# Indirect Routing of Mobile IP: A Non-Encapsulation Approach

**Basil M. Al-Kasasbeh, Rafa E. Al-Qutaish and Khalid T. Al-Sarayreh**

Faculty of Information Technology, Applied Science University, Amman 11931, Jordan

**Summary**
Currently, when using the mobile IP indirect routing technique, it explicitly includes the encapsulation (such encapsulation is also called tunneling) approach. However, it is uncommon to use the non-encapsulation approach with the mobile IP indirect routing technique. In this paper, we propose a new approach in which we use the non-encapsulation approach to the indirect routing. In this way, the delay and the speed of CoA registration and communication processes within the indirect routing will be positively affected. Moreover, this way will decrease the delay and increase the speed of transmission.

***Key words:***
*Mobile IP, Indirect Routing, Non-Encapsulation, Non-Tunneling, registration, Address Mapping.*

## 1. Introduction

Mobile IP is a standard protocol that builds on the Internet Protocol by making mobility transparent to applications and higher level protocols like TCP. Moreover, Mobile IP works with a permanent IP address while moving around.

This address appears for routing purposes to be local to the Home Agent router. As the Mobile Station moves, there are no changes of routes in corporate routing tables. Mobile IP can even work with Internet routing tables at a global scale. All it takes is protocol support, a Home Agent router, and one or more Foreign Agents to provide mobile access [1].

Foreign Agent routers work with the Mobile IP host to register new roaming locations with a Home Agent router. Advertisements from the Foreign Agent notify the Mobile Station of its presence as it roams.

The Mobile Station sends a Registration message to the Home Agent via the new Foreign Agent, letting the Home Agent know that message to it should be sent via a tunnel to the Care-of Address (CoA) [2 and 3].

Packets headed from a "Correspondent node" towards the mobile node get routed normally to the Home Agent router. The Home Agent router encapsulates (such encapsulation also called tunneling) these packets to the Foreign Agent router near the Mobile Station. The Foreign Agent router de-encapsulates the packets from the tunnel and transmits them to the connected mobile node (visitor). Return packets go from Mobile Station to Foreign Agent and then directly to Correspondent node, unless "reverse tunneling" is enabled. In order for all this to work, the Mobile Node needs to have a special Mobile IP stack that knows how to work with the Foreign Agent router, and also how to send registration messages to the Home Agent [4].

Basically, there is some MAC layer "cheating" on the subnet between Foreign Agent and Mobile Station. For outbound traffic, the Mobile Station dynamically sets the Foreign Agent as default gateway, and forwards traffic to it, even though they are not on the same subnet. For traffic going towards the Mobile Station, the Foreign Agent uses a host route and a local ARP entry to get traffic to the Mobile Station, even though its address may not be that of the local subnet [1], see Figure 1.

As commonly known, the encapsulation process itself will increase the transmission delay, and the process of encapsulation of the sending packet will enlarge its size, and then the speed of communication process will be decreased based on the enlarged size of the new packet sent from the home agent. In addition, the de-encapsulation process will need a time to return the new packet to its original structure in which this process will also increase the delay of the communication process.

In this paper, we propose a new approach in which we use the non-encapsulation approach to the indirect routing. In this way, the delay and the speed of transmission of the CoA registration and communication processes within the indirect routing will be positively affected. Moreover, this way will decrease the delay and increase the speed.

The rest of this paper is organized as follows: Section 2 gives a general overview about the indirect routing technique for Mobile IP. In section 3, we describe the details of the proposed approach. Section 4 illustrates an example of the proposed approach, and finally, section 5 concludes the paper.

Manuscript received July 5, 2008.
Manuscript revised July 20, 2008.

