Mobile IP

- Mobile IP is a communication protocol
- Allows the users to move from one network to another with the same IP address.
- Ensures that the communication will continue without the user's sessions or connections being dropped
- Mobile IP (Internet Protocol) is a protocol that enables mobile devices to maintain a continuous Internet connection even when moving between different networks

Requirements

- **Compatibility:** Mobile networks need to be compatible with a wide range of devices, operating systems, and applications to ensure that users can connect to the network with their preferred device.
- **Transparency:** Mobility should remain 'invisible' for many higher layer protocols and applications.
- **Scalability and Efficiency :** Enhancing IP for mobility must not generate too many new messages flooding the whole network. Special care has to be taken considering the lower bandwidth of wireless links
- **Security:** Mobile networks need to be secure and protect user data from unauthorized access or interception. Mobility poses many security problems. minimum requirement is that of all the messages related to the management of Mobile IP are authenticated. IP layer must be sure that if it forwards a packet to a mobile host that this host receives the packet. e IP layer can only guarantee that the IP address of the receiver is correct.

Goal

- provide a means for mobile devices to communicate with each other and with other devices on the network.
- This layer is responsible for the establishment and management of communication links between devices, as well as for the routing of data packets between them

Entities and terminology

- **Mobile node (MN)**
  - A mobile node is a device that can move from one location to another while maintaining its network connectivity
  - It is assigned a unique identifier called the Mobile Node Identifier (MNID)

- Mobile nodes are not necessarily small devices such as laptops with antennas or mobile phones.
- The current location of the mobile node is tracked by the network through the use of its IP address and the Home Agent (HA) - the router that is responsible for managing the mobile node's mobility
- The mobile node can also communicate directly with other devices on the same network or with devices on other networks using the Mobile IP protocol

- **Correspondent node (CN)**
  - corresponding node refers to a network node that communicates with another network node in a specific way
  - also be referred to as a peer node or a counterpart node.
  - each node in a mobile network protocol has one or more corresponding nodes with which it communicates to perform specific functions such as routing, handover, authentication, and billing.
  - The specific corresponding nodes and their functions depend on the network architecture and the protocol used
- **Home network**
  - home network typically refers to a set of devices that are connected to each other through a local area network (LAN) within a residence or building
  - home network is the subnet the MN belongs to with respect to its IP address.
  - No mobile IP support is needed within the home network
- **Foreign network:**
  - Foreign network refers to a mobile network operator that a user is roaming on when they are outside of their home network
  - foreign network is the current subnet the MN visits and which is not the home network
  - When a user travels to a different country, they may need to connect to a foreign network in order to use their mobile phone and access mobile services
  - When a user connects to a foreign network, their home network and the foreign network need to communicate with each other to ensure that the user can access services and that the appropriate charges are applied
  - foreign networks play an important role in enabling mobile users to stay connected while traveling outside of their home network's coverage area
- **Foreign agent (FA)**
  - foreign agent in mobile network protocol refers to a network entity that facilitates mobility management in mobile communication systems
  - typically used in wireless communication networks such as cellular networks and wireless LANs
  - responsible for managing communication with mobile nodes that are visiting a network that is different from their home network.

- The foreign agent is responsible for tracking the location of the mobile node and forwarding the data packets to and from the mobile node to its home network
- foreign agents play an important role in ensuring seamless communication and mobility management in mobile communication systems
- FA can be the default router for the MN.
- FAs can also provide security services because they belong to the foreign network

➢ **Care-of address (COA)**

- refers to the address of a mobile node (MN) in a foreign network when it is away from its home network.
- The COA is used to facilitate communication between the mobile node and other nodes on the internet while the mobile node is roaming
- When a mobile node moves to a new network, it registers its COA with its home agent (HA), which is a router in its home network that maintains a binding between the mobile node's home address (HA) and COA.
- COA can be either a temporary or a permanent address assigned by the foreign network, depending on the network's configuration.
- COA defines the current location of the MN from an IP point of view
- There are two different possibilities for the location of the COA

