting of TPDUs, packets, and frames

- Getting back to our client-server example the client's CONNECT call causes a CONNECTION REQUEST TPDU to be sent to the server.
- When it arrives, the transport entity checks to see that the server is blocked on a LISTEN (i.e., is interest in handling requests).
- It then unblocks the server and sends a CONNECTION ACCEPTED TPDU back to the client. When this TPDU arrives, the client is unblocked and the connection is established.
- Data can now be exchanged using the SEND and RECEIVE primitives. In this simplest form, either party can do a (blocking) RECEIVE to wait for the other party to do a SEND.
- When the TPDU arrives, the receiver is unblocked. It can then process the TPDU and send a reply.
- When a connection is no longer needed, it must be released to free up table space within the two transport entities.
- Disconnection has two variants: asymmetric and symmetric. In the asymmetric variant, either transport user can issue a DISCONNECT primitive, which results in a DISCONNECT TPDU being sent to the remote transport entity.
- Upon arrival, the connection is released. In the symmetric variants, each direction is closed separately, independently of the other one.
- When one side does a DISCONNECT, that means it has no more data to sent but it is small willing to accept data from its partner. In this model, a connection is released when both sides have done a DISCONNECT.

3. Berkeley sockets:

- The socket primitives used in Berkeley UNIX for TCP. These primitives are widely used for internet programming. They are listed below in fig.

Primitive	**Meaning**
SOCKET	Create a new communication end point
BIND	Attach a local address to a socket
LISTEN	Announce willingness to accept connections; give queue size
ACCEPT	Block the caller until a connection attempt arrives
CONNECT	Actively attempt to establish a connection
SEND	Send some data over the connection
RECEIVE	Receive some data from the connection
CLOSE	Release the connection

Fig: The socket primitives for TCP

- The first four primitives in the list are executed in that order by servers. The socket primitive creates a new end point and allocates table space for it within the transport entity.

- Newly-created sockets do not have network addresses. These are assigned using the BIND primitive. Once a server has bound an address to a socket, remote clients can connect to it.
- The LISTEN call, which allocates space to queue incoming calls for the case that several clients try to connect at the same time.
- To block waiting for an incoming connection, the server executes an ACCEPT primitive.
- When a TPDU asking for a connection arrives, the transport entity creates a new socket with the same properties as the original one and returns a file descriptor for it.
- ACCEPT returns a normal file descriptor, which can be used for reading and writing in the standard way, the same as for files.
- The CONNECT primitive blocks the caller and actively starts the connection process. Both sides can now use SEND and RECV to transmit and receive data over the full-duplex connection.

Connection release with sockets is symmetric. When both sides have executed a CLOSE primitive, the connection is released.

THE ELEMENTS OF TRANSPORT PROTOCOLS

- The transport service is implemented by a transport protocol used between the two transport entities.
- These differences are due to major dissimilarities between the environments in which the two protocols operate, as shown in the fig.

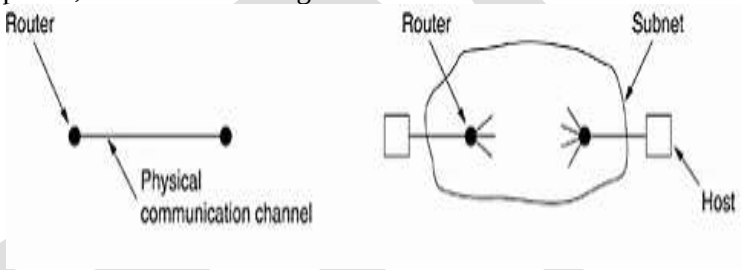


Fig: (a) Environment of the data link layer. (b) Environment of the transport layer.

- The entire data link layer, two routers communicate directly via a physical channel, whereas qt the transport layer, this physical channel is replaced by the entire subnet.
- For one thing, in the data link layer, it is not necessary for a router to specify which router it wants to talk to each outgoing line uniquely specifies a particular router.
- In the transport layer, explicit addressing of destinations is required.
- For another thing, the process of establishing a connection over the wire of fig (a) is simple: the other end is always there.

1) Addressing:

- When an application process wishes to set up connection to a remote application process, it must specify which one to connect to.
- The method normally used is to define transport addresses to which processes can listen for connection requests.
- In the internet, these end points are called ports. In ATM networks, they are called AAL-SAPs. The generic term TSAP (transport service access point). The analogous and points in the network layer (i.e., network layer addresses) are then called NSAPs. IP addresses are examples of NSAPs.

Fig. illustrates the relationship between the NSAP, TSAP and transport connection. Application processes, both clients and server, can attach themselves to a TSAP to establish a connection to a remote TSAP.

- These connections run through NSAPs on each host, as shown. The purpose of having TSAPs, is that in some networks, each computer has a single NSAP, so some way is needed to distinguish multiple transport end points that share that NSAP.

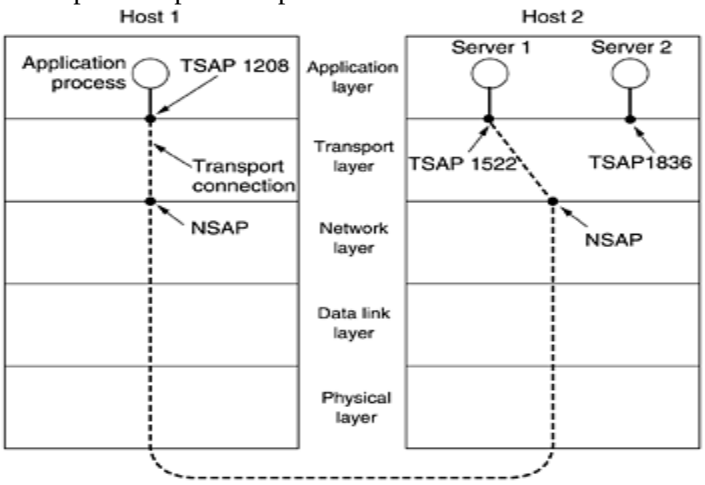


Fig: TSAPs, NSAPs, and transport connections

A possible scenario for a transport connection is as follows:

- A time of day server process on host 2 attaches itself to TSAP 1522 to wait for an incoming call.
- How a process attaches itself to a TSAP is outside the networking model and depends entirely on the local operating system. A call such as our LISTEN might be used, for example.
- The application process then sends over a request for the time.
- The time server process responds with the current time.
- The transport connection is then released.

