NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

MOBILE INTERNET PROTOCOL ANALYSIS

by

Lawrence J. Brachfeld

September 1999

Thesis Advisor: Bert Lundy

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
September 1999

3. REPORT TYPE AND DATES COVERED
Master's Thesis

4. TITLE AND SUBTITLE :
Mobile Internet Protocol Analysis

5. FUNDING NUMBERS

6. AUTHOR(S)
Brachfeld, Lawrence J.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

Mobile Internet Protocol (IP) is a proposed standard that builds on the current Internet Protocol by making the fact that a user is mobile transparent to applications and higher level protocols such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

Mobile IP allows mobile computers to send and receive packets addressed with their home network IP address, regardless of the IP address of their current point of attachment on the Internet while maintaining any current connections even if the point of attachment changes while the current connection is still active. Additionally, it is independent of the physical medium over which the mobile computer communicates. In order to meet the goals of location transparency and connection durability each mobile node has a permanent IP address. This unchanging address allows conventional Internet hosts, which are unaware of mobility issues, to communicate with the mobile node. When the mobile node is at home, it functions like a normal non-mobile Internet node. When it is away from home, it communicates through the use of home agents and foreign agents.

This thesis will explain Mobile IP and analyze the protocol to determine strengths and weaknesses of the protocol.

14. SUBJECT TERMS
Local Area Network, Mobile IP, TCP/IP, Internet Protocol, Protocol Analysis

15. NUMBER OF PAGES
69

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

19. SECURITY CLASSIFICATION OF ABSTRACT
Unclassified

20. LIMITATION OF ABSTRACT
UL

Approved for public release; distribution is unlimited.

MOBILE INTERNET PROTOCOL ANALYSIS

Lawrence J. Brachfeld
Lieutenant Commander, United States Navy
B.S., Rensselear Polytechnic Institute, 1988
M.S., Naval Postgraduate School, 1996

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
September 1999

Author: Lawrence Jay Brachfeld
Lawrence J. Brachfeld

Approved by: 8/9/1999
Bert Lundy, Thesis Advisor

Wolfgang Baer
Wolfgang Baer, Associate Advisor

D C Boger
Dan C. Boger, Chairman
Department of Computer Science

ABSTRACT

Mobile Internet Protocol (IP) is a proposed standard that builds on the current Internet Protocol by making the fact that a user is mobile transparent to applications and higher level protocols such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

Mobile IP allows mobile computers to send and receive packets addressed with their home network IP address, regardless of the IP address of their current point of attachment on the Internet while maintaining any current connections even if the point of attachment changes while the current connection is still active. Additionally, it is independent of the physical medium over which the mobile computer communicates. In order to meet the goals of location transparency and connection durability each mobile node has a permanent IP address. This unchanging address allows conventional Internet hosts, which are unaware of mobility issues, to communicate with the mobile node. When the mobile node is at home, it functions like a normal non-mobile Internet node. When it is away from home, it communicates through the use of home agents and foreign agents.

This thesis will explain Mobile IP and analyze the protocol to determine strengths and weaknesses of the protocol.

TABLE OF CONTENTS

I. INTRODUCTION 1

A. PURPOSE 1

B. THESIS OUTLINE 1

C. BASIC CONCEPTS 2

1. Network 2

2. Inter-network 2

3. Intra-network 2

4. Internet 2

5. Transmission Control Protocol (TCP) / Internet Protocol (IP) 3

II. MOBILE IP BACKGROUND 5

A. INTRODUCTION TO MOBILE IP 5

B. SOLUTIONS OTHER THAN MOBILE IP 8

1. Host-Specific Routes 8

2. Change the Node's IP address 8

3. Link Layer Solutions 9

a. Cellular Digital Packet Data (CDPD) 9

b. Wireless LAN (IEEE 802.11) 10

III. MOBILE IP VERSION IV DISCUSSION 11

A. HOW DOES MOBILE IP WORK 11

1. Agent Discovery 12

2. Agent Registration 16

3. Care-of-Address Tunneling 21

B. MOBILE IP IN ACTION 22

IV. MOBILE IP VERSION VI DISCUSSION 25

A. MOBILE IP VERSION VI OVERVIEW 25

1. Binding Update Option 28

2. Binding Acknowledgement Option 30

3. Binding Request Option 32

B. MOBILE IP VERSION 6 SUMMARY 33

V. MOBILE IP PROTOCOL ANALYSIS 35

A. MOBILE IP PROTOCOL SPECIFICATION 35

1. Overall Discussion of Mobile IP Protocol Specification 35

2. Mobile Node 36

3. Home Agent 37

4. Foreign Agent 39

B. MOBILE IP REACHABILITY ANALYSIS 40

C. MOBILE IP PROTOCOL ANALYSIS DISCUSSION 43

1. Protocol Analysis Items Accomplished 43

2. Protocol Analysis Items Not Accomplished 43

3. Protocol Analysis Results 44

a. Mobile IP Protocol Weaknesses 44

b. Mobile IP Protocol Strengths 45

VI. APPLICATIONS OF MOBILE IP TO THE US NAVY 47

A. NAVAL APPLICATIONS FOR MOBILE IP 47

1. Mobile Ship Networks 47

2. Mobile Squadrons 47

B. NAVAL TEST PLAN FOR ADOPTING MOBILE IP 48

1. Phase 1 : Lab Research 48

2. Phase 2 : Testing aboard USS Coronado and Navy Network Operations Center (NOC) 48
3. Phase 3 : Implementation 49

VII. CONCLUSION 51
A. MOBILE IP CONCLUSIONS 51
B. FUTURE RESEARCH AREAS 52

LIST OF REFERENCES 53

INITIAL DISTRIBUTION LIST 55

LIST OF FIGURES

FIGURE 1. A NETWORK WITH MOBILITY SUPPORT.......7
FIGURE 2. MOBILE IP AGENT ADVERTISEMENT.......13
FIGURE 3. MOBILE IP AGENT SOLICITATION.......13
FIGURE 4. MOBILITY AGENT ADVERTISEMENT EXTENSION.......14
FIGURE 5. MOBILE IP REGISTRATION WITH HOME AGENT.......16
FIGURE 6. MOBILE IP REGISTRATION WITH FOREIGN AGENT.......17
FIGURE 7. MOBILITY AGENT REGISTRATION REQUEST.......18
FIGURE 8. MOBILITY AGENT REGISTRATION REPLY.......19
FIGURE 9. IP DATAGRAM FLOW TO A MOBILE NODE AWAY FROM ITS HOME NETWORK.......22
FIGURE 10. IPV6 OVERALL PICTURE.......26
FIGURE 11. BINDING UPDATE DESTINATION OPTION FORMAT.......29
FIGURE 12. BINDING ACKNOWLEDGEMENT.......31
FIGURE 13. BINDING REQUEST OPTION.......33
FIGURE 14. MOBILE NODE MOVING FROM HOME NETWORK TO FOREIGN NETWORK.......35
FIGURE 15. MOBILE NODE SPECIFICATION.......36
FIGURE 16. HOME AGENT SPECIFICATION.......38
FIGURE 17. FOREIGN AGENT SPECIFICATION.......39

LIST OF TABLES

TABLE 1. ABBREVIATIONS WITH CORRESPONDING DEFINITIONS FOR THE MOBILE NODE SPECIFICATION.........37
TABLE 2. ABBREVIATIONS WITH CORRESPONDING DEFINITIONS FOR THE HOME AGENT SPECIFICATION 38
TABLE 3. ABBREVIATIONS WITH CORRESPONDING DEFINITIONS FOR THE FOREIGN AGENT SPECIFICATION 39

ACKNOWLEDGMENT

I must take this opportunity to acknowledge the constant support of my wife, Annamarie, without which I would not have completed this thesis. I also want to thank my children, Hannah and Aaron for their support and understanding as I worked on my thesis when I could have been playing games with them. Additionally, I would like to thank the many people that have influenced my Naval career and led me to Monterey twice.

I. INTRODUCTION

In the last few years we have seen an explosion in the number of notebook computers and in the growth of the Internet. While notebook computers continue to improve with respect to size, weight, and capabilities, the Internet continues to grow at a mind-boggling pace. (Solomon, 1998)

A. PURPOSE

This research focuses on the Mobile Internet Protocol (IP), a proposed Internet standard. This thesis will explain Mobile IP, analyze the protocol to determine strengths and weaknesses, examine the protocol from the perspective of IP version four as well as IP version six, and discuss the need for Mobile IP within the US Navy.

Mobile IP is a modification to the well known Internet Protocol to solve the problem of transferring information to and from mobile computers. It allows a mobile computer to change its location or point of attachment on the Internet without restarting its applications and without disrupting any ongoing communications. Additionally, it is independent of the physical medium over which the mobile computer communicates. This continuous connectivity will allow users to be quickly notified of changing events and provide them with the resources necessary to respond to them even when in transit.

Mobile IP is the harbinger of untethered computing advances in wireless network technology. What cellular technology did for telephony, mobile IP will do for the TCP/IP based mode of data transport that is ubiquitous today.

B. THESIS OUTLINE

This thesis consists of seven chapters. Chapter II provides background information on the overview and history of Mobile IP, and the design philosophy of Mobile IP. Chapter III examines Mobile IP version IV in depth. Chapter IV examines mobile IP version VI changes and requirements. Chapter V analyzes the protocol using formal specification and reachability analysis. Chapter VI discusses the applications of Mobile IP to the US Naval forces. Chapter VII concludes the thesis and provides suggestions for future research.

C. BASIC CONCEPTS

In order to focus on what we mean technically by Mobile Internet Protocol, we should first explain some other terms. Even though many of them are basic and almost common sense to the technically erudite, these other concepts will function as building blocks towards a clearer understanding of Mobile IP.

1. Network

A network is a configuration of nodes capable of inter-nodal communications and bound together by a common network identity. A data network is understood in terms of layers one, two, and three of the OSI model. Inter-nodal communication is made possible by protocols regarding how the nodes will operate with respect to layers one, two, and three. These protocols will yield a common network identity. For example, 10BaseT Ethernet with nodes speaking TCP/IP configured with a 255.255.255.0 subnet mask defines a unique network identity.

2. Inter-network

An inter-network is a configuration of networks that enables internodal communications across network boundaries. To stretch beyond the set of nodes which share your network identity in order to communicate with other nodes on other networks is to engage in inter-network communications.

3. Intra-network

An intra-network reflects organizational boundaries and policy umbrellas applicable to internodal communications within the borders and is recognizable by nodes and networks outside the intra-network boundary as a distinct communications environment.

4. Internet

The Internet is a global, virtual computer network combining heterogeneous networks together using a common network layer protocol. Today the Internet Protocol (IP) is predominantly used to route IP datagrams node by node across the Internet to the destination network and host.

5. Transmission Control Protocol (TCP) / Internet Protocol (IP)

The IP is part of the TCP/IP protocol suite and is the most widely used internetworking protocol. It allows for the routing of datagrams from one network to another. The 32 bit IP address is composed of two components, the network part and the host part. The routing of the datagrams towards the destination is based on the network component of the address. Once the destination network is reached, the host portion of the address is used. The IP is used by the transport protocols Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). The TCP offers reliable end to end transmission services with error correction and guaranteed delivery, while UDP provides connectionless services.

Throughout this thesis we will see how these terms relate to Mobile IP.

THIS PAGE INTENTIONALLY LEFT BLANK

II. MOBILE IP BACKGROUND

A. INTRODUCTION TO MOBILE IP

Recent developments in computer technology have made it possible to build more powerful portable computer devices. As a result, people are not constrained to using their computers in a single location. At the same time, computer networking is becoming indispensable and people increasingly desire to attach their computers to the network, with the same level of service, wherever they happen to be working. It is for this reason among others that the Mobile IP has been developed.

The current Internet Protocol assumes that a node's IP address uniquely identifies the node's point of attachment to the Internet. Therefore, a node must be located on the network indicates by its IP address in order to receive packets destined for it; otherwise these packets will be undeliverable. For a node to change its point of attachment without losing its ability to communicate, one of two methods must be employed:

1. the node must change its IP address whenever it changes its point of attachment, or
2. host-specific routes must be propagated throughout much of the Internet.

Both of these alternatives are unacceptable. The first makes it impossible for a node to maintain transport and higher layer connections when the node moves. The second is impossible to scale based on the current size of the Internet.

