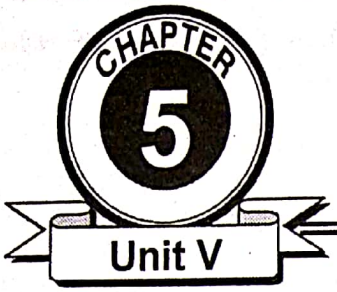

Mobility Management

Syllabus

5.1 Mobility Management : Introduction, IP Mobility, Optimization, IPv6

5.2 Macro Mobility : MIPv6, FMIPv6,

5.3 Micro Mobility : CellularIP, HAWAII, HMIPv6,

Introduction

IP Mobility is a mechanism that allows mobile device to move from one network to another network without changing its permanent IP address. This chapter discusses various protocols to support IP Mobility. **Mobile IP** was the first communication protocol developed by IETF to support IP mobility with the current version of IPV4. Later **Mobile IPV6 (MIPV6)** was developed as an update to IPV6 protocols to supports IP mobility. IPV6 header has some new features and options that supports IP mobility. The chapter also discusses various Micro mobility mechanisms to support fast and seamless handover while mobile device is changing its network or point of attachment.

5.1 Introduction to IP Mobility

- **IP mobility** refers to the set of mechanisms that allow an **IP** mobile node to move freely between different **IP** networks while maintaining **IP** connectivity in a transparent way.
- Current versions of the Internet Protocol (IPV4) assume that the point at which a computer attaches to the Internet or a network is fixed and its IP address identifies the network to which it is attached.
- Packets are sent to a mobile device based on the location information contained in the IP address.
- If a mobile device, or **mobile node**, moves to a new network while keeping its IP address unchanged, its address does not reflect the new point of attachment.
- Consequently, existing routing protocols cannot route packets to the mobile node correctly.
- In this situation, we must reconfigure the mobile node with a new IP address representing its new location. Thus, under the current Internet Protocol (IPV4) , if the mobile node moves without changing its address, it loses routing; and if it does change its address, it loses connections.
- One of the most desirable features of **IP mobility** mechanisms is the ability of maintaining connectivity without interrupting ongoing communications.

5.1.1 Mobile IP

- **Mobile IP** (or MIP) is an IETF 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 an enhancement of the internet protocol (IP) that adds mechanisms for forwarding internet traffic to mobile devices when they are connecting through other than their home network. Fig. 5.1.1 shows generic Mobile IP topology.

- Every host will have a "Home Address (Permanent IP)" within a "Home Network". A home network has a "Home Agent" that provides several services for the mobile node
- Traffic destined to the "Home Address" of mobile node (MN) will always be routed to the "Home Agent."
- If the mobile node is in its "Home Network", traffic will be forwarded directly the mobile node.
- If the mobile node has moved to some other network called "Foreign Network", traffic will be IP tunneled by the "Home Agent" to a "Care-of- Address". The Care- of- address defines the current location of the mobile node.
- Every Foreign network has 'Foreign agent (FA) '. The foreign agent can provide several services to the mobile node during its visit to the foreign network. The FA can have the COA (care or address) acting as a tunnel endpoint when forwarding packets to the MN.

