İSTANBUL TECHNICAL UNIVERSITY ★ INSTITUTE OF SCIENCE AND TECHNOLOGY

MOBILE IP AND SECURITY

M.Sc. Thesis by
Şerif BAHTİYAR, B.Sc.

Department : Computer Engineering

Programme: Computer Engineering

MAY 2004

İSTANBUL TECHNICAL UNIVERSITY ★ INSTITUTE OF SCIENCE AND TECHNOLOGY

MOBILE IP AND SECURITY

M.Sc. Thesis by
Şerif BAHTİYAR, B.Sc.

(504011415)

Date of submission : 20.04.2004

Date of defence examination: 04.05.2004

Supervisor (Chairman): Prof. Dr. Bülent ÖRENCİK

Members of the Examining Committee Assoc. Prof. Dr. Coşkun SÖNMEZ (İ.T.Ü.)

Assoc. Prof. Dr. Erdal ÇAYIRCI (İ.T.Ü.)

MAY 2004

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

GEZGİN IP VE GÜVENLİK

YÜKSEK LİSANS TEZİ
Müh. Şerif BAHTİYAR
(504011415)

Tezin Enstitüye Verildiği Tarih : 20 Nisan 2004
Tezin Savunulduğu Tarih : 4 Mayıs 2004

Tez Danışmanı :	**Prof. Dr. Bülent ÖRENCİK**
Diğer Jüri Üyeleri	**Doc. Dr. Coşkun SÖNMEZ (İ.T.Ü.)**
	Doc. Dr. Erdal ÇAYIRCI (İ.T.Ü.)

MAYIS 2004

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my thesis supervisor Professor Bülent Örencik for his invaluable guidance, support, suggestions, motivation and encouragement during the preparation of this dissertation.

I am grateful to my all professors in Istanbul Technical University who have been thought me both scientific approaching and hard working.

I would like to thank my friends, valuable people of TÜBİTAK UEKAE and especially members of IP Group for their close friendship and kind support during my M.Sc. study. Particularly, my thanks go to my project manager Oktay Adalıer for his support and vast tolerance. Special thanks to my colleague and my friend Cenk Özden, who helped me to construct the testpad. Also, I would like to express my thanks to my friend and colleague Şenol İşçi, who helped me to correct grammar mistakes.

And finally thanks to my family for their encouragement and precious help.

May 2004 Şerif BAHTİYAR

TABLE OF CONTENTS

ABBREVIATIONS

IP : Internet Protocol
IPv4 : Internet Protocol version 4
IPv6 : Internet Protocol version 6
OSI : Open System Interconnection
DoD : U.S. Department of Defense
IETF : Internet Engineering Task Force
IPSec : IP Security Protocol
VPN : Virtual Private Network
TCP/IP : Transmission Control Protocol/Internet Protocol
ICMP : Internet Control Message Protocol
ARP : Address Resolution Protocol
TCP : Transmission Control Protocol
UDP : User Datagram Protocol
HTTP : HyperText Transfer Protocol
FTP : File Transfer Protocol
SNMP : Simple Network Management Protocol
DNS : Domain Name System
SMTP : Simple Mail Transfer Protocol
DARPA : Defense Advanced Research Projects Agency
UCLA : University of California at Los Angeles
UCSB : University of California an Santa Barbara
PSN : Packet-Switched Node
MILNT : Military Network
IPng : next-generation Internet
PDU : Protocol Data Unit
SSRR : Strict Source and Record Route
CDPD : Cellular Digital Packet Data
Mobile IPv4 : Mobile IP version 4
GRE : Generic Routing Encapsulation
IGMP : Internet Group Management Protocol
MTU : Maximum Transfer Unit
Mobile IPv6 : Mobile IP version 6
AH : Authentication Header
ESP : Encapsulating Security Payload
SA : Security Association
SPI : Security Parameter Index
SSH : Secure SHell
SCP : Secure CoPy
SSL : Secure Socket Layer
S-HTTP : Secure HyperText Transfer Protocol
WWW : World Wide Web
VPN : Virtual Private Network
AAA : Authentication, Authorization, Accounting
DMZ : De-Militarized Zone

ACL **:** Access Control List
AAAL **:** Local Authority
AAAH **:** Home Authority
MN **:** Mobile Node
FA **:** Foreign Agent
HA **:** Home Agent
ISP **:** Internet Service Provider
SecMIP **:** Secure Mobile IP
GPRS **:** General Packet Radio Service
NCG **:** Network Crypto Gate
PSTN **:** Public Switched Telephone Network
aHA **:** Intranet Home Agent
eHA **:** Internet Home Agent
CN **:** Correspondent Node
HSI **:** Header Size Increase
THS **:** Total size of headers on a packet
SIPHS **:** Standard IP Header Size
DES **:** Data Encryption Standard
MD5 **:** Message Digest 5
IKE **:** Internet Key Exchange
LAN **:** Local Area Network
MAN **:** Metropolitan Area Network
WAN **:** Wide Area Network
UTP **:** Unshielded Twisted Pair
Mbps **:** Mega bit per second

LIST OF TABLES

Page No

LIST OF FIGURES

GEZGİN IP VE GÜVENLİK

ÖZET

Yirminci yüzyılın ilk yarısından sonra, en önemli devrimlerden biri bilgisayar ağları olmuştur. Bunların modern yaşamdaki önemi gün geçtikçe artmaktadır. Bilgisayar ağlarının yaygın kullanımının güdüsü, insanların genel ve ortak çıkarları için haberleşme gereksiniminden kaynaklanmaktadır. Dünyadaki en büyük ağlardan biri olan Internet, bu gereksinimleri karşılamak amacıyla tasarlanmıştır.

Internet kullanıcılarının yeni gereksinimlerinden biri olan gezginlik, teknolojinin hızlı ilerlemesi sonucu ortaya çıkmıştır. Gezginlik, bir düğümün bağıntı noktasını değiştirirken, mevcut haberleşmelerini sürdürebilme yeteneği olarak tanımlanmaktadır. Bilgisayar tabanlı haberleşme sistemlerinde, gezginliği sağlamak için OSI referans modelinin veya DoD referans modelinin tüm katmanları gezginliği desteklemesi gerekir. Ancak, bu tezde sadece dünya çapında gezginliği sağlamada en önemli katmanlardan biri olan ağ katmanı gezginliği üzerinde çalışılmıştır.

Internet kullanıcılarının diğer bir yeni ihtiyacı da güvenliktir. Bilgisayar haberleşme ağlarının güvenliğini sağlama ile ilgili bir çok yöntem vardır, fakat en yaygın olanı IPSec'tir. IPSec, sistemin ihitiyacı olan protokolü seçmeyi sağlayan, servisler için kullanılmak istenen algoritmayı belirleyen ve istenilen servis için gereksinim duyulan kriptografik anahtarları arzeden bir çözümdür.

Farklı cihazlar üzerinde çalıştırılan Gezgin IP ve IPSec, ağlar arasında sınırlı gezginlik gibi problemlere sebep olmaktadır. Bunların sebebi, protokollerin doğasından kaynaklanmaktadır. Bundan dolayı, IPSec kullanan sistemlerde gezginliğin görünmezliğinin sağlanma ihtiyacı vardır.

Bu tezde, Internet ve Intranette gezginliğin ve güvenliğin biribirine görünmez olduğu yeni bir mimari önerilmiştir. Bu mimaride, standart protokollerin özelliklerinden ve yeni mimari ile gelen özelliklerden yararlanılmıştır. İlk önce, önerilen yeni mimari sunulmuş ve mimarinin özellikleri tanımlanmıştır. Sonra, mimari ile ilgili muhtemel senaryolardan söz edilmiştir. Son olarak, önerilen mimari, senaryolar doğrultusunda paket boyu, yük ve güvenlik yönünden analiz edilmiştir.

Gezgin IPv4'ün IPSec tabanlı Sanal Özel Ağ Geçidinin olduğu bir sistemde gezmesine yönelik önerilen mimarinin sunumu ve analizine ek olarak, Gezgin IPv6'nin IPSec tabanlı Sanal Özel Ağ Geçidinin olduğu bir sistemde gezmesine yönelik oluşturulabilecek bir mimarinin gereksinimleri belirlenmiştir. Bunun amacı Gezgin IPv6 ile IPSec'in bir sistemde problemsiz bir arada var olmalarını sağlayacak çalışmaların başlangıcını oluşturmaktır.

Internet ve Intranette gezginliği ve güvenliği sağlamaya yönelik oluşturulacak efektif bir mekanizma için daha yapılacak çok iş vardır. Örneğin, IPSec ve Gezgin IPv4 birbirleri ile uyumlu değildir. Ancak gezginlik ve güvenlik bu protokollerin ikisine de ihtiyaç duymaktadır. Dolayısıyla, IPSec ve Gezgin IPv4'ün aynı sistemde bulunmalarına yönelik yeni çözümlere ihtiyaç vardır. Ayrıca, önerilen yeni

mimarinin gerçeklenmesi gelecekte yapılması gereken işlerden biridir. Bir de yeterli bir ağ sezme algoritması tasarlanmalıdır. Bunlara ek olarak, yönlendirme işleminin optimizasyon çalışmaları sürdürülmelidir. Ayrıca, belirlenen gerekler doğrultusunda Gezgin IPv6'ya yönelik yeni mimariler gerçeklenebilir. Diğer taraftan, gezginliği ve güvenliği sağlamaya yönelik yeni çözümler, Gezgin IPv6 ve IPv6 güncellenerek bulunabilir.

Önerilen mimarinin daha iyi anlaşılması için bir benzetim yazılımı hazırlanmıştır. Benzetim yazılımın koşması, bir senaryo örneği üzerinde açıklanmıştır.

MOBILE IP AND SECURITY

SUMMARY

Computer networks have been one of the most significant revolution of twentieth century. They have come to play an increasingly important role in modern life. The motivation for the widespread use of computer networks has been the need for communication between people for their common and shared interests. One of the biggest networks, which network is the Internet, was designed to meet these requirements.

Due to the rapid technological progress, the services demanded by Internet users introduce new requirements such as mobility that can be described as the ability of a node to change its point-of-attachment from one link to another while maintaining its all-existing communications. To ensure complete mobility for a computer communication system, all layers of OSI reference model or DoD reference model must support mobility features. However, the motivation of this thesis is the impact at mobility to the Network Layer of OSI reference model.

Security is another requirement due to the new services. There are various security mechanisms to protect computer communication networks; however, the most popular one is IPSec. The IPSec provides security services at the IP layer by enabling the system to select required security protocols, determine the algorithms to use for the services, and put in place any cryptographic keys required to provide the requested services.

Using Mobile IP and IPSec on different devices causes problems such as limited mobility between different networks. The reasons for these are related with the nature of the protocols. Therefore, there is a need to support seemless mobility in systems that use IPSec.

In this thesis, a new architecture to establish seemless mobility and security both in the Intranet and in the Internet by using and by adding new features to standard communication protocols was presented. First, the new architecture was presented and its properties were described. Then, several scenarios for this architecture were discussed. And finally, the scenarios were analyzed with respect to message size, overhead and security properties.

In addition to proposal and analysis a new architecture of Mobile IPv4 traversing IPSec based VPN Gateway, requirements of possible solutions for Mobile IPv6 traversing IPSec based VPN Gateway were established. The aim of this is to start the work for coexistence of both Mobile IPv6 and IPSec in a system without any problem.

It needs great effort to establish efficient mechanism for accommodating both security and mobility in the Internet and in the Intranet. For instance, IPSec and Mobile IPv4 are not compatible with each other. However, mobility and security features necessitate both of them. Therefore, new solutions for coexistence of both

IPSec and Mobile IPv4 in same system are needed. On the other hand, future works have to be carried on realizing the new architecture. A sufficiently secure network detection algorithm should be designed. In addition to these, researches on routing optimization may be carried on. Also, new architectures can also be designed to use with Mobile IPv6 according to requirements. On the other hand, new solutions should be found to ensure security and mobility worldwide with updating Mobile IPv6 and also IPv6.

Simulation software that was used to simulate the proposed architecture was introduced. Moreover, the explanation of execution of the software in respect of one scenario was given.

1. INTRODUCTION

Nowadays, the Internet has become a universal network [1] that allows full connectivity, and that is accessible from various networks. The network layer protocol of the Internet is Internet Protocol (IP), which has two main versions, IPv4 [2] and IPv6 [3]. As the number of Internet users increase, expectations of them become different. The main two expectations are security and mobility. Security of a node is related with all communication layers [1] of a computer network, and there are different mechanisms to protect each of them. The second main expectation of Internet users are mobility which has become popular after wireless technologies have been deployed such as 802.11b, Bluetooth, and etc.

To ensure complete mobility for a computer communication system all layers of OSI [4,5] reference model or DoD [4,5] reference model must support mobility features. However, the motivation of this thesis is mobility on Network Layer. "In the Internet, mobility is the ability of a node to change its point-of attachment from one link to another while maintaining its all existing communications and using the same IP address at its new link"[6]. Normally, a node may not move from one link to another if it wants to continue its ongoing communications without changing the network-prefix portion of its IP address. Mobile IP that is an ongoing effort under Internet Engineering Task Force (IETF) towards an Internet Standard is a mobility solution only for the network layer. Mobile IPv4 defines extension mechanisms on the top of existing IPv4 to allow transparent routing of IP datagram between a Mobile Node and its Corresponding Node when the Mobile Node changes its point-of attachment in the Internet.

There are different security mechanisms to protect Internet Layer (Network Layer). However, the most known is the IP Security Protocol (IPSec), which protocol is used in this thesis to support security on the proposed architecture. IPSec is a protocol proposed by the IETF as a standard protocol. The IPSec provides security services at the IP layer by enabling a system to select required security protocols, determine the

algorithms to use for the services, and put in place any cryptographic keys required to provide the requested services.

Using Mobile IP and IPSec on different devices causes problems such as limited mobility between different networks. The reasons of these are related with the nature of these protocols. Therefore, there is a need to support seemless mobility in systems that use IPSec. In this thesis, the architecture of Mobile IPv4 traversing IPSec based VPN Gateways that ensures seemless secure mobility is proposed, and the simulation software is realized according to the proposed architecture. Then, analytical analyses of proposed architecture are done. Moreover, design requirements of Mobile IPv6 traversing IPSec based VPN Gateways are proposed.

The thesis consists of six chapters and an appendix whose descriptions are given in following paragraphs.

The first chapter is the introduction chapter. In this chapter, the motivation of the thesis is presented. After this, the basic terms related with this topic are presented. For instance, computer networks and Internet Protocol are some of them.

In the second chapter, the basic properties of Mobile IPv4 and the properties of Mobile IPv6 are presented.

In chapter three, various security threats, protocols, and solutions related with Mobile IP are described. Generally, this section is constructed as follows. At the beginning, basics of cryptography are overviewed. Then, the security architecture for the Internet Protocol (IPSec) is described. Afterwards, other security protocols are shortly presented. Next, some key distribution mechanisms are described. Also, security threats and security solutions are presented.

In the chapter four, it is proposed a new architecture of Mobile IPv4 traversing IPSec based VPN Gateway. At the beginning of the section, related works are summarized. Analytical analysis of the proposed architecture is done after description of this architecture.

The chapter five establishes requirements of possible solution of Mobile IPv6 traversing IPSec based VPN Gateway.

Last chapter, chapter six, is devoted to conclusions and discussion. The conclusions are derived according to analyses and requirements.

In Appendix A, simulation software that was used to simulate the proposed architecture was introduced. Moreover, the explanation of execution of the software in respect of one scenario was given.

1.1 Computer Networks

Computers communicate over a network by transmitting and receiving digital information. This information consists of binary digits, called bits, which take on the values zero or one. Bits are grouped into 8-bit chunks, called bytes, which can further be grouped into bundles called frames or packets.

Before two computers can exchange packets, they must be connected by some form of physical medium, such as copper wire, optical fiber, or electromagnetic radiation (radio waves). Occasionally, the two computers will be connected by the same uninterrupted piece of physical wire or wireless link, in which case they can send packets directly. In most cases, however, the packets sent by a computer will have to traverse one or more intermediate switching devices in order to reach their final destination [5,6,7].

The merging of computers and communications has had a profound influence on the way computer systems are organized. The concept of the "computer center" as a room with a large computer to which users bring their work for processing is now totally obsolete. The old model of a single computer serving all of the organization's computational needs has been replaced by one in which a large number of separate but interconnected computers do the job. These systems are called computer networks [5].

There are two main reference models for computer networking which are The Open System Interconnection (OSI) reference model for computer networking as defined by the International Organization of Standardization (ISO). The other reference model is the DoD (U.S. Department of Defense) reference model [4,5].

The OSI model has seven layers. Each of seven layers performs a specific set of functions and in turn provides a distinct set of services to the layer above it. The rules and procedures governing the operation of the various layers are called protocols [5,6].

Each protocol in OSI model is theoretically independent of the protocols in the layers above and below it. This allows for new technologies to be incorporated into a protocol layer without affecting the other layers – so long as the service provided it is replacing. While this is the theory, efficiency and other considerations tend to cause some degree of independency between the layers.

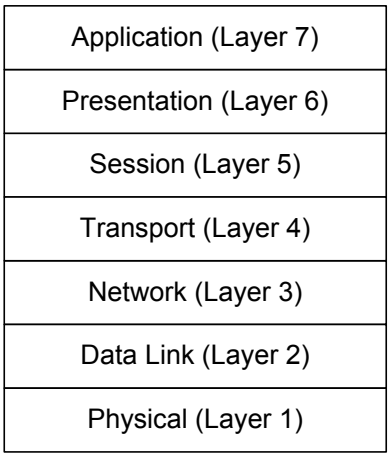

Figure 1.1. The OSI reference model

The OSI model is shown in Figure 1.1 [4,5,6]. Below it is discussed each layer of the model in turn, starting at the bottom layer.

- The physical layer moves raw bits across a communications facility, or medium. A physical-layer protocol defines the electrical and the mechanical characteristics of the medium, the bit rate, the voltage, etc.
- The data link layer uses the raw bit- transmission facility provide by the physical layer to move frames from one computer to a neighboring computer on the same link. A frame consists of a small data link-layer header plus a network-layer packet. A data-link layer protocol defines methods for ensuring the reliability of each frame and also arbitrates access to those media types which are shared by many computers.
- The network layer uses the frame-transmission facility provided by the data link layer to move packets from their original source to their ultimate destination, traversing one or more intermediate links if necessary. A packet consists of a small network-layer header plus data from the higher layer. A network-layer protocol defines how network devices discover each other and how packets are routed to their final destination.

- The transport layer is responsible for making the end-to-end packet-transmission facility provided by the network layer. The data, which flows across this reliable, end-to-end transmission facility, is generally called stream. Each individual transmission at the transport layer, called a segment, consists of a small transport-layer header plus data from a higher-layer protocol. Thus, a segment forms the payload portion of a network-layer packet. A transport-layer protocol defines the methods for detecting errors in the transmission of segments and for correcting them when they occur.
- The session layer takes the reliable stream provided by the transport layer and delivers rich, application-oriented services to the higher layers. Some session-layer protocols, for example, provide periodic checkpoints, to which communications can be resumed in the event of a catastrophic network failure. This is useful when sending very large files over unreliable networks, where restarting the entire transmission from the beginning would be extremely wasteful of network resources.
- The presentation layer defines the syntax and semantics of the information being exchanged by an application. This means that a presentation-layer protocol defines how the integers, text messages, and other data of an application are to be encoded and transmitted over the network. This allows all computers of varying hardware and operating systems to exchange information, regardless of their own particular method of storing such data.
- The application layer provides the transfer of information that is specific to the computer program being run by a user. Some application-layer protocols define how electronic mail is to be exchanged. Some application layer protocols define how files are to be transferred from one computer to another, and some define World Wide Web pages are to be fetched form a web server by a web client.

The Internet model of communications, as embodied in the TCP/IP suite of protocols, resembles but varies slightly from the OSI model. For instance, the Internet model generally groups the highest three layers of the OSI model together and considers them to be one layer, the application layer. The TCP/IP reference model is shown in Figure 1.2 [4,5,6].

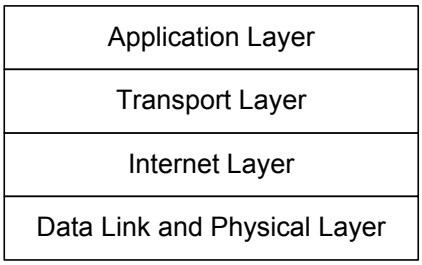

Figure 1.2. Internet (TCP/IP) reference model

The Internet model consists of four layers as it is shown in Figure 1.2. These layers are described below:

- The data link and physical layer is that it specifies details of how data is physically sent through the network, including how bits are electrically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted-pair copper wire. Protocols run on this layer are Ethernet, Token Ring, X.25, Frame Relay, RS-232, v.35 and etc.
- The Internet layer is second layer in this model. It packages data into IP datagrams, which contain source and destination address information that is used to forward the datagrams between hosts and across networks. Performs routing of IP datagrams. IP, ICMP, ARP are some of the protocols run on this layer.
- The transport layer provides communication session management between host computers. Defines the level of service and status of the connection used when transporting data. TCP and UDP are protocols run on this layer.
- The application layer defines TCP/IP application protocols and how host programs interface with transport layer services to use the network. HTTP, Telnet, FTP, SNMP, DNS, SMTP, X Windows, other application protocols are some of application layer protocols.

1.2 IP (Internet Protocol)

1.2.1 Introduction to the Internet protocol

The Internet Protocol is designed for use in interconnected systems of packet-switched computer communication networks. The Internet Protocol provides for

transmitting blocks of data called datagram from sources to destinations, where sources and destinations are hosts identified by fixed length addresses [2].

In the late 1960s, DARPA (Defense Advanced Research Projects Agency) of the United States noticed that there was a rapid proliferation of computers in military communications. Computers, because they could be easily programmed, provided flexibility in achieving network functions that was not available with other types of communication equipment. The computers that were used in military communications were manufactured by different vendors and were designed to interoperate with computers from that vendor only. Vendors used proprietary protocols in their communication equipment. The military had a multivendor network but no communication protocol to support the heterogeneous equipment from different vendors.

To solve these problems, the U.S. Department of Defense (DoD) mandated that the DARPA define a common set of protocols. The reason for having a common set of protocols includes the following:

- Procurement simplification.
- Fostering of competition among vendors.
- Interoperability.
- Vendor productivity and efficiency.

In 1969, an experiment was conducted by DARPA to use a computer network to connect four sites that are University of California at Los Angeles (UCLA), University of California at Santa Barbara (UCSB), University of Utah and SRI International.

In 1972, an ARPAnet demonstration was done with 50 packet-switched nodes (PSNs) and 20 hosts. Like preceding 4-node experiment, this one was also a success, and it set the stage for large-scale deployment of PSNs and hosts on the ARPAnet. The ARPAnet continued to grow and went through a series of transformations. Prior to 1984, the ARPAnet consisted of specialized military networks connected with the ARPAnet. After 1984, the specialized military networks formed their own network that was not connected to any other network. By 1986, the ARPAnet had expanded

to encompass all major universities, the military network called MILNET, research laboratories.

Gradually the ARPAnet itself was replaced by the Internet. The Internet is experiencing a rapid commercialization and is no longer the exclusive domain of universities and research organizations than any other source on the Internet. [4]

IP is a network layer protocol at OSI reference model and network layer protocol at Internet (TCP/IP) reference model. IP, like all network-layer protocols, moves packets of information from the original source to the ultimate destination. This service is sometimes referred to as “end-to-end packet delivery”. The reliability of the service provided by IP is called “best-effort”, which means that IP will try very hard to deliver a packet to the destination, but IP makes no guarantee that the packet will arrive without error [5].

1.2.2 IPv4 (Internet Protocol version 4)

The IPv4 is specifically limited in scope to provide the functions necessary to deliver a package of bits (an Internet datagram) from a source to a destination over an interconnected system of networks. There are no mechanisms to augment end-to-end data reliability, flow control, sequencing, or other services commonly found in host-to-host protocols. The IPv4 can capitalize on the services of its supporting networks to provide various types and qualities of service [2].

The IP implements two basic functions: addressing and fragmentation. The Internet modules use the addresses carried in the Internet header to transmit Internet datagram toward their destinations. The selection of a path for transmission is called routing.

The Internet modules use fields in the Internet header to fragment and reassemble Internet datagram when necessary for transmission through "small packet" networks.

The model of operation is that an Internet module resides in each host engaged in Internet communication and in each gateway that interconnects networks. These modules share common rules for interpreting address fields and for fragmenting and assembling Internet datagram. In addition, these modules (especially in gateways) have procedures for making routing decisions and other functions.

The IP treats each Internet datagram as an independent entity unrelated to any other Internet datagram. There are no connections or logical circuits (virtual or otherwise) [2].

The IPv4 consists of only one type IP header that is described in [2].

The following scenario illustrates the model of operation for transmitting a datagram from one application program to another:

- It is supposed that this transmission will involve one intermediate gateway.
- The sending application program prepares its data and calls on its local Internet module to send that data as a datagram and passes the destination address and other parameters as arguments of the call.
- The Internet module prepares a datagram header and attaches the data to it. The Internet module determines a local network address for this Internet address; in this case it is the address of a gateway. It sends this datagram and the local network address to the local network interface.
- The local network interface creates a local network header, and attaches the datagram to it, then sends the result via the local network.
- The datagram arrives at a gateway host wrapped in the local network header; the local network interface strips off this header, and turns the datagram over to the Internet module. The Internet module determines from the Internet address that the datagram is to be forwarded to another host in a second network. The Internet module determines a local net address for the destination host. It calls on the local network interface for that network to send the datagram.
- This local network interface creates a local network header and attaches the datagram sending the result to the destination host.
- At this destination host the datagram is stripped of the local net header by the local network interface and handed to the Internet module.
- The Internet module determines that the datagram is for an application program in this host. It passes the data to the application program in response

to a system call, passing the source address and other parameters as results of the call [2].

1.2.3 IPv6 (Internet Protocol version 6)

As the Internet has grown, it became apparent to many observers that the existing version of IP was inadequate to meet the performance and functional requirements for the Internet. In response to these needs, the IETF issued a call for proposals for a next-generation IP (IPng) in July of 1992. A number of proposals were received, and by 1994 the final design for IPng emerged. A major milestone was reached with the publication of RFC 1752, "The Recommendation for the IP Next Generation Protocol," issued in January 1995. RFC 1752 outlines the requirements for IPng, specifies the PDU formats, and highlights the IPng approach in the areas of addressing, routing, and security. A number of other Internet documents define details of the protocol, now officially called IPv6 [6,9-23].

In addition, a number of new security features have been designed for use with IPv6 but can also be used with the existing IPv4. The driving motivation for the adoption of a new version of IP was the limitation imposed by the 32-bit address field in IPv4. But other considerations as well drove the design of IPv6 [8].

The only header that is required is referred to simply as the IPv6 header. This is of fixed size with a length of 40 octets, compared to 20 octets for the mandatory portion of the IPv4 header. The following extension headers have been defined [3]:

- Hop-by-hop options header: Defines special options that require hop-by-hop processing
- Routing header: Provides extended routing, similar to IPv4 source routing
- Fragment header: Contains fragmentation and reassembly information
- Authentication header: Provides packet integrity and authentication
- Encapsulating security payload header: Provides privacy
- Destination options header: Contains optional information to be examined by the destination node.

The IPv6 standard recommends that, when multiple extension headers are used, the IPv6 headers appear in the following order:

- IPv6 header: Mandatory, must always appears first.
- Hop-by-hop options header.
- Destination options header: For options to be processed by the first destination that appears in the IPv6 destination address field plus subsequent destinations listed in the routing header.
- Routing header
- Fragment header
- Authentication header
- Encapsulating security payload header
- Destination options header: For options to be processed only by the final destination of the packet.

1.2.3.1 Addressing architecture

IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy, a much greater number of addressable nodes, and simpler auto-configuration of addresses. The scalability of multicast routing is improved by adding a "scope" field to multicast addresses. And a new type of address called an "anycast address" is defined, used to send a packet to any one of a group of nodes [3,16,19,21-22].

1.2.3.2 Header format

Some IPv4 header fields have been dropped, or they made optional. The reasons of these are to reduce the common-case processing cost of packet handling and to limit the bandwidth cost of the IPv6 header [3].

1.2.3.3 Support for extensions and options

Changes in the way IP header options are encoded allows for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future. [3,9-11]

1.2.3.4 Flow labeling capability

A new capability is added to enable the labeling of packets belonging to particular traffic "flows" for which the sender requests special handling, such as non-default quality of service or "real-time" service [3].

