TRANSMISSION MEDIA

The cables/media which is used to connect the computers in a network called Transmission Media/Communication Channel.

Communication media are divided into two categories:

(i) **Guided/ Wired Media** - it includes cables.
(ii) **Unguided/Wireless technologies** – It include waves through air, water or vacuum.

GUIDED MEDIA

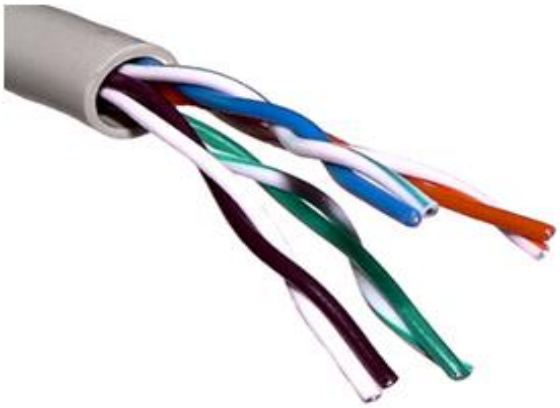
1. Twisted Pair Cable
2. Coaxial Cable
3. Optical Fibers

UNGUIDED MEDIA

1. Microwave
2. Radio wave
3. Satellite
4. Infrared
5. Laser
6. Bluetooth

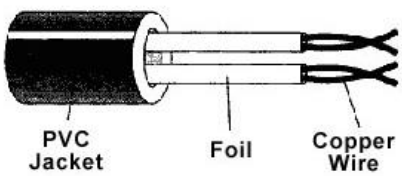
Twisted Pair Cable

- Most common form of wiring in data communication.
- It consists of two identical wires wrapped together in a double helix.



-

- A special type of twisted pair cable known as **CAT5** or **CAT6** is mostly used in a specific type of LAN namely **Ethernet**, hence it is also known as ***Ethernet cable.***



Why the wires are twisted in TWISTED PAIR CABLE?

The twisting of wires reduces **Crosstalk**. The bleeding of a signal from one wire to another and which can corrupt signal and cause network errors. This form of signal interference is called **Crosstalk.**

ADVANTAGES

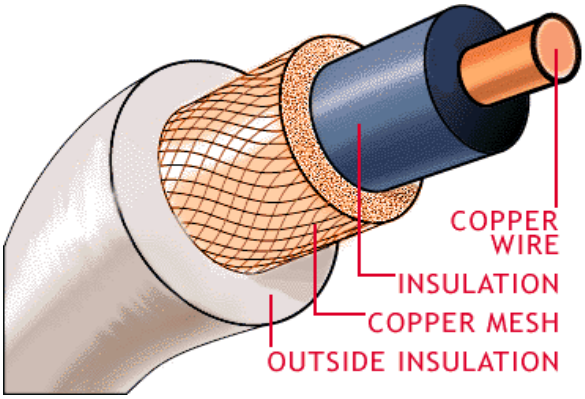
1. It has low weight.
2. It is very inexpensive.
3. It is easy to install and maintain.

DISADVANTAGES

1. Because of high attenuation (weakening of signal), it is incapable carrying a signal over long distances without the use of repeaters.
2. It has low bandwidth (data carrying capacity) capabilities.

COAXIAL CABLE

- This type of cable consists of a solid wire core surrounded by one or more wire shields, each separated by some kind of plastic insulator. The inner core carries of the cable carries the signal.



- This cable has high electrical properties and is suitable for high speed communication. It is widely used for television signals.