1. **Foreign agent COA:**
    - foreign agent is a network entity that helps a mobile device maintain connectivity and mobility while it roams outside of its home network
    - Care-of address (CoA) is an IP address that is used by the foreign agent to forward data packets to the mobile device.
    - When the mobile device roams to a foreign network, it registers with the foreign agent and provides its home address and the CoA.
    - The foreign agent then uses the CoA to forward data packets to the mobile device while it is roaming in the foreign network
    - When the mobile device moves to a new foreign network, it reregisters with the foreign agent and provides a new CoA.
    - This process continues as the mobile device moves from network to network
2. **Co-located COA:**
    - When a mobile device moves from one network to another, its IP address changes, which can disrupt its ongoing connections.
    - avoid this, the mobile device can use a Co-located CoA, which is an IP address assigned by the local network that the device is currently connected to.
    - This address serves as a temporary address for the device, allowing it to maintain its connections while it roams

    - typically assigned by the local network's router or gateway and is used in combination with the mobile device's permanent home address to identify it on the Internet.
    - When the mobile device moves to a new network, it can request a new Co-located CoA from the new network's router or gateway.

- **Home agent (HA)**
    - home agent is a network node that is responsible for managing the communication between a mobile node and its home network.
    - The home agent is part of the Mobile IP protocol, which allows mobile devices to maintain a consistent IP address as they move between different networks
    - When a mobile node moves to a new network, it registers with the home agent to inform it of its new location.
    - The home agent then forwards all incoming packets for the mobile node to its current location.
    - This allows the mobile node to maintain its connection to the home network and continue to receive data without interruption, even as it moves between different networks
    - home agent also authentication and security

Packet Delivery

- Packet delivery in mobile network protocols involves the transmission of data packets between different nodes or devices within a mobile network.
- When the Mobile Node moves out of its home network and enters a foreign network, it registers with the Foreign Agent, which informs the Home Agent about the registration.
- The Home Agent is responsible for routing packets destined for the Mobile Node's home network, while the Foreign Agent is responsible for routing packets destined for the Mobile Node while it is in the foreign network
- When a packet is sent to the Mobile Node, it is first forwarded to the Home Agent, which determines the current location of the Mobile Node.
- The Home Agent then encapsulates the packet and sends it to the Foreign Agent serving the Mobile Node's current location
- The Foreign Agent decapsulates the packet and forwards it to the Mobile Node.
- If the Mobile Node moves to another foreign network, it must register with a new Foreign Agent, and the process is repeated.

Tunneling and Encapsulation

- tunnel establishes a virtual pipe for data packets between a tunnel entry and a tunnel endpoint
- sending a packet through a tunnel, is achieved by using encapsulation
- Encapsulation is the mechanism of taking a packet consisting of packet header and data and putting it into the data part of a new packet
- reverse operation, taking a packet out of the data part of another packet, is called decapsulation
- Tunneling refers to the process of encapsulating a packet within another packet, so that it can be transmitted across a network.
- In mobile networks, tunneling is commonly used to transport IP packets between different parts of the network, such as between the mobile device and the gateway or between different parts of the core network.
- Encapsulation refers to the process of adding a header and possibly a footer to a packet to provide additional information about the packet and to facilitate its transport across the network.
- In mobile networks, encapsulation is commonly used to add a header to the IP packet that contains information about the source and destination addresses, as well as other routing information.
- This header is then used to route the packet through the network

IP-in-IP

- IP in IP encapsulation is a protocol that is used to encapsulate one IP packet in another IP packet.
- outer header of the IP packet has the Source IP, which is the entry point of the traffic
- tunnel. The Destination IP is the exit point
- In networking, a packet is the smallest unit of data, and a basic data packet contains information of both the receiver and sender in the header.
- Encapsulation is the process in which a protocol is added to the packet header. This way, when the data enters into the transport tunnel, it is no longer called data, but it is known as a segment
- In networking, a packet is the smallest unit of data, and a basic data packet contains information of both the receiver and sender in the header.
- Encapsulation is the process in which a protocol is added to the packet header.
- when the data enters into the transport tunnel, it is no longer called data, but it is known as a segment

