NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

SECURE WIRELESS HANDOFF

by

Romelo B. Nafarrete
Lionel J. Valverde

June 2003

Thesis Advisor: George Dinolt
Co-Advisor: Gurminder Singh

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

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** June 2003	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Secure Wireless Handoff			**5. FUNDING NUMBERS**
6. AUTHOR(S) Joel Valverde and Romelo B. Nafarrete			
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)***

With the rapidly growing demand for portable devices such as laptops, handheld computers and Personal Digital Assistants (PDAs) with wireless networking capabilities, the need for reliable wireless data network communication has also increased. Just like in mobile voice communication, users demand uninterrupted, secure wireless data communication as they move from place to place. Mobile IP satisfies some of these demands - it enables mobile devices with fixed IP addresses to be permanently reachable even as their point of attachment to the network changes. This allows for routing of data packets to and from the mobile device irrespective of its location on the network. While uninterrupted data flow can be achieved with Mobile IP, it introduces additional security vulnerabilities, including data privacy, data integrity and authentication. The goal of this thesis is to investigate such vulnerabilities and explore implementations to overcome them.

14. SUBJECT TERMS Mobile IP, Mobile Node, Foreign Agent, Home Agent, Internet Protocol, IPSec, WEP			**15. NUMBER OF PAGES** 98
			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

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

SECURE WIRELESS HANDOFF

Romelo B. Nafarrete
Civilian, Scholarship For Service, National Science Foundation
B.S., University of California, San Diego, 2001
M.S., Naval Postgraduate School, 2003

Lionel J. Valverde
Civilian, Scholarship For Service, National Science Foundation
B.S., California State University, Monterey Bay, 2001
M.S., Naval Postgraduate School, 2003

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
June 2003

Authors: Romelo B. Nafarrete
Lionel J. Valverde

Approved by: Dr. George W. Dinolt
Thesis Advisor

Dr. Gurminder Singh
Co-Advisor

Dr. Peter J. Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

With the rapidly growing demand for portable devices such as laptops, handheld computers and Personal Digital Assistants (PDAs) with wireless networking capabilities, the need for reliable wireless data network communication has also increased. Just like in mobile voice communication, users demand uninterrupted, secure wireless data communication as they move from place to place. Mobile IP satisfies some of these demands - it enables mobile devices with fixed IP addresses to be permanently reachable even as their point of attachment to the network changes. This allows for routing of data packets to and from the mobile device irrespective of its location on the network. While uninterrupted data flow can be achieved with Mobile IP, it introduces additional security vulnerabilities, including data privacy, data integrity and authentication. The goal of this thesis is to investigate such vulnerabilities and explore implementations to overcome them.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The authors would like to thank many people who contributed to the completion of this thesis and to the great learning experience the authors had in this concept of Mobile IP. Mobile IP has and is proving to be the accepted form of computing for the future. Both Government and Industry have shown interest and are making progress in this area. We are grateful to have gone through this learning experience.

We would first like to thank the National Science Foundation for giving us the opportunity to expand our knowledge in the area of Computer Security. We have learned a great deal about Computer Security and we are anxious apply what we have learned in our future endeavors.

We would like to thank our advisor Professor George Dinolt and co-advisor Professor Gurminder Singh for asking the tough questions, which provoked us to seek and to dig deep into Mobile IP and as a result learned a great deal about doing research in general and Mobile IP. We would like to thank Professor Dinolt for his understanding and getting his hands dirty with us as we fought to get Mobile IP up and running. We would like to thank Professor Singh for the interest he showed and consistently approaching us and checking our progress.

We would also like to thank a couple of people we never met personally but who helped us through email dialogue on solving our initial problem, which consumed much of our time at the beginning of this project. The first of these is Marc Danzeisen from Switzerland. The authors are grateful the ongoing dialogue via email which lasted approximately three weeks and in which the authors learned a great deal about secure Mobile IP. He was generous enough to let us see the scripts he wrote when he secure Mobile IP. Marc is currently a leader in the Mobile IP arena in Switzerland. He is currently working for a company that has developed a proprietary Mobile IP implementation for Windows. The next person is Bryan Hartwell who was one of the

few people who still used the Dynamics e-mail list. We would like to thank him for his suggestions, which helped us in resolving some issues we had with Dynamics.

Lastly to Albert Einstein, man of the 21st century, for his insight, which has helped us and many others. "If we knew what it was we were doing, it would not be called research, would it?"

--Albert Einstein

I. INTRODUCTION

The rapid growth of new and competing radio technology has allowed designers to create devices with a very small form factor but significantly enhanced functionality. This small form factor and added functionality has increased mobility, which, in turn, has increased the popularity of devices such as PDAs, handheld computers and laptops. With wireless functionality built into these devices, people are now able to access information easily. The popularity of wireless technology has rapidly increased as new "hotspots" have popped up across the nation. These "hotspots" include places such as airports, coffee shops, school campuses and public libraries. As more of these places are established, the concern for security grows larger because information is transmitted over the air on radio waves, anyone with radio equipment can intercept sensitive information and masquerade their location [BOR1].

Security risks of wireless include insertion attacks, interception and monitoring of wireless traffic, misconfiguration, jamming, and client-to-client attacks. Other attacks include broad network exposure, invisible intruders, guest access, and rapid technology evolution [SIG]. These risks are being handled using such technologies such as Wired Equivalent Privacy (WEP), dynamic WEP, firewalls and encrypted tunnels (VPN, IPSec, etc), and wireless LAN managers such as REEFEDGE [SIG].

Wireless mobility is very useful for people who want to stay connected to the Internet or a network all the time. Wireless mobility is nothing new, but new technology has it made more convenient and lowered the cost, which, in turn has made wireless mobility more desirable. In our fast paced world, mobility allows a convenient way for people who are always on the move to stay connected and efficiently get more work done. With the addition of Mobile IP, the hassles of staying connected will be lessened. It will provide the "mobility" of the cell phone to Mobile IP networks.

This thesis uses IP networking and network protocols. We assume the reader is knowledgeable of specifics such as the format of IP data packets (i.e. the number of bits in a packet, the size of the header, etc.), networking basics (OSI stack), and basic network security issues (eavesdropping, replay attacks, etc.)

A. PURPOSE

Our overall goal is to research and implement Mobile IP securely using IPSec. One of the goals of Mobile IP is to traverse access points with out losing connectivity. Ultimately Mobile IP will allow one to download a 10 MB file or perform a business transaction while driving down the highway. Security concerns arise when business and personal information is transmitted in the clear over the air.

IPSec, the Internet Security protocol, is a suite of protocols that provides integrity, confidentiality, protection against replay attacks, etc. Our research focuses on security within Mobile IP. This thesis will explain Mobile IP, its need in the wireless arena, and how security can be implemented. We examine Mobile IP in IPv4 and the security issues involved with Mobile IP. We investigate the benefits of using Mobile IP since as a society we are becoming more mobile the way we do business and pleasure. Telecommuting has increases significantly compared to a decade ago and the use of cellular telephones has grown exponentially.

Our research focuses on security enhancements for Mobile IP. More specifically, we look at IPSec and how to implement it within a Mobile IP implementation. After examining IPSec within Mobile IP, we discuss the problems and issues that are involved with it.

We also examine how to provide a secure channel, and the different integrity issues involved. With each handoff, there is going to be a configuration change between the different agents and the mobile node.

B. THESIS OUTLINE

This thesis is divided into 6 chapters. Chapter I introduces the different concepts and technologies involved with Mobile IP. Chapter II covers the discussion on Mobile IP and goes into the details of Mobile IP in general. Chapter III goes into more detail and we discuss the specific implementation of Mobile IP that we used for this thesis. Chapter IV covers security associated with wireless and a solution to the weak security provided

by Mobile IP. Chapter IV discusses the problems we had with implementing Mobile IP. We feel this section will be very helpful to the interested reader implementing Mobile IP.

C. BACKGROUND

Among the rapidly growing current technologies mobile telephony and wireless data networking are near, if not at, the top. Just like with mobile telephones, people want their data devices to remain connected as they roam from place to place. Currently limited roaming is available with IP based networks. However, there is a lot of current research and work going into combining cellular technology with Mobile IP. These two technologies are very similar in functionality and therefore we feel it is important to discuss them in this thesis.

1. Mobile Telephony

Mobile IP works similarly to cellular technology. In this section we will discuss briefly how cellular technology works and then compare it to Mobile IP. Figure 1 is a very simplified diagram of the components in cellular telephone systems. [ALE].

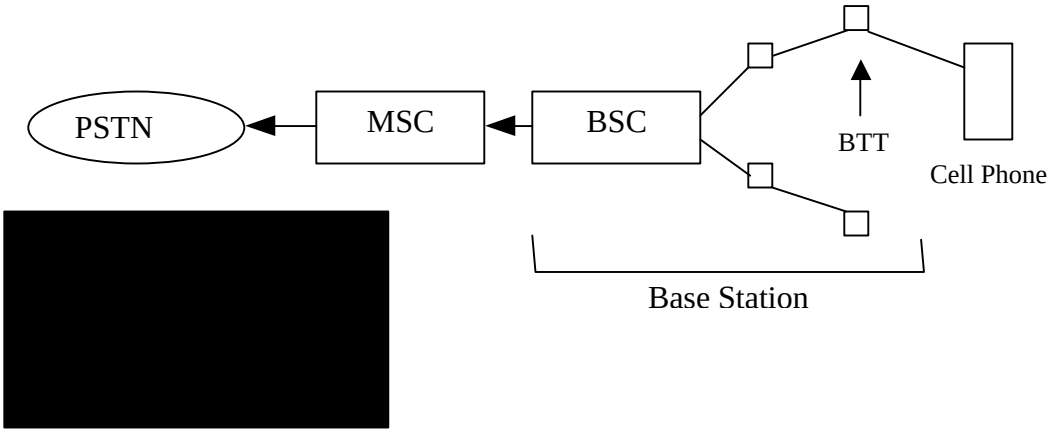

Figure 1. Base Stations and Cell Sites

For TDMA and CDMA systems, the phone maintains a cell site location. When a user dials a number from his/her cell phone and pushes the send button, the phone first requests authorization to make a call. Next, the base station checks the phone's

mechanical serial number (MSN) and electronic serial number (ESN) [ALE]. The ESN is a unique identification number built into a cell phone for security and billing purposes. The MSN is the actual hardware number. It is used most in cases where the phone gets lost or stolen.

After authorizing the call, the base station sends a channel assignment message to the phone where the phone is issued a channel to talk. If the phone is analog, the voice signal is sent as a modulated radio wavelength [ALE]. Else if the phone is digital, the voice is sent as a binary digital language in ones and zeros. Next, the base station connects a landline call to the mobile switching center (MSC) through Public Switch Telephone Network (PSTN), the local phone network; to the number dialed, and then conversation can begin.

The PSTN enables the members of the general public to communicate with each other. The MSC is the interface between the radio (i.e., radio waves) system and the public switched network. The MSC performs all signaling functions that are necessary to establish calls to and from mobile stations [YHL]. The PSTN is the nationwide telephone switching system operated by various telephone companies [YGL].

In a call from one cell phone to another, the mobile switching center tries to find the caller. However, previous to this the cell phone transmits a registration request to the MSC. If the system identification code programmed on the caller's phone matches with that of the MSC then the caller's phone knows it is at home. The MSC knows which cell the phone is in when it wants ring the phone [STF]. Within GSM, the BSC is responsible for the radio resource (RR), which is a protocol that controls the resources over an air interface, frequency administration and handover between BTTs controlled by the BSC. One of the goals of a cellular system is for the user to remain connected even as he/she moves through the system from one BTT to the next and from one MSC to the next.

In cellular technology Code Division Multiple Access (CDMA) does soft handoff. CDMA refers to the IS-95 standard, which is a transmission protocol that employs CDMA, which is just a means to transmit bits of information. In CDMA when a phone switches cell sites a soft handoff occurs. In a soft handoff situation the cell sites share the same frequency. When a cell is at the edge of its cell site the phone only needs

to change the pseudo-random sequence it uses to decode the desired data from the all the bits sent for everyone else. While a call is in progress the network chooses two or more alternate sites that it feels are handoff candidates. It broadcasts a copy of the call on each of these sites simultaneously. The caller's phone then chooses between the different sources for the call, and moves between them whenever it feels like it. It can even combine the data received from two or more different sites to ease the transition from one to the other [ARX]. In most other technologies hard handoff occurs when the network informs a user's phone of the new channel to switch to which it must switch. The phone then stops receiving and transmitting on the old channel, and continue transmitting and receiving on the new channel. [ARX]

Lastly, when the call is received the digital data, or radio waves, are converted back into voice [ALE]. In this thesis we will show the similarities and differences between Mobile IP and cellular technology and how they relate to one another. Table 1 shows a comparison of Mobile IP and mobile telephony.

THIS PAGE INTENTIONALLY LEFT BLANK

II. MOBILE IP

A. ARCHITECTURE OF MOBILE IP

The Request For Comment (RFC) 2002 by Charles Perkins [PER2] introduces and defines the concept of Mobile IP. A Mobile IP network involves several different components. The basic components of Mobile IP consist of a mobile node (MN), home network (HN), home agent (HA), foreign network (FN), foreign agent (FA), and correspondent node (CN). Figure 2 shows the various Mobile IP components, including examples of each the hosts' network numbers, or network prefixes, which is the network number field and leading portion of a 32-bit IP address, identifying the network number (Figure 3) [3CO].

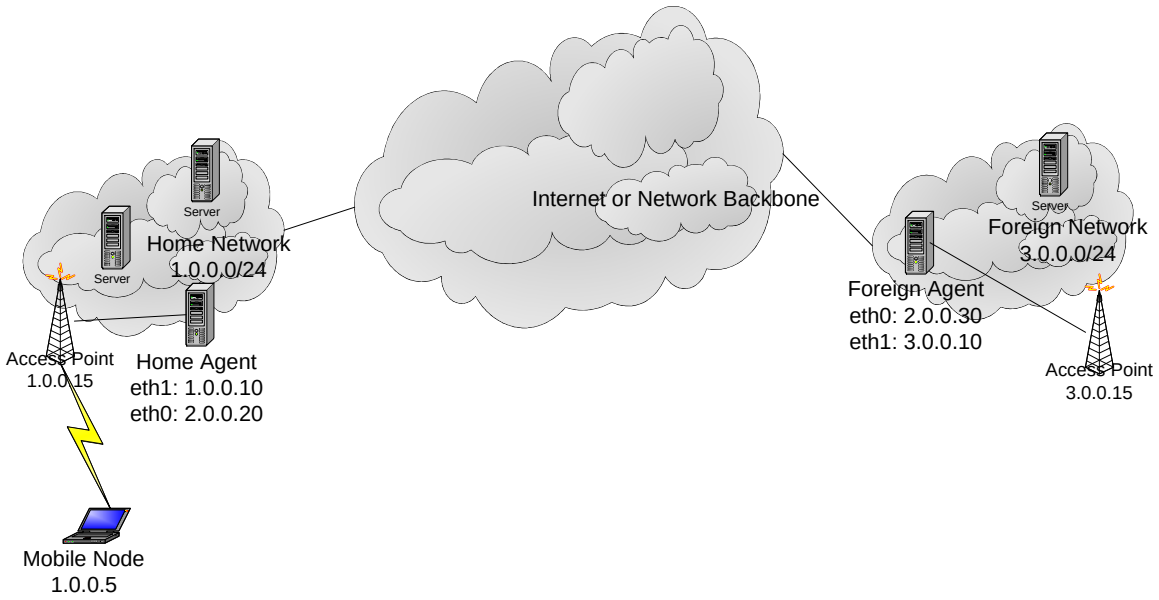

Figure 2. Mobile IP Components

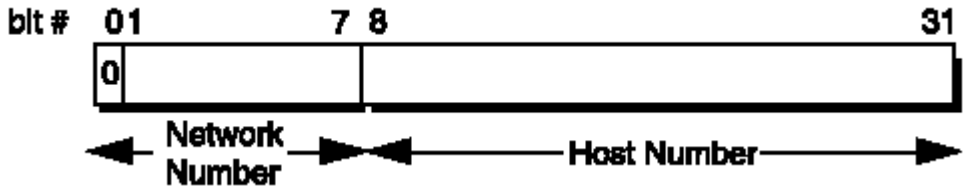

Figure 3. IP Address Format [3CO]

For a more detailed description on IP addressing please refer to [3CO]. Figure 2 also shows examples of possible interfaces with IP addresses belonging to an agent (i.e. eth0 and eth1) and examples of Access Points (AP) and their IP addresses that the MN creates the wireless connection to. The following is a detailed description of each component:

- Mobile Node (MN): This can be any mobile device such as a laptop with wireless connectivity, wireless PDA, wireless handheld computers, etc. with wireless connectivity
- Home Network (HN): A MN will have a fixed (constant) IP address (name) that is registered on this network. The network prefix of this network is the network prefix of the MN.
- Foreign Network (FN): Any network other than the HN, which has a different network prefix from the MN
- Home Agent (HA): Essentially a router that has at least one interface whose network prefix is the same as the MN's home network. This is the original point of attachment that the MN is registered to. Point of attachment refers to the current agent (HA or FA) that the MN is connected to.
- Foreign Agent (FA): Essentially a router that is a potential point of attachment, which has at least one interface whose network prefix is different from the MN's network prefix
- Access Points (AP); A station that transmits and receives data wirelessly. The physical interface, which MNs wirelessly connect to.

A node's IP address is the unique identifier for its point of attachment to the Internet. Before Mobile IP there were two ways in which a MN could change its point of attachment without losing its ability to communicate. One involves changing the node's IP address whenever its point of attachment changed and the other involves propagating host-specific routes throughout the Internet routing arrangement [PER2]. If all gateways had to update their routing tables every time a mobile host changed its point of attachment, the size of the routing tables would become enormous.

Figure 4 is an example of the different states that a Mobile IP Network may encounter. This diagram is to be used as a reference for the tables that follow. When the MN moves from one network to the other (i.e. from HN to FN1), the host-specific route table for each host (FA, Server, and HA), must all get updated by first deleting a route and then adding the new route to the table. The following tables show how a host-specific route table will change as the MN moves into the different networks.

