SHRI SHAMBHUBHAI V. PATEL COLLEGE OF COMPUTER SCIENCE & BUSINESS MANAGEMENT
T.Y.B.C.A (FIFTH SEMESTER)
FIRST INTERNAL (2016-17)
SUBJECT: –Network Technologies

Time: 1:00 PM – 3:00 PM Date: 29/09/2016

Paper Solution by Prof. Viral S. Patel

Q.1 Answer the following questions. (Any Five) **[10]**

1› Which layer of OSI model is responsible for Routing Packets ? Explain.

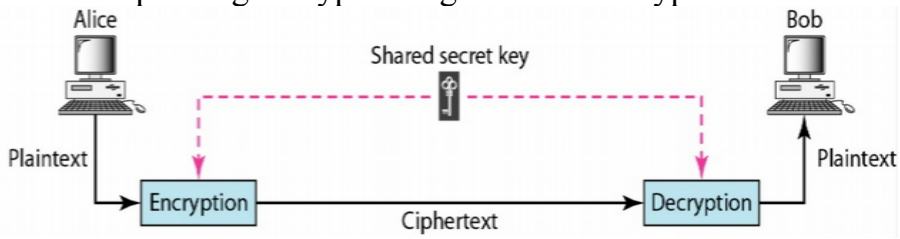
Ans ➔Network layer of OSI model is responsible for routing packets.
➔This layer create packets and provides data routing paths by contains hardware devices such as routers and network protocols such as Internet Protocol. The router examines the header fields of all the IP packets that pass through it.

2› Define Analog and Digital Signal.

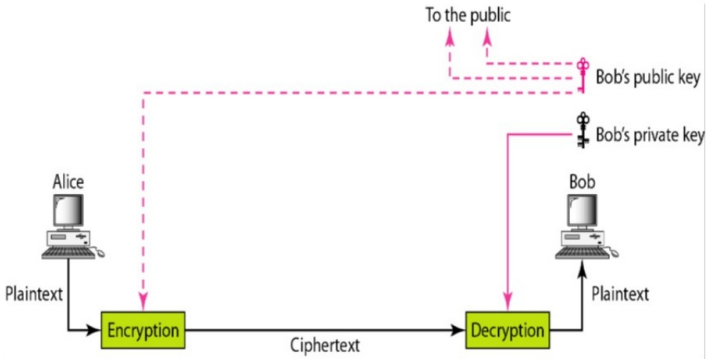
Ans ➔An Analog signal is continuous signal and Digital Signal is discrete values signal. Analog signal denoted by sine wave and digital signal denoted by square wave.
➔Example : audio signal is analog signal, the instantaneous voltage of the signal varies continuously. 0s and 1s bit stream in computer are digital signals.

3› What is Symmetric and Asymmetric cryptography ?

Ans ➔In Symmetric key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data.



➔In Asymmetric or public-key cryptography, there are two keys : private key and a public key. public key that is used by sender to encryption and private key that is different from the public key used by receiver to decryption.



4› What is IP address ? List classful addressing with range.

Ans ➔An IP address means Internet Protocol address. It is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. It is a logical address which contain host or network interface identification.

IP addresses are usually written and displayed in human-readable notations, such as 172.16.254.1 (IPv4), and 2001:db8:0:1234:0:567:8:1 (IPv6).

The Internet Assigned Numbers Authority (IANA) manages the IP address space allocations globally. And we can get it from local Internet service providers (ISP).

➔Classful addressing range :

Class A : 0 to 127
Class B : 128 to 191
Class C : 192 to 223
Class D : 224 to 239
Class E : 240 to 255

5› What is the function of SMTP and HTTP ?

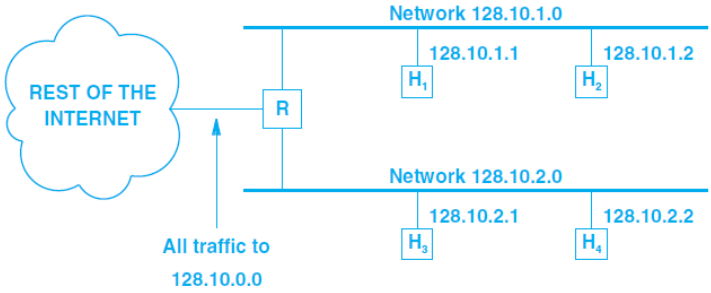
Ans ➔SMTP is a communication protocol for mail servers to transmit email over the Internet. It is a ASCII (American Standard Code for Information Interchange) based.

➔HTTP is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. This protocol defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. HTTP is called a stateless protocol because each command is executed independently, without any knowledge of the commands that came before it.

6› Define subnetting.

Ans ➔**Subnetting** is the strategy used to partition a single physical network into more than one smaller logical sub-networks (subnets).

Example :



7› What are the advantages and disadvantages of star topology ?

Ans **Advantages :**

➔Less cabling and Less expensive then Mesh Topology.

➔Each device needs only one link and one I/O port to connect.

➔Easily add, move and delete nodes.

➔Easy to install and reconfigure.

➔Robustness : If one link fails, all other links remain active.

➔Easy to fault identification and fault isolation.

Disadvantages :

➔Whole topology depend on one single point, the HUB. If HUB goes down, the whole system is dead.

➔more cabling required than ring and bus topology.

by Prof. Viral S. Patel

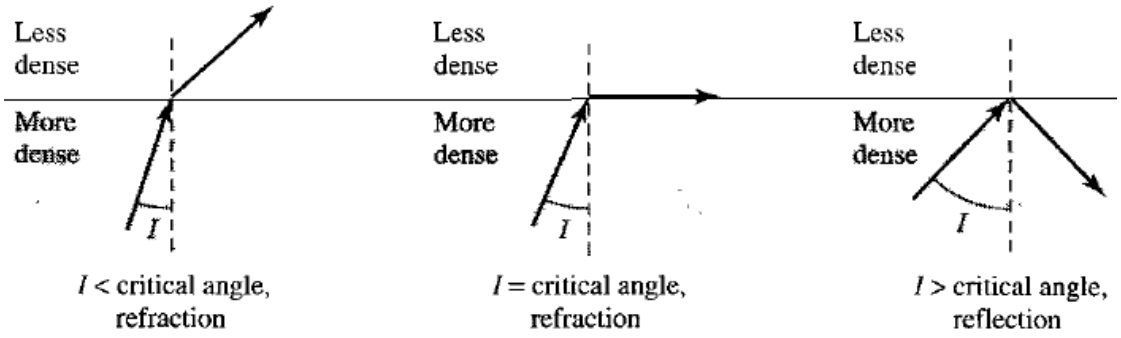
Q.2 Answer the following. (Any Four) **[16]**

1› Explain fiber optic cable with advantages and disadvantages.

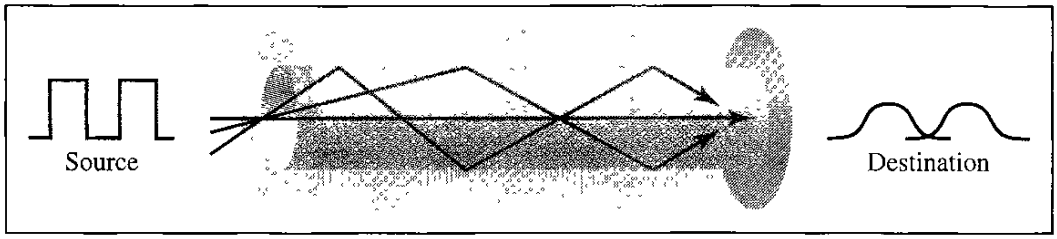
Ans A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.

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

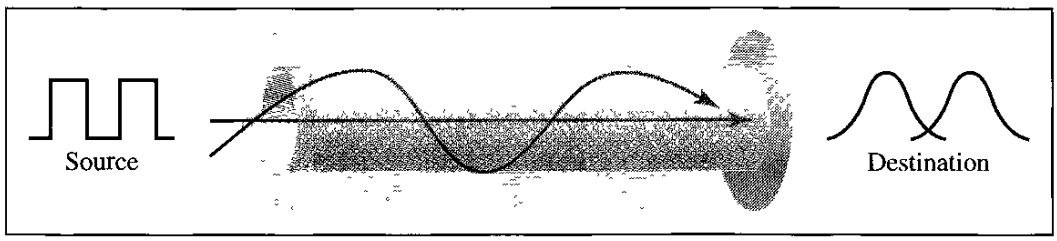
➔Figure show the working principle of fiber-optic. If angle of ray called incidence I is greater than critical angle then ray reflect from surface.