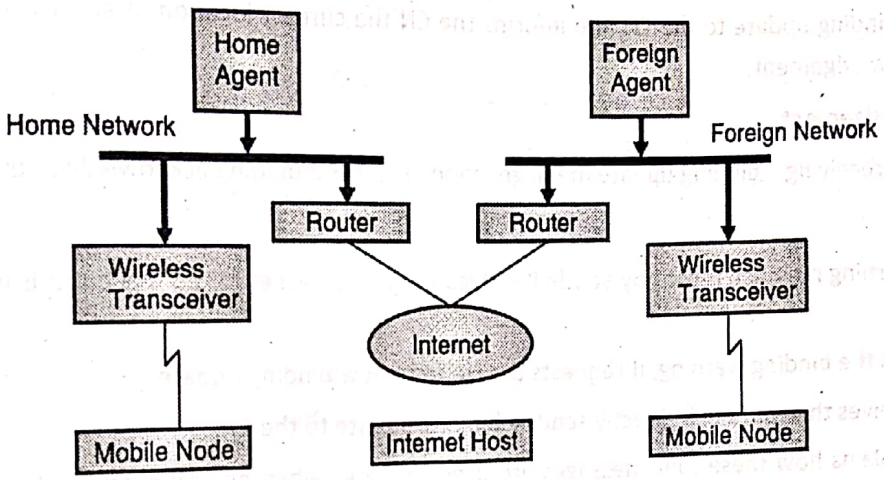

Fig. 5.1.1 : Mobile IP topology

5.1.2 Optimization

Triangular routing

- With Mobile IPv4 there is always a triangular traffic pattern. As shown in Fig. 5.1.2 the IP packet from a CN (Correspondent Node) destined to an MN needs to be routed to its HA first and then tunneled to the foreign agent of the MN.
- If the Corresponding Node (CN)and MN are very near, then also the IP packet has to travel a long way to reach the MN. This in efficient behavior of a non optimized mobile IP is called ***Triangular Routing***.
- The triangle is made of the three segments : CN to HA, HA to COA/MN and MN back to CN.

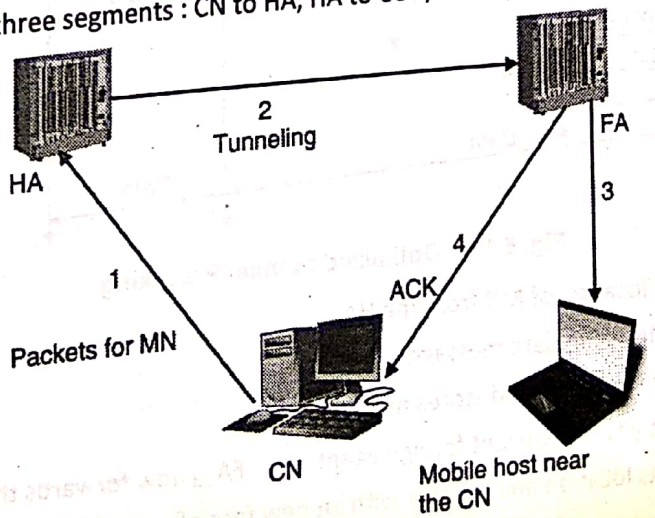

Fig. 5.1.2 : Triangular Routing

Route optimization to avoid triangular routing

To solve triangular routing problem, a route optimization protocol has been introduced. Basically this protocol defines some messages as to inform CN of an upto date location of MN. Once the current location of the MN is known, the CN itself performs tunneling and sends packet directly to MN.

The optimized mobile IP protocol needs four additional messages; these are :

1. **Binding request**

   If a node wants to know where the MN is currently located, it can send a binding request to the HA.

2. **Binding update**

   The HA sends a binding update to the CN and informs the CN the current location of an MN. The binding update can request an acknowledgement.

3. **Binding acknowledgement**

   On request, after receiving a binding update message, anode returns a binding acknowledgement.

4. **Binding warnings**

   - A binding warning message is sent by anode if it decapsulates a packet for an MN but it is not the FA for that MN currently.
   - If CN receives the binding warning, it requests the HA for a new binding update.
   - If the HA receives the warning it directly sends a binding update to the CN.
   - Fig. 5.1.3 explains how these four messages are used together when an MN changes its FA and also shows the exchange of messages in optimization protocol.