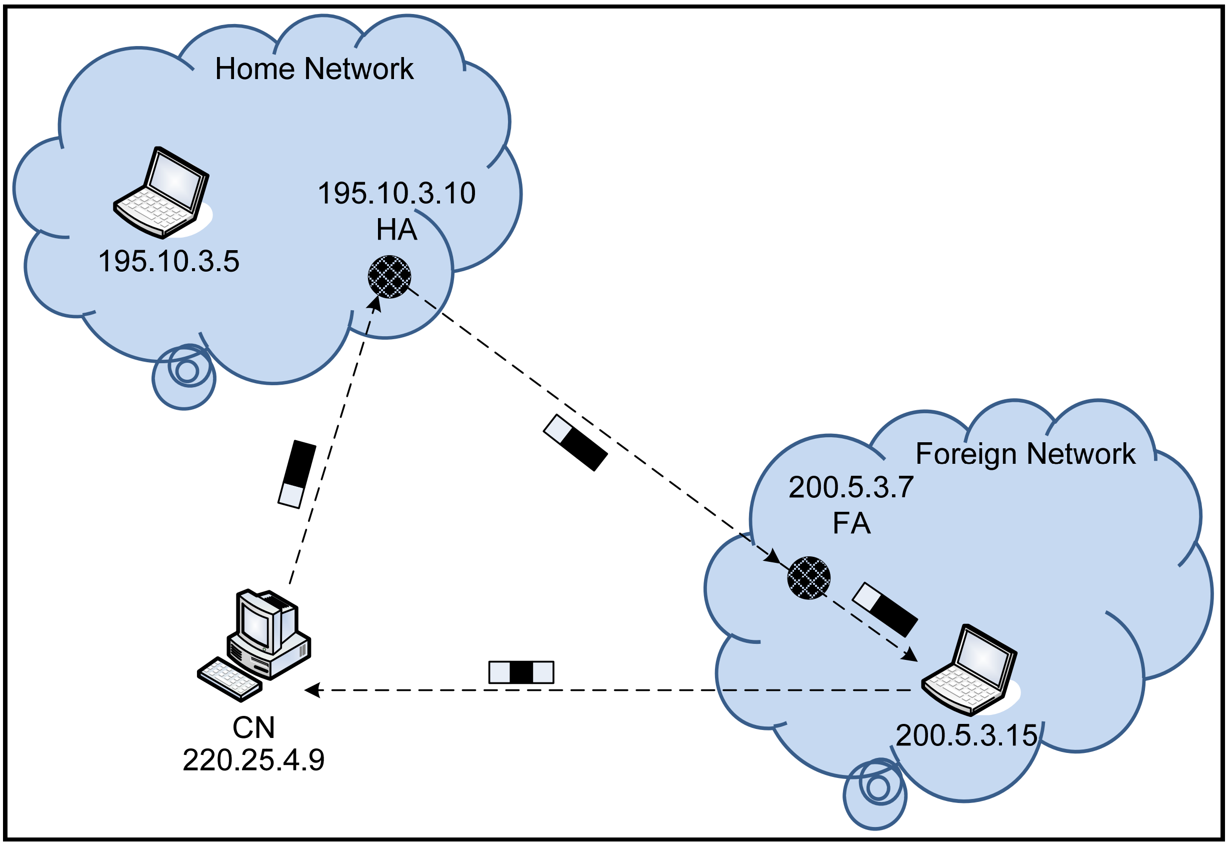


Fig. 1 Indirect Routing Scenario

## 2. Indirect Routing: General Overview

### 2.1 How Mobile IP Works using Indirect Routing Approach

IP routes packets from a source endpoint to a destination by allowing routers to forward packets from incoming network interfaces to outbound interfaces according to routing tables. The routing tables typically maintain the next-hop information for each destination IP address, according to the number of networks to which that IP address is connected. The network number is derived from the IP address by masking off some of the low-order bits. Thus, the IP address typically carries with it information that specifies the IP node's point of attachment. In Mobile IP the home agent redirects packets from the Home Network to the Care-of Address by constructing a new IP header that contains the Mobile Station's Care-of Address as the destination IP address. This new header then encapsulates the original packet, causing the Mobile Station's home address to have no effect on the encapsulated packet's routing until it arrives at the Care-of Address. Such encapsulation suggests that the packet burrows through the Internet, bypassing the usual effects of IP routing.

Mobile IP, then, is best understood as the cooperation of three separable mechanisms [1 and 3]:

- Discovering the Care-of Address (CoA),
- Registering the Care-of Address (CoA), and
- Tunneling to the Care-of Address (CoA).