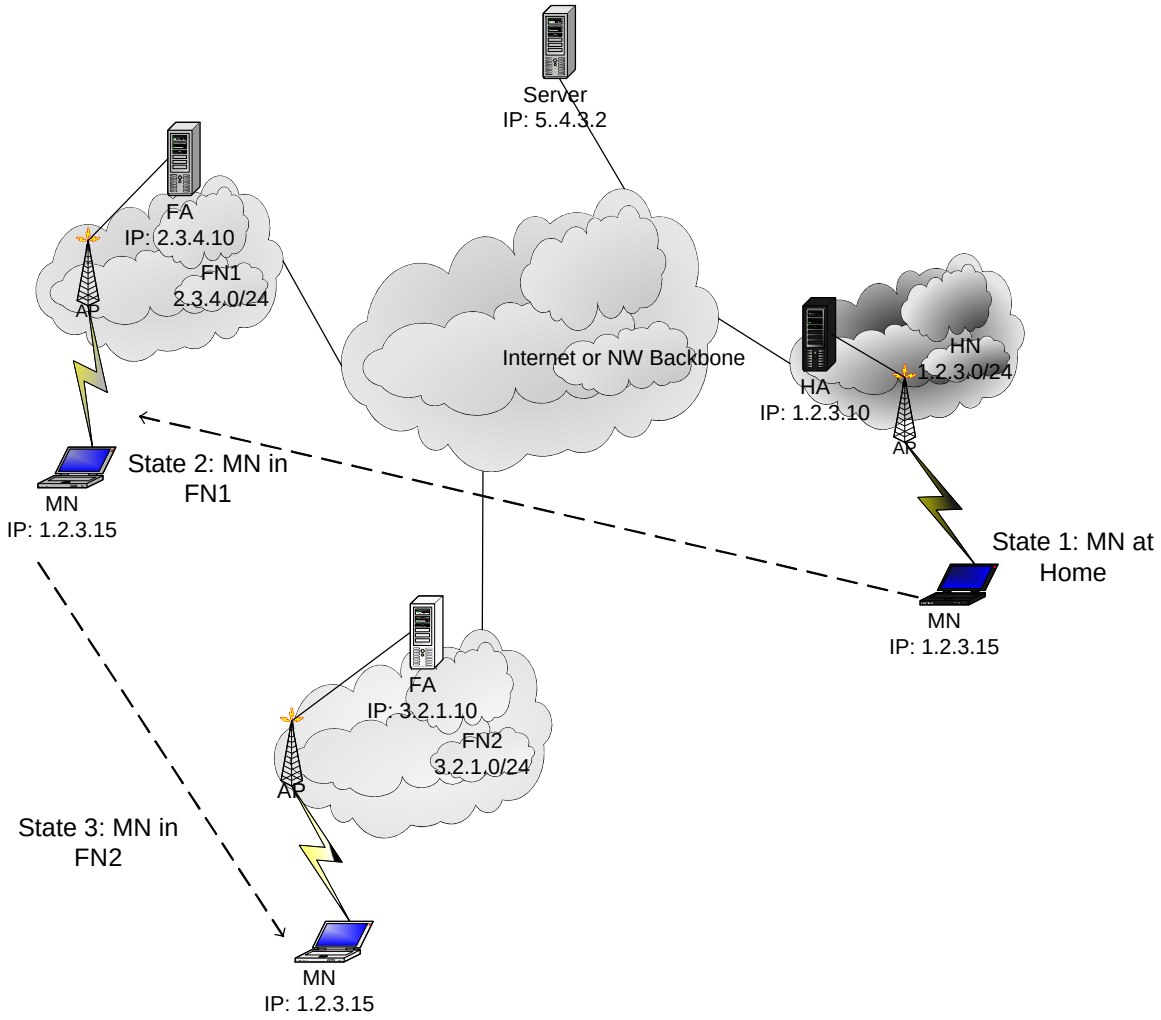

Figure 4. MN in Different States within a Mobile IP Network

Destination Host	Route To
1.2.3.0	1.2.3.10

Table 1. Host-Specific Route Table, MN in State 1 (see Figure 4)

When the MN is in the HN, the host-specific route tables of each of the components (FA or Server) contain the entry seen in Table 2. The *Destination Host* column contains the network prefix of the network that data will be sent to. The *Route To* column contains the gateway through which the data packets will be sent. Once the gateway receives packets, it forwards them to the ultimate destination. However, when the MN moves to another network, the tables will change. The following tables show this change.

Destination Host	Route To
2.3.4.0	2.3.4.10

Table 2. Host-Specific Route Table, MN in State 2 (see Figure 4)

Table 3 shows the updated table of the components. When the MN moves into State 2, the previous entries of the host-specific route tables are deleted and replaced with the updated information.

Destination Host	Route To
3.2.1.0	3.2.1.10

Table 3. Host-Specific Route Table, MN in State 3 (see Figure 4)

In Table 4, the MN has moved into State 3, where the network prefix is 3.2.1.0. Once again, the previous entries in the table are deleted and replaced with the new information.

There are several problems associated with these mechanisms. The first mechanism, changing the IP address of a MN whenever the point of attachment changes, makes it impossible for a node to maintain its current session level connections. This approach makes the end user reestablish a new connection, losing the information that was originally being sought after.

The second mechanism has scaling problems [PER2]. As described in [SKE], by next year users will prefer to access the Internet on the go with a wireless Internet device rather than sit down in front of a PC. Shipments of wireless Internet devices should reach

double and triple digit growth through 2004. As more and more wireless devices are activated on the web, the second mechanism will pose a big problem for handling all the mobile devices.

Mobile IP addresses these problems by enabling the MN to keep its IP address throughout its connected session. As a MN moves from one subnet to another, the IP address is kept the same. This is done through a link-layer handoff during the move. When a MN moves from its home network to a foreign network, it must go through several phases to seamlessly handoff. The different phases are characterized by agent discovery, a registration process and tunneling considerations.

1. Agent Discovery

Agent discovery is the process by which a mobile node determines which network it is currently connected to, whether at home or a foreign network. It also allows a mobile node to detect when it has moved from one network to another.

The primary method used for agent discovery is the ICMP Router Discovery method [PER2]. Both home agents and foreign agents use this method to periodically broadcast advertisement messages (Figure 5). These messages contain information about the addresses of mobility agents and supported services [MAL]. They also contain a lifetime value, which determines how long they are valid [PER2]. These messages are used by the MN to determine whether or not it has moved. Optionally, a MN may send an agent solicitation broadcast message to quickly find a foreign agent to form an association with.

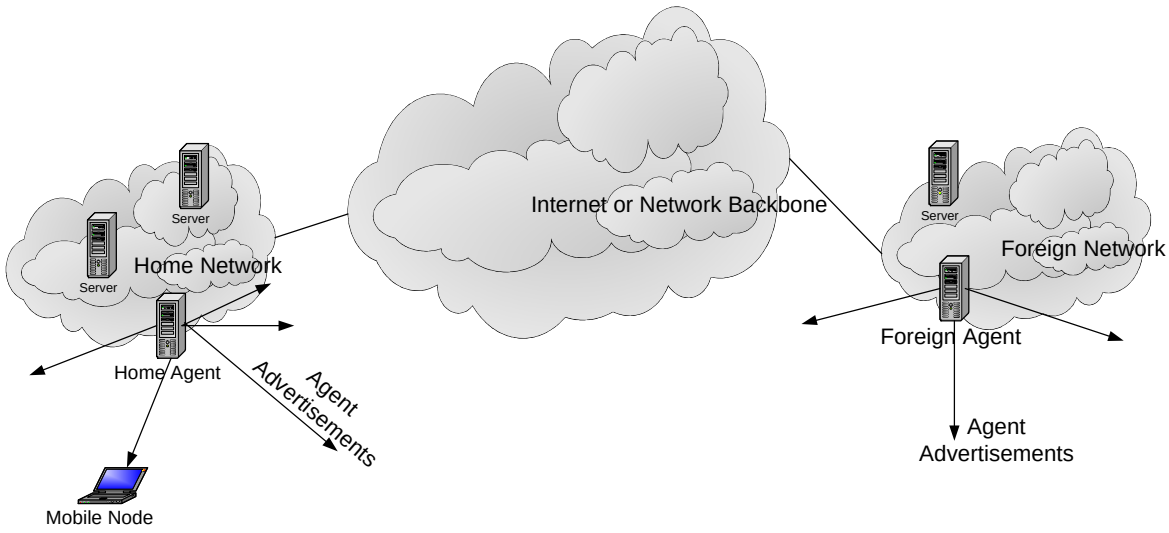

Figure 5. Agent Discovery (Agent Advertisements)

Each foreign agent sends three unsolicited advertisements during the lifetime of its advertisement messages (Figure 6). If a mobile node misses three consecutive advertisements, it can deduce that the last advertisement it previously received has probably expired [MAL]. Upon expiration, the mobile node assumes the foreign agent is unreachable and tries to find a different foreign agent.

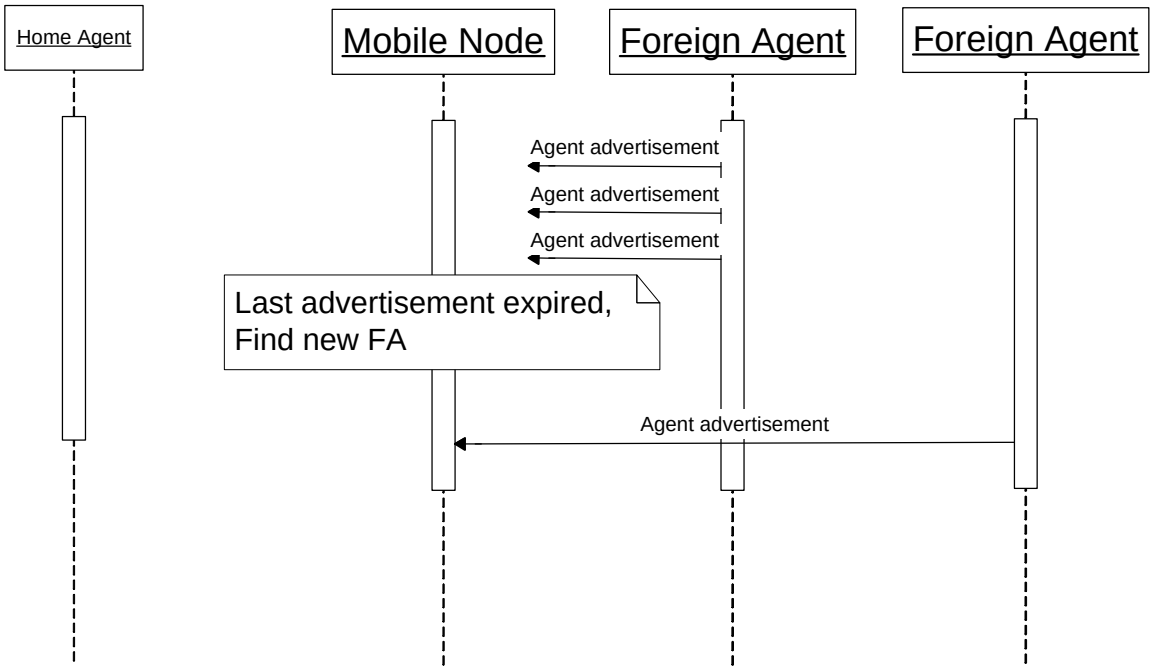

Figure 6. Expiration of Lifetime of Advertisements

A mobile node can also detect that it has moved to a new network using the network prefix of the advertisements. In Figure 7, the IP address of the HA is 1.2.3.10 with a network prefix of 1.2.3.0/24. The IP address of the MN is 1.2.3.5, which has the same network prefix as the HA. Once the MN moves to a FN, the agent advertisement that it receives has an IP address of 3.2.1.10, with a network prefix of 3.2.1.0/24. The network prefix of the FA is different from the MN's network prefix. A mobile node initially starts out accepting agent advertisements from its HA, which contain the home network's address prefix. After it moves, it will start receiving advertisements from other agents. Once a mobile node receives an agent advertisement from an agent with a new network address, it assumes that it is in a new subnet [MAL].

Once the MN detects that it is in a new network, it must obtain a collocated care-of address (CCOA) or a care-of address (COA).

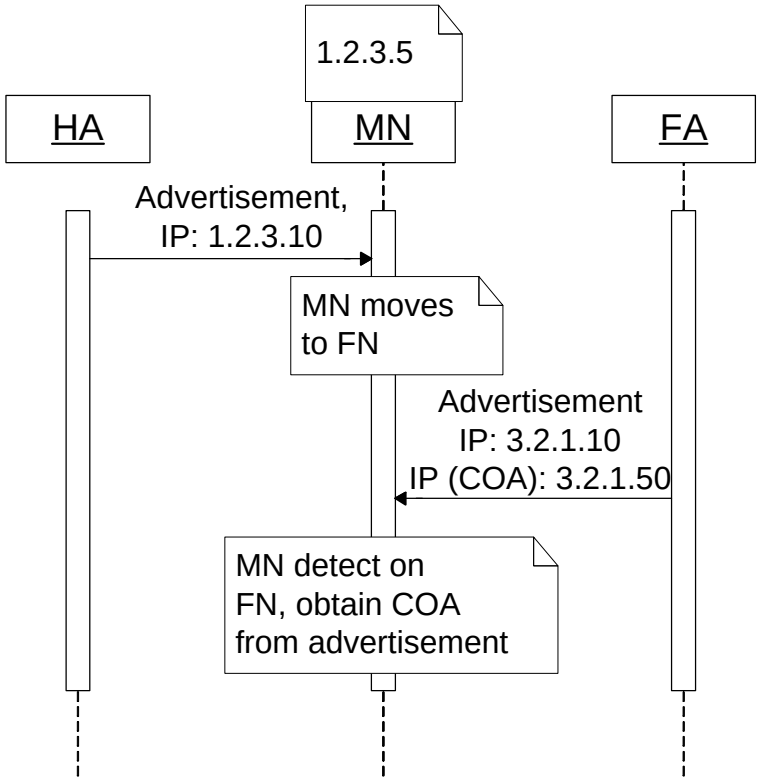

Figure 7. MN Detects New Network from Network Prefix

A CCOA is a temporary IP address that the MN obtains from the FN, through DHCP. This protocol has been discussed in detail in section C of this chapter. A COA is a temporary IP address contained in the FA agent advertisement that the MN uses to receive data packets; it usually represents an interface on the FA. Both care-of addresses are the exit point of the tunnel (this will be explained later in Routing/Tunneling). After the MN obtains the correct care-of address, the MN must then register with its HA.

2. Registration

Once a mobile node determines that it has entered a new network and obtains a care-of address, it registers its care-of address with its HA. This allows the MN to inform it's HA of its current point of attachment. There are two ways that the mobile node can register with its HA, depending on its method of attachment.

In the first method, the mobile node can register directly with its HA. Within this first method, there are two scenarios that can take place. The first scenario occurs when

the MN returns from a FN to its HN. In the sequence diagram below, the MN's original IP address is 1.2.3.5 (Figure 8). When it returns home, it receives agent advertisements from the HA that contain the IP address of 1.2.3.10. Once the MN detects that it's home, it then sends a registration request directly to the HA.

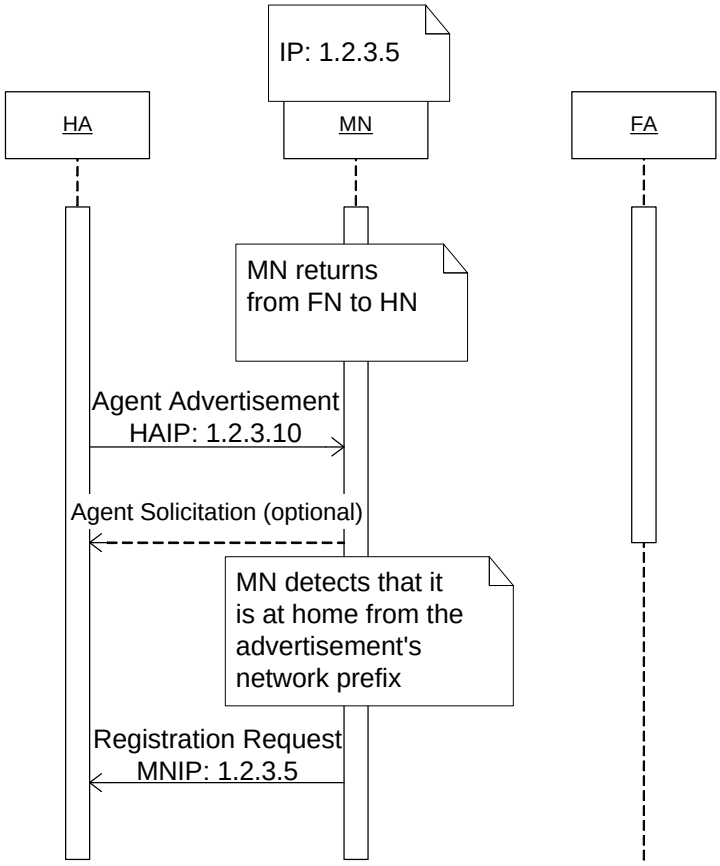

Figure 8. Registration (MN Returning to HN)

In the other scenario, the MN obtains a CCOA from the FN. It uses this IP address as the endpoint of the tunnel between it and the HA. In the sequence diagram below, after receiving agent advertisements from the FA, the MN detects, from the network prefix of the advertisement (i.e. IP of FA is 3.2.1.10) that it is in a foreign network (Figure 9). Once the detection is made, the MN obtains a CCOA (i.e. 3.2.1.25) through DHCP from the FA. It then registers its new CCOA directly with its HA, who replies to the CCOA.

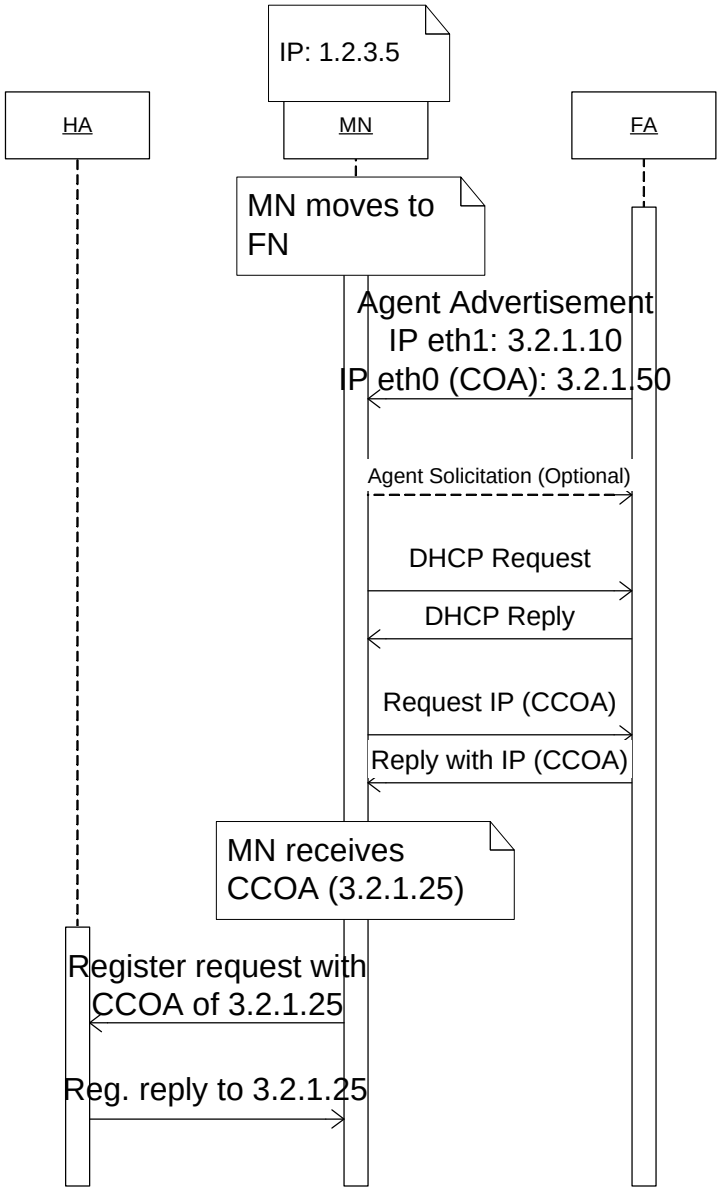

Figure 9. Registration (MN in FN with CCOA)

In the second method of registration, after the MN detects it is in a FN, it registers through a FA, which forwards the registration to the HA (Figure 10) [PER1]. Once the HA receives the registration request, it does a check on the authenticity of the request (this will be explained later in the section *Authentication in Registration*). After the request is authenticated, the HA sends a registration reply back to the MN at the COA. Whichever method is used to register, the home agent uses the same method to send a reply message. This reply message lets the mobile node know whether or not the registration was successful.

