Complete Unit -3 MC

IP/Mobile-IP Network Layer

1️⃣ IP (Internet Protocol) — Network Layer

- **IP** is the fundamental protocol of the network layer that **routes data packets** from source to destination across multiple networks.
- It provides **logical addressing** via **IP addresses** and decides the path for packets.
- Used in wired and wireless networks.
- Examples: IPv4, IPv6.

Key features of IP:

- Packet forwarding based on IP addresses.
- Connectionless protocol (no setup before sending).
- Best-effort delivery (no guarantee packets arrive).
- Routers use IP addresses to forward packets.

2️⃣ Mobile IP — Network Layer Protocol for Mobility

Why Mobile IP?

- Traditional IP doesn't support **mobility** well.
- When a device moves from one network to another, its IP address changes.
- This causes **connection loss** (e.g., calls drop, sessions break).

What Mobile IP does:

- Allows a mobile device to **keep the same IP address** even when moving across different networks.
- Ensures **continuous connectivity** without changing the IP address.

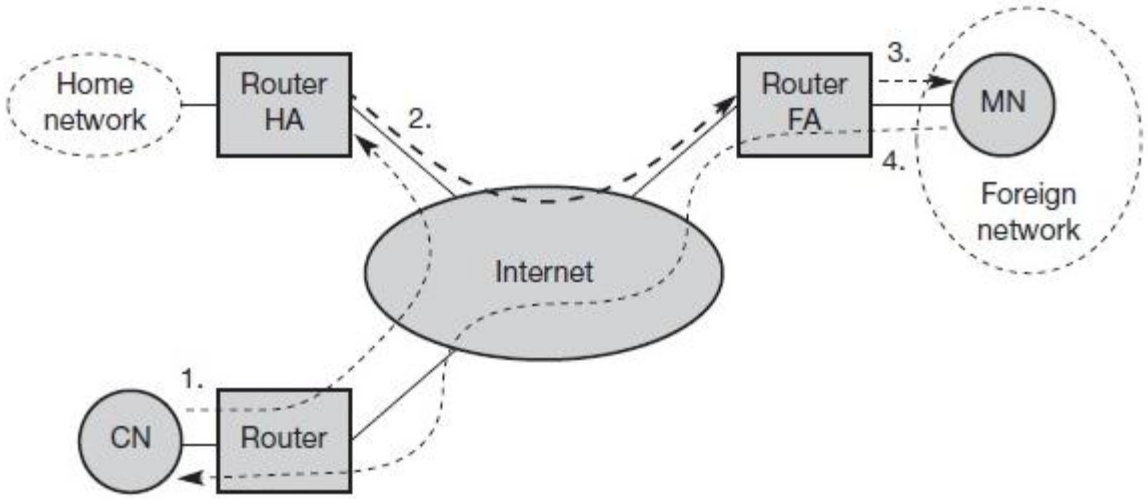
Mobile IP Components:

Component	Description
Home Agent (HA)	Located in home network, keeps track of mobile node's location.
Foreign Agent (FA)	Located in visited network, provides care-of address to mobile node.
Mobile Node (MN)	The device that moves and wants to maintain its IP.
Correspondent Node (CN)	The device communicating with the mobile node.

How Mobile IP Works:

1. Mobile Node moves to a new network.
2. It gets a **Care-of Address (CoA)** from Foreign Agent.
3. Mobile Node informs Home Agent about the new CoA.
4. Home Agent **forwards packets** destined for Mobile Node to the new location.
5. Mobile Node receives data without changing its IP address.

IP Packet Delivery



1. A correspondent node CN wants to send an IP packet to the MN.

2. One of the requirements of mobile IP was to support hiding the mobility of the MN.

3. CN does not need to know anything about the MN's current location and sends the packet as usual to the IP address of MN (step 1).

This means that CN sends an IP packet with MN as a destination address and CN as a source address. The internet, not having information on the current location of MN, routes the packet to the router responsible for the home network of MN. This is done using the standard routing mechanisms of the internet

4. The HA now intercepts the packet, knowing that MN is currently not in its home network.

5. The packet is not forwarded into the subnet as usual, but encapsulated and tunnelled to the COA.

6. A new header is put in front of the old IP header showing the COA as new destination and HA as source of the encapsulated packet (step 2).

7. The foreign agent now decapsulates the packet, i.e., removes the additional header, and forwards the original packet with CN as source and MN as destination to the MN (step 3).

8. Again, for the MN mobility is not visible. It receives the packet with the same sender and receiver address as it would have done in the home network.

What is Handover Management?

Handover (or Handoff) is the process of **transferring an ongoing call or data session from one cell (base station) to another** without dropping the connection.

It's crucial in mobile communication to maintain **seamless connectivity** when a user is moving.

Types of Handover:

Type	Description
Hard Handover	Break-before-make: Disconnect from old cell before connecting to new one. May cause brief interruption.
Soft Handover	Make-before-break: Connect to new cell before disconnecting from old one. Used in CDMA networks for smooth transition.
Vertical Handover	Switching between different types of networks (e.g., from Wi-Fi to cellular).

