T.E. : Computer Networks

Notes

75

CONTENTS

Vidyalankar

T.E.[INFT/CMPN] - Computer Networks

Syllabus

Time : 3 Hrs. **Theory : 100 Marks**
Termwork : 25 Marks

1. **Introduction :**
   Network Applications. Network Hardware. Network Software. Reference Models.

2. **The Physical layer :**
   Guided Transmission Media, Wireless Transmission. Communication Satellite. The Public Switched Telephone Network. The Mobile Telephone System. Cable Television.

3. **The Data Link Layer :**
   Data link layer design issues. Elementary data link protocols. Sliding window protocols example of Data Link Protocols: HDLC: High–Level Data Link Control. the Data Link Layer in the Internet.

4. **The Medium Access Sub–layer :**
   The channel allocation problem. Multiple access protocols. Ethernet. Wireless LANS. Broadband wireless. Blue tooth. Data link layer switching.

5. **The Network Layer :**
   Network Layer Design Issues. Routing Algorithms. Congestion Control Algorithm. Quality of Service. Internetworking. The Network Layer in the Internet: The IP Protocol, IP Addresses. Internet Control Protocols, The Interior Gateway Routing Protocol; OSPF. The Exterior Gateway Routing Protocol: BGP, Internet Multicasting, Mobile IP, Ipv6.

6. **The Transport Layer :**
   The Transport Service. Elements Of Transport Protocols. A Simple Transport Protocol. The Internet Transport Protocols: UDP;
   TCP: Introduction to TCP, The TCP Service Model, The TCP Protocol the TCP Segment Header, TCP Connection Establishment, TCP Connection Release, Modeling TCP Connection Management, TCP Transmission Policy, TCP Congestion Control, TCP timer Management, Wireless TCP and UDP, Transactional TCP.
   Performance Issues: Measuring Network Performance, System Design for better PERFORMANCE, FAST TPDU Processing, Protocols for Gigabit Networks.

7. **The Application Layer :**
   DNS : The Domain name system; Electronic Mail; SNMP.

8. **ATM Network :**
   ATM Layer : ATM Application Layer. ATM Signaling. PNNI Routing.

9. **Case study with Window 2000/ Linux**

□□□□□□

Vidyalankar

Ch.1 : Introduction

Network : A network is a set of devices (often referred to as nodes) connected by media links. The links connecting the devices are called communication channels.

Difference between Computer Network and a Distributed System :

- In a distributed system, the existence of multiple autonomous computers is transparent to the user.
- The user of a distributed system is not aware that there are multiple processors; it looks like a virtual uniprocessor.
- With a network, users must explicitly log on to one machine, explicitly submit jobs remotely, explicitly move files around and generally handle all the network management personally.

  With a distributed system, nothing has to be done explicitly; it is automatically done by the system without the user's knowledge.
- A distributed system is a software built on top of a network.

  Thus the distinction between a network and distributed system lies with the software (especially the operating system) rather than with the hardware.

Network Goals :

1. Resource sharing
2. High Reliability
3. Saving money
4. Powerful communication medium

Transmission technology :

1. Broadcast networks :

Broadcast networks have a single communication channel that is shared by all the machines on the network. Packets sent by any machine are received by all the others. An address field within the packet specifies for whom it is intended. Upon receiving the packet, the machine checks the address field. If the packet is intended for some other machine, it is just ignored.

Point–to–Point Networks :

Point–to–Point networks consists of many connections between individual pairs of machines. To go from the source to destination, a packet on this type of network may have to first visit one or more intermediate machines.

As a general rule, (although there are exceptions), smaller geographically localized networks tend to use broadcasting, whereas larger networks usually are point–to–point.

Network Topologies :

1. Local Area Network (LAN) :

LAN's are privately–owned networks within a single building or campus of upto few kilometers in size.

They are widely used to connect personal computers and workstations in company offices and factories to share resources and exchange information.
Traditional LAN's run at speeds of 10 to 100 Mbps.

2. Metropolitan Area Networks (MAN) :

MAN is basically a bigger version of LAN and normally uses similar technology. It might cover a group of nearly corporate offices or a city and might be either private or public.

A MAN can support both data and voice, and might even be related to local cable television network.

3. Wide Area Network (WAN) :

A WAN spans a large geographical area, often a country or continent. It contains a collection of machines intended for running user programs.

In most wide area networks, the subnet consists of two distinct components : transmission lines and switching elements.

Transmission lines move bits between machines.

The switching elements are specialized computers used to connect two or more transmission lines. When data arrive on an incoming line, the switching element must choose an outgoing line to forward them on.

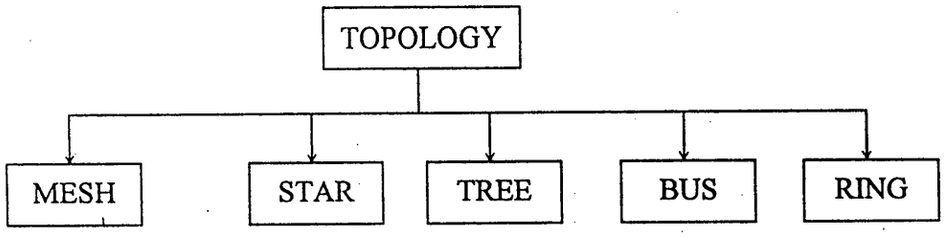
Line Configuration :

Line configuration refers to the way two or more communication devices attach to link. There are two possible line configurations –

1. **Point–to–point**
   A point–to–point line configuration provides a dedicated link between two devices.
2. **Multipoint :**
   A multipoint (also called multidrop) line configuration is one in which more than two specific devices share a single link.

Topology :

The term topology refers to the way a network is laid out, either physically or logically.

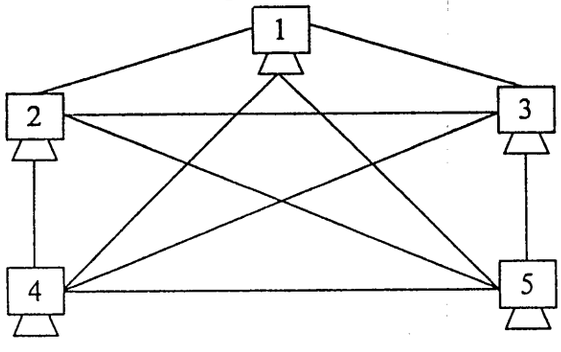


Five basic technologies are :

I. MESH :

Every device has dedicated point–to–point link to every other device.

(n(n – 1))/2 physical channels are required to link n devices.



5 devices

$\frac{5(5-1)}{2} = 10$ links

Advantages :

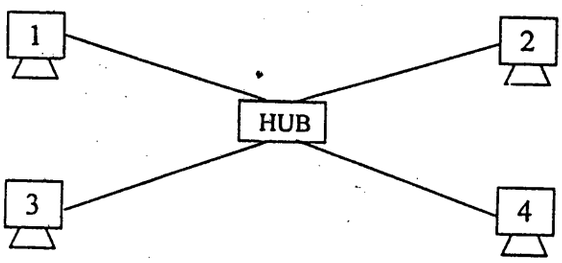
1. **No Traffic :**
   The use of dedicated links guarantees that each connection can carry its data load, thus eliminate traffic problems.
2. **Robust :**
   If one link becomes unusable, it does not affect the entire problem.
3. **Privacy or Security :**
   Every message travels along a dedicated link, hence only the intended recipient sees it.
4. **Fault identification and fault isolation is easy.**

Disadvantages :

1. Installation and reconfiguration is difficult.
2. The sheer bulk of wiring can be greater than the available space can accommodate.
3. The hardware required to connect each link (I/O port and cable) are expensive.

II. STAR :

Each device has a dedicated point–to–point link only to a central controller, usually called a hub.



Advantages :

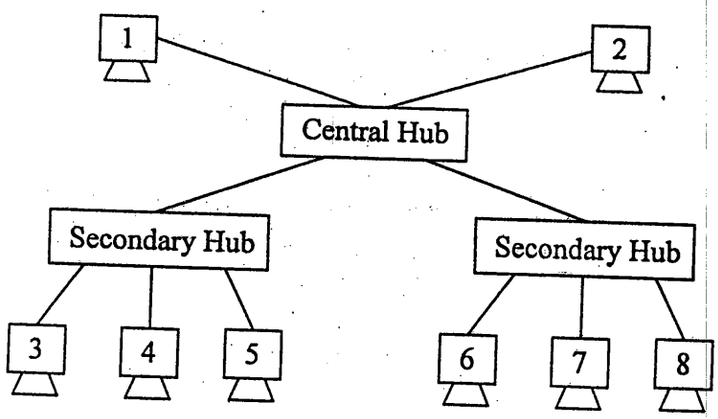
1. Less expensive than mesh topology.
2. Easy to install and configure
3. Less cabling required as compared to mesh
4. Robust:
   One link is damaged then the complete system is not affected. This also leads to easy fault identification and isolation.

Disadvantages :

1. More cabling compared to bus or ring topology.
2. Central controller is required.

III. TREE : (Variation of STAR)

In TREE majority devices are connected to a secondary hub that in turn is connected to the central hub.



Advantages :

1. Less expensive than mesh topology.
2. Easy to install and configure
3. Less cabling required as compared to mesh
4. Robust
5. More devices can be attached to a single hub.
6. Allows network to isolate and prioritize communication from different computers.

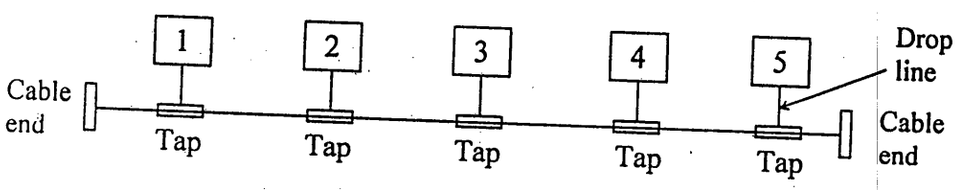
Disadvantages :

1. More cabling compared to bus or ring topology.
2. Central controller is required.

IV. BUS :

It uses multipoint configuration.

One long cable acts as a backbone to link all devices in the network.



Advantages :

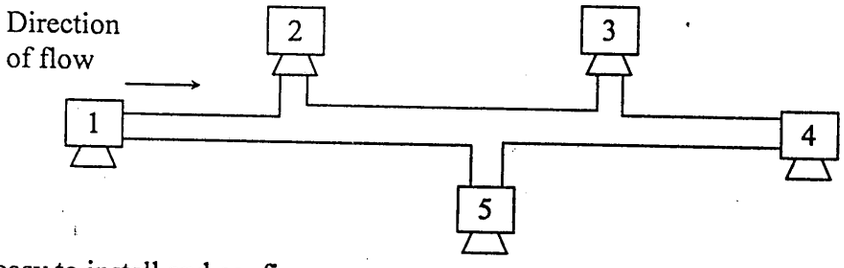
1. Ease of installation
2. Backbone cable can be laid along the most efficient path.
3. Less cabling required.

Disadvantages :

1. Difficult reconfiguration and fault isolation.
2. Signal reflection at the taps can cause degradation in quality.
3. A fault or break in the bus cable stops transmission.

V. RING :

Each device has a dedicated point–to–point line configuration only with the two devices on other side of it.



Advantages :

1. Relatively easy to install and configure.

Disadvantages :

1. Unidirectional traffic can be a disadvantage.
2. A break in the ring can disable the entire network.

Transmission Mode :

Transmission mode term is used to define the direction of signal flow between two linked devices.

There are three types of transmission modes :

1. **Simplex :**
   In simplex mode, the communication is unidirectional. Only one of the two stations on a link can transmit, the other can only receive.
   e.g. keyboard, T.V., pager.
2. **Half duplex :**
   In half duplex mode, each station can both transmit and receive, but not at the same time.
   e.g. Walky talky.
3. **Full duplex :**
   In full duplex mode, both stations can transmit and receive simultaneously.
   e.g. Telephone.

Some Definitions :

1. **Protocol :**
   A protocol is a set of rules that govern data communication.
   A protocol defines what is communicated and when it is communicated.
2. **Internet :**
   A collection of interconnected networks is called an internetwork or just internet.
   A common form of internet is a collection of LAN's connected by a WAN.
   Internet(note uppercase I) means a specific worldwide internet that is widely used to connect universities, government offices, companies etc.
3. **Intranet :**

- An intranet is a private network that is contained with an enterprise. It may consist of many interlinked local area networks and also use leased lines in the wide area network.
- An intranet includes connections through one or more gateway computers to the outside internet.
- The main purpose of intranet is to share company information and computing resources among employees.
- An intranet can also be used to facilitate working in groups and for teleconferences.

Related Questions :

1. Compare and contrast tree and ring topologies in LAN.
2. Give definitions –
   (i) LAN (ii) WAN (iii) Protocol (iv) Full duplex
3. Explain different types of network topology.
4. Define the following terms –
   (i) Topology (ii) Protocol (iii) Internet (iv) Intranet
5. What is a network topology? Explain the different factors to be considered in the selection of a network topology.

The OSI Reference Model :

The model is called the ISO OSI (Open systems Interconnection) model because it deals with connecting open systems i.e. systems that are open for communication with other systems. The OSI model is not a network architecture because it does not specify the exact services and protocols to be used in each layer. It just tells what each layer should do.

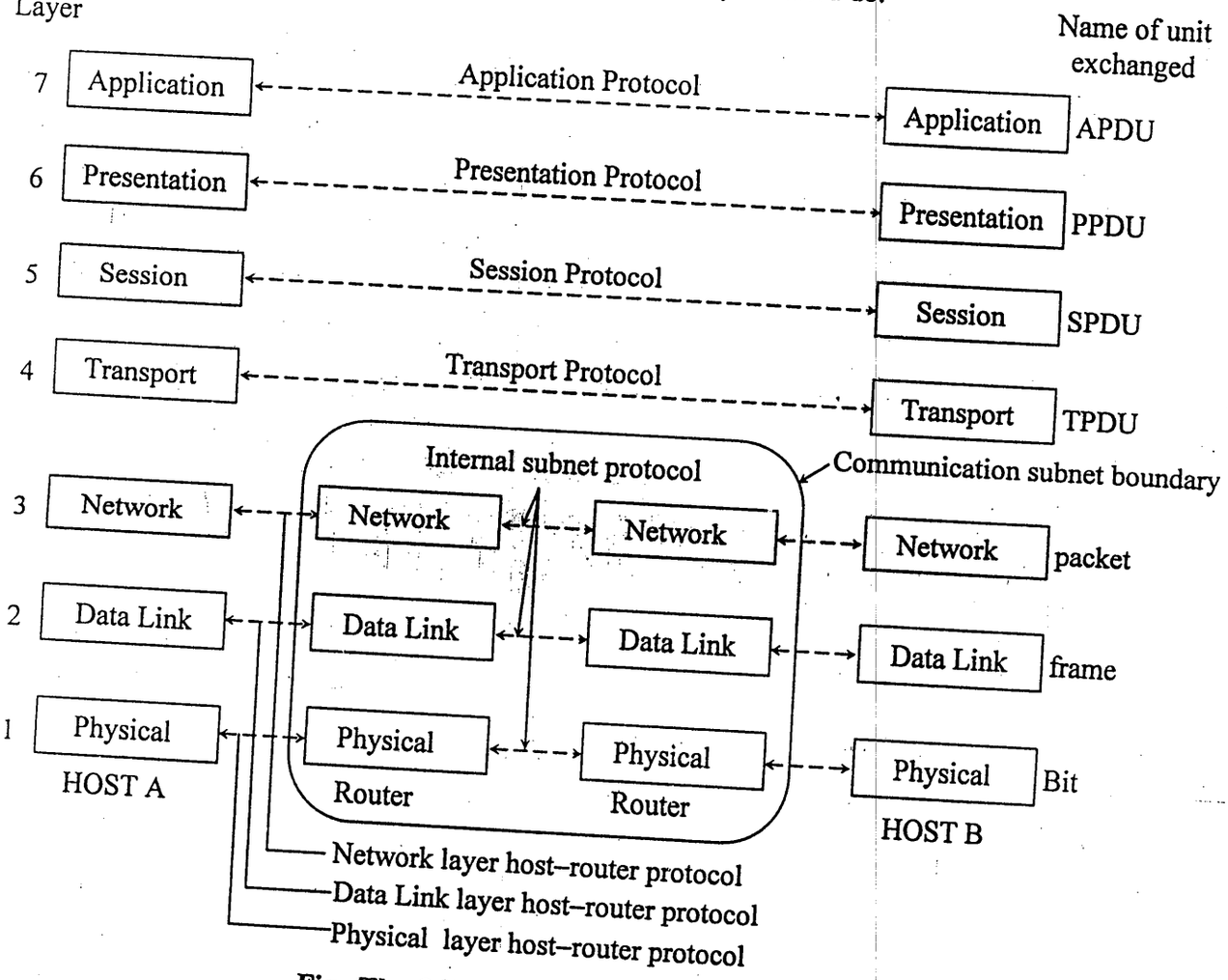


Fig. The OSI reference model

The OSI model has seven layers –

1. **The Physical layer :**
   - The physical layer is concerned with transmitting raw bits over a communication channel.
   - This layer deals with mechanical and electrical specifications of primary connections such as cables, connectors and signaling options that physically link 2 nodes on a network.
2. **The Data Link Layer :**

   The Data Link Layer is responsible for delivering data units from one station to the next without errors.

   A data unit with header and trailer is called a frame.

   Responsibilities :

   a. *Node–to–node delivery.*
   b. *Addressing* : Physical addressing is done at data link layer.

c. *Access Control* : When two or more devices are connected to the same link, which device has control over the link is decided by DLL.
d. *Flow Control* : Flow control avoids the fast transmitter from drowning the slower receiver.
e. *Error control:* Error control means error correction. It allows the receiver to inform the sender of any frame lost or damaged in transmission and co-ordinates the re-transmission of those frames by the sender.
f. *Synchronization:*
DLL is divided into : (1) LLC (2) MAC

3. The Network Layer :
The network layer is responsible for source to destination delivery of packet across multiple network links.

Responsibilities :
a. Source to destination delivery.
b. Logical addressing.
c. Routing
d. Multiplexing

4. The Transport Layer :
The transport layer is responsible for source to destination delivery of entire message.

Responsibilities :
a. End–to–end message delivery
b. Service–point(port or sockect) addressing
Guaranteeing delivery of message to appropriate application of computer.
c. Segmentation and reassembly.
d. Connection control
Deciding whether or not to send all packets by a single path.

5. The Session Layer :
One of the services of the session layer is to manage dialogue control.

It establishes, maintains and synchronizes the interaction between communicating devices.

Responsibilities :
a. *Session management :*
Introduction of checkpoints and dialog units appropriate for transmission.
b. *Synchronization :*
Deciding in what order to pass the dialog units to the transport layer and where in the transmission to require confirmation from the receiver.
c. *Dialog control* :
Deciding who sends and when.
d. *Graceful close :*
Ensuring that exchange has been appropriately completely before the session closes..

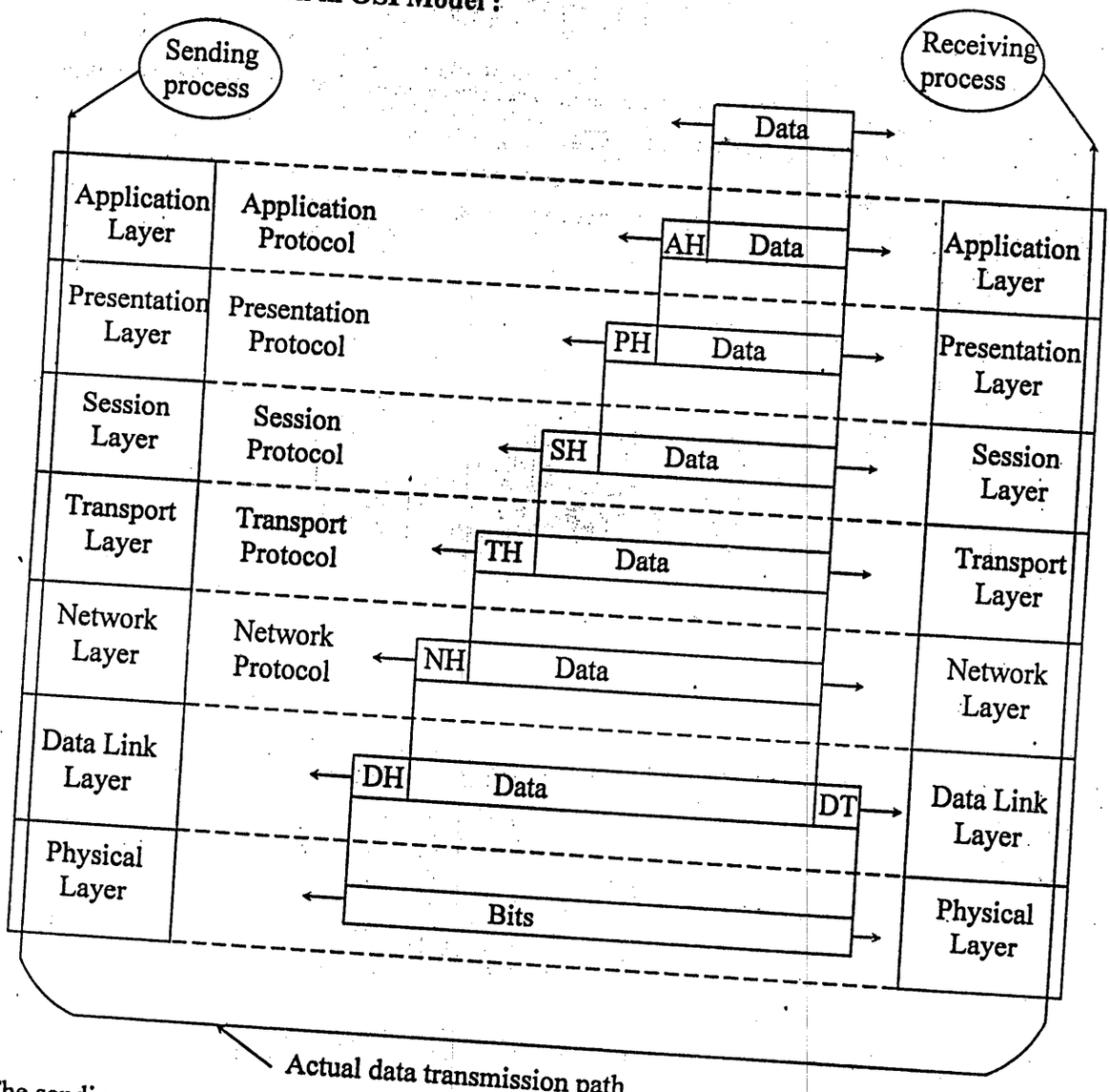
6. Presentation Layer :
The Presentation layer ensures interoperability among communicating devices.
It provides the necessary translation of different control codes, character sets, graphics characters.

Responsibilities :
a. Translation
b. Encryption
c. Compression
d. Security validating passwords and login codes.

7. Application layer :
The Application layer provides user interfaces and support for services such as e–mail, remote file access and transfer, shared database management and others.

Applications :
a. Network virtual terminal
b. File access, transfer and management
c. Mail services
d. Directory services.

Data Communication in OSI Model :



The sending process has some data it wants to send to the receiving process.

It gives the data to the application layer, which then attaches the application header, AH to the front of it and gives the resulting item to the presentation layer.

The presentation layer may transform this item in various ways and possibly add a header to the front, giving the result to the session layer.

This process is repeated until the data reach the physical layer where they are actually transmitted to the receiving machine.

On the receiving machine the various header are stripped off one by one as the message propagates up the layers until it finally arrives at the receiving process.

Related Questions :

1. Explain in brief the network architecture and data transmission in ISO–OSI reference model?
2. Explain in brief the ISO–OSI reference model.
3. Which are the key plus points of layered approach in architecture of network?

Soln: The key plus points of layered approach in architecture of network are –

1. A layer should be created where a different level of abstraction is needed.
2. Each layer should perform a well defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity, and small enough that the architecture does not become unwieldy.

MAXIMUM DATA RATE OF THE CHANNEL :

Nyquist's Theorem :

Nyquist proved that if an arbitrary signal has been run through a low pass filter of bandwidth H, the filtered signal can be completely reconstructed by making only 2H samples per second.

If the signal consists of V discrete levels,

Nyquist's Theorem states :

Maximum data rate = $2 H \log_2 V$ bits/sec

e.g. A noiseless 3KHz channel cannot transmit binary signal at a rate exceeding 6000 bps.

Shannon's Theorem :

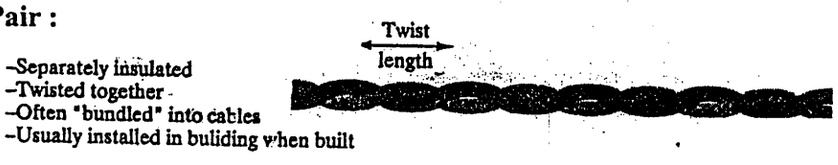
Shannon's major result is that the maximum data rate of a noisy channel whose bandwidth is H Hz, and whose signal–to–noise ratio is S/N, is given by,

Maximum number of bits/sec = $H \log_2 (1+S/N)$

Shannon's result was derived using information theory arguments and applied to any cannel subject to Gaussian (thermal) noise.

Transmission Media :

1. **Magnetic Media :**
   One of the most common ways to transport data from one computer to another is to write them onto magnetic tape or floppy disks, physically transport the tape or disks to the destination machine, and read them back in again. Although bandwidth is excellent delay characteristics are poor.
2. **Twisted Pair :**



(a) Twisted pair

A twisted pair consists of two insulated copper wires, typically about 1mm thick.

The wires are twisted together in a helical form, just like a DNA molecule. The purpose of twisting the wires is to reduce electrical interference from similar pairs close by. (Two parallel wires constitute a simple antenna; a twisted pair does not).

Twisted pairs can be used for either analog or digital transmission.

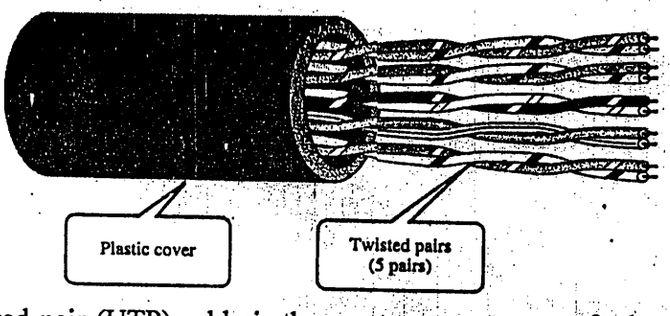
The bandwidth depends on the thickness of the wire and distance traveled.

Twisted pair cabling comes in various varieties:

Twisted pair comes in two varieties :

1. Unshielded twisted-pair (UTP) 2. Shielded twisted pair (STP)

Unshielded twisted-pair (UTP):



Unshielded twisted-pair (UTP) cable is the most common type of telecommunication medium in use. Its frequency range is suitable for transmitting both data and voice. A twisted pair consists of two conductors (usually copper), each with is its own colored plastic insulation. The Plastic insulation is color-banded for identification .Colors are used both to identify the specific conductors in a cable and to indicate which wires belong in pairs and how they relate to other pairs in a larger bundle.

Advantages of UTP are:

- UTP is cheap, flexible, and easy to install.
- Ease of use.
- Higher grades of UTP are used in many LAN technologies ,including Ethernet and Token Ring.

a. Category 1: The basic twisted –pair cabling used in telephone systems. This level of quality is fine for voice but inadequate for all but low-speed data communication.

b. Category 2: The next higher grade, suitable for voice and for data transmission of up to 4 Mbps.

c. Category 3 :

Required to have at least three twists per foot and can be used for data transmission of up to 10 Mbps. It is the standard cable for most telephone systems.

UTP cables and associated connected hardware whose transmission characteristics are specified upto 16 MHz.

d. Category 4 :

Must also have at least three twists per foot as well as other conditions to bring the possible transmission rate to 16 Mbps.

UTP cables and associated connected hardware whose transmission characteristics are specified upto 20 MHz.

e. Category 5 :

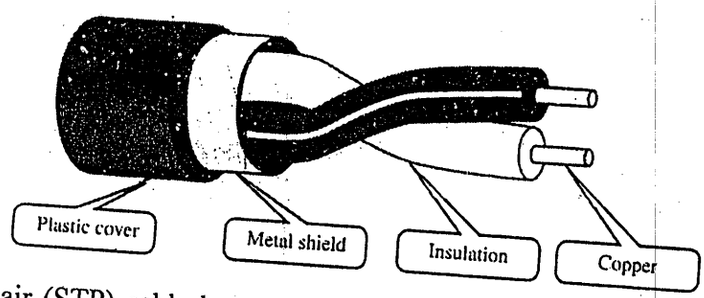
Used for data transmission up to 100 Mbps.

UTP cables and associated connected hardware whose transmission characteristics are specified upto 100 MHz.

It is commonly used medium in the telephone network.

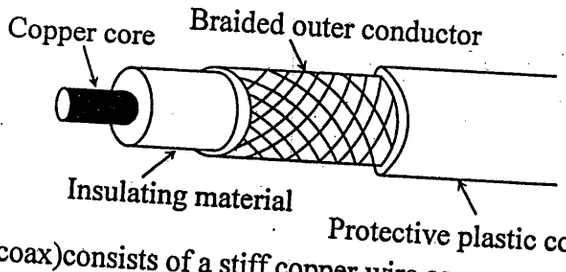
Total Data rate	4 Mbps
Bandwidth	3 MHz
Repeater spacing	2 to 10 km

Shielded twisted-pair (STP) :



Shielded twisted-pair (STP) cable has a metal foil or braided–mesh covering that encases each pair of insulated conductors .The metal casing prevents the penetration of electromagnetic noise.It also can eliminate a phenomenon called **crosstalk**,which is the undesired effect of one circuit (or channel) on another circuit (or channel) .It occurs when one line (acting as a kind of sending antenna).This effect can be experienced during telephone conversations when one can hear other conversations in the background .Shielding each pair of a twisted-pair cable can eliminate most crosstalk.

3. Coaxial Cable :



A coaxial cable (coax)consists of a stiff copper wire as core, surrounded by an insulating material. The insulator is encased by a cylindrical conductor, often as a closely woven braided mesh.

Coaxial cable carries signals of higher frequency ranges than twisted-pair cable.Instead of having two wires,coax has a central core conductor of solid or stranded wire enclosed in an insulating sheath,which, is in turn,encased in an outer conductor of metal foil.The outer metallic wrapping serves both as a shield against noise and as a second conductor ,which completes the circuits.

The outer conductor is covered in a protective plastic sheath.

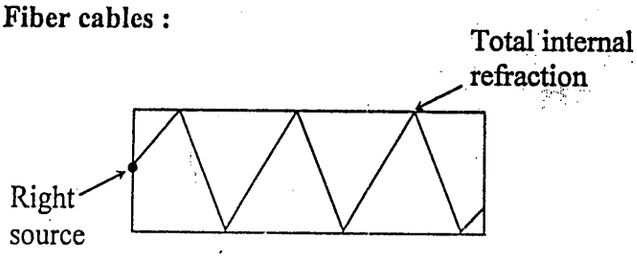
Two kinds of coaxial cable are widely used.

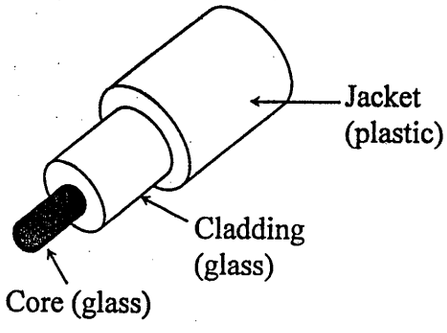
- 50 – ohm cable used for digital transmission
- 75 – ohm cable used for analog transmission

Coaxial cable is widely used for cable television.

Total Data Rate	500 Mbps
Bandwidth	350 MHz
Repeater spacing	1 to 10 km

4. Fiber cables :





Optical fiber is made of glass or plastic and transmits signals in the form of light.

Principle on which fiber cables work :

When a light ray passes from one medium to another, for example, from fused silica to air, the ray is refracted at the silica/air boundary.

For angles of incidence above a certain critical value, the light is refracted back into the silica, none of it escapes into the air.

Thus a light ray incident at or above the critical angle is trapped inside the fiber and can propagate for many kilometers with virtually no loss.

Construction :

At the center is the glass core through with the light propagates. In multimedia fibers, the core is 50 microns in diameter and in case of single mode fibers it is 8 to 10 microns.

The core is surrounded by a glass cladding with a lower index of refraction than the core, to keep all the light in the core.

Next comes a thin plastic jacket to protect the cladding.

Optical fibers main applications are long haul trunks, Metropolitan trunks, etc.

Total Data Rate	2 Gbps
Bandwidth	2 GHz
Repeater Spacing	10 to 100 km

Related Questions :

1. Write a short note on Transmission media in computer networks.
2. Fiber optic transmission media.
3. State Nyquist and Shannon's limits for maximum data rates through channel.
4. State different physical media properties. Also write about twisted pair cables.
5. Compare different transmission media for different parameters.

Mobile Phones have gone through three distinct generations, with different technologies :

1. Analog voice
2. Digital voice
3. Digital voice and data (Internet, e–mail, etc)

First–Generation Mobile Phones : Analog Voice

In 1946, the first system for car–based telephones was set up in St. Louis. This system used a single large transmitter on top of a tall building and has 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, known as **push–to–talk systems,** were installed in several cities beginning in the late 1950s.

In the 1960s, **IMTS (Improved Mobile Telephone System)** was installed. It, too, used a high–powered (200–watt) transmitter, on top of a hill, but now had two frequencies, one for sending and one for receiving, so the push–to–talk button was no longer needed. Since all communication from the mobile telephones went inbound on a different channel than the outbound signals, the mobile users could not hear each other.

IMTS supported **23 channels** spread out from **150 MHz to 450 MHz.** Due to the small number of channels, users often had to wait a long time before getting dial tone. Also, due to the large power of the hilltop transmitter, adjacent system has to be several hundred kilometers apart to avoid interference. All in all the limited capacity made the system impractical.

Advanced Mobile Phone System

In all mobile phone systems, a geographic region is divided up into cells, which is why the devices are sometimes called cell phones. In AMPS, the cells are typically 10 to 20 km across; in digital systems, the cells are smaller. Each cell uses some set of frequencies not used by any of its neighbors. The key idea that gives cellular systems far more capacity than previous systems is the use of relatively small cells and the reuse of transmission frequencies in nearby (but not adjacent) cells.

Thus, the cellular design increases the system capacity by at least an order of magnitude, more as the cells get smaller. Furthermore, smaller cells mean that less power is needed, which leads to smaller and cheaper transmitters and handsets.

The idea of frequency reuse is illustrated in the Fig.(a). The cells are normally roughly circular, but they are easier to model as hexagons. In Fig. (b), the cells are all the same size. They are grouped in units of seven cells. Each letter indicates a group of frequencies. Notice that for each frequency set, there is a buffer about two cells wide where that frequency is not reused, providing for good separation and low interference.

In an area where the number of users has grown to the point that the system is overloaded, the power is reduced, and the overloaded cells are split into smaller **microcells** to permit more frequency reuse, as shown in Fig. (b). Telephone companies sometimes create temporary microcells, using portable towers with satellite links at sporting events, rock concerts, and other places where large number of mobile users congregate for a few hours.

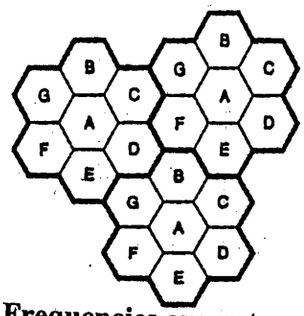


Fig (a) : Frequencies are not reused in adjacent cells

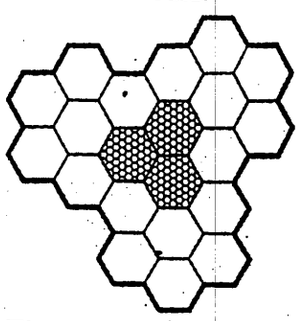


Fig (b) : To add more users, smaller cells can be used.

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 as **MTSO (Mobile Telephone Switching Office) or MSC (Mobile Switching Center).** In a larger one, several MTSOs may be needed, all of which are connected to a second–level MTSO, and so on. The MTSOs are essentially end offices as in the telephone system, and are, in fact, connected to at least one telephone system end office.

At any instant, each mobile telephone is logically in one specific cell and under the control of that cell's base station. When a mobile telephone physically leaves a cell, its base station notices the telephone's signal fading away and asks all the surrounding base stations how much power they are getting from it. The base station then transfers ownership to the cell getting the strongest signal, that is, the cell where the telephone is now located. The telephone is then informed of its new boss, and if a call is in progress, it will be asked to switch to a new channel (because the old one is not reused in any of the adjacent cells). This process, called handoff, takes about 300 msec. Channel assignment is done by the MTSO, the nerve center of the system. The base stations are really just radio relays.

Handoffs can be done in two ways. In a **soft handoff,** the telephone is acquired by the new base station before the previous one signs off. In this way there is no loss of continuity. The downside here is that the telephone needs to be able to tune to two frequencies at the same time (the old one and the new one). Neither first nor second generation devices can do this.

In a **hard handoff,** the old base station drops the telephone before the new one acquires it. If the new one is unable to acquire it (e.g. because there is no available frequency), the call is disconnected abruptly. Users tend to notice this, but it is inevitable occasionally with the current design.

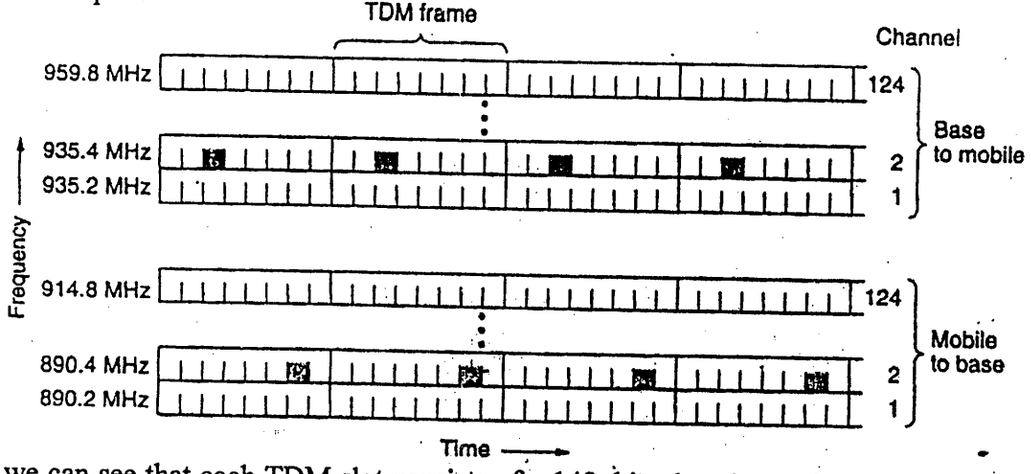
D - AMPS – The Digital Advanced Mobile Phone System

D–AMPS was carefully designed to co–exist with AMPS so that both first and second generation mobile phones could operate simultaneously in the same cell. In particular, D–AMPS uses the same 30 kHz channels as AMPS and at the same frequencies so that one channel can be analog and the adjacent ones can be digital. Depending on the mix of phones in a cell, the cell's MTSO determines which channels are analog and which are digital, and it can change channel types dynamically as the mix of phones in a cell changes.

GSM – The Global System for Mobile Communications

Virtually everywhere else in the world, a system called **GSM (Global System for Mobile communications)** is used, and it is even starting to be used in the U.S. on a limited scale. To a first approximation, GSM is similar to D–AMPS. Both are cellular systems. In both systems, frequency division multiplexing is used, with each mobile transmitting on one frequency and receiving on a higher frequency (80 MHz higher for D–AMPS, 55 MHz higher for GSM). Also in both systems, a single frequency pair is split by time division multiplexing into time slots shared by multiple mobiles. However, the SGM channels are much wider than the AMPS channels (200 kHz versus 30 kHz) and hold relatively few additional users (8 versus 3), giving GSM a much higher data rate per user than D–AMPS.

Each frequency band is 200 kHz wide, as shown in the figure. A GSM system has 124 pairs of simplex channels. Each simplex channel is 200 kHz wide and supports eight separate connections on it, using time division multiplexing. Each currently active station is assigned one time slot on one channel pair.



Here we can see that each TDM slot consists of a 148–bits data frame that occupies the channel for 577 μsec (including a 30–μsec guard time after each slot). Each data frame starts and ends with three 0 bits, for frame delineation purposes. 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. Between the Information fields is a 26–bit Sync (training) field that is used by the receiver to synchronize to the sender's frame boundaries.

CDMA – Code Division Multiple Access

D – AMPS and GSM are fairly conventional systems. They use both FDM and TDM to divide the spectrum into channels and the channels into time slots. However, there is a third kid on the block. CDMA (Code Division Multiple Access), which works completely differently.

CDMA is completely different from AMPS, D–AMPS, and GSM. Instead of dividing the allowed frequency range into a few hundred narrow channel, CDMA allows each station to transmit over the entire frequency spectrum all the time. Multiple simultaneous transmissions are separated using coding theory. CDMA also relaxes the assumption that colliding frames are totally garbled. Instead, it assumes that multiple signals add linearly.