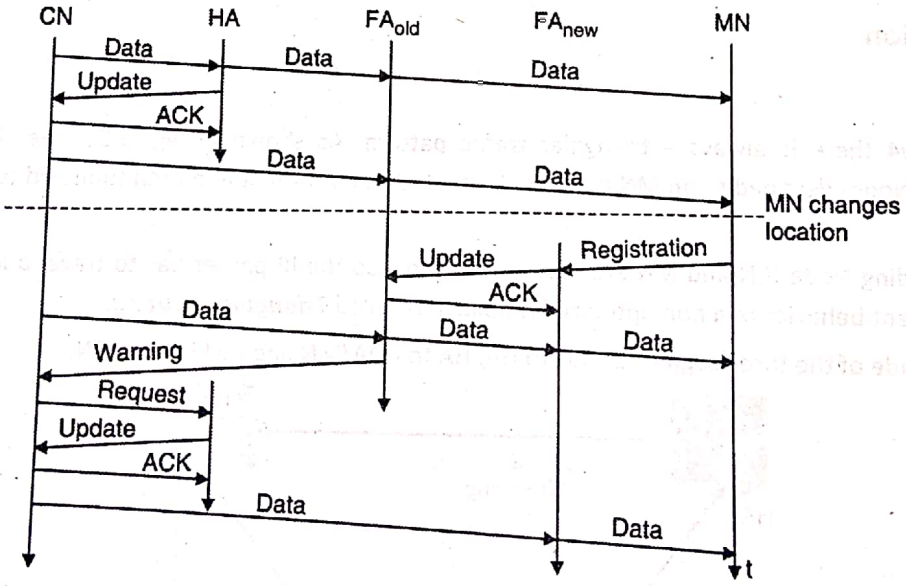

Fig. 5.1.3 : Optimized mobile IP working

- The CN requests the current location of MN from the HA.
- HA returns the COA of the MN via update message.
- CN acknowledge this updated message and stores mobility binding.
- Now CN can send data directly to the current foreign agent FA_{old}. FA_{old} now forwards these data to MN.
- The MN might now change its location and register with an new foreign agent FA_{new}.
- FA_{new} informs FA_{old} about new registration of MN via an update message and FA_{old} acknowledged this update message.

- CN doesn't know about the current location of MN, its till tunnels its packets for MN to the old foreign agent FA_{old}.
- The FA_{old} notices packets destined to MN but also knows MN currently not in current FA.
- FA_{old} might now forward these se packets to the new COA of MN which is new foreign agent.
- Thus the packets that are in transit are not lost. This behavior is another optimization to basic mobile IP and provides smooth handover.
- FA_{old} sends binding warning message to CN. CN then requests a binding update.
- The HA sends an update to inform the CN about the new location, which is acknowledged. Now CN cans end data directly to FA_{new}, and avoid triangular binding.
- However, the optimization will not work if the MN does not want to reveal its current location to the CN because of security.

5.2 IPv6 – Internet Protocol Version 6

- To overcome these problems, IPv6 also known as **IPng** (Internet Protocol next generation) was proposed. In IPv6, the Internet protocol was extensively modified to accommodate the growth and new demands of the Internet. The format and the length of the IP addreses were changed along with the packet format.
- Related protocols such as ICMP were also modified. Other protocols in the network layer, such as ARP, RARP, IGMP were either deleted or included in ICMPv6 protocol. Routing protocols such as RIP and OSPF were slightly modified to accommodate these changes. The fast spreading use of Internet and new services such as mobile IP, IP telephony, and IP-capable mobile telephony, may require the total replacement of IPv4 by IPv6.

Advantages of IPv6

1. **Larger address space :** An IPv6 address is 128 bit long. Compared with the 32 bit long IPv4 address, this is huge increase in address space.
2. **Better Header format :** IPv6 uses a new header format in which options are separated from the base header and inserted when needed, between the base header and the upper layer data. This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.
3. **New Options :** IPv6 has new options to allow for additional functionalities.
4. **Allowance for extension :** IPv6 is designed to allow the extension of protocol if required by new technologies or applications.
5. **Support for resource allocation :** In IPv6, the ***type-of-service*** field has been removed, but mechanism called ***Flow label*** has been added to enable the source to request special handling of packet. This mechanism can be used to support traffic such as real-time audio and video.
6. **Support for more security :** The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

Features of Ipv6 to support mobility

- No special mechanisms are needed for securing mobile IP registration. In every Ipv6 node **address auto configuration** i.e. the mechanism for acquiring a COA is inbuilt.
- **Neighbor discovery** mechanism is also mandatory for every Ipv6 node. So special foreign agents are no longer needed to advertise services.
- Combining the features of address auto configuration and neighbor discovery enables every Ipv6 mobile node to create and obtain a topologically correct address or the current point of attachment.
- Every Ipv6 node can send binding updates to another node, so the MN can send its COA directly to the CN and HA. The FA is no longer needed. The CN processes the binding updates and makes corresponding entries in its routing cache.

- The MN is now able to decapsulates the packets
  - To detect when it needs a new COA and
  - To determine when to send binding updates to the HA and CN
- A **soft handover** is possible with Ipv6. The MN sends its new COA to the old router serving the MN at the old COA, and the old router can encapsulate all incoming packets for the MN and forwards them to new COA.