How Handover Works:

1. **Mobile device moves** away from current base station coverage.
2. Signal strength from current cell **weakens**, and signal from neighboring cell **improves**.
3. Network monitors signal quality and decides when to handover.
4. Connection is **transferred** to new base station.
5. User continues call/data without noticeable disruption.

Why Handover is Important?

- Prevents **call drops**.
- Maintains **continuous internet/data sessions**.
- Provides **better signal quality** as users move.
- Enables **mobility** in cellular networks.

📦 1. What is Encapsulation?

Encapsulation means **wrapping one packet inside another packet**.

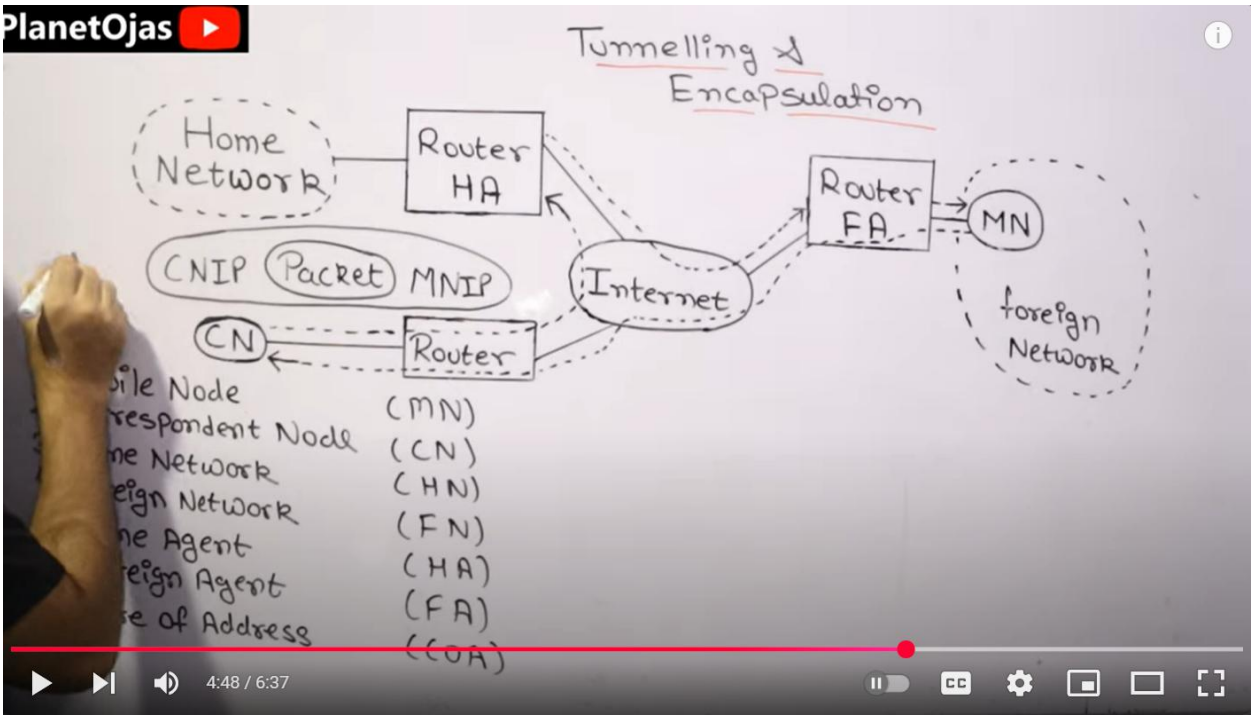
🔹 **In Mobile IP:**

- When the **Home Agent** wants to send data to the **Mobile Node** (which is now on a different network), it **encapsulates** the original IP packet inside a new IP packet.

- This is done to **deliver the packet to the Mobile Node's current location** (care-of address).

📌 **Think of it like:**

A courier puts a gift (original packet) inside a bigger box (new packet) to ship it safely to a new address.



📡 2. What is Tunneling?

Tunneling is the **process of sending encapsulated packets** over the internet to reach the destination.

🔹 **In Mobile IP:**

- The **Home Agent (HA)** sends the encapsulated packet through a **tunnel** to the **Foreign Agent (FA)** or directly to the Mobile Node's **Care-of Address (CoA)**.
- Tunnel = A **virtual path** that carries encapsulated packets between two IP addresses.

🧠 **How Tunneling + Encapsulation Work in Mobile IP:**

1. Mobile Node leaves home network, registers its Care-of Address with the Home Agent.

2. Correspondent Node sends packet to Mobile Node's **Home Address**.
3. Home Agent:
    - **Encapsulates** the packet.
    - Sends it through a **tunnel** to the Care-of Address.
4. Foreign Agent decapsulates and delivers to the Mobile Node.

🔄 **Summary:**

Concept	Meaning
Encapsulation	Wrapping the original IP packet inside another packet (like double packing)
Tunneling	Sending the encapsulated packet from one network node to another (via a virtual path)

📦 **Example:**

Imagine you moved to another city temporarily:

- Your friend sends a letter to your **home address** (Correspondent → Home Address).
- Your dad (Home Agent) **puts it in another envelope** with your new city address (Encapsulation).
- He **couriers it via a secure service** (Tunneling) to your new address (Care-of Address).