ADVANTAGES

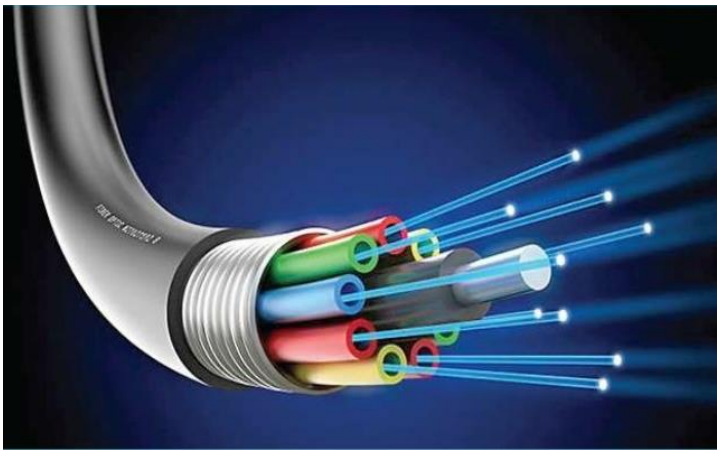
1. It provides higher bandwidths as compared to twisted pair cable.
2. The data transmission characteristics of coaxial cables are considerably better than those of twisted pair cables.
3. The coaxial cables can be used for broadband transmission.

DISADVANTAGES

1. Expensive compared to twister pair cables.
2. The coaxial cables are not compatible with twisted pair cables.

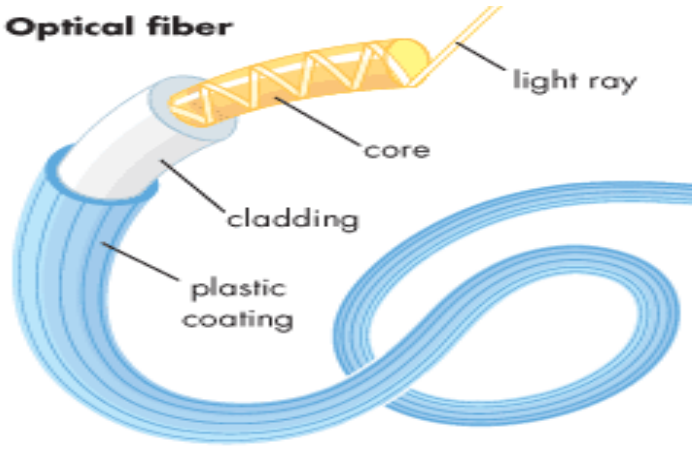
OPTICAL FIBERS

- It consist of thin strands of glass which are used to carry light from a source at one end of the fiber to a detector at the other end. The bandwidth of this medium is very high.



The fiber cable consists of three pieces:

1. **Core** : the glass strand through which the light travels.
2. **Cladding** : which is a covering of the core that reflects light back to the core.
3. **Protective coating** : which protects the fiber cable from hostile environment.



ADVANTAGES

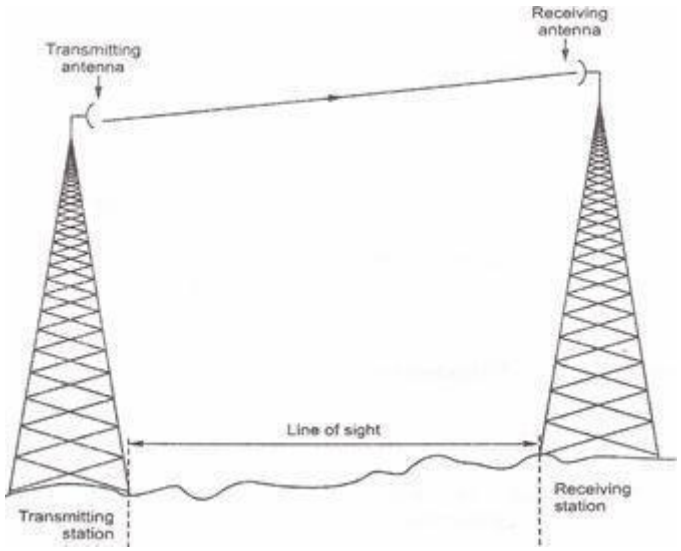
1. It is immune to electrical and magnetic interference i.e., noise in any form because the information is travelling on a modulated light beam.
2. It guarantees secure transmission and has a very high transmission capacity.
3. It is highly suitable for harsh industrial environments.