Limitation of Ipv6

It does not solve any firewall or privacy problems. Additional mechanisms on higher layers are needed for this.

Ipv6 Header

Fig. 5.2.1 shows both Ipv4 and Ipv6 header format.

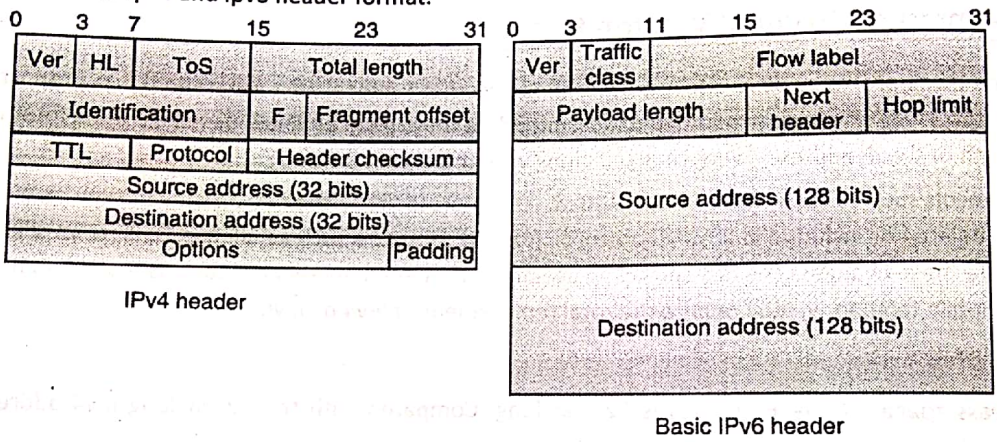

Fig. 5.2.1 : Comparison of Ipv4 and Ipv6 Header format

Fields of Ipv6 header :

1. **Version :** 4 bits - IPv6 version number.
2. **Traffic Class :** 8 bits - Used to specify different classes or priorities of IPv6 packets.
3. **Flow Label :** 20 bits - Used for specifying special router handling from source to destination(s) for a sequence of packets. It distinguish the different types of packets such as audio, video, txt etc. and accordingly provides quality of services to them.
4. **Payload Length :** 16 bits unsigned - Specifies the length of the data in the packet.
5. **Next Header :** 8 bits - Specifies the next encapsulated protocol. The values are compatible with those specified for the IPv4 protocol field.
6. **Hop Limit :** 8 bits unsigned - For each router that forwards the packet, the hop limit is decremented by 1. When the hop limit field reaches zero, the packet is discarded. This replaces the TTL field in the IPv4 header that was originally intended to be used as a time based hop limit.
7. **Source address :** 16 bytes - The IPv6 address of the sending node.
8. **Destination address :** 16 bytes - The IPv6 address of the destination node.

5.3 Macro Mobility

5.3.1 MIPv6 (Mobile IPv6)

- The first IP Mobility protocol, **Mobile IP** (discussed in Section 5.1.1) was developed for **IPv4**. The Mobile IP protocol solves the TCP/IP Layer 3 mobility problem, by assigning a permanent IP address to the mobile node.

- Mobile IP supports of both MIPv4 and MIPv6, but IPv4 has a couple of drawbacks. The main drawback of IPV4 is address exhaustion, making MIPv6 the future option for mobility protocol in IP Networks.
- **Mobile IPv6** (MIPv6) is a protocol developed as a subset of IPv6 to support mobility.
- MIPv6 is an update of the Mobile IP standard designed to authenticate mobile devices using IPv6 addresses.
- In traditional IP routing, IP addresses represent a topology. Routing mechanisms rely on the assumption that each network node will always have the same point of attachment to the Internet, and that each node's IP address identifies the network link where it is connected.
- In this routing scheme, if you disconnect a mobile device from the Internet and want to reconnect through a different network, you have to configure the device with a new IP address, and the appropriate netmask and default router.
- Otherwise, routing protocols have no means of delivering packets, because the device's network address doesn't contain the necessary information about the node's network point of attachment to the Internet.
- Mobile IPv6 allows a mobile node to transparently maintain connections while moving from one subnet to another.
- Each device is identified by its home address although it may be connecting to through another network. When connecting through a foreign network, a mobile device sends its location information to a home agent, which intercepts packets intended for the device and tunnels them to the current location.