You get your letter, and the friend didn't even know you moved

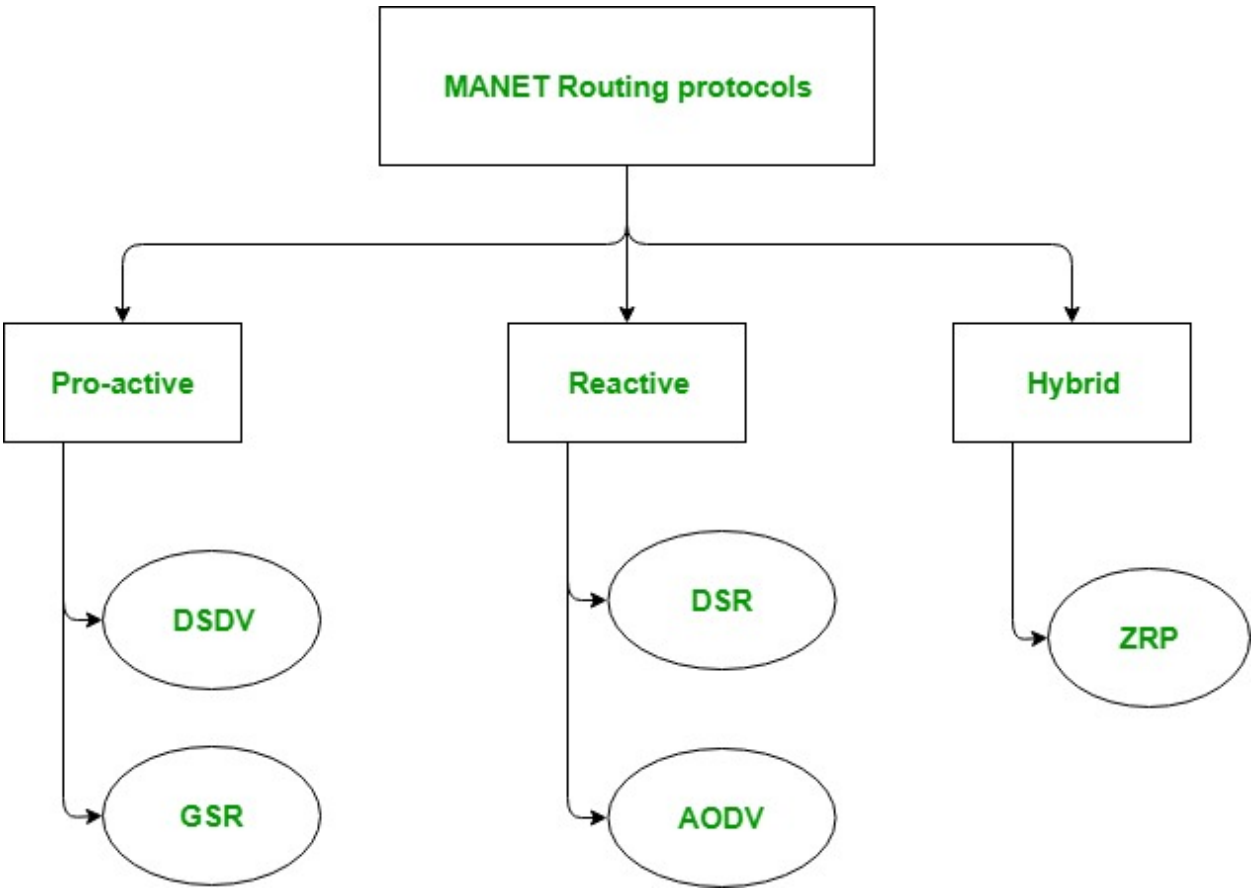
📡 What is MANET (Mobile Ad hoc Network)?

A **MANET** is a type of **wireless network** where:

- There is **no fixed infrastructure** (like routers or access points).
- Each device (called a **node**) can **move freely** and acts as **both a host and a router**.
- Devices communicate **directly or through other devices** (multi-hop routing).

📌 **Key Features of MANET:**

Feature	Description
Infrastructure-less	No central router or base station is needed
Dynamic Topology	Nodes move, join, or leave the network anytime
Multi-hop Routing	Data is passed through other devices if far away
Self-configuring	Nodes automatically form the network on the go
Decentralized	No single control point—fully distributed system