Agent Discovery

- A mobile node uses a method known as agent discovery to determine the following information
- When the node has moved from one network to another

- Whether the network is the node's home or a foreign network
- What is the foreign agent care-of address offered by each foreign agent on that network
- In the absence of agent advertisements, a mobile node can solicit advertisements. This is known as agent solicitation
- **Agent advertisement:** first method, FA and HA advertise their presence periodically using special agent advertisement messages
- **Agent solicitation:** If no agent advertisements are present or the inter arrival time is too high, and an MN has not received a COA, the mobile node must send agent solicitations

Agent Registration

- main purpose of the registration is to inform the home agent of the current location for correct forwarding of packets
- If the COA is at the FA, MN sends its registration request containing the COA to the FA which is forwarding the request to the HA
- If the COA is co-located, registration can be very simpler. mobile node may send the request directly to the HA and vice versa

Dynamic host configuration protocol

- Dynamic Host Configuration Protocol (DHCP) is a protocol used in mobile networks to assign IP addresses to devices
- When a mobile device connects to a network, it sends a request for an IP address to the DHCP server.
- The DHCP server responds with an available IP address and other configuration information, such as the subnet mask, gateway address, and DNS server addresses.
- The mobile device then uses this information to configure its network settings and establish a connection to the network
- DHCP plays an important role in mobile networks because it enables devices to move from one network to another without having to manually configure their network settings each time
- DHCP port number for server is 67
- DHCP port number for the client is 68
- In DHCP, the client and the server exchange mainly 4 DHCP messages in order to make a connection, also called DORA process, but there are 8 DHCP messages in the process

DHCP discover message

- discover message is sent by a mobile device when it is seeking an IP address and other network configuration information from a DHCP server
- This message is sent to locate a DHCP server on the network that can provide the device with an IP address, subnet mask, gateway, and other network configuration details

- This message is generated by Client host in order to discover if there is any DHCP server/servers are present in a network or not
- This message is broadcasted to all devices present in a network to find the DHCP server

DHCP offer message

- server will respond to host in this message specifying the unleased IP address and other TCP configuration information.
- This message is broadcasted by server
- If there are more than one DHCP servers present in the network then client host will accept the first DHCP OFFER message it receives
- DHCP offer message is typically sent by the DHCP server to a mobile device that is requesting an IP address.
- The DHCP offer message contains an available IP address that the mobile device can use to connect to the network
- The DHCP server receives the discovery message and responds with a DHCP offer message, which contains an available IP address, subnet mask, gateway IP address, and other network configuration information
- The mobile device receives the DHCP offer message and can choose to accept or reject the offer. If it accepts the offer, it sends a DHCP request message to the DHCP server, confirming that it will use the offered IP address

DHCP request message

- DHCP (Dynamic Host Configuration Protocol) is used to assign IP addresses to mobile devices.
- When a mobile device connects to the network, it sends a DHCP request message to request an IP address
- DHCP request message includes the following information:
    1. Source MAC address: This is the MAC address of the mobile device requesting the IP address
    2. DHCP message type: This indicates that the message is a DHCP request message
    3. Transaction ID: This is a unique identifier for the DHCP transaction
    4. Requested IP address: This is the IP address that the mobile device is requesting
- The DHCP server responds to the request message by sending a DHCP offer message that includes an available IP address and the other necessary configuration information.
- The mobile device then sends a DHCP request message to accept the offer, and the DHCP server sends a DHCP acknowledgement message to confirm the assignment of the IP address to the mobile device