5.3.2 FMIPv6 (Fast Hand Over for Mobile IPV6)

- Mobile IPv6 (MIPv6) enables a Mobile Node (MN) to maintain its connectivity to the Internet when moving from one Access point to another. This process is referred to as **'handover'**.
- During handover, there is a period during which the Mobile Node is unable to send or receive packets. This period is called **'Hand over latency'**.
- Hand over latency results from the standards handover procedure such as movement detection, new Care of address configuration, binding updates etc.
- This Hand over latency is often unacceptable to real-time traffic such as Voice over IP (VoIP).
- The fast handover for mobile IPv6 (FMIPv6) aims at reducing the long handover latency in mobile IPv6 by fast movement detection and fast binding update.
- It uses anticipation based on layer 2 trigger information of the mobile node (MN) to obtain a new care-of address at the new link while still connected to the previous link, thus reducing handover delay.
- Furthermore, it also reduces packet loss by buffering before the real link layer handover takes place.

5.4 Micro Mobility

- Mobile IP represents a simple and scalable global mobility solution but lacks the support for fast handoff control and paging.
- Imagine a large number of mobile devices changing networks quite frequently ; a high load on the home agents as well as on the networks is generated by registration and binding update messages.
- IP micro-mobility protocols can complement mobile IP by offering fast and almost seamless handover control in limited geographical areas.
- The basic underlying idea is the same for all micro-mobility protocols: Keep the frequent updates generated by local changes of the points of attachment away from the home network and only inform the home agent about major changes, i.e., changes of a region.
- In some sense all micro-mobility protocols establish a hierarchy.
- The following section presents three of the most commonly used approaches.

5.4.1 Cellular IP

Why Cellular IP ?

- Mobile IP exhibits several problems when there is a large number of mobile devices changing network frequently and moving very fast. In such cases, a high load on home agents and on the network is generated by registration and binding update messages.
- Mobile IP is basically designed only for **macro level mobility** and relatively **slow moving hosts.**
- Cellular IP (CIP) is a new robust, simple, and flexible protocol for highly mobile hosts.
- CIP complements Mobile IP by supporting **local mobility.**
- It can accommodate large number of users by separating **idle hosts** from **active hosts.**

CIP architecture

The architecture of Cellular IP is shown in Fig. 5.4.1. It consists of three major components.

- Cellular IP gateway (GW),
- Cellular IP node or the base station (BS)
- Cellular IP mobile host (MH)

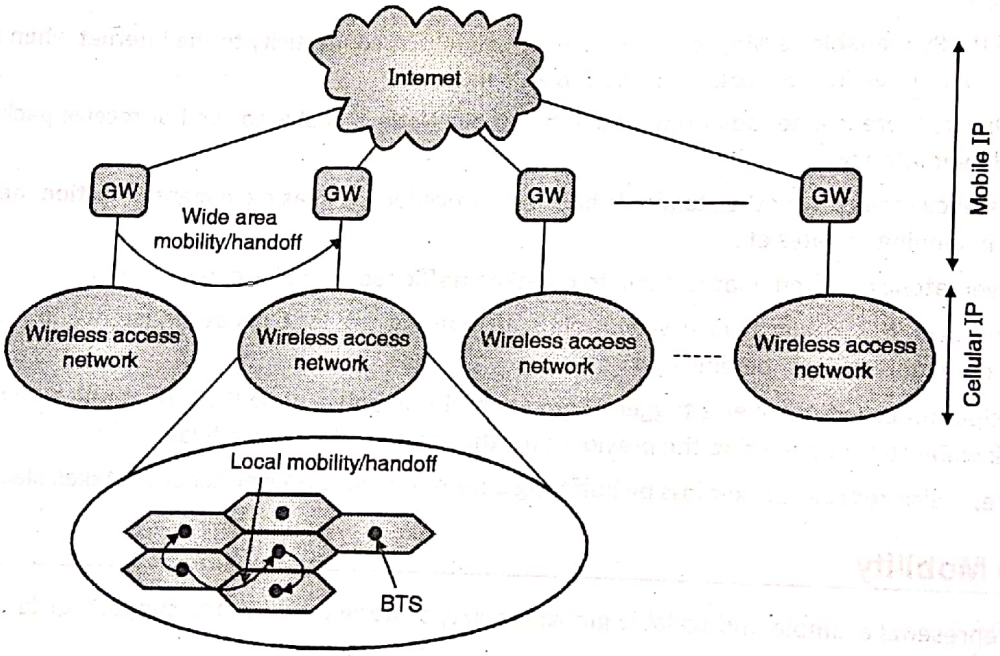

Fig. 5.4.1 : Cellular IP access network (architecture)