2) Connection Establishment:

- The connection establishment looks very simple and straight forward. But the problem occurs when the network can lose, or store duplicate packets.
- Where there is heavy congestion on the subnet, the acknowledgement will not get back in time. Due to this delay, the packets are retransmitted two or three times.
- After some time the original packets may arrive at destination following different route. These duplicate create a lot of problem and confusion in real time applications.
- The solutions are proposed to avoid duplicate packets, some of them are:

Throw away transport address: If there is disconnection. Each time when transport address is needed, a new one is generated. When connection is released, the address is discarded and never used again.

Using connection identifier: the connection identifier is given to each connection. Connection identifier is a sequence number incremented for each connection established.

The three protocol scenarios for establishing a connection using three ways handshake is explained with three cases:

Case 1: Normal operation

Case 2: Old duplicate CONNECTION_REQUEST

Case 3: Duplicate CONNECTION_REQUEST and duplicate ACK

Case 1: Normal setup as shown in fig (a)

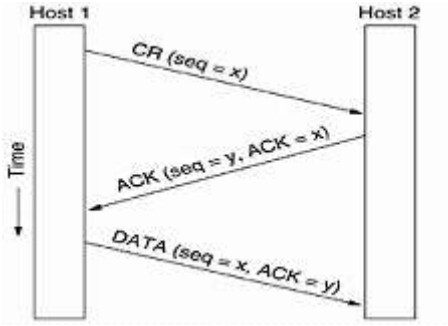


Fig: (a) Normal operation.

Host1 choose a sequence number k and sends a CONNECTION_REQUEST TPDU to host2. Host2 receives CONNECTION_REQUEST TPDU and replies with ACK (acknowledgement) TPDU acknowledgement x and assigns its own initial sequence number y.

Finally, host1 acknowledges host2's choice of an initial sequence number in the first data TPDU. The DATA TPDUs has sequence number x, indicating the connection identifier for that connection.

Case 2: Delayed duplicate CONNECTION_REQUEST TPDUs

First, TPDU is a delayed duplicate CONNECTION_REQUEST from an old connection as shown in the fig (b). This delayed CR TPDU arrives at host 2 without the knowledge of host1.

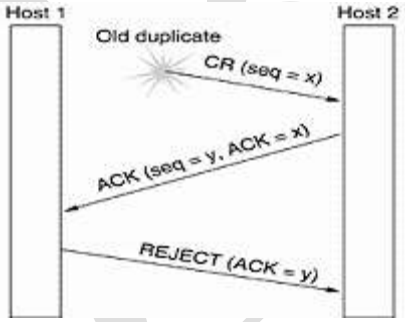


Fig :(b) Old duplicate CONNECTION REQUEST appearing out of nowhere

Host2 replies to this delayed TPDU by sending ACK TPDU to host1. Host1 gets ACK TPDU without sending CR TPDU. This is because host1 does not have the knowledge of CR TPDU have been sent because it is delayed one. So, host1 rejects host 2's attempt to establish a connection, host2 realizes that is was a delayed duplicate and abandons the connection. In this way delayed duplicate does not any damage.

Case 3: Duplicate CONNECTION_REQUEST and duplicate ACK

This situation arises, when both CONNECTION_REQUEST and ACK TPDUs are delayed. This case is shown in the fig c)

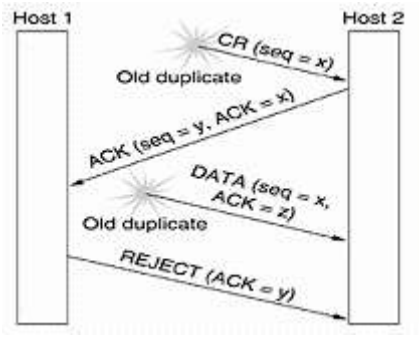


Fig: (c) Duplicate CONNECTION REQUEST and duplicate ACK

Host2 gets a delayed CONNECTION_REQUEST and replies to it. The CONNECTION_REQUEST is acknowledged by host2 by assigning its own sequence number y.

At this point, second delayed duplicate from old connection with acknowledge sequence number z arrives at host2. But, the sequence number y is not acknowledged from host1, because host1 is not aware of the CONNECTION_REQUEST sent to host2. This indicates that both CR and old duplicate
DATA with ACK z are duplicate TPDUs. So, host1 send REJECT TPDUs for reject connection to host2.

3. Connection Release:

- Connection release is easier than establishing the connection. The connections are released in two ways: **asymmetric release and symmetric release.**
- In **asymmetric release**, either side can release connection or there may be chances of losing the data.
- In **symmetric release,** the connection is treated as two separate unidirectional connections and requires either side to be released separately. If user on one side release connection, but still it wait for other side to release connection. Here there is no chance of loosing the data.