1.2.3.5 Authentication and privacy capabilities

Extensions to support authentication, data integrity, and (optional) data confidentiality are specified for IPv6 [3,24-25].

2. MOBILE INTERNET PROTOCOL

Mobile IP is the mobility protocol for Internet Protocol. It has versions, which are Mobile IP version 4 and Mobile IP version 6. Mobile IP version 4 is proposed in [26] by IETF while Mobile IP version 6 is proposed in [27].

In the terminology, mobility is defined as the ability of a node to change its point-of-attachment from one link to another while maintaining its all-existing communications and using the same IP address at its new link. On the other hand, nomadicity is defined as the ability of a node, which must terminate all existing communications before changing its point-of-attachment, but then can initiate new connections with a new address once it reaches its new location.

This chapter is presented in six sections. The first section explains the need for Mobile IP. The second section introduces Mobile IP. Next section proposes requirements for Mobile IP. The forth section explains mobility support for IPv4. The fifth section explains mobility support for IPv6. And the last section shows the main differences between Mobile IPv4 and Mobile IPv6.

2.1 Need for Mobile IP

2.1.1 The problem of changing link for a node

Routing decisions in an IP network are made based upon the network-prefix portion of the IP Destination Address. This implies that all nodes with interfaces on a given link must have identical network-prefix portions of their IP addresses on those interfaces. In addition to this, IP packets directed to a specific address will be routed toward the routers, which advertise reachability to the network-prefix of that address.

If a node is not located on the link where its network-prefix paints, then packets sent to that node cannot be delivered. Obviously, this means that such a node is incapable of communicating with any other node. As a corollary, a node may not move from one link to another if it wishes to communicate – without minimally changing the network-prefix portion of its IP address to reflect its new point-of-attachment to the network [6,26].

2.1.2 Host-specific routes

The strict source and record route (SSRR) provides a means for the source of an Internet datagram to supply routing information to be used by the gateways in forwarding the datagram to the destination, and to record the route information [2]. The following points make host-specific routes an unworkable solution to node mobility in the Internet:

- Minimally, host-specific routes must be propagated to all nodes along the path between a mobile node's home link and its foreign link.
- Some (in the worst case all) of these routes must be updated every time the node moves from one link to another.
- It is expected millions of mobile nodes to be operating in the Internet within coming years. Thus, we must multiply the number of host-specific routes suggested by the first two items by a million or so in order to determine the full impact of this solution.
- Unless host-specific routes are propagated to a much larger set of routers than the minimal set described in the first item above, then host-specific routing negates the Internet's ability to route around isolated node and link failures.
- There are serious security implications to using host-specific routes to accomplish node mobility in the Internet, which would require authentication and complicated key management protocols to address.

2.1.3 Changing a node's IP address

If host-specific routing is not an acceptable solution to node mobility, then how about simply changing a node's IP address as it moves from link to link? This is the question that is set out to answer in this section.

The two transport-layer protocols in wide use in the Internet are TCP and UDP. Both of these protocols have nasty habit of using IP addresses as end-point identifiers.

A TCP connection within a node is uniquely identified by the following four values: IP Source Address, IP Destination Address, TCP Source Port, and TCP Destination Port. In fact, the TCP Checksum field in each segment is computed using these four fields in addition to the data in the payload of the segment.

There is an enormous installed base of IPv4 nodes, all of which assume that these four quantities will remain constant over the duration of a TCP connection. This installed base would simply drop its connections to a destination node whose IP address was to change. Thus all ongoing communications between a mobile node and any of these existing nodes would have to be terminated, with the new connections being initiated by the mobile node at its new address. Thus changing a mobile node's address as it moves does not solve the problem of node mobility. However, changing a node's IP address as it moves does solve a related problem, known as nomadicity. There are new problems that must be dealt with:

- The nomadic node's IP address entry in the DNS must be updated every time the node changes link. Otherwise, other nodes doing an address lookup would receive an old address rather than the nomadic node's current address.
- A node that looks up a nomadic node's IP address must realize that the address returned from a name server is subject to change at any moment, and in fact might change quite rapidly.

Changing a node's IP address does not provide a solution to node mobility, though it can be useful solution to node nomadicity. Nomadicity, however, makes it next to impossible within the current Internet for another node to initiate contact with a nomadic node because the first node can never be sure at what IP address the nomadic node can be reached [6].

2.1.4 Link layer solution

There are indeed link-layer solutions to node mobility that have been devised for use with Internet-related protocols. However, link-layer solutions are not sufficiently generic to provide node mobility on the global Internet. The problems related with link-layer solutions are given below [6]:

- First of all, by definition, link-layer solutions provide node mobility only in the context of a single type of medium. Thus, link-layer solutions enable only nomadicity between media of different types.
- Another problem with link-layer solutions is that they inherently necessitate N different mobility solutions for each of N possible media over which nodes might want to send IP packets. A single solution, which works over all media

types, is to be preferred over multiple medium-specific solutions, if such a thing is architecturally possible. Mobile IP is such a solution.

- Finally, link-layer solutions necessarily provide mobility within a limited geographic area. Local-area solutions such as 802.11 can provide mobility throughout a campus or a building, but unusable once the node leaves this area. Wide-area solutions such as Cellular Digital Packet Data (CDPD) can provide much more geographically diverse areas in which coverage is available. However, the limited throughput of such systems makes a node prefer to be connected to another type of medium, if such is available.

2.1.5 Mobility instead of nomadicity

If all communications are initiated by the user of a mobile node, and the user does not mind shutting down his applications and re-starting them at a new location, then nomadicity is indeed sufficient and mobility is not absolutely required. However, there are many reasons why mobility is preferable to nomadicity, even in those situations where it is not absolutely required. A few of these reasons are listed in this section, and most of them involve the virtues of using fixed IP address:

- Many applications have configurations databases, which depend on IP addresses, as opposed to hostnames. In the presence of rapidly changing IP addresses, these applications would break.

- There is a reason to believe that at some point in the future, servers would need to become mobile. In this case, clients that know their servers only by their IP addresses will be incapable of locating them unless the servers have the mobility properties provided by Mobile IP.

- Some application vendors provide network-licensing systems, which restrict access to only those nodes possessing specific ranges of IP addresses. Without Mobile IP, a nomadic node, which changes link, would no longer be able to obtain a license over the network to use these applications.

- Some security mechanisms provide access-privileges to node based upon their IP address. Mobile nodes employing Mobile IP allow such mechanisms to work in the presence of node mobility.

- Maintaining a pool of addresses for assignment to nomadic nodes can be difficult, and in some cases no assignment mechanism might be available. Mobile IP, which lets nodes keep their IP addresses as they move, does not exacerbate the problem of the limited availability of IPv4 addresses.

For these and other reasons, mobility as provided by Mobile IP can be extremely useful, even in those situations where it is not absolutely required [6,7].

2.2 Introduction to Mobile IP

Mobile IP is a solution for mobility on the global Internet which is scalable, robust, secure, and which allows nodes to maintain all ongoing communications while changing links. Specifically, Mobile IP provides a mechanism for routing IP packets to mobile nodes, which may be connected to any link while using their permanent IP address.

Mobile IP is a network-layer solution to node mobility in the Internet. By this it means that Mobile IP accomplishes its task by setting up the routing tables in appropriate nodes, such that IP packets can be sent to mobile nodes not connected to their home link. In fact, Mobile IP can be considered to be routing protocol, which has very specialized purpose. The purpose of Mobile IP is to allow IP packets to be routed to mobile nodes, which could potentially change their location very rapidly.

As a network-layer protocol, Mobile IP is completely independent of the media over which it runs. This is in keeping with the design philosophy behind the Internet Protocol itself, which was designed to be independent of the underlying characteristics of the links over which it runs.

Mobile IP solves the primary problem of routing IP packets to mobile nodes, which is an enormous first step in providing mobility on the Internet. However, a complete mobility solution would involve enhancements to other layers of the protocol stack as well.

2.3 Requirements for Mobile IP

The requirements [6,26], which drove the design of Mobile IP, are as follows:

- A mobile node must be able to communicate with other nodes after changing its link layer point-of-attachment to the Internet.

- A mobile node must be able to communicate using only its home (permanent) IP address, regardless of its current link-layer point-of-attachment to the Internet.
- A mobile node must be able to communicate with other computers that do not implement the Mobile IP mobility functions.
- A mobile node must not be exposed to any new security threats those to which any fixed node on the Internet is exposed.

2.4 Mobility for IP Version 4 (Mobile IPv4)

2.4.1 The main components of Mobile IPv4

Mobile IP generally uses seven main components, which are described below.

2.4.1.1 Mobile node

A Mobile Node is a node which can change its point-of-attachment in the Internet from one link to another while maintaining its all ongoing communications and using only its (permanent) IP home address [26].

2.4.1.2 Home agent

The home agent is a router with an interface on the mobile node's home link [6,26] which:

- The mobile node keeps informed of its current location, as represented by its care-of address, as the mobile node moves from link to link.
- In some cases, the home agent advertises reachability to the network-prefix of the mobile node's home address, thereby attracting IP packets that are destined to the mobile node's home address.
- The home agent intercepts packets destined to the mobile node's home address and tunnels them to the mobile node's current location.

2.4.1.3 Foreign agent

The foreign agent is a router on a mobile node's foreign link [6,26] which:

- The foreign agent assists the mobile node in informing its home agent of its current care-of address.

- In some cases, the foreign agent provides a care-of address and de-tunnels packets for the mobile node that have been tunneled by its home agent.
- The foreign agent serves as a default router for packets generated by the mobile node while connected to this foreign link.

2.4.1.4 Home address

The home address is an IP address assigned to the mobile node permanently. The home address does not change as a mobile node moves from link to link. Rather, a mobile node's home address would change only for the same reasons, and under same circumstances, as the address of a stationary host or router would change [6,26].

2.4.1.5 Home link

The network-prefix of the mobile node's home address defines its home link. A mobile node's home link is that link which has been assigned the same network-prefix as the network-prefix of the mobile node's home address. A mobile nodes home agent is a router that has at least one interface on the mobile node's home link [6,26].

2.4.1.6 Foreign link

The foreign link of a mobile node is that link which has not been assigned the same network-prefix as the network-prefix of the mobile node's home address [6].

2.4.1.7 Care-of address

A care-of address [6,26] is an IP address associated with a mobile node that is visiting a foreign link. Properties of a care-of address are given below:

- A care-of address is specific to the foreign link currently being visited by a mobile node.
- A mobile node's care-of address generally changes every time the mobile node moves from one foreign link to another.
- Packets destined to a care-of address can be delivered using existing Internet routing mechanisms.
- A care-of address is used as the exit-point of a tunnel from the home agent toward the mobile node.

- A care-of address is almost never used as the IP Source or the IP Destination Address in a mobile node's conversations with other nodes. Specifically, the care-of address will never be returned by a DNS when another node looks up the mobile node's hostname.

There are two conceptual types of care-of address which are described below:

- A foreign agent care-of address is an IP address of a foreign agent, which has an interface on the foreign link being visited by a mobile node. A foreign agent care-of address can be any one of the foreign agent's IP addresses, so long as the foreign agent has at least one interface on the foreign link. Thus, the network-prefix of a foreign agent care-of address need not equal the network-prefix that has been assigned to the foreign link. A foreign agent care-of address can be shared by many mobile nodes simultaneously.[6,26]
- A collocated care-of address is an IP address temporarily assigned to an interface of the mobile node itself. The network-prefix of a collocated care-of address must equal the network-prefix that has been assigned to the foreign link being visited by a mobile node. This type of care-of address might be used by a mobile node in situations where no foreign agents are available on the foreign link. A collocated care-of address can be used by only one mobile node at a time [6,26].

Summarizing, a care-of address is an IP address that is close to a mobile node's visited, foreign link.

2.4.2 Protocol overview

The functions, nodes, and protocols of Mobile IP are all interrelated, which makes them hard to describe without an annoying number of forward and backward references. Therefore, it is described high-level how Mobile IP works:

1. Home agents and foreign agents advertise their presence on any attached links by periodically multicasting or broadcasting special Mobile IP messages called Agent Advertisements.
2. Mobile nodes listen to these Agent Advertisements and examine their contents to determine whether they are connected to their home link or foreign link. While connected to their respective home links, mobile nodes

act just like stationary nodes – that is, they make use of no other Mobile IP functionality. The rest of the steps, which follow, therefore, assume that a mobile node has discovered that is connected to a foreign link.

3. A mobile node connected to a foreign link acquires a care-of address. A foreign agent care-of address can be read from one of the fields within the foreign agent's Agent Advertisement. A collocated care-of address must be acquired by some assignment procedure, such as Dynamic Host Configuration Protocol, the Point-to-Point Protocol's IP Control Protocol, or manual configuration.

4. The mobile node registers the care-of address acquired in step three with its home agent, using message-exchange defined by Mobile IP. In the registration procedure, the mobile node asks for service from a foreign agent, if one is present on the link. In order to prevent remote denial-of-service attacks, the registration messages are required to be authenticated.

5. The home agent or some other router on the home link advertises reachability to the network-prefix of the mobile node's home address, thus attracting packets that are destined to the mobile node's home address. The home agent intercepts these packets, possibly by using proxy ARP [26], and tunnels them to the care-of address that the mobile node registered in step four.

6. At the care-of address – either the foreign agent or one of the interfaces of the mobile node itself – the original packet is extracted from the tunnel and then delivered to the mobile node.

7. In the reverse direction, packets sent by the mobile node are routed directly to their destination, without any need for tunneling. The foreign agent serves as a router for all packets generated by a visiting mobile node.

These steps show the case of a mobile node connected to a foreign link and using a foreign agent care-of address. The case of a mobile node visiting a foreign link and using collocated care-of address is very similar, but introduces some new wrinkles [6].

2.4.3 Agent discovery

Agent Discovery is the process by which:

- A node determines whether it is currently connected to its home link or a foreign link.
- A node detects whether it has moved from one link to another.
- A node obtains a care-of address when connected to a foreign link.

The Mobility Agent Advertisement Extension follows the ICMP Router Advertisement fields. It is used to indicate that an ICMP Router Advertisement message is also an Agent Advertisement being sent by a mobility agent [26].

Agent Discovery consists of two simple messages.

2.4.3.1 Agent advertisement

The first, Agent Advertisements are used by agents (home, foreign or both) to announce their capabilities to mobile nodes. Specifically, Agent Advertisements are periodically transmitted as multicast or broadcasts to each link on which a node is configured to perform as a home agent, a foreign agent, or both. This allows a mobile node that is connected to such a link to determine whether any agent is presented and, if so, their respective identities (IP addresses) and capabilities [6,26].

2.4.3.2 Agent solicitation

Mobile nodes that do not have the patience to wait around for the next periodic transmission of an Agent Advertisement send messages of second type, Agent Solicitations. The sole purpose of an Agent Solicitation, then, is to force any agent on the link to immediately transmit an Agent Advertisement. This is useful in those situations where the frequency at which agents are transmitting is too low for a mobile node that is moving rapidly from link to link [6,26].

2.4.4 Move detection

There are two ways by which mobile nodes can determine that they have moved from one link to another. In next two subsections it is assumed that there is at least one agent present on every link to which the mobile node might connect. Then, the question is what happens when there are no agents present and, therefore, a mobile node hears no advertisements on its current link.

2.4.4.1 Move detection using lifetimes

The first method uses the Lifetime field within the ICMP Advertisement [28] portion of an Agent Advertisement. This field effectively tells the mobile node how soon it should expect to hear another advertisement from that same agent. Because, advertisements can be lost, especially when sent over error-prone, wireless links, home agents and foreign agents send advertisements faster than the Lifetime field required.

If a mobile node is registered with a foreign agent, and fails to hear an advertisement from that agent within the specified Lifetime, then the mobile node can assume that it has moved to a different link or that its foreign agent is terribly confused or broken. In either case, the mobile node would be wise to register with the next foreign agent from which it receives an Agent Advertisement and to send an Agent Solicitation if no such advertisement is forthcoming [6,26].

2.4.4.2 Move detection using network-prefixes

The second method for move detection uses network-prefixes. It is possible to have multiple foreign agents on the same link, the mobile node must determine if it received the two advertisements on the same or different links. If they were received on the same link, then the mobile node need not register with the new foreign agent. Otherwise, the mobile node has changed location and should register with a foreign agent on the new link.

To determine whether two advertisements were received on the same link, the mobile node computes the network-prefixes of respective advertisements. This computation can be performed only if both Agent Advertisements contained the Prefix-Length Extensions.

A mobile node computes the network-prefixes of two advertisements and compares them. If they differ, then the mobile node concludes that the two advertisements were received on different links. Otherwise, the mobile node concludes they were received on same link. In the case of a mobile node comparing a newly received advertisement with that of the foreign agent with which it is currently registered, the mobile node should register with a foreign agent on the new link if it determines that it has moved.

Otherwise, if an advertisement is received from another agent on the same link, the mobile node concludes that it has moved [6].

2.4.4.3 Move detection without advertisements

Assuming that a mobile node is able to obtain a collocated care-of address, the mobile node still must be able to determine when it moves from one agentless link to another. There are two ways that a mobile node might infer that such movement has occurred. The first is to note whether any forward progress has recently been made in any of its open TCP connections. If not, then the mobile node might conclude that it has moved since the last time it registered.

Also, the mobile node can put its network-interface driver into" promiscuous mode". In this mode, the mobile node examines all packets on the link, not just packets destined to it. If none of the packets flying across the link have network-prefixes that equal the mobile node's current care-of address, then the mobile node might infer that it has moved to a new link from the one on which the care-of address was obtained. If so, the mobile node should acquire a new care-of address and register with its home agent.

Both of these methods – TCP progress monitoring and promiscuous link examination – require some form of assistance from layers other than the network layer [6,26].

2.4.5 Registration

A mobile node registers whenever it detects that its point-of-attachment to the network has changed from one link to another. Also, because these registrations are valid only for a specified Lifetime, a mobile node reregisters when it has not moved but when its existing registration is due to expire. Mobile IP Registration is the process by which:

- A mobile node requires routing services from a foreign agent on a foreign link.
- A mobile node informs its home agent of its current care-of address.
- A mobile node renews a registration, which is due to expire.
- A mobile node deregisters when it returns to its home link.

Some of the more subtle capabilities of Registration are also described which allow a mobile node to:

- have multiple, simultaneous care-of addresses registered with its home agent, wherein the home agent tunnels a copy of packets destined to the mobile node's home address to each of the multiple care-of addresses;
- deregisters a specific care-of address while retaining others; and
- dynamically ascertain the address of a potential home agent, if the mobile node has no prior knowledge of its home agent.

Mobile IP Registration follows Mobile IP Agent Discovery. When a mobile node detects that it is connected to its home link, it deregisters with its home agent and begins acting like any fixed host or router.

When the mobile node detects that it is connected to a foreign link, it acquires a care-of address and registers this care-of address with its home agent, possibly via a foreign agent.

2.4.5.1 Registration messages

Mobile IP Registration consists of the exchange of two messages: a Registration Request and a Registration Reply. A registration messages is carried within data portion of a UDP segment, which is in turn placed within the payload portion of an IP packet.

A Registration Request message is sent by a mobile node to begin the registration process. In some instances the Registration Request is sent directly to the mobile node's home agent. In other cases, it is sent via an objectionable, relays it to the mobile node's home agent.

The home agent receives the Registration Request and sends back to the mobile node a Registration Reply, which, among other things, tells the mobile node whether or not its attempted registration was successful.

If a mobile node does not receive the Registration Reply within a reasonable period of time, then the mobile node retransmits the Registration Request a number of times until it does receive a Reply.

2.4.5.2 Registration scenarios

There are three most common scenarios for registration [6], which are as follows:

1. A mobile node registers on a foreign link using a foreign agent's care-of address:

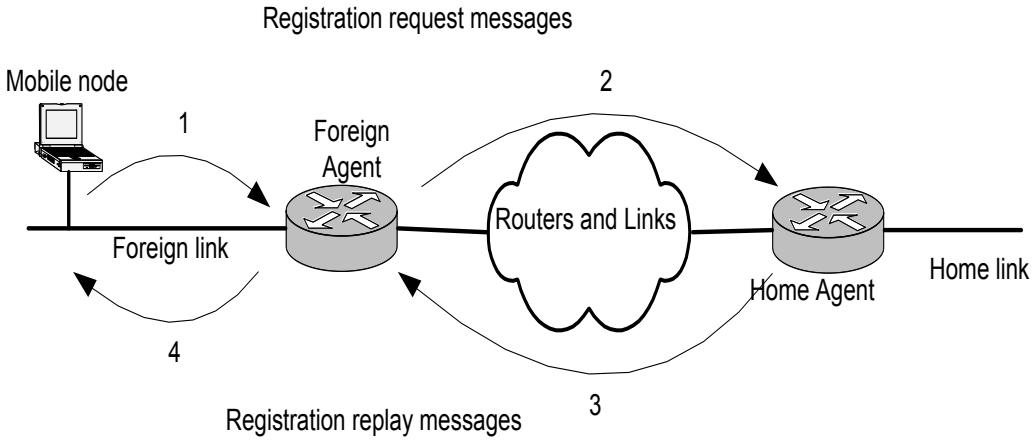

Figure 2.1. Registration scenario 1 of a mobile node

2. A mobile node registers on a foreign link using a collocated care-of address:

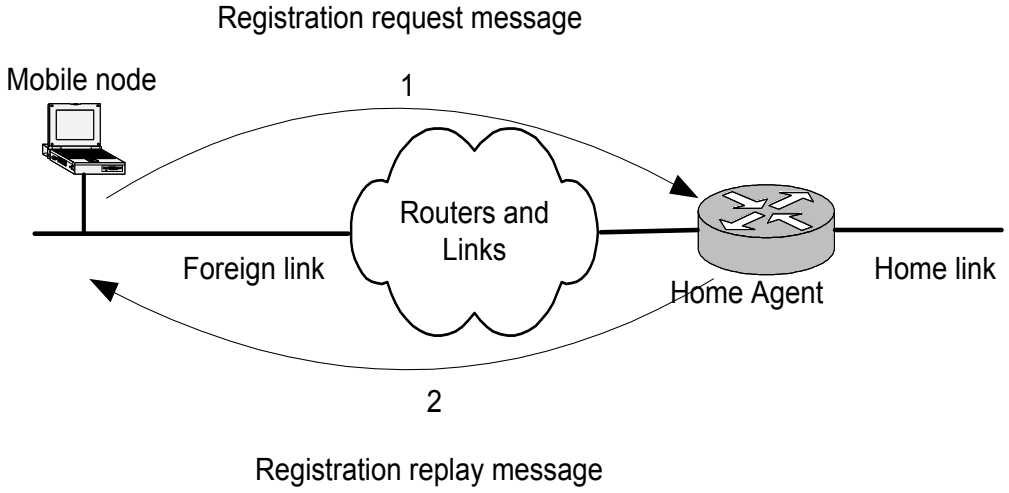

Figure 2.2. Registration scenario 2 of a mobile node

3. A mobile node deregisters upon returning to its home network:

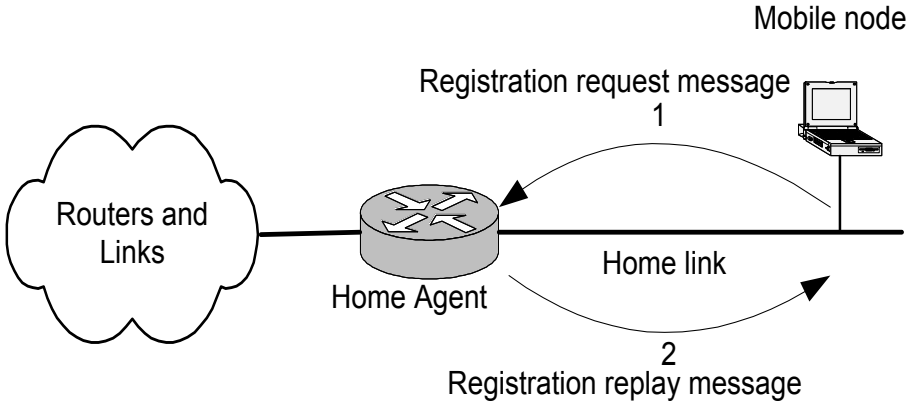

Figure 2.3. Registration scenario 3 of a mobile node

2.4.5.3 A mobile node registration time

A mobile node always begins the registration process when it detects that it has moved from one link to another. There are other circumstances under which it should register, even if it has not changed links. For example, the mobile node should register when it detects that its current foreign agent has rebooted. Also, the mobile node should reregister when its current registration is due to expire soon [6,26].

2.4.5.4 The time of sending registration request by a mobile node

The mobile node uses the information it learned through Agent Discovery to determine which of the registration scenario applies, and it builds its Registration Request accordingly.

For a mobile node, the trickiest part about registration is figuring out the Link-Layer Destination Address of the frame in which it places the Registration Request message for transmission on its current link. On the home link this is easy – the mobile node uses the ARP to determine the home agent's link-layer address, and sends the frame accordingly.

On foreign links, however, it is very dangerous for a mobile node to transmit ARP frames that contain its home address. This is because other nodes on the foreign link will get terribly confused if they place the mobile node's home address into their respective ARP tables, especially if these nodes attach to multiple links. Therefore, as rule, a mobile node must never send an ARP frame containing its home address on a foreign link.

When registering via a foreign agent, then, the mobile node should record the foreign agent's link-layer address from the Link-Layer Source Address field of that foreign agent's Agent Advertisements. The mobile node should use this address as the Link-Layer Destination Address of the frame, which carries Registration Request message.

Finally, it is assumed that the same method by which a mobile node acquires a collocated care-of address will also provide the mobile node with the IP address of a default router on the foreign link. This router will be the first hop for the Registration Request. In this situation, the mobile node may ARP for its default router's link-layer address, provided that the mobile node's ARP Request message contains its care-of address and not its home address.

2.4.5.5 A registration request processing by a foreign agent

In this subsection, it is assumed that the mobile node is registering via a foreign agent. Upon receipt of a Registration Request, the foreign agent applies a sequence of validity checks. If any of them fail, then the foreign agent rejects the registration by sending a Registration Reply to the mobile node with a Code field indicating the cause of the rejection. Some reasons that a foreign agent might reject a registration are as follows:

- The mobile node included a Mobile-Foreign Authentication Extension, which included an invalid Authenticator field.
- The mobile node requested a Lifetime, which exceeds the maximum value, permitted by the foreign agent.
- The foreign agent has insufficient resources to handle any additional mobile nodes.

If all is well with the mobile node's Registration Request, then the foreign agent relays it to the mobile node's home agent. The foreign agent consumes the original IP and UDP headers that contained the Registration Request and creates new ones for transmission to the home agent. The new UDP/IP packet contains the same payload, as did the original packet. The IP Destination Address of the new packet is read from the home agent field of the Registration request, and the IP Source Address is the IP address of the foreign agent on the interface over which it will transmit the packet [6,26].

2.4.5.6 A registration request processing by a home agent

Upon receipt of a Registration Request, a home agent performs a set of validity checks not unlike those performed by a foreign agent. If the Registration Request is invalid for any reasons, the home agent sends a Registration Replay to the mobile node with a suitable Code field indicating the reasons for the failure.

If the Registration Request is valid, then the home agent updates the mobile node's binding entries. Finally, the home agent sends a Registration Reply to the mobile node indicating that the registration was successful. The IP Source and Destination Address and UDP Source and Destination Port in the Registration Replay are simply reversed from the respective fields in the Registration Request [6,26].

2.4.5.7 A registration replay processing by a foreign agent

It is assumed that the mobile node is registering via a foreign agent – otherwise, the Registration Replay would be sent directly to the mobile node from the home agent, bypassing the foreign agent altogether. Upon receipt of a Registration Reply, the foreign agent performs a series of validity checks.

If the Replay is found to be invalid in any way, then the foreign agent generates a new Registration Reply containing suitable rejection Code field and sends it to the mobile node. An invalid Reply is one, which fails the foreign agent's criteria for being a legitimate Registration Reply. For example, an invalid Reply is one, which is malformed, contains an unrecognized extension, or fails home-agent-to-foreign-agent authentication.

If the Registration Reply is valid, then the foreign agent updates its list of known, visiting mobile nodes and relays the Registration Reply to the mobile node, using some of the fields it recorded from the original Registration Request to transmit the Reply [6].

2.4.5.8 A registration replay processing by a mobile node

Upon receipt of a Registration Reply, the mobile node performs its own sequence of validity checks. If the reply is valid, then the mobile node examines the Code field to examine whether the registration was accepted or rejected by the home agent (and foreign agent, if applicable).

If the Code field indicates rejection, then the mobile node can attempt to repair the error that caused the rejection and attempt a new registration. Common reasons for rejection include excessive Lifetimes and invalid Identification fields.

