

Performance Evaluation of Mobile Networking Using Mobile  
Internet Protocol

By  
Haytham Kamel Abdallah Qasem

Supervisor  
Jamil Ayoup

Co-Supervisor  
Souheil Odeh

Thesis (M. Sc. In Electrical Engineering/ Communication)

2002



This thesis was successfully defended and approved on 1/8/2002

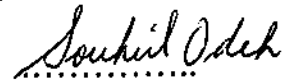
Examination Committee

Signature

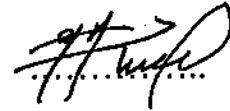
Prof. Jamil Ayoub



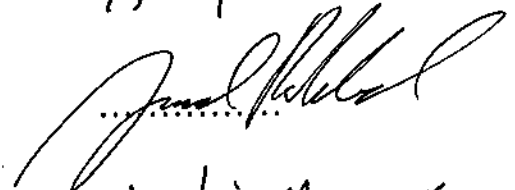
Dr. Souheil Odeh



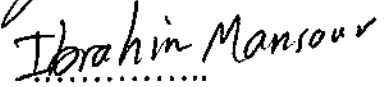
Dr. Ibrahim Ghareeb



Dr. Jamal Rahal



Dr. Ibrahim Mansour







**Dedication**

*To my lovely parents*

*To my brothers and sisters*

## Acknowledgement

*First, and foremost, I would like to introduce my great gratitude and respect to my lovely parents for their continuous encouragement and efforts. Also, my thanks to my supervisors, Professor Jamil Ayoub and Dr. Souheil F. Odeh for their support and advice. Finally, I would like to thank the examination committee for their efforts in evaluating this study.*

## Table of Contents

Examination Committee	ii
Dedication	iii
Acknowledgement	iv
Table of Contents	v
List of Tables	viii
List of Figures	ix
Abstract (English)	xi
<b>Introduction</b>	<b>1</b>
1.1 Preface	1
1.2 The Need for Mobile IP	4
<b>Background</b>	<b>10</b>
2.1 Preview	10
2.2 Agent Discovery	11
2.2.1 Agent Advertisement and Solicitation ICMP Messages	11
2.2.2 Automatic Home Agent Discovery	12
2.3 Registration	13
2.3.1 Registration Overview	14
2.3.1.1 Registration Scenarios	16
2.3.2 Authentication	17
2.3.3 Replay Protection for Registration Requests	18
2.3.4 Home Agent Receiving and Processing For Registration	19
2.3.5 Registration Request and Reply Format	20
2.3.6 Registration Extensions	22
2.4 Datagram Delivering (Tunneling)	23
2.4.1 IP-in-IP Encapsulation	24
2.4.2 Minimal Encapsulation	25
2.4.3 Generic Record Encapsulation	27
2.5 Proxy Address Resolution Protocol (ARP) and Gratuitous ARP	27
2.6 Triangle Route and Route Optimization	28
2.7 General Home/Foreign Agents Operations	31
2.8 Movement Detection	31
2.9 Smooth Handoffs	33



2.10 Mobile IP Version 6	34
2.11 Route Optimization in Mobile IPv6	35
2.12 Security	36
2.13 Source Routing	36
2.14 Mobility Attach Schedule Using Mobile IPv6	39
2.15 Location and Movement Detection in MobileIPv6	40
2.16 Notification	41
2.17 Notification Scenarios	42
2.18 Home Subnet Renumbering	43
2.19 Mobility Requirements	44
2.20 Mobile IP and DHCP	44
2.21 Applying Mobile IP	46
<b>Mobile IP and Other Protocols</b>	47
3.1 Mobile IP Security	47
3.1.1 Preventing Replay Attacks	48
3.1.2 Mobile IP and Firewalls	51
3.1.2.1 Simple Key Internet Protocol (SKIP) Firewall Transversal	51
3.1.2.1.1 Registration Procedure	52
3.1.2.1.2 Building a Tunneled Registration Request	54
3.1.2.2 ISKAMP/ Oakley Firewall Transversal	55
3.2 Mobile IP with PPP	56
3.2.1 Preventing Attacks within The Frame Work of Mobile IP and PPP	57
3.3 Mobile Networks and Mobile IP	58
3.3.1 Preview and Components	58
3.3.2 Routing Tables in Mobile Networks	60
3.3.3 Mobile Routing within Mobile Networks	63
3.3.4 Mobile Router in Mobile IPv4	64
3.3.5 Mobile IP and Real-Time Traffic	66
3.4 Routing Protocols in Ad Hoc Networks and Mobile IP	68
3.4.1 Dynamic Source Routing (DSR) Protocol	68
3.4.2 Destination Sequenced Distance Vector Protocol	70

3.4.3 Zone Routing Protocol (ZRP)	71
3.4.4 The Ad Hoc on Demand Distance Vector (AODV)	72
3.4.4.1 AODV and MIP	74
3.5 Cellular IP	75
3.6 Hierarchical Mobile IP	76
3.7 Transmission Control Protocol (TCP) and Mobile IP	79
3.8 Mobile IP and GPRS	82
3.8.1 General Description of GPRS	82
3.8.2 GPRS Attach Schedule Overview	86
3.8.3 GPRS Handover Schedule Overview	87
3.8.4 Mobile IP in GPRS	88
3.8.5 GPRS, Mobile IP: Comparison Study	90
3.8.6 Mobile IP Combination with GPRS	93
<b>Simulation Tools</b>	95
4.1 Introduction	95
4.2 Simulation Hardware and Software Specifications	98
4.3 Mobile IP Simulation Source Code	103
<b>Analysis and Simulation of Mobile IP</b>	108
5.1 Simple Model	108
5.2 Encapsulation Techniques Tests	110
5.3 Registration Delay Tests	114
5.4 Throughput Analysis of Mobile IP	117
5.5 Delay Analysis of Mobile IPv6	121
5.6 Throughput Analysis of Mobile IPv6	126
5.7 Link Utilization Study of Mobile IP	130
5.8 Reformulation of Simulation Results	133
<b>Conclusions and Recommendations for Future Work</b>	142
6.1 Conclusions	142
6.2 Future Work	145
References	146
Abstract (Arabic)	149

## List of Tables

Table (2.1) Mobility Differences Between Mobile IPv6 and Mobile IPv4	38
Table (3.1) Routing Table of Home Agent	61
Table (3.2) Routing Table of Mobile Router	61
Table (3.3) Modified Routing Table of Home Agent	62
Table (3.4) Routing Table of Mobile Router on Foreign Link	63
Table (4.1) Hardware Specifications	99
Table (4.2) Software Specifications	99
Table (5.1) Results of Registration Delay	115
Table (5.2) Routing to Mobile Node	120
Table (5.3) Routing to Fixed Node	120
Table (5.4) Delay Measurements in Mobile IPv6	124
Table (5.5) Delay Measurements from CND to Mobile Node B	125
Table (5.6) Throughput over 150 Seconds Transmission Delay	126
Table (5.7) Throughput Analysis (Period = 100 Seconds)	127
Table (5.8) Throughput over 50 Seconds Transmission Time	128
Table (5.9) Throughput over 20 Seconds Transmission Time	129
Table (5.10) Utilization Measurements	130
Table (5.11) Utilization Results with Different Message Size	131
Table (5.12) Utilization Results for Mobile IPv6	132
Table (5.13) Effect of Larger Message size on Link Utilization	133

## List of Figures

Figure (1.1) Node Movement	5
Figure (2.1) Home Agent Discovery	13
Figure (2.2) Registration Process in Mobile IP	15
Figure (2.3) Registration Message Structure	15
Figure (2.4) Registration Scenarios	16
Figure (2.5) Registration Packet Format	20
Figure (2.6) Packet Format of Registration Reply	21
Figure (2.7) Packet Format of Mobile-Home Authentication Extension	22
Figure (2.8) Tunneling	23
Figure (2.9) IP-in-IP Encapsulation	24
Figure (2.10) Minimal Encapsulation	25
Figure (2.11) Header Format of Minimal Encapsulation	26
Figure (2.12) Packet Structure of GRE	27
Figure (2.13) Triangle Route	30
Figure (2.14) Entities of Mobile IPv6	35
Figure (2.15) Message Exchange in Mobile IPv6	42
Figure (3.1) Authentication of Registration Message	50
Figure (3.2) Firewall Reference Diagram	52
Figure (3.3) Reference Model of Mobile IP/PPP Interaction	57
Figure (3.4) Mobile Internet Router	59
Figure (3.5) Example of Mobile Network	60
Figure (3.6) Mobility Support in Mobile Networks	66
Figure (3.7) Ad Hoc Network Routing Discovery	69
Figure (3.8) Networking Using ZRP	72
Figure (3.9) TCP Segments	80
Figure (3.10) Total System Overview	84
Figure (3.11) UMTS Terrestrial Radio Access Network	85
Figure (3.12) GPRS Packet Domain Overview	86
Figure (3.13) GPRS Attach Schedule	87
Figure (3.14) Inter-GPRS Routing Area Update	88
Figure (3.15) Handover Between Different accesses with Mobile IP	89

Figure (3.16) GPRS Architecture	90
Figure (3.17) Mobile IPv4 Architecture (with Foreign Agent)	90
Figure (4.1) Simulation Steps Using NS	96
Figure (4.2) Base Station Nodes in NS	97
Figure (5.1) Mobile IP Simple Scenario	109
Figure (5.2) Mobile Node at Home	109
Figure (5.3) Encapsulation Methods Tests	111
Figure (5.4) Registration Delay Module	116
Figure (5.5) Proposed Model for Throughput analysis	118
Figure (5.6) Routing Paths for Mobile and Fixed Nodes	119
Figure (5.7) Delay Measurements of Mobile IPv6	121
Figure (5.8) Mobile IPv6 Delay for Real Model	123
Figure (5.9) Delay in Mobile IPv4	134
Figure (5.10) Comparison of Message Delay	135
Figure (5.11) Delay in Mobile IPv6	136
Figure (5.12) Message Delay Difference for Mobile IPv6	136
Figure (5.13) Throughput of Mobile IPv4	137
Figure (5.14) Home/Foreign Link Throughput Comparison	137
Figure (5.15) Throughput of Mobile IPv6	138
Figure (5.16) Mobile IPv6 Throughput Comparison	139
Figure (5.17) Mobile IPv4 Link Utilization	140
Figure (5.18) Utilization Ratio for Mobile IPv4	140
Figure (5.19) Link Utilization for Mobile IPv6	141
Figure (5.20) Utilization Ratio for Mobile IPv6	141

# Performance Evaluation of Mobile Networking Using Mobile Internet Protocol

By

Haytham Kamel Abdallah Qasem

Supervisor  
Prof. Jamil Ayoub

Co-Supervisor  
Dr. Souheil F. Odeh

## Abstract

In recent years, we have faced a rapid growth in the need to support mobile nodes. In an Internet-based mobile computing system, mobile nodes require special support to maintain connectivity as they change their point of attachment. The aim of the design for the mobility support is to make computers and laptops keep connectivity without any additional modification and changes when roaming or changing the points of their attachments. To achieve this goal, the network layer is chosen to make a slight alteration, and protocols in the other layer keep unchanged as possible. One of the popular used protocols of the network layer is Internet Protocol (IP). In the IP networking, one IP address indicates the point of the attachment for each node. Mobility support in IP (Mobile IP) is designed to address the problem of keeping connectivity without any further modifications when end nodes roam or switch to another network. Mobile IP has been developed to provide internet mobility services. The purpose of this research is to evaluate the performance of mobile IP in terms of different performance measures such as end-to-end message delay, link utilization and throughput. The basic protocol is discussed, with details given on the three major components: Agent advertisement, Registration and Tunneling. A comparison study between the different functionalities of mobile IPv4, mobile IPv6 and other proposals in this field is presented. Moreover, how mobile IP works under different connections, like General Packet Radio Service (GPRS), wireless Ad Hoc networks and the connection via Point-to-Point (PPP) link, is also included.

## Introduction

### 1.1 Preface

In the last few years, the mobile networking and computing industry has faced a huge evolution. The weight of laptops has a dramatic decrease, and their prices become affordable for the public. More and more students and businessmen enjoy the advantages of the portability and flexibility of the laptops' properties. The increasing number of portable computers, combined with the rapid growth of wireless services, makes supporting Internet mobility important. Mobile hosts need to switch between networks in different administrative domains as they move around the network, and they need to switch between different types of networks (Packet radio, Ethernet, Fiber Distributed Data Interface (FDDI), Cellular telephone, etc.). Cellular phones are well suited to voice communication where the provided bandwidth is too small to get an acceptable data transmission rate for mobile laptops. As computers become less expensive and smaller in size, it is expected that mobile computer equipment will support communication mobility (Halsall, 1996).

Mobility is the ability to change location while connected to the network. One of the main problems that faced mobility is the address migration problem, where mobile computers will use different network access points (addresses). Today's networking is not designed for dynamically changing addresses. Once an address for a host name is known to a system it is typically cached with a long expiration time and with no way to invalidate entries. Another problem is the portability, where a laptop computer can be operated at any of a set of points of attachment, but not during the time that the computer changes its point of attachment.

Mobile computing is the technology in which users carrying portable devices have an access to a shared infrastructure independent of their physical location. The technical

challenges to establishing this vision of computing is nontrivial. The main challenges facing this technology are:

- **Heterogeneous networks:** Mobile computers, in contrast to stationary computers, encounter more heterogeneous network connections. As they leave the range of one network transceiver they switch to another, and sometimes they can access multiple transceivers on different frequencies. Even when plugged in, they may use wireless access. This heterogeneity makes mobile networking more complex than traditional networking.
- **Wireless links:** Mobile computers require wireless network access. Wireless networking is more difficult to achieve than wired one since the surrounding environment interacts with the signal, blocking signal paths, introducing noise, path losses and more frequent disconnection. These in turn, will increase communication latency due to retransmission and decrease the overall throughput.
- **Security problems:** The security of wireless links is much worse of a wired one; this is why it is so easy to connect to a wireless link, especially, when the working space covers large area. Interleaving, scrambling, data encryption and several other algorithms are used to achieve secure communication over insecure wireless links.
- **Lower bandwidth:** Wireless networks delivers lower bandwidth than wired networks, as an example, Cellular GSM can achieve 9.6 kbps, infrared communication up to 1 Mbps, GPRS up to 171 kbps. While Ethernet provides 10 Mbps, 100 Mbps, and 1000 Mbps. This requires mobile computing designs to be more concerned about bandwidth consumption.



By the use of the conventional network configuration, a computer must be shut down and modify its network settings when moving or connecting to a different network. This causes much more inconvenience for the end users. The situation becomes even worse when the computer keeps roaming and switching to different networks. For example, a businessman uses the video conference while traveling by train. The aim of the design for the mobility support is to make computers and laptops keep connectivity without any additional modification and changes when roaming or changing the points of their attachments. To achieve this goal, the network layer is chosen to make a slight alternation, and protocols in the other layer keep unchanged as much as possible. The advantage of designing mobile IP based on modifying the network layer protocol is to make it physical layer independent, which means that any communication media, including wired and wireless networks, will support mobile IP. The main problem with link-layer solutions is that they are limited to a single medium.

One of the popular used protocols of the network layer is the Internet Protocol (IP). In the IP networking, one IP address indicates the point of the attachment for each node, which is similar to the telephony network. For instance, each telephone socket has a fixed telephone number, which does not matter what type of the telephone set is connected. Likely, when a laptop connects to a different network, it needs a new IP address to indicate its current location and keep its communication with the Internet. Otherwise, the packet addressed to the node connected to a different network becomes unroutable, just like that a postman is not able to deliver a mail with a wrong address. As a consequence, it is evident that the key point of the mobile IP design is how to make IP address transparent.

The rest of this thesis is organized as follows. Chapter 2 is a brief overview of the basic functionalities of mobile IP versions 4 and 6. The main distinctions between the two proposals are also presented there. Chapter 3 concerned with the security of mobile IP,

different security algorithms are discussed. Operation of mobile IP in cooperation with other protocols and technologies in this area, such as Mobile networks, Wireless Ad Hoc networks, Cellular IP, and GPRS technology are also discussed. Chapter 4 mainly gives a description of the mobile IP simulation through several networking scenarios. Transmission delays, throughput, and link utilization are the main performance measures which are studied through this simulation. Simulation results are drawn and explained. The last chapter gives a brief conclusion of this study, and some interesting directions for the future work of mobile computing design.

## 1.2 The Need for Mobile IP

IP nodes, hosts, and routers base their packet forwarding decisions on information contained within the IP packet header. Namely, routing decisions are made based upon the network-prefix portion of the IP destination address. Thus, all nodes with interfaces on a given link must have identical network-prefix portions of their IP addresses on those interfaces. The following example is considered to see what happens if a host whose network-prefix has been assigned to one link, disconnects from that link and then connects to a new link which has been assigned a different network-prefix. In Figure (1.1) below, network-prefix of 2.0.0 has been assigned to host 4, but host 4 is shown connected to a link whose network-prefix is 4.0.0. The routing table of router A is also shown. Let's see what happens if host 1 tries to send a packet to host 4:

- Host 1 generates an IP packet whose IP source address is 1.0.0.1 and the IP destination address is 2.0.0.4. This will match a default route in the routing table of host 1, which specifies a next hop (1.0.0.254) of router A via interface "a". Thus host 1 forwards packet to router A.
- Router A forwards the packet to router B (3.0.0.253) via interface "c" depending on the entries in its routing table.

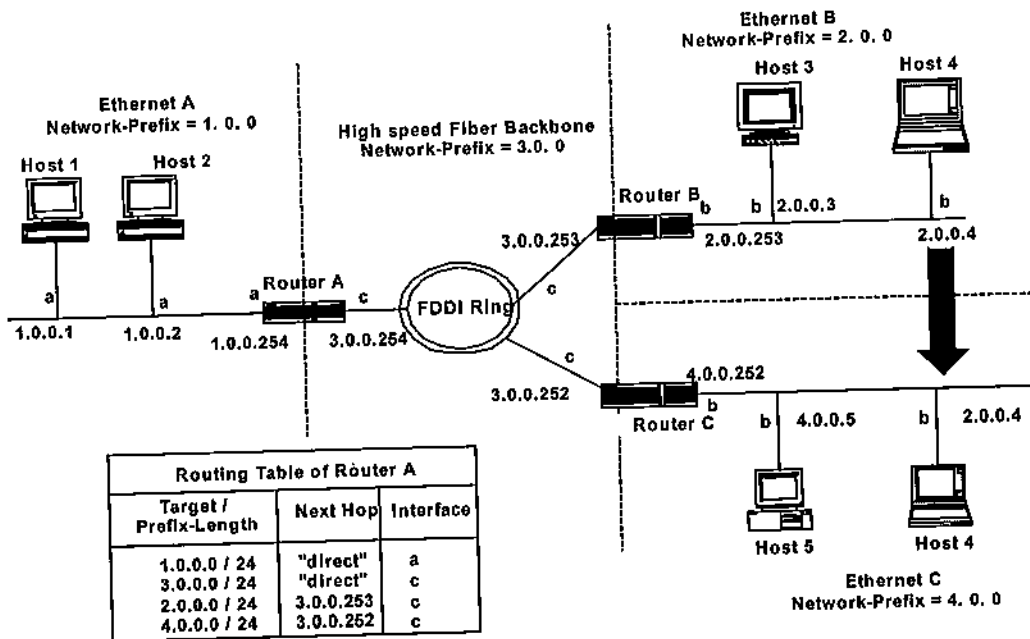


Figure (1.1) Node Movement

- Router B sends the packet via interface "b" on Ethernet B since it has a direct path in its routing table for targets with network-prefix equal to 2.0.0. However, the packet is undeliverable because host 4 is not yet connected to Ethernet B (where it is supposed to be based upon its network-prefix). An Internet Control Message Protocol (ICMP) host unreachable error message will be sent by router B to the packet source (host 1). This means that such a node (host 4) is incapable of communicating with any other nodes unless it minimally changes the network-prefix portion of its IP address to reflect its new point of attachment to the network.

Host-specific routing can be considered as a possible solution to this problem. Thus, the problem of delivering a packet to host 4 in the previous example can be solved by placing host-specific routes in the routing tables of routers A, B, and C as follows:

Router A: {Target / Prefix-Length = 2.0.0.4 / 32, Next Hop = 3.0.0.252, Interface = "c"};

TCP connection within a node is uniquely identified by four values: IP source address, IP destination address, TCP source port, and TCP destination port. There is an enormous installed base of IPv4 nodes, all of which assume that these four quantities will remain constant over the duration of a TCP connection. This installed base would simply drop its connections to a destination node whose IP address was to change. And so, all ongoing communication between a mobile node and any of these existing nodes would have to be terminated, with new connections being initiated by the mobile node at its new address. In summary, changing a mobile node's address as it moves does not solve mobility problem completely, scalably, and transparently. On the other hand, it is a good solution for a problem known as Nomadicity. A nomadic node is one which must terminate all existing communication before changing its point of attachment but then can initiate new connections with a new address once it reaches its new location. This can be done by Dynamic Host Configuration Protocol (DHCP) and PPP control protocol.

Link-layer solutions are another type of solutions to the mobility problem which are also not sufficiently general to provide node mobility on the global Internet, because:

- By definition, they provide node mobility only in the context of a single type of medium. For example, Cellular Digital Packet Data (CDPD) provides mobility when the mobile node moves from one CDPD cell to another. However, CDPD requires a mobile node to acquire new IP address when it is moved to another medium, such as a wired token ring network.
- Link-layer solutions inherently necessitate  $N$  different mobility solutions for each of  $N$  possible media over which node might want to send IP packets. A single solution which works over all media types is to be preferred; if such solution is possible. Mobile IP is such a solution.

- Finally, link-layer solutions such as wireless LANs provide mobility within a limited geographical area, a university campus, or a building. However, wide-area solutions such as CDPD can provide much more geographically diverse areas but the limited throughput of such systems makes them less efficient.

Mobile IP is unique in its ability to provide mobility over all types of media and through an arbitrary large geographical area. Using mobile IP, a node can communicate using a fixed IP address whenever it can obtain a connection to the network.

Mobility can be defined as the ability of a node to change its point of attachment from one link to another while maintaining all existing communications and using the same IP address at its new link. Mobility as provided by mobile IP can be extremely useful for the following reasons:

- Many applications have configuration databases which depend on IP addresses, as opposed to hostnames. In the presence of rapidly changing IP addresses, these applications would break.
- Some application vendors provide network-licensing systems which restrict access to only those nodes possessing specific ranges of IP addresses.
- Some security mechanisms provide access privileges to nodes based on their IP address.

Mobile IP is a network-layer solution to node mobility in the Internet. It can be considered as a routing protocol which is used to solve the following problems:

- If a node moves from one link to another without changing its IP address, it will be unable to receive packets at the new link.
- If a node changes its IP address when it moves, it will have to terminate and restart any ongoing connections each time it moves.

It accomplishes its task by setting up the routing tables in appropriate nodes, such that IP packets can be sent to mobile nodes not connected to their home link.

Mobile IP solves the above problems in a secure, robust and medium independent manner whose scaling properties make it applicable throughout the entire Internet. As a network-layer protocol it is completely independent of the media over which it runs. It is unique in its ability to accommodate heterogeneous mobility in addition to homogenous mobility (Solomon, 1998).

## Background

### 2.1 Preview

Mobile IP is a modification to IP that allows nodes to continue to receive datagrams no matter where they happen to be attached to the Internet. It involves some additional control messages that allow the IP nodes involved to manage their IP routing tables reliably. It is just as suitable for mobility across heterogeneous media as it is for mobility across homogeneous media. Mobile IP does not place any requirements on the link layer operation of a mobile node. This means that it is equally suitable to manage the mobility of a node no matter what the physical nature of the node's link to the Internet. Mobile IP introduces the following functional entities:

- **Mobile node:** A host or a router that changes its point of attachment from one network to another.
- **Home agent:** A router on the mobile node's home network that tunnels datagrams for delivery to the mobile node when it is away from home and maintains current location information for the mobile node.
- **Foreign agent:** A router on the mobile node's visited network that provides routing services to the mobile node while registered. It detunnels and delivers datagrams to the mobile node that were tunneled by the mobile node's home agent.

The basic mobile IP is a way of doing three relatively separate functions:

- Agent discovery (advertisement)
- Registration
- Tunneling

## 2.2 Agent Discovery

Home and foreign agents may advertise their availability on each link for which they provide service. A newly arrived mobile node can send a solicitation on the link to learn if any prospective agents are present. By agent discovery, a mobile node can determine whether it is currently connected to its home network or to a foreign network and detects when it has moved from one network to another. An agent advertisement is formed by including mobility agent advertisement extension in an ICMP router advertisement message. Hosts on a link must use the services of a directly attached router to deliver their datagrams to hosts on any other link. Determining the IP addresses of the locally attached router or routers was historically a matter of manual configuration. Router discovery provides the means by which IP hosts can determine the local routers' IP addresses and can monitor their continued presence. This is done by using two ICMP messages, one is transmitted by the routers where the other transmitted is by the hosts. More recently, it has become feasible to configure IP addresses by using DHCP (Perkins, 1998).

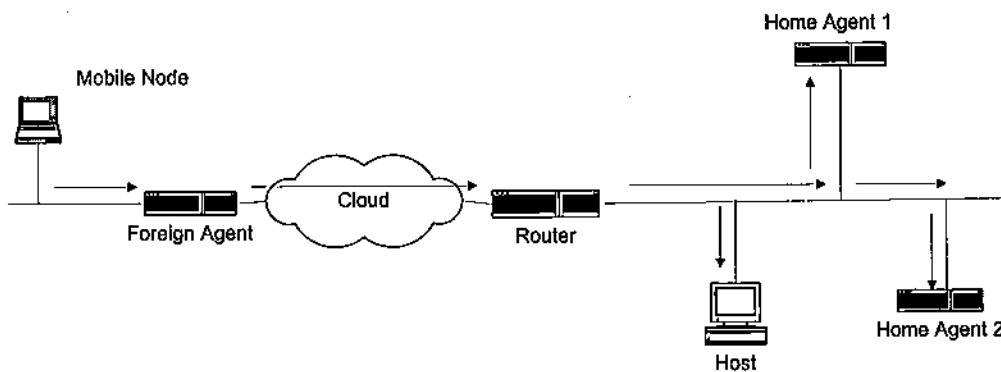
### 2.2.1 Agent Advertisement and Router Solicitation ICMP Messages

A mobility agent transmits agent advertisements to advertise its service on a link. An agent advertisement is an ICMP router advertisement that has been extended to carry mobility agent advertisement extension. Mobile nodes use these advertisements to determine their current point of attachment to the Internet. When an IP host needs timely information about local default routers, it can multicast or broadcast a router solicitation message. Any router in the vicinity that obeys the router discovery protocol will respond with a unicast router advertisement message sent directly to the soliciting host. After receiving the advertisement, the host responds just as if the advertisement were unsolicited and received at the broadcast or multicast address (Perkins, 1998).

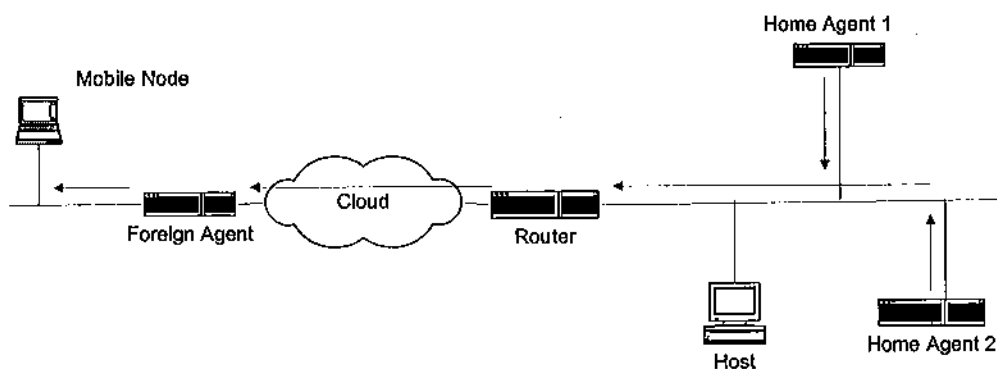


### 2.2.2 Automatic Home Agent Discovery

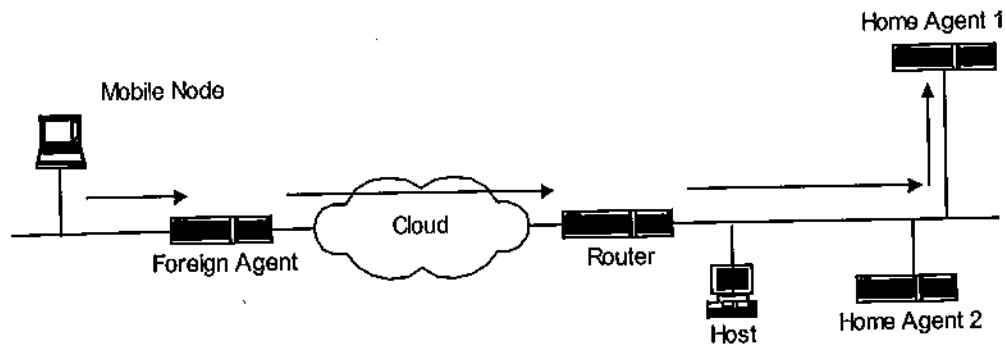
When the mobile node cannot contact its home agent, mobile IP has a mechanism that lets the mobile node try to register with another unknown home agent on its home network. The method of automatic home agent discovery works by using a broadcast IP address instead of the home agent's IP address as the target for the registration request. When the broadcast packet gets to the home network, other home agents on the network will send a rejection to the mobile node; however, their rejection notice will contain their address for the mobile node to use in a freshly attempted registration message. Note that the broadcast is not an Internet-wide broadcast, but a directed broadcast that reaches only IP nodes on the home network. This process is clarified in Figure (2.1).



(a) Mobile node broadcasts registration request to all nodes on the home link.



(b) Home agents reject the registration with their unicast IP address included in their replies.



(c) Mobile node processes the replies and registers with one of the home agents.

**Figure (2.1) Home Agent Discovery**

### 2.3 Registration

Registration is the method by which mobile nodes:

- Request forwarding services when visiting a foreign network.
- Inform their home agent with their current care-of address.
- Renew a binding that is due to expire.
- Deregister when they return home.
- Discover the address of the home agent if the mobile node is not configured with this information.
- Select certain alternative tunneling protocols.
- Maintain multiple simultaneous registrations so that a copy of each datagram will be tunneled to each active care-of address.
- Deregister certain care-of addresses while retaining others.

Registration messages exchange the mobile node's current binding information among a mobile node, its home agent, and a foreign agent. Registration creates or modifies a mobility binding at the home agent. Associating the mobile node's care-of address with the node's home address is called registration life time.

### 2.3.1 Registration Overview

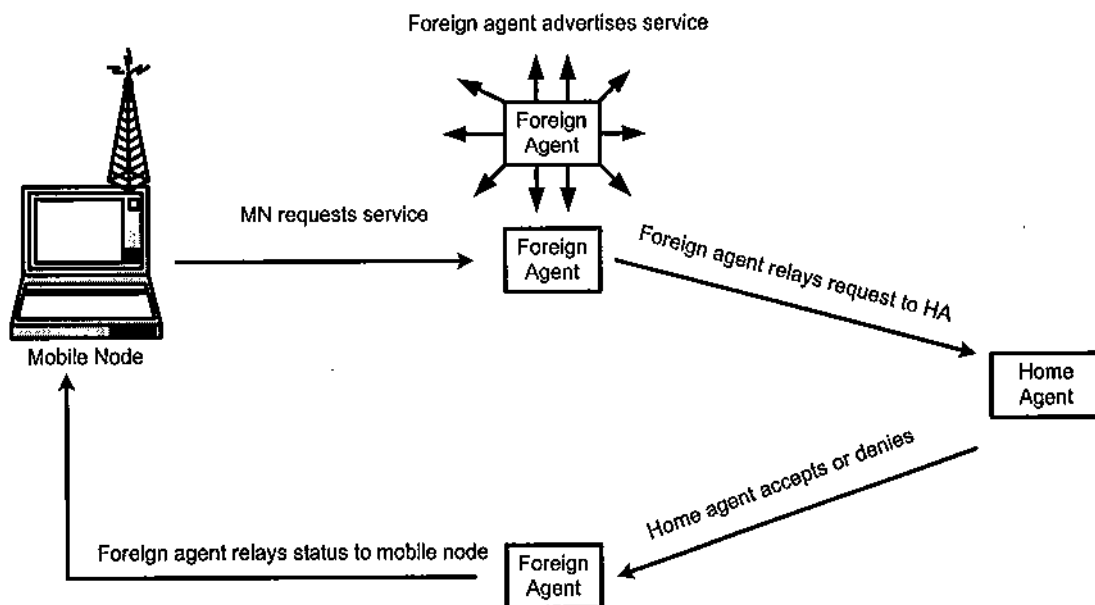
Mobile IP has two kinds of registration procedures, one by means of a foreign agent and the other without such any intermediary. Registration via a foreign agent requires the following messages as shown in Figure (2.2).