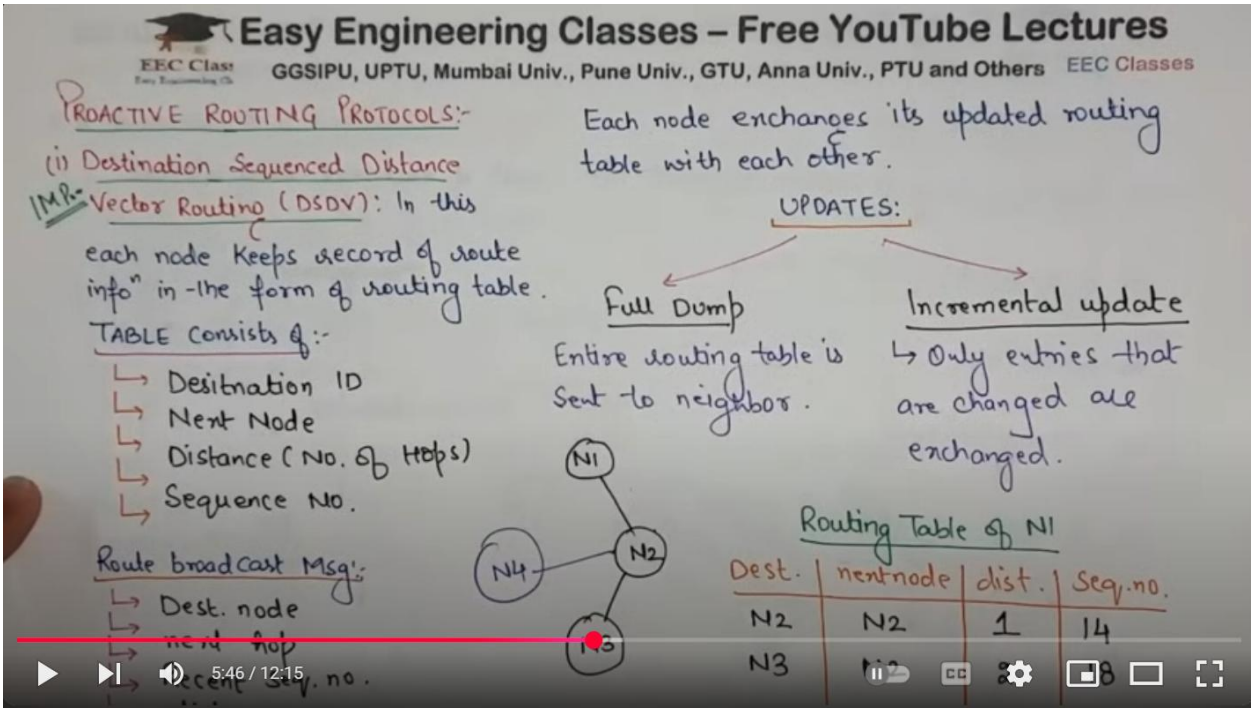


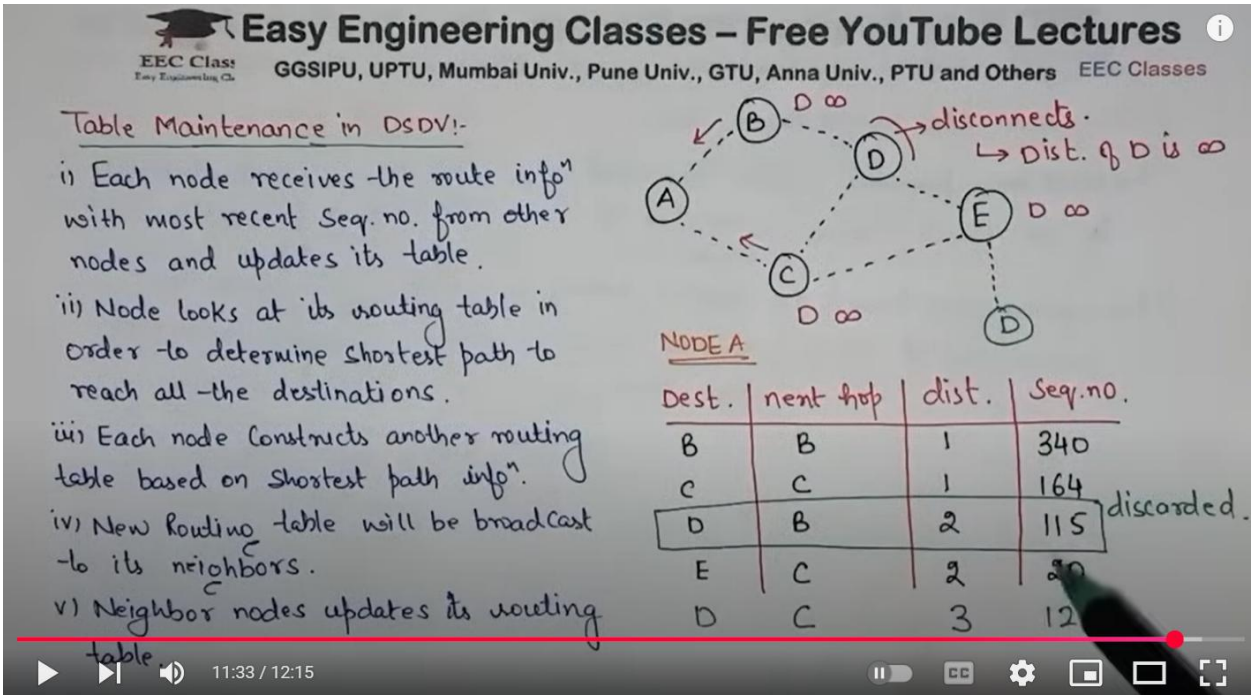
1. Pro-active routing protocols: These are also known as table-driven routing protocols. Each mobile node maintains a separate routing table which contains the information of the routes to all the possible destination mobile nodes.

Since the topology in the mobile ad-hoc network is dynamic, these routing tables are updated periodically as and when the network topology changes. It has a limitation that it doesn't work well

for the large networks as the entries in the routing table becomes too large since they need to maintain the route information to all possible nodes.