Four protocol scenarios for releasing a connection are discussed with the following cases:

- Normal connection release
- Final ACK lost
- Response lost
- Both response lost and subsequent DISCONNECTION_REQUEST lost

Case (i) Normal Connection release:

One of the users sends a DISCONNECTION_REQUEST TPDU to initiate the connection release as shown in the fig 6.10(a)

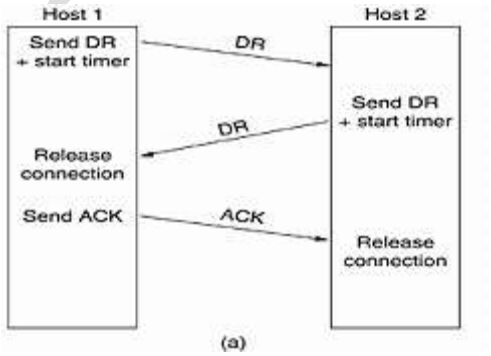


Fig:(a) Normal case of three-way handshake.

When DR arrives at host2, it sends back a DR TPDU indicating its willingness to release. Timers are started when DR TPDU is sent, to keep track of the time. When DR TPDU arrives at host1, the original sender sends back an ACK TPDU and releases the connection. Finally, ACK TPDU arrives at the host2 and also releases the connection.

Case (ii) Final ACK TPDU is lost:

When final ACK TPDU is lost, the timer will save the situation. Host2 will wait for time out. When the timer expires, the connection is released anyway. The case (ii) shown in the fig(b)

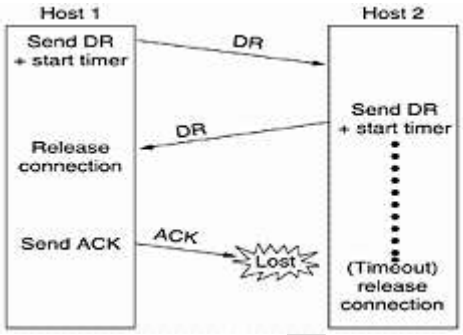


Fig:(b) Final ACK lost.

Case (iii) Response lost:

This is the case, when second DR TPDU is lost. This is shown in the fig (c)

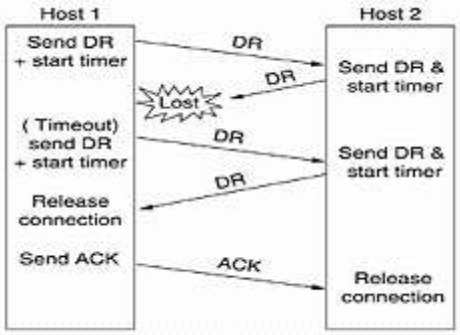


Fig:(c) Response lost.

The host1 indicating the disconnection will not receive the excepted response. This is due to second DR from host2 is lost. At host1, time out occurs and will start all over again. i.e., once again DR is sent. Host2 upon arrival of DR replies back. Host1 receives second DR and releases connections and send ACK to host2. Host2 upon receiving the ACK, host2 releases connection.

Case (iv) Both response and subsequent DR are lost:

In this case, assume all the repeated attempts to retransmit the DR also fails due to lost TPDUs as shown in the fig (d).

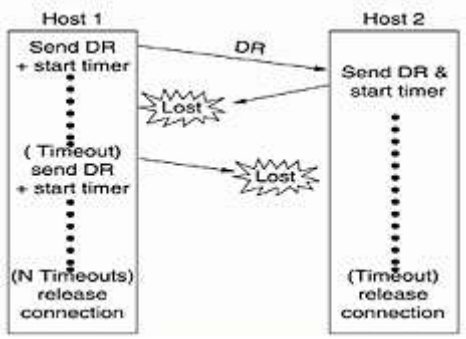


Fig:(d) Response lost and subsequent DRs lost

- After N retries, the sender just gives up and releases the connection. The receiver times out and also exits.
- The sender side will give up and release the connection, while other side does not know about the attempts to disconnect. This situation results in a half open connection.
- Half open connection can be avoided by not allowing the sender to give up after N retries. But if other side is allowed to time out, the sender will not release connection for ever.
- Another way is to have ruled if no TPDUs have arrived for a certain number of seconds, then connection is automatically disconnection.
- If one side ever disconnects, the other side will detect lack of activity and also disconnect.

4. Flow control and Buffering:

- Flow control problem on the transport layer is same as in the data link layer and other issues are different.
- In both the layer sliding window scheme is used to keep a fast transmitter from over running a slow receiver.
- Flow control scheme used at data link layer and transport layer are different. In transport layer receiver may maintain a single pool shared by all connections.
- When TPDUs comes in, new buffer is acquired for that connection. If buffer is available, the TPDU is accepted, otherwise, it is discarded.
- Even if TPDU is discarded, no harm because sender is prepared to retransmit lost TPDUs by the subnet. The problem is resources are wasted.
- **The buffering at receiver** side has some problems. It is very difficult to allocate buffer size at the receiver. If the all TPDUs are in same sizes, then it is easy to organize the buffer.
- Here buffer can be a pool of identically size buffers, with one TPDU per buffer.
- **The problem with fixed size buffers are:** if there is wide variation in TPDU from few characters to thousands of characters, then fixed size buffers fails. For few characters TPDUs space is wasted and for long TPDU, it overflow as shown in the fig (a)

