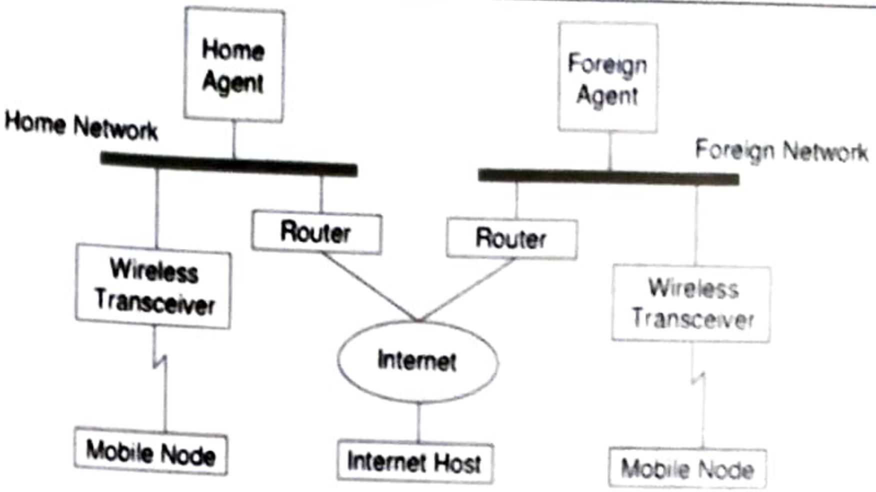
UNIT–IV

MOBILE NETWORK AND TRANSPORT LAYER

4.1 MOBILE IP

Mobile IP is an Internet Engineering Task Force standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address.

Mobile IP is a networking protocol that allows mobile devices, such as smartphones, laptops, and tablets, to maintain continuous and uninterrupted connectivity to the Internet or a network as they move between different locations or access points. Traditionally, IP addresses are tied to specific physical locations or networks. When a mobile device changes its point of attachment to the Internet (e.g., moving from one Wi-Fi network to another or switching from Wi-Fi to cellular data), its IP address typically changes as well, leading to a disruption in ongoing communications and services.



MOBILE IP TOPOLOGY

1. **Process of Mobile IP**

The mobile IP process has following three main phases, which are:

a. **Agent Discovery:**

i. During the agent discovery phase the HA and FA advertise their services on the network by using the ICMP router discovery protocol (IROP).

ii. Mobile IP defines two methods: agent advertisement and agent solicitation which are in fact router discovery methods plus extensions.

iii. **Agent advertisement:** For the first method, FA and HA advertise their presence periodically using special agent advertisement messages. These messages advertisement can be seen as a beacon broadcast into the subnet. For this advertisement internet control message protocol (ICMP) messages according to RFC 1256, are used with some mobility extensions.

iv. **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. These solicitations are again bases on RFC 1256 for router solicitations.

b. **Registration**

i. The main purpose of the registration is to inform the home agent of the current location for correct forwarding of packets.

ii. Registration can be done in two ways depending on the location of the COA.

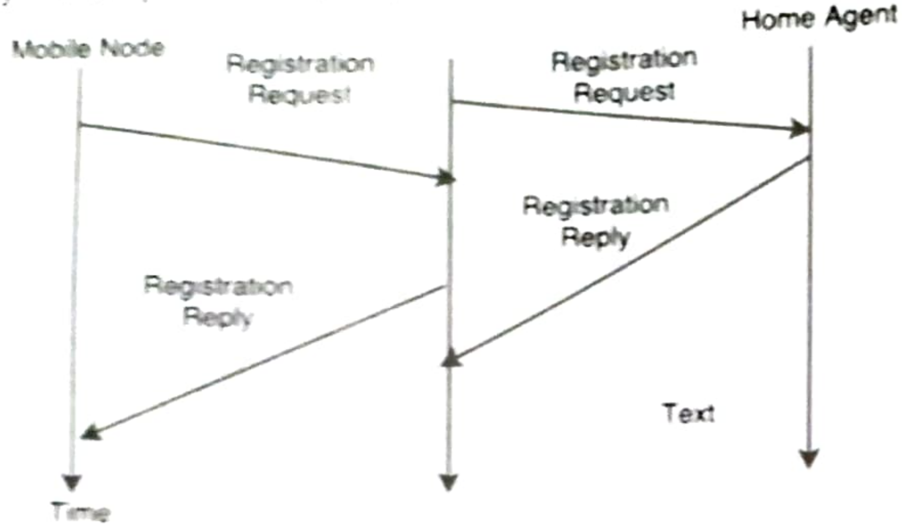
iii. If the COA is at the FA, the MN sends its registration request containing the COA to the FA which is forwarding the request to the HA. The HA now set up a mobility binding containing the mobile node's home IP address and the current COA.

iv. If the COA is co-located, registration can be very simpler. The mobile node may send the request directly to the HA and vice versa. This by the way is also the registration procedure for MNs returning to their home network.

c. **Tunneling**

i. A tunnel is used to establish a virtual pipe for data packets between a tunnel entry and a tunnel endpoint. Packets which are entering in a tunnel are forwarded inside the tunnel and leave the tunnel unchanged. Tunneling, i.e., sending a packet through a tunnel is achieved with the help of encapsulation.

i. Tunneling is also known as "port forwarding" is the transmission and data intended for use only within a private, usually corporate network through a public network.