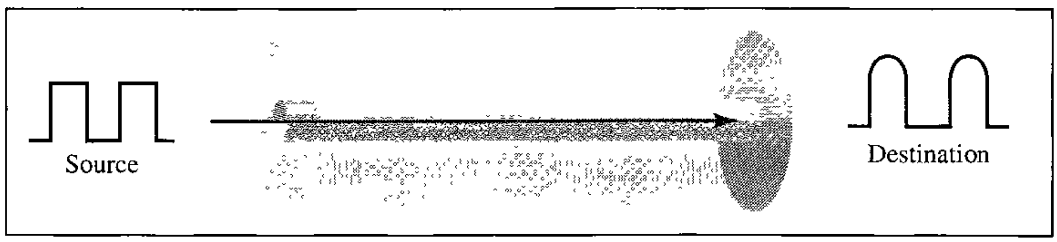
➔Propagation modes in fiber optic : Single model and Multimode
➔Multimode can be implemented in two forms : step index or graded index.
➔**Multimode step index fiber :** Here step index refers to suddenness of change. density of core remain constant from center to edges. At the interface due to the lower density reflection can occur at proper angle.
➔**Multimode graded index :** Here graded index refers to slowly and continue change density, highest at the center of the core and decreases gradually to edge. Figure show how refraction and reflection occurs.
➔**Single Mode :** Single mode uses step-index and a highly focused source of light that close to the horizontal as shown in figure. Diameter of core is very small and critical angle is close enough to 90°.



a. Multimode, step index



b. Multimode, graded index



c. Single mode

Cable composition and connectors :
➔ Outer jacket is made of either PVC or Teflon. Inside the jacket Kevlar material is used to provide strengthen to the cable. Below the Kevlar is another plastic coating provided to fiber.
➔ The subscriber channel (**SC**) connector, straight-tip (**ST**) connector and **MT-RJ** connectors are used in cabling.

Applications :
Local area network such as 100Base-FX network and 1000Base-X use fiber optic cable. Some cable TV companies also use combination of optical fiber and coaxial cable.

Advantages :

➔Higher bandwidth and higher data rates than twisted pair or coaxial cable.

➔Less signal attenuation as we can send signal 50 km without need of repeaters. We need repeaters every 5 km in twisted pair and coaxial cable.

➔Electromagnetic noise cannot affect fiber-optic cable.

➔Glass is more resistant to corrosive materials than copper.

➔Cable is Light weighted and greater immunity to tapping.

by Prof. Viral S. Patel

Disadvantages :

➔Require expertise for installation and maintenance as new technology.

➔Unidirectional light propagation so need two cable for bidirectional communication.

➔More expensive than other guided media.

by Prof. Viral S. Patel

2› Explain satellite communication.

Ans ➔**Satellite networks** are like cellular networks in that they divide the planet into cells. Satellites can provide transmission capability to and from any location on earth, no matter how remote.

➔ The **orbit** is the path in which it travels around the earth can be equatorial, inclined, or polar.

➔ The period of satellite, the time required for a satellite to make a complete trip around the earth, is determined by **Kepler's law**,

$$\textbf{Period} = C \times \textbf{distance}^{1.5}$$

➔ The signal from a satellite is normally aimed at a specific area called the **footprint.**

➔ Based on the location of the orbit, satellite can be divided into three categories : GEO, MEO and LEO.

➔ Different orbits is due to the existence of two Van Allen belts.

A Van Allen belt is a layer that contains charged particles. The MEO orbits are located between these two belts.

GEO : geostationary-Earth-orbit :

➔Altitude of **35,786 km** for the GEO satellites.

➔The satellite must move at the **same speed as the earth** so that it seems to remain fixed above a certain spot. Such satellites are called **geostationary**.

➔Three satellites, each **120°** from another in geosynchronous orbit around the equator.

MEO : middle-Earth-orbit :

➔ Altitude about **5000 to 15000 km** for the MEO satellites.

➔ GPS uses 24 satellites in **six orbits.** GPS is based on a principle called **trilateration.** On a plane, if we know our distance from three points, we know exactly where we are.

➔ GPS is used by military forces, in navigation, in clock synchronization.

LEO : low-Earth-orbit :

➔ Altitude is between **500 and 2000 km** for the LEO satellites.

➔ LEO satellites can be divided into **three** categories :

little LEOs, big LEOs and broadband LEOs.

➔ The little LEOs operate under 1 GHz. They are mostly used for low-data-rate **messaging.**

➔ The big LEOs operate between 1 and 3 GHz. **Globalstar** (six orbits with 8 satellites in each orbit) **and Iridium** (six orbits, with 11 satellites in each orbit) systems are examples of big LEOs.

➔ The broadband LEOs provide communication similar to fiber optic networks. The first broadband LEO system was **Teledesic**. It is also called "**Internet in the sky**".

by Prof. Viral S. Patel

3› Explain print server and message server. **by Prof. Viral S. Patel**

Ans **Print Server :**

Network

- Allow users to **share printers**
- Allow to **place** printers where convenient, not just near individual computers - Achieve better workstation **performance** by using high-speed network data transfer, print queues and spooling
- Allow users to share network **fax services**

➔ **Print services** manage and control printing on a network. Print jobs are stored on storage areas and sent to the printer in an organized fashion or may be prioritized in accordance with other criteria.

➔ **Advantage :** Network printing also cuts costs by allowing shared access to printing devices.

➔ With network print services, we can **fax** straight from workstation to a receiving fax machine.

➔ With a **fax server,** we can receive faxes directly on workstation. **Optical character recognition (OCR)** software can even convert these faxes into editable text, thereby saving a lot of time and effort.

Message Server :

➔ With message services, data can take form of graphics, digitized video, or audio, as well as text and binary data.

➔ As hypertext links become more common in messages, which transmitting data across a network.

➔ Four main types of message services are

- Electronic Mail
- Workgroup applications
- Object-oriented applications
- Directory services

➔ **Electronic Mail :** With email we can easily send a message to another user on internet. Email can transfer video, audio, and graphics as well. Integrated voice is the one of the most popular of the recent developments. Email is much faster, cheaper and simple than courier and file transferring services in communication system.

➔ **Workgroup Applications :** Workgroup applications produce more efficient processing of tasks among multiple users on a network.

The two main workgroup applications are

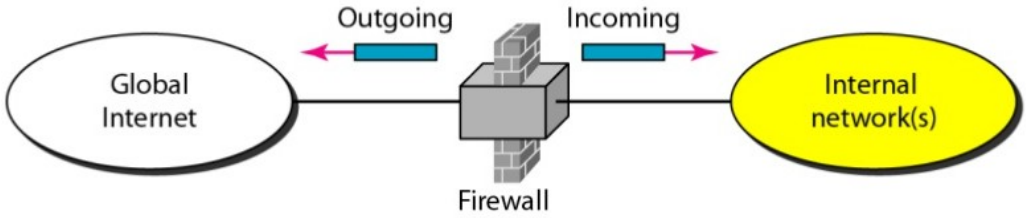
- **Workflow management applications**
- **Linked-object documents**

Workflow management applications route documents, forms and notices among network users for require the input of multiple users. The application

would send the form around from one person to the next.
Linked-object documents are documents containing multiple data objects. For example, a single linked object document could contain voice, video, text and graphics linked together. A network message service can then act as an agent for each of these objects, passing messages between the object and its originating application or file.
➔ **Object-Oriented Applications** are programs that can accomplish complex tasks by combining smaller applications, called objects. Message services facilitate communication between these objects by acting as a go-between.
➔ **Directory Services** servers help users locate, store, and secure information on the network. Both Active Directory and Novell Directory services store information about users and computers.

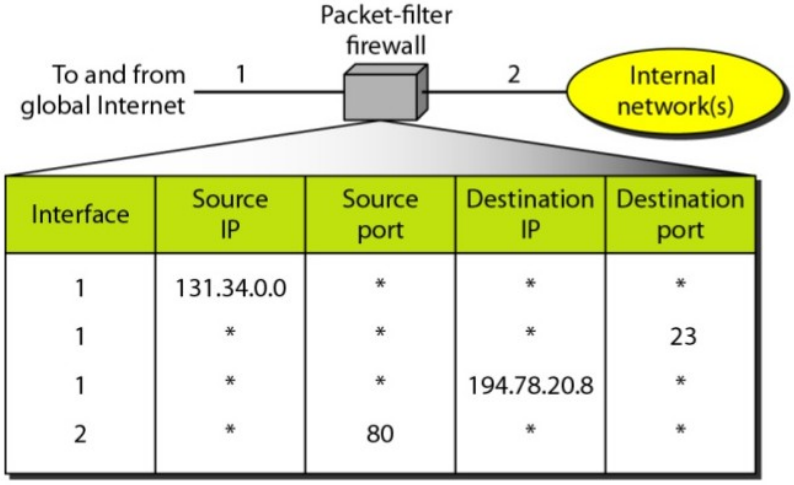
4› Explain Firewall.

Ans A firewall is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the internet. It is designed to forward some packets and filter (not forward) others.



A firewall is usually classified as a packet-filter firewall or a proxy-based firewall.