- An important component of a Cellular IP network is the **base station (BS)**. A cellular IP network consists of several interconnected BSs.
- The BSs communicate with mobile hosts (MHs) via wireless interface and also route IP packets inside the cellular network. The base stations are built on regular IP forwarding engines, but IP routing is now replaced by Cellular IP routing and cellular location management.
- ***CIP gateway router*** connects a cellular IP network and the regular Internet.
- Mobility between gateways is managed by Mobile IP while mobility within access networks is handled by Cellular IP.
- Now the IP address of gateway serves as the care-of-address for all mobile hosts that are currently attached to the network.

Routing in CIP

- **Uplink packets** (packets originated from mobile host) are routed from mobile host to the gateway on a hop-by-hop basis.
- The path taken by these packets is cached in base stations. This cache is called **routing cache.**
- To route **downlink packets** addressed to a mobile host the path used by recent packets transmitted by the host (that are already stored in route cache) is reversed.
- A mobile host may wants to maintain its routing cache mappings even though it is not regularly transmitting data packets.
- Such mobile hosts transmit route-update packets at regular interval to keep their routing cache mappings valid. These packets are empty data packets addressed to the gateway.

Paging in CIP

- In Cellular IP, an **idle mobile host** is one that has not received data packets for a system specific time.
- For such idle hosts, their downlink soft state routes timeout and are removed from the routing cache.
- These hosts transmit **paging-update** packets at regular intervals. The paging update packet is an empty IP packet addressed to the gateway. It is distinguished from route update packet by its IP type parameter.
- Similar to data and route update packets, paging update packets are routed on a hop-by-hop basis to the gateway. Base stations may optionally maintain paging cache.
- Thus all idle mobile hosts have mappings in paging caches but not in routing caches.
- In addition, active mobile hosts will have mappings in both routing as well as paging cache.
- Packets addressed to a mobile host are normally routed by routing cache mappings. Paging occurs when a packet is addressed to an idle mobile host and the gateway or base stations find no valid routing cache mapping for the destination.
- The paging cache is used to avoid broadcast search procedures found in cellular systems.
- If there is no entry in the paging cache, then the packet addressed to an idle mobile host is broadcast in the access network. This may happen when transmitting first packet to the any host.
- Idle mobile hosts that receive a packet, move from idle to active state and immediately transmit a route-update packet.

Handover in CIP

- CIP implements MCHO (Mobile controlled handover) thus, in CIP, handoff is initiated by Mobile Host (MH).
- MH listens to the beacon transmitted by BSs and initiates handover based on signal strength measurements.
- To perform a handoff, an MH tunes its radio to the new BS. It then sends a route update packet to this new BS.
- This creates entry in a routing cache on route to the gateway, thus, configuring the downlink route to the new BS.
- During the handoff process time, downlink packets may be lost. The mappings associated with the old base station are not cleared at handover, rather, they timeout as the associated soft-state timers expire.
- The mappings associated with the old BS are cleared after the expiry of a timer.
- Before the timeout, both the old and new downlink routes remain valid and packets are delivered through both the BSs. Thus, Cellular IP uses semisoft handover to improve handoff performance.

Advantages of CIP

1. Provides easy Global migration
2. Cheap Passive Connectivity

3. Efficient Location Management
4. Flexible Handoff
5. Simple Memory less Mobile hosts

5.4.2 HAWAII

HAWAII (Handoff-Aware Wireless Access Internet Infrastructure) tries to keep micro-mobility support as transparent as possible for both home agent and MN.

Working

Step 1 : On entering an HAWAII domain, a mobile node obtains a co-located COA.

Step 2 : MN registers with the HA.

Step 3 : When MN moving another cell inside the foreign domain, the MN sends a registration request to the new base station as to a foreign agent.