- Mobile host sends a registration request to the prospective foreign agent to begin the registration process.
- Foreign agent processes the registration request and relays it to the home agent whose address is provided by the mobile node in the request.
- The home agent sends a registration reply to the foreign agent to grant or deny the request.
- The foreign agent processes the registration reply and then relays it to the mobile node to inform it of the disposition of the request.

Direct registration requires only two messages:

- The mobile node sends a registration request to the home agent.
- The home agent sends a registration reply to the mobile node that grants or denies the request.

Mobile IP registration messages use the UDP (Postel, 1980). The overall data structure of the registration message is shown in Figure (2.3).



**Figure (2.2) Registration Process in Mobile IP**

IP header fields	UDP header	Mobile IP message header	Extensions
------------------	------------	--------------------------	------------

**Figure (2.3) Registration Message Structure**

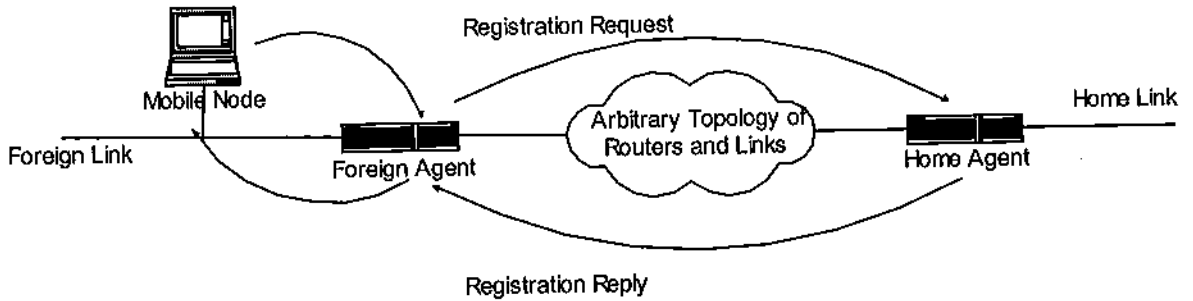
For each pending registration, the mobile node maintains the following information:

- The link-layer address of the foreign agent to which the registration request was sent.
- The IP destination address of the registration request.
- The care-of address used in the registration.
- The identification value sent in the registration.
- The originally requested life time.
- The remaining life time of the pending registration.

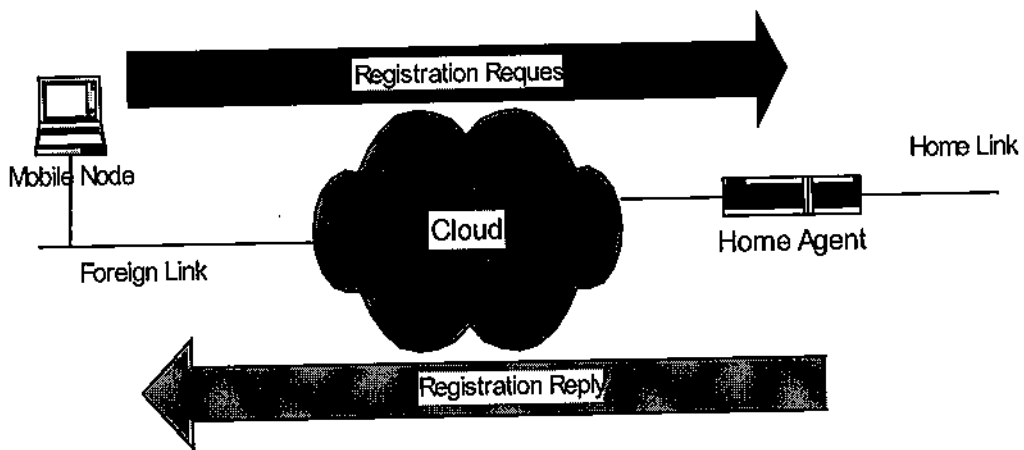
A mobile node should initiate a registration whenever it detects a change in its network connectivity.

### 2.3.1.1 Registration Scenarios

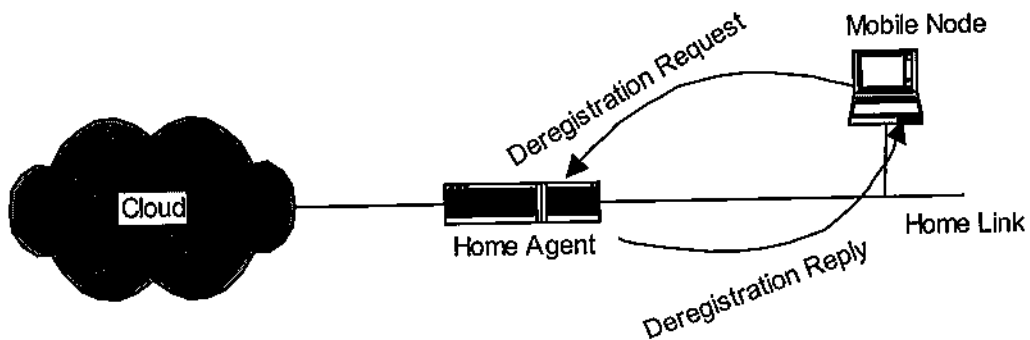
The three common scenarios for registration are shown in Figure (2.4).



(a) A mobile node registers on a foreign link using a foreign agent's care-of address



(b) A mobile node registers on a foreign link using a colocated care-of address



(c) A mobile node deregisters upon returning home

Figure (2.4) Registration Scenarios

### 2.3.2 Authentication

Authentication is the process by which a sending node proves its identity to the receiving node. Mobile IP requires each mobile node, home agent, and foreign agent to be able to support a mobility security association for mobile entities. When a home agent accepts a registration request from a mobile node, a binding is established and associated with the mobile node's home IP address, care-of address and a registration lifetime. Accordingly, registration request can also be called as binding update. The binding is valid till the lifetime expires. Because binding update is an example of a remote redirect, the binding cache is easily attacked when the registration is in progress. For instance, an end node may lose its connection, because a malicious user pretends to be the mobile node by attacking and sending a tricking binding update to the home agent (Teraoka and Tokoro, 1993).

In mobile IP mechanism, a foreign agent generally plays a passive role. Most of its jobs are just forwarding packets to either a home agent or a mobile node, and do the encapsulation and decapsulation as well. As a result, it is not recommended that foreign agents need a strong authentication function or a security association with a home agent or a mobile node. However, a strong security association is desired between a home agent and a mobile node. One of the existing authentication functions uses a 128-bit Message Digest 5 (MD5) keys to create a particular code to protect a registration request between a mobile node and a home agent. In order to keep the procedure of registration in secret and avoid that the code is captured and copied by a malicious user, the code has to be changed frequently and kept unique. There are two mechanisms to achieve this aim. One is by using timestamps, and the other is based on adopting Nonce (Pseudo-Random Numbers). When a home agent receives a binding update protected by using a timestamp, the binding update will be accepted only if the timestamp in the current binding update is greater and close to the one received in the previous one.

By using Nonce, every time a sender adds a new random number in the packet, the reply from the receiver must be authenticated by checking if it includes the same random number. In mobile IP, the home agent supposes to have the capability to generate a pseudo-random number to put in the high-order 32 bits of the identification field. Once the mobile node receives it, the high-order 32 bits of the identification field in the binding acknowledgement is copied into the high-order 32 bits of the same field in the binding update. Moreover, the mobile node needs to insert a new low-order 32 bits of the identification field in the binding update, which can be simply generated by doubling the high-order 32 bits of the identification field in the registration reply. The authentication in the registration request involves the following three operations:

- The foreign agent is required to check for the presence of a valid mobile-home authentication extension and perform the indicated authentication.
- The home agent is required to check that the registration identification field is correct using the context selected by the Security Parameter Index (SPI) within the mobile home authentication extension.
- The home agent is required to check for the presence of a valid foreign-home authentication extension.

### **2.3.3 Replay Protection for Registration Requests**

The identification field is used by the home agent to verify that a registration message has been freshly generated by the mobile node. Two methods are used: Timestamps and Nonce. Whatever method is used, the low-order 32 bits of the identification are required to be copied unchanged from the registration request to the reply. The mobile node is required to verify that the low-order 32 bits of any registration reply are identical to the bits it sent in the registration request.

The basic idea of timestamp replay protection is that the node generating a message inserts the current time of day, and the receiving node checks that this timestamp is close to its time of day, given that the two nodes have synchronized clocks. Using timestamps the mobile node sets the identification field to a 64-bit value formatted as specified by the Network Time Protocol (NTP) (Mills, 1992). The low-order 32 bits of the NTP represent fractional seconds. On receipt of a registration request with a valid mobile-home authentication extension, the home agent is required to check the identification field for validity. To be valid the timestamp contained in the identification field is required to be:

- Close to the home agent's time-of-day clock.
- Greater than all previously accepted timestamps for the requesting node.

If the timestamp is valid, the home agent copies the entire identification field into the registration reply. If it is not valid, the home agent copies only the low-order 32 bits into the registration reply and supplies the high-order 32 bits from its own time-of day.

Using Nonce replay protection, the basic idea is that node A includes a new random number in every message to node B, and checks that node B returns the same number in its next message to A, both messages use an authentication code to protect against alternation by an attacker (Jacobs, 1997).

#### **2.3.4 Home Agent Receiving and Processing of Registration**

Home agent plays an active role in the registration process. The home agent receives registration requests from the mobile node, either directly or relayed by a foreign agent, updates its record of the mobility bindings for this mobile node, and issues a suitable registration reply in response to each. A home agent is not allowed to transmit a registration reply except when replying to a registration request received from a mobile node. The home agent is required to be configured with the home address and mobility



With the fields defined as follows:

Type: Registration request; S: Simultaneous binding; B: Broadcast datagram;  
 D: Decapsulation; M: Minimal encapsulation; G: Generic record encapsulation;  
 V: Van Jacobson header compression; RSV: Reserved bit.

Lifetime: The period remaining before the registration is expired.

Home address: IP address of the mobile node.

Home agent: IP address of the mobile node's home agent.

Care-of address: IP address of the tunnel end point.

Identification: A 64-bit number constructed by the mobile node and used for matching registration requests with registration replies, as well as for protection.

Extensions: What follows the fixed portion of the registration request.

Mobility agents return a registration reply messages to a mobile node that has sent a registration request message. Figure (2.6) shows the format of this reply.

Type	Code	Lifetime
Home address		
Home agent		
Identification		
Extensions		

**Figure (2.6) Packet Format of Registration Reply**

Fields have the same explanations as for the registration request, while the code field has a value indicating the result of the registration request (Perkins, 1996).

### 2.3.6 Registration Extensions

Three registration extensions are defined in the base mobile IP protocol, all of which allow additional security measures to be applied to the registration process. These extensions are:

- Mobile-home authentication extension.
- Mobile-foreign authentication extension.
- Foreign-home authentication extension.

Each extension includes an SPI that indicates the mobility security association that contains the secret and the other information needed to compute the authenticator. Each of the extensions defined above has the format illustrated in Figure (2.7) with fields defined as follows:

Type: One of the three extensions mentioned above.

Length: 4 plus the number of bytes in the authenticator.

SPI: Four bytes; an opaque identifier.

Authenticator: Variable length, depending on the SPI.

Type	Length	SPI
SPI (continued)		Authenticator

**Figure (2.7) Packet Format of Mobile-Home Authentication Extension**

## 2.4 Datagrams Delivering (Tunneling)

When a mobile node is away and some packets are addressed to the mobile node's home address, the packets will be intercepted by the mobile node's home agent. Before being tunneled to the foreign agent, the packets have to be encapsulated by the home agent. Each original packet will be modified and attached with an additional outer header. Its destination address is set to the foreign agent's address. Mobile IP requires the use of encapsulation to deliver datagrams from the home network to the care-of address of the mobile node. Three types of encapsulation (tunneling) are supported by mobile IP:

- Minimal encapsulation.
- IP-in-IP encapsulation.
- The Generic Record Encapsulation (GRE).

In the most general tunneling case, the source, encapsulator, decapsulator, and destination are separate nodes. Figure (2.8) shows a general tunneling case.

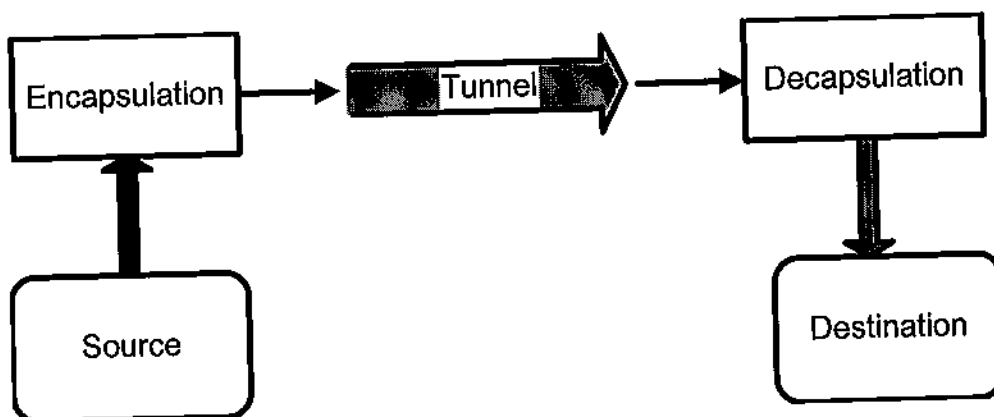


Figure (2.8) Tunneling

Mobile IP requires each home agent and foreign agent to support tunneling datagrams using IP-in-IP encapsulation (Perkins, 1996a). Mobile nodes that use collocated care-of address are required to support IP-in-IP encapsulation.

### 2.4.1 IP-in-IP Encapsulation

To encapsulate an IP datagram using this method:

- An outer IP header is inserted before the datagram's existing IP header as shown in Figure (2.9).

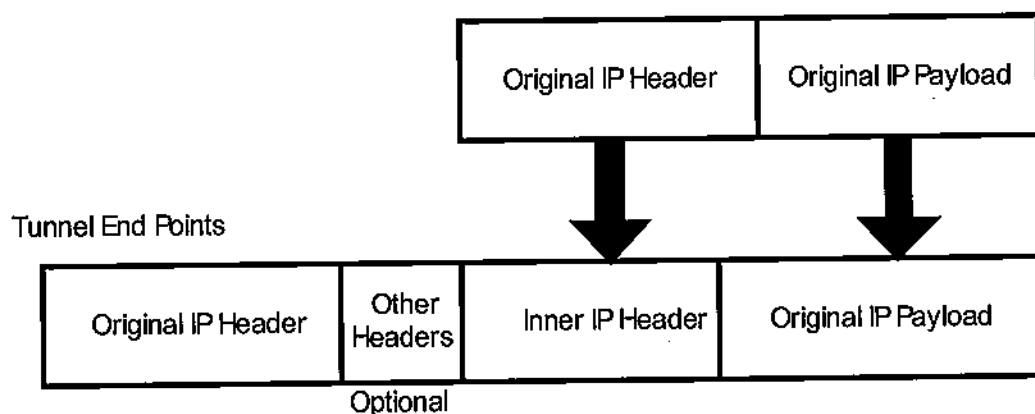


Figure (2.9) IP-in-IP Encapsulation

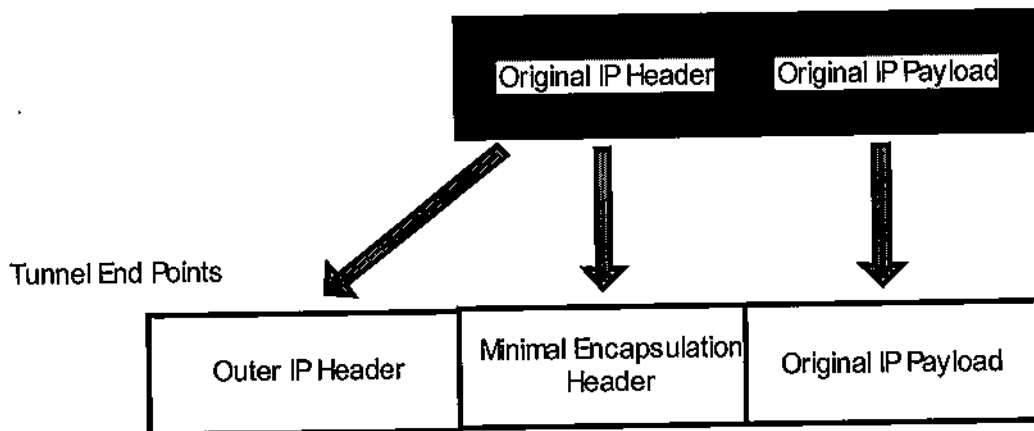
- The outer IP header source address and destination address identify the end points of the tunnel.
- The inner IP header source address and destination address identify the original and recipient of the datagram.
- The inner IP header is not changed by the encapsulation and remains unchanged during its delivery to the tunnel exit point. No change to IP options in the inner header occurs during delivery of the encapsulated datagram through the tunnel.

- Sometimes, other protocol headers such as the authentication headers (Kent, 1997a) may be inserted between the outer IP header and the inner IP header.
- The security options of the inner IP header may affect the choice of the security options for the outer IP header.

Applying IP-in-IP encapsulation at least enlarges the size of the packet by 20 bytes.

#### 2.4.2 Minimal Encapsulation

Using IP headers to encapsulate IP datagrams requires the duplication of several fields within the inner IP header. To overcome this and save some additional space, minimal encapsulation is used. To encapsulate an IP datagram using minimal encapsulation, the minimal forwarding header is inserted into the datagram after the IP header, followed by the unmodified IP payload of the original datagram, as shown in Figure (2.10).



**Figure (2.10) Minimal Encapsulation**

The following modifications are done on the original IP header:

- For minimal encapsulation, the protocol field in the IP header is replaced by protocol number 55.
- The source address field in the IP header is replaced by the IP address of the encapsulator if the encapsulator is not the original source of the datagram.

- The header checksum field in the IP header is recomputed or updated to account for the changes in the IP header described for encapsulation.
- The destination address field in the IP header is replaced by the IP address of the exit point of the tunnel.
- The total length field in the IP header is incremented by the size of the minimal forwarding header added to the datagram.

The general form of the minimal encapsulator header is shown in Figure (2.11).

Protocol	S	Reserved	Header checksum
Original destination address			
Original source address			

**Figure (2.11) Header Format of Minimal Encapsulation**

To decapsulate the datagrams:

- The forwarding header is removed from the datagram.
- The fields in the minimal forwarding header are restored to the IP header.
- The total length field of the IP header is decremented by the size of the removed minimal forwarding header.
- The checksum field in the IP header is updated to reflect the new values in the fields of the IP header.

### 2.4.3 Generic Record Encapsulation

GRE can encapsulate numerous other protocols besides IP, and so, it is more general than the previous two encapsulation methods. The encapsulated packet format of this type is shown in Figure (2.12)

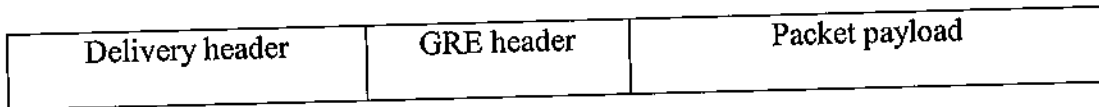


Figure (2.12) Packet Structure of GRE

### 2.5 Proxy Address Resolution Protocol (ARP) and Gratuitous ARP

A proxy ARP is an ARP reply sent by one node on behalf of another node that is either unable or unwilling to answer its own ARP requests. The sender of a proxy ARP reverses the sender and target protocol address fields, but supplies some configured link-layer address in the sender hardware address field. The node receiving the reply associates this link-layer address with the IP address of the original target node, causing it to transmit future datagrams for this target node to the node with that link-layer address.

A gratuitous ARP is an ARP packet sent by a node to update other node's ARP caches. It may use either an ARP request or an ARP caches. In either case, the ARP sender protocol address and the ARP target protocol address are both set to the IP address of the cache entry to be updated, and the ARP sender hardware address is set to the link-layer address to which this cache entry should be updated.

As a result, the function of proxy ARP and gratuitous ARP are to help home agents to intercept packets addressed to mobile node's home addresses when the mobile nodes are away. After accepting a registration request from the mobile node, the home agent informs other routers located within the same network of receiving packets addressed to the mobile node on behalf of the mobile node. To do so, the home agents floods

gratuitous ARP message around the home network, and makes use of proxy ARP to reply to any ARP request on behalf of the mobile node. When other routers receive these two types of ARP messages, their ARP caches will be updated. The gratuitous ARP should be broadcasted several times in order to raise the reliability. Afterwards, the home agent should be able to collect all the packets addressed to the mobile node's home address while the mobile node is away.

## 2.6 Triangle Route and Route Optimization

Packets that are sent by a correspondent to a mobile node connected to a foreign link are routed first to the mobile node's home agent and then tunneled to the mobile node's care-of address. Whereas, packets sent by the mobile node are routed directly to the correspondent. This is known as a triangle problem as shown in Figure (2.13). Route optimization extensions are introduced to:

- Enable nodes that implement them to cache the binding of a mobile node and then to tunnel datagrams directly to the care-of address indicated in that binding.
- Allow datagrams in flight to be forwarded directly to the mobile node's new care-of address.

Route optimization is divided into four parts:

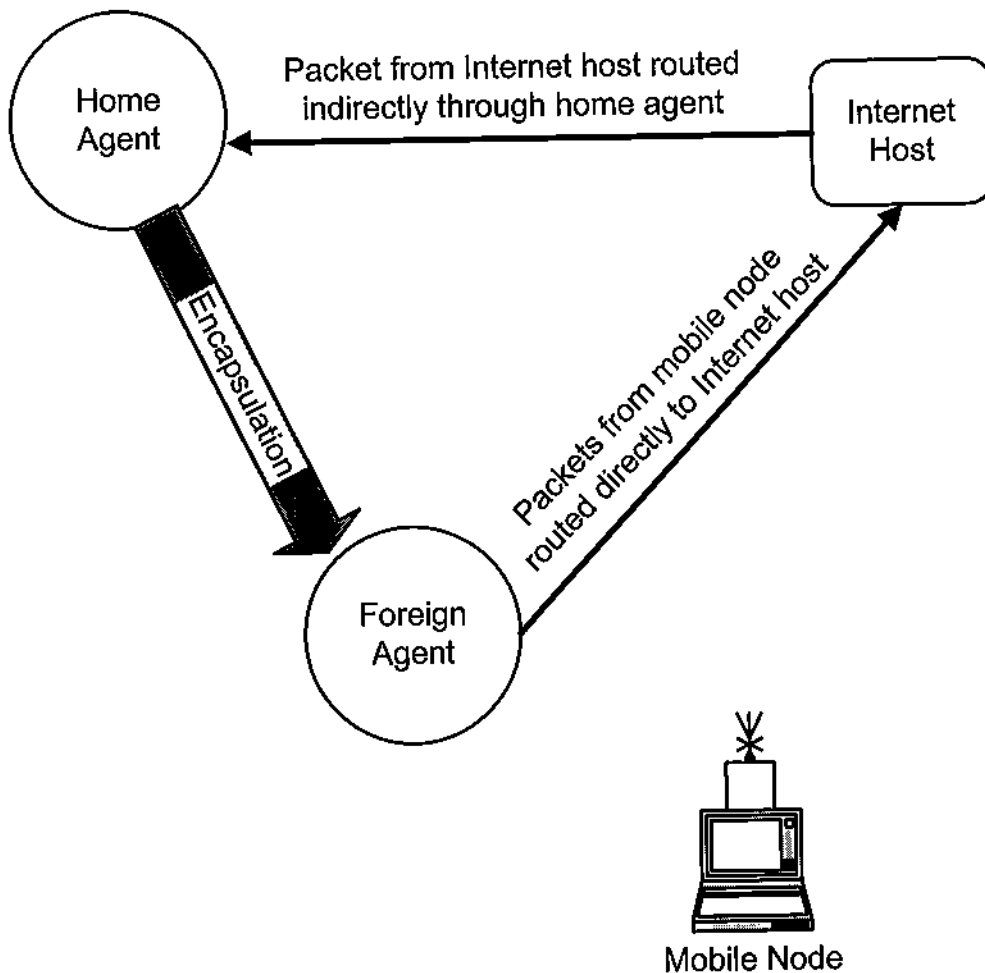
- a) Updating binding caches: A binding cache is a cache of mobility bindings of mobile nodes maintained by a node for use in tunneling datagrams to mobile nodes, a binding update is a message indicating mobile node's current care-of address.
- b) Managing smooth handoffs between foreign agents: Route optimization provides a means for the mobile node's previous foreign agent to be notified for the mobile node's new mobility binding, allowing datagrams in flight to the mobile node's previous foreign agent to be forwarded to its new care-of address.



This notification allows also any datagram tunneled to the mobile node's previous foreign agent, without of date binding cache entries for the mobile node, to be forwarded to its new care-of address. Finally, this notification allows any resources consumed by the mobile node at the previous foreign agent to be released immediately, rather than waiting for its registration life time to expire.

c) Acquiring registration keys for smooth handoffs: To perform securely the operations needed for smooth handoffs from one agent to the next, any agent should require assurance that it is getting authentic handoffs information. The following methods are used to establish a registration key with the mobile node during the registration process:

- If the mobile node and foreign agent or home agents share a security association, or can establish such association using Simple Key Internet Protocol (SKIP), the foreign/home agents can choose the new registration key.
- If the mobile node includes its public key in its registration request, the foreign/home agents can choose the new registration key.



**Figure (2.13) Triangle Route**

- The mobile node and its foreign/home agents can execute a Diffie-Hellman key exchange protocol (Diffie and Hellman, 1976) as part of the registration protocol.

Once the registration key is established, performing smooth handoffs will be done smoothly.

- d) Using special tunnels: This method allows the home agent to see the address of the node that tunneled the datagram and to avoid tunneling the datagram back to the same node. It also allows home agent to avoid possible routing loop when a foreign agent has forgotten that it is serving as the mobile node's foreign agent (Perkins and Johnson, 1999).

## 2.7 General Home/Foreign Agents Operations

The major duties of home agent are:

- Home agent rate limiting: It is the mechanism used by the home agent to limit the rate at which it sends binding update messages to the same node about given mobility binding.
- Receiving registration key requests.
- Mobility security association management.
- Using a master key: With a master key, the home agent could build a key for any given node by computing the node-specific key.
- Supplying registration keys: When the home agent receives a registration request message with registration key extension, it either selects or encodes a registration key for mobile node and foreign agent or it transcribes the registration key already selected by the foreign agent into the appropriate extension to the registration reply message.

For the foreign agent to support smooth handoffs, it must:

- Process previous notification messages.
- Maintain up-to-date binding cache entries.
- Use foreign agent algorithm to establish registration keys.
- Be able to use special tunnels.

## 2.8 Movement Detection

Mobile nodes can utilize three methods to detect their movement from one subnet to another:

- 1) Lazy cell switching: This method is based on the lifetime field within the main body of the ICMP router advertisement portion of the agent advertisement. If the agent advertisement is expired and the mobile node has not received any

other advertisement from the same agent, the mobile node will be sure that it moved to another network.

- 2) **Prefix matching:** The prefix-length extension may be used by a mobile node to determine whether a newly received agent advertisement was received on the same subnet as the mobile node's current care-of address. If the prefix differs, this will indicate movement. This method should not be used in the advertisement sent over wireless links, due to irregular coverage areas provided by wireless transmitters.
- 3) **Eager cell switching:** This method is preferred when mobile node can detect beacons from multiple foreign agents simultaneously. In wireless communication environment, the covered areas of the cell are partly overlapped. A mobile node can decide to change its foreign agent when entering a new cell, and therefore, keeps the registration with the foreign agent that resides in the newest cell (Thomson and Narten, 1998).

## 2.9 Smooth Handoffs

In the wireless communication environment, a mobile node might need to frequently register to a new foreign agent. For example, a businessman keeps using his laptop to fetch files from his company on a moving train. Because the basic mobile IP mechanism does not have a cure for frequently changing mobile node's attachment, this frequent registration to the foreign agent will cause packets addressed to the out-of-date mobile node's care-of address to be lost. Some packets are lost in flight before the mobile node registers its new care-of address to the home agent. Others are lost because correspondent nodes have the out-of-date binding entry for the mobile node. A simple and obvious means is to let the previous foreign agent know the mobile node's current care-of address as soon as possible when the mobile node just moved to another foreign network. In this circumstance, the previous foreign agent only plays a role of a forwarding pointer, and re-tunnels packets to the mobile node.

When the mobile node gets into another foreign network, the previous foreign agent is notified of the mobile node's current care-of address as a part of the registration request procedure. The registration request, sent by the mobile node, will be expanded with a previous foreign agent notification extension. Once receiving the registration request, the foreign agent can be aware that the mobile node just moved in from another foreign network, and sends a binding update to the previous foreign agent. This process needs an acknowledgement message returned from the previous foreign agent. Afterwards, packets tunneled to the previous foreign agent will be able to be re-tunneled to the mobile node's current care-of address.

In order to have a higher reliability, it is necessary to avoid that packets are discarded when the previous foreign agent has not yet had a binding entry of the mobile node's care-of address. A solution which addressed this problem is called special tunnel. By applying this mechanism, the previous foreign agent is able to re-tunnel the packets to

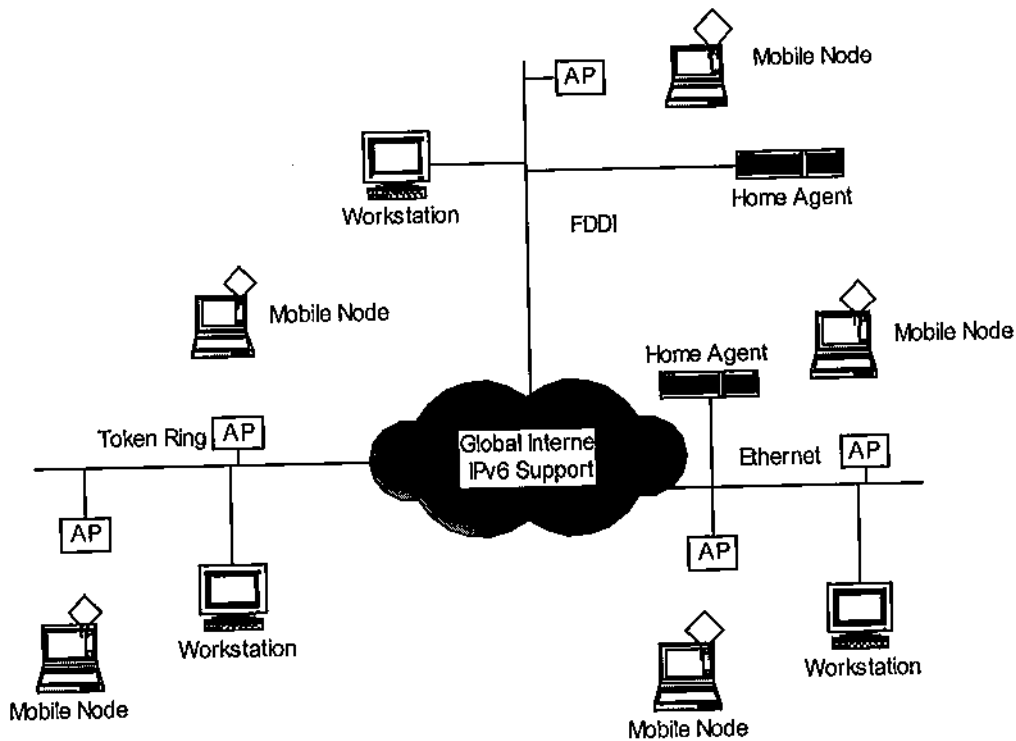
the home agent after realizing that the binding entry or the visitor list entry for the mobile node does not exist. Besides, the previous foreign agent also needs to send a binding warning to the home agent to inform that the correspondent node has an out-of-date binding entry for the mobile node.

However, the home agent will not tunnel these packets to the mobile node until ascertaining that the address of the previous foreign agent and the mobile node's current care-of address are not the same. If they are not the same, the home agent will discard these packets. This possibly happens when the previous foreign agent loses the visitor list and the mobile node still attaches to the same foreign network. For example, the foreign agent just crashed and rebooted (Soliman and Malki, 2000).

### **2.10 Mobile IP Version 6**

How will mobile IP change when IP version 6 is adopted? IPv6 includes many features for streamlining mobility support that are missing in IPv4 (current version), including stateless address auto-configuration and neighbor discovery. IPv6 also attempts to drastically simplify the process of renumbering, which could be critical to the future routability of the Internet. Because the number of mobile computers accessing the Internet will likely increase, efficient support for mobility will make a decisive difference in the Internet's future performance. This, along with the growing importance of the Internet and the Web, indicates the need to pay attention to supporting mobility.

Mobility support in IPv6, as proposed by the mobile IP working group, follows the design for mobile IPv4. It retains the ideas of a home network, home agent, and the use of encapsulation to deliver packets from the home network to the mobile node's current point of attachment. While discovery of a care-of address is still required, a mobile node can configure its care-of address by using stateless address auto-configuration and neighbor discovery. Thus, foreign agents are not required to support mobility in IPv6. An overview of the entities of mobile IPv6 is shown in Figure (2.14).



