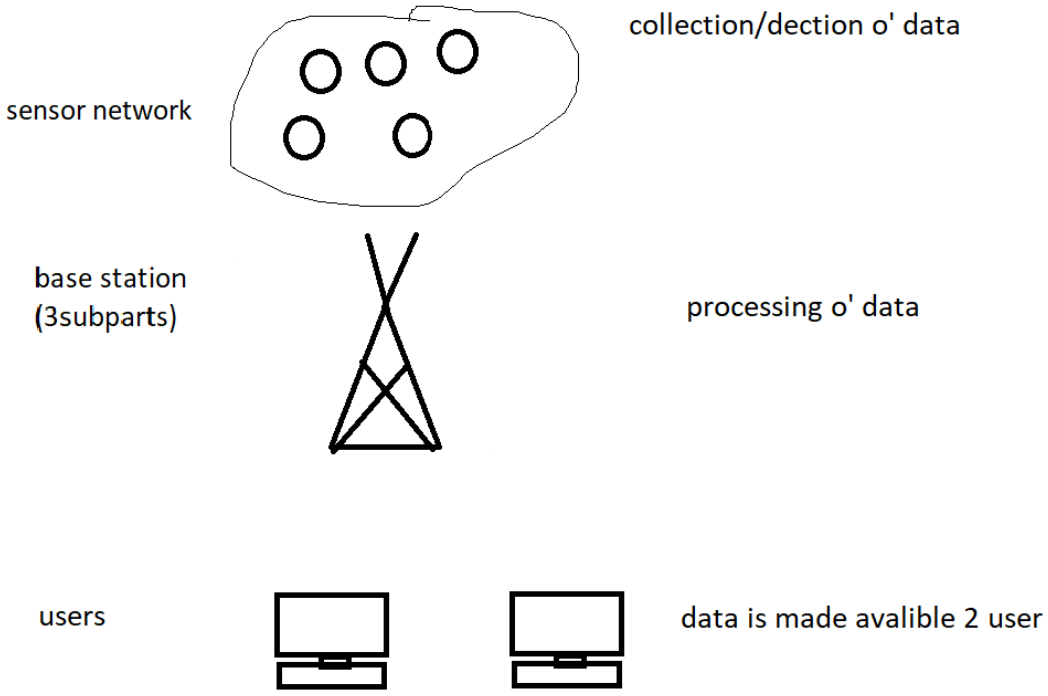
1. The architecture of WSN / working of WSN?

Ans-

1. When a large number of sensor nodes are deployed in a large area to monitor a physical environment, the networking of these sensor nodes is equally important.
2. A sensor node in a WSN not only communicates with other sensor nodes but also with a Base Station (BS) using wireless communication.
3. The base station sends commands to the sensor nodes and the sensor node perform the task by collaborating with each other.
4. The sensor nodes in turn send the data back to the base station. A base station also acts as a gateway to other networks through the internet.
5. After receiving the data from the sensor nodes, a base station performs simple data processing and sends the updated information to the user using internet.
6. If each sensor node is connected to the base station, it is known as Single-hop network architecture.
7. Hence, Multi-hop network architecture is usually used. Instead of one single link between the sensor node and the base station, the data is transmitted through one or more intermediate node.

Diagram of architecture of wsn



2) What is Manet?

Ans-

- MANET stands for Mobile Adhoc Network also called a wireless Adhoc network or Adhoc wireless network that usually has a routable networking environment on top of a Link Layer ad hoc network.
- They consist of a set of mobile nodes connected wirelessly in a self-configured, self-healing network without having a fixed infrastructure.
- MANET nodes are free to move randomly as the network topology changes frequently. Each node behaves as a router as they forward traffic to other specified nodes in the network

- MANET may operate a standalone fashion or they can be part of larger internet. They form a highly dynamic autonomous topology with the presence of one or multiple different transceivers between nodes.

- The main challenge for the MANET is to equip each device to continuously maintain the information required to properly route traffic.

Pros:

1. Separation from central network administration.
2. Each node can play both the roles ie. of router and host showing autonomous nature.
3. Self-configuring and self-healing nodes do not require human intervention.
4. Highly scalable and suits the expansion of more network hub.

Cons:

1. Resources are limited due to various constraints like noise, interference conditions, etc.
2. Lack of authorization facilities.
3. More prone to attacks due to limited physical security.
4. High latency i.e. There is a huge delay in the transfer of data between two sleeping nodes

Advantages:

Flexibility: MANETs are highly flexible, as they can be easily deployed in various environments and can be adapted to different applications and scenarios.
Scalability: MANETs can easily scale to accommodate a large number of nodes, making them suitable for large-scale deployments.
Cost-effective: Since MANETs do not require any centralized infrastructure, they are often more cost-effective than traditional wired or wireless networks.
Rapid Deployment: MANETs can be rapidly deployed in areas where infrastructure is not available, such as disaster zones or rural areas.