If a mobile host, moves to a new network while keeping its assigned IP address unchanged, its address will not reflect the new point of attachment. Consequently, existing routing protocols will be unable to route datagrams to it correctly. This is referred to as mobility and is 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. Without Mobile IP, in this situation the mobile host must be reconfigured with a new IP address that represents its new point of attachment to the network. This process presents the problem of informing potential correspondents of the new IP address and will cause already established transport layer connections to be lost. Under the current IP if the mobile host moves without changing its address, it will lose routing; but if it does change its address, it will lose connections. (Lancki, 1996)

Simply put, Mobile IP is an enhancement to the current IP which allows a mobile host to freely roam on the Internet while maintaining the same IP address. The Internet Engineering Task Force (IETF) is currently developing a Mobile IP standard, which is currently in its sixteenth revision. Mobile IP is completely independent of the media over which it runs and has four basic requirements that the IETF is attempting to support with this proposed standard:

1. A mobile node must be able to communicate with other nodes after changing its link layer point of attachment to the Internet.
2. A mobile node must be able to communicate using only its home IP address, regardless of its current link layer point of attachment to the Internet.
3. A mobile node must be able to communicate with other computers that do not implement the Mobile IP functions.
4. A mobile node must not be exposed to security threats over and above those to which any fixed node on the Internet is exposed.

Figure 1 (Lancki, 1996) shows a mobility supported internetwork.

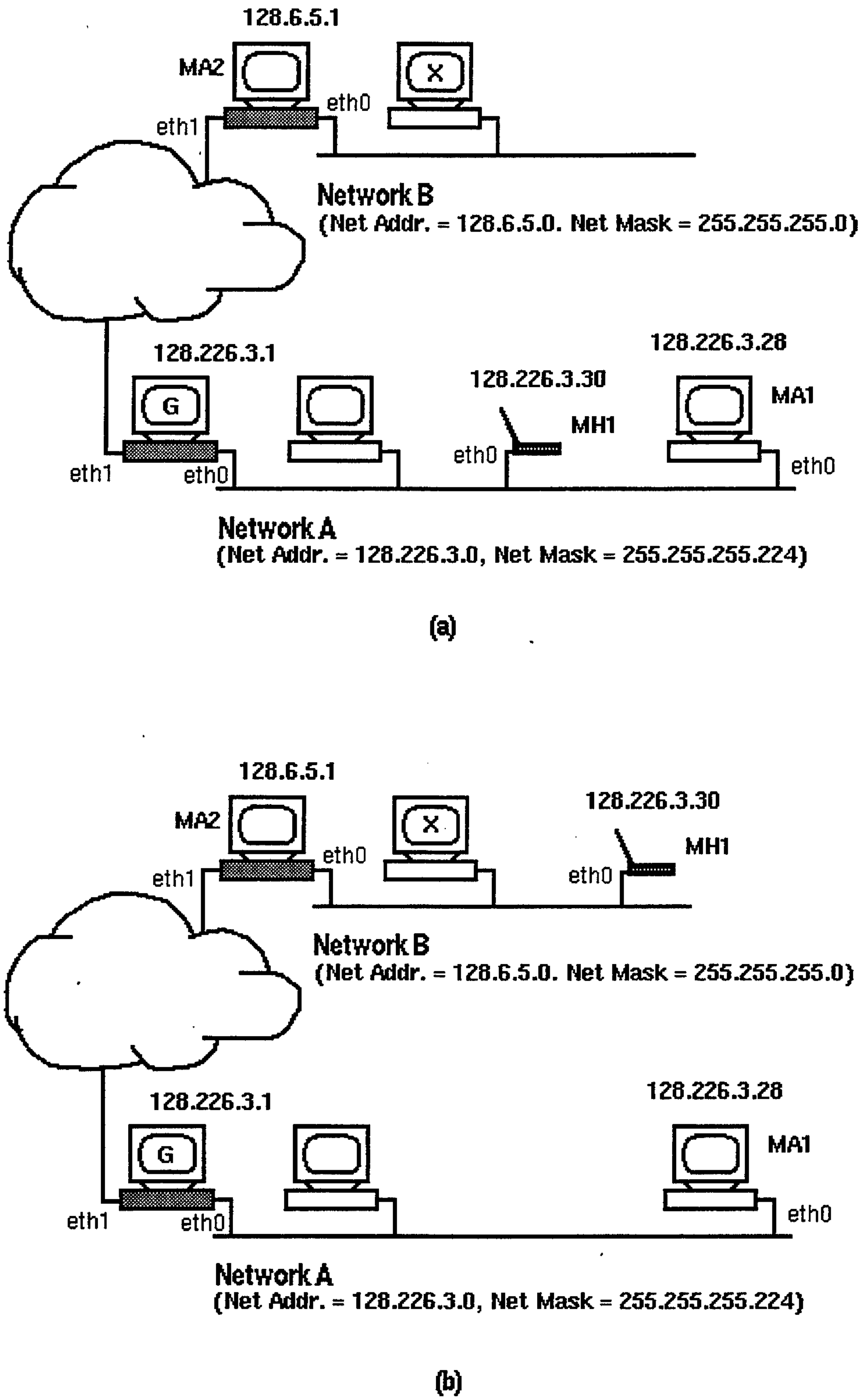

128.6.5.1
MA2
eth0
eth1
Network B
(Net Addr. = 128.6.5.0. Net Mask = 255.255.255.0)
128.226.3.1
128.226.3.30
128.226.3.28
G
MH1
MA1
eth1
eth0
eth0
eth0
Network A
(Net Addr. = 128.226.3.0, Net Mask = 255.255.255.224)
(a)
128.6.5.1
MA2
eth0
eth1
128.226.3.30
MH1
eth0
Network B
(Net Addr. = 128.6.5.0. Net Mask = 255.255.255.0)
128.226.3.1
128.226.3.28
G
MA1
eth1
eth0
eth0
Network A
(Net Addr. = 128.226.3.0, Net Mask = 255.255.255.224)
(b)

Figure 1. A network with mobility support

Figure 1(a) and 1(b) shows two networks, network A and network B, which are equipped with mobility agents MA1 and MA2 respectively. A mobile host, MH1, is also shown, whose home network is network A. Whenever MH1 is away, MA1 acts as its home agent. When MH1 visits network B, MA2 acts as its foreign agent. In (a), MH1 is on its home network. In (b), MH1 is visiting a foreign network, network B. As shown, each mobile host is associated with a unique home network as indicated by its permanent IP address. Normal IP routing always delivers packets meant for the mobile host to its home network. When a mobile host is away, the home agent is responsible for intercepting and forwarding its packets. (Lancki, 1996)

B. SOLUTIONS OTHER THAN MOBILE IP

There are several methods that people have proposed to solve the problem of mobility, but none are robust enough for Internet use. The major contenders to mobile IP will be discussed here.

1. Host-Specific Routes

A host-specific route is a routing-table entry that provides a match for exactly one IP destination address. Therefore, in order to use host-specific routes as a solution for mobility every router along the path that the packet may take would need to have this information. There are several reasons why host-specific routes are an unworkable solution:

- Host-specific routes must be propagated to all nodes along the path between a mobile node's home link and its foreign link.
- All of these routes must be updated every time the node moves from one link to another.
- As the number of mobile nodes increases, the number of host-specific routes required must be increased substantially.
- There are serious security implications to using host-specific routes to accomplish node mobility in the Internet. (Solomon, 1998)

2. Change the Node's IP address

Since host-specific routing is unacceptable, why not simply change the node's IP address as it moves from link to link? Since all nodes on the same mink have the same network-prefix portion of their IP addresses, a node must change this to reflect the network-prefix of the new link. The node may be able to keep the host portion of its IP address as long as no other node on this link was using the same address. Once these changes were made, it could begin communicating on the new link with its new IP address. The problem with this is that the Internet predominantly uses Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) which both use IP addresses as end point identifiers. For example, a TCP connection within a node is uniquely defined by four values: IP source address, IP destination address, TCP source port, and TCP destination port. IP version four expects these four quantities to remain constant over the duration of a TCP connection, thus all ongoing communications between a mobile node and any existing nodes would be terminated.

Therefore, changing a node's IP address does not provide a solution to node mobility.

3. Link Layer Solutions

a. Cellular Digital Packet Data (CDPD)

CDPD is a standard for sending IP packets over unoccupied radio channels within the analog cellular telephone systems of North America. Obtaining CDPD service involves purchasing a CDPD modem for your computer and signing a service agreement with a CDPD service provider. Since these providers have roaming agreements in place, in theory you can use CDPD service in any geographic area where there is analog cellular coverage by a CDPD carrier. When you sign up for CDPD service you are given an IP address for use throughout the CDPD network. The link layer protocols are responsible for ensuring that packets can be delivered to the carrier provided IP address anywhere within the CDPD network. Although conceptually similar to the Mobile IP approach, it is important to note that CDPD's protocols provide mobility only within the context of the CDPD system itself and is why it is classified as a link layer solution. Additional problems with the CDPD approach is that the maximum speed of CDPD is approximately 11 kilobits per second (Kbps) and that the CDPD service is extremely limited in availability. For theses reasons CDPD is not seen as a viable solution to the mobility problem that needs to be solved.

b. Wireless LAN (IEEE 802.11)

The Institute for Electrical and Electronics Engineers (IEEE) includes a body which produces protocol standards. One of the technologies they have standardized is for wireless local-area networks (wireless LANs), published in [802.11]. This is a much faster, but a more geographically constrained solution to node movement than is CDPD, supporting speeds in the one to two Megabits per second (Mbps) range, although recently speeds in the ten Mbps range have been discussed. This standard defines a set of wireless transceivers which provide a bridge between the wireless medium and the wired infrastructure. Link layer protocols make the entire network of wireless LAN transceivers appear to be one link as viewed by the network layer. Thus mobility in the wireless LAN is transparent to the IP layer. However, any change of location that results in a node crossing a router boundary requires the node to change its IP address and therefore, interrupts any ongoing communications (Solomon, 1998).

In summary, this section showed several reasons why link layer solutions are not sufficiently general to provide node mobility throughout the Internet. First, by definition, link layer solutions provide node mobility only in the context of a single type of medium. For example, CDPD provides mobility when the mobile node travels from one CDPD cell to another. However, CDPD requires a mobile node to acquire a new IP address if the mobile node connects to another medium. Additionally, link layer solutions are severely limited in the geographic areas they can provide mobility.

This chapter provided the background to show why Mobile IP is required 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; and
- If a node changes its IP address when it moves, it will have to terminate and restart any ongoing communications each time it moves.

III. MOBILE IP VERSION IV DISCUSSION

A. HOW DOES MOBILE IP WORK

The functions and protocols of Mobile IP are described here at a very high level. Each component will then be explained in greater detail.

Here are the chronological sequence of events that allows Mobile IP to work:

1. Home and foreign agents advertise their presence by periodically sending agent advertisement messages. Optionally, a mobile node can solicit an Agent Advertisement message from any locally attached mobility agent through an Agent Solicitation message.
2. Mobile nodes receive these agent advertisement messages and examines their contents to determine whether they are connected to their home network or a foreign network. While a mobile node is connected to its home network, it acts just like a stationary node, therefore this discussion will continue with the assumption that the mobile node is on a foreign network.
3. The mobile node acquires a care-of-address from the foreign agent's agent advertisement.
4. The mobile node registers the care-of-address with its home agent through the exchange of Registration Request and Registration Reply messages.
5. Packets sent to the mobile node's home address are intercepted by the mobile node's home agent and tunneled by the home agent to the mobile node's care-of-address.
6. At the care-of-address, the foreign agent extracts the original packet from the tunnel and delivers it to the mobile node.

This entire process can be thought of as akin to the way you update the post office with your new address when you move. To update your address you fill out a form with your old address and new address, when a letter is received at the post office for your old address, it acts as a home agent and forwards the letter to the post office that services your new address, your foreign agent. This post office then delivers the letter to your home. Mobile IP is best understood by the cooperation of three separate mechanisms, agent discovery, agent registration, and tunneling. The specifics of these three processes will now be discussed.