**Figure (2.14) Entities of Mobile IPv6**

In Figure (2.14), AP stands for access point which is the point at which mobile node may connect to IPv6 Internet, this entity formerly serving as foreign agents.

### 2.11 Route Optimization in Mobile IPv6

The basic idea underlying route optimization is that the routes to mobile nodes from their correspondent nodes can be improved if the correspondent node has an up-to-date mobility binding for the mobile node in its routing table. IPv6 mobility borrows heavily from the route optimization ideas specified for IPv4, particularly the idea of delivering binding updates directly to correspondent nodes. When it knows the mobile node's current care-of address, a correspondent node can deliver packets directly to the mobile node's home address without any assistance from the home agent, and so, eliminating the triangle routing problem. Route optimization is likely to dramatically improve performance for IPv6 mobile nodes. It is realistic to require this extra functionality of all IPv6 nodes for two reasons. First, on a practical level, IPv6 standards documents are still at stages of test and standardization, so it is possible to place additional

requirements on IPv6 nodes. Second, processing binding updates can be implemented as a fairly simple modification to IPv6's use of the destination cache.

### **2.12 Security**

One of the biggest differences between IPv6 and IPv4 is that all IPv6 nodes are expected to implement strong authentication and encryption features to improve Internet security. This affords a major simplification for IPv6 mobility support, since all authentication procedures can be assumed to exist when needed and do not have to be specified in the mobile IPv6 protocol. Even with the security features in IPv6; however, the current working group draft for IPv6 mobility support specifies the use of authentication procedures as infrequently as possible. The reasons for this are two fold. First, good authentication comes at the cost of performance and so should be required only occasionally. Second, questions about the availability of Internet-wide key management are far from resolved now (Bhagwat, Perkins, and Tripathi, 1996).

### **2.13 Source Routing**

In contrast to the way in which route optimization is specified in IPv4, in IPv6 correspondent nodes do not tunnel packets to mobile nodes. Instead, they use IPv6 routing headers, which implement a variation of IPv4's source routing option. A number of early proposals for supporting mobility in IPv4 specified a similar use of source routing options, but two main problems precluded their use:

- IPv4 source routing options require the receiver of source-routed packets to follow the reversed path to the sender back along the indicated intermediate nodes. This means that malicious nodes using source routes from remote locations within the Internet could impersonate other nodes, a problem exacerbated by the lack of authentication protocols.



- Existing routers exhibit terrible performance when handling source routes. Consequently, the results of deploying other protocols that use source routes have not been favorable.

However, the objections to the use of source routes do not apply to IPv6, because IPv6's more careful specification eliminates the need for source-route reversal and lets routers ignore options that do not need their attention. Consequently, correspondent nodes can use routing headers without penalty. This allows the mobile node to easily determine when a correspondent node does not have the right care-of address. Packets delivered by encapsulation instead of by source routes in a routing header must have been sent by correspondent nodes that need to receive binding updates from the mobile node. It is a further point of contrast to route optimization in IPv4 that, in IPv6 mobility support, the mobile node delivers binding updates to the correspondent nodes instead of the home agent. In IPv6, key management between the mobile node and correspondent node is more likely to be available.

Other features supported by IPv6 mobility include:

- Coexistence with Internet ingress filtering.
- Smooth handoffs, which in Mobile IPv4, is specified for foreign agents as part of route optimization.
- Renumbering of home networks.
- Automatic home agent discovery.

Table (2.1) summarizes the main differences between mobility of IPv6 and IPv4.

Table (2.1) Mobility Differences between IPv6 and IPv4

Mobile IPv4 Concepts	Mobile IPv6 Concepts
Mobile nodes, home agents, home links, foreign links	No difference
Mobile node's home address	Globally routable home address and link local home address
Foreign agent	No foreign agents
Foreign agent care-of address, collocated care-of address	All care-of address are collocated
Care-of address are obtained via agent discovery, DHCP, or manually	Obtained via stateless address auto-configuration, DHCP, or manually
Agent discovery	Router discovery
Authenticated registration with home agent	Authenticated notification of home agent and other correspondents
Routing to mobile nodes via tunneling	Routing to the mobile nodes via tunneling and source routing
Route optimization via separate protocol specification	Integrated support for route optimization

### 2.13 Mobility Attach Schedule Using Mobile IPv6

The operation of mobile IPv6 can be summarized as follows:

- A mobile node determines its current location using the IPv6 version of router discovery.
- The mobile node acts as any fixed host or router when connected to its home link.
- Otherwise, when connecting to a foreign link, mobile node uses IPv6 defined address auto-configuration to acquire a collocated care-of address on the foreign link.
- The mobile node notifies its home agent of its care-of address.
- The mobile node also reports its care-of address to correspondents assuming it can do so securely.
- Packets sent by correspondents that are ignorant of the mobile node's care-of address are routed just as in mobile IPv4; specifically, they are routed to the mobile node's home network, where the home agent tunnels them to the care-of address.
- Packets sent by correspondents that know the mobile node's care-of address are sent directly to the mobile node using an IPv6 routing header, which specifies the mobile node's care-of address as an intermediate destination.
- In the reverse direction, packets sent by the mobile node are routed directly to their destination using no special mechanisms.

## 2.14 Location and Movement Detection in Mobile IPv6

The mobile node examines the network-prefix contained in the received advertisement. If any of these prefixes match the network-prefix of the mobile node home address, then the mobile node is connected to its home link. Otherwise, if none of the prefixes matches the network-prefix of the mobile node's home address, then the mobile node is connected to a foreign link. At this point the mobile node compares the prefix in the most recently received advertisement with those of previous advertisements to see if it has moved. If the mobile node has moved, then it should acquire a care-of address at the new link. Once it acquires a care-of address it should inform both its home agent and appropriate set of correspondents of its new care-of address. Mobile node obtains care-of address at the foreign link by two methods:

- **Stateful address auto-configuration:** In this method the mobile node simply asks a server for an address and uses that address as a care-of address. The protocol used to do this is the DHCP.
- **Stateless address auto-configuration:** The mobile node forms an interface token, a link-dependent identifier for the interface by which it connects to the foreign link. The interface token is typically the node's link layer address on that interface. The mobile node examines the prefix information options that are contained within router advertisement to determine the valid network- prefix on the current link. The mobile node forms a care-of address by concatenating one of the valid network-prefixes with the interface token (Thomson and Narten, 1998).

561395

## 2.15 Notification

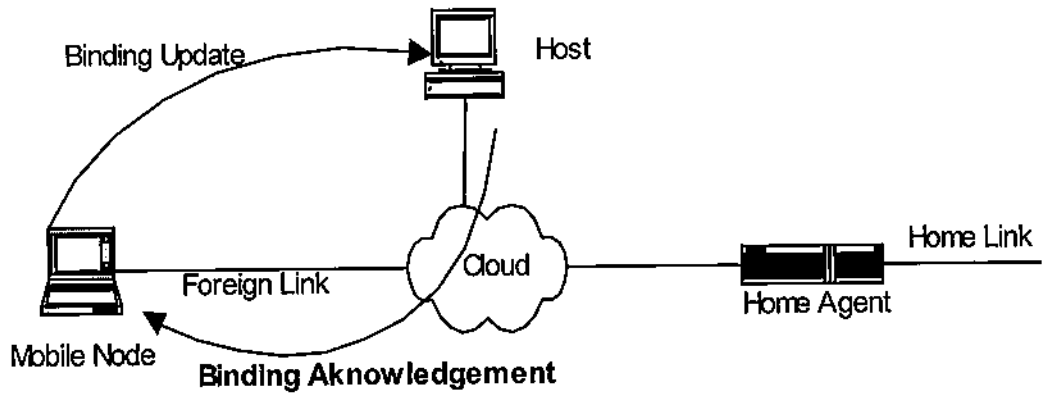
Notification is the method, used in mobile IPv6, by which a mobile node informs its home agent and various correspondent nodes of its current care-of address. Home agent uses the care-of address as the exit point of the tunnel to get packets to the mobile node when it is connected to a foreign link, where correspondent nodes use the care-of address to route packets directly to the mobile node without requiring the packets to be routed through the home agent. Mobile IPv4 notification consists of a simple exchange of messages, There are three messages used by mobile IPv6:

binding update, binding acknowledgement and binding request where:

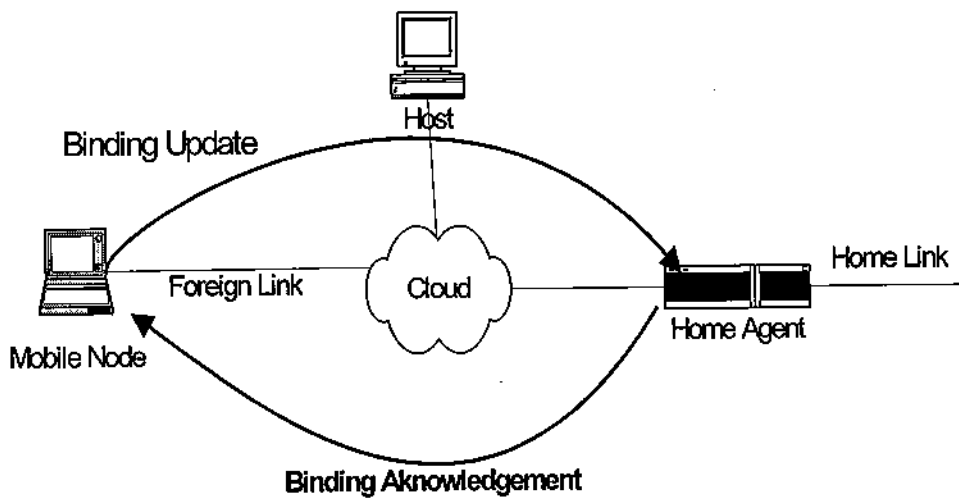
- **Binding update:** A message sent by a mobile node to its home agent or correspondent node to inform them of its current care-of address.
- **Binding acknowledgement:** A message sent to a mobile node from home agent or correspondent nodes to indicate that binding updates are received successfully.
- **Binding request:** A message sent by the correspondent node to the mobile node to request that the mobile node sends a binding update message (Deering and Hidden, 1996).

## 2.17 Notification Scenarios

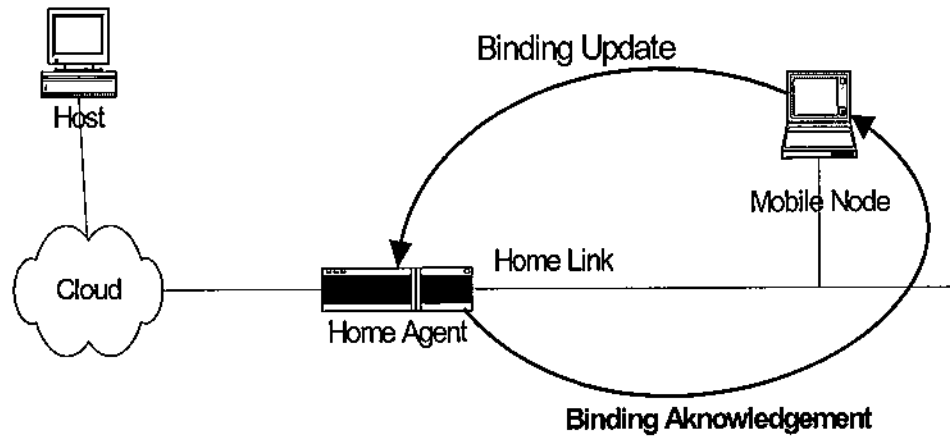
The message exchange for common scenarios is shown in Figure (2.15).



(a) A mobile node connects to a foreign link and informs a correspondent node of its new care-of address.



(b) A mobile node connects to a foreign link and informs its home agent of its new care-of address.



(c) A mobile node returns to its home link and informs its home agent that it is no longer attached to a foreign link.

**Figure (2.15) Message Exchange in Mobile IPv6**

In mobile IPv6 correspondent node that knows a mobile node's care-of address sends packets directly to the mobile node using an IPv6 routing header. If a correspondent node doesn't know a mobile's node care-of address, then it sends packets to the mobile node just as it would send packets to any other fixed node. A packet this way, will be routed towards the mobile node's home link the same way as in mobile IPv4. When a mobile node is connected to a foreign link, it can select any router on the foreign link from which it has received router advertisements, it configures its routing table so that all packets it generates are sent to this router.

### 2.18 Home Subnet Renumbering

Network renumbering is necessary when a whole subnet switches to another network. There is no problem for all the nodes currently connected to the home subnet to get a new address via either stateful or stateless IP address auto-configuration. However, mobile nodes away from their home network need some additional assistance to realize the change of the home network-prefix. For all fixed nodes on the home subnet, they are informed by receiving a multicast router advertisement which includes the new prefix of the home network. To extend renumbering to mobile nodes away from home, their home agent is required to tunnel a multicast router advertisement renumbering

packets to the care-of address of each mobile node. When a mobile node receives a tunneled router advertisement containing a new home network prefix, it must use address auto-configuration via the home agent to create its new home address. Once returning home, mobile node is required to use duplicate address detection to assure that no neighbor is using the same address before deregistering the binding with its home agent (Johnson and Perkins, 1999).

### **2.19 Mobility Requirements**

To be mobile, the mobile node has to be able to detect when it needs a new care-of address. In addition, it needs to determine when to transmit binding updates to their correspondent nodes and their home agents. Lastly, the mobile node has to be able to decapsulate packets sent to it by the home agent when correspondent nodes have no valid binding for the mobile node, and to process binding acknowledgment and binding request destination options. For a router to offer home agent services, it is required to perform encapsulation and proxy neighbor advertisements, in addition to process binding update. For better availability in the face of home agent crashes, it is preferable for home agent to maintain in a nonvolatile storage list of the current bindings for mobile hosts on its home network.

### **2.20 Mobile IP and DHCP**

DHCP can be used by a mobile node to obtain a care-of address without a redundant foreign agent co-operation. DHCP server also allows the mobile node to have more than one IP address assigned to it, especially when the mobile node can exist within range of more than wireless access point at the same time. To obtain a care-of address from a DHCP server, the mobile node can proceed as follows:

- Mobile node sends a DHCP discovery message to the link to which it is currently attached, and waiting to receive a DHCP offer.



- Once an offer is received, mobile node completes DHCP request and waits for acknowledgment.
- After the reply is received, the mobile node then initiate mobile IP registration request with the newly acquired care-of addresses.
- Mobile node uses the care-of address as the source address on the registration request and receives a registration reply from home agent with no need for foreign agent.
- DHCP provides an extra option, which enables mobile hosts to configure themselves automatically when they are not preconfigured with a home address. This option enables a mobile host to derive a mobile home address to determine the subnet mask of the home network. Of course, the mobile node needs to be DHCP client to use this method (Bound and Perkins, 1999).

## 2.21 Applying Mobile IP

A given computer network can be transformed into one which supports mobile IP by upgrading all of the routers to be both home agents and foreign agents and by installing mobile node software on the hosts. Specifically, the functions that must be performed to upgrade the network to support mobile IP can be summarized as follows:

- Mobile node software is installed on every host computer that is relatively portable such as notebook computers.
- Home and foreign agent software is installed on all of the routers in the network.
- Each mobile node is assigned a home link, a home address, and a home agent. The mobile nodes of the home link would be given IP home address whose network-prefix is equal to the network-prefix assigned to that link, and the router that connects to that link would be the mobile node's home agent.
- A shared secret key is configured between each mobile node and its home agent.
- For managing mobile nodes, home agents and foreign agents on the network, mobile IP Management Information Base (MIB) can be used. MIB defines a set of variables which can be examined or modified remotely (Solomon, 1998).

## Mobile IP and Other Protocols

### 3.1 Mobile IP Security

Security, in general, involves the following topics:

- Confidentiality: Transforming data such that, it can be decoded by authorized parties.
- Authentication: Proving or disproving someone's claimed identity.
- Integrity checking: Ensuring that data can't be modified without such modification being detectable.
- Non-reproduction: Proving that a source of data did in fact send data that the source might later deny sending.

Cryptography is the technology used to accomplish all of the above security features.

Cryptographic systems consist of two basic components:

- An algorithm: Which is a complicated mathematical function.
- Keys: Which are a chunk of binary data that are known only to the parties which wish only to communicate securely.

Mobile IP allows mobile node and home agent to use any authentication algorithm they choose. However, all implementations must support the default algorithm of Keyed Message Digest "Keyed MD5". It is a special set of cryptographic algorithms used to provide secret keys for authentication. It takes a large chunk of data (message) and computes from it a fixed length (smaller) chunk of data called message digest. Using Keyed MD5 mobile IP works as follows:

- Mobile node generates registration request consisting of the fixed length portion and the mobile authentication extension. Mobile node fills in all of the fields of the request and extension except for the authentication field.

- Mobile node computes an MD5 message digest over a sequence of bytes that includes:
  - a) The shared secret key which is known to the mobile node and its home agent.
  - b) The fixed length portion of the registration message.
  - c) All extensions, including the fields of the mobile-home authentication, but the authentication field itself.
  - d) The shared secret key again.
- The output of the MD5 computation is a 16-byte message digest that the mobile node places within the authenticator field of the mobile-home authentication extension. Mobile node sends the complete registration request to its home agent.
- After receiving the request, home agent computes its own message digest using the shared secret key and the fields of the registration request.
- If the computed message digest is equal to the one received within the authenticator field from the mobile node, the home agent knows that the request is surely sent by the mobile node.
- The inverse of the procedure described above happens when the home agent returns a reply to the mobile node (Rivest, 1992)

The procedure described above is shown in Figure (3.1).

### 3.1.1 Preventing Replay Attacks

Replay attack is the process by which unauthorized person can store a copy of an authenticated or encrypted message and retransmitting that message at a later time. To prevent this, mobile node can generate a unique value for the identification field in each

successive attempted registration. Mobile IP uses two ways in which the identification field can be chosen:

- **Timestamps:** Mobile node uses its current estimate of time and date-of-day in the identification field. If this estimate is not sufficiently close to the home agent's estimate of current time, then it rejects this registration request and sends the mobile node an information to synchronize its clock with the home agent clock.
- **Nonce:** Mobile node specifies to the home agent the value that the home agent must place in the lower half of the identification field in the next registration reply. The same thing is done by the home agent. If either nodes receives a registration message in which the identification field does not match this next expected value, then the message is rejected in the case of home agent and ignored in the case of mobile node.

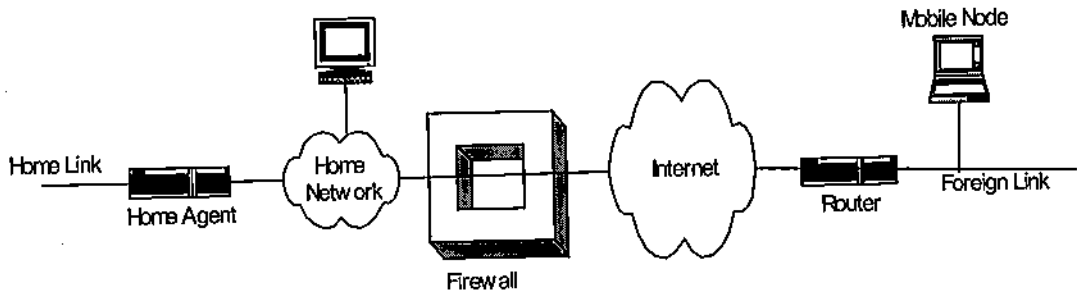
### 3.1.2 Mobile IP and Firewalls

Mobile nodes that are within the public portion of the Internet can transverse a firewall that protects their private network from unauthorized access in two ways:

#### 3.1.2.1 Simple Key Internet Protocol (SKIP) Firewall Transversal

SKIP is a key management protocol for use within the IP-layer security. It supports inline-keying, so it allows a node to establish session keys with another node in the same packets that are used to exchange user data. Mobile nodes can transverse firewalls protecting their private network, where SKIP is implemented by those firewalls for key management. Using SKIP for security has two main advantages. One advantage is that each SKIP packet contains an authentication header. As a result, the packet arriving at a firewall will be immediately determined to be discarded or pass through the firewall after authentication. Therefore, the firewall is able to make a decision without negotiating with the mobile node. The other advantage of applying SKIP is that it meets the demand of mobility. Normally, to testify if a security association is established, the source and destination address of the communication are verified when two end-points use an IP security channel for the communication. For SKIP, the security association can be verified by looking up the key ID, which is contained in the SKIP header. Figure (3.2) shows a reference diagram for SKIP-based firewall transversal. From administrative point of view and in order for the mobile node to transverse the firewall securely, the mobile node must be configured with the firewall public value. Mobile node and firewall must have hardware or software that implements at least one common secret key authentication algorithms and one common secret key encryption algorithm. The mobile node must be configured with a range of IP addresses that are known to within the private network. The home agent must be also configured within this range of IP addresses known to be within the private network. This will allow the home agent to determine that a mobile node is attempting to register a care-of address outside of the

private network. Hence, the home agent must modify its normal forwarding function in order to deliver tunneled packets to the firewall before the firewall can forward them towards the care-of address (Atkinson, 1995).



**Figure (3.2) Firewall Reference Diagram**

### 3.1.2.1.1 Registration Procedure

When a mobile node is away from the home network protected by firewalls, and moves into the public network, it must set up a binding with its home agent to keep connectivity. The first step is to send a registration request to its home agent because a firewall exists on the outbound interface of the home network, the registration packet can not bypass it. Therefore, in order to pass through the firewall, the packet must contain enough and correct information to meet the demand of the restriction on the firewall. The registration procedure consists of:

**1) Registration request:** The mobile node connects to a foreign link, and obtains a collocated care-of address via DHCP or PPP. It registers this address with its home agent. The components of this request message are as follows:

- An outer IP packet header, accomplishing the tunnel to the firewall.
- A SKIP header to inform the firewall of the identity of the mobile node and enables the firewall to determine the encryption and authentication algorithms used by the mobile node.

- An encapsulating security payload: Used to encrypt the data portion of the registration request message.
- An authentication header: Used to authenticate the mobile node to the firewall and provide integrity checking for the entire contents of the packet.
- The encrypted registration request message: This includes the mobile-home authentication extension, inner UDP/IP headers, and the fixed length portion of the registration request.

**2) Registration reply:** After receiving the securely tunneled registration request, the firewall uses the fields in the SKIP header to determine the identity of the mobile node, the authentication/encryption procedures used by the mobile node. The journey of the reply is divided into the following steps:

- The firewall tests the authenticator contained within the IP authentication header and decrypts the contents of the IP security payload to recover the normal registration request.
- After inspecting the decrypted registration request to find the mobile node's care-of address, the firewall tunnels the registration request to the home agent.
- Home agent receives the tunneled request, and verifies the mobile node's identity by validating the mobile-home authentication extension.
- A registration reply is tunneled by the home agent through the firewall to the mobile node's care-of address, this assuming that the mobile node is outside the firewall. Otherwise, the home agent sends the reply directly.
- Once this reply is received by the firewall, it recognizes the mobile node's care-of address as an address with which it has a security relationship. It then tunnels



the reply to the mobile node by the same way the mobile node tunnels the registration request to the firewall.

- Mobile node receives the reply and makes use of the SKIP header to determine the identity of the firewall, how to decrypt the packet and validates the authenticator within the IP authentication header.

Once the registration process completes, the home agent begins attracting packets destined to the mobile's node home address and tunneling them to the care-of address.

### **3.1.2.1.2 Building a Tunneled Registration Request**

Firstly, the mobile node builds a normal registration request message. This message contains UDP/IP header followed by the fixed-length portion of the registration request and the mobile home authentication extension. The normal registration request is then encrypted and placed within the payload portion of an encapsulated security payload header. The mobile node generates the outer IP header by:

- Placing the tunnel entry point, the care-of address, in the source address field.
- Placing the tunnel exit point, the firewall IP address, in the destination address field.
- The IP protocol field is set to 57 to indicate that the next header is a SKIP header.
- It generates the specific keys that it will use to authenticate and encrypt the tunneled message, as follows:
  - a) The mobile node combines the firewalls public value with its own Diffie-Hellman secret value to create a shared secret key.
  - b) The mobile node creates a random number to use as a key for protecting the current packet.

- c) From the number, the mobile node generates the specific authentication key and the specific encryption key using various operations involving message digest.

The mobile node proceeds to build the encapsulating security payload and authentication header once it has built the normal registration request, the tunneling IP header, and the SKIP header. Once it completes building, the mobile node assembles all of the pieces and transmits the packets. This securely tunneled packet is routed to the firewall where it verifies the authentication, decrypts the contents, and passes the normal registration request to the home agent (Rivest, 1992).

### **3.1.2.2 ISAKMP/Oakley Firewall Transversal**

The Internet Security Association and Key Management Protocol (ISAKMP) is the second way of firewall transversal used in mobile IP. All the assumptions, requirements, and administrative considerations used for firewall transversal with SKIP can be applied here.

The following points outline the differences and properties of the two approaches:

- Using ISAKMP/Oakley mobile node and firewall requires at least one round trip of negotiation before any packet could actually traverse the firewall. Two security associations would be created, one for authentication and the other for encryption. A single security association could be created using SKIP, which integrates both authentication and encryption.
- Packets sent between mobile node and firewall wouldn't contain a key management header as in the SKIP. Furthermore, an unauthorized person doesn't know which algorithms are being used for authentication and encryption, unlike the case in SKIP.

- Mobile node and firewall use each other's public keys in conjunction with some public key encryption algorithm to protect the fields within their ISAKMP/Oakley parameter negotiation and session-key derivation.
- SKIP header is present in every securely tunneled packet between the mobile node and the firewall, this adds 20 or more bytes that need not be sent in every packet. On the other hand, SKIP is easy to comprehend and implement as compared with ISAKMP/Oakley, and so it is desirable with computers with limited processing power (Jacobs, 1997).

### 3.2 Mobile IP with PPP

The PPP is the most common layer protocol by which one can connect to the Internet via their service provider. It is designed for transporting multiple network layer protocols over point-to-point links. When nodes connect to the Internet via PPP link, one of the PPP options named IP Control Protocol (IPCP) helps the nodes to negotiate the desirable IP parameters. However, this protocol is designed for regular IPv4. The problem is that IPCP provides no mechanism for either end-to-end PPP link to inform the other that it supports mobile IP. The configuration option for PPP IPCP is introduced to solve the problem of interaction between mobile IP and PPP IPCP, it provides also the following benefits:

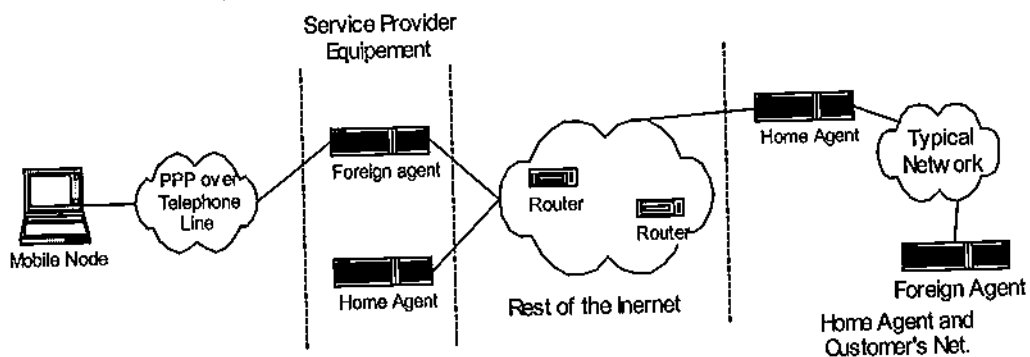
- A foreign agent can be deployed by a service provider without the need for a pool of addresses for assignment to dial up customers.
- An IP address is assigned to a mobile node only if it absolutely requires one.

For non mobile node, it must not send any configure request with a mobile IPv4 option. When a mobile node connecting to the Internet via PPP link sends a request to a peer, it can begin to send the request with requirement of using a foreign agent or collocated care-of address. If the peer realizes that the mobile node is at home, a `configure_nak`

must be returned to the mobile node to inform it of the truth. The IPCP state is opened when a configure-ack is received. Thereafter, the mobile node can start to listen to agent advertisements or broadcast an agent solicitation (Glass, 1998).

### 3.2.1 Preventing Attacks within the Framework of Mobile IP and PPP

Commercial Internet Service Providers (ISP) can support mobile IP functionality to work over PPP, which means that the ISP provides dial-up access to foreign agents via PPP. The reference model of mobile IP/PPP operation is shown in Figure (3.3).



**Figure (3.3) Reference Model of Mobile IP/PPP Interaction**

An ISP can prevent theft of service within this framework by using mobile IP as follows:

- Mobile IP solution: Mobile IP authentication extension within registration messages can be used for this purpose. Mobile IP defines extensions for authenticating mobile nodes to foreign agents, foreign agents to home agents and vice versa. These authentication extensions are based on two methods:
  - a) Secret key technology: Solutions based on this technology have scalability problems, if a mobile node requires to get authenticated with a service provider foreign agent, there is a need to be a unique secret key between each mobile node and foreign agent. This will result in a very large number of keys which make this method scales poorly. Secret key,

on the other hand, may require home agent to foreign agent authentication. Optimization is done here by requiring a single unique key between the set of all home agents within a corporation and all foreign agents owned by the service provider on the other hand.

- b) Public key technology: This method transverse the computing intensive calculations involved in public key algorithms from the mobile nodes to the foreign agents and home agents. In this method, the mobile node places a valid digital signature in the authentication field of its registration request. A registration reply from the home agent to the foreign agent that contains a valid digital signature authorizes the service provider to bill the owner of the home agent for the resources consumed by the indicated mobile node (Perkins, 1998).

### **3.3 Mobile Networks and Mobile IP**

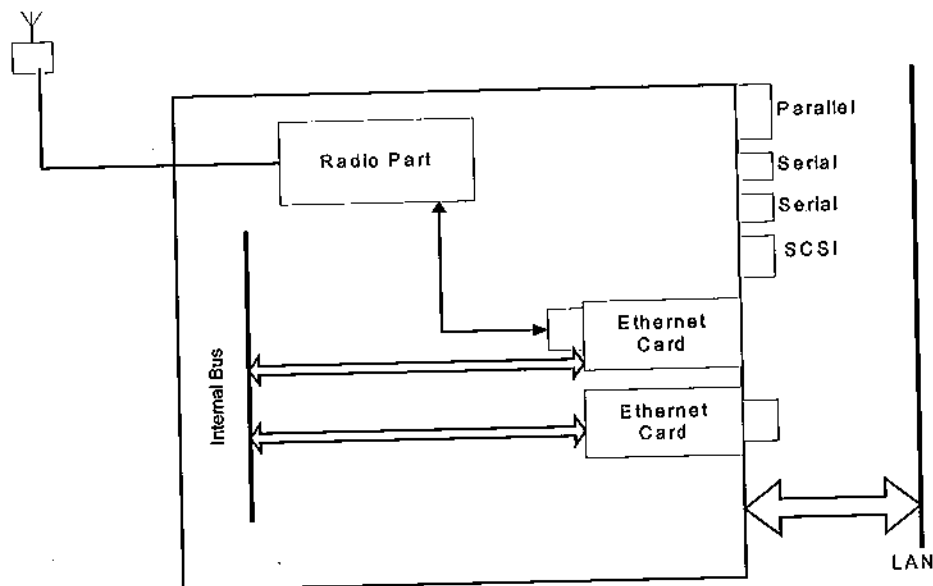
#### **3.3.1 Preview and Components**

A mobile network is a network whose hosts and routers are usually static with respect to each other, but are as a unit, mobile with respect to the rest of the Internet. Such mobile network may be found in a train, airplane and a ship. A mobile node on such network works on two level of mobile IP. In the inner architecture, a router that is used for communicating with the rest of the Internet can be defined as a mobile router. The mobile router has the following properties:

- It can be made compatible with many different types of mobile hosts, and so no changes have to be made with the operating system of the mobile host.
- All computation necessary for communication can be done by the mobile router and don't have to burden the mobile host.

- By putting all mobile functionalities into one device, it is transparent to the users and their computers.

Figure (3.4) shows an example of a typical mobile Internet router.



**Figure (3.4) Mobile Internet Router**

In this type of networks, the mobile router, when connected to its home link, works like any other fixed router. Namely, the mobile router and the home agent are neighboring routers which forward appropriate packets between each other and exchange routing updates. When a mobile router is connected to a visited link, it still exchange routing updates and forwards packets to home agent, but through a bi-directional tunnel. In this case, packets destined for hosts on the mobile network are tunneled to the mobile routers' care-of address where they are extracted from the tunnel and forwarded to the destination hosts on the mobile network.

The mobile router can use a collocated care-of address, but this requires the home agent to use nested encapsulation. However, in the reverse direction, the mobile router may use the foreign agent as a default router for packets generated by the hosts on the mobile network. Routing updates exchange must be continued between home agent and mobile router to prevent confusing routers along the path from the home agent to the

mobile router. Figure (3.5) shows an example of mobile networks (Forman and Zahorjan, 1993).

