Q 21 Explain with examples and diagram where-ever required Tree based and Mesh based Protocols in detail?

Ans:

TREE BASED

Imagine a large wireless sensor network deployed to monitor environmental conditions in a forest. Sensors are spread throughout the forest to collect temperature, humidity, and other environmental data. The goal is to efficiently collect and transmit this data to a central base station for analysis.

#### ****How LEACH Works:****

**Cluster Formation**

* 1. The network is divided into clusters. Each cluster has a designated cluster head (CH). The CH is responsible for aggregating data from its cluster members (sensor nodes) and forwarding the aggregated data to the base station.
  2. The selection of CHs is done in a distributed manner. Each sensor node probabilistically chooses to become a CH, with the intention of rotating the role of CH among different nodes to balance energy consumption.

**Communication:**

* Data travels from the sensor nodes to the CH and then from the CH to the base station.
* The base station is the root node in this tree-based structure.

[Base Station]

|

[Cluster Head 1]------[Cluster Head 2]

/ \ / \

[Node 1] [Node 2] [Node 3] [Node 4]

· **Base Station:** The root node collecting data from all clusters.

· **Cluster Heads (CH1 and CH2):** Intermediate nodes aggregating data from their clusters.

· **Sensor Nodes (Node 1, Node 2, Node 3, Node 4):** Leaf nodes sending data to their respective CHs.

### ****Mesh-Based Protocol: AODV (Ad-hoc On-Demand Distance Vector)****

#### ****Scenario:****

Consider a mobile ad-hoc network (MANET) where a group of devices, such as laptops and smartphones, are moving around a conference hall. They need to establish temporary communication paths to share files and messages without relying on a fixed infrastructure.

#### ****How AODV Works:****

**Route Discovery:**

* 1. When a device (say Device A) wants to send data to another device (Device B) but doesn’t know the route, it initiates a route discovery process.
  2. Device A broadcasts a Route Request (RREQ) message to its neighbors. This message is propagated through the network until it reaches Device B or a device with a route to Device B.

**Route Establishment:**

* 1. When Device B receives the RREQ, it sends a Route Reply (RREP) back to Device A, either directly or via intermediate nodes.
  2. The RREP message travels back along the reverse path established by the RREQ, setting up the route between Device A and Device B.

**Data Transmission:**

* 1. With the route established, Device A can now send data to Device B using the discovered path.
  2. Intermediate nodes forward the data packets as per the established route.

**Route Maintenance:**

* 1. If a node along the route moves out of range or fails, AODV will detect the break and initiate a new route discovery process.

[A] --- [C] --- [D]

| | |

[B] --- [E] --- [F]

\ / |

\ / [G]

[H]

### ****Summary:****

* **LEACH (Tree-Based Protocol):** Efficient for static networks with a hierarchical structure, such as a sensor network monitoring an environment. It organizes nodes into clusters with a single path from cluster heads to the base station.

**AODV (Mesh-Based Protocol):** Suitable for dynamic, mobile networks where nodes frequently change locations. It creates routes on-demand and supports multiple paths, adapting to network changes and node movements.

Q 22 What is Multicast with Quality of Service Provision ?

### Ans ****Multicast with Quality of Service (QoS) Provision:****

**Multicast** refers to the process of sending data from one source to multiple destinations (or receivers) simultaneously, rather than creating separate connections for each receiver as in unicast. It is commonly used in applications like live video streaming, online gaming, and video conferencing, where the same data must be delivered to many users at the same time.

**Quality of Service (QoS)** refers to mechanisms or techniques used to manage network resources and ensure that certain performance parameters (like bandwidth, latency, jitter, and packet loss) are met for specific types of traffic. In networking, QoS ensures that high-priority applications (like real-time video or voice traffic) receive the necessary bandwidth and network performance.

### ****Multicast with QoS Provision:****

**Multicast with QoS Provision** involves delivering multicast data streams (e.g., video, voice, etc.) while ensuring that the quality of the transmission is maintained according to predefined performance criteria. The goal is to manage network resources effectively so that all receivers in the multicast group receive the data with acceptable levels of quality, regardless of network conditions.

#### ****Components of Multicast with QoS:****

**Multicast Communication:**

* 1. A source transmits data to multiple receivers using a **multicast group**.
  2. Each device (or node) in the network that wants to receive the multicast data joins the multicast group by subscribing to a specific multicast address.