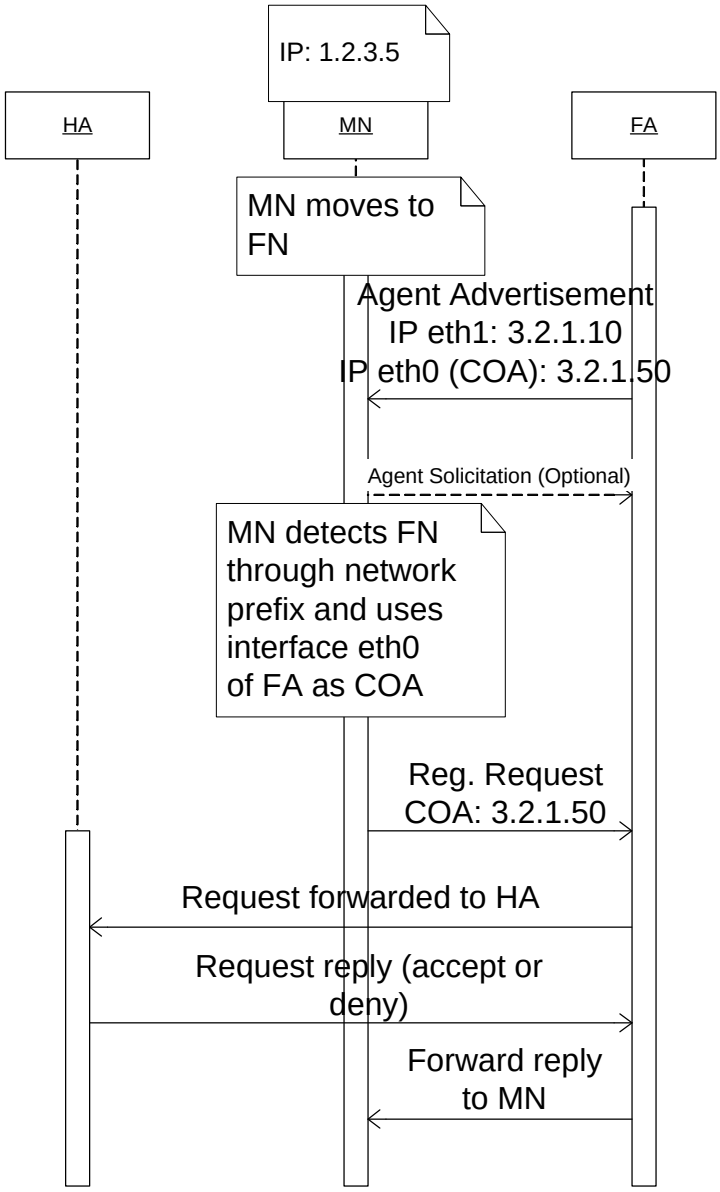

Figure 10. Registration

Registration changes or generates a mobility binding, which is the association of a home address with a care-of address, along with the remaining lifetime of that association at the HA [PER1]. There are important fields that are included in the registration request from the mobile node to create the mobility binding. This request contains a new care-of address for the mobile node, specific flags for the connection type and authentication data [MAL]. Whether the registration is done directly to the HA or through the foreign agent,

this mobility binding is maintained. Either way, the agent's data structures are updated and the home address of the mobile node is associated to its current care-of address and lifetime of the binding. If registration is performed through the foreign agent, the data packets are forwarded to the current point of attachment of the mobile node. Once the authentication to protect the data from unauthorized changes by the HA, the foreign agent can then update its bindings [MAL].

As previously mentioned, each mobility binding contains a lifetime. Once it expires, the binding gets removed automatically [MAL]. It is the responsibility of the mobile node to keep the mobility binding alive. Before the lifetime expires, the mobile node must reregister. If a mobile node does not receive a registration reply before the lifetime expires, it periodically sends a registration message until it receives a reply.

a. Authentication in Registration

The registration request packet contains registration extensions, which define the authentication measure (Figure 11) [PER1]. Each extension has a Security Parameter Index (SPI), which indicates the mobility security association. The mobility security association contains the secret (i.e. private/public key pair), an authentication algorithm (default is keyed MD5), and a style of replay protection (i.e. nonces or timestamps), which are all used in calculating the authenticator [PER1]. Keyed MD5 uses prefix+suffix mode, meaning it creates a secret that is placed before and after the data to be authenticated [PER1]. The authenticator is the parameter used to authenticate the MN to the HA in the registration process.

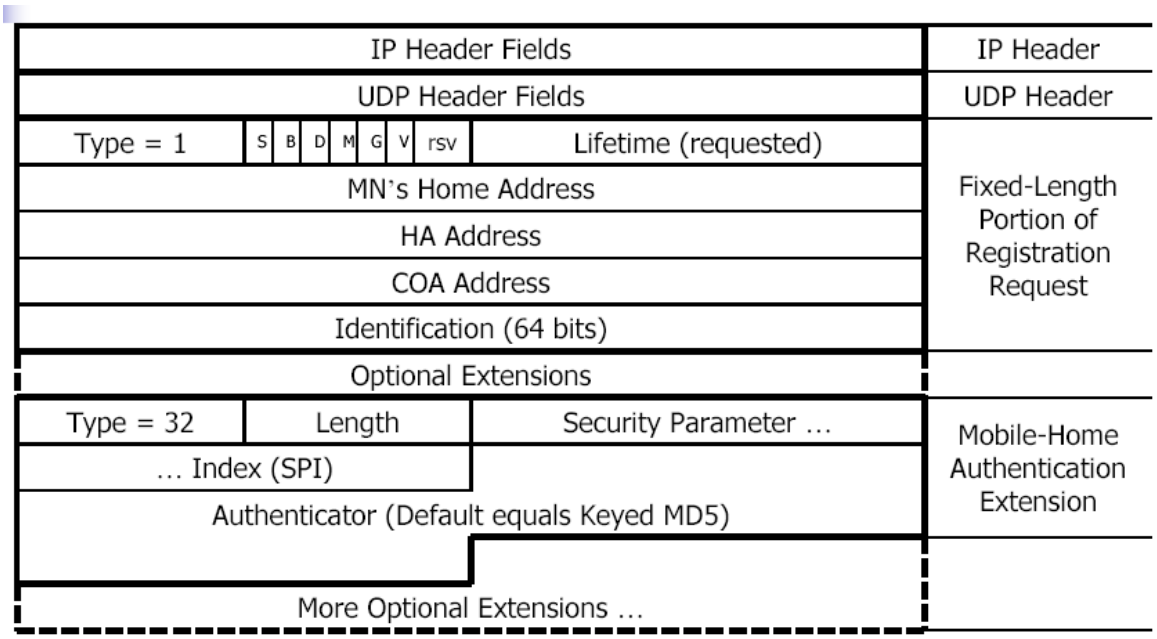

Figure 11. Registration Request Packet

3. Tunneling

Encapsulation or Tunneling is used in Mobile IP to deliver packets from a MN's home network to its current point of attachment, which is the COA or CCOA [PER1]. Tunneling enables all external nodes (HAs and FAs) to "see" the same IP address for the MN, no matter where its current point of attachment may be.

Tunneling involves the encapsulation and decapsulation of IP Packets by the node agents within the Mobile IP network. Tunneling utilizes IP-in-IP encapsulation to correctly route the original packet to its ultimate destination (Figure 12). The original packet is encapsulated within the payload of the outer packet. The header of the outer packet contains the IP addresses of the source (IP address of HA) and destination (COA). These IP addresses are considered to be the tunnel entry point and tunnel exit point, respectively. Encapsulation is performed by the sender and decapsulation is performed by the receiver. Depending on how the tunnel is set up, the decapsulator could either be the FA or the MN.

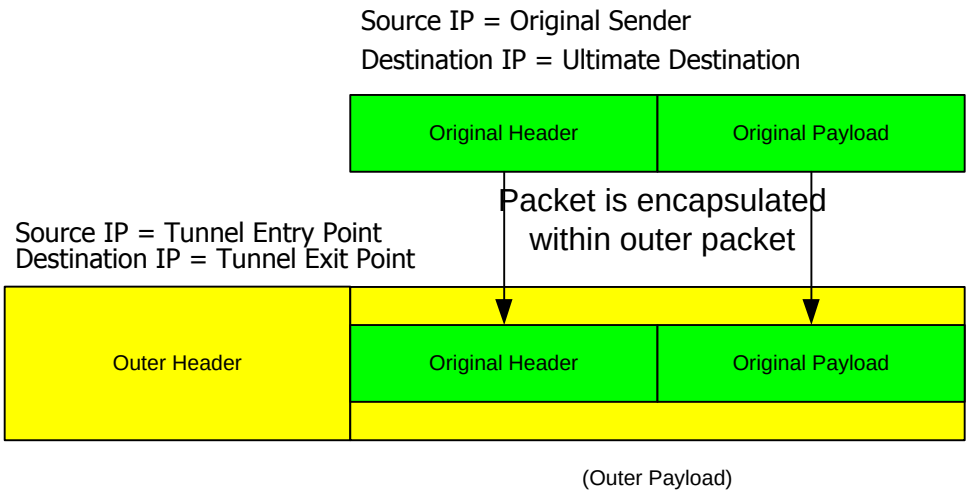

Figure 12. IP-in-IP Encapsulation

The packet routing procedures used depend on the point of attachment (Home Agent or Foreign Agent). If a mobile node is in its home network, sending and receiving data packets does not require any special routing method. However, when a mobile node is in a foreign network, sending and receiving data packets by the mobile node requires several steps.

When a mobile node is sending packets from a foreign network, it uses its care-of address or collocated care-of address to forward the packets. As described by [JAR], when a MN is receiving packets (Figure 13), the steps are as follows:

- A HA on the home link advertises reachability of the mobile node's home address network prefix
- Packets destined to the mobile node's home address are therefore routed to the mobile node's home agent.
- The HA intercepts the packets destined to the mobile node and tunnels a copy to the appropriate care-of address that was registered by the mobile node.
- After arriving at each care-of address, the original packet is decapsulated and delivered to the mobile node.

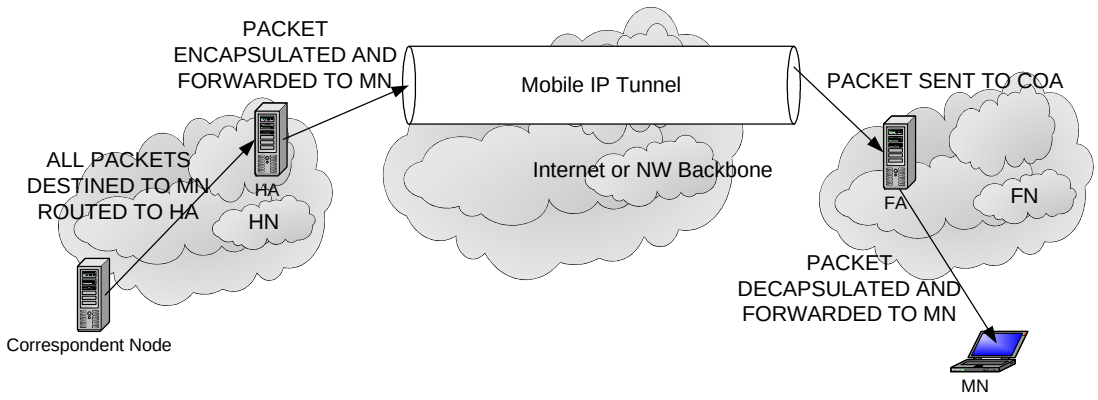

Figure 13. MN Receiving Packets on a FN

B. SECURITY CONCERNS IN MOBILE IP

There are standard security issues that apply to any network, which must be considered before going on to concerns in Mobile IP. Security issues such as authentication, data privacy and data integrity are common in any system. Weaknesses in these areas can be used to create network attacks such as passive eavesdropping, active replay attacks, denial of service, and session stealing. The addition of mobility creates additional security issues both in allowing a mobile device and connecting it to a network by dialing in or physically taking a laptop from one network to another. The security threat is that the mobile device can penetrate any network if it is allowed to physically enter the network.

However, for the purposes of this thesis, the idea of mobility will be synonymous with the idea of being mobile and wirelessly connected. The use of wireless technology brings along additional security issues on top of the standard security ones. Wireless technology operates on radio waves. Intercepting radio wave communication signals is trivial with the right tools. Sniffer tools such as Sniffer Technologies' Sniffer Wireless Tool and AirSnort from Sourceforge.net allow malicious attackers access to sensitive information sent over wireless communication sessions. In the following sections we describe these security issues in greater detail.

1. Passive Eavesdropping

Passive eavesdropping involves an attacker using some sort of IP packet sniffer such as Ethereal which is available on many systems including Linux, various BSD OSes, Solaris, Windows and MacOS X based on the libpcap library [ETH], WebSniff [SEC], or Sniffer Technologies' various sniffer products [SNI], to capture data flow on a communication line and wirelessly. Using this method, an attacker viewing unencrypted communications can gain information such as user accounts, user names, passwords, messages, etc. This is particularly dangerous in a wireless network because the attack could happen anywhere, whereas in a wired network, the attacker usually needs physical access to the communication lines (and/or bridges or routers), which are used to carry the traffic between the communicating parties [SOL].

This attack can be prevented using two methods, end-to-end encryption or Low Probability of Intercept/ Low Probability of Detection (LPI/LPD). End-to-end encryption encrypts and decrypts the data at the source and the destination can be used. This encryption provides protection against eavesdroppers because any information that gets delivered is encrypted. Therefore, any information that is "sniffed" off of the wireless communication link is useless ciphertext to the eavesdropper because it cannot be decrypted [SOL]. Unfortunately, encryption does not fully protect against traffic analysis, which involves identifying usage patterns and the protocols that are being used. Adding IPSec (explained later in the thesis) can defend against traffic analysis because the attacker will not know where the packets originally came from [NIC]. LPI/LPD provides a method that the military uses to send data. One way to accomplish this is to transmit the information in very short, (pseudo) randomly spaced bursts. This makes it difficult for attackers to find the radio-frequency signals [MEN].

2. Active Replay Attacks

An active replay attack is one in which a malicious user can use (parts of a) previously recorded session to impersonate a valid user to gain access to a network. In the case of a wireless network, this could be done more easily and more covertly than on

a wired network because the attacker could perform the attack from anywhere that is within the range of the wireless network.

This type of attack can theoretically be applied to a Mobile IP network. When a MN registers with its HA, an attacker can copy the registration request and use it at a later time, to “replay” to gain “legitimate” access. If the mobile node uses a collocated care-of address, the MN registers directly to the HA (Figure 14). Therefore, the malicious user can copy the registration requests with session information and use them later to send a counterfeit collocated care-of address with the “replayed” session. This allows the attacker to communicate directly to the HA, pretending to be a legitimate mobile node of the home network. Although we have not tried to perform this type of attack, the tools that were previously mentioned make it seem highly possible. To protect against this type of attack, there needs to be mechanisms such as timestamps and nonces together to give each packet a unique identifier. If another packet was used with the same timestamp and nonce, then the receiver could deduce that the packet was sent from a malicious source and deny any services.

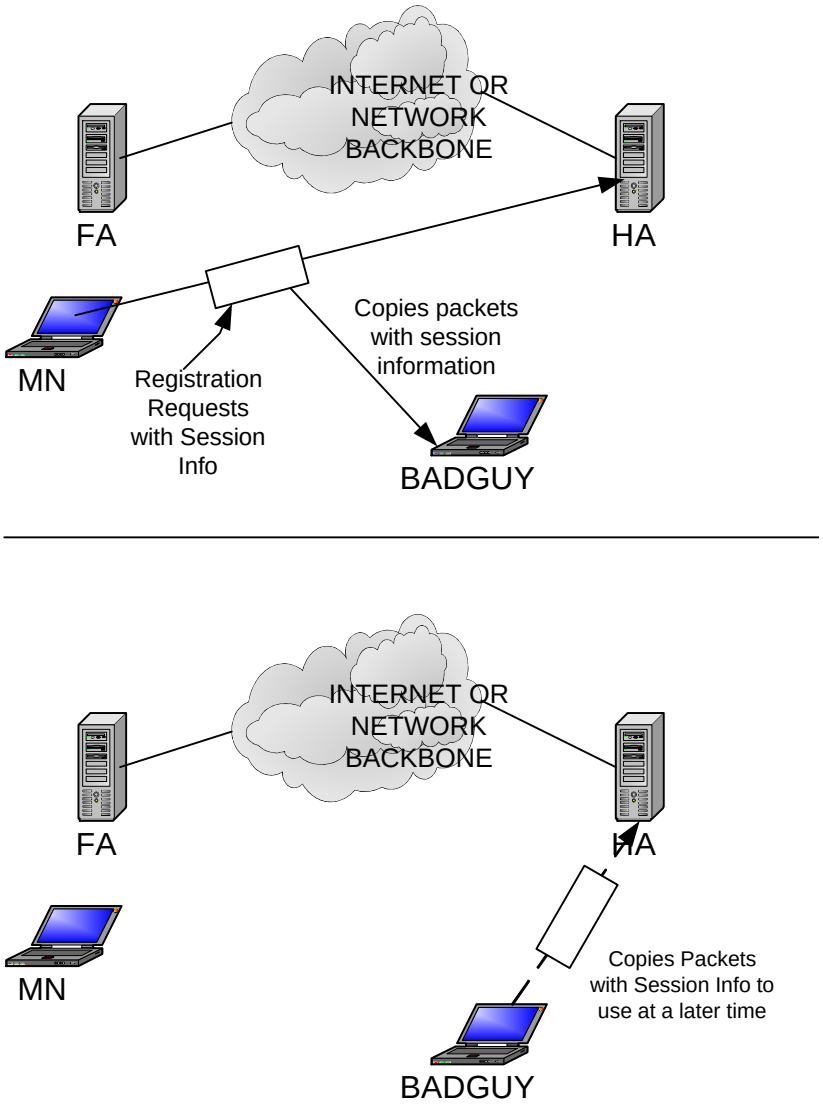

Figure 14. Theoretical Active Replay Attack in Mobile IP using CCOA

3. Denial of Service

Denial of Service is an attack on a network in which access to resources and/or information is purposely prevented by an attacker. This attack makes it impossible for the parties to communicate. This is not limited only to wireless networks. This applies to any network. It can be performed by one of the following:

- A large number of packets can be sent to a host, making it impossible for the host's CPU to process all of them. Since the CPU is trying to process

all of these packets, it is impossible for an exchange of any useful information between the host and a legitimate user [SOL].