If the Code field indicate acceptance, then the mobile node adjust its routing table as appropriate for the current link and begins (or continues) communicating [6,26].

2.4.5.9 The mobile node ping-pong back and forth between wireless cells

The area over which the signal from a wireless transmitter can be accurately received is referred to as its coverage area. The coverage area, or cell, of a transmitter rarely looks like hexagons. Instead, the cells generally overlap each other.

In fact, the situation is even worse than this, because the shapes of the cells tend to vary with time. This variation makes it possible for a mobile node, which is receiving a first transmitter to lose contact with that transmitter and begin receiving the signal from a second transmitter without moving an inch. If each wireless cell was its own link, each having been assigned a unique network-prefix, then the mobile node could potentially be changing links very rapidly, despite remaining completely still. This would generate a tremendous number of Mobile IP Registrations, since the mobile node must register every time it changes link.

There are two solutions to this problem of rapid mobility across wireless cells. One is outside the Mobile IP and involves link-layer mechanisms. The other uses Mobile IP's simultaneous binding capability. These two solutions are described below:

The link-layer solution involves making the cells of a wireless network from a few large links. A bridge is a network element, which makes several media segments, appears as one link. The use of bridges in this way prevents every change of cell from likewise being a change of link, and therefore requiring a new Mobile IP Registration. Rather link-layer-specific mechanisms are used to accomplish "handoffs" between cells that are part of the same link- then Mobile IP is used to accomplish mobility between cells that are part of different links [6].

The second solution uses Mobile IP's simultaneous binding capability to reduce the number of registrations. The S bit in the Registration Request – if set to 1 – indicates to the home agent that the mobile node wishes to create a binding for the specified care-of address, but wishes to leave all existing bindings unmodified. For example, if a mobile node has registered a care-of address on the first link and then registers

another care-of address on a second link, the home agent of the mobile node will then have two bindings for the mobile node – one for each of these respective care-of addresses.

Packets sent to a mobile node's home address are intercepted by its home agent and tunneled to its care-of address. In actuality, the home agent tunnels a copy of packets to every one of the care-of addresses that have been registered by the mobile node.

A mobile node is located at the border between two wireless cells where they are physically separated. If the mobile node is moving back and forth between two cells, it can register a care-of address on both links. Then the mobile node simply receives a tunneled packet from the transmitter in whichever cell it happens to be receiving at the current moment. The other packet (sent by the other transmitter) will likely be lost, though there is also a chance that the mobile node, too, will receive it. In either case, IP does not guarantee that exactly one copy of a packet will arrive at its ultimate destination – in fact, TCP/IP implementations are specifically required to accommodate the receipt of zero, one, or multiple copies of an IP packet.

Thus, the simultaneous-binding feature of Mobile IP can be used to prevent large number of registrations by a mobile node that is on the border between two wireless cells. Support for this feature is optional by home agents, however. A home agent, which does not support multiple simultaneous bindings, does not reject a Registration Request in which this feature is requested.

It is unclear whether this feature of Mobile IP has any applicability in the real world, however. Most wireless systems with overlapping coverage areas tend to be architect as suggested earlier in this section. Namely, numerous cells tend to be grouped together into confederations which form a single link as viewed by the network layer (IP), with a mobile node using link-layer handoffs to maintain connectivity as it moves within a single confederation of cells [6].

2.4.6 Routing in Mobile IPv4

It is described a major topic area of Mobile IP – the procedures by which packets are routed to and from mobile nodes, depending upon their current location.

There are two primary cases: a mobile node connected to its home link and a mobile node connected to a foreign link.

2.4.6.1 A mobile node at home link

Packets destined to a mobile node's home address are routed to the mobile node's home link as a result of the normal functioning of network-prefix routing. Thus, no special routing procedures are required to deliver packets to a mobile node that is connected to its home link. This implies that the rules for routing packets to a mobile node, which is connected to its home link, are identical to the rules for routing packets to any conventional IP host or router.

In addition, no special rules are needed to route packets generated by a mobile node that is connected to its home link. Likely, any host or router, such a mobile node uses its routing table to select an appropriate Next Hop for any packet it generates. Similarly, no special rules are needed for populating with entries the routing table of a mobile node while it is connected to its home link [6].

2.4.6.2 A mobile node at foreign link

In this subsection it is described how unicast packets are routed to and from a mobile node that is connected to a foreign link. The procedures for routing packets to a mobile node that is connected to a foreign link can be summarized as follows:

- A router on the home link, possibly the home agent, advertises reachability to the network-prefix, which equals that of the mobile node's home address.
- Packets destined to the mobile node's home address are therefore routed toward its home link and specifically toward the mobile node's home agent.
- The home agent intercepts packets destined to the mobile node, assuming the mobile node has registered one or more care-of addresses, and tunnels a copy to each such care-of address.
- At each care-of address – an address of a foreign agent or an address collocated with the mobile node itself – the original packet is extracted from the tunnel and delivered to the mobile node.

In both cases – a foreign agent care-of address and a collocated care-of address – the home agent receives a packet destined to one of its mobile nodes and looks up the corresponding bindings. The home agent then tunnels the packet to the care-of address, not knowing or caring whether the mobile node or a foreign agent is the tunnel exit-point. Thus, in both cases, the encapsulated (inner) packet is from the

host to the mobile node's home address, and in the both cases the encapsulating (outer) packet is from the home agent to the care-of address.

In the case of the foreign agent care-of address, when the foreign agent receives the tunneled packet, it removes the encapsulating (outer) packet to recover the encapsulated (inner, original) packet. It then sees that the IP Destination Address is that of a registered mobile node, looks up the appropriate interface, and sends the packet to the mobile node. In the case of collocated care-of address, the mobile node performs similar processing upon receiving the tunneled packet. The mobile node removes the outer packet to recover the original packet, and ultimately passes the contents of the original packet up the stack to the higher-layer protocol.

All home agents and foreign agents are required to implement IP in IP Encapsulation [29] for tunneling purposes. In addition, they may implement Minimal Encapsulation within IP [30] and Generic Routing Encapsulation (GRE) [31]. Mobile nodes, which are capable of operating with a collocated care-of address, have identical requirements with respect to tunneling [6,26].

2.4.6.3 Source routing

IP Version 4 defines an IP Header Option called the Loose Source and Record Route Option. This option lists one or more intermediate destinations that a packet containing the option must visit along its journey to its final destination.

When a router receives the packet, it inspects the options and realizes that it is only an intermediate destination. It then grabs the next address in the Loose Source and Record Route Option – the destination host – and forwards the packet to the Next Hop along the path to the destination host. Before forwarding the packet, the router "records" its own IP address within the Loose Source and Record Route Option. Specifically, the router records its IP address on the interface over which it forwards the packet.

When the packet arrives at the destination host, it inspects the options and determines that it is the ultimate destination of the packet. Therefore, the destination host "consumes" the packet by passing it to the higher-layer protocol indicated by the IP Protocol field. The option specifies that when a destination host responds to a source host that included the Loose Source and Record Route Option in its packets, that destination host should include a "reversed" source routing option in the response

packet. In this example, the original destination host would include a Loose Source and Record Route Option specifying the same router as an intermediate destination when sending packets back to the original source host.

Whenever a mobile node has a packet to send to a correspondent, the mobile node includes a Loose Source and Record Route Option in the packet specifying its current care-of address as an intermediate destination. Then, when the correspondent replies to the mobile node, it reverses the source route and the packet is routed to the mobile node via its care-of address.

The mobile node still requires a home agent, though, for correspondents that do not know the mobile node's current care-of address. For these correspondents, packets to the mobile node are sent normally, in which case they are routed to the home link, where they are intercepted by the home agent and loose-source routed to the mobile node via the care-of address. Obviously, then, the mobile node would still be required to register its care-of address with its home agent.

There are three primary reasons why Mobile IP working group as a solution rejected source routing. The first reason is that the Loose Source and Record Route Option, despite having been defined in the original IPv4 specification [2], is rarely, if ever, implemented correctly in IPv4 hosts. Some needs simply drop all packets that contain this option. Others actually crash upon receiving IP packets containing options. Finally, few, if any, implementations actually reverse the source route, even though this was a requirement of the IPv4 specification.

The second reason is that IP packets containing options require additional processing by every router along the path from source to destination – not just the routers listed in the source routing option! This is because each router to see if they contain an option that might be relevant to that router before it forwards the packet must parse the options. Conversely, packets that do not contain options can generally be routed very quickly, often in hardware, which allows current router technology to route IP packets at pretty blazing speeds. A packet containing any IP option can experience as much as a 10-to-1-performance penalty in some commercial routers. This was deemed to be an unacceptable performance penalty, especially when compared with tunneling which requires only two routers to do "special" processing – the home agent and the tunnel exit-point.

The final reason that loose-source routing was deemed unacceptable relates to security. A Bad Guy could send a packet to a mobile node's correspondent specifying some bogus care-of address as an intermediate destination in a loose-source route. This would cause the correspondent to reverse the source route, specifying this bogus care-of address as an intermediate destination in its replies. At this point, the mobile node is cut off from communicating this correspondent, and the Bad Guy gets to see a copy of all packets sent by that correspondent to the mobile node. This problem could be eliminated with the proper use of authentication, but it has the same key management problems as route optimization [6].

2.4.6.4 Triangle routing

Packets that are sent by a correspondent to a mobile node connected to a foreign link are routed first to the mobile node's home agent and then tunneled to the mobile node's care-of address. However, packets sent by the mobile node are routed directly to the correspondent, thus forming a triangle as shown in Figure 2.4. The question is why does not the mobile node inform correspondents of its care-of address and have them tunnel directly to the mobile node, bypassing the home agent? This optimized routing is potentially more efficient in terms of delay and resource consumption than is triangle routing, because, in general, the packets will have to traverse fewer links on their way to their destination.

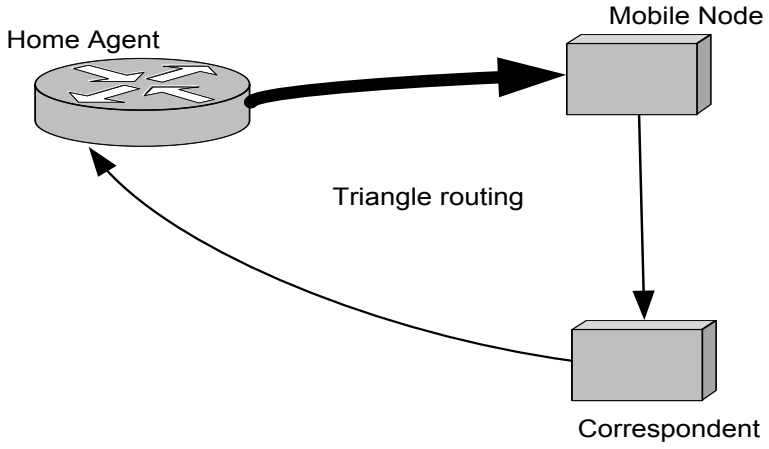

Figure 2.4. Triangle routing

The main obstacle to route optimization relates to security. For a correspondent to tunnel directly to a mobile node, the correspondent must be informed of the mobile node's current care-of address. Note the similarity between this and Mobile IP Registration, the purpose of which is to inform a mobile node's home agent of the

mobile node's current care-of address. Without strong authentication in the messages that inform a mobile node's correspondent of its current care-of address, trivial denial-of service attacks would be possible to perform with respect to correspondents.

Specifically, a Bad Guy needs only to send a bogus registration to the mobile node's correspondent in order to cut off all communication between the two nodes. This is the challenge presented by any attempts to optimize the routing in Mobile IP. It is conceivable that a network administrator could configure a secret key between a mobile node and its home agent, in order to protect the registration messages against forgeries. It is not practical, however, to likewise distribute keys between a mobile node and every other node with which it might correspond. In the absence of automated mechanisms, distributing keys between a mobile node and its correspondents is simply unworkable [6,26].

2.4.6.5 Routing of broadcast datagram

A mobile node can obtain a copy of broadcasts that are transmitted on its home link, even when the mobile node is currently connected to a foreign link. The mobile node requests that its home agent forward all broadcasts by setting B bit in its Registration Requests. This instructs the home agent to deliver a copy of all such broadcasts via a tunnel to the mobile node. The exact delivery mechanism depends upon whether the mobile node is using a foreign agent care-of address or a collocated care-of address.

A mobile node with a collocated care-of address receives broadcast packets in exactly the same way as it receives unicast packets. Namely, its home agent tunnels the broadcast packet to the mobile node's collocated care-of address, the mobile node de-tunnels the packet, and the mobile node passes the encapsulated (inner) broadcast packet to the higher layer. A mobile node using a collocated care-of address must set the D bit to 1 in its Registration Request, to inform its home agent that the mobile node itself is decapsulating packets.

A mobile node with a foreign agent care-of address receives broadcast packets far differently from the way in which it receives unicast packets. Consider what would happen if the home agent simply tunneled broadcast packets to the foreign agent's care-of address. The foreign agent would de-tunnel the packet and then have absolutely no clue what to do with it, because the IP Destination Address of the

encapsulated (inner) packet would be a broadcast address and the foreign agent would not know which mobile node was supported to receive it. Thus, the foreign agent would not know on which interface to transmit the de-tunneled broadcast packet.

For this reason, a home agent must use nested encapsulation to deliver broadcast packets to mobile nodes, which have registered a foreign agent, care-of address. First, the home agent encapsulates a broadcast within a first encapsulating packet with IP Source Address equal to the home agent's address and IP Destination Address equal to the mobile node's home address. Then, the home agent encapsulates this first encapsulating packet within a second packet with IP Source Address equal to the home agent's address and IP Destination Address equal to the care-of address.

In this way, when the doubly encapsulated packet arrives at the care-of address, the foreign agent decapsulates (once) and sees a unicast packet that's Source Address is the home agent's address and whose Destination Address is the mobile node's home address. This packet looks like any other unicast packet that the home agent might tunnel for delivery to the mobile node. Therefore, the foreign agent looks in its routing table and sends the packet to the mobile node over the appropriate link. Further, this unicast packet contains the encapsulated broadcast packet, which must be de-tunneled by the mobile node before being passed the higher-layer protocol [26].

The way in which a mobile node sends broadcasts is independent of whether it has a collocated or a foreign agent care-of address. However, transmission of broadcasts by mobile nodes does depend upon the type of broadcast, as specified by the following three cases:

- If the destination is a link-specific broadcast (255.255.255.255) intended for the mobile node's foreign link, and then the mobile node simply transmits the packet on the foreign link, using the link-layer broadcast address to deliver the frame containing this packet to all nodes on the link.
- If the destination is a link-specific broadcast (255.255.255.255) intended for the mobile node's home link, then the mobile node must tunnel this packet to its home agent. The encapsulating (outer) packet has an IP Source Address

equal to the mobile node's home address, and the IP Destination Address is the mobile node's home agent.

- If the destination is a prefix-specific broadcast (network-prefix.11...11), then the mobile node has two alternatives. First, it can tunnel the packet to its home agent. Second, the mobile node can transmit the packet normally; sending it in a link-layer frame that's Link-Layer Destination Address is that of its router, just like any unicast packet transmitted by the mobile node. However, some intermediate routers might be configured to filter broadcast packets, in which case a mobile node will be better off tunneling such packets to its home agent.

Thus, mobile nodes can participate in broadcasts either as senders or receivers, simply by setting the appropriate bits (B and D) in their Registration Requests and using the procedures described above [6,26].

2.4.6.6 Routing of multicast datagram

IP multicasts are, by definition, those packets with IP Destination Address whose four leftmost bits are "1110" – that is, they have the form 1110.multicast-group. In dotted-decimal notation, the range of IP multicast addresses, also known as Internet Class D Address, is therefore 224.0.0.1 through 239.255.255.255.

Any node can send a packet to a multicast group, simply by building an IP packet in which the IP Destination Address is set to the group's multicast address. Senders do not need to be members of a group in order to send multicasts to the receivers of that group. A node joins a multicast group, and therefore becomes a receiver of the packets sent to that group, by sending special messages to multicast routers. A multicast router is a router that is capable of routing multicast packets.

The Internet Group Management Protocol (IGMP) defines the messages that nodes use to join multicast groups. Specifically, nodes send IGMP Host Membership Reports to express their desire to join multicast groups. IGMP is considered to be a part of network layer. Also IGMP messages are carried within the payload portion of IP packets.

Unlike IP unicast and IP broadcast packets, IP multicast packets are routed based upon both the IP Destination Address and the IP Source Address. The IP Source Address must be topologically correct; that is, the network-prefix of the IP Source

Address must equal to the network-prefix of the link of which the IP multicast is originated. Equivalently stated, a node, which sends a multicast packet, must be connected to its home link. Obviously, this causes problems for mobile nodes that are currently connected to a foreign link [6].

A mobile node that is connected to a foreign link must not send multicast packets directly on that network using its home address as the IP Source Address; otherwise, multicast routers will not be able to deliver the packets to all of the group's receivers. Such a mobile node has two options for sending multicasts. First, the mobile node can tunnel them to its home agent, in exactly the way as specified for broadcast packets. This method requires the mobile node's home agent to be a multicast router; that is, the home agent must be capable of forwarding IP multicast packets.

Alternatively, a mobile node that has an acquired a collocated care-of address can use that address as the IP Source Address of its multicast packets and send them directly to the foreign link. This method requires that one or more multicast routers be present on the foreign link. Further, this method is only useful if the multicast application does not use the IP Source Address of multicast packets as identity of sender, since a mobile node's care-of address changes when it moves [6].

A receiver must send IGMP Host Membership Reports on its attached network to inform a neighboring multicast router that the node whishes to receive multicasts for a specified group. A mobile node that is connected to a foreign link has two options available if it wishes to receive multicasts.

The first option is for the mobile node to tunnel IGMP packets to its home agent – which assumes that its home agent is also a multicast router. The home agent then adds the mobile node to the multicast delivery tree [6]. To actually deliver multicast packets, the home agent tunnels them to the mobile node. The form of these tunneled packets depends on whether the mobile node is using a foreign agent care-of address or a collocated care-of address, and the mechanism is exactly the same as it is described for broadcast packets in Receiving Broadcasts with a foreign agent care-of address and Receiving Broadcasts with a collocated care-of address.

This first option, in which the mobile node joins the multicast delivery tree by way of its home agent, is useful in those situations where the multicast group is administratively restricted to a specific set of networks owned, for instance, by a

single corporation. In such a case, multicast packets tunneled to the mobile node by its home agent can be encrypted, authenticated, or both if the mobile node is currently connecting via a public, untrusted network.

The second option for a mobile node that wishes to receive multicasts is for the mobile node to send IGMP Host Membership Reports directly on the foreign link. This assumes that there is at least one multicast router present on the foreign link. If the mobile node has a collocated care-of address, then the mobile node should use this address as the IP Source Address of its IGMP packets, though a mobile node with a foreign agent care-of address may use its home address to send these packets. The reason the latter is permissible is that the IGMP messages merely inform the neighboring multicast router that there is a receiver present – the multicast router normally does not care about the identity of receiver.

The second option, in which the mobile node joins the multicast delivery tree by way of a multicast router on a foreign link, might be more efficient than joining by way of its home agent. This would be the case when there are many receivers of single multicast group simultaneously connected to the same network. In the first method, each such receiver would obtain a private copy of the multicast via a tunnel from its home agent, which further implies many transmissions on the foreign link. In the second method, the multicast router transmits each individual multicast packet only once on the foreign link.

Finally, a mobile node that joins a group via a router on a foreign link must rejoin that group when it moves to a new link, if it wishes to remain a member of that group [6,26].

2.4.7 Tunneling

The tunnel is the path followed by a datagram while it is encapsulated. The model is that, while it is encapsulated, a datagram is routed to a knowledgeable decapsulating agent, which decapsulates the datagram and then correctly delivers it to its ultimate destination [26].

First, IP Fragmentation is described shortly, since fragmented IP packets affect which type of encapsulation methods can be used by a tunnel entry-point. Then it is described the three types of tunneling used by Mobile IP: IP in IP Encapsulation, Minimal Encapsulation, and GRE.

2.4.7.1 IP fragmentation

Many link layers and the hardware over which they run place the upper limit on the size of a frame that they are capable of transferring. This limit, called the link MTU (Maximum Transfer Unit), in turn limits the maximum size of an IP packet that may be transferred within a single frame. An IP packet, which is larger than the link MTU of the link over which it is to be forwarded must be fragmented before it, may be transmitted. Fragmentation is the process by which a large IP packet is chopped up into smaller pieces in order for the smaller pieces to fit within a link's MTU.

IP fragmentation is performed either by the original source of a packet or by a router along the path to the ultimate destination. The fragments are created in such a way as to be reassembled at the ultimate destination of the original packet. The exception is fragmentation that occurs within a tunnel, where the tunnel fragments are reassembled at the tunnel's exit-point, which, in fact, is the ultimate destination of the tunneling packet.

2.4.7.2 IP in IP encapsulation

IP in IP Encapsulation [29] provides a standard method of encapsulating IPv4 packets within the payload portion of another IPv4 packet. Unlike Minimal Encapsulation, IP in IP Encapsulation works in all cases, whether the original IP packet is fragmented or not.

IP in IP Encapsulation requires more overhead – 20 bytes versus 8 or 12 – than Minimal Encapsulation. By maintaining soft state, tunnel entry points can relay ICMP messages generated within the tunnel to the original source of an offending packet [6].

2.4.7.3 Minimal encapsulation

Minimal Encapsulation [30] can save usually 8 bytes over IP in IP Encapsulation but carries with it the following disadvantages:

- It does not work when an original packet is already fragmented.
- It results in the Time to Live of the original packet being decremented at every router within the tunnel, which increases the change that a mobile node is reached if its home agent uses Minimal Encapsulation.

- Its mysteriously chosen packet layout does not put the Original Source Address in an area that guarantees it will be returned by an ICMP message within the tunnel, implying that a tunnel entry-point still has to implement soft state in order to relay such messages to the original source of the packet.

2.4.7.4 Generic routing encapsulation (GRE)

Generic Routing Encapsulation [31] is the final tunneling method accommodated by Mobile IP. GRE supports other network-layer protocols in addition to IP. It allows a packet of a first protocol suite to be encapsulated within the payload portion of a packet of a second protocol suite. This is in contrast to IP in IP Encapsulation and Minimal Encapsulation, both of which support only IP.

2.5 Mobility for IP Version 6 (Mobile IPv6)

This section discusses mobility support for Internet Protocol Version 6 (IPv6). IPv6 is the next generation of the Internet Protocol, which will ultimately replace IPv4 as the primary network-layer protocol of the Internet.

The Mobile IPv6 protocol is just as suitable for mobility across homogeneous media as for mobility across heterogeneous media. For example, Mobile IPv6 facilitates node movement from one Ethernet segment to another as well as it facilitates node movement from an Ethernet segment to a wireless LAN cell, with the mobile node's IP address remaining unchanged in spite of such movement [27].

Mobile IPv6 does not attempt to solve all general problems related to the use of mobile computers or wireless networks. In particular, this protocol does not attempt to solve:

- Handling links with partial reachability, or unidirectional connectivity, such as are often found in wireless networks.
- Access control on a link being visited by a mobile node.
- Local or hierarchical forms of mobility management (similar to many current link-layer mobility management solutions).
- Assistance for adaptive applications.
- Mobile routers.

- Service Discovery.
- Distinguishing between packets lost due to bit errors vs. network congestion [27].

2.5.1 The basic operation of Mobile IPv6

The operation of Mobile IPv6 can be summarized as follows [6]:

- A mobile node determines its current location using the IPv6 version of Router Discovery.
- The mobile node acts like any fixed host or router when connected to its home link; otherwise, in the case of a foreign link.
- A mobile node uses IPv6-defined address autoconfiguration to acquire a (collocated) care-of address on the foreign link.
- The mobile node notifies its home agent of its care-of address.
- The mobile node also reports its care-of address to select correspondents, assuming it can do securely.
- Packets sent by correspondents that are ignorant of the mobile node's care-of address are routed just as in Mobile IPv4 – namely, they are routed to the mobile node's home network, where the home agent tunnels them to the care-of address.
- Packets sent by correspondents that know the mobile node's care-of address are sent directly to the mobile node using IPv6 Routing Header, which specifies the mobile node's care-of address as an intermediate destination.
- In the reverse direction, packets sent by a mobile node are routed directly to their destination using no special mechanisms; however, in the presence of ingress filtering, the mobile node can tunnel packets to its home agent using its care-of address as the IP Source Address of the tunnel.

2.5.2 Location determination

This subsection describes Mobile IPv6 Agent Discovery, the process by which a mobile node:

- Determines whether it is currently connected to its home link or a foreign link.
- Detects whether it has moved from one link to another.
- Obtains a care-of address when connected to a foreign link.

2.5.2.1 Router discovery

ICMPv6 Router Discovery is very similar to Mobile IPv4 Agent Discovery. Router Discovery defined in the IPv6 Neighbor Discovery document [20], consists of two messages: Router Solicitations and Router Advertisements. As before Router Advertisements are periodically transmitted as broadcasts by routers and home agents on each of their attached link. Mobile nodes that are too impatient to wait for the next periodically transmitted Router Advertisements send router Solicitations. As in Mobile IPv4, Router Discovery messages do not require to be authenticated.

First of all, the mobile node examines the network-prefixes contained in received advertisements. If any of these prefixes match the network-prefix of the mobile node's home address, then the mobile node is connected to its home link. At this point, the mobile node should inform its home agent that it has returned home.

Otherwise, if none of prefixes matches the network-prefix of the mobile node's home address, then the mobile node is connected to a foreign link. At this point, the mobile node compares the prefixes in the most recently received advertisement with those of previous advertisements to see if it has moved.

2.5.2.2 Obtaining a care-of address

There are two methods by which a mobile node can acquire a care-of address, once it determines that it is connected to a foreign link. Recall that there is no such thing as a foreign agent in Mobile IPv6, so the only type of care-of address in the Mobile IPv6 is the collocated care-of address. A mobile node uses the M bit at any received Router Advertisements to determine which method should be used. If M bit is equal to 1, then the mobile node uses Stateful Address Autoconfiguration; otherwise the mobile node uses Stateless Address Autoconfiguration [10,19].

Mobile nodes can acquire a care-of address by Stateful Address Autoconfiguration, which is fancy way of saying, "from a server that remembers what address it handed out of whom". In this method, the mobile node simply asks a server for an address

and uses that address as a care-of address. As in IPv4, one protocol for "stateful" address assignment is the Dynamic Host Configuration Protocol for IPv6 (DHCPv6). DHCPv6 is very similar to DHCP for IPv4. Also PPP's IPv6 Configuration Protocol provides a method by which a server can provide a mobile node with a care-of address [6].

Mobile nodes can also acquire a care-of address by "Stateless Address Autoconfiguration", which is a fancy way of saying "automatically". Stateless Address Autoconfiguration [10,19] is new to IPv6, meaning that there is no similar functionality defined in IPv4. Simplifying greatly, Stateless Address Autoconfiguration works as follows:

- The mobile node first forms an interface token, a link-dependent identifier for the interface by which it connects to the foreign link. The interface token is typically the node's link-layer address on that interface. For example, on Ethernet, the interface token would be the mobile node's 48-bit Ethernet address.
- The mobile node examines the Prefix Information Options that are contained within Router Advertisements to determine the valid network-prefix on the current link.
- The mobile node forms a care-of address by concatenating one of the valid network prefixes with the interface token.

Address Autoconfiguration, both stateful and stateless, contains mechanisms by which a node can determine whether the address it has acquired is identical to an address being used by any other node on the link. If there is such a duplicate address, then the autoconfiguration protocols define ways in which a unique address can be acquired by the node [6].

2.5.3 Notification

This subsection describes the Mobile IPv6 equivalent of Mobile IPv4 Registration, which is used by mobile nodes to inform their home agent and various other nodes of their current care-of address. The term Notification is used because Mobile IPv6 Notification is very different from Mobile IPv4 Registration.

Mobile IPv6 Notification is the method by which a mobile node informs both its home agent and various correspondent nodes of its current care-of address. The home agent uses the care-of address as the exit point of a tunnel to get packets to the mobile node when it is connected to a foreign link, as in Mobile IPv4. In addition, correspondent nodes use the care-of address to route packets directly to the mobile node, without requiring the packet to be routed first to the mobile node's home agent. Thus, Mobile IPv6 has built-in support for route optimization. Mobile nodes must also notify their home agents when they return to their home link.

Like Mobile IPv4 Registration, Notification consists of a simple exchange of messages. However, Mobile IPv6 Notification uses an extension to the IPv6 packet header to realize its exchange, whereas Mobile IPv4 uses messages within the payload of UDP/IP packets [6, 27].