**Quality of Service (QoS) Parameters:**

* 1. **Bandwidth:** Ensuring that the multicast stream has sufficient bandwidth allocated to meet the requirements of all receivers.
  2. **Latency:** Controlling the delay in data transmission so that multicast data (such as real-time video or audio) reaches all receivers with minimal delay.
  3. **Jitter:** Reducing variability in packet arrival times to prevent quality degradation in real-time applications.
  4. **Packet Loss:** Minimizing packet loss so that the quality of the data (such as video frames) is not significantly affected.

**Traffic Differentiation:**

* 1. Different types of traffic (e.g., multicast video, audio, and file downloads) may have different QoS requirements. Traffic is classified, and higher priority is assigned to real-time multicast traffic to ensure smooth delivery.

**Network Resource Management:**

* 1. **Admission Control:** Before a multicast stream starts, the network checks whether it has enough resources (bandwidth, etc.) to support the QoS requirements for the stream. If the network cannot meet the QoS needs, the multicast session may be rejected or delayed.
  2. **Traffic Shaping and Policing:** The network ensures that the multicast traffic conforms to the agreed-upon QoS policy by shaping or policing traffic at the network edges.

### ****Examples of Multicast with QoS Provision:****

**Video Conferencing:**

* 1. During a video conference involving multiple participants, multicast is used to send the video feed from one participant to many others. QoS ensures that the video and audio streams have low latency and minimal packet loss, providing a real-time experience to all participants.

### ****Q 23**** Write short notes on Reactive Routing, Coverage , Signal Strength and Bandwidth

### ****Ans: Reactive Routing:****

Reactive routing is a type of routing protocol used in dynamic or mobile networks, such as ad-hoc networks, where routes are created on-demand rather than maintained continuously. In reactive routing, when a source node needs to send data to a destination, it initiates a route discovery process to find the route, rather than keeping all possible routes in a routing table.

* **Key Feature:** Routes are discovered and established only when needed, reducing the overhead associated with continuously maintaining routing tables.
* **Example Protocols:** AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing).
* **Advantages:** Reduces routing overhead in networks with sporadic traffic, conserving bandwidth and power.
* **Disadvantages:** Route discovery process introduces delays, which can affect performance in time-sensitive applications.

### ****2. Coverage:****

Coverage refers to the geographical area or range within which a wireless communication system (like Wi-Fi, cellular networks, or sensor networks) can provide service. It defines how far a signal can travel and still be received with acceptable quality.

* **Key Factors:** Transmission power, antenna design, environmental obstacles (such as buildings or trees), and interference.
* **Types:**
  + **Full Coverage:** Ensures that every location within the target area has network access.
  + **Partial Coverage:** Only certain areas are covered, leaving dead zones.
* **Challenges:** Achieving optimal coverage without gaps while minimizing energy consumption and signal interference.

### ****3. Signal Strength:****

Signal strength measures the power level of a wireless signal received by a device from a transmitter (e.g., a Wi-Fi router or cellular tower). It is usually measured in decibels relative to a milliwatt (dBm).

* **Impact on Performance:** Stronger signal strength leads to faster data transmission rates, better connectivity, and fewer dropped packets. Weaker signals can result in lower data rates and connectivity issues.
* **Factors Affecting Signal Strength:** Distance from the transmitter, physical obstructions (walls, buildings), interference from other devices, and weather conditions.
* **Optimization:** Placing the transmitter centrally, minimizing obstacles, and using signal boosters can help improve signal strength.

### ****4. Bandwidth:****

Bandwidth is the maximum amount of data that can be transmitted over a network connection in a given amount of time, typically measured in bits per second (bps), kilobits (Kbps), megabits (Mbps), or gigabits (Gbps).

* **Key Role:** It determines the capacity of a network to handle data traffic. Higher bandwidth allows more data to be transmitted simultaneously, leading to better performance for tasks like streaming or file transfers.
* **Bandwidth vs. Throughput:** Bandwidth is the maximum potential data rate, while throughput is the actual rate achieved, which can be lower due to network congestion or errors.
* **Factors Influencing Bandwidth:** Type of connection (wired vs. wireless), network congestion, signal interference, and the capabilities of network hardware.

Q 24 What are the different parameters that decide the quality of Service of

Adhoc network?

ANs: The **Quality of Service (QoS)** in an ad-hoc network is influenced by various parameters that ensure optimal performance for different types of network traffic, particularly real-time and multimedia applications. In ad-hoc networks, which are decentralized and dynamic, managing QoS is more challenging than in traditional networks. Here are the key parameters that determine the QoS in ad-hoc networks:

### 1. ****Bandwidth:****

* **Definition:** The maximum data rate that can be supported by the network.
* **Role in QoS:** Higher bandwidth allows more data to be transmitted simultaneously, improving the performance of high-traffic applications like video streaming or file sharing. Limited bandwidth can lead to delays and reduced throughput.