### 2.2 Discovering the Care-of Address

The Mobile IP *discovery* process has been built on top of an existing standard protocol, Router Advertisement, specified in [6]. Mobile IP discovery does not modify the original fields of existing router advertisements but simply extends them to associate mobility functions. Thus, a router advertisement can carry information about default routers, just as before, and in addition carry further information about one or more Care-of Addresses. When the router advertisements are extended to also contain the needed Care-of Address, they are known as *agent advertisements*. Home agents and foreign agents typically broadcast agent advertisements at regular intervals. If a

Mobile Station needs to get a Care-of Address and does not wish to wait for the periodic advertisement, the Mobile Station can broadcast a request which will be answered by any foreign agent or home agent that receives it. Home agents use agent advertisements to make themselves known, even if they do not offer any Care-of Addresses. However, it is not possible to associate preferences to the various Care-of Addresses in the router advertisement, as is the case with default routers.

The IETF working group was concerned that dynamic preference values might destabilize the operation of Mobile IP. Because no one could defend static preference assignments except for backup mobility agents, which do not help distribute the routing load, the group eventually decided not to use the preference assignments with the Care-of Address list.

Thus, an agent advertisement performs the following functions [6]:

- allows for the detection of mobility agents,
- lists one or more available Care-of Addresses,
- informs the mobile node about special features provided by foreign agents, for example, alternative encapsulation techniques,
- lets mobile nodes determine the network number and status of their link to the Internet, and
- lets the mobile node know whether the agent is a home agent, a foreign agent, or both, and therefore whether it is on its home network or a foreign network.

Mobile Station use router solicitations as defined in [6] to detect any change in the set of mobility agents available at the current point of attachment. If advertisements are no longer detectable from a Foreign Agent that previously had offered a Care-of Address to the Mobile Station, the Mobile Station should assume that Foreign Agent is no longer within range of the Mobile Station’s network interface. In this situation, the Mobile Station should begin to hunt for a new Care-of Address, or possibly use a Care-of Address known from advertisements it is still receiving. The Mobile Station may choose to wait for another advertisement if it has not received any recently advertised Care-of Addresses, or it may send an agent request [1].

### 2.3 Registering the Care-of Address

Once a Mobile Station has a Care-of Address, its home agent must find out about it. The registration process has already been defined by Mobile IP for this purpose. The process begins when the Mobile Station, possibly with the assistance of a Foreign Agent, sends a registration request with the Care-of Address information. When the Home Agent receives this request, it adds the necessary information to its routing table, approves the request, and sends a registration reply back to the Mobile Station [7].

### 2.4 Tunneling to the Care-of Address

The default encapsulation mechanism that must be supported by all mobility agents using Mobile IP is IP-within-IP. Using IP-within-IP, the home agent, the tunnel source, inserts a new IP header, or tunnel header, in front of the IP header of any datagram addressed to the mobile node's home address. The new tunnel header uses the mobile node's Care-of Address as the destination IP address, or tunnel destination. The tunnel source IP address is the home agent, and the tunnel header uses 4 as the higher level protocol number, indicating that the next protocol header is again an IP header. In IP-within-IP the entire original IP header is preserved as the first part of the payload of the tunnel header. Therefore, to recover the original packet, the foreign agent only has to eliminate the tunnel header and deliver the rest to the mobile node [5].

## 3. The Proposed Approach

The proposed approach will use the non-encapsulation technique with the indirect routing of Mobile IP.

In this section, we will discuss the CoA registration process (see Figure 2) and the related packet delivery mechanism (see Figure 3).

### 3.1 The Proposed CoA Registration Process

Using the proposed approach, when the Mobile Station moves from its own network (Home Network) to another network (Foreign Network), Mobile Station receives an ICMP advertisement message (with mobility agent advertisement extension) that contains a Core-of Address (CoA) and new field which called flags (instead of old RBHFMGrT).

The new proposed Flags field contains the following bits R0HF0000, and this means that there is no encapsulation format since R bit used for registration (if it is required), H stands for home bit, F for foreign bit, and other bits set to zeros, see Table 1.