- An attacker can prevent traffic from flowing between the communicating nodes [SOL].

An attacker can theoretically perform this type of attack by capturing information during the start of the registration request session (Figure 15). The attacker could eavesdrop on the registration requests and receive the IP address of the HA. Then, the attacker could flood the HA with spoofed packets, making it unable to provide any normal services [SOL]. Spoofed packets are packets whose source address is set as a nonexistent address or a valid address; therefore the true source of the packet is unknown [SOL]. This makes it difficult to know where the attack came from. Again, although we have not tried to perform this type of attack, the tools that are available make this vulnerability seem possible.

A way to foil this type of attack is to use ingress filtering, which enables the router to discard packets that enter an interface that is not normally used to forward packets [SOL]. This does not prevent the attack because packets can still be sent with seemingly legitimate spoofed IP packets [SOL].

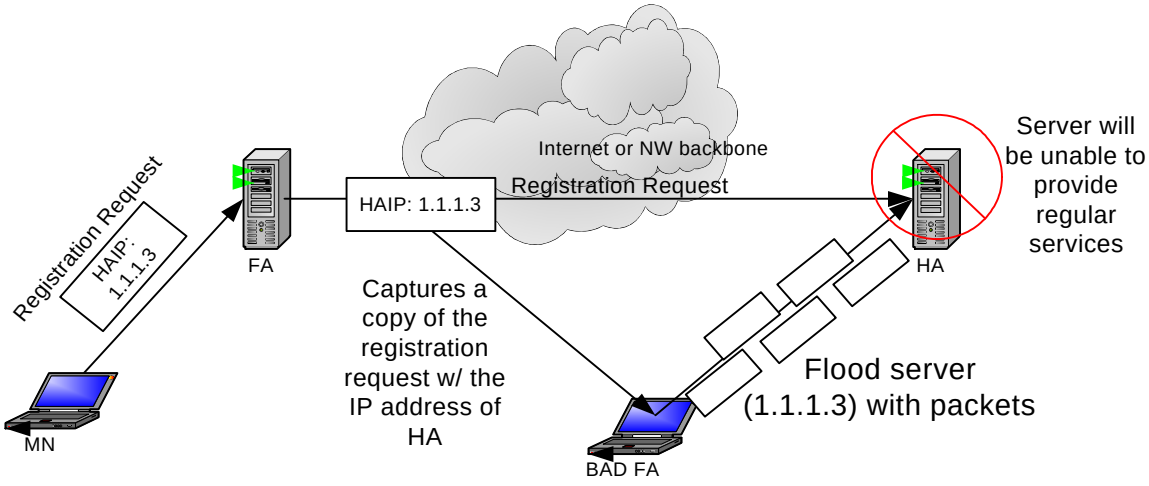

Figure 15. Theoretical DoS Attack on Mobile IP

4. Session Hi-jacking

Session Hi-jacking involves an attacker stealing the established connection of a valid user. This enables the attacker to act as if they are the legitimate user while the real user thinks that the server is down. The server does not know that the attacker is the one that is connected and keeps the communication link going.

In theory, an attacker can perform this attack in a Mobile IP network by waiting for the mobile node to register back to its HA, eavesdrop, flood the mobile node with spoofing packets, steal the session by sending packets to the HA that appear to have come from the mobile node and finally capture packets destined to the mobile node (Figure 16) [DAN]. Since this is similar to the passive eavesdropping attack, using end-to-end encryption could prevent a malicious user from obtaining any useful information [SOL].

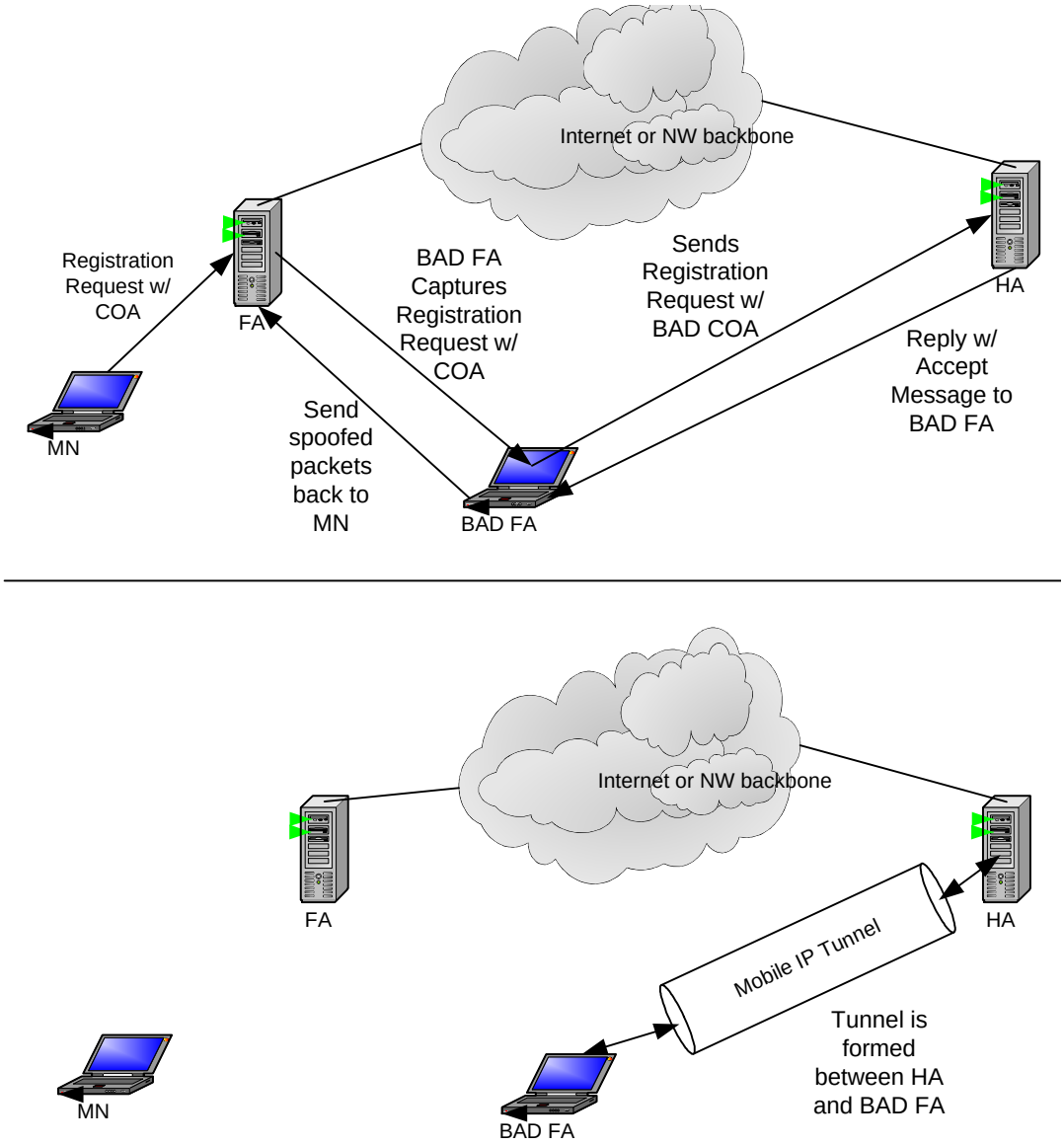

Figure 16. Theoretical Session Hi-Jacking in Mobile IP

C. DHCP AND SECURE MOBILE IP

1. DHCP

One important part of secure Mobile IP is the dynamic host configuration protocol (DHCP). Although Mobile IP can be implemented without DHCP, our implementation used DHCP to distribute a collocated care of address to the mobile node.

Secure Mobile IP requires that the tunnel be encrypted from the mobile node back to the HA. MN Decapsulation, in which the MN performs the decapsulation of the outer packet to reveal the original packet, allows for this type of implementation. It establishes a tunnel from the roaming mobile node to the HA. FA Decapsulation, in which the FA performs the decapsulation of the outer packet to reveal the original packet to forward, establishes a tunnel from the HA to the foreign agent, which is used as a care-of-address. It's important to note that tunneling always stops at the care-of-address in Mobile IP. In MN Decapsulation the mobile node acquires a collocated care-of-address via DHCP, which is then used as the care-of-address. This is important since anything coming out of the mobile node needs to be encrypted and if the tunnel is only to the foreign agent then some one on the same network subnet could be sniffing traffic from the visiting mobile node.

The Internet Engineering Task Force (IETF) created the Dynamic Host Configuration Protocol. DHCP is useful in secure Mobile IP (SecMIP) because SecMIP requires the use of MN Decapsulation as described in chapter II. DHCP provides a means of distributing a collocated care of address to a visiting mobile node. DHCP was originally defined in RFC 1531 but the most recent update is RFC 2131. DHCP allows for in response to the need of having management of IP addresses on centralized servers vice client systems. It was developed from an earlier protocol called Bootstrap (BOOTP), which was used to pass information during initial booting to client systems. It was designed to store and update static information for clients, including IP addresses. The BOOTP server always issued the same IP address to the same client. As a result, while BOOTP addressed the need for central management, it did not address the problem of managing IP addresses as a dynamic resource [SUN].

a. What is DHCP

DHCP is used to assign IP addresses, track their usage and follow their traces. This is important for logging especially when there is a security breach, and to recover a predetermined list of IP addresses and other configuration information shared in

a network of systems. DHCP dynamically assigns IP addresses to hosts that attach themselves to networks. Figure 17 is a DHCP leasing sequence timeline [TAR].

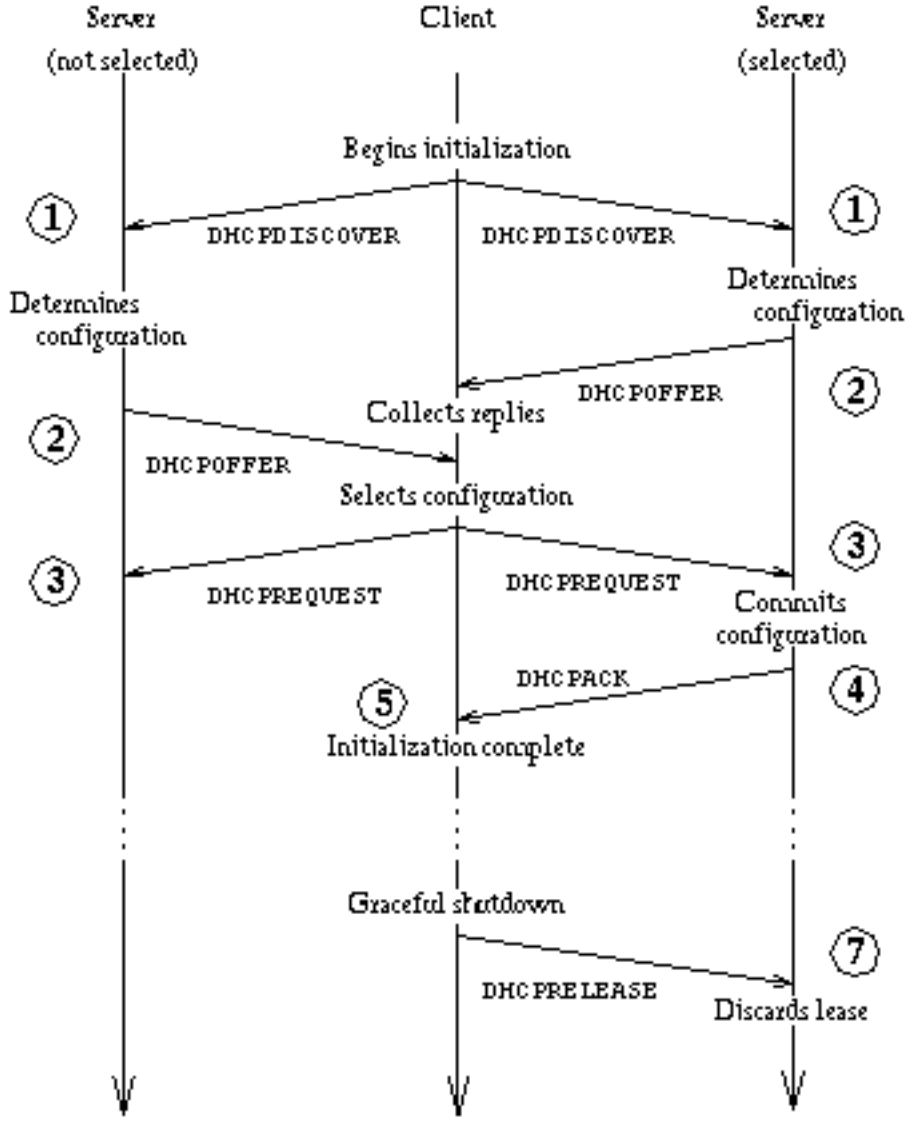

Figure 17. Messages Exchanged Between DHCP Server and Client.

Step 1: The client broadcasts a DHCPDISCOVER

Step 2: Each server may respond with a DHCPOFFER message.

Step 3: The client receives one or more DHCPOFFER messages from one or more servers and chooses one server from which to request configuration parameters. The client then broadcasts a DHCPREQUEST message.

Step 4: Those servers not selected by the DHCPREQUEST message use the message as notification that the client has declined that server's offer. The server selected commits and responds with a DHCPACK message containing the configuration parameters for the requesting client.

Step 5: The client receives the DHCPACK message with configuration parameters. At this point, the client is configured. If the client receives a DHCPNAK message the client restarts the configuration process.

Step 6: The client may choose to relinquish its lease on a network address by sending DHCPRELEASE message to the server.

Step 7: The server receives the DHCPRELEASE message and marks the lease as free.

Organizations that support DHCP have at least one or more DHCP servers, which maintain a block of IP addresses unique to that organization. In our test bed, we implemented DHCP on Linux Redhat 8.0 with the 2.4.18 kernel machines. There are different ways of assigning addresses. One can define a block of IP addresses to be assigned to clients. One can also assign a specified address to a specified machine . There at least a half dozen ways of assigning addresses via DHCP however; we will not go into the details in this paper. The DHCP service can be started and restarted in Redhat through command line or GUI. When a user boots a client system, that system broadcasts a request for a DHCP server to issue it an IP address. The server responds with an IP address, gateway, lease time information, etc. The information that the client gets is limited to what the DHCP administrator configures in the dhcpd.conf file.

b. Where DHCP is Useful

The most common usage of DHCP is to move the management of IP addresses away from the distributed client systems and onto one or more centrally

managed servers. These central servers maintain databases of network specific information (addresses, netmasks, and so on) which relieves the client from having to store static network information on their machines Sites that have many TCP/IP clients such as NPS would be an environment where DHCP would be useful because it would too big of a task for a network administrator to keep track of all these clients. Also, sites where laptops commonly move among networks within the site, again much like NPS's wireless network would be candidates for a DHCP implementation.

Another environment where DHCP would be useful is in secure Mobile IP. When the mobile node moves from its home network to a foreign network it acquires a collocated care-of-address via DHCP, which is then the care-of-address where the tunnel stops. The tunnel goes from the HA all the way to this newly acquired address of the mobile node, which is the focus of this thesis will be discussed more in-depth in Chapter II and IV.

D. MOBILE IP VS. MOBILE TELEPHONY

In table 4 we show the similarities in functionality between mobile telephony and Mobile IP. Listed are the mobile functions then a brief description of how Mobile IP and mobile telephony deal with the function.

Functions	**Mobile Telephony**	**Mobile IP**
Communication	Base station controller, which includes the base transceiver tower, communicates directly with mobile phone.	Access Point. Communicates directly with the mobile node.
Handoff	Depends on the technology. It can be either hard of soft (discussed in previous paragraphs). In CDMA the phone does the handoff. Other technology such as TDMA the network informs the phone.	In Mobile IP, the mobile node performs the handoff. Dynamics breaks the connection completely while MN registers then continues connection. Connection drops after a few minutes of inactivity.
Location/ Update	When the phone powers up it sends out its SID (System Identification Number) which is a unique n umber assigned to every wireless operator in the US that is then programmed into the phone. If it matches then it knows it's at home. If it doesn't match then it knows it's roaming. The local MSC communicates with the home MSC of the phone and the phone sends a registration to its local MSC. Once it's validated then the MSC knows the location of the phone and knows	In Mobile IP the mobile node once connected to the foreign agent will send a registration request to its HA, which is found by the HA address set in the MN. Once accepted the mobile node can begin transmitting and receiving packets via the HA.

	where to send its calls.	
Registration	Registration request is sent to the local MSC, which validates or rejects. If the phone is not at home the local MSC communicates with home MSC. Once the phone registers with the home MSC the MSC keeps track of location in a database. This database is the home location register, which maintains routing information.	If the mobile node is at home it registers with its HA, which either accepts or rejects. If it's in a foreign network the mobile node registers with the foreign agent, which forwards it registration to the MN's HA. The HA then keeps track of the MN's care-of-address and forwards packets destined for the MN to it the MN's care of address.
Routing	The public switched telephone network, which is, comprised of the telephone companies', routes calls to the appropriate destination.	Since Mobile IP is packet based all packets are routed over the internet to the appropriate destination.

Table 4. Comparison of Mobile IP and mobile telephony

III. DYNAMICS HUT – MOBILE IP IMPLEMENTATION

We chose Dynamics for our project because of the fact that the source code was readily available and it was built on top of Linux. In addition, this implementation had the best documentation. On the other hand, only marginal support was available as this project has been dormant for nearly three years. We found an active mailing list that was somewhat helpful in getting the implementation up and running.

A. DYNAMICS BACKGROUND

The Dynamics project began during the academic year of 1998-1999 at Helsinki University of Technology offered as a course. Originally, the assignment was to build a hierarchical Mobile IP implementation for IPv4 networks [MAL].

A hierarchical Mobile IP network includes more than one foreign agent in a foreign network (Figure 18). These foreign agents comprise the hierarchical structure of the network.