### 2. ****Latency (Delay):****

* **Definition:** The time it takes for a data packet to travel from the source to the destination.
* **Role in QoS:** Low latency is crucial for real-time applications such as voice and video communication. In ad-hoc networks, where nodes are mobile and the network topology changes, minimizing latency is important for maintaining smooth communication.

### 3. ****Jitter:****

* **Definition:** The variation in packet arrival times, which can cause irregularities in the data flow.
* **Role in QoS:** Inconsistent jitter can lead to degraded performance in real-time applications like voice and video, where data needs to arrive at a consistent rate. Minimizing jitter ensures smoother playback in multimedia applications.

### 4. ****Packet Loss:****

* **Definition:** The percentage of packets that are lost during transmission and fail to reach the destination.
* **Role in QoS:** High packet loss can severely degrade network performance, particularly in applications requiring reliable data delivery, such as file transfers or online gaming. QoS mechanisms aim to reduce packet loss by prioritizing critical traffic.

### 5. ****Throughput:****

* **Definition:** The actual rate of successful data delivery over a communication link.
* **Role in QoS:** High throughput ensures that the network can handle a large volume of data efficiently. Maintaining good throughput is vital for applications with large data demands, like video streaming or downloading.

Q 25 Explain about the Security of MANET in point form?

### Ans: ****Security in MANET (Mobile Ad-Hoc Network):****

**Decentralized Structure:**

* 1. MANETs lack a central authority for managing security, making it challenging to enforce security policies uniformly across all nodes.

**Dynamic Topology:**

* 1. Nodes in MANETs frequently move, causing frequent changes in the network topology, which makes it hard to maintain consistent security protocols.

**Open Medium:**

* 1. Wireless communication in MANETs is vulnerable to eavesdropping, interception, and jamming, as there is no physical boundary to restrict access.

**Limited Resources:**

* 1. Devices in MANETs typically have limited battery power, processing capability, and memory, which makes implementing robust security mechanisms challenging.

**Lack of Predefined Trust:**

* 1. Since nodes can join and leave the network at any time, there is no predefined trust relationship among nodes, increasing the risk of malicious behavior.

Q 26 Explain in detail about different types of Routing Algorithm?

### Ans : ****Classification Based on Route Update Mechanism****

#### ****a. Static Routing Algorithms:****

* **Definition:** Routes are manually defined and fixed by the network administrator. The routes do not change unless manually reconfigured.
* **Key Features:**
  + No overhead for route updates.
  + Works well for small, simple networks where routes don’t change frequently.
* **Advantages:**
  + Easy to implement.
  + No bandwidth consumed for routing updates.
* **Disadvantages:**
  + Inflexible; cannot adapt to network changes.
  + Not suitable for large or dynamic networks.
* **Example:** A router manually configured to forward all packets for a specific destination to a predetermined next hop.

#### ****b. Dynamic Routing Algorithms:****

* **Definition:** Routes are automatically adjusted based on network changes such as topology, traffic, or congestion.
* **Key Features:**
  + Routes are updated periodically or in response to topology changes.
  + Adapts to changing network conditions.
* **Advantages:**
  + More flexible and suitable for large or frequently changing networks.
  + Can find new paths automatically if a link fails.
* **Disadvantages:**
  + Consumes network bandwidth to exchange routing information.
  + Complexity is higher compared to static routing.
* **Examples:** RIP (Routing Information Protocol), OSPF (Open Shortest Path First), BGP (Border Gateway Protocol).

### ****2. Classification Based on Path Selection****

#### ****a. Distance Vector Routing:****

* **Definition:** Each router maintains a table (vector) that holds the distance (in terms of hops or metrics like bandwidth) to every other network node. Routers exchange this table with their neighbors to update routes.
* **Key Features:**
  + The routing table contains information about the distance to the destination and the next hop.
  + Uses the Bellman-Ford algorithm.
* **Advantages:**
  + Simple to implement.
  + Requires less computational power.
* **Disadvantages:**
  + Slow convergence in larger networks.
  + Prone to routing loops.
* **Examples:** RIP, IGRP (Interior Gateway Routing Protocol).
* **Operation Example:**
  + A router sends its routing table to its neighbors. Neighbors update their tables based on this information and propagate it further.