DHCP acknowledgement message

- Dynamic Host Configuration Protocol (DHCP) acknowledgement message is used to assign IP addresses dynamically to mobile devices.
- The DHCP acknowledgement message is sent from the DHCP server to the mobile device after the DHCP request message is received
- When a mobile device connects to a mobile network, it sends a DHCP request message to the DHCP server requesting an IP address.
- The DHCP server responds with a DHCP acknowledgement message, which includes the assigned IP address, subnet mask, default gateway, and other network configuration information

Advantages DHCP

- Ease of adding new clients to a network
- Reuse of IP addresses reducing the total number of IP addresses that are required
- Efficient IP address management: allows mobile network operators to efficiently manage IP addresses by automatically assigning IP addresses to mobile devices as they connect to the network
- Flexibility: DHCP allows mobile devices to obtain IP addresses dynamically, which means that they can be assigned different IP addresses each time they connect to the network. This provides flexibility to both the mobile device and the network operator
- Scalability: DHCP can easily scale to support large numbers of mobile devices, making it ideal for mobile networks that need to support a large number of users

Mobile Ad Hoc Network

- MANET stands for Mobile Adhoc Network also called a wireless Adhoc network or Adhoc wireless network
- Each node behaves as a router as they forward traffic to other specified nodes in the network
- self-configuring network of mobile devices connected by wireless links
- each device can act as a router, forwarding packets to other devices in the network to enable communication between devices that are not directly within wireless range of each other
- MANET can be used to provide communication in areas where traditional infrastructure-based networks are not available
- Mobile devices can connect to each other directly or through intermediate devices, forming a network that is highly flexible and adaptable to changing conditions
- One of the main challenges in MANETs is routing
- MANET consists of a number of mobile devices that come together to form a network as needed, without any support from any existing internet infrastructure or any other kind of fixed stations
- no such infrastructure exists and network topology may be changed dynamically in an unpredictable manner since nodes are free to move and each node

Issues

- raise another issue, that of symmetric and asymmetric (bidirectional) and asymmetric (unidirectional) links. Consider symmetric links with associative radio range.

Characteristics of MANET

- Limited battery life: Since mobile devices in a MANET rely on their own batteries to communicate with other devices, power management is critical. Routing protocols must be designed to minimize energy consumption to extend the life of the devices
- Limited bandwidth: MANETs typically have limited bandwidth compared to wired or cellular networks, and the available bandwidth is shared among all devices in the network
- Dynamic topology: Since nodes in a MANET can move freely, the network topology can change frequently and unpredictably. As a result, routing protocols must be able to adapt quickly to changes in the network topology to maintain connectivity and minimize packet loss
- Quality of Service (QoS): In a MANET, providing QoS guarantees is a challenging task due to the limited bandwidth and dynamic topology

Applications of MANET

- **Defense applications:** require on the fly communications set-up, and ad hoc/sensor networks. In military operations, soldiers and vehicles often operate in an ad-hoc and dynamic environment
- **Disaster management:** During natural disasters, communication infrastructure may be damaged, and traditional communication networks may fail. MANETs can be used to establish a communication network for rescue teams, emergency responders, and affected people
- **Transportation:** In transportation systems, vehicles can form a MANET to communicate with each other and share information about traffic, road conditions, and accidents. This can improve traffic management and reduce accidents
- **Healthcare:** In healthcare applications, MANETs can be used for patient monitoring, remote diagnosis, and emergency response
- **Smart cities:** In smart city applications, MANETs can be used for communication between different devices, such as sensors, cameras, and smart meters

Routing

- process of finding the best path for traffic in a network, or across multiple networks
- we need to deliver messages at proper location and in an appropriate way
- Routing in a mobile ad-hoc network depends on many factors such as:
  – Modeling of the topology,
  – Selection of routers,
  – Initiation of a route request