Let us consider an analog; an airport lounge with many pairs of people conversing. TDM is comparable to all the people being in the middle of the room but taking turns speaking. FDM is comparable to the people being in widely separated clumps, each clump holding its own conversation at the same time as, but still independent of, the others. CDMA is comparable to everybody being in the middle of the room talking at once, but with each pair in a different language. The French speaking couple just hones in on the French, rejecting everything that is not French as noise. Thus, the key to CDMA is to be able to extract the desired signal while rejecting everything else as random noise.

In CDMA, each bit time is subdivided into m short intervals called **chips.** Typically, there are 64 or 128 chips per bit, but in the example given below we will use 8 chips/bit for simplicity.

Each station is assigned a unique m–bit code called a **chip sequence.** To transmit a 1 bit, a station sends its chip sequence. To transmit a 0 bit, it sends the one's complement of its chip sequence. No other patterns are permitted. Thus, for m = 8, if station A is assigned the chip sequence 00011011, it sends a 1 bit by sending 00011011 and a 0 bit by sending 11100100.

Increasing the amount of information to be send from b bits/sec to mb chips/sec can only be done if the bandwidth available is increased by a factor of m, making CDMA a form of spread spectrum communication (assuming no changes in the modulation or encoding techniques). If we have a 1–MHz band available for 100 stations, with FDM each one would have 10 kHz and could send at 10 kbps (assuming 1 bit per Hz). With CDMA, each station uses the full 1 MHz, so the chip rate is 1 megachip per second. With fewer than 100 chips per bit, the effective bandwidth per station is higher for CDMA than FDM, and the channel allocation problem is also solved.

A : 0 0 0 1 1 0 1 1
B : 0 0 1 0 1 1 1 0
C : 0 1 0 1 1 1 0 0
D : 0 1 0 0 0 0 1 0

(a)

Binary chip sequences for four stations.

A : (–1 –1 –1 +1 +1 –1 +1 +1)
B : (–1 –1 +1 –1 +1 +1 +1 –1)
C : (–1 +1 –1 +1 +1 +1 –1 –1)
D : (–1 +1 –1 –1 –1 –1 +1 –1)

(b)

Bipolar chip sequences

Six examples :

– – 1 –	C
– 1 1 –	B + $\overline{C}$
1 0 – –	A + $\overline{B}$
1 0 1 –	A + B + C
1 1 1 1	A + B + $\overline{C}$ + D
1 1 0 1	A + $\overline{B}$ + C + D

$S_1 = (-1 +1 -1 +1 +1 +1 -1 -1)$
$S_2 = (-2\ \ 0\ \ 0\ \ 0 +2 +2\ \ 0 -2)$
$S_3 = (\ 0\ \ 0 -2 +2\ \ 0 -2\ \ 0 +2)$
$S_4 = (-1 +1 -3 +3 +1 -1 -1 +1)$
$S_5 = (-4\ \ 0 -2\ \ 0 +2\ \ 0 +2 -2)$
$S_6 = (-2 -2\ \ 0 -2\ \ 0 -2 +4\ \ 0)$

(c)

Six examples of transmissions

$S_1 \bullet C = (1 +1 +1 +1 +1 +1 +1 +1)/8 = 1$
$S_2 \bullet C = (2 +0 +0 +0 +2 +2 +0 +2)/8 = 1$
$S_3 \bullet C = (0 +0 +2 +2 +0 -2 +0 -2)/8 = 0$
$S_4 \bullet C = (1 +1 +3 +3 +1 -1 +1 -1)/8 = 1$
$S_5 \bullet C = (4 +0 +2 +0 +2 +0 -2 +2)/8 = 1$
$S_6 \bullet C = (2 -2 +0 -2 +0 -2 -4 +0)/8 = -1$

Fig. (d) Recovery of station C's signal

Each station has its own unique chip sequence. Let us use the symbol S to indicate the m–chip vector for station S, and $\overline{S}$ for its negation. All chip sequences are pair wise **orthogonal,** by which we mean that the normalized inner product of any two distinct chip sequences, S and T (written as S·T), is 0. It is known how to generate such orthogonal chip sequences using a method known as Walsh codes. In mathematical terms, orthogonality of the chip sequences can be expressed as follows :

$$S \cdot T \equiv \frac{1}{m}\sum_{i=1}^{m} S_i T_i = 0$$

In plain English, as many pairs are the same as are different. This orthogonality property will prove crucial later on. Note that if S·T = 0, then $S \cdot \overline{T}$ is also 0. The normalized inner product of any chip sequence with itself is 1:

$$S \cdot S = \frac{1}{m}\sum_{i=1}^{m} S_i S_i = \frac{1}{m}\sum_{i=1}^{m} (\pm 1)^2 = 1$$

This follows because each of the m terms in the inner product is 1, so the sum is m. Also note that S·S = –1.

During each bit time, a station can transmit a 1 by sending its chip sequence, it can transmit a 0 by sending the negative of its chip sequence, or it can be silent and transmit nothing. For the moment, we assume that all stations are synchronized in time, so all chip sequences begin at the same instant.

When two or more stations transmit simultaneously, their bipolar signals add linearly. For example, if in one chip period three stations output +1 and one station outputs –1, the result is +2. One can think of this as adding voltages: three stations outputting +1 volts and 1 station outputting –1 volts gives 2 volts.

In fig. (c) we see six examples of one or more stations transmitting at the same time. In the first example, C transmits a 1 bit, so we just get C's chip sequence. In the second example, both B and C transmit 1 bits, so we get the sum of their bipolar chip sequences, namely:

$$(-1-1+1-1+1+1+1-1)+(-1+1-1+1+1+1+1-1-1) = (-2\ 0\ 0\ 0\ +2\ +2\ 0\ -2)$$

In the third example, station A sends a 1 and station B sends a 0. The others are silent. In the fourth example, A and C send a 1 bit while B sends a 0 bit. In the fifth example, all four stations send a 1 bit. Finally, in the last example, A, B, and D send a 1 bit, while C sends a 0 bit. Note that each of the six sequences S_1 through S_6 given in fig.(c) represents only one bit time.

To recover the bit stream of an individual station, the receiver must know that station's chip sequence in advance. It does the recovery by computing the normalized inner product of the received chip sequence (the linear sum of all the stations that transmitted) and the chip sequence of the station whose bit stream it is trying to recover. If the received chip sequence is S and the receiver is trying to listen to a station whose chip sequence is C, it just computes the normalized inner product S·C.

To see why this works, just imagine that two stations, A and C, both transmit a 1 bit at the same time that B transmits a 0 bit. The receiver sees the sum, S = A + B + C and computes

$$S \cdot C = (A + \overline{B} + C) \cdot C = A \cdot C + \overline{B} \cdot C + C \cdot C = 0 + 0 + 0 = 1$$

The first two terms vanish because all pairs of chip sequences have been carefully chosen to be orthogonal. Imagine that the three chip sequences all came in separately, rather than summed. Then, the receiver would compute the inner product with each one separately and add the results.

Due to the orthogonality property, all the inner products except C·C would be 0. Adding them and then doing the inner product is in fact the same as doing the inner products and then adding those.

To make the decoding process more concrete, let us consider the six examples of Fig. (c) again as illustrated in Fig. (d). Suppose that the receiver is interested in extracting the bit send by station C from each of the six sums S_1 through S_6. It calculates the bit by summing the pair wise products of the received S and the C vector of Fig. (b) and then taking 1/8 of the result (since m = 8 here). As shown, the correct bit is decoded each time. It is just like speaking French

In an ideal, noiseless CDMA system, the capacity (i.e number of stations) can be made arbitrarily large, just as the capacity of a noiseless Nyquist channel can be made arbitrarily large by using more and more bits per sample. In practice, physical limitations reduce the capacity considerably. First, we have assumed that all the chips are synchronized in time. In reality, such synchronization is impossible. What can be done is that the sender and receiver synchronize by having the sender transmit a predefined chip sequence that is long enough for the receiver to lock onto. All the other (unsynchronized) transmissions are then seen as random noise. If there are not too many of them, however, the basic decoding algorithm still works fairly well.

An implicit assumption in our discussion is that the power levels of all stations are the same as perceived by the receiver. CDMA is typically used for wireless systems with a fixed base station and many mobile stations at varying distances from it. The power levels received at the base station depend on how far away the transmitters are.

Community Antenna Television

The system initially consisted of a big antenna on top of a hill to pluck the television signal out of the air, an amplifier, called the head end, to strengthen it, and a coaxial cable to deliver it to people's houses, as illustrated in figure below.

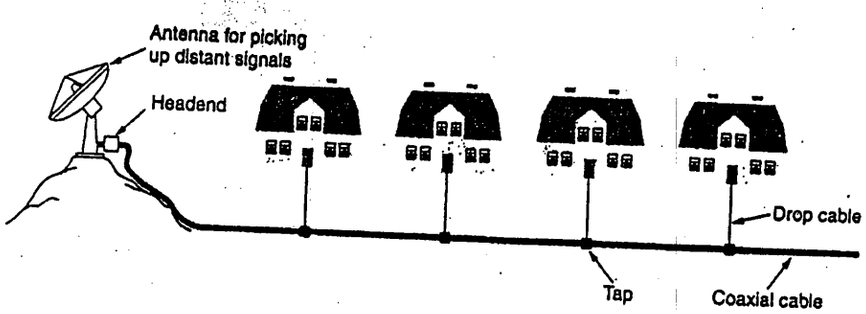


Fig. An early cable television system

In the early years, cable television was called Community Antenna Television. As the number of subscribers grew, additional cables were spliced onto the original cable and amplifiers were added as needed. Transmission was one way, from the head end to the users.

A system with fiber for the long–haul runs and coaxial cable to the houses is called an HFC (Hybrid Fiber Coax) system. The electro–optical converters that interface between the optical and electrical parts of the system are called fiber nodes. Because the bandwidth of fiber is so much more than that of coax, a fiber node can feed multiple coaxial cables. part of a modern HFC system is shown in figure below.

However, there is another difference between the HFC system to figure (a) and the telephone system of figure (b) that is much harder to remove. Down in the neighborhoods, a single cable is shared by many houses, whereas in the telephone system, every house has its own private local loop. When used for television broadcasting, this sharing does not play a role. All the programs are broadcast on the cable and it does not matter whether there are 10 viewers or 10,000 viewers. When the same cable is used for Internet access, it matters a lot if there are 10 users or 10,000. If one user decides to download a very large file, that bandwidth is potentially being taken away from other users. The more the users, the more competition for bandwidth. The telephone system does not have this particular property: downloading a large file over an ADSL line does not reduce your neighbor's bandwidth. On the other hand, the bandwidth of coax is much higher than that of twisted pairs.

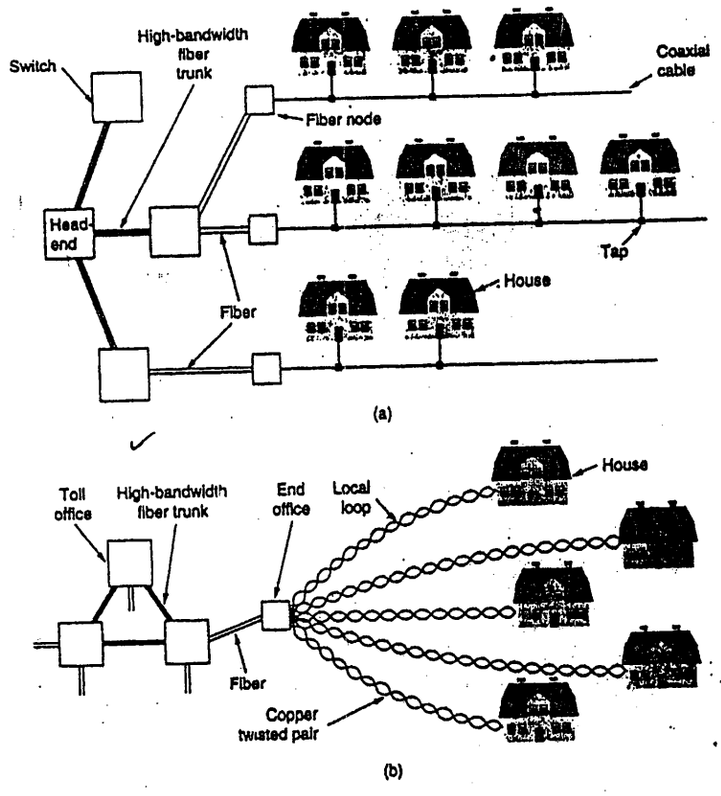


Fig. (a) Cable television (b) The fixed telephone system

The way the cable industry has tackled this problem is to split up long cables and connect each one directly to a fiber node. The bandwidth from the headend to each fiber node is effectively infinite, so as long as there are not too many subscribers on each cable segment, the amount of traffic is manageable. Typical cables nowadays have 500–2000 houses, but as more and more people subscribe to Internet over cable, the load may become too much, requiring more splitting and more fiber nodes.

The 802.11 Protocol Stack

A partial view of the 802.11 protocol stack is given in figure below. The physical layer corresponds to the OSI physical layer fairly well, but the data link layer in all the 802 protocols is split into two or more sublayers. In 802.11, the MAX (Medium Access Control) sublayer determines how the channel is allocated, that is, who gets to transmit next. Above it is the LLC (Logical Link Control) sublayer, whose job it is to hide the differences between the different 802 variants and make them indistinguishable as far as the network layer is concerned.

802.11 standard specifies three transmission techniques allowed in the physical layer. The infrared method uses much the same technology as television remote controls do. The other two use short–range radio, using techniques called FHSS and DSSS. Both of these use a part of the spectrum that does not require licensing (the 2.4GHz ISM band).

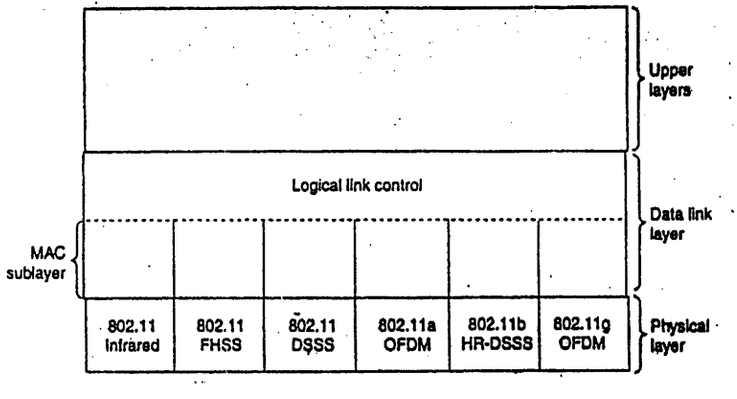


Fig. Part of the 802.11 protocol

All of these techniques operate at 1 or 2 Mbps and at low enough power that they do not conflict too much. In 1999, two new techniques were introduced to achieve higher bandwidth. These are called OFDM and HR–DSSS.

Each of the five permitted transmission techniques makes it possible to send a MAC frame from one station to another.

The infrared options uses diffused (i.e. not line of sight) transmission at 0.85 or 0.95 microns. Two speeds are permitted : 1Mbps and 2 Mbps.
Infrared signals cannot penetrate walls, so cells in different rooms are well isolated from each other.

FHSS (Frequency Hopping Spread Spectrum) uses 79 channels, each 1–MHz wide, starting at the low end of the 2.4GHz ISM band. A pseudorandom number generator is used to produce the sequence of frequencies hopped to. As long as all stations use the same seed to the pseudorandom number generator and stay synchronized in time, they will hop to the same frequencies simultaneously. The amount of time spent at each frequency, the dwell time, is an adjustable parameter, but must be less than 400 msec.

It also provides a modicum of security since an intruder who does not know the hopping sequence or dwell time cannot eavesdrop on transmissions. Over longer distances, multipath fading can be an issue, and FHSS offers good resistance to it. It is also relatively insensitive to radio interference, which makes it popular for building to building links. Its main disadvantage is its low bandwidth.

The third modulation method. DSSS (Direct Sequence Spread Spectrum), is also restricted to 1 or 2 Mbps.

Each bit is transmitted as 11 chips, using what is called a Barker sequence.
The first of the high–speed wireless LANs, 802.11a, uses OFDM (Orthogonal Frequency Division Multiplexing) to deliver up to 54 Mbps in the wider 5–GHz ISM band.
Splitting the signal into many narrow bands has some key advantages over using a single wide band, including better immunity to narrowband interference and the possibility of using noncontiguous bands.

HR–DSSS (High Rate Direct Sequence Spread Spectrum) another spread spectrum technique, which uses 11million chips/sec to achieve 11Mbps in the 2.4–GHz band. It is called 802.11b but is not a follow–up to 802.11a.Although 802.11b is slower than 802.11a., its range is about 7 times greater, which is more important in many situations.

An enhanced version of 8.2.11b, 802.11g. It uses the OFDM modulation method of 802.11a but operates in the narrow 2.4–GHz ISM band along with 802.11b. In theory it can operate at up to 54 Mbps. It is not yet clear whether this speed will be realized in practice.

The 802.11MAC sublayer protocol is quite different from that of Ethernet due to the inherent complexity of the wireless environment compared to that of a wired system.

Since not all stations are within radio range of each other, transmissions going on in one part of a cell may not be received elsewhere in the same cell. In this example, station C is transmitting to station B. If A senses the channel, it will not hear anything and falsely conclude that it may now start transmitting to B.

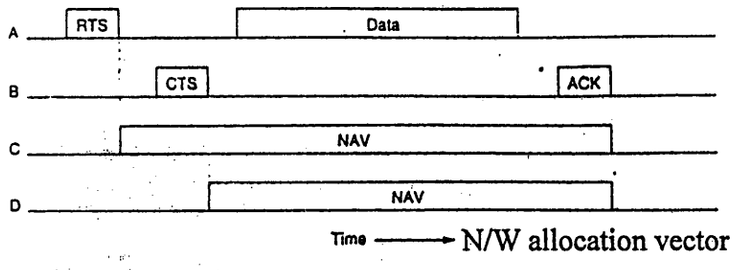
Is the inverse problem, the exposed station problem, illustrated in fig. below. Here B wants to send to C so it listens to the channel. When it hears a transmission, it falsely concludes that it may not send to C, even though A may be transmitting to D (not shown). 802.11 supports two models of operation. The first, called DCF (Distributed Coordination Function), does not use any kind of central control (in that respect, similar to Ethernet). The other, called PCF (Point Coordination Function), uses the base station to control all activity in its cell. All implementations must support DCF but PCF is optional. We will now discuss these two modes in turn.

When DCF is employed, 802.11 uses a protocol called CSMA/CA(CSMA with Collision Avoidance). In this protocol, both physical channel sensing and virtual channel sensing are used. Two methods of operation are supported by CSMA/CA. In the first method, when a station wants to transmit, it senses the channel. If it is idle, it just starts transmitting. It does not sense the channel while transmitting but emits its entire frame, which may well be destroyed at the

receiver due to interference there. If the channel is busy, the sender defers until it goes idle and then starts transmitting. If a collision occurs, the colliding stations wait a random time, using the Ethernet binary exponential back off algorithm, and then try again later.

The other mode of CSMA/CA operation is based on MACAW and uses virtual channel sensing, as illustrated in figure below. In this example, A wants to send to B. C is a station within range of A (and possibly within range of B, but that does not matter). D is a station within range of B but not within range of A.

The protocol starts when A decides it wants to send data to B. It begins by sending an RTS frame to B to request permission to send it a frame. When B receives this request, it may decide to grant permission, in which case it sends a CTS frame back. Upon receipt of the CTS. A now sends its frame and starts an ACK timer. Upon correct receipt of the data frame, B responds with an ACK frame, terminating the exchange. If A's ACK timer expires before the ACK gets back to it, the whole protocol run again.



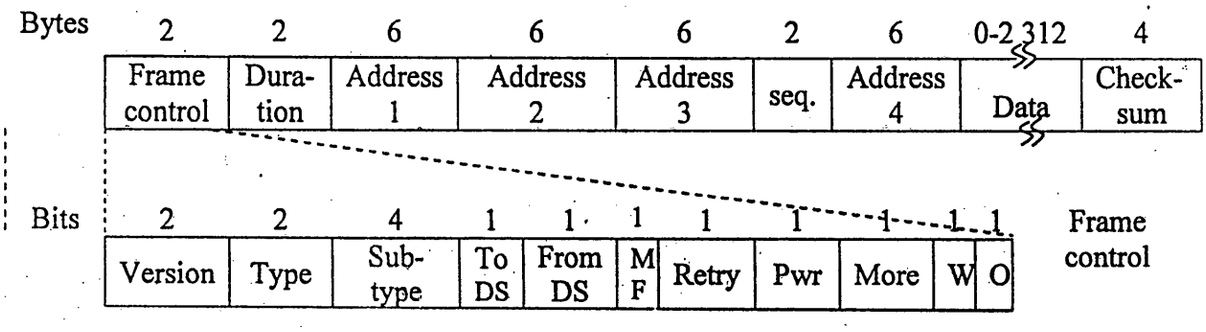
The use of virtual channel sensing using CSMA/CA

Now let us consider this exchange from the viewpoints of C and D. C is within range of A, so it may receive the RTS frame. If it does, it realizes that someone is going to send data soon, so for the good of all it desists from transmitting anything until the exchange is completed. From the information provided in the RTS request, it can estimate how long the sequence will take, including the final ACK , so it asserts a kind of virtual channel busy for itself, indicated by NAV (Network Allocation Vector) in figure. D does not hear the RTS, but it does hear the CTS, so it also asserts the NAV signal for itself. Note that the NAV signals are not transmitted; they are just internal reminders to keep quiet for a certain period of time.

In contrast to wired networks, wireless networks are noisy and unreliable.

The 802.11 standard defines three different classes of frames on the wire: data, control and management.

The frame Control field. It itself has 11 subfields. The first of these is the protocol version, which allows two versions of the protocol to operate at the same time in the same cell. Then come the Type (data, control, or management) and subtype filed (e.g., RTS or CTS). The To DS and From DS bits indicate the frame is going to or coming from the inter cell distribution system (e.g. Ethernet). The MF bit means that more fragments will follow. The retry bit marks a retransmission of a frame sent earlier. The power management bit is used by the base station to put the receiver into sleep state or take it out of sleep state. The more bit indicates that the sender has additional frames for the receiver. The W bit specifies that the frame body has been encrypted using the WEP (Wired Equivalent Privacy) algorithm. Finally, the 0 bit tells the receiver that a sequence of frames with this bit on must be processed strictly in order.



The second field of the data frame, the Duration field, tells how long the frame and its acknowledgement will occupy the channel. This filed is also present in the control frames and is how other stations manage the NAV mechanism. The frame header contains four addresses, all in standard IEEE 802 format. The source and destination are obviously needed, but what are the other two for ? Remember that frames may enter or leave a cell via a base station. The other two addresses are used for the source and destination base stations for inter cell traffic.

The sequence filed allows fragments to be numbered. Of the 16 bits available, 12 identify the frame and 4 identify the fragment. The Data filed contains the payload, upto 23.12 bytes, followed by the usual checksum.

Management frames have a format similar to that of data frames, except without one of the base station addresses, because management frames are restricted to a single cell. Control frames are shorter still, having only one or two addresses, no Data filed, and no sequence filed. The key information here is in the Subtype field, usually RTS.CTS or ACK.

The basic unit of a Bluetooth system, is a piconet, which consists of a master node and up to seven active slave nodes within a distance of 10 meters. Multiple piconets can exist in the same (large) room and can even be connected via a bridge node, as shown in figure below. An interconnected collection of piconets is called a scatternet.

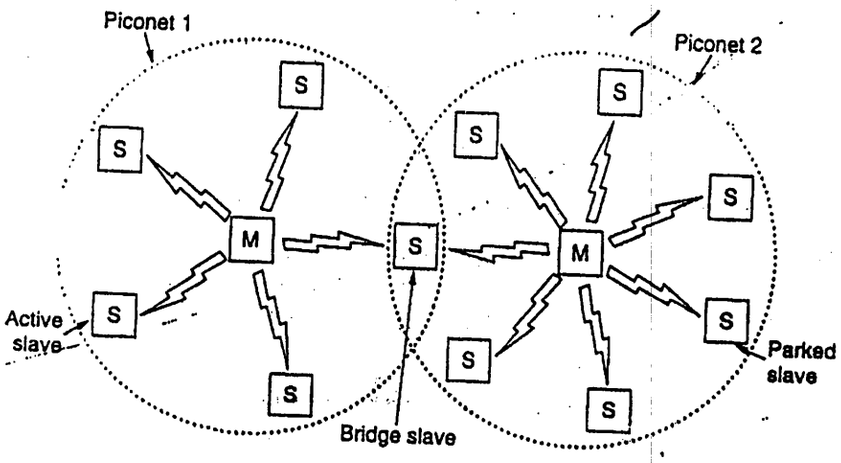


Fig. Two piconets can be connected to form a scatternet.

In addition to the seven active slave nodes in a piconet, there can be up to 255 parked nodes in the net. These are devices that the master has switched to a low power state to reduce the drain on their batteries. In parked state, a device cannot do anything except respond to an activation or beacon signal from the master.

The reason for the master / slave design is that the designers intended to facilitate the implementation of complete Bluetooth chips for under $5. At its heart, a piconet is a centralized TDM system, with the master controlling the clock and determining which device gets to communicate in which time slot.

Bluetooth VI.I specification names 13 specific applications to be supported and provides different protocol stacks for each one. The 13 applications, which are called profiles, are listed in figure below.

Name	Description
Generic access	Procedures for link management
Service discovery	Protocol for discovering offered services
Serial port	Replacement for a serial port cable
Generic object exchange	Defines client–server relationship for object movement
LAN access	Protocol between a mobile computer and a fixed LAN
Dial–up networking	Allows a notebook computer to call via a mobile phone
Fax	Allows a mobile fax machine to talk to a mobile phone
Cordless telephony	Connects a handset and its local base station
Intercom	Digital walkie–talkie
Headset	Allows hands free voice communication
Object push	Provides a way to exchange simple objects
File transfer	Provides a more general file transfer facility
Synchronization	Permits PDA to synchronize with another computer

The generic access profile is not really an application, but rather the basis upon which the real applications are built. Its main job is to provide a way to establish and maintain secure links (channels) between the master and the slaves. Also relatively generic is the service discovery profile, which is used by devices to discover what services other devices have to offer.

The bottom layer is the physical radio layer, which corresponds fairly well to the physical layer in the OSI and 802 models. It deals with radio transmission and modulation.

The base band layer is somewhat analogous to the MAC sub layer but also includes elements of the physical layer. It deals with how the master controls time slots and how these slots are grouped into frames.

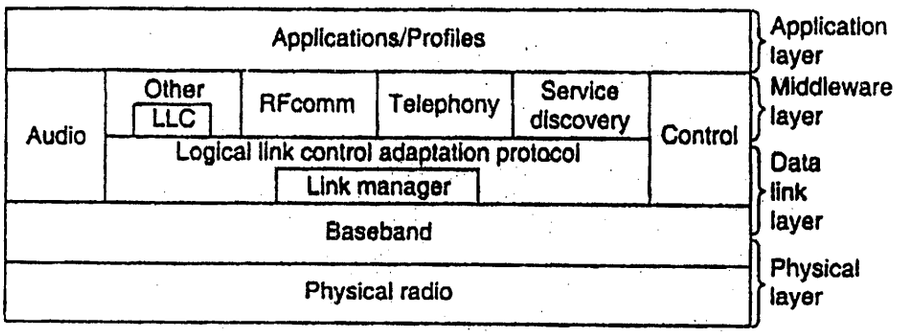


Fig. The 802.15 version of the Bluetooth protocol architecture

The link manager handles the establishment of logical channels between devices, including power management, authentication, and quality of service. The logical link control adaptation protocol (often called L2CAP) shields the upper layers from the details of transmission.

The audio and control protocols deal with audio and control, respectively. The applications can get at them directly, without having to go through the L2CAP protocol.

The middleware layer, which contains a mix of different protocols. The 802 LLC was inserted here by IEEE for compatibility with its other 802 networks. The RF comm. telephony and service discovery protocols are native. RF comm. (Radio Frequency communication) is the protocol that emulates the standard serial port found on PCs for connecting the keyboard, mouse, and modem, among other devices. The telephony protocol is a real–time protocol used for the three speech–oriented profiles. It also manages call setup and termination. Finally, the service discovery protocol is used to locate services within the network.

The top layer is where the applications and profiles are located. They make use of the protocols in lower layers to get their work done. Each applications had its own dedicated subset of the protocols. Specific devices, such as a headset, usually contain only those protocols needed by that application and no others.

The radio layer moves the bits from master to slave, or vice versa. It is a low–power system with a range of 10 meters operation in the 2.4GHz ISM band. The band is divided into 79 channels of 1 MHz each. Modulation is frequency shift keying, with 1 bit per Hz giving a gross data rate of 1 Mbps, but much of this spectrum is consumed by overhead.

The baseband layer is the closest thing Bluetooth has to a MAC sublayer. It turns the raw bit stream into frames and defines some key formats. In the simplest form, the master in each piconet defines a series of 625 μ sec time slots, with the master's transmissions starting in the even slots and the slaves' transmissions starting in the odd ones. This is traditional time division multiplexing, with the master getting half the slots and the slaves sharing the other half. Frames can be 1, 3, or 5 slots long.

Each frame is transmitted over a logical channel, called a link, between the master and a slave. Two kinds of links exist. The fist is the ACL (Asynchronous Connection Less) link, which is used for packet–switched data available at irregular intervals. These data come from the L2CAP layer on the sending side and are delivered to the L2CAP layer on the receiving side. ACL traffic is delivered on a best–efforts basis. No guarantees are given. Frames can be lost and may have to be retransmitted. A slave may have only one ACL link to its master.

The other is the SCO (Synchronous Connection Oriented) link, for real time data, such as telephone connections. This type of channel is allocated a fixed slot in each direction. Due to the time–critical nature of SCO links, frames sent over them are never retransmitted. Instead, forward error correction can be used to provide high reliability. A slave may have up to three SCO links with its master. Each SCO link can transmit one 64,000 bps PCM audio channel.

The L2CAP layer has three major functions. First, it accepts packets of up to 64 KB from the upper layers and breaks them into frames for transmission. At the far end, the frames are reassembled into packets again.

Second, it handles the multiplexing and demultiplexing of multiple packet sources.
Third, L2CAP handles the quality of service requirements, both when links are established and during normal operation.

There are several frame formats, the most important of which is shown in figure below. It begins with an access code that usually identifies the master so that slaves within radio range of two masters can tell which traffic is for them. Next comes a 54–bit header containing typical MAC sub layer fields. Then comes the data field, of up to 2744 bits (for a five – slot transmission). For a single time slot, the format is the same except that the data field is 240 bits.

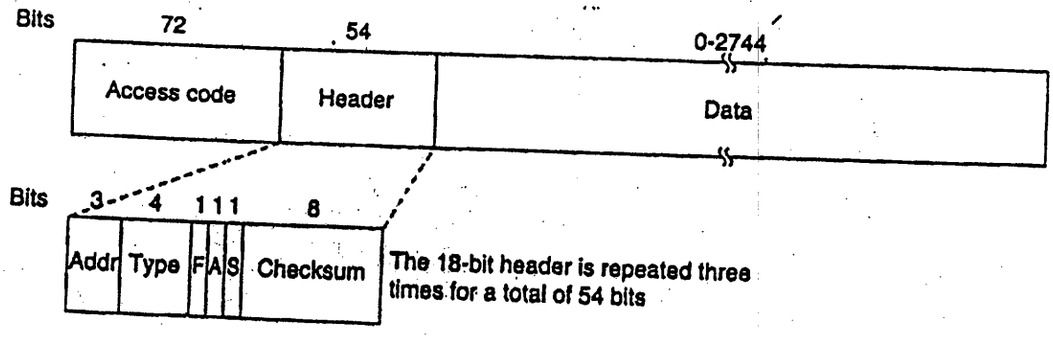


Fig. A typical Bluetooth data frame

The address field identifies which of the eight active devices the frame is intended for. The type field identifies the frame type (ACL, SCO, poll, or null), the type of error correction used in the data field, and how many slots long the frame is. The Flow bit is asserted by a slave when its buffer is full and cannot receive any more data.

The acknowledgement bit is used to piggyback an ACK onto a frame. The sequence bit is used to number the frames to detect retransmissions. The protocol is stop–and–wait, so 1 bit is enough. Then comes the 8–bit header Checksum. The entire 18–bit header is repeated three times to form the 54–bit header shown in figure below. On the receiving side, a simple circuit examines all three copies of each bit. If all three are the same, the bit is accepted. If not, the majority opinion wins. Thus, 54 bits of transmission capacity are used to send 10 bits of header.

Major Issues dealt by Data Link Layer :

Framing :

Data link layer is responsible to detect and if necessary correct errors. For this purpose DLL breaks the bit streams into discrete frames and compute the checksum for each frame.

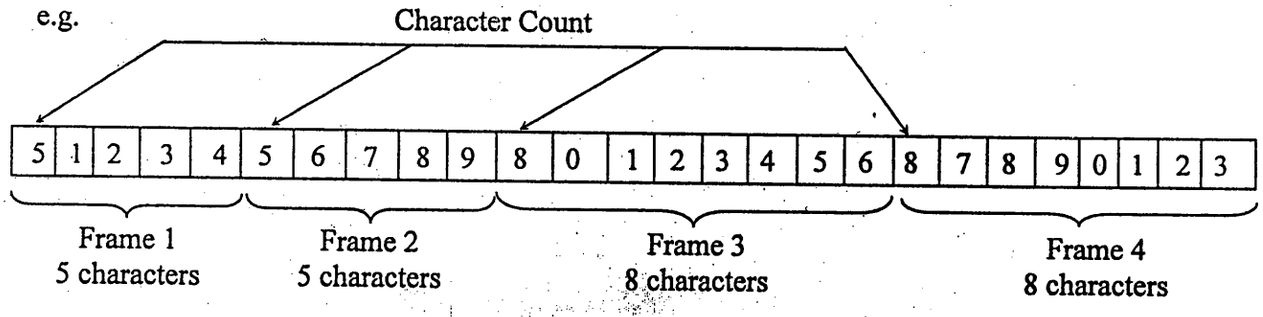
Breaking bit streams into frames required the need for identifying the start and end of the frame. The various methods used for framing are :

1. Character Count :

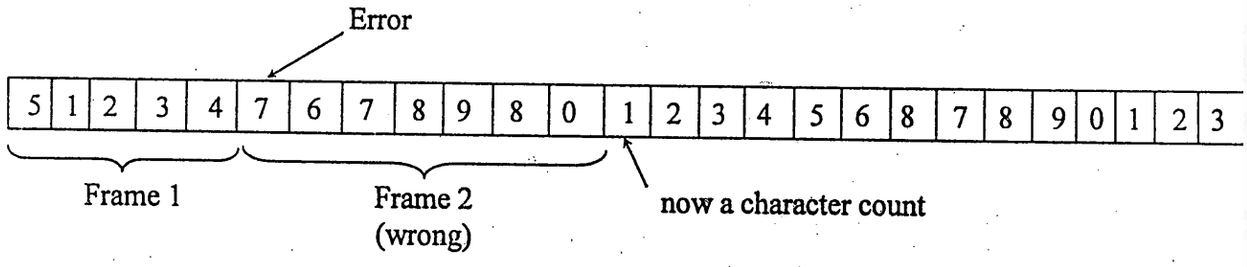
A field in the header specifies the number of characters in the frame.

When the data link layer at the destination sees the character count, it knows how many character to follow and hence where the end of frame is.

e.g.



(a) A character stream without errors



(b) A character stream with one error

The trouble with this algorithm is that the count can be garbled by a transmission error.

2. Character Stuffing :

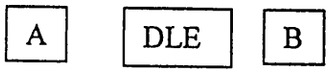
Each frame starts with an ASCII character sequence DLE STX and end with the sequence DLE ETX (DLE) is Data Link Escape, STX is Start of Text, ETX is End of Text.

A serious problem occurs when the characters DLE STX or DLE ETX occur in the data.

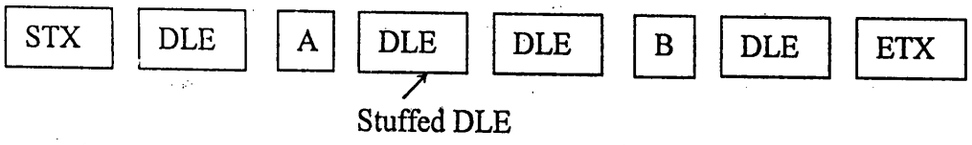
To solve this problem the sender's DLL inserts an ASCII DLE character first before each accidental DLE character in data.

The DLL on the receiving end removes the DLE before the data is given to the network layer. This technique is called character stuffing.

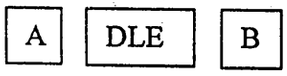
e.g.



(a) Data sent by network layer



(b) Data after being character stuffed by the DLL



(c) Data passed to the network layer on the receiving side

A major disadvantage is that this method is closely tied to 8 bit characters and the ASCII character code in particular.

3. Bit Stuffing :

Each frame begins and ends with a special pattern, 01111110 called the flag byte.

Whenever the sender's DLL encounters five consecutive 1's in the data, it automatically stuffs a 0 bit into the outgoing bit stream.

When the receiver sees five consecutive incoming 1 bits, followed by a 0 bit, it automatically destuffs a zero bit. This process is called bit stuffing.

e.g. 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

(a) The original data

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

Stuffed bits

(b) The data as they appear on the line

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

(c) The data as they are stored in the receiver's memory after destuffing

4. Physical Layer Coding Violations :

This framing method is applicable to networks in which the encoding on the physical medium contains some redundancy.

e.g. Some LAN's encode 1 bit of data using 2 physical bits 1 bit is a high low pair, 0 bit is a low high pair.

The combination high–high and low–low are not used for data and hence can be used to indicate frame boundaries.

This use of invalid physical codes is a part of 802.2 standards.

Error Detection and Correction :

Polynomial code/ Cyclic Redundancy code.

'm' is the message to be transferred having 'k' bits.
'p' is the pattern (polynomial) having 'n + 1' bits

The actual message that is transferred (T) has 'k + n' bits.
Message is constructed by using

$$T = 2^n . m + \text{Rem}\left(\frac{m \times 2^n}{p}\right)$$

Example: m = 1 0 1 0 0 0 1 1 0 1 (10 bits)
p = 1 1 0 1 0 1 (6 bits)

Calculate the frame check sequence (FCS) and also message T that is actually transmitted.

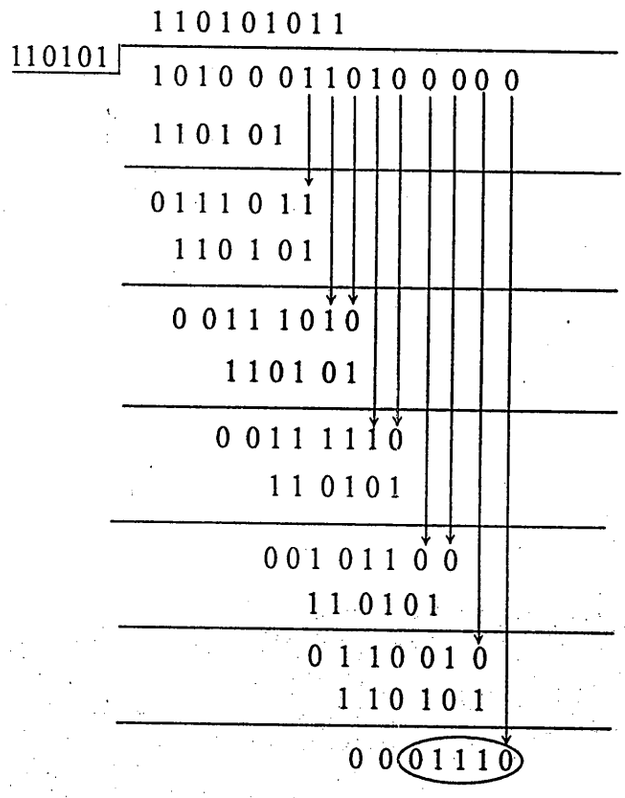
Soln: m = 1 0 1 0 0 0 1 1 0 1 ....10 bits (k)
p = 1 1 0 1 0 1 ....6 bits (n + 1)

$2^5 . m$ = 1 0 1 0 0 0 1 1 0 1 0 0 0 0 0 (i.e. append 5 zeros)

Division uses modulo –2 arithmetic (EX–OR)

$$\text{Rem}\left(\frac{m \times 2^n}{p}\right) = \text{Rem}\left(\frac{2^5 . m}{p}\right)$$

Remainder is given by



Maximum no. of bits in the remainder = 5

$R = 0\,1\,1\,1\,0$

$$T = 2^n . m + \text{Rem}\left(\frac{2^n . m}{p}\right)$$

$T = 1\,0\,1\,0\,0\,0\,0\,1\,1\,0\,1\,0\,0\,0\,0\,0 + 0\,1\,1\,1\,0$

$T = 1\,0\,1\,0\,0\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,0$

Related Questions :

1. What is meant by bit stuffing and character stuffing? Why are they used ?
2. Explain with suitable examples, the physical layer coding violation framing technique.
3. Write short notes on framing methods.
4. For message frame 1101011011 and $G(x) = x^4 + x + 1$, Show transmitted frame and draw Manchester encoding for 100001101111
5. What is the remainder obtained by dividing $x^7 + x^5 + 1$ by generator polynomial $x^3 + 1$
6. What is CRC?
   Evaluate the message using CRC–16 " 1110001001111001101"

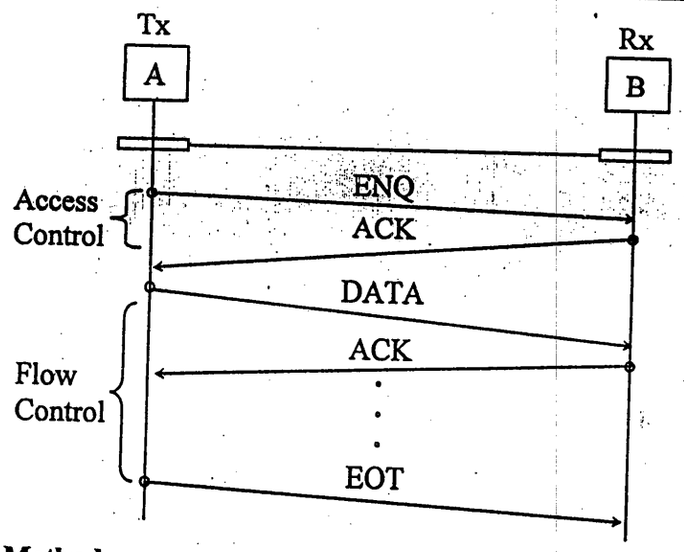
Access Control :

- Access control methods manage establishment of links.
- Right of a particular device to transmit is given by access control methods.