#### ****b. Link State Routing:****

* **Definition:** Each router has a complete view of the network topology and uses this information to compute the shortest path to all nodes using algorithms like Dijkstra’s algorithm.
* **Key Features:**
  + Routers maintain a map of the entire network.
  + Each router sends **link-state advertisements (LSAs)** to all other routers.
* **Advantages:**
  + Fast convergence.
  + Provides loop-free routes.
* **Disadvantages:**
  + High computational and memory overhead.
  + Requires more bandwidth for topology updates.
* **Examples:** OSPF, IS-IS (Intermediate System to Intermediate System).
* **Operation Example:**
  + A router detects a link state change (e.g., a new neighbor or a broken link) and floods this information across the entire network. Each router then recalculates its routing table based on the updated topology.

#### ****c. Hybrid Routing:****

* **Definition:** Combines features of both distance vector and link-state routing. Initially, routing tables are built using distance vector routing, and then changes are propagated using link-state routing.
* **Key Features:**
  + Balances scalability and convergence speed.
  + Suitable for larger and hierarchical networks.
* **Advantages:**
  + Efficient for large-scale networks.
  + Faster convergence than distance vector but with less overhead than link-state.
* **Disadvantages:**
  + More complex than distance vector or link-state individually.
* **Examples:** EIGRP (Enhanced Interior Gateway Routing Protocol).

Q27 What are fixed infrastructure network? What are the problems with fixed infrastructure network? Explain the Architecture of MANET?

Ans: A **Fixed Infrastructure Network** refers to a traditional network setup where devices communicate through a pre-established and centralized infrastructure. The infrastructure includes a network of wired or wireless devices such as routers, switches, and base stations that are typically fixed in specific locations and act as intermediaries to facilitate communication between devices.

#### ****Key Features of Fixed Infrastructure Networks:****

**Centralized Management**

**Fixed Base Stations:**

**Wired or Wireless Connections:**

**Static Topology**

### ****Problems with Fixed Infrastructure Networks:****

**Costly to Set Up and Maintain:**

* 1. Installing and maintaining fixed infrastructure (e.g., laying cables, setting up base stations) is expensive and time-consuming.

**Lack of Flexibility:**

* 1. These networks are static, meaning changes to the network’s physical layout are difficult and costly. Mobile nodes cannot communicate if they move beyond the range of a base station.

**Single Point of Failure:**

* 1. Since the network relies on centralized devices, a failure in key components (like routers or base stations) can disrupt the entire network.

### ****Architecture of MANET (Mobile Ad-Hoc Network):****

A **Mobile Ad-Hoc Network (MANET)** is a decentralized wireless network where devices (nodes) communicate directly with each other without relying on any fixed infrastructure. The network is dynamic, meaning nodes can join and leave the network freely, and the network topology changes frequently as nodes move.

#### ****Key Characteristics of MANET:****

**Infrastructure-less:**

* 1. Unlike fixed networks, MANETs don’t rely on centralized infrastructure like routers or base stations. All devices act as routers that forward data.

**Dynamic Topology:**

* 1. Nodes can move freely, and the network topology constantly changes. Devices must adapt to changing routes and new connections.

**Multi-hop Communication:**

* 1. Communication between devices may require intermediate nodes to relay data, especially when the destination is beyond direct transmission range.

**Decentralized Control:**

* 1. MANETs operate without any centralized control. Nodes cooperatively manage routing and data forwarding based on distributed algorithms.

Q29 What do you understand by Proactive Routing Protocol? Explain in detail with examples.

### ****Ans Proactive Routing Protocol****

A **Proactive Routing Protocol** (also known as a **Table-Driven Routing Protocol**) is a type of routing protocol in which all nodes in a network continuously maintain up-to-date routing information to every other node, regardless of whether the routes are currently needed. This ensures that a route is immediately available whenever data needs to be transmitted, reducing the delay associated with route discovery.

#### ****How Proactive Routing Works (with an Example)****

Let's explain how proactive routing works with an example where **Node A** sends data to **Node B**.

##### ****Step 1: Initial Setup****

In a proactive routing protocol, each node in the network maintains a routing table. This table contains information such as:

* The destination node.
* The next hop to reach the destination.
* The distance or number of hops to reach the destination.

All nodes (including Node A and Node B) continuously exchange routing updates with their neighboring nodes. This ensures that the routing tables in all nodes are always updated with the latest information about the network.

##### ****Step 2: Nodes Maintain Routing Tables****

For example, Node A maintains the following table:

| **Destination Node** | **Next Hop** | **Hop Count** |
| --- | --- | --- |
| B | C | 2 |
| C | C | 1 |
| D | C | 2 |

Here, Node A knows that it can reach **Node B** via **Node C**, and the distance is 2 hops. This information is stored in the routing table.