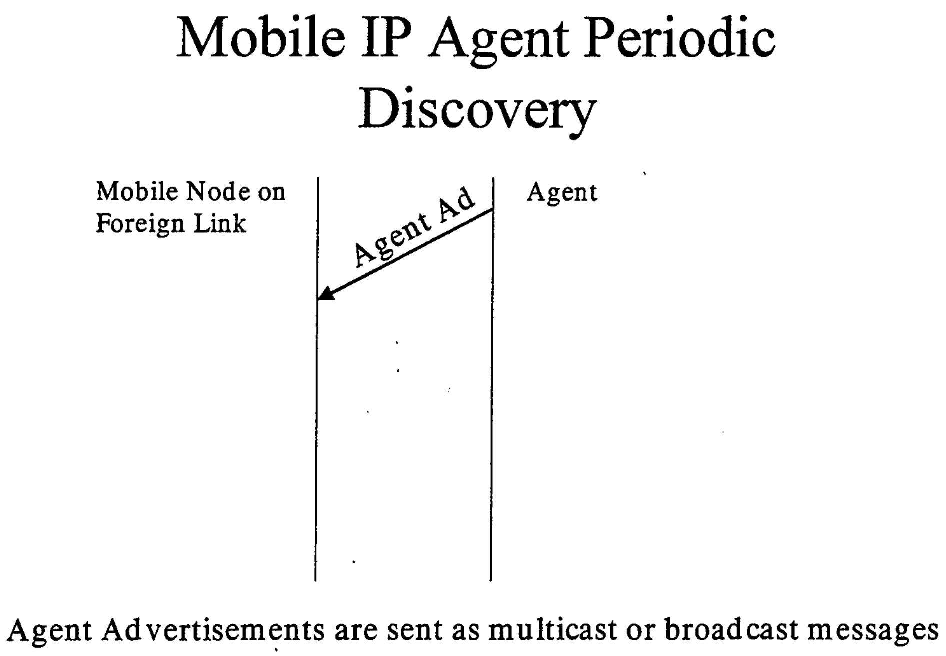
1. Agent Discovery

Agent discovery is the process by which a mobile node determines whether it is currently connected to its home network or to a foreign network, and by which a mobile node can detect when it has moved from one network to another. When connected to a foreign network, the agent discovery process allows the mobile node to determine the foreign agent's care-of-address.

We will now describe how mobile nodes, foreign agents, and home agents cooperate to accomplish these functions. Mobile IP extends ICMP router discovery as its primary mechanism for agent discovery. An agent advertisement is formed by including a Mobility Agent Advertisement Extension in an ICMP Router Advertisement message.

Agent discovery consists of two messages. The first, agent advertisements, are used by home or foreign agents to announce their capabilities to mobile nodes. These agent advertisements are periodically transmitted as a broadcast message, which allows any mobile node connected to the link to gain their IP address and capabilities. The second type of message is an agent solicitation. These are sent by mobile nodes to force a home agent or foreign agent to transmit an agent advertisement message. This is especially useful when the frequency at which agents are transmitting is too low for a mobile node that is rapidly moving from one network to another.

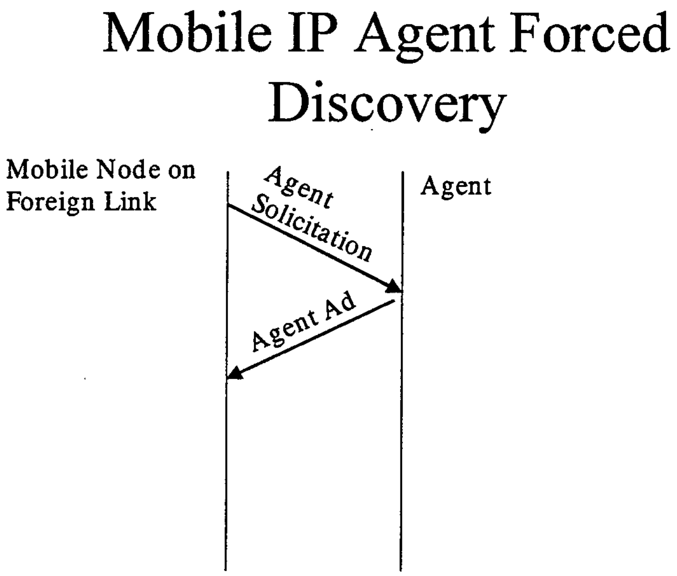
Figure 2 depicts the Mobile IP Agent Advertisement process and Figure 3 depicts the Mobile IP Agent Solicitation process.



Mobile IP Agent Periodic Discovery

Agent Advertisements are sent as multicast or broadcast messages

Figure 2. Mobile IP agent advertisement



Mobile IP Agent Forced Discovery

Figure 3. Mobile IP agent solicitation

An agent advertisement is an ICMP Router Advertisement that has been extended to carry mobility agent advertisement extensions. Figure 4 shows the frame format of this extension.

Mobility Agent Advertisement Extension

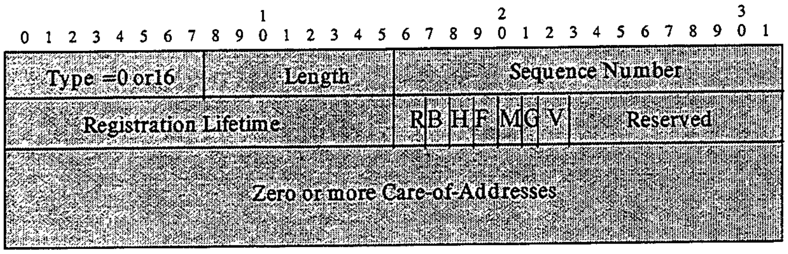


Figure 4. Mobility agent advertisement extension

The individual fields of the mobility agent advertisement extension are defined as follows:

- Type: 0 means the mobility agent handles both Mobile IP and regular IP traffic. 16 means that the mobility agent does not route regular IP traffic
- Length: (6 + 4*N), where N is the number of care-of-addresses advertised
- Sequence Number: The count of agent advertisement messages sent since the agent was initialized
- Registration Lifetime: The longest lifetime (measured in seconds) that this agent is willing to accept in any registration request; a value of 65,535 indicates infinity
- R: This bit means registration required. Registration with this foreign agent is required
- B: This bit means the agent is busy. If this bit is set, the foreign agent will not accept registrations from additional mobile nodes.

- H: This bit means agent is a home agent. If this bit is set, this agent offers service as a home agent on the link on which the agent advertisement message is sent.
- F: This bit means agent is a foreign agent. If this bit is set, this agent offers service as a foreign agent on the link on which the agent advertisement message is sent.
- M: This bit means minimal encapsulation is used. If this bit is set, this agent implements receiving tunneled datagrams that use minimal encapsulation.
- G: This bit means generic record encapsulation is used. If this bit is set, the agent implements receiving tunneled datagrams that use generic record encapsulation
- V: This bit means Van Jacobsen header compression is used. If this bit is set, the agent supports use of Van Jacobsen header compression over this link with any registered mobile node.
- Reserved: Sent as 0; ignored on reception
- Care-of-Address: The advertised foreign agent care-of-addresses provided by this foreign agent. An agent advertisement is required to include at least one care-of-address if the F bit is set. The number of care-of-addresses present is determined by the length of the extension

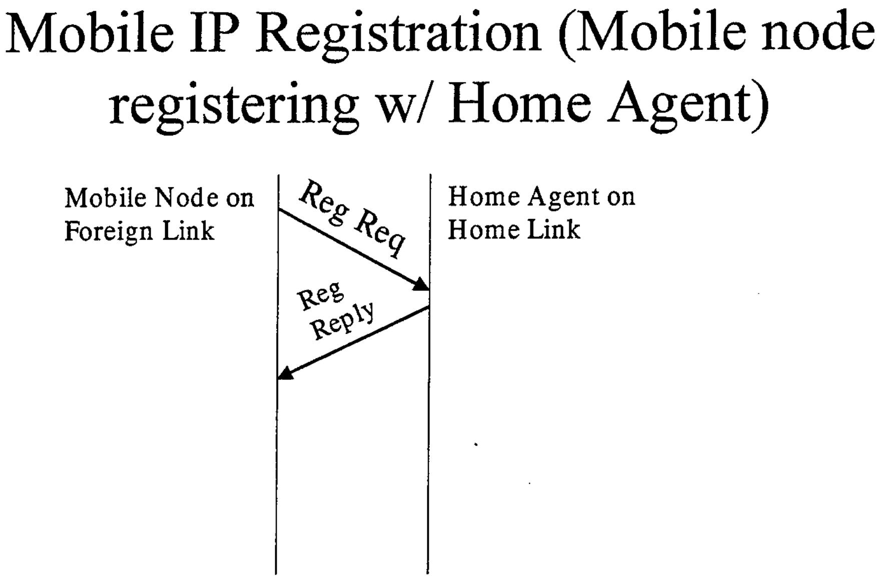
The mobile agent solicitation message is identical to the ICMP router solicitation and is defined by RFC 1256. Since Mobile IP makes no changes to this message, the reader is referred to RFC 1256 for the details of the solicitation message. When a home or foreign agent receives one, it should immediately respond with an agent advertisement.

To summarize, an agent advertisement performs the following functions:

- Allows for the detection of mobility agents
- Lists one or more available care-of-addresses
- Informs the mobile node about any special features provided by the foreign agent with respect to encapsulation techniques
- Allows the mobile node to determine the network number and the status of their link to the Internet
- Allows the mobile node to determine whether the agent is a foreign agent, a home agent, or both, and therefore whether it is on its home network or foreign network

2. Agent Registration

Once a mobile node has obtained a care-of-address and has determined that it is on a new network, its home agent must find out about it. This process begins with a registration request either directly to the home agent or with the assistance of the foreign agent as shown in Figure 5 and Figure 6.



Mobile IP Registration (Mobile node registering w/ Home Agent)

Figure 5. Mobile IP registration with home agent

Mobile IP Registration (Mobile node registering w/ Foreign Agent)

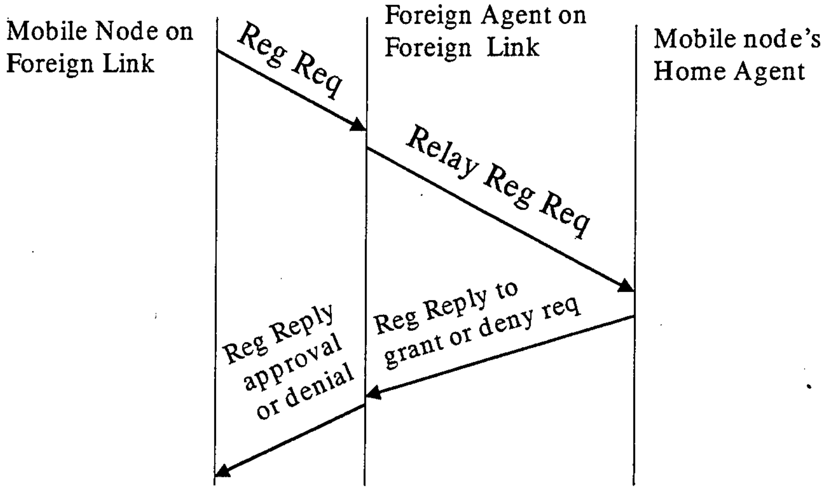

Mobile Node on Foreign Link
Foreign Agent on Foreign Link
Mobile node's Home Agent
Reg Req
Relay Reg Req
Reg Reply to grant or deny req
Reg Reply approval or denial

Figure 6. Mobile IP registration with foreign agent

The registration request and registration reply are carried within the data portion of a User Datagram Protocol (UDP) segment. When the home agent receives the registration request, it adds the necessary information to its routing table, approves the request, and sends a registration reply back to the mobile node. Registration requests contain parameters and flags that characterize the tunnel through which the home agent will deliver packets to the care-of-address. When a home agent accepts the request, it begins to associate the home address of the mobile node with the care-of-address, and maintains this association until the registration lifetime expires. The triplet that contains the home address, care-of-address, and registration lifetime is called a binding for a mobile node. The need for authentication in the registration process is extremely clear. The home agent must be certain that the registration was originated by the mobile node and not by some malicious node pretending to be the mobile node. The frame format of the registration request and registration reply are shown in Figure 7 and Figure 8.