DISADVANTAGES

1. Optical fibers are quite fragile and may need special care in installation.
2. Because of noise immunity, optical fibers are virtually impossible to tap.
3. They are the most expensive of all the cables.

MICROWAVE

- Microwave signals are wireless transmission media and are used for long distance transmission. The microwave transmission consists of a transmitter, receiver and the atmosphere.



- In microwave communication, parabolic antennas are mounted on towers to send a beam to other antennas tens of kilometers away. The higher the tower, the greater the range. With a 100-meter high tower, distances of 100 km between towers are feasible.

- The microwave transmission is line of sight transmission.

ADVANTAGES

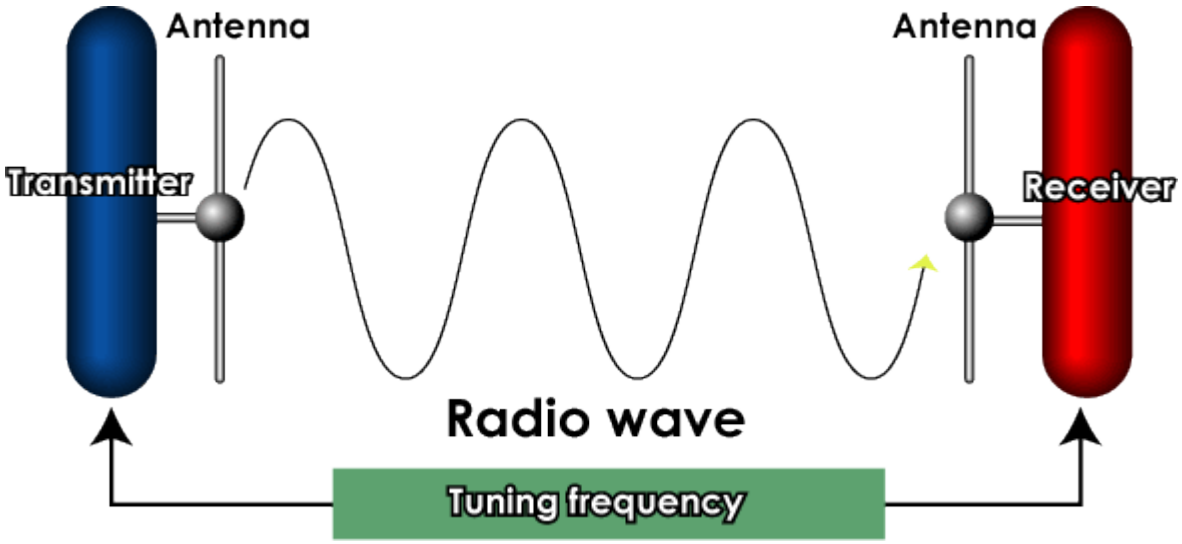
1. This transmission media proves cheaper than digging trenches for laying cables.
2. It offers ease of communication over difficult terrain.

DISADVANTGES

1. Microwave communication is an insecure communication.
2. Microwave signals is susceptible to weather effects like rains, thunderstorms etc.

RADIO WAVE

- This transmission media make use of radio frequencies. In this transmission continuous sine waves are used to transmit information.
- Transmission through radio wave consist two parts : (i) transmitter (ii) receiver



- The transmitter takes some sort of message (it could be the sound of someone's voice, pictures for a TV set etc.), encodes/change it onto a sine wave and transmits it with radio waves. The receiver receives the radio waves and decodes the message from the sine wave it receives. Both the transmitter and receiver use antennas to radiate and capture the radio signal.