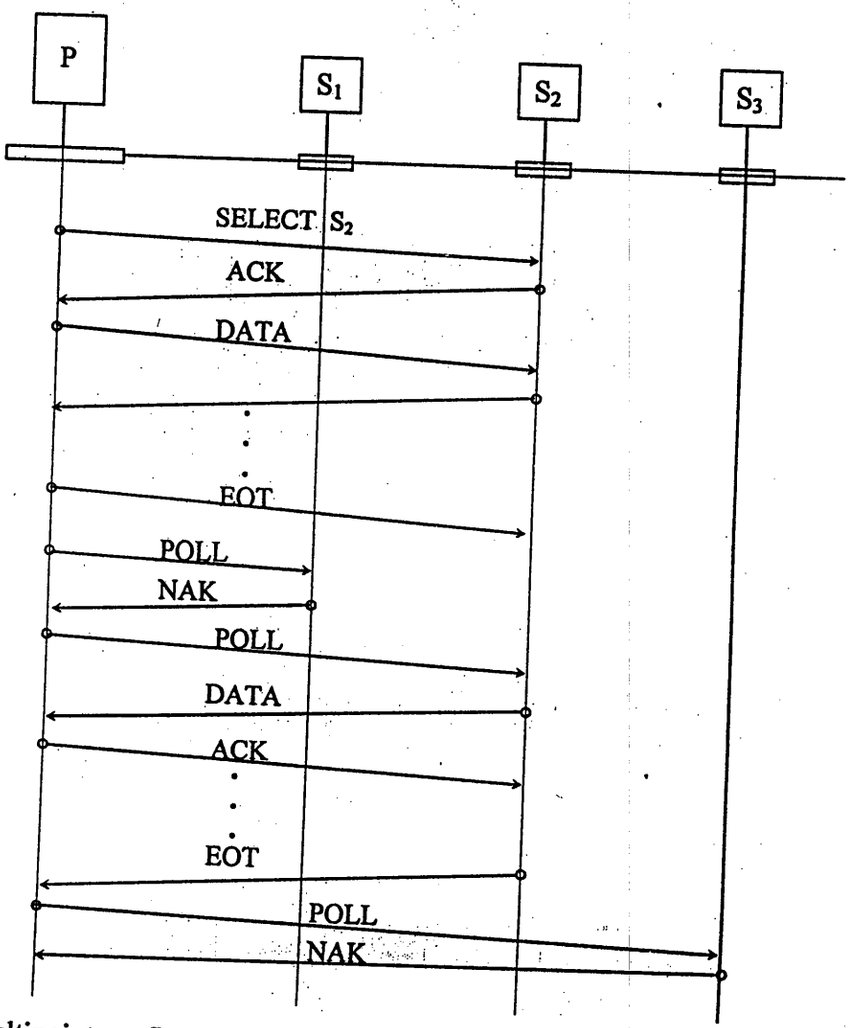
The two access control methods are :

1. ENQ –ACK method (Enquiry/ Acknowledgement)

- Used in case of point to point configurations.
- Used for dedicated path.
- 'A' sends an ENQ frame if it wants to initiate data transfer. If 'B' is not ready it sends a NAK else sends ACK.
- If 'B' is not ready or ACK is lost then 'A' will send ENQ frame again. This process repeats 3 times and then it will disconnect if no ACK and then try after sometime.



2. POLL/SELECT Method :



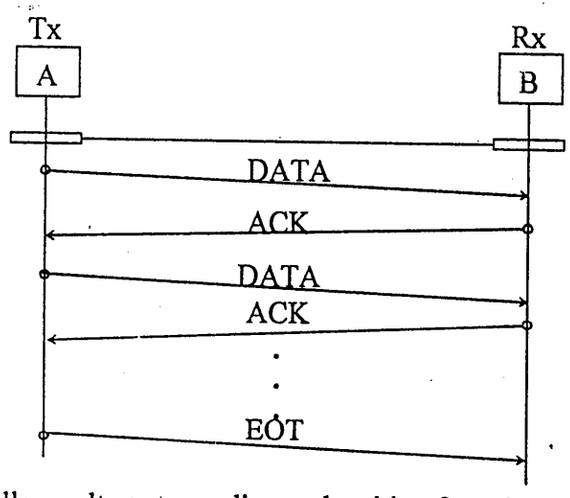
- Used with multipoint configurations i.e. used in a system where one device works as primary and other as secondary.
- PRIMARY is always initiator of the session. Primary device controls the link and determines which device is allowed to transmit at a given time.
- Whenever multipoint link consists of primary device and multiple secondary devices using a single transmission line all exchanges must be made through the primary device even if ultimate destination device is secondary .
- SELECT : Transmission of data from primary to secondary.
  POLL : Transmission of data from secondary to primary.
  POLLING is done by PRIMARY in a sequence.
- Data transmission in POLL mode can be terminated by either 'EOT' from secondary or 'TIME'S UP' by primary which depends on protocol and length of message.

Flow Control :

Flow control methods are basically set of procedures that tell the sender how much data it can transmit before it must wait for an acknowledgement from the receiver.

The two flow control methods are :

1. STOP and WAIT Method :



Stop and Wait method allows alternate sending and waiting for acknowledgement until EOT.

Advantage :

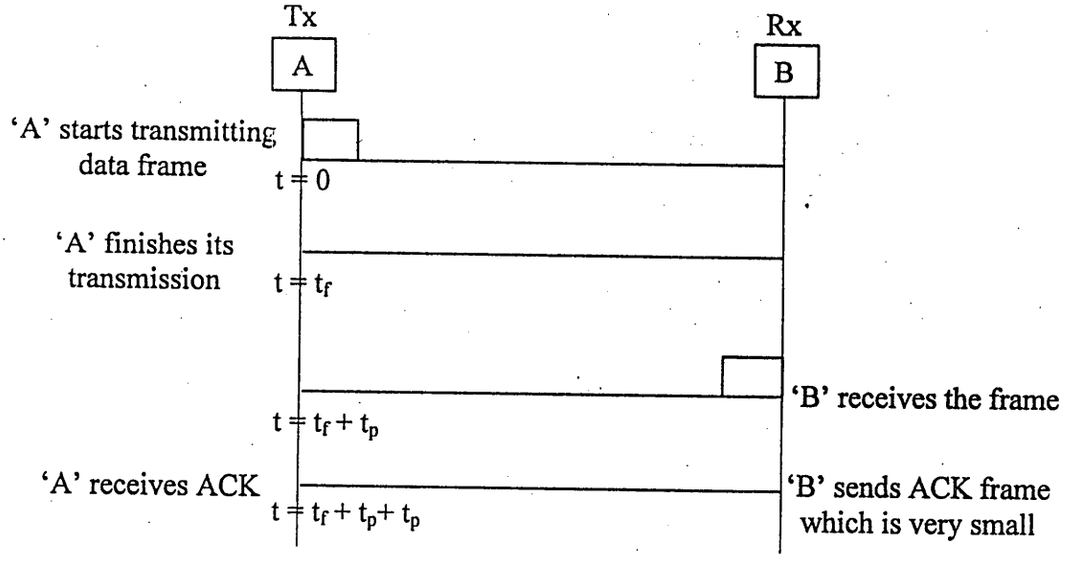
- *Simplicity* : Since each frame is checked and acknowledged before next frame is sent, it is simple.

Disadvantage :

- *Inefficiency* : Each frame is alone on the wire and hence stop and wait is slow.

If distance between devices is long time spend waiting for ACK's between each frame adds to frame transmission.

Calculation of Efficiency :



$$\text{Channel utilization} = \frac{t_f}{t_f + 2t_p}$$

$$= \frac{1}{1 + 2t_p / t_f}$$

Let $A = t_p / t_f$

$$\therefore \quad u = \frac{1}{1 + 2A}$$

$$\text{Efficiency, } \eta = \frac{1}{1+2A} \times 100\,\%$$

$$u = \frac{1}{1+2A}$$

$\because$ μ increases implies A decreases

$$A = \frac{t_p}{t_f}$$

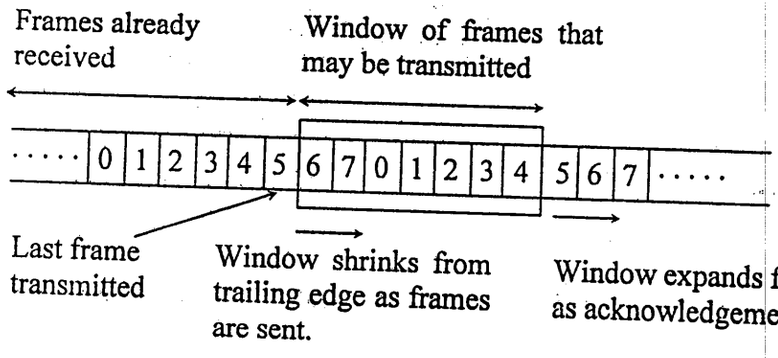
$\because$ A decreases implies t_f increases.

Frame transmission time t_f, can be increased by increasing frame size.

2. Sliding Window Method :

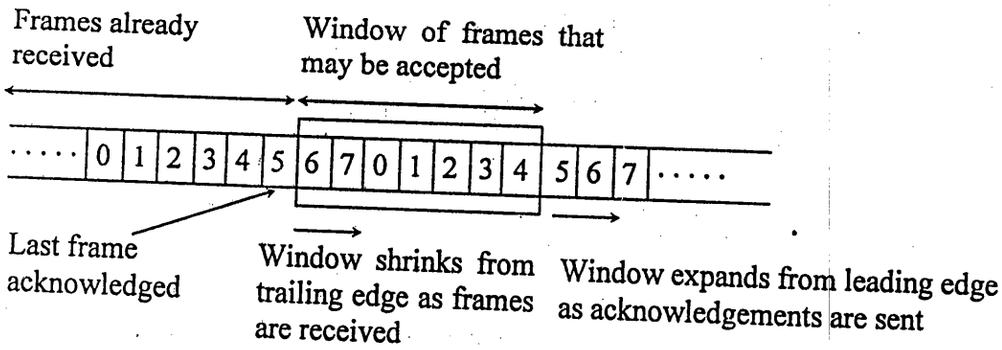
- In sliding window method, sender can transmit several frames without waiting for an acknowledgement.
- To keep track of each frame, identification scheme is based on size of the window.
- The frames are numbered modulo–n, which means they are numbered from 0 to n – 1. If n = 8 then frames are numbered from 0 to 7. Maximum window size = n – 1 i.e. 7.

- ***Sender's Window :***

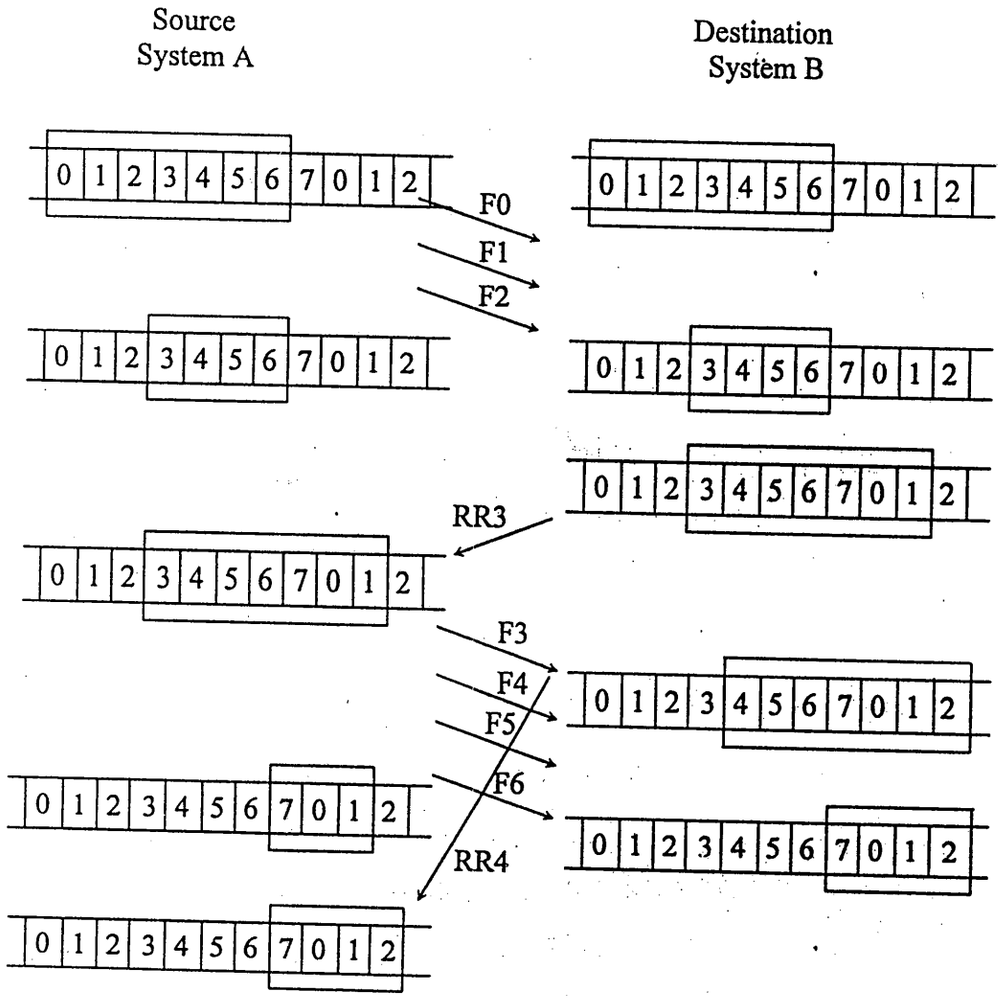


- When frames are transmitted the left boundary moves inward and hence window shrinks.
- When ACK arrives the right boundary moves outward and hence window expands to allow number of few frames equal to number of frames expanded.

- ***Receiver's Window :***



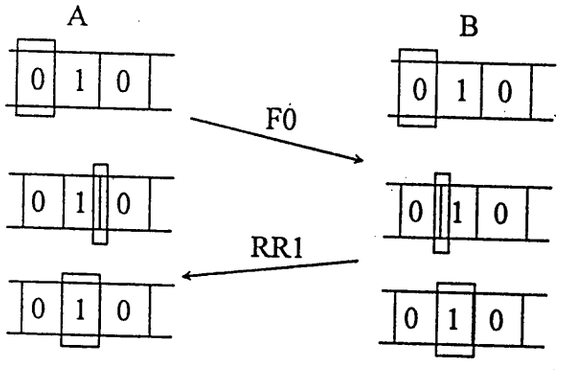
- When new frames come in, the left boundary moves inward and hence window shrinks.
- When the receiver acknowledges a frame, the right boundary moves outward and hence window expands.
- When sizes of both the sender and receiver are same.



RR – Receive Ready
RNR – Receive not ready
RNR 5 means I have received all frames upto no. 4 but I am unable to accept any more.

One bit Sliding Window Protocol :

- One bit sliding protocol is a sliding window protocol with a maximum window size of 1.
- Such a protocol uses stop–and–wait, since the sender transmit a frame and waits for an acknowledgement before sending the next one.



Error Control :

- Error control refers to the mechanism to detect and correct errors.
- There is a possibility of 2 types of errors :
  1. *Lost Frames* : A frame fails to arrive at the other side
  2. *Damaged Frames* : A recognizable frame does arrive but some of the bits are in error.

Some Ingredients for Error Control :

1. *Error Detection* : Using CRC
2. *Positive Acknowledgement* :
   The destination returns a positive acknowledgement to successfully received, error free frames.

3. *Retransmission after time out*
The source retransmits a frame that has not been acknowledged after a predetermined amount of time.

• All these methods are referred to as Automatic Repeat Request (ARQ)

1. Stop–and–wait ARQ :

- Stop–and–wait ARQ is based on stop–and–wait flow–control technique.
- The source station transmits a single frame and then must await an acknowledgement.
- The frame that arrives at the destination could be damaged.

The source station is equipped with a timer. After transmitting the frame, the source station waits for an acknowledgment.

If no acknowledgement is received by the time, the timer expires, then the same frame is sent again.

- The second sort of error is damaged acknowledgement. This works same as above case. ACK is not received, timer expires and data is retransmitted which is duplicate data and is discarded by the receiver.

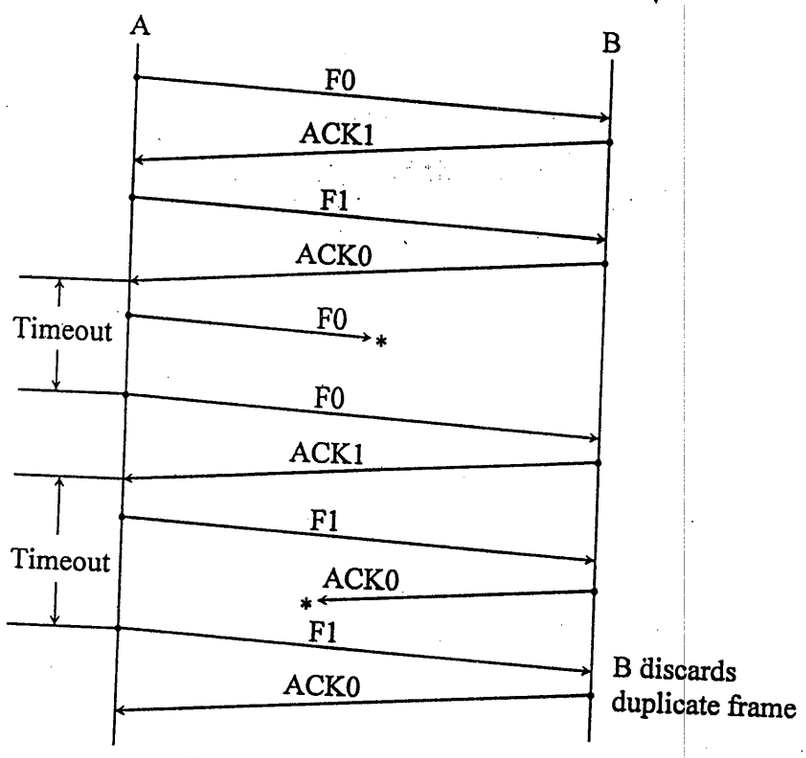


Fig. Stop–and–Wait ARQ

2. Go–back–n–ARQ :

The Go–back–n–ARQ technique takes into account the following contingencies :

(a) *Damaged Data Frame* :

(i) 'A' transmits frame i, B detects an error and has previously successfully received frame (i –1) .B sends REJ i, indicating frame i has been rejected.

(ii) Frame i is lost in transmit. 'A' subsequently sends frame (i + 1). 'B' receives frame (i + 1) out of order and sends REJ i.
'A' must transmit frame i and all next.

(iii)Frame i is lost in transit and 'A' does not soon send additional frames.
'B' receives nothing and returns neither RR nor an REJ.

When A's timer expires, it transmits an RR frame that includes a bit known as the p bit which is set to 1.

'B' interprets the RR frame with a p bit of 1 as a command that must be acknowledged by sending an RR indicating the next frame that it expects.

When 'A' receives the RR, it retransmits frame i.

(b) *Damaged RR* :

(i) 'B' receives frame i and sends RR (i + 1) which is lost in transit. Next RR arrives before 'A's timer expires.

(ii)If 'A' timer expires, it transmits RR command.

(c) *Damaged REJ* :

(i) Frame i is lost in transit and 'A' does not soon send additional frames.
'B' receives nothing and returns neither RR nor an REJ.

When A's timer expires, it transmits an RR frame that include a bit known as the p bit which is set to 1.

'B' interprets the RR frame with a p bit of 1 as a command that must be acknowledged by sending an RR indicating the next frame that it expects.

When 'A' receives the RR, it retransmits frame i.

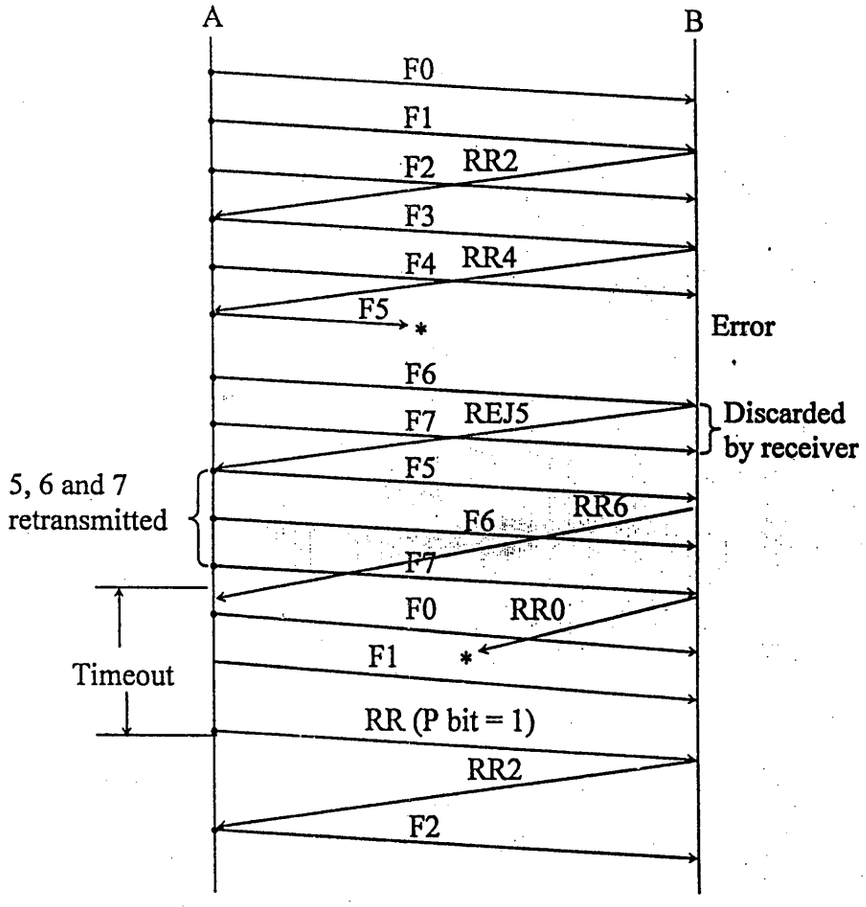


Fig. Go–back–n– ARQ

3. Selective – Reject – ARQ :

- With Selective Reject ARQ, the study frames retransmitted are those that receive a negative acknowledgement in this case called SREJ.
- It is more efficient than Go–back–n because it minimizes the amount of retransmission.
- The receiver has to maintain a buffer large enough to save post–SREJ frames until the frame in error is retransmitted, and it must contain logic for reinserting that frame in the proper sequence.

PROTOCOL PERFORMANCE :

1. Stop and Wait Method :

$$u = \frac{t_f}{t_f + 2t_p} = \frac{1}{1 + 2t_p / t_f} = \frac{1}{1 + 2A}$$

t_f – single frame transmission time

t_p – total time the line is engaged in transmission of single frame.

2. Sliding Window Protocol :

There are two possibilities :

a. Sender receives an ACK before it exhausts the window.

window size = ω

i.e. $\omega \cdot t_f >= t_f + 2t_p$

b. Sender exhausts the window before it receives an ACK.

$\omega \cdot t_f < t_f + 2t_p$

$$\therefore \quad u = \frac{\omega \cdot t_f}{t_f + 2t_p}$$

Utilization is given by,

$$u = 1 \qquad \omega \geq 2a + 1$$

$$= \frac{\omega}{2a+1} \qquad \omega < 2a + 1$$

High Level Data Link Control Protocol (HDLC)

HDLC is the most important data link control protocol.

Basic Characteristics:

To satisfy a variety of applications, HDLC defined

- Three types of stations
- Two link configurations
- Three data transfer modes of operation

Types of Stations :

Primary Station	Has the responsibility for controlling the operation of the link. Frames issued by the primary are called commands.
Secondary Station	Operates under the control of the primary station. Frames issued by a secondary are called responses. The primary maintains a separate logical link with each secondary station on the line
Combined Station	Combines the features of primary and secondary. A combined station may issue both commands and responses.

Two Link Configurations :

Unbalanced Configuration	Consists of one primary and one or more secondary and supports both full-duplex and half-duplex transmission.
Balanced Configuration	Consists of two combined stations and supports both full-duplex and half-duplex transmission.

Three Data Transfer Modes :

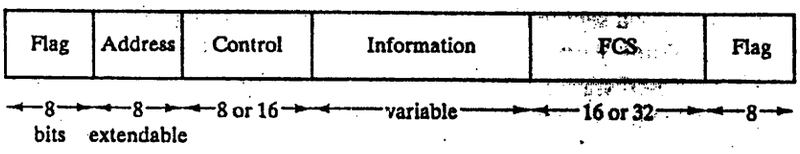
Normal Response Mode (NRM)	Used with an unbalanced configuration. The primary may initiate data transfer to a secondary, but a secondary may only transmit data in response to a command from the primary.
Asynchronous Balanced Mode (ABM)	Used with a balanced configuration. Either combined station may initiate transmission without receiving permission from the other combined station.
Asynchronous Response Mode (ARM)	Used with an unbalanced configuration. The secondary may initiate transmission without explicit permission of the primary. The primary still retains responsibility for the line, including initialization, error recovery and logical disconnection.

Frame Structure

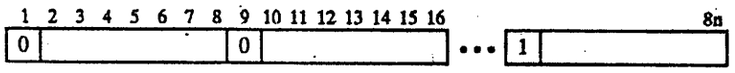
HDLC uses synchronous transmission. All transmission are in the form of frames and a single frame format suffices for all types of data and control exchanges.

Header : The flag, address and control fields that precede the information field.

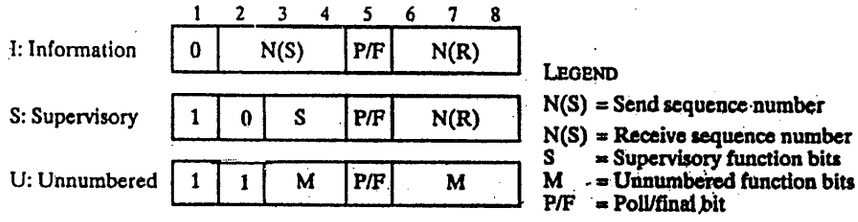
Trailer : The FCS and flag fields following the data field.



(a) Frame format



(b) Extended address field



(c) 8-bit control field format

HDLC Frame Structure

Flag Fields :

Flag fields delimit the frame at both ends with the unique pattern 01111110. The data is bit stuffed at the transmitter and unstuffed at the receiver.

Address Fields :

The address fields identify the secondary station that transmitted or is to receive the frame.

Control Fields :

HDLC defines three types of frames, each with a different control field format.

Information frames (I-frames)	They carry the data to be transmitted for the user. Additionally flow and error control data using the ARQ mechanism are piggybacked on an information frame.
Supervisory frames (S-frames)	They provide the ARQ mechanism when piggybacking is not used.
Unnumbered frames (U-frames)	They provide supplemental link control functions.

Frame Check Sequence Field :

FCS is an error-detecting code calculated from the remaining bits of the flags, exclusive of flags and uses 16-bit CRC

Operation:

The operation of HDLC involves three phases:

Initialization :

Initialization may be requested by either side. The commands serves three purposes:

1) It signals the other side that initialization is requested.
2) It specifies which of the three modes (NRM, ABM, ARM) is requested.
3) It specifies whether 3 – or 7 bit sequence numbers are to be used.

If the other sides accepts this request, then the HDLC module on that end transmits an unnumbered acknowledged (UA) frame back to the initiating side. If the request is rejected, then a disconnected mode (DM) frame is sent.

Data Transfer :

When the initialization had been requested and accepted, then a logical connection is established. Both sides may begin to send user data in I-frames, starting with sequence number 0. The N(S) and N(R) fields of the I-frame are sequence numbers that support flow control and error control.

Disconnect :

Either HDLC module can initiate a disconnect by issuing a disconnect (DISC) frame. The other side reply's with UA.

Related Questions :

1. Write short note on sliding window protocol.
2. What is sliding window protocol? What determines the sizes of the transmitting and receiving windows at any time?
3. Write short note on protocol using Go–back–N.
4. In a network that has maximum packet size of 129 bytes, a maximum lifetime of 30 sec, and a 8 bit packet sequence number, what is the maximum data rate per connection?
5. A channel has a bit rate of 20 kbps and a propagation delay of 100 msec. For what sizes does stop and wait give an efficiency of atleast 50%.

Soln : Data rate = 2 kbps

$t_p = 100$ m sec

$\eta = 50\% = 0.5$

Frame size = ?

For stop and wait method,

$$\eta = \frac{t_f}{t_f + 2t_p} \times 100$$

$$\eta = \frac{1}{1+2A} \times 100, \quad A = \frac{t_p}{t_f}$$

Let frame size = L bits

20000 bits are transmitted in 1 sec

L bits are transmitted in t_f sec

where L = frame size, t_f = frame transmission time

$$t_f = \frac{L}{20000}$$

$$\therefore \quad 50 = \frac{1}{1+2\left(\frac{100\times10^{-3}}{L/20000}\right)} \times 100$$

$$\therefore \quad 0.5 = \frac{1}{1+\frac{4000}{L}}$$

$$\therefore \quad 0.5 + \frac{2000}{L} = 1$$

$$\therefore \quad \frac{2000}{L} = 0.5$$

$$\therefore \quad L = 4000 \text{ bits}$$

For efficiency to be atleast 50%, frame size should be greater than or equal to L i.e. 4000 bits i.e. $L \geq 4000$ bits.

6. What is sliding window protocol? Give the performance analysis of sliding window protocol with respect to error–free and error–prone channels.

Protocol Performance :

1. *Stop and Wait Method* :

- $u = \dfrac{t_f}{t_f + 2t_p} = \dfrac{1}{1 + 2t_p / t_f} = \dfrac{1}{1+2A}$

  t_f – single frame transmission time

  t_p – total time the line is engaged in transmission of single frame

  $u = \dfrac{t_f}{t_f + 2t_p}$ (without errors)

- With errors,

  $u = \dfrac{tr}{N_r(t_f + 2t_p)} = \dfrac{1}{N_r(1+2A)}$

  where N_r = expected number of transmissions of a frame

- Let P be the probability that a single frame is in error.

  Assuming ACK and NAK are never in error, the probability that will take exactly 'i' attempts to transmit a frame successfully is

  $P^{i-1}(1-P)$

  Thus, $N_r = \sum_{i=1}^{\infty} i\, P^{i-1}(1-P)$

  $\left\{ \sum_{i=0}^{\infty} r^i = \sum_{i=1}^{\infty} r^{i-1} = \dfrac{1}{1-r} \right.$

  $\left. \sum_{i=1}^{\infty} i\, r^{i-1} = \dfrac{1}{(1-r)^2} \right\}$

  $\therefore \quad N_r = (1-P)\sum_{i=1}^{\infty} i\, P^{i-1}$

  $\therefore \quad N_r = (1-P) * \dfrac{1}{(1-P)^2}$

  $\therefore \quad N_r = \dfrac{1}{(1-P)}$

  Thus $u = \dfrac{1}{N_r(1+2A)}$

  $\therefore \quad u = \dfrac{1-P}{1+2A}$

2. *Sliding Window Protocol :*

   There are two possibilities :

i) Sender receives an ACK before it exhausts the window. (window size = ω)

   i.e. $\omega \cdot t_f \geq t_f + 2t_p$

   i.e. $\omega \geq 1 + 2A$

ii) Sender exhausts the window before it receives an ACK.

   $\omega \cdot t_f < t_f + 2t_p$

$\therefore \quad u = \dfrac{\omega \cdot t_f}{t_f + 2t_p}$

- For error free operation,

$u = 1 \quad ; \omega \geq 2a + 1$

$= \frac{\omega}{2A+1} \quad ; \omega < 2A + 1$

- **Selective Reject ARQ :**

With errors in selective reject ARQ, we can use the same reasoning applied to stop–and–wait ARQ i.e error free equations must be divided by N_r and $N_r = \frac{1}{1-p}$

$\therefore \quad \mu = 1 - P \quad ; \omega \geq 2A + 1$

$= \frac{\omega(1-P)}{2A+1} \quad ; \omega < 2A + 1$

- **Go–back–n ARQ :**

With errors in go–back–n ARQ,

N_r = E[number of transmitted frames to successfully transmit one frame]

$$N_r = \sum_{i=1}^{\infty} f(i)\ P^{i-1}(1-P)$$

where f(i) is the total number of frames transmitted if the original frame is transmitted i times.

$f(i) = 1 + (i-1)k$

$= (1-k) + ik$

Substituting,

$$N_r = (1-k)\sum_{i=1}^{\infty} P^{i-1}(1-P) + k\sum_{i=1}^{\infty} i\,P^{i-1}(1-P)$$

Using,

(1) $$\sum_{i=0}^{\infty} r^i = \sum_{i=1}^{\infty} r^{i-1} = \frac{1}{1-r}$$

(2) $$\sum_{i=1}^{\infty} i\,r^{i-1} = \frac{1}{(1-r)^2}$$

We get,

$$N_r = (1-k)\frac{(1-P)}{(1-P)} + k\frac{(1-P)}{(1-P)^2}$$

$$N_r = 1 - k + \frac{k}{1-P}$$

$$N_r = \frac{1-P-k+kP+k}{1-P} = \frac{1-P+kP}{1-P}$$

- k is approximately equal to 2A + 1 for $\omega \geq 2A + 1$ and $k = \omega$ for $\omega < 2A + 1$
- For Go–back–N with errors,

$$N_r = \frac{1-P+(2A+1)P}{1-P} \quad ; \omega \geq 2A + 1$$

$$= \frac{1-P+2AP+P}{1-P} = \frac{1+2AP}{1-P}$$

$$N_r = \frac{1+2AP}{1-P}$$

$$N_r = \frac{1-P+\omega P}{1-P} \quad ; \omega < 2A + 1$$

- $\therefore$ Utilization,

$$u = \frac{1-P}{1+2AP} \quad ; \omega \geq 2A + 1$$

$$= \frac{\omega(1-P)}{(2A+1)(1-P+\omega P)} \quad ; \omega < 2A + 1$$

7. A 50kbps satellite channel with 500 msec round trip propagation delay uses Sliding Window protocol sends 1500 bits frame, calculate window size ω?

Soln : Time taken to send 1500 bits frame = t_f

$$t_f = \frac{1500}{\text{Data rate}} = \frac{1500}{50\times10^3} = 30\,\text{msec}$$

$\therefore\ t_f = 30\text{msec}$

- Round robin propagation delay, $2t_p = 500\text{msec} \therefore t_p = 250\,\text{msec}$
- To receive a frame, time required, $t_1 = t_p + t_f$

$$\therefore \quad t_1 = 250+30 = 280$$

$$\therefore \quad t_1 = 280\ \text{msec}$$

- Considering the waiting time and short acknowledgement frames it takes 280 + 250 i.e. t = 530 msec to get back an ACK
- Maximum window size, $\omega = \frac{t_f + 2t_p}{t_f} = \frac{t}{t_f} = \frac{530\,\text{msec}}{30\ \text{msec}}$

$$\omega = 17.6667$$

Always select higher value for window size to increase efficiency.
Hence ω = 18

8. A satellite channel of capacity of b bits/sec, the frame size ℓ bits and round trip propagation time of R sec uses stop–and–wait protocol, what is the channel utilization u?

Soln : Channel capacity = 'b' bits/sec

frame size = 'ℓ' bits

$$2t_p = \text{'R'sec}$$

$$u = ?$$

$$u = \frac{t_f}{t_f + 2t_p}$$

Frame transmission time, $t_f = \frac{\text{frame size}}{\text{Data rate}}$

$$\therefore \quad t_f = \frac{\ell}{b}$$

$$t_p = \frac{R}{2}$$

$$\therefore \quad u = \frac{(\ell/b)}{(\ell/b)+2(R/2)}$$

$$u = \frac{\ell/b}{\ell/b+R}$$

$$u = \frac{\ell}{\ell+bR}$$

9. What is the significance of ACK nos. and SEQ nos. in flow control protocol? Why pipelining is necessary with sliding window protocol?

Soln:

Pipelining :

- The rule requires a sender to wait for an ACK before sending another frame. Because of this rule long transit time, high bandwidth and short frame length, low efficiency problems occur.
- If we relax this restriction much better efficiency can be achieved. The sender may be allowed be transmit upto 'ω' frames before blocking, instead of just 1.
- With an appropriate choice of ω, the sender will be able to continuously transmit frames for a time equal to the round–trip transit time without filling up the window.

This technique is known as pipelining.

To increase the efficiency of the channel, lower transient time, etc. pipelining is used.

NOTE : SLIDING WINDOW PROTOCOL IS SOMETIMES CALLED PIPELINING PROTOCOL.

10. Consider an error free 64 kbps satellite channel used to send 512 byte data frames in one direction, with very short ACK coming back the other way. What is the maximum throughput for window sizes 1, 7, 15 and 127.

Soln: Data rate = 64 kbps

Frame size = 512 bytes = 512×8

$t_p = 270$ msec ($2t_p$ is assumed as 540 msec for satellite channel)

- 64 k bits can be transmitted in 1 sec

  512×8 bits can be transmitted in t_f sec

  $\therefore \quad t_f = \frac{512 \times 8}{64 \times 10^3} = 64 \text{ msec}$

- For Sliding Window method,

  Sender can receive ACK after $t_f + 2t_p$ time at the earliest.

  i.e. $t = t_f + 2t_p = 64 \text{ msec} + 2(270) \text{ msec}$

  $t = 604$ msec

  Window Size, $\omega = \frac{t}{t_f} = \frac{604}{64} = 9.4$

- Select higher window size to increase utilization.

  Hence $\omega = 10$

  $u = 1 \quad ; \omega \geq 1 + 2A$

  $= \frac{\omega}{1 + 2A} \quad ; \omega < 1 + 2A$

- Data throughput $= \frac{\omega \times \text{frame size}}{t_f + 2t_p} \leq$ channel capacity

- If $\omega \geq$ maximum window size then

  Data throughput = channel capacity.

  (a) $\omega = 1$

  Max. throughput $= \frac{512 \times 8}{604} = \frac{4096 \text{ bits}}{604 \text{ ms}} = 6781 \text{ bits/sec}$

  (b) $\omega = 7$

  Max. throughput $= \frac{7 \times 512 \times 8}{604} = 47470 \text{ bits/sec}$

  (c) $\omega = 15$

  $\because \omega > 10$ i.e > maximum windows size,

  $\therefore$ Max. throughput = 64 kbps

  (d) $\omega = 127$

  $\because \omega >$ maximum windows size, i.e. > 10

  $\therefore$ Max. throughput = 64 kbps

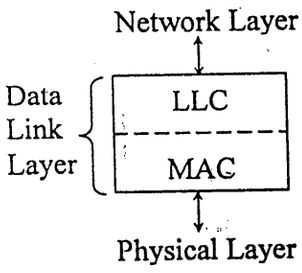
11. Frames of 1000 bits are sent over 1 Mbps satellite channel. ACK's are always piggybacked onto data frames. Headers are very short. Three bit sequence numbers are used. What is maximum channel utilization for stop–and–wait protocol as well as for pipelining protocol?

12. Explain DLL flow control protocol

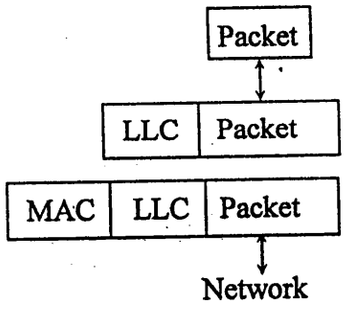
13. Draw and explain HDLC protocol

14. What is the role of LLC?

Soln : Logical Link Control (LLC) hides the difference between the various kinds of 802 networks by providing a single format and interface to the network layer.