- Routing protocol can be classified as
  1. **Proactive Protocol**
     - also known as table-driven routing protocol
     - evaluate continuously the routes within the network
     - continuously maintain the routing information, so that when a packet needs to be forwarded, the path is known already and can be immediately used
     - whenever a route is needed, there is negligible delay in determining the route
     - Requires more amounts of data for maintaining routing information
     - Low reaction on re-structuring network and failures of individual nodes
  2. **Reactive Protocol**
     - do not maintain routes but invoke a route determination procedure only on demand or we can say reactive protocols build the routes only on demand
     - when a route is required, some sort of global search procedure is initiated
     - family of classical flooding algorithms belongs to the reactive protocol group
     - reactive ad-hoc network routing protocols include
     - ad hoc on demand distance vector (AODV)
     - No large overhead for global routing table maintenance as in proactive protocols
     - Reaction is quick for network restructure and node failure
     - Latency time is high in route finding
     - Excessive flooding can lead to network clogging
  3. **Hybrid Protocol**
     - take advantage of best of reactive and proactive schemes
     - basic idea behind such protocols is to initiate route discovery on demand but at a limited search cost
     - popular hybrid protocols is zone routing protocol (ZRP)
- Table-driven routing protocol
  - protocols are called table-driven because each node is required to maintain one or more tables containing routing information on every other node in the network
  - proactive in nature so that the routing information is always consistent and up to date
  - protocols respond to changes in network topology by propagating the updates throughout the network so that every node has a consistent view of the network
  - The table driven routing protocols are categorized as follows
    1. **Destination**
       - based on Bellman-Ford algorithm
       - Each entry in the table contains a sequence number assigned by the destination node
       - sequence numbers allow the node to distinguish stale routes from new ones
       - A new route broadcast contains:
         - destination address
         - number of hops required to reach the destination
         - sequence number of the information received about the destination and a new sequence number unique to the broadcast
       - If there multiple routes are available for the same destination, the route with the most recent sequence number is used
       - If two updates have the same sequence number, the route with smaller metric is used to optimize the routing

        - Destination sequenced distance vector routing was one of the early algorithms available
        - suitable for creating ad-hoc networks with small no. of nodes
        - sequenced distance vector routing requires a regular update of its routing tables, which uses more battery power and a small amount of bandwidth even when the network is idle
        - algorithm is not suitable for highly dynamic networks
    2. Cluster Head gateway switch Routing
    3. Wireless routing protocol (WRP)

Source initiated on -demand protocols

- Source - initiated on demand routing is reactive in nature
- generates routes only when a source demands it
- when a source node requires a route to a destination, the source initiates a route discovery process in the network
- process finishes when a route to the destination has been discovered or all possible routes have been examined without any success
- discovered route is maintained by a route maintenance procedure, until it is no longer desired or the destination becomes inaccessible

Dynamic Source Routing (DSR)

- on-demand routing protocol which is based on source routing
- uses source routing instead of relying on the routing table at each intermediate device
- protocol works in two main phases
    - Route discovery
    - Route maintenance
- Dynamic Source Routing (DSR) is a protocol used at the network layer of the OSI model for mobile ad hoc networks (MANETs).
- It is a reactive protocol, which means that it establishes routes on-demand when required rather than maintaining a pre-determined routing table
- each node in the network maintains a cache of routes it has learned from previous communications.
- When a node needs to send a packet to a destination node, it first checks its cache to see if it has a route to the destination.
- If a route is found, the packet is forwarded along the route. If there is no route, the source node initiates a route discovery process
- In the route discovery process, the source node broadcasts a route request (RREQ) packet to its neighbour.
- The RREQ contains the source and destination addresses and a unique identifier for the request.
- Each intermediate node receiving the RREQ checks its cache to see if it has a route to the destination. If not, it appends its own address to the RREQ and broadcasts it to its neighbour

- When the RREQ reaches the destination node, the destination sends a route reply (RREP) packet back to the source node.
- The RREP contains the path from the source to the destination, which is stored in the cache of each node along the path.
- The source node then uses this path to forward its original packet