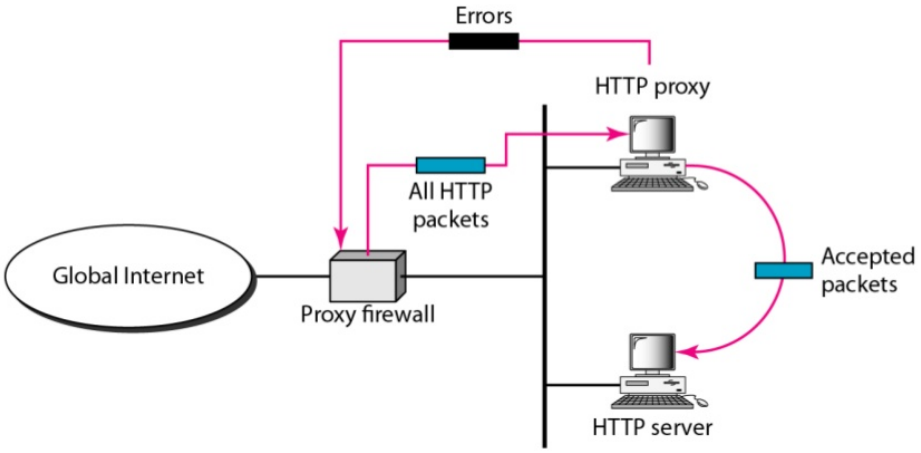
Packet-Filter Firewall



Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	80	*	*

➔A firewall can be used as a packet filter. It can forward or block packets based on the information in the network layer and transport layer headers : source and destination IP addresses, source and destination port addresses, and type of protocol (TCP or UDP).
➔A packet-filter firewall is a router that uses a filtering table to decide which packets must be discarded.
➔As shown in figure packets from network 131.34.0.0 are blocked. Packets for TELNET server (port 23) are blocked. Packets for host 194.78.20.8 are blocked. Outgoing packets destined for an HTTP server (port 80) are blocked.

Proxy Firewall



➔The packet-filter firewall is based on the information available in the network layer and tranport layer headers (IP and TCP/UDP). However, sometimes we need to filter a message based on the information available in the message itself.
As an example, assume that an organization wants to Only those Internet users who have previously established business relations with the company can have access, access to other users must be blocked.
➔ One solution is to install a proxy computer which stands between the customer and the corporation computer shown in figure.
➔Here the requests of the external users are filtered based on the contents at the application layer.

5› Explain frame structure of IEEE 802.3 with CSMA/CD. **by Prof. Viral S. Patel**

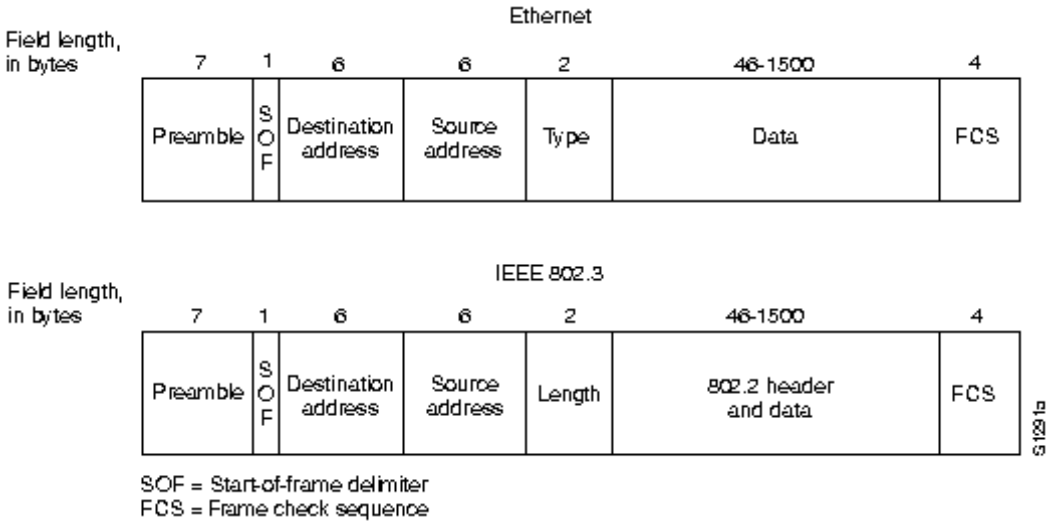
Ans **IEEE 802.3 Standard :**

➔ IEEE 802.3 Ethernet was standardized as a **10 Mbps** network by 802 committee of IEEE.

➔ Ethernet is also called logical bus topology.

➔**Information travels in Ethernet network in frame consists of six parts.**

- ➔ **Preamble :** Consists of eight bytes of information used to coordinate the rest of the information in the frame.
- ➔ **Destination address :** Consists of the hardware address of the workstation that receive this information
- ➔ **Source's address :** Consists of the hardware address of the workstation that sent the information.
- ➔ **Type :** Designates the type of information that is held within the data part of this frame, whether it is graphic information, ASCII text information or whatever.
- ➔ **Actual data :** Can be anywhere from 46 to 1500 bytes long.
- ➔ **Frame checked sequence :** Resembles a packing slip; it is used to verify that the rest of the frame reached its destination intact.



The 802.3n standard feature is the carrier sense multiple access with collision detection (CSMA/CD).

- ➔ **"Carrier sense"** means that **all nodes on the network listen** to the network to see whether it is clear before attempting to transmit.
- ➔ **"Multiple access"** means that **all nodes on the network have access to the same cable** – that signals are broadcast across the entire LAN.
- ➔ **"Collision detection"** means that **each node can tell** if another node starts transmitting data at the same time the first node is already sending data.
- ➔ In short, CSMA/CD provides a means for reducing packet collision by having each PC broadcast a signal known as the **carrier sensing signal** before transmitting in order to see if any other workstations are broadcasting.
- ➔ If not, the signal gives the workstation the "**all-clear**" and the workstation **transmits** its packet. If the carrier-sensing signal **detects another** workstation's transmittal, the workstation **waits** before broadcasting.

Problem :

➔ This process avoids collisions so long as network traffic isn't heavy and the LAN's cables are not any longer than their rating. If either of those conditions exit, then collisions are likely to happen regardless of CSMA/CD.

- ➔ CSMA/CD is **not in charge of** making sure that **only one workstation transmits at a time**, it is in charge of making sure all workstations are quiet before one transmits.
- ➔ If two workstations happen to begin **transmitting at the same time**, there's **nothing that CSMA/CD can do** to avoid the collision.

Solution :

➔ If two packets collide, CSMA/CD tries to avoid a repeat collision. First time a collision happens, each workstation chooses a **random number** between **one and two** before transmitting again.

➔ If the workstations choose the same number, causing another collision by beginning their broadcasts at the same time, they each choose a number between **one and four** and try again.

➔ This process goes on until either the workstations have both successfully completed their transmissions or they have **tried 16 times** without success.

➔If they flunk out by the sixteenth try, both workstations have to pause and **give the other workstations a chance to transmit.**

In short, CSMA/CD is not designed to prevent every collision, but it tries to minimize the time that collisions tie up the network.

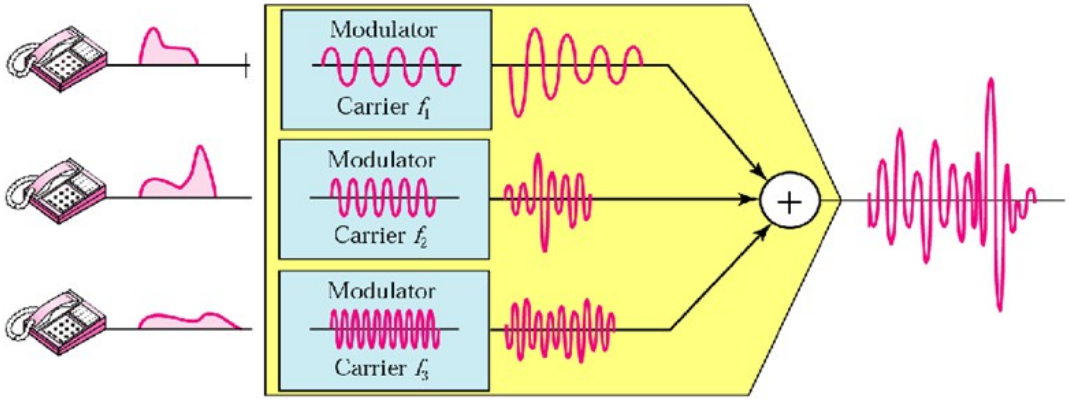
6› What is multiplexing ? Explain FDM. **by Prof. Viral S. Patel**

Ans **Multiplexing** is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link.

Frequency Division Multiplexing – FDM :

➔ It is an analog technique that can be applied when the bandwidth of a link (in hertz) is greater than the combined bandwidths of the signals to be transmitted.

Multiplexing Process :

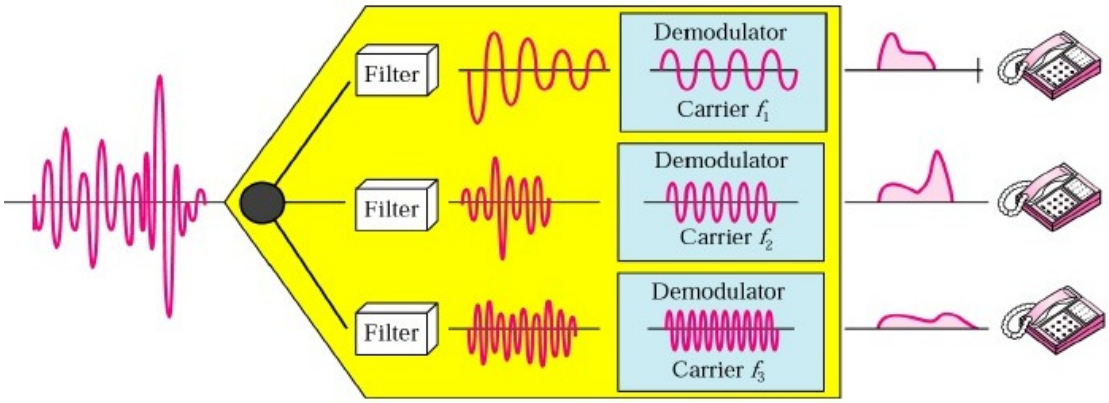


➔ As shown in figure signal generated by each sending device modulated by different carrier frequencies. These modulated signals are then combined into a single composite signal that is send out over a media link that has enough bandwidth to send it.