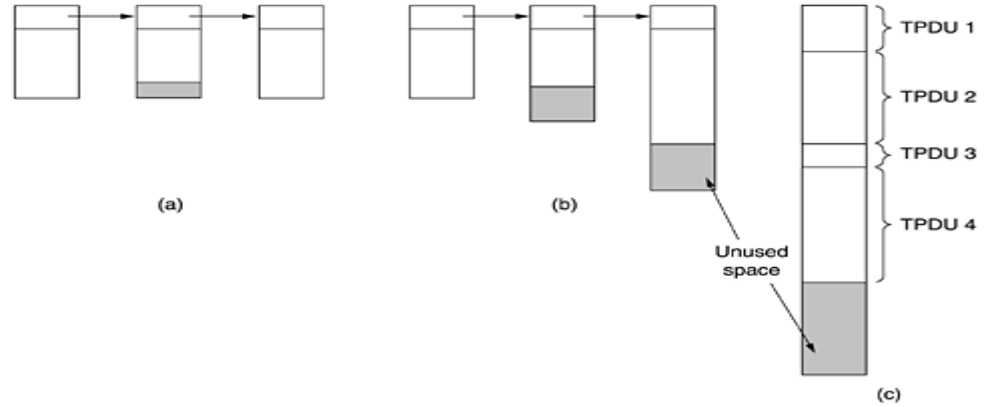


Fig: (a) Chained fixed-size buffers. (b) Chained variable-sized buffers. (c) One large circular buffer per connection.

- If the buffer size is chosen equal to the largest possible TPDU, space will be wasted when a short TPDU arrives.
- If the buffer size is less than the maximum TPDU size, multiple buffers will be needed for long TPDUs, with incoming the complexity. In this approach, variable sized buffers are used as shown in the fig(b).
- Advantage of using variable sized buffers is better memory utilization and disadvantage is more complicated buffer management.
- Third approach uses a single large circular buffer per connection as shown in fig(c). This approach makes good use of memory, provided that all connections are heavily loaded. Utilization of memory is very poor, if the connections are slightly loaded.

5. Multiplexing:

Multiplexing conversation linked to one or distributed to many connections can be called ad multiplexing with respect to transport layers. Multiple users may be using different port to get their required services. The multiplexing can be classified into:

- Upward Multiplexing
- Downward Multiplexing

1) Upward Multiplexing:

In upward multiplexing, the multiple connections are multiplexed on to a single connection as shown in fig(a)

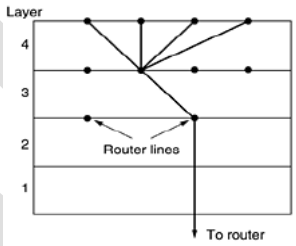


Fig: **(a) Upward multiplexing.**

- For example, all transport connections on the host must use only one network address available.
- Four distinct transport connections all use the same network connection (IP address) to the remote host.
- If more number of users is multiplexed, then performance is degraded. If there are less users multiplexed, the service will be expensive.

(ii) Downward Multiplexing:

In downward multiplexing, a single connection is split and distributed among multiple connections as shown in the fig(b)

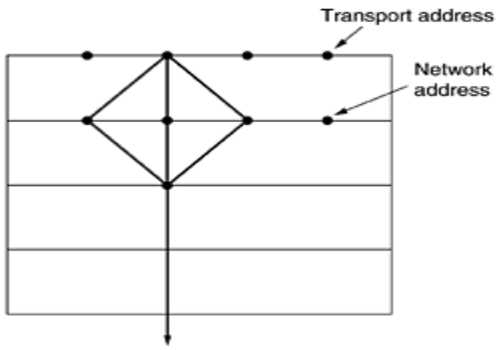


Fig: (b) Downward

multiplexing.

- For example, if subnet uses virtual circuit internally and imposes maximum data rate on each one.
- If user needs a more bandwidth than one virtual circuit can provide, open multiple network connections and distribute traffic among them on round robin basis.

6) Crash Recovery:

- When hosts and routers are subject to crashes, recoveries from these crashes are difficult. It may be desirable for clients to be able to continue working when servers crash and then quickly reboot.
- The difficult task in crash recovery is to recover the previous status of server. One way is to broadcast. TPDU to all the other hosts, announcing that it had just crashed and requesting its client inform it of the status of all open connections.
- Clients can be in any one of the state:

S1 -> one TPDU outstanding and

S0 -> no TPDU outstanding

- Based on this state information, client must decide whether to retransmit the most recent TPDU. The client should retransmit, if and only if it has an unacknowledged TPDU outstanding S1, when it learns about the crash.
- There are some difficulties in this approach. If crash occurs after the acknowledgement has been sent but before the write has been done at server side.
- Client and server are programs in different ways, but there are some situations where the protocol fails to recover properly.

Server can be programmed in two ways:

1) Acknowledge first and

2) Write first

Client can be programmed in four ways:

- always retransmit the last TPDU
- never retransmit the last TPDU
- retransmit only in state S0
- Retransmit only in state S1

CONGESTION CONTROL

- TCP congestion control and Internet traffic management issues in general is an active area of research and experimentation.
- This final section is a very brief summary of the standard congestion control algorithms widely used in TCP implementations today.

1 Slow Start

- Slow Start, a requirement for TCP software implementations is a mechanism used by the sender to control the transmission rate, otherwise known as sender-based flow control.
- This is accomplished through the return rate of acknowledgements from the receiver.
- In other words, the rate of acknowledgements returned by the receiver determine the rate at which the sender can transmit data.
- When a TCP connection first begins, the Slow Start algorithm initializes a congestion window to one segment, which is the maximum segment size (MSS) initialized by the receiver during the connection establishment phase.

- When acknowledgements are returned by the receiver, the congestion window increases by one segment for each acknowledgement returned.
- Thus, the sender can transmit the minimum of the congestion window and the advertised window of the receiver, which is simply called the transmission window.