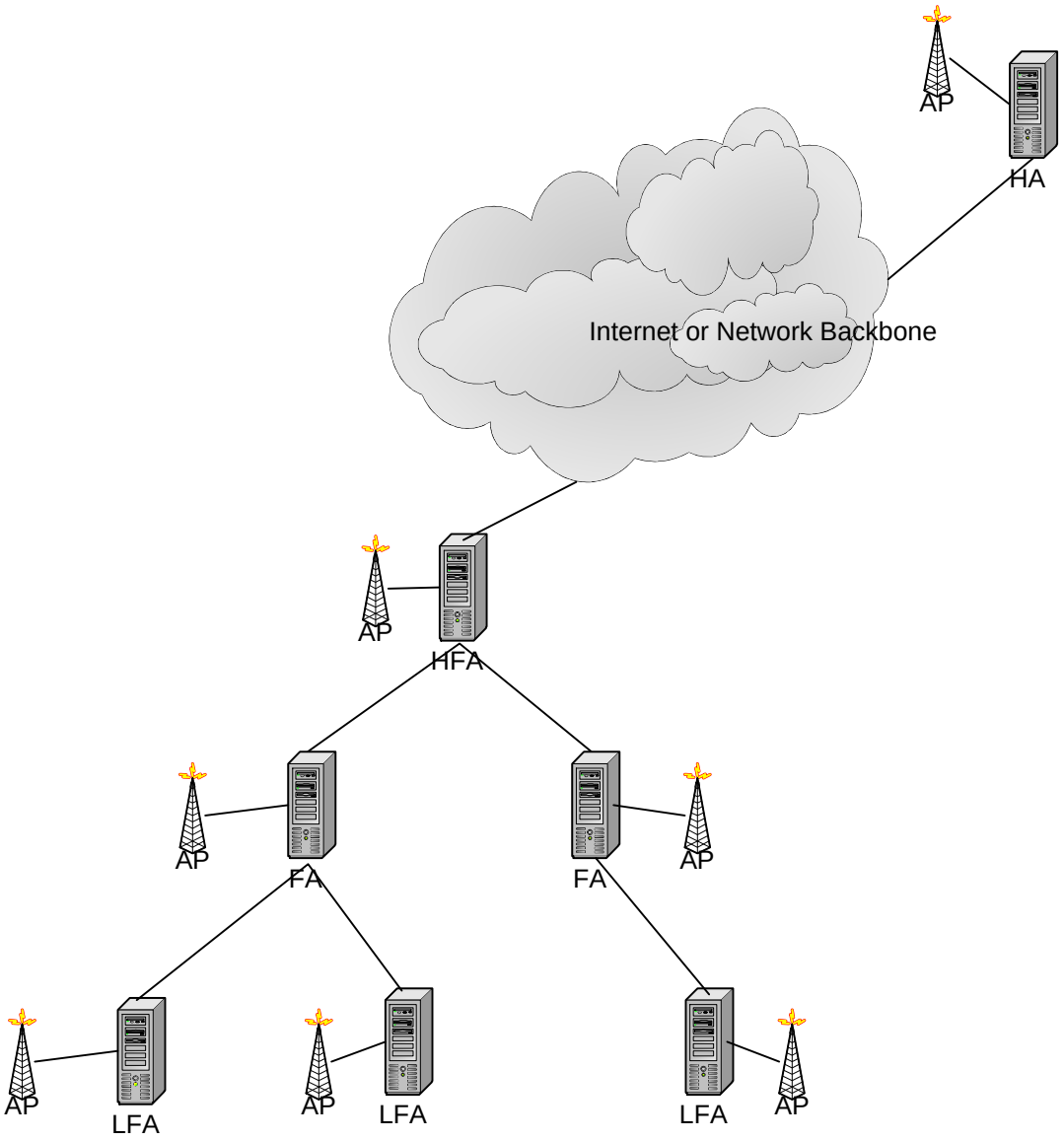

Figure 18. FA Hierarchy

The goal of this type of structure is to make the distance of the registration requests and replies as minimal as possible. The tunnel is established between the HA and the highest FA (HFA), between each FA in the path to the lowest FA (LFA), where FA decapsulation takes place [FOR]. In FA decapsulation, the end of the tunnel is the IP address of the LFA that is connected to the MN. The following sections will describe the different system elements and the dynamics of this implementation.

B. SYSTEM ESSENTIALS

This implementation of Mobile IP contains the essential elements of a HA, mobile node and a foreign agent. These are all common elements needed in a Mobile IP network, according to RFC 2002. However, the Dynamics implementation adds more functionality by allowing for a hierarchical structure of foreign agents.

1. The Home Agent and the Mobile Node

These two elements have the basic functionality as previously described in Chapter 2, section A, entitled, *Architecture of Mobile IP?*. The HA also has an added operation of producing and distributing the session keys needed for regional registrations in a foreign network [MAL]. It is considered to be the key distribution center for the foreign agent and the mobile node [MAL].

2. The Foreign Agent

The foreign agent in this implementation allows for regional registration, which allows the mobile node to register with all the FAs between itself and it's HA [PER1]. When the MN registers with the LFA in the FA hierarchy, the registration request gets relayed to the next higher level FA. For each registration request, each FA stores the address of the next lower FA in the hierarchy. That address is determined by the address in the request message [PER1]. Regional registration limits the effect of latency over congested links and remote hosts [MAL]. Each time the mobile node changes is position in the foreign network, the first agent advertisement that it receives from a FA will be considered as the closest to the MN. When the MN sends out a registration request, that request goes to the FA closest to the MN. The registration request is forwarded up the hierarchy to another foreign agent until it reaches the highest FA, HFA. The HFA then forward the registration request to the HA. The reply message from the HA will take the same path through which the request came from.

C. TUNNELING/ROUTING

In this implementation of Mobile IP, the establishment of the tunnel occurs between the home agent (HA) and the current registered location of the mobile node (MN). Depending on which decapsulation method is used, the tunneling will differ. If FA decapsulation is used, then the tunnel is created from the HA to the FA (Figure 13). In the case of a hierarchical structure, the tunnel is created between the HA and the FA and between each FA all the way down to the lowest foreign agent [FOR] (Figure 19).

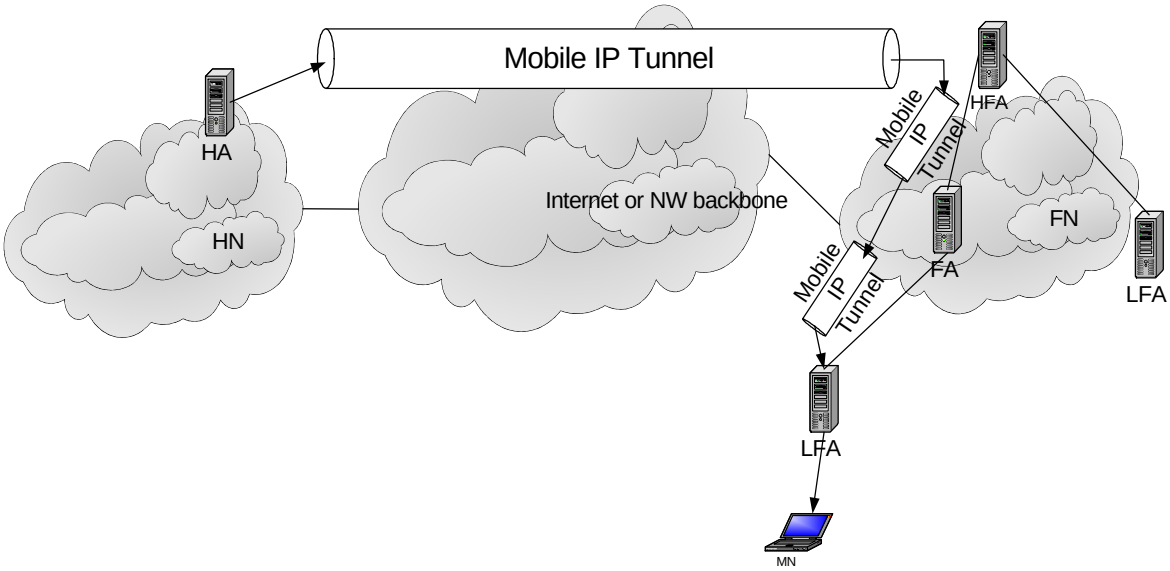

Figure 19. Tunnel Representation in Hierarchical FN (FA decapsulation)

In the case of MN decapsulation, the tunnel is directly created between the HA and the MN (Figure 20). This last method allows the mobile node and the HA to communicate directly with each other through this tunnel.

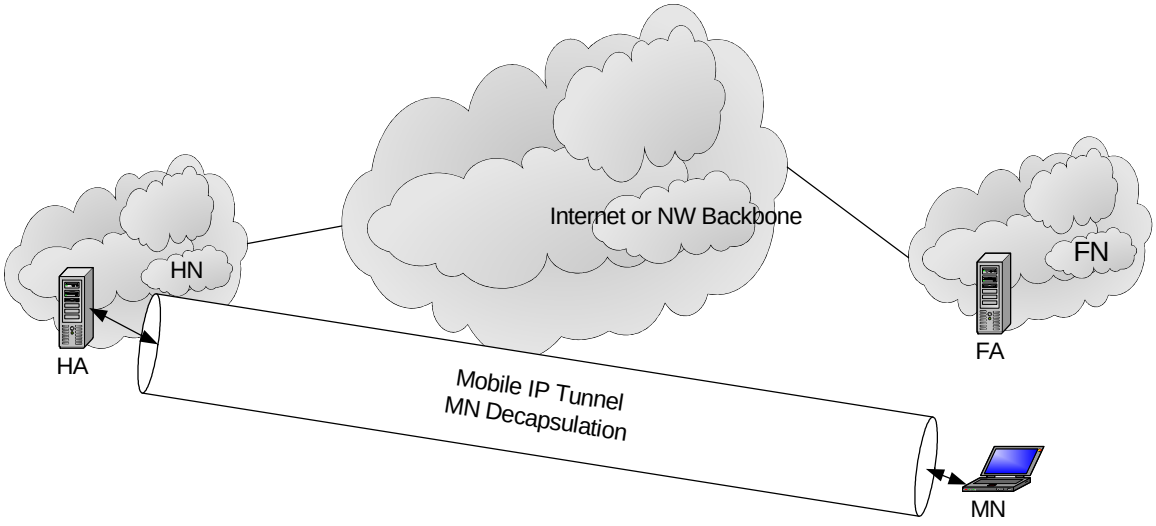

Figure 20. Tunnel Representation for MN Decapsulation

Dynamics uses the IP-in-IP and Generic Record Encapsulation (GRE) encapsulation modules. GRE is more of a general protocol compared to IP-in-IP because it can encapsulate other protocols other than IP [PER1]. For the purpose of this thesis, we chose to use the default protocol IP-in-IP for simplicity.

The tunnel that is created is represented in the Linux operating system as another interface that can be referenced in the same way as a physical Ethernet interface such as eth1 or eth0. The endpoints of the tunnel are the HA and the care-of address. For FA decapsulation, the name of the tunnel has the format TUNL with a number appended to the end, with the starting number at 0. In our implementation, we only had one tunnel up at a time so the name of our tunnel in FA decapsulation mode was always TUNL0. In MN decapsulation, the standard name of the tunnel is TUNLMNA.

D. POLICY-BASED ROUTING

Dynamics routing is based on policy routing in Linux [FOR]. Policy routing protocols share the idea that one route should be selected out of all available routes to minimize some measure of the route, such as, delay [CLA]. Policy-based routing uses both the source and destination addresses to correctly route packets [MAR]. To correctly route packets to MN, the FAs in the hierarchy must know the ultimate destination as well

as the packet origin [MAL]. In a large FA hierarchy with many different paths, policy-based routing is needed for the FAs to choose the correct path to route the packets and minimize delay. For a more detailed description of policy routing and policy-based routing please refer to [CLA] and [BRA]. For more information on policy-based routing in Linux please refer to [MAR].

IV. WIRELESS SECURITY

As we have discussed, the use of wireless devices has grown exponentially, which means that the amount of information traveling over the air has increased. Now with the invention of Mobile IP, security is an even bigger technical problem because Mobile IP allows for roaming of mobile devices which means there will be much more sensitive information such as business information, personal credit card numbers, or social security numbers more easily accessible in the air. In this section we will cover some of the wireless security issues. We will start out by covering the Wired Equivalent Privacy (WEP) algorithm [ISA]. Next we will discuss the use of IPSec, and lastly IPSec integrated with for Secure Mobile IP to create secure Mobile IP and its' advantages and disadvantages.

A. WEP

It is common in schools and business to have 802.11-based wireless local area networks (WLANs). A WLAN allows a user to connect to a local area network through a wireless (radio) connection. The IEEE 802.11 standard specifies technologies for LANs. It uses the WEP (Wired Equivalent Privacy) algorithm for encryption. While WEP provides some level of security for WLANs there are security issues concerned with WEP that make WLANs that use WEP, vulnerable to various types of attacks. [NIC].

WEP can be used to help prevent passive eavesdropping and provide some level of authentication. The goal of the WEP model is to prevent casual eavesdropping or unauthorized data modifications [NIC].

However, there are security flaws associated with WEP, which make WEP practically unusable for organizations that require privacy. Because an eavesdropper can sniff packets while attached to a wired network, there may need to be other mechanisms for encrypting and authenticating mobile users.

WEP protects only the data packet information and does not protect the physical layer header so that other stations on the network can listen to the control data needed to manage the network [NIC]. An attacker could easily analyze the traffic and after about 5-

6 MB of data can have enough information to have a key. For these reasons we don't believe that WEP would be a solution to privacy for a mobile device.

WEP uses a secret key that is shared between a wireless station and an access point (AP). WEP uses an RC4 40-bit or 64-bit stream cipher from RSA Data Security to encrypt and decrypt data. The 32-bit CRC (Cyclic Redundancy Check) is also encrypted along with the frame body [GDB]. Figure 21 [GDB] shows a WEP packet.

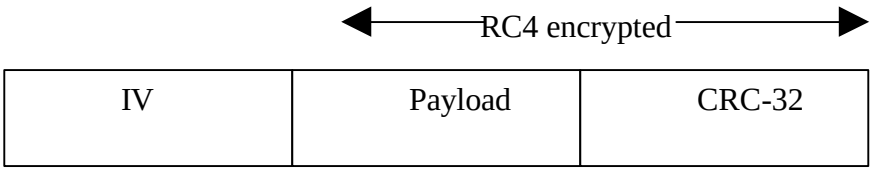

Figure 21. Packet Format [GDB]

CRC is a technique to obtain data integrity. It has three significant advantages: error detection capabilities, little overhead, and ease of implementation [RAD]. According to the ISAAC (Internet Security, Applications, Authentication and Cryptography), the WEP algorithm can be broken through various attacks [BOR2], which will be discussed in the following paragraphs. ISAAC is a small research group in the Computer Science Division at the University of California, Berkeley. According to this paper WEP is susceptible to the following:

- passive attacks to decrypt traffic based on statistical analysis
- active attack to inject new traffic from unauthorized mobile stations based on known plaintext
- active attacks to decrypt traffic based on tricking the access point
- dictionary-building attacks

1. Passive Attacks to Decrypt Traffic Based on Statistical Analysis

This attack is based on collecting information over a period of time and using the information to perform an attack. We like to compare this to social engineering. A

passive eavesdropper can intercept all wireless traffic, until an Initialization Vector (IV) collision occurs. By XORing two packets that use the same IV, the attacker obtains the XOR of the two plain text messages, which enables the attacker to perform statistical attacks to recover the plaintexts [ISA]. The resulting XOR can be used to infer data to gain information on the contents of the two messages. IP traffic is often very predictable and includes a lot of redundancy due to the initialization vector [ISA]. The initialization vector in WEP is a 24-bit field, which is sent in the cleartext part of a message. A 24-bit field initialization vector guaranteed the reuse of the same key stream. A busy access point, which constantly sends 1500 byte packet at 11Mbps, will exhaust the space of IVs after 5 hours [ISA]. This redundancy can be used to eliminate many possibilities for the contents of messages. This gives an attacker many possibilities get at the data in the messages. Further educated guesses about the contents of one or both of the messages can be used to statistically reduce the space of possible messages, and in some cases it is possible to determine the exact contents. When such statistical guessing doesn't work, the attacker can just look for more collisions of the same initialization vector. With just a small amount of time, depending on the situation, it is possible to recover a modest number of messages encrypted with the same key stream, and the success rate of statistical analysis grows quickly. Once it is possible to recover the entire plain text for one of the messages, the plain text for all other messages with the same IV follows directly, since all the pairwise XORs are known [BOR2].

2. Active Attack to Inject Traffic

If an attacker knows the exact plaintext for one encrypted message, he can use this knowledge to construct correctly encrypted packets. The procedure involves creating a new message, calculating the CRC-32, and performing bit flips on the original encrypted message to change the plaintext to the newly created message [BOR2]. The basic property is that RC4(X) xor X xor Y = RC4(Y) [BOR2]. This packet can now be sent to the access point or mobile station, and it will be accepted as a valid packet. [BOR2]

3. Active Attack from Both Ends

This is just an expansion of the previous attack. It can be expanded further to decrypt arbitrary traffic. In this case, the attacker makes a guess not about the contents, but rather the headers of an IP packet. This information is usually quite easy to obtain or guess; in particular, all that is necessary is the destination IP address. Armed with this knowledge, the attacker can flip appropriate right bits to transform the destination IP address to send the packet to a machine he/she controls, somewhere in the world of the internet, and transmit it using a rogue mobile station. Most wireless installations have Internet connectivity; the packet will be successfully decrypted by the access point and forwarded unencrypted through appropriate gateways and routers to the attackers machine, revealing the plaintext. If a guess can be made about the TCP headers of the packet, it may even be possible to change the destination port on the packet to be port 80, which will allow it to be forwarded through most firewalls. [BOR2]

4. Dictionary-building Attack

The dictionary-building attack allows, after analysis of about 5-6 MB of traffic, real-time automated decryption of all traffic. An experiment performed by three students at Rice University showed that 5-6MB of packets is enough data to find the key [STU]. With a small number of initialization vectors an attacker can build a decryption table. Once he/she learns the plaintext for some packet, he/she can compute the RC4 key stream generated by the IV used. This key stream can be used to decrypt all other packets that use the same IV. Over time an attacker can build up a table of IV's and corresponding key streams. Armed with this table, an attacker can decrypt every packet that is sent over the wireless link [BOR2].

B. IPSEC

IP Security (IPSec) is a set of open standards developed by the IETF and documented in Internet general Request-For-Comments (RFC 2401) and related RFCs. The following is the IPSec protocol suite RFCs. The three main components of IPSec are AH, ESP, and IKE.