Similarly, **Node B** also maintains its routing table with information about other nodes, including Node A.

##### ****Step 3: Data Transmission from Node A to Node B****

Now, let's say Node A wants to send data to Node B. Since this is a proactive routing protocol, Node A doesn't need to initiate a route discovery process (like in reactive protocols). It can immediately consult its routing table and see that:

* The next hop to reach Node B is via Node C.
* The total number of hops is 2.

##### ****Step 4: Forwarding the Data****

* **Step 4.1:** Node A forwards the data packet to **Node C**, the next hop according to its routing table.
* **Step 4.2:** Node C, upon receiving the packet, consults its own routing table. It sees that the next hop to reach Node B is **Node B** itself.
* **Step 4.3:** Node C forwards the data to **Node B**, completing the transmission.

The proactive nature of the routing protocol ensures that there is no delay in finding the route, as all the routing information is pre-computed and readily available in the routing tables of the nodes.

##### ****Step 5: Continuous Updates****

Even while data is being transmitted, nodes continue to update their routing tables periodically. This means that if the network topology changes (e.g., Node C moves away), nodes will detect this change and update their routing tables accordingly. This ensures that the routing information is always current and accurate.

Q30 MAC layer has multiple issues related to Routing , Explain them in detail

Ans: The **MAC (Media Access Control) layer** is responsible for managing how data is transmitted over the network medium. In wireless networks, particularly in Mobile Ad-Hoc Networks (MANETs), the MAC layer faces several challenges related to routing. These issues stem from the shared and dynamic nature of wireless communication and can significantly impact network performance.

### ****Issues Related to Routing at the MAC Layer****

#### ****1. Collision and Interference****

**Collision:** In wireless networks, multiple devices might try to transmit data simultaneously over the same channel, leading to collisions. Collisions occur when two or more nodes transmit at the same time, causing their signals to interfere with each other and resulting in data loss or corruption.

**Impact on Routing:**

* + Collisions can cause packet loss, requiring retransmissions. This can lead to increased latency and reduced throughput, as well as increased overhead for the MAC layer's collision avoidance mechanisms.

**Interference:** Wireless communication is susceptible to interference from other wireless devices and environmental factors (e.g., physical obstacles, weather conditions).

**Impact on Routing:**

* + Interference can degrade signal quality, leading to increased packet errors and retransmissions. This affects the reliability of routing protocols and can reduce overall network performance.

#### ****2. Hidden Node Problem****

**Description:** The hidden node problem occurs when two nodes (A and C) are within range of a common node (B) but are not within range of each other. Node A and Node C may transmit to Node B without being aware of each other’s transmissions, causing collisions at Node B.

**Impact on Routing:**

* + Collisions caused by hidden nodes can lead to packet loss and reduced throughput. Routing protocols may need to implement additional mechanisms to address this issue, increasing complexity and overhead.

#### ****3. Exposed Node Problem****

**Description:** The exposed node problem arises when a node (A) is prevented from transmitting to another node (B) because it overhears a transmission between a third node (C) and node B. Even though node A’s transmission would not interfere with the ongoing transmission, the MAC protocol may unnecessarily prevent it.

**Impact on Routing:**

* + This issue can lead to reduced network utilization and throughput as nodes are unnecessarily restricted from transmitting when they could do so without causing interference. It affects the efficiency of routing protocols by limiting available bandwidth.

#### ****4. Dynamic Topology****

**Description:** In mobile networks, nodes frequently move, leading to constantly changing network topologies. This dynamic nature makes it challenging for MAC protocols to maintain stable and efficient communication channels.

**Impact on Routing:**

* + Frequent topology changes can cause routing tables to become outdated, requiring constant updates and adaptations. This increases the complexity of routing algorithms and can lead to increased control overhead and reduced performance.

#### ****5. Power Consumption****

**Description:** Wireless nodes are often battery-powered, and managing power consumption is crucial. The MAC layer must balance between efficient transmission and conserving battery life.

**Impact on Routing:**

* + Energy-efficient MAC protocols are necessary to extend the lifespan of battery-powered nodes. Inefficient power management can lead to nodes running out of battery quickly, impacting network connectivity and routing stability.