(a) Position of LLC



(b) Protocol Formats

- Usage of LLC :

  The network layer on sending machine passes the packet to LLC where an LLC header is added which contains sequence and acknowledgement number. The resulting structure is then inserted in the payload field of 802.X frame and transmitted. At the receiver, the reverse process takes place.

- LLC provides three service options: unreliable datagram service, acknowledged datagram service and reliable connection–oriented service.

15. Consider a half duplex point to point link using stop and wait scheme.
    a. What is the effect on the utilization of increased number of frames for a constant message size?
    b. What is the effect on line utilization of increasing the frame size?

Soln: $\mu = \frac{t_f}{t_f + 2t_p} = \frac{1}{1+2A}$; $A = \frac{t_p}{t_f}$

(a) By increasing number of frames; frame size reduces and hence t_f decreases, therefore A increases, μ decreases.

$\therefore$ Channel utilization decreases,

i.e. $t_f \downarrow$; $A = \frac{t_p}{t_f} \uparrow$; $u \downarrow$

(b) By increasing frame size; no. of frames will reduce.

$\therefore$ Frame transmission time, $t_f \uparrow$

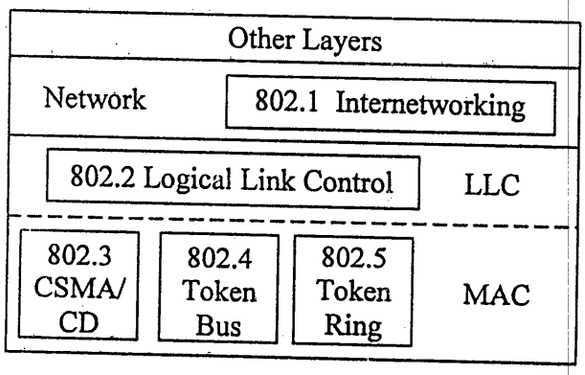
i.e. $t_f \uparrow$; $A = \frac{t_p}{t_f} \downarrow$; $u = \frac{1}{1+2A} \uparrow$

$\therefore$ Channel utilization increases.

16. Two stations communicate via 1 Mbps satellite link with a propagation delay of 270 ms. The satellite serves merely to transmit data received from one station to another with negotiable switching delay. Using HDLC frames of 1024 bits with 3 bits sequence numbers, what is the maximum possible data throughput?

❑❑❑❑❑❑

PROJECT 802.2



Medium Access Control :

- MAC layer provides access to shared media.
- It contains synchronization, flag, flow and error control specifications necessary to move information from one place to another, as well as physical address of the next station to receive and route a packet.
- MAC layer functions include :
  a. At transmitter, assemble data into frame with address and error detection field.
  b. At receiver, disassemble frame, perform address recognition and error detection.
  c. Govern access to the LAN transmission media.

Standard MAC techniques :

1. **Round robin :**
   Permission to transmit is forwarded to next device in the form of token.
   e.g. 802.4 – Token bus, 802.5 – Token ring
2. **Reservation :**
   This technique is used for stream traffic (continuous). A station wishing to transmit reserves future slots for an extended period.
   e.g. 802.6 – DQDB used in MAN.
3. **Contention :**
   For bursty traffic contention techniques are used. No control is exercised to determine whose turn it is.
   e.g. 802.3 – CSMA/CD.

MULTIPLE ACCESS PROTOCOLS :

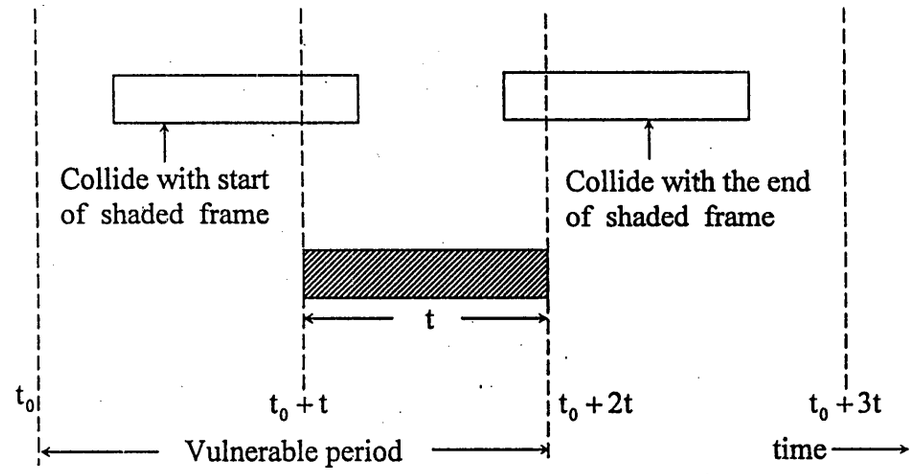
I. ALOHA

- ALOHA used ground based radio broadcasting, the basic idea is applicable to any system in which uncoordinated users are competing for the use of single shared channel.
- There are two versions of ALOHA
  (a) Pure(b) Slotted
  In Pure ALOHA time is not divided into discrete slots which in Slotted ALOHA it is. Pure ALOHA does not require global time synchronization; Slotted ALOHA does.

Pure ALOHA :

- The basic idea is; let users transmit whenever they have data to be sent.
- There will be collisions and the colliding frames will be destroyed.
- With LAN the feedback is immediate but with satellite a delay of 270 msec is required before the sender knows if the transmission was successful.
- If the frame was destroyed, the sender waits for a random amount of time and sends it again.
  Sender waits for random amount of time because if it doesn't then the same frames will collide over and over in lockstep.
- Systems in which multiple users share a common channel in a way that can lead to conflict are called contention systems.

Efficiency :



- Let the "frame time" denote the amount of time needed to transmit the standard, fixed length frame.
- Let S be the average number of new frames generated per frame time.
- If $S > 1$, the user is generating frames at a higher rate than the channel can handle and nearly every frame suffers collision.

  For reasonable throughput $0 < S < 1$
- In addition to new frames, station also generates retransmissions of frames that previously suffered collisions.
- Let G be the average number of attempts (old + new) per frame time.

  Clearly $G \geq S$.
  1. At low load ($S \approx 0$) there will be few collisions and few retransmissions $\therefore G = S$
  2. At high load, $S = GP_0$ where P_0 is the probability that a frame does not suffer collision.
- A frame will not suffer a collision if no other frames are sent within one frame time of its start.
- Let 't' be the time required to send a frame.
- If any other user has generated a frame between time t and $t_0 + t$, the end of the frame will collide with the shaded one.

  Similarly any other frame started between $t_0 + t$ and $t_0 + 2t$ will collide with the end of the shaded one.

  If the frame starts after $t_0 + 2t$ there will be no collision.
- The probability that k frames are generated during a given frame time is given by Poisson distribution

$$P_k = \frac{G^k e^{-G}}{k!}$$

- The probability of zero frame is e^{-G}
- In an interval two frame times long, the average number of frames generated is 2G.
- The probability of no other traffic being initiated i.e. zero frame generated during the entire vulnerable period is thus given by, $P_0 = e^{-2G}$
- With $S = GP_0$ we get $S = Ge^{-2G}$. The maximum throughput occurs at $G = 0.5$

  where $G = 0.5$, $S = 0.5e^{-2(0.5)}$

  $= 0.5e^{-1}$

  $\therefore \quad = 0.184$

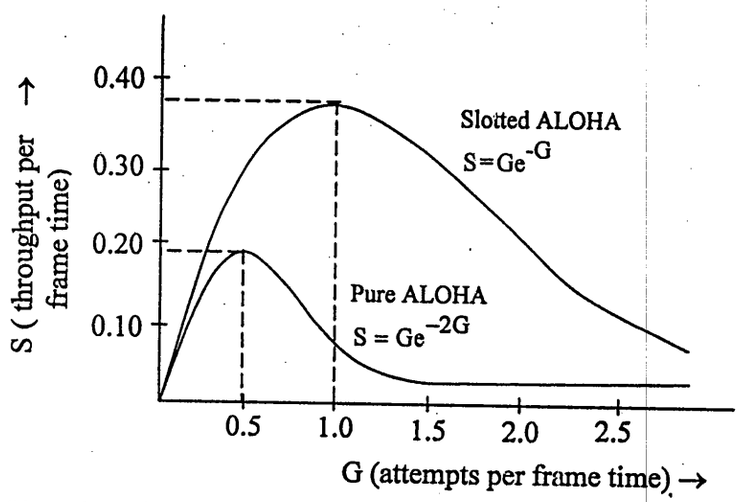
  This means channel initialization is 18.4%.
- With Slotted ALOHA, station is required to wait for the beginning of the next slot.
- The probability of no other traffic during the frame time is thus $P_0 = e^{-G}$
- With $S = GP_0 = Ge^{-G}$

  The maximum throughput occurs at $G = 1$

  $\therefore S = Ge^{-G} = e^{-1} = 0.368$

  $S = 0.368$

  This means channel utilization is 36.8%.



NOTE: (For Slotted ALOHA)

1. Probability that avoids collision = e^{-G}.
2. Probability of a collision = $1-e^{-G}$.
3. Probability of a transmission requiring exactly k attempts i.e. (k –1) collisions followed by one success is,

$$P_k = e^{-G}(1-e^{-G})^{k-1}$$

4. Expected number of transmissions: E

$$E = \sum_{m=1}^{\infty} m P_m$$

$$E = \sum_{m=1}^{\infty} m e^{-G}(1-e^{-G})^{m-1}$$

$$E = e^{G}$$

II. CARRIER SENSE MULTIPLE ACCESS PROTOCOLS:

Protocols in which stations listen for a carrier and act accordingly are called carrier sense protocol.

- Persistent and Non–persistent CSMA.

1–Persistent CSMA:

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

Advantages :

It is still better than ALOHA

Disadvantages :

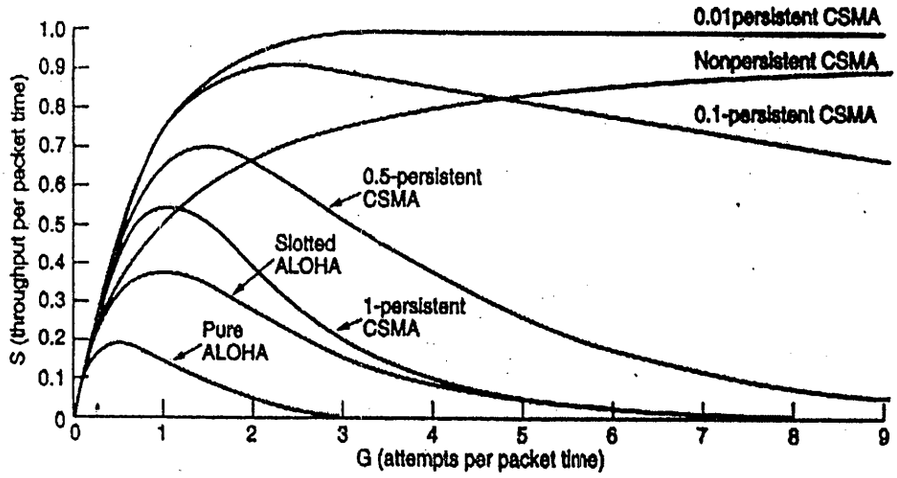
1. Propagation delay has an important effect on the performance of protocol.
   There is a small chance that just after a station begins sending, another station will become ready to send and sense the channel.
   If the first station's signal has not yet reached the second one, the latter will sense an idle channel and will also begin sending, resulting in a collision.
   Propagation delay increases, performance decreases.
2. Even if propagation delay = 0, there will still be collisions.
   If two station become ready in the middle of a third station's transmission, both will wait politely until the transmission ends and then both will begin transmitting exactly simultaneously, resulting in a collision.

Non–persistent CSMA :

- Before sending, a station senses the channel.
- If no one else is sending, a station begins doing so itself.
- However, if the channel is already in use, the station does not continually sense it for the purpose of seizing it immediately upon detecting the end of pervious transmission. Instead, it waits a random period of time and then repeats the algorithm.
- It is better than 1–persistent CSMA.

P–persistent CSMA :

- p–persistent CSMA is used for slotted channels.
- When a station becomes ready to send, it senses the channel. If it is idle, it transmits with a probability p. With a probability q = 1 – p it defers until the next slot.
- If that slot is idle, it either transmits or defers again, with probability p and q.
- This process is repeated until either the frame has been transmitted or another station has begun transmitting.
- If the station initially sense's the channel bus it waits until the next slot and applies the above algorithm.



III. Carrier Sense Multiple Access With Collision Detection (CSMA/CD) :

- An improvement for CSMA is to abort transmissions as soon as they detect a collision.
- Quickly terminating damaged frames saves time and bandwidth. This is called CSMA/CD.

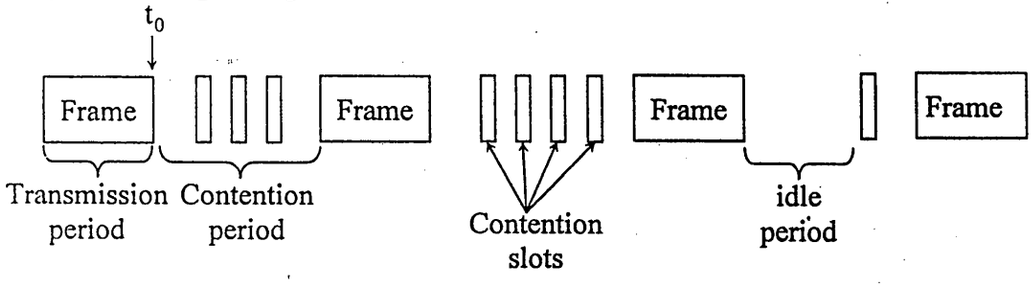


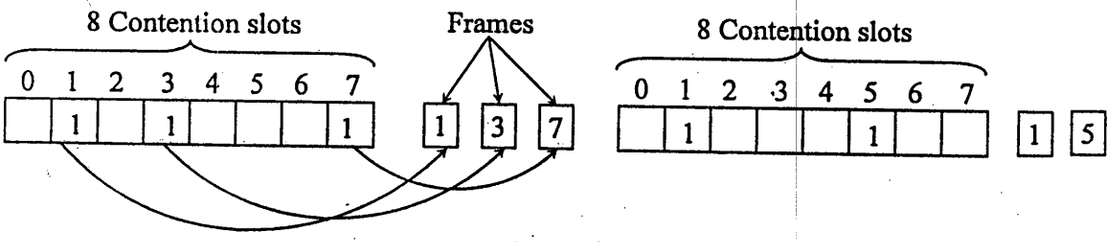
Fig. Conceptual model for CSMA/CD as well as many other LAN protocols

- At the point marked t_0, a station has finished transmitting its frame.
- Any other station having a frame t_0 send may now attempt to do so.
- If two or more stations decide to transmit simultaneously there will be a collision.
- Collision can be detected by looking at the power or pulse width of the received signal and comparing it to the transmitted signal.
- After a station detects a collision, it aborts its transmission, waits for random period of time, and then tries again, assuming that no other station has started transmitting in the mean time.

IV. COLLISION FREE PROTOCOLS :

(i) Bit–map Protocol :

- In Bit–map method each contention period consists of exactly N slots.
- If station 0 has frame to send, it transmits a 1 bit during the zeroth slot. No other station is allowed to transmit during this slot.
- Regardless of what station 0 does, station 1 gets the opportunity to transmit a 1 during slot 1 but only if it has a frame queued.
- In general, station i may announce the fact that it has frame to send by inserting a 1 bit into slot j.
- Protocols like this in which the desire to transmit is broadcast before the actual transmission are called reservation protocols.

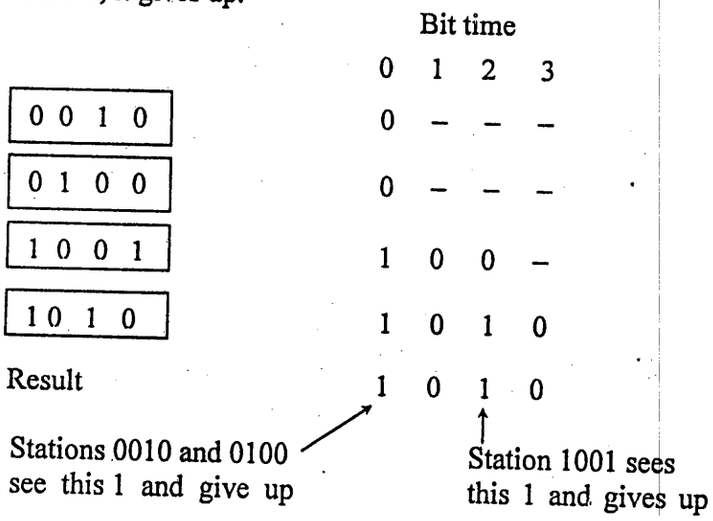


Basic Bit map protocol

(ii) Binary Countdown :

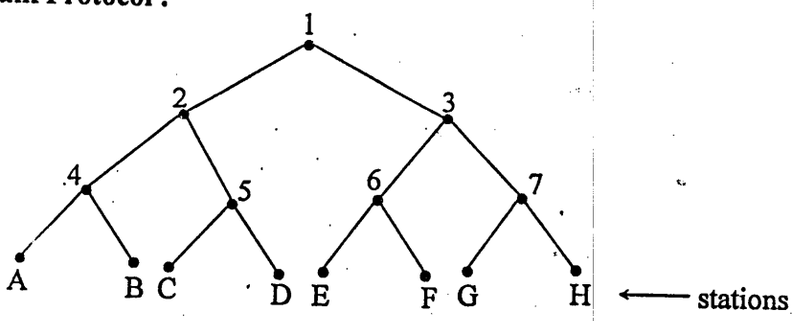
- The problem with bit–map protocol is that the overhead is 1 bit per station.
- Binary station addresses are used.
- A station wanting to use the channel now broadcasts its address as a binary bit string, starting with the higher–order bit.
- The bits in each address position from different stations are BOOLEAN ORed together.
- As soon as a station sees that a higher order bit position that is 0 in its address has been overwritten with a 1; it gives up.

e.g.



V. LIMITED CONTENTION PROTOCOL :

- **Adaptive Tree Walk Protocol :**



- It is convenient to think of stations as the leaves of a binary tree.
- In the first contention slot following the successful frame transmission, slot 0, all the stations are permitted to try to acquire the channel. If one of them does so, fine.

- If there is a collision during slot 1 only those stations falling under node 2 in tree may compete. If one of them acquire the channel, the slot following the frame is reserved for those stations under node 3.
- If two or more stations under node 2 want to transmit, there will be a collision during slot 1, in which case it is node 4's turn during slot 2.
- If a collision occurs during slot 0, the entire tree is searched, depth first, to locate all ready stations.

Related Questions :

1. A group of N stations share 5 kbps ALOHA channel. Each station outputs 1000 bit packet at an average rate of one every 100 sec. What is the maximum value of N?

Soln. : PURE ALOHA channel,

Rate = 5kbps

1000 bits are transmitted in 100 sec

? bits are transmitted in 1 sec

$\therefore$ Each station outputs $\frac{1000}{100} = 10$ bits/sec

No. of stations, N = ?

For PURE ALOHA,

Channel Bandwidth = 18.4%

Usable bandwidth = 5kbps × 18.4 %

= 920 bps

All 'N' stations will output 920 bps

i.e. $10 \times N = 920$ bps

$\therefore \quad N = \frac{920}{10}$

$\therefore$ N = 92 stations.

2. Prove that slotted ALOHA is better than pure ALOHA.
3. Derive the formula for measuring the efficiency of the ALOHA system, explain how the efficiency is increased for slotted ALOHA system.
4. A large population of ALOHA users manages to generate 50 requests/sec. The time is slotted in units of 40msec and chances of collision is 10%.
   (i) What is channel load, G?
   (ii) What is the chance of success on the first attempt?
   (iii) What is the probability of exactly 5 collisions and then a success?
   (iv) What is the expected number of transmission attempts needed?

Soln : No. of request = 50 request/sec

slot time = 40msec

no. of slots = $\frac{1}{40 \times 10^{-3}} = 25$ slots/sec

(i) G = no. of request/slot = $\frac{50}{25} = 2$ req/slot

(ii) Chance of success on first attempt,

$p_0 = e^{-G}$ { $\because$ Slotted ALOHA }

$p_0 = e^{-2}$

$p_0 = 0.1353$

(iii) Probability of exactly 5 collisions and then success i.e. $m - 1 = 5 \quad \therefore m = 6$

$p_m = e^{-G}(1 - e^{-G})^{m-1}$

$\therefore \quad p_m = e^{-2}(1 - e^{-2})^5$

$\therefore \quad p_m = 0.06521$

(iv) Expected number of transmission attempts needed,

$E = e^G$

$E = e^2$

5. A group of N stations share 56 kbps slotted ALOHA channel, each station outputs a 500 bits on an average of once every 1000ms. What is the maximum value of N?

Soln : With slotted ALOHA,

usable B/w = 0.368 × 56 kbps
= 20.608 kbps

Each station requires 500 bits/1000 ms = 50 bps

$$\therefore \quad N = \frac{20608}{50} = 412.16$$

$\therefore$ N = 412 stations.

6. 1 Gbps CSMA/CD LAN is to be designed over 1km cable without repeater. The cable supports signal speed of 200,000 km/sec. What is the minimum frame size that data link layer should consider?

7. Prove that for unslotted ALOHA protocol, $S = Ge^{-2G}$, where symbols have their standard meaning.

8. Write short note on slotted ALOHA.

9. 5000 airline reservation stations are competing for the use of a single slotted ALOHA channel. The average station makes 18 requests per hour. A slot is 125 micro seconds. What is approximate total channel load?

IEEE Standard 802 for LAN's and MAN's

The standards collectively called as IEEE 802, include CSMA/CD, token bus and token ring. The various standards differ at physical layer and MAC layer but are compatible at data link layer 802.2 standard describes the upper part of DLL which uses the LLC (Logical Link control) protocol.

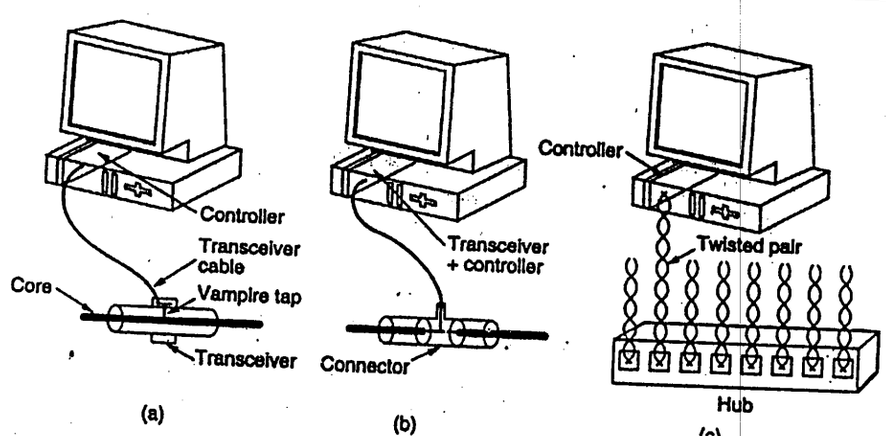
Parts 802.3 through 802.5 describe the three LAN standards, the CSMA/CD, token bus and token ring respectively.

IEEE Standard 802.3 and Ethernet :

- IEEE standard 802.3 is for a 1–persistent CSMA/CD LAN.
- This system was called Ethernet after the luminiferous ether, through which electromagnetic radiation was once thought to propagate.

802.3 Cabling :

Name	Cable	Maximum segment	Nodes/seg.	Advantages
10–Base 5	Thick coax	500 m	100	Good for backbones
10–Base 2	Thin coax	200 m	30	Cheapest system
10–Base T	Twisted pair	100 m	1024	Easy maintenance
10–Base F	Fiber optics	2000 m	1024	Best between building



Three kinds of 802.3 cabling (a) 10Base5 (b) 10Base2 (c) 10Base-T

1. 10–Base 5

- It is popularly called Thick Ethernet.
- There are markings every 2.5m to show where the taps go.
- Connections are generally made using vampire taps, in which a pin is carefully forced halfway into the coaxial cables core.
- 10 Base 5
  - operates at 10 Mbps
  - uses base–band signaling
  - can support segments upto 500m.

2. 10 – Base 2 or Thin Ethernet :

- It bends easily than thick Ethernet.
- Connections are made using BNC connectors to form T junctions rather than vampire taps.
- They are easier to use, reliable, cheaper and easier to install.

Time Domain reflectometry :

- It is a solution for detecting cable breaks, bad taps and loose connectors.
- A pulse of known shape is injected into the cable.
- If the pulse hits an obstacle or end of the cable, an echo will be generated and sent back.
- By carefully timing the interval between sending the pulse and receiving the echo, it is possible to localize the origin of the echo.

This technique is called time domain reflectometry.

- 10 –Base 2
  - operates at 10 Mbps
  - uses base–band signaling
  - can support segments upto 200 m.

3. 10 – Base T

- Problems with cable breaks resulted into different wiring pattern in which a station has a cable running to a central hub.
- They are usually twisted pairs. This scheme is called 10 –Base T
- 10 –Base –T
  - operates at 10 Mbps
  - uses base–band signaling
  - can support segments upto 100m

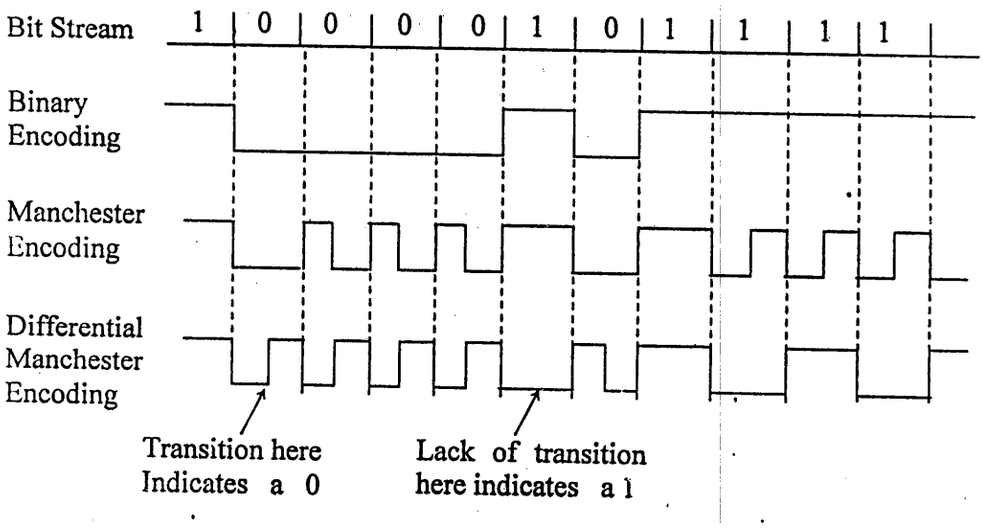
4. 10 – Base F

- 10 – Base F uses fiber optics
- This scheme is expensive due to cost of connectors and terminators.
- They have excellent noise immunity
- 10 – Base T
  - operates at 10 Mbps
  - uses base–band signaling
  - can support segments upto 2000 m
- To allow larger networks multiple cables can be connected by repeaters.
- A repeater is a physical layer device.
  It receives, amplifies and retransmits signals in both directions.
- There is no difference between single network and network with repeaters except for the delay introduced by repeaters.

NOTE :

1. No two transceivers may be more than 2.5 km apart.
2. No path between two transceivers may traverse more than four repeaters.

MANCHESTER ENCODING :



- Receiver needed a way to unambiguously determine the start end, or middle of each bit without reference to external clock.
- Two such approaches are
  1. Manchester encoding
  2. Differential Manchester encoding.

Manchester Encoding :

- Each bit period is divided into two equal intervals.
- A binary bit 1 is sent by having the voltage set high during the first interval and low in the second one.
- A binary 0 is just the reverse : first low and then high.

Advantages :

- This scheme ensures that every bit period has a transaction in middle, making it easy for the receivers to synchronize with the sender.

Disadvantages :

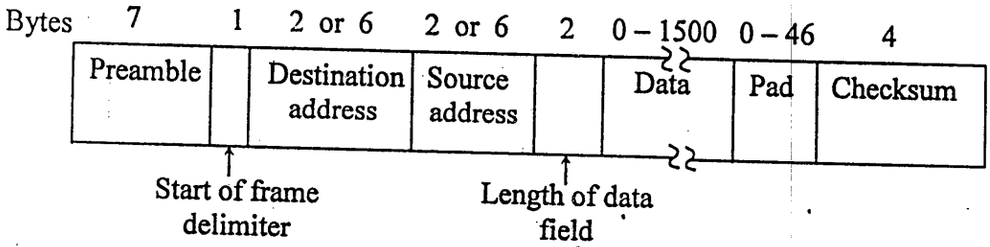
- It requires twice as much bandwidth as binary encoding because pulses are half the width.

Differential Manchester Encoding :

- A 1 bit is indicated by the absence of a transition at the start of the interval.
- A 0 bit is indicated by the presence of a transition at the start of the interval.
- The differential scheme requires more complex equipment but offers better noise immunity.
- All 802.3 baseband systems use Manchester encoding for simplicity.
- The high signal is +0.85 volts and the low signal is –0.85 volts, giving a DC value of 0 volts.

802.3 MAC sublayer protocol

- 802.3 frame format



Preamble :

7 bytes alternate 0's and 1's that alter the receiving system to the coming frame and enable it to synchronize its input timing.

Start frame delimiter (SFD) :

The SFD sequence 10101011 indicates the actual start of frame.

Destination address and source address :

The frame contains the physical address of the destination and source which can be 2 bytes or 6 bytes. But the parameters defined for the 10 – Mbps baseband signaling use only the 6 – byte address

Length of data field :

The length of field tells how many bytes are present in the data field, from a minimum of 0 to a maximum of 1500 bytes.

Data :

Data could be between 0 to maximum of 1500 bytes

Pad : (0 – 46 bytes)

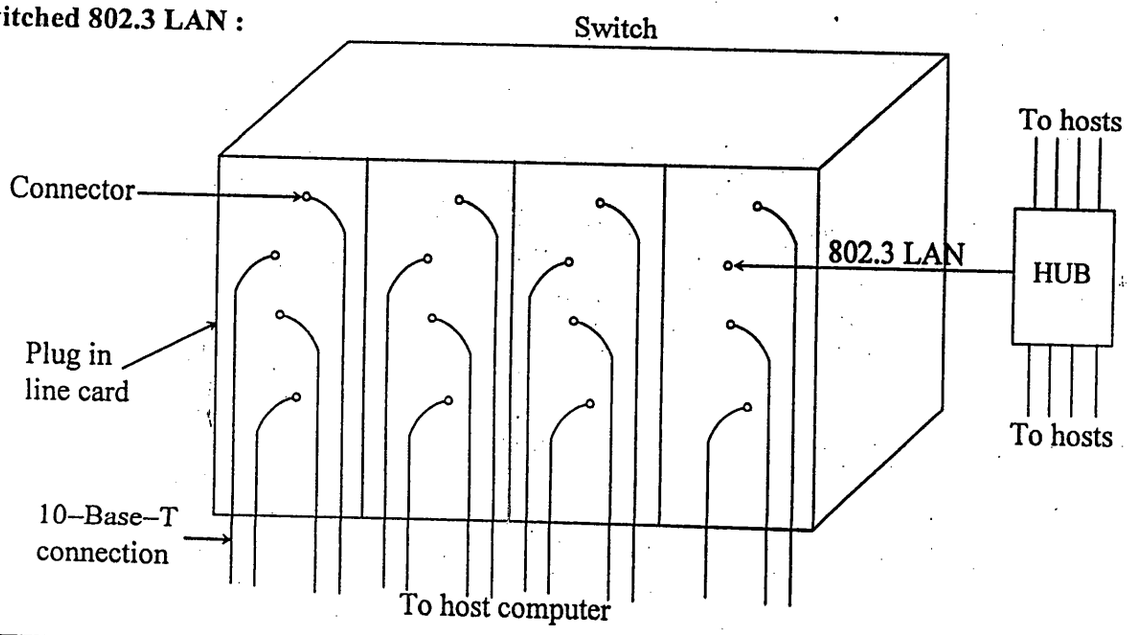
- Write data field of 0 bytes is legal, it causes a problem.
- Whenever a transceiver detects a collision, it truncates the current frame, which means that stray bits and pieces of frame appear on the cable all the time.
- To make it easier to distinguish valid frames from garbage, 802.3 states that valid frames must be atleast 64 bytes long. The pad field is used to fill out the frame to the minimum size.
- Another reason for having minimum length frame is to prevent a station from completing the transmission of a short frame before the first bit has even reached the far end of the cable, where it may collide with another frame.
- For a 10 – Mbps LAN with a maximum length of 2500 meters and four repeaters, the minimum allowed frame must take 51.2 μsec. This time corresponds to 64 bytes. Hence frames with fewer bytes than 64 bytes are padded out to 64 bytes.

Checksum : It is 32 – bit hash code of data.

Collision Recovery Technique of 802.3 :

- **Binary exponential Backoff algorithm :**
- Randomization is done when a collision occurs.
- After a collision, time is divided up into discrete slots whose length is equal to the worst case round – trip propagation time on the ether (2τ)
- After the first collision, each station waits either 0 or 1 slot times before trying again. If two stations collide and each one picks up the same random number, they will collide again.
- After the second collision, each one picks either 0, 1, 2, 3 at random and waits that number of slot times.
- If a third collision occurs, then the next time the number of slots to wait is chosen at random from the interval 0 to $2^3 - 1$.
- In general after 'i' collisions, a random number between 0 and $2^i - 1$ is chosen, and that no. of slots are skipped.
- However, after ten collisions have been reached, the randomization interval is frozen at a maximum of 1023 slots.
- After 16 collisions, the controller throws in the towel, and reports failure back to the computer.

Switched 802.3 LAN :



- As more and more stations are added to 802.3 LAN, the traffic will go up.
  One way to go for higher speed say from 10Mbps to 100 Mbps is buying new adaptor cards.
- One less drastic solution is switched 802.3 LAN.

Construction :

- The heart of this system is a switch containing a high speed backplane and a room for 4 to 32 plug–in–line cards, each containing one to eight connectors.
  Most often each connector has a 10–Base–T twisted pair connection to a single host computer.

Working :

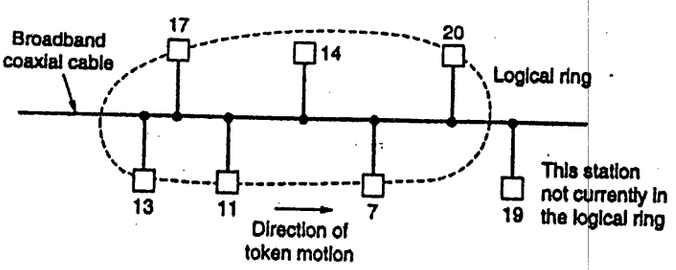
- When a station wants to transmit an 802.3 frame, it outputs a standard frame to the switch.
- The plug–in–line card checks to see if it is for one of the other stations connected to the same card.

  If so the frame is copied there else is sent over high–speed backplane to the destination stations card.
- The backplane typically runs at over 1 Gbps using a proprietary protocol.

What if two machines attached to the same plug in card transmit frames at the same time ?

- One possibility is for all the ports on the card to be wired together to form a local oncard LAN. With this design, each card forms its own collision domain.
- With other kind of plug–in card, each input port is buffered, so incoming frames are stored in the card's on–board RAM as they arrive. This design allows all input ports to receive (and transmit) frames at the same time, for parallel full duplex operation.
- If all the input ports are connected to holes, rather than to individual stations, the switch just becomes an 802.3 to 802.3 bridge.

IEEE Standard 802.4 : Token bus

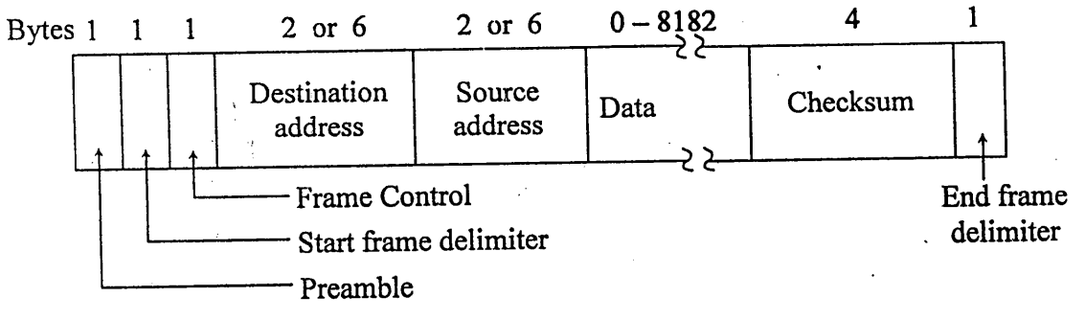


A token bus

Working :

- Physically, token bus is a linear or tree shaped cable onto which stations are attached.
- Logically stations are organized into a ring in which each station knows the address of the station to its "left" and "right".
- When the logical ring is initialized, the highest numbered station may send the first frame.
- After it is done, it passes permission to its immediate neighbour by sending the neighbour a special control frame called a token.
- The token propagates around the logical ring, with only the token holder being permitted to transmit frames.
  Since only one station at a time holds the token, collisions do not occur.
- An important point to realize is that the physical order in which the stations are connected to the cable is not important. Since the cable is inherently a broadcast medium, each station receives each frame, discarding these not addressed to it.
- Physical layer of 802.4 uses 75 ohm broadband coaxial cable.

The token bus MAC sublayer protocol :



- Preamble :
  Same as 802.3 i.e. alternate 1's and 0's but only 1 byte.
- Start frame delimiter and End frame delimiter:
  It contains analog encoding symbols other than 0's and 1's.
- Frame control :
  This byte is used to distinguish data and control frames.
- Data frames : carry priority indicator to send ACK or not.
- Control frames : This gives type of frames like
  (a) Token passing (b) Ring maintenance
  (c) Enter ring (d) Seave ring.
- Data :
  It may range from 8174 to 8182 bytes.
- Checksum :
  It gives 32 bit hash code.

Logical Ring Maintenance :

- Once the ring has been established, each stations interface maintains the addresses of the predecessor and successor stations internally.
- The token holder solicits bids from stations not currently in the ring that wish to join by sending one of the **SOLICIT_SUCCESSOR** frames. The frame gives the sender's address and the successor's address. Stations inside that range may bid to enter.
  - If no station bids to enter within a slot time, the response window is closed and the token holder continues with its normal business.
  - If exactly one station bids to enter, it is inserted into the ring, and becomes the token holder's successor.
  - If two or more stations bid to enter their frames will collide. The token holder then runs an arbitration algorithm, starting with the broadcast of a **RESOLVE_CONTENTION** frame.
- **Leaving the Ring :**
  A station X, with successor S and predecessor P leaves the ring by sending P a SET_SUCCESSOR frame telling it that henceforth its successor is S instead of X. Then X just stops transmitting.
- **Ring Initialization :**
  Consider an idle system with all stations powered off. When the first station comes on line, it notices that there is no traffic for a certain period. Then is sends a **CLAIM_TOKEN** frame. Not hearing any competitors contending for the token, it creates a token and sets up a ring containing only itself. As new stations are powered on, they will respond to these bids and join the ring using the contention algorithm. Eventually every station that wants to join the ring will be able to do so.
- **Station trying to pass the token to a station that has gone down :**
  After passing the token, a station listens to see if its successor either retransmits a frame or passes the token. If it does neither, the token is passed a second time.

If that also fails, the station transmits a **WHO_FOLLOWS** frame specifying the address of its successor. When the failed stations successor sees a **WHO_FOLLOWS** frame naming its predecessor, it responds by sending a **SET_SUCCESSOR** frame to that station whose successor failed, naming itself as the new successor. In this way the failed station is removed from the ring.

- **Station fails to pass the token to its successor and also fails to locate the successor's successor, which may also be down :**
  It adopts a new strategy by sending a **SOLICIT_SUCCESSOR_2** frames to see if anyone else is still alive. Once again the standard contention protocol is run, with all stations that want to be in the ring now bidding for a place. Eventually the ring is established.
- **Token holder goes down and takes the token with it :**
  This problem is solved using the ring initialization algorithm. Each station has a timer that is reset whenever a frame appears on the network. When this timer hits a threshold value, the station issues a **CLAIM_TOKEN** frame, and the modified binary countdown algorithm with random bits determines who gets the token.
- **If there are Multiple Tokens :**
  If a station holding the token notices a transmission from another station, it discards its toke. If there were two, there will now be one. If there were more than two, this process will be repeated sooner or later until all but one are discarded.