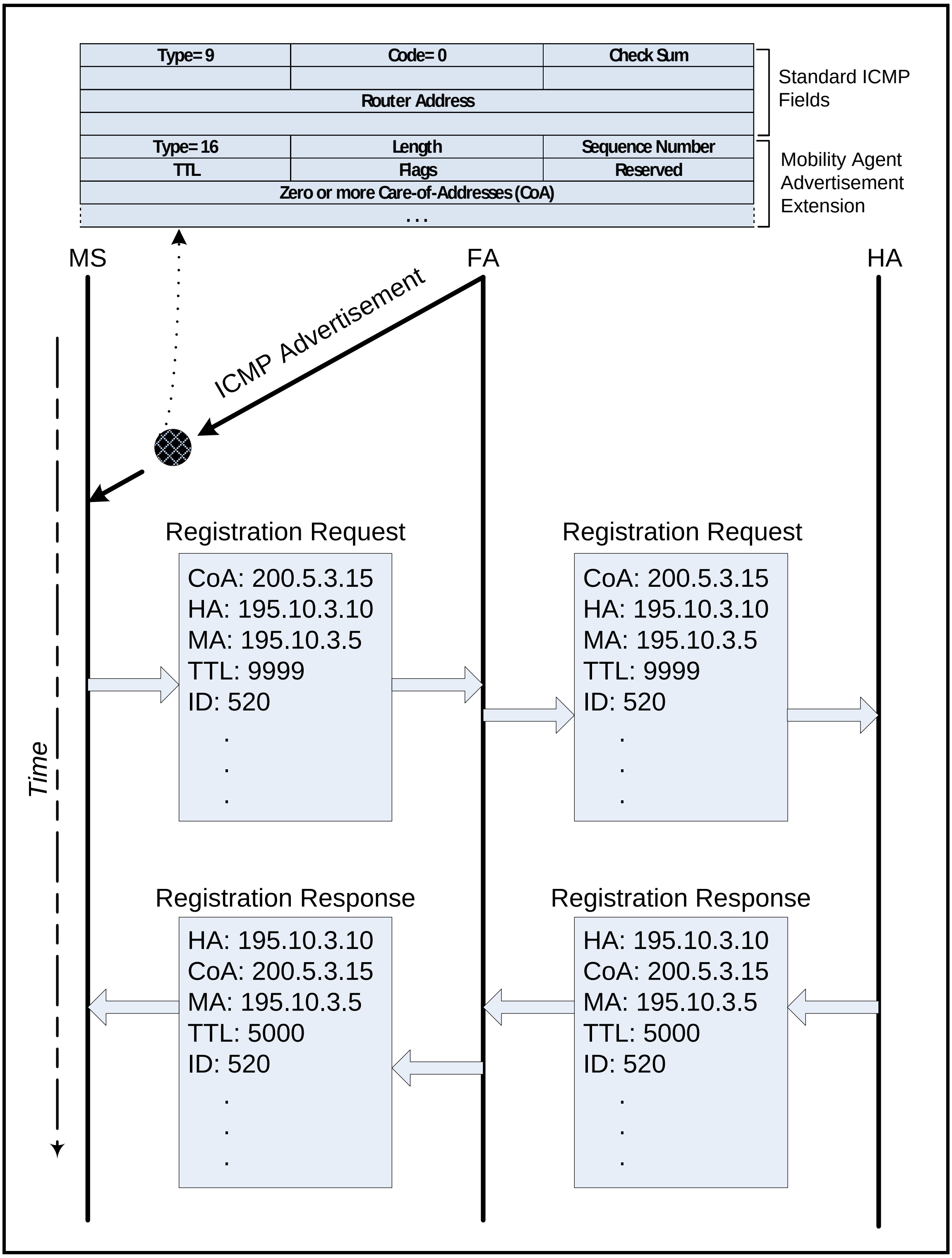


Fig. 2 The Non-Encapsulation Registration Process

Mobile station after receiving its new address (CoA) must register CoA in its home agent. It sends a registration request message to the foreign agent, foreign agent binds mobile permanent address to the new CoA which already given to mobile station in its own table. Then foreign agent forwards a registration request message to the home agent which has the original mobile station. The home agent receives a registration request message, then updates its own addressing table by binding the CoA to MA of a particular mobile station. The home agent sends a registration response message to the foreign agent, and then the foreign agent forwards a registration response message to the mobile station.

In this registration process, we can note that the encapsulation format is ignored in all steps. This approach will save the time of registration process and decrease the processing delay in all parties of the registration process.