- Internet Key Exchange – RFC 2409[ITF]
- IP Authentication Header – RFC 2402[ITF]
- IP Encapsulating Security Payload (ESP) – RFC 2406[ITF]
- Security Architecture for the Internet Protocol – RFC 2401[ITF]
- Internet Security Association and Key Management Protocol – RFC 2408[ITF]
- The Internet IP Security Domain of Interpretation for ISAKMP – RFC 2407[ITF]

IPSec provides for end-to-end encryption and authentication at the IP layer to protect IP packets between IPSec-compliant devices. IPSec is currently supported in IPv4 and IPv6. IPSec is most commonly found in network devices such as router, switches, firewalls, and remote access servers as well as many clients as part of VPN solutions. Some of the services offered by the IPSec protocol suite include: Access control, Connectionless integrity, Data origin authentication, Protection against replays, Confidentiality (encryption), and Limited traffic flow confidentiality. These services use transmission protocols, IP Authentication Header (AH) and IP Encapsulating Security Payload (ESP), together with one of the available key management protocols [NIC]. The following paragraphs will cover IPSec in more detail. Before doing so we believe it is important to cover two fundamental aspects of IPSec: Security Associations (SA) and Tunneling. These two concepts are not new to IPSec, but IPSec makes use of them.

A Security Associations (SA) is a unidirectional, logical connection between two IPSec systems. The Security Association is identified by a security parameter index, IP destination address, and security protocol [MUR]. The security parameter index is a 32-bit value used to identify different SAs with identical destination address and security protocol. For bi-directional communication between two IPSec systems, there must be two SAs defined, one in each direction.

Tunneling is a common technique in packet-switched networks. It is basically the concept of wrapping a packet inside a new one. This makes it possible to route the nonroutable such as NetBIOS, IPX or, specific to this thesis, private IP addresses. In the

case of IPSec, IP packets are tunneled through IP to provide security thereby avoiding malicious attacks [MUR]. The following points will cover the different aspects of IPSec in greater detail.

1. Internet Key Exchange (IKE)

In order for hosts to create the secure tunnels that make up a VPN, they must create secure associations, authenticate each other, and exchange the keys they will use for the encryption for their data. One way of accomplishing this is with the Internet Key Exchange (IKE) protocol. IKE is responsible for providing authentication of all peers, handling the security policy negotiations, and controlling the exchange of keys [SCT]. It is used to create an initial encryption session, enabling the exchange of the information required to make the final encryption session.

This protocol uses parts of ISAKMP and parts of the Oakley and SKEME key exchange protocols to provide management of keys and security associations for the IPSec AH and ESP protocols, and the ISAKMP itself [MUR]. The IKE inherits its security association (SA) and key management (but not key exchange) from the ISAKMP protocol, and supports the pre-shared key, digital signature, and public key encryption methods of authentication. Oakley was originally the key exchange protocol used for VPNs and lent its abilities to IKE. Oakley is vital to security, since no matter how strong the encryption and authentication algorithms are, they are worthless if the key is compromised [MUR].

IKE is performed in two phases. In phase one, two hosts establish a secure connection, called the IKE SA. Authentication is either incorporated into phase one with digital certificates, or takes place between phases one and two with extended authentication techniques (Bird, pp. 89-90). In phase two, the final keys used for encryption will be generated, and the IPSec SA will be negotiated. After these two phases, the IPSec SA has been created and is used for all further communication, creating the secure “tunnel.”

In the first phase, IKE chooses between two modes to complete the IKE SA: Main mode and Aggressive mode. During the second phase, IKE uses its third mode,

Quick mode, to negotiate the final IPSec SA. If extended authentication is required, another step is inserted between these two to authenticate the user.

a. Main Mode

To create an IKE SA, Main mode will take the two hosts through three two-way exchanges, totaling six steps. In the first exchange, steps one and two, the hosts agree on basic algorithms and hashes that will be used throughout the remaining four steps. In steps three and four, they prepare to create an encrypted tunnel by using the Diffie-Hellman key agreement, exchanging the necessary items to create their shared secret key. If the two sides have digital certificates then these are also exchanged [YJL]. Steps five and six complete the Diffie-Hellman exchange, leaving each with the shared secret, which is used to encrypt the rest of the communication [TIM].

b. Aggressive Mode

This mode is used to accomplish the same end result as Main mode, but it does so in only three steps instead of six. This mode is quicker, but at the sacrifice of not protecting the identity of each host. In main mode, host identities are not normally divulged until the encrypted fifth and sixth steps of Main mode.

Aggressive mode is accomplished by sending the IKE SA proposal, the Diffie-Hellman information, digital certificates if used, and the ID packet all in the initial exchanges between the two hosts during steps one and two, instead of breaking them down into six steps. The last step of this mode is just a confirmation exchange [TIM].

c. Extended Authentication (XAUTH)

If the hosts choose not to use digital certificates to authenticate each other, then authentication must take place before continuing on to phase two, Quick mode. In Extended Authentication mode an extra set of exchanges takes place between the hosts to authenticate each other using an extended authentication method such as RADIUS [YKL]. RADIUS is a protocol for exchanging information between a RADIUS server

and a RADIUS client. Its main purpose is to provide authentication, authorization, and accounting for remote access users when they connect to a network.

d. Quick Mode

Quick mode is used in phase two to negotiate the final IPSec information between the now-authenticated and secure hosts. This is accomplished using the current IKE SA to ensure security of the exchange. The end result of this phase is the creation of the final IPSec SA and the generation of fresh keying material, including the symmetric key used for all further encryption between the hosts.

To generate the new SA, the initiating host sends the Quick mode message, protected by the IKE SA, requesting the new IPSec SA. This request includes which Security Parameter Index (SPI) to use in future communications. This SPI, combined with the destination IP address and protocol to be used, uniquely identifies a single IPSec SA. It is important to remember that these SAs are only for one-side of the conversation. As we mentioned earlier SAs are unidirectional therefore it takes two SAs for bi-directional communication.

e. Perfect Forward Security (PFS)

PFS is an option in generating the final set of symmetric keys in Quick mode. The goal of PFS is provide the confidence that the compromise of a long-term private key does not compromise any earlier session keys [YMJ]. It is used to create a key that does not have any information derived from or depending on the previous key used.

When the final keys are to be created, there are two ways this can be done. Quick mode can be set to create the new key by just hashing the original key used during IKE phase one. Though this is simple and fast, the problem is that if the original key is later cracked, it is a simple step to hash that cracked key, giving the cracker the next key. To keep this from happening, Quick mode can use PFS to initiate a new Diffie-Hellman key exchange. This use of Diffie-Hellman ensures that even if the original key is cracked, it gives no information on the next key. The cracker would then have to go back

and crack the new key instead of just being able to hash the previous key value to find the new key. The down side to this is that it takes more time, steps, and computational power to create new keys using Diffie-Hellman algorithm then it does to just hash the previous one, so security needs to be balanced with threats to meet each individual communities needs [TIM].

f. Security Associations (SA)

In the previous sections we used the term security association, SA, because this is such an important part of IPSec we feel it is important to discuss a security association.

A SA is a logical security connection between two IPSec systems. SAs are negotiated when IPSec hosts create their connection, and take the form of

<Security Parameter Index, IP Destination Address, Security Protocol>

The Security Parameter Index (SPI) is a unique 32-bit value used to identify the SA. It is carried in the header of the security protocol, and selected by the destination system during SA establishment . When the SA is established, the 32-bit SPI value is chosen by the destination system [MUR].

The Security Protocol is either ESP or AH, which will be discussed in the following sections. SAs define a security association in only one direction, to the destination. Since communication is often a bi-directional activity, two SAs must be established during an IPSec session, one in each direction [MUR].

It is possible to use both ESP and AH together, but in order for this to happen an SA bundle is created. SA Bundles are two SAs defined in each direction, establishing a total of four SAs for the IPSec session. This is seen most often when a mobile host needs to create an AH SA between itself and the network gateway, and a nested ESP SA extends to the host behind the gateway [MUR].

2. Authentication Header (AH) Protocol

The Authentication Header Protocol is defined in RFC 2402. AH guards against denial-of-service attacks, but does not provide confidentiality. It provides integrity and authentication for IP datagrams. These services work on a per-packet basis to ensure protection on each and every packet thereby protecting the entire flow of information. Some fields are not protected by AH these are called mutable. However, the payload of the IP packet is considered immutable and is always protected.

When packets arrive at intermediate routers, the packet is first authenticated before being sent it its final destination. AH can be used in both transport and tunnel mode. Since tunnel mode is specific to our thesis we will cover how AH is used in tunnel mode.

A new IP header is applied to the original IP packet. Next, the authentication header is applied in front of the original packet but after the new IP header. The new IP header is stripped, the AH authenticates then original destination IP address and finally the packet is reassembled and forwarded on to its destination.

AH can be used in tunnel mode or transport mode [MUR]. The following diagrams, Figure 22 and Figure 23, show AH in tunnel mode and transport mode, which were acquired from the Murhammer reference on pages 54-61.

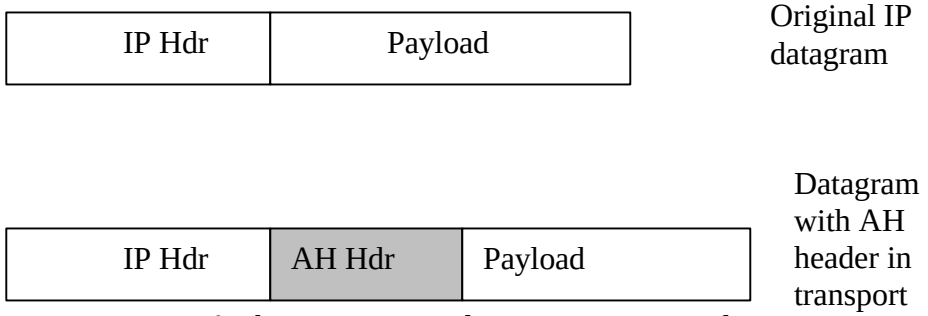

Figure 22. Authentication Header in Transport Mode

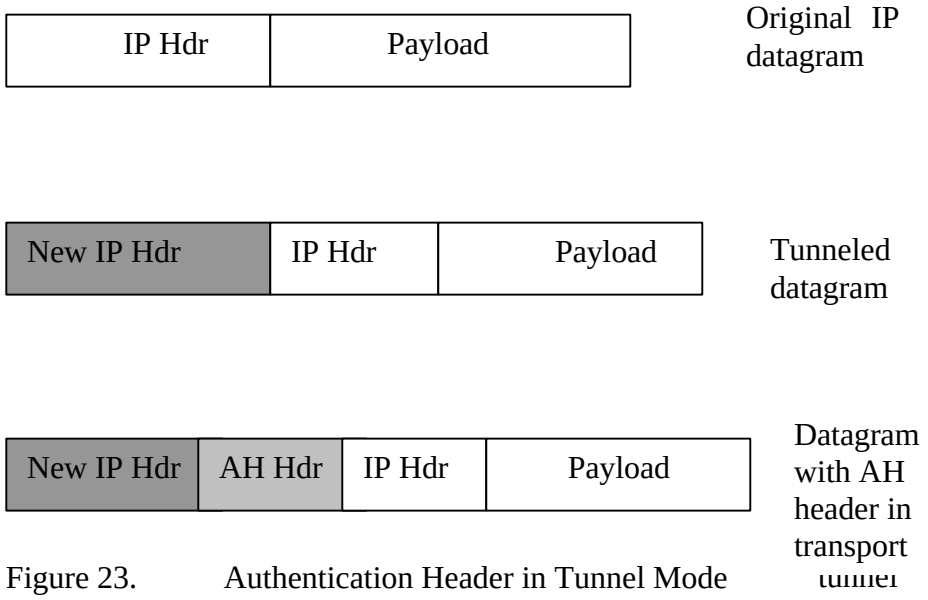

Figure 23. Authentication Header in Tunnel Mode

3. Encapsulating Security Payload (ESP)

The Encapsulating Security Payload is defined in RFC 2406. It offers authentication, integrity, and replay protection. Unlike AH, ESP provides confidentiality. The set of desired services is selected upon negotiation of the security association (SA). ESP is performed on each individual packet, on a per-packet basis. Both the integrity and encryption aspects are optional, and the administrator can choose to implement either or both. If both are selected, the receiver of the packet must first authenticate the packet, and only if it authenticates, will the packet be decrypted. Integrity check and authentication methods must be chosen so that they complement each other. The encryption algorithm used is independent of whatever choice is made for integrity and authentication. ESP can be used in transport mode (Figure 24) or tunnel mode (Figure 25)[MUR].

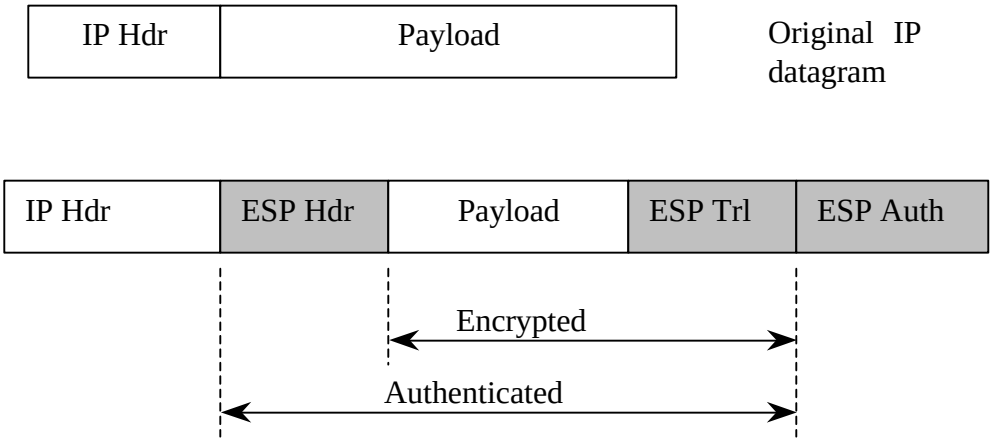

Figure 24. ESP in Transport Mode [MUR]

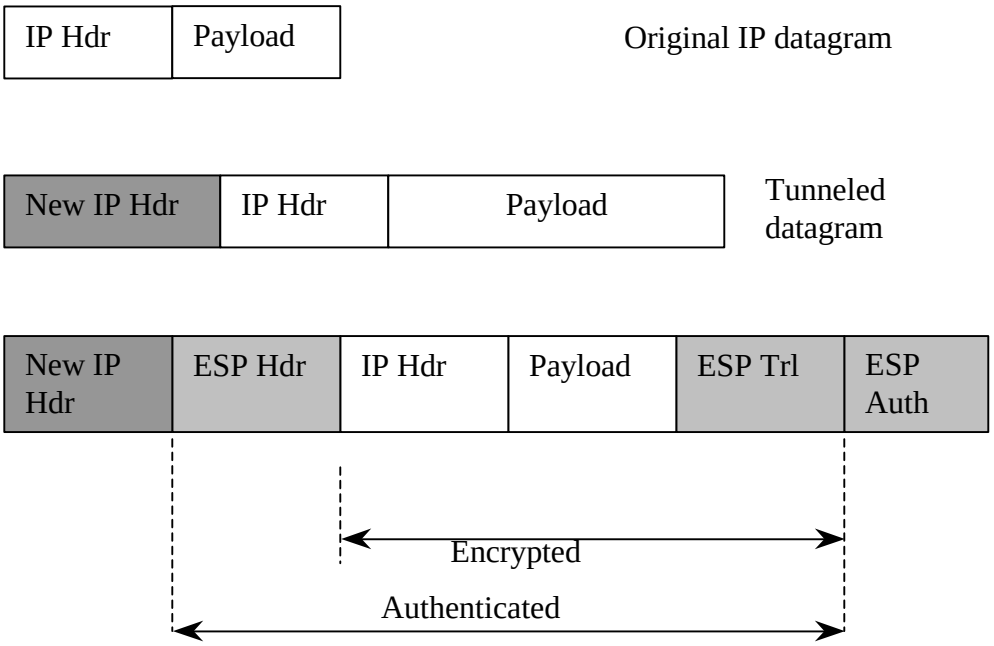

Figure 25. ESP in Tunnel Mode [MUR]

4. Transport Mode

Transport mode is used for transmitting data between two hosts. Only the data is encrypted (Figure 26). An IPSec header is placed before the payload (data), but after the original IP header. This is best used in an internal network where source and destination IP addresses are not of vital importance. To protect that kind of information one would use tunnel mode.

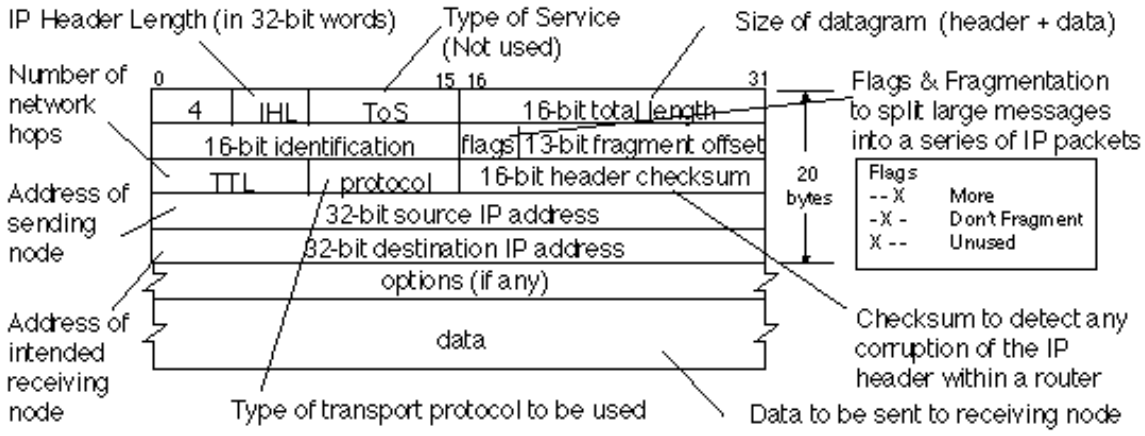

Figure 26. IP Data Packet [YNJ].

5. Tunnel Mode

Tunnel mode is used when transmitting data between two security gateways such as two routers. Tunnel mode is needed to secure Mobile IP because there are many foreign networks the mobile node can join. Therefore it is necessary to protect the packets as they go through each intermediate router and to keep knowledge of the home network hidden from the public. This mode was implemented in our thesis. Implementation details are discussed in the implementation chapter.

Figure 25is a visual picture of what goes on with tunnel mode. The sending gateway encrypts the entire IP packet and appends a new IP header that includes the receiving gateways address as the destination address. When the receiving gateway receives the packet, it strips off the outer IP header, decrypts the packet, and sends the packet to the final destination.

This configuration is typically referred to as a Virtual Private Network (VPN) [NIC]. It would not be possible for one to see the source or destination address since this information is hidden. This is the preferred choice when using private, non-routable addresses over a wide area network [NIC].

B. IPSEC IN MOBILE IP

One of the problems with Mobile IP is the firewall traversal problem. Access to a virtual private network is granted only to authorized users. This section describes how IPSec is used with Mobile IP to provide Mobile IP users secure access to their company's firewall protected virtual private network. Mobile nodes that belong to an organization have to traverse the firewall to access the VPN. Therefore, they have to authenticate themselves. This authentication is realized with IPSec. Secure Mobile IP (SecMIP) uses an IPSec tunnel to protect the Mobile IP tunnel passing the insecure parts of the Internet. Figure 27 [DAN] further illustrates the idea behind SecMIP tunneling.