REGISTRATION OF MOBILE IP

2. Goals of Mobile IP

a. **Seamless Mobility:** The primary goal of Mobile IP is to enable mobile devices to maintain connectivity as they move between different networks without any interruption in ongoing communications or services.

b. **Transparent Connectivity:** The user's mobile device should remain reachable at the same IP address, regardless of its location in different networks.

c. **Minimal Disruption:** Mobile IP should minimize the need for manual intervention or reconfiguration when switching networks, ensuring a smooth user experience.

3. **Assumptions**

a. **Mobile Devices:** The system assumes the presence of mobile devices that can change their point of attachment to the Internet by connecting to different networks (e.g., Wi-Fi, cellular, etc.).

b. **Network Infrastructure:** The network infrastructure must support the Mobile IP protocol and allow the forwarding of packets to mobile devices regardless of their current location.

c. **Multiple Networks:** The system assumes the existence of multiple interconnected networks, and the mobile device can move between these networks.

4. **Requirements**

a. **Unique Identifier:** Each mobile device must have a unique identifier, typically an IP address, which remains consistent even as the device moves between different networks.

b. **Home Network:** A home network is the network where a mobile device is originally registered and assigned a home IP address.

c. **Care-of Address:** When a mobile device moves to a foreign network, it acquires a temporary IP address known as a care-of address (CoA).

d. **Registration:** The mobile device needs to register its current care-of address with its home network or a designated home agent, informing it about its current location.

e. **Routing Updates:** Network routers need to be updated dynamically to direct incoming packets to the mobile device's current care-of address.

f. **Security:** Mobile IP should provide mechanisms to ensure the security and privacy of data transmitted between the mobile device and the home network.

5. **Entities and Terminology**

a. **Mobile Node (MN):** The mobile device, such as a smartphone or laptop, which is capable of moving between different networks while maintaining its IP connectivity.

b. **Home Network:** The network to which the mobile device is originally associated and assigned its permanent home IP address.

c. **Home Agent (HA):** The router or network entity within the home network responsible for maintaining information about the mobile device's location and forwarding packets to its current care-of address.

d. **Foreign Network:** The network in which the mobile device is currently located (visited) and using a care-of address.

e. **Care-of Address (CoA):** The temporary IP address assigned to the mobile device when it attaches to a foreign network.

f. **Correspondent Node (CN):** The device or node with which the mobile device is communicating, either within the same network or a different network.

g. **Mobility Binding:** The association between the mobile device's home IP address and its current care-of address, registered with the home agent.

h. **Tunneling:** The mechanism used to encapsulate packets destined for the mobile device's home address and deliver them to its care-of address.

i. **Registration:** The process where the mobile device informs its home agent about its current care-of address, updating the mobility binding.

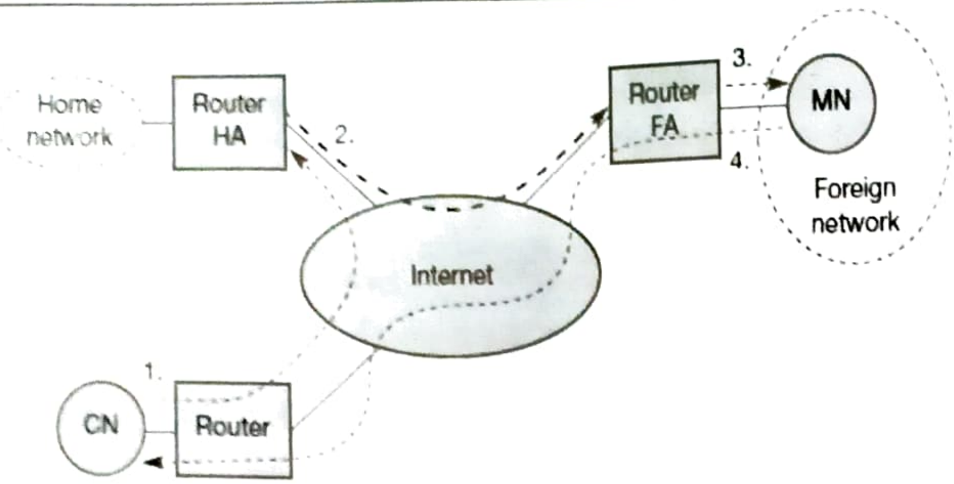
j. **Encapsulation/Decapsulation:** The process of adding an additional header (encapsulation) or removing it (decapsulation) to transmit data between the home agent and the mobile node.

Mobile IP enables seamless mobility for users and devices, allowing them to access the Internet and other services without interruption, regardless of their physical location and the network they are connected to at any given time.

4.2 PACKET DELIVERY, HANDOVER MANAGEMENT AND LOCATION REQUIREMENT

1. **Packet Delivery**

Packet delivery in the context of mobile IP refers to the process of ensuring that data packets are successfully routed from the source (correspondent node or any device on the Internet) to the destination mobile device, even when the mobile device is moving between different networks and has a changing care-of address (CoA).