ADVANTAGES

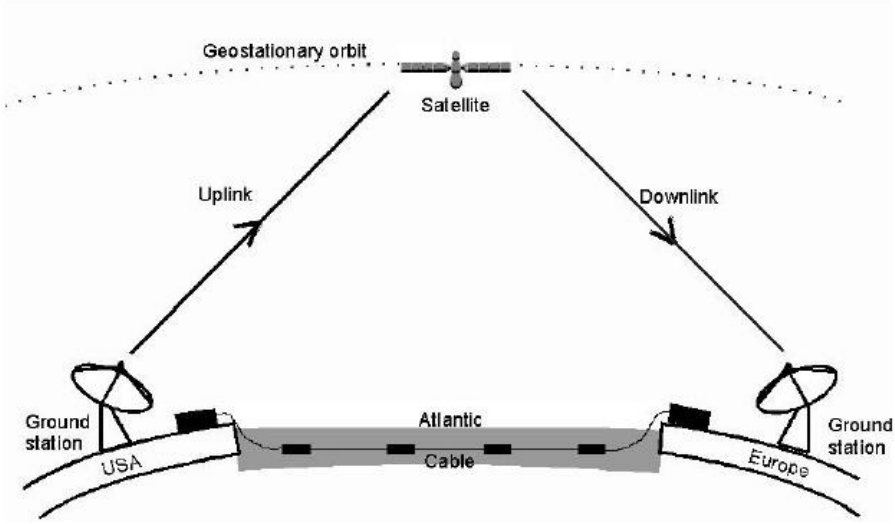
1. This transmission media proves cheaper than digging trenches for laying cables.
2. It offers ease of communication over difficult terrain.

DISADVANTAGES

1. Radio wave communication is an insecure communication.
2. Radio wave signals is susceptible to weather effects like rains, thunderstorms etc.

SATELLITE

- Satellite communication is special case of microwave relay system. It satellite communication the earth station consists of a satellite dish that functions as an antenna and communication equipment to transmit and receive data from satellites passing overhead.



- The satellites accept data/signals transmitted from an earth station, amplify them, and retransmit them to another earth station.

ADVANTAGES

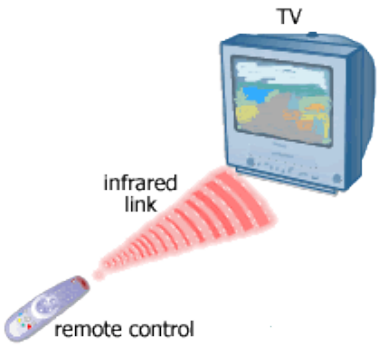
1. The area coverage through satellite transmission is quite large.
2. The laying and maintenance of intercontinental cable is difficult and expensive and this is where the satellite proves to be the best alternative.

DISADVANTAGES

1. The costs associated with satellites are significantly high.

INFRARED

- This type of transmission uses infrared light to send data. TV remotes, automatic garage doors, wireless speakers etc., all make use of infrared as transmission media.



- The infrared light transmits data through the air and can propagate throughout a room , but will not penetrate walls.

LASER

- The laser transmission requires direct line of sight. It is unidirectional like microwave, but has much higher speed than microwaves.

BLUETOOTH

- Bluetooth is a telecommunication industry specification that describes how mobile phones and computers can be easily interconnected using a short range wireless connection.

- The maximum range of connection is 10 meters. Data can be exchanged at a rate of 1 megabit per second.