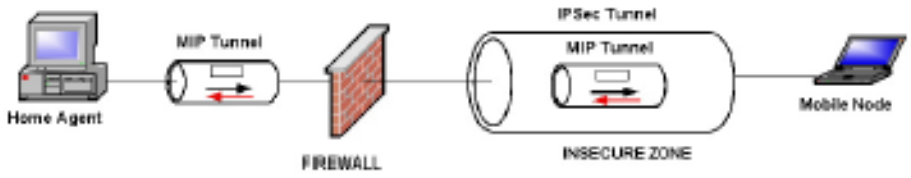

Figure 27. SecMIP Tunneling

After entering a new network area, a mobile node has to be connected via a wireless access point. Foreign agent advertisements are broadcasted regularly into this demilitarized zone (DMZ), which is a network or computer host between a private network and the outside public network that prevents outside users direct access to data on a private server.. The mobile node learns about its physical change of location when it receives this ICMP message. Figure 28 [DAN] illustrates network detection.

Figure 28. Network Detection

When the mobile node enters the new network it disables any old IPSec tunnels that had been established from an older locations using an old collocated care-of-address. The mobile node then needs to acquire a new collocated care-of-address through a DHCP server or from a foreign agent and finally a tunnel is established. Once the IPSec tunnel is established, data transfer is secured. The IPSec tunnel will be between the mobile node's new care-of-address and the home firewall. Figure 29 [DAN] further illustrates the IPSec tunnel between the MN and the home firewall.

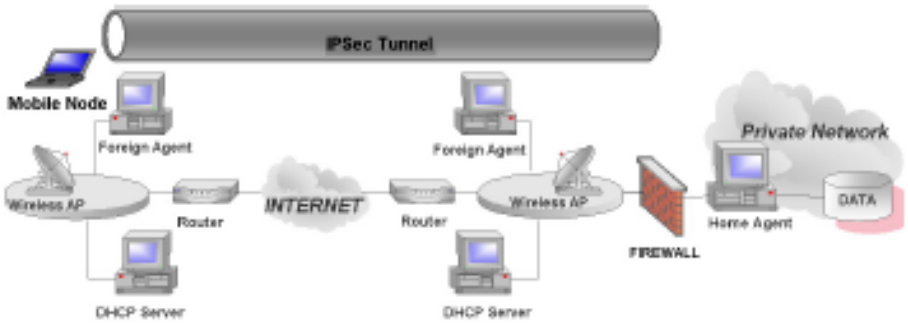

Figure 29. IPSec Tunnel MN ⇔ Home Firewall

THIS PAGE INTENTIONALLY LEFT BLANK

V. IMPLEMENTATION

For our implementation, we used the Dynamics HUT Mobile IP implementation to set up the Mobile IP network. The version that we used was 0.8.1, which is the most up to date, stable release. Our setup consisted of the following hardware items:

- 2 Linksys WAP11 Access Points
- 2 Dells Dimension 8200
- 4 Netgear DS108 Hubs
- 1 Micron Millennia, Linux Router/Gateway
- 1 Gateway 9100 Solo Laptop

A. MOBILE IP NETWORK ARCHITECTURE

Our initial goal was to create a configuration to see how the Mobile IP implementation works (Figure 30). We based our configurations based on the project conducted by Yan, Zan, et al. [YAN]. In the next sections, the configurations for each piece of hardware will be explained. We tried to simulate two subnets and the seamless handoff between them.

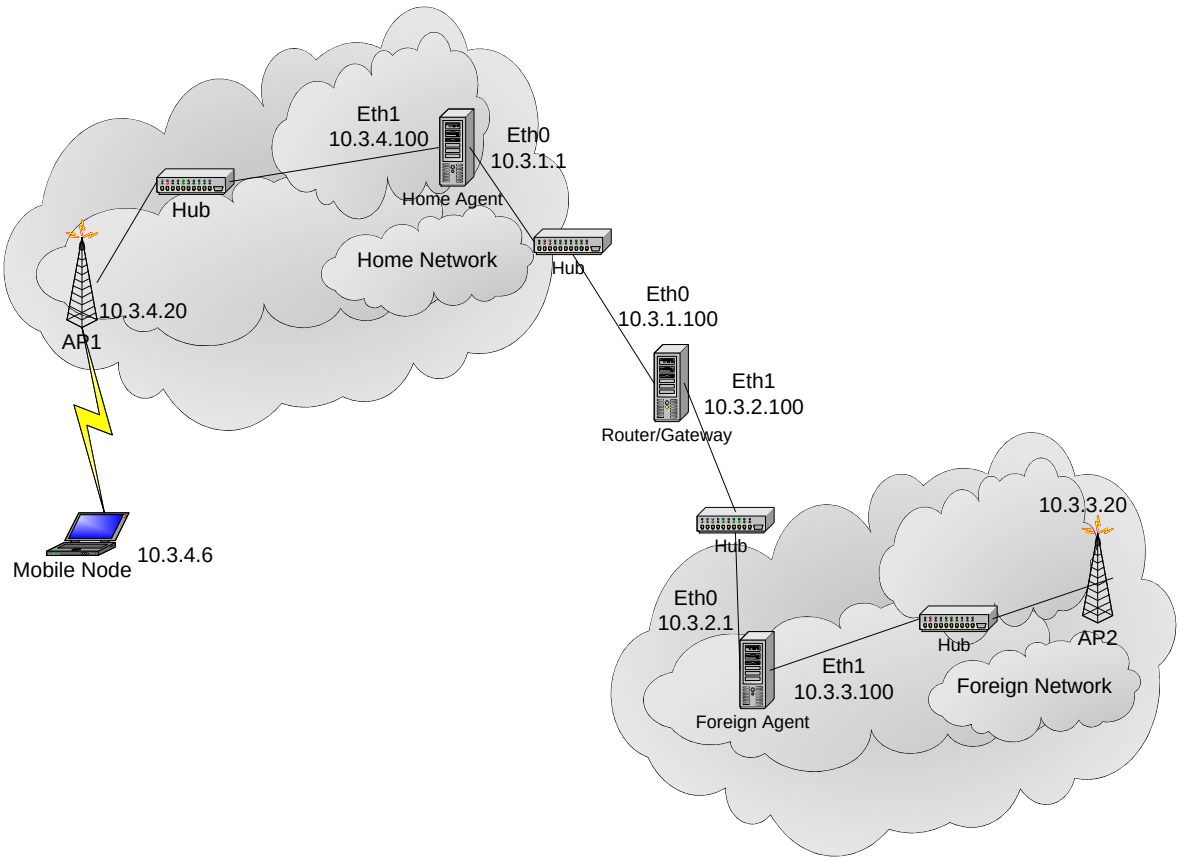

Figure 30. Initial Mobile IP Setup

1. Agents

The configurations for both the home agent and the foreign agent are very similar. The following configurations are for both of the agents:

- Pentium 4, 2.3 GHz, 40 Gig HD, 512 MB RAM
- Redhat Linux 8.0, kernel version 2.4.18-14
- Two NIC cards:
  - 1 Realtek RTL-8139, SMC EZ Card and
  - 1 3Com 3c590/3c595/3c90x

Both agents had the Dynamics implementation installed on them. Each used their respective code to start running. For instance, the code for the Foreign Agent was located

in “/root/dynamics-0.8.1/src/fa/” directory. This would be the same for the Home Agent except that the end of the directory would be “ha” instead of “fa”. The documentation was located in “/root/dynamics-0.8.1/doc/” directory. The executables for each agent was located in “/usr/local/sbin/” directory. There the “dynfad”, “dynhad”, “dynmn”, “dynfa_tool”, “dynha_tool”, and “dynmn_tool” executables are found.

2. Mobile Node

The configuration for the Mobile Node is as follows:

- Pentium 3, 500 MHz, 128 MB RAM
- Redhat Linux 8.0, kernel version 2.4.18-14
- One Wireless NIC Card [Linksys Ver 3]
- One NIC (for wired test) Card – D-Link DFE-680TXD

3. Gateway/Router

The gateway/router performed as a transparent medium between the two subnets. It forwarded all packets to the destinations according to its routing table. The configuration for the gateway/router is as follows:

- Micron Mellennia, Pentium II
- Redhat Linux 7.x
- 2 NIC Cards (Both 3Com 3c590/3c595/3c90x)
    - eth0: 10.3.1.100
    - eth1: 10.3.2.100

The gateway/router needed to have “ipchains” turned off in order for it to be transparent (see Problems). The command ‘ipchains’ in Redhat Linux contains code with rules to manage IP packet filters in firewalls [LIN2]. For this implementation, we needed to turn off packet filtering to allow every packet to pass through the router, making it transparent. For detailed information on *ipchains*, please refer to [LIN2].

4. Access Points

The two access points are connected to the home network and the foreign network. The AP1 is connected to the home network and the AP2 is connected to the foreign network. Please see Figure 30 for the IP addresses. The models of the APs are as follows:

- 1 Linksys WAP11 2.4GHz (AP1), IP Address: 10.3.4.20
- 1 Linksys WAP11 (AP2), IP Address: 10.3.3.20

B. CONFIGURATIONS

The next subsections will explain the different configurations for each agent, the mobile device and the router/gateway. For the agents and router/gateway, we issued the commands:

- echo 0 > /proc/sys/net/ipv4/conf/eth0/rp_filter
- echo 0 > /proc/sys/net/ipv4/conf/eth1/rp_filter
- echo 1 > /proc/sys/net/ipv4/conf/eth0/proxy_arp
- echo 1 > /proc/sys/net/ipv4/conf/eth1/proxy_arp

We also had to change the parameter “net.ipv4.ip_forward” in the file “/etc/sysctl.conf” to equal 1. This allowed all packets to be forwarded between the two interfaces on the agents and the router/gateway.

1. Home Agent

The following configurations for the home agent are:

- IP Addresses
  - Eth0: 10.3.1.1
  - Eth1: 10.3.4.100

- In the “dynhad.conf” file located in /usr/local/etc, we made changes to the following parameters:

Each interface has four parameters associated with it. Ha_disc determines whether or not to allow dynamic home agent discovery. A ‘0’ does not allow dynamic HA discovery. A ‘1’ allows dynamic HA discovery with broadcast messages. We chose eth1 since this was the mobile node’s home network. Agentadv has three options: ‘0’, ‘1’, or ‘-1’. A ‘0’ tells the interface not to send agent advertisements without agent solicitation. A ‘1’ sends agent advertisements regularly, which is what we chose because we wanted the home agent to constantly send out advertisement so we could debug. A ‘-1’ does not send any agent advertisements (even solicited). Force_IP_addr is the local address to be forced for this interface. By not using this parameter the primary address of the interface is used by default.

```
INTERFACES_BEGIN
#interfaces      ha_disc      agentadv      interval      force_IP_addr
eth1                1              1              10
INTERFACES_END
```

The network access identifier is a unique identifier for the home agent. This is needed if private address space is used in the home network, which was the case in our thesis.

```
NetworkAccessIdentifier “test”
```

Triangle tunnel means that the packets to the mobile nodes are sent via the home agent, but packets from the mobile node are routed directly to the destination. We set this to false because it is not possible to use triangle and reverse concurrently. The problem with triangle tunneling is that since all packets from the mobile node are routed directly then if the mobile node tries to communicate with a node in its home network most firewalls will reject those packets.

```
EnableTriangleTunneling FALSE
```

Reverse tunneling means bi-directional tunneling in which both the sent and received packets from the mobile node are sent via the home agent. The home agent intercepts all packets destined to and from the mobile node and forwards them on to their destination. We used reverse tunneling since this is what Secure Mobile IP requires because all packets to and from the mobile node are handled by the HA.

EnableReverseTunneling TRUE

This is the list of MNs that our HA accepts with a unique SPI number of 1000. The SPI is the key identifier for the MN.

AUTHORIZEDLIST_BEGIN

1000 10.3.4.6

AUTHORIZEDLIST_END

2. Foreign Agent

The following configurations for the foreign agent are:

- IP Addresses
  - Eth0: 10.3.2.1
  - Eth1: 10.3.3.100
- In the "dynfad.conf" file located in /usr/local/etc, we made changes to the following parameters:

This parameter shows the interfaces that are used for Mobile IP services. The "interfaces" column is the name of the interface(s) that is being used. The column "type" could be one of the following:

1 = both upper and lower direction

2 = only upper direction (to upper FA/HA)

3 = only lower direction (to lower FA/MN)

We decided to have interface eth0 communicate in both directions and have eth1 only send data to the MN. This allowed us to receive data packets from the HA on eth0 and forward them to interface eth1, who forwarded them on to the MN. The column "agentadv" is used to define whether or not agent advertisements should be sent on the interfaces. We left them to be 1, which indicates to send agent advertisements regularly. The column "interval" defines the number of seconds to wait between two agent advertisements. We set this to be 10 to allow for faster detection of attachment point by the MN. The "force_IP_addr" column is used to define a local address for the interface. We did not need to do use this option so we left it blank. By doing this, the primary address of the interface was used.

```
INTERFACES_BEGIN
#interface      type    agentadv        interval        force_IP_addr
eth0            1       1               10
eth1            3       1               10
INTERFACES_END
```

The "NetworkAccessIdentifier" parameter is used as the unique identifier for the FA. This can be any string. For simplicity, we chose the string "test".

```
NetworkAccessIdentifier "test"
```

The "HighestFAIPAddress" parameter is used as the IP address of the HFA or FA, used to communicate with the HA. For our implementation, we had this set to be eth0, which was 10.3.2.1.

```
HighestFAIPAddress 10.3.3.100
```

This parameter defines whether or not FA Decapsulation is being used. For our first trial implementation, we used FA Decapsulation.

```
EnableFADecapsulation TRUE
```

The parameter "EnableTriangleTunneling" defines how the packets are routed. If this is enabled, then packets sent to the MN are sent through the HA, but packets from the MN are routed directly to their destination. For our trial implementation, we did not want

to use Triangle Tunneling because we wanted to create a tunnel between the FA and the HA, causing all traffic to flow between them.

EnableTriangleTunneling FALSE

This parameter is used for bi-directional tunneling, which means that packets to and from the MN are sent through the HA. This allowed us to create the tunnel between the HA and the FA.

EnableReverseTunneling TRUE

The steps that we took to start the foreign agent are:

- Run the setup script, "/usr/local/sbin/dynamics-fa-setup"
    - Enables the user to set parameters such as HighestFA IP address and what type of tunneling to use. Those values are written into the file "dynfad.conf".
- Run the command, "/usr/local/sbin/rsakeygen 728"
    - This command generates a RSA key and stores it in a file. It is used to generate keys for FAs, to use in authentication.
- Run the foreign agent daemon, "/usr/local/sbin/dynfad --fg --debug"
    - This allows the foreign agent to run in the foreground in debug mode.
- Run the foreign agent tool, "/usr/local/sbin/dynfa_tool"
    - This is a tool that has command line user interface that shows the status of the Mobile IP service. Commands within the user interface such as "tunnels" and "st" allow users to see if there any tunnels were created and update the status of the service.

Once we had the tool up and running, we used the command "st 1" to get a constant update of the parameters such as "tunnels", "request accepted", "request rejected", which were the most important parameters to check. We were looking for the

"tunnels" parameter to change from 0 to 1 and we were also looking for the "request accepted" parameter to increase. Once we saw that these certain parameters were changing, we were able to assess that the implementation was working.

3. Mobile Node

The following configurations for the mobile node are:

- IP Address: 10.3.4.6
- In the "dynfad.conf" file located in /usr/local/etc, we made changes to the following parameters:

The mobile node's IP address in the home network.

MNHomeIPAddress 10.3.4.6

The IP address of the mobile node's home agent.

HAIPAddress 10.3.4.100

The home agent network access identifier (NAI) is used to match the HA agent advertisements when a MN is determining whether it is at home or not. This is mainly used with private HA addresses.

HANetworkAccessIdentifier "test"

This enables the foreign agent to decapsulate the IP-within-IP encapsulated IP packets. If this is set to false then the mobile node decapsulates the IP packets. In secure Mobile IP MN Decapsulation is required as described in chapter II, the Mobile IP chapter.

EnableFADecapsulation TRUE

The HomeNetPrefix is the network address of the home network.

HomeNetPrefix 10.3.4.0/24

This selects the tunneling mode to be used. A 1 is automatic, but prefer reverse tunneling, a ‘2’ is automatic, but prefer triangle tunnel, a ‘3’ accepts only reverse tunnel and ‘4’ accepts only triangle tunnel

TunnelingMode 4

C. ARCHITECTURE OF MOBILE IP WITH IPSEC

The implementation with IPSec did not involve dramatic changes (Figure 31). The only changes we made to our set up are as follows:

- Both the Home Agent and Foreign Agent are now configured to be DHCP Servers. The home agent gives out addresses in the range 10.3.4.25 – 10.3.4.50. The foreign agent gives out addresses in the range 10.3.3.25 – 10.3.3.50.
- The Mobile Node is set up as a DHCP client instead of having a static address.