PACKET DELIVERY

The key steps involved in packet delivery in Mobile IP are as follows:

a. **Sender Initiates Communication:** When a correspondent node (CN) or any device wants to communicate with a mobile device, it sends data packets to the mobile device's permanent home IP address, which remains constant regardless of the mobile device's current location.

b. **Home Agent's Role:** The home agent (HA) in the mobile device's home network intercepts the incoming packets. It is aware of the mobile device's mobility binding, which associates the home IP address with the current care-of address (CoA) of the mobile device.

c. **Encapsulation:** The home agent encapsulates (wraps) the original data packets inside new packets, with the CoA of the mobile device as the destination address in the new packets.

d. **Tunneling:** The home agent then tunnels the encapsulated packets to the foreign network where the mobile device is currently located. Tunneling involves routing the packets through the Internet to reach the foreign network.

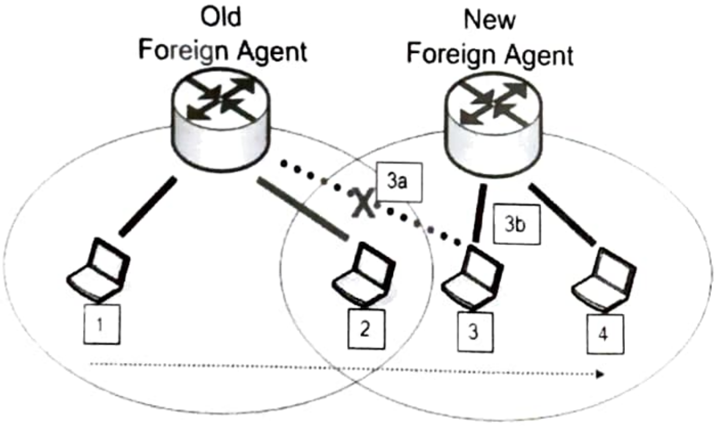
e. **Delivery to Mobile Device:** When the encapsulated packets arrive at the foreign network, they are delivered to the mobile device based on the CoA specified in the packet's destination field.

f. **Decapsulation:** The mobile device receives the encapsulated packets, decapsulates (unwraps) them to retrieve the original data packets, and processes them as usual.

This process of encapsulation, tunneling, and decapsulation ensures that packets are delivered to the mobile device regardless of its current location, allowing for seamless mobility and uninterrupted communication.

2. Handover Management

Handover management, also known as handoff management, is the process of smoothly transferring an ongoing communication session or service from one network (access point) to another as a mobile device moves from one coverage area to another. Handover management is essential to maintain continuous connectivity and quality of service for real-time applications like voice calls, video streaming, or online gaming.



HANDOVER MANAGEMENT

The handover management process involves the following steps:

a. **Detection:** The mobile device continuously monitors signal strength and quality from nearby access points or base stations. When the signal from the current access point becomes weak or deteriorates below a certain threshold, the mobile device starts searching for a better access point to handover to.

b. **Selection:** The mobile device evaluates available access points based on signal strength, quality, and other criteria. It selects the most suitable access point to handover to.

c. **Authentication and Association:** The mobile device initiates authentication and association with the selected access point. This step ensures that the mobile device is allowed to access the new network and can securely communicate with it.

d. **Data Path Switch:** Once the mobile device successfully authenticates with the new access point, the data path is switched from the old access point to the new access point. This allows ongoing data transmission to continue seamlessly.

e. **Notification:** In some cases, the handover process involves notifying the corresponding network entities (e.g., home agent, foreign agent) about the change in the mobile device's location to ensure proper routing of data packets.

Handover management plays a crucial role in maintaining a consistent connection and user experience as mobile devices move between different access points or networks.

3. Location Management

Location management in mobile IP refers to the mechanisms used to track and update the current location of a mobile device as it moves between different networks or access points. The goal of location management is to ensure that data packets are efficiently routed to the mobile device's current location, even if it has a changing care-of address (CoA).

The key components and processes involved in location management are as follows:

a. **Care-of Address (CoA):** When a mobile device moves to a foreign network, it obtains a temporary IP address known as the care-of address (CoA) from the foreign network. The CoA represents the current location of the mobile device.

b. **Registration:** When the mobile device moves to a foreign network, it needs to inform its home network or a designated home agent about its current CoA. This is achieved through the registration process. The mobile device sends a registration request, which contains its home IP address and current CoA, to its home agent.

c. **Mobility Binding:** Upon receiving the registration request, the home agent updates its records to establish a "mobility binding" between the mobile device's home IP address and its current CoA. This binding allows the home agent to know where to forward incoming packets meant for the mobile device.

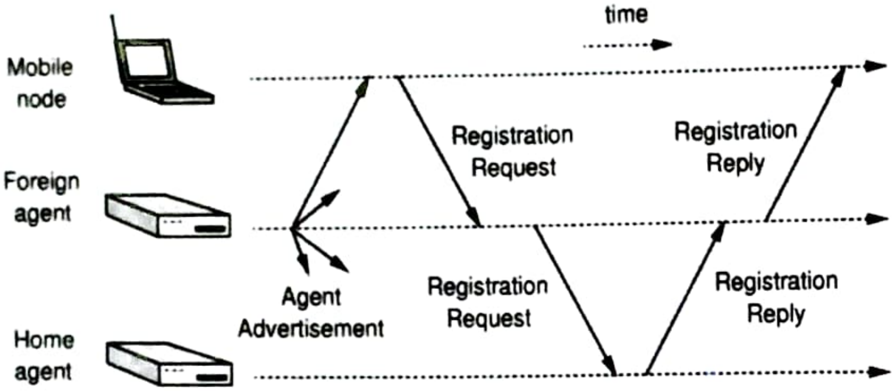
d. **Periodic Updates:** The mobile device and the home agent periodically exchange control messages to keep each other informed about their availability and updated CoA if it changes during the device's movement.