NETWORK DEVICES

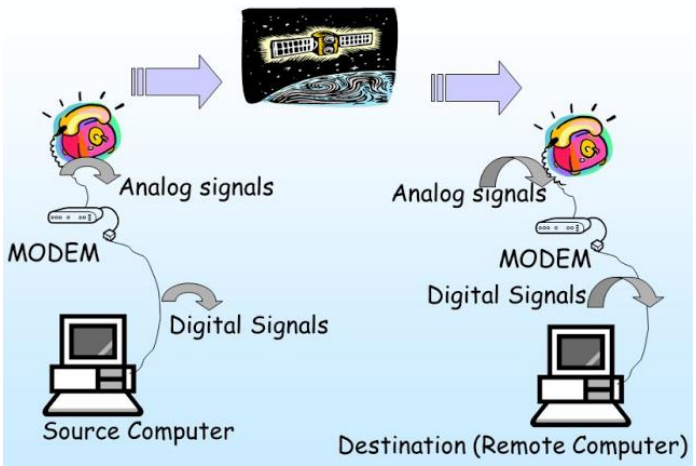
1. **MODEM**

- A modem is a computer peripheral that allows you to connect and communicate with other computers via telephone lines.

Working of Modem

- Because ordinary telephone lines cannot carry digital information, a modem changes the digital data from your computer into analog data, a format that can be carried by telephone lines. In similar manner, the modem receiving the data then changes the analog signal back into digital data that the computer can understand.

MO – Modulation DEM- Demodulation



Modem comes in two varieties:

a) **Internal Modem**: Those which are fixed within the computer.

b) **External Modem**: The modems that are connected externally to a computer.

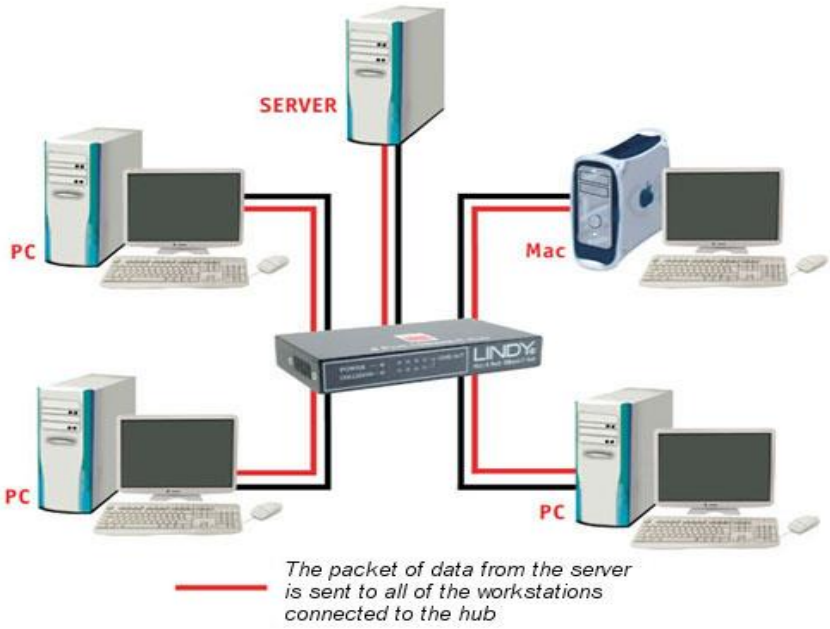
2. HUB

- A hub is a hardware device used to connect several computers together. Hubs can be either passive or active.

Active hubs : It electrically amplify then signal as it moves from one connected device to another.
Passive hubs : It allow the signal to pass from one computer to another without any change.

FUNCTIONING OF HUB

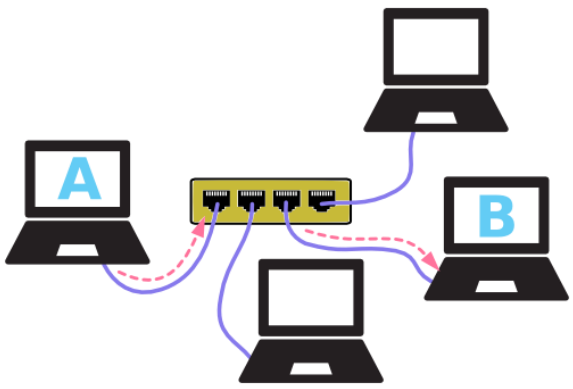
- Hubs forward any data packets, they receive over one port from one workstation to all of their remaining ports. It means all the workstations connected to the Hub will receive the packet/message.