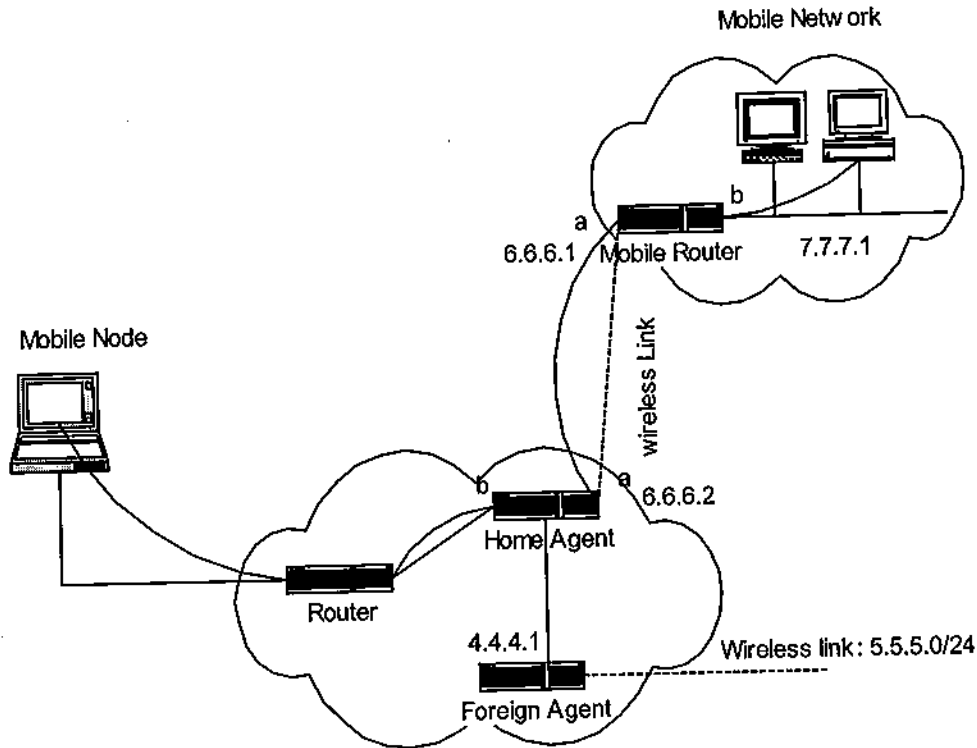


Figure (3.5) Example of Mobile Network

### 3.3.2 Routing Tables in Mobile Networks

When the mobile router is connected to its home link, the entries of the home agent's routing table are straightforward. As an example, Table (3.1) shows three of the home agent's routing table entries.

**Table (3.1) Routing Table of Home Agent**

Target/Prefix-Length	Next Hop	Interface
6.6.6.0/24 (all nodes on the home link)	directly	a (wireless interface)
5.5.5.0/24 (foreign agent wireless link)	4.4.4.1 (foreign agent)	b (wireless interface )
7.7.7.0/24 (all nodes on the mobile network)	6.6.6.1 (mobile router)	a (wireless interface)

Table (3.2) shows an example of routing table of mobile router. This routing table has direct, network-prefix routes to nodes on the home link and on the mobile network. Mobile router has also default route to all other nodes via the home agent. Packets generated by hosts on the mobile network and destined for nodes not on the mobile nodes will be forwarded firstly to the mobile router. Mobile router will use either its network-prefix route to nodes on the home link or its default route via the home agent to forward the packet towards its final destination.

**Table (3.2) Routing Table of Mobile Router**

Target/Prefix-Length	Next Hop	Interface
6.6.6.0/24 (all nodes on the home link)	directly	a (wireless interface)
0.0.0.0/0 (every thing else)	6.6.6.2 (home agent)	a (wireless interface)
7.7.7.0/24 (all nodes on home network)	directly	b (ethernet interface)



When the mobile router is away from home, it connects to a foreign link. In this case, mobile router registers with its home agent via a collocated care-of address. Once registration is successful, mobile router and home agent must modify their routing tables to perform bi-directional tunneling. As in the case of mobile host, the home agent adds a host-specific route to the mobile router via the care-of address and through a virtual interface as shown in Table (3.3).

**Table (3.3) Modified Routing Table of Home Agent**

Target/Prefix-Length	Next Hop	Interface
6.6.6.0/24 (most nodes on the home link)	Directly	a (wireless interface)
6.6.6.1/32 (mobile router)	5.5.5.1(care-of address)	w (tunnel virtual interface)
7.7.7.0/24 (all nodes on the mobile network)	5.5.5.1(care-of address)	w (tunnel virtual interface)
5.5.5.0/24 (the foreign agent's wireless link)	4.4.4.1(foreign agent)	b (wired interface)

Additionally, the home agent must modify any routes which specify the next hop of the mobile router to likewise point to the mobile router's care-of address and the virtual interface. Similarly, the mobile router must modify some of its routing table entries when connected to the foreign link. Mobile router changes all routes which formerly pointed to the home link to be via a tunnel to its home agent. Also, the mobile router must add a host specific route to its home agent to be via the foreign agent through its physical interface on the foreign link. As a result, the routing table of the mobile router is shown in Table (3.4). Packets that are generated by hosts on the mobile network and destined for nodes not on the mobile network will be forwarded to the mobile router.

When the packet is not destined to the home agent itself, the mobile router will use either the first or the fourth entry of Table (3.4) to forward the packets. This is done as follows:

- Mobile router encapsulates the packet in a new packet whose IP destination address is the address of its home agent.
- Mobile router uses host-specific route to forward the encapsulated packet to the foreign agent.
- Foreign agent forwards the encapsulated packet to the home agent where it is decapsulated and routed to its destination.

**Table (3.4) Routing Table of Mobile Router on a Foreign Link**

Target/Prefix-Length	Next Hop	Interface
6.6.6.0/24 (all nodes on the home link)	6.6.6.2 (home agent)	w (tunnel virtual interface)
6.6.6.2/32 (home agent)	5.5.5.2 (foreign agent )	a (wireless interface)
7.7.7.0/24 (all nodes on the home network)	directly	b (wired interface)
0.0.0.0/0 (every thing else)	4.4.4.1 ( foreign agent)	w (tunnel virtual interface)

### 3.3.3 Mobile Routing within Mobile Networks

Previously, hosts and routers on the mobile network were considered as fixed with respect to each other and with respect to the mobile router. Here, we will consider the case of a mobile host with the mobile network. As an example, a businessman who brings a notebook computer onto an airplane, in this case the notebook computer is

mobile with respect to the airplane's hosts and routers and the entire airplane is moving with respect to the entire Internet. This situation is described in Figure (3.6).

The procedure to transfer a packet from the correspondent node to mobile host on the mobile network can be stated as follows:

- Firstly, mobile host's home agent receives the packet transmitted by the correspondent node.
- Packet is tunneled by the mobile host's home agent to the IP home address of the mobile router, which is the care-of address of the mobile host.
- The tunneled packet is routed to the mobile router's home agent.
- Mobile router's home agent intercepts the tunneled packet and tunnels it to the mobile router's care-of address. The mobile router's foreign agent receives the packet and removes the outer most tunneling header.
- The packet at this stage is received by the mobile router, it removes the remaining tunneling header to see the final destination of the packet. It then sends the original packet over the mobile network link to the mobile host.

#### **3.3.4 Mobile Router in Mobile IPv4**

When a mobile node is away from home and attached to a remote and moving network, like a LAN constructed on a ship or an aeroplane, it can be considered that the mobile node is working under a two-level architecture of mobile IP. In the inner architecture, a router that is used for communicating with the rest of the Internet on the aeroplane can be defined as a mobile router. Moreover, it is easy to imagine that the mobile router plays a role of a mobile node in the inner architecture and represents the LAN existing in an aeroplane. Normally, the mobile router's home network is located in the airline headquarter.

The procedure for mobile IPv4 mobile router is described below:

- When a laptop computer is away from its home network area and attached to a LAN on an aircraft, the mobile router on the plane will take the responsibility in being its foreign agent, and assign a care-of address to the mobile node as well.
- For the inner architecture, the mobile router frequently registers to a foreign agent when the aircraft is in flight, and the foreign agent is located in a foreign network under the aircraft.
- When some packets addressed to the laptop computer from a correspondent node, they will be sent to the mobile node's home network and intercepted by the home agent. The home agent encapsulates the packets and tunnels them to the mobile node's foreign agent.
- Because the mobile node's foreign agent is the mobile router, the packets will be sent to the mobile router's home network, whose routing is based on the network number of the mobile router's home address.
- Once being intercepted by the mobile router's home agent, the packets will be encapsulated again and tunneled to the mobile router's foreign agent. An instant later when arriving at the mobile router's foreign agent, they will be decapsulated and forwarded to the mobile router.
- As soon as receiving the packets, the mobile router decapsulates and delivers them to the laptop node (Barke, 1996).

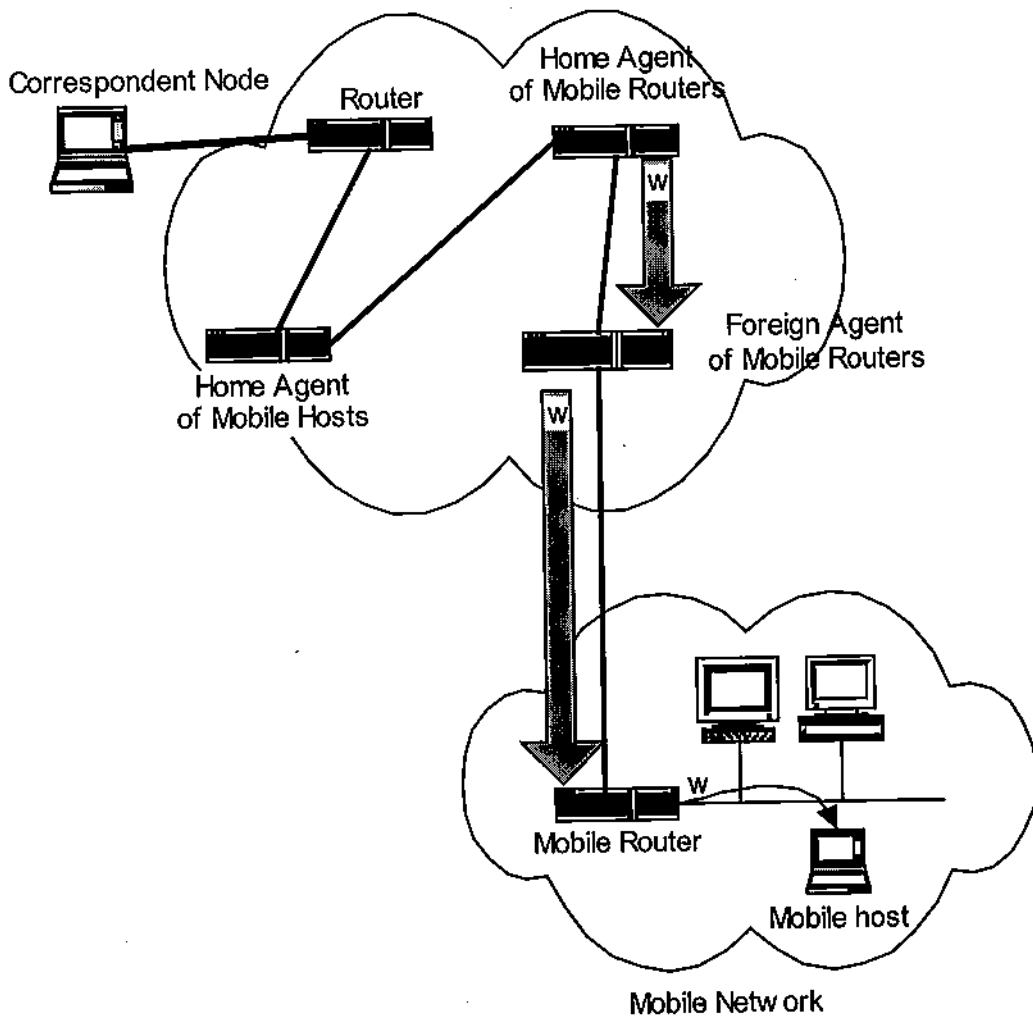


Figure (3.6) Mobility Support in Mobile Networks

### 3.3.5 Mobile IP and Real-Time Traffic

The most obvious challenges to real-time traffic introduced by mobile IP is the fact that mobile nodes change their location up to once per second. Resource reservation protocol (RSVP) is used by a host on behalf of an application to request a given quality of service from the network. Unfortunately, this protocol reserves resources only along a specific path. This implies that new reservations will be required every time a mobile node changes link. In the case of route optimization, mobile node must reserve resources from its care-of address back to the original sender. If route optimization is not used, mobile node has to reserve resources for the new tunnel from its care-of address back to the home agent, each time it moves. The presence of tunnel in mobile IP introduces a new complication for real time applications. RSVP path and

Reservation message contains a description of the flow for which resource reservation are being requested. This flow description contains a list of packet header fields that a router can use to distinguish packets of the real-time flow from all other packets that might pass through the router. It usually contains sender's and receiver's IP addresses, IP protocol field, and optionally transport-layer port numbers. The problem is that IP-in-IP encapsulation moves all these fields to a different location within the encapsulating packet. To solve this problem, the tunneling method should include not only an outer IP header but also a transport layer header (UDP), such that port numbers can be used to classify tunneled packets as well.

Another problem to accommodate in this field is IP level security, where the use of authentication header will change the fields which router would use to classify packets. Also, the encapsulating security payload can render some of these fields encrypted and so unidentifiable to intermediate routers, resulting in hard classification of packets. SPI field from the encapsulating security payload header may be used here to solve the packet classification problem. As sender of real-time traffic, the problem of IP level security is identical for mobile nodes as receivers. The problem of the presence of tunnel will make no effect in the absence of ingress-filtering routers. To deal with this problem in the presence of ingress-filtering, the mobile node can reserve tunnel to its home agent.

Mobile IP registration is exactly the type of explicit notification that a home agent could use to reserve resources on behalf of mobile node as a sender of real-time traffic. The home agent is required to perform reservation between itself and the mobile node every time mobile node registers at a new location. By this method, the mobile node can reserve the tunneling of its real-time traffic to its home agent.

In summary, the three issues that we considered when the mobile node is a sender or receiver of real-time traffic are:

- IP-level security which may encrypt or change the location of header fields.
- The presence of mobile IP tunnel.
- Mobility, and the need for the mobile node to re-reserve resources every time the mobile node changes location.

### **3.4 Routing Protocols in Ad Hoc Networks and Mobile IP**

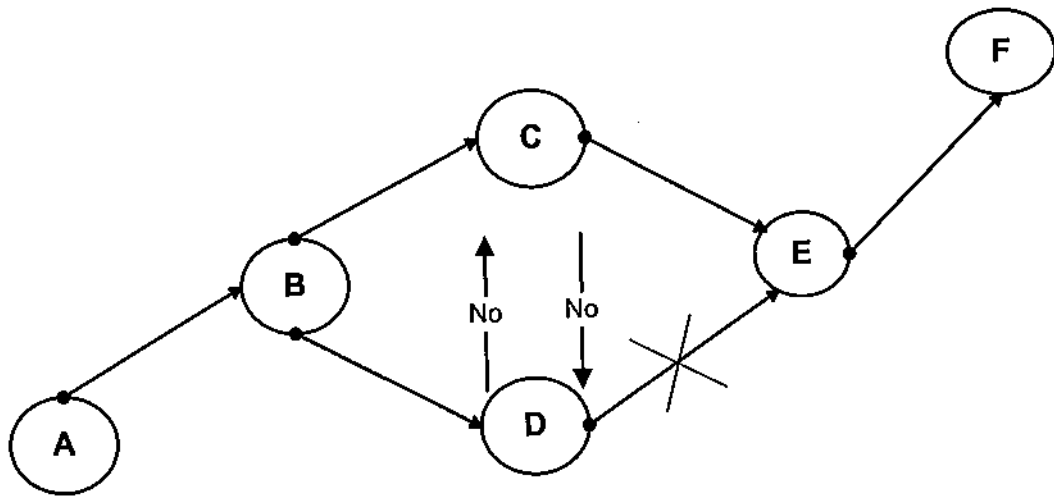
An Ad Hoc network is one that comes together as needed without any assistance from the existing infrastructure of the Internet. Ad Hoc networks are self configuring, i.e., there is no central management system with configuration responsibilities. Some nodes on such networks are capable of assuming router functionality when needed; this enables terminals to communicate with each other when they are out of radio range. The general structure of such nodes can change constantly because of the movement of the nodes. In contrast with cellular networks, there is no need to build network infrastructure with base stations. Ad Hoc networks can be viewed as stand-alone groups of mobile terminals, but they may also be connected to a pre-existing network infrastructure and use it to access nodes which are not part of the Ad Hoc network. Routing is a central issue in mobile Ad Hoc networking. Most routing algorithms have been derived from algorithms that were originally devised for fixed networks and usually consider homogenous Ad Hoc networks. Now, we are going to discuss the most routing protocols used in Ad Hoc networks (Perkins, 2000).

#### **3.4.1 Dynamic Source Routing (DSR) Protocol**

In the wired network, the routing protocols are divided into two types: distance vector and link state routing protocol. However, these protocols are not able to efficiently function in an Ad Hoc network. As a consequence, a new protocol, DSR, is designed for routing in an Ad Hoc network. In an Ad Hoc network, each host must have the capability to forward packets to the adjacent hop. In order to use the limited bandwidth,

the hosts can not periodically broadcast routing message in the network. However, an exception occurs when the interface index of a host is set to `IF_INDEX_MA`, which indicates that the host acts as a mobility agent. The mobility agent is allowed to frequently broadcast an agent advertisement in the Ad Hoc network. Let's see how DSR works when host A would like to send a packet to host F, as illustrated in Figure (3.7). Firstly, host A must check out its route cache if a route to host F already exists. If not, a route request will be flooded among the link. Once a host receives the request, it will look up its route cache. If there is a route to host F recorded, the host will attach this routing information with the record of the previous route into a route reply. The packet is returned to host A along the route recorded in the route reply. If the routing information does not exist, the host just needs to pad its address in the packet and forwards it to the next hop.

This procedure will last till the packet reaches host F. Host F then copies the routing information into a routing reply and returns it along the reverse route.



**Figure (3.7) Ad Hoc Network Routing Discovery**

In order to avoid duplicate forwarding of the route request packet, each request contains a request ID. When a host receives a route request and finds out that it has the same



request ID as the one contained in the previous, the host must silently discard the packet (Royer, 1999).

### **3.4.2 Destination Sequenced Distance Vector (DSDV) Protocol**

It is a hop-by-hop distance vector routing protocol, in each node it has a routing table for all reachable destinations. It requires that each node periodically broadcasts routing updates. This protocol guarantees loop freedom by using a sequence number to tag each route. The sequence number shows the freshness of a route and routes with higher sequence numbers are favorable. A route R is considered more favorable than other routes if R has a higher sequence number or if the routes have the same sequence number but R has lower hop count. The sequence number is increased when a node detects that a route to a destination has broken. Next time this node advertises the route to that destination with an infinite hop count and a sequence number that is larger than before.

Basically, this protocol is distance vector with small adjustments to make it suitable for Ad Hoc networks. These adjustments consist of triggered updates that will take care of topology changes in the time between broadcasts. To reduce the amount of information in these packets, there are two types of update messages: full and incremental dump. The incremental dump carries the information that has changed since the last dump, whereas the full dump carries all available routing information.

DSDV needs some time to converge before a route can be used, since it is dependent on periodic broadcast. This converge time can be considered negligible in a static wired network, where the topology is not changed so frequently. On the other hand, this converge time will probably mean a lot of dropped packets before a valid route is detected in Ad Hoc networks, since the topology is expected to be very dynamic.

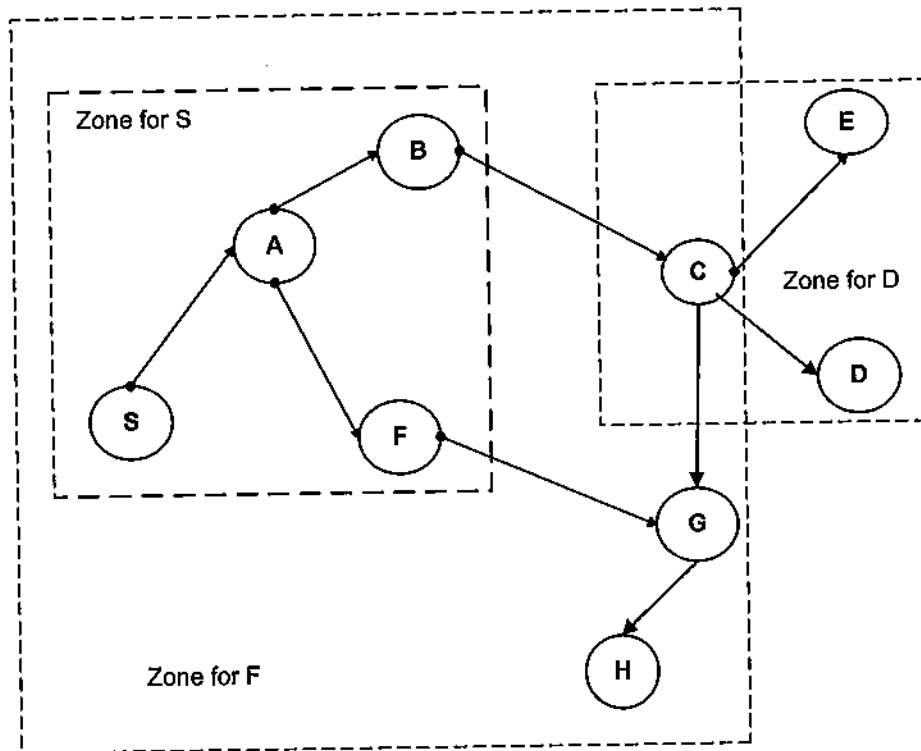
### 3.4.3 Zone Routing Protocol (ZRP)

This protocol is a hybrid of a reactive and a proactive protocol. It divides the network into several routing zones and specifies two totally detached protocols that operate inside and between the routing zones.

The intra-zone routing protocol operates inside the routing zone and learns the minimum distance and routes to all the nodes within the zone. A change in topology means that update information only propagates within the affected routing zones as opposed to affecting the entire network. The inter-zone is the second routing protocol. It is reactive and used for finding routes between different routing zones. This protocol broadcasts a route request to all border nodes within the routing zone, which in turn forwards the request if the destination node is not found within their routing zone. This procedure is repeated until the requested node is found and a route reply is sent back to the source indicating the route.

To illustrate the operation of this protocol, we will consider the network shown in Figure (3.8). Here node S wants to send a packet to node D, a route request is sent to border nodes B and F since D is not in the routing zone of node S, each border node checks to see if D is in their routing zone. Neither B nor F finds the requested node in their routing zone. Thus, the request is forwarded to the respective border nodes. F sends the request to S, B, C, and H while B sends the request to S, F, E, and G. The requested node D is found within the routing zones of both C and E, thus a reply is generated and sent back towards the source node S.

Using ZRP, routes inside the routing zone can be found very fast, while routes outside the zone can be found by efficiently querying selected nodes in the network. ZRP limits propagation of information about topological changes to the neighborhood of the change only, where changing the topology can affect several routing zones.



**Figure (3.8) Networking Using ZRP**  
(dashed lines show the routing zones)

#### 3.4.4 The Ad Hoc On Demand Distance Vector (AODV)

This protocol is designed as a routing protocol for Ad Hoc mobile networks. AODV is capable of both unicast and multicast routing. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources. Additionally, AODV forms trees which connect multicast group members. The trees are composed of the group members and the nodes needed to connect the members. AODV uses sequence numbers to ensure the freshness of routes. It is loop-free, self-starting, and scales to large numbers of mobile nodes.

AODV builds routes using a route request/route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the

route tables. In addition to the source node's IP address, current sequence number, and broadcast ID, the request packet also contains the most recent sequence number for the destination of which the source node is aware. A node receiving the request packet may send a route reply if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the request packet. If this is the case, it unicasts a route reply back to the source. Otherwise, it rebroadcasts the request packet. Nodes keep track of the request packet's source IP address and broadcast ID. If they receive a request packet which they have already processed, they discard the request packet and do not forward it. As the route reply propagates back to the source, nodes set up forward pointers to the destination. Once the source node receives the route reply, it may begin to forward data packets to the destination. If the source later receives a route reply containing a higher sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route.

As long as the route remains active, it will continue to be maintained. A route is considered active as long as there are data packets periodically traveling from the source to the destination along that path. Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. If a link break occurs while the route is active, the node upstream of the break propagates a route error message to the source node to inform it of the now unreachable destination(s). After receiving the route error, if the source node still desires the route, it can reinitiate route discovery.

Multicast routes are set up in a similar manner. A node wishing to join a multicast group broadcasts a route request with the destination IP address set to that of the multicast group, and with the join flag set to indicate that it would like to join the group. Any node receiving the request packet which is a member of the multicast tree that has

Internet, there must be at least one node within the Ad Hoc network that agrees to connect to Internet and to serve as a foreign agent. The process continues as follows:

- This foreign agent node is expected to issue periodic advertisements to the wireless nodes within its range, informing them of the availability of mobile IP services and other relevant services conditions.
- In order to have the service, the neighboring nodes of the foreign agent must rebroadcast the advertisement throughout. This is done by assigning the IP identification field of the advertisement as the 32-bit sequence number of the advertisement.
- For the hop count metric to be handled correctly, the foreign agent should allow registration from mobile nodes that are farther than one hop from its wireless interface. With this approach each mobile Ad Hoc node determine whether mobile IP services are available or not. In addition to what is stated above, mobile IP and Ad Hoc algorithms must have coordinated access to the route table for better work (Perkins, 2000; Royer, 1999).

### **3.5 Cellular IP**

Cellular IP is a micro-mobility protocol optimized to provide local access to a mobile IP enabled Internet in support of fast moving wireless hosts. This protocol tries to minimize handoff latencies within a mobility domain. Cellular IP inherits cellular principles for mobility management such as passive connectivity, paging and fast handoff control, but implements them around the IP paradigm. Control signaling is minimized by using regular data packets transmitted by mobile hosts to establish host location information. The access network consists of several base stations and a border router; the gateway. Cellular IP was developed with IPv4 in mind, so the gateway also implements foreign agent functionality. Mobile terminals visiting a Cellular IP network

declare the address of the gateway as their care-of address. Conventional mobile IP is used to communicate with the correspondent nodes and the home agent (Campbell, 2000).

In Cellular IP, location management and handoffs support are integrated with routing. To minimize control messaging, regular data packets transmitted by mobile hosts are used to refresh host location information. Uplink packets are routed from a mobile host to the gateway on a hop-by-hop basis. The path taken by these packets is cached by all intermediate base stations. To route downlink packet addressed to a mobile host, the path used by recently transmitted packets from the mobile host is reserved. When the mobile host has no data to transmit, it sends small, special IP packets toward the gateway to maintain its downlink routing state. Following the principle of passive connectivity, mobile hosts that have not received packet for some period of time allow their down

link routes to be cleared from the cache as dictated by a soft timer. Paging is used to route packets to idle mobile hosts in a Cellular IP access network (Campbell, Gomez, and Valko, 1999).

### **3.6 Hierarchical Mobile IP**

Internet mobile users require special support to maintain connectivity as they change their point of attachment. This support should provide performance transparency to mobile users and should be scalable. Providing performance transparency means that higher level protocols should be unaffected by the addition of mobility support. Issues that may affect performance transparency are optimum routing of packets to and from mobile nodes and efficient network transition procedures. The mobility support should be scalable in the sense that it should keep providing good performance to mobile users and should keep the network load low as the network grows and the number of mobile

nodes increases. This scalability issue is a very important one in the context of a still growing worldwide network such as the Internet. The Internet Engineering Task Force (IETF) mobile IPv6 proposal, which provides a mobility management scheme for the Internet, does not completely meet these design goals. In mobile IPv6, a mobile node sends a location update to each of its correspondent nodes periodically and at any time it changes its point-of-attachment. The resulting signaling and processing load may become very significant as the number of mobile nodes increases. This limitation is the result of the lack of hierarchy in the mobility management procedures of mobile IPv6. In fact, mobile IPv6 handles global area mobility and local area mobility identically. Since most of a user's mobility is local, a hierarchical scheme that separates micro-mobility from macro-mobility is preferable. Mobile IPv6 handles local mobility of a host (i.e., within a site or a network) in the same way as it handles global mobility (inter-site or inter-network mobility). In mobile IP, a mobile host sends binding updates to its home agent and its correspondent nodes each time it changes its point of attachment regardless of the locality and amplitude of its movement. As a consequence, the same level of signaling load is introduced in the Internet independently of the user's mobility pattern. This approach is not scalable since the generated signaling load can become quite overwhelming as the number of mobile hosts increases in the Internet. A hierarchical scheme that differentiates local mobility from global mobility is more appropriate to the Internet. Using hierarchical approach has at least two advantages:

- It improves handoff performance, since local handoffs are performed locally. This increases the handoff speed and minimizes the loss of packets that may occur during transitions.

- It significantly reduces the mobility management signaling load on the Internet since the signaling messages corresponding to local moves do not cross the whole Internet but stay confined to the site.

The main operations of the hierarchical mobile IP protocol are as follows:

- 1) **Inter-site mobility:** When a mobile host enters into a new site, it gets two care-of addresses:
  - a) Private (or Physical) care-of address: Which is on the link to which it is attached
  - b) Virtual care-of address: Which is in the mobility network of the site (in mobile IPv6 only the first is required).

The mobile host then sends some binding updates. It sends:

- A binding update that specifies the binding between its virtual care-of address and its private care-of address to the site of mobility agent. Upon reception of this binding update, the mobility agent performs admission control such as authentication and charging. If the request is accepted, an acknowledgement is sent back to the mobile host.
- A binding update that specifies the binding between its home address and its virtual care-of address to its home agent and each of its external correspondents that are outside of the site.
- A binding update that specifies the binding between its home address and its private care-of address to each of its local correspondents that are within the site (Soliman and Malki, 2000)

As a result:

- An external host that sends packets to the mobile host uses its virtual care-of address. Packets are then routed to the mobility network of the visited site,



intercepted by the mobility agent and forwarded (tunneled) to the current private care-of address of the mobile host.

- A local host that sends packets to the mobile host uses its private care-of address. Packets are then directly delivered to the mobile host.

2) **Intra-site mobility:** When a mobile host moves within the site, it gets a new private care-of address on its new point of attachment. The virtual care-of address remains constant as long as the mobile host is roaming locally.

The mobile host then sends the following binding updates:

- A binding update that specifies the binding between its home address and its new private care-of address to each of its local correspondent hosts that are within the site.
- A binding update that specifies the binding between its virtual care-of address and its new private care-of address to the site of mobility agent.

During intra-site mobility, no binding update is sent on the Internet and that transitions are performed locally (Postel, 1981).

### 3.7 Transmission Control Protocol (TCP) and Mobile IP

TCP is the reliable transport layer protocol in the Internet. It has the following properties:

- TCP guarantees that the application's data is delivered to the ultimate destination, sequentially, and error free.
- It is a full-duplex, stream-oriented protocol. This means that information can flow simultaneously in both directions between two communicating nodes.
- It is a connection-oriented protocol, it has three distinct phases: connection establishment, data transfer, and connection close.

- It accepts data from the application layer, it chops it into suitably sized chunks, prepends a transport layer header to form segments.
  - Each segment is transmitted as the payload portion of the network layer packet.
- As shown in Figure (3.9).

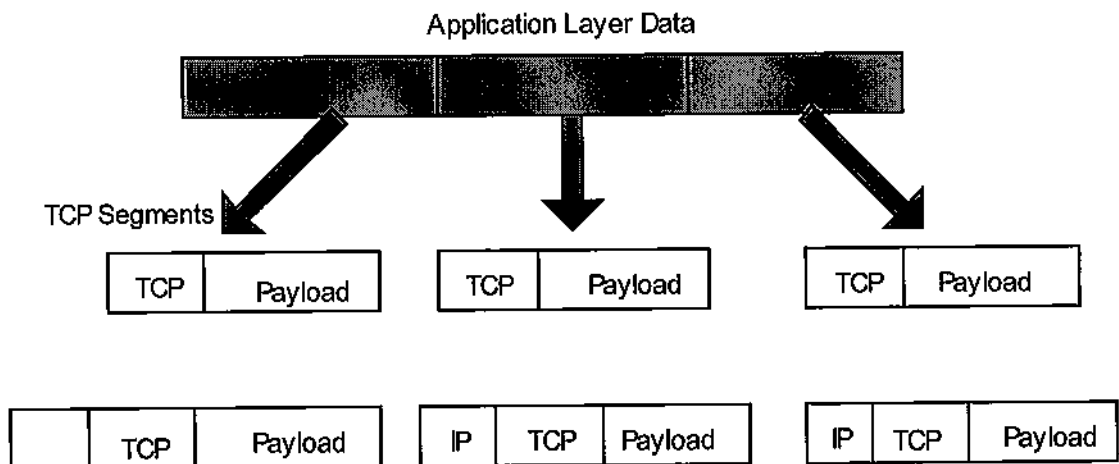


Figure (3.9) TCP Segments

TCP assumes that the majority of lost segments and acknowledgments are due to congestion in the Internet. For wired network infrastructure this assumption is valid, but for wireless links, this assumption is generally not valid due to errors that occur in the transmission. When these errors occur, TCP assumes the network is congested and reduces its transmission of segments. This results with poor performance of TCP over wireless links. For mobile nodes two points characterize mobile nodes: Mobility itself and the wireless link over which mobile nodes communicate, both of them participate to degrade the performance of TCP. The possible enhancement for TCP to improve its performance for mobile nodes should be applied, which are: Link-layer protocols, TCP itself, and application-layer protocols.