2.5.3.1 Notification scenarios

Mobile IPv6 Notification consists of an exchange of a Binding Update and a Binding Acknowledgement between a mobile node and a home agent or correspondent node, possibly prompted by the mobile node receiving a Binding Request. These message exchanges for common scenarios [6] are as follows:

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

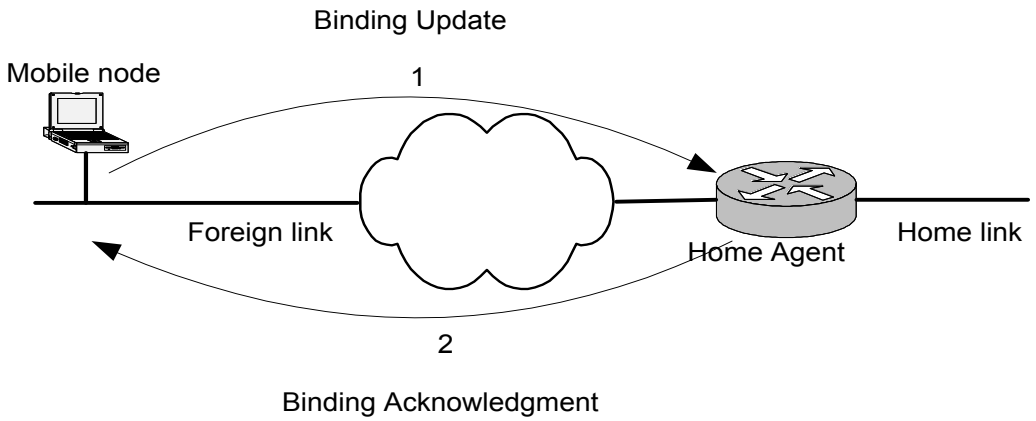

Figure 2.5. Notification scenario 1 of a mobile node

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

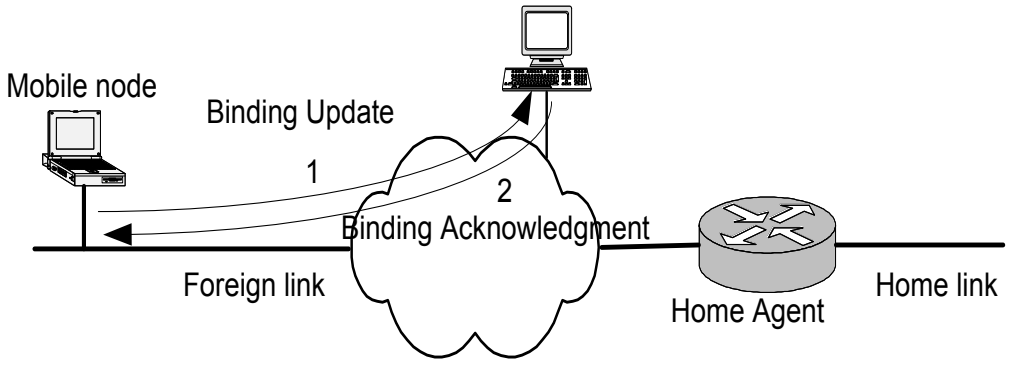

Figure 2.6. Notification scenario 2 of a mobile node

- A mobile node returns to its home link and informs its home agent that is no longer attached to a foreign link:

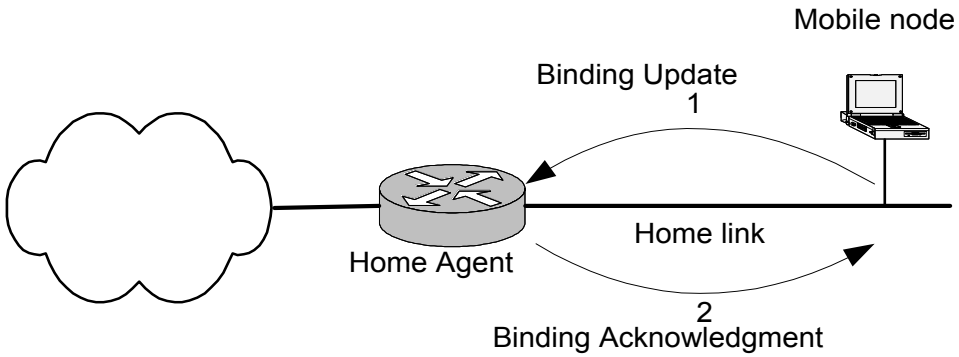

Figure 2.7. Notification scenario 3 of a mobile node

2.5.3.2 Notification messages

In some cases, a correspondent node initiates the notification process by sending a Binding Request to a mobile node. Otherwise, the mobile node initiates the process by sending a Binding Update. In both cases, the mobile node sends a Binding Update to its home agent or a correspondent node to inform them of its current care-of address. The mobile node can specify within a Binding Update whether or not the receiver should respond by sending a Binding Acknowledgment to the mobile node. The Binding Acknowledgment tells the mobile node first that the original Binding Update was received and second whether it was accepted or rejected.

The three messages defined for Mobile IPv6 Notification are Binding Updates, Binding Acknowledgments, and Binding Requests. All of these messages are encoded as options to be carried within a Destination Options Header. This means

that the options are examined only by the ultimate destination and not by any of the routers along the path [6].

2.5.3.3 Sending time of binding update messages

A mobile node should send Binding Updates to its home agent and to various correspondent nodes.

A mobile node that moves to a new link acquires a care-of address on that link and then immediately sends a Binding Update to its home agent. The Binding Update has the H bit set to 1 to indicate that the mobile node expects the receiving node to act as its home agent. Also the A bit is set to 1 to request that the home agent send a Binding Acknowledgment upon receiving the Binding Update. As in Mobile IPv4, the mobile node retransmits the Binding Update until it receives a Binding Acknowledgment [6].

Correspondent nodes that have received a Binding Update from a mobile node can send packets directly to that mobile node without the packets being routed first to the mobile node's home link. Thus, it is desirable for a mobile node to send Binding Updates to correspondent nodes with which it will be communicating while connected to a given link [6].

2.5.4 Routing in Mobile IPv6

Because mobile nodes send and receive packets just like any other (fixed) node when they are connected to their home link, the remainder of this section assumes that a mobile node is connected to a foreign link. Also it is assumed that the mobile node has already notified its home agent of its current care-of address [27].

2.5.4.1 Correspondents that know the care-of address of a mobile node

A correspondent node that knows a mobile node's care-of address sends packets directly to the mobile node using an IPv6 Routing Header. These packets do not necessarily pass through the mobile node's home agent; rather, they take an optimal route from the correspondent node to the mobile node.

The IPv6 Routing Header, as defined in [27], contains a list of intermediate destinations that a packet containing the header must visit along its path to the ultimate destination. Note that, especially in Mobile IPv6, a mobile node's care-of address makes a fine choice for such an intermediate destination, since the care-of

address is collocated with the mobile node itself. Thus, a correspondent node specifies the mobile node's care-of address as the lone intermediate destination within a Routing Header in order to route a packet directly to the mobile node at its current location.

2.5.4.2 Correspondents that do not know the care-of address of a mobile node

If a correspondent node does not know a mobile node's care-of address, then it sends packets to the mobile node just as it would send packets to any other (fixed) node. In this case, the correspondent node simply places the mobile node's home address – the only address it knows – in the IPv6 Destination Address field and places its own address in the IPv6 Source Address field. The correspondent node then forwards the packet to a suitable Next Hop, as determined by examining its IPv6 routing table.

A packet sent in this way will be routed toward the mobile node's home link in the same way as in Mobile IPv4. There, the home agent will intercept the packet and tunnel it to the care-of address. The mobile node decapsulates the packet sees that the inner packet is destined to its home address, and passes the inner packet up to the higher-layer protocol.

So far, it is identical to packet routing in Mobile IPv4. However, in Mobile IPv6, the mobile node interprets the presence of the tunnel to mean that the correspondent node does not know the mobile node's current care-of address. Thus, if the mobile node can develop a security association with that correspondent node, then the mobile node might send a Binding Update to it, based upon its policy for sending Binding Updates. Once this occurs, the correspondent node can then send packets directly to the mobile node [6].

2.5.4.3 Packets sending process of mobile node

When a mobile node is connected to a foreign link, it must have a way to determine a router that can forward packets generated by the mobile node. This is easier in Mobile IPv6 than it was in Mobile IPv4, because all IPv6 routers are required to implement Router Discovery. Thus, a mobile node can select any router on the foreign link from which it has received Router Advertisements. The mobile node configures its routing table such that all packets it generates are sent to this router.

2.6 Main Differences between Mobile IPv4 and Mobile IPv6

Both the experiences gained from the development of Mobile IP support in IPv4 (Mobile IPv4) and the opportunities provided by IPv6, affect the design of Mobile IP support in IPv6 (Mobile IPv6). Mobile IPv6 thus shares many features with Mobile IPv4, but is integrated into IPv6 and offers many other improvements. This section summarizes the major differences between Mobile IPv4 and Mobile IPv6:

- There is no need to deploy special routers as "foreign agents", as in Mobile IPv4. Mobile IPv6 operates in any location without any special support required from the local router.
- Support for route optimization is a fundamental part of the protocol, rather than a nonstandard set of extensions.
- Mobile IPv6 route optimization can operate securely even without pre-arranged security associations. It is expected that route optimization can be deployed on a global scale between all mobile nodes and correspondent nodes.
- Support is also integrated into Mobile IPv6 for allowing route optimization to coexist efficiently with routers that perform "ingress filtering"
- The IPv6 Neighbor Unreachability Detection assures symmetric reachability between the mobile node and its default router in the current location.
- Most packets sent to a mobile node while away from home in Mobile IPv6 are sent using an IPv6 routing header rather than IP encapsulation, reducing the amount of resulting overhead compared to Mobile IPv4.
- Mobile IPv6 is decoupled from any particular link layer, as it uses IPv6 Neighbor Discovery [20] instead of ARP. This also improves the robustness of the protocol.
- The use of IPv6 encapsulation (and the routing header) removes the need in Mobile IPv6 to manage "tunnel soft state".

- The dynamic home agent address discovery mechanism in Mobile IPv6 returns a single reply to the mobile node. The directed broadcast approach used in IPv4 returns separate replies from each home agent.

Other documents related with mobility are in [32-53].

3. SECURITY

In this chapter, it is given an introduction to computer and network security. When computer scientists and network managers talk about security, they are generally referring to the science of protecting computers, network resources, and information against unauthorized access, modification, and destruction. This generally involves four related topics, the definition of which has been paraphrased from Security Architecture for the Internet Protocol [54]:

- Confidentiality – transforming data such that only authorized parties can decode it.
- Authentication – proving or disproving someone's or something's claimed identity.
- Integrity checking – ensuring that data cannot be modified without such modification being detectable.
- Non-repudiation – proving that a source of some data did in fact send data that he might later deny sending.

Broadly speaking, technology employed to accomplish all of these security features is called cryptography [6].

This chapter is presented in few sections. First, cryptology is explained basically. Then, some of security protocols are presented. Next, some security threads in a mobile system are shown. And then, origin of security problems of Mobile IP is presented. Finally, some existing security solutions are shown.

3.1 Cryptography

A cryptographic system consists of two fundamental components: a complicated mathematical function, called an algorithm, and one or more secret or public values, called keys. A key is a chunk of binary data that is (supposed to be) known only to the parties, which wish to communicate securely. In contrast, an algorithm is usually published and is available to anyone who wants to read it. This state of affairs is

fortunate, because it is relatively easy to generate a new chunk of binary data (a key) but difficult to devise new cryptographic algorithms.

A strong cryptographic algorithm is one that has withstood the attempts of really smart mathematicians to break it. An algorithm is said to be broken when someone figures out a weakness or a flaw that can be exploited by Bad Guys to do bad things. When an algorithm is broken to the point at which it can be easily defeated, then it ceases to be useful. Algorithms are considered to be good ones when many smart people have tried to break them, over long period of time, without being successful.

A good key is one that is known only to the appropriate person, is not easily guessable, and is sufficiently long. Specifically, a key should be long enough to withstand brute-force attacks in which a Bad Guy simply tries every possible key until he finds the right one. A cryptographic system is not considered to be secure unless it uses a strong algorithm [8].

3.2 Security Architecture for the Internet Protocol (IPSec)

IPSec is designed to provide interoperable, high quality, cryptographically based security for IPv4 and IPv6. The set of security services offered includes access control, connectionless integrity, data origin authentication, replay protection (a form of partial sequence integrity), confidentiality (encryption) and limited traffic flow confidentiality. These services are provided at the IP layer, offering protection for IP and/or upper layer protocols.

These objectives are met through the use of two traffic security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols. The set of IPSec protocols employed in any context, and the ways in which they are employed, will be determined by the security and system requirements of users, applications, and/or sites/organizations.

When these mechanisms are correctly implemented and deployed, they ought not to adversely affect users, hosts, and other Internet components that do not employ these security mechanisms for protection of their traffic. These mechanisms also are designed to be algorithm-independent. This modularity permits selection of different sets of algorithms without affecting the other parts of the implementation. For

example, different user communities may select different sets of algorithms (creating cliques) if required.

A standard set of default algorithms is specified to facilitate interoperability in the global Internet. The use of these algorithms, in conjunction with IPSec traffic protection and key management protocols, is intended to permit system and application developers to deploy high quality, Internet layer, cryptographic security technology [54].

3.2.1 The roles of IPSec

IPSec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithms to use for the services, and put in place any cryptographic keys required to provide the requested services. IPSec can be used to protect one or more "paths" between a pair of hosts, between a pair of security gateways, or between a security gateway and a host. (The term "security gateway" is used throughout the IPSec documents to refer to an intermediate system that system implements IPSec protocols. For example, a router or a firewall implementing IPSec is a security gateway.)

The set of security services that IPSec can provide includes access control, connectionless integrity, data origin authentication, replayed packets rejection (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality. Because these services are provided at the IP layer, they can be used by any higher layer protocol, e.g., TCP, UDP, ICMP, etc [6,8,54].

3.2.2 IPSec working principles

IPSec uses two protocols to provide traffic security - AH and ESP. Both protocols are described in more detail in their respective RFCs [24,25].

- The AH [24] provides connectionless integrity, data origin authentication, and an optional anti-replay service.
- The ESP protocol [25] may provide confidentiality (encryption), and limited traffic flow confidentiality. It also may provide connectionless integrity, data origin authentication, and an anti-replay service. (One or the other set of these security services must be applied whenever ESP is invoked.)

- Both AH and ESP are vehicles for access control, based on the distribution of cryptographic keys and the management of traffic flows relative to these security protocols.

These protocols may be applied alone or in combination with each other to provide a desired set of security services in IPv4 and IPv6. Each protocol supports two modes of use: transport mode and tunnel mode. In transport mode the protocols provide protection primarily for upper layer protocols; in tunnel mode, the protocols are applied to tunneled IP packets [54].

3.2.3 Security associations (SA)

A Security Association (SA) is a simplex "connection" that affords security services to the traffic carried by it. Security services are afforded to an SA by the use of AH, or ESP, but not both. If both AH and ESP protection is applied to a traffic stream, then two (or more) SAs are created to afford protection to the traffic stream. To secure typical, bi-directional communication between two hosts, or between two security gateways, two SAs (one in each direction) are required.

An SA is uniquely identified by a triple consisting of a Security Parameter Index (SPI), an IP Destination Address, and a security protocol (AH or ESP) identifier. In principle, the Destination Address may be a unicast address; an IP broadcast address, or a multicast group address. However, IPSec SA management mechanisms currently are defined only for unicast SAs. Hence, in the discussions that follow, SAs will be described in the context of point-to-point communication, even though the concept is applicable in the point-to-multipoint case as well.

Two types of SAs are defined: transport mode and tunnel mode. A transport mode SA is a security association between two hosts. In IPv4, a transport mode security protocol header appears immediately after the IP header and any options, and before any higher layer protocols (e.g., TCP or UDP). In IPv6, the security protocol header appears after the base IP header and extensions, but may appear before or after destination options, and before higher layer protocols. In the case of ESP, a transport mode SA provides security services only for these higher layer protocols, not for the IP header or any extension headers preceding the ESP header. In the case of AH, the protection is also extended to selected portions of the IP header, selected portions of

extension headers, and selected options (contained in the IPv4 header, IPv6 Hop-by-Hop extension header, or IPv6 Destination extension headers).

A tunnel mode SA is essentially an SA applied to an IP tunnel. Whenever either end of a security association is a security gateway, the SA must be tunnel mode. Thus an SA between two security gateways is always a tunnel mode SA, as is an SA between a host and a security gateway. Note that for the case where traffic is destined for a security gateway, e.g., SNMP commands, the security gateway is acting as a host and transport mode is allowed. But in that case, the security gateway is not acting as a gateway, i.e., not transiting traffic. Two hosts may establish a tunnel mode SA between themselves. The requirement for any (transit traffic) SA involving a security gateway to be a tunnel SA arises due to the need to avoid potential problems with regard to fragmentation and reassembly of IPSec packets, and in circumstances where multiple paths (e.g., via different security gateways) exist to the same destination behind the security gateways.

For a tunnel mode SA, there is an "outer" IP header that specifies the IPSec processing destination, plus an "inner" IP header that specifies the (apparently) ultimate destination for the packet. The security protocol header appears after the outer IP header, and before the inner IP header. If AH is employed in tunnel mode, portions of the outer IP header are afforded protection (as above), as well as the entire tunneled IP packet (i.e., all of the inner IP header is protected, as well as higher layer protocols). If ESP is employed, the protection is afforded only to the tunneled packet, onto the outer header [54].

3.3 IP Authentication Header (AH)

The AH is used to provide connectionless integrity and data origin authentication for IP datagram, and to provide protection against replays. Latter this, optional service may be selected, by the receiver, when an SA is established. (Although the default calls for the sender to increment the Sequence Number used for anti-replay, the service is effective only if the receiver checks the Sequence Number.) AH provides authentication for as much of the IP header as possible, as well as for upper level protocol data. However, some IP header fields may change in transit and the value of these fields, when the packet arrives at the receiver, may not be predictable by the

sender. The values of such fields cannot be protected by AH. Thus the protection provided to the IP header by AH is somewhat piecemeal [24].

3.4 IP Encapsulating Security Payload (ESP)

The ESP header is designed to provide a mix of security services in IPv4 and IPv6. ESP may be applied alone, in combination with the IP Authentication Header [24], or in a nested fashion, e.g., through the use of tunnel mode [54]. Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a host.

The ESP header is inserted after the IP header and before the upper layer protocol header (transport mode) or before an encapsulated IP header (tunnel mode).

ESP is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality. The set of services provided depends on options selected at the time of SA establishment and on the placement of the implementation. Confidentiality may be selected independent of all other services. However, use of confidentiality without integrity/authentication (either in ESP or separately in AH) may subject traffic to certain forms of active attacks that could undermine the confidentiality service. Data origin authentication and connectionless integrity are joint services and are offered as an option in conjunction with confidentiality. The anti-replay service may be selected only if data origin authentication is selected, and its election is solely at the discretion of the receiver. (Although the default calls for the sender to increment the Sequence Number used for anti-replay, the service is effective only if the receiver checks the Sequence Number.) Traffic flow confidentiality requires selection of tunnel mode, and is most effective if implemented at a security gateway, where traffic aggregation may be able to mask true source-destination patterns. Note that although both confidentiality and authentication are optional, at least one of them must be selected [25].

3.5 Other Security Protocols

There are many other security protocols used in the Internet. It is mentioned some of them below:

- Secure SHell (SSH) and Secure CoPy (SCP) provide secure remote login, command execution, and file transfer in the Unix.
- SOCK provides a general mechanism for secure, application-layer, firewall traversal.
- The Secure Socket Layer (SSL) and the Secure HyperText Transfer Protocol (S-HTTP) are frequently used to provide confidentiality and authentication for the World Wide Web (WWW) and for other applications.

3.6 Key Distribution

A cryptographic system is considered to be secure only if it uses a strong algorithm, avoids certain pitfalls, and chooses and distributes keys carefully. A well-chosen key is one that is not easy guessable and is sufficiently long. A well-managed key is one that is known only to the appropriate person. The challenge of key management is to make sure that no one other than the intended person can obtain the appropriate keys, particularly when keys must be distributed to various individuals over a network. Specifically:

- If two parties wish to communicate securely using secret-key cryptology [8], then only those two parties are able to obtain a copy of their shared, secret key.
- If two parties wish to communicate securely using public-key cryptography [8], then each individual is able to obtain the other person's public key authentically; i.e., each is able to determine that they have indeed obtained the other person's public key and not one substituted by a Bad Guy.

Key management in secret-key cryptography is extremely difficult to do securely. However, if it can be figured out a way to manage public keys securely, then it can be always encrypted a secret key using a public-key encryption algorithm before sending it over the network. Thus, if it can be solved the easier problem of distributing public keys securely, then it can be also solved the harder problem of distributing secret keys securely [6].

3.7 Some Security Threats in a Mobile System

There are lots of security threats in a mobile system. However, only three of them are explained in this section.

3.7.1 A denial-of service attack

Generally speaking, a denial-of service attack is something that a Bad Guy does in order to prevent someone from getting useful work done. In the context of computer networking, a denial-of service attack usually takes one of the following forms:

- By sending a tremendous number of packets to a host (e.g., a Web server), a Bad Guy can make the host's CPU processing too many useless packets. In the meantime, no useful information can be exchanged with the host while it processing the entire nuisance.
- A Bad Guy somehow interferes with the packets that are flowing between two nodes on the network. Generally speaking, a Bad Guy must be on the path between the two nodes in order wreak any such havoc [6].

In the first form attack, a popular method using spoofed Source IP Address send many TCP connection setup requests to bombard target host is known as "TCP SYN Flooding and IP Spoofing Attacks". One reason of making spoofing possible is the fact that the IP unicast packet routing depends only on IP Destination Address without the need of the IP Source Address. This allows the attacker to spoof the IP Source Address while still being able to bombard the host with TCP connection requests.

In the second form of denial-of service attack, a Bad Guy generally, need be on the path between two corresponding hosts in order cut off their traffic flow completely. But in the case of Mobile IP, a Bad Guy can wage the denial-of service attack from anywhere in the network. As it is known, if a mobile node is connected on the foreign link, it must use registration to inform its home agent of its current care-of address to which the home agent will subsequently tunnel all packets destined to the mobile node's home address. So a Bad Guy can send a bogus registration request message specifying his own IP Address as the care-of address for a mobile node to the home agent. Thus, all packets sent by correspondent nodes will be tunneled to the Bad Guy while the mobile node cannot get deserved services [55].

3.7.2 Replay attack

The Mobile-Home Authentication Extension prevents the denial-of service attack described above. However, it is not enough by itself, because a Bad Guy could obtain a copy of a valid Registration Request, store it, and then "reply" it at a later time, thereby registering a bogus care-of address for the mobile node. To prevent this reply attack from happening, the mobile node generates a unique value of the Identification field in each successive attempted registration. The Identification field is generated in such a way as to allow the home agent to determine what the next value should be. In this way, the Bad Guy is thwarted because the home agent will recognize the Identification field in its stored Registration Request as being out-of-date.

Mobile IP specifies two ways in which the Identification field can be chosen in order to prevent these reply attacks. The first uses timestamps, wherein the mobile node uses its current estimate for the date-and-time-of-day in the Identification field. If this estimate is not sufficiently close to the home agent's estimate of the current time, then it rejects the mobile node's registration and at the same time provides the mobile node with enough information to synchronize its clock to the home agent's clock. Then, any future Identification values generated by the mobile node will be within the home agent's tolerance [6].

The other method uses random number named as nonces. In this method, the mobile node and the home agent specify the value placed in the Identification field accordingly. If either node receives a registration message in which the Identification field does not match the expected value, then the message is rejected in the case of the home agent or ignored in the case of mobile node. Also, using the latter method, a mobile node can synchronize to the home agent [55].

3.7.3 Theft of information attack

A serious threat faced by the mobile node on the network is theft of information. Generally speaking, this kind of attack can take one of the following two methods:

- Passive Eavesdropping: As it is known, the physical security is seldom perfect and unauthorized people are often unintentionally allowed to access the network. It should be noted that wireless links can provide a serious vulnerability, in that someone need not physically be connected to the network to gain access to the information being sent across the link.

- Session-Stealing Attack: A session-stealing attack is one in which a baddy waits for a legitimate node to authenticate itself and start an application session, then takes over the session by impersonating the identity of the legitimate node. The baddy firstly wait for a mobile node to register with its home agent and eavesdrop to see if the date being sent is valuable to him. Then he floods the mobile node with nuisance packets while stealing the session by sourcing packets that appear to have come from the mobile node and by intercepting packets destinated to the mobile node. In the meantime, the user of the mobile node might has no idea that his session has been hijacked because there is no indication showing like this has occurred.

3.8 Some Security Solutions for Mobile IP

In this section, three types of security solutions for Mobile IP are presented. First of them is security solution using Virtual Private Network. Second, security solution using Firewall is presented. And last, security solution using Authentication, Authorization, Accounting (AAA) Servers is described.

3.8.1 Security solution using virtual private network (VPN)

3.8.1.1 Mobile IPv4 home agents inside the Intranet behind a VPN gateway

Mobile IPv4 home agents are deployed inside the Intranet protected by a VPN gateway, and is not directly reachable by the mobile nodes outside the Intranet. Figure 3.1 shows the architecture of this scenario.

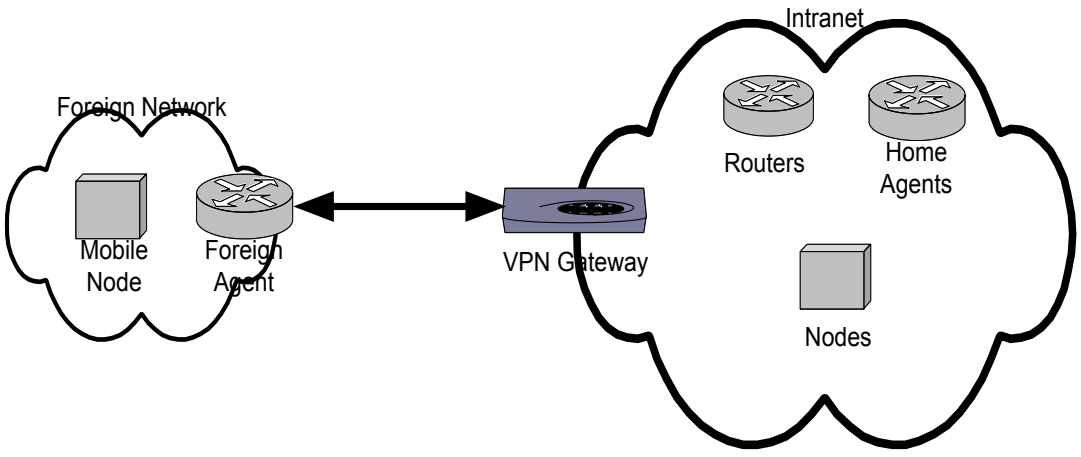

Figure 3.1. Mobile IPv4 home agents inside the Intranet behind a VPN gateway

Direct application of Mobile IPv4 standards [26] is successfully used to provide mobility for users inside the Intranet. However, mobile users outside the Intranet can

only access the intranet resources (e.g., Mobile IP agents) through the VPN Gateway, which will allow only authenticated IPSec traffic inside. This implies that the Mobile IPv4 traffic has to run inside IPSec, which leads to two distinct problems:

- When the foreign network has a foreign agent deployed, Mobile IPv4 registration becomes impossible because the traffic between mobile node and VPN Gateway, which the foreign agent sees, is encrypted and the foreign agent is not set up to decrypt it.
- In co-located mode, successful registration is possible but the VPN tunnel has to be re-negotiated every time the mobile node changes its point of network attachment.

This deployment scenario may not be common yet, but it is practical and becoming important as there is an increasing need for providing corporate remote users with continuous access to the Intranet resources [56].

3.8.1.2 VPN gateway and Mobile IPv4 home agents in parallel

A Mobile IPv4 home agent is deployed in parallel with the VPN gateway, and it is directly reachable by mobile nodes inside or outside the Intranet. Figure 3.2 shows the architecture of this scenario.