3. <u>SWITCH</u>

- A switch is a device that is used to segment networks into different sub-networks called subnets or LAN segments. A switch is responsible for filtering i.e., transforming data in a specific way and forwarding packets between LAN segments.

- ***Switch is also called an intelligent Hub*** because it delivers the data packets only to the intended workstation connected in a network, not to all workstations connected.



4. REPEATER

- A repeater is a network device that amplifies and restores signals for long distance transmission.

Working of Repeater

- Over distance, the cables connecting a network lose the signal transmitted. If the signal degrades too much, it fails to reach the destination. So, Repeaters can be installed along the way to ensure that data packets reach their destination.

Repeater are of two kinds:

1. **Amplifier** - It amplifies both the signal and any concurrent noise.
2. **Signal Repeater** – It only amplify the desired message/signal.

5. GATEWAY

- A Gateway is a network device that connects dissimilar networks. It establishes an intelligent connection between a local network and external networks with completely different structures.

- A gateway is actually a node on a network that serves as an entrance to another network. In homes, the gateway is the ISP that connects the user to the Internet.

6. BRIDGE

- A bridge is a device, which is used to connect two local-area networks or two segments of the same LAN. But LAN segments connected by a bridge must follow the same protocol.

- A bridge allows to cross only that data which has a valid MAC address of other side of Bridge.

7. ROUTER

- A Router is a network device that connects multiple networks irrespective of their protocol. This is because a router can handle different protocols.

- A Router forwards data packets from one connected network to another depending upon their IP addresses and not their MAC addresses.

NETWORK SECURITY

- Network Security means the ability of a system to protect information and system resources with respect to confidentiality and integrity.

TYPES OF ATTACKS ON NETWORKS

1. **Intrusion Problem/Access Attacks**

   When a unauthorized user attempts to gain access to protected sensitive information, it is known as Access Attack or Intrusion Problem.

   Some common intrusion/access attacks are :

   (i) **Snooping**- It refers to opening and looking through files in unauthorized manner. It may involve things like casually observing someone else's email or monitoring activity of someone else computer through a sophisticated software.

(ii) **Eavesdropping** – Eavesdropping is the act of secretly listening/intercepting someone else's private communication/data/information.

2. **Denial of Service(DoS) Attacks**

DoS Attacks are those attacks that prevent the legitimate users of the system, from accessing or using the resources, information, or capabilities of the system. There can be different forms of DoS attacks:

(i) **Denial of Access to Information** – This type of DoS attack causes the information on a system to be unavailable.

(ii) **Denial of Access to Applications** – This type of DoS attack targets the applications that manipulate or displays information.

(iii) **Denial of Access to System** – In this type of DoS attack, the system along with all applications that run on the system and all the information that is stored on the system become unavailable.