1) **Enhancement of TCP:** Possibly, four enhancements can be applied to TCP:

- Fast retransmit of mobile-node movement: Usually, when a mobile node moves to a new link, tunneled packets to the old link will be undeliverable, resulting in

timeout and congestion control to occur in the correspondent node and in the mobile node itself. To avoid this problem, TCP on the mobile node should go into fast retransmit once it registers on a new link. This will cause a mobile node to immediately transmit unacknowledged segments without going into a congestion mode. Cooperation between mobile IP and TCP software should be involved here which requires the mobile IP software to provide an indication to TCP whenever the mobile node moves to a new link.

- **Connection segmentation:** This approach allows the TCP in mobile nodes to be more aggressive in the presence of errors, without causing congestion and without diminishing the mobile nodes ability to communicate with older TCP implementations in other nodes. This approach treats the TCP connection between a mobile node and a correspondent node as two concatenated connections. Where the first connection is between a correspondent node and another intermediate node over the wired Internet. The second connection is between the intermediate node and the mobile node over some wireless link. The intermediate node serves as a relay between the two TCP connections.
- **Transmission and timeout freezing:** Sometimes, nodes on wireless links experience long periods during which no data can be exchanged. Fortunately, the link layers of various wireless systems are often capable of detecting such events. So, to solve this problem, such link layer should inform TCP upon finding any disruption in service. Therefore, TCP software won't send any new packets and won't make any assumption about the round-trip time, and thus when the service resumes, the link-layer can again signal TCP, causing it to begin transmitting once again (Pear, 97).

- **Selective acknowledgment:** This scheme allows a node to inform another node of all segments it has received, not just those that have been received sequentially. This will prevent unnecessary retransmission when a hole appears in the data. It is especially important for mobile nodes that communicate over slow wireless links.

**2) Link-layer enhancement:** One thing to include here is for a link-layer to examine the higher layer protocol headers of all its frames to determine if multiple copies of the same segment are waiting to transverse the link. If so, the link layer will discard the duplicates and will attempts to move a single copy of the segment.

**3) Application-layer Enhancement:** Intelligent caching and distribution of information are new techniques which can be used to improve the performance of applications in mobile and wireless networks.

### **3.8 Mobile IP and GPRS**

#### **3.8.1 General Description of GPRS**

GPRS is an access technology used to establish a packet switched bearer, it handles mobility in the Global System of Mobile (GSM) communication and Universal Mobile Telecommunication System (UMTS). In addition, GPRS has the ability to support the mobile IP protocol. The Gateway Support Nodes (GSN), Serving GPRS Support Node (SGSN), and Gateway GPRS Support Node (GGSN) handle both packet forwarding and signaling. SGSN and GGSN can be co-located in one physical node. The cost of the nodes is very high, which is a result of the high-intelligence level and complex equipment. The Radio Network Controllers (RNC) and the Base Station Controller (BSC) have different requirements for delivery of packet data from the core network (SGSN). However, these differences affect the SGSN's terms of delivery at a minimum. A Packet Control Unit (PCU) that has been added to the BSC makes the needed

changes for the BSC's requirements; only ciphering and packet buffering for the GSM network is performed in the SGSN. The RNC is more intelligent than the BSC, and contains functions for header compression, ciphering and tunneling. The GGSN is permanent and will never be replaced during the lifetime of a Packet Data Protocol (PDP) context, even if its location results in cumbersome routing and extra distance for tunneling of the packet data.

The GPRS core network contains the SGSN and the GGSN nodes. It provides packet-switched communication and can both be used with a GSM and a UMTS access networks. Home Location Register (HLR) and Equipment Identity Register (EIR), which GPRS uses, are "old" GSM nodes enhanced with GPRS-specific functionality. The circuit-switched domain is common for GSM and UMTS. The UMTS radio system, UMTS Terrestrial Radio Access Network (UTRAN), is designed for both packet-switched communication and circuit-switched communication. The architecture of UTRAN is shown in Figure (3.11), where BTS refers to Base Transceiver Station. GSM's radio system, Base Station Subsystem (BSS), is being modified with a PCU next to the BSC to handle packet data traffic. The common packet domain core network provides packet-switched services and is designed to support several Quality of Service (QoS) levels in order to allow efficient transfer of real-time traffic and non-real-time traffic. It supports end users who wish to access the Internet using a packet-data Mobile Station (MS) as the connecting device. The GPRS involves three main components: the MS, a radio network, and a core network. The MS consists of a Mobile Terminal (MT), a telephone with GPRS functionality, and Terminal Equipment (TE); a computer interconnected with the MT. MT and a TE can also be integrated into one piece of equipment. The charging is performed by a billing system connected to the Charging Gateway Functionality (CGF) node that has an interface towards the SGSN and the GGSN nodes. Charging should be flexible and allow to bill according to the amount of

data transferred; volume-based charging. The QoS supported and duration of the connection is also recorded and can be used for charging (Faccin and Purnadi, 1999).

The mobility handling in GSM GPRS and the mobility handling in UMTS GPRS are similar to each other, hence sequences are not shown for both of them. Some of the figures will be based on the GSM scheme, while others will be based on the UMTS scheme, according to the easiest way of describing the actual functions.

Figure (3.10) shows a total system overview where GPRS packet domain, circuit-switched domain, and the radio systems are interconnected.

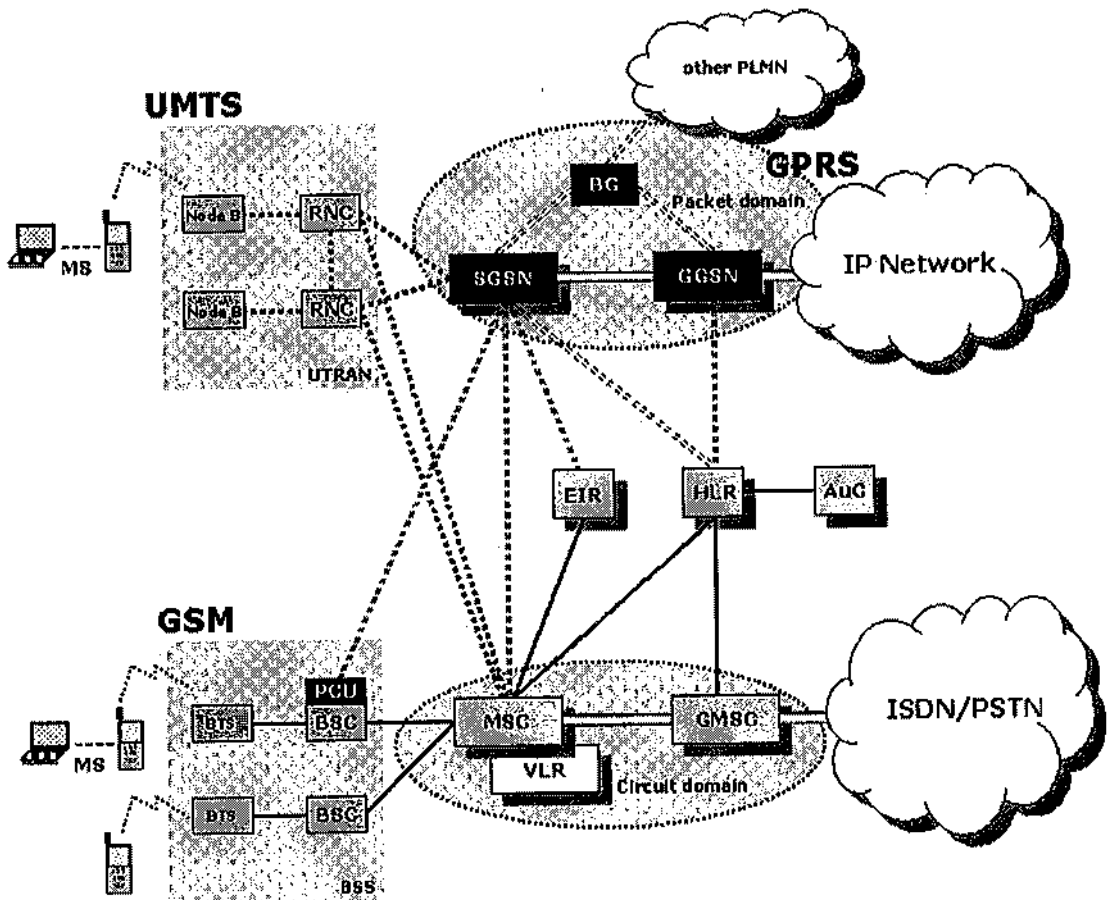
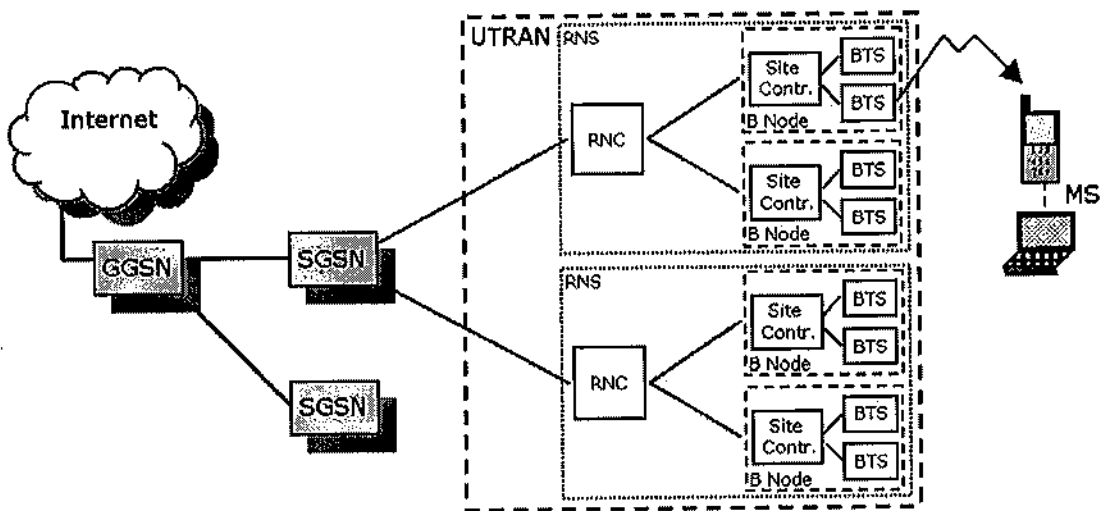


Figure (3.10) Total System Overview

The different components that are used in the GPRS network have a hierarchic structure. Some nodes in UMTS are different from the nodes in GSM, but approximately the same functionality is performed.

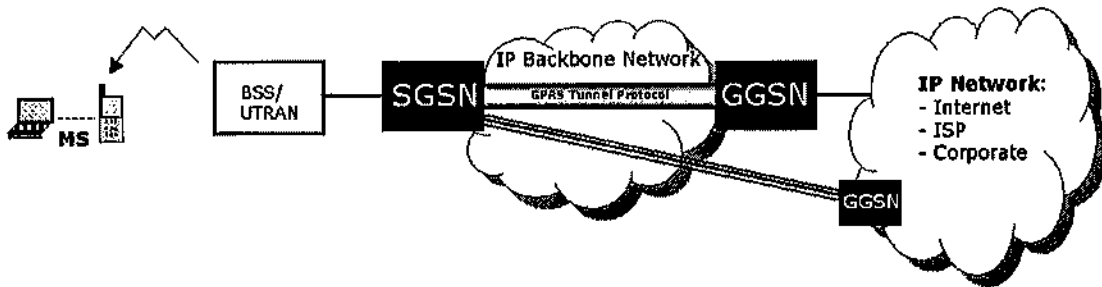
With a hierarchic structure means (explained with UMTS terms), the SGSN is connected to several RNCs, the RNC is connected to several site controllers, and the site controller is connected to several base transceiver station (William, 1995).



**Figure (3.11) UMTS Terrestrial Radio Access Network**

The SGSN and the GGSN constitute the GPRS core network and have common HLR and EIR with the circuit-switched domain. The SGSN serves a given geographical area and forwards incoming and outgoing IP packets addressed to and from an MS that is attached within the SGSN service area. It also provides authentication, session management, and mobility management. In addition, the SGSN provides ciphering for the GSM network. The GGSN is the interface towards the external IP packet networks. From the external IP network's point of view, the GGSN acts as a router for the IP addresses of all subscribers served by the GPRS network.

The GPRS Tunneling Protocol (GTP) is executing transport of data between RNC and SGSN, and between SGSN and GGSN in the backbone network. The Base Station System GPRS Protocol (BSSGP) executes the transport of data from SGSN to BSC.



**Figure (3. 12) GPRS Packet Domain Overview**

No user data or header compression is done in the GGSN. UMTS performs header compression in RNC. GSM performs header compression and user data compression in SGSN. Communication with an external IP network will always pass through a GGSN node (Patel and Dennet, 2000). Figure (3.12) shows the packet domain infrastructure of the GPRS network. It characterizes the required stages for MS to get access to the Internet from through the GPRS domain.

### **3.8.2 GPRS Attach Schedule Overview**

Figure (3.13) shows the attach schedule of GPRS, where MS request access, and a logical link to an SGSN is initiated. Mobility Management (MM) contexts are established at the MS and SGSN.



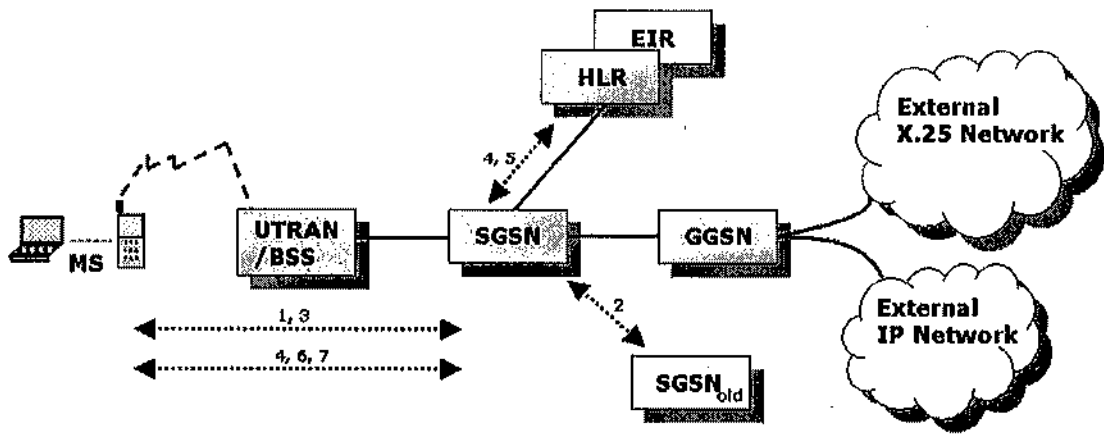


Figure (3.13) GPRS Attach Schedule

1. Attach request
2. Identification request/response
3. Identity request/response
4. Authentication
5. Update location
6. Attach accept
7. Attach complete

### 3.8.3 GPRS Handover Schedule Overview

Handover is a change of node(s) in the GPRS system, most often caused by movement of the MS. Possible handover combinations explained with UMTS terms when a handover results in a;

1. Change of BTS, the connection between the site controller and the GGSN remains unchanged.
2. Change of node B, the connection between the RNC and the GGSN remains unchanged (Heine, 2000).
3. Change of RNC, the connection between the SGSN and the GGSN remains unchanged.
4. Change of SGSN, the GGSN is still the same.

### 3.8.5 GPRS, Mobile IP: Comparison Study

This section will evaluate if Mobile IP complements, competes with, or is a total separate issue from GPRS, as specified by 3GPP today in terms of the mobility aspect.

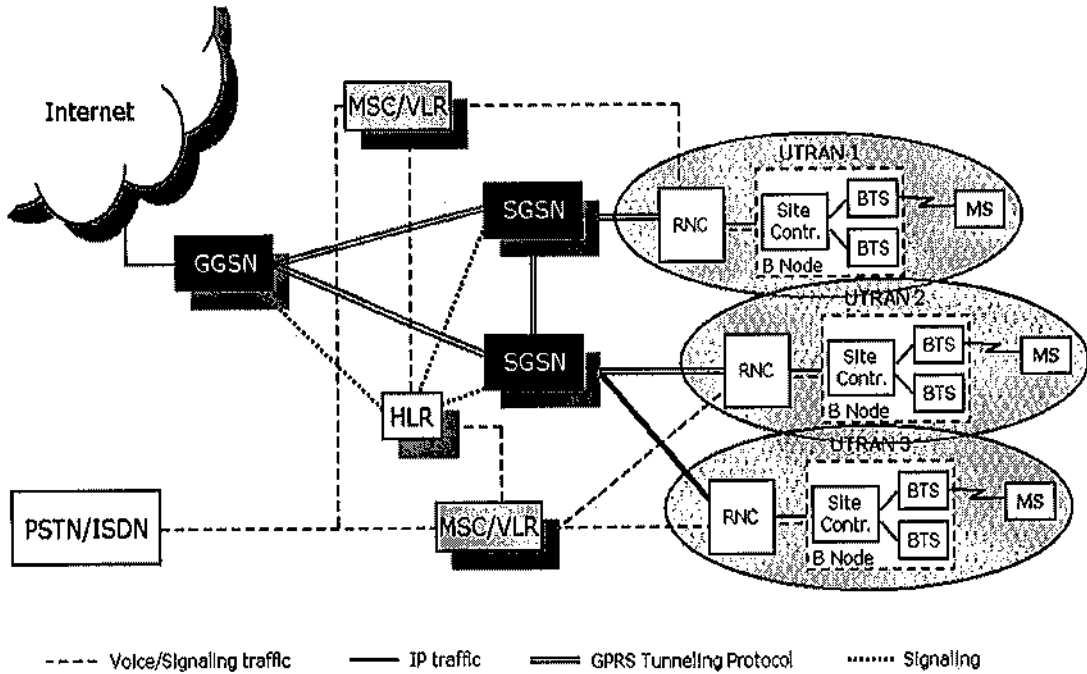


Figure (3.16) GPRS Architecture

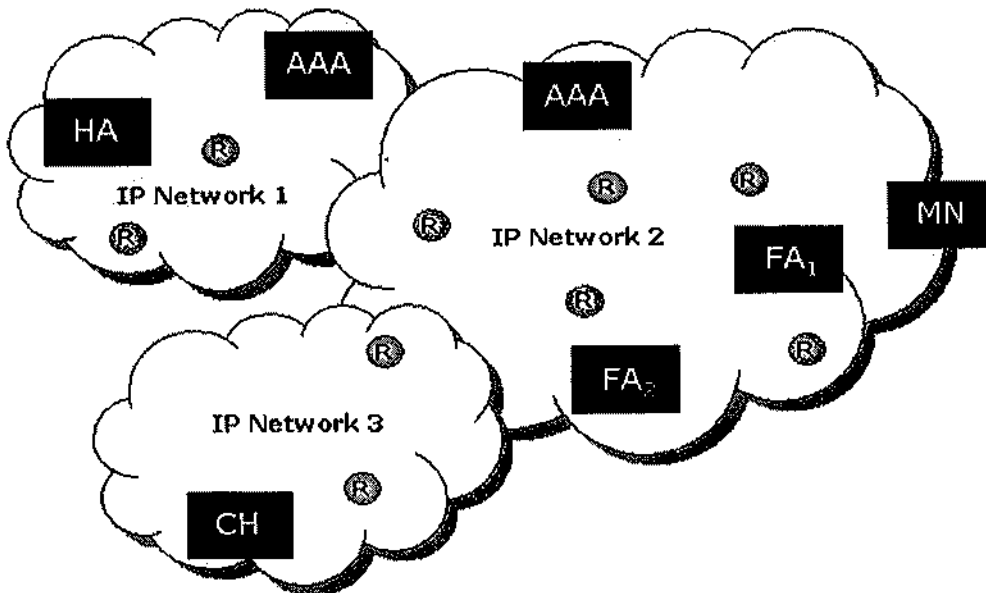


Figure (3.17) Mobile IPv4 Architecture (with Foreign Agent)

Figures (3.16) and (3.17) show the architectures of GPRS and mobile IPv4, where AAA refers to Authentication, Authorization, and Accounting protocol.

The most important differences are:

- GPRS is an access technology, while mobile IP handles mobility only, and in an access independent way.
- GPRS does not have a home agent that controls tunneling and intercepts all traffic towards the MS, as there is in mobile IP, but GPRS uses HLR that stores the users profiles and current destinations. This register also contains information related to roaming permissions and security functions.
- The GGSN node in GPRS has foreign agent functionality (as in mobile IPv4) implemented, but there are still differences between these two technologies at this point; the foreign agent functionality in GPRS is only standardized for roaming between access technologies and only the use of foreign agent care-of address is specified. The GGSN node, foreign agent in GPRS network, can (as a result of movement) have its location outside of the current provider network, which is not an option for a foreign agent care-of address in mobile IPv4.
- Mobile IP's location updating is a cumbersome procedure compared to GPRS handovers. Mobile IP tears down the tunnel all the way from the old foreign agent to the home agent, for then building a new tunnel all the way back to the new foreign agent, while GPRS (GSM and UMTS) rebuilds the needed connection only. Mobile IP in a way solves macro mobility, while GPRS solves micro mobility, i.e., mobility within an access network. The GPRS way of doing it is simpler, e.g., when the MS moves in such a way that it changes from one RNS to another RNS, which is connected to the same SGSN, only the

connection between the SGSN and the MS will need to be re-established. Mobile IP would in this case had to replace the entire connection from the home agent via the foreign agent to the MS.

- Movement of an MS results in a change of the path used in the currently ongoing session(s). These changes may cause ineffective routing. Route optimization, which can be done in mobile IP, makes bindings in such a way that the correspondent host may send directly to the foreign agent, instead of via the home agent. This is an integrated part of mobile IPv6 and an option in mobile IPv4, but the corresponding functionality is not specified in GPRS.
- The binding updates are done in different ways depending on which version of mobile IP is used. Mobile IPv4 has to do the binding updates through home agent to the correspondent nodes, while mobile IPv6 does it directly from the MS to the correspondent nodes, since routing optimization is an integrated part of mobile IPv6 and the foreign agent is an integrated part of the MS. In order for route optimization to work in mobile IPv4 the correspondent nodes need additional functionality.
- GPRS uses the GTP for internal transport of data through the IP backbone network (between SGSN and GGSN), while mobile IP uses ordinary IP routing or IP-in-IP encapsulation if that is needed.
- The foreign agent in the GPRS is a GGSN node with capability to communicate with a mobile IP home agent since it has foreign agent functionality implemented. A foreign agent in mobile IP is a normal IP router enhanced with mobile IP functionality. The GPRS functions make the GGSN foreign agent node expensive, compared to an IP router.

- The GPRS nodes, SGSN and GGSN, are designed for a close relationship with a radio access network, while mobile IP is designed for use in a wired network without the question of whether roaming is allowed or not.
- Mobile IP is using the AAA protocol for security related services. This is different in GPRS, where several registers, e.g., EIR, HLR, and VLR control these security functions. The HLR register contains important information regarded to a subscriber's location. Unfortunately, the SGSN uses the Mobile Application Protocol (MAP) for signaling to HLR. The MAP protocol is a member of the Signaling System No.7, and this makes it not compatible with the mobile IP protocol.

### **3.8.6 Mobile IP Combination with GPRS**

There are many differences between mobile IP and GPRS, but in general not in a way that makes them competitors. They are totally separate issues and a combination is possible. The fact that GPRS is an access technology that handles micro mobility management, while mobile IP handles macro mobility, suggests that they complement each other. GPRS has the possibility to support mobile IP, since mobile IP handles mobility in an access-independent way. To enable an MS use the best available access technology in an area, e.g., giving the highest bandwidth and/or the most secure connection GPRS should contain mobile IP functionality. To fully exploit the power of mobile IP, e.g., the optimized routing, mobile IP can be used in another way than specified today in the GPRS network. The mobile IP functionality can be implemented closer to or in the radio network. In this way, mobile IP can also suggest that the GPRS architecture could evolve to a simpler architecture.

The GTP is being used from RNC to SGSN and from SGSN to GGSN in UMTS GPRS. A change from GTP to IP-in-IP encapsulation will be a step towards an all IP-network,

and is to be desired to avoid too many protocol conversions. IP-in-IP encapsulation will be used if mobile IP becomes the mobility handler in the packet domain core network of GPRS.

It is desired that handovers between different access technologies should be possible, and an important aspect will be to maintain the security at all levels. This can be maintained by mobile IP's AAA function.

As a result, There are positive and negative aspects related to these technologies, but by using the best from both technologies in a combination that will be a future result, where the radio system is from GPRS and mobile IP is used for the mobility handling.

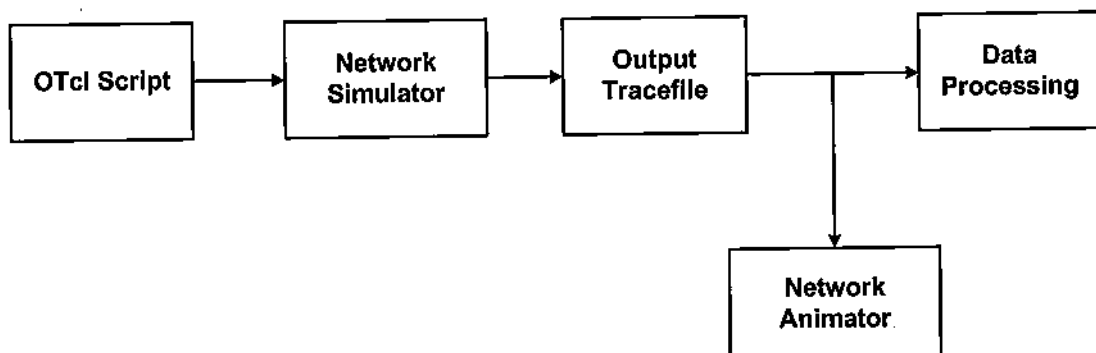
The preliminary conclusion of this discussion is that mobile IP and GPRS are two separate issues that complement each other, but that mobile IP can be used to evolve the GPRS architecture.

- 4) All the networks are interconnected using routers, in which user defined routing tables are used to simulate the selected model.
- 5) Finally, the model is verified and executed and the results can be shown in graphs or presented through reports of text format.

NS is a discrete event driven network simulator written in C++ and a script language called OTcl. It is used to simulate wired and wireless networks. NS uses an OTcl interpreter towards the user and the simulation is done as follows:

- First, an OTcl script is written which defines the network topology (number of nodes, links types), the traffic in the network (sources, destinations, type of traffic) and which protocol it to be used.
- This script is used by NS during simulation. The output of simulation is a trace file that can be used to do data processing (calculating delays, throughput, link utilization) and to visualize the simulation with the visualization tool, Network Animator (NAM).

Figure (4.1) summarizes the simulation steps in NS.



**Figure (4.1) Simulation Steps Using NS**

Since, OTcl is an object oriented scripting language, there is a tight coupling between objects in OTcl and C++, which makes it easy to move functionality between the two programming languages. This tight coupling is achieved by the use of split objects. These objects reside simultaneously in both languages and permit access to instance variables from either languages.

The wireless model in NS mainly consists of a mobile node at the core, with additional supporting features that allows simulation of multi-hop Ad Hoc networks, wireless LANs and mobile IP. The mobile node object is a split object and it consists mainly from the following components: channel; network interface; radio propagation model; Medium Access Control (MAC) protocols; Interface Queue (IfQ); Link Layer (LL) and Address Resolution Protocol (ARP) model. The scenario for mobile IP consists of home agent, foreign agent and mobile hosts moving between their home agents and foreign agents. Home and foreign agents are basically base-station nodes. Figure (4.2) shows a schematic diagram of home/foreign agent node implementation in NS.

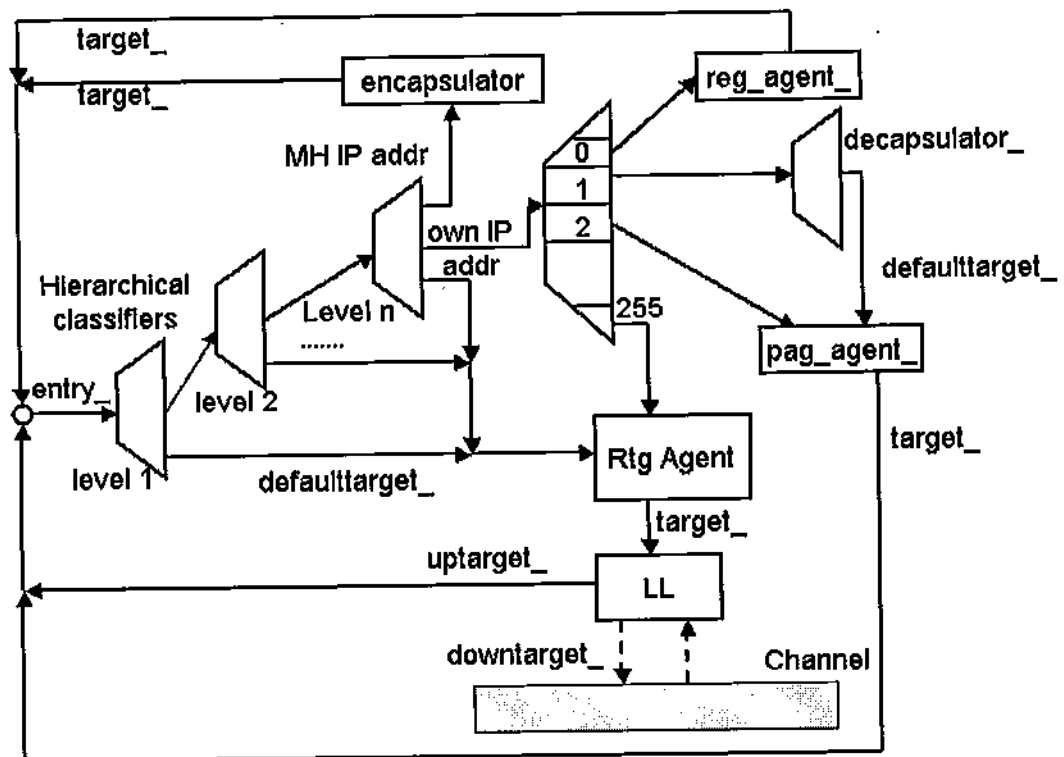


Figure (4.2) Base Station Nodes in NS



## 4.2 Hardware and Software Specifications

In this research, we study the performance of mobile IPv4 and v6 through simulation and using three simulation measures. Simulation is performed using two discrete event simulation packages specialized for networking analysis, NS2 and Commnet3. Simulation is done by building and defining a number of simulation models of two types simple and complex, where each model basically consists of:

- Wired Internet nodes with maximum buffer size of 100 Mega Byte (MB) and processing rate of 1000 Kilo Bytes / second (KB/s)
- Home and foreign agents, which are equivalent to base station nodes in GSM
- Connection links ( Ethernet, FDDI, Token ring and Wireless interfaces)
- Routers: Cisco7010 v10.0 with bus rate of 533.0 Mb/s, processing rate of 10000 KB/ms and maximum buffer capacity of 100 MB
- TCP/IP Internet protocol suite, Microsoft v.1 with the IEEE 802.11 wireless Medium Access Control (MAC) protocol with 5 Mb/s bandwidth
- The shared media wireless interface parameters are set to make it work like the 914 MHz lucent wave LAN Direct Sequence Spread Spectrum Radio Interface (DSSSRI) with:
  1. Capture threshold power = 10 dB
  2. Carrier sense threshold power =  $1.559 * \exp(-10)$
  3. Receiver power threshold =  $3.652 * \exp(-10)$
  4. Carrier sense threshold power = 1.0 dB
  5. Wireless system loss factor = 1 dB
  6. Wireless working frequency = 914 MHz
  7. Transmitter power = 0.302 Watt
  8. Antenna type : Omni directional antenna (used in mobile systems)

In the simple case model, single mobile node is assumed firstly attached to its home network through registration with its home agent. Then, it starts moving to a foreign link at a constant speed of 20 m/s, while traffic still destined to that mobile node during the movement stage.

The results of simulation including the three previously mentioned performance measures (Delay, Link utilization and Throughput) are stored in a trace file or can be demonstrated on screen.

Regarding this study, the hardware and software specifications used throughout the development of this work are listed in Tables (4.1) and (4.2), respectively.