Figure 2 illustrates the non-encapsulation registration process. Also, Table 1 describes the proposed and old flags fields of the ICMP advertisement message.

### 3.2 The Related Packet Delivery Mechanism

To explain this packet delivery mechanism, we have to discuss two potential scenarios. The first scenario is when the mobile station (MS) is currently located within the home network (HN). In this way, the correspondent node (CN) directly sends a packet to the home agent (HA) using the traditional internet routing mechanisms, taking into consideration that the destination IP address of the sent packet is the mobile permanent address (MA). Since the mobile is already located within the home agent scope, then it will directly forward the packet to the intended mobile station. The mobile station receives the packet and reply a confirmation response if it is required.

The second scenario is when the mobile station is currently located at a foreign network (outside the home network). In this scenario, the correspondent node sends a packet to the home agent where the destination IP address of the sent packet is a mobile permanent address (MA). The home agent receives the packet and checks its addressing table to identify the current temporary IP address (CoA) of the mobile station. Furthermore, the home agent perform a header processing by coping all fields along with the data as it is except the destination IP address filed which must be change to be the CoA instead of MA, see Figure 3.

The home agent forwards the processed packet to the foreign agent. When the foreign agent received the packet, it will forward it directly to the mobile station since no need to any further header translation. The mobile station receives the packet which has the CoA as its destination address, and it will recognize that this packet is sent to its attention. If it is required, the mobile station will send a reply message to the CN, we should note that the source IP address of the reply message is MA and the destination IP address is CN, see Figure 3.

Figure 4 presents a flowchart of the two potential scenarios of the packet delivery mechanism which is discussed within this section.

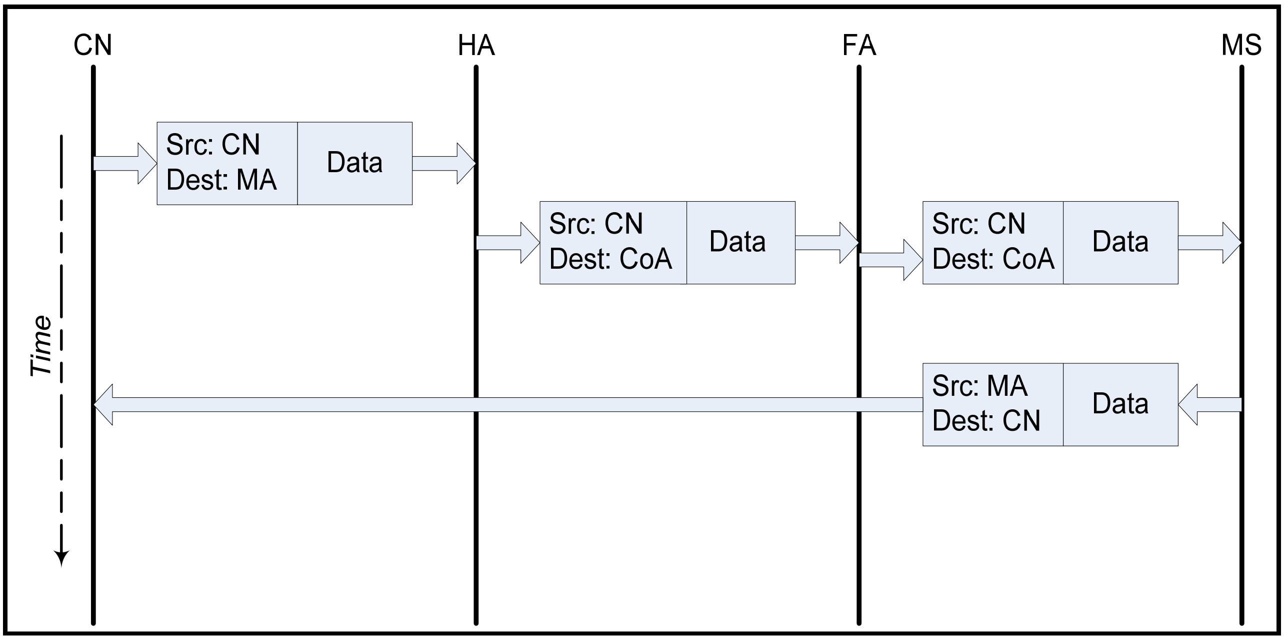


Fig. 3 Non-Encapsulation Communication Process

Table 1: Description of the Proposed and Old Flags Field

| **The Proposed Flags Field** | |
|---|---|
| **Agent** | **Flags (R0HF0000)** |
| Home Agent | 00100000 |
| Foreign Agent | 10010000 |
| R: Registration is required<br>H: Home Agent<br>F: Foreign Agent | |
| **The Old Flags Field (RBHFMGrT)** | |
| R: Registration Bit<br>H: Home Bit<br>F: Foreign Bit<br>MG: Encapsulation Format | |