2 Congestion Avoidance

- During the initial data transfer phase of a TCP connection the Slow Start algorithm is used.
- However, there may be a point during Slow Start that the network is forced to drop one or more packets due to overload or congestion.
- If this happens, Congestion Avoidance is used to slow the transmission rate.
- However, Slow Start is used in conjunction with Congestion Avoidance as the means to get the data transfer going again so it doesn't slow down and stay slow.
- In the Congestion Avoidance algorithm a retransmission timer expiring or the reception of duplicate ACKs can implicitly signal the sender that a network congestion situation is occurring.
- The sender immediately sets its transmission window to one half of the current window size (the minimum of the congestion window and the receiver's advertised window size), but to at least two segments.
- If congestion was indicated by a timeout, the congestion window is reset to one segment, which automatically puts the sender into Slow Start mode.
- If congestion was indicated by duplicate ACKs, the Fast Retransmit and Fast Recovery algorithms are invoked.

3 Fast Retransmit

- When a duplicate ACK is received, the sender does not know if it is because a TCP segment was lost or simply that a segment was delayed and received out of order at the receiver.
- If the receiver can re-order segments, it should not be long before the receiver sends the latest expected acknowledgement.
- Typically no more than one or two duplicate ACKs should be received when simple out of order conditions exist.
- If however more than two duplicate ACKs are received by the sender, it is a strong indication that at least one segment has been lost.
- The TCP sender will assume enough time has lapsed for all segments to be properly re-ordered by the fact that the receiver had enough time to send three duplicate ACKs.

4 Fast Recovery

Since the Fast Retransmit algorithm is used when duplicate ACKs are being received, the TCP sender has implicit knowledge that there is data still flowing to the receiver.

INTERNET TRANSPORT PROTOCOL-TCP

TCP is often described as a byte stream, connection-oriented, reliable delivery transport layer protocol. In turn, we will discuss the meaning for each of these descriptive terms.

1. Byte Stream Delivery

- TCP interfaces between the application layer above and the network layer below.
- When an application sends data to TCP, it does so in 8-bit byte streams.
- It is then up to the sending TCP to segment or delineate the byte stream in order to transmit data in manageable pieces to the receiver.

2. Connection-Oriented

- Before two communicating TCPs can exchange data, they must first agree upon the willingness to communicate.
- Analogous to a telephone call, a connection must first be made before two parties exchange information.

3. Reliability

A number of mechanisms help provide the reliability TCP guarantees. Each of these is described briefly below.

- ***Checksums***. All TCP segments carry a checksum, which is used by the receiver to detect errors with either the TCP header or data.
- ***Duplicate data detection***. It is possible for packets to be duplicated in packet switched network; therefore TCP keeps track of bytes received in order to discard duplicate copies of data that has already been received.[2]
- ***Retransmissions***. In order to guarantee delivery of data, TCP must implement retransmission schemes for data that may be lost or damaged. The use of positive acknowledgements by the receiver to the sender confirms successful reception of data. The lack of positive acknowledgements, coupled with a timeout period (see timers below) calls for a retransmission.
- ***Sequencing*.** In packet switched networks, it is possible for packets to be delivered out of order. It is TCP's job to properly sequence segments it receives so it can deliver the byte stream data to an application in order.
- ***Timers*.** TCP maintains various static and dynamic timers on data sent. The sending TCP waits for the receiver to reply with an acknowledgement within a bounded length of time. If the timer expires before receiving an acknowledgement, the sender can retransmit the segment.

4.5.TCP Header Format

Remember that the combination of TCP header and TCP in one packet is called a TCP segment. Figure 1 depicts the format of all valid TCP segments. The size of the header without options is 20 bytes. We will briefly define each field of the TCP header below.

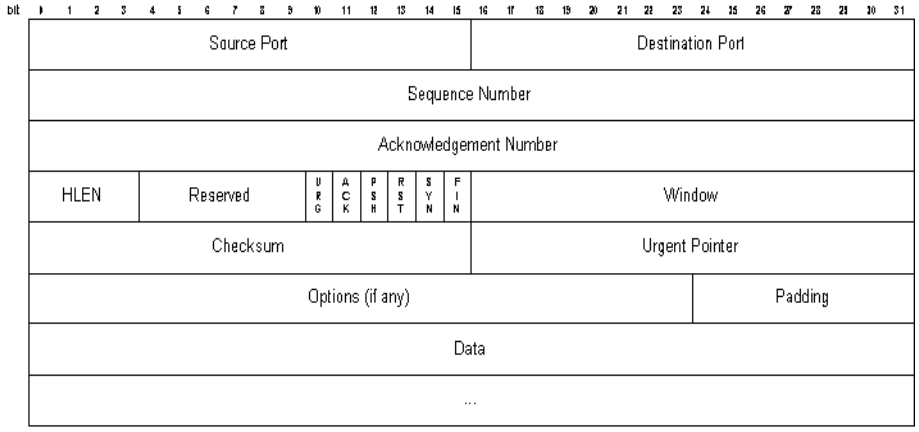


Figure 1 - TCP Header Format

1 Source Port

- A 16-bit number identifying the application the TCP segment originated from within the sending host.
- The port numbers are divided into three ranges, well-known ports (0 through 1023), registered ports (1024 through 49151) and private ports (49152 through 65535).
- Port assignments are used by TCP as an interface to the application layer. For example, the TELNET server is always assigned to the well-known port 23 by default on TCP hosts.
- A complete pair of IP addresses (source and destination) plus a complete pair of TCP ports (source and destination) define a single TCP connection that is globally unique

2 Destination Port

- A 16-bit number identifying the application the TCP segment is destined for on a receiving host. Destination ports use the same port number assignments as those set aside for source ports.

3 Sequence Number

A 32-bit number identifying the current position of the first data byte in the segment within the entire byte stream for the TCP connection. After reaching 2^{32} -1, this number will wrap around to 0.