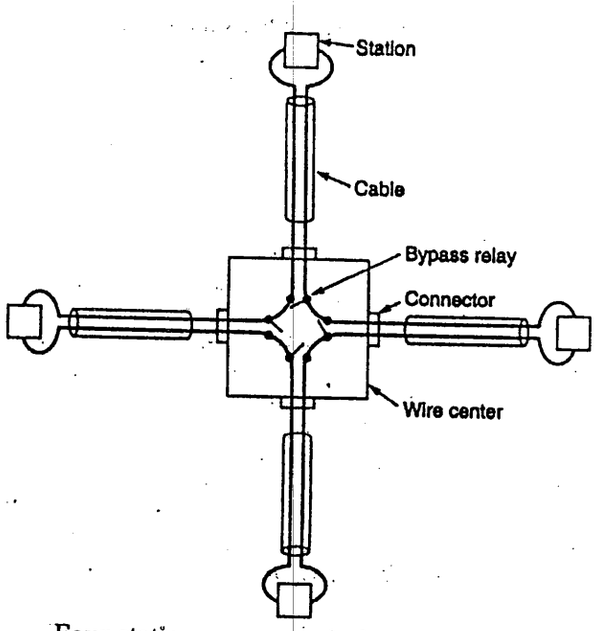
IEEE Standard 802.5 : Token ring

Working :

- In a token ring a special bit pattern called the token, circulates around the ring whenever all stations are idle.
- When a station wants to transmit a frame it is required to seize the token and remove it from the ring before transmitting. Because there is only one token, only one station can transmit at a given instant thus solving the channel access problem the same way the token bus solves it.
- A station may hold the token for token holding time, which is 10 ms. If there is enough time left after the first frame has been transmitted to send more frames, these may be sent as well. On the transmission of another frame if it would exceed the token-holding time, the station re-generates the 3-byte token frame and puts it out onto the ring.
- As the bits that have propagated around the ring come back, they are removed from the ring by the sender. Also after the last bit of its last frame it must regenerate the token.

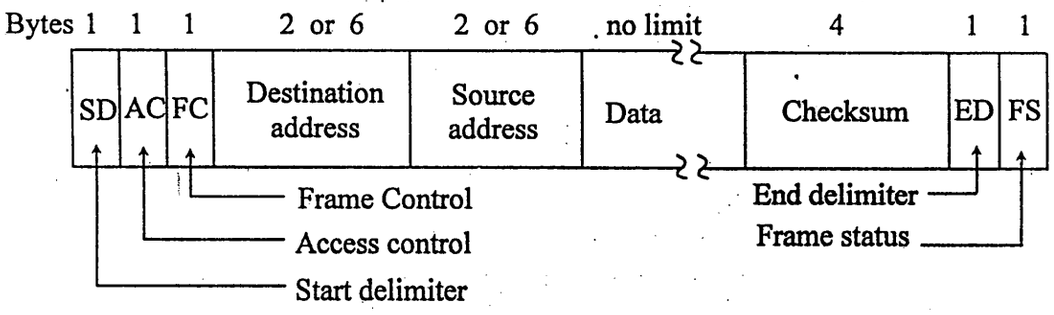
Note :
802.5 aims at office automation where a failure is once in a rare while could be tolerated as the price for a simpler system.

Wire Center :
While logically still a ring, physically each station is connected to the wire center by a cable containing two twisted pairs, one for data to the station and one for data from the station. Inside the wire center are bypass relays that are energized by current from the stations. If the ring breaks/station goes down, loss of drive current will release the relay and bypass the station. The ring can then continue with the bad segment bypassed.

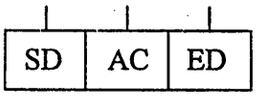


Four stations connected via a wire center

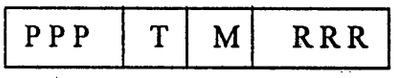
- **Token Ring MAC sublayer protocol :**



(a) Data frame protocol

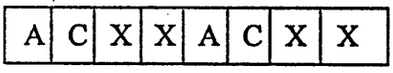


(b) Token format



(c) Access control byte

P = priority bits
T = Token bit
M = Monitor bit
R = Reservation bits



(d) Frame status byte

A = address recognized
C = Copied bit

- Starting delimiter and Ending delimiter :
  They mark beginning and end of frame. Each contains invalid differential Manchester pattern (HH and LL) to distinguish them from data bytes.
- Access Control :
  It contains taken bit, monitor bit, priority bits and reservation bits.
- Frame control :
  This byte distinguishes data frames from various possible control frames.
- Destination address and Source address :
  It can be 2 or 6 bytes long.
- Data :
  The data may be as long as necessary provided that the frame can be still be transmitted with the token–holding time.
- Checksum :
  It is 32 bit hash code.
- Frame Status :
  It contains A and C bits.

  When frame arrives at the interface of a station with the destination address, the interface turns on the A bit as it passes through.

  If the interface copies the frame to the station, it also turns on the C bit.
  A station may fail to copy a frame due to lack of buffer space of other reasons.

Three combinations are possible :

1. A = 0, C = 0 : destination not present or not powered up.
2. A = 1, C = 0 : destination present but frame not accepted.
3. A = 1, C = 1 : destination present and frame copied.

Logical Ring Maintenance :

- Each token ring has a monitor station that oversees the ring. If the **monitor goes down**, a contention protocol insures that another station is elected monitor quickly.
- When the ring comes up or any station notices that there is **no monitor,** it can transmit a **CLAIM_TOKEN** control frame. If this frame circumnavigates the ring before any other CLAIM_TOKEN frames are sent, the sender becomes the new monitor.

- To check for **lost tokens**, the monitor has a timer that is set to the longest possible tokenless interval. If this timer goes off, the monitor drains the ring and issues a new token.
- When a **garbled frame** appears, the monitor can detect it by its invalid format or checksum, and then open the ring to drain it, issuing a new token when the ring has been cleaned up.
- The monitor detects **orphan frames** by setting the monitor bit in the AC byte whenever it passes through. If the incoming frame has this set, something is wrong since the frame has passed the monitor twice without having being drained, so the monitor drains it.

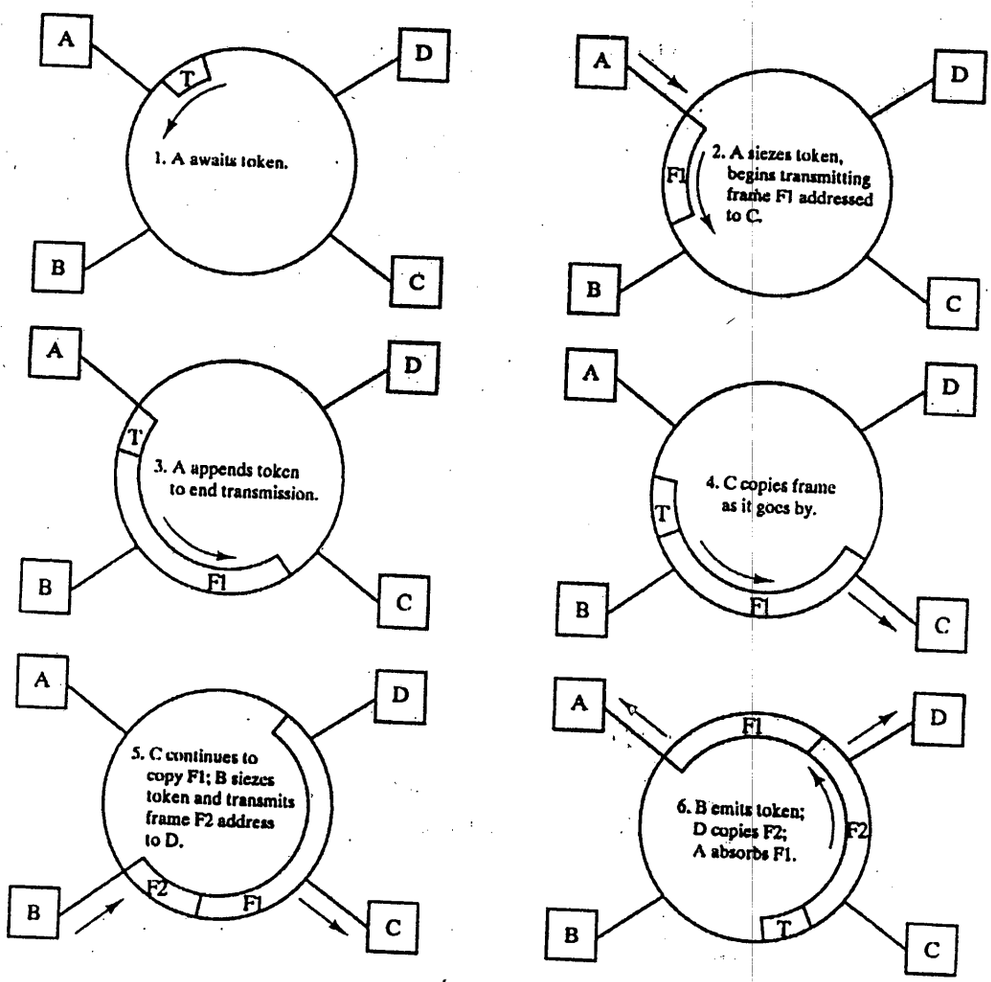
When a station notices that either of its **neighbors appears to be dead,** it transmits **BEACON** frame giving the address of the presumably dead station. When the BEACON has propagated around as far as it can, it is then possible to see how many stations are down, and delete them from the ring using the bypass relays in the wire center, all without human intervention.

Fiber distributed data interface (FDDI) :

FDDI is a token ring scheme that is designed to support data rates of 100 Mbps.

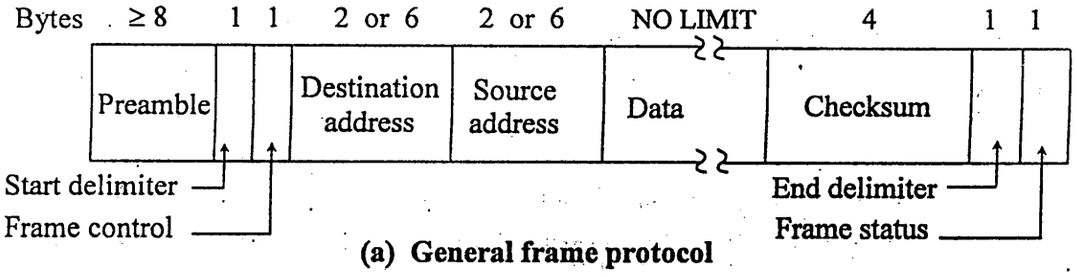
Working :

- In FDDI, a station waiting for a token seizes the token by aborting the token transmission as soon as the token frame is recognized.
- After the captured token is completely received, the station begins transmitting one or more data frames.
- The station releases a new token as soon as it completes data frame transmission, even if has not begun to receive its own data transmission.

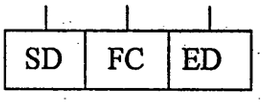


Example of FDDI token ring operation

FDDI MAC Frame :



(a) General frame protocol



(b) Token frame format

- Physical layer doesn't use Manchester encoding
  It uses 4 out of 5 encoding i.e. Each group of 4 MAC symbols are encoded as a group of 5 bits on the medium.

Related Questions :

1. Explain in brief the 802.3 MAC sublayer protocol. Draw and explain the frame format of 802.3.
2. Explain in detail, thick ethernet and thin Ethernet systems.
3. Explain the collision recovery technique implemented in IEEE 802.3 LAN.
4. Compare and contrast FDDI with IEEE 802.5 LAN.
5. List advantages of Manchester encoding.
6. Draw the frame format of token ring 802.5.
7. What happens in token bus if a station accepts the token and then crashes immediately?

Soln :

If a station accepts the token and then crashes immediately, it is similar to the situation that is station is unable to pass the token.
Since after passing the token the station waits to see if the next station either passes the token or sends the frame.
If neither happens, it issues a WHO–FOLLOWS frame and the failed situation is handled.

8. Draw token ring frame format.
   A 4Mbps token ring network has token holding timer value 10msec. What is the longest frame size?
9. What is time domain reflectometry?
10. Does the value of wire centre have any influence on performance of token ring?

Soln:

Adding a wire center increases total cable length and hence the token rotation time.

- The performance degrades as the token rotation time increases.
- For a network whose diameter is small, the effect is less, but for large networks effect is visible.
- There is always a trade–off between performance and reliability. Since adding the wire center increases reliability and maintainability.

11. With respect to the IEEE 802.4 architecture, identify
    (i) token management functions
    (ii) ring management functions.
12. Write SN on Manchester encoding mechanisms.
13. Write SN on FDDI protocol.
14. Why padding restriction is imposed with 802.3 ethernet protocol?
15. List and state 802.4 frame control fields.

16. Explain the significance of propagation delay in Ethernet minimum frame length calculation.

Soln.:

The reason for having a minimum length frame is to prevent a station from completing the transmission of short frame before the first bit has been reached the far end of the cable, where it may collide with another frame.

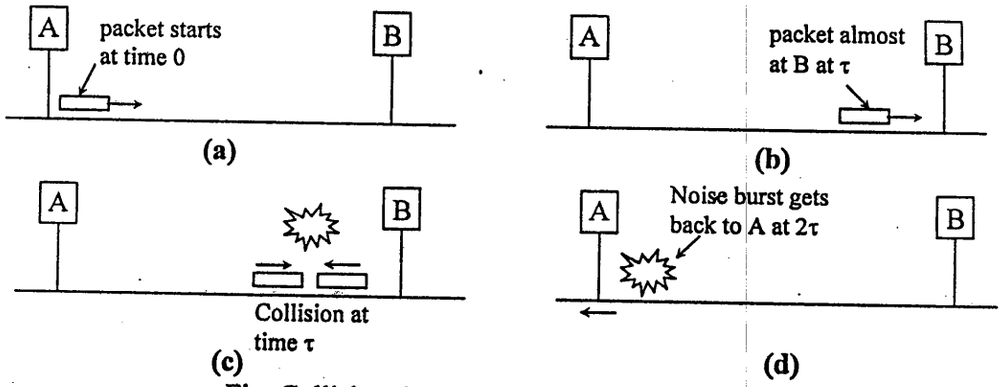


Fig. Collision detection can take as long as 2τ.
τ – Propagation time to reach the other end

- The sender incorrectly conclude that the frame was successfully sent.
- To prevent this all the frames must take more than 2τ to send.
- For 10Mbps LAN with a maximum length of 2500 meters and four repeaters the minimum allowed frame must take 51.2 μsec.

17. Explain AC, FC, FS fields in token ring network.

18. A Mbps token ring network has 10 stations attached each providing 1 bit delay. Determine the length of the conductor to be used so that the token is contained within the ring.

Soln.:

Length of token for token ring = 3 byte = 24 bits.
Data rate = 1 Mbps

Total token transfer time = 24 μsec $\left\{ \text{i.e. } \frac{\text{Length of token}}{\text{Data rate}} \right\}$

No. of stations = 10

Additional delay required from the conductor length = 24 μsec – 10 μsec = 14μsec
Assuming speed of propagation = 2.5×10^8 m/sec

$$\text{speed} = \frac{\text{length}}{\text{time}}$$

$\therefore$ conductor length = 2.5×10^8 m/s $\times$ 14×10^{-6} μsec
$= 35 \times 10^3$ m = 35 km

19. List advantages and disadvantages of Manchester encoding.

20. How do low priority station gains the token in 802.5 standard?

Soln.:

- The 3 byte token frame contains a field in middle byte i.e. access control giving the priority of the token.
- When a station wants to transmit priority n frame, it must wait until it can capture a token whose priority is less than or equal to n.
- When a data frames goes by, a station can try to reserve the next token by writing the priority of the frame, frame it wants to send into the frame's Reservation bits. However, if a higher priority has already been reserved there, the station may not make reservation. When the current frame is finished, the next token is generated at the priority that has been reserved.
- The problem here is that the reservation priority keeps on jumping higher and higher and hence low priority station cannot gain the token.
- To eliminate the problem, the protocol says that the station raising the priority is responsible for lowering the priority again when it is done.
  Hence the low priority station can now gain the token.

Bridges :

Need for bridges :

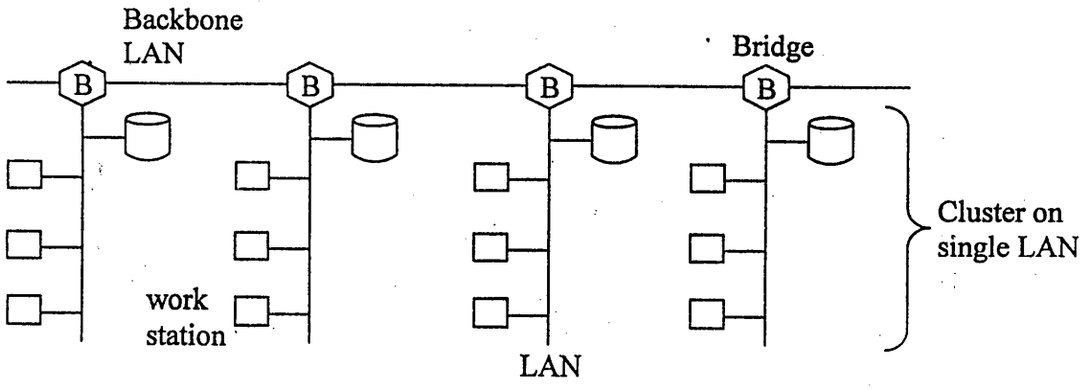


Fig. Multiple LAN's connected by a backbone to handle a total load higher than the capacity of a single LAN

1. Since the goals of different departments in a company differ, different LAN's are chosen. But still at times they require interaction among each other, so bridges are needed.
2. If the geographically distance between workstations is large it may be cheaper to have separate LAN's in each area and then connect them with bridges.
3. It is necessary to split a single LAN into separate LAN's to accommodate the load. Each LAN contains a cluster of workstations with its own file server, so that most traffic is restricted to a single LAN and does not add load to the backbone.
4. Bridges are used when the physical distance between workstation is to a great (e.g. more than 2.5 km for 802.3)
5. Bridges add to the reliability in the network. Unlike repeaters, a bridge can be programmed to exercise some discretion about what it forwards and what is does not forward. (e.g. garbage will not be forwarded)
6. Bridges enable security.
   By inserting bridges at various places and careful not to forward sensitive traffic, it is possible to isolate parts of the network so that its traffic cannot fall into wrong hands.

Bridges from 802.x to 802.y

- There are some difficulties that will be encountered when trying to build a bridge between various 802 LANs.
- Each of the nine combinations of 802.x to 802.y has its own unique set of problems.
- However some general problems are
  1) Each of the LAN uses a different frame format.
  2) Interconnected LAN's may not work at same data rate.
  3) All the three 802 LAN's have a different maximum frame length.
- The other specific problems for a bridge from 802.x to 802.y are :–

Destination LAN

Source LAN		802.3 (CSMA/CD)	802.4 (Token Bus)	802.5 (Token Ring)
	802.3		1, 4	1, 2, 4, 8
	802.4	1, 5, 8, 9, 10	9	1, 2, 3, 8, 9, 10
	802.5	1, 2, 5, 6, 7, 10	1, 2, 3, 6, 7	6, 7

Actions :

1. Reformat the frame and compute new checksum
2. Reverse the bit order
3. Copy the priority, meaningful or not

4. Generate a fictitious priority.
5. Discard priority
6. Drain the ring (somehow)
7. Let A and C bits (by lying)
8. Worry about congestion (fast LAN to slow LAN)
9. Worry about token handoff ACK being delayed or impossible.
10. Panic if frame is too long for destination.

Parameters assumed :

802.3 : 1500 – byte frames 10 Mbps (minus collisions)
802.4 : 8191 – byte frames 10 Mbps
802.5 : 5000 – byte frames 4 Mbps

Transparent Bridge :

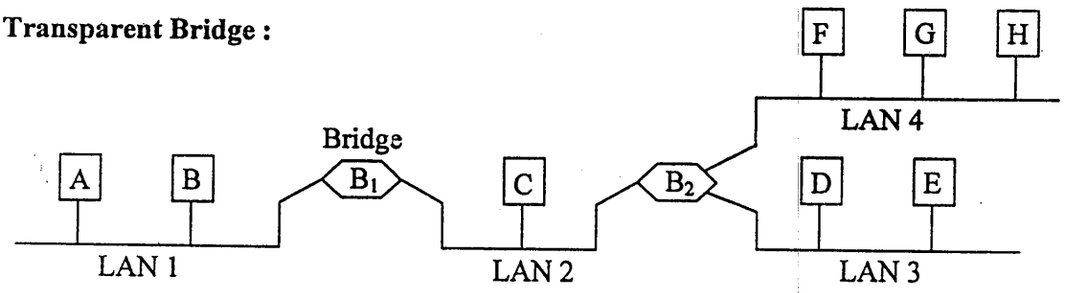


Fig. A configuration with four LAN's and two bridges.

e.g.
- A frame arriving at bridge B_1 on LAN 1 destined for A can be discarded immediately because it is already on the right LAN, but a frame arriving on LAN 1 for C for F must be forwarded.
- The decision of forwarding or discarding is made by looking up the big hash table inside the bridge.

Operation :

- When the bridges are first plugged in, all has tables are empty.
- None of the bridges know where any of the destinations are, so they use the flooding algorithm.
- Every incoming frame for an unknown destination is output on all the LAN's to which a bridge is connected except the one it arrived on.
- The algorithm used by transparent bridges is backward learning.
- By looking at the source address, they can tell which machine is accessible on which LAN. e.g. If bridge B_1 sees a frame on LAN 2 coming from C it knows that C is reachable via LAN 2, so it makes an entry in its hash table noting that frames going to C should use LAN 2.
- Periodically, a process in the bridge scans the hash table and purges entries more than few minutes old.
- The routing procedure for an incoming frame depends on the LAN it arrives on (the source LAN) and the LAN its destination is on (the destination LAN) as follows :
  1. If destination and source LANs are the same, discard the frame.
  2. If the destination and source LANs are different, forward the frame.
  3. If the destination LAN is unknown use flooding.

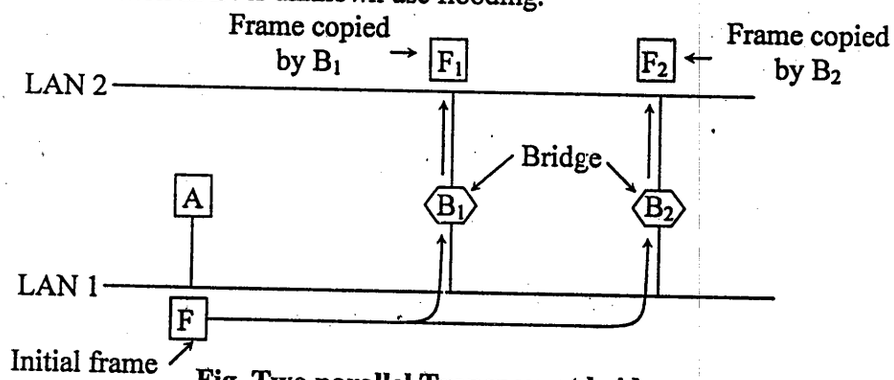
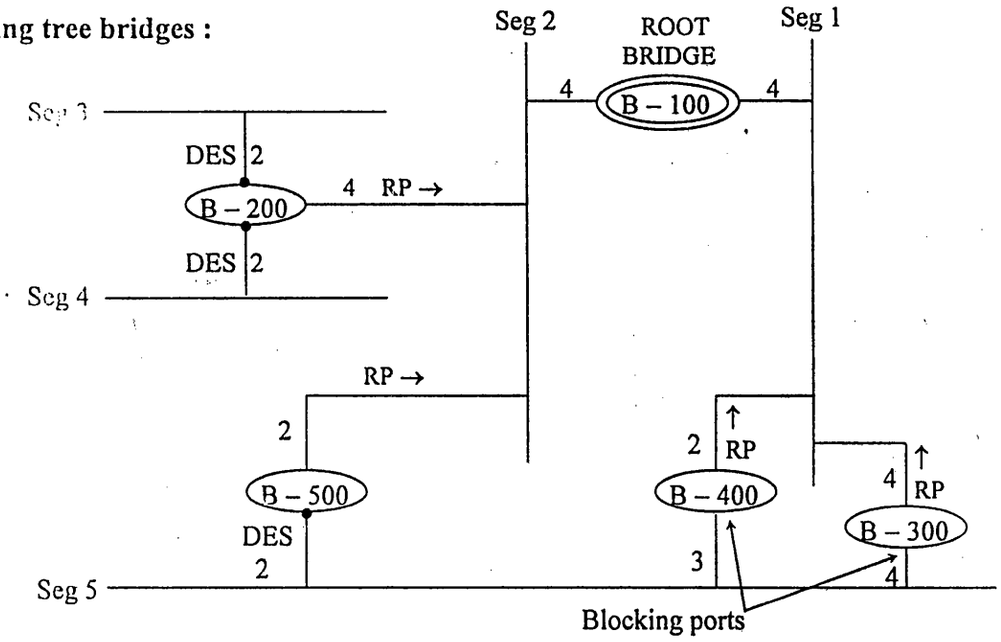


Fig. Two parallel Transparent bridges

- To increase reliability, some sites use two or more bridges in parallel between LAN's This arrangement creates loops in the topology.

Spanning tree bridges :



- To avoid loops, spanning tree bridges are used.
- Each bridge is assigned an unique ID number.

Algorithm :

1. Finding the root bridge.
   Bridge with smallest ID is chosen as ROOT BRIDGE.
2. Finding root port :
   - Root bridge records the accumulated root cost of every port.
   - The root port is the port which has minimum accumulated root cost i.e. cost from bridge to root.
3. Choosing the designated bridge :
   - All the connected to the same segment send frame to each other.
   - The bridge that can carry the frame from the segment to the root with cheapest cost is designated bridge and the particular port that connects the bridge to that segment is called designated port.
   - Blocking ports are the ports that are neither root ports nor designated ports.

Note :

- Root port cannot be chosen as designated port.
- A bridge can have only one Root port but more than on designated port.

Source routing bridges :

- Source routing assumes that the sender of each frame knows whether or not the destination is on its own LAN.
- When sending a frame to a different LAN, the source machine sets the high–order bit of the source address to 1, to mark it.
- Furthermore, it includes in the frame header the exact path that the frame will follow. A route is a sequence of bridge, LAN, bridge, LAN, numbers.
- A source routing bridge is only interested in the frames with the high–order bit of the destination set to 1. For each such frame that it sees, it scans the route looking for the number of the LAN on which the frame arrived.

  If this LAN number is followed by its own bridge number, the bridge forwards the frame onto the LAN whose number follows its bridge number in the route.

  If the incoming LAN number is followed by the number of some other bridge, it does not forward the frame.
- In source routing every machine in the internet work knows, or can find the best path to every other machine.
- If a destination is unknown, the source issues a broadcast frame asking where it is. This discovery frame is forwarded by every bridge so that it reaches every LAN on the internetwork.
- When the reply comes back, the bridges record their identity in it, so that the original sender can see the exact route taken and ultimately choose the best route.

Related Questions :

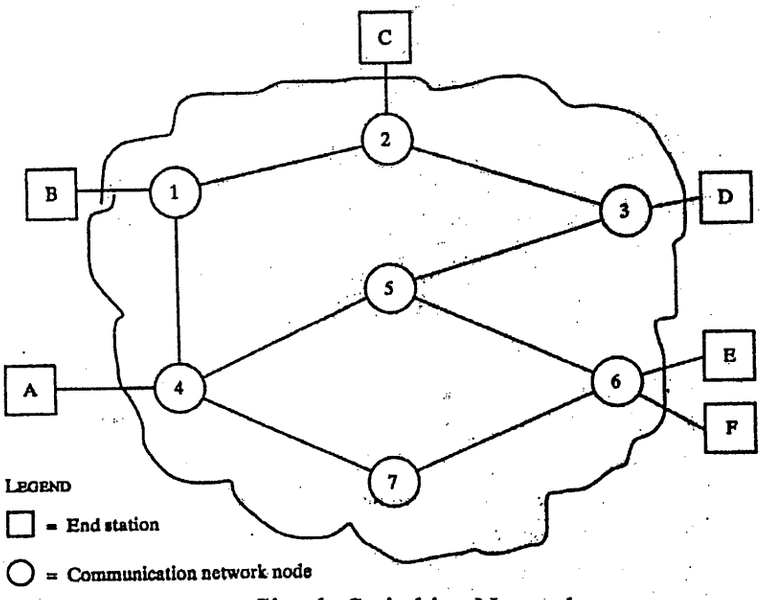
1. Give reasons for the use of multiple LANs connected by bridges.
2. Write SN on Transparent bridges.
3. Write SN on bridge.
4. Explain the various problems encountered in building a bridge from 802.3 to 802.5.
5. Consider two bridges, one which has to forward 1000 512 bytes frames per second and other bridge has to forward 200 4096 bytes frames per second. Which bridge do you think would need faster CPU? Why?
6. List steps of spanning tree algorithm.
7. State two important reasons to bridge LANs. Also state two important issues while bridging LANs.
8. Compare source routing bridges and transparent bridges.

	Source Routing Bridges	Transparent Bridges
1.	Installation is manual, hence difficult to install.	Installation is transparent done by the bridges themselves.
2.	Source to destination route is set in the bridges using discovery frames	Route is identified using backward learning algorithm.
3.	Optimal use of bandwidth	Does not make optimal use of bandwidth since spanning tree uses subset of topology.
4.	Sender of the frame knows whether receiver is on the same LAN or not	Bridges have to worry about whether receiver is on same LAN or not.
5.	Failure is handled by host	Failure is handled by bridges
6.	The whole path from the source to destination is send along with the frame.	Only the destination address is send along with the frame.
7.	They are connection–oriented	They are connectionless.

Circuit Switching

Switching Networks :

For transmission of data beyond local area, communication is typically achieved by transmitting data from source to destination through a network of intermediate switching nodes. Each station attaches to a node and the collection of nodes is referred to as a communication network.



Simple Switching Network

From the above figure:

1) Some nodes connect only to other nodes. Their sole task is the internal switching of data.
2) Node-Node links are multiplexed using FDM or TDM.
3) The network is not fully connected i.e. there is no direct link between every possible pair of nodes.

Circuit Switching Networks :

Communication via circuit switching implies that there is a dedicated communication path between two stations. That path is a connected sequence of links between network nodes. On each physical link, a logical channel is dedicated to the connection. Communication via circuit switching involves three phases.

1. Circuit Establishment :
Before any signals can be transmitted, an end-to-end circuit must be established.

2. Data Transfer :
Information can now be transmitted through the network established. The data may be analog or digital.

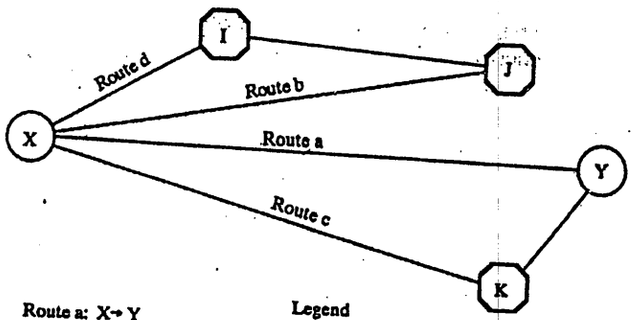
3. Circuit Disconnect :
After some period of data transfer the connection is Terminated usually by the action of one of the two stations.

Routing in Circuit Switched Networks

A dynamic routing approach is one in which routing decisions are influenced by current traffic conditions. Two broad classes of dynamic routing algorithms have been implemented.
(a) Alternate Routing (b) Adaptive Routing

Alternate Routing :

The essence of alternate routing schemes is that the possible routes to be used between two end offices are predefined. It is the responsibility of the originating switch to select the appropriate route for each call. Each switch is given a set of pre-planned routes for each destination, in order of preference. The preferred choice is a direct trunk connection between two switches. If the trunk is unavailable then the second choice is to be tried and so on.



Route a: X→Y
Route b: X→J→Y
Route c: X→K→Y
Route d: X→I→J→Y

Legend
= End office
= Intermediate switching node

(a) Topology

Time Period	First route	Second route	Third route	Fourth and final route
Morning	a	b	c	d
Afternoon	a	d	b	c
Evening	a	d	c	b
Weekend	a	c	b	d

(b) Routing table

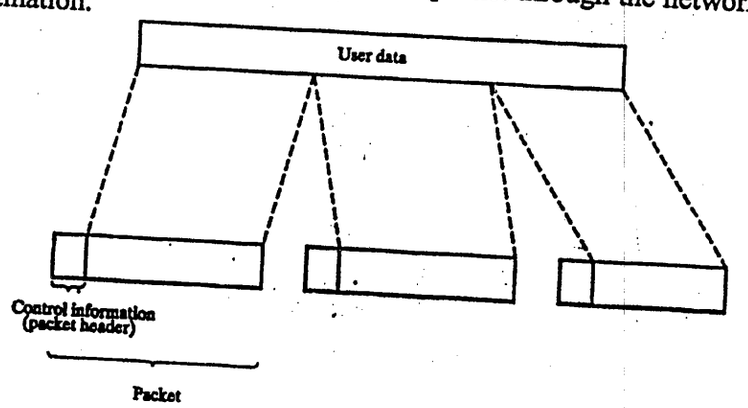
Example :
MAR – Multi alternate Routing
DNHR – Dynamic Non-Hierarchical Routing

Adaptive Routing :
An adaptive routing scheme is designed to enable switches to react to changing traffic patterns on the network. Such schemes require greater management overhead, as the switches must exchange information to learn of network conditions. However, compared to an alternative-routing scheme, an adaptive scheme has the potential for more effectively optimizing the use of network resources.

Example :
DTM – Dynamic Traffic Management : It uses a controller to find the best alternate route choices depending on congestion in the network. The central controller collects the status data from each switch in the network every 10 sec. to determine preferred alternate routes.

Shortcomings of Circuit Switching Network :
1) In a typical user host data connection much of the time the line is idle. Thus the circuit-switching approach is inefficient.
2) In a circuit-switching network, the two devices that are connected must transmit and receive at the same rate as the other; this limits the utility of the network in interconnecting a variety if host computers and terminals.

Packet Switching
Data are transmitted in short packets. If a source has a Longer message to send, the message is broken up into a series of packets, each packet containing a portion of the
users data plus some control information. The control information includes the information that the network requires in order to be able to route the packet through the network and deliver it to the intended destination.



At each node on the route, the packet is received, stored briefly and passed onto the next node.

Advantages over **Circuit Switching :**

1) Line efficiency is greater, as a single node-to-node link can be dynamically shared by many packets over time.
2) A packet switching network can perform data rate conversion. Two station of different data rates can exchange packets.
3) When traffic becomes heavy on a circuit switched network, some calls are blocked. On a packet switching network, packets are still accepted, but delivery delay increases.

Switching Technique

1) Datagram Approach : Each packet treated independently is referred to as a Datagram. The packets, each with the same destination Address, do not follow the same route. It is also possible that the packets will be delivered to the end station in a different sequence from the one in which they were sent. It is upto the destination station to figure out how to reorder them.
2) Virtual Circuit Approach : A pre-planned route is established before any packets are sent. Because the route is fixed for the duration of the logical connection, it is somewhat similar to a circuit in a circuit switching network and is referred to as a virtual circuit. Each packet now contains a virtual circuit identifier as well as data; each node on the pre-established route, knows where to direct such packets; no routing decisions are required. Eventually one station terminates the connection with a clear-request packet.

   Virtual circuit is not a dedicated path like circuit Switching. A packet is still buffered at each node, and Queued for output over time. The difference from the Datagram approach is that, with virtual circuits, the node need not make a routing decision for each packet; it is made only once for all packets using that virtual circuit.

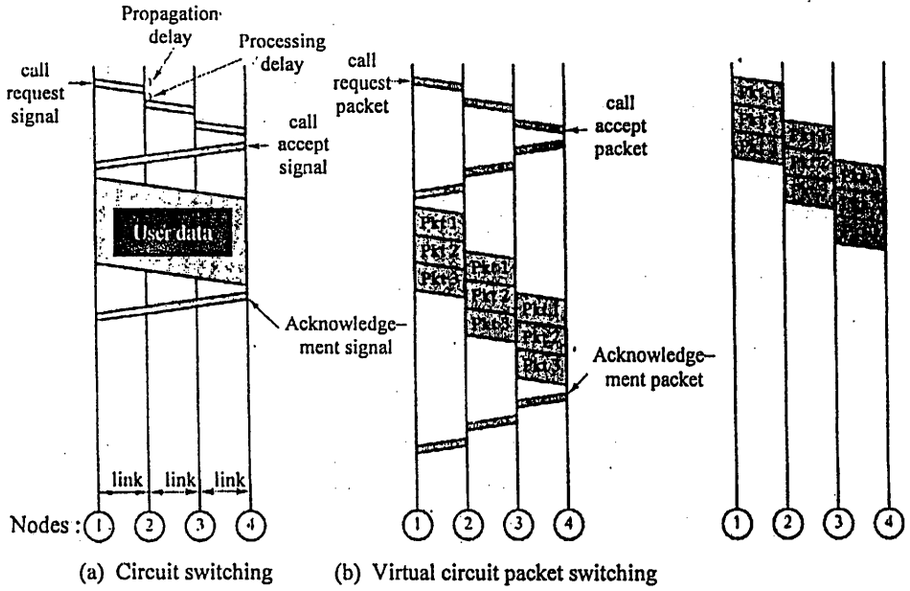
Advantages to Virtual Circuit over Datagram approach :

1) Packets arrive in the original order.
2) Network should transmit the packets more rapidly, because no routing decisions need to be made.

Advantages to Datagram Approach over Virtual Circuit :

1) Call setup phase is avoided. Therefore for few packets datagram delivery will be quicker.
2) More flexible. For example if congestion develops in one part of the network, incoming datagrams can be routed away from the congestion.
3) More reliable. With the use of virtual circuits if a node fails, all virtual circuits that pass through that node are lost. With datagram delivery if a node fails, subsequent packets may find an alternate route that bypasses that node.

Comparison of Circuit and Packet Switching :



(a) Circuit switching (b) Virtual circuit packet switching

Event timing for circuit switching and packet switching

Circuit Switching	Virtual Circuit Switching	Datagram Packet Switching
Dedicated transmission path	No dedicated path	No dedicated path
Continuous transmission of data	Transmission of packets	Transmission of packets
Messages are not stored	Packets are stored until delivered	Packets may be stored until delivered
The path is established for entire conversation	Route established for entire conversation	Route established for each packet
Call setup delay; negligible transmission delay	Call setup delay; packet transmission delay	Packet transmission delay
Busy signal if called party busy	Sender notified of connection denial	Sender may be notified if packet not delivered
Electromechanical or computerized switching nodes	Small switching nodes	Small switching nodes
Fixed bandwidth transmission	Dynamic use of bandwidth	Dynamic use of bandwidth
No overhead bits after call setup	Overhead bits in each packer	Overhead bits in each message
Usually no speed of code conversion	Speed and code conversion	Speed and code conversion

Routing algorithms :

- Routing algorithms is that part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on.
- Routing algorithms can be grouped into two major classes :
  Non adaptive and Adaptive
- Non adaptive algorithms do not base their routing decisions on measurements and estimate of the current traffic and topology.
  The choice of the route to use is computed in advance, offline and downloaded to the routers when the network is booted.
  This procedure is sometimes called static routing.
- Adaptive algorithms change their routing decision to reflect changes in the topology, and the traffic as well.
  Adaptive algorithms differ in where they get their information (e.g. locally from adjacent routers or from all routers), when they change the routes (e.g. every ΔT sec, when the load changes or when the topology changes) and what metric is used for optimization (e.g. distance, number of hops, or estimated transit time).

Shortest path routing :

- The idea is to build a graph of the subnet with each node of the graph representing a router and each arc of the graph representing a communication line. To choose a route between a given pair of routers, the algorithm finds the shortest path between them on the graph.
- Some algorithms used to find the shortest path between two nodes are :
  (a) Djikstra's algorithm
  (b) Bellman ford algorithm
  (c) Kruskal's algorithm
  (d) Prim's algorithm

(a) Djikstra's algorithm :

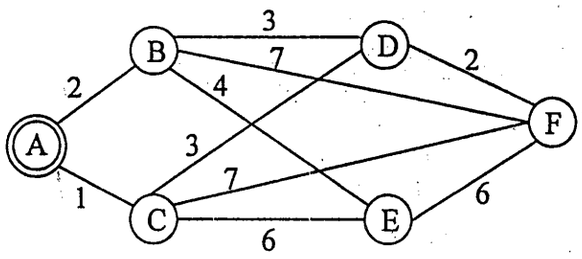
- It is called shortest path algorithm or forward search algorithm.
- It is a centralized, static algorithm although it could be made adaptive by executing it periodically.

Algorithm :

1. Define S as a set of nodes. Initially node contains the start node.
2. Define cost(X) as the cost of the cheapest route from start node to X using only nodes from S.
   do {
   a) Determine the set of nodes not in S but connected to a node in S. Call this set W.
   b) Choose a node X in W for which cost(X) is minimum.

c) For each V not in S, define
cost(V) = minimum {cost(V), cost(X) + cost of link connecting X to V }
If cost(V) is changed define prior(V) = X
d) Add X to the set S.
} while not all nodes in S.

e.g.

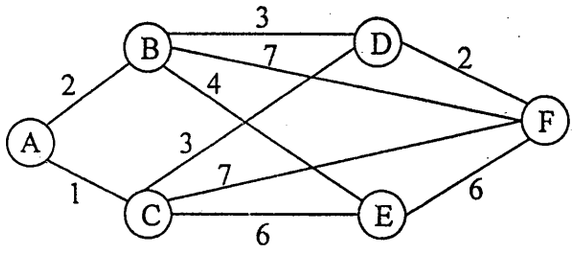


Step	S	W	Cost functions for						Prior functions for				
			X	B	C	D	E	F	B	C	D	E	F
I	{A}	{B, C}	C	2	1	∞	∞	∞	A	A	–	–	–
II	{A, C}	{B, D, E, F}	B	2	1	4	7	8	A	A	C	C	C
III	{A, B, C}	{D, E, F}	D	2	1	4	6	8	A	A	C	B	C
IV	{A, B, C, D}	{E, F}	E	2	1	4	6	6	A	A	C	B	D
V	{A, B, C, D, E}	{F}	F	2	1	4	6	6	A	A	C	B	D
VI	{A, B, C, D, E, F}	{ }	–	2	1	4	6	6	A	A	C	B	D

Shortest path from A to F is
F ← D ← C ← A
Least cost = 6

(b) Bellman ford Algorithm :

e.g.