➔ Channels can be separated by strips of unused bandwidth – guard bads o tp prevent singlas from overlapping.

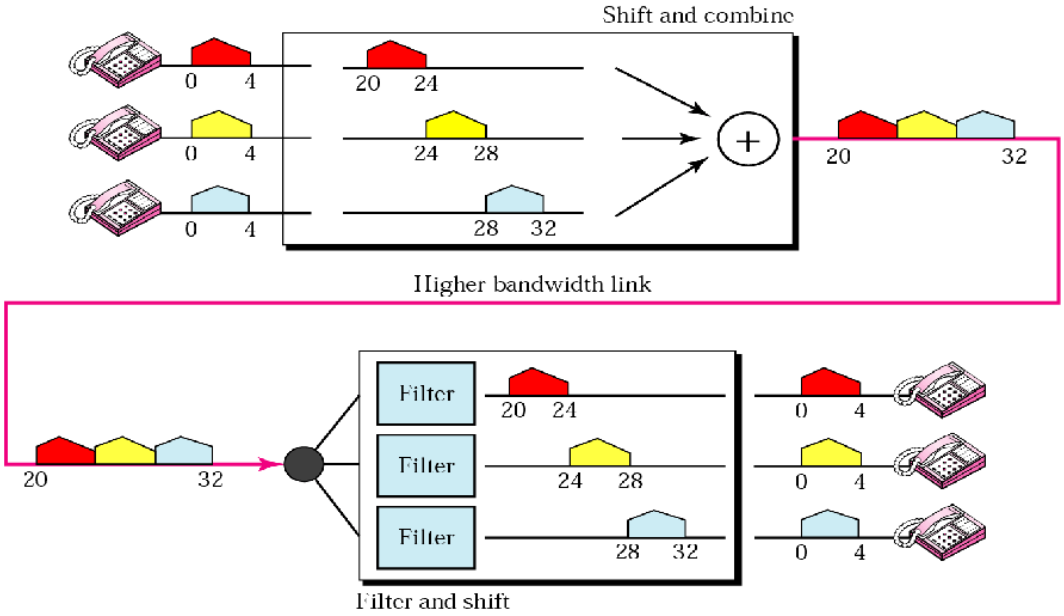
Demultiplexing Process :

➔ The demultiplexer uses a series of filters to decompose the multiplexed signal called demodulater that separates signals from their carriers and passes them to the output lines.



Example :

Assume that a voice channel occupies a bandwidth of 4 kHz. We need to combine three voice channels into a link with a bandwidth of 12 kHz, from 20 to 32 kHz. Assume that there are no guard bands.



Q.3 Answer the following. (Any Three) **[15]**

1› Explain network support layer (physical, datalink and network) of OSI model.

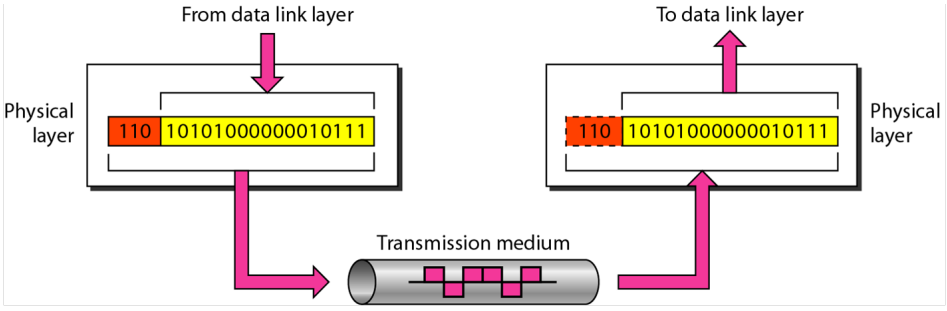
Ans **Network Support Layer of OSI model :**

Physical layer, Data link layer and network layer

Physical Layer :

Type of Transmission media - Physical characteristic of interfaces and medium
Transmission rate (Data rate) – bits per second
Synchronization of bits – sender and receiver use clocks.
Line configuration – point to point , multipoint
Physical topology - mesh, star, ring, bus
Transmission mode – simplex, half-duplex, full-duplex

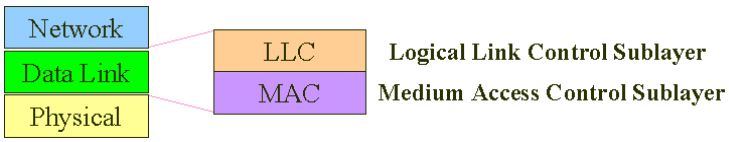
by Prof. Viral S. Patel

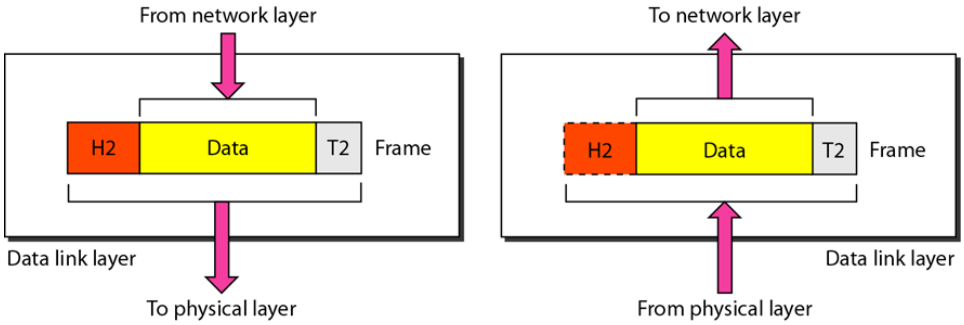


Data link Layer :

Framing : Divides the stream of bits received from network layer into frames.
Physical addressing : adds a header to the frame to define address of sender and/or receiver of the frame.
Flow control : data absorbed by the receiver is less than the rate at which data are produced in the sender managed by flow control mechanism
Error control : trailer added to the end of the frame.
Access control : when more devices are connected to the same link.
Hop-to-Hop (node-to-node) delivery of packet on the same network
LLC sublayer handles error control, flow control, framing and MAC sublayer addressing

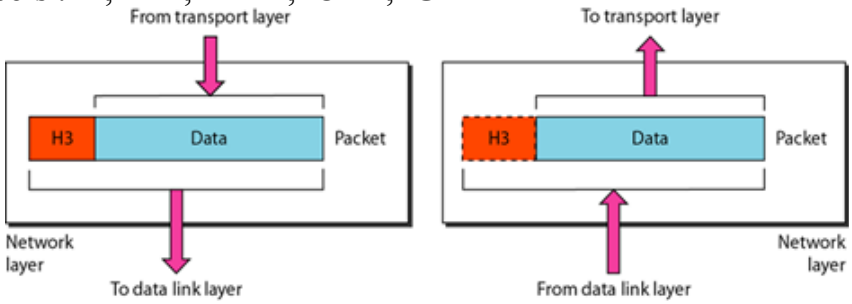
MAC sublayer handles access to share media such as Token passing or Ethernet.





Network Layer : by Prof. Viral S. Patel

Logical addressing : Physical addressing implement by data link layer only handles addressing problem locally but a packet passes the network boundary we need logical addressing (IP address)
Routing : Independent networks are connected by devices (routers) route the packets to their destination.
Source-to-Destination Host delivery of packets across multiple networks.
Protocols : IP, ARP, RARP, ICMP, IGMP



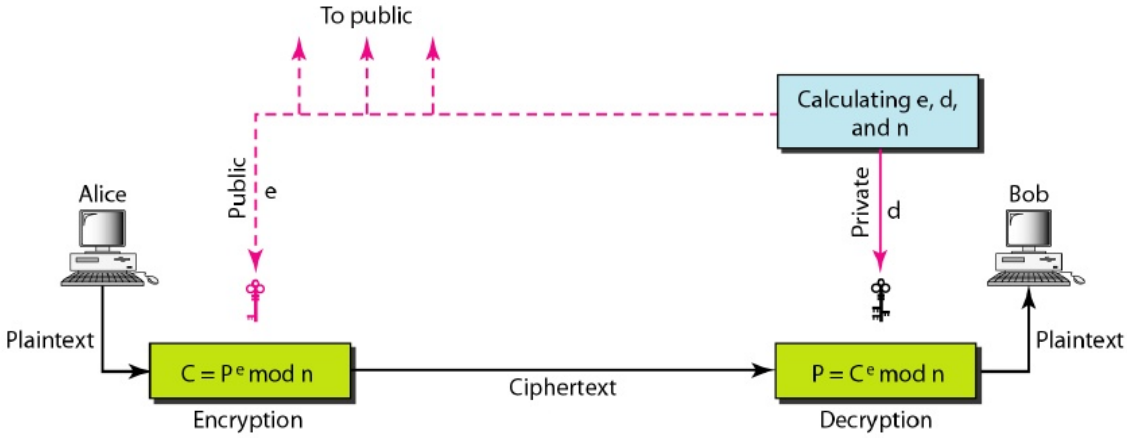
2› Ans Difference between OSI and TCP/IP.