1. **Destination Sequenced Distance Vector Routing Protocol (DSDV):** It is a pro-active/table driven routing protocol. It actually extends the distance vector routing protocol of the wired networks as the name suggests. It is based on the Bellman-ford routing algorithm. Distance vector routing protocol was not suited for mobile ad-hoc networks due to count-to-infinity problem. Hence, as a solution Destination Sequenced Distance Vector Routing Protocol (DSDV) came into picture. Destination sequence number is added with every routing entry in the routing table maintained by each node. A node will include the new update in the table only if the entry consists of the new updated route to the destination with higher sequence number.



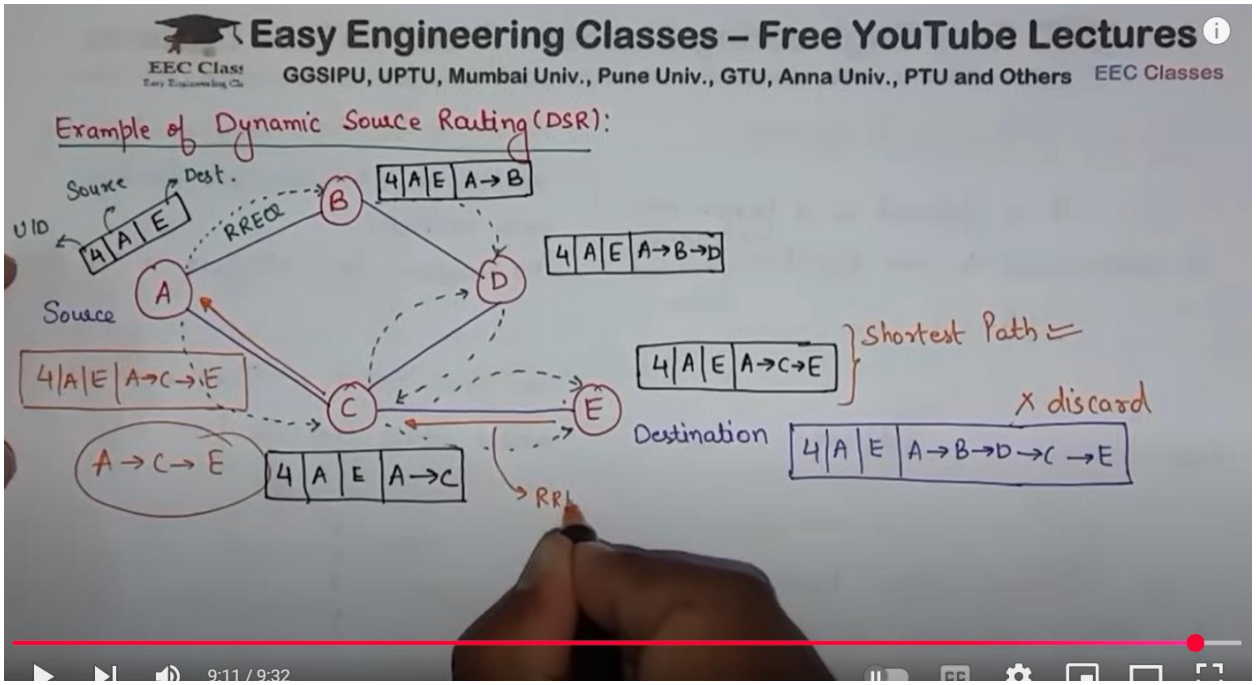


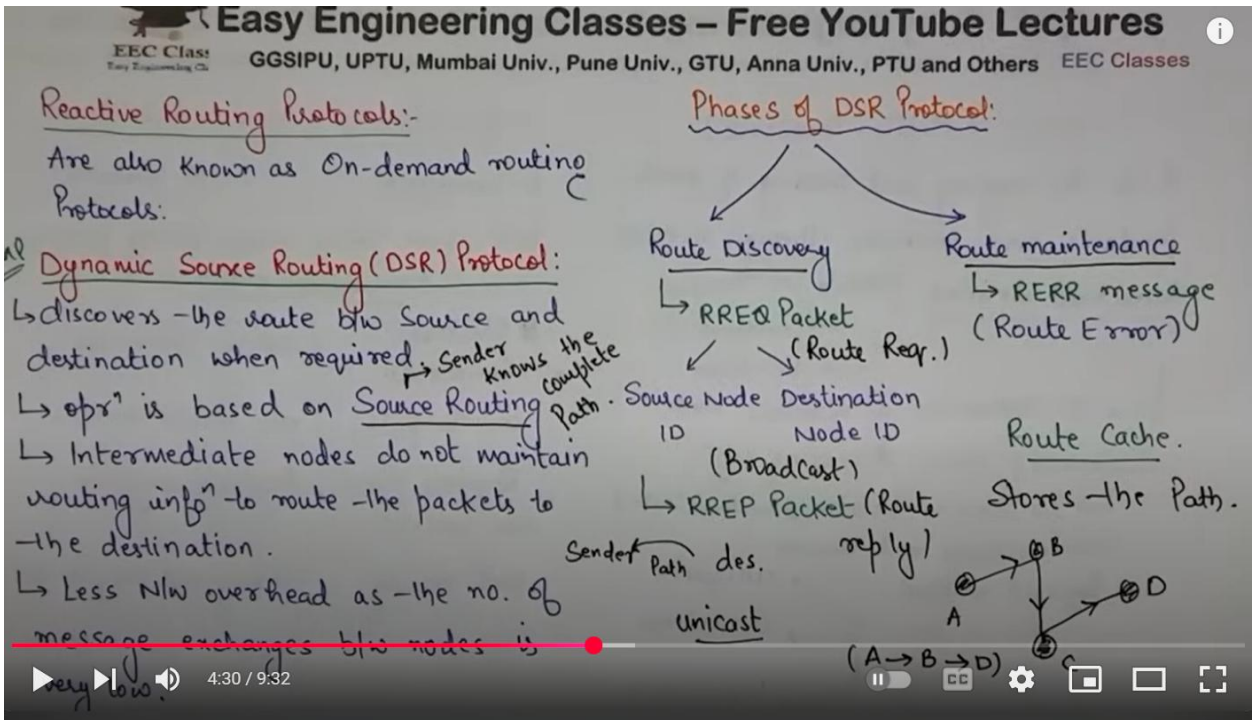
2. **Global State Routing (GSR):** It is a pro-active/table driven routing protocol. It actually extends the link state routing of the wired networks. It is based on the Dijkstra's routing algorithm. Link state routing protocol was not suited for mobile ad-hoc networks because in it, each node floods the link state routing information directly into the whole network i.e. Global flooding which may lead to the congestion of control packets in the network.