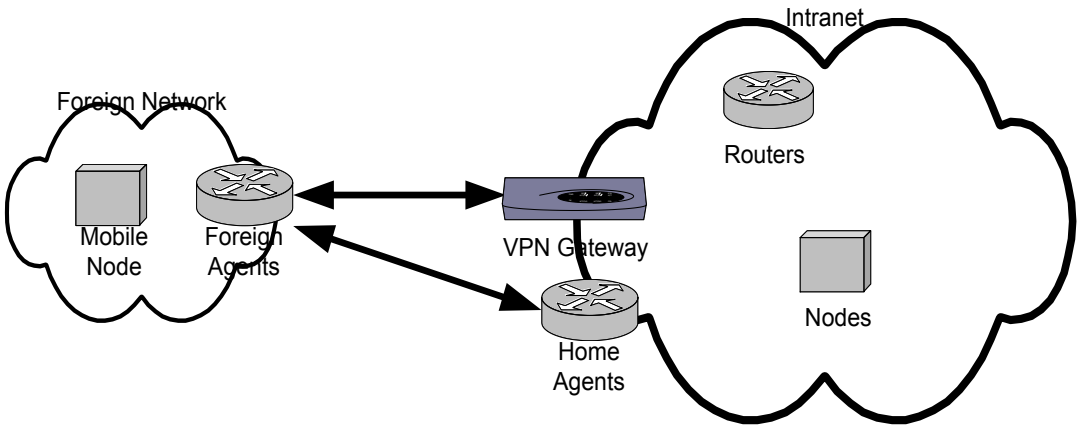

Figure 3.2. VPN gateway and Mobile IPv4 home agents in parallel

The Mobile IPv4 home agent has a public interface connected to the Internet, and a private interface attached to the Intranet. Mobile users will most likely have a virtual home network associated with the Mobile IPv4 home agent's private interface, so that the mobile users are always away from home and hence registered with the Mobile IPv4 home agent. Furthermore, in deployments where the VPN Gateway and the

home agent are placed in a corporate DMZ, this implies that Mobile IPv4 traffic will always be routed through the DMZ (regardless of whether mobile nodes are located outside or inside the Intranet), which may not be acceptable by IT departments in large corporations.

This deployment can be used with two different configurations: "Mobile IPv4 inside IPSec-ESP tunnel" and "IPSec-ESP inside Mobile IPv4 tunnel". The "Mobile IPv4 inside IPSec-ESP tunnel" has the same problems as the scenario of Section 3.8.1.1. The "IPSec-ESP inside Mobile IPv4 tunnel" does not have problems described in Section 3.8.1.1, however it will require some modifications to the routing logic of the Mobile IPv4 home agent or the VPN Gateway [56].

3.8.1.3 Combined VPN gateway and Mobile IPv4 home agent

This is similar to deployment scenario described in Section 3.8.1.2., with the exception that the VPN Gateway and Mobile IPv4 home agent are running on the same physical machine. Figure 3.3 shows the architecture of this scenario.

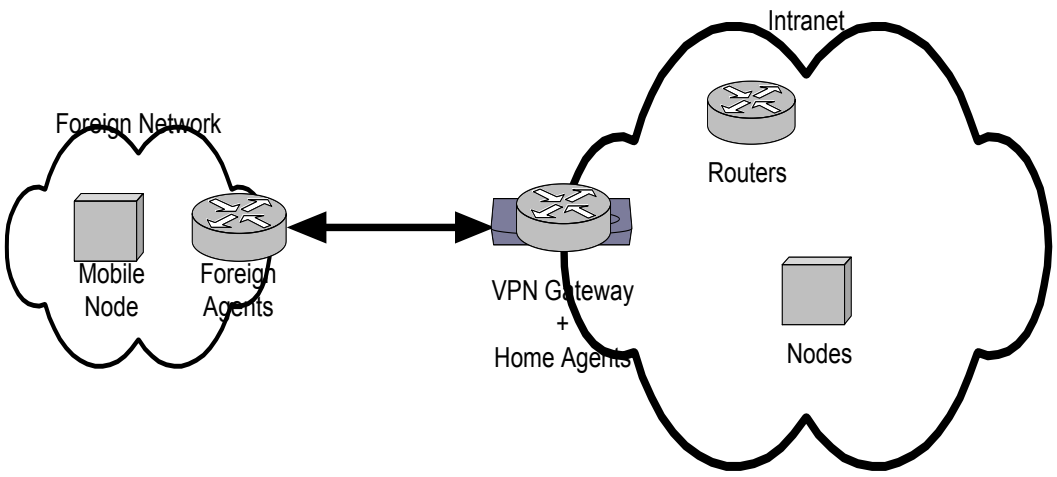

Figure 3.3. Combined VPN gateway and Mobile IPv4 home agent

Running Mobile IPv4 home agent and VPN on the same machine resolves routing related issues that exist in Section 3.8.1.2 when an "IPSec-ESP inside Mobile IPv4 tunnel" configuration is used. However, it does not promote multi-vendor interoperability in environments where Mobile IPv4 home agent and VPN technologies must be acquired from different vendors [56].

3.8.1.4 Mobile IPv4 home agents outside the VPN domain

In this scenario, Mobile IPv4 home agents are deployed outside the Intranet (e.g., in an operator network), as depicted in Figure 3.4 below.

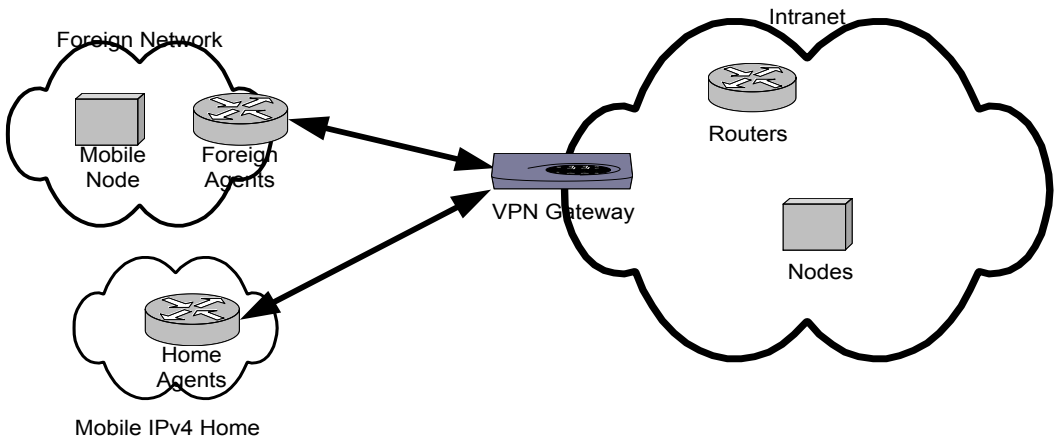

Figure 3.4. Mobile IPv4 home agents outside the VPN domain

This deployment works today without any technical problems with IPSec-ESP running inside a Mobile IPv4 tunnel. And it has the same problems as in Section 3.8.1.3 if Mobile IPv4 is run inside the IPSec-ESP tunnel. This is not common or practical for large deployments (on the order of thousands of users) because of the large and distributed security perimeter [56].

3.8.2 Security solution using firewall

A firewall is a device or a set of devices, which separates a trusted, private network from an untrusted, public network such as the Internet. A firewall protects a private network from intrusion by Bad Guys but it should not prevent people on the inside from exchanging information with others on the public network. The basic architecture of a firewall is shown in Figure 3.5. It is described two types of firewalls in this section.

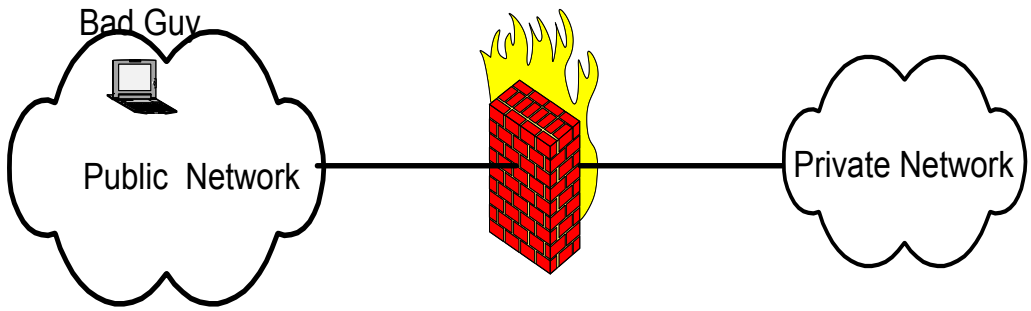

Figure 3.5. Basic architecture of a firewall

3.8.2.1 Packet-filtering router

Packet filtering router determines whether or not to forward a given packet by looking at the packet's header fields. Based upon these header fields the packet is classified according to a set of rules that are part of the router's configuration. These

rules specify whether certain packets may be forwarded or whether they must be discarded. Rules are also known as Access Control List (ACL). Packets that are discarded because of an ACL are said to filter or screened. Packet-Filtering Router is shown in Figure 3.6.

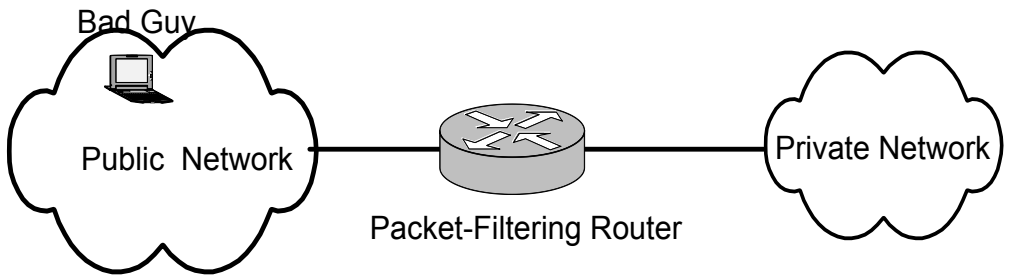

Figure 3.6. Packet-filtering router as firewall

Packet-filtering routers are attractive because they are fast and because they are largely independent of applications. They are fast because they perform relatively simple processing. They are independent of applications because they do not have to be upgraded or replaced when a new application comes along. This is in contrast to application-layer relays. Finally, packet-filtering routers can be an inexpensive solution because most private networks already have a router of some sort, which they use to connect to the Internet.

The problem with packet-filtering firewalls is that they are extremely difficult to configure correctly. ACLs must frequently be written in an obscure syntax without the help of graphical user interfaces. Any mistake in an ACL can leave the private network vulnerable to attack by a Bad Guy. Often, there is no way to verify that a set of ACLs is correct until it is too late.

There are other problems with packet-filtering routers. Because they are by definition routers, the IP address of the machines in the private network are visible to the public network, making those machines more vulnerable to attack than they might otherwise be. Also, a good security system has the ability to log suspect activity, and routers generally have little or no disk space on which to record such events. Finally, they do not support certain security policies, such as requiring users to be authenticated before being allowed to communicate outside the firewall [6].

3.8.2.2 Application-layer relay

A configuration involving an application-layer relay is shown in Figure 3.7.

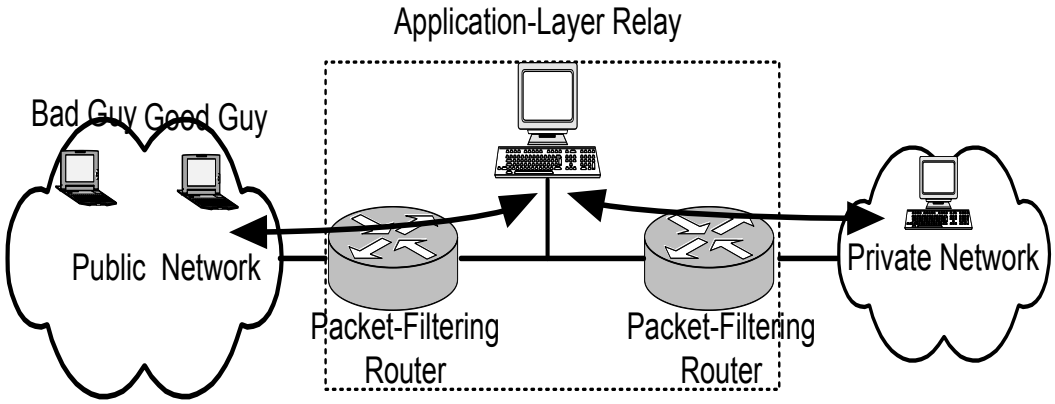

Figure 3.7. Application-layer relay as firewall

A host in a private network sets up a connection to the firewall and sends application-layer data to the firewall. The firewall then relays this application-layer data over a new connection that it sets up to the ultimate destination host. The two routers in the figure are configuring with ACLs, which allow packets only to and from the relay host. Specifically, the routers do not allow any packets to flow directly between the private network and the public network.

Application-layer relay are able to enforce more sophisticated security policies because they understand not only packet headers but also the applications themselves. In addition, they are often easier to configure and they are able to hide from the public network the address of nodes within the private network. Because they can be built with plenty of disk capacity, they have the ability to provide full auditing and logging capability.

Application-layer relays are normally slower than packet-filtering routers, however, simply because they have much more work to do. Specifically, application-layer relays must process packets at all of the protocol layers and might have many TCP connections open at any given time. Also, by definition, an application-layer relay must specifically support an application before it can be used across the firewall. Typically, new applications are available to users well before the firewall catches up and is able to relay the associated traffic. An application-layer relay is thus “visible” to end users, who either must have firewall-aware applications or must modify their behavior in order to use their existing applications.

Another problem with application-layer relay is that they prevent even legitimate mobile users from enjoying the same connectivity they enjoy when connected to the private network. This because some applications that are in use in private network might not be supported by the firewall and possibly because the firewall does not work symmetrically in both directions [6].

3.8.3 Security solution using authentication, authorization, accounting (AAA) servers

3.8.3.1 Basic model of an AAA

In this section, it is attempt to capture the main features of a basic model for operation of AAA servers that seems to have good support within the Mobile IP working group. Within the Internet, a client belonging to one administrative domain (called the home domain) often needs to use resources provided by another administrative domain (called the foreign domain). An agent in the foreign domain that attends to the client's request (call the agent the "attendant") is likely to require that the client provide some credentials that can be authenticated before access to the resources is permitted. These credentials may be something the foreign domain understands, but in most cases they are assigned by, and understood only by the home domain, and may be used for setting up secure channels with the mobile node.

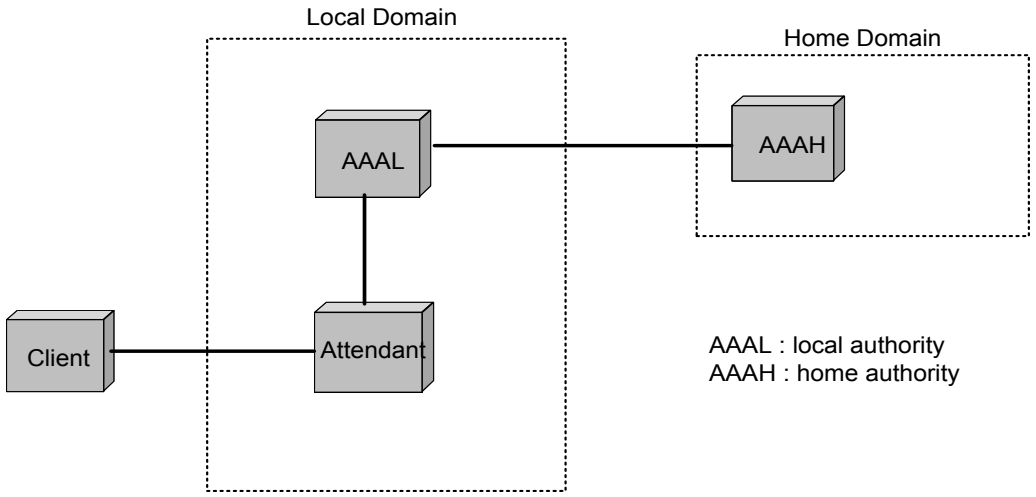

Figure 3.8. AAA servers in home and local domains

The attendant often does not have direct access to the data needed to complete the transaction. Instead, the attendant is expected to consult an authority (typically in the same foreign domain) in order to request proof that the client has acceptable credentials. Since the attendant and the local authority are part of the same

administrative domain, they are expected to have established, or be able to establish for the necessary lifetime, a secure channel for the purposes of exchanging sensitive (access) information, and keeping it private from (at least) the visiting mobile node.

The local authority (AAAL) itself may not have enough information stored locally to carry out the verification for the credentials of the client. In contrast to the attendant, however, the AAAL is expected to configure with enough information to negotiate the verification of client credentials with external authorities. The local and the external authorities should be configured with sufficient security relationships and access controls so that they, possibly without the need for any other AAA agents, can negotiate the authorization that may enable the client to have access to any/all requested resources. In many typical cases, the authorization depends only upon secure authentication of the client's credentials.

Once the local authority has obtained the authorization, and the authority has notified the attendant about the successful negotiation, the attendant can provide the requested resources to the client.

In Figure 3.8., there might be many attendants for each AAAL, and there might be many clients from many different Home Domains. Each Home Domain provides an AAAH that can check credentials originating from clients administered by that Home Domain.

There is a security model implicit in the above figure, and it is crucial to identify the specific security associations assumed in the security model.

First, it is natural to assume that the client has a security association with the AAAH, since that is roughly what it means for the client to belong to the home domain.

Second, from the model illustrated in Figure 3.8 it is clear that AAAL and AAAH have to share a security association, because otherwise they could not rely on the authentication results, authorizations, nor even the accounting data, which might be transacted between them. Requiring such bilateral security relationships is, however, in the end not scalable; the AAA framework must provide for more scalable mechanisms.

Finally, in Figure 3.8., it is clear that the attendant can naturally share an SA with the AAAL. This is necessary in order for the model to work because the attendant has to know that it is permissible to allocate the local resources to the client [57].

3.8.4 AAA for Mobile IP

Clients using Mobile IP require specific features from the AAA services, in addition to the requirements already mentioned in [57] connection with the basic AAA functionality and what is needed for IP connectivity. To understand the application of the general model for Mobile IP, it is considered the mobile node to be the client in Figure 3.8, and the attendant to be the foreign agent. If a situation arises that there is no foreign agent present, e.g., in the case of an IPv4 mobile node with a collocated care-of address or an IPv6 mobile node, the equivalent attendant functionality is to be provided by the address allocation entity, e.g., a DHCP server. The home agent, while important to Mobile IP, is allowed to play a role during the initial registration that is subordinate to the role played by the AAAH. For application to Mobile IP, it is modified the general model as illustrated in Figure 3.9. After the initial registration, the mobile node is authorized to continue using Mobile IP at the foreign domain without requiring further involvement by the AAA servers. Thus, the initial registration will probably take longer than subsequent Mobile IP registrations.

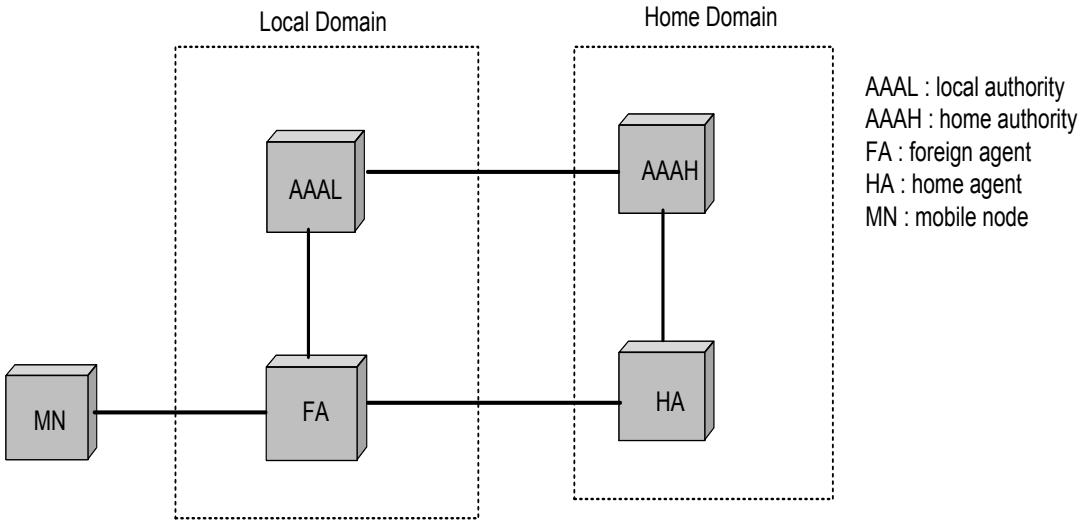

Figure 3.9. AAA servers with Mobile IP agents

In order to reduce this extra time overhead as much as possible, it is important to reduce the time taken for communications between the AAA servers. A major component of this communications latency is the time taken to traverse the wide-area Internet that is likely to separate the AAAL and the AAAH. This leads to a further strong motivation for integration of the AAA functions themselves, as well as integration of AAA functions with the initial Mobile IP registration. In order to reduce the number of messages that traverse the network for initial registration of a

mobile node, the AAA functions in the visited network (AAAL) and the home network (AAAH) need to interface with the foreign agent and the home agent to handle the registration message. Latency would be reduced as a result of initial registration being handled in conjunction with AAA and the Mobile IP mobility agents. Subsequent registrations, however, would be handled according to [6,26]. Another way to reduce latency as to accounting would be the exchange of small records.

As there are many different types of sub-services attendants may provide to mobile clients, there must be extensible accounting formats. In this way, the specific services being provided can be identified, as well as accounting support should more services be identified in the future.

The AAA home domain and the home agent home domain of the mobile node need not be part of the same administrative domain. Such a situation can occur if the home address of the mobile node is provided by one domain, e.g., an ISP that the mobile user uses while at home, and the authorization and accounting by another (specialized) domain, e.g., a credit card company. The foreign agent sends only the authentication information of the mobile node to the AAAL, which interfaces to the AAAH. After a successful authorization of the mobile node, the foreign agent is able to continue with the mobile IP registration procedure. Such a scheme introduces more delay if the access to the AAA functionality and the mobile IP protocol is sequentialized. Subsequent registrations would be handled according to [26] without further interaction with the AAA. Whether to combine or separate the Mobile IP protocol data with/from the AAA messages is ultimately a policy decision. Separation of the Mobile IP protocol data and the AAA messages can be successfully accomplished only if the IP address of the mobile node's home agent is provided to the foreign agent performing the attendant function.

All needed AAA and Mobile IP functions should be processed during a single Internet traversal. This must be done without requiring AAA servers to process protocol messages sent to Mobile IP agents. The AAA servers must identify the Mobile IP agents and SAs necessary to process the Mobile IP registration, pass the necessary registration data to those Mobile IP agents, and remain uninvolved in the routing and authentication processing steps particular to Mobile IP registration [57].

Other documents related with security are in [58-78].

4. A NEW SECURITY ARCHITECTURE OF MOBILE IPv4 TRAVERSING IPSEC BASED VPN GATEWAY

In this chapter, a new architecture is proposed, which the architecture enables seemless secure mobility when a mobile node traverses an IPSec based VPN Gateway. At first, related works on secure mobility in literature are overviewed. After this, components of the proposed architecture, the basic topology of the architecture and scenarios according to the position of a mobile node are given in sequence. Consequently, analysis of the new architecture is done according to experiments and analytical approach.

4.1 Related Works

T. Braun and M. Danzeisen describe a solution called Secure Mobile IP (SecMIP) to provide Mobile IP users secure access to their company's firewall protected VPN [74]. The organization's interior network is isolated from the Internet by a DMZ. The firewall between the DMZ and private interior network is the only entry point to the organization's private network. When the mobile node changes its care-of address, the mobile node dissolves the old IPSec tunnel and establishes a new IPSec tunnel according to the new care-of address. This solution needs dynamic SA support.

J. P. Aspas and F. B. Arroyo presented the design of a VPN supporting user mobility [69]. The VPN has two parts: the access network and the public Internet to connect to the corporate Intranet. The access network can be based on GPRS or a WLAN network. The system uses the security provided by the access network and IPSec in the public Internet. The mobility of the terminal is supported by the use of Mobile IP. Mobile nodes require dynamic set-up and tearing down of tunnels between various gateways on the basis of each user's current point-of attachment. Again, these dynamic set up of tunnels need dynamic SA support.

Y. Tsuda, et al described an implementation example of a system, "Network Crypto Gate (NCG)" [70], which employs the Mobile IPv4 and IPSec on stationary security

gateways (NCG servers) and mobile hosts (NCG clients). Using IP security primitives, both packets going into a corporate network and packets going out of the visiting network are securely guarded, however, it does not promote multi-vendor interoperability [57].

L. Morand and S. Tessier described a global mobility approach with Mobile IP in all IP networks [45]. They describe how the EURESCOM project P1013 FIT-MIP evaluates the use of Mobile IP in an IP core network, acting as a mobility management protocol federating heterogeneous access network technologies such as PSTN, WLAN or GPRS. The aim is to provide a wide IP environment with an always-on access to IP applications (Voice over IP, VPN, mobile Internet, etc.), Mobile IP functionalities enabling seemless mobility through the various networks. However, this architecture is only related with accessing to IP environments. It does not solve secure roaming between the Internet and the Intranet.

In contrast to these solutions, the new architecture enables seemless secure mobility between the Internet and the Intranet without any problem.

4.2 Components of the Proposed Architecture

The proposed architecture contains mainly five components, which are listed as Mobile Node (MN), Intranet Home Agent (aHA), Internet Home Agent (eHA), Foreign Agent and IPSec based VPN Gateway. The Foreign Agent and the VPN Gateway are same as described in the standard protocols. Therefore, they are not explained in this section.

4.2.1 Mobile node (MN)

The properties of the MN are as follows:

- The MN supports both Mobile IPv4 and IPSec.
- The MN operates in two modes, namely normal mode and secure mode. The MN supports functions defined in the standard Mobile IPv4 when it operates in normal mode. However, when operating in secure mode, it has additional properties. For instance, the MN only sends and receives user IP packets tunneled with IPSec.

- The MN has a network detection mechanism to detect where it roams, in the Internet or in the Intranet (This is different from movement detection described in standard [26]).

4.2.2 Intranet home agent (aHA)

The properties of the aHA are as follows:

- The aHA is located in the Intranet.
- The aHA supports all functions defined in Mobile IPv4 standard [26].
- The aHA's binding table contains information about modes of MNs that are registered to the aHA and the eHA.
- The aHA informs the eHA about MNs registered to it.
- The aHA is informed by the eHA about MNs registered to the eHA.
- The aHA serves to MNs in the Intranet.
- Also, the aHA serves to MNs which are in another network that can be accessed over an IPSec based VPN Gateway.
- The aHA serves in two modes for a node, which are master (active) mode and slave (passive) mode. When the aHA is in master mode for an MN, the aHA is able to communicate (to make binding updates related with this MN) with the MN. Whereas, when the aHA is in passive mode, it does not exchange any binding update message with the MN. In slave mode, the aHA is only ready to serve for this MN when it moves to the Intranet.
- When the aHA is in slave mode for an MN, it tunnels user IP packets to the eHA because it knows that the specified MN is in the Internet.
- When the aHA is in active mode for an MN, the aHA tunnel the user messages directly to the MN's care-of address (foreign agent care-of address or collocated care-of address).

4.2.3 Internet home agent (eHA)

The eHA is the new component in the proposed architecture. The properties of the eHA are as follows:

- The eHA supports both Mobile IPv4 and IPSec protocols.

- The eHA's binding table contains information about modes of MNs that are registered to the aHA and the eHA.
- The eHA informs the aHA about MNs registered to it.
- The eHA is informed by the aHA about MNs registered to the aHA.
- The eHA serves to MNs in the Internet.
- The eHA is able to establish an IPSec based VPN tunnel with the IPSec based VPN Gateway.
- The eHA serves in two modes, which are master (active) mode and slave (passive) mode, for a node. When the eHA is in master mode for an MN, the eHA is able to communicate (to make binding updates related with this MN) with the MN. Whereas, when the eHA is in passive mode, it does not exchange any binding update message with the MN. In slave mode, the eHA is only ready to serve for this MN when it moves to the Internet.
- When the eHA is in slave mode for an MN, the eHA is not responsible to affect any packet destined to the MN. The eHA is ready to serve to this MN as quickly as possible when the MN moves to the Internet.
- When the eHA is in master mode for an MN, it is responsible to tunnel the user IP packets to the MN, which packets are tunneled by the aHA in a Mobile IPv4 tunnel and by the IPSec based VPN Gateway in an IPSec tunnel.

4.3 The Basic Topology of the Proposed Architecture

The basic topology of this architecture is shown in Figure 4.1.