**Table (4.1) Hardware Specifications**

Hardware	Specifications
Computer	Pentium II; 400 MHz processor; 128 MB RAM; Windows XP

**Table (4.2) Software Specifications**

a) Commnet III v1.1d	Specifications
Computer and communication nodes	To simulate Internet host; maximum buffer size =100 MB and processing capability of 1000 KB/second
Links	Ethernet; the IEEE 802.11 5Mbps wireless Ethernet standard, Token Ring; 802.5 16Mbps, FDDI with bandwidth of 100 Mbps and frame maximum bytes = 4500. Point-to-Point links are used for Wide Area Networks (WANs) connectivity with a bandwidth of 2.048 Mbps.

Message sources	Used to represent traffic load based on the TCP/IP v.1-Microsoft protocol with payload = 1000 bytes, overhead = 50 bytes, window size = 10, and retransmit time = 500 ms. Message size is taken as a random process with uniform distribution of 1000 packet/message on average, and it may be changed based on the type of the message.
Routers	Cisco, 7010 SP v 10.0, routers are used to simulate the operation of home, foreign agents, and traditional routing functions. They are configured with bus rate = 533.0 Mbps. Processing rate = 10000 Kbytes/ms, and maximum buffer capacity = 100 M bytes.
Response sources	Used as acknowledgements to assure the reception of a transmitted message. A payload of 200 bytes and header of 50 bytes are used throughout the simulation.

b) NS	Specifications
Simulation time	200 seconds
Coverage radius	600 meter
Number of base station nodes	2 nodes
Home/foreign agents configuration	Set HA [\$ns_ node 1.0.0] Set FA [\$ns_ node 2.0.0]
Channel type	Wireless
Interface queue type	Drop Tail/ Primary queue
MAC type	802_11; It handles collision detection, fragmentation, and collision. It is A carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol.
Maximum packet size in Queue	50
Number of mobile nodes	1
Radio propagation model	Two-ray ground
Antenna Model	Omni antenna
Dimension of Topology	600 x 600
Traffic type	Constant bit rate
Time between retransmitted requests	3 seconds
Periodic route update interval	8 seconds
Route advertisement time	2 seconds
Maximum packets buffered per node per destination	10 packets
Transmission power	0.302 Watt

Link layer minimum delay	50 Microseconds
System loss factor	1.0
Raw bit rate	$2 * \exp(6)$
Receiver power threshold	$3.652 * \exp(-10)$
Carrier sense threshold	$1.558 * \exp(-11)$
Capture threshold (in decibel)	10.00
TCP packet size	1460 bytes

## 4.3 Mobile IP Simulation Source Code

```

## wireless-mobileIP-simulation
#           o W1           WIRED NODES
#           |
#           o W2
#           /\
#           /\
#...*-*-*-*-*-*-*-* o o base-stn nodes --*-*-*-*-*-*-*
#           HA   FA
#           o
#           o WL   o WIRELESS NODE MOVING
#           WL     WL FROM HA TO FA.
#
#
#options
set opt(chan)           Channel/WirelessChannel
set opt(prop)           Propagation/TwoRayGround
set opt(netif)          Phy/WirelessPhy
set opt(mac)            Mac/802_11
set opt(ifq)            Queue/DropTail/PriQueue
set opt(ll)             LL
set opt(ant)            Antenna/OmniAntenna
set opt(x)              670   ;# X & Y dimension of the topography
set opt(y)              670   ;# hard wired for now...
set opt(rp)             dsr    ;# routing protocols: dsdv/dsr
set opt(ifqlen)         50     ;# max packet in ifq
set opt(seed)           0.0
set opt(stop)           250.0   ;# simulation time
set opt(cc)             "off"
set opt(tr)             wireless-mip-out.tr   ;# trace file
set opt(cp)             ""
set opt(sc)             ""
set opt(ftp1-start)    100.0
#
=====

====
set num_wired_nodes  2
set num_bs_nodes     2
set num_wireless_nodes 1
set opt(nn)          3   ;# total number of wireless nodes
#=====

=====
# Other class settings
set AgentTrace       ON
set RouterTrace      OFF
set MacTrace         OFF
LL set mindelay_     50us

```

```

LL set delay_          25us
Agent/Null set sport_  0
Agent/Null set dport_  0
Agent/CBR set sport_   0
Agent/CBR set dport_   0
Agent/TCPSink set sport_ 0
Agent/TCPSink set dport_ 0
Agent/TCP set sport_   0
Agent/TCP set dport_   0
Agent/TCP set packetSize_ 1460
Queue/DropTail/PriQueue set Prefer_Routing_Protocols 1
# unity gain, omni-directional antennas
# set up the antennas to be centered in the node and 1.5 meters above it
Antenna/OmniAntenna set X_ 0
Antenna/OmniAntenna set Y_ 0
Antenna/OmniAntenna set Z_ 1.5
Antenna/OmniAntenna set Gt_ 1.0
Antenna/OmniAntenna set Gr_ 1.0
# Initialize the SharedMedia interface with parameters to make
# it work like the 914MHz Lucent WaveLAN DSSS radio interface
Phy/WirelessPhy set CPTthresh_ 10.0
Phy/WirelessPhy set CSTthresh_ 1.559e-11
Phy/WirelessPhy set RXTthresh_ 3.652e-10
Phy/WirelessPhy set Rb_ 2*1e6
Phy/WirelessPhy set Pt_ 0.2818
Phy/WirelessPhy set freq_ 914e+6
Phy/WirelessPhy set L_ 1.0
#
=====
====
#source ../lib/ns-bsnode.tcl
#source ../mobility/com.tcl
#source ../mobility/dsr.tcl
#source ../lib/ns-mip.tcl
source ../lib/ns-wireless-mip.tcl
# intial setup - set addressing to hierarchical
set ns [new Simulator]
$ns set-address-format hierarchical
# set mobileIP flag
Simulator set mobile_ip_ 1
set namtrace [open wireless-mip.nam w]
$ns namtrace-all $namtrace
set trace [open wireless-mip.tr w]
$ns trace-all $trace
AddrParams set domain_num_ 3
lappend cluster_num 2 1 1

```

561395

```

AddrParams set cluster_num_ $cluster_num
lappend eilastlevel 1 1 4 1
AddrParams set nodes_num_ $eilastlevel
##debug 1
## setup the wired nodes
set temp {0.0.0 0.1.0}
for {set i 0} {$i < $num_wired_nodes} {incr i} {
    set W($i) [$ns node [lindex $temp $i]]
}
## create common objects reqd for wireless sim.
if { $opt(x) == 0 || $opt(y) == 0 } {
    puts "No X-Y boundary values given for wireless topology\n"
}
set chan [new $opt(chan)]
set prop [new $opt(prop)]
set topo [new Topography]
set tracefd [open $opt(tr) w]
# setup topography and propagation model
$topo load_flatgrid $opt(x) $opt(y)
$prop topography $topo
# Create God
create-god $opt(nn)
## setup ForeignAgent and HomeAgent nodes
set HA [create-base-station-node 1.0.0]
set FA [create-base-station-node 2.0.0]
#provide some co-ord (fixed) to these base-station nodes.
$HA set X_ 1.000000000000
$HA set Y_ 2.000000000000
$HA set Z_ 0.000000000000
$FA set X_ 650.000000000000
$FA set Y_ 600.000000000000
$FA set Z_ 0.000000000000
# create a mobilenode that would be moving between HA and FA.
# note address of MH indicates its in the same domain as HA.
set MH [$opt(rp)-create-mobile-node 0 1.0.2]
set HAaddress [AddrParams addr2id [$HA node-addr]]
[$MH set regagent_] set home_agent_ $HAaddress
# movement of the MH
$MH set Z_ 0.000000000000
$MH set Y_ 2.000000000000
$MH set X_ 2.000000000000
# starts to move towards FA
$ns at 100.000000000000 "$MH setdest 640.000000000000 610.000000000000
20.000000000000"
# goes back to HA

```



```

$ns at 200.000000000000 "$MH setdest 2.000000000000 2.000000000000
20.000000000000"
if { $opt(x) == 0 || $opt(y) == 0 } {
    usage $argv0
    exit 1
}
if { $opt(seed) > 0 } {
    puts "Seeding Random number generator with $opt(seed)\n"
    ns-random $opt(seed)
}
#
# Source the Connection and Movement scripts
#
if { $opt(cp) == "" } {
    puts "*** NOTE: no connection pattern specified."
    set opt(cp) "none"
} else {
    puts "Loading connection pattern..."
    source $opt(cp)
}
if { $opt(sc) == "" } {
    puts "*** NOTE: no scenario file specified."
    set opt(sc) "none"
} else {
    puts "Loading scenario file..."
    source $opt(sc)
    puts "Load complete..."
}
# create links between wired and BaseStation nodes
$ns duplex-link $W(0) $W(1) 5Mb 2ms DropTail
$ns duplex-link $W(1) $HA 5Mb 2ms DropTail
$ns duplex-link $W(1) $FA 5Mb 2ms DropTail
$ns duplex-link-op $W(0) $W(1) orient down
$ns duplex-link-op $W(1) $HA orient left-down
$ns duplex-link-op $W(1) $FA orient right-down
# setup TCP connections between a wired node and the MobileHost
set tcp1 [new Agent/TCP]
$tcp1 set class_ 2
set sink1 [new Agent/TCPSink]
$ns attach-agent $W(0) $tcp1
$ns attach-agent $MH $sink1
$ns connect $tcp1 $sink1
set ftp1 [new Application/FTP]
$ftp1 attach-agent $tcp1
$ns at $opt(ftp1-start) "$ftp1 start"
#

```

```

# Tell all the nodes when the simulation ends
#
for {set i 0} {$i < $num_wireless_nodes } {incr i} {
    $ns_ at $opt(stop).0000010 "$node_($i) reset";
}
$ns_ at $opt(stop).0000010 "$HA reset";
$ns_ at $opt(stop).0000010 "$FA reset";
$ns_ at $opt(stop).21 "finish"
$ns_ at $opt(stop).20 "puts \"NS EXITING...\" "; "
###$ns_ halt"
proc finish { } {
    global ns_ trace namtrace
    $ns_ flush-trace
    close $namtrace
    close $trace
    #puts "running nam..."
    #exec nam out.nam &
    puts "Finishing ns.."
    exit 0
}
puts $tracefd "M 0.0 nn $opt(nn) x $opt(x) y $opt(y) rp $opt(rp)"
puts $tracefd "M 0.0 sc $opt(sc) cp $opt(cp) seed $opt(seed)"
puts $tracefd "M 0.0 prop $opt(prop) ant $opt(ant)"
puts "Starting Simulation..."
$ns_ run

```

## Analysis and Simulation of Mobile IP Protocol

In this thesis we are interested in evaluating the performance of the mobile IP protocol, concentrating on its main functionalities. In order to do so, we have done some experiments based on an assumed simulation models. These simulation models are studied depending on some performance measures which are delay, link utilization and throughput. Delay or mean delay is one of the basic measures in communication and computer networks which refer to the time needed to receive a response for a message sent from a certain point in the network, where throughput is a measure of how much traffic is successfully received at the intended destination. These experiments and the results we have drawn are presented in this chapter.

### 5.1 Simple Model

This model consists of:

- A single mobile node which transferred from its home network to a foreign network.
- A correspondent node belonging to another network that wants to get access to the mobile node.

This model illustrates the simplest case of any mobile IP architecture. This scenario is shown in Figure (5.1).

In this experiment, we want to measure the time it took for a packet to travel from a fixed host (the correspondent node) to a mobile node on the foreign network, and to compare this with the time when the mobile node is at home. The results are:

Maximum travel time = 105.62 ms

Minimum time = 79.56 ms

Average roundtrip time = 91.47 ms

Standard deviation = 8.04 ms

The message size is assumed uniformly distributed with average 1000 packet, where the packet size is fixed at 1000 byte.

The next step is to measure the time it took for sending a message to a mobile node when it is at home, our assumed model is shown in Figure (5.2).

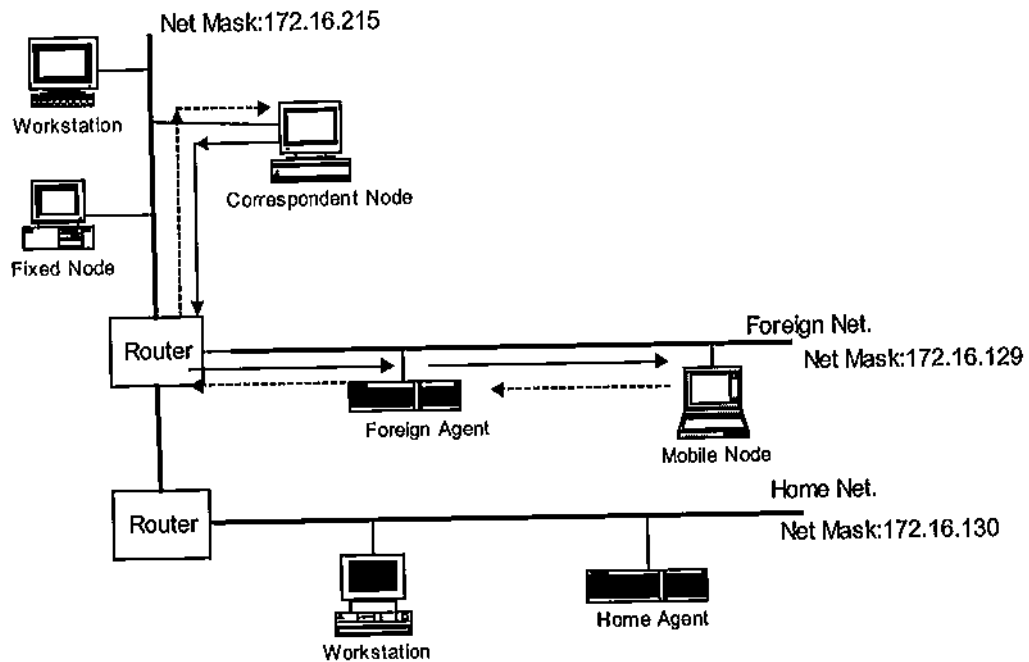


Figure (5.1) Mobile IP Simple Scenario

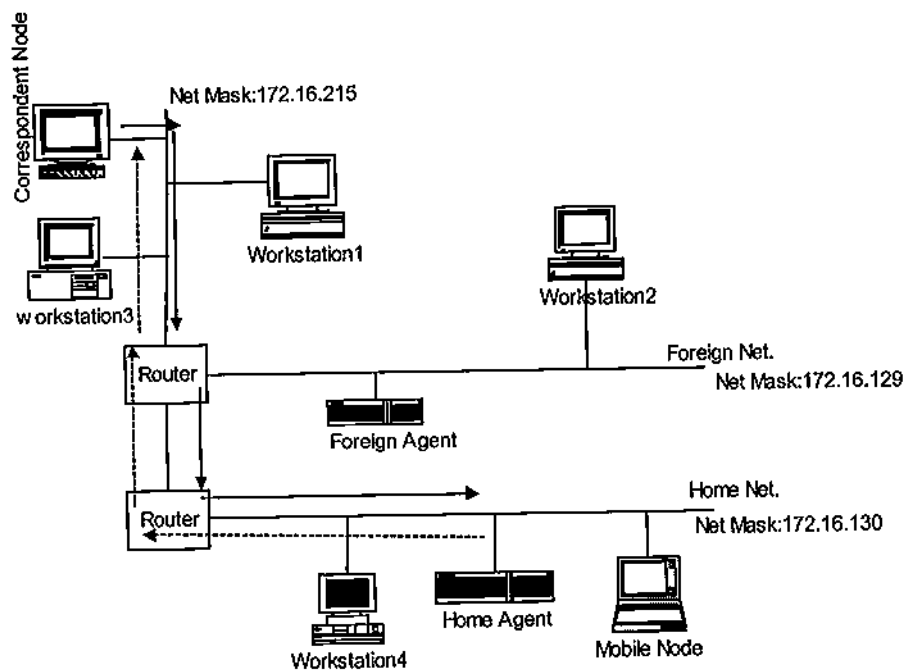


Figure (5.2) Mobile Node at Home

The results in this experiment are:

Maximum time = 73.4 ms

Minimum time = 44.6 ms

Average roundtrip time = 66.7 ms

Standard deviation = 7.6 ms

It is expected that the roundtrip time in this case be much smaller than the first one, and as we see, there is relatively, a big difference between the average round trip times in the two cases above and this is because packets are routed through the home agent in the first case, which is known as the triangle routing problem.

Using the model shown in Figure (5.2), we want also to measure the time it takes to send a message from home agent node to foreign agent node, the results are:

Maximum time = 50.5 ms

Minimum time = 28.4 ms

Average roundtrip time = 33.3 ms

Standard deviation = 2.9 ms

The results for the time it takes to send a message from foreign agent to mobile node are:

Maximum time = 35.2 ms

Minimum time = 19.4 ms

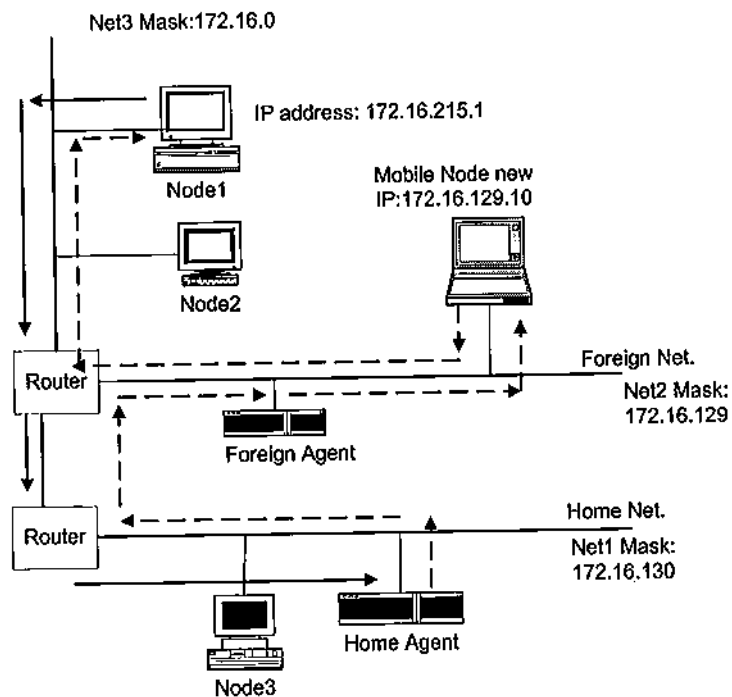
Average roundtrip time = 27.6 ms

Standard deviation = 2.2 ms

## 5.2 Encapsulation Techniques Tests

In this experiment, we measure the delay resulted from the two encapsulation techniques used in mobile IP, Minimal encapsulation, and IP-in-IP encapsulation. We make use of the model shown in Figure (5.3) to do this.

In the first test, node1 sends a message to the mobile node's home network, which has the netmask: 172.16.130. This message is captured by the home agent which encapsulates the received message and sends it to the foreign agent through a tunnel. Foreign agent decapsulates the received tunnel and forwards the original message to the mobile node. Upon receiving the message, mobile node sends a reply directly to the correspondent node (node1) without the help of neither foreign agent nor home agent, and this is because the IP address of the transmitter has been known.



**Figure (5.3) Encapsulation Methods Tests**

The results for minimal encapsulation are:

Maximum time = 102 ms

Minimum time = 81.6 ms

Average round trip time = 87.65 ms

Standard deviation = 3.64 ms

For IP-in-IP encapsulation the results are:

Maximum time = 112 ms

Minimum time = 82.9 ms

Average round trip time = 90.75 ms

Standard deviation = 2.24 ms

In this test we assume a message size of uniform distribution with average at 1000 packets/message. The results show that there is no big difference between the average round trip times in the two encapsulation tests, where it is expected that the time needed by minimal encapsulation is smaller since it is used to remove the redundant information carried by the encapsulating outer IP header and the encapsulating inner IP header in the IP-in-IP encapsulation.

In the next test, the delay caused by encapsulation/decapsulation at the different entities in the process of transmission and reception will be discussed. In the first test, we measure the total overhead time the protocol caused in the communication between a stationary node and a mobile one.

When the home agent receives a message that is destined to one of the mobile nodes that it is serving, basically, it does two operations:

- First, it looks up the mobile node in the registration table to get its care-of address.
- Once finding the care-of address, it encapsulates the packet and sends it.

We use the same reference model shown in Figure (5.3) to measure the time spent by the home agent from that it has received the packet until the packet is encapsulated but not sent. Still we use the same two encapsulation methods as above. The message size is assumed to be 1000 packet/message on average and with uniform distribution.

The simulation is done and the results are as follows:

For IP-in-IP encapsulation:

Maximum time = 19.75 ms

Minimum time = 9 ms

Average time = 12.47 ms

Standard deviation = 1.6 ms

For Minimal encapsulation:

Maximum time = 18.3 ms

Minimum time = 5 ms

Average time = 11.5 ms

Standard deviation = 1.2 ms

The results show a small difference between the two encapsulation techniques, with 0.95 ms minimal encapsulation time smaller than IP-in-IP encapsulation as we expect. Foreign agent, as with the home agent, has to do two things to do once it receives a packet:

- First, it checks if this packet should be forwarded.
- If so, it decapsulates the packet and forwards it to the destined mobile node.
- Otherwise, it forwards it without decapsulation using wired routing algorithms.

In this test, the time spent by the foreign agent handling the packet from the moment it receives the packet to when it has decapsulated but not yet sent, will be measured.

Once again Figure (5.3) is used.

The results are as follows:

IP-in-IP encapsulation:

Maximum time = 15.4 ms

Minimum time = 4.5 ms

Average time = 7.95 ms

Standard deviation = 0.75 ms



The results show that, there is not large difference between home/foreign agents IP-in-IP encapsulation times, where it is smaller for foreign agent by nearly 4 ms.

For Minimal encapsulation:

Maximum time = 14 ms

Minimum time = 4.5 ms

Average time = 6.75 ms

Standard deviation = 0.685 ms

The difference between the average encapsulation/decapsulation time in the two techniques =  $7.95 - 6.75 = 1.2$  ms which is not so large since the two operations are nearly similar in complexity.

From the previous delay analysis that we have done we conclude the following:

- The time to process a packet at the home and foreign agent constitutes a large portion of the total time to deliver the packet to its destination.
- This part of total time will decrease when sending the packets for longer distances. Although it can be optimized and this is what was done in mobile IPv6, where foreign agent is discarded and mobile node can connect to its corresponding directly.
- It is found that there are no large differences between the two encapsulation techniques used in mobile IP.

### 5.3 Registration Delay Tests

Registration is the process by which mobile node requests service from a foreign agent on a foreign link and informs its home agent about its new care-of address. Apart from the additional latency mobile IP protocol introduces, registration time is another time value of interest from the mobile node's side. It is the time to set up a connection after it had arrived at the foreign link. This time includes the time to get information about

which foreign agents that are currently available, and the time to set up the connection by registering with the home agent.

The objectives of this test are:

- To measure the solicitation time; the time from the first solicitation sent by the mobile node until it received a registration request. Solicitations are the messages sent by mobile node when it is connected to a new link, searching for any available foreign agent to be served.
- To measure the time from the first advertisement sent by foreign/home agents until a valid registration request is sent by mobile node. An advertisement is the message sent by home/foreign agents to announce their presence.
- To measure the time from the first registration request is sent by the mobile node until a valid registration reply is received.
- To measure the complete registration time (signaling time), from first solicitation until the first valid registration reply.

In this test we use the model shown in Figure (5.4). The results of registration delay measurements are shown in Table (5.1).

**Table (4.1) Results of Registration Delay**

Registration delay	Solicitation time (s)	Advertisement time (s)	Registration request time	Signaling time(s)
Maximum	2.00	0.40	0.928	2.95
Minimum	0.150	0.065	0.680	0.804
Average	1.25	0.247	0.820	2.105
Standard dev.	0.250	0.035	0.095	0.450

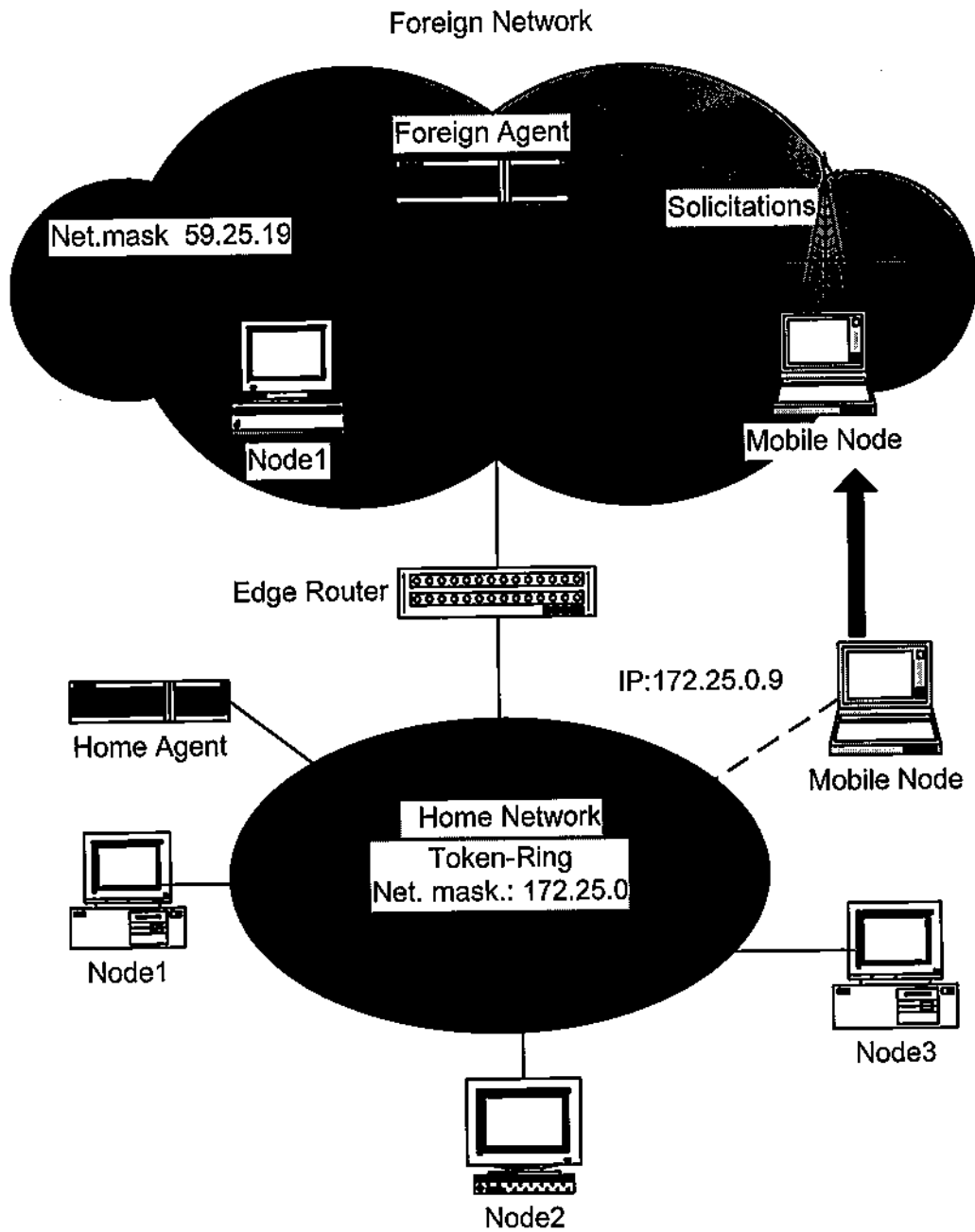


Figure (5.4) Registration Delay Module

The results above show that over 67.7 % of the time is spent in solicitation phase where the mobile node is trying to contact a foreign agent. This is because there are a number of packets that have to be sent before the first registration request can be transmitted. Firstly, mobile node sends agent solicitation as a broadcast message. When this packet has been received and processed by the foreign agent, it sends an ARP request to get the mobile node sub-network address. This is done in order for the foreign agent to send an agent advertisement to the correct sub-network address. Once mobile node has received the agent advertisement, it has to send an ARP message to get the sub-network address of the foreign agent where the foreign agent IP address has been known for it. Finally, the foreign agent sends an IP reply to the mobile node which now can send its first registration request. From another point of view, mobile node has to send a large number of solicitations, not less than 7, before the first agent advertisement is received, and this is why this time is large.

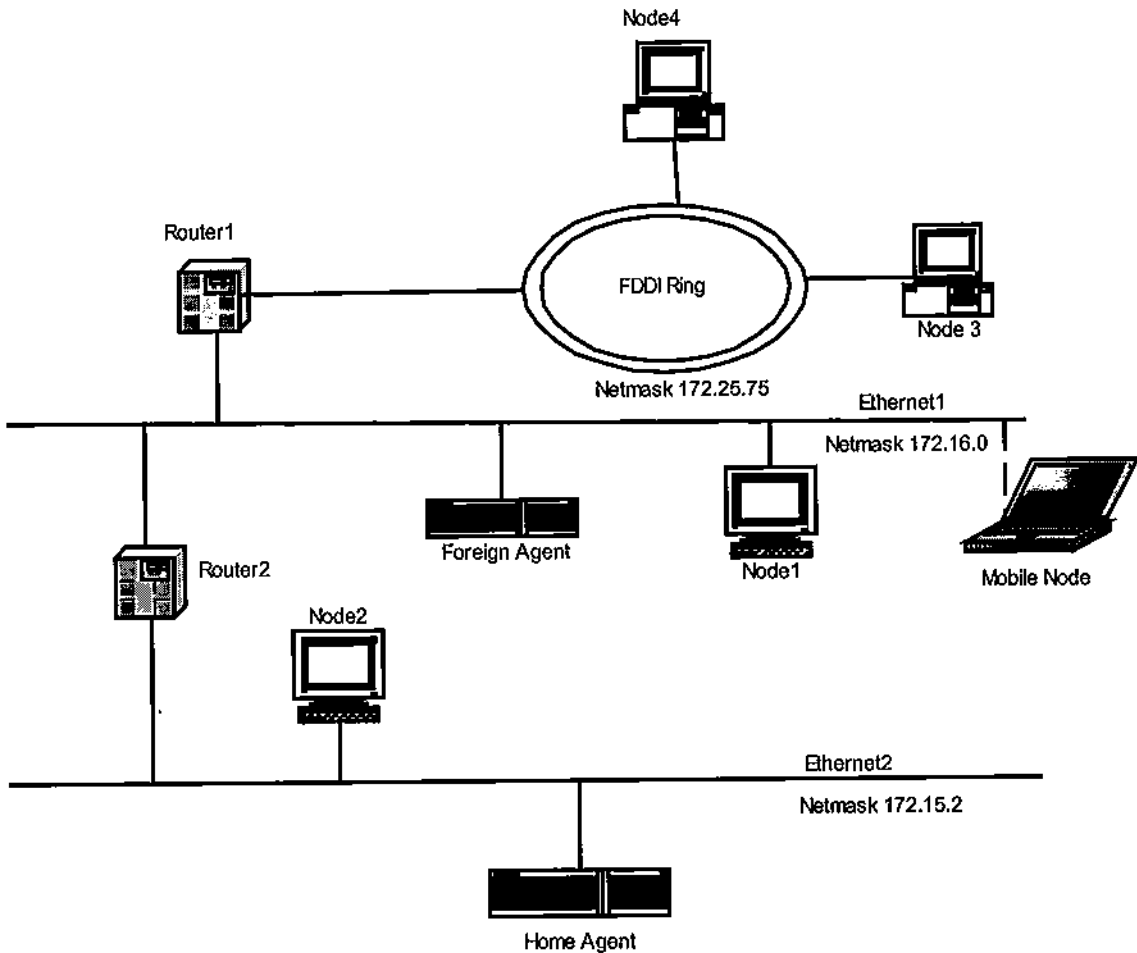
Sometimes, the time between the first solicitation and first advertisement is extremely low and this is because foreign agent multicasts agent advertisement within a short time after the mobile node has entered his zone, and there is no need for the mobile node to send any agent solicitation at all.

#### **5.4 Throughput Analysis of Mobile IP**

The main aim of this section is to find how many packets per second are actually received by the mobile node when the packets are tunneled at constant rate, compared to the rate at which a stationary system could handle.

In this test we use the scenario shown in Figure (5.5). In this experiment we set a message of uniform distribution with an average of 1000 packets/message. This message will be sent from node3 to both mobile node and node1 on Ethernet1. The paths in both cases are shown in Figure (5.6).

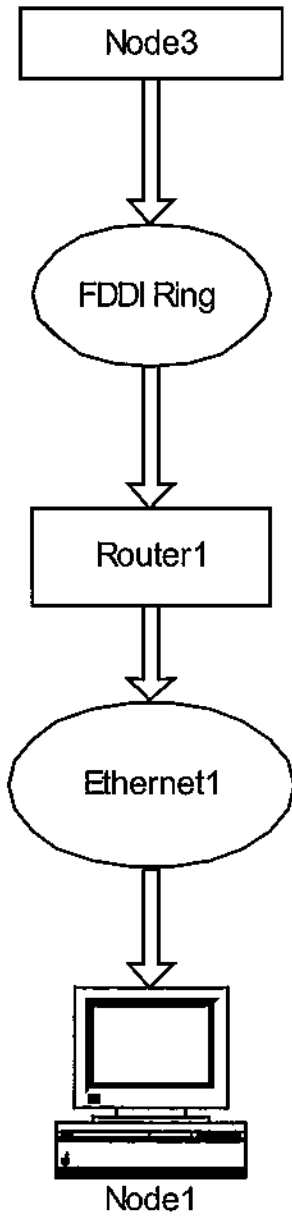
This experiment was done 100 times for each case, each time lasts for 5 minutes and the results are listed in Table (5.2) for the first case and in Table (5.3) for the second one.