Hence, as a solution Global State Routing Protocol (GSR) came into the picture. Global state routing doesn't flood the link state routing packets globally into the network. In GSR, each of the mobile node maintains one list and three tables namely, adjacency list, topology table, next hop table and distance table.

2. Reactive routing protocols: These are also known as on-demand routing protocol. In this type of routing, the route is discovered only when it is required/needed. The process of route discovery occurs by flooding the route request packets throughout the mobile network. It consists of two major phases namely, route discovery and route maintenance.

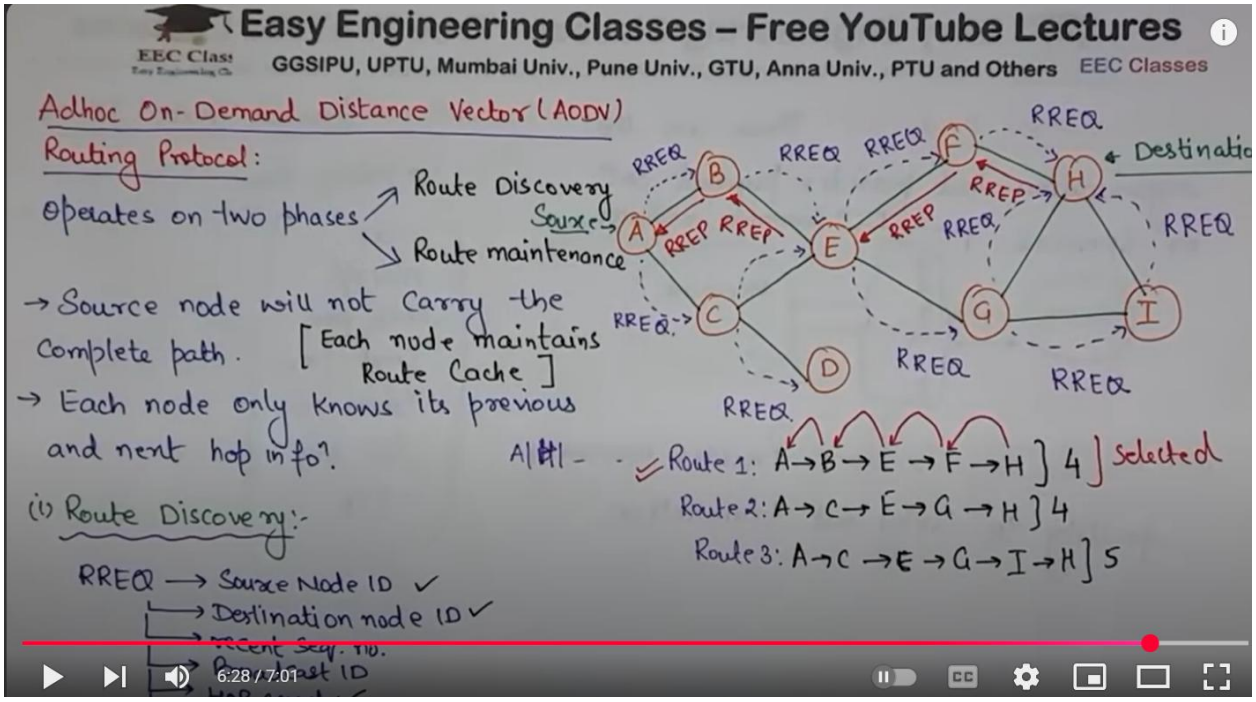
1. **Dynamic Source Routing protocol (DSR):** It is a reactive/on-demand routing protocol. In this type of routing, the route is discovered only when it is required/needed. The process of route discovery occurs by flooding the route request packets throughout the mobile network. In this protocol, Source node stores the complete path information and intermediate nodes do not need to maintain routing information. It consists of two phases:
    - **Route Discovery:** This phase determines the most optimal path for the transmission of data packets between the source and the destination mobile nodes.
    - **Route Maintenance:** This phase performs the maintenance work of the route as the topology in the mobile ad-hoc network is dynamic in nature and hence, there are many cases of link breakage resulting in the network failure between the mobile nodes.