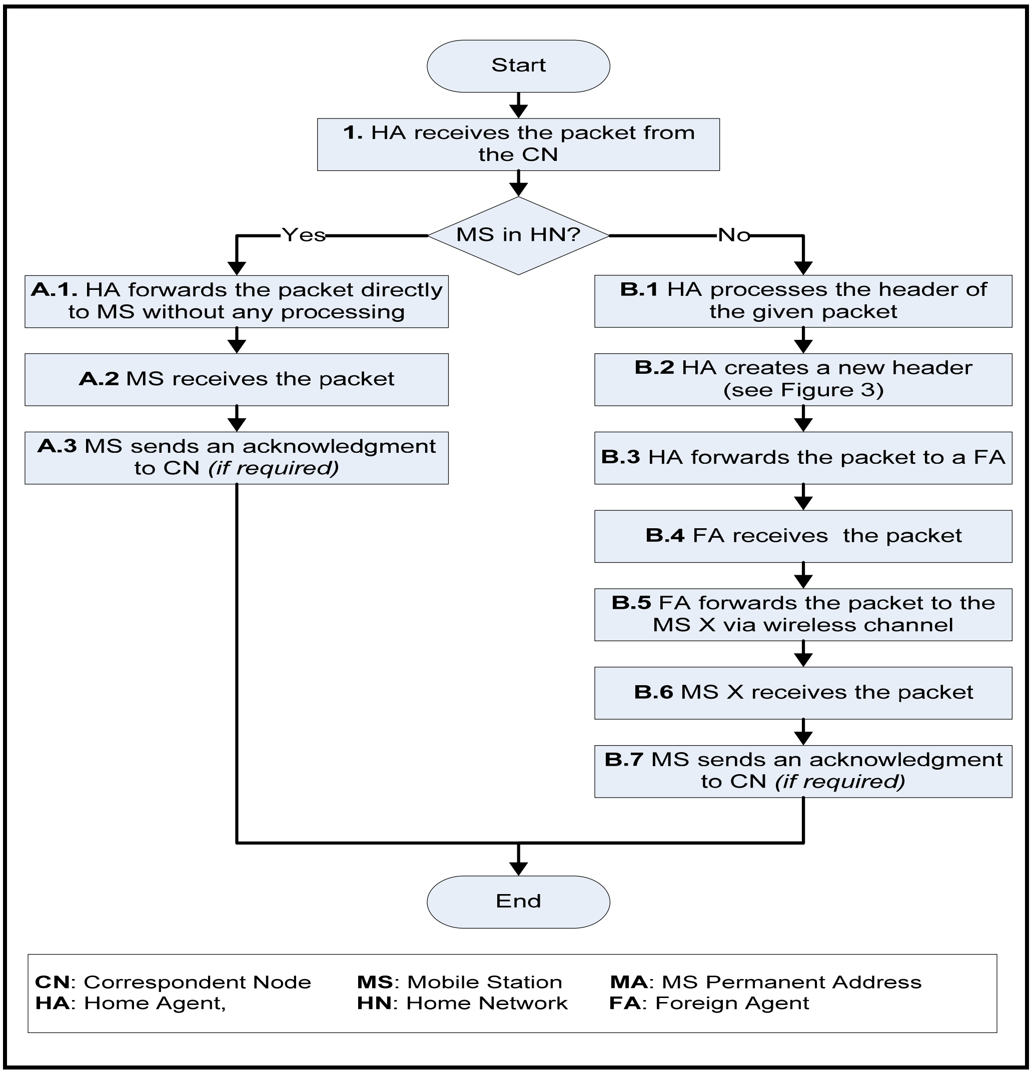


Fig. 4 The Packet Delivery Mechanism

## 4. An Example

Assume the following:

1. the mobile station permanent address (MA) is 195.10.3.5 which is belongs to a network 195.10.3.0 (Home Network),
2. Home Agent address is 195.10.3.10,
3. Mobile Station (MS) moves from the Home Network to a Foreign Network 200.5.3.15,
4. when the MS arrives at the given Foreign Network, it obtains CoA 200.5.3.15 as a temporary address (see Figure 1), and
5. Correspondent Node (CN 220.25.4.9) entity which wishes to communicate with the MS.