Disadvantages:

Security: MANETs are vulnerable to security threats, such as attacks by malicious nodes, eavesdropping, and data interception.
Reliability: MANETs are less reliable than traditional networks, as they are subject to interference, signal attenuation, and other environmental factors that can affect the quality of the connection.
Bandwidth: Since MANETs rely on wireless communication, bandwidth can be limited..
Routing: Routing in MANETs can be complex, particularly when dealing with dynamic network topologies.
Power Consumption: Since MANETs rely on battery-powered devices, power consumption can be a significant issue.

3) RIP (routing information protocol)?

Ans –

- Routing Information Protocol (RIP) is one of the oldest distance-vector routing protocols which employs the hop count as a routing metric.
- RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination.
- The largest number of hops allowed for RIP is 15, which limits the size of networks that RIP can support
- RIP implements the split horizon, route poisoning, and hold down mechanisms to prevent incorrect routing information from being propagated.
- In RIPv1 routers broadcast updates with their routing table every 30 seconds. In the early deployments, routing tables were small enough that the traffic was not significant.
- As networks grew in size, however, it became evident there could be a massive traffic burst every 30 seconds, even if the routers had been initialized at random times.
- In most networking environments, RIP is not the preferred choice of routing protocol, as its time to converge and scalability are poor compared to EIGRP, OSPF, or IS-IS.
- However, it is easy to configure, because RIP does not require any parameters, unlike other protocols.
- RIP uses the User Datagram Protocol (UDP) as its transport protocol, and is assigned the reserved port number 520.

4) BGP(border gateway protocol)?

Ans-

- BGP (Border Gateway Protocol) is the protocol underlying the global routing system of the internet. It manages how packets get routed from network to network through the exchange of routing and reachability information among edge routers.
- BGP directs packets between autonomous systems (AS), which are networks managed by a single enterprise or service provider.
- BGP creates network stability by guaranteeing routers can adapt to route failures: when one path goes down, a new path is quickly found.
- BGP makes routing decisions based on paths, defined by rules or network policies set by network administrators

How it works?

- Each router maintains a routing table controlling how packets are directed. Routing table information is generated by the BGP process on the router, based on incoming information from other routers, and information in the
- BGP routing information base (RIB), which is a data table stored on a server on the BGP router.
- The RIB contains information both from directly connected external peers, as well as internal peers, and based on policies for what routes should be used and what information should be published, continually updates the routing table as changes occur.

What is BGP used for?

- BGP offers network stability that guarantees routers can quickly adapt to send packets through another reconnection if one internet path goes down.
- BGP makes routing decisions based on paths, rules or network policies configured by a network administrator.
- Each BGP router maintains a standard routing table used to direct packets in transit. BGP uses client-server topology to communicate routing information, with the client-server initiating a BGP session by sending a request to the serve

5)Tiny OS

Ans –

- TinyOS is an embedded component-based operating system and platform for low-power wireless devices in wireless sensor networks (WSNs), ubiquitous computing, personal area networks, building automation and smart meters.
- It is written in the programming language nesC, as a set of cooperating tasks and processes. It was collaboration between the University of California, Berkeley, Intel Research and Crossbow Technology.
- It was released as open-source software under BSD license and has grown into an international consortium, the TinyOS Alliance. TinyOS has been used in space, being implemented in ESTCube1

Features of TinyOS

- TinyOS applications are written in the programming language nesC a dialect of C language optimized for the memory limits of sensor networks.
- Its supplementary tools are mainly in the form of Java and shell script front-ends. The associated libraries and tools are mostly written in C.
- TinyOS programs are built of software components and they present hardware abstractions. Components are connected to each other using interfaces.
- TinyOS provides interfaces and components for common abstractions such as packet communication, routing, sensing, actuation and storage.

Characteristics of TinyOS

- TinyOS is fully non-blocking and it has one call stack. All I/O operations are asynchronous and have a callback.
- TinyOS uses nesC's features to link these callbacks called events to enable the native compiler for better optimization, TinyOS forces programmers to write complex logic by combining together many small event handlers.
- TinyOS provides tasks similar to a Deferred Procedure Call in order to support larger computations,. Tasks are non-preemptive and run in first in first out order.