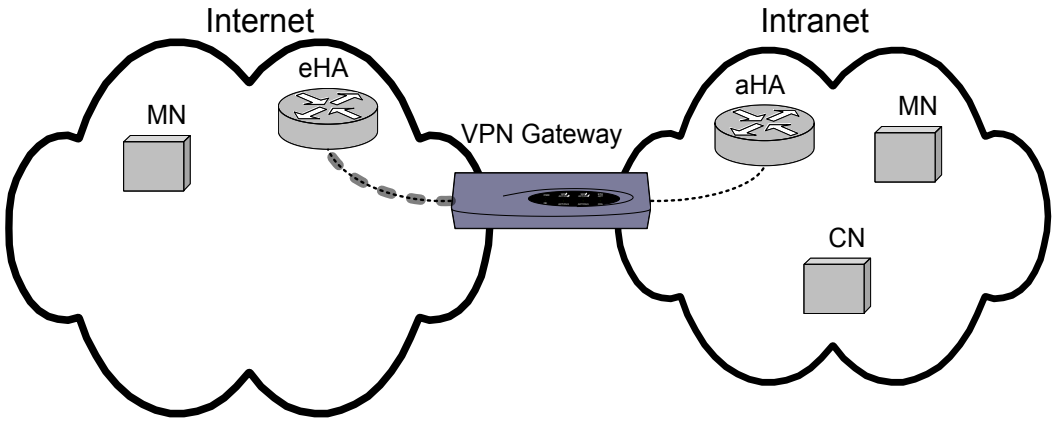

Figure 4.1. The basic topology of the proposed architecture

The eHA and the aHA communicate with each other to manage their binding tables related with an MN's state. An MN can only communicate with either the aHA or the eHA at any specific time. HAs work as slave (passive) HAs or as master (active) HAs for an MN. The aHA and the eHA send their binding table to each other over the VPN Gateway to determine ultimate mode of an MN that MN is registered to these HAs. For security reason, the eHA must be able to establish an IPSec tunnel with the VPN Gateway in order to exchange information messages with the aHA to update its binding table securely. In contrast to the eHA, the aHA does not need to establish any tunnel with the VPN Gateway because it is assumed to be in a secure network.

The MN can access any of HA at any time. When the MN is in the Intranet, it has to access to the aHA. But as soon as, it has left the Intranet, the eHA takes control. The aHA exchanges unencrypted data packets with the MN, but the eHA receives and sends only encrypted packets. Moreover, the eHA is not able to decrypt the packets destined to the MN. In contrast to data packets, Mobile IPv4 registration and update packets are exchanged as proposed in Mobile IPv4.

MNs can use a collocated care-of address or a foreign agent care-of address when they are in a foreign network. If the MN uses a foreign agent care-of address, packets destined to the MN traverse an FA as proposed in [26]. The relationship between the MN and the aHA is the same as described in the Mobile IPv4 standard. This solution provides mobility for all IP packets in the Intranet and mobility for IPSec traffic in the Internet. If the security of Mobile IPv4 in the Internet is broken in this context, traffic redirection attacks on the IPSec traffic are possible. However, such routing attacks do not affect other IPSec properties, because IPSec does not consider the network between two IPSec endpoints to be secure in any way.

When the MN traverses a VPN Gateway, it must be able to detect where it roams, because the MN has to know its location to maintain its communications securely. The MN sends plaintext packets in the Intranet, and ciphertext packets in the Internet. If the MN mistakenly believes that it is in the Intranet and sends plaintext packets although it is in the Internet, the IPSec security will be compromised undoubtedly. On the other hand, when the MN changes its network, the modes of the aHA and the eHA must be switched. For these reasons, the overall security, confidentiality and integrity of user data is a minimum of IPSec security and security

of the network detection mechanism. It is assumed in this thesis that on MN a network detection algorithm exists and works properly.

The main advantage of this architecture is to provide seemless mobility both in the Internet and in the Intranet. Moreover, as physically the Internet and the Intranet are separated from each other, there cannot be any leak between these two networks. Additionally, this architecture has some advantages over Mobile IP Proxy [62]. It does not cause any problem to use different IP address for a VPN client and for a Mobile IP client because of secure communication of HAs. As a final advantage, the proposed architecture is eliminating unnecessary messaging as the status of an MN is known by the aHA and by the eHA at any specific time.

4.4 Scenarios According to the Mobile Node

4.4.1 Mobile node in the Intranet

When the MN roams in the Intranet, mobility features are done as proposed in [26]. In this scenario, the MN uses the aHA as an HA to meet its requirements to roam in the Intranet. In addition to standard processes, the aHA informs the eHA about the MN's state as it is mentioned in Section 4.3. Figure 4.2 shows user data packets flow for this scenario.

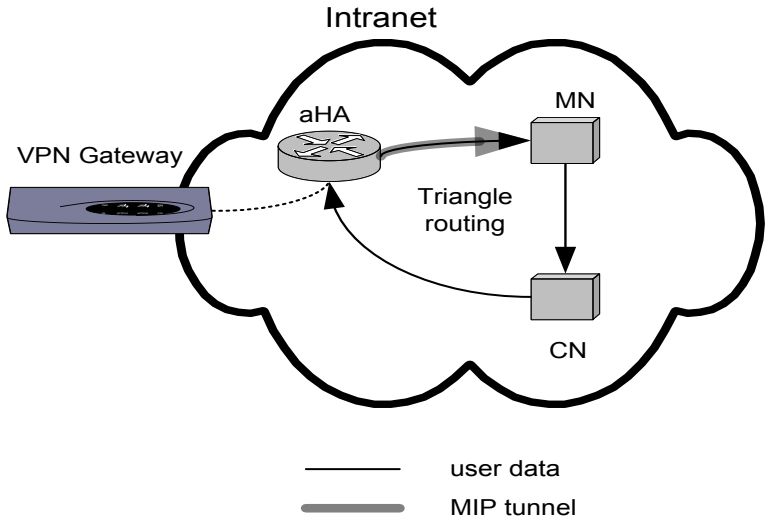

Figure 4.2. User data flow in the Intranet (triangle routing).

4.4.2 Mobile node moves from the Intranet to the Internet

In this scenario, the MN moves from the Intranet to the Internet traversing the VPN Gateway. When the MN changes its network, it needs to maintain its communications. To move from the Intranet to the Internet, the MN has to change its

active HA from the aHA to the eHA, and also its mode from the normal mode to the secure mode. Then, the MN can continue to communicate with the Correspondent Node (CN), without any interruption.

When the MN is in the Intranet, the registration and the binding updates are done as described in Section 4.4.1. When the MN moves form the Intranet to the Internet, it has to detect network change immediately, and has to stop sending plaintext IP packets in the normal mode.

4.4.3 Mobile node in the Internet

When the MN is in the Internet, it uses extra features that come with the new architecture. Figure 4.3 shows user data flow of this scenario.

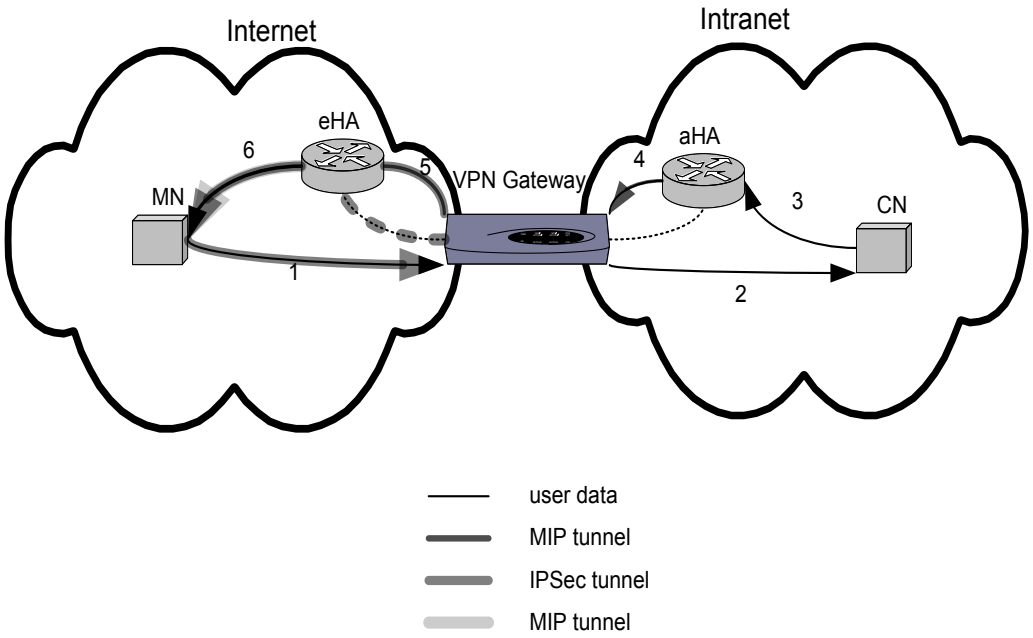

Figure 4.3. User data flow when the MN is in the Internet

The registration and the binding update are accomplished between the MN and the eHA according to standard mechanisms. Furthermore, the eHA informs the aHA about the MN. Informing the aHA is achieved via an IPSec tunnel, that tunnel is established between the eHA and the VPN Gateway. After the registration process, the MN can exchange user data with a CN.

The steps of user data flow are shown in Figure 4.3. First, the MN sends IP packets via an IPSec tunnel directly to the CN (denoted by 1 and 2 in Figure 4.3). The CN sends IP packets to the MN's permanent address, and these IP packets are received by the aHA (3). The aHA knows that the MN is in the Internet. So, it tunnels these IP

packets to the VPN Gateway through a Mobile IPv4 tunnel (4). In the next step, the VPN Gateway tunnels IP packets via an IPSec tunnel to the MN's permanent address (5). The eHA receives the tunneled IP packets and sends them through another Mobile IPv4 tunnel to the MN's care-of address (6). Finally, the MN receives tunneled packets and decapsulates them from Mobile IPv4 and IPSec tunnels.

4.4.4 Mobile node moves from the Internet to the Intranet

When the MN moves from the Internet to the Intranet, it detects the network change. Afterwards, the MN changes its mode from the secure mode to the normal mode. It also has to register itself to aHA to roam in the Intranet. On the other hand, when the aHA receives a registration message from an MN, it checks its binding table to decide whether MN is a new one or MN comes from Internet. In this scenario, the aHA concludes that the MN comes from the Internet, and it changes its mode according to the MN. If the registration step is completed successfully, the MN can keep on its communications.

4.4.5 Correspondent node as a mobile node

In the previous four scenarios, it is assumed that the CN is in the Intranet. It contains confidential information, and it is not allowed to move. However, the CN can be an MN, whose permanent IP Address is in the Intranet. Therefore, flow steps of messages will change, according to the CN's movement. In this case, packets destined to the CN are routed by the aHA as described in previous subsections.

4.5 Analysis of the Proposed Architecture

The new architecture is analyzed in three aspects: the IP packets size on path between a CN and an MN, overhead based on throughput and packet delay, and security.

4.5.1 Analysis of the IP packet size

In this section, IP packets analyses of the architecture are performed according to scenarios given in Section 4.4. At first, number of headers and their total size for paths from the aHA to the eHA, from the eHA to the aHA, from the MN to the CN and from the CN to the MN are calculated. Then, the increase or the decrease percentages of total headers are determined to find the header size characteristic and

number of headers characteristic. The total header size increase is defined as in Formula 4.1.

HSI = (THS-SIPHS)/SIPHS (4.1)

HSI = Header Size Increase

THS = Total size of headers on a packet (byte)

SIPHS = Standard IP Header Size (byte)

The HSI is used to determine extra load that is based on headers on network links.

In this thesis, the size of an IP header is assumed to be 20 bytes as a worst case (minimum value). The ESP header and the AH header sizes are assumed to be 10 and 12 bytes, respectively, because authentication data and padding fields are variable due to cryptographic algorithms.

Finally, all architecture is analyzed according to the results.

Related documents with this type of measurements results are in [79-83].

4.5.1.1 Analysis of binding exchange messages

In the new architecture, the aHA and the eHA construct their binding tables according to three different types of messages. These are normal registration messages, binding update messages and messages that come from the peer. User data flow and the HSI for this analysis are shown in Figure 4.4.

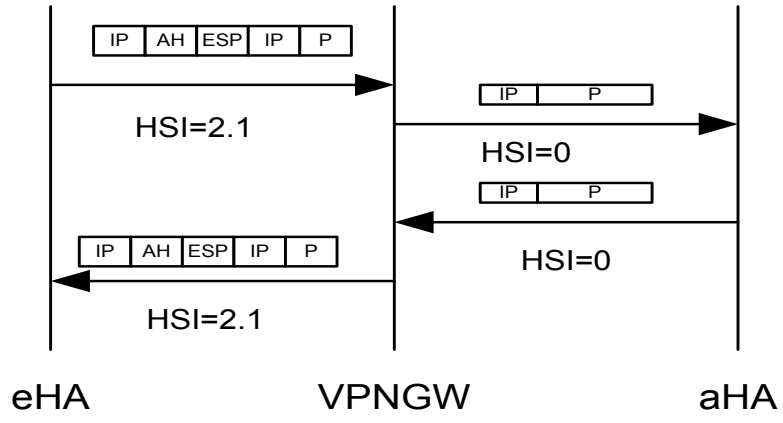

Figure 4.4. Messages between the eHA and the aHA

In this situation, the number of headers between the eHA and the VPN Gateway for both directions is higher than number of headers between the VPN Gateway and the aHA, as seen in Figure 4.4. The HSI values are different, which means that a packet on different parts of the paths consume different bandwidths because of extra headers as seen in Figure 4.4. As a result, the HSI values indicate that the bottleneck in this scenario can be between the eHA and the VPN Gateway.

4.5.1.2 Analysis of the scenario in Section 4.4.1

User data flow and the HSI values are given in Figure 4.5 for this scenario.

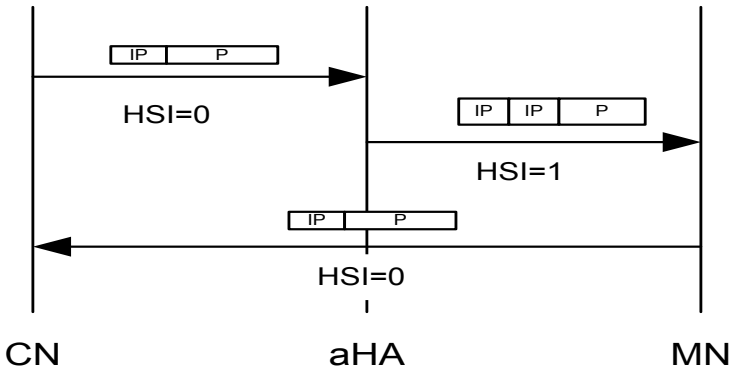

Figure 4.5. User data between the CN and the MN

As it is presented in Figure 4.5, there is not any ESP and AH header between nodes. Most of HSI values are zero. Only header size of the messages sent by the aHA increase, due to the Mobile IP tunnel established from the aHA to the MN. Actually, when the MN is in the Intranet, there is not any additional header caused by the proposed architecture. Additional header only is caused by Mobile IP encapsulation in which IP in IP encapsulation is assumed to use.

4.5.1.3 Analysis of the scenario in Section 4.4.3

This scenario is the main scenario to which the proposed architecture is claimed to be used for secure seemless mobility. User data flow and the HSI values for this scenario are given in Figure 4.6.

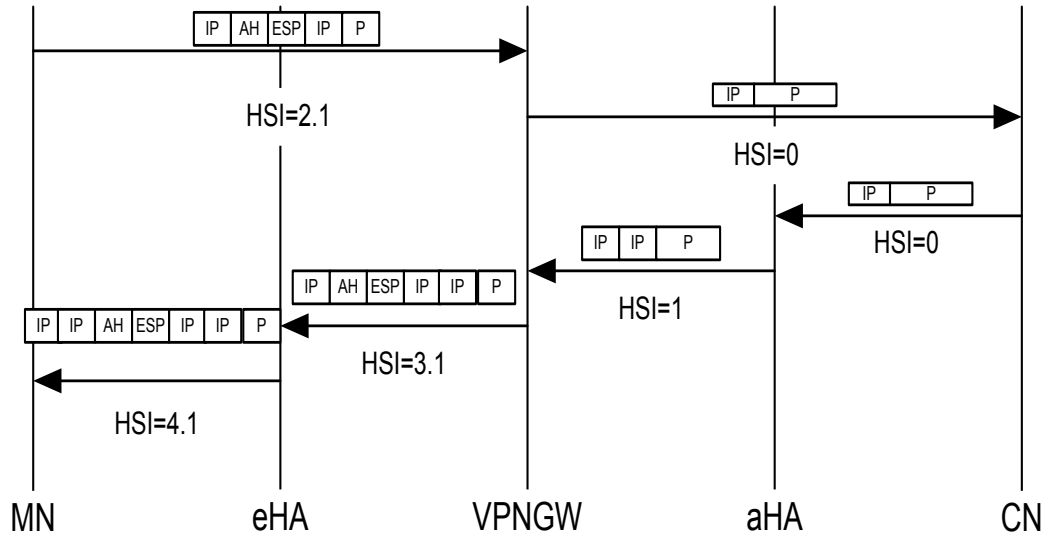

Figure 4.6. User data flow between the CN and the MN

The HSI values for this scenario are generally greater than that of other scenarios. This means that bandwidth consumption of headers in some part of paths increases more than in all other parts. Furthermore, the HSI values vary between all components in system because the MN in the Internet uses Mobile IPv4, IPSec and properties that comes with the proposed architecture. Remarkably is that the bandwidth consumption of packets on the path from the CN to the MN is much greater than that on the path from the MN to the CN. This asymmetry might indicate that routing mechanism of Mobile IP has not been optimized yet.

Consequently, the analyses show that the HSI value increases from the CN to the MN. The reason for this is related with the need for establishing both security and mobility features in the Internet. The derivative of the HSI on the path from the CN to the MN is greater than the derivative of the HSI on the path from the MN to the CN. Therefore, the bandwidth consumption of packets on the path from the CN to the MN is greater than that of reverse direction. This leads us to that optimal routing has not been achieved yet. The smallest value of the HSI in the Internet is measured as 2.1. This is the extra load on links that comes with security features of IPSec. On

the other hand, the cost of mobility is less than the amount for security in the Internet. In contrast to this, the extra load in the Intranet only stems from mobility.

4.5.1.4 Analyses of other scenarios

Since scenarios in Section 4.4.2 and in Section 4.4.4 are derived from scenarios in Section 4.4.1 and in Section 4.4.3, they give rise to similar results, and they are not analyzed again. Also, scenario in Section 4.4.5 is similar to scenario in Section 4.4.3. Therefore, it is not analyzed.

4.5.2 Analysis of overhead

Throughput and packet delay are used to demonstrate the overhead of the new architecture.

To give an impression about the performance of the proposed architecture, a testpad, which is shown in Figure 4.7, was constructed. Then, some measurements were taken on the testpad to determine throughput values for specific cases. After this step, the results were analyzed.

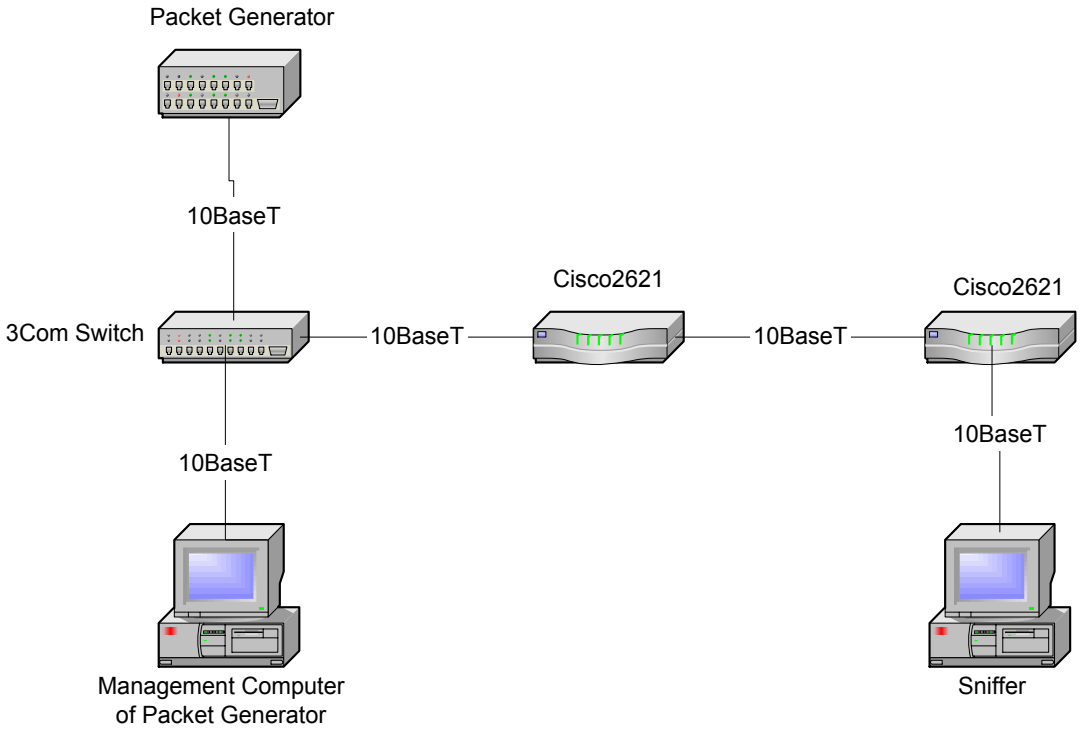

Figure 4.7. Testpad for measuring throughput values

The properties of the testpad are described below:

- The testpad was established at TÜBİTAK-UEKAE IP Group laboratory.

- The aim is to give an idea about a possible overhead of IPSec on any system that uses IPSec properties to establish security. It was not planed to test either mobility or security properties on this testpad.
- A hardware packet generator, SHOMITI hardware (Shomiti Systems Inc., San Jose, USA), was used to generate traffic with various rates.
- A personnel computer on which SHOMITI Surveyor3.1 (Shomiti Systems Inc., San Jose, USA) software runs was used as a packet sniffer.
- IPSec properties of the testpad were tested on Cisco2621 (Cisco Systems Inc., San Jose, USA) devices on which run c2600-ik903s3-mz.12z15T.bin ios.
- A personnel computer on which management software of SHOMITI hardware packet generator run was used.
- 3Com-SuperStackII Switch 3300 12 Port 3C16981 (3Com Corporation, 350 Campus Drive, Malborough, MA 01752-3064) switch was used to connect a Cisco2621 router, the packet generator, and management computer of the packet generator.
- All links between devices were 10BaseT. Two devices were connected with a UTP (Unshielded Twisted Pair) cable.

The test methods were prepared as follows:

- Various rate of traffic (0.5 Mbps, 1Mbps, 2Mbps, 4Mbps, 8Mbps) were tested.
- IP packets with different length (128 byte, 256 byte, 512 byte, 1024 byte) were generated.
- Various IPSec configurations (AH-MD5 and ESP-DES-MD5) were tested on Cisco2621 routers whose operating systems accommodate IPSec properties.
- DES was chosen as an encryption algorithm and MD5 was used as an authentication algorithm in these test cases.
- IKE (Internet Key Exchange) was chosen as the key distribution mechanism in tests.

- The sniffer was used to determine throughput values for all test cases on this testpad.
- The packet generator generated identical packets in over 1 minute for each test case.
- The packet sniffer received packets sent by the packet generator and it calculated average throughputs.
- The test results are presented in Table 4.1 and in Table 4.2.

In the testpad, the performance of IP encapsulation was approximately 100 percentages for all throughput values. Therefore, the performance of IP encapsulation was not analyzed in this section.

Table 4.1. Test results of throughput for AH-MD5 configuration of Cisco2621

Packet Size (byte) Throughput (Mbps)	128	256	512	1024
0.5	0.49	0.49	0.49	0.48
1	0.97	0.98	0.98	0.98
2	0.79	1.77	1.98	1.98
4	0.37	1.3	2.91	3.94
8	0.76	1.93	3.52	5.25

In Table 4.1, test results of authentication properties of AH are shown. The input throughput values for this configuration are presented on first column in Table 4.1. The first row represents size of packets for a test case. Results of measurements are found by intersection of a column and a row in the table. The measurements are done on sniffer as Mbps for a specific packet size and for a specific input throughput value.

Performance comparisons for different packet size as percentage of AH-MD5 configuration for each test case are shown in Figure 4.8.

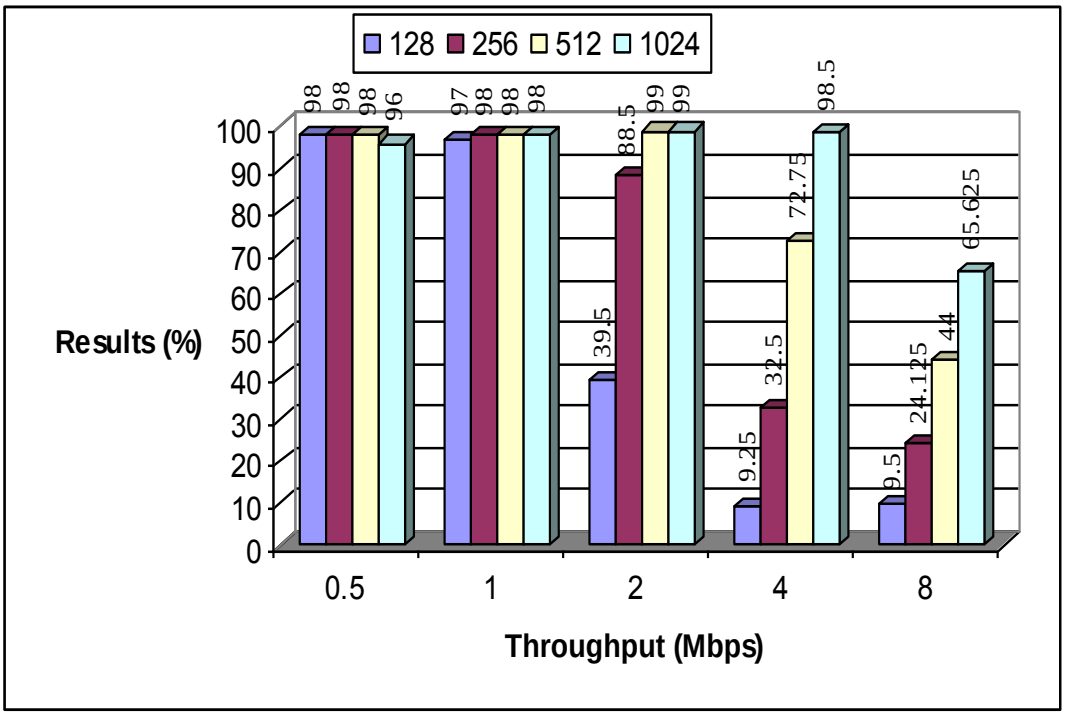

Figure 4.8. Performance analysis of AH-MD5 configuration

The performance of AH-MD5 configuration for throughput values less than 1 Mbps is approximately 98 percent. For throughput values greater than 1 Mbps, the performance of AH-MD5 configuration decreases with the packet size being used for a specific test case. The overhead of small packets is greater than the overhead of larger packets for a specific throughput value.

In Table 4.2, test results of authentication and encryption properties of ESP are shown. The input throughput values for this configuration are presented on first column in Table 4.2. The first row demonstrates size of packets for a test case. Results of measurements are found by intersection of a column and a row in the table as in Table 4.1. The measurements are done on sniffer as Mbps for a specific packet size and for a specific input throughput value.

Table 4.2. Test results of throughput for ESP-DES-MD5 configuration of Cisco2621

Packet Size (byte) Throughput (Mbps)	128	256	512	1024
0.5	0.48	0.49	0.5	0.49
1	0.76	0.99	0.98	0.99
2	0.57	1.08	1.67	1.98
4	0.24	0.79	1.43	2.07
8	0.47	0.83	1.51	2.1

Performance comparisons for different packet size as percentage of ESP-DES-MD5 configuration for each test case are shown in Figure 4.9.

It is seen that the performance of ESP-DES-MD5 configuration is better for packets with size 512 bytes and for low throughput values for the testpad. Overhead for this case is approximately zeros. The change of output throughput performance varies according to packet size. While packet size decreases, the performance for a specific throughput value goes down. This situation especially occurs for high rate traffic.