Q 31 Compare Reactive and Hybrid Routing Protocols. Use diagram and examples where required

Ans :

| **Reactive Routing Protocols** | **Hybrid Routing Protocols** |
| --- | --- |

|  |  |  |
| --- | --- | --- |
| **1. Route Discovery** | On-demand (routes are discovered only when needed) | Combination of proactive and reactive discovery |

|  |  |  |
| --- | --- | --- |
| **2. Route Maintenance** | Routes are maintained only for active paths | Proactive maintenance in local areas, reactive in other areas |

|  |  |  |
| --- | --- | --- |
| **3. Route Overhead** | Low control message overhead when there is no traffic | Medium overhead due to hybrid approach |

|  |  |  |
| --- | --- | --- |
| **4. Latency** | High initial latency due to on-demand route discovery | Lower latency in frequently used routes, higher in others |

|  |  |  |
| --- | --- | --- |
| **5. Scalability** | Suitable for smaller networks due to lower control overhead | More scalable for larger networks |

|  |  |  |
| --- | --- | --- |
| **6. Routing Table Size** | No need for full routing tables, maintained only for active routes | Partial routing tables for local nodes, reactive for distant ones |

|  |  |  |
| --- | --- | --- |
| **7. Control Traffic** | Less control traffic when the network is idle | Moderate control traffic due to periodic updates in local areas |

|  |  |  |
| --- | --- | --- |
| **8. Suitability** | Best for highly dynamic networks where traffic is unpredictable | Suitable for large or heterogeneous networks with varying traffic |

|  |  |  |
| --- | --- | --- |
| **9. Example Protocols** | AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) | ZRP (Zone Routing Protocol), HSR (Hierarchical State Routing) |

|  |  |  |
| --- | --- | --- |
| **Complexity** | Simple to implement but inefficient in high traffic networks | More complex due to the mix of proactive reactive approaches |

### ****Examples of When Reactive and Hybrid Routing Protocols Are Required****

#### ****Reactive Routing Protocols (On-Demand)****

Reactive protocols are best suited for networks with infrequent communication, dynamic topologies, or where minimizing control message overhead is critical. Some key scenarios include:

**Highly Dynamic Networks:** In situations like disaster recovery or military operations, where network nodes (e.g., rescue teams or soldiers) move frequently and unpredictably, reactive protocols such as **AODV (Ad-hoc On-Demand Distance Vector)** and **DSR (Dynamic Source Routing)** are ideal. These protocols initiate route discovery only when needed, reducing unnecessary control message overhead in frequently changing environments.

**Sporadic Communication:** When communication between nodes happens infrequently, such as in sensor networks monitoring environmental conditions, reactive protocols like **AODV** are effective. Since routes are established only when data needs to be sent, they avoid the constant exchange of routing information, making them more efficient for low-traffic networks.

**Resource-Constrained Networks:** In wireless sensor networks or small mobile ad-hoc networks (MANETs) where conserving bandwidth and battery life is critical, **DSR** is used. It reduces the load by maintaining routes only for ongoing transmissions, making it efficient for energy-constrained nodes.

#### ****Hybrid Routing Protocols****

Hybrid protocols combine proactive and reactive features, making them ideal for larger, more complex networks where different areas of the network exhibit varying traffic patterns. Key scenarios where hybrid protocols are effective include:

**Large-Scale Networks with Varying Traffic:** In large-scale ad-hoc networks, such as those used in smart cities or intelligent transportation systems, **ZRP (Zone Routing Protocol)** is beneficial. It proactively maintains routes within a local zone (to reduce latency) and uses reactive discovery for distant nodes, which helps manage the scalability and complexity of routing in such vast networks.

**Hierarchical Networks:** In hierarchical networks like those found in large organizational setups or structured mobile sensor networks, **HSR (Hierarchical State Routing)** is required. It combines proactive routing within each hierarchy or cluster and reactive routing between clusters. This optimizes both control overhead and efficiency.

**Networks with Both Stable and Dynamic Regions:** In networks where some parts of the network are stable (e.g., base stations) and others are highly dynamic (e.g., mobile users), hybrid protocols like **ZRP** are useful. Proactive routing is applied in the stable parts, while reactive routing is triggered in the dynamic regions to efficiently handle mobility without excessive control messages.

Q36 Differentiate between Cellular Network and Adhoc Wireless Network in detai?