6) Multiplexing and demultiplexing

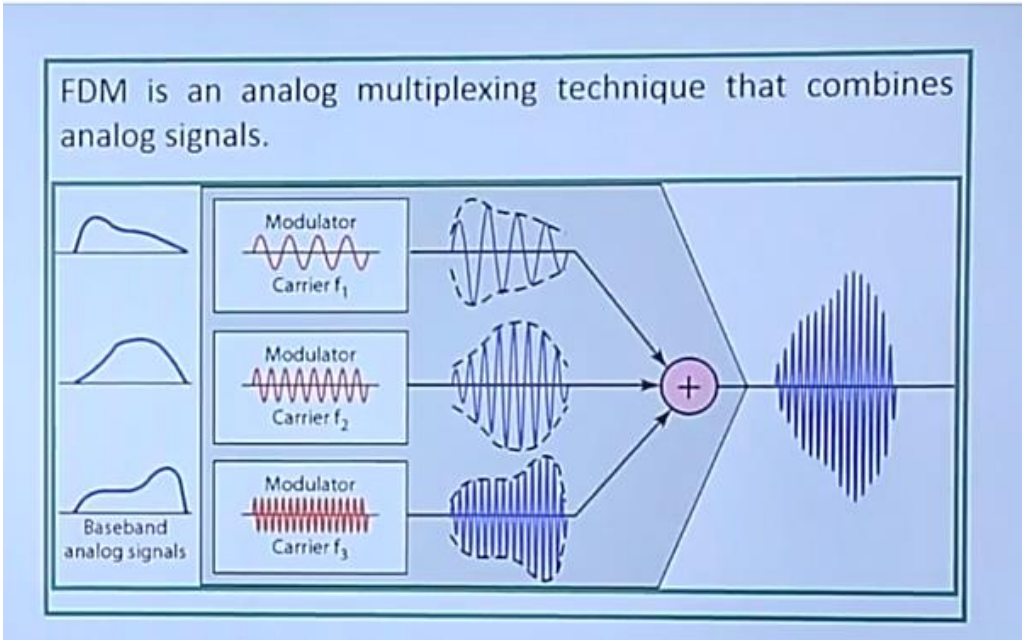
Ans –

- In telecommunications and computer networks, **multiplexing** (sometimes called as **muxing**) is a method by which multiple analog or digital signals are combined into one signal over a shared medium.
- It is the process in which multiple signals coming from multiple sources are combined and transmitted over a single communication/physical line.
- Multiplexing is a method used by networks to consolidate multiple signals digital or analog into a single composite signal that is transported over a common medium, such as a fiber optic cable or radio wave. When the composite signal reaches its destination, it is demultiplexed, and the individual signals are restored and made available for processing
- For example, in telecommunications, several telephone calls may be carried using one wire.
- The multiplexed signal is transmitted over a communication channel such as a cable.

- Multiplexing is used in a wide range of industries to facilitate both analog and digital communications. It was first introduced in the 1870s to support telegraphy but has since become a mainstay in telecommunications, such as radio, television and telephone.

<u>Types of Multiplexing</u>

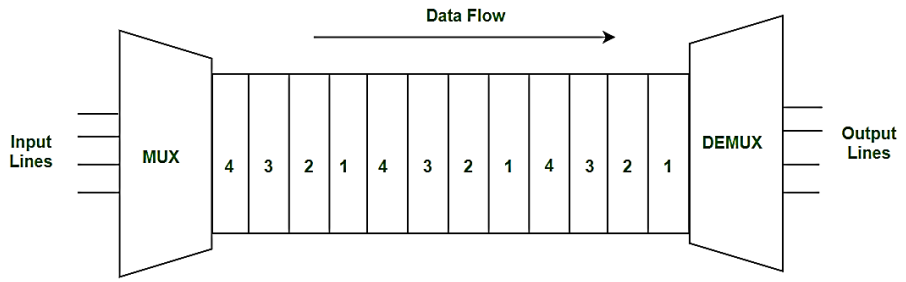
1) Frequency Division Multiplexing (FDM)



- Frequency division multiplexing is defined as a type of multiplexing where the bandwidth of a single physical medium is divided into a number of smaller, independent frequency channels.
- Frequency Division Multiplexing is used in radio and television transmission.
- In FDM, we can observe a lot of inter-channel cross-talk, due to the fact that in this type of multiplexing the bandwidth is divided into frequency channels. In order to prevent the inter-channel cross talk, unused strips of bandwidth must be placed between each channel. These unused strips between each channel are known as guard bands.