OSI	**TCP/IP**
Open System Interconnection	Transmission Control Protocol / Internet Protocol
The Open Systems Interconnection (OSI) model is a “generic, protocol-independent standard” created by the International Organization for Standardization (ISO) to describe how the different software and hardware components involved in a network communication and interact with one another.	TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
It has 7 layers Application, Presentation, Session, Transport, Network, Data link and Physical layers.	It has 4 layers Application, Transport, Network, Host to Network layers.

OSI model is a reference model	TCP/IP is an implementation of OSI model.
OSI model has a separate Presentation layer and Session layer.	TCP/IP combines the presentation and session layer issues into its application layer
OSI model has separate physical layer and data link layer.	TCP/IP combines the OSI data link and physical layers into the network access layer
It is protocol independent. Protocols are hidden in OSI model and are easily replaced as the technology changes.	It is protocol dependent. In TCP/IP replacing protocol is not easy.
In network layer, OSI support both connectionless and connection oriented communication.	In network layer, TCP/IP support for connection less communication.
OSI is vertical approach.	TCP/IP is horizontal approach.
OSI have strict boundaries.	TCP/IP do not have strict boundaries.
OSI is developed more as a model rather than a protocol suit.	TCP/IP is developed as a protocol suit rather than a model.

3› Explain public key and private key algorithm. By Prof. Viral Patel

Ans RSA (Rivest, Shamir, Adleman) is asymmetric key cryptography algorithm as it used public key and private key.



1. Select two large prime numbers p and q
2. $n = p \cdot q$
3. $\emptyset = (p-1) \cdot (q-1)$
4. Select e such that $e < \emptyset$ and $\gcd(e, \emptyset)=1$
5. Find d such that $d \cdot e \bmod \emptyset = 1$ **or** $d \cdot e = 1 \bmod \emptyset$ **or** $d = e^{-1} \bmod \emptyset$
6. e and n are announced to public. (**e is public key**)
7. d and Ø are kept secret. (**d is private key**)

Encryption : $C = P^e \pmod n$
Decryption : $P = C^d \pmod n$

Example :

➔ p = 7 & q = 11

➔ n = p · q = 7 · 11 = 77

➔ Ø = (p-1) · (q-1) = (7-1) · (11-1) = 60

➔ We can select e = 13
because e < Ø and gcd(e, Ø)=1

➔ d · e mod Ø = 1
d · 13 mod 60 = 1
so, d = 37

Encryption : Plain text = 5

$C = P^e \pmod n$

$= 5^{13} \pmod{77}$

$= 26$

Decryption : Cipher text = 26

$P = C^d \pmod n$

$= 26^{37} \pmod{77}$

$= 5$

by Prof. Viral S. Patel

4› Explain Primary Network Components.

Ans Three primary network components : Servers, Clients and Resources

Servers :

➔Servers are core component of networks the capability of **centralizing the control of resources** and can thus **reduce administrative difficulties**.
➔They can be used to distribute processes for **balancing the load** on the computers and can thus **increase speed and performance**.
➔They can also offer the departmentalizing of files for **improved reliability**.

Servers perform several tasks:
➔For example, servers that provide files to the users on the network are called **file servers.** Servers that provide printing services for users are called **print servers.**

Servers can be multi-purpose or single-purpose :
If they are multi-purpose, they can be, for example, both a file server and a print server at the same time.
If the server is a single-purpose server, it is a file server only or print server only.

Servers is whether they are dedicated or non dedicated:
Dedicated Servers :
Dedicated servers provide specific applications or services

Non-dedicated Servers :
These servers provide one or more network services and local access.

Clients (or workstations) :

➔In network workstations are also known as client computers. As clients, they send request to servers in the network to use the network's resources and access other services.
➔Client have network interface card **(NIC) and client software** to talk on a network.
➔Client (users) on network get some benefits :
They can store more information, because they can now store data on other computers on the network.
They can now share and receive information from other users.
They can use programs that would be too large for their computer to use by itself.

Resources :

➔A resource is any item that can be used on a network.
For examples, **Printers, Files, Applications, Disk storage** etc.
➔Resources can be share on network. For example no need of separate printer to individually. One printer in network can be share and used by every client in network. So cost is reduce.
➔Networks also give more storage space to files.
➔Applications no longer need to be on every computer. Server is capable of handling the overhead of an application requires.

by Prof. Viral S. Patel

5› Explain Wireless media (radio waves, micro waves and infrared).

Ans

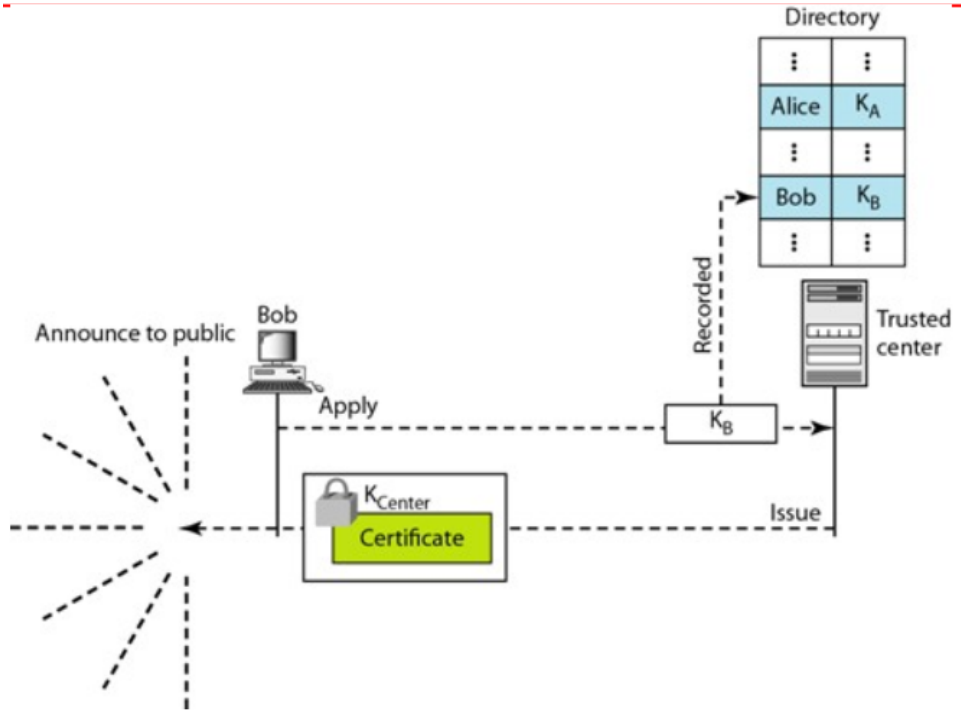
Radio Waves	**Micro Waves**
frequency of radio waves 3 kHz to 1 GHz	Frequency of microwave 1 GHz to 300 GHz
Omni-directional property	Unidirectional (ling-of-sight) property
Radio waves in general have long distance communication capabilities	Repeaters are often needed for long distance communication.
Can penetrate walls	Cannot penetrate walls
Radio band is relatively narrow. Just under 1 GHz, compared to microwave. So subbands are also narrow leading to a low data rate.	Microwave band is relatively wide, almost 299 GHz. So subbands can be assigned and give high data rate.
Radio waves are mostly used in AM and FM radio, television, cordless phones, navigation.	microwaves are used in RADAR, astronomy, cellular phones, satellite communication.
Using any part of the band requires permission from the authorities.	Certain portions of the band requires permission from authorities.
Infrared	
Frequency of Infrared : 300 GHz to 400 THz	
Unidirectional (ling-of-sight) property	
Used in sort range communication system. Useless for long-range communication.	
Cannot use outside a building because the sun's rays contain infrared waves that can interfere.	
Cannot penetrate walls. So cannot be affected by another system in the next room.	
Very high data rate. The standard defined data rate of 75 kbps for a distance of 8 m. The recent standard defines a data rate of 4 Mbps.	

Infrared used in communication between devices such as keyboards, mice, PCs and printers.
IrDA (Infrared Data Association) port that allows a wireless keyboard to communicate with a PC.

Q.4 Answer the following.

a. Explain Digital certificate. **[03]**

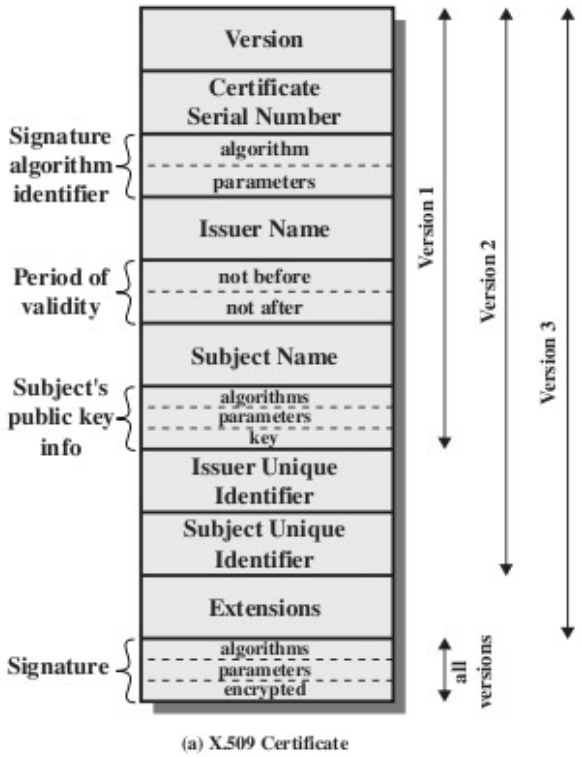
Ans if the number of requests is large for public key then it create a heavy load on the center. The alternative is to create public-key certificates. As shown in figure Bob can go to a Certification Authority (CA) – a federal or state organization that binds a public key to an entity and issues a certificates.