Max. no. of arcs	Destination node					Prior node				
	B	C	D	E	F	B	C	D	E	F
1	2	1	–	–	–	A	A	–	–	–
2	2	1	4	6	8	A	A	C	B	C
3	2	1	4	6	6	A	A	C	B	D
4	2	1	4	6	6	A	A	C	B	D

(c) Kruskal's Algorithm :

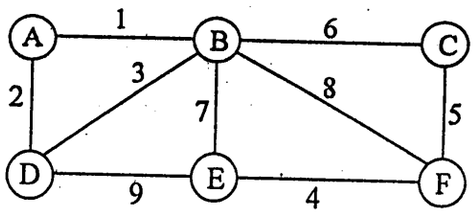
1. Consider all the nodes.
2. Select the link with the least weight.
3. Check whether this link forms a loop with the links already present in the graph.
4. If it forms a loop then reject it ,else include it in the graph.
5. Continue the alone steps till a tree connecting all the node is formed.

Kruskal's algorithm starts with each node being a single node fragment.

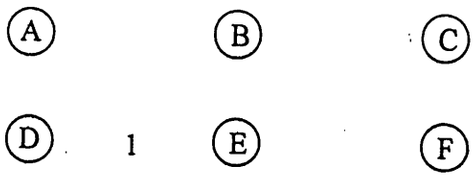
It then successively combines two of the fragment by using the arc that has minimum weight over all arcs that when added to the current set of fragments do not form a cycle.

Kruskal's algorithm

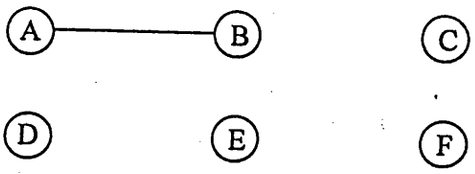
i)



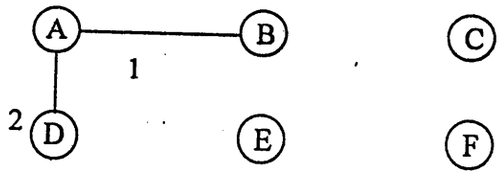
ii)



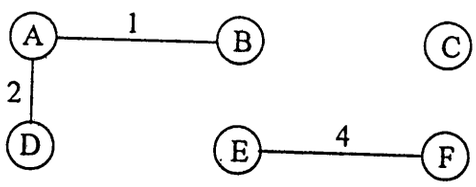
iii)



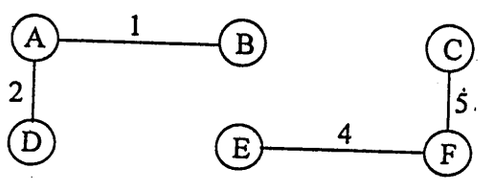
iv)

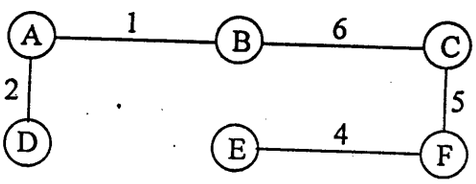


v)



vi)





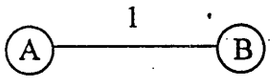
Prims Algorithm :

1. Start with the source node.
2. Select the lowest cost link connected to the source code.
3. Include this link in the graph.
4. Add the connected node now into the selected source node set.
5. Go to step 1. Repeat steps 1 to 4 till all the nodes in the network are included in the source node list.

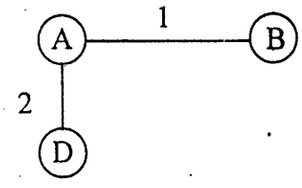
Consider the following Example :
Suppose A is the source node.

Step 1:

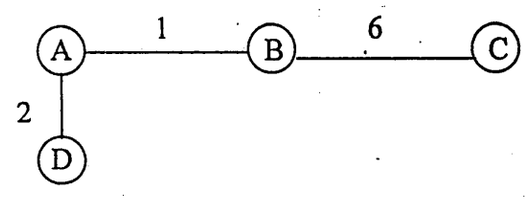
Step2:



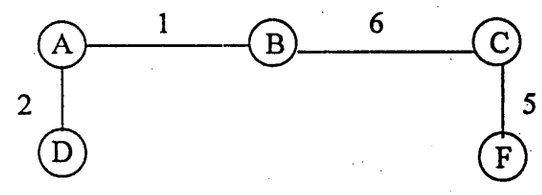
Step 3:



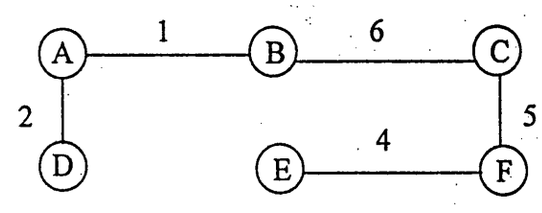
Step4:



Step5:



Step6:



Dynamic Algorithms :

- The two dynamic routing algorithms are :

1. Distance Vector Routing

Operation :

a. Routing table has entry for each router in the network.

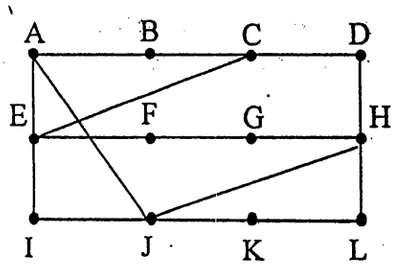
b. Routing table is send to all the neighbours.

c. Routing table is send at regular intervals.

d. Calculation is done using the routing table of all routers and the best estimate is found and new routing table is produced.

e.g. Bellman–ford algorithm.

e.g. Figure shows the subnet



Delay vectors received from neighbours of Router J are :
(Delay metric used is queue length)

J_0	A	I	H	K
A	0	24	20	21
B	12	36	31	28
C	25	18	19	36
D	40	27	8	24
E	14	7	30	22
F	23	20	19	40
G	18	31	6	31
H	17	20	0	19
I	21	0	14	22
J	9	11	7	10
K	24	22	22	0
L	29	33	9	9
	JA delay is 8	JI delay is 10	JH delay is 12	JK delay is 6

vectors received from J's four neighbours.

new estimated delay from J	Line
8	A
20	A
28	I
20	H
17	I
30	I
18	H
12	H
10	I
0	–
6	K

new routing table for J

Problems of Distance Vector Spacing :

1. Delay metric was queue length and did not line bandwidth into account.
2. Count to infinity problem.

Count to Infinity problem :

- In distance vector routing, goods news spread rapidly but bad news take time.
- Consider the five–node (linear) subnet where delay metric is the number of hops.
- Suppose A is down initially and all other routers know this. When A comes up, the other routers learn about it via the vector exchanges.
  The good news spread at the rate of one hop per exchange.
- Suppose all the lines and routers are initially up. Suddenly A goes down or line between A and B is cut, which is same thing from B's point of view. Hence we see bad news travel slowly.
  All the routers work their way upto infinity.
  This problem is known as count–to–infinity problem.

A — B — C — D — E

∞	∞	∞	∞	Initially
1	∞	∞	∞	After 1 exchanges
1	2	∞	∞	After 2 exchanges
1	2	3	∞	After 3 exchanges
1	2	3	4	After 4 exchanges

A — B — C — D — E

1	2	3	4	Initially
3	2	3	4	After 1 exchange
3	4	3	4	After 2 exchange
5	4	5	4	After 3 exchange
5	6	5	6	After 4 exchange
7	6	7	6	After 5 exchange
7	8	7	8	After 6 exchange
∞	∞	∞	∞	
⋮	⋮	⋮	⋮	

2. Link State Routing :

a) Routing table has entry only for the neighbours.
b) Routing table is send to all the routers in the network.
c) Routing table is send only when there is a change in the network.

Operation :

Each router must :

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

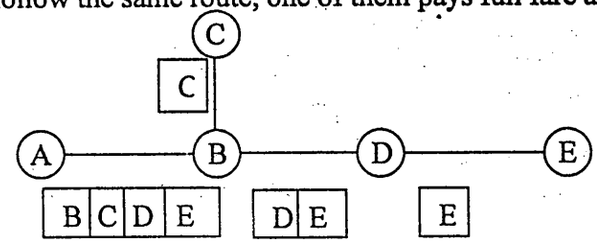
e.g. Dijktra's algorithm.

Broadcast Routing :

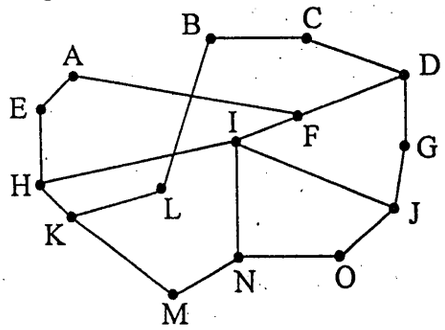
Sending packet to all destinations simultaneously is called broadcasting.

The various broadcasting algorithms are–

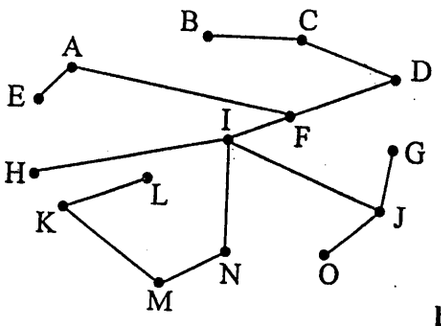
1. **Send distinct packet to all destinations :**
   This requires source to have a complete list of destinations.
2. **Flooding :**
   Send the packet to all the outgoing lines except the line from which it has come.
3. **Multidestination routing :**
   Each packet contains a list of destinations indicate the desired destinations.
   When a packet arrives at the router, router checks all the destinations to determine the set of output lines that will be needed.
   The router generates a new copy of the packet for each output line to be used and includes in each packet only those destinations that are to use the line.
   After sufficient number of hops, each packet will carry only one destination and can be treated as a normal packet.
   Multidestination 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.



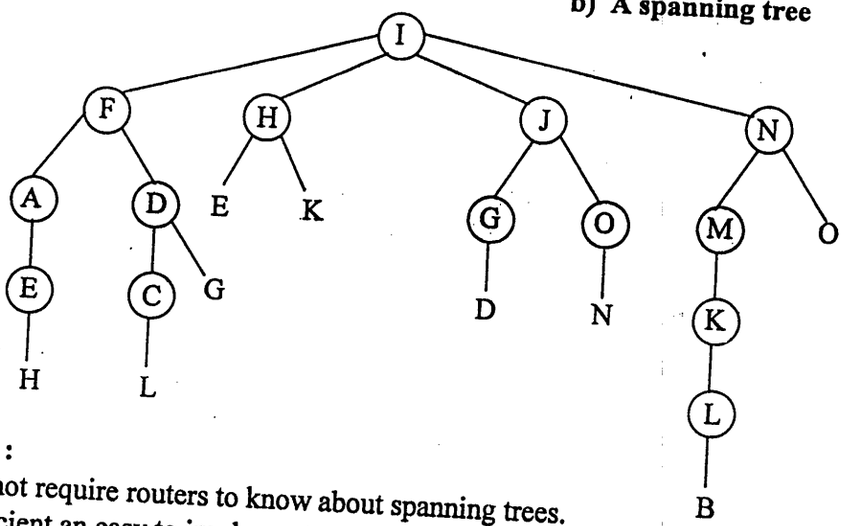
4. **Sink tree :**
   A spanning tree is a subset of the subnet that includes all the routers but contains no loops.
   When hop count is used as metric, spanning tree is called sink tree.
   Problem :
   Each router must have knowledge of some spanning tree for it to be applicable. Sometimes this information is available (e.g. Link state routing) but sometimes it is not (e.g. distance vector routing)
5. **Reverse path forwarding :**
   When a broadcast packet arrives at a router, the router checks to see if the packet arrived on the line that is normally used for sending packets to the source of the broadcast.
   The router forwards copies of packet arrived on a line other than the one it arrived on.
   If, however the broadcast packet arrived on a line other than the preferred one for reaching the source, the packet is discarded as a likely duplicate.
   This is an example of algorithm called reverse path forwarding.



Reverse path forwarding a) A subnet



b) A spanning tree

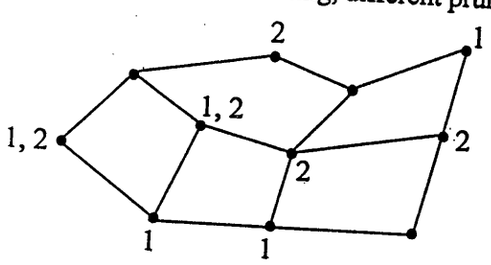


Advantage :

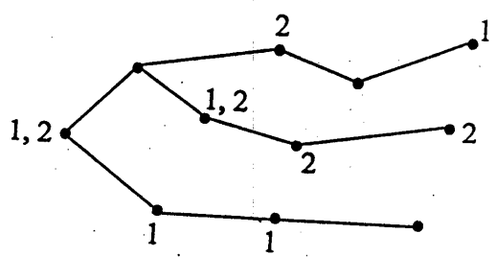
- It does not require routers to know about spanning trees.
- It is efficient an easy to implement.

Mulitcasting Routing :

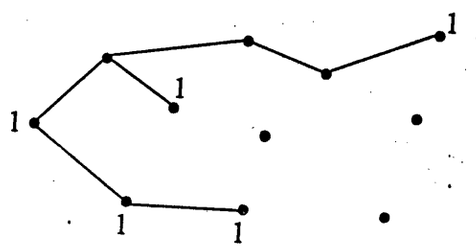
- It is frequently necessary to send message to all the other members of a group. If the group is small, point to point messaging is possible. If group is large this is expensive.
- Sending a message to a group is called multicasting and its routing algorithm is called multicast routing.
- Group management required, i.e. processes for create, destroy, join and leave group is required. Changes must be informed to the routers.
- To do multicast routing, each router computes a spanning tree covering all other routers in the subnet.
- When a process sends a multicast packet to a group, the first router examines its spanning tree and prunes it, removing all lines that do not lead to hosts that are members of the group.
- Various ways of pruning a spanning tree are possible :
  1. Link state routing, simple since each router is aware of the complete subnet topology, including which hosts belong to which groups.
  2. Distance vector routing, different pruning strategy has to be used– Reverse path forwarding.



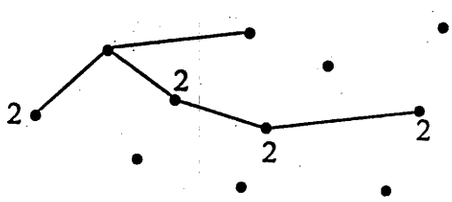
a) A subnet



b) A spanning tree for the leftmost router

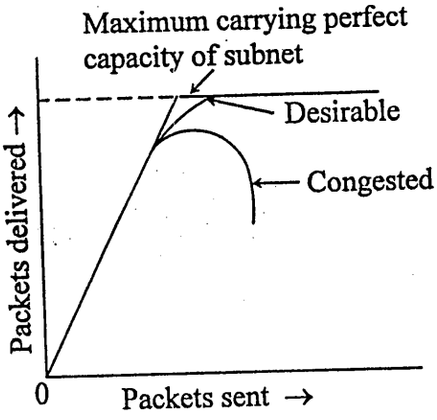


c) A multicast tree for group 1



Congestion Control Algorithms :

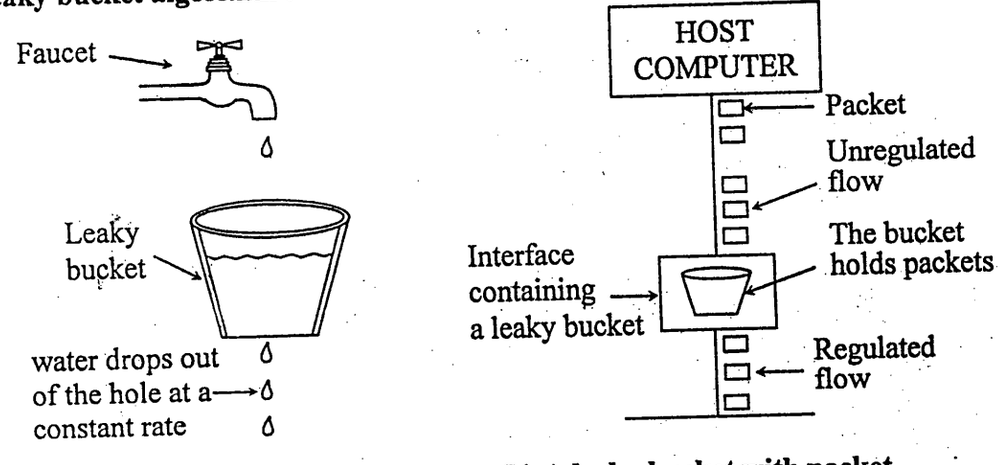
Congestion :



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

- Causes of congestion :
  1. If all of a sudden, stream of packets begin arriving on three or four input lines and all need the same output line, a queue will build up.
  2. Slow processors
  3. Low bandwidth lines.
- Traffic shaking :
  1. One of the main causes of congestion is that traffic is often bursty.
  2. If hosts could be made to transmit at uniform rate, congestion would be less common.
  3. Traffic shaping is about regulating the average rate of data transmission.

Leaky bucket algorithm :

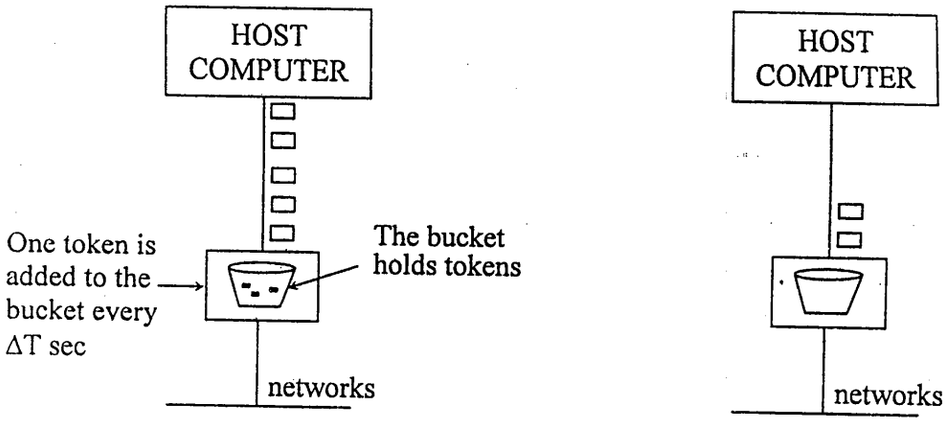


(a) A leaky bucket with water **(b) A leaky bucket with packet**

- A bucket with a small hole.
- No matter at what rate water enters the bucket, the outflow is at constant rate, S, when there is any water in the bucket and zero when bucket is empty.
- Once the bucket is full, any additional water entering it spills over the sides and it lost.
- Each host is connected to the network by an interface containing a leaky bucket (i.e. a finite internal queue)
  This arrangement can be built into the network interface or simulated by the host O.S. The host is allowed to put one packet per clock tick on the network.

1. When the packets are all of the same size at every clock tick, one packet is transmitted.
2. When variable size packets are used
   a. At every 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.
   b. Additional packets may also be sent, as long as the counter is high enough.
   c. 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 overwritten and lost.

Token bucket algorithm :



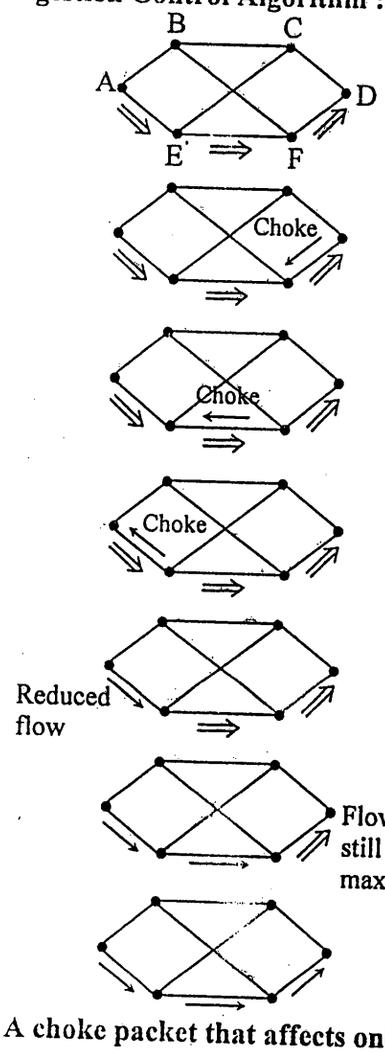
(a) Before **(b) After**

- The leaky bucket algorithm enforces a rigid output pattern at the average rate, no matter how bursty the traffic is.
- For many applications, it is better to allow the output to speed up somewhat when large bursts arrive. Hence we go for token bucket algorithm.
- The leaky bucket holds tokens generated by a clock at the rate of one token every ΔT sec. Form fig (a), the bucket holds the three tokens, with five packets waiting to be transmitted. For a packet to be transmitted it must capture and destroy one token. From fig.(b), the three of five packets have got through, but the other two are waiting for two more tokens to be generated.

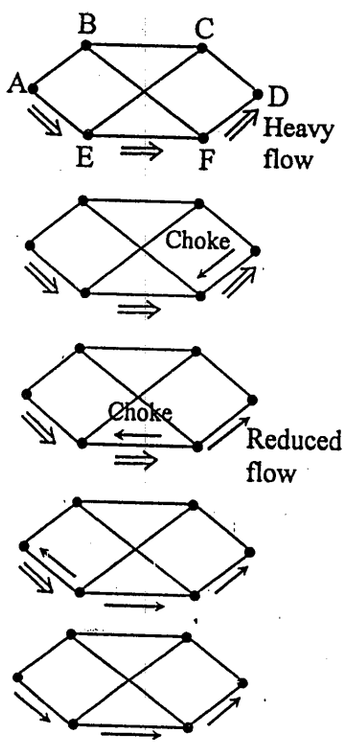
Difference between Leaky bucket and Token bucket :

1. The leaky bucket does not allow idle host to save up permission to send large bursts later.
   The token bucket allows saving up to maximum size of bucket 'n'
2. The leaky bucket discards packet when the bucket fills up.
   The token bucket throws away token when the bucket fills up but never discards packets.

Congestion Control Algorithm :



(a) A choke packet that affects only the source



(b) A choke packet that affects each hop it passes through

1. *Choke packets* :

- Each router can monitor the utilization of its output lines.
  e.g. $\mu_{new} = a\,u_{old} + (1-a)f$
  where μ = utilization between 0 and 1
  a = how fast router forgets recent history.
  f = sample of instantaneous line utilization.
- When 'μ' moves above threshold output line enter a "warning" state.
- Each newly arriving packet is checked to see if its output line is in warning state. If so router sends choke packet back to source host.
- The original packet is tagged so that it will not generate any more choke packets further along the path.

2. *Hop by hop choke packets* :

- At high speeds and over long distance, sending a choke packet to the source host does not work well because the reaction is very slow.
- An alternative approach is to have the choke packet take effect at every hop it passes through.
- The net effect of hop–by–hop scheme is to provide quick relief at the point of congestion at the price of using up more buffers upstream.

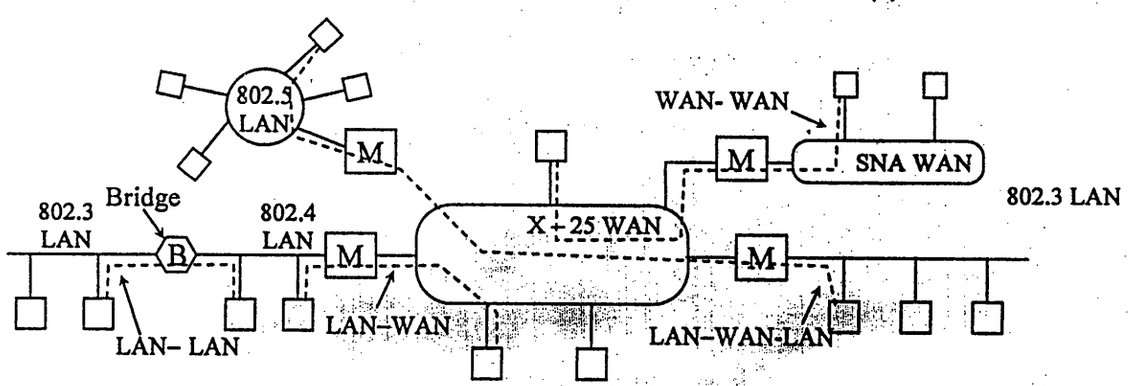
Load Shedding :

- There are two ways of controlling congestion
  (1) Reduce load (2) Increase resources.
- In load shedding, load is reduced by dropping packets at random.
- There is one more approach of providing intelligence so that packets are not dropped at random.
- For file transfers it is better to drop new packets than the old (wine) e.g. If 6 is dropped, receiver may force 6–10 to be retransmitted.
- For multimedia it is better to drop old packets than the new ones (milk)
  Certain algorithms for compressing video first send entire frame and then differences are sent. Difference frame is more important than the entire frame.
- To implement this intelligent discard policy, applications must mark their packets in priority classes to indicate how important they are.

INTERNETWORKING

2 or more networks together form an internet. Four types of connections are as follows

(a) LAN–LAN (b) LAN–WAN (c) WAN–WAN (d) LAN–WAN–LAN



It is necessary to insert a "black box" at the junction between 2 networks to handle the necessary conversions as packets more from one network to another. The name used for the black box connecting two networks depends on the layer that does the work. Some common names are given below.

Layer 1 : Repeaters

Layer 2 : Bridges store & forward data link frames between LAN's

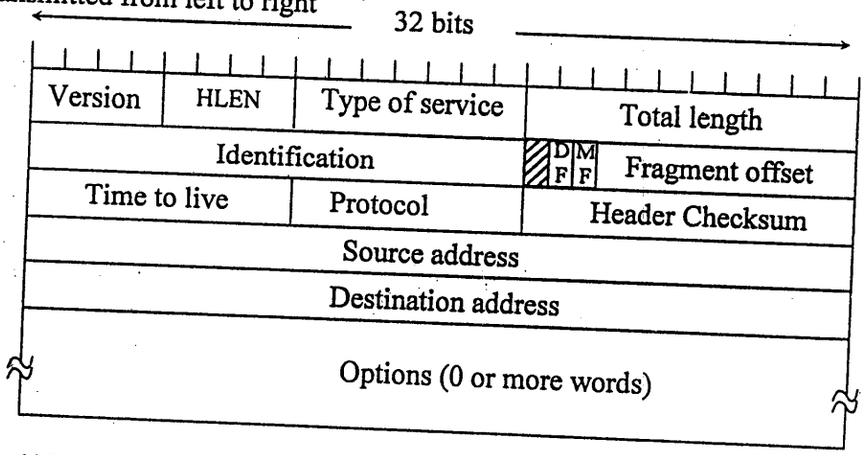
Layer 3 : Multiprotocol routers forward packets between dissimilar networks.

Layer 4 : Transport gateways connect byte streams in the transport layer.

Above 4 : Application gateways allow internetworking above layer 4.

The network layer in the internet –
IP protocol –

- IP datagram consists of header part and text part.
  HEADER has 20 byte FIXED PART and variable length OPTIONAL PART.
- The header format is shown as follows –
  It is transmitted from left to right

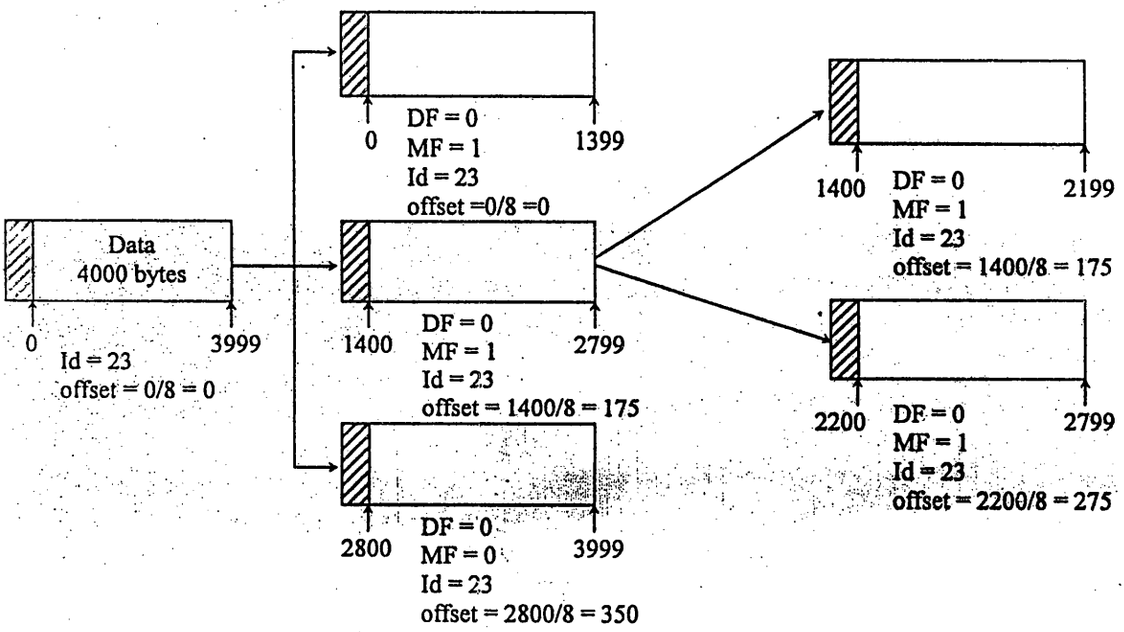


- **Version (4 bit) :** keeps track of which version of the protocol the datagram belongs to
- **HLEN (4 bit):** ∴Header length is not constant, HLEN gives header length min. value is 5 which applies when options are not present. Maximum value for 4 bit field is 15 which limits header to 60 bytes and thus option field to 40 bytes.
  Header length can be calculated as 4 * HLEN
- **Service Types(8bit):**To tell the host what kind of service he wants various combinations of reliability and speed are possible. The field contains 3 bit precedence field, three flags D, T & R & 2 unused bits. Precedence field (priority) from 0 (normal) to 7 (network control packet)
  The three flag bits allow the host to specify what is cares most about from the set (Delay, throughout, Reliability) In practice current routes ignore this field.
- **Total length (16 bits):**Total length = header + data. Max length = 65535 bytes.
- **Identification(16 bits):** Identification field is needed to allow the destination host to determine which datagram a newly arrived fragment belongs to
  All the fragments of a datagram contain the same Identification value.
- **DF:** Don't fragment. It is an order to the routers hot to fragment the datagram because the destination is incapable of putting the pieces back together.
- **MF:** More fragments. All fragments except the last one have this bit set. It is needed to know when all fragments of datagram have arrived.
- **Fragment offset(13 bits) :** Tells where in the current datagram this fragment belongs . All fragments except the last one in a datagram must be a multiple of 8 bytes. Since 13 bits are provided, there is maximum of 8192 fragments / datagram.
- **Time to live(8 bits):** Counter used to limit packet lifetime. It is supposed to count time in seconds, allowing a max lifetime of 255 sec. It must be decremented on each hop and is supposed to be decremented multiple times when queued for a long time in a router.
  When it hits zero, packet is discarded 4 war4ning packet is sent back to the source host
- **Protocol(8 bits):** Protocol tells it which transport process to give it to

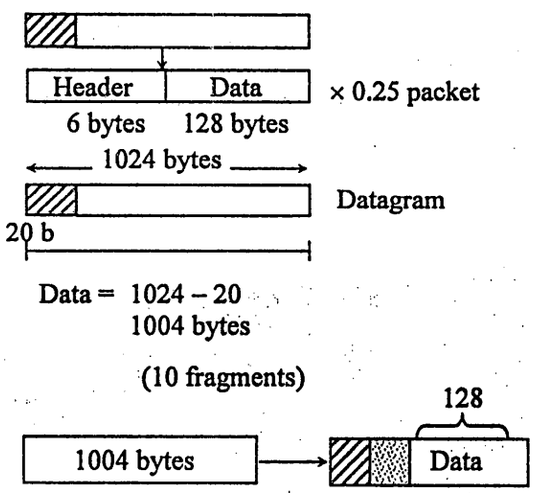
Value	Protocol
1	ICMP
2	IGMP
6	TCP
17	UDP
41	IPV6

- **Header checksum(16 bits) :**It verifies header only. It has to be recomputed at every hop since at least one field i.e. time to live changes. The error detection method used by IP is the check sum..
- **Source address :**This 32 bits field defines the IP address of the source .This field must remain unchanged during the time the IP datagram travels from the source to destination.
- **Destination address :**This 32 bits field defines the IP address of the destination. This field must remain unchanged during the time the IP datagram travels from the source to destination.
- **Options:** Options field is padded with a multiple of 4 bytes.

IP encapsulation , fragmentation and Reassembly
Maximum transfer unit (MTU)

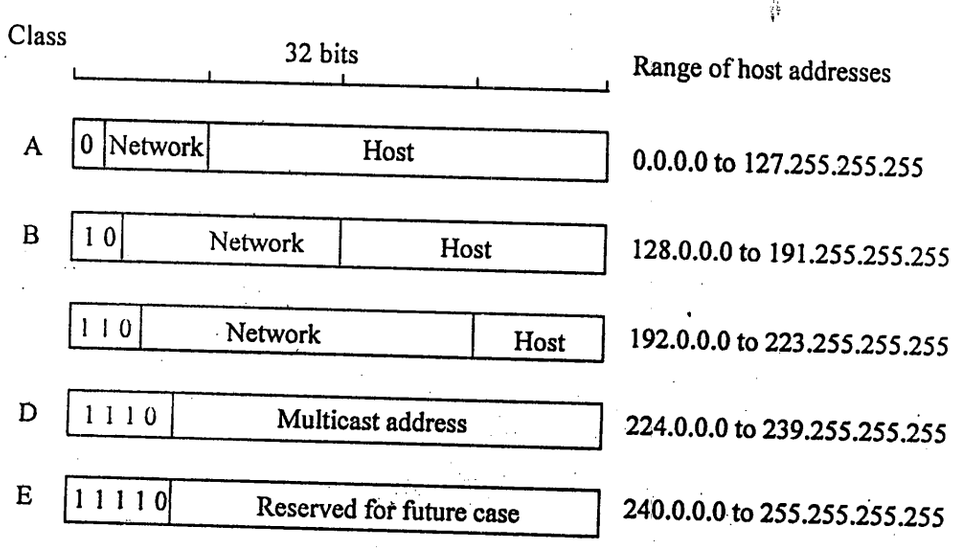


- An IP datagram of 1024 bytes is fragmented into pieces. Each piece is sent as a separate fragment over **X.25** network whose packet size allows 128 bytes of data per packet. How many fragments are needed and what is the efficiency of TX counting both X.25 and IP packet overhead ?



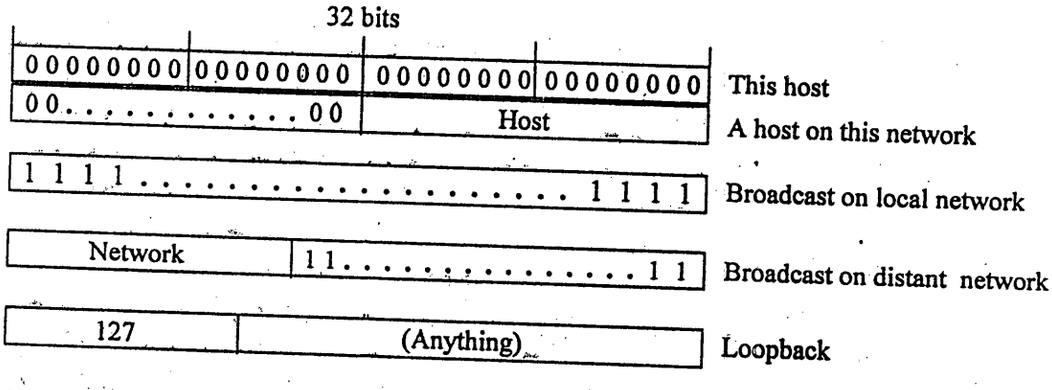
IP addresses :

- Each host and routes on the Internet has an IP address which encodes its network no. and host no.
- No. 2 m/c's have same IP address
- All IP addresses are 32 bit long (4 bytes)



- Network numbers are assigned by NIC (Network information center) to avoid conflicts.
  Lowest IP address – 0.0.0.0
  Highest IP address – 255.255.255.255
  0 → This network or this host
  1 → All hosts on indicated network

Special IP addresses

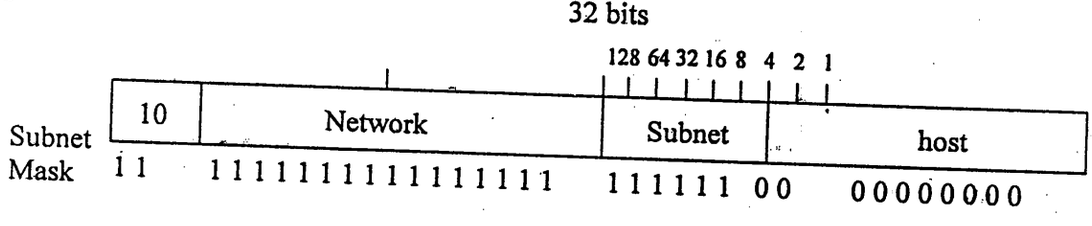


* 0.0.0.0 is used by host when they are being boated and not afterwards
* 127 . xx.yy.zz are reserved for loop black testing

Subnets

A single network is split up into several parts for internal use but still act as a single network to the outside world. These parts are called as subnets
To find which network the dest. address belongs to the router has to do a Boolean AND with the subnet mask–of the network

e.g.



e.g. 130·50·4·1 first subnet
8 second subnet
12 third subnet

packet addressed to 130.50.15.8 arriving at a router is ANDED with the subnet mask 255.255 255.255.252.0 to give the address 130.50.12.0. This address is looked up in the routing table to find out how to get to hosts on subnet no.3 i.e. 12.

Routing protocols (RIP, OSPF, BGP)

- Created for dynamic routing tables
- Definition RP is a combination of rules and procedure that let routers in the internet inform each other of changes.

⇒ Interior and Exterior routing

- An autonomous system (AS) is a group of networks and router under the authority of single administration.
- Routing inside the AS is called interior routing. Routing between AS is called exterior routing

⇒ Routing information protocol (RIP) is an interior routing protocol used inside AS.
It is based on Distance vector routing which uses Bellman Ford algo.

Timers in RIP :

1. **Periodic timers :** Regular update messages
   Timer value = 30sec (practically)
   working model uses random no. between 25 and 35 sec to prevent overload on the internet if all routers update simultaneously.
2. **Expiration timer :** validity of a route
   When a route info is updated expiration timer is set to 180 sec for that route. Energy time a new update for the route is received timer is reset.
   In case no update is received within 180 sec the route is considered expired and the hop count of the route is set to 16 which means destination is unreachable.
3. **Garbage collection timer :**
   When a route expires the router does not immediately remove it but continues to advertise it with metric value 16. At the same time garbage collection timer is set to 120 sec for that route. When the count reaches zero, route is removed from the table.
   This timer allows neighbors to become aware of the invalidity of the route.

OSPF

- Open shortest path first is interior routing protocol
- It uses link state routing

BGP

- Border gateway protocol is an inter–autonomous system routing protocol which is based on path vector routing
- Each entry in the routing table contains the destination network, the next router and the path to reach the destination. The path is usually defined as an ordered list of AS that a packet should travel to reach the destination.

Internet Multicasting

IP supports multicasting, using class D addresses. Each class D address identifies a group of hosts. Twenty–eight bits are available for identifying groups, so over 250 million groups can exist at the same time. When a process sends a packet to a class D address, a best–efforts attempt is made to deliver it to all the members of the group addressed, but no guarantees are given. Some members may not get the packet.

Two kinds of group addresses are supported: permanent addresses and temporary ones. A permanent group is always there and does not have to be set up. Each permanent group has a permanent group address. Some examples of permanent group addresses are:

224.0.0.1 All systems on a LAN
224.0.0.2 All routers on a LAN
224.0.0.5 All OSPF routers on a LAN
224.0.0.6 All designated OSPF routers on a LAN

Temporary groups must be created before they can be used. A process can ask its host to join a specific group. It can also ask its host to leave the group. When the last process on a host leaves a group, that group is no longer present on the host. Each host keeps track of which groups its processes currently belong to.

Multicasting is implemented by special multicast routers, which may or may not be colocated with the standard routers. About once a minute, each multicast routers sends a hardware (i.e., data link layer) multicast to the hosts on its LAN (address 224.0.0.1) asking them to report back on the groups their processes currently belong to. Each host sends back responses for all the class D addresses it is interested in.

Multicast routing is done using spanning trees. Each multicast routers exchanges information with its neighbors, using a modified distance vector protocol in order for each one to construct a spanning tree per group covering all group members.