Location management ensures that data packets are correctly routed to the mobile device's current location, regardless of its movements between different networks, enabling seamless mobility and uninterrupted communication.

4.3 REGISTRATION, TUNNELING AND ENCAPSULATION

1. Registration

Registration is a crucial process in Mobile IP that allows a mobile device (also known as the Mobile Node - MN) to inform its home network (or home agent - HA) about its current location in a foreign network. The primary purpose of registration is to establish a "mobility binding" between the mobile device's home IP address and its current temporary IP address (care-of address - CoA) acquired in the foreign network.



MOBILE IP REGISTRATION

The steps involved in the registration process are as follows:

a. When the mobile device moves to a foreign network, it detects its new location and obtains a CoA from the foreign network.

b. The mobile device initiates a registration request by sending a message to its home agent, indicating its home IP address and the acquired CoA.

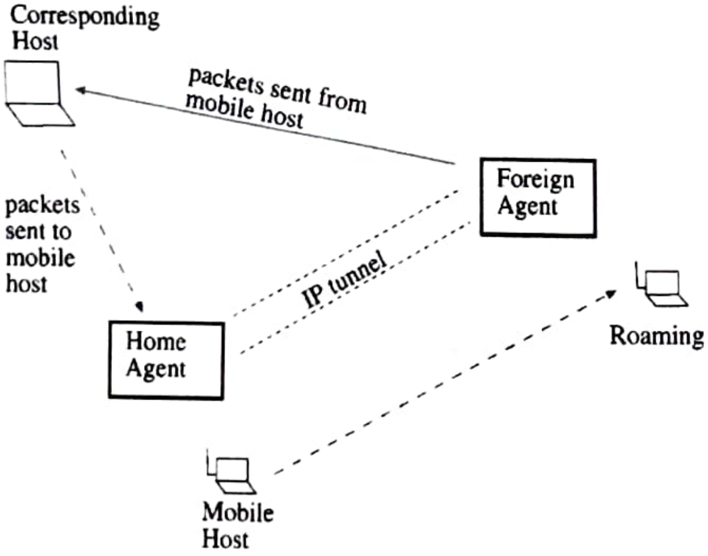
c. The home agent receives the registration request and updates its mobility binding table, associating the mobile device's home IP address with its current CoA.

d. The home agent acknowledges the successful registration by sending a registration reply back to the mobile device, confirming the updated mobility binding.

e. Subsequently, the home agent uses this mobility binding to correctly route incoming packets from the correspondent node (CN) to the mobile device's current location (CoA) in the foreign network.

2. Tunneling

Tunneling is a technique used in Mobile IP to facilitate the transmission of data packets between the home network and the mobile device's current location (care-of address) in the foreign network. Since the mobile device's home IP address is constant, packets sent to the home IP address must be forwarded to the mobile device's current CoA.



TUNNELING IN MOBILE IP

The steps involved in tunneling are as follows:

a. When the home agent receives data packets destined for the mobile device's home IP address, it encapsulates (wraps) these packets inside new packets. The new packets have the mobile device's CoA as the destination address.

b. The original data packets become the payload of the new packets, and additional headers are added to the new packets, including the CoA as the destination address and other necessary information for proper routing.

c. The encapsulated packets are then forwarded (tunneled) to the foreign network where the mobile device is currently located.

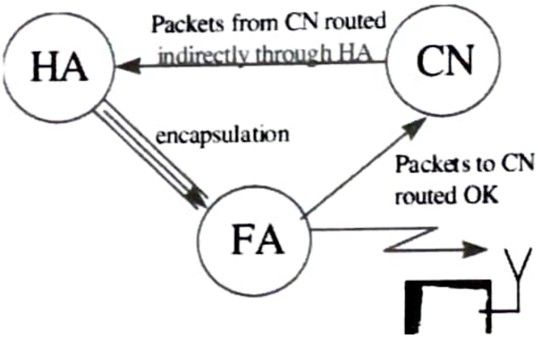
d. The tunneled packets reach the mobile device in the foreign network, where they are decapsulated (unwrapped) to reveal the original data packets.

e. The mobile device processes the original data packets as usual, allowing seamless communication between the mobile device and the correspondent node.

3. Encapsulation

Encapsulation is an essential part of the tunneling process, where data packets are wrapped with additional headers before being transmitted through a tunnel to their destination.