Based on the above assumptions, the following steps explain the first part of our proposed approach (the Non-Encapsulation Registration Process):

1. MS must register its new CoA in the Home Agent, and MS creates a registration request message which contains the following:
   - CoA: 200.5.3.15
   - HA: 195.10.3.10
   - MA: 195.10.3.5
   - Identification field: 520
   - Leasing (TTL): 9999
   - Some related service information

   Note that the message does not has anything related to encapsulation format (it is not required here). MS forwards the created required registration request message to the Foreign Agent.

2. After receiving the required registration message by the Foreign Agent, it registers MA as 195.10.3.5 and CoA as 200.5.3.5 (i.e. 195.10.3.5 is equivalent to 200.5.3.5. Then it forwards a registration request message to the Home Agent.

3. Home Agent receives the registration request message which was forwarded from the Foreign Agent. It registers the given CoA and MA in its addressing table, see Figures 2 and 5. Then Home Agent sends a registration response message to the Foreign Agent. Note that the Home Agent reduces the leasing time of CoA almost by half for reliable mobility issues.

4. The Foreign Agent (200.5.3.5) receives a registration response message from HA: 195.10.3.10, then forwards it to the MS with CoA: 200.5.3.15, see Figure 2.

Now, if the correspondent node (CN: 220.25.4.9) wants to send a packet(s) to Mobile Station (MA: 195.10.3.5) which is already located in a foreign network (200.5.3.0). The following steps explain this process which represents the second part of our approach (the Non-Encapsulation Packet Delivery Process):

1. The Correspondent Node sends an IP packet to the Mobile Station, the source IP address of a packet is 220.25.4.9 and the destination IP address is 195.10.3.5.

2. The Home Agent receives the packet. It already knows the Mobile Station (MA: 195.10.3.5) is located at the Foreign Network (220.5.3.0). Also, it performs a header translation of the received packet by copying all of the header fields of the given packet as they are and without any kind of changes except the destination IP address field which will be the Care-of Address (CoA: 200.5.3.15) instead of the permanent address (MA: 195.10.3.5). The Home Agent forwards the new processed packet to the Foreign Agent (FA: 220.5.3.7). Note that the Home Agent does not perform any encapsulation as in the traditional Mobile IP indirect routing, see Figures 3 and 5.

3. The Foreign Agent (200.5.3.7) receives the packet from the Home Agent (195.10.3.10) and the Foreign Agent will works as a traditional router to deliver a packet to the Mobile Station (CoA:200.5.3.15).

4. The Mobile Station (CoA: 200.5.3.15 and MA: 195.10.3.5) receives the packet, if response is required, the Mobile Station directly sends a packet to Correspondent Node (CN: 220.25.4.9) with 195.10.3.5 as a source IP address and 220.25.4.9 as a destination IP address, see Figure 1.

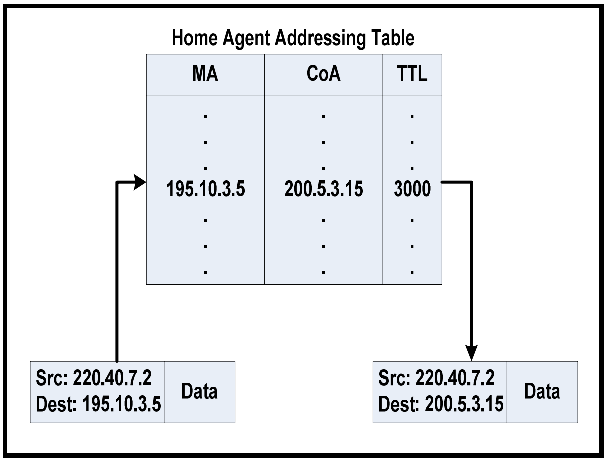


Fig. 5 Address Translation Process

## 5. Conclusion

Presently, the encapsulation (or what is also called tunneling) of the packets is the common approach of the Mobile IP indirect routing. By other hand, it is uncommon to use the non-encapsulation approach with the mobile IP indirect routing technique.