Mobility Agent Registration Request

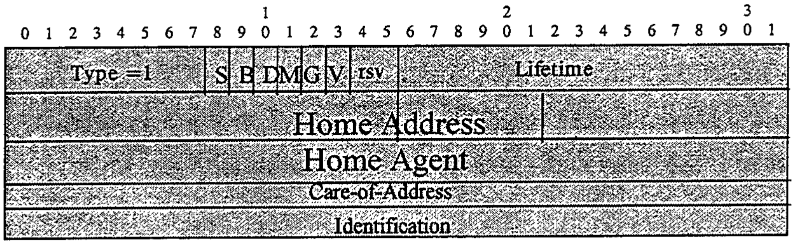


Figure 7. Mobility agent registration request

The individual fields of the mobility agent registration request are defined as follows:

- Type: 1 means this is a registration request
- S: This bit means that simultaneous bindings are used. By setting this bit, the mobile node requests that the home agent retain its prior mobility settings
- B: This bit means that datagrams be broadcast. By setting this bit, the mobile node requests that the home agent tunnel to it any broadcast datagrams that it receives on the home network
- D: This bit means that decapsulation will be performed. By setting this bit, the mobile node informs the home agent that it will decapsulate datagrams that are sent to the care-of-address.
- M: This bit means minimal encapsulation is used. By setting this bit, the mobile node requests that its home agent use minimal encapsulation for datagrams tunneled to the mobile node
- G: This bit means generic record encapsulation is used. By setting this bit, the mobile node requests that its home agent use generic record encapsulation for datagrams tunneled to the mobile node

- V: This bit means Van Jacobsen header compression is used. By setting this bit, the mobile node requests that its home agent use Van Jacobsen header compression over its link with the mobile node
- Rsv: reserved bit; sent as 0 and ignored on reception
- Lifetime: The number of seconds remaining before the registration is expired
- Home Address: The IP address of the mobile node
- Home Agent: The IP address of the mobile node's home agent
- Care-of-Address: The IP address for the tunnel endpoint
- Identification: A 64 bit number constructed by the mobile node and used for matching registration requests with registration replies, as well as for protecting against replay attacks of registration messages

Mobility agents return a registration reply message to a mobile node that has sent a registration request message. If the mobile node is requesting service from a foreign agent, that foreign agent will receive the reply from the home agent and subsequently relay it to the mobile node. The reply message informs the mobile node of the status of its request and indicates the lifetime granted by the home agent.

Mobility Agent Registration Reply

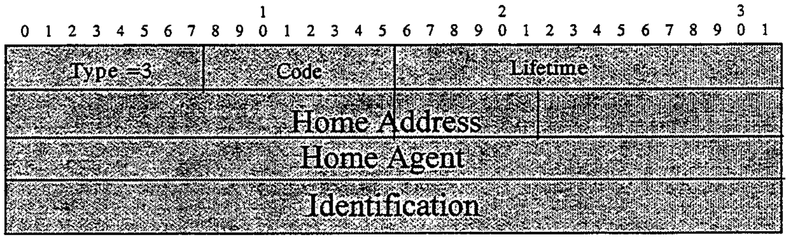


Figure 8. Mobility agent registration reply

The individual fields of the mobility agent registration reply are defined as follows:

- Type: 3 means this is a registration reply
- Code: A value indicating the result of the registration request. These will be explained in detail after all the fields have been discussed
- Lifetime: The duration for which a binding is valid. If the code field indicated that the registration was accepted, the lifetime field is set to the number of seconds remaining before the registration is considered expired.
- Home Address: The IP address of the mobile node
- Home Agent: The IP address of the mobile node's home agent
- Identification: The 64 bit number used for matching the registration request with an eventual registration reply, and for detecting future replay attacks of the registration message

The value of the code field are defined as follows:

Registration successful

- 0 indicates that the registration was accepted
- 1 indicates that the registration was accepted, but simultaneous mobility bindings are not supported

Registration denied by the foreign agent

- 64 indicates that the reason is unspecified
- 65 indicates that the reason is the node is administratively prohibited
- 66 indicates that the reason is insufficient resources
- 67 indicates that the reason is that the mobile node failed authentication
- 68 indicates that the reason is that the home agent failed authentication
- 69 indicates that the requested lifetime is too long
- 70 indicates that the reason is that the request is poorly formed
- 71 indicates that the reason is the reply is poorly formed
- 72 indicates that the reason is that the requested encapsulation method is unavailable
- 73 indicates that the reason is that the requested Van Jacobsen compression is unavailable

- 80 indicates that the reason is that the home network is unreachable (ICMP error received)
- 81 indicates that the reason is that the home agent host is unreachable (ICMP error received)
- 82 indicates that the reason is that the home agent port is unreachable (ICMP error received)
- 88 indicates that the home agent is unreachable (ICMP error received)

Registration denied by the home agent

- 128 indicates that the reason is unspecified
- 129 indicates that the reason is the node is administratively prohibited
- 130 indicates that the reason is insufficient resources
- 131 indicates that the reason is that the mobile node failed authentication
- 132 indicates that the reason is that the foreign agent failed authentication
- 133 indicates that the reason is that there is a registration identification mismatch
- 134 indicates that the reason is that the request is poorly formed
- 135 indicates that the reason is that there are too many simultaneous mobility bindings
- 136 indicates that the reason is that the home agent address is unknown

3. Care-of-Address Tunneling

Mobile IP provides two methods of acquiring a care-of-address. First is a care-of-address provided by a foreign agent through its agent advertisement messages. In this case the care-of-address is an IP address of the foreign agent. Second is called a collocated care-of-address, which is a care-of-address acquired by the mobile node as a local IP address through some external means, which the mobile node then associates with one of its own network interfaces. The address may be dynamically acquired as a temporary address by the mobile node, such as through DHCP or it may be owned by the mobile node for use only when visiting some foreign network, such as a CDPD address when in the range of a CDPD network. When using a collocated care-of-address the mobile node serves as the endpoint of the tunnel and performs decapsulation of the datagrams tunneled to it. This allows a mobile node to function without a foreign agent, but does require some means of acquiring an IP address. There is an important distinction to be made here between the care-of-address and the foreign agent functions. The care-of-address is simply the endpoint of a tunnel. It might be a foreign agent care-of-address or an address temporarily acquired by the mobile node. A foreign agent, on the other hand, is a mobility agent that provides services to mobile nodes.

B. MOBILE IP IN ACTION

Figure 9 (Lancki, 1996) further illustrates the main ideas behind Mobile IP.

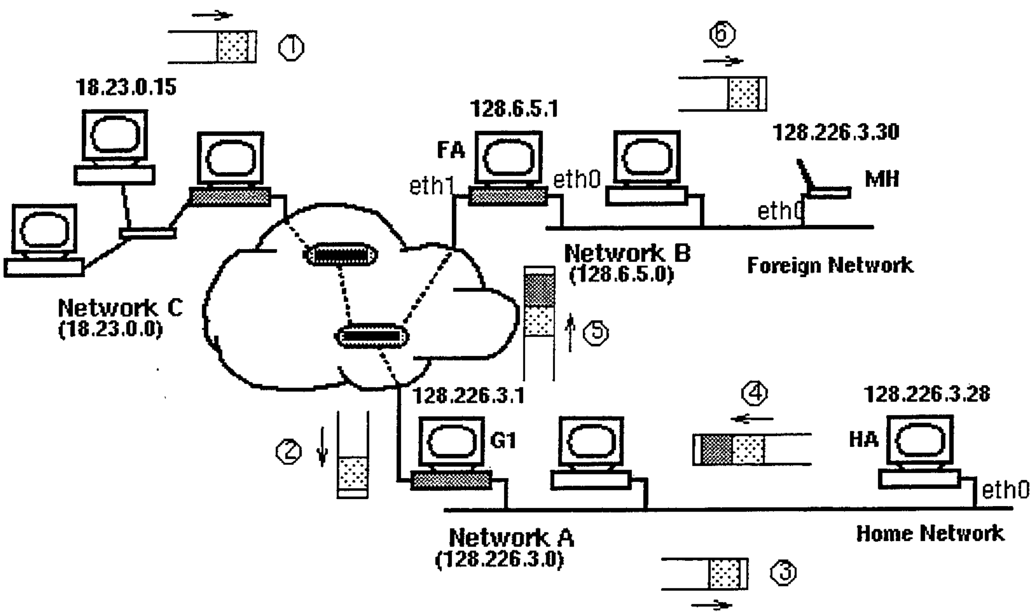


Figure 9. IP datagram flow to a mobile node away from its home network

This figure shows an IP datagram as it flows from the node with IP address 18.23.0.15 to the mobile host with IP address 128.226.3.30. The mobile node is away from its home network as shown in this figure. The node with IP address 128.226.3.28 and labeled as HA is acting as the home agent for this mobile node and the node with IP address 128.6.5.1 and labeled as FA is acting as the foreign agent for this mobile node. The IP header in the datagram as it leaves Network C indicates 128.226.3.30 as the destination. Therefore, this datagram is routed to Network A (steps 1 and 2). Here, the home agent picks up the datagram and inserts an additional IP header before re-injecting it into the network (steps 3 and 4). The new IP header carries 128.6.5.1 as its destination address. As this header is seen by the intermediate routers along the way, the datagram is correctly routed to the foreign agent (step 5). Assuming the registration process has already informed the foreign agent of the mobile node's presence on the network, when the encapsulated datagram arrives at the foreign agent, the outer header is stripped. The newly exposed header reveals the mobile node as the destination and the datagram is forwarded appropriately (step 6).

THIS PAGE INTENTIONALLY LEFT BLANK

IV. MOBILE IP VERSION VI DISCUSSION

A. MOBILE IP VERSION VI OVERVIEW

This chapter discusses mobility support for the Internet Protocol Version 6 (IPv6). IPv6 is expected to replace IPv4 as the primary network layer protocol of the Internet. This discussion assumes a basic knowledge of the IPv6 protocol and will very simply highlight the major differences between IPv4 and IPv6. For readers unfamiliar with IPv6, most TCP/IP networking texts will have the required background information. The two biggest differences between IPv4 and IPv6 are the size of the addresses, 128 bits in IPv6 versus 32 bits in IPv4, and that many of the less frequently used fields in IPv4 have been moved out of the IPv6 header and into the optional extension headers.

Mobility for IPv6 borrows the general ideas of a home network, home agent, and care-of-address from Mobile IP for IPv4. As with Mobile IP for IPv4, a mobile node should always be reachable by sending packets to its home address. If the mobile node is no longer attached to its home network, the home agent is responsible for sending datagrams to the mobile node. This implies that the home agent and mobile node cooperate to make sure that the home agent is aware of the care-of-address of the mobile node, this cooperation is the registration process that occurs whenever the mobile node acquires a new care-of-address.

Figure 10 describes the overall picture for IPv6. In this figure we see there are home networks, foreign networks, home agents, and mobile nodes. However, in IPv6 there are no foreign agents, instead there are access points, or points at which the mobile nodes may connect to the IPv6 Internet.

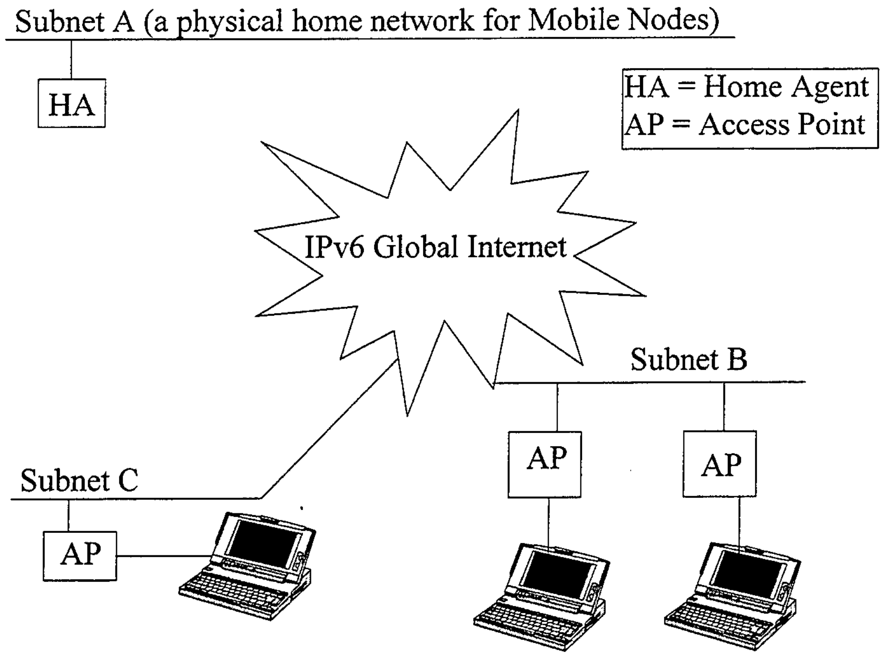


Figure 10. IPv6 overall picture

The design of IPv6 is much better suited to Mobile IP than IPv4. Mobility is supported by the action of the mobile node, which takes the responsibility of supplying location information to each of its corresponding nodes. The methods of IPv6 for automatic address configuration are perfect for allowing mobile nodes to configure their care-of-addresses at each new point of attachment.