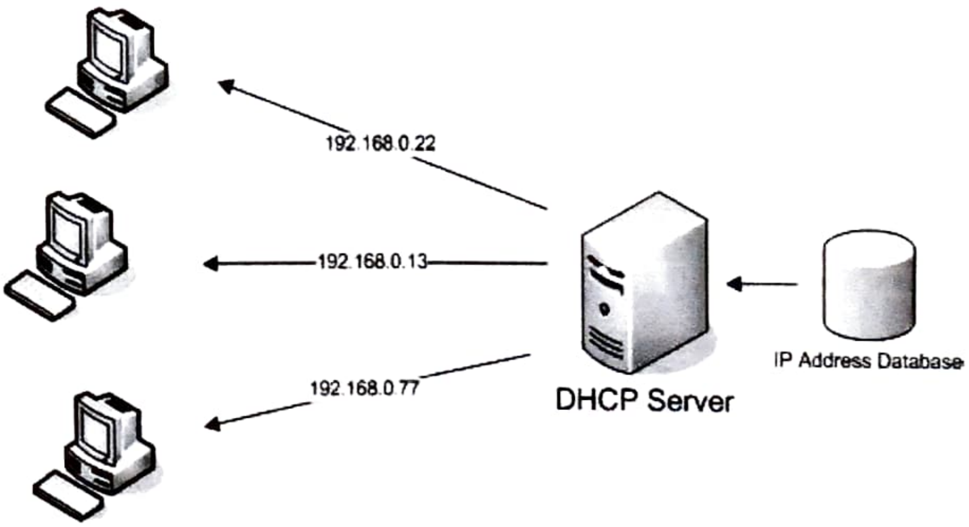
In the context of Mobile IP, encapsulation takes place at the home agent when it prepares the data packets for tunneling to the mobile device's current CoA. The encapsulated packets contain the original data packets (payload) and additional headers that include the mobile device's CoA as the destination address.



ENCAPSULATION IN MOBILE IP

Encapsulation ensures that the data packets are correctly delivered to the mobile device, even when the device is moving and its IP address changes due to its movement between different networks.

4.4 DYNAMIC HOST CONFIGURATION



DYNAMIC HOST CONFIGURATION PROTOCOL

Dynamic Host Configuration Protocol (DHCP) is a network protocol used to automatically assign IP addresses, subnet masks, default gateways, and other network configuration settings to devices on a network. DHCP simplifies the process of network configuration by eliminating the need for manual IP address assignment, especially in larger networks where managing IP addresses manually can be cumbersome and error-prone.

Here's how DHCP works in a mobile network context:

a. **Client Request:** When a device, referred to as a DHCP client, connects to a network, it sends a DHCP request broadcast message to discover available DHCP servers on the network.

b. **DHCP Server Response:** The DHCP servers on the network respond to the client's request with DHCP offer messages. Each offer includes an available IP address, subnet mask, lease duration, and other configuration parameters.

c. **Client Selection:** The client receives multiple DHCP offers and evaluates them. It selects one offer, typically the first received, and sends a DHCP request message indicating its acceptance of the offer.

d. **DHCP Server Acknowledgment:** The DHCP server that sent the selected offer responds with a DHCP acknowledgment (ACK) message, confirming the allocation of the IP address and other configuration parameters to the client.

e. **Lease Duration:** The client and DHCP server agree upon a lease duration for the IP address assignment. This determines how long the client can use the assigned IP address before needing to renew the lease.

f. **Renewal and Rebinding:** As the lease duration approaches its expiration, the client can attempt to renew the lease by sending a DHCP request to the original DHCP server. If the original server is unreachable, the client can also request a renewal from any available DHCP server in the network, a process known as rebinding.

g. **Release:** When the client disconnects from the network or no longer requires the IP address, it sends a DHCP release message to inform the DHCP server that the IP address is no longer in use.

Benefits and Use Cases:

a. **Automation:** DHCP eliminates the need for manual IP address configuration, saving time and reducing the risk of errors.

b. **Scalability:** In larger networks, managing IP addresses manually becomes impractical. DHCP scales easily to handle numerous devices joining and leaving the network.

c. **Centralized Management:** DHCP allows administrators to centrally manage IP address assignments and configurations from a single location.

d. **IP Address Reuse:** DHCP can reuse released IP addresses for other devices, optimizing IP address utilization.

e. Dynamic Environments: DHCP is especially useful in environments where devices frequently connect and disconnect, such as in wireless networks or public Wi-Fi hotspots.

Drawbacks and Considerations:

a. **Single Point of Failure:** If the DHCP server fails, new devices cannot obtain IP addresses, potentially causing network connectivity issues.

b. **IP Address Conflicts:** In some cases, IP address conflicts can occur if a device manually configures an IP address that DHCP later assigns to another device.