Ans :

| **Aspect** | **Cellular Network** | **Ad-hoc Wireless Network** |
| --- | --- | --- |

|  |  |  |
| --- | --- | --- |
| **Infrastructure** | Requires fixed infrastructure (e.g., base stations, cell towers) for communication. | No fixed infrastructure required; nodes communicate directly with each other. |

|  |  |  |
| --- | --- | --- |
| **Centralized Control** | Operates with centralized control via a base station that manages communication. | Decentralized, as each node operates independently and routing is done cooperatively. |

|  |  |  |
| --- | --- | --- |
| **Communication Range** | Limited to the range of the base station or cell tower. | Nodes communicate over short distances and can form multi-hop routes to extend range. |

|  |  |  |
| --- | --- | --- |
| **Mobility Handling** | Handled through handoff between different base stations as a user moves between cells. | Mobility is managed dynamically with nodes updating routes based on changing topology. |

|  |  |  |
| --- | --- | --- |
| **Scalability** | Highly scalable, as infrastructure can be expanded by adding more towers or base stations. | Limited scalability due to increased overhead and complexity with a larger number of nodes. |

|  |  |  |
| --- | --- | --- |
| **Power Consumption** | Mobile devices rely on base stations, which consume significant power for wide-area coverage. | Nodes must manage their own power, making energy efficiency a major consideration. |

|  |  |  |
| --- | --- | --- |
| **Reliability** | Generally high reliability, as communication is supported by fixed infrastructure and strong signals. | Less reliable due to dynamic topology and potential issues with node mobility, signal strength, and interference. |

|  |  |  |
| --- | --- | --- |
| **Cost** | Expensive due to the need for infrastructure and maintenance of base stations. | Lower cost since no infrastructure is required, making it suitable for temporary or emergency deployments. |

|  |  |  |
| --- | --- | --- |
| **Routing** | Routing is handled by the network infrastructure (e.g., via cellular towers). | Each node participates in the routing process, with routes created dynamically based on current network topology. |

|  |  |  |
| --- | --- | --- |
| **Application Areas** | Used in cellular telephony, mobile internet services, and IoT networks with fixed infrastructure. | Used in military operations, disaster recovery, sensor networks, and peer-to-peer applications. |

Q 35 What is Multicasting? Define Computer Network and explain its two components.

Ans: **Multicasting** is a communication method used in computer networks where data is sent from a single source to multiple designated recipients or nodes simultaneously. Unlike **unicast** (one-to-one communication) or **broadcast** (one-to-all communication), multicasting is **one-to-many** but only targets a specific group of recipients who have expressed interest in receiving the data.

**Example:** Video conferencing, live streaming, or any situation where the same data needs to be delivered to multiple recipients without unnecessary duplication of transmission across the network.

### ****Computer Network: Definition****

A **Computer Network** is a collection of interconnected computing devices (like computers, servers, routers, and switches) that communicate with each other to share resources, exchange data, and perform tasks. These devices communicate through a combination of hardware, software, and protocols, which define the rules of data transmission.

### ****Two Components of a Computer Network****

**Hardware**

* 1. **Definition:** Hardware refers to the physical devices that make up the network infrastructure, including end devices, transmission media, and intermediate devices.
  2. **Examples of Hardware:**
     1. **End Devices:** Computers, servers, smartphones, printers, etc.
     2. **Transmission Media:** Cables (Ethernet, fiber-optic), wireless signals (Wi-Fi, Bluetooth).
     3. **Network Devices:** Routers, switches, hubs, modems.

**Software**

* 1. **Definition:** Software manages and controls the communication between the hardware components, including operating systems, applications, and network protocols.
  2. **Examples of Software:**
     1. **Network Operating Systems (NOS):** Software like Windows Server, Linux, that manages network resources.
     2. **Protocols:** Rules that determine how data is transmitted, such as **TCP/IP** (Transmission Control Protocol/Internet Protocol), **HTTP** (HyperText Transfer Protocol), and **FTP** (File Transfer Protocol).
     3. **Network Management Software:** Tools that monitor and maintain network performance, security, and configuration.

Q 34 Differentiate between Mobile Adhoc Network (MANET) and Wireless Sensor Network in tabular form considering its features.