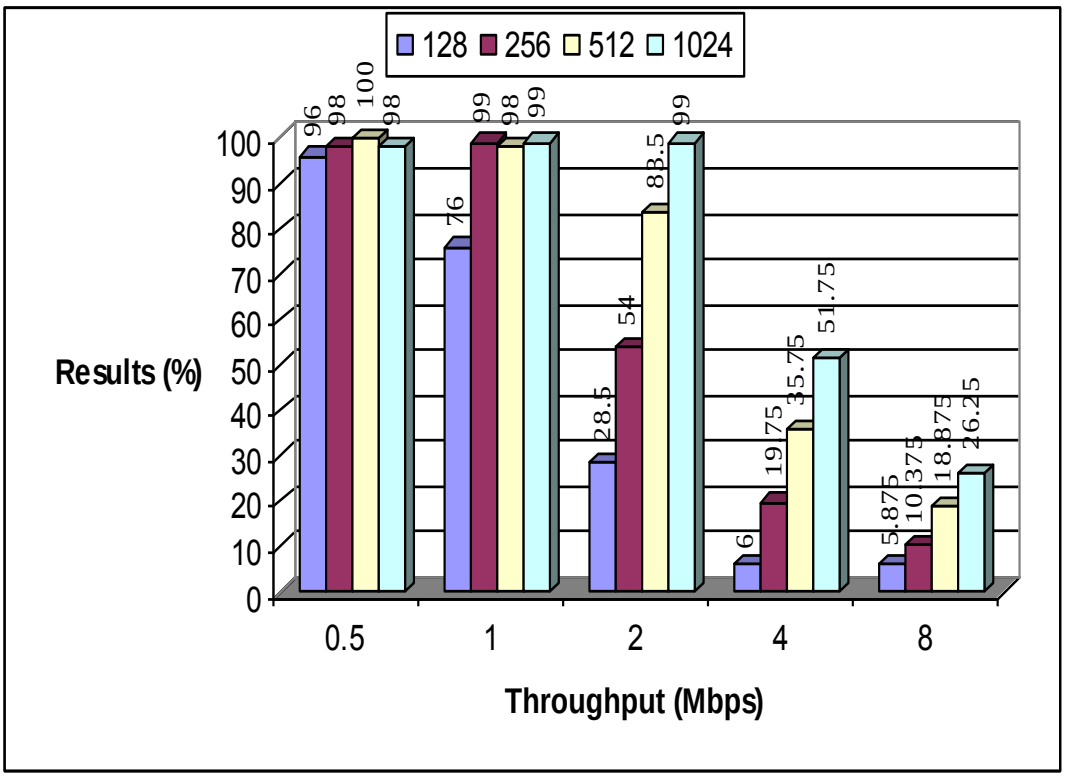

Figure 4.9. Performance analysis of ESP-DES-MD5 configuration

For both AH-MD5 and ESP-DES-MD5 configurations, performances on low throughput (throughput values less than 1Mbps) values are better than that of greater throughput values. However, the decrease percentages of performance for both

configurations are not same. Actually, the difference stems from the use of power for processing the AH, the ESP and the cryptographic algorithms. Processing cycles needed for some hash algorithms are shown in Table 4.3.

Table 4.3. Performance need of some hash algorithms [84]

Algorithm	MD4	MD5	RIPEMD	RIPEMD-128	SHA-1	RIPEMD-160
Cycles	241	337	480	592	837	1013

In addition to cryptographic algorithm that is used to establish encryption and authentication properties, specifications of devices are significant on performance. For instance, the size of memory where queues may be stored plays a crucial role. Another example is the type of system; it can contain parallel processing units that can positively affect the performance.

A packet transmission delay overhead is affected from many factors. It is related with size and type of network. Moreover, devices and protocols affect the performance of packet transmission. To give an idea about packet delay overhead, it was used the result of Fasbender's work [75] which describes a packet transmission delay overhead. The overhead for encapsulating and tunneling an IP packet is estimated by 7 ms in accordance to [85] and [86]. Also, the overheads for RSA encryption and decryption, is estimated by respectively 1 ms. for 1000 bit using a 512 bit key and a hardware-based implementation. The mean transmission times in Mobile IP are measured by respectively 57 ms for Medium Range WAN, and 207 for Long Haul WAN. These results indicate that the packet transmission (packet delay) overhead is related with the number of hops between source and destination for an IP packet. In addition to number of hops, transmission delay depends on devices being used in the system.

As a result, it can be said that the performance of any system, which uses IPSec properties and Mobile IP features, depends on the traffic characteristic and devices that are used in this system. Therefore, the performance of the proposed architecture according to throughput values and transmission delays of these instances cannot be generalized. However, it can be said that the overhead on nodes can be greater when an MN is in Internet than when an MN is in Intranet because the new architecture does not need any IPSec properties in Intranet.

4.5.3 Security analysis of the proposed architecture

In the scenario of Section 4.4.1, the MN is in the Intranet where there is no need to any additional security mechanism because the Intranet is assumed to be a secure network. Actually, there are many security threats that come from internal intruders. Some of these threats are presented in [55] for Mobile IPv4. Threats related with IP security are valid for this scenario and also for all other scenarios discussed in this thesis.

In the scenario of Section 4.4.3 where the MN is in the Internet, there is no additional security threat. This architecture may only cause a new security threat (scenario of Section 4.4.2), if the MN does not detect the network change while traversing the VPN Gateway sufficiently fast. In this case, unencrypted messages may be sent to the Internet, which may cause loss of security. Therefore, the performance of the network detection algorithm is crucially important for the security of the architecture.

5. REQUIREMENTS TO DESIGN AN ARCHITECTURE FOR MOBILE IPv6 TRAVERSING IPSEC BASED VPN GATEWAY

This chapter highlights some of the key features that should be considered to design an architecture that provides a Mobile IPv6 traversing IPSec based VPN Gateway.

Most of current researches related with Mobile IPv6 are about signaling, registration and binding update. Because IPSec is mandatory for IPv6, there are not enough researches about traversing IPSec based VPN Gateways. However, this does not mean that there will be no need to traverse any VPN Gateway in IPv6 by mobile nodes. The properties of VPN Gateways are changing, and lots of these properties cannot be put on any node such as on an MN. Therefore, VPN Gateways will continue to be used until new technologies accommodating properties of a VPN Gateway emerge. For these reasons, there will be mechanisms to traverse VPN Gateways in IPv6.

Requirements for traversing an IPSec based VPN Gateway for IPv6 are given below;

- The solution must not cause any new security threat.
- The solution must not need to change the IPSec protocol.
- An MN must be able to detect network changes when it traverses an IPSec based VPN Gateway.
- The signaling between an HA and an MN must be secure. The security of signaling is related with the location of the HA. Also, it is related with properties of the HA. In IPv6, HAs are planned to be on routers. Therefore, routers may need to be secured.
- The MN must always access to an HA or HAs no matter where the MN roams.
- If a VPN Gateway is able to support dynamic SA, an MN must support dynamic SA. In this situation, there is no need for two HAs, one in the Internet and one in the Intranet. The HA can be placed on either in the Internet or in the Intranet;

    - If the HA is settled in the Intranet, the MN must establish dynamic SA with the VPN Gateway.
    - If the HA is set in the Internet, the MN must also establish dynamic SA. In this circumstance, the MN must establish dynamic SA not only with the VPN Gateway but also with the HA. Because MNs must access to the HA from the Intranet, they have to be able to accomplish IPSec tunnel over the VPN Gateway.

- If the VPN Gateway does not support dynamic SA as in the proposed architecture for IPv4 VPN Gateways, there is no need for MN to be able to establish dynamic SA with the VPN Gateway. In this situation, there must be two HAs like the eHA and the aHA in system.
- To guarantee the mobility and security when traversing IPSec based VPN Gateway for IPv6, the HA must be able to operate both as the eHA and as the aHA.
- If an HA (router) is mobile such as mobile networks in a plane, it must contain an MN's properties that are described above.
- Establishing an eHA properties and an aHA properties on same device may be better than to set them on separate devices.
- Routing optimization for all situations should be kept in mind.
- A CN must operate as before.
- The solution must be open to improvements according to changes on the IPv6 and on the Mobile IPv6.
- The solution may require supporting compatibility with Mobile IPv4. Therefore, the solution may need to be compatible with solutions proposed for IPv4.
- The solution must be cost effective.

6. CONCLUSION AND DISCUSSION

During the twentieth century, the key technology has been information gathering, processing and distribution. Computer networks have happened one of the most significant revolution after first half of twenty century. They have come to play an increasingly important role in modern life.

The biggest network in the world is the Internet, which is founded on IP. IP is the network layer protocol in DoD model. Until the last decade, lots of IP based computer networks had been relied on IPv4. However, needs of the Internet users have increased, and IPv4 has not meet requirements of them since 1990. Therefore, IPv6 is established to cover the requirements. In IPv6, some features of IPv4 are improved. Moreover, new abilities are added to the protocol. Finally, the IPv6 is considered to be the network layer protocol for future Internet.

Due to the rapid technological progress, the Internet users, one of which is mobility, accompany new requirements. Mobility has become an important phenomenon especially after development of wireless technologies. In IPv4, Mobile IPv4 is used to accommodate the requirements. In development of IPv6, mobility has been one of main aspects. Mobile IPv4 was not taken into account. Therefore, it is seemed as a patch to IPv4 if mobility is demanded to be in systems. In contrast, mobility has been considered since the development of IPv6 began.

Security, which is another new requirement of Internet users, has become the most significant key point in the IP based communication systems since the beginning of twenty first century. There are various security mechanisms to protect computer communication networks; however, the most popular one is IPSec. The IPSec is a security solution for IP. Like mobility, security was not considered when IPv4 was designed. Conversely, IPSec is mandatory to be implemented in IPv6.

In this thesis, it was presented a new architecture to establish seemless mobility and security both in the Intranet and in the Internet by using standard communication protocols and new features that come with the proposed architecture. First, it was presented the new architecture and described its properties. Then, possible scenarios

for this architecture are discussed. The scenarios in the proposed architecture were constructed according to movement of the MN and also the CN, the CN as an MN. And finally, the scenarios were analyzed according to message size, overhead and security. To give an impression about overhead based on throughput values, a testpad was constructed, and some measurements were done on it. Analyses and measurements results show that the performance of any system, which uses IPSec and Mobile IP, depends on many factors such as traffic characteristic. Therefore, the performance of the proposed architecture cannot be generalized. However, it can be said that the overhead on nodes can be greater when an MN is in Internet than when an MN is in Intranet because the new architecture does not need any IPSec properties in Intranet. In addition to performance results, if the network detection mechanism works properly, the new architecture does not introduce any new security threat. Also, simulation software that was used to simulate the proposed architecture was introduced and explained with an example.

The thesis highlights some of the key features that should be considered to design an architecture that provides Mobile IPv6 traversing IPSec based VPN Gateway.

It needs lots of work to establish efficient mechanism for accommodating both security and mobility in the Internet and in the Intranet. For instance, most of IPSec based VPN Gateways are not compatible with either Mobile IPv4 or Mobile IPv6. However, to establish security and mobility in a system both IPSec and Mobile IP must be implemented. On the other hand, future works have to be carried on realizing the new architecture. A sufficiently secure network detection algorithm should be designed, which is assumed to exist already in this work. In addition to these, routing optimization may be carried out. Also, new architectures according to requirements can be accomplished to use with Mobile IPv6. On the other hand, new solutions can be done with updating Mobile IPv6 and also IPv6 to ensure security and mobility worldwide.

The nation’s prosperity will be related with how much they accommodate mobility and security in their networks.

REFERENCES

[1] **Comer, D. E.,** 1995. Internetworking with TCP/IP Vol I: Principles, *Protocols, and Architecture, Third Edition,* Prentice-Hall International Inc., Upper Saddle River, New Jersey

[2] **RFC 791,** 1981. INTERNET PROTOCOL, *IETF,* Defense Advanced Research Projects Agency, Information Processing Techniques Office Arlington, Virginia

[3] **RFC 2460,** December 1998 Internet Protocol, Version 6 (IPv6) Specification, *IETF, Network Working Group*

[4] **Siyan, K. S.,** 1997. Inside TCP/IP, *Third Edition,* New Riders Publishing, Indianapolis

[5] **Tanenbaum, A. S.,** 1996. Computer Networks, *Third Edition,* Prentice Hall, Upper Saddle River, New Jersey

[6] **Solomon, J. D.,** 1998. MOBILE IP, *The Internet Unplugged,* Prentice Hall PTR, Upper Saddle River, New Jersey

[7] **Norris, M.,** 2001. Mobile IP Technology for M-Business, ARTECH HOUSE, INC., 685 Canton Street Norwood, MA 02062

[8] **Stallings, W.,** 1999. Cryptography and Network Security, *Principles and Practice, Second Edition,* Prentice Hall, Upper Saddle River, New Jersey

[9] **RFC 3122,** June 2001. Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification, *IETF Network Working Group*

[10] **RFC 3041,** January 2001. Privacy Extensions for Stateless Address Autoconfiguration in IPv6, *IETF Network Working Group*

[11] **RFC 2874,** July 2000. DNS Extensions to Support IPv6 Address Aggregation and Renumbering, *IETF Network Working Group*

[12] **RFC 3178,** October 2001. IPv6 Multihoming Support at Site Exit Routers, *IETF Network Working Group*

[13] **RFC 2894,** August 2000. Router Renumbering for IPv6, *IETF Network Working Group*

[14] **RFC 2710,** October 1999. Multicast Listener Discovery (MLD) for IPv6, *IETF Network Working Group*

[15] **RFC 2675,** August 1999. IPv6 Jumbograms, *IETF Network Working Group*

[16] **RFC 2526,** March 1999. Reserved IPv6 Subnet Anycast Addresses, *IETF Network Working Group*

[17] **RFC 2473,** December 1998. Generic Packet Tunneling in IPv6 Specification, *IETF Network Working Group*

[18] **RFC 2463,** December 1998. Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, *IETF Network Working Group*

[19] **RFC 2462,** December 1998. IPv6 Stateless Address Autoconfiguration, *IETF Network Working Group*

[20] **RFC 2461,** December 1998. Neighbor Discovery for IP Version 6 (IPv6), *IETF Network Working Group*

[21] **RFC 2375,** July 1998. IPv6 Multicast Address Assignments, *IETF Network Working Group*

[22] **RFC 2372,** July 1998. IP Version 6 Addressing Architecture, *IETF Network Working Group*

[23] **RFC 1981,** August 1996. Path MTU Discovery for IP version 6, *IETF Network Working Group*

[24] **RFC 2402**, November 1998. IP Authentication Header, *IETF Network Working Group*

[25] **RFC 2406**, November 1998. IP Encapsulating Security Payload (ESP), *IETF Network Working Group*

[26] **RFC 3344,** August 2002. IP Mobility Support for IPv4, *IETF*

[27] **Internet Draft,** January 2003. draft-ietf-mobileip-ipv6-20.txt, Mobility Support in IPv6, *IETF Mobile IP Working Group*

[28] **RFC 1256,** September 1991. ICMP Router Discovery Messages, *IETF Network Working Group*

[29] **RFC 2003,** October 1996. IP Encapsulation within IP, *IETF Network Working Group*

[30] **RFC 2004,** October 1996. Minimal Encapsulation within IP, *IETF Network Working Group*

[31] **RFC 1701,** October 1994. Generic Routing Encapsulating (GRE), *IETF Network Working Group*

[32] **RFC 3115,** April 2001. Mobile IP Vendor/Organization-Specific Extensions, *IETF*

[33] **RFC 3024**, January 2001. Reverse Tunneling for Mobile IP, revised, *IETF*

[34] **RFC 3012,** November 2000. Mobile IPv4 Challenge/Response Extensions, *IETF*

[35] **RFC 2794,** March 2000. Mobile IP Network Access Identifier Extension for IPv4, *IETF*

[36] **RFC 2005,** October 1996. Applicability Statement for IP Mobility Support, *IETF*

[37] **Internet Draft,** June 2002. draft-ietf-mobileip-lowlatency-handoffs-v4-04.txt, Low Latency Handoffs in Mobile IPv4, *IETF Mobile IP Working Group*

[38] **Internet Draft,** February 2003. draft-ietf-mobileip-reg-revok-05.txt, Registration Revocation in Mobile IPv4, *IETF Mobile IP Working Group*

[39] **Internet Draft,** October 2002. draft-ietf-mobileip-reg-tunnel-07.txt, Mobile IPv4 Regional Registration, *IETF Mobile IP Working Group*

[40] **Internet Draft,** December 2002. draft-ietf-mobileip-rfc3012bis-04.txt, Mobile IPv4 Challenge/Response Extensions (revised), *IETF Mobile IP Working Group*

[41] **Internet Draft,** March 2003. draft-ietf-mobileip-fast-mipv6-06.txt, Fast Handovers for Mobile IPv6, *IETF Mobile IP Working Group*

[42] **Internet Draft,** April 2002. draft-ietf-mobileip-piggyback-00.txt, Nonfinal Mobility Header for Mobile IPv6, *IETF Mobile IP Working Group*

[43] **Internet Draft,** December 2002. draft-ietf-ipv6-cellular-host-03.txt, IPv6 for Some Second and Third Generation Cellular Hosts, *IETF*

[44] **Omar, H. Saadawi, T. and Lee, M.,** 1999. Supporting Reduced Location Management Overhead and Fault Tolerance in Mobile IP Systems, *IEEE*, **0-7695-0250-4/99**, 347-353

[45] **Morand, L. and Tessier, S.,** 2002. Global mobility approach with Mobile IP in "All IP" networks, *IEEE*, **0-7803-7400-2/02**, 2075-2079

[46] **Kim, J. H.,** 2001. Demonstration of Static Network Mobile Router for Mobile Platforms, *IEEE*, **0-7803-7225-5/01**, 746-750

[47] **Leu, Y. R.,** 1997. Implementation Considerations for Mobile IP, *IEEE,* **0730-3157/97**, 478-481

[48] **Xie, J. and Akyildiz, I. F.,** 2002. An Optimal Location Management Scheme for Minimazing Cost in Mobile IP, *IEEE*, **0-7803-7400-2/02**, 3313-3317

[49] **Garg, W. K. and Tejwani, H.,** 2000. Mobile IP for 3G Wireless Networks, *IEEE-ICPWC2000*, **0-7803-5893-7/00**, 240-244

[50] **Wong, K. D.,** 2002. Architecture Alternatives for Integrating Cellular IP and Mobile IP, *IEEE*, **0-7803-7371-5/02**, 197-204

[51] **Wu, I. W. Chen, W. S. Liao, H. E. and Young, F. F.,** 2002. A SEEMLESS HANDOFF APPROACH OF MOBILE IP PROTOCOL FOR MOBILE WIRELESS DATA NETWORKS, *IEEE,* **0098-3063/00**, 335-344

[52] **Chen, Y. and Boult, T.,** 2002. Dynamic Home Agent Reassignment in Mobile IP, *IEEE*, **0-7803-7376-6/02**, 44-48

[53] **Khalil, M. and Pillai, K.,** ARCHITECTURE FOR IP MOBILITY, *IP Mobility Group, Nortel Networks,* 2221 Lakeside Boulevard Richardson, Texas 75082, USA

[54] **RFC 2401**, November 1998. Security Architecture for the Internet Protocol, *IETF Network Working Group*

[55] **Haitao, W. and Shaoren, Z.,** 2001. The Security Issues and Countermeasures in Mobile IP, *IEEE*, **0-7803-7010-4/01**, 122-127

[56] **Internet Draft,** January 2003. draft-ietf-mobileip-vpn-problem-statement-req-01, Problem Statement: Mobile IPv4 Traversal of VPN Gateways, *IETF Mobile IP Working Group*

[57] **RFC 2977,** October 2000. Mobile IP Authentication, Authorization, and Accounting Requirements, *IETF*

[58] **RFC 2356,** June 1998. Sun's SKIP Firewall Traversal for Mobile IP, *IETF*

[59] **Internet Draft,** May 2003. draft-ietf-mobileip-aaa-key-12.txt, AAA Registration Keys for Mobile IP, *IETF Mobile IP Working Group*

[60] **Internet Draft,** Jan 2003. draft-ietf-mobileip-aaa-nai-04, AAA NAI for Mobile IPv4 Extension, *IETF Mobile IP Working Group*

[61] **Internet Draft,** November 2002. draft-ietf-mobileip-nat-traversal-07.txt, Mobile IP NAT/NAPT Traversal using UDP Tunnelling, *IETF Mobile IP Working Group*

[62] **Internet Draft,** January 2003. draft-ietf-mobileip-vpn-problem-solution-00, Mobile IPv4 Traversal Across IPsec-based VPN Gateways, *IETF Mobile IP Working Group*

[63] **Internet Draft,** April 2003. draft-ietf-mobileip-vpn-problem-solution-01, Mobile IPv4 Traversal Across IPsec-based VPN Gateways, *IETF Network Working Group*

[64] **Internet Draft,** September 2003. draft-ietf-mobileip-vpn-problem-solution-03, Mobile IPv4 Traversal Across IPsec-based VPN Gateways, *IETF Mobile IP Working Group*

[65] **Internet Draft,** February 2003. draft-ietf-mobileip-mipv6-ha-ipsec-03.txt, Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents, *IETF Mobile IP Working Group*

[66] **Internet Draft,** March 2003. draft-ietf-mobileip-mipv6-ha-ipsec-04.txt, Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents, *IETF Mobile IP Working Group*

[67] **Scheffler, T.** 2002. Security Architectures for Mobile IPv6, *Euro6IX/6NET Workshop*, Limerick, Ireland, June 5

[68] **Shankaran, R. Varadharajan, V. and Hitchens, M.,** 2001. Secure Distributed Location Management Scheme for Mobile Hosts, *IEEE,* **0-7695-1321-2/01,** 296-305

[69] **Aspas, J. P. and Arroyo, F.B.,** 2002. Design of a mobile VPN able to support a large number of users, *IEEE,* **0-7803-7422-3/02**, 219-222

[70] **Tsuda, Y. Ishiyama, M. Fukumoto, A. and Inoue, A.,** 1998. Design and Implementation of Network CryptoGate-IP Layer Security and Mobility Support, *IEEE,* **1060-3425/98**

[71] **Berthe, K. and Yang, Y.,** 2001. Intelligent Network for military task, *IEEE,* **0-7803-7010-4/01**, 217-222

[72] **Mink, S. Pahlke, F. Schafer, G. and Schiller, J.,** 2000. Towards SecureMobility Support for IP Networks, *IEEE,* **0-7803-6394-9/00**, 555-562

[73] **Cappiello, M. Floris, A. and Veltri, L.,** 2002. Mobility amongst Heterogeneous Networks with AAA Support, *IEEE,* **0-7803-7400-2/02**, 2064-2069

[74] **Braun, T. and Danzeisen, M.,** 2001. Secure Mobile IP Communication, *IEEE,* **0-7695-1321-2/01**, 586-593

[75] **Fasbender, A. Kesdogan, D. and Kubitz, O.,** 1996. Analysis of Security and Privacy in Mobile IP, *4th International Conferance on Telecommunication Systems, Modelling and Analysis*, Nashville,TN, USA, March 21-24, 1-17

[76] **Conn, D.,** 2001. Security Aspects of Mobile IP, *As a part of the Information Security Reading Room,* SANS Institute, December 17

[77] **Tuquerres, G. Salvador, M. R. and Sprenkels, R.,** 1999. MOBILE IP: SECURITY & APPLICATION, *Telematics Systems and Services-Center for Telematics and Information Technology, University of Twente,* P.O. Box 217-7500 AE Enshende, The Netherlands, December 1

[78] **Hansen, H.,** 2000. IPSec and Mobile IP in Mobile Ad Hoc Networking, *Department of Computer Science and Engineering,* Helsinki University of Technology, April 25

[79] **RFC 1810,** June 1995. Report on MD5 Performance, *IETF Network Working Group*

[80] **Hsieh, R. and Senevirante, A.,** 2001. Performance Analysis of Mobile IP and SLM, *in Proceedings of International Conference on Networks (ICON),* Bangkok, Thailand

[81**] Ergen, M. and Puri, A.,** 2002. MEWLANA-Mobile IP Enriched Wireless Local Area Network Architecture, *IEEE*, **0-7803-7467-3**

[82] **Fan, C. et al,** 1989. Interoperability Analysis and TCP Performance in a Heteregenous Mobile IP Enviroment, *9th IEEE Workshop on Local and MetropolitanArea Networks*, May 25, GMD FOKUS Kaiserin-Agusta-Allee 31 D-10589 Berlin

[83] **Blondia, O. et al.**, 2003. Performance Comparison of Low Latency Mobile IP Schemes, *WiOpt'03 Modeling and Optimization in Mobile Ad Hoc and Wireless Networks*, March 2003, INRIA Sophia Antipolis, France

[84] **Bosselaers, A.**, 1999. The RIPEMD 160, *http://www.east.kuleuven.ac.be/~bosselae/ripemd160.html*, August 1999

[85] **Cho, G. and Marshall, L.F.**, 1995. An Efficient Location and Routing Scheme for Mobile ComputingEnvironments, *IEEE Journal on Selected Areas in Communications 13/5*, p.p. 868 - 879.

[86] **Ioannidis, J. and Maguire, G.Q.Jr.**, 1993. The Design and Implementation of a Mobile Internetwor-king Architecture, *in: Proceedings of the 1993 Winter USENIX*, San Diego, CA, January, 491 - 502.

[87] **Shand, M. and Vuillemin, J.,** 1993. Fast Implementations of RSA Cryptography, *in: Proceedings of the 11th IEEE Symposium on Computer Arithmetic, IEEE Computer Society Press*, Los Ala-mitos, CA, 1993, 252 - 259.

[88] **Claffy, K.C. et al**, 1993. Measurement Considerations for Assessing Uni-directional Latencies, in: Internetworking, *Research and Experience, 4*, John Wiley & Sons, 121 - 132.

APPENDIX A. EXPLANATION OF SIMULATION SOFTWARE

A.1 Introduction

The simulation software based on the analytical analyses of the system is developed to demonstrate operations of the proposed architecture according to given scenarios. One of motivation of the simulation software is to show packet flows according to movement of MN. Another motivation is to denote what is done on an IP packet during its route.

A.2 Development Platform of the Software

- Operating System: Windows2000 Professional (Microsoft Corporation)
- Programming environment: Borland C++ Builder 5.0 (Inspire Corporation)

A.3 Details of the Simulation Software

The aim of this simulation software is to show steps of the proposed architecture as simple as possible. Therefore, details of the software are presented using images of user interface of the simulation software.

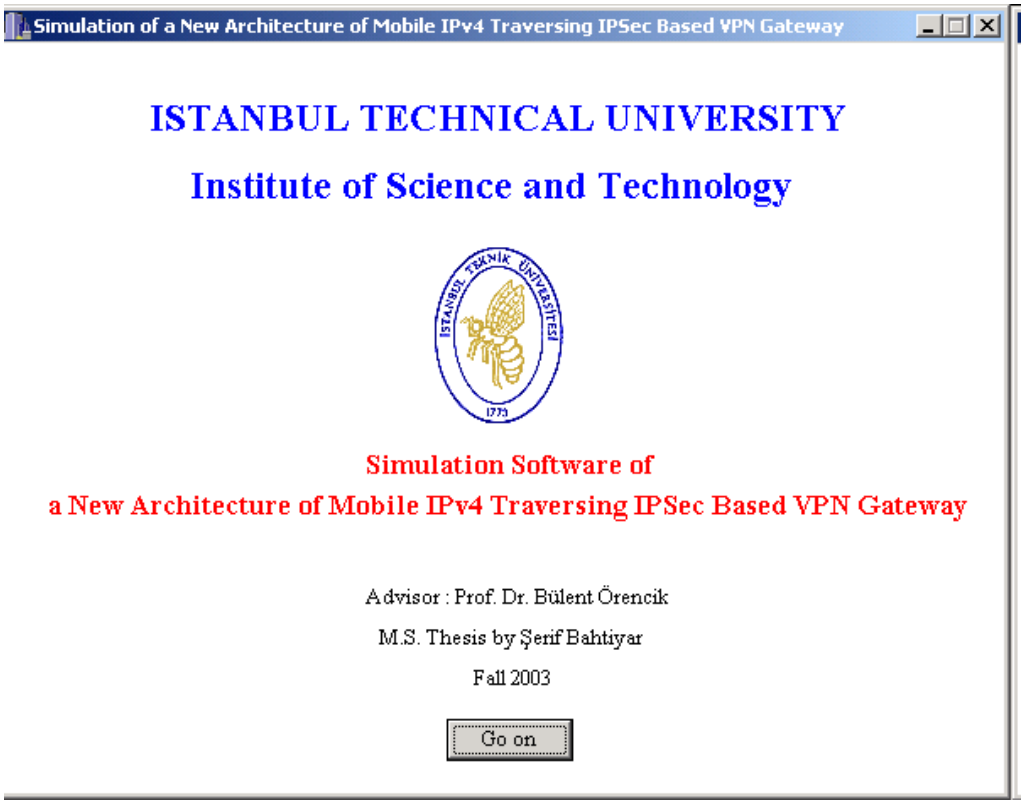

Figure A.1. The entrance screen of the simulation software

The entrance screen of the simulation software is shown in Figure A.1. To go to main part of the software, a user has to click on **Go on** button. After clicking the **Go on** button, the main portion of the simulation software will appear on the screen as it is shown in Figure A.2.