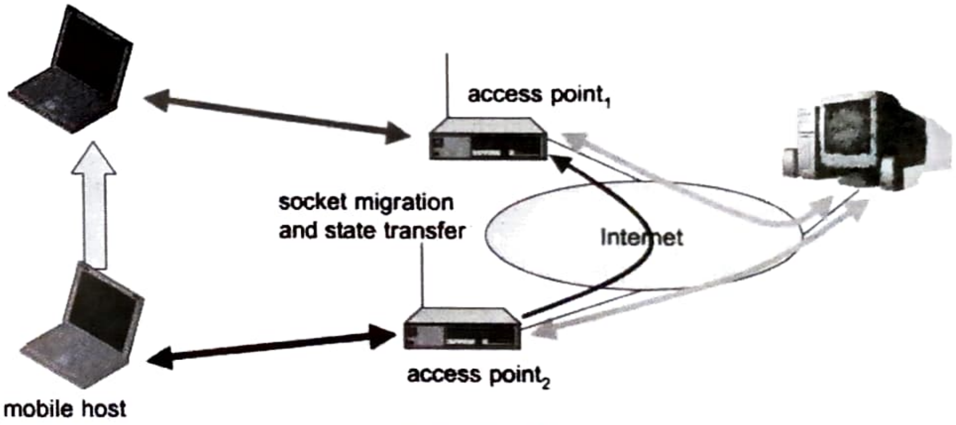
c. **Lease Management:** Administrators need to manage lease durations effectively to ensure IP addresses are renewed or released as needed.

By using DHCP in a mobile network, mobile devices can automatically obtain the necessary network configurations, including IP addresses, as they move between different access points or locations. This dynamic IP address allocation process enables seamless mobility and uninterrupted communication for mobile devices within the network. DHCP simplifies network management and enhances the user experience by removing the need for manual configuration of IP addresses and network settings on mobile devices.

4.5 INDIRECT TCP, SNOOPING TCP AND MOBILE TCP

Indirect TCP, Snooping TCP, and Mobile TCP are all variants of the traditional Transmission Control Protocol (TCP) designed to address specific challenges in mobile or wireless networks. Each of these protocols aims to improve the performance and efficiency of TCP communication in their respective scenarios.

1. Indirect TCP



INDIRECT TCP

Indirect TCP, also known as I-TCP, is a TCP variant designed to optimize TCP communication in multi-hop wireless networks. In multi-hop wireless networks, data packets may traverse multiple intermediate nodes before reaching the destination. This situation can lead to increased packet loss, delays, and reduced throughput due to the effects of wireless fading, interference, and contention.

To mitigate these issues, Indirect TCP introduces a store-and-forward mechanism at intermediate nodes. Instead of directly forwarding received TCP segments, intermediate nodes buffer the segments and then retransmit them to the next hop, allowing for more efficient error recovery. This mechanism reduces the number of end-to-end retransmissions and improves the overall reliability and performance of TCP in multi-hop wireless scenarios.

Working of Indirect TCP (I-TCP)

The working of Indirect TCP (I-TCP) involves the introduction of a store-and-forward mechanism at intermediate nodes in a multi-hop wireless network. This mechanism allows for more efficient error recovery and reduced retransmissions, improving TCP performance in such challenging network environments. Let's walk through the steps involved in the working of Indirect TCP:

a. **Node Initialization:** In a multi-hop wireless network, multiple nodes (e.g., routers) act as intermediate hops between the sender and receiver of TCP data. These nodes are responsible for forwarding TCP segments towards the destination.

b. **TCP Segment Transmission:** When a sender (source node) wishes to transmit data to the receiver (destination node), it divides the data into smaller units known as TCP segments. Each segment is assigned a sequence number to facilitate reordering and reassembly at the receiver.

c. **Intermediate Node Buffering:** Unlike traditional TCP, where intermediate nodes immediately forward received segments, in Indirect TCP, these intermediate nodes buffer the incoming TCP segments before forwarding them. The buffering allows the nodes to hold the segments temporarily and wait for possible packet loss or errors to be repaired.

d. **Selective Retransmissions:** When an intermediate node detects errors or packet loss in a buffered segment, it can request retransmission of only those specific segments that experienced errors or were lost. This is in contrast to traditional TCP, where both the sender and receiver may independently trigger retransmissions.

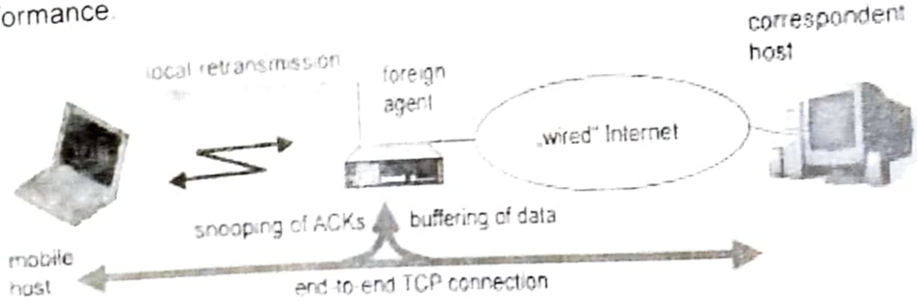
e. **Feedback Mechanisms:** Indirect TCP employs feedback mechanisms to communicate between intermediate nodes and the sender. For example, the intermediate node can acknowledge the receipt of segments and request retransmissions when necessary. This feedback helps improve the reliability of the communication.

f. **Efficient Error Recovery:** With the selective retransmission and feedback mechanisms, Indirect TCP can efficiently recover from errors and lost segments without requiring immediate end-to-end retransmissions. This approach reduces network congestion and ensures a more efficient utilization of available network resources.

g. **Final Delivery:** As the TCP segments traverse through the intermediate nodes, the destination node (receiver) performs reassembly to reconstruct the original data. The segments are then delivered to the application layer of the receiving device.