Mobile IP

Many users of the Internet have portable computers and want to stay connected to the Internet when they visit a distant Internet site and even on the road in between.

Every IP address contains a network number and a host number. For example, consider the machine with IP address 160.80.40.20/16. The 160.80 gives the network number (8272 in decimal); the 40:20 is the host number (10260 in decimal). Routers all over the world have routing tables telling which line to use to get to network 160.80. Whenever a packet comes in with a destination IP address of the form 160.80.xxx.yyy, it goes out on that line.

If all of a sudden, the machine with that address is carted off to some distant site, the packets for it will continue to be routed to its home LAN (or router). The owner will no longer get e–mail, and so on. Giving the machine a new IP address corresponding to its new location is unattractive because large numbers of people, programs, and databases would have to be informed of the change.

Another approach is to have the routers use complete IP addresses for routing, instead of just the network. However, this strategy would require each router to have millions of table entries, at astronomical cost to the internet.

When people began demanding the ability to connect their notebook computers to the Internet wherever they were, IETF (Internet Engineering Task Force) set up a Working Group to find a solution. The Working Group quickly formulated a number of goals considered desirable in any solution. The major ones were :

1. Each mobile host must be able to use its home IP address anywhere.
2. Software changes to the fixed hosts were not permitted.
3. Changes to the router software and tables were not permitted.
4. Most packets for mobile hosts should not make detours on the way.
5. No overhead should be incurred when a mobile host is at home.

The solution chosen was as described: Every site that wants to allow its users to roam has to create a home agent. Every site that wants to allow visitors has to create a foreign agent. When a mobile host shows up at a foreign site, it contacts the foreign host there and registers. The foreign host then contacts the user's home agent and gives it a **care–of address**, normally the foreign agent's own IP address.

When a packet arrives at the user's home LAN, it comes in at some router attached to the LAN. The router then rises to locate the host in the usual way, by broadcasting an ARP packet asking, for example: What is the Ethernet address of 160.80.40.20? The home agent responds to this query by giving its own Ethernet address. The router then sends packets for 160.80.40.20 to the home agent. It, in turn, tunnels them to the care–of address by encapsulating them in the payload field of an IP packet addressed to the foreign agent. The foreign agent then decapsulates and delivers them to the data link address of the mobile host. In addition, the home agent gives the care–of address to the sender, so future packets can be tunneled directly to the foreign agent. This solution meets all the requirements stated above.

IPv6

The main features of IPv6 are discussed below.

First and foremost, IPv6 has longer addresses than Ipv4. They are 16 bytes long, which solves the problem that IPv6 set out to solve: provide an effectively unlimited supply of Internet addresses.

The second major improvement of Ipv6 is the simplification of the header. It contains only seven fields (versus 13 in IPv4). This change allows routers to process packets faster and thus improve throughput and delay.

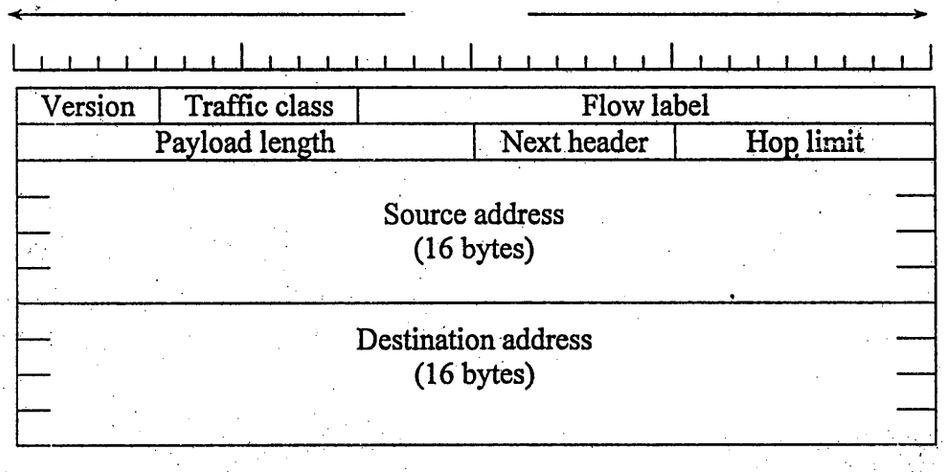
The third major improvement was better support for options. This change was essential with the new header because fields that previously were required are now optional. In addition, the way options are represented is different, making it simple for routers to skip over options not intended for them. This feature speeds up packet processing time.

A fourth area in which IPv6 represents a big advance is in security.

The Main IPv6 Header

The IPv6 header is shown in following figure. The Version field is always 6 for Ipv6 (and 4 for IPv4).

The *Traffic class* field is used to distinguish between packets with different real–time delivery requirements. A field designed for this purpose has been in IP since the beginning, but it has been only implemented by routers.



The *Flow label* field is also still experimental but will be used to allow a source and destination to set up a pseudoconnection with particular properties and requirements. For example, a stream of packets from one process on a certain source host to a certain process on a certain destination host might have stringent delay requirements and thus need reserved bandwidth. The flow can be set up in advance and given an identifier. When packet with a nonzero *Flow label* shows up, all the routers can look it up in internal tables to see what kind of special treatment it requires. In effect, flows are an attempt to have it both ways: the flexibility of a datagram subnet and the guarantees of a virtual–circuit subnet.

The *Payload* length field tells how many bytes follow the 40–byte header of above figure. The name was changed from the IPv4 *Total length* field because the meaning was changed slightly : the 40 header bytes are no longer counted as part of the length.

The *Next header field* tells which of the (currently) six extension headers, if any, follow this one. If this header is the last IP header, the *next header field* tells which transport protocol handler (e.g.TCP, UDP) to pass the packet to.

The *Hop limit* field is used to keep packets from living forever. It is, in practice, the same as the *Time to live* field in IPv4, namely, a field that is decremented on each hop.

Source & Destination address

Source & Destination address are fixed – length 16–bytes addresses.

A new notation has been devised for writing 16–byte addresses. They are written as eight groups of four hexadecimal digits with colons between the groups, like this :

8000:0000:0000:0000:0123:4567:89AB:CDEF

Since many addresses will have many zeros inside them, three optimizations have been authorized. First, leading zeros within a group can be omitted, so 0123 can be written as 123. Second, one or more groups of 16 zero bits can be replaced by a pair of colons. Thus, the above address now becomes

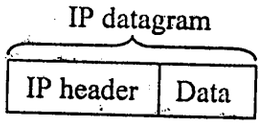
8000::123:4567:89AB:CDEF

Related Questions :

1. Write SN on congestion and congestion control in computer network.
2. Explain shortest path routing with illustration.
3. Explain in brief, concatenated virtual circuits.
4. Explain any one routing algorithm with the merit over other routing algorithm.
5. What is congestion and congestion prevention policies?
6. What is inter–networking? Explain the different relays used in it.
7. Explain the frame format of IP datagram when a minimum size IP datagram travels across an Ethernet, how large is the Ethernet frame?

Soln.: • Give IP frame format and explain

• IP datagram is given by



minimum size of IP datagram is when data is not present.

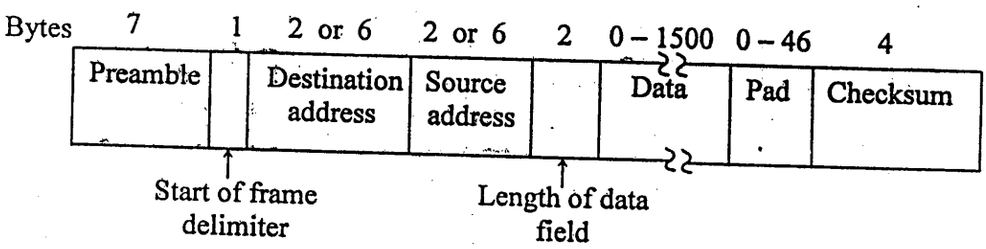
Hence min. size = min. header size

∵ Min. header size = fixed header part

= 20 bytes

Hence min. size of IP datagram is 20 bytes.

IEEE standard 802.3 is Ethernet whose frame format is :



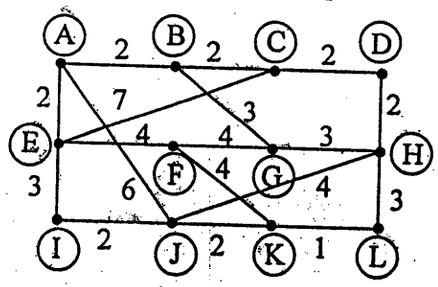
Our IP datagram is placed in "Data" field. The total size of the frame after inserting 20 bytes IP datagram is 38 bytes which is less than 64 bytes (i.e. min frame size for 802.3)

802.3 states that valid frames must be atleast 64 bytes long hence frame is padded with Pad bits to give 64 byte frame.

Hence Ethernet frame is 64 bytes long.

8. An IP datagram of 1024 bytes is fragmented into pieces. Each piece is sent as a separate fragment over an X.25 network whose packet size allowed is 128 bytes of data per packet. How many fragments are needed and what is the efficiency of transmission, counting both the X.25 and IP packet overhead but ignoring that of lower layers.

9. Find the shortest path between E and H by applying any one algorithm (Clearly specify one which you are using). Show each steps output.



Soln. : Dijkstra's shortest path algorithm is used.

Step	S	W	Cost functions												Prior functions										
			X	A	B	C	D	F	G	H	I	J	K	L	A	B	C	D	F	G	H	I	J	K	L
1	{E}	{A,C,F,I}	A	2	∞	7	∞	4	∞	∞	3	8	∞	∞	E	–	E	–	E	–	–	E	–	–	–
2	{E,A}	{B,C,F,I,J}	I	2	4	7	∞	4	∞	∞	3	8	∞	∞	E	A	E	–	E	–	–	E	A	–	–
3	{E,A,I}	{B,C,F,J}	B	2	4	7	∞	4	∞	∞	3	5	∞	∞	E	A	E	–	E	–	–	E	I	–	–
4	{E,A,B,I}	{C,F,J,G}	F	2	4	6	∞	4	7	∞	3	5	∞	∞	E	A	B	–	E	B	–	E	I	–	–
5	{E,A,B,I,F}	{C,J,G,K}	J	2	4	6	∞	4	7	∞	3	5	9	∞	E	A	B	–	E	B	–	E	I	F	–
6	{E,A,B,I,F,J}	{C,G,K,H}	C	2	4	6	∞	4	7	9	3	5	7	∞	E	A	B	–	E	B	J	E	I	J	–
7	{E,A,B,I,F,J,C}	{G,K,H,D}	G	2	4	6	8	4	7	9	3	5	7	∞	E	A	B	C	E	B	J	E	I	J	–
8	{E,A,B,I,F,C,G}	{K,H,D}	K	2	4	6	8	4	7	9	3	5	7	∞	E	A	B	C	E	B	J	E	I	J	–
9	{E,A,B,I,F,C,G,K}	{D,H,L}	D	2	4	6	8	4	7	9	3	5	7	8	E	A	B	C	E	B	J	E	I	J	K
10	{E,A,B,I,F,C,G,K,D}	{H.L}	L	2	4	6	8	4	7	9	3	5	7	8	E	A	B	C	E	B	J	E	I	J	K
11	{E,A,B,I,F,C,G,K,D,L}	{H}	H	2	4	6	8	4	7	9	3	5	7	8	E	A	B	C	E	B	J	E	I	J	K
12	{A,B,C,D,E,F,G,H,I,J,K,L}	{ }	–	2	4	6	8	4	7	9	3	5	7	8	E	A	B	C	E	B	J	E	I	J	K

Destination → H Min. cost = 9
Shortest path : H → J → I → E
The actual path from E to H is E → I → J → H

10. What is congestion? Explain the working of discarding congestion control algorithm. Also give its merits and demerits.

11. List special IP addresses.

12. List idea of Link State routing in five steps.

13. What is internetworking? Identify the devices needed to achieve such a network and clearly illustrate the addressing mechanism employed at various layers of the OSI model.

14. With suitable examples, explain IP addressing scheme.

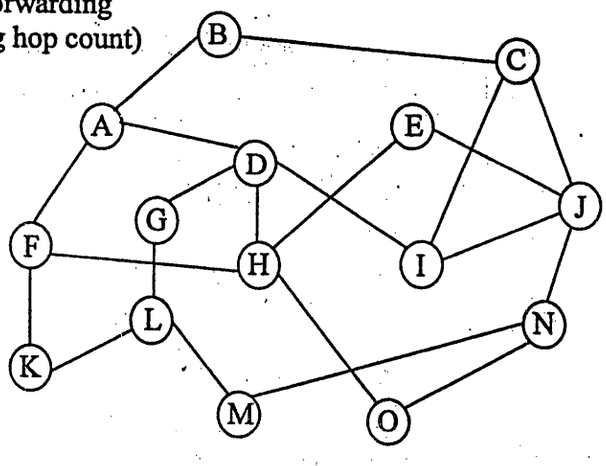
15. Just brief about data structure used for Dijkstra's shortest path algorithm.

Soln.:

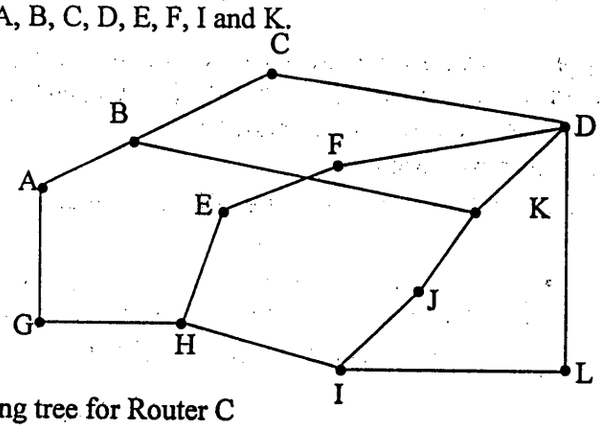
```
# define MAX_NODES 1024          /*maximum no. of nodes*/
# define INFINITY 1000000000          /*a no. larger than every maximum path */
int n, dist[MAX_NODES] [MAX_NODES] ;
                        /* dist [i] [j] is the distance from i to j   */

void shortest path (int s, int t, int path[])
{ struct state                  /* the path being worked on*/
  { int predecessor ;               /*  previous node   */
    int length ;                /*  length from source to this node   */
    enum {permanent, tentative} label ;       /* label state */
} state[MAX_NODES] ;
int i, k, min ;
struct state * p ;
```

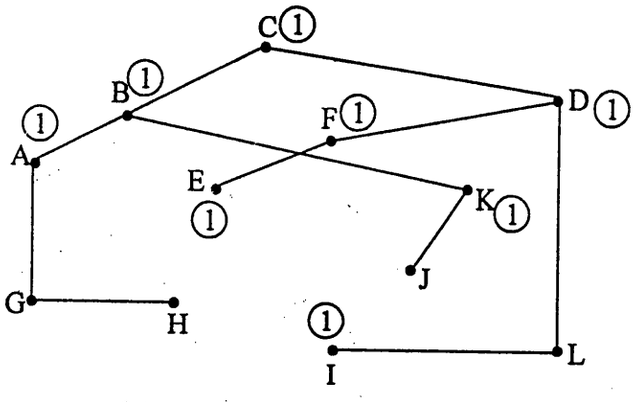
16. Consider the following subnet, how many packets are generated by a broadcast from B.
using (1) Reverse path forwarding
(2) Sink tree (using hop count)



17. Compute a multicast spanning tree for router C in the subnet below for a group with members at routers A, B, C, D, E, F, I and K.

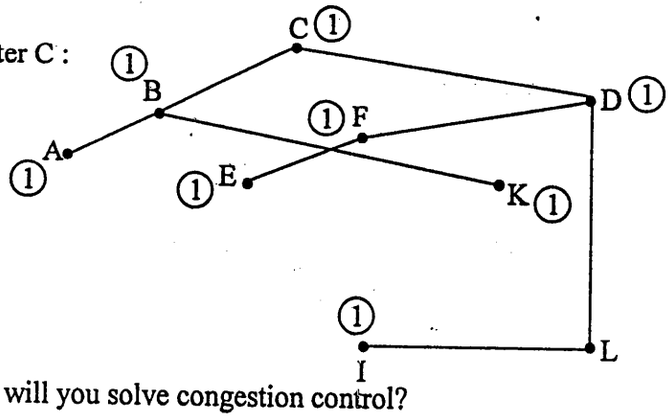


Soln. : Spanning tree for Router C



(1) indicates the group of A, B, C, D, E, F, I and K

• Multicast tree for Router C :



18. Explain in brief how will you solve congestion control?
19. Write SN on datagram.
20. Write SN on Routers and gateway.
21. Explain IP subnetting with example.
22. Consider two adjacent routers K and J in a network that runs RIP. Router K's routing table and the routing update from router J are as shown below. Give router K's routing table after it incorporates update from J.

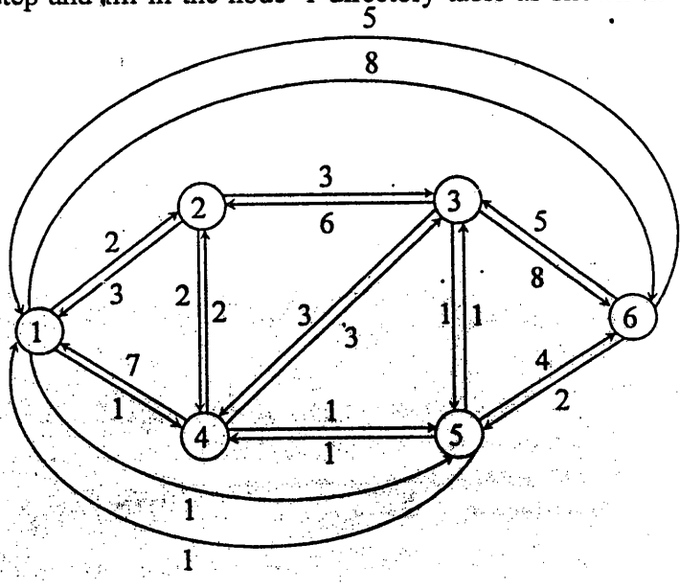
K's Routing table		
Destination	**Distance**	**Line**
Net 1	0	Direct
Net 2	0	Direct
Net 4	8	Router L
Net 17	5	Router M
Net 24	6	Router J
Net 30	2	Router Q
Net 42	2	Router J

Update from J	
Destination	**Distance**
Net 1	2
Net 21	4
Net 4	3
Net 17	6
Net 24	5
Net 30	10
Net 42	3

23. Consider Ethernet 802.3 DLL. Consider standard TCP/IP. Transport layer has 3500 bytes stream which has to be given to IP. Packet ID is 3297. Show different fragmentation, calculations with diagrams.

24. Just state the reasons and solutions of congestion in network. Is infinite buffers in routers a problem or solution. Justify.
25. Draw and label the diagram showing internetworking of LAN's and WAN's with IP and MAC addresses. Consider some routers network. Briefly tell how packet is delivered from source to destination on local segment and distant network.
26. Explain the steps involved in Dijkstra's algorithm.
27. Explain fixed routing, Flooding and adaptive routing strategies with their advantages and disadvantages.
28. Using Dijkstra's algorithm generate a least–cost path to all other nodes for node S = 1 for the packet switched network as shown in the figure. Display the results for each iteration in the tabular form using sketches for each step and fill in the node–1 directory table as shown in figure Node – 1 Directory :

Destination	Next Node
2	
3	
4	
5	
6	



29. Write SN on IP frame format.

□□□□□□

Quality of Service

The transport service may allow the user to specify preferred, acceptable and minimum values for various service parameters at the time a connection is set up.

It is upto the transport layer to examine these parameters and depending on the kind of network service is available to it, determine whether it can provide the required service.

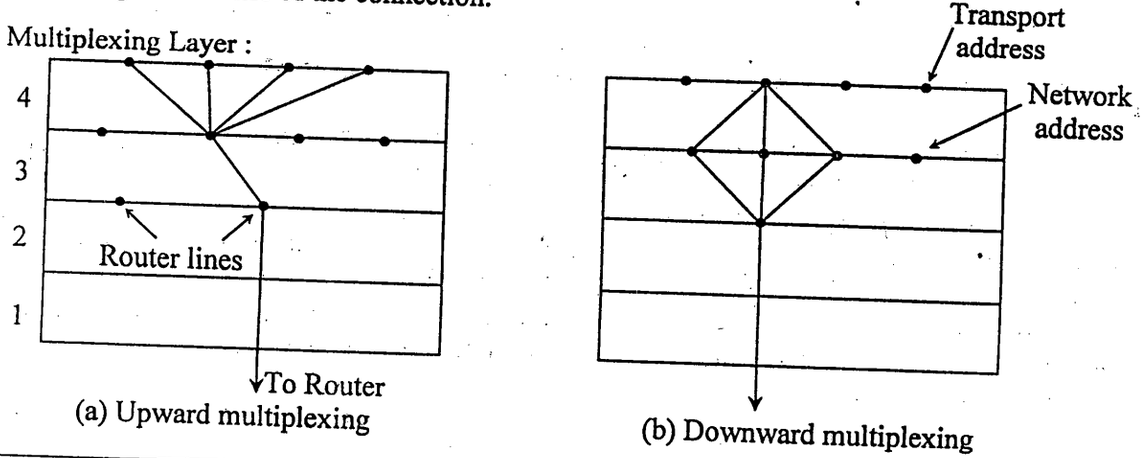
* Typical transport layer quality of service parameters

Connection establishment delay
Connection establishment failure probability
Throughput
Transit delay
Residual error ratio
Protection
Priority
Resilience

* Connection establishment delay is the amount of time elapsing between a transport connection being requested and the confirmation being received by the user of the transport service. Shorter the delay better the service
* Connection establishment : failure probability is the chance of connection not being established within the maximum establishment delay time eg. due to network congestion, lack of table space somewhere, etc.
* Throughput – It measures no. of bytes of user data transferred per sec, measured over some time interval. Throughput is measured separately for each direction.
* Transit delay time between message being sent by the transport user on the source machine and it being received by the transport user on the destination machine. Each direction is handled separately.
* Residual error ratio number of lost or garbled messages as a fraction of the total sent. In theory it should be zero since it is the job of the transport layer to hide all network layer errors. In practice it may have some finite value.
* Protection provides a way for the transport user to specify interest in having the transport layer provide protection against unauthorized third parties reading on modifying the transmitted data.
* Priority – indicates that some of its connections are more important than others and in case of congestion high priority connections get serviced before low priority ones.
* Resilience – gives the probability of transport layer itself spontaneously terminating a connection due to internal problems or congestion.

The QOS parameters are specified by the transport user when a connection is requested. Both the desired and minimum acceptable values can be given

* When the transport layer knows it cannot achieve even acceptable goal it tells the caller that connection attempt failed.
* If the connection is established, the values of the parameters are agreed upon. This is called OPTION NEGOTIATION. Once the options have been negotiated they remain that way throughout the life of the connection.



(a) Upward multiplexing

(b) Downward multiplexing

Multiplexing of different transport connections on to the same network connections is called UPWARD MULTIPLEXING

For high priority traffic, transport layer opens multiple network connections and distribute the traffic among them on a round robin basis such multiplexing is called DOWNWARD MULTIPLEXING

Internet Transport protocols (TCP & UDP)

Transmission control protocol (TCP) is a reliable end to end transport layer protocol
TCP is connection oriented
UDP is connectionless & unreliable
It is basically IP with a short header added.

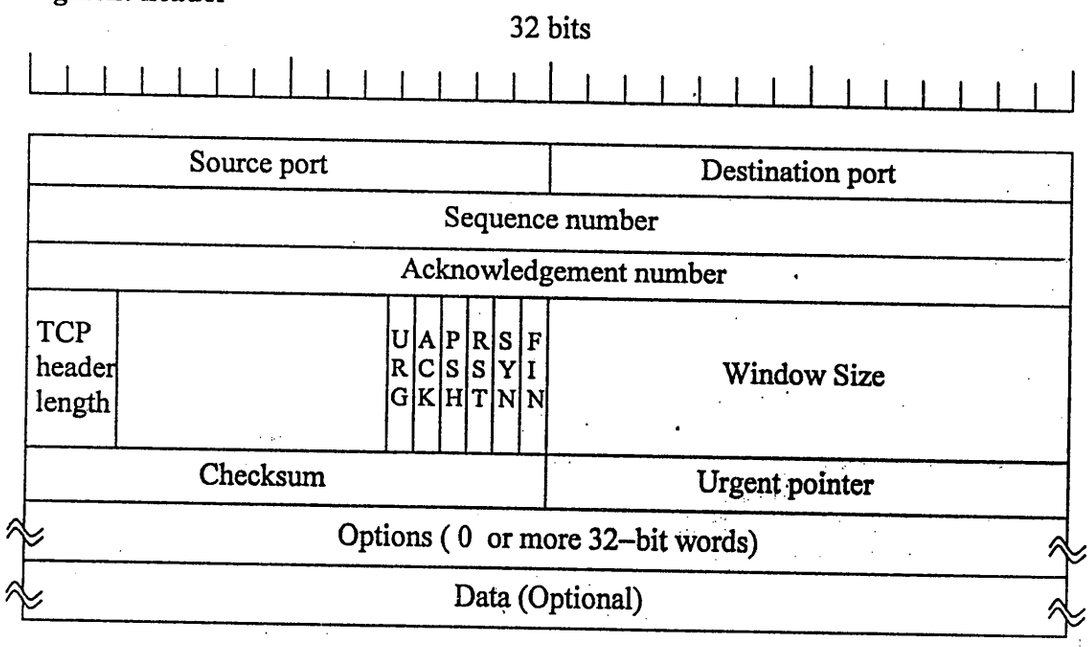
TCP service model

* TCP service is obtained by having both sender & receiver create end points called sockets.
* Each socket has socket number (address) consisting of the IP address of the host & a 16–bit number local to that host called a **port**. A port is TCP name for TSAP.
* Connections are identified by the socket identifiers at both ends i.e. (socket 1, socket 2)
* Ports below 1024 are called well known ports reserved for std. services
  eg. FTP 21
  TELNET 23
  Well known ports are given in PFC1700
* All TCP connections are full duplex and point to point

TCP protocol

* The sending and receiving TCP entities exchange data in the form of segments
* A segment consists of fixed 20 byte header followed by 0 or more data bytes
* It can accumulate data from several writes into one segment or split data from one write over multiple segments.
* Two limits restrict segment size
  (1) Each segment including TCP header must fit in 65,535 byte IP payload.
  (2) Maximum transfer unit (MTU)
* The basic protocol used by the TCP entities is sliding window protocol.

TCP segment header



* Source port & Destination port – These fields identify the local endpoints of the connection.
  A port plus its host's IP address forms a 48–bit unique TSAP.
  Src & destination socket numbers together identify the connection.
* Sequence number & Acknowledgement number perform their usual functions.
  Acknowledgement Number specifies the next byte expected.
* TCP header length tells how many 32 bit words are contained in the TCP header. This information is needed because options field is of variable length so is header too.
  It indicates start of data.

* Six 1 bit flags.
  URG = 1 if urgent pointer is in use
  Urgent pointer is used to indicate a byte offset from the current sequence number at which urgent data are to be found.
* ACK = 1 to indicate acknowledgement number is valid else it is ignored i.e. piggypacking not used.
* PSH bit indicates pushed data.
  The receiver is requested to deliver the data to the application upon arrival & not buffer it until a full buffer has been received (which it might otherwise do for efficiency reasons).
* RST bit is used to reset a connection that has become confused due to a host crash or some other reason.
* SYN bit is used to establish connections
  Connection Request – SYN = 1 & ACK = 0 to indicate piggyback acknowledgement field is not in use.
  Connection Reply = SYN = 1 & ACK = 1 since it does bear an acknowledgement.
* F/N bit is used to release a connection
  It specifies that the sender has no more data to transmit.
  However after closing the connection a process may continue to receive indefinitely. Both SYN & FIN segments have sequence numbers and are thus guaranteed to be processed in correct order.
* Window size of 0 is legal saying that the receiver is currently badly in need of rest and would like no more data for the moment.
* Checksum – for extreme reliability. It checksums the header, data and conceptual pseudo header. When performing this computation, TCP checksum field is set to zero and data field is padded out with additional zero byte if the length is an odd number.
  The checksum algo is simply to add up all the 16–bit words in 1's complement and then to take the 1's complement of the sum.
  As a consequence when the receiver performs the calculation on entire segment, including checksum field, the result should be zero.

32 bits

Source address		
Destination address		
00000000	Protocol = 6	TCP segment length

The pseudo header contains 32 bit IP address of the source & destination machines, protocol number for TCP (6), byte count for TCP segment (including header).

* Options field was designed to provide a way to add extra facilities not covered by the regular header.

UDP (User data protocol)

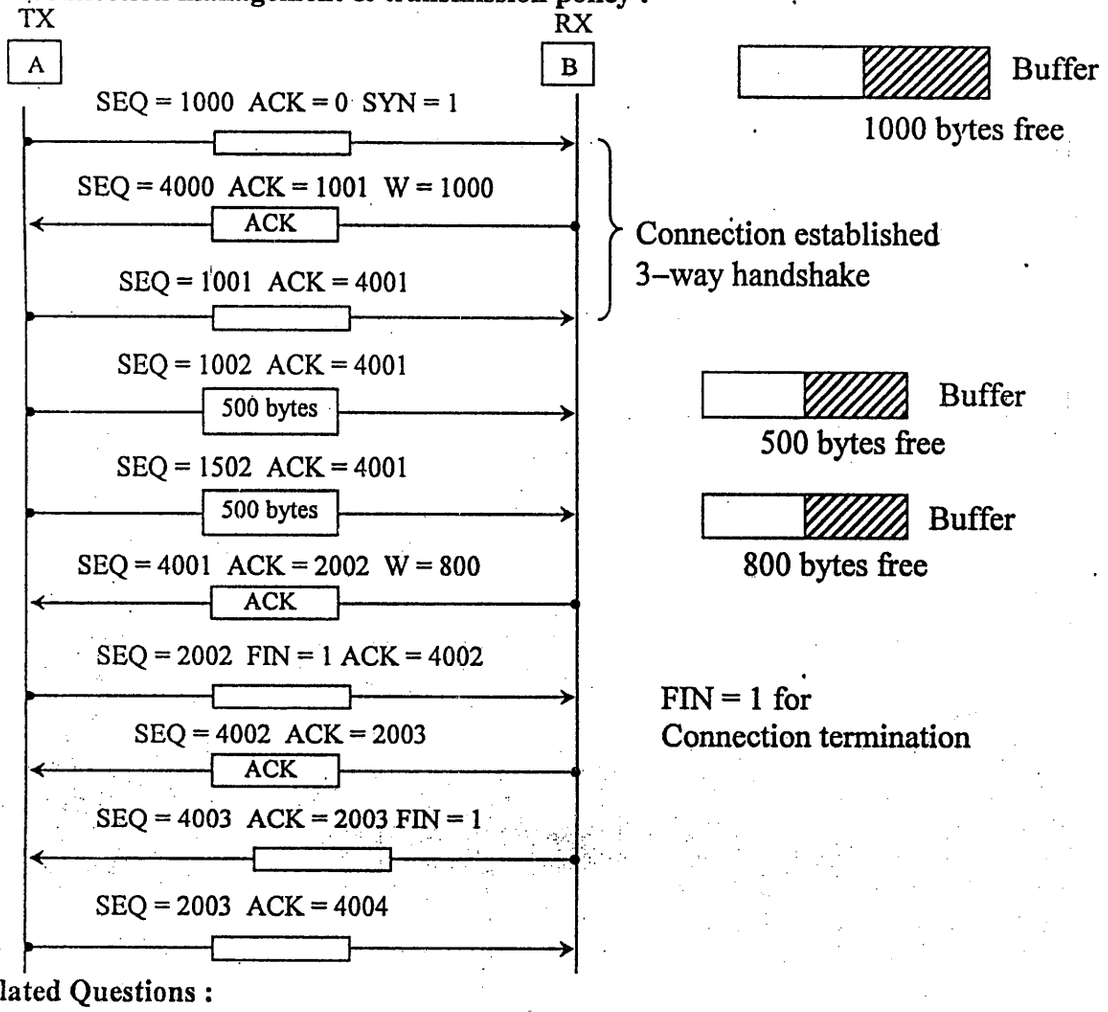
* Connectionless transport protocol

32 Bits

Source port	Destination port
UDP length	UDP checksum

* UDP segment consists of 8 byte header followed by data.
* UDP length field includes 8 byte header and data
* UDP checksum includes the same format pseudoheader, UDP header and UDP data padded out to an even number of bytes if need by. It is optional and stored as 0 if not computed.

TCP connection management & transmission policy :



Related Questions :

1. Write a SN on TCP/IP
2. Describe the transport layer quality of service parameters in detail.
3. Explain how acknowledgements are implemented in TCP?
4. What are the different services provided to session layer and network layer services used by the transport layer? Also specify the parameters that examine the quality of service.
5. Explain different TCP flags.
6. Why does UDP exists? Would it not have been enough to gist let user processes and Raw IP packets ?

Soln.: No, it is not just enough to let user processes send Raw IP packets.
This is because IP packets contain IP addresses which specify a destination machine.
But once a packet is arrived at the destination, how will the network handler know which processes to give it to.
UDP packet contains a destination port. This information is essential so they can be delivered to the correct process.

7. State TCP frame format and brief about it.
8. Consider a TCP client application that writes a small application header (8 bytes) followed by a small request (12 bytes). It then waits for a reply from the server. What happens if the request is sent using two writes. (8 bytes, then 12 bytes) versus a single write of 20 bytes?
9. If the TCP round trip time, RTT, is currently 30msec and the following acknowledgments come in after 26, 32 & 24 msec respectively, what is the new RTT estimate? Use $\alpha = 0.9$
10. What is the OBJECT IDENTIFIER for the TCP object?
11. Why are the source and destination port numbers at the beginning of the TCP header?

Soln. : Source and destination port numbers are required in TCP header to indicate the end points of the destination where the entire message has to be delivered correctly.
The source and destination port numbers are at the beginning of the TCP header because as soon as the header comes, the port number is checked and whatever comes after the port number is directly given to the process, whose port number is been identified.

12. Compare UDP and TCP protocol. List outlines of socket calls.
13. Why three way handshake is required for TCP?
14. Just give one line reason or use for each of the flags in TCP frame format (Not definition of flags)
15. Explain transport layer connection management.

□□□□□□

Ch.7 : The Application Layer

Electronic Mail

The attraction of electronic mail or email is that it is very fast. Email has the speed of the telephone without requiring both the parties be available at the same instant. It also leaves a written copy of the message that can be filed away or forwarded. Furthermore, a message can be sent to many people at once.

Electronic mail systems are constructed of two distinct but closely related parts:

- **User Agents**
  Providing the human interface (e.g. composition, editing and reading mail.)
- **Message Transfer Agents**
  For transporting mail (e.g. managing mailing lists and providing notification of delivery)

Email system supports five basic functions:-

Composition	Refers to the process of creating messages and answers
Transfer	Refers to moving message from the originator to the recipient
Reporting	To tell the originator what happened to the message. Was it delivered? Was it rejected? Was it lost?
Displaying	Incoming messages is needed to be displayed so people can read their email
Disposition	Concerned with what the recipient does with the message after receiving it

Additional to the basic services are mailbox, mailing list etc...

The User Agent

- **Sending Email**
  To send email message, a user must provide the message, the destination address and possibly some other parameters.
  The email address is in the format- username@domainname.

- **Reading Email**
  When the user agent is started up, it will look at the users mailbox for incoming email before displaying anything on the screen. Then it may announce the number of messages in the mailbox or display onetime summary of each message and wait for a command.

Message Formats

- RFC 822
  The user agent builds the message and passes it to the message transfer agent which then uses some of the header field to construct the actual envelope.
  RFC 822 header fields related to the message are:
  to cc bcc from sender subject return_path date reply_to message_id reference keywords

  In the message body user can put the text, ascii cartoons, political statements and disclaimers of all kinds.

- **MIME - Multipurpose Internet Mail Extensions**
  The basic idea of MIME is to continue to use the RFC 822 format, but to add structure to the message body and define the encoding rules for the non-ASCII messages. By not deviating from RFC 822 MIME messages can be send using existing mail programs and protocols.

  MIME defines five new message headers:-

Header	Meaning
MIME version	Identifies the MIME version
Content_Desc.	String telling what is in the message
Content_Id	Unique Identifier
Content_tranfer_encoding	How the body is wrapped for Xmssn
Content_type	Nature of the message (Text, image, audio, video, application, message)

Message Transfer Agent

The message transfer system is concerned with relaying messages from originator to the recipient.

- **SMTP (Simple Mail Transfer Protocol)**
  SMTP is the standard protocol for transferring mail messages between hosts in the TCP/IP suite; it is defined in RFC821. The messages transferred by SMTP follow the format of RFC822.

  SMTP is not concerned with the format or content of messages themselves with two exceptions:
  1) SMTP standardizes the message character set as 7-bit ASCII
  2) SMTP adds log information to the start of the delivered message that indicated the path the message took.

  SMTP uses information written on envelope of the mail (message header) but does not look at the contents (message body) of the envelope.

The SMTP can be used only to send messages that are composed using ASCII character set. MIME can be used to exchange email messages containing non-textual data such as graphics, sound and other multimedia files. The MIME encodes these files in a textual form that can be sent using the SMTP. The recipient can then decode MIME-encoded data to the original nontext file.

Final Delivery

Many companies have one or more email servers that can send and receive email. To send or receive messages, a PC must talk to an email server using some kind of delivery protocol.

POP3 (Post Office Protocol)
- Simple protocol for fetching email from remote mailbox.
- It is defined in RFC1225.
- It has commands for log in, log out, fetch messages and delete messages.
- POP3 is used to fetch email from the remote mailbox and store it on the user's local machine to be read later.
- The protocol itself consists of ASCII text.

IMAP (Interactive Mail Access Protocol)
- Sophisticated delivery protocol defined in RFC 1064.
- IMAP does not copy email to user's personal machine but the email server maintains a central repository that can be accessed from any machine.
- IMAP has the ability to address mail not by arrival number but by using attributes.

DMSP (Distributed Mail System Protocol)
- A part of PCMAIL system and defined in RFC 1056
- It does not assume that all email is on one server (as do POP3 and IMAP). It allows users to download email from the server to a workstation, PC or laptop and then disconnect.
- The email can be read and answered while disconnected. When connection occurs later, email is transferred and the system is resynchronized.

File Transfer Protocol (FTP)

File Transfer Protocol, usually called FTP, is a utility for managing files across machines without having to establish a remote session with Telnet. FTP enables you to transfer files back and forth, manage directories, and access electronic mail.

FTP uses two TCP channels.
TCP port 20 is the data channel, and port 21 is the command channel. FTP conducts all file transfers in the foreground, instead of the background. (In other words, FTP does not use spoolers or queues, so you are watching the transfer process in real time.) By using TCP, FTP eliminates the need to worry about reliability or connection management, because FTP can rely on TCP to perform these functions properly.

In FTP parlance, the two channels that exist between the two machines are called the *protocol interpreter,* or PI, and the *data transfer process,* or DTP. The PI transfers instructions between the two implementations using TCP command channel 21, and the DTP transfers data on TCP data channel 20.

- **FTP Third-Party Transfers**
  FTP enables a transfer to occur through a third machine positioned between the client and the server. This procedure is known as a ***third-party transfer*** and is sometimes necessary to obtain proper permissions to access the remote machine.

  When setting up a third-party connection, the client opens the control connections between the remote machine and the second client that handles the control channel. Only the control channel goes through the second client, whereas the data channel goes directly between the two ends.
  When a transfer request is submitted, it is transferred through the second client, which checks permissions and then forwards the request to the server. The data transfer can take place directly, because the permissions were checked on the control channel.

- **Anonymous FTP Access**
  FTP requires a user ID and password to enable file transfer capabilities, but there is a more liberal method of enabling general access to a file or directory, called ***anonymous FTP.*** Anonymous FTP removes the requirement for a login account on the remote machine, usually enabling the login anonymous with a password of either guest or the user's actual login name.

- **Trivial File Transfer Protocol (TFTP)**
  The Trivial File Transfer Protocol (TFTP) is one of the simplest file transfer protocols in use. It differs from

FTP in two primary ways:

- it does not log onto the remote machine, and
- it uses the User Datagram Protocol (UDP) connectionless transport protocol instead of TCP.

By using UDP, TFTP does not monitor the progress of the file transfer, although it does have to employ more complex algorithms to ensure proper data integrity. By avoiding logging onto the remote, user access and file permission problems are avoided. TFTP uses the TCP port identifier number 69, even though TCP is not involved in the protocol.

TFTP's Advantages over FTP :

It is not usually used for file transfers between machines where FTP could be used instead, although TFTP is useful when a diskless terminal or workstation is involved. Typically, TFTP is used to load applications and fonts into these machines, as well as for bootstrapping. TFTP is necessary in these cases because the diskless machines cannot execute FTP until they are fully loaded with an operating system. TFTP's small executable size and memory requirements make it ideal for inclusion in a bootstrap, where the system requires only TFTP, UDP, and a network driver, all of which can be provided in a small EPROM.