One of the requirements of IPv6 is that every node must support address autoconfiguration and neighbor discovery, which is an improved protocol that takes the place of Address Resolution Protocol (ARP) in IPv4. Using these protocols, a mobile node is able to determine the network prefix at any new point of attachment it might select, and subsequently create or obtain a globally routable IPv6 address that is appropriate for that point of attachment. These are the only steps necessary for obtaining a care-of-address. So, by using built in functions of IPv6, mobile nodes can perform for themselves the functions for which foreign agents were needed in IPv4. Therefore, foreign agents are eliminated from the protocol for Mobile IPv6.

When the mobile node moves, it informs its correspondent nodes, any node which a mobile node may be communicating with, about its new location. The intermediate nodes between the mobile and correspondent nodes do not need to know about the mobile node's new location. When a correspondent node wishes to deliver a packet to a mobile node, it does so by simply including a routing header in the packet with the care-of-address used as the address of the intermediate node in the routing header.

The home agent, while not usually a node with which the mobile node maintains active connections, must nevertheless always be aware of any change in the care-of-address by the mobile node as soon as possible. Although the home agent discovers and maintains the care-of-address information from the mobile node in a manner identical in almost all respects to that of any correspondent node, the home agent uses the information differently. First, when the home agent discovers that the mobile node has moved, it uses techniques from IPv6 neighbor discovery to indicate it has discovered a new MAC layer address for the mobile node to all the mobile node's correspondent nodes, this is similar to the operation of proxy ARP in IPv4. Second, when the home agent receives a packet destined to the mobile node, it must assume that the datagram is not to be modified in any way. Thus, the home agent uses IPv6 data encapsulation to deliver the datagram to the care-of-address. When the mobile node receives an encapsulated datagram, it will know to inform the correspondent node about its care-of-address. Lastly, since it is so important for reachability of the mobile node, the home agent must always acknowledge receipt of any care-of-address information from the mobile node.

Mobility is supported in IPv6 by the use of new destination options, each containing fields that specify the type and length of the option. Destination options are preferable for this purpose, since there is no need for intermediate routers to do any processing in route. Extensions to mobility support destination options may be included after the fixed portion of the option. The presence of such extensions will be indicated by the option length field. When the option length is greater than the number of octets taken up by the predetermined part of the header, the remaining octets are interpreted as extensions. Currently, the extensions are not defined. The three highest order bits of each destination option type are encoded to indicate specific processing of the option. For the mobility support destination options, these three bits are set to 110, to indicate the following processing details:

- The data within the option can't change en route to the packet's final destination
- When the destination is a multicast address, any node processing this option that doesn't recognize the option type must discard the packet
- When the destination is a unicast address, any node processing this option that doesn't recognize the option type must discard the packet and return an ICMP message to the packet's source address

Mobile IPv6 operation can be summarized as follows:

- A mobile node determines its current location using the IPv6 version of router discovery;
- The mobile node, when connected to a foreign link, uses IPv6 address autoconfiguration to acquire a care-of-address on the foreign link;
- The mobile node notifies its home agent of its care-of-address;
- The mobile node reports its care-of-address to any correspondents;
- Packets sent by correspondents that do not know the care-of-address route the packet to the mobile node's home agent, where the home agent then tunnels them to the mobile node;
- Packets sent by correspondents that do know the care-of-address are sent directly to the mobile node using an IPv6 routing header;
- Packets sent by mobile nodes are routed directly to their destination using no special mechanisms.

1. Binding Update Option

A mobile node uses a new destination option, called the binding update option, to inform its home agent and any correspondent nodes about its new care-of-address. Any packet that includes a binding update option is required to meet the following two requirements:

- The source address in the IP header of the packet has to be the home address for the binding, since the option does not contain a field to carry the mobile node's home address separately.
- The packet must include an IPv6 authentication header to protect against forged binding updates.

Figure 11 shows the binding update destination option format.

Binding Update Option

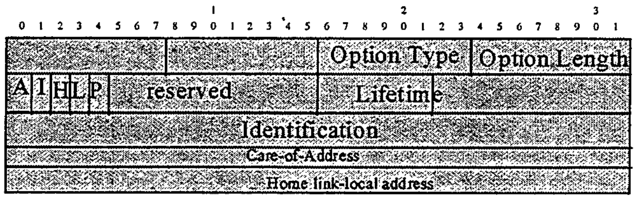


Figure 11. Binding update destination option format

The individual fields of the binding update option are defined as follows:

Option Type: 192 means that this is a binding update

Option Length: an eight bit unsigned integer, length of the option, in octets, excluding the option type and option length fields. For the current definition of the binding update option, this field must be set to 24 if the home link-local address present (L) bit is not set, and must otherwise be set to 40.

A: This bit means acknowledge. This bit is set by the sending node to request that a binding acknowledgement message be returned on receipt of the binding update option.

H: This bit means home registration. This bit is set by the sending node to request that the receiving node act as this node's home agent. The destination address in the IPv6 header of the packet carrying this option is required to be that of a router sharing the same network prefix as the source address in the IPv6 header of the packet.

L: This bit means home link-local address field is present. This bit is set by the sending node to request that the receiving node act as a proxy for the neighbor discovery protocol for the node while it is away from home. This bit is not allowed to be set unless the home registration (H) bit is also set.

P: Not yet defined.

I: Not yet defined.

Reserved: Sent as 0; ignored on reception

Lifetime: This field is a 16 bit unsigned integer. It represents the number of seconds remaining before the binding must be considered expired. A value of all ones, 65535, indicates infinity. A value of zero indicates that the binding cache entry for the mobile node should be deleted.

Identification: This field is a 32 bit number. It is used by the receiving node to sequence binding updates, and by the sending node to match a returned binding acknowledgement message with this binding update. The identification field also serves to protect against replay attacks for binding updates.

Care-of-address: This field is the care-of-address of the mobile node for this binding. When it is set equal to the home address of the mobile node, the binding update option instead indicates that any existing binding for the mobile node should be deleted and no binding for the mobile node should be created in this case.

Home link-local address: The link-local address of the mobile node used by the mobile node when it was last attached to its home network. This field is optional and is only used when the home link-local address (L) bit is set.

The binding update and binding acknowledgement between a mobile node and a home agent or correspondent are prompted by the mobile node receiving a binding request. This message exchange has three common scenarios (Solomon, 1998):

Scenario 1: A mobile node connects to a foreign link and informs its home agent of its new care-of-address.

Scenario 2: A mobile node connects to a foreign link and informs a correspondent node of its new care-of-address.

Scenario 3: A mobile node return to its home link and informs its home agent that it is no longer attached to a foreign link.

2. Binding Acknowledgement Option

The binding acknowledgement option is not required in most cases for binding updates. The mobile node will know that the correspondent node has received the update, because the correspondent node will no longer send datagrams to the old address. However, the mobile node must be sure right away that the home agent has received binding updates, so the home agent must always acknowledge receipt of binding updates.

Any packet that includes a binding acknowledgement option is required to meet the following two requirements:

- The packet destination address in the IP header is required to be sent back to the node sending the binding update. Only the mobile node is authorized to send the binding update. This means that the binding update will be sent to the mobile node. The acknowledgement is delivered to the mobile node at its home address by way of a routing header containing the mobile node's care-of-address.
- The packet is also required to include an IPv6 authentication header in order to protect against forged binding acknowledgements.

Figure 12 shows the binding acknowledgement option format.

Binding Acknowledgement Option

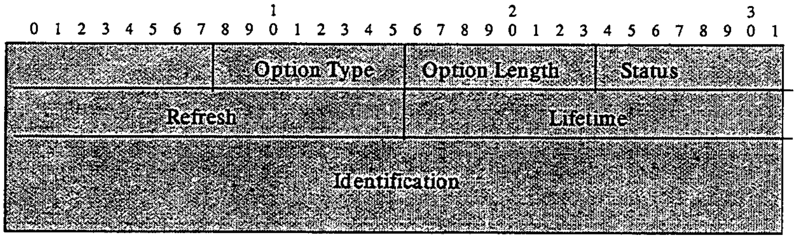


Figure 12. Binding acknowledgement

The individual fields of the binding acknowledgement option are defined as follows:

Option Type: 193 means that this is a binding acknowledgement

Option Length: an eight bit unsigned integer, length of the option, in octets, excluding the option type and option length fields. For the current definition of the binding update option, this field must be set to 8.

Status: an eight bit unsigned integer indicating the disposition of the binding update. Values of less than 128 indicate that the binding update was accepted by the receiving node. The only currently defined status less than 128 is 0, which means the binding update was accepted. Values of greater than 128 indicate that the binding was rejected by the receiving node. The following status values are currently defined:

- 128: Reason unspecified
- 129: Poorly formed binding update
- 130: Binding administratively prohibited
- 131: Insufficient resources
- 132: Home registration unsupported
- 133: Not home network
- 134: Identification field mismatch
- 135: Unknown home agent address

Refresh: This field is the recommended period at which the mobile node should send a new binding update to this node to refresh the mobile node's binding in this node's binding cache.

Lifetime: This field is the granted lifetime for which this node will attempt to retain the entry for this mobile node in its binding cache. If the node sending the binding acknowledgement is serving as the mobile node's home agent, the lifetime period also indicates the period for which this node will continue this service. If the mobile node requires home agent service from this node beyond this period, the mobile node is requires to send a new binding update to it before the expiration of this period to extend the lifetime.

Identification: The acknowledgement is copied from the binding update option, for use by the mobile node in matching the acknowledgement with an outstanding binding update.

A binding acknowledgement is sent to a mobile node by a home agent or any other correspondent node to indicate that it has successfully received the mobile node's binding update.

3. Binding Request Option

The binding request option is sent to a mobile node by a correspondent node to request that the mobile node send it a binding update. A binding request indicates that the correspondent would like to know the mobile node's care-of-address. This is useful when the lifetime in an original binding update is near expiration and the correspondent node has reason to believe that it will continue to send packets to the mobile node. The binding request can be encoded in only a very few bytes as shown in Figure 13. Binding request are not required to be authenticated because they are solely advisory in nature and a mobile node should respond by sending a binding update to the requesting node.

Binding Request Option

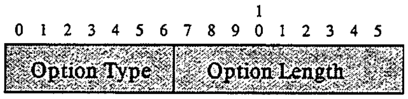


Figure 13. Binding request option

The individual fields of the binding request option are defined as follows:

Option Type: 194 means that this is a binding request

Option Length: an eight bit unsigned integer, length of the option, in octets, excluding the option type and option length fields. For the current definition of the binding update option, this field must be set to 0.

B. MOBILE IP VERSION 6 SUMMARY

IPv6 has been designed to offer a huge address space useful for the foreseeable future to enable better routing technology and to clean up various architectural details that are seen to be deficiencies in IPv4. Option processing in IPv6 is able to be done without the loss of performance associated with the IPv4 options. Security is a required feature for every IPv6 compliant node. This has the effect of allowing a much cleaner specification for supporting mobility because of the requirement to authenticate care-of-addresses. The binding updates that provide the care-of-addresses to home agents and correspondent nodes are in destination options, and the needed authentication is also in a destination option. Thus, IPv6 mobility offers all the good features of IPv4 mobility with less additional protocol code and a natural fit with the rest of the base IPv6 protocol. IPv6 mobility uses movement detection and care-of-address acquisition techniques available with the standard IPv6 protocol, thus IPv6 mobility requirements place few additional requirements on IPv6 nodes.

In mobile IPv6, a mobile node notifies not only its home agent, but also certain correspondent nodes of its current care-of-address. This allows correspondents which know the mobile node's care-of-address to route packets directly to the mobile node using a routing header. Packets sent by correspondents that do not know that care-of-address are routed just as in Mobile IPv4. They are routed to the home link where the home agent tunnels them to the care-of-address. Also, as in Mobile IPv4, packets sent by mobile nodes are routed directly to their destination, without the need for any special routing mechanisms..

Finally, the specification for Mobile IPv6 is still changing rapidly and the information contained in this chapter is based on the draft work in progress of version 2 of the Mobile IPv6 protocol.

V. MOBILE IP PROTOCOL ANALYSIS

This chapter is divided into three sections. Section A will describe the specification of the Mobile IP protocol from the perspective of the three main entities, section B will describe the reachability analysis, and section C will discuss the reachability analysis in detail.