4 Acknowledgement Number

- A 32-bit number identifying the next data byte the sender expects from the receiver. Therefore, the number will be one greater than the most recently received data byte. This field is only used when the ACK control bit is turned on.

5 Header Length

- A 4-bit field that specifies the total TCP header length in 32-bit words (or in multiples of 4 bytes if you prefer).
- Without options, a TCP header is always 20 bytes in length. The largest a TCP header may be is 60 bytes.
- This field is required because the size of the options field(s) cannot be determined in advance. Note that this field is called "data offset" in the official TCP standard, but header length is more commonly used.

6 Reserved

- A 6-bit field currently unused and reserved for future use.

7 Control Bits

- ***Urgent Pointer (URG).*** If this bit field is set, the receiving TCP should interpret the urgent pointer field (see below).
- ***Acknowledgement (ACK).*** If this bit field is set, the acknowledgement field described earlier is valid.
- ***Push Function (PSH).*** If this bit field is set, the receiver should deliver this segment to the receiving application as soon as possible. An example of its use may be to send a Control-BREAK request to an application, which can jump ahead of queued data.
- ***Reset the Connection (RST).*** If this bit is present, it signals the receiver that the sender is aborting the connection and all queued data and allocated buffers for the connection can be freely relinquished.

- ***Synchronize (SYN).*** When present, this bit field signifies that sender is attempting to "synchronize" sequence numbers. This bit is used during the initial stages of connection establishment between a sender and receiver.
- ***No More Data from Sender (FIN).*** If set, this bit field tells the receiver that the sender has reached the end of its byte stream for the current TCP connection.

8 Window

- A 16-bit integer used by TCP for flow control in the form of a data transmission window size. This number tells the sender how much data the receiver is willing to accept.
- The maximum value for this field would limit the window size to 65,535 bytes, however a "window scale" option can be used to make use of even larger windows.

9 Checksum

- A TCP sender computes a value based on the contents of the TCP header and data fields.
- This 16-bit value will be compared with the value the receiver generates using the same computation.
- If the values match, the receiver can be very confident that the segment arrived intact.

10 Urgent Pointer

- In certain circumstances, it may be necessary for a TCP sender to notify the receiver of urgent data that should be processed by the receiving application as soon as possible.
- This 16-bit field tells the receiver when the last byte of urgent data in the segment ends.

11 Options

- In order to provide additional functionality, several optional parameters may be used between a TCP sender and receiver.
- Depending on the option(s) used, the length of this field will vary in size, but it cannot be larger than 40 bytes due to the size of the header length field (4 bits).
- The most common option is the maximum segment size (MSS) option.
- A TCP receiver tells the TCP sender the maximum segment size it is willing to accept through the use of this option.
- Other options are often used for various flow control and congestion control techniques.

12 Padding

- Because options may vary in size, it may be necessary to "pad" the TCP header with zeroes so that the segment ends on a 32-bit word boundary as defined by the standard.

13 Data

- Although not used in some circumstances (e.g. acknowledgement segments with no data in the reverse direction), this variable length field carries the application data from TCP sender to receiver.
- This field coupled with the TCP header fields constitutes a TCP segment.

**** Difference between TCP and UDP are transport level Internet protocols.**

TCP	UDP
Connection Oriented	Connectionless
Complete reliability corrects lost, corrupted and out-of-order packets	best effort delivery
Full Duplex communication	Full Duplex communication
Point to Point communication	Point to Point communication or broadcast
Stream Interface	Packet Interface
Reliable connection startup	no connection

UNIT – V

APPLICATION LAYERS

Application layer is the top most layer in OSI and TCP/IP layered model. This layer exists in both layered Models because of its significance, of interacting with user and user applications. This layer is for applications which are involved in communication system.

A user may or may not directly interacts with the applications. Application layer is where the actual communication is initiated and reflects. Because this layer is on the top of the layer stack, it does not serve any other layers. Application layer takes the help of Transport and all layers below it to communicate or transfer its data to the remote host.

When an application layer protocol wants to communicate with its peer application layer protocol on remote host, it hands over the data or information to the Transport layer. The transport layer does the rest with the help of all the layers below it.

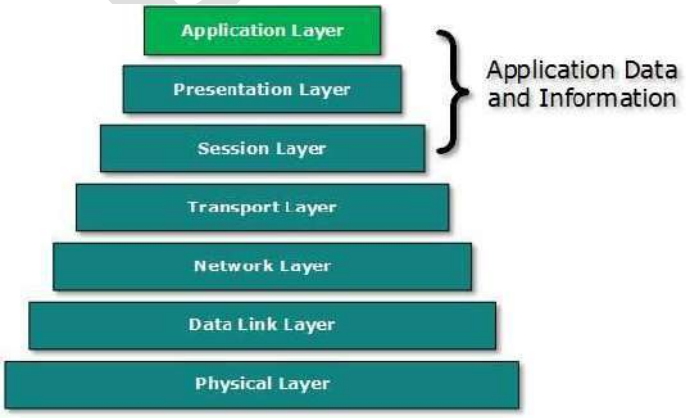


Fig. Application Layer

There's an ambiguity in understanding Application Layer and its protocol. Not every user application can be put into Application Layer. Except those applications which interact with the communication system. For example, designing software or text-editor cannot be considered as application layer programs.

DOMAIN NAME SYSTEM

On the internet, each host is identified by address. These addresses are hard and difficult for people to remember. People started preferring names instead of addresses. We need a system that can map an ASCII name to an address.

When internet was small, this mapping was accomplished by a simple file hosts.txt. The host file had two columns comprising name and IP address.