**Figure (5.5) Proposed Model for Throughput Analysis**

In our analysis we only consider the effect of adding home/foreign agents in the way to mobile node, other factors are the same in the two cases. It can be seen that a lot of packets were lost at the home agent in the first case. This is because home agent has large traffic to handle and so it didn't take care of all incoming packets. The packets that were delivered from home agent almost reached the foreign agent with small losses and then to the mobile node. In the fixed routing case, a very small number of packets are lost in the way between the two fixed nodes.

## Second case



## First case

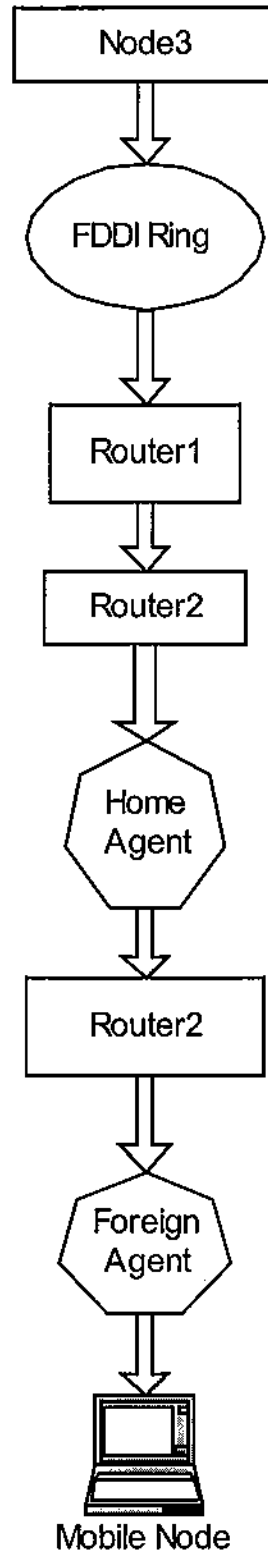


Figure (5.6) Routing Paths for Mobile and Fixed Nodes

### 1. First case: Routing to mobile node

**Table (5.2) Routing to Mobile Node**

Throughput of mobile IPv4	Number of packets sent from node3	Number of packets received by home agent	Number of packets received by foreign agent	Number of packets received by mobile node
Maximum	10000	8890.9	8780.0	8760.56
Minimum	10000	5600.5	5548.6	5530.7
Average	10000	7125.0	7101.0	7100.2
Standard dev.	0.0000	580.3	578.78	576.4

### 2. Second case: Routing to fixed node

**Table (5.3) Routing to Fixed Node**

Throughput of mobile IPv4	Number of packets sent from node3	Packets received by node1
Maximum	10000	9996.56
Minimum	10000	9987.7
Average	10000	9995.2
Standard dev.	0.0000	3.2

It is the same topology used previously except that there is no foreign agent, and the other functionalities of mobile IPv6 are activated here. The results are shown below:

Maximum delay time: 64.5 ms

Minimum delay time: 42.6 ms

Average delay time: 56.75 ms

Standard deviation: 4.2 ms

Changing the message size to be uniform with an average of 500 packets, we obtain the following:

Maximum delay time: 25 ms

Minimum delay time: 15 ms

Average delay time: 18.27 ms

Standard deviation: 1.56 ms

Using a more complicated scenario as shown in Figure (5.8), this figure shows a scenario in which more than one mobile hosts (mobile node A, mobile node B) migrate from their home networks to foreign ones. The aim here is to discuss how correspondent nodes (CAN, CNC, CND) can reach mobile nodes and to find the delay associated with each case.

- First, mobile node A migrates from its home network to network C, it gets a care-of address from the edge router on that link, and starts sending binding updates to its correspondents. It also notifies its home agent of its new care-of address.
- CND wants to send to mobile node A, since CND has received a binding updates from this mobile node, it can start sending packets directly to the care-of address of mobile node A, without the aid of home and foreign agents as in mobile IPv4. This will save time.



- Mobile node A can also reach mobile node B on its home network directly via home agent A since it knows the care-of address of mobile node B through the binding updates that has been sent.

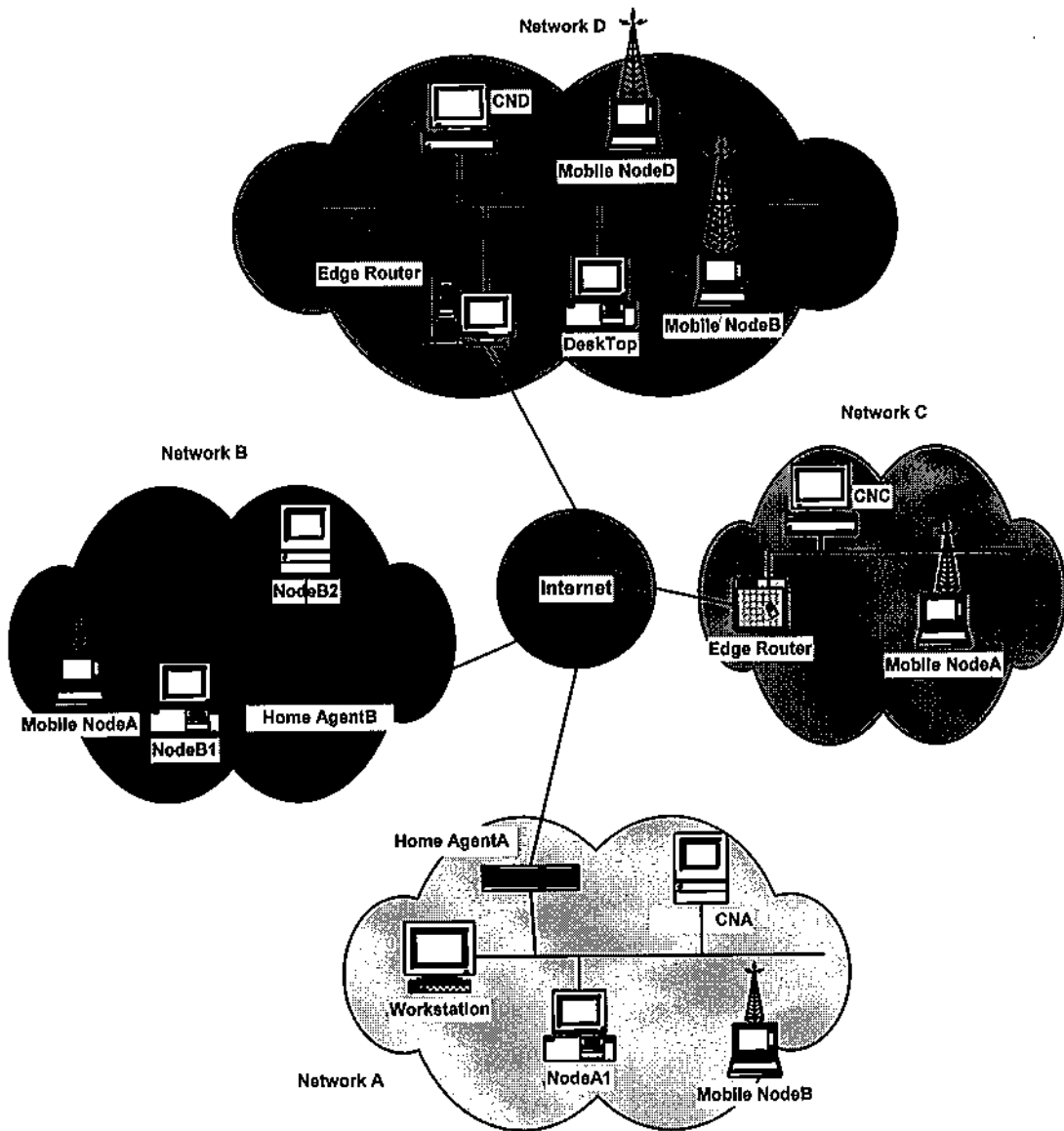


Figure (5.8) Mobile IPv6 Delay for Real Model

- Mobile node A decides to go to network B, while in flight across the way, all packet destined to this node are stored in the edge router of network C.

- Once reached network B, mobile node A registers with home agent B, gets new care-of address, and starts sending binding updates to inform its correspondents of its new care-of address.
- After receiving the binding updates, the edge router of network B can now delete the old care-of address of mobile node A and sends the stored packet to the new care-of address of this node.
- Unlike mobile IPv4, CNA is another correspondent node at the network A, it can reach mobile node B on its foreign link (Network D) directly through the edge router of this network and without the aid of home agent B.
- Any packets sent by any of the correspondent node that is not notified with the new care-of address of the destination mobile node are routed just as in mobile IPv4.

The results of delay measurement using the scenario shown above are listed in Table (5.4). These measurements are taken assuming that the source is CNC and the destination is the mobile node A, which is moving from its home link to network B.

**Table (5.4) Delay Measurements in Mobile IPv6**

	Binding update delay (ms)	Routing delay (ms)	Tunneling delay (ms)	Registration delay (ms)
Maximum delay	100	250	78	50
Minimum delay	79	160	48.5	34.99
Average delay	82	190	63.8	42.7
Standard dev.	3.8	15.6	10.5	2.2

The results obtained show that delays in mobile IPv6 are less than that of mobile IPv4 by comparing the results of tables (5.1) and (5.4). Namely, registration delay is so small in mobile IPv6 and this because the IPv6 functionalities like auto-configuration discovery and statefull address auto-configuration are designed to solve delay problems in mobile IPv4.

Delay also is measured assuming CND on network D is trying to get contact with node B on the foreign link A. The results are drawn and listed in Table (5.5).

In this test the same message size is considered as above, but the results shows that routing delay here is larger than the previous case and this is because the routing path is relatively larger. Also, by referring to Figure (5.8) above, the edge router at network B is of different type. But still the registration time, for example, is less than that for mobile IPv4. It is expected that there is no big difference between the two binding update delays, on the contrary, the results show that the binding delay in the second case is 1.5% of that in the first case (Table (5.4)). The reason for this may be related to the load at the time of taking these values.

**Table (5.5) Delay Measurements from CND to Mobile Node B**

	Binding update delay (ms)	Routing delay (ms)	Tunneling delay (ms)	Registration delay (ms)
Maximum delay	170	380	120	86.6
Minimum delay	95	225.82	71.7	59.95
Average delay	145	315.25	94.56	74.67
Standard dev.	22	42.7	20.5	6.9

Regarding encapsulation, it is nearly the same as used in mobile IPv4, so we expect no major differences in the delay.

Of course, there are many other factors which affect the delay, such as, faults on the network, traffic, and physical layer errors.

### 5.6 Throughput Analysis of Mobile IPv6

Throughput is a measure of how much traffic is successfully received at the intended destination per unit of time. The maximum throughput is equivalent to the system capacity. Ideally, throughput is the same as the offered load, which is the amount of traffic actually transmitted in the cases where the channel is error free. In general, throughput may only equal the offered load up to the system capacity. Here, the system capacity is a measure of the quantity of traffic which the system can cope.

In this study of throughput and referring to the scenario shown in Figure (5.8), a number of experiments have been done. In each one a number of packets, namely 3000 on average, are sent from a source node as a multicast. The difference between these experiments is the rate with which the packets are sent. The results are shown in the following tables.

The first table of data, Table (5.6), shows that a small number of packets are lost, this is because the transmission time is relatively large.

**Table (5.6) Throughput over 150 Seconds Transmission Time**

	Packets sent by home agent B	Period of transmission (second)	Packets received by mobile node A	Packets received by mobile node B	Packets received by mobile node D
Maximum	3000	150	2999.5	2998.2	2997.5
Minimum	3000	150	2996.4	2995.1	2997.1
Average	3000	150	2998	2997.2	2997.4
Standard dev.	0.000	0.000	1.3	1.5	0.6

In the second test, the same number of packets is transmitted over a period of 100 seconds and the results are shown in Table (5.7).

**Table (5.7) Throughput Analysis (period = 100 seconds)**

	Packets received by edge router D	Packets received by node A1	Packets received by mobile node A	Packets received by mobile node B	Packets received by home agent A
Maximum	2995	2997	2985.5	2994.2	2992.3
Minimum	2990	2989.6	2969.4	2991.1	2987.1
Average	2992	2994.8	2977.2	2993.2	2990.4
Standard dev.	1.070	2.12	8.3	1.067	3.6

Still the results show no large difference between the two set of data above except for the mobile node A in the second case, where it is assumed that it isn't connected to its home link, for this reason the number of packets received by this node are less than that received by the other nodes. From a comparison point of view, the percentage loss of packets for edge router D is 0.26% and for mobile node A it is 0.76%. This means that out of 140 packets sent to mobile node A, one packet is being lost, which is acceptable. It is worth to note that the percentage difference between the maximum and minimum number of messages received is not so large, and this is since we assume error free link. The next table contains the same criteria stated above but over a transmission period of 50 seconds, the results are shown in Table (5.8).

**Table (5.8) Throughput over 50 Seconds Transmission Time**

	Packet received by CND	Packets received by edge router D	Packets received by mobile node A	Packets received by mobile node B	Packets received by home agent A
Maximum	2985	2985	2980.7	2977.2	2991.3
Minimum	2974.2	2975.6	2970.6	2963.1	2972.1
Average	2980.23	2982.9	2974.2	2972.2	2981.4
Standard dev.	4.6	2.8	6.4	5.8	12.45

It is clear from this data that the number of packets lost on the route between the edge router D and CND is negligible, where there are about 0.57% of packets lost in the way to edge router D. This is reasonable, since CND is a fixed node on network D and the local path is considerably shorter than the routing path through the Internet. Paths to mobile nodes have more lost packets here, and this referred to the decrease in the time of transmission and larger size of traffic on the network at that moment. The worst case is for mobile node B where it suffers from a percentage number of lost packets up to 0.9266% which is here assumed to have a care-of address at link D. On the other hand, it is noted that there is no big difference between the number of packets received by mobile nodes A and B.

In the last test of throughput analysis, a transmission time of 20 seconds is taken to multicast a message of 3000 packets in size. The results are shown in Table (5.9).

**Table (5.9) Throughput over 20 Seconds Transmission Time**

	Packet received by mobile node D	Packets received by edge router D	Packets received by mobile node A	Packets received by mobile node B	Packets received by home agent A
Maximum	1958	2700	2370.8	2763.2	2650.3
Minimum	1620	2604	1800	2490.6	2372.18
Average	1702	2650	1990	2670	2521.4
Standard dev.	245	25	310	259	175

From this table we see that a lot of packets are lost, since the speed of transmission is very large. This doesn't give the opportunity for home agents and edge routers to take care of all the incoming packets and so many packets are discarded. The worst case is for mobile node D where 43.26% of the transmitted packets are lost and need to be retransmitted. For mobile node B, the lost packet ratio is 11%, here mobile node B is connected to its home network, while mobile node D is trying to move to another link. Finally, throughput analysis shows that there is a considerable difference between the number of packets received by mobile nodes and that received by fixed ones. By inspecting typical numbers taken from the previous tables, lost packet ratio for home agent A is 15.9%, where it is 36.66% for mobile node A. This is related to the nature of works for mobile node, where care-of address may change from time to time.

### 5.7 Link Utilization Study of Mobile IP

Link utilization is one of the important performance measures that can be taken into consideration in the study of computer networks. It can be defined as how much the link is busy throughout the operation of the network. In other words, it can be used to determine to what degree the link is free or idle during simulation.

In this study, and referring to Figure (5.4), we will consider two modes of communication:

- The first when the mobile node is connected to its home and we will define this as home link utilization.
- The other will be when the mobile node moved to foreign link and this will be defined as foreign link utilization.

In each case, we will assume a message of variable size to be sent to the mobile node from a correspondent node which may be connected to the same link of mobile node, or on any other link. In this case, the home or the foreign network. Home and foreign agents utilization, which indicates how much the home/foreign agents nodes are busy throughout the simulation, is also included.

The results are tabulated in Table (5.10).

**Table (5.10) Utilization Measurements**

	Home link utilization (%)	Foreign link utilization (%)	Home agent utilization (%)	Foreign agent utilization (%)
Maximum	17.2	13.35	35.45	18.21
Minimum	15.4	11.28	27.74	16.5
Average	15.8	12.06	33.85	17.8
Standard dev.	1.15	0.975	1.79	0.64



The simulation results support the logical expectation for less utilization of foreign link and foreign agent. Relatively, big difference is shown between the utilization of foreign agent node and home agent node, where it is not small for foreign and home links. This is referred to the passive role played by the foreign agent.

Using different message size, which is greater than the previous one, we get the data in Table (5.11).

**Table (5.11) Utilization Results with Different Message Sizes**

	Home link utilization (%)	Foreign link utilization (%)	Home agent utilization (%)	Foreign agent utilization (%)
Maximum	22.5	15.67	43.78	20.64
Minimum	16.98	12.45	28.74	17.5
Average	20.24	13.29	39.53	19.8
Standard dev.	2.05	1.005	2.24	0.978

It is obvious that the utilization is increased by increasing the message size. Again, the increase for home agent link is larger than that for foreign agent. Of course, there are other factors which affect utilization such as, traffic size, simulation time, and number of nodes connected to link at the time of simulation. To test link utilization for mobile IPv6, the scenario in Figure (5.8) will be considered. For the purpose of simplicity we will assume the following:

- The Internet link for the network A, which is the home network of mobile node A, to be link A.
- The link which connects network B, home network of mobile node B, with the Internet to be link B.

- The Internet link for network D, the home network of mobile node D, to be link D.
- Link C, the Internet link for network C, which can be considered as foreign link for mobile node A.

We are mainly concerned with links A and B since they are connected with home agent A and home agent B. The remaining criteria are set as in the previous case. The results are shown in Table (5.12).

**Table (5.12) Utilization Results for Mobile IPv6**

	Link A (%)	Link B (%)	Link C (%)	Link D (%)
Maximum	16.75	14.86	19.91	10.95
Minimum	15.00	11.47	18.09	8.20
Average	15.56	13.67	19.15	8.74
Standard dev.	0.89	1.30	0.652	0.78

A quick comparison between Tables (5.10) and (5.12) shows that a small improvement is achieved using mobile IPv6, namely, for link B where the home agent resides. On the contrary, utilization of link C is larger using mobile IPv6, the difference is about 7.09%. The logical interpretation for this is that, mobile node on foreign links working under mobile IPv6 has to do all of the jobs done by the foreign agent in mobile IPv4. Utilization of link D is smaller than in other links since the mobile node at link D doesn't change its location while the simulation is done.

Increasing the message size is expected to inversely affect link utilization. Using the same model with larger message size, we get the data listed in Table (5.13).

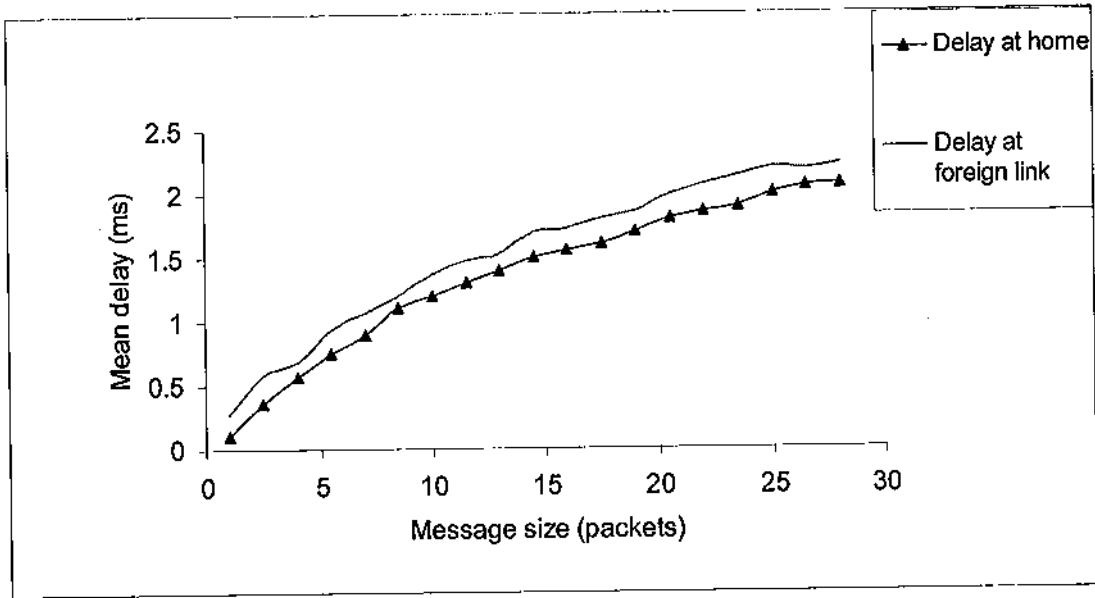
**Table (5.13) Effect of Larger Message Size on Link Utilization**

	Link A (%)	Link B (%)	Link C (%)	Link D (%)
Maximum	21.2	15.12	24.45	13.43
Minimum	17.9	10.30	17.00	9.76
Average	18.5	12.75	19.86	11.84
Standard dev.	1.10	1.88	2.01	0.98

Different changes are noticed, as expected, the link utilization increases for all cases with different ratios. Although the differences may not be significant in such typical sample, it might not be the case in real Internet that carries million of transferred packets per second. The maximum utilization is measured to be 24.45% for link C, where the minimum is 9.76% for link D. In general, link utilization increases as we increase the message size until it reaches steady state, which is the capacity of the link.

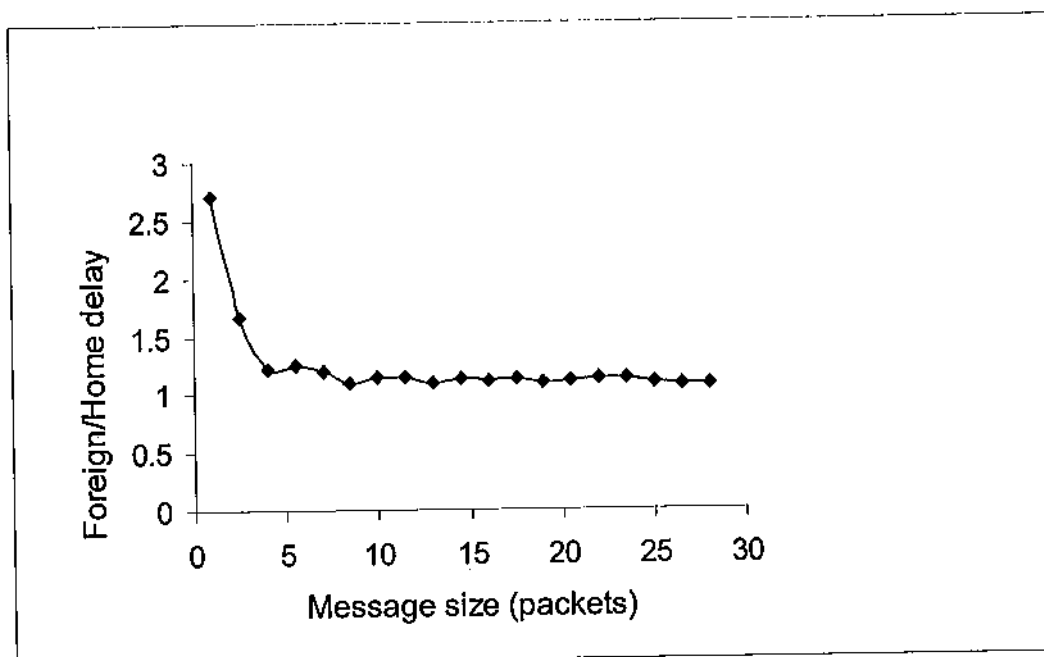
### 5.8 Reformulation of Simulation Results

In this section several graphs are plotted representing the results of transmission delay, link utilization, and throughput for both mobile IPv6 and mobile IPv4. The same configuration shown in Figure (5.4) is used for mobile IPv4 test. The delay is measured by sending a number of messages with different size from the correspondent node, say node1, to the mobile node, and then the delay time is measured from sending a packet to receiving a response. Two cases will be considered. The first one is when the mobile node is at home and the second when it is connected to a foreign link. The result is drawn in Figure (5.9).



**Figure (5.9) Delay in Mobile IPv4**

It is clear that both delays increase by increasing the size of message, and the time of delay becomes worse almost linearly when the size of the delivered message increases. The difference between the two delays is not so large, it is about 7.5% of the maximum mean delay time, which is not the case in real Internet where thousands of mobile nodes and home/foreign agents are working at the same time, so the delay is expected to have larger values. Figure (5.10) shows the ratio of the mean delay when mobile node visiting foreign link to that when it is at home. It is obvious that the delay increases about 1.2 to 1.7 times when it is at home.



**Figure (5.10) Comparison of Message Delay**

To reform the delay results for Mobile IPv6, the configuration shown in Figure (5.8) will be considered. In this case, we will concentrate on the delay introduced by mobile nodes A and B. To perform simulation, the same precondition used above will be applied here where a message of different sizes is sent from CNA to mobile node A when it is at home and when connected to a foreign link C. The same is for mobile node B. The only difference here is that, the functionalities of mobile IPv6 will be applied. The results are plotted in Figure (5.11). This figure shows that the difference between the delays at foreign and home links is large compared with that in mobile IPv4, where the delay in general is smaller for mobile IPv6. Figure (5.12) shows the difference between the two delays defined as:

$$\text{Delay difference} = \text{Foreign link delay} / \text{Home link delay}.$$

At foreign link, the delay increases about 1.5 to 2.5 times when the mobile node is at home.

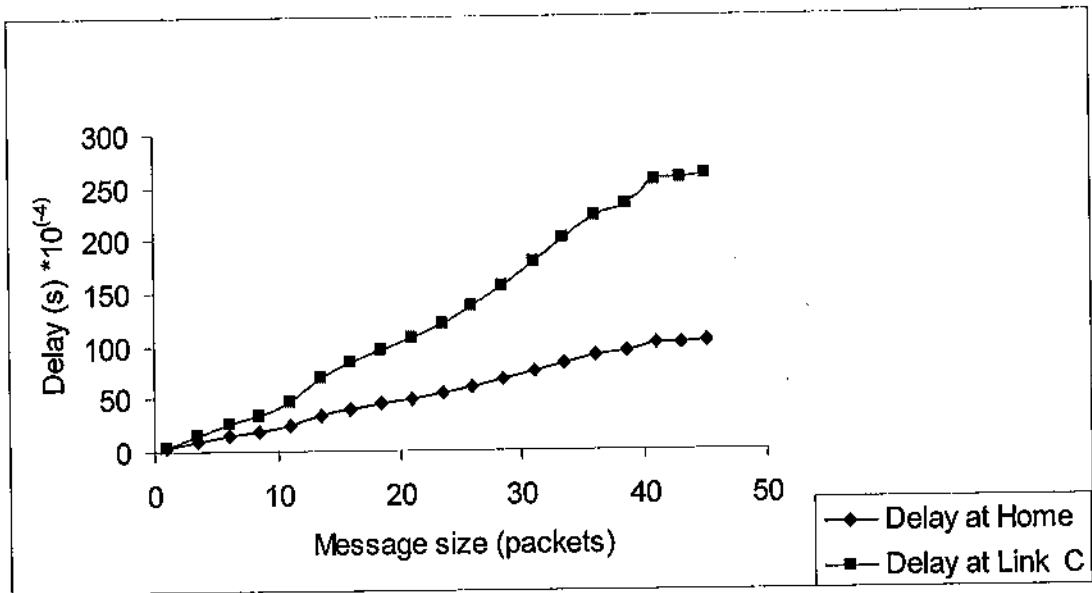


Figure (5.11) Delay in Mobile IPv6

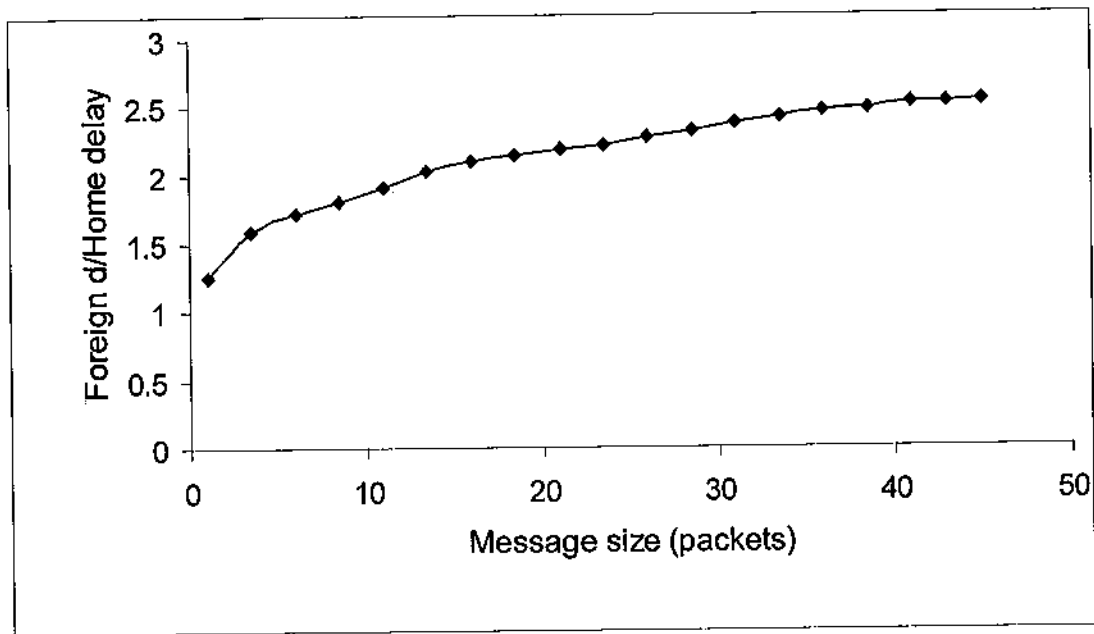


Figure (5.12) Message Delay Difference for Mobile IPv6

The configuration shown in Figure (5.5) is used to measure the throughput for mobile IPv4. In this case, a number of messages of different sizes are sent from node 4 to mobile node at its home and at the foreign link (Ethernet1, 172.16.00), and the size of each packet is fixed. Throughput is measured as the number of packets received per second. For each case of message size, the experiment is repeated many times and the average outcome is taken. The results are plotted in Figure (5.13). Results show that the

throughput increase as the delivered message size increases, and the behavior of the increase is nearly linear.

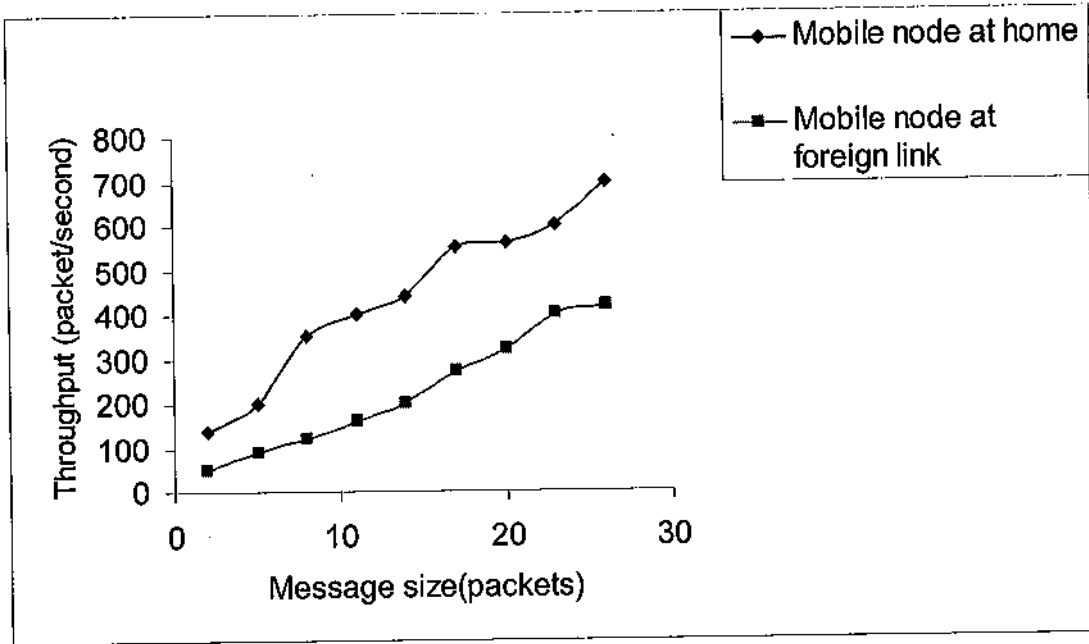


Figure (5.13) Throughput of Mobile IPv4

Figure (5.14) shows a comparison between throughputs at home and foreign links. In this figure the ratio of throughput at foreign link to that at home is represented.