➔The CA has a well-known public key itself that cannot be forged. The CA checks Bob's identification and then asks for Bob's public key and writes it on the certificate. To prevent the certificate itself from being forged, the CA signs the certificate with its private key K_{center}. Now Bob can upload the signed certificate.
➔ Anyone who wants Bob's public key downloads the signed certificate and uses the public key of the center to extract Bob's public key.

X.509 certificate
Universal format ITU has designed a protocol called X.509. It uses a well know protocol called ASN.1 (Abstract Syntax Notation 1) that defines fields familiar to C programmers.

Version : started at 0.Current is 2 (3rd version).
Serial number : unique number given to certificate
Signature : specify algorithm used to sign and its parameters.
Issuer name :name of Certificate Authority
Period of validity : time of certificate valid.
Subject : name of owner / beholder of the public key.
Subject's public key : public key, corresponding algorithm and its parameters.
Issuer Unique identifier : allows two issuers unique identifiers.
Subject unique identifier : allows two different subject unique identifiers
Extension : allows issuer to add more private information
Signature : algorithm identifier, secure hash of other fields and digital signature of that hash.



(a) X.509 Certificate

b. Explain wireless ad-hoc network and wireless sensor network. **[06]**

Ans **Wireless ad-hoc network:**

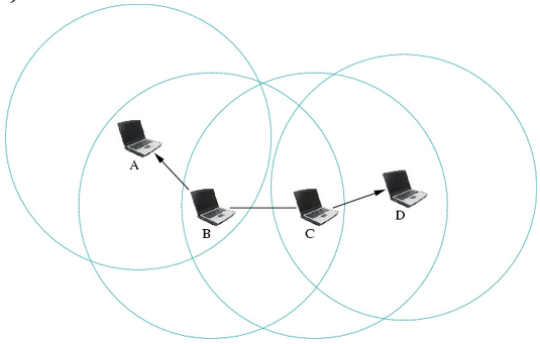
➔ A mobile ad hoc network (MANET) is an autonomous system of nodes connected by wireless links to form a network. Messages are exchanged and relayed between nodes.

➔In fact, an ad hoc network has the capability of making communications possible even between two nodes that are not in direct range with each other, data packets are transmitted from a source to a destination via intermediate nodes.

Intermediate nodes serve as routers using a routing algorithm in this case.

Hence, a MANNET may spread over a large distance, provided that its ends are interconnected by a chain of links between nodes (also called routers).

➔In the ad hoc network shown in figure Node A can communicate with node D via nodes B and C, and vice versa.



Wireless sensor networks:

➔Wireless sensor networks are a special class of ad hoc networks, composed of devices equipped with sensors to monitor temperature, sound or any other environmental condition.

➔Sensor networks are very useful in unpredictable, unreliable environments.
➔Sensor networks are primarily **data collection points**. They are widely used in defense, environment, meteorology and study of nature.
➔A wireless sensor network is a collection of **low-cost, low-power disposable devices.**
➔Each of these devices holds **sensing, memory and communication modules.**
➔Sensors may not have any **power source** other than **small batteries.** Therefore power control is a major challenge in sensor networks to ensure long life of the network.

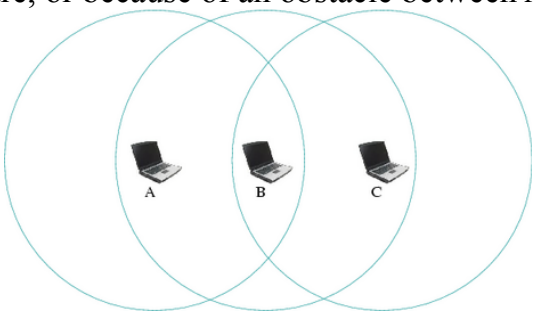
Advantages :
➔The main advantages is that a wireless **network allows the machines to be fully mobile**, as long as they remain in radio range.
➔Even when the machines do not necessarily need to be mobile, a wireless network avoids the burden of having cables between the machines. From this point of view, **setting a wireless network is simpler and faster**.
➔Extending the network is **cheaper**. As there are no wires, there is **no cost for material, installation and maintenance**. To add, remove or displace a machine – is easy.

Prof. Viral S. Patel

Disadvantages :
➔The strength of the radio signal weakens (with the square of the distance), hence the machines have **a limited radio and a restricted scope** of the network.

This causes the well-known **hidden station problem** consider three machines A,B and C, where both A and C are in radio range of B but they are not in radio range of each other.

This may happen because the A-C distance is greater than the A-B and B-C distances, as in figure, or because of an obstacle between A and C.



The hidden station problem occurs whenever C is transmitting: when A wants to send to B, A cannot hear that B is busy and that a message collision would occur, hence A transmits when it should not; and when B wants to send to A, it mistakenly thinks that the transmission will fail, hence B abstains from transmitting when it would not need to.
➔ Wireless networks are also subject to **interferences** by other equipment that shares the same band, such as microwave ovens and other wireless networks.
➔Considering the limited range and possible interferences, the **data rate is often lower than that of a wired network**.
➔Due to limitations of the medium, it is **not possible to transmit and to listen at the same time**, therefore there are higher chances of message collisions.
➔Being mobile computers, the machines have limited battery and computation power. This may generate **high communication latency(delay/wait)** : machines may be off most of the time (i.e. power saving mode) and turning on their receivers periodically, therefore it is necessary to wait until they wake up and are ready to communicate.

➔As data is transmitted over wireless networks are inherently **less secure**.

OR

b. Explain HUB, Bridge and Router.

Ans **HUBs :** (also called a **concentrator or multiport repeater**)

➔Like repeaters, hubs operate at the OSI physical layer, which means they **do not alter or look at the contents** of a packet travelling across the wire.

➔Hubs typically provide from **8 to 24 twisted pair connections.**

➔In **twisted pair** networking, Hubs amplified incoming signals (**same as repeaters**) before they are retransmitted across its ports.

➔Hubs can also be connected to each other by means of BNC (Bayonet Neill Concelman, AUI (attachment unit interface) ports or crossover cables to provide flexibility as networks grow.

➔**Share bandwidth implication** for Collision handling only for small scale, such as eight-port Hub.Tthe amount of bandwidth available to a connected host is inversely proportional to the number of hosts sharing that bandwidth.

For **example** : cascading of four 24-port hubs, where 96 hosts share the same bandwidth (100Mbps). So each hub have only 1.042 Mbps. So throughput is decrease.

➔**Classification of HUBs : Active and Passive**

➔An **active hub** is usually **powered**, and it actually amplifies and clean up the signal it receives. Data can be send long distance in segment compare to passive hub.

➔An **passive hub** is typically **unpowered** and makes only physical, electrical connections. The hub **takes some power away from the signal strength** in order to do its job. Data can be send short distance in segment compare to active hub.

Bridges :

➔Just like a repeater, a bridge is a network device used to connect two network segments.

➔It operate at the **data link layer** of the OSI reference model.

➔Bridges **connect dissimilar media access architectures such as Ethernet and Token Ring**.

➔ The primary use for a bridge is to **maintain traffic**

➔Four types of bridging:

1. **Transparent bridging :** Typically found in **Ethernet** environments, the transparent bridge analyzes the incoming frames and forwards them to the appropriate segments one hop at a time.
   They build a **table of addresses** (bridging table) as they receive packets. If the address is not in the bridging table, the packet is forwarded to all segments other than the one it came from.
2. **Source-route bridging :** Typically found in **Token Ring**, environments. In source-route bridging, each ring is assigned a unique number on the source-route bridge port. The source computer provides **path information** inside the packet. Token Ring frames contain address information, **including a ring number**, to forward the frame to the appropriate ring.
3. **Source-route transparent bridging :** Source-route transparent bridging is an extension of source-route bridging to receive the **routing benefits** of source-route bridging **and** a **performance increase** associated with transparent bridging.
4. **Translation bridging :** Translation bridging is used to connect network segments with different underlying media-access technologies such as

Ethernet to Token Ring or **Ethernet to FDDI** (Fiber Distributed data interface) etc.

➔Bridging is one technique that can **solve the shared-bandwidth problem** that exists with hubs. We cascaded four 24 port hubs through the use of bridges, throughput is therefore increased.

➔Bridges can accommodate a maximum of seven physical segments.