1.The DNS name space:

In the internet domains are divided into 200 top levels, where each domain covers many hosts. Each domain is further partitioned into subdomains and these subdomains into further subdomain and so on. A namespace that maps each address to a unique name.

The top-levels domains are classified into two categories: (1) Generic domain and (2) countries domain.

The generic domains are:

.com (commercial)

.edu (educational institutions)

.gov (government)

.int (some international organizations)

.mil (US military forces)

.net (network providers) and

.org (non profit organizations)

The country domains include one entry for every country, for example India's domain is .in, Australia has .au, etc. all these domain can be represented by a tree, as shown below:

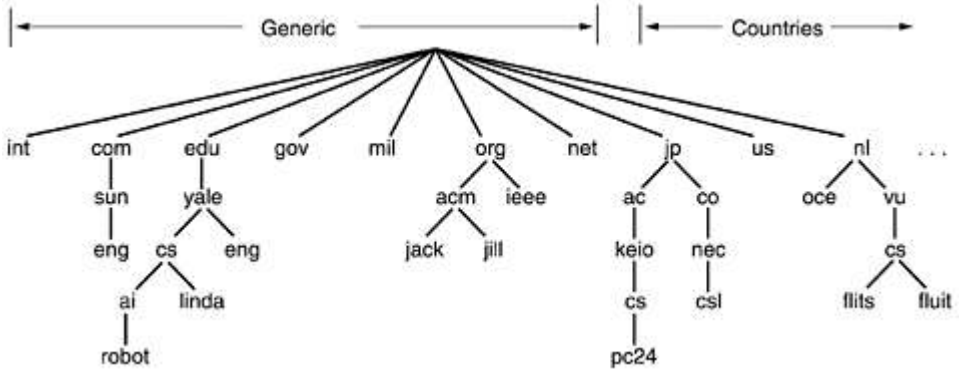


Fig: A portion of the Internet domain name space.

2.Resource Records:

Each domain name is associated with a record called the resource record. The server database consists of resource records. These records are returned by the server to the client. Server is a DNS server which returns resource records associated with that name. the primary function of DNS is to map domain names onto resource records.

Format of resource record:

Resource record consists of five tuple and all fields are encoded in binary form for efficiency. Resource records are represented as ASCII, text, one line per resource record. The five tuple are domain name, time to live, class, type and value.

1) Domain Name:

This variable length field tells the domain to which this record applies. This field is used as primary search key to satisfy queries.

2) Time – to –live:

This field is 32-bit that defines the number of seconds the answer is valid. If the information is highly stable is assigned with a large value and highly volatile information is assigned with a small value. The receiver can cache the answer for this period of time. If this filed is zero, then the resource record is used only for single transaction and it is not stored for future use.

3) Domain class:

This field identifies domain class of every resource record. For example, internet information, it is always IN and for non-internet information other codes can be used.

4) Domain Type:

This field tells what type of resource record it is. There are various types of resource records are:

Domain type	**Meaning**	**Value**
SoA	Start of Authority	Parameter for this zone
A	IP address of a host	32-bit Integer
MX	Mail Exchange	Priority, domain willing to accept email
NS	Name server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for IP address
HINFO	Host Description	CPU and OS in ASCII
SRV	Service Available	Defines services available in zone eg. Idap, http, etc.
SIG	Signature	Signature contains data authenticated in a source DNS
TXT	Text information	Text information associated name
WKS	Well known services	Well known services depreciated in favour of SRV

SoA (Start of Authority):

Record starts with SoA which provides the name of primary source information. This information may be name server's zone or email address of administrator, a unique serial number, various flags and timeouts.

A (Address):

This record is most important record type holds a 32-bit IP address for some host. Each host on the internet is identified or addressed by atleast one IP address. This IP address is used by other machine for communication. Even if network connections are more than one for some hosts, but they will have only one type of A resource per IP address.

MX (Mail Exchange):

The MX record provides the name of the host prepared to accept e-mail for the specified domain. MX record is used because, every machine is not prepared to accept e-mail. It redirects mail to a mail server.

NS (Name Server) record:

The NS records are used to specify the name servers. Every DNS database normally has an NS record for each of the top-level domains.

CNAME (canonical Name) record:

CNAME records will have domain name as value. CNAME records allow aliases to be created. Sometime address will not be correct. For example, a person familiar with Internet naming wants to send a message to his friend whose name is X in the computer science department at iisc. He might guess that x@cs.iisc.edu will work. But the actual address is x@cse.iisc.edu. Making CNAME entry, one can do the job in the following way:

Cs.iisc.edu 864001N CNAME cse.iisc.edu

PTR record:

PTR is a regular DNS data type whose interpretation depends on the context in which it is found. PTR is used to associate a name with an IP address. For a given IP address it returns the name of the corresponding machine. This mechanism is known as reverse lookups.

HINFO record:

This record gives the type of machine and operating system a domain corresponds to. It gives the host description with type of CPU and OS.

TXT record:

This record contains uninterpreted ASCII text and allows domains to identify themselves in arbitrary ways.

5) Domain value:

This field can be a number, a domain name or an ASCII string. The semantics depend on the record type.

3.Name Servers:

The DNS name was divided into non over lapping zones. Each zone contains some part of the true and also contains name servers holding the information about that zone. Zone will have one primary name server and one or more secondary name servers. Primary name servers get their information from a file on its disk and secondary name servers get their information from the primary name servers.

The domain is remote and no information about the requested domain is available locally, then name server sends a query message to the top level name server for the domain requested.

Electronic Mail

E-mail or electronic mail is one of the most popular network services. The email system simply consists of file transfer protocols with the convention that the first line of each message, contained in the recipient's address.