A. MOBILE IP PROTOCOL SPECIFICATION

1. Overall Discussion of Mobile IP Protocol Specification

The discussion that follows will first specify the three defined entities in Mobile IP, Mobile Node (MN), Home Agent (HA), and Foreign Agent (FA). For simplification, this discussion assumes there is only one of each entity. In all cases, 0 is the initial state and the format is as follows: -AA,MN means that an Agent Advertisement is sent from the Mobile Node and +RR,FA means that a Registration Reply is received from the Foreign Agent.

Figure 14 provides a simple pictorial description of the example network this protocol specification will be describing, it shows a Mobile Node (MN) moving from its home network to a foreign network.

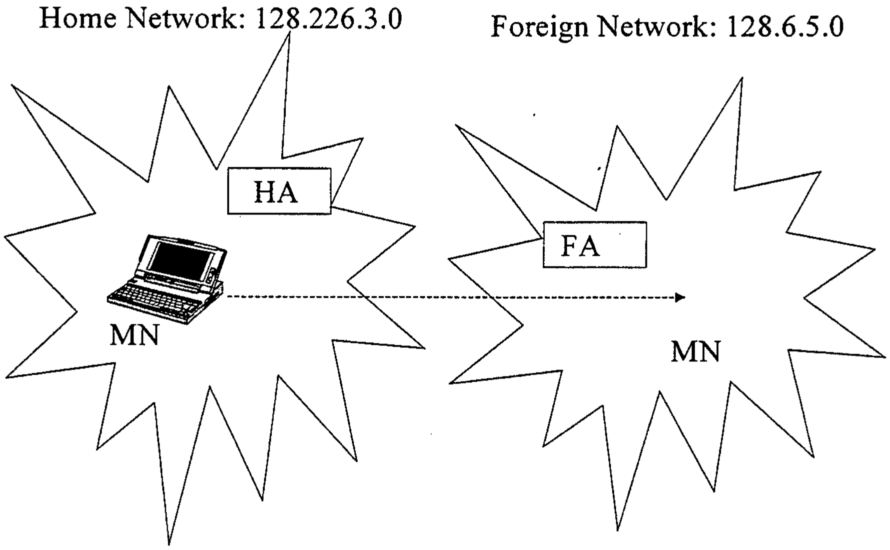


Figure 14. Mobile node moving from home network to foreign network

2. Mobile Node

Figure 15 describes the protocol specification of the Mobile Node.

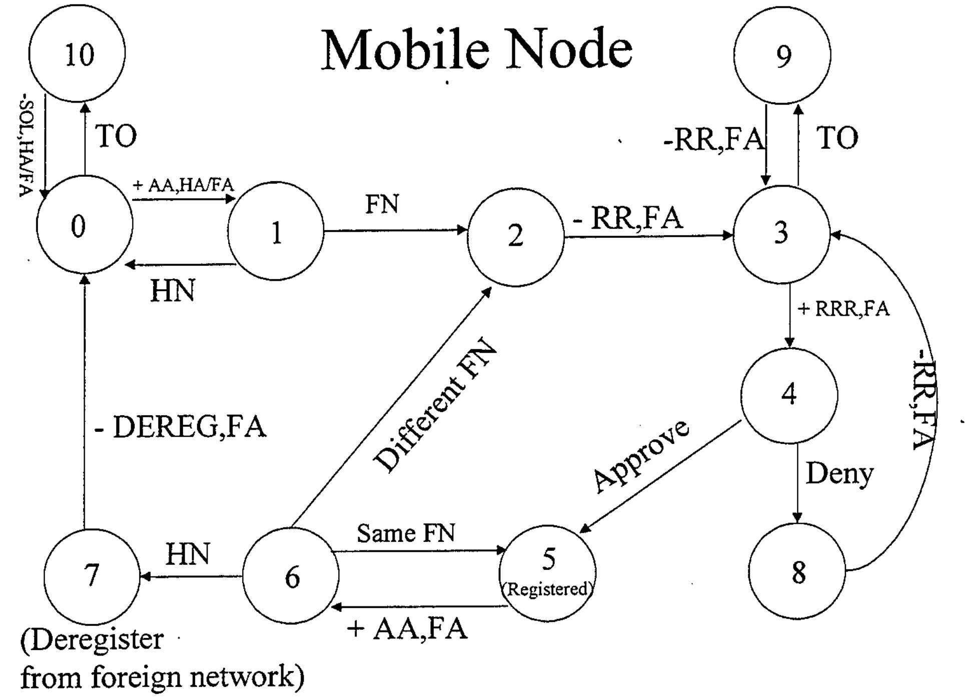


Figure 15. Mobile node specification

Table 1 lists all the message type abbreviations and corresponding definitions used in this discussion that relate to the Mobile Node specification.

Abbreviation	Definition
AA	Agent Advertisement
APPROVE	Registration Request Approved
DENY	Registration Request Denied
DEREG	Deregister Message
FA	Foreign Agent
FN	Foreign Network
HN	Home Network
RR	Registration Request
RRR	Registration Request Reply
SOL	Solicitation
TO	Time Out

Table 1. Abbreviations with corresponding definitions for the mobile node specification

3. Home Agent

Figure 16 describes the protocol specification of the Home Agent.

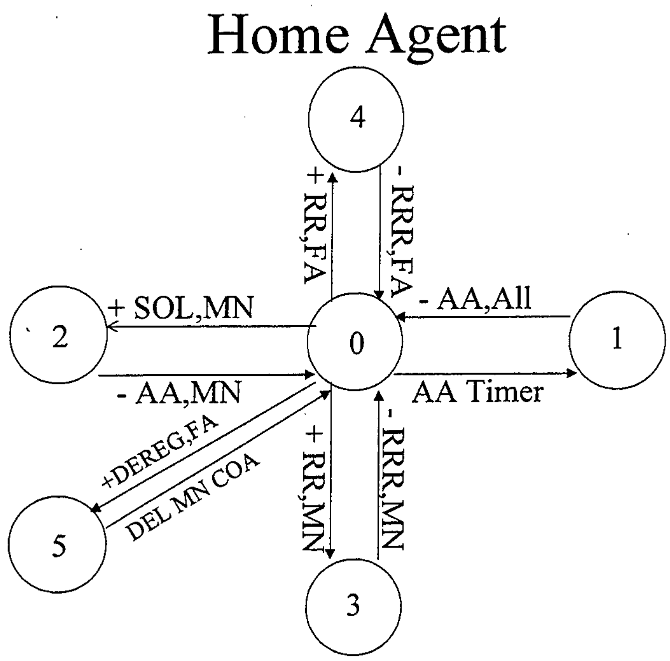


Figure 16. Home agent specification

Table 2 lists all the message type abbreviations and corresponding definitions used in this discussion that relate to the Home Agent specification.

Abbreviation	**Definition**
AA	Agent Advertisement
COA	Care-of-Address
DEL	Delete
DEREG	Deregister Message
FA	Foreign Agent
MN	Mobile Node
RR	Registration Request
RRR	Registration Request Reply
SOL	Solicitation

Table 2. Abbreviations with corresponding definitions for the home agent specification

4. Foreign Agent

Figure 17 describes the protocol specification of the Foreign Agent.

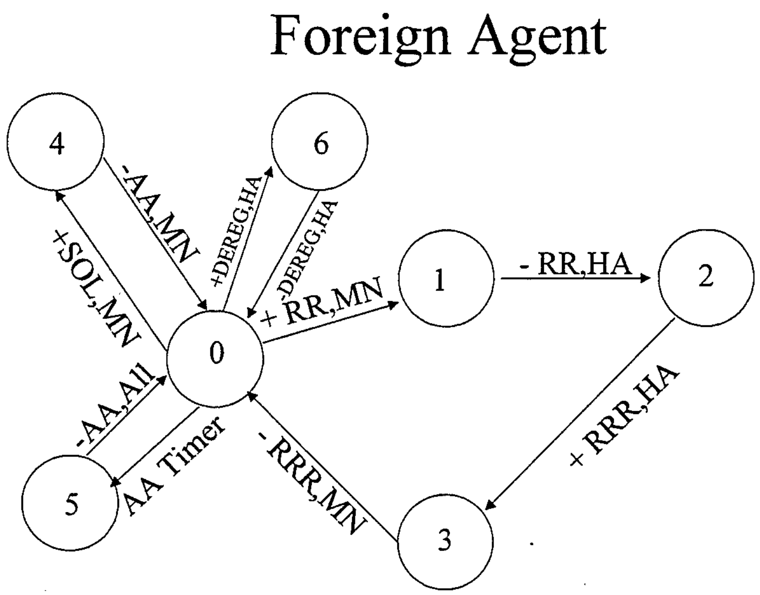


Figure 17. Foreign agent specification

Table 3 lists all the message type abbreviations and corresponding definitions used in this discussion that relate to the Foreign Agent specification.

Abbreviation	**Definition**
AA	Agent Advertisement
DEREG	Deregister Message
HA	Home Agent
MN	Mobile Node
RR	Registration Request
RRR	Registration Request Reply
SOL	Solicitation

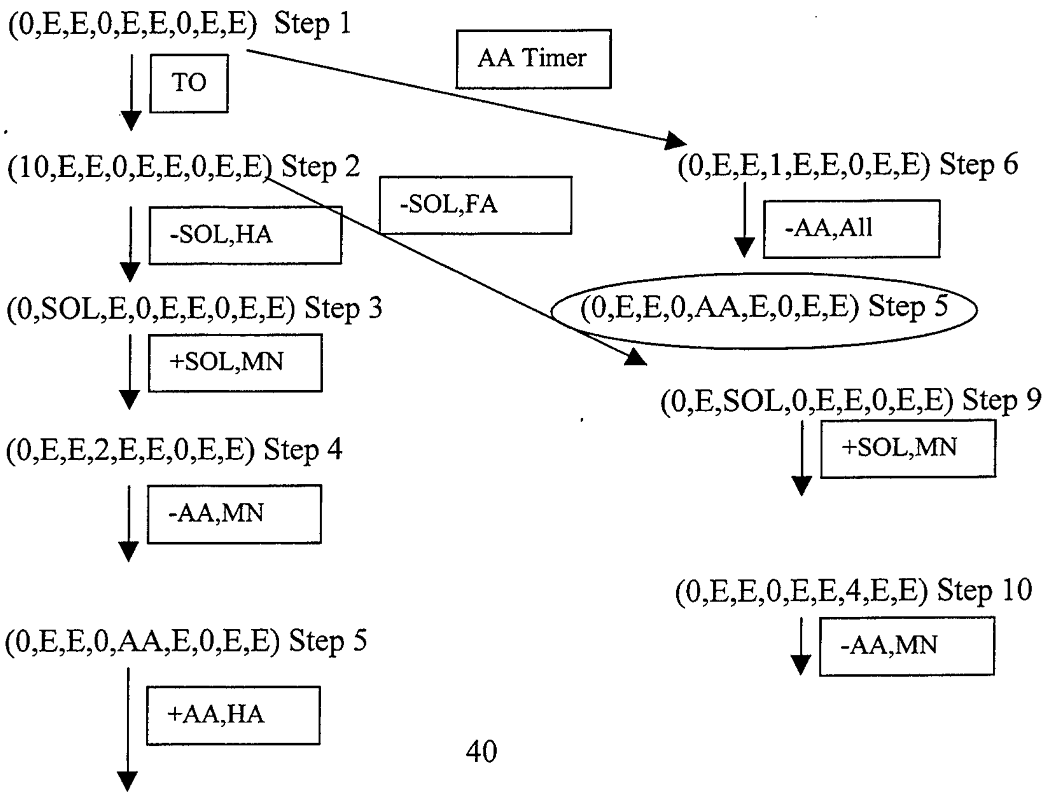
Table 3. Abbreviations with corresponding definitions for the foreign agent specification