Routers:

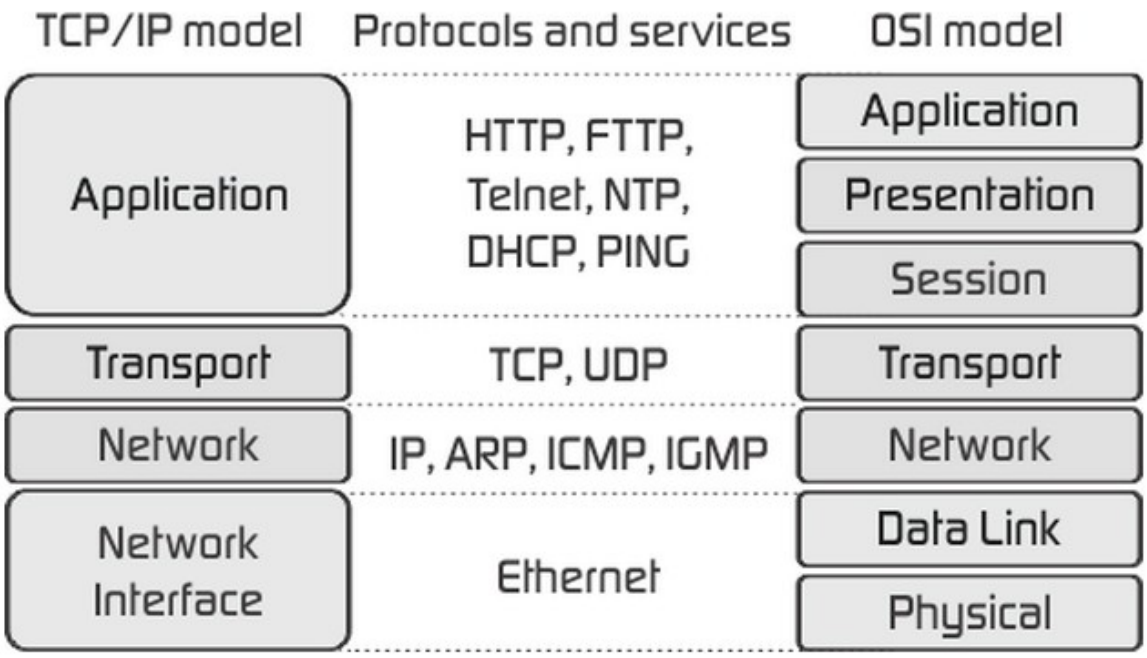
- ➔ The router is the device that **connects multiple networks or segments** to form a large internetwork. Such as internet.
- ➔ Routers are **packet-forwarding devices**. Routers operate at the **network layer** of the OSI reference model, forwarding packets based on network ID.
- ➔ Router have **many functions** other than simply routing packets:
  - Router can **connect many small segments** into a network.
  - Routers can also **connect dissimilar lower-layer topologies**. For example, we can connect an Ethernet and a Token Ring network using a router.
  - Additionally, with added software, routers can perform **firewall functions and packet filtering.**
- ➔ **It makes the decision based on** information contained within its own routing table.

  Routing table are associations of **network IDs and interfaces** that know how to get to that network.
- ➔ By using this table, router **forwards the packet to** either the **intended recipient or** to the **next router** in the chain. Otherwise, the router informs the sender that it doesn't know how to reach the destination network.
- ➔ Routers enabled with the **TCP/IP protocol . IP is responsible** for forwarding or delivering packets.

---

1. Explain TCP/IP protocol suite. (7)

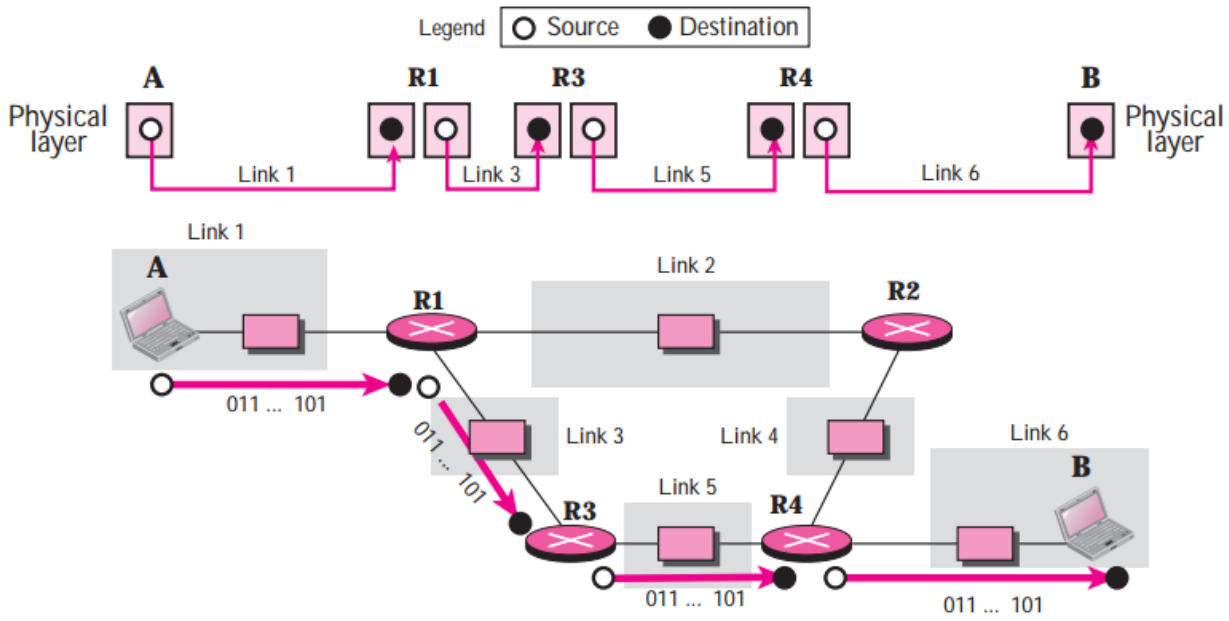
   The TCP/IP protocol suit was developed prior to the OSI model. The original TCP/IP protocol suite was defined as having **four layers** : host-to-network (also called as network access or network interface), internet (also called as network), transport and application.



➔Some times for easy understanding we assume that TCP/IP protocol suit having **five layers** : physical , data link, network, transport and application.
➔The **three topmost layers** in the OSI model represented in TCP/IP by a single layer called the **application layer.**
➔The TCP/IP protocol suite contain relatively independent protocols that can be mixed.
Internet is developed using TCP/IP model.

Physical and Data Link Layers : At the physical and data link layers, TCP/IP does not define any specific protocol. It supports all the standard and proprietary protocols. A network in a TCP/IP internetwork can be a local-area network or a wide area network.

Physical Layer :
➔When the connection is established between the two nodes, a stream of bits is flowing between them. The physical layer, however, treats each bit individually. **The unit of communication is a single bit**. **(Viral S. Patel)**
➔If a node is connected to **n links**, it needs **n physical-layer protocols**, one for each link. The reason is that different links may use different physical-layer protocols.
➔It is the **responsibility** of physical layer to **delivery of bits.**
➔Figure shows the communication between nodes.

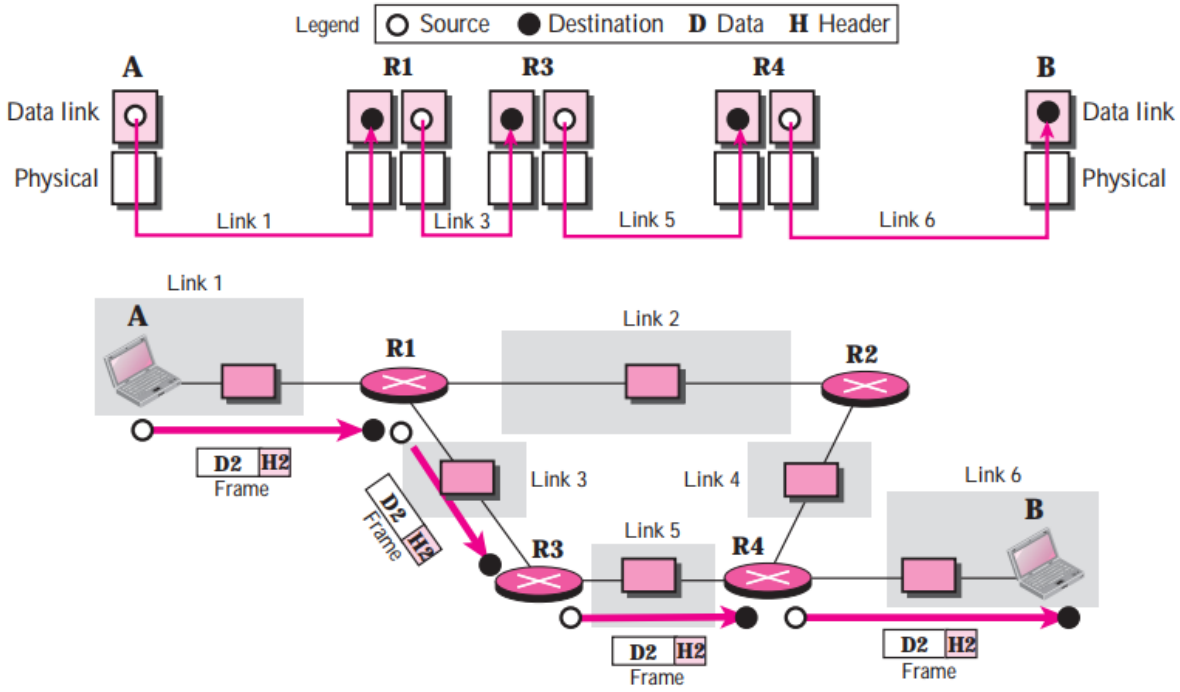


Data Link Layer :

➔The unit of communication is a packet called a **frame.**

➔The frame is a packet that encapsulates the data received from the network layer with an added **header** and sometimes a **trailer**. The head, includes the source and destination physical address. The source address is needed for possible response or acknowledgement.