As well known, the encapsulation process itself will increase the transmission delay, and the process of encapsulation of the sending packet will enlarge its size, and then the speed of communication process will be decreased based on the enlarged size of the new packet sent from the home agent. In addition, the de-encapsulation process will need a time to return the new packet to its original structure in which this process will also increase the delay of the communication process.

In this paper, we proposed a new approach in which we used the non-encapsulation technique in the indirect routing. Consequently, the delay and the speed of transmission of the CoA registration and communication processes within the indirect routing will be positively affected. Moreover, this way will decrease the delay and increase the speed. Furthermore, there is no any kind of size enlargement of the sent packets.

**Acknowledgments**

This work was supported by the Applied Science University, Amman, Jordan.

## References

[1] C. E. Perkins, "Mobile Networking Through Mobile IP", *IEEE Internet Computing Journal*, Vol. 2, No. 1, 1998, pp. 58-69.

[2] J. Kurose, K. Ross, *Computer Networking: A Top-Down Approach Featuring the Internet*, 4th edition. Pearson Education, Addison-Wesley, Boston, MA, USA, 2008.

[3] C. E. Perkins, "IP Mobility Support for IPV4", *RFC Editor*, REC3344, USA Online: http://portal.acm.org/citation.cfm?id=RFC3344#, 2002.

[4] C. E. Perkins, "Mobile IP: Design Principles and Practice", Addison-Wesley, Reading, MA, USA, 1998.

[5] C. E. Perkins, "IP Encapsulation within IP", *Internet RFC*, REC2003, USA, Online: http://portal.acm.org/citation.cfm?id=RFC2003, 1996.

[6] S. Deering, "ICMP Router Discovery Messages", *RFC Editor*, REC1256, USA, Online: http://portal.acm.org /citation.cfm?id=RFC1256, 1991.

[7] H. Haverinen, A. Kuikka and T. Maattanen, "A portable mobile IP implementation", in *Proceedings of 25th Annual IEEE Conference on Local Computer Networks – (LCN'2000)*, Tampa, Florida, USA, November, 8-10, 2000.

**Dr. Basil M. Al-Kasasbeh (1971)** received the M.S. and PhD degrees in Networks, Systems and Communication Devices from Siberian State University of Telecommunications and Informatics, Novosibirsk in 1994 and 2002, respectively. During 2002-2003, he was an Assistant Professor at the Faculty of Information Technology, University of Jordan. Since 2003, he is an Assistant Professor at the Faculty of Information technology, Applied Science University in Jordan. His research interests include: Mobile and Wireless Systems, Mobile IP, and IPV6.

**Dr. Rafa E. Al-Qutaish (1970)** received the B.S. degree in Computer Science from Yarmouk University, Jordan in 1993, the MSc degree in Software Engineering from University of Putra, Malaysia in 1998, and PhD degree in Software Engineering from the School of Higher Technology, University of Quebec, Canada in 2007. Since 2007, he is an Assistant Professor at the Faculty of Information Technology, Applied Science University. His research interests include: Communication Software Engineering, Software Measurements, Software Engineering Standardizations, Software Quality Engineering, and Applied Artificial Intelligence. He is a senior member of IEEE-CS and acting member of ACM.

**Dr. Khalid T. Al-Sarayreh (1971)** received the B.S. degree in Computer Science from Mu'tah University, Jordan in 1993, the MSc in Computer Engineering from Yarmouk University, Jordan in 2003, and PhD in Computer Information Systems from the Arab Academy for Financial and Banking Sciences, Jordan in 2005. During 2002-2005, he stayed in the KADDB, Ministry of Defense. From 2005 to 2006, he was an Assistant Professor at the Jordan University. Since 2006, He is as an Assistant Professor at the Faculty of Information Technology, Applied Science University/ His research interests include: Software Real-Time Embedded Systems, Computer Networks, and Applied Artificial Intelligence