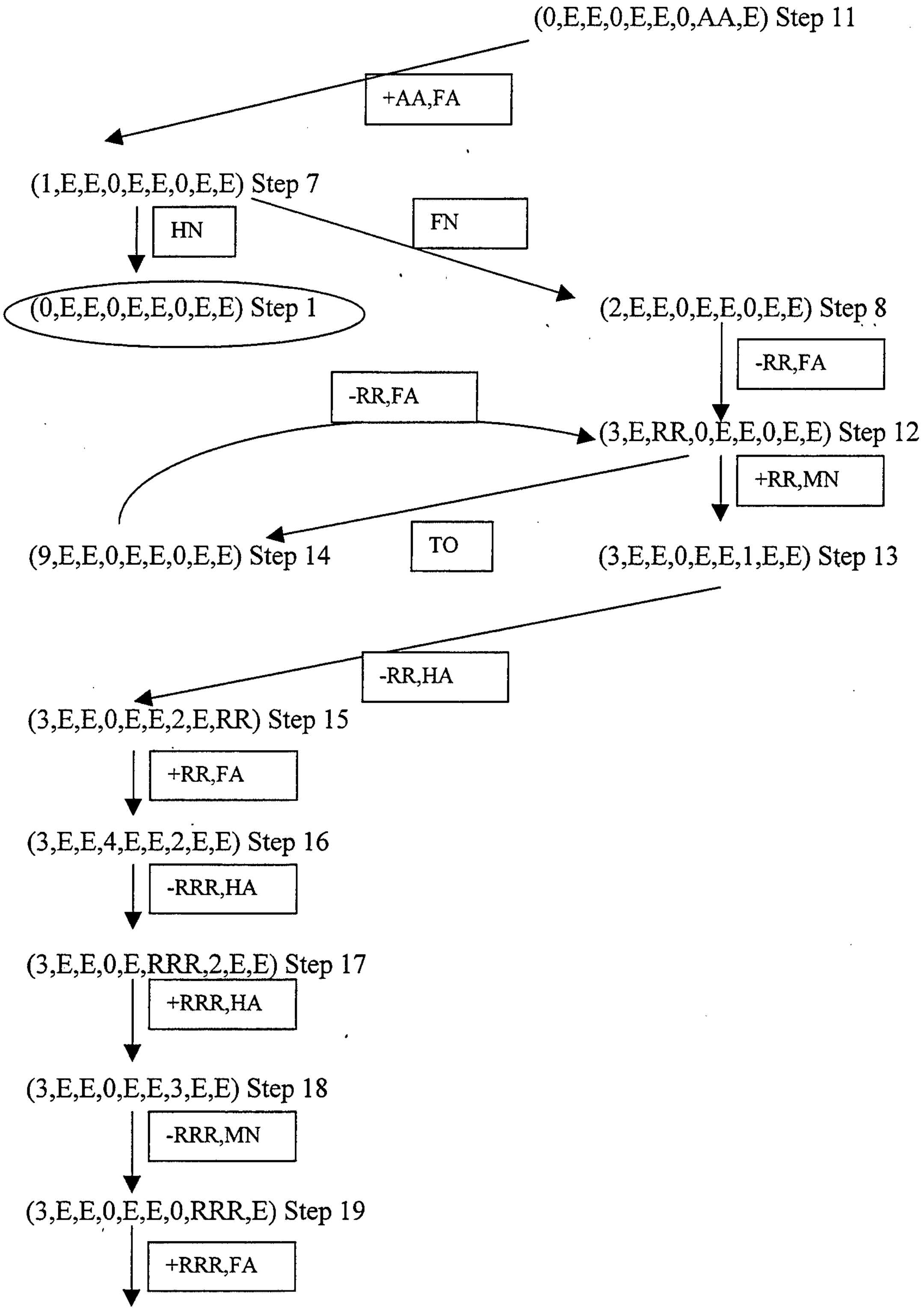
B. MOBILE IP REACHABILITY ANALYSIS

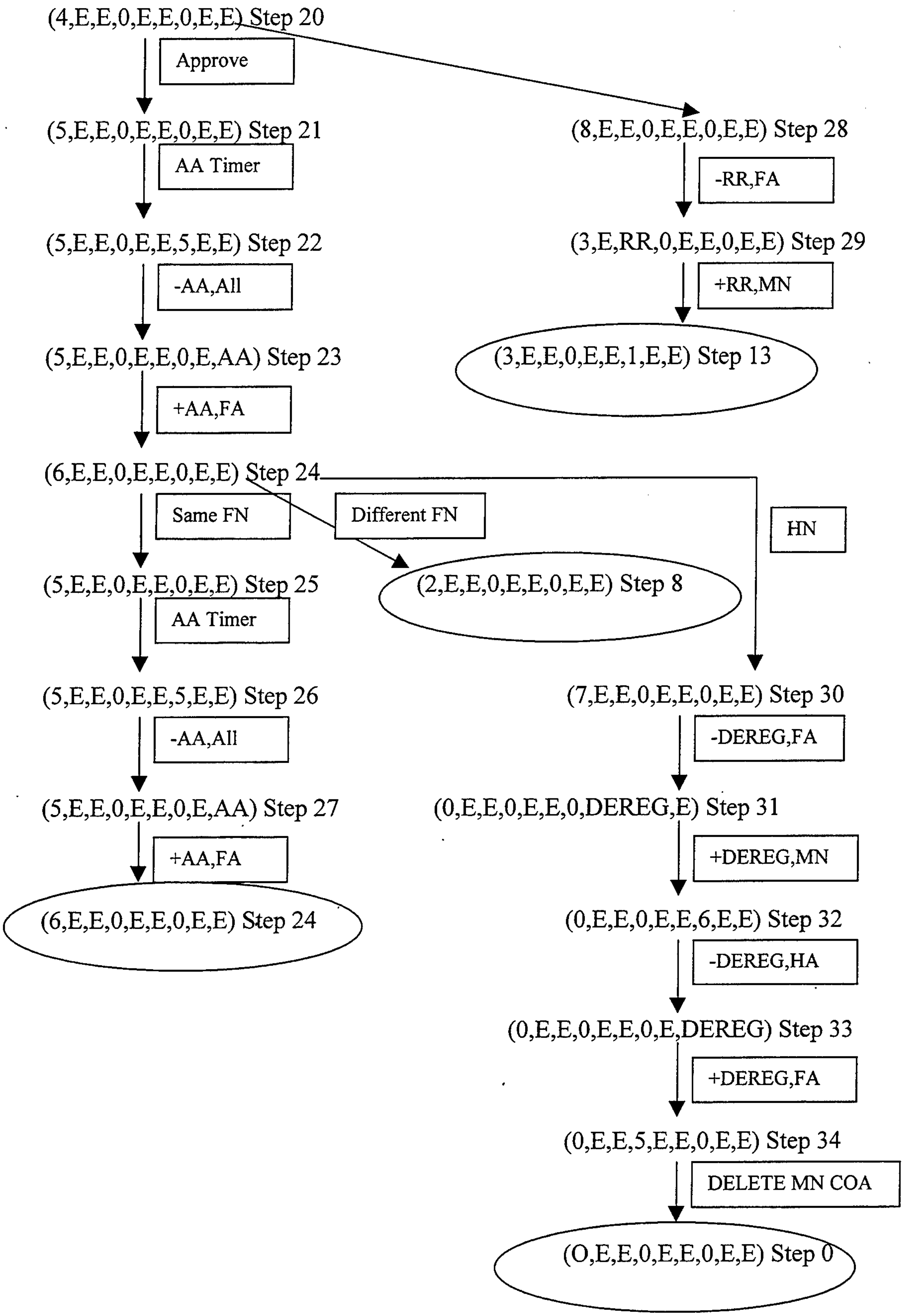
Now that we have specified the states that a Mobile Node, Home Agent or Foreign Agent can achieve and the messages that they can send and receive, we must perform a reachability analysis in order to be sure that the protocol is sound. By sound we mean that no state is unreachable and there are no states with unspecified receptions. The analysis will follow the following format: (MN,CH1,CH2,HA,CH3,CH4,FA,CH5,CH6).

In this format MN represents Mobile Node, HA represents Home Agent and FA represents Foreign Agent, CH1 represents the channel from the MN to the HA, CH2 represents the channel from the MN to the FA, CH3 represents the channel from the HA to the MN, CH4 represents the channel from the HA to the FA, CH5 represents the channel from the FA to the MN, and CH6 represents the channel from the FA to the HA.

The initial state, step 1 is (0,E,E,0,E,E,0,E,E) this means that the MN, HA, and FA are all in state 0 and all the channels are empty. Step 2 is (10,E,E,0,E,E,0,E,E) this means that the MN is in state 10 and the HA and FA are in state 0 and all channels are still empty. Step 3 is (0,SOL,E,0,E,E,0,E,E) this means that the MN, HA, and FA are all in state 0 and CH1 contains the message SOL and all other channels are empty. A state with a circle around it means that this state has been visited before. The reachability analysis will continue with this format.


(0,E,E,0,E,E,0,E,E) Step 1
TO
AA Timer
(10,E,E,0,E,E,0,E,E) Step 2
-SOL,HA
-SOL,FA
(0,E,E,1,E,E,0,E,E) Step 6
-AA,All
(0,SOL,E,0,E,E,0,E,E) Step 3
(0,E,E,0,AA,E,0,E,E) Step 5
+SOL,MN
(0,E,SOL,0,E,E,0,E,E) Step 9
+SOL,MN
(0,E,E,2,E,E,0,E,E) Step 4
-AA,MN
(0,E,E,0,E,E,4,E,E) Step 10
-AA,MN
(0,E,E,0,AA,E,0,E,E) Step 5
+AA,HA


(0,E,E,0,E,E,0,AA,E) Step 11
+AA,FA
(1,E,E,0,E,E,0,E,E) Step 7
HN
FN
(0,E,E,0,E,E,0,E,E) Step 1
(2,E,E,0,E,E,0,E,E) Step 8
-RR,FA
-RR,FA
(3,E,RR,0,E,E,0,E,E) Step 12
+RR,MN
TO
(9,E,E,0,E,E,0,E,E) Step 14
(3,E,E,0,E,E,1,E,E) Step 13
-RR,HA
(3,E,E,0,E,E,2,E,RR) Step 15
+RR,FA
(3,E,E,4,E,E,2,E,E) Step 16
-RRR,HA
(3,E,E,0,E,RRR,2,E,E) Step 17
+RRR,HA
(3,E,E,0,E,E,3,E,E) Step 18
-RRR,MN
(3,E,E,0,E,E,0,RRR,E) Step 19
+RRR,FA


(4,E,E,0,E,E,0,E,E) Step 20
Approve
(5,E,E,0,E,E,0,E,E) Step 21
AA Timer
(5,E,E,0,E,E,5,E,E) Step 22
-AA,All
(5,E,E,0,E,E,0,E,AA) Step 23
+AA,FA
(6,E,E,0,E,E,0,E,E) Step 24
Same FN
Different FN
HN
(5,E,E,0,E,E,0,E,E) Step 25
AA Timer
(5,E,E,0,E,E,5,E,E) Step 26
-AA,All
(5,E,E,0,E,E,0,E,AA) Step 27
+AA,FA
(6,E,E,0,E,E,0,E,E) Step 24
(8,E,E,0,E,E,0,E,E) Step 28
-RR,FA
(3,E,RR,0,E,E,0,E,E) Step 29
+RR,MN
(3,E,E,0,E,E,1,E,E) Step 13
(2,E,E,0,E,E,0,E,E) Step 8
(7,E,E,0,E,E,0,E,E) Step 30
-DEREG,FA
(0,E,E,0,E,E,0,DEREG,E) Step 31
+DEREG,MN
(0,E,E,0,E,E,6,E,E) Step 32
-DEREG,HA
(0,E,E,0,E,E,0,E,DEREG) Step 33
+DEREG,FA
(0,E,E,5,E,E,0,E,E) Step 34
DELETE MN COA
(O,E,E,0,E,E,0,E,E) Step 0

This reachability analysis concludes that the protocol will work as specified in the case of one Mobile Node, one Home Agent, and one Foreign Agent.

C. MOBILE IP PROTOCOL ANALYSIS DISCUSSION

Section A described the specification of the mobile node, the home agent, and the foreign agent. Section B performed a reachability analysis of the protocol. This section will expand upon the analysis conducted to discuss exactly what was accomplished, what was not accomplished and what the results of the analysis were.

1. Protocol Analysis Items Accomplished

This specification and reachability analysis accomplished a thorough review of a Mobile IP version IV system with one Mobile Node, one Home Agent and one Foreign Agent. As shown in Figure 14, this thesis explored the Mobile Node moving from its home network to a foreign network. Additionally, through the specification and reachability analysis process this thesisI explored the possibility that the Mobile Node could remain on this foreign network for any amount of time or move to a different foreign network or move back to its home network. Also the specification of the Home Agent and Foreign Agent was conducted to verify that all three could effectively communicate to make Mobile IP a viable protocol option for mobility. All three possibilities were explored and the protocol works correctly in all three cases. This analysis began with a Mobile Node in state zero and showed that as long as the agent advertisement that was received matched the Mobile Node's home network then no actions were required and the Mobile Node could be considered just another stationary node on the network. However, as soon as an agent advertisement was received that did not match the Mobile Node's home network then the Mobile IP protocols were activated. While performing the reachability analysis it was discovered that with no data loss the protocol works as advertised.