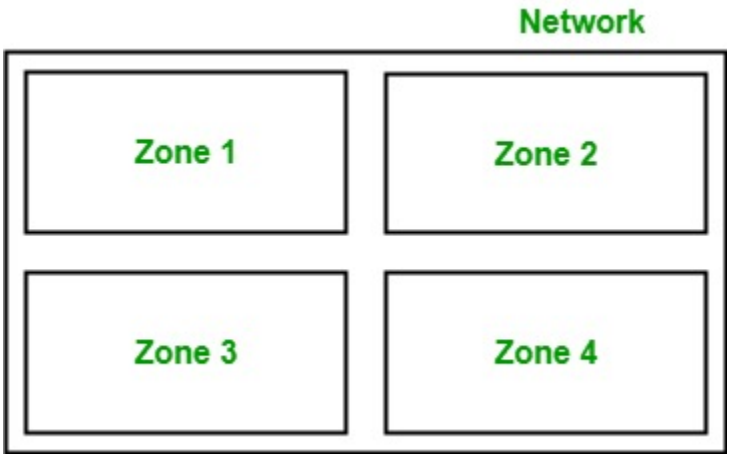
2. **Ad-Hoc On Demand Vector Routing protocol (AODV):** It is a reactive/on-demand routing protocol. It is an extension of dynamic source routing protocol (DSR) and it helps to remove the disadvantage of dynamic source routing protocol. In DSR, after route discovery, when the source mobile node sends the data packet to the destination mobile node, it also contains the complete path in its header. Hence, as the network size increases,

the length of the complete path also increases and the data packet's header size also increases which makes the whole network slow. Hence, Ad-Hoc On Demand Vector Routing protocol came as solution to it. The main difference lies in the way of storing the path, in AODV Sourcenode does not stores complete path information, instead of that each not stores information of its previous and next node. It also operates in two phases: Route discovery and Route maintenance.



3. Hybrid Routing protocol: It basically combines the advantages of both, reactive and pro-active routing protocols. These protocols are adaptive in nature and adapts according to the zone and position of the source and destination mobile nodes. One of the most popular hybrid routing protocol is **Zone Routing Protocol (ZRP)**.

The whole network is divided into different zones and then the position of source and destination mobile node is observed. If the source and destination mobile nodes are present in the same zone, then proactive routing is used for the transmission of the data packets between them. And if the source and destination mobile nodes are present in different zones, then reactive routing is used for the transmission of the data packets between them.



Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol is a network protocol used to automate the process of assigning IP addresses and other network configuration parameters to devices (such as computers, smartphones, and printers) on a network. Instead of manually configuring each device with an IP address, DHCP allows devices to connect to a network and receive all necessary network information, like IP address, subnet mask, default gateway, and DNS server addresses, automatically from a DHCP server.

This makes it easier to manage and maintain large networks, ensuring devices can communicate effectively without conflicts in their network settings. DHCP plays a crucial role in modern networks by simplifying the process of connecting devices and managing network resources efficiently.

What is DHCP?

DHCP stands for Dynamic Host Configuration Protocol. It is the critical feature on which the users of an enterprise network communicate. DHCP helps enterprises to smoothly manage the allocation of IP addresses to the end-user clients' devices such as desktops, laptops, cellphones, etc. is an application layer protocol that is used to provide:

DHCP is based on a client-server model and based on discovery, offer, request, and ACK.

Why Do We Use DHCP?

DHCP helps in managing the entire process automatically and centrally. DHCP helps in maintaining a unique IP Address for a host using the server. DHCP servers maintain information on TCP/IP configuration and provide configuration of address to DHCP-enabled clients in the form of a lease offer.

Components of DHCP

The main components of DHCP include:

- **DHCP Server:** DHCP Server is a server that holds IP Addresses and other information related to configuration.
- **DHCP Client:** It is a device that receives configuration information from the server. It can be a mobile, laptop, computer, or any other electronic device that requires a connection.
- **DHCP Relay:** DHCP relays basically work as a communication channel between DHCP Client and Server.
- **IP Address Pool:** It is the pool or container of IP Addresses possessed by the DHCP Server. It has a range of addresses that can be allocated to devices.
- **Subnets:** Subnets are smaller portions of the IP network partitioned to keep networks under control.
- **Lease:** It is simply the time that how long the information received from the server is valid, in case of expiration of the lease, the tenant must have to re-assign the lease.
- **DNS Servers:** DHCP servers can also provide DNS (Domain Name System) server information to DHCP clients, allowing them to resolve domain names to IP addresses.
- **Default Gateway:** DHCP servers can also provide information about the default gateway, which is the device that packets are sent to when the destination is outside the local network.
- **Options:** DHCP servers can provide additional configuration options to clients, such as the subnet mask, domain name, and time server information.
- **Renewal:** DHCP clients can request to renew their lease before it expires to ensure that they continue to have a valid IP address and configuration information.
- **Failover:** DHCP servers can be configured for failover, where two servers work together to provide redundancy and ensure that clients can always obtain an IP address and configuration information, even if one server goes down.
- **Dynamic Updates:** DHCP servers can also be configured to dynamically update DNS records with the IP address of DHCP clients, allowing for easier management of network resources.
- **Audit Logging:** DHCP servers can keep audit logs of all DHCP transactions, providing administrators with visibility into which devices are using which IP addresses and when leases are being assigned or renewed.