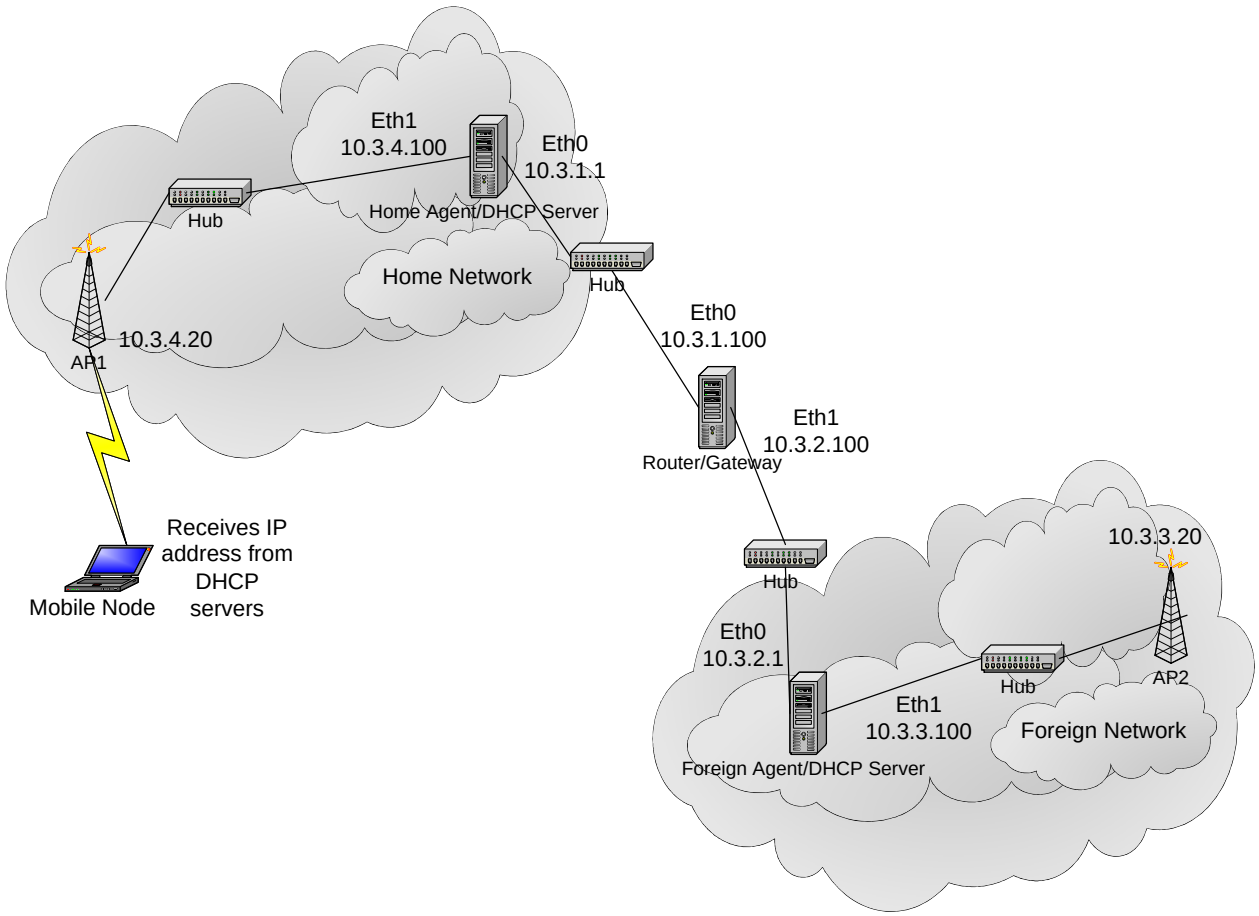

Figure 31. Network Setup with DHCP and IPSec

We also had to make changes to the configuration files. Those changes are as follows:

- Home Agent
    - In the “dynhad.conf” file, we changed the following parameters:

We needed to have reverse tunneling in order to create the tunnel between the MN and the HA. Triangle tunneling does not allow us to do so. Therefore, we set this parameter to be FALSE.

EnableTriangleTunneling FALSE

Enables a tunnel to be created between the MN and the HA. Communication will be able to flow directly between the two, which is needed for IPSec tunnel to be used with this implementation.

EnableReverseTunneling TRUE

- Foreign Agent
    - In the "dynfad.conf" file, we changed the following parameters:

By using IPSec within Mobile IP, the tunnel needs to be established between the MN and the HA. Therefore, MN Decapsulation is needed for this implementation. This allows communication directly between the MN and the HA. The IPSec tunnel will provide the security of communication between the HA and MN.

EnableFADecapsulation FALSE

Triangle Tunneling does not enable the tunnel to be established between the MN and the HA. Therefore, we set this parameter to FALSE.

EnableTriangleTunneling FALSE

Reverse Tunneling allows the tunnel to be established between the MN and the HA. With this parameter set to TRUE, all communication to and from the MN goes through the HA.

EnableReverseTunneling TRUE

- Mobile Node
    - In the "dynmnd.conf" file, we changed the following parameters:

MNHomeIPAddress 10.3.4.25 # which was the DHCP assigned address

FA Decapsulation does not work with what IPSec was providing. In order for the MN to decapsulate the packets, we had to set this parameter to FALSE. This allows direct communication between the MN and the HA.

EnableFADecapsulation FALSE

This parameter means that the MN will only accept reverse tunneling. This allows the MN to directly communicate with the HA. Reverse tunneling allows the MN to create a tunnel with the HA. To implement IPSec with this implementation, direct communication between the HA and the MN is essential.

TunnelingMode 3

1. IPsec Implementation

In order to implement setup Secure Mobile IP with dynamics on a Linux machine, it is necessary to use an IPSec implementation. For this we decided to research FreeS/Wan, which is free and the source code is provided [LIN1]. FreeS/Wan stands for "free secure WAN" and is the result of a project started by John Gilmore, who wanted to make an IPSec implementation for Linux available for free. FreeS/Wan works with RSA and is easy to configure. For each IPSec node an RSA key pair has to be created and the allowed connections have to be described in a configuration file. In Secure Mobile IP implementation FreeS/Wan would do the following:

- Negotiate keys between MN and Home Firewall
- Establishing secured tunnels between MN and Home Firewall
- Encrypting and authenticated all data between MN and Home Firewall.

2. Dynamics in Secure Mobile IP

In Secure Mobile IP implementation, the job of Dynamics Mobile IP would be the following:

- Handling agent advertisements (home and foreign)
- Establishing Mobile IP tunnels between HA and MN
- Capturing and redirecting packets for MN on the home network.

D. INITIAL TRIAL

Initially, we conducted the Mobile IP implementation using the wired interface instead of wireless with both static IPs and dynamic IPs for the mobile node. We used a D-Link Ethernet card for the mobile node. We faced some difficulty at first (see Problems section) but we finally were able to find the configuration parameters that allowed us to move on to try wireless. Once we saw that the tunnels were correctly getting built and torn down, we knew that we could move on.

E. WIRELESS

After our initial trial, wireless was trivial. The only problem that we had with it was that we had to reactivate the wireless Ethernet card every time we entered a different subnet. This was an annoyance, but we determined that it was not because of the Mobile IP implementation but rather, it was a problem with the OS drivers. Other than that, performing the implementation wirelessly worked like the initial wired trial.

F. DIFFICULTIES ENCOUNTERED

We believe anyone trying to implement Mobile IP will find this section most useful. We found that when searching through many documents, the problems section was most useful because it contained similar problems that others were experiencing. This section will cover the problems we encountered. Some of the problems we faced were not directly associated with Mobile IP. However, it is important to point out these problems, as they are necessary steps in getting Mobile IP to work.

1. Installing the Wireless Card

The first problem we ran into was setting up the wireless card on the MN. We installed the latest driver for the wireless card, linux-wlan-ng-0.1.16-pre9.tar.gz. The implementation chapter discusses the necessary steps to install the card. After the installation, we were unable to communicate on the network. We edited the /etc/stab file with the following changes:

```
Socket 0:  Instant Wireless Network PC Card
0              network Orinoco_cs      0       eth0
```

Initially, Socket 0 did not contain any information. After inserting this information into the parameter and rebooting, the NIC card was able to communicate on the network.

2. Problems with Dynamics

In Redhat 7.3, ipchains is loaded and runs by default. The ipchains module is contained in Linux Kernel versions 2.1.102 and above, and is required to administer IP packet filters. With a full-installation, it incorporates firewall rules automatically into the operating system. In Linux kernel versions 2.4.x and above, ipchains is replaced by iptables, which has the same functionality. However, iptables does not automatically include filtering rules during installation. Redhat 7.3 was installed on our router and Redhat 8.0 was installed on our agents.

Running the command 'ipchains –L' shows the configured filtering rules. Since our router loaded ipchains by default, it was necessary to turn it off to allow all packets through. The command, 'ipchains –F' disabled the filtering rules and allowed all packets through, including the Mobile IP registration packets.

Another difficulty we faced was with the assignment of the CCOA using DHCP in MN Decapsulation mode. In the Mobile IP protocol, when the CCOA gets assigned to the MN, it is considered to be the endpoint of the tunnel. However, this was not the case in Dynamics. The endpoint of the tunnel was assigned as the IP address of eth1 on the FA (Figure 31). During registration, the MN should communicate directly to the HA. Using the 'dynha_tool' tool we were able to determine if the tunnels were up and if there were any errors. The tool reported the tunnel (tunl0) with an IP address of 10.3.4.25. However, we were unable to communicate through the tunnel interface. Upon further observation, 'dynha_tool' reported the warning message 'Registration for this FA failed, trying to find a new one'. This showed that the MN was trying to register through the FA, which was not supposed to happen.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS

A. MOBILE IP CONCLUSIONS

Mobile IP is the protocol of choice to support mobility in wireless data networking, but issues such as security and performance need to be improved in order for it to become more widely accepted. It solves many questions about mobility, but it also introduces a lot of questions about security, including data privacy, data integrity and authentication. Our research focused on security enhancements for Mobile IP. The specific security enhancement that we chose was IPSec within Mobile IP.

We used the Dynamics-HUT implementation of Mobile IP and Marc Danziesen's version of Secure Mobile IP (SecMIP), to conduct our research. We explored each implementation thoroughly by setting up a small Mobile IP network. This enabled us to examine how Mobile IP operated.

Setting up the small network seemed trivial, at first glance, but we encountered many difficulties along the way. Issues such as poor documentation and dysfunctional network card driver made it difficult to get started. Once we had all the hardware and operating systems set up, we ran into further difficulties.

Installing the Dynamics-HUT Mobile IP implementation was not very difficult but we encountered many difficulties in running it correctly. Since the documentation on the implementation was scarce, we had to figure things out as we went along. We did find other sources that implemented Mobile IP using Dynamics, which helped. Using other sources was the key to figuring out how to make it run correctly.

We first ran the Mobile IP implementation without wireless interface. This enabled us to check that the implementation ran correctly. After several trials, and after fixing several problems, we switched over to the wireless interface. Running the implementation wirelessly did not pose any big problems for us. We ran into minor issues, which were more of a hassle than problems. Once we were able to run the Mobile IP implementation, we were ready to incorporate IPSec.

To incorporate IPSec, we had to make a few changes to the configurations of the computers and configurations of the Mobile IP implementation. Making those changes was not a problem. Our problem was getting the Mobile IP implementation to run correctly with the new settings.

Mobile IP supports mobility in every sense of the word. It allows mobile nodes to roam different networks without losing communication, while keeping the same IP address. The speed of technology will only make this protocol better and more widely used. Incorporating security functions will provide confidence to users of it. In time, Mobile IP will continue to progress and improve.

B. FUTURE WORK

People everywhere are catching on to the world of wireless. People want to be connected anywhere, any time. The growth of technology has enabled wireless devices to be evermore popular. However, there are many areas in which Mobile IP require research. Some of them include:

- Integrated security in Mobile IP
- Mobile IP Continuous Streaming Data
- Mobile IP implementation strategy
- Mobile IP Scalability Measurement Issues
- Mobile IP and IPSec

To implement a more secure wireless data network than is currently supported by Mobile IP, the IPSec tunnel needs to surround the Mobile IP tunnel, providing integrity, authentication and data privacy, wirelessly over a network. The data packets can then be delivered with confidence without sacrificing security.

Wireless mobility is a growing demand. And, as technology gets more advanced, the ability to stay connected any where, any time, will be realized. Each one of these areas of research could potentially enhance the functionality and performance of Mobile IP.

LIST OF REFERENCES

[3CO] 3COM, *Understanding IP Addressing*. http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf, June 2001

[ALE] Alesso, Peter H. The Intelligent Wireless Web. Boston: Addison-Wesley, 2002.

[BOR1] Borisov, Nikita., Goldberg, Ian., & Wagner, David. *Intercepting Mobile Communications: The Insecurity of 802.11 Draft*, 2001.

[BOR2] Borisov, Nikita., Goldberg, Ian., & Wagner, David. *Security of the WEP Algorithm.* http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html, June 2003

[BRA] Braun, H-W. Models of Policy Based Routing. RFC1104, 1989

[CLA] Clark, D. Policy Routing in Internet Protocols. RFC1102, 1989

[COM] Comer, Douglas E. *Internetworking with TCP/IP Principles, Protocols, And Architectures.* New Jersey: Prentice Hall, 2000.

[DAN] Danzeisen, Marc & Braun, Torsten. *Access of Mobile IP Users to Firewall Protected VPNs.* Unpublished masters thesis, University of Bern, Bern, Switzerland.Dynamics Mobile IP documentation, http://www.cs.hut.fi/Research/Dynamics/, June 2003

[ETH] Ethereal. *http://www.ethereal.com*, June 2003.

[FOR] Forsberg, Dan. *Communication Availability with Mobile IP in Wireless LANs*, Master's Thesis, Helsinki University of Technology.
Dynamics Mobile IP documentation, http://www.cs.hut.fi/Research/Dynamics/, June 2003

[GDB] Goldberg, Ian & Wagner, David. *Analysis of 802.11 Security or Wired Equivalent Privacy : Isn't.*

[GEI] Geier, Jim. WEP Tutorial. *802.11 WEP Concepts and Vulnerability* http://www.80211-planet.com/tutorials/article.php/1368661, June 2003

[HUB] Hubert, Bert. *Linux Advanced Routing & Traffic Control HOWTO*. http://www.lartc.org., June 2003.

[ITF] http://www.ietf.org/rfc.html, June 2003

[JAR] Jarvi, Antero. *Mobile IP Introduction Security Issues.* http://staff.cs.utu.fi/courses/computer_and_network_security/spring_2000/MIP.pdf, June 2003.

[JUP] Juptner, Olaf (2002). Mcommerce transactions to hit USD25 billion http://www.e-gateway.net/infoarea/news/news.cfm?nid=2262, June 2003

[LIN1] Linux FreeS/Wan documentation,

[LIN2] Linux Online, *Linux IPCHAINS-HOWTO.* http://www.linux.org/docs/ldp/howto/IPCHAINS-HOWTO.html, June 2003.

[MAL] Malinen, Jouni K. *Using Private Addresses with Hierarchical Mobile IPv4*, Master's Thesis, Helsinki University of Technology
Dynamics Mobile IP documentation, http://www.cs.hut.fi/Research/Dynamics/, June 2003

[MAR] Marsh, Matthew G. Policy Routing with Linux – Online Edition. http://www.policyrouting.org/PolicyRoutingBook/ONLINE/TOC.html, June 2003

[MEN] Mendez-Wilson, Deborah. Not Playing the Same Old War Games. *http://www.wirelessweek.com/index.asp?layout=article&articleid=CA72183.*, June 2003.

[MUR] Murhammer, Martin W. *A Guide to Virtual Private Networks*. pp. 47-49, 51-55, 56-57, 71. New Jersey: Prentice Hall, 1998.

[NIC] Nichols, Randall K. *Wireless Security:Models, Threats and Solutions,* pp. 11, 334, 374-375, 377, 378. New York: McGraw-Hill, 2001.

[NOR1] Norris, Mark. *Mobile IP: Technology for M-Business*. Massachusetts: Artech House, Inc., 2001

[NOR2] Northcutt, Stephen. *Inside Network Perimeter Security.* Indianapolis: New Riders.

[PER1] Perkins, Charles E. *Mobile IP: Design Principles and Practices*. pp. 55-92, 194. Massachusetts: Addison Wesley., 1998.

[PER2] Perkins, Charles. *IP Mobility Support*, rfc2002., 1996

[PRU] Pruitt-Billingsley. *Analysis Of Digital Cellular Standards.* pp.3-4. Unpublished Masters Thesis, Naval Postgraduate School, Monterey, California, USA, 1996.

[RAD] RAD, http://www2.rad.com/networks/1994/err_con/crc.htm, June 2003.

[SCT] Erwin, M., Scott, C., and Wolfe, P., "Virtual Private Networks" 2nd Edition, O'Reilly, 1999

[SEC] Security Focus. http://www.securityfocus.com/tools/243, Jun 2003.

[SIG] Singhal, Dr. Sandeep K. *Understanding Wireless LAN Security*, 2001

[SKE] Skedd, Kirsten. *Wireless Phones, Pagers and Modems to Surpass PCs as Most Popular Internet Access Devices.* http://www.instat.com/pr/2001/md0006md_pr.htm, June 2003.

[SNI] Sniffer Technologies, Network Associates. http://www.networkassociates.com/us/products/sniffer/home.asp June 2003.

[SOL] Solomon, James D. *Mobile IP: The Internet Unplugged.* New Jersey: PTR Prentice Hall, 1998.

[STU] Stubblefield, Adam. Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. August 6, 2001 http://www.cs.rice.edu/~astubble/wep/wep_attack.html, June 2003

[SUN] Sun Microsystems, Technical White Paper, *Dynamic Host Configuration Protocol.* wwws.sun.com/software/whitepapers/solaris9/dhcp.pdf, June 2003

[TAR] Dynamic Host Configuration Protocol http://www.tarunz.org/~vassilii/TAU/protocols/dhcp/timeline.htm, June 2003

[TIM] TimeStep, *Understanding the IPSec protocol suite*, pp. 19-23. 1998.

[YAN] Yan, Henry C., Lei, Zan, Zhang, Li, Yee, Kien-Yeng, Huang and Yu-Ren, "Report for Mobile IP Project".

[YGL] Cellular Glossary http://www.ecellularconnection.com/c_glossary.htm, June 2003

[YHL] Mobile Services Switching Center
http://glossary.its.bldrdoc.gov/fs-1037/dir-023/_3347.htm, June 2003

[YJL] Making IPSec Work For You
http://www.networkcomputing.com/922/922ws2side1.html, June 2003

[YKL] The Remote Access Conundrum Part 1: Extended Authentication
http://www.isp-planet.com/technology/remote_access_conundrum-1-1.html, June 2003

[YMJ] What is ‘forward secrecy’?
http://www.itsecurity.com/asktecs/may201.htm, June 2003

[YNJ] IP Packet Header
http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/ip-packet.html, June 2003

[YOJ[General Information and hardware requirements
http://r703a.chem.nthu.edu.tw/~ks/linux/howto/PCMCIA-HOWTO-3.html, June 2003

[YPJ] Dynamic Host Configuration Protocol
http://www.linktionary.com/d/dhcp.html, June 2003

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Dr. Ernest McDuffie
   National Science Foundation
   Arlington, VA

4. RADM Zelebor
   N6/Deputy DON CIO
   Arlington, VA

5. Russell Jones
   N641
   Arlington, VA

6. David Wirth
   N641
   Arlington, VA

7. CAPT Sheila McCoy
   Headquarters U.S. Navy
   Arlington, VA

8. CAPT Robert Zellmann
   CNO Staff N614
   Arlington, VA

9. Dr. Ralph Wachter
   ONR
   Arlington, VA

10. Dr. Frank Deckelman
    ONR
    Arlington, VA

11. Richard Hale
    DISA
    Falls Church, VA

12. George Bieber
OSD
Washington, DC

13. Deborah Cooper
DC Associates, LLC
Roslyn, VA

14. David Ladd
Microsoft Corporation
Redmond, WA

15. Marshall Potter
Federal Aviation Administration
Washington, DC

16. Ernest Lucier
Federal Aviation Administration
Washington, DC

17. Keith Schwalm
DHS
Washington, DC

18. RADM Joseph Burns
Fort George Meade, MD

19. Howard Andrews
CFFC
Norfolk, VA

20. Steve LaFountain
NSA
Fort Meade, MD

21. Penny Lehtola
NSA
Fort Meade, MD

22. Dr. George Dinolt
NPS
Monterey, CA

23. Dr. Gurminder Singh
NPS
Monterey, CA

24. Romelo B. Nafarrete
Civilian, Naval Postgraduate School
San Diego, CA

25 Lionel J. Valverde
Civilian, Naval Postgraduate School
Salinas, CA