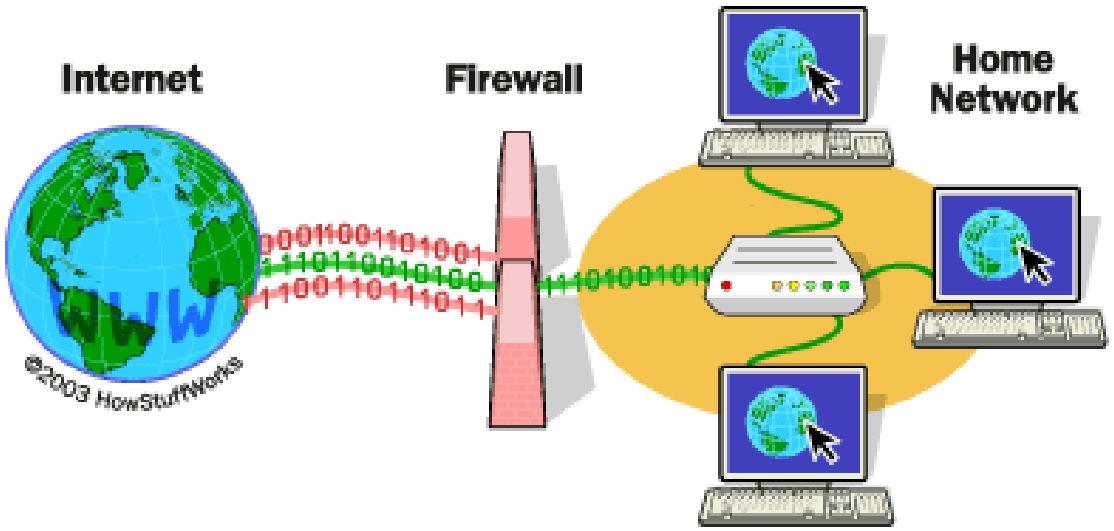
(iv) **Denial of Access to Communications** - This type of attack involves cutting a wire or jamming radio communication etc.

NETWORK SECURITY MEASURES

Two Techniques used for network security are : 1. **Active Protection** 2. **Preventive Protection**

ACTIVE PROTECTION

1. **Authorization** – Asking the user a legal login id performs authorization. If the user is able to provide a legal login id, he/she is considered an authorized user.
2. **Authentication** – Authentication is also termed as password protection as the authorized user is asked to provide a valid password, and if he/she is able to do this, he/she is considered to be an authentic user.
3. **Firewall** – A system designed to prevent unauthorized access to or from a private network is called Firewall.



4. **Intrusion Detection** – It is the art and science of sensing when a system or network is being used inappropriately or without authorization.

PREVENTIVE PROTECTION

1. Use proper File access permission when sharing files on the Internet – File access permissions refer to privileges that allow a user to read, write or execute a file.
2. Disconnect from the Internet when away

LAST YEAR PRE-BOARD & BOARD QUESTIONS ASKED FROM ABOVE TOPICS

Q1. Differences between the following:

(i) Star Topology and Bus Topology
(ii) Ring Topology and Star Topology
(iii) LAN and WAN

Q2. Define the following:

(i) Node
(ii) Network
(iii) Server
(iv) Domain name
(v) Snooping
(vi) Eavesdropping
(vii) Dos

Q3. Explain any 2 security threats to Computer networks.
Q4. What do you understand by firewall?
Q5. Give one advantage and one disadvantage of using Star topology over Bus Topology.
Q6. Name two wireless transmission media.
Q7. What is a modem? What is its function?
Q8. What is the function of a Repeater?
Q9. Read the given activities carefully and mention whether the activity is snooping or eavesdropping:

(i) Getting someone's login information by casually watching what he/she is typing.

(ii) Setting up unauthorized parallel telephone lines.

(iii) Installing some software/hardware which captures the data while on its way.

(iv) Reading the files on someone's computer in an unauthorized manner.

Q10. Give one advantage and one disadvantage of optical fiber cable and coaxial cable used in communication.

Q11. What are hubs? What are its types?

Q12. What is the role of a switch in a network?

Q13. What do you understand by Network Security? Name two common threats to it.

Q14. What is the difference between Domain name and URL?

Q15. Identify the following devices:

(i) An intelligent device that connects several nodes to form a network and redirects the received information only to intended node(s).

(ii) A device that regenerates (amplifies) the received signal and re-transmits it to its destination.

(iii) A device that is used to connect different types of networks. It performs the necessary translation so that the connected networks can communicate properly.

(iv) A device that converts data from digital bit stream into an analog signal and vice versa.

Q16. Why a switch is called an intelligent hub?

Q17. Ms. Kant Sengupta wants to prevent unauthorized access to/from his company's local area network. Write the name of a system (software/hardware), which he should install to do the same.

****