2) ***Time Division Multiplexing (TDM) :***

- Time-division multiplexing is defined as a type of multiplexing wherein FDM, instead of sharing a portion of the bandwidth in the form of channels, in TDM, time is shared. Each connection occupies a portion of time in the link.
- In Time Division Multiplexing, all signals operate with the same frequency (bandwidth) at different times.



There are two types of Time Division Multiplexing :

- Synchronous Time Division Multiplexing
- Statistical (or Asynchronous) Time Division Multiplexing

Synchronous TDM :

Synchronous TDM is a type of Time Division Multiplexing where the input frame already has a slot in the output frame. Time slots are grouped into frames. One frame consists of one cycle of time slots.

Statistical TDM :

Statistical TDM is a type of Time Division Multiplexing where the output frame collects data from the input frame till it is full, not leaving an empty slot like in Synchronous TDM.

7) LEACH routing protocol / heirarchial routing protocol ?

Ans- Low energy adaptive clustering hierarchy (LEACH)

- LEACH is a routing protocol that organizes the cluster such that the energy is equally divided in all the sensor nodes in the network. In LEACH protocol several clusters are produced of

sensor nodes and one node defined as cluster head and act as routing node for all the other nodes in the cluster.

- As in routing protocols the cluster head is selected before the whole communication starts and the communication fails if there is any problem occurs in the cluster head and there is much chances that the battery dies earlier as compare to the other nodes in cluster as the fix cluster head is working his duties of routing for the whole cluster.
- LEACH protocol apply randomization and cluster head is selected from the group of nodes so this selection of cluster head from several nodes on temporary basis make this protocol more long lasting as battery of a single node is not burdened for long.
- Sensor nodes elect themselves as cluster head with some probability criteria defined by the protocol and announce this to other nodes

8) SPIN routing protocol / Data centric?

Ans-

- SPIN is abbreviation of sensor protocol for information via negotiation. This protocol is defined to use to remove the deficiency like flooding and gossiping that occurs in other protocols.
- The main idea is that the sharing of data, which is sensed by the node, might take more resources as compare to the meta-data, which is just a descriptor about the data sensed, by the node.
- The resource manager in each node monitors its resources and adapts their functionality accordingly.
- Three messages namely ADV, REQ and DATA are used in SPIN. The node broadcast an ADV packet to all the other nodes that it has some data.
- This advertising node ADV message includes attributes of the data it has. The nodes having interests in data, which the advertising node has requested by sending REQ message, to the advertising node. On receiving the REQ message the advertising node send data to that node. This process continues when the node on reception of data generate an ADV message and send it.

9) Flat architecture?

Ans-

- This can be implemented in two ways. Flat network architecture and Hierarchical network architecture.
- In flat architecture, the base station sends commands to all the sensor nodes but the sensor node with matching query will respond using its peer nodes via a multi-hop path.
- In hierarchical architecture, a group of sensor nodes are formed as a cluster and the sensor nodes transmit data to corresponding cluster heads. The cluster heads can then relay the data to the base station
- Flat based routing is where all nodes will participate equally in the functionality and plays a similar role; hence it is not feasible to assign the global identifier to all nodes.

10) Applications of MANET?

Ans-

Defense applications: Many defense applications require on the fly communications set-up, and ad hoc/sensor networks are excellent candidates for use in battlefield management.

Crisis management applications: These arise, for example, as a result of natural disasters in which the entire communication infrastructure is in disarray. Restoring communications quickly is essential.

Telemedicine: The paramedic assisting the victim of a traffic accident in a remote location must access medical records (e.g. X-rays) and may need video conference assistance from a surgeon for an emergency intervention. In fact, the paramedic may need to instantaneously relay back to the hospital the victim's X-rays and other diagnostic tests from the site of the accident.

Tele-geoprocessing application: The combination of GPS, GIS (Geographical Information Systems), and high-capacity wireless mobile systems enables a new type of application referred to as tele- geo processing.

Virtual Navigation: A remote database contains the graphical representation of building, streets, and physical characteristics of a large metropolis. They may also "virtually" see the internal layout of buildings, including an emergency rescue plan, or find possible points of interest.

Education via the internet: Educational opportunities available on the internet or remote areas because of the economic infeasibility of providing expensive last-mile wire line internet access in these areas to all subscribers.

Vehicular area network: This a growing and very useful application of adhoc network in providing emergency services and other information. This is equally effective in both urban and rural setup. The basic and exchange necessary data that is beneficial in a given situation.

11) what is Mobile Ip?

Ans –**Mobile IP** is a communication protocol (created by extending Internet Protocol, IP) that allows the users to move from one network to another with the same IP address. It ensures that the communication will continue without the user’s sessions or connections being dropped.