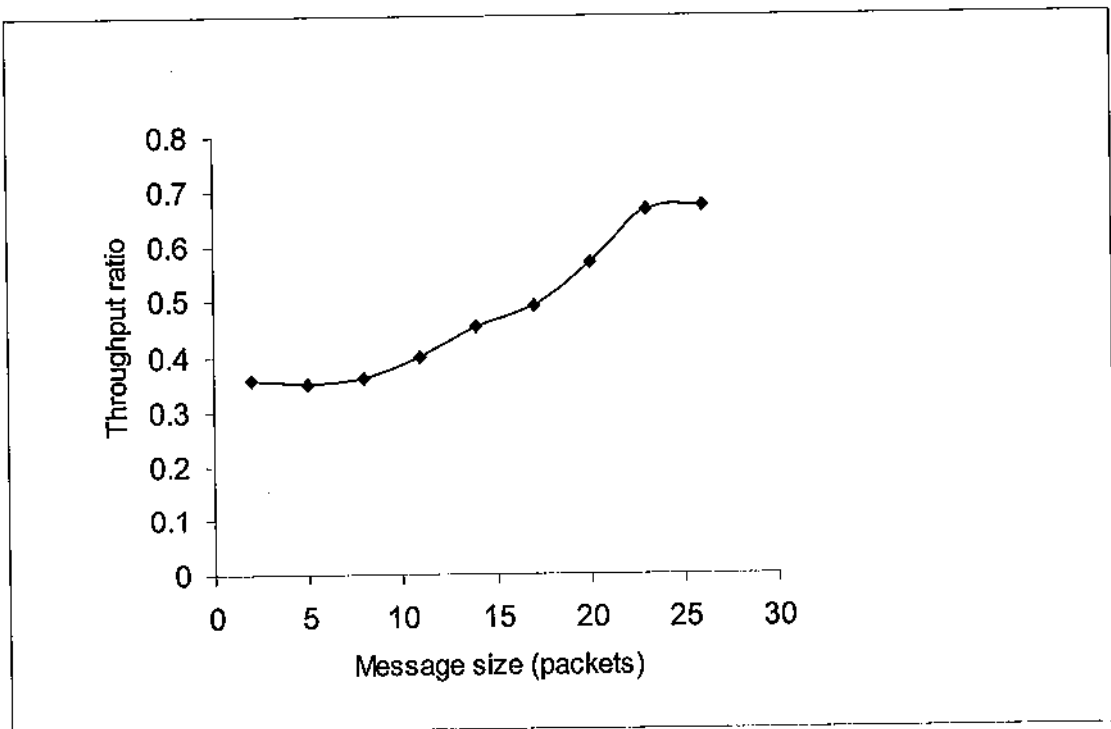


Figure (5.14) Home/Foreign Link Throughput Comparison

It is clear that the throughput is 1.25 to 3.333 times that at foreign link.

The same discussion is considered for mobile IPv6. The configuration in Figure (5.8) is taken into account here. A number of messages of varying sizes will be sent from node B2 to mobile node A. Throughput is found to be the rate of packets received per unit time at home and foreign links, where network C is taken to be the foreign link. The results are shown in Figure (5.15).

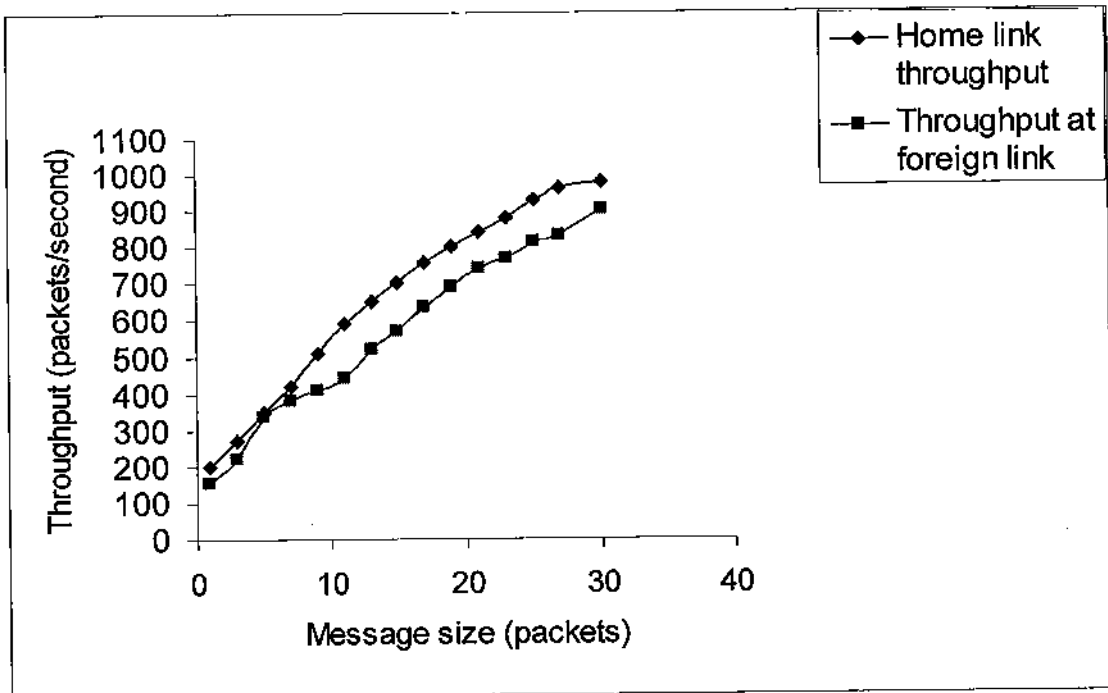
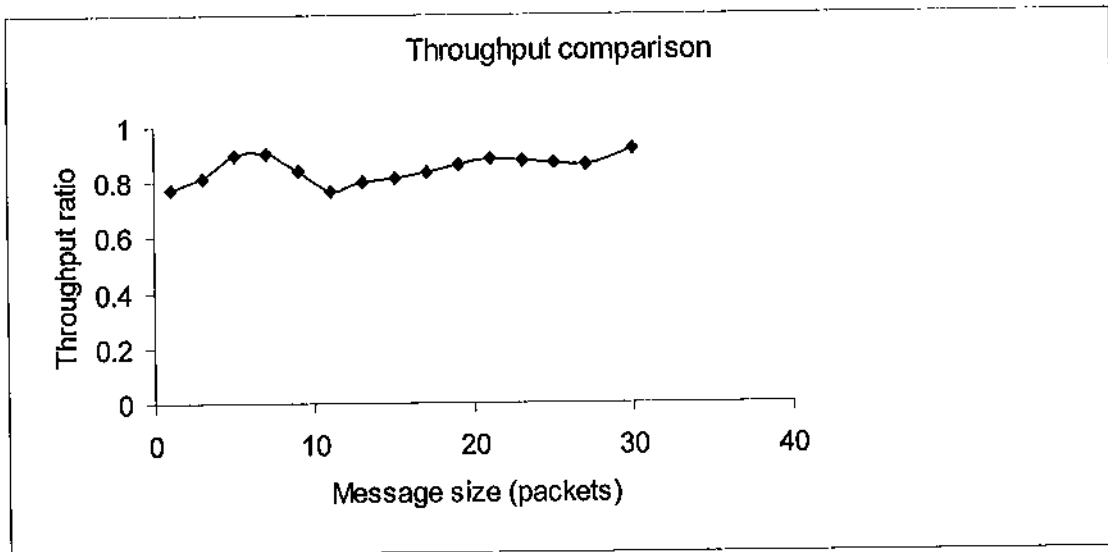


Figure (5.15) Throughput of Mobile IPv6

Throughput analysis with respect to the message size shows no great difference whether the mobile node is connected to its home or foreign link as represented in Figure (5.16). When sending to mobile node at foreign link, the throughput declines by 80% as a minimum value, since using mobile IPv6 mobile node and its correspondent can communicate directly without the aid of foreign or home agents, which is not the case for mobile IPv4 as shown in Figure (5.13), where foreign link throughput declines to 30% of its value at home link. While this is good to enhance delay and throughput in mobile IPv6, it inversely affects security issues.





**Figure (5.16) Mobile IPv6 Throughput Comparison Ratio**

The last thing to reformulate in graphs is the link utilization both for mobile IPv4 and mobile IPv6. For mobile IPv4, Figure (5.4) is considered with different message sizes to be sent from node1 to mobile node on its home and foreign links. The results are plotted in Figure (5.17). This figure shows that link utilization increases for both home and foreign links by increasing the message size. Figure (5.18) shows the ratio of foreign link utilization to that of home link. In numbers, utilization of foreign link ranges between 60% and 95% of that for home link. It is expected to obtain larger difference since home agent has a lot to do compare with foreign agent.

For mobile IPv6, link utilization and utilization ratio versus message size are shown in Figures (5.19) and (5.20), respectively. The case is inverted in mobile IPv6, where foreign link is shown to be utilized more than home link, and the utilization ratio fluctuates between 1.4 and 2 indicating that the utilization of foreign link is a multiple of home link utilization on maximum. In general, simulation results show that there is a good quantitative improvement, by adopting mobile IPv6, with respect to throughput and delay, Where mobile IPv4 still better for link utilization. It is worth to mention that all parameters that have been applied throughout the simulation are taken as an

assumption, where changing such parameters will definitely change the output numerical results. However, such modification will not change the general trends of the output results.

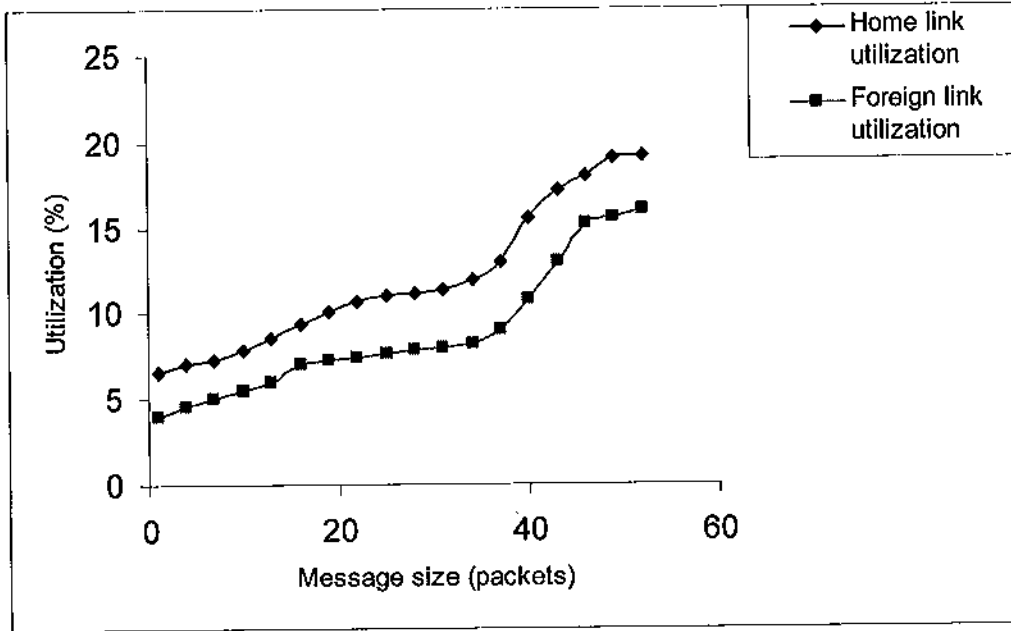


Figure (5.17) Mobile IPv4 Link Utilization

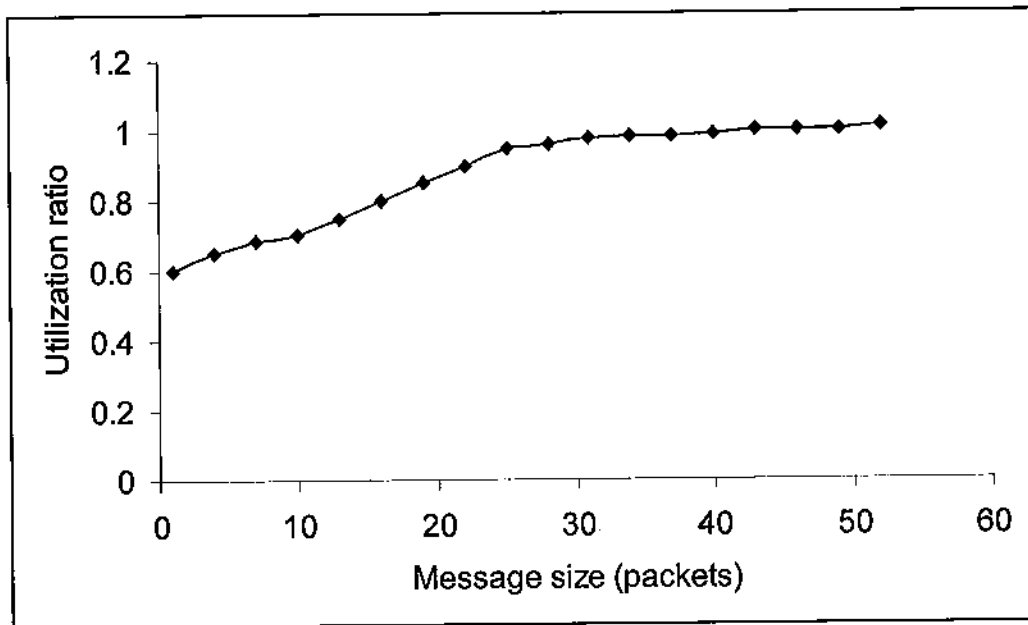


Figure (5.18) Utilization Ratio for Mobile IPv4

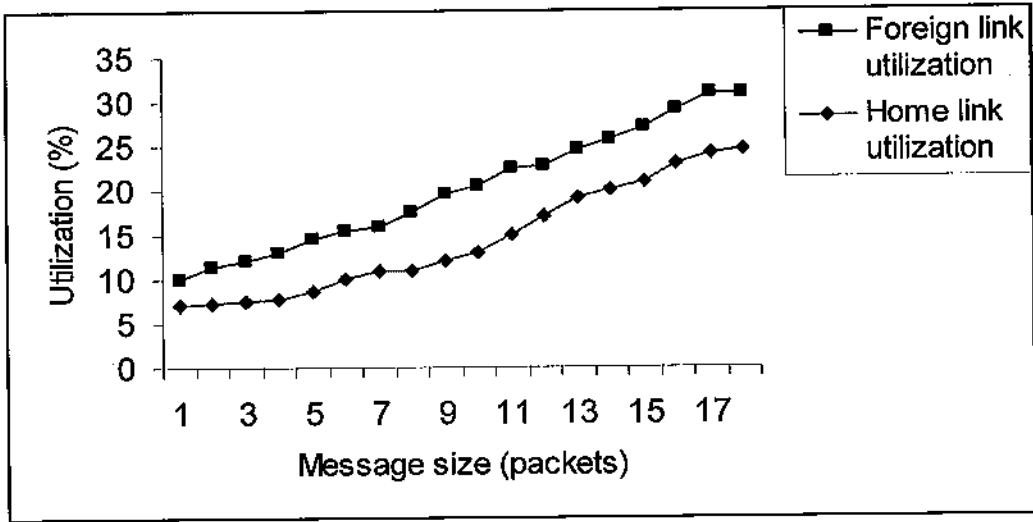


Figure (5.19) Link Utilization for Mobile IPv6

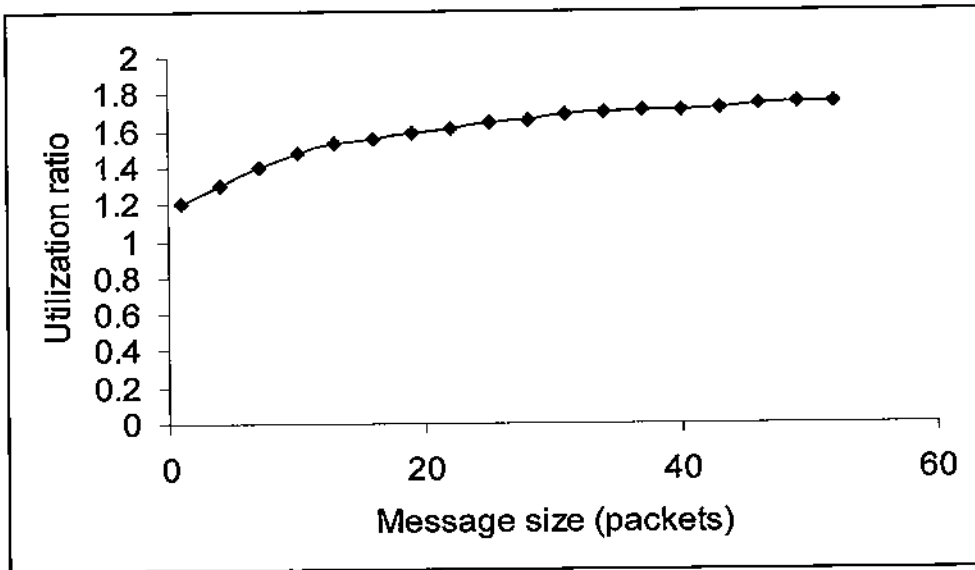


Figure (5.20) Utilization Ratio for Mobile IPv6

## Conclusions and Recommendations for Future Work

Mobile IP is a new track in Internet Technology, which represents a solution to Internet mobility. It is designed to maintain connectivity without any additional changes of the network settings when a mobile node roams to a different network. The main goal of this research study is to do performance evaluation of mobile IP. The performance measures used in this study are delay, link utilization, and throughput. Several networking scenarios are introduced to perform this simulation study. This chapter concludes this study and presents some recommendations for future work in related fields.

### 6.1 Conclusions

- Care-of address is used as a temporary address in order to make the mobile node's home address transparent. Since the IP address space in IPv4 is much less than that in IPv6, foreign agent is introduced in mobile IPv4 to provide the mobile node with care-of address on foreign link.
- Home agents are designed for the responsibility of receiving packets addressed to the mobile node and forwarding them to the mobile node's current care-of address. When moving to another network, mobile node firstly registers with its home agent and informs its home agent of its current point of attachment.
- The main difference between mobile IPv4 and mobile IPv6 design is caused due to the existence of foreign agents. In mobile IPv4, a mobile node borrows an address of a foreign agent's interface. Therefore, the foreign agent is responsible to receive tunneled packets from its home agent and sends packets to a correspondent node. The foreign agent communicates with other nodes or routers on behalf of the mobile node. As a consequence, all the functions for the mobility support, such as

encapsulation and exchanging the registration messages, must be implemented on the foreign agent.

- In contrast, a mobile node always uses an additional address to be its temporary address in mobile IPv6. This additional address is routable and represents the mobile node's current point of the attachment. As a result, other nodes and routers are able to directly communicate with the mobile node if they acknowledge the mobile node's secondary address. Moreover, and without the assistance of foreign agents, mobile node has the ability to function most of foreign agents services in mobile IPv4, such as negotiation of the registration and encapsulation.
- Regarding security, mobile IP allows mobile entities to choose any authentication algorithm they choose. The design of mobile IP combines the mechanism of IP secure (IPsec) to establish an IPsec tunnel for transmitting packets between mobile nodes and mobility agents. When packets need to pass a firewall to reach the destination in mobile IP, the packets are required to contain a SKIP header to negotiate the authentication with the firewall. Keyed MD5 and ISAKMP/Oakley are also supported by mobile IP to provide secret keys for authentication and to enable mobile IP packets transverse firewalls securely.
- In order to work with PPP, additional support from slightly modifying link-layer protocol is required. Mobile IP can provide connectivity not only for single mobile hosts but also for entire mobile network via mobile router, such architecture can be considered as working under two levels of mobile IP.
- Applying mobile IP in Ad Hoc networks requires that at least one host of the Ad Hoc network must have the capacity to support functions of a router. Moreover, this host must be the default router of the Ad Hoc network.
- While mobile IP is designed to provide wide area mobility support, cellular IP is another approach introduced to provide micro mobility support for fast moving

wireless hosts. The access network for this protocol is based on several base stations and border router. Hierarchical mobile IP separates micro mobility from macro mobility in order to decrease the signaling load as a result of the expected rapid increase of mobile nodes in the Internet. Several enhancements have to be applied to TCP in order to have a complete mobility solution.

- Mobile IP and GPRS are two separate issues that complement each other. GPRS is an access technology that handles micro mobility, while mobile IP handles macro mobility. Mobile IP can be used to evolve the GPRS architecture by implementing the functionalities of mobile IP closer to or in the radio network. In order to enable handover between different technologies, mobile IP foreign agent can be specified to reside in the GGSN node of the GPRS network.
- Smooth handoffs is supported in mobile IPv6, where a mobile node moving from one radio link to another on a different channel and unable to monitor packets transmitted over both these channels at once can send a binding update to the previous router so that those packets will instead be delivered via its new care-of address.
- Analysis of mobile IP shows that, applying the new functionalities of mobile IPv4 introduces new delays, depending on the nature of the state of mobile node connection. It is found that the largest delay is introduced by solicitation, where mobile node try to find new agent to be served on foreign links, which sometimes rises up to few seconds (2 seconds in our results). Encapsulation and registration delays are in ms and they don't exceed 150 ms in the worst case in our study, and so they are in the acceptable range. Applying mobile IPv6 using the same topology results in smaller delays and up to 20% of the total transmission time can be saved. As a result, great attention must be devoted to improve mobile IP functionalities in

order to decrease delays as much as possible since such delays degrade the performance of this protocol.

- Throughput analysis reveals the importance of home agents in mobile IPv4, and the need to use high quality routers to perform the actions of home agents, otherwise, considerable amount of packets, up to 30% in the worst case, are discarded. Mobile IPv6 gives better results regarding throughput, the results improves the dependency of throughput on the transmission time of a chunk of data.
- Finally, the link utilization study indicates that mobile IPv6 utilization is greater than mobile IPv4. While this can be considered as a disadvantage since links have to be consumed more, several enhancements can be adopted to overcome this drawback of IPv6, such as increasing the time between successive binding updates sent by mobile nodes or distributing the traffic load on more than one router in each sub-network.

## 6.2 Future Work

This study discusses the concept of mobility in the Internet using mobile IP protocol. Many aspects related to the same field weren't mentioned or covered well, and are recommended for future work. Some of these subjects are:

- Security of mobile IPv6.
- Multimedia application over mobile IP.
- Real-time traffic in mobile IP.
- Handoffs in mobile IPv4 and mobile IPv6.
- Performance of Ad Hoc Networks.

## References

- Atkinson, R., 1995. *Security Architecture for the Internet*, RFC 1825, <http://www.ietf.org>
- Aziz, A., Markson, T., and Prafullchandra, H. 1997. *Simple Key-Management for Internet Protocols (SKIP)*. April. <http://skip.incog.com>
- Bakre, A. 1996. *Design and Implementation of Indirect Protocols for Mobile Wireless Environment*. Ph.D. Thesis. The State University of New Jersey, New Jersey, USA.
- Bhagwat, P., Perkins, C. and Tripathi S. K. 1996. *Network Layer Mobility: an Architecture and Survey*. *IEEE Personal Comm.*, Vol.3, No.3, June, pp. 54-64.
- Bound, J., and Perkins, C. 1999. *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*. <http://www.ietf.org> Internet Draft, draft-ietf-dhc-dhcpv6-14.txt.
- Campbell, A. 2000. *Cellular IP*. <http://www.ietf.org> Work in Progress, Columbia University, January.
- Caceres, R., and Padmanabhan, V., 1996. *Fast and Scalable Handoffs for Wireless Inter-Networks*, Proceedings of ACM, Mobicom.
- Campbell, A.; Gomez, J and Valko, A. 1999. *Overview of Cellular IP*. *IEEE Wireless Communications and Networking*. Conference New Orleans.
- Corson, S., and Macker, J. 1999. *Mobile Ad Hoc Networking (MANET): Routing Protocol Issues and Evaluation Considerations*. <http://www.ietf.org> RFC 2501.
- Deering, S., and Hinden, R. 1998. *Internet Protocol Version 6 (IPv6) Specifications*. <http://www.ietf.org> RFC 2460.
- Deering, S. and Hinden, R. 1995. *Internet Protocol, Version 6 (IPv6) Specification*. <http://www.ietf.org> RFC 1883.
- Deering, S., 1991. *ICMP Router Discovery Messages*. <http://www.ietf.org> RFC 1256, Xerox PARC.
- Faccin, S., and Purnadi, R. 1999, *GPRS and IS-136 Integration for Flexible Networks and Service Evolution*. *IEEE Personal communication*, pp. 48-54.
- Forman, G. and Zahorjan, J. 1993. *The Challenges of Mobile Computing*. Computer Science & Engineering, University of Washington. Addison-Wesley.
- Halsall, F. 1996. *Data communications, Computer Networks and Open Systems*. 4<sup>th</sup> edition. Addison-Wesley, UK.
- Hinden, R., and Deering, S. 1998. *IP Version 6 Addressing Architecture*. <http://www.ietf.org> RFC 2373.

561395



- Higginbottom, G. 1998. *Performance Evaluation of Communication Networks*. Artech House Book, UK.
- Ioannidis, J., Duchamp, D., Gerald Q. and Maguire Jr. 1995. *IP-based Protocols for Mobile Internetworking*. Department of Computer Science, Columbia University.
- Ioannidis, J. and Maguire Jr. G. 1993. *The Design and Implementation of a Mobile Internetworking Architecture*. In *Proceedings of Winter USENIX*, San Diego, CA January, pp. 491-502.
- Jacobs, S. 1997. *Security of Current Mobile IP Solution*. *IEEE MILCOM 97 Proceedings*. Volume 3, pp 1122-1128.
- Johnson, D., and Perkins, C. 1999. *Mobility Support in IPv6*. <http://www.ietf.org> Internet Draft, draft-ietf-mobileip-IPv6-08.txt.
- Johnson, B.D. 1994. *Scalable and Robust Internetworking Routing for Mobile Hosts*. 14<sup>th</sup> Intl. Conf. Distributed Computing Systems, June, pp.2-11.
- Maltz, D., and Johnson, D. 1996. *Protocols for Adaptive Wireless and Mobile Networking*. *IEEE Personal Communications*. Vol.3., pp 490-498.
- Patel, G., and Dennet, S. 2000. *The 3GPP and 3GPP2 Movement Towards an All-IP Mobile Network*. *IEEE Personal Communications*, August. pp 62-64.
- Perkins, C., Myles, A. and Johnson, B. 1994. *Mobile Host Protocol for the Internet*. *Computer Networks and ISDN Systems 27*, December, pp. 479-491.
- Perkins, C. and Myles A. 1994. *Mobile IP*. *SBT/IEEE International Telecommunications Symposium*, Rio De Janeiro.
- Perkins, C. 1996. *IPv4 Mobility Support*. <http://www.ietf.org> RFC 2002.
- Perkins, C. 1997. *Mobile IP: Design Principles and Practices*. Addison-Wesley.
- Perkins, C. and Johnson, B. 1997. *Route Optimization in Mobile IP*. Internet draft, <http://www.ietf.org>.
- Perkins, C. 2001. *Ad Hoc Networks*, Addison-Wesley
- Perkins, C. 1998. *Mobile Networking Through Mobile IP*. *IEEE Internet Computing*, February, pp. 58-69.
- Postel, J.B. 1981. *Internet Protocol*. <http://www.ietf.org> RFC 791.
- Postel, J.B. 1981. *Transmission Control Protocol*. <http://www.ietf.org> RFC 793.
- Rahnema, M. 1993. *Overview of the GSM System and Protocol Architecture*. *IEEE Communications*, Volume 31, pp.92-100.

- Rappaport, TS. 1996. *Wireless Communications Principles and Practice*. Prentice-Hall, Englewood Cliffs, NJ.
- Rekhter, Y. and Perkins, C. 1992. *Loose Source Routing for Mobile Hosts*. <http://www.ietf.org> Internet draft.
- Rivest, R. 1995. *The MD5 Message-Digest Algorithm*, <http://www.ietf.org> RFC 1321.
- Royer, R., 1999. *Review of Current Routing Protocols for Ad Hoc Networks*. *IEEE Personal Communication*, April, pp. 46-55.
- Simpson, W. 1994. *The Point to Point Protocol*. <http://www.ietf.org> RFC 1661.
- Soliman, H., and Malki, K.E. 2000. *Hierarchical mobile IPv6 and fast handoffs*. <http://www.ietf.org> Internet Draft.
- Solomon, J., and Glass, S. 1998. *Mobile IP configuration Option for PPP IPCP*. <http://www.ietf.org> RFC 2290, February.
- Teraoka, F., Claffy K. and Tokoro M. 1992. *Design, Implementation and Evaluation of Virtual Internet Protocol*. In *Proceedings of the 12<sup>th</sup> International Conference on Distributed Computing Systems*, June, pp. 170-177.
- Teraoka, F. and Tokoro, M. 1993. *Host Migration Transparency in IP Networks*. *Computer Communication Review*, January, pp. 45-65.
- The Network Simulator ns-2, <http://www.isi.edu/ns-2>
- Thomson, S. and Narten, T. 1998. *IP6 Stateless Address Auto-configuration*. <http://www.ietf.org> RFC 2462, December.
- 3GPP2, 3GPP2 P.R0001 v1.0.0.2000. *Wireless IP, Architecture Based on IETF Protocols*, 14 July. [http://208.45.131.70/docs/newsd/3GPP2\\_Specs\\_Doc\\_New.html](http://208.45.131.70/docs/newsd/3GPP2_Specs_Doc_New.html).
- 3GPP, 3G TS 29.061.2000. *Interworking Between the PLMN Supporting Packet Based Services and Packet Data Networks (PDN)*, March. <http://www.3GPP2.org>.
- 3GPP, 3G TR 23.923. 2000. *Combined GSM and Mobile IP Mobility Handling in UMTS IP CN*, May, Page 20. <http://www.3GPP2.org>
- William, C.Y. Lee. 1995. *Mobile Cellular Telecommunications*. 2<sup>nd</sup> edition, McGraw-Hill, Inc.
- Heine, G., 2000. *GPRS from A-Z. Seminars and Training, Hotline for Your Questions on Mobile Communications*. ACON GmbH.

## تقييم أداء ترابط الشبكات المتنقلة باستخدام بروتوكول الإنترنت المتنقل

إعداد

هيثم كامل عبد الله قاسم

المشرف الرئيس

أ. د. جميل أيوب

المشرف المشارك

د. سهيل عودة

ملخص

حديثاً، أصبحنا نواجه نمواً سريعاً في الحاجة لخدمة الحواسيب المتنقلة. في نظام الحوسبة المبني على الإنترنت، تحتاج الحواسيب المتنقلة إلى تقنية خاصة للمحافظة على بقاء الإتصال أثناء تغيير نقاط ربطها مع الإنترنت. إن الهدف من تصميم توفير الخدمة المتحركة هو جعل الحواسيب الخاصة وحواسيب دفاتر الملاحظات تحافظ على إستمرارية الاتصال بدون أي تعديلات أو تغييرات إضافية عند انتقالها أو تغيير نقاط ربطها. لتحقيق هذا الهدف، أختيرت طبقة الترابط لعمل تعديل بسيط بحيث أن بروتوكولات الطبقات الأخرى تركت بدون تعديل قدر الإمكان. بروتوكول الإنترنت (IP) هو من أشهر البروتوكولات المستعملة في طبقة الشبكة. في الترابط باستخدام هذا البروتوكول، عنوان واحد يحدد نقطة الربط لكل عقدة. خدمة التنقل في بروتوكول الإنترنت صممت بالأخذ بعين الإعتبار مشكلة المحافظة على الاتصال بدون أي إضافات أثناء انتقال الحواسيب أو دخولها ضمن شبكات أخرى. بروتوكول الإنترنت المتنقل طور لمواكبة خدمات الإنترنت المتنقلة. الهدف من هذا البحث هو تقييم أداء بروتوكول الإنترنت المتنقل باستخدام معايير تقييم مختلفة منها الزمن الذي ينقضي لإرسال رسالة من نقطة إلى أخرى في الشبكة وكمية المعلومات الفعلية التي تصل المستقبل. تمت مناقشة البروتوكول الأساسي وبالتركيز على الأجزاء

الرئيسية الثلاث لهذا البروتوكول وهي: الإعلان عن وجود عامل خدمة والتسجيل وإرسال المعلومات. تم إعداد دراسة مقارنة بين الوظائف الرئيسية للإصدار الرابع والإصدار السادس من بروتوكول الإنترنت المتنقل، وكذلك مقارنة عمل البروتوكولان مع مقترحات أخرى في مجال تنقل الإنترنت. علاوة على ذلك، تمت دراسة عمل بروتوكول الإنترنت المتنقل تحت توصيلات أخرى مثل الخدمة الراديوية العامة لإرسال المعلومات على شكل وحدات منفصل (GPRS) والشبكات الافتراضية اللاسلكية وكذلك التوصيل باستخدام وصلة النقطة إلى النقطة.