TFTP's Disadvantages over FTP :

1) TFTP transfers can fail for many reasons, because practically any kind of error encountered during a transfer operation causes a complete failure.
2) TFTP does support some basic error messages, but it cannot handle simple errors such as insufficient resources for a file transfer or even a failure to locate a requested file.

Virtual Terminal

Ordinarily, access to a host is gained through a terminal. Terminals are physically linked to the host. This physical connection is referred to as local access. Each host contains a software designed to provide an interface with the specific terminal types usually attached to it.

One of the attractions of networks is the ability to log on to a host to which your terminal is not directly linked. The users terminal is connected to a local host, which is in turn connected through a network to a remote host.

If the terminal and remote host are of the same type then the network merely acts as an extra long local link. Problems arise when a terminal of one type wishes to be connected(remotely or locally) to a host of another type. A machine designed to communicate with every type of terminal in the world would require hundreds of terminal drivers.

The problem is solved by a construct called a **Virtual Terminal (VT).** A virtual terminal is an imaginary terminal (a software model of a terminal) with a set of standard characteristics that every host understands. It is a software version of a physical terminal.

1) A terminal that wishes to communicate with a remote host communicates to its local host.
2) The local host contains VT software that translates the request or data received from the actual terminal into the intermediary format used by the virtual terminal.
3) The reformatted data travel over the network to the remote host. The remote host passes the transmission to its own VT software, which transforms it from its VT format into the format used by the remote hosts own terminals.
4) The remote hosts therefore receives the input as if from a local host. After processing the request, the remote host can return a response following the same procedure in reverse.

Directory Services

The OSI directory service is designed according to the ITU-T X.500 standard. A directory is a global source of information about many different objects. An OSI directory service is an application program used to represent and locate objects (such as programs and files) contained in an OSI directory. The type of information that a directory holds varies according to the type of the object.

To the user of directory service, all of this information appears to be stored in a single database, located in a single host. Actually a directory is a distributed database with each host holding only a part.

Note that the user of a directory service can be either a person or an application.

DIB (Directory Information Base) :
The information contained in the directory is called the DIB. It is stored as a set of entries, each describing one object. An entry may consist of several parts, each which describes a different attribute of the object.

DUA (Directory User Agents) & DSA (Directory Service Agents) :
Users gain access to the DS through a mechanism called DUA. The DUA communicates with one or more entities called DSA's contained within the DS itself.

The DUA passes a request for information to a DSA. If the DSA knows the where about of the information sought, it either fills the request or passes it on to another DSA with the necessary access and so on. The requested information is retrieved and passed back through successive DSAs to the DUA.

If the DSA does not know how to fill a request it has three options:
- It can forward the request to another DSA
- It can broadcast the request and wait for a response
- It can return a failure to the DUA

File Transfer Access and Management:

The FTAM protocol is used to
- Transfer (copy)
- Access (read, write or modify)
- Manage (control)

Virtual files and filestores :
To allow the interaction of different file systems FTAM uses the concept of virtual files and virtual filestores. A virtual filestore is a non-implementation. Specific model for files and databases can be used as an intermediary for file transfer access and management.

FTAM is based on a symmetrical access of a virtual file. Each transaction requires an initiator and a responder. The initiator requests the transfer of access or management of a file from the responder. The responder creates a virtual file model of its actual file and allows the initiator to use the virtual model rather than the real file because the model is software, it can be designed to be independent of hardware and the O.S. constraints.

Attribute and content :

The creation of virtual filestore is based on two aspects of the file

1) attribute and 2) content.

The attributes of a file are a set of properties or security measures used to control either the contexts or access per content attributes are those related to the contents of the file. Per access attributes are security measures that control access to the file.

The OSI FTAM (File Transfer, Access and Management) model is based on the idea of a virtual store that is mapped to real filestore by software.

FTAM has one basic file type, the hierarchical file, but it is possible to specify constraints that give other types as special cases. The virtual filestore is highly connection oriented, with a series of nested regimes.

Related Questions :

1. Electronic mail
2. Directory services
3. FTP
4. Virtual terminal.
5. Discuss the issues in implementing the 'ftp' service in a UNIX system. Explain its working with the help of protocol used.
6. Explain file transfer, access and management.
7. Write SN on Virtual terminal

□□□□□□

Integrated Services Digital Network

Integrated Services Digital Network (ISDN) is comprised of digital telephony and data-transport services offered by regional telephone carriers. ISDN involves the digitization of the telephone network, which permits voice, data, text, graphics, music, video, and other source material to be transmitted over existing telephone wires.

The emergence of ISDN represents an effort to standardize subscriber services, user/network interfaces, and network and internetwork capabilities. ISDN applications include high-speed image applications, high-speed file transfer, and videoconferencing. Voice service is also an application for ISDN.

The ISDN integrates customer services with the IDN. With ISDN all customer services will become digital rather than analog, and the flexibility offered by the new technology will allow customer services to be made available on demand. Most important, ISDN will allow all communication connections in a home or building to occur via a single interface.

ISDN incorporates all communication connections in a home or building into a single interface.

Figure below gives a conceptual view of the connections between users and an ISDN central office. Each user is linked to the central office through a digital pipe. These pipes can be of different capacities to allow different rates of transmission and support different subscriber needs.

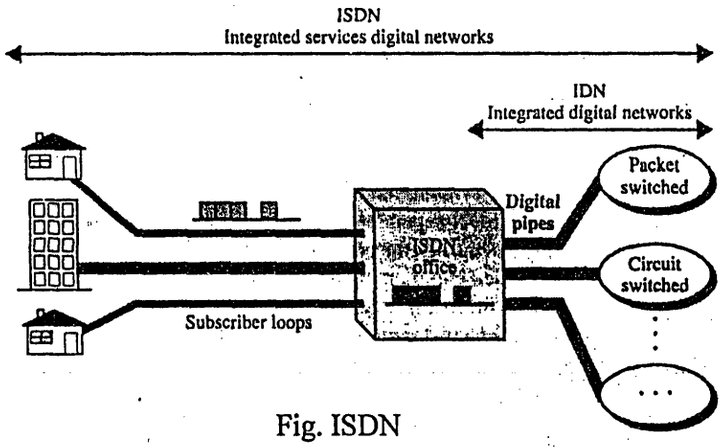


Fig. ISDN

SUBSCRIBER ACCESS TO THE ISDN

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

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

B Channels

A bearer channel (B channel) is defined at a rate of 64 Kbps. It is the basic user channel and can carry any type of digital information in full-duplex mode as long as the required transmission rate does not exceed 64 Kbps. For example, a B channel can be used to carry digital data, digitized voice, or other low data-rate information. Several transmissions can be accommodated at once if the signals are multiplexed first. Multiplexed transmissions of this sort, however, must be destined for a single recipient. A B channel carries transmissions end-to-end. It is not designed to demultiplex a stream midway in order to separate and divert transmissions to more than one recipient.

D Channels

A data channel (D channel) can be either 16 or 64 Kbps, depending on the needs of the user. Although the name says *data,* the primary function of a D channel is to carry control signaling for the B channels.

Up to this point, the transmission protocols we have examined all use in-channel (in-band) signaling. Control information (such as call establishment, ringing, call interrupt, or synchronization) is carried by the same channel that carries the message data. The ISDN separates control signals onto a channel of their own, the D channel. A D channel carries the control signaling for all of the channels in a given path, using a method called common-channel (out-of-band) signaling.

In this mechanism, a subscriber uses the D channel to connect to the network and secure a B channel connection. The subscriber then uses the B channel to send actual data to another user. All the devices attached to a given subscriber loop use the same D channel for signaling, but each sends data over a B channel dedicated to a single exchange for the duration of the exchange. Using the D channel is similar to having a telephone operator place a call for you. You pick up the phone and tell the operator what type of call you wish to place and the number you wish to contact. The operator finds an open line appropriate for your needs, rings your party, and connects you. The D channel acts like an operator between the user and the network at the network layer.

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

H Channels

Hybrid channels (H channels) are available with data rates of 384 Kbps (HO), 1536 Kbps (HI 1), or 1920 Kbps (HI2). These rates suit H channels for high data-rate applications such as video, teleconferencing, and so on.

ISDN Devices

ISDN devices include terminals, terminal adapters (TAs), network-termination devices, line-termination equipment, and exchange-termination equipment.

ISDN terminals come in two types:

- Specialized ISDN terminals are referred to as terminal equipment type 1 **(TE1).** TE1s connect to the ISDN network through a four-wire, twisted-pair digital link.
- Non-ISDN terminals, such as DTE, that predate the ISDN standards are referred to as terminal equipment type 2 **(TE2).** TE2s connect to the ISDN network through a TA. The ISDN TA can be either a standalone device or a board inside the TE2. If the TE2 is implemented as a standalone device, it connects to the TA via a standard physical-layer interface. Examples include EIA/TIA-232-C (formerly RS-232-C), V.24, and V.35.

Beyond the TE1 and TE2 devices, the next connection point in the ISDN network is the network termination type 1 **(NT1)** or network termination type 2 **(NT2)** device. These are network-termination devices that connect the four-wire subscriber wiring to the conventional two-wire local loop. In North America, the NT1 is a customer premises equipment (CPE) device. In most other parts of the world, the NT1 is part of the network provided by the carrier.

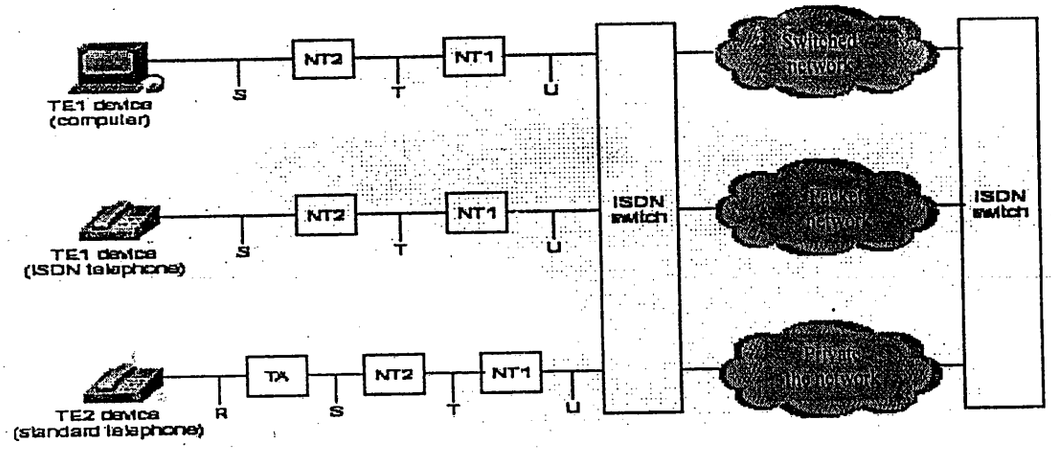
The NT2 is a more complicated device that typically is found in digital private branch exchanges (PBXs) and that performs Layer 2 and 3 protocol functions and concentration services.

An **NT1/2** device also exists as a single device that combines the functions of an NT1 and an NT2.

ISDN specifies a number of reference points that define logical interfaces between functional groups, such as TAs and NT1s.

ISDN reference points include the following :

- **R**—The reference point between non-ISDN equipment & a TA.
- **S**—The reference point between user terminals and the NT2.
- **T**—The reference point between NT1 and NT2 devices.
- **U**—The reference point between NT1 devices and line- termination equipment in the carrier network. The U reference point is relevant only in North America, where the NT1 function is not provided by the carrier network.



ISDN BRI Service

The ISDN Basic Rate Interface (BRI) service offers two B channels and one D channel (2B+D).

BRI B-channel service operates at 64 kbps and is meant to carry user data;
BRI D-channel service operates at 16 kbps and is meant to carry control and signaling information.

BRI also provides for framing control and other overhead, bringing its total bit rate to 192 kbps.

The BRI physical layer specification is International Telecommunication Union–Telecommunications. Standards Section (ITU-T) (formerly the Consultative Committee for International Telegraph and Telephone [CCITT]) I.430.

ISDN PRI Service

ISDN Primary Rate Interface (PRI) service offers 23 B channels and 1 D channel in North America and Japan, yielding a total bit rate of 1.544 Mbps (the PRI D channel runs at 64 kbps). ISDN PRI in Europe, Australia, and other parts of the world provides 30 B channels plus one 64-kbps D channel and a total interface rate of 2.048 Mbps. The PRI physical layer specification is ITU-T I.431.

Packet Radio Networks :

There are three situations in which packet radio is attractive as a method of local distribution from a central site to remote stations:

1. The stations are located in areas where the telephone system is poorly developed or nonexistent.
2. The stations are mobile.
3. The stations have a high peak-to-average traffic ratio, or a low data rate.

Ground radio packet broadcasting differs from satellite packet broadcasting in the following ways:

- Stations have limited range introducing the need for radio repeaters.
- If two stations are too far apart, they will not be able to hear each other's transmissions at all, making CSMA impossible and complicating the MAC sub layer protocol.

Design Issues for Packet Radio Network :

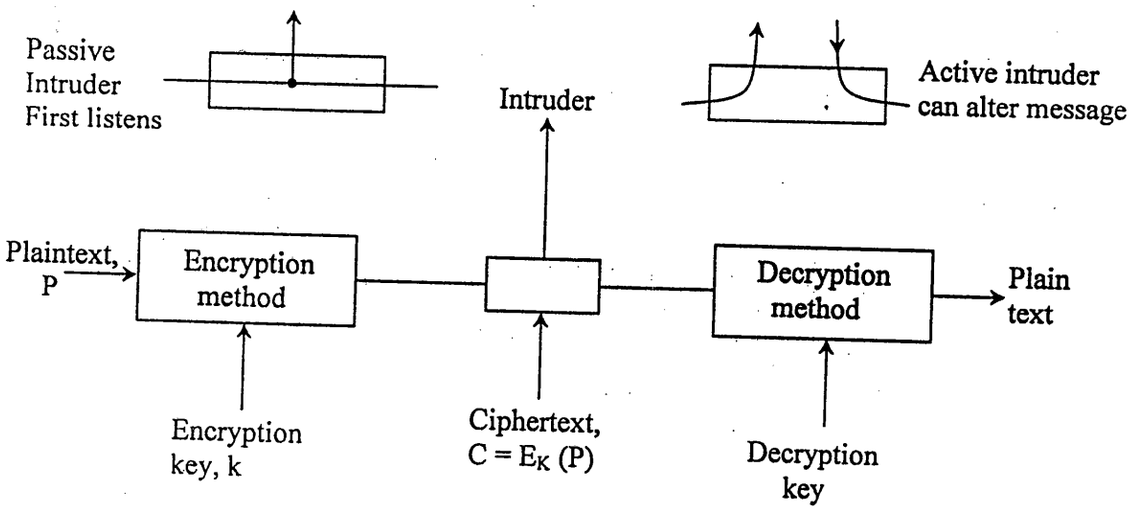
The introduction of a large number of repeaters top increase the geographic coverage of the system, brings with it a number of complications because repeaters store incoming packets and then rebroadcast them on the same frequency. Simultaneous reception and transmission is therefore impossible. When a packet radio system contains multiple repeaters, routing becomes an issue.

Cryptography :

Cryptography is the art of secret writing.
The messages to be encrypted, known as the **plaintext**, are transformed by a function that is parameterized by a **key**. The output of the encryption process, known as the **ciphertext**, is then transmitted, often by messenger or radio. We assume that the enemy, or **intruder**, hears and accurately copies down the complete ciphertext. However, unlike the intended recipient, he does not know what the decryption key is and so cannot decrypt the ciphertext easily. Sometimes the

intruder can not only listen to the communication channel (passive intruder) but can also record messages and play them back later, inject his own messages, or modify legitimate messages before they get to the receiver (active intruder).

Network Security



* Art of breaking ciphers is called CRYPTANANALYSIS.
* Art of devising ciphers is called CRYPTOGRAPHY.
* Art of devising ciphers & breaking them is collectively called CRYPTOLOGY.

$$D_K [E_K (P)] = P$$

Substitution Ciphers :

In substitution cipher each letter or group of letters is replaced by another letter or group of letter to disguise it.

* **Monoalphabetic Substitution :**
  The oldest cipher is called Caesar cipher. Here each character is replaced by another character.

  Plain Character : a b c d e f g ...
  Cipher Character : Q W E R T Y U

* **Polyalphabetic substitution :** (not to be done)
  Here, plain text character is replaced by different cipher character, substitution depends not only on the character but also on the position of the character in text.

Transposition Ciphers :

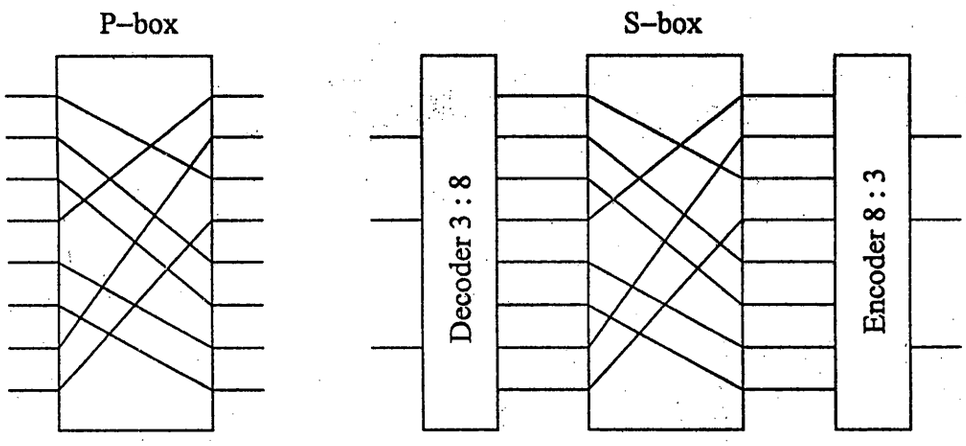
Transposition Ciphers reorder the letters but do not disguise them.
Plain text : SEND ONE LAKH RUPEE
The key (known by receiver) is NUMBER

4	6	3	1	2	5
N	U	M	B	E	R
S	E	N	D	O	N
E	L	A	K	H	R
U	P	E	E	A	B

Cipher text : DKEOHANAESEUNRBELP

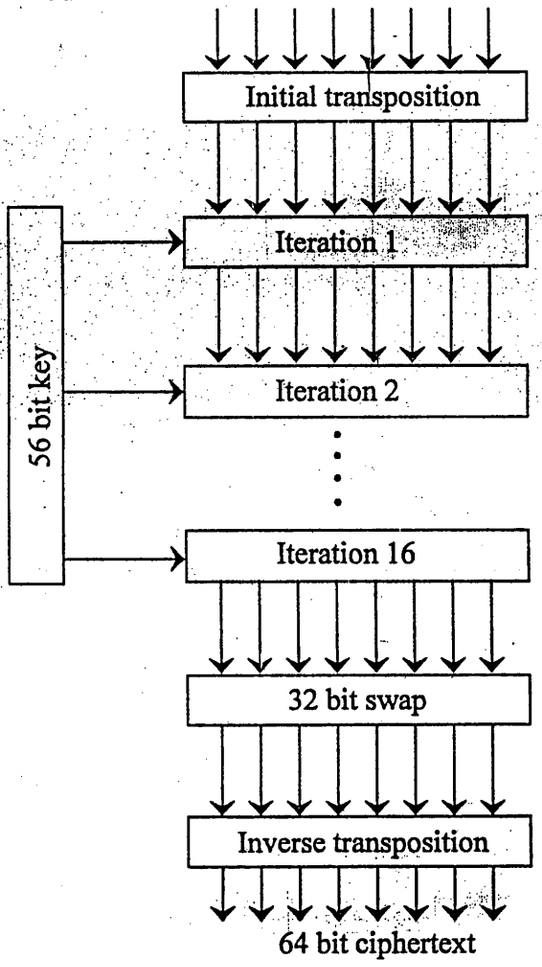
Secret key algorithms :

* Transpositions & Substitutions can be made with simple circuits.
* P–box (O stands for permutation) used to effect a transposition on an 8–bit input.
* S–box performs substitutions
  In this e.g. 3 bit plain text is entered and 3–bit ciphertext is output. The 3–bit input selects one of the light lines.

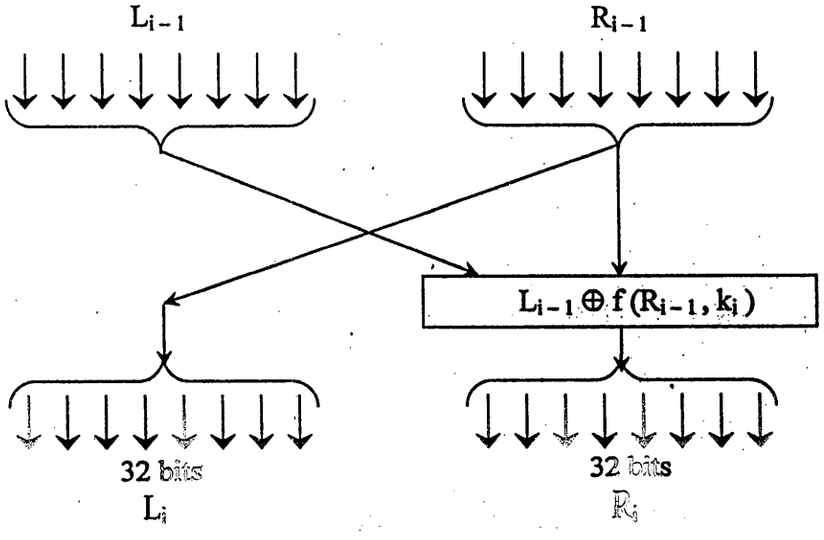


* Product Cipher

DES (Data encryption standard)



a) General outline



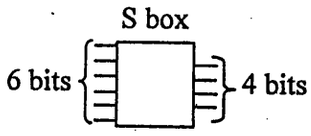
General Outline

* Plain text is encrypted in blocks of 64 bits yielding 64 bits of ciphertext.
* Algorithm is parameterized by a 56 bit key has 19 distinct stages.
  - → First stage is key independent transposition on 64–bit plaintext.
  - → Last stage is the exact inverse of this transposition
  - → The stage prior to the last one exchanges the leftmost 32 bits with the rightmost 32 bits.
  - → The remaining 16 stages are functionally identical but are parameterized by different functions of the key.
  - → The algorithm has been designed to allow decryption to be done with the same key as encryption. The steps are just run in reverse order.

Detail of one Iteration :

- → Each stage takes two 32 bit input and produce two 32 bit outputs.
- → The left output is simply a copy of right input.
- → The right output is the bitwise EXCLUSIVE or of the left input and a function of the right input and the key for this stage, k_i. All the complexity lies in this function.

* 4 steps for the functions $f(R_{i-1}, k_i)$
  i) 48 bit no. E is constructed by expanding 32 bit R_{i-1} according to fixed transposition and duplication rule.
  ii) E and k_i are EXCLUSIVE ORed together
  $E \oplus k_i$
  iii) This output is partitioned into eight groups of 6 bits each which is fed into a separate S–box.

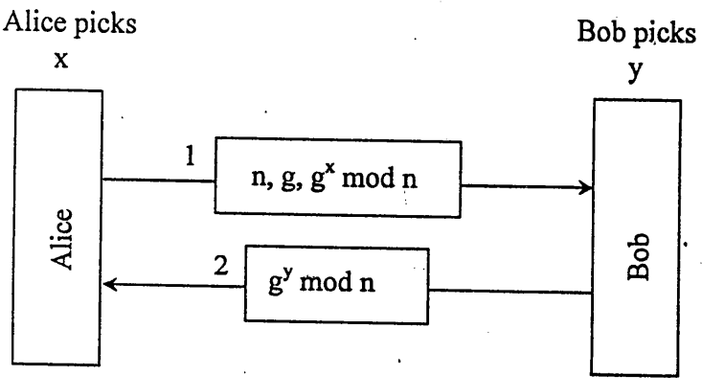


  Each of the 64 possible inputs to an S–box is mapped onto a 4–bit output.
  iv) Finally these 8 × 4 bits are passed through a P–box.

* In each of the 16 iterations, a different key is used.
  1) Before the algorithm starts, a 56 bit transposition is applied to the key.
  2) Just before each iteration, the key is partitioned into two 28 bit units, each of which is rotated left by a number of bits dependent on the iteration number.
  3) K_i is derived from this rotated key by applying yet another 56–bits transposition on it.
  4) A different 48–bit subset of the 56 bits is extracted and permuted on each round.

Authentication based on shared secret key.

Establishing a shared key : The DIFFLE–HELLMAN key exchange.



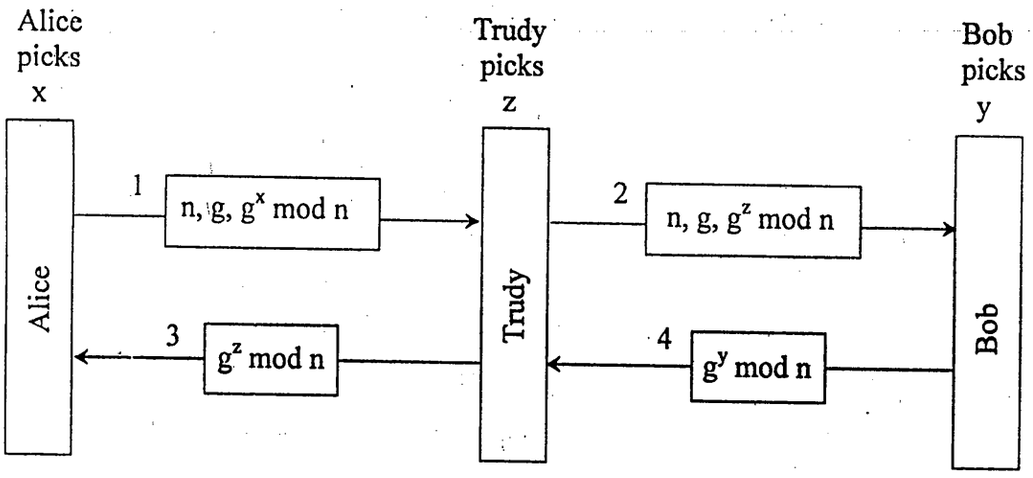
Alice computes
$(g^y \bmod n)^x$
$= g^{xy} \bmod n$

Bob computes
$(g^x \bmod n)^y$
$= g^{xy} \bmod n$

* This protocol allows strangers to establish a shared secret key.
* Alice and Bob have to agree to two large primes n & g where $(n - 1)/2$ is also prime and certain conditions apply to g.
* n & g must be public any one of them can just pick n & g and tell other openly.

* Alice picks large number, x & keeps it secret. Similarly Bob picks up y.

There is a problem. When Bob gets the triple (47, 3, 28), how does he know it is from Alice & not from Trudy. Unfortunately Trudy can deceive both Alice and Bob.



Bucket brigade attack / woman–n–the–middle attack

Alice and Bob now share a secret key.
Eg. For normal exchange
N = 47, g = 3, x = 8, y = 10
Alice to Bob (47, 3, 28) $\because 3^8 \bmod 47 = 28$
Bob to Alice (17) $\because 3^{10} \bmod 47 = 17$
Alice computes $17^8 \bmod 47 = 4$
Bob computes $28^{10} \bmod 47 = 4$
Alice and Bob have independently determined the secret key as 4. Trudy has to solve the equation $3^x \bmod 47 = 28$ which can be done by exhaustive search for small numbers like this, but not when all the numbers are hundreds of bits long.

Public Key algorithm :
Public–key cryptography requires each user to have two keys: a public key, used by the entire world for encrypting messages to be sent to that user, and a private key, which the user needs for decrypting messages.

RSA (Rivest, Shamir & Adleman)
RSA is a public–key algorithm developed by Rivest, Shamir & Adleman)
The RSA method is based on some principles from number theory.
The RSA method is as follows :
1. Choose two large primes, p and q (typically 1024 bits).
2. Compute $n = p \times q$ and $z = (p-1) \times (q-1)$
3. Choose a number relatively prime to z and call it d.
4. Find e such that exd = 1 mod z.

To encrypt a message P, compute $C = P^e \pmod n$.
To decrypt C, compute = $P = C^d \pmod n$.
The security of the method is based on the difficulty of factoring large numbers.

An example of how the RSA algorithm works is as given below.

Suppose p = 3 and q = 11, giving n = 33 and z = 20. A suitable value for d is d = 7, since 7 and 20 have no common factors. With these choices, e can be found by solving the equation 7e = 1 (mod 20), which yields e = 3. The ciphertext, *C*, for a plaintext message, *P*, is given by $C = p^3 \pmod{33}$. The ciphertext is decrypted by the receiver by making use of the rule $P = C^7 \pmod{33}$. The figure shows the encryption of the plaintext "SUZANNE" as an example.

Plaintext (P)			Ciphertext (C)		After decryption	
Symbolic	Numeric	P^3	P^3 (mod 33)	C^7	C^7 (mod 33)	Symbolic
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E

Sender's Computation

Receiver's Computation

Fig: An example of the RSA algorithm.

Certificates

As a first attempt at distributing public keys securely, we could imagine a key distribution center available on–line 24 hours a day to provide public keys on demand. One of the many problems with this solution is that it is not scalable, and the key distribution center would rapidly become a bottleneck. Also, if it ever went down, Internet security would suddenly grind to a halt.

For these reasons, people have developed a different solution, one that does not require the key distribution center to be on–line all the time. In fact, it does not have to be on–line at all. Instead, what it does is certify the public keys belonging to people, companies, and other organizations. An organization that certifies public keys is now called a **CA (Certification Authority)**.

As an example, suppose that Bob wants to allow Alice and other people to communicate with him securely. He can go to the CA with his public key along with his passport or driver's license and ask to be certified. The CA then issues a certificate similar to the one in following figure and signs its SHA–1 hash with the CA's private key. Bob then pays the CA's fee and gets a floppy disk containing the certificate and its signed hash.

I hereby certify that the public key
19836A8B03030CF83737E3837837FC3s87092827262643FFA82710382828282A
belongs to
Robert John Smith
12345 University Avenue
Berkeley, CA 94702
Birthday: July 4, 1958
Email: bob@superdupernet.com

SHA–1 hash of the above certificate signed with the CA's private key

Fig: A possible certificate and its signed hash

The fundamental job of a certificate is to bind a public key to the name of a principal (individual, company etc). Certificates themselves are not secret or protected. Bob might, for example, decide to put his new certificate on his Web site, with a link on the main page saying: Click here for my public–key certificate. The resulting click would return both the certificate and the signature block (the signed SHA–1 hash of the certificate).

While the standard function of a certificate is to bind a public key to a principal, a certificate can also be used to bind a public key to an **attribute**. For example, a certificate could say: This public key belongs to someone over 18. It could be used to prove that the owner of the private key was not a minor and thus allowed to access material not suitable for children, and so on, but without disclosing the owner's identity. Typically, the person holding the certificate would send it to the Web site, principal, or process that cared about age. That site, principal, or process

would then generate a random number and encrypt it with the public key in the certificate. If the owner were able to decrypt it and send it back, that would be proof that the owner indeed had the attribute stated in the certificate. Alternatively, the random number could be used to generate a session key for the ensuing conversation.

Another example of where a certificate might contain an attribute is in an object–oriented distributed system. Each object normally has multiple methods. The owner of the object could provide each customer with a certificate giving a bit map of which methods the customer is allowed to invoke and binding the bit map to a public key using a signed certificate. Again here, if the certificate holder can prove possession of the corresponding private key, he will be allowed to perform the methods in the bit map. It has the property that the owner's identity need not be known, a property useful in situations where privacy is important.

Issues in Network Security :

1) **Privacy :**

Privacy relates to individuals wanting to restrict what other people can see about them.

What has changed in the past decade is both the ease with which governments can spy on their citizens and the ease with which the citizens can prevent such spying. In the 18th century, for the government to search a citizen's papers, it had to send out a policeman on a horse to go to the citizen's farm demanding to see certain documents. It was a cumbersome procedure. Nowadays, telephone companies and Internet providers readily provide wiretaps when presented with search warrants. It make life much easier for the policeman and there is no danger of falling off the horse.

Real privacy means it is much harder for them to spy on criminals of all stripes, but it is also much harder to spy on journalists and political opponents.

2) **Freedom of Speech**

A second key social issue is freedom of speech, and its opposite, censorship, which is about governments wanting to restrict what individuals can read and publish. With the Web containing millions and millions of pages, it has become a censor's paradise. Depending on the nature and ideology of the regime, banned material may include Web sites containing any of the following:

1. Material inappropriate for children or teenagers.
2. Hate aimed at various ethnic, religious, sexual or other groups.
3. Information about democracy and democratic values.
4. Accounts of historical events contradicting the government's version.
5. manuals for picking locks, building weapons, encrypting messages, etc.

Increasingly, many countries are now trying to regulate the export of intangibles, which often include Web sites, software, scientific papers, e–mail, telephone helpdesks, and more. Even the U.K., which has a centuries–long tradition of freedom of speech, is now seriously considering highly restrictive laws.

3) **Copyright**

A third one is copyright. **Copyright** is the granting to the creators of **IP (Intellectual Property)**, including writers, artists, composers, musicians, photographers, cinematographers, choreographers, and others, the exclusive right to exploit their IP for some period of time, typically the life of the author plus 50 years or 75 years in the case of corporate ownership. After the copyright of a work expires, it passes into the public domain and anyone can use or sell it as they wish.

Network Operating System

In Network operating system, the users are aware of the existence of multiple computers and can log in to remote machines and copy files from one machine to another. Each machine run its own local operating system and his its own local user (or users).

Network operating systems are not fundamentally different from single processor operation systems. They need a network interface controller and some low level software to drive it, as well as programs to achieve remote login and remote file access, but these additions do not change the essential structure of the operating system.

Related Questions :

- **ISDN :**

1. What is ISDN? Explain the interfaces in ISDN model?
2. Write SN on ISDN.
3. Describe in brief the two standard types of services available on ISDN.
4. Discuss the ISDN system architecture and its application.
5. ISDN PBXes versus LAN.
6. Draw and explain basic ISDN structure.

- **Switching techniques :**

1. Compare circuit, message and packet switching.
2. Compare virtual circuit and datagram.

- **Other topics :**

1. SN on connection–oriented and connectionless gateways.
2. Discuss connectionless internetworking.
3. What are the differences between connection–oriented and connectionless services / protocols?
4. Explain X.25 in detail.
5. How a satellite based computer network works?
   Explain any channel allocation algorithm used in satellite network.
6. Write short note on satellite network.
7. What is Network operating system? Explain with example of any one Network operating system, with respect to application, protocols, topology, structure.
8. Write short note on Network operating system.
9. Explain the process of circuit set–up in X.25. Show the various contents of the packets exchanged during the process.
10. Explain virtual circuit diagram.
11. Web server listens on port 80. If two web clients make request on same port, how server decides where to send reply. (Hint : Full TCP/IP connection)
12. Give one example of security threat in DLL, Network layer, transport layer.
13. Why should not we allow timeouts in computer networks?
14. State the use of timers in physical, Data link, Network and Transport layer.
15. State delay–bandwidth product, IP spoofing.
16. Design a LAN for a typical branch office of ABC bank. Bank has got 40 terminals. Employees access their emails through one email server. Another server is DB server for transactions. List goals, design constraints, hardware, software. Draw diagram of the set up.
17. Customers arrive at a fast food restaurant at a rate of 5 per minute and wait to receive their order for an average of 5 minutes. Customers eat in the restaurant with probability of 0.5 and carry out their order without eating with probability of 0.5. A meal requires an average of 20 minutes. What is the average no. of customers in the restaurant?
18. Consider router with table entries for subnet number, subnet mask, Next hop, Next hop may be a local interface or another router. It receives packet with D destination. Write algorithm in pseudo language to handle the packet.
19. State different socket calls for client and server. (do not bother about syntax).
20. State Load balancing, Scalability of Network applications. Also state UDP applications, Disadvantages of Distance vector routing.
21. For LINUX or WINDOWS, Identify and state networking commands as well as configuration files.
22. You are browsing internet from home (modem). You are logged in yahoo where shu support is available. Now identify the software and hardware components and relate them with OSI 7 layer model.
23. A 3000 km long T1 trunk is used to transmit 64 bytes frame using pipelining. If the propagation speed is 6 microsecond/km, how many bits should the sequence number be? (T1 = 1.536 Mbps)
24. State two reasons each for ARP and RARP.

25. Write short notes on :
    (a) Hot potato algorithm (b) Data compression
26. Compare the following :
    (a) ISDN versus PSTN (b) Bridge Vs Router (c) DTE–DCE interface.
27. A LAN consists of 12 client workstations and a server that manages the queue for a single printer. Each user at a working station has to print on an average 20 pages per hour. The lengths of documents are exponentially distributed with a mean size of 2 pages. The printer is capable of printing 5 pages per minute.
    (i) Evaluate the mean number of print jobs that have to wait in the queue.
    (ii) Determine the average time delay for print job.
    (iii)How many pages/minute should the printer be able to print in order to reduce the mean time delay to 1 minute.
28. Compare and contrast :
    Switch, Bridge, Router and hub.
29. What is the significance of propagation delay in
    (1) Ethernet channel (2) Long distance communication channel
30. State which of OSI layers uses sliding window features and briefly why?
31. Write short note on Graphs/ Trees and computer networks (Relation).
32. Just make one line most important statement about following :
    SNMP, SMTP, ARP, RARP, TELNET, PPP.
33. Draw diagram showing client–server applications using sockets and other layers (also write about socket calls)
34. Write system design rules for better performances (for networks)
35. Briefly write about data structures and algorithms usage in computer Networks.
36. Company has got 3 sites A, B, C. A is head office. B is 2 km from A, C is 100 km away from others. You as a network designer, design, draw, list hardware and software required. Also company wants to restrict access to internet to and fro.
37. Novell netware and UNIX networks are to be interconnected. Show all necessary hardware and software setup.
38. A 100 km long cable runs at T1 data rate. The propagation speed in the cable is 2/3 speed of light. How many bits fit in the cable (T1 speed is 1.536 Mbps)
39. An institute has registered the domain name as "mycollege.edu" and has obtained two static IPs. The institute has 5 departments and an administration using, each having its own networked computer centre. The departments offer Windows NT and LINUX/UNIX environments to its students. A centralized online digital library is also existing, providing information access to students/ teachers. The institute has a 128 kbps dedicated internet connection. The institute provides mail, remote login, ftp services, for its students.
    Identify a campus network with all related blocks (servers, routers, gateways, etc.) and components to set up such a facility. Clearly indicate the role of each of the component and the specifications. Ensure proper security of the network.
40. Suppose that the web contains 10 million pages, each with an average of 10 hyperlinks. Fetching a page averages 100 msec. What is the minimum time to index the entire web?
41. You login to a UNIX system that you have never used before and want to find the subnet directed broadcast address for all attached interfaces that support broadcasting? How can you do this?
42. A source is on an Ethernet with a propagation delay of 100 μs and a service rate of 10 Mbps. This is connected to a T1 line via a router with propagation delay 30ms. The destination is connected via a symmetric arrangement. Assuming 1ms service times at the routers, what are the equivalent delay and service rates for a reduced flow model that describes this path?
43. Write Short Notes on :
    (a) Hot potato algorithm (b) IPV6 (c) DNS & DHCP
44. Explain data link layer protocols of ARPANET or any other network you know.
45. Which are the key plus points of layered approach in architecture of Network.
46. A business man wants to set up LAN where number of nodes may increase or decrease depending on business success which topology you will suggest with justification.
47. Just make one line most import statement about following : –
    PPP, RARP, FDDI, ALOHA, SMTP, TCP/IP
48. Explain briefly addressing the computers and devices in different OSI layers.
49. What is data compression? Why it is required?

50. What is data encryption and compression and why it is required?

51. Data compression.

52. What is cryptography? Which layer is responsible for data encryption? Explain one data encryption standard.

53. Digital certificates.

54. According to Diffie and Hellman, what are the three requirements that encryption and decryption algorithms follow?

Soln.: The three requirements that encryption and decryption algorithms follow are : –

1. $D(E(P)) = P$
2. It is exceedingly difficult to deduce D from E.
3. E cannot be broken by a chosen plaintext attack.

55. Give RSA steps for public key security.

Soln.: RSA steps for public key security are

1. Choose two large primes, p and q (typically 1024 bits)
2. Compute $n = p \times q$ and $z = (p - 1) \times (q - 1)$
3. Choose a no. relatively prime to z and call it d.
4. Find e such that $e \times d = 1 \bmod z$.

56. What is authentication, Integrity control, Non repudiation related to network security.

Soln.:
- Authentication deals with determining who you are talking to before revealing sensitive information or entering into a business deal.
- Non–repudiation – Sender has to agree legally that he only send the message and later he cannot turn down about his actions.
- Integrity control – Message you received is really the one sent and not a malicious modified in transit.

57. Write a SN on RSA for public security.

58. What is symmetric and asymmetric key algorithms? Explain DES.

Soln.: Symmetric key algorithms use the key for encryption and decryption e.g. DES.
Asymmetric key algorithms use different keys encryption and decryption.

59. Explain different key exchange schemes.

Soln.: The different key exchange schemes are :

1. Authentication based on a shared secret key.
2. Establishing are shared key. Diffie–Hellman key exchange.
3. Authentication using a key distribution center.
4. Authentication using Kerberos.
5. Authentication using public–key cryptography.

60. What are security threats for information ? What are symmetric and asymmetric key algorithms ? Explain RSA or DES in detail ?

❑❑❑❑❑❑