There were some limitations and problems of using file transfer protocol. They are:

- It was not possible or difficult to send message group of people.
- No internal structure of messages, which makes computer processing difficult.
- There was no way to intimate the arrival of new email messages to the senders.
- There was no facility of re-directing messages to secretaries, when some one was away on business.
- Poor user interface.
- Not possible to create and send messages containing a combination of text, images, voices and facsimile.

1.Architecture and Services:

The email system consists of two subsystems: 1) user agents (UA) and 2) message transfer Agents (MTA).

User agents will allow people to read and send mail, whereas message transfer agents more the messages from the source to the destination MTAs are typically system daemons. Daemons are the process which runs in the background and their job is to move email through the system. User agents are program at the client side that provide a command based, menu based or graphical based method for interacting with the email systems.

Email systems support five basic functions. These basic functions are:

1) Compositions:

The process of creating or writing a messages and answers. The email system itself will support to compose a mail. After writing a mail address and other header field can be attached to each message.

2) Transfer:

This refers to transferring a mail from sender to the recipient. We need to establish a connection to the destination or intermediate machine. After transferring the messages the connection can be released. The email system will automatically connects/disconnects without the intervention of the user.

3) Reporting:

This process will inform the sender about the email sent. This information can be whether mail was delivered or rejected or lost. Reporting helps in providing confirmation about the email sent.

4) Displaying:

This support is provided to show or display the email received. People can read their emails. Email cannot be viewed directly. Conversion is required or special viewer tools are needed to get the messages.

5) Disposition:

After reading the mail what the recipient want to do. The mail may be read and deleted or not read or read and saved so on. The emails are saved, whenever it is need it can be reread or retrieved or forwarded.

Addition to the basic services, some email systems advanced features. They are:

1) Mail Boxes:

These are created to store incoming email explicit commands are needed to create and destroy mailboxes, check the contents of mailboxes, insert and delete messages from mail boxes and so on.

2) Mailing list:

The mailing list is a list of email addresses. When a email is sent to this mailing list, the same copies are delivered to everyone on the list.

3) Advanced features:

The advanced features like carbon copies (CC), blind carbon copies (Bcc), higher priority email, encrypted email, automated reply email and so on are developed.

2.The User Agents:

User Agents (UA) is a part of e-mail systems used at client side. A user agent is a program that accepts a variety of commands. These commands are used to compose, receive, send, delete and move mails to a folder, etc.

Send e-mail:

Email can be sent through User Agent (UA) by creating mail that looks very similar to postal or snail mail. It has an envelope and a message. A user must provide destination address, message and other parameters. The message can be prepared by text editor or work processing like program which is built into the user agent.

The envelope contains the sender address, receiver address and other related information. The message contains the header and the body. The header of the message contains the sender, the receiver and subject of the message. The body contains the actual information to be read by the receipt.

The destination address of the receipt must be in the form of username@dns-address.

Receive e-mail:

User agent checks the mail boxes periodically for incoming email. If a user has a mail in mailbox then the UA informs the user first by giving a notice or number of messages in the mailbox. If the user is ready to read the mail, a list is displayed in which each line contains a summary of the information about a particular message in the mailbox as shown below:

Sl.no	Flags	Sender address	Subject	Size
1	K	Raj	Hello	413K
2		Ravi	Conference	20k
3	KA	roopa@yahoo.com	Re:CSE Dept	612K
4	KF	Raghu	Request	212K

Table: Screenshot of the contents of a mail box

The first field is the message number. Second field contain flags K, A and F. flag K indicates that message is not new and was read already. Flag KA indicates that message is already read and answered. Flag KF indicates that message was read and forwarded to someone. The third field tells who has sent the message. The field may contain only first name or email address or full names. The next field, subject gives the brief summary of what the message is about. Finally, the last field tells the size of the message is bytes.

3.Message Formats:

The format of the email messages which is described in RFC 822. The message consist of: 1) primitive envelope, 2) header fields 3) blank line and 4) message body.

The header fields related to the message transport have the following fields as shown in below:

Header	**Meaning**
To	Filed gives email addresses of the primary recipient(s)
Cc	Gives the addresses of any secondary recipient(s)
Bcc	Email addresses for blind carbon copies
From	Who wrote or created the message
Sender	Email address of the actual sender
Receiver	Line added by each transfer agent along the route
Return-path	Can be used to identify a path black to the sender

Table: RFC 822 Header fields

The RFC 822 headers are described below:

1) To field:

This field gives the email address of the primary recipient (to whom message has to be sent).

2) CC field:

This field gives the email addresses of the any secondary recipients. Cc stand for carbon copy. There is no specific distinction between the primary and secondary recipients.

3) Bcc field:

This field is referred as blind carbon copy, it is similar to cc field, except this line is deleted from all the copies sent to the primary and secondary recipients. So that primary and secondary recipients cannot know the copies sent from Bcc field.

4) From field:

This field tells who wrote the mail or from whom message has been received.

5) Sender field:

This field tells who has sent the mail. For example, boss may write a message, but his assistant may be one who actually sends it. In this case boss would be listed in from field and his assistant in the sender field.

6) Received field:

This field is added by each message transfer agent along the way. The line contains the agent's identify, the date and time the message was received.

7) Return-path:

This field is added by the final message transfer agent and was used to tell how to get back to the sender.

In addition, RFC 822 messages may also contain a variety of header fields. The important fields are listed on the table below:

Header	**Meaning**
Date	Date and time the message was sent
Reply to	Email address to which replies should be sent
Message-id	Unique number for referring this message later
In-reply to	Message-id of the message to which this is a reply
References	Other relevant message-ids
Keywords	User chosen keywords
Subject	Short summary of the message for the one-line display