2. **Snooping TCP**

Snooping TCP, also known as S-TCP, is a TCP enhancement developed to optimize TCP performance in wireless LAN environments. In wireless LANs, nodes can overhear transmissions not intended for them due to the broadcast nature of wireless communication. Snooping TCP leverages this characteristic to improve TCP performance.



SNOOPING TCP

In a Snooping TCP environment, access points or wireless nodes "snoop" on the wireless medium to capture packets transmitted between other devices. When an access point detects a TCP acknowledgement (ACK) packet sent from a receiving node to the sender, it immediately responds with an ACK acknowledgment of its own, even if it didn't receive the original data packet. This behavior reduces the round-trip time for TCP ACKs, effectively reducing the latency of TCP communication and improving its throughput in wireless LANs.

orking of Snooping TCP (S-TCP)

Snooping TCP (S-TCP) is a variant of the traditional Transmission Control Protocol (TCP) designed optimize TCP performance in wireless local area networks (LANs). In wireless LANs, nodes can overhear ansmissions not intended for them due to the broadcast nature of wireless communication. Snooping CP leverages this characteristic to improve TCP performance.

Here's how Snooping TCP works:

a. **Snooping Behavior:** In a wireless LAN environment, access points or wireless nodes can "snoop" on the wireless medium to capture packets transmitted between other devices. When an access point detects a TCP acknowledgement (ACK) packet sent from a receiving node to the sender, it immediately responds with an ACK acknowledgment of its own, even if it didn't receive the original data packet.

b. **ACK Spoofing:** This behavior is known as "ACK spoofing" or "ACK sneaking." By spoofing the ACKs, the access point fools the sender into believing that the data packets have been successfully received by the intended receiver. This helps to reduce the round-trip time for TCP ACKs, effectively reducing the latency of TCP communication in wireless LANs.

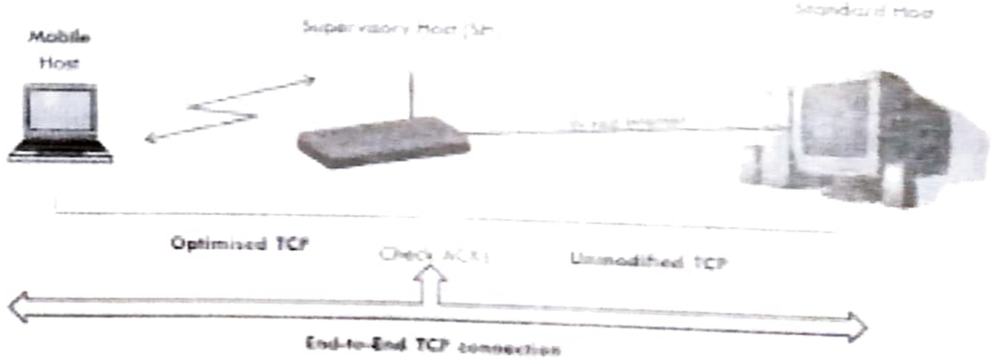
c. **Faster Retransmissions:** In traditional TCP, the sender waits for an acknowledgment (ACK) from the receiver before retransmitting any unacknowledged packets. In wireless LANs with higher latencies and potential packet loss, this process can lead to delays in retransmission and negatively impact TCP throughput.

d. **Immediate Feedback:** With Snooping TCP, the sender receives immediate feedback (ACK) from the access point, indicating that the data packets were successfully forwarded to the receiver, even if the receiver itself hasn't sent an ACK yet. As a result, the sender can initiate retransmissions more quickly in case of packet loss, reducing the time spent waiting for the ACK from the actual receiver.

e. **Improved TCP Performance:** By reducing the round-trip time for ACKs and enabling faster retransmissions, Snooping TCP can significantly improve TCP performance in wireless LANs. It leads to reduced latency, better throughput, and improved overall efficiency of TCP communication in wireless environments.

. Mobile TCP

Mobile TCP, also known as M-TCP, is a TCP enhancement designed to handle the challenges of obile networks, particularly frequent handovers between different wireless access points or networks. n mobile networks, when a mobile device moves from one cell to another, it may experience interruptions r delays in TCP communication due to changes in network conditions.



MOBILE TCP

Mobile TCP addresses this issue by implementing a host-based mobility management mechanism. When a mobile device moves to a new network, Mobile TCP uses fast retransmit and fast recovery mechanisms to reduce the impact of packet loss during the handover. It avoids triggering unnecessary time-out and retransmission delays, thereby maintaining TCP connection continuity and reducing latency in the presence of mobility events.

Mobile TCP (M-TCP) is a variant of the traditional Transmission Control Protocol (TCP) designed to address the challenges of TCP performance in mobile networks. In mobile networks, mobile devices, such as smartphones and tablets, frequently move between different networks or access points, leading to changing network conditions and disruptions in TCP communication.

The primary goal of Mobile TCP is to ensure seamless TCP communication for mobile devices during handovers and movements between different networks. It achieves this by implementing host-based mobility management mechanisms that minimize the impact of mobility events on TCP connections. Mobile TCP focuses on reducing latency, improving data delivery, and maintaining TCP connection continuity during handovers.