2. Protocol Analysis Items Not Accomplished

This specification and reachability analysis did not accomplish examining what happens in all cases of lost information. The only two messages that were analyzed if they were lost were the mobile node sending a solicitation or a registration request. If additional losses are introduced in the system a much more in depth analysis would be required to be conducted to determine how each entity would handle various types of data losses. This is especially imperative in the case of implementing Mobile IP over any type of wireless media, as the error rates are much larger than with Ethernet. This would involve adding additional time out (TO) states to the entities and would then require a software analysis of the protocol.

This analysis did not look at Mobile IP version VI at all, it was dedicated only to Mobile IP version IV. This was done since the Mobile IP version VI standard is still in a state of flux. Also, not examined is the case of a Mobile Node registering directly with a Home Agent, vice using the Foreign Agent as an intermediary. This was not explored because it has not been decided yet if the final version of the protocol will allow both types of registration processes. For reasons of simplicity and the direction that the Mobile IP working group appears to be heading, the former was ignored.

3. Protocol Analysis Results

The results of this analysis are that the Mobile IP protocol is sound, but there are some strengths and weaknesses that are worth pointing out explicitly.

a. Mobile IP Protocol Weaknesses

The major weakness of the Mobile IP protocol is the number of messages that are required to be sent from one entity to another. In the case of a large mobile network where the home network is extremely far away from the current foreign network there may be significant message delays. For example if the Mobile Node's home network is in California and the Mobile Node is currently on a foreign network in Europe, there will be significant packet delays especially during the registration process where the Mobile Node has to send a registration request to the Foreign Agent and then the Foreign Agent must relay this request to the Home Agent. The Home Agent then sends a registration request reply to the Foreign Agent who then finally notifies the Mobile Node of the decision either to approve the request or deny it. In this scenario there are significant delays involved without any packet losses introduced. If there are lost packets and retransmissions required then the delays will be even more substantial and the possibility exists that the Mobile Node's connections may be terminated due to nonresponse, therefore defeating the purpose of Mobile IP to maintain connections while transiting between networks.

Another weakness of the protocol is that if a registration request to a Foreign Agent is repeatedly denied the Mobile Node can get stuck in state 3, because it cannot move to state 4 until a registration request reply is received. In order to rectify this situation the implementers of Mobile IP would need to ensure that there is some way of avoiding this situation if the Mobile Node is authenticated and is simply having transmission or reception errors. On the positive side, this may act as a security feature that does not allow a Mobile Node intruder to ever get past the registration process.

Another weakness of the protocol is the requirement for the Mobile Node to deregister with the Foreign Agent prior to notifying the Home Agent that it is in the process of doing this. This could cause the Home Agent to forward packets to the Foreign Agent for delivery to the Mobile Node, but the Mobile Node has already deregistered and these packets may be discarded by the Foreign Agent. There are two ways to solve this, either the Mobile Node sends a message to the Home Agent not to forward any more packets as it is in the process of deregistering and returning home or by simply requiring that foreign agents return packets to the Home Agent that sent them if they are undeliverable to a particular Mobile Node. This would be the preferable option if I were implementing this protocol. This would allow not only for the case of the registration delay issue but also the case of a Mobile Node that is quickly moving from one network to another. There may be delays in receiving the packets, but at least they will not be discarded and will eventually arrive.

Another weakness of the protocol is in the overhead required for the Home Agent and Foreign Agent to keep track of which packets have been forwarded to the Mobile Node, which have been received by the Mobile Node, and which have been acknowledged for by the Mobile Node.

b. Mobile IP Protocol Strengths

The major strength of the Mobile IP protocol is the very precise message formats that are exchanged between the entities. These message formats allow all three entities to know the status of each request and each response allowing for smoother transitions between networks even in the presence of unreliable wireless links. The key messages are periodically broadcast and if the Mobile Node does not receive one when it expects to it can send a request for the Home Agent or Foreign Agent to broadcast the expected message. Another strength of the protocol is that the Foreign Agent and Home Agent specifications are nearly identical. The only difference between the two is that the Foreign Agent has a mechanism for forwarding a registration request to a Home Agent and then sending the registration request reply to the Mobile Node. The fact these two entities are nearly identical makes the implementation of the protocol easier and allows the router acting as a Home Agent to be easily modified to act as a Foreign Agent or vice versa. This is important from the perspective of redundancy, as a Foreign Agent can act as a Home Agent of required or likewise, a Home Agent can act as a Foreign Agent. This is also important as the migration from Mobile IP version IV to Mobile IP version VI takes place and Foreign Agents are no longer required, as discussed in Chapter IV. Any investment that was made in additional routers can be preserved since these routers are easily modifiable to now perform the functions of additional Home Agents.

Although this thesis has pointed out several weaknesses of the protocol, the effects of these weaknesses can be minimized if the designers that are implementing the protocol take these weaknesses into account and provide a viable Mobile IP protocol implementation. The strengths of the protocol outweigh the weaknesses and make this an excellent choice for any network consisting of a large population of users who travel significantly.

VI. APPLICATIONS OF MOBILE IP TO THE US NAVY

A. NAVAL APPLICATIONS FOR MOBILE IP

1. Mobile Ship Networks

The first application that the Navy could adopt is for Mobile IP aboard all Navy ships. Mobile IP can provide connectivity not only for single mobile nodes, but also for entire mobile networks. A mobile network is a network whose hosts and routers are usually non-mobile with respect to each other, but are collectively mobile with respect to the rest of the fixed Internet. A mobile network such as this could be located on every ship in the Navy (Solomon, 1998). This is accomplished by placing at least one mobile router onboard each ship that we want to provide mobile functionality. This mobile router will maintain connectivity for all the nodes on the ship's network. The nodes within the ship are fixed with respect to the fixed portion of the Internet. The mobile router communicates wirelessly, most likely via satellite, with the foreign agents at the Navy's network operations centers, depending on the ship's current location. The way this works is that the mobile router has a home address just like any mobile node, but the network prefix of the mobile router's home address equals the network prefix assigned to its home link. When connected to its home link, the mobile router and the home agent are simply neighboring routers which exchange routing updates according to their routing protocol. When the mobile router is connected to a foreign link, the routing is accomplished through a tunnel to the foreign router.

2. Mobile Squadrons

The second application is an application of Mobile IP that will allow squadrons and other entities that routinely embark different ships of the Navy a smoother transition. In this case the nodes and routers on the mobile network are mobile with respect to the ship's mobile network. For example, a squadron member brings a mobile configured laptop computer onto any ship configured with Mobile IP. This mobile node is mobile with respect to ship's nodes and routers while the entire ship moves with respect to the rest of the Internet. The following assumptions apply to this scenario:

- The mobile node has a home agent somewhere on the fixed portion of the Internet
- The mobile router has a home agent somewhere else on the fixed portion of the Internet
- The mobile router provides foreign agent functionality on behalf of the mobile nodes that are connected to the mobile network link
- The mobile node and the mobile router have respectively discovered and registered foreign agent care-of-addresses with their home agents

These are just two possibilities for implementing Mobile IP within the Navy; there are a multitude of others that are possible. Next, I will briefly describe a possible plan for exploring the use of Mobile IP within the Navy.

B. NAVAL TEST PLAN FOR ADOPTING MOBILE IP

In order to thoroughly examine the implications of Mobile IP for the Navy, I have developed a three phase test plan which I will describe below.

1. Phase 1 : Lab Research

This phase would consist of research performed at the Space and Naval Warfare Systems Center (SPAWAR), the Naval Postgraduate School (NPS) and possibly the Naval Research Lab (NRL). These three entities are the leaders for the Navy in system design and testing and are therefore the best choices for the initial research. This phase would consist of implementing various commercial applications of Mobile IP at all three sites and thoroughly testing these implementations to ensure they could be successfully implemented Navy wide. Additionally, the security aspects of Mobile IP would be explored during this phase.

2. Phase 2 : Testing aboard USS Coronado and Navy Network Operations Center (NOC)

This phase would consist of extending the communications between the Mobile networks that were tested at SPAWAR, NPS and NRL to two additional Mobile networks, one onboard the USS Coronado and a second at one of the Navy's NOCs. This will allow us to determine what problems exist in "real scenarios" during the annual Joint Warrior Interoperability Demonstration (JWID) which is designed to test new technological solutions in typical Naval exercises.

3. Phase 3 : Implementation

Upon successful completion of phases one and two, implementation can begin. This phase will depend upon available funding at the time that the US Navy decides to go ahead with this promising new technology.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CONCLUSION

A. MOBILE IP CONCLUSIONS

Even though the specifications for Mobile IP have not been completed there are several commercial implementations of Mobile IP already available. The following URLs provide links to these implementations:

- http://www.monarch.cs.cmu.edu
- http://www.cs.pdx.edu/research/SMN
- http://mip.ee.nus.sg
- http://www.mcl.cs.columbia.edu/source.html
- ftp://ftp.it.kth.se/pub/klemets
- http://anchor.cs.binghamton.ed/~mobileip
- http://mosquitonet.stanford.edu/software/mip.html

If Mobile IP continues to gain support in the commercial world, eventually all routers will be capable of serving as home agents, foreign agents, or both and all mobile devices including laptop computers, handheld computers and whatever new mobile devices come along, will be preloaded with the appropriate Mobile IP enabling software. Once this happens, Internet Service Providers (ISPs) will be forced to support this technology in order to meet consumer demand. This may be done via Point to Point Protocol (PPP) connections over telephone lines or through some form of wireless access, in either case there are many new hurdles that will have to be overcome to accomplish this. For example, the current model of contracting for service with an ISP could make it difficult to implement Mobile IP. A more desirable solution is one in which a user pays digital cash to a service provider for access to the Internet. In this case, a user may not need to establish a relationship with a service provider in advance. A user simply plugs in to a link and pays for services used on a real time basis. This could open up the possibilities of the locations and media over which Internet service can be provided.

We have seen that Mobile IP answers many questions about how to implement network mobility, but raises many questions about how to best implement this protocol as well.

Mobile IP is unique in that it allows a mobile node to connect anywhere without requiring applications or any other state of the machine to be modified. Mobile IP will continue to evolve and adapt to emerging technologies.

B. FUTURE RESEARCH AREAS

There are many areas of Mobile IP that require additional research. I have listed some of these below:

- Protocol Analysis for more than one Mobile Node, Home Agent, and Foreign Agent
- Mobile IP network simulation
- Mobile IP network modeling
- Mobile IP network performance analysis
- Mobile IP network security issues
- Mobile IP implementation strategy

Each one of these areas could have an entire thesis devoted to it and is worthy of future research in this burgeoning area of mobility.

LIST OF REFERENCES

Brodsky, I., “No longer Achilles’ heel,” Cellular Business, July, 1997.

Cheshire, S. and Baker, M., “Internet Mobility 4x4,” Proceedings of the ACM SIGCOMM ’96 Conference, August 1996.

Deering, S. and Hinden, R., “Internet Protocol, Version 6 (IPv6) Specification,” IETF RFC 1883, December, 1995.

Hamalainen, J. and Jokiaho, T., “GSM access to Internet,” Telecommunications (International Edition), March, 1994.

Lancki, B., Dixit, A., and Gupta, V., “Mobile-IP: Supporting Transparent Host Migration on the Internet,” Linux Journal, August, 1996.

Perkins, Charles E., *Mobile IP: Design Principles and Practices*, Addison Wesley Longman, 1998.

Perkins, Charles E., “IP Mobility Support,” IETF RFC 2002, October, 1996.

Perkins, Charles E, “Minimal Encapsulation within IP,” Work in Progress, October, 1995.

Solomon, James D., *Mobile IP: The Internet Unplugged*, Prentice Hall, Inc., 1998.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Road, Ste 0944
   Fort Belvoir, VA 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Road
   Monterey, California 93943-5101

3. Chairman, Code CS 1
   Computer Science Department
   Naval Postgraduate School
   Monterey, CA 93943

4. Professor G. M. Lundy, Code CS/LN 1
   Computer Science Department
   Naval Postgraduate School
   Monterey, CA 93943

5. Professor W. Baer, Code CS/BA 1
   Computer Science Department
   Naval Postgraduate School
   Monterey, CA 93943

6. LCDR Lawrence J. Brachfeld 3
   10262 Veracruz Court
   San Diego, CA. 92124

7. Mr. and Mrs. James Brachfeld. 1
   20 Dell Street
   Sleepy Hollow, NY 10591