| **Aspect** | **Mobile Ad-hoc Network (MANET)** | **Wireless Sensor Network (WSN)** |
| --- | --- | --- |

|  |  |  |
| --- | --- | --- |
| **Node Type** | Nodes are typically mobile devices (e.g., smartphones, laptops, vehicles). | Nodes are usually low-power sensors deployed for monitoring physical conditions. |

|  |  |  |
| --- | --- | --- |
| **Mobility** | Nodes are highly mobile, leading to frequent topology changes. | Nodes are usually stationary but can be mobile in some applications like tracking. |

|  |  |  |
| --- | --- | --- |
| **Power Consumption** | Devices generally have more power capacity, but energy efficiency is still important. | Nodes are energy-constrained with limited battery life, requiring low-power operations. |

|  |  |  |
| --- | --- | --- |
| **Network Size** | Typically consists of fewer nodes compared to WSNs (dozens to hundreds). | Consists of a large number of sensor nodes (can range from hundreds to thousands). |

|  |  |  |
| --- | --- | --- |
| **Data Transmission** | Data transmission is multi-hop, with nodes acting as both routers and end devices. | Data is usually collected by sensors and transmitted to a base station (sink node). |

|  |  |  |
| --- | --- | --- |
| **Application** | Used for mobile communication in dynamic environments (e.g., military, vehicular). | Used for environmental monitoring, health, agriculture, and industrial applications. |

|  |  |  |
| --- | --- | --- |
| **Topology** | Highly dynamic due to node mobility, requiring adaptive routing protocols. | Relatively static, with a more predictable network topology. |

|  |  |  |
| --- | --- | --- |
| **Communication Range** | Nodes communicate over longer distances than WSN, using ad-hoc routing protocols. | Short-range communication with multi-hop routing to reach distant nodes. |

|  |  |  |
| --- | --- | --- |
| **Node Intelligence** | Nodes are more intelligent and capable of complex processing and decision-making. | Nodes are generally simple, focused on sensing and transmitting data to the base station. |

|  |  |  |
| --- | --- | --- |
| **Fault Tolerance** | Lower fault tolerance due to higher node mobility and potential connectivity issues. | High fault tolerance with redundancy in sensor nodes and self-healing capabilities. |

Q 33 Explain the Characteristics of Mobile Adhoc Network (MANET)? Also explain its Pros and Cons? What are the improvements in MANET?

### Ans: ****Characteristics of Mobile Ad-hoc Network (MANET)****

**Decentralized Network**: MANET operates without a centralized authority or fixed infrastructure. Nodes communicate directly or through other nodes.

**Dynamic Topology**: The network topology changes frequently due to the mobility of nodes, leading to a constantly evolving network structure.

**Multi-hop Routing**: In MANET, data may pass through multiple intermediate nodes before reaching its destination, as direct communication is not always possible.

**Self-Healing**: MANETs are capable of automatically adjusting routes when nodes move or become unavailable, ensuring data delivery despite frequent changes.

**Autonomous Nodes**: Each node in a MANET functions as an independent device capable of acting as a router or host, forwarding data to others.

**Scalability**: MANETs can scale to accommodate a large number of nodes, although increased size can introduce complexity and overhead.

**Limited Bandwidth and Power**: Since MANETs often use wireless communication, bandwidth is limited, and energy consumption is a concern, particularly for battery-powered nodes.

**Network Security**: MANETs are more vulnerable to security attacks due to the lack of centralized control and the open nature of wireless communication.

**Frequent Disconnections**: Due to node mobility and varying signal strength, frequent disconnections can occur, causing intermittent communication.

### ****Pros and Cons of MANET****

#### ****Pros:****

**No Infrastructure Required**: Suitable for areas where infrastructure is unavailable or damaged, like disaster recovery zones.

**Flexible and Scalable**: Can be deployed quickly and scale according to the number of participating nodes.

**Mobility Support**: Allows continuous communication even while nodes are moving, making it ideal for mobile scenarios (e.g., military operations, vehicular networks).

**Autonomous and Self-organizing**: Nodes manage their own communication and routing, reducing dependency on external management.

**Cost-Effective**: Since it does not rely on expensive fixed infrastructure, the setup cost is significantly reduced.

#### ****Cons:****

**Limited Resources**: Battery life, bandwidth, and processing power are often constrained in mobile devices.

**Security Risks**: Vulnerable to attacks such as eavesdropping, spoofing, and denial-of-service attacks due to the lack of centralized control and open wireless communication.

**Unstable Connectivity**: Constant changes in the network topology due to node mobility can lead to frequent route breaks and packet losses.

**High Routing Overhead**: The need to constantly update routing information increases overhead, especially in large networks with high mobility.

**Scalability Issues**: As the number of nodes increases, routing complexity and latency also rise, making it harder to manage larger networks efficiently.

### ****Improvements in MANET****

**Efficient Routing Protocols**: Development of more robust and scalable routing protocols like **AODV**, **DSR**, and **OLSR** (Optimized Link State Routing) to handle dynamic topologies and reduce routing overhead.

**Security Enhancements**: Implementation of security mechanisms such as encryption, authentication, and intrusion detection systems to protect the network from potential threats.