Step 4 : The base station interprets the registration request and sends out a handoff update message, which reconfigures all routers on the paths from the old and new base station to the crossover router. When the routing has been reconfigure successfully, the base station sends a registration reply to the MN, again as if it were a foreign agent.

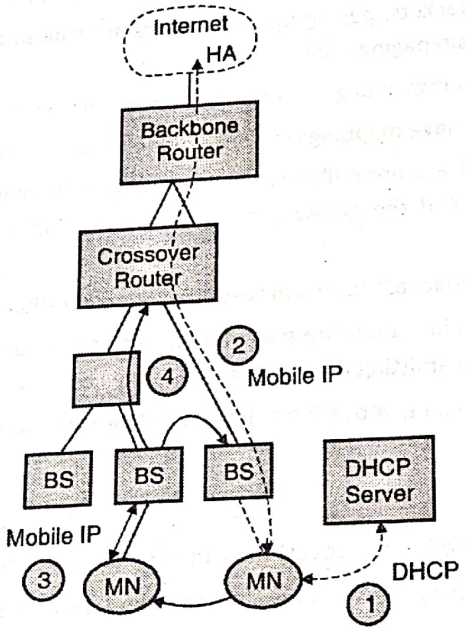

Fig. 5.4.2 : Basic architecture of HAWAII

Advantages

1. **Security :** Challenge response extensions are mandatory. In contrast to cellular IP, routing changes are always initiated by the foreign domain's infrastructure.
2. **Transparency :** HAWAII is mostly transparent to mobile nodes.

Disadvantages

- Co-located COA raises DHCP security issues(DHCP has no strong authentication).
- Decentralized security-critical functionality(Mobile IP registration processing during handover)in base stations.
- Authentication of HAWAII protocol messages unspecified (potential attackers: stationary nodes in foreign network).

- MN authentication requires PKI or AAA infrastructure.
- There are no provisions regarding the setup of IPsec tunnels.
- No private address support is possible because of co-located COAs.

5.4.3 HMIPv6 – Hierarchical Mobile IPv6

- Hierarchical Mobile IPV6 (HMIPv6) provides micro-mobility support by installing a **mobility anchor point (MAP).** MAP is an entity which is responsible for a certain domain and acts as a local HA within this domain for visiting MNs.
- Fig. 5.4.3 shows basic architecture of Hierarchical Mobile IP.
- The MAP receives all packets on behalf of the MN, encapsulates and forwards them directly to the MN's current address **LCOA** (Link COA).

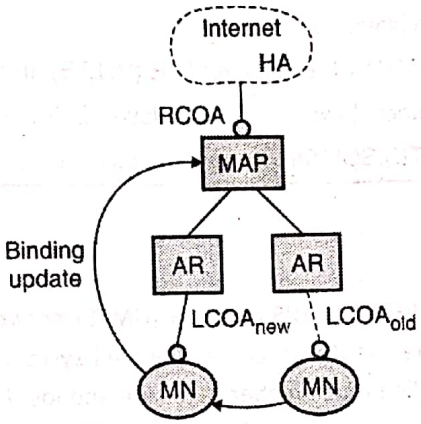

Fig. 5.4.3 : Basic architecture of hierarchical mobile IP

Advantages

1. **Security :** MNs can have (limited) location privacy because LCOAs can be hidden.
2. **Efficiency :** Direct routing between CNs sharing the same link is possible

Disadvantages

1. **Transparency :** Additional infrastructure component (MAP).
2. **Security :** Routing tables are changed based on messages sent by mobile nodes. This requires strong authentication and protection against denial of service attacks. Additional security functions might be necessary in MAPs

Review Questions

Q. 1 What is a need of Micro Mobility? Explain HAWAII in details.

Q. 2 Draw a neat sketch of IPv6 header. Compare IPv4 and IPv6 with respect to IP mobility.

Q. 3 What advantages IPv6 offer over IPv4.

Q. 4 Explain MIPv6 and FMIPv6 for Micro mobility.

Q. 5 What is Cellular IP. Explain CIP architecture along with routing and paging procedure in CIP.

Q. 6 What are the problems with standard Mobile IP protocol? Explain how MIPv6 overcome these problems.

❑❑❑