➔Figure shows the communication at the data link layer.



Network Layer :

➔At the network layer (internetwork layer), TCP/IP supports the Internet Protocol (IP). IP uses four supporting protocols : ARP, RARP, ICMP and IGMP.

➔**Internet Protocol (IP) :** IP transports data in packets called **datagrams,** each of which is transported separately. So the unit of communication at the network layer is a datagram. Datagrams can travel along **different routes** and can arrive **out of sequence or be duplicated.** It is **unreliable and connectionless** protocol – a **best-effort** delivery service. IP **does not keep track** of the routes and has **no facility for reordering** datagrams once they arrive at their destination.

➔**Address Resolution Protocol (ARP) :**

ARP is used to **determine the physical address** (MAC address) of the device only when its IP address is known.

Each device has a physical address imprinted on the Network Interface Card (NIC).

➔**Reverse Address Resolution Protocol (RARP) :**

RARP is used to **determine the IP address** of the host only when the physical address (MAC address) is known. It is useful when the computer is connected to the network for the first time.

➔**Internet Control Message Protocol (ICMP) : (Viral S. Patel)**

This protocol is used by computer and gateways to send notification of datagram problems such as query and **error reporting** messages back to the sending device.

Its only function is to **report problems to the original sender** not to correct them.

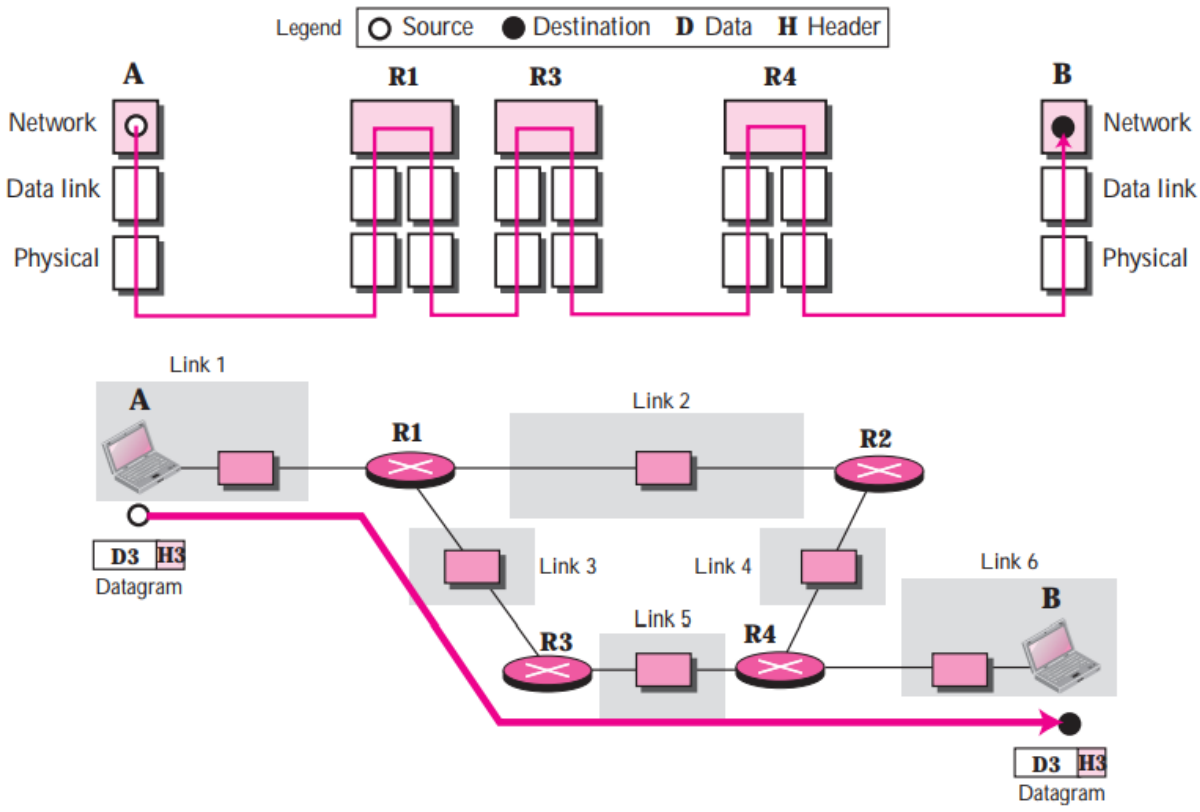
Ping command is an example of ICMP protocol

➔**Internet Group Message Protocol (IGMP) :**

This protocol is used for **multicasting** means to transmit message to multiple recipients at the same time.

Class D IP address is used for this protocol.

➔**Communication** at the network layer is **end to end** while communication at the other two layers are node to node.

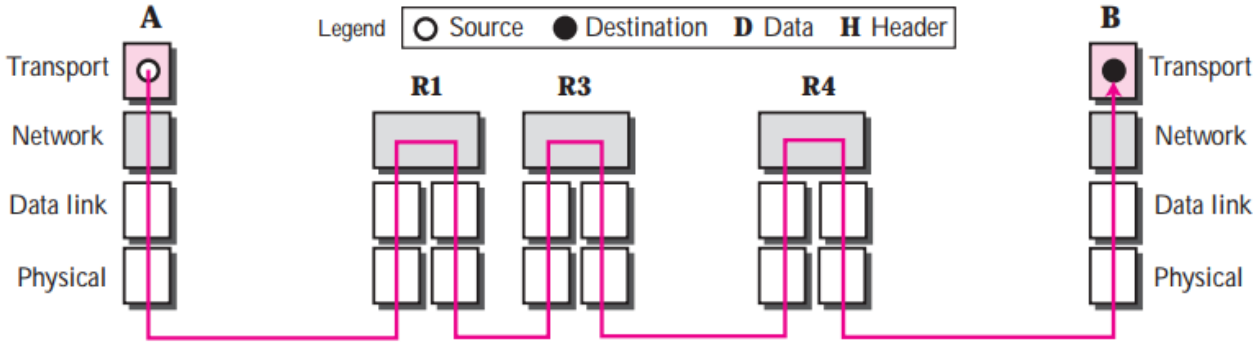


Transport Layer :

➔The transport layer is responsible for delivering the whole message, which is called a segment. (Viral S. Patel)

➔The unit of communication at the transport layer is segment, user datagram or a packet, depending on the specific protocol used in this layer.

➔A segments need to be broken into datagrams and each datagram has to be delivered to the network layer for transmission.



TCP (Transmission Control Protocol) :

➔ TCP is a network communication protocol designed to send data packets over the Internet.

➔ TCP provides **reliable**, full-duplex, **connection-oriented** transport service to upper-layer protocols.

➔ Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same **order** in which they were sent.

UDP (User Datagram Protocol) :

➔ UDP is an alternative communications protocol to TCP to send data packets over the Internet. But **does not acknowledge of their receipt**.

➔ UDP is **unreliable**, **best-effort**, **connection-less** protocol.

➔ There is **no ordering** of messages.

SCTP (Stream Control Transmission Protocol)

➔ It provides support for newer applications such as voice over the internet.

➔ It combines the best features of UDP and TCP.

➔ It is a reliable, message-oriented and byte-oriented protocol.

Application Layer :

It is combined session, presentation and application layers of OSI model. It allows a use to access the services of private internet or the global Internet. The unit of communication at the application layer is a message. Application layer have may protocols, some of which describe following.

FTP (File Transfer Protocol) :

➔The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files between a client and server on a computer network.

SMTP (Simple Mail Transfer Protocol) :

➔SMTP is a communication protocol for mail servers to transmit **email** over the Internet. It is a ASCII (American Standard Code for Information Interchange) based.

MIME (Multipurpose Internet Mail Extensions) :

➔SMTP had some limitation when it came to dealing with binary files e.g. Images because it is ASCII based. MIME allows non-ASCII data such as images, video, audio etc to be sent through e-mail.

Telnet (Terminal Network – for remote logging) : (Viral S. Patel)

➔ Telnet is an underlying TCP/IP protocol for **accessing remote computers.** Through Telnet, an administrator or another user can access someone else's computer remotely on the Internet or local area networks.

POP3 (Post Office Protocol, version 3)

➔ Transfer email messages from a permanent remote mailbox on the server to a local computer or portable device.

(**IMAP4** – Internet Mail Access Protocol, version 4 – is similar to POP3, but it has more features, more powerful and more complex)

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

HTTP (Hypertext Transfer Protocol) :

➔HTTP is the set of **rules for transferring files** (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.

➔This protocol defines **how messages are formatted and transmitted,** and what actions Web servers and browsers should take in response to various commands.

➔HTTP is called a **stateless protocol** because each command is executed independently, without any knowledge of the commands that came before it.