Here's how Mobile TCP works:

a. **Handover Detection:** When a mobile device moves from one network to another or switches between different access points, it detects the handover event. Handover detection may be initiated by the mobile device itself or by network entities monitoring the device's movements.

b. **Fast Retransmit and Fast Recovery:** During a handover, Mobile TCP employs fast retransmit and fast recovery mechanisms to avoid unnecessary time-outs and retransmissions. Instead of waiting for the standard TCP retransmission timer to trigger, Mobile TCP quickly retransmits lost packets based on the detection of multiple duplicate acknowledgments (ACKs). This reduces the latency in recovering from packet loss during handovers.

c. **Mobility Support in the Network:** To support seamless mobility, Mobile TCP requires cooperation from the network infrastructure. Network entities, such as routers or access points, may assist in buffering and forwarding packets during handovers. Additionally, mechanisms like "triangular routing" may be employed to ensure packets are routed to the mobile device's new location efficiently.

d. **Optimization for Wireless Networks:** Mobile TCP takes into account the unique characteristics of wireless networks, such as higher error rates, variable signal strengths, and changes in network topology. It adapts its behavior to minimize the impact of these wireless-specific challenges on TCP performance.

e. **Host-Centric Approach:** Mobile TCP follows a host-centric approach, meaning that the mobile device itself takes more responsibility for handling mobility events and optimizing TCP performance during handovers. This approach allows for greater flexibility and adaptability based on the device's mobility patterns.

f. **Connection Continuity:** By employing the fast retransmit and fast recovery mechanisms, Mobile TCP ensures that TCP connections remain continuous and uninterrupted during handovers. This ensures that applications relying on TCP communication, such as web browsing, email, and real-time communication, can seamlessly function as the device moves between different networks.

4.6 TCP OVER 3.0G MOBILE

TCP (Transmission Control Protocol) over 3G mobile networks works similarly to TCP over other types of networks but with considerations for the characteristics and challenges specific to 3G mobile networks. 3G (Third Generation) mobile networks provide higher data transfer rates and enable services like mobile internet browsing, video streaming, and multimedia applications. However, they also have limitations that can affect TCP performance.

Here are some key considerations for TCP over 3G mobile networks:

a. **Latency:** 3G networks generally have higher latency compared to wired networks, such as Wi-Fi or Ethernet. Latency refers to the time it takes for a data packet to travel from the source to the destination. Higher latency can lead to delays in establishing connections and longer round-trip times for data exchange, impacting TCP performance.

b. **Packet Loss:** 3G networks may experience higher packet loss due to factors like wireless signal fluctuations, interference, and handovers between different cell towers. TCP interprets packet loss as network congestion and reduces its sending rate, which may unnecessarily slow down the data transfer.

c. **Bandwidth Fluctuations:** The available bandwidth in 3G networks can vary depending on factors like network congestion and signal strength. TCP's congestion control algorithms may interpret these fluctuations as network congestion, leading to suboptimal throughput.

d. **Mobility:** Mobile devices in 3G networks are often in motion, causing frequent handovers between different base stations. TCP connections can be disrupted during handovers, leading to retransmissions and increased latency if not managed properly.

To address these challenges, various TCP enhancements and optimizations have been proposed and implemented for 3G networks. Some of the techniques include:

a. **Buffering:** Buffering of TCP segments at the intermediate network nodes can help mitigate the impact of latency and packet loss, improving TCP performance.

b. **Fast Retransmit and Fast Recovery:** These mechanisms help TCP quickly recover from packet loss without waiting for retransmission timers, reducing latency during packet recovery.

c. **Mobile TCP (M-TCP):** As mentioned earlier, Mobile TCP is a TCP variant designed specifically for mobile networks. It employs host-based mobility management mechanisms to handle handovers more efficiently and maintain TCP connection continuity during movements between different networks.

d. **TCP ACK Manipulation:** Some TCP optimizations involve modifying ACK behavior to provide faster feedback to the sender, reducing round-trip times and enhancing TCP performance.

Overall, TCP over 3G mobile networks aims to strike a balance between reliable data transfer and adaptability to the dynamic network conditions. TCP enhancements and mobile-specific optimizations help improve performance and user experience in 3G mobile environments, enabling smooth communication and data transfer for mobile applications.

QUESTION BANK

■ Multiple Choice Questions (MCQs):

1. ___________ is an Internet Engineering Task Force standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address.

   (a) Mobile ip (b) MAC (c) SMTP (d) POP

2. Elaborate the following terms:

   (a) MN (b) HA (c) CoA (d) CN.

   (e) DHCP.

3. Define Handover Management.

4. Define Packet Delivery.

ANSWERS

1. (a) Mobile ip

■ Short Questions:

1. Enlist the terminology required in mobile computing.
2. Define mobile ip and explain its uses.
3. What are the goals of mobile ip.
4. Explain the use of DHCP protocol.

■ Long Questions:

1. Explain mobile ip in brief.
2. Explain steps of packet delivery in mobile ip.
3. Explain Handover management in mobile ip.
4. Explain Location management in mobile ip.
5. Explain Registration, tunneling and encapsulation in mobile ip.
6. Explain DHCP with its working with the help of a neat diagram and also explain its advantages.
7. Enlist different types of TCP and explain each of them in brief.
8. Why TCP is used over 3G networks?

■ * ■