🔷 What is Traditional TCP/IP?

Traditional TCP/IP refers to the **original suite of communication protocols** developed to enable networking and reliable data transmission across interconnected devices, primarily in **wired networks**.

It consists mainly of two core protocols:

---

1. TCP (Transmission Control Protocol)

Role: Ensures **reliable**, **ordered**, and **error-checked** delivery of data between applications over a network.

Key Features:

- **Connection-oriented**: Establishes a connection before data transfer.
- **Reliable**: Ensures data is delivered correctly using acknowledgment (ACK) and retransmission.
- **Flow and Congestion Control**: Manages data rate to avoid overwhelming receivers or network.
- Commonly used for applications like web browsing (HTTP), email (SMTP), file transfers (FTP), etc.

---

2. IP (Internet Protocol)

Role: Handles **addressing** and **routing** packets from source to destination across networks.

Key Features:

- **Connectionless**: Each packet is routed independently.
- **Best-effort delivery**: No guarantees of delivery, order, or integrity.
- Uses **IP addresses** to identify devices (IPv4/IPv6).

- ### 🔁 TCP/IP Layered Architecture
- The TCP/IP model has **4 layers** (compared to OSI's 7 layers):

TCP/IP Layer	Equivalent OSI Layer(s)	Function
Application	Application, Presentation, Session	User applications (HTTP, FTP, DNS, etc.)
Transport	Transport	Reliable delivery (TCP) or fast delivery (UDP)
Internet	Network	Addressing and routing (IP, ICMP, etc.)
Network Access	Data Link + Physical	Physical transmission over media (Ethernet, Wi-Fi)

🔷 Mobile TCP (M-TCP)

Definition: Mobile TCP is a variant of TCP optimized for **mobile and wireless networks** to handle challenges like disconnections, handoffs, and high error rates.

Key Features:

- **Splits the TCP connection** between the mobile host and the fixed host via a **mobility support node** (such as a base station).
- **Maintains end-to-end TCP semantics**, unlike some other solutions like split-TCP.
- **Freezes TCP window size** during disconnection to avoid unnecessary congestion control behavior.
- **Avoids timeouts** by recognizing temporary disconnections (e.g., during handoff) and informing the fixed host not to reduce its sending rate.

Advantages:

- Reduces performance degradation during handoffs.
- Improves throughput by **avoiding unnecessary congestion control**.
- Maintains TCP reliability and ordering.

🔁 **Comparison Table:**

Feature	Traditional TCP	Mobile TCP (M-TCP)
Designed for	Wired networks	Wireless/mobile networks
Handles disconnections	Poorly	Gracefully (e.g., window freezing)

Feature	Traditional TCP	Mobile TCP (M-TCP)
Packet loss handling	Assumes congestion	Differentiates between causes
Throughput in mobile cases	Often low	Higher
End-to-end semantics	Yes	Yes
Congestion control	Always triggered on loss	Avoids when loss is not due to congestion

Transport layer protocols - indirect, snooping, mobile Tcp

📝 **Imagine a situation:**

You (📱 Mobile User) want to send messages to your friend (💻 Computer User) through a post office (🏢 Base Station). But you're on a moving train (mobile environment), and sometimes your network is weak (disconnections or handoffs).

Now let's see how each TCP variant works:

🔷 **1. Indirect TCP (I-TCP)**

🔹 **What happens**:

- The connection is **split in two**:
  - 📱 ↔ 🏢 (Mobile ↔ Base Station): One connection
  - 🏢 ↔ 💻 (Base Station ↔ Computer): Another connection

🔹 **How it works**:

- The **base station handles problems** like weak signals or disconnections.
- You don't need to tell the computer everything — the base station hides mobile issues.

🔹 **Drawback**:

- If a message is lost on the way to you, the computer **thinks everything was fine** because the base station said "delivered."

📌 **Like two people relaying your message — but the final receiver trusts the middleman.**

🔷 **2. Snooping TCP**

🔹 **What happens**:

- There is **only one connection**: 📱 ↔ 💻
- The **base station "snoops" (watches)** your messages quietly.

🔹 **How it works**:

- It **keeps a copy** of each message.
- If the mobile user doesn't get it (due to weak signal), the base station **resends it**.

🔹 **Drawback**:

- Can't work if messages are **encrypted** (like locked letters).
- Needs both directions to pass through the base station.

📌 **Like a smart postman watching your messages, ready to resend if needed.**

🔷 3. Mobile TCP (M-TCP)

🔹 **What happens**:

- One full connection 📱 ↔ 💻
- But if the signal is weak or you're moving (handoff), the **base station tells the computer to pause**.

🔹 **How it works**:

- During disconnection, the base station **freezes the window** (tells computer: "wait, don't send more!").
- After reconnection, data continues smoothly.

📌 **Like telling your friend to stop sending messages until you reach a better network.**