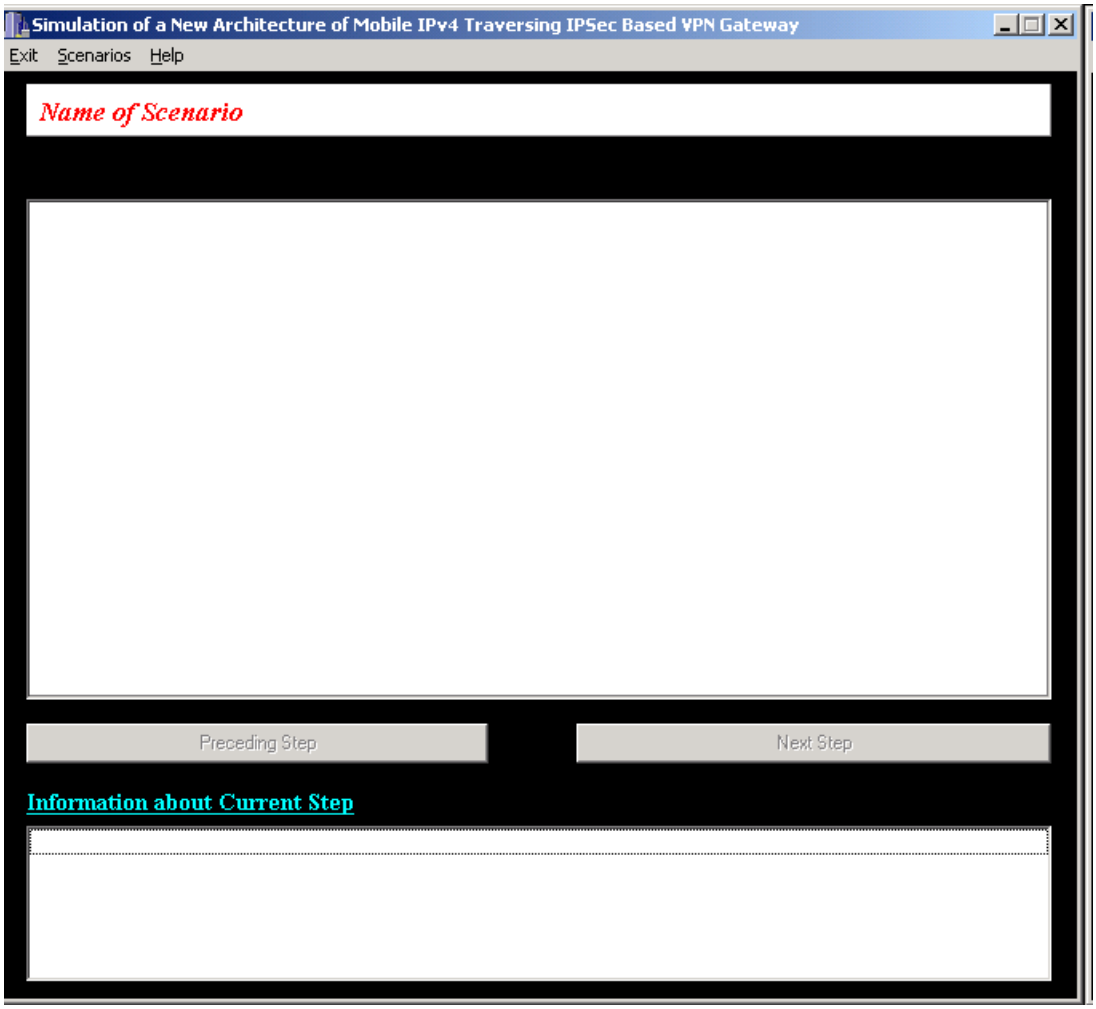

Figure A.2. The main portion of the simulation software

The user interface of the simulation software consists of five parts. Generally, these parts are an input or an output part of the software.

Scenarios option on menu bar is an input variable in the software. This option enables a user to select a simulation scenario. Scenarios option contains six different simulation alternatives, which are listed below;

- Mobile Node in Intranet,
- Mobile Node in Internet,
- Mobile Node moves from Intranet to Internet,
- Mobile Node moves from Internet to Intranet,
- Correspondent Node as a Mobile Node in Intranet
- Correspondent Node as a Mobile Node in Internet.

After selecting a scenario, components of the selected scenario display on the screen as it is shown in Figure A.3.

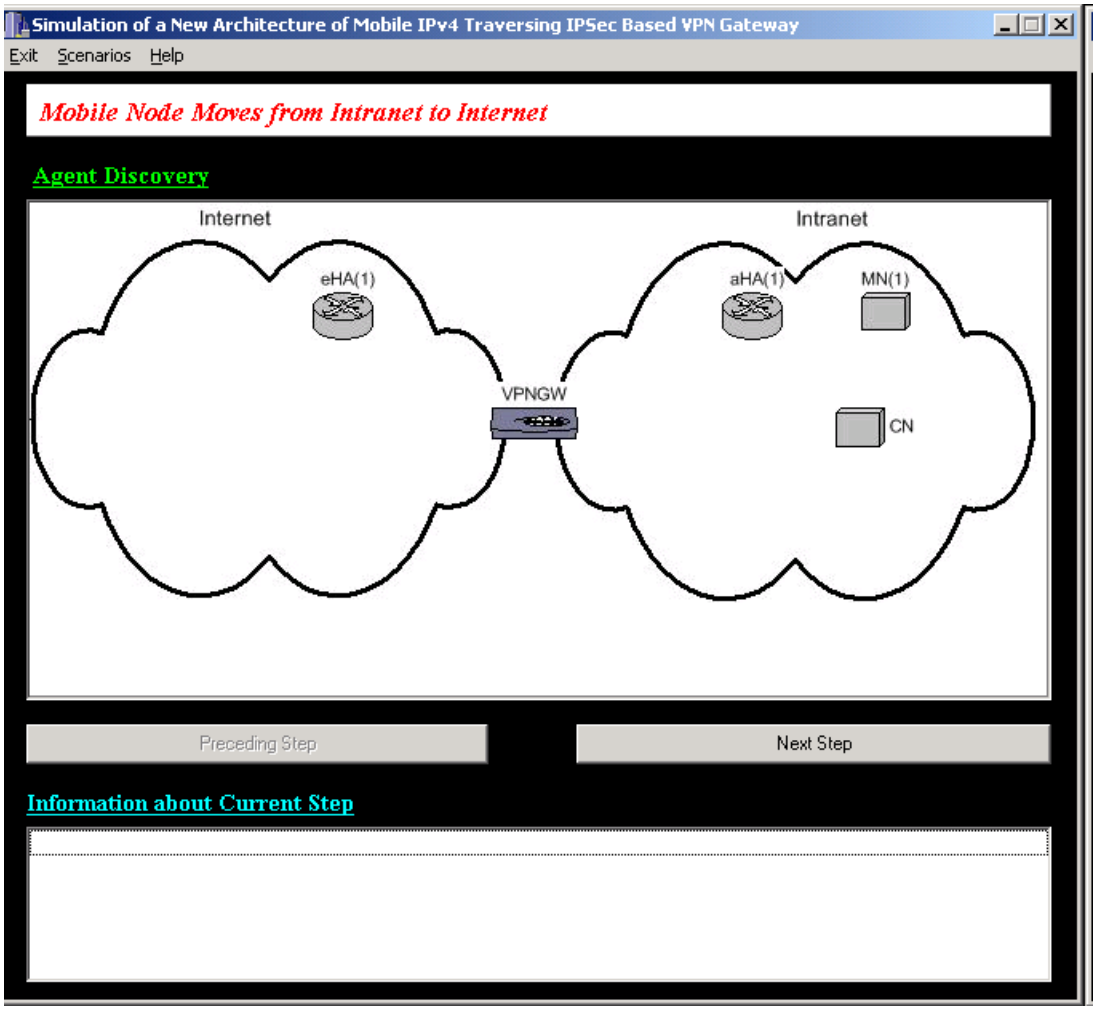

Figure A.3. The main part of the simulation software after selecting a scenario

The **Preceding Step** and the **Next Step** buttons in Figure A.3 can be categorized in input part. These buttons are used to show all steps in sequence. A user can see next step or preceding step of a selected scenario.

The name of the selected scenario appears at the top of the main portion of the simulation software as an output part. The name part is shown in Figure A.3.

The animation part is the second output part in the software. This part is shown with the biggest rectangle on the screen. Briefly, this part visualizes the components related with a selected scenario. In addition to this, the animation part visualizes packets flow and the state of the selected simulation.

Last part is the **Information about Current Step**. This part demonstrates changes between two steps of a selected scenario. For example network change is one of them.

Details about the simulation software is given in next with an explanation example.

A.4 A Simulation Example

In this section, a simulation scenario example, which scenario is one of six scenarios mentioned in Section 4.6.2, is given to make clear the operations of the simulation software.

The scenario Mobile Node Moves form Intranet to Internet is selected to demonstrate all steps of a simulation of the scenario. These steps are shown below.

- Firstly, the scenario is selected. This step is shown in Figure A.4.

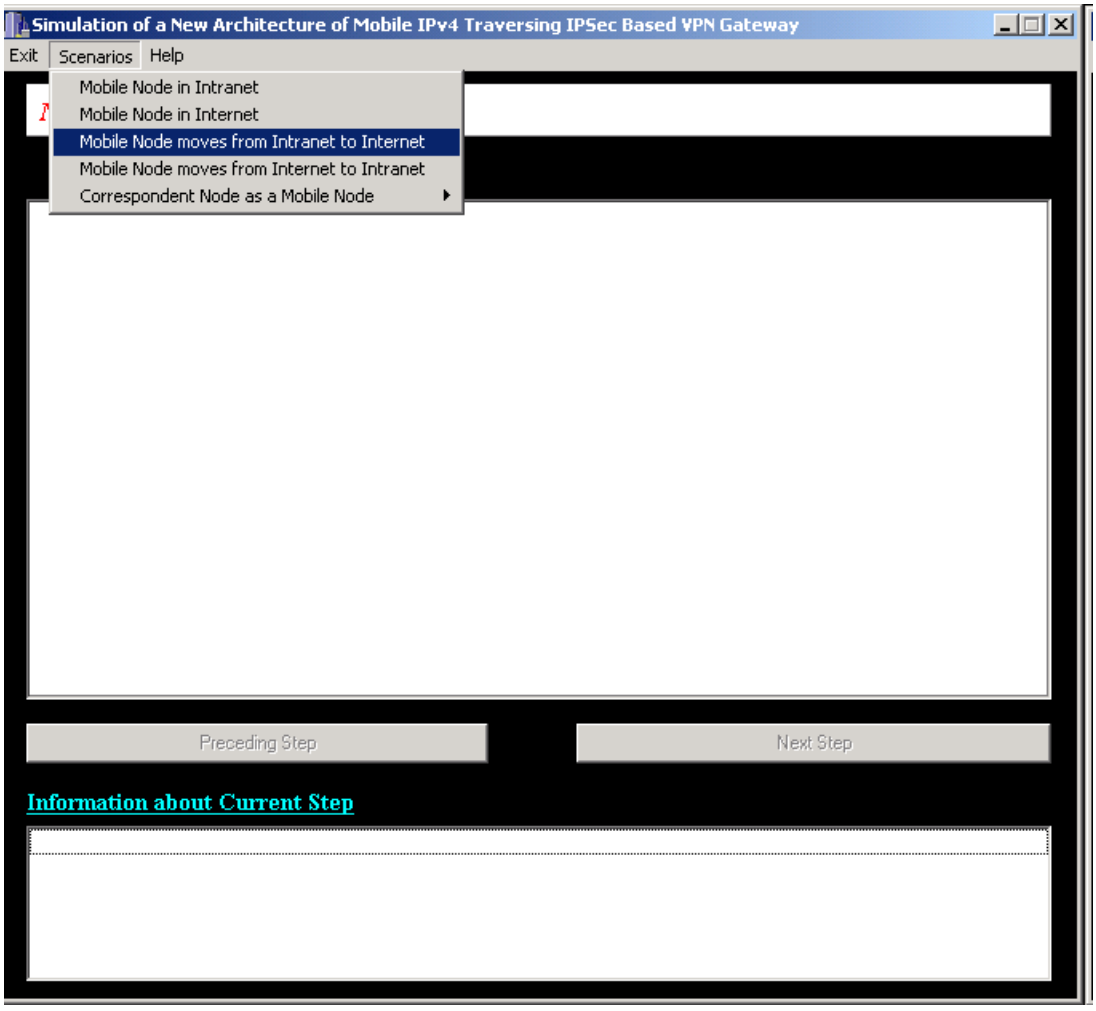

Figure A.4. Scenario selection for the simulation example

- After selection the scenario, the software is ready to begin the simulation. The components at the beginning of the simulation appear at the animation part. This step is shown in Figure A.5.

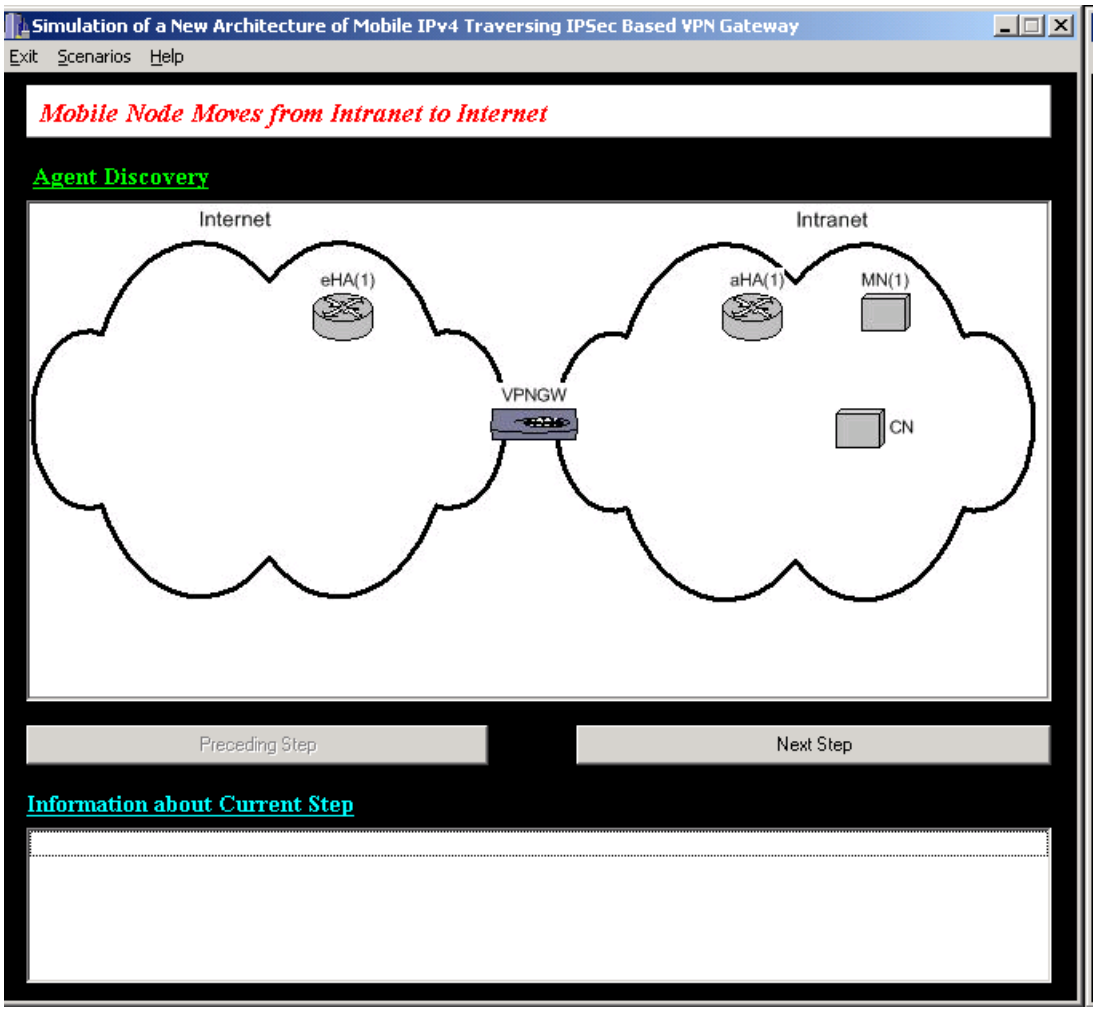

Figure A.5. After selection a scenario for the simulation example

- First step of agent discovery process in Intranet
    - This step is shown in Figure A.6,
    - The aHA or any FA broadcasts Agent Advertisements messages.
    - Agent Advertisements are periodically transmitted as multicasts or broadcasts to each link on which a node is configured to perform as a home agent, a foreign agent, or both. This allows a mobile node that is connected to such a link to determine whether any agent is present and, if so, their respective identities (IP addresses) and capabilities.

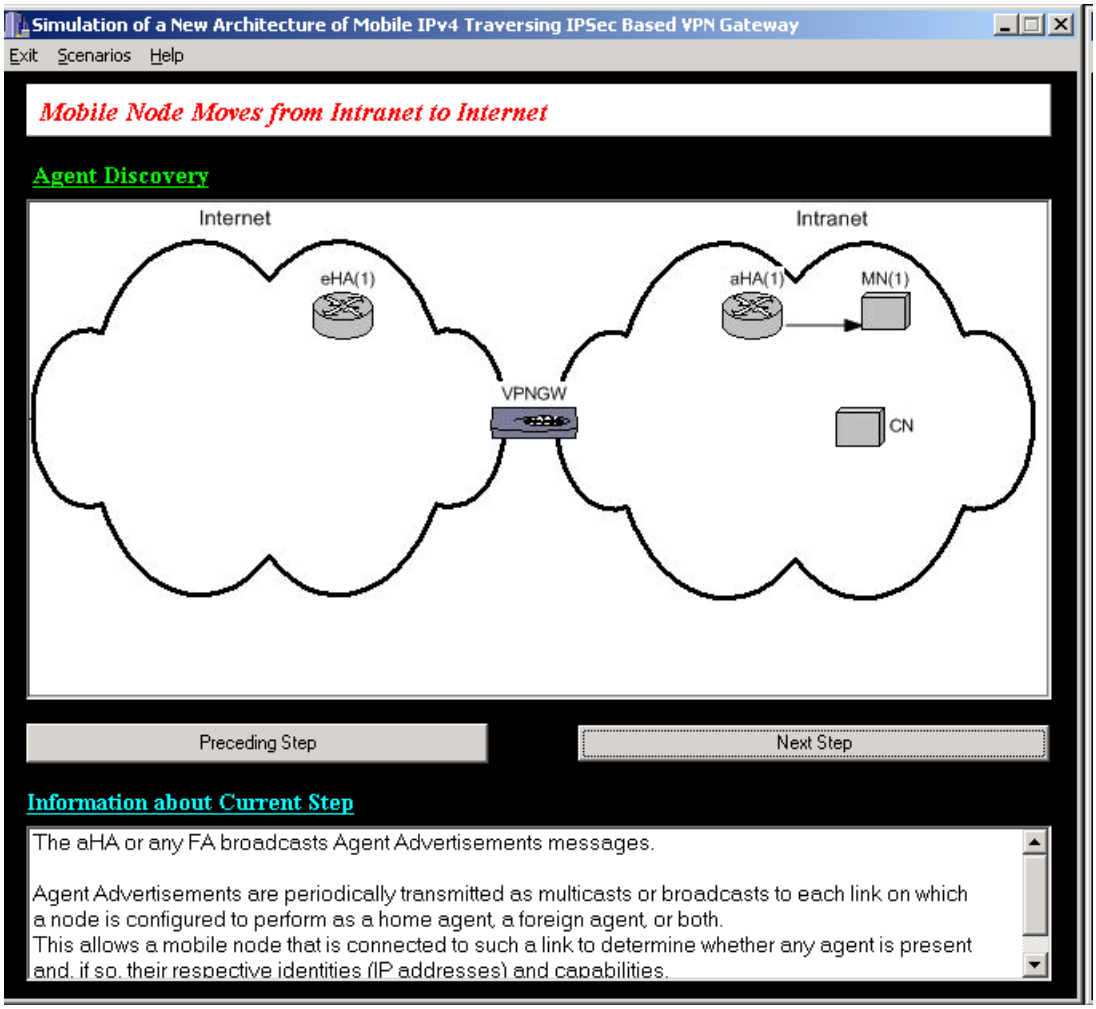

Figure A.6. First step of agent discovery in Intranet for the simulation example

- Second step of agent discovery process in Intranet
    - This step is shown in Figure A.7.
    - The MN receives an Agent Advertisement message that is sent by the aHA or any FA.
    - The MN detects whether it has moved from one link to another.
    - The MN obtains a care-of address when connected to a new link.

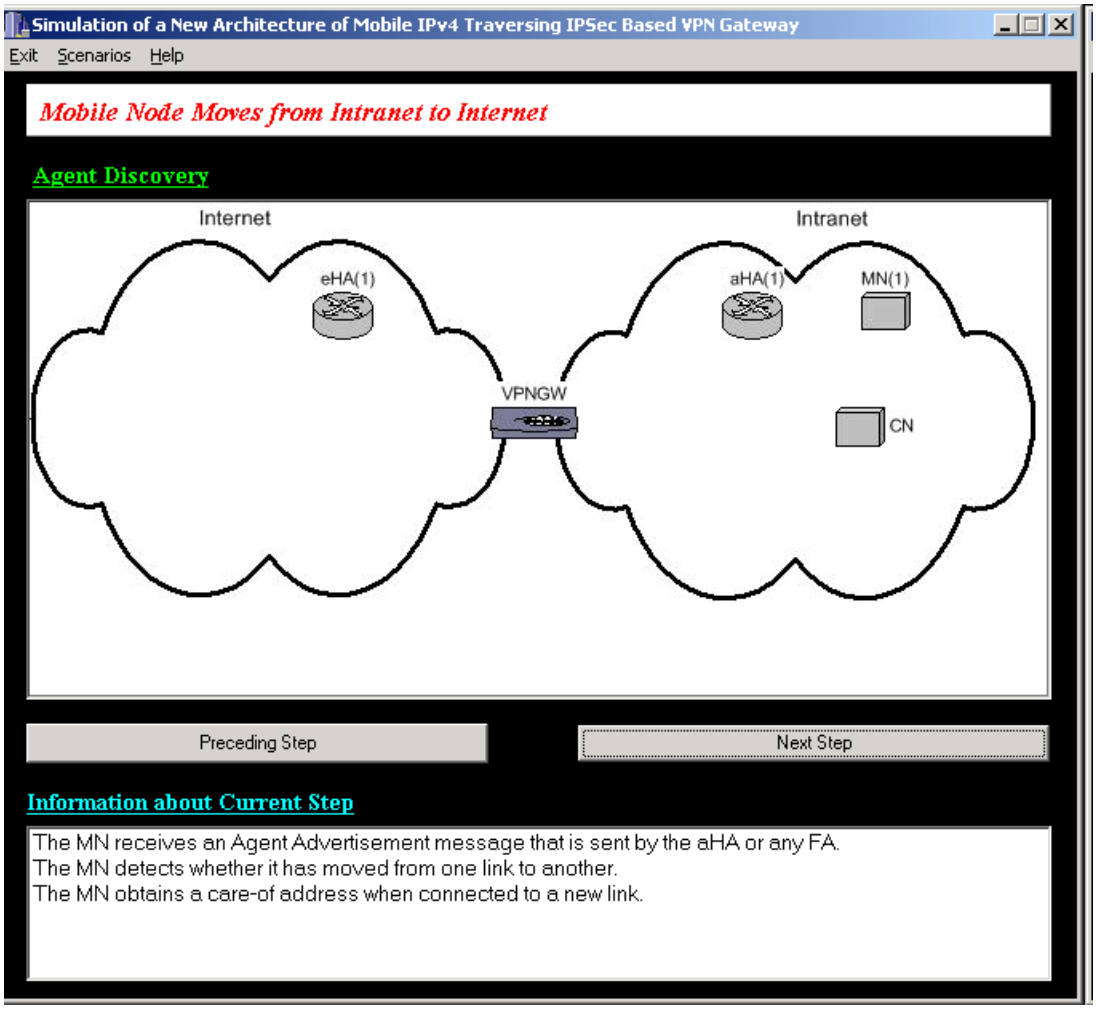

Figure A.7. Second step of agent discovery in Intranet for the simulation example

- First step of registration process in Intranet
    - This step is shown in Figure A.8.
    - The MN sends a Registration Request message to the aHA.
    - A Registration Request message is sent by a mobile node to begin the registration process.

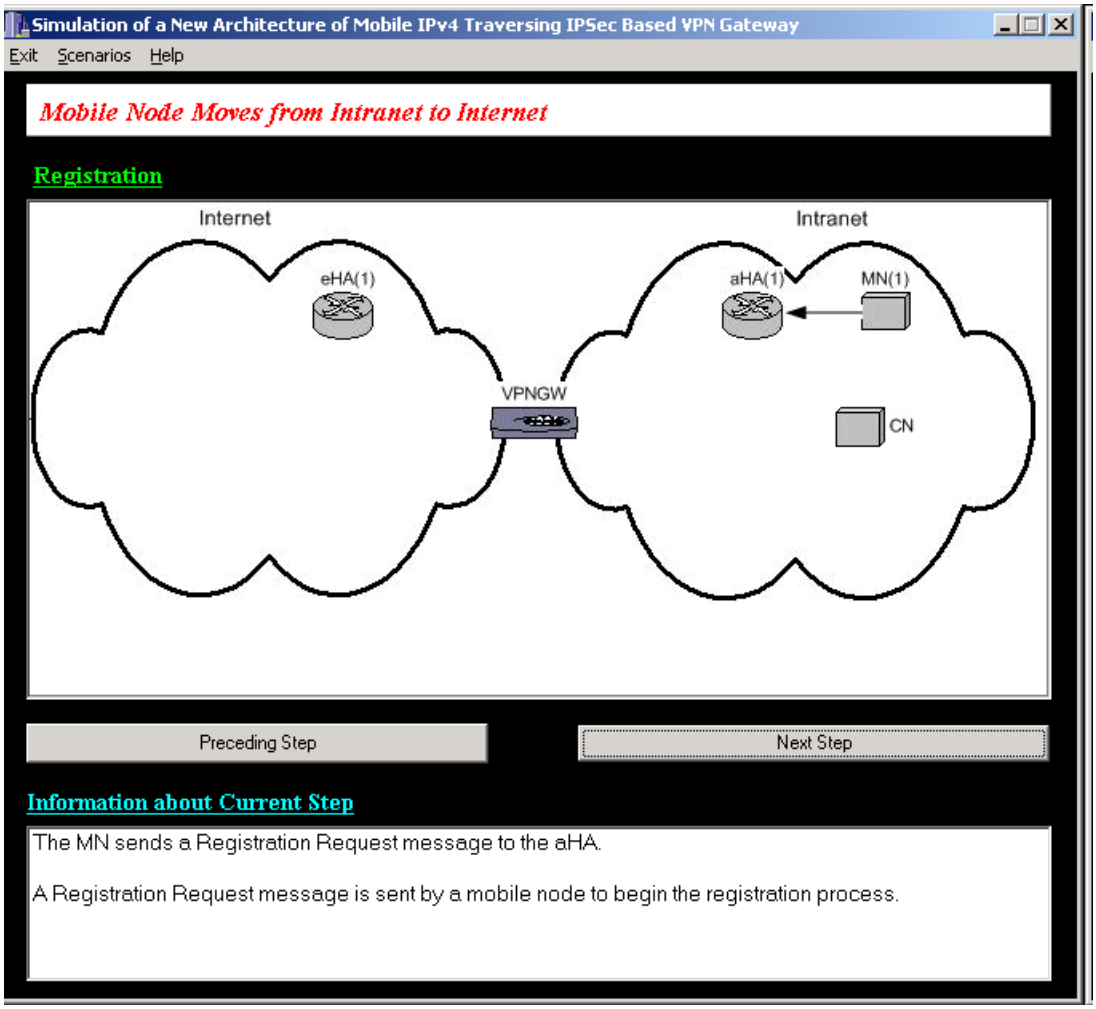

Figure A.8. First step of registration in Intranet for the simulation example

- Second step of registration process in Intranet
    - This step is shown in Figure A.9.
    - The aHA checks the Registration Request message if the MN comes from the Internet or is a new MN that is not registered before to the eHA.
    - If the MN comes from the Internet, the aHA updates its binding entry and its mode form slave to master for this MN.
    - If the MN is a new MN, the aHA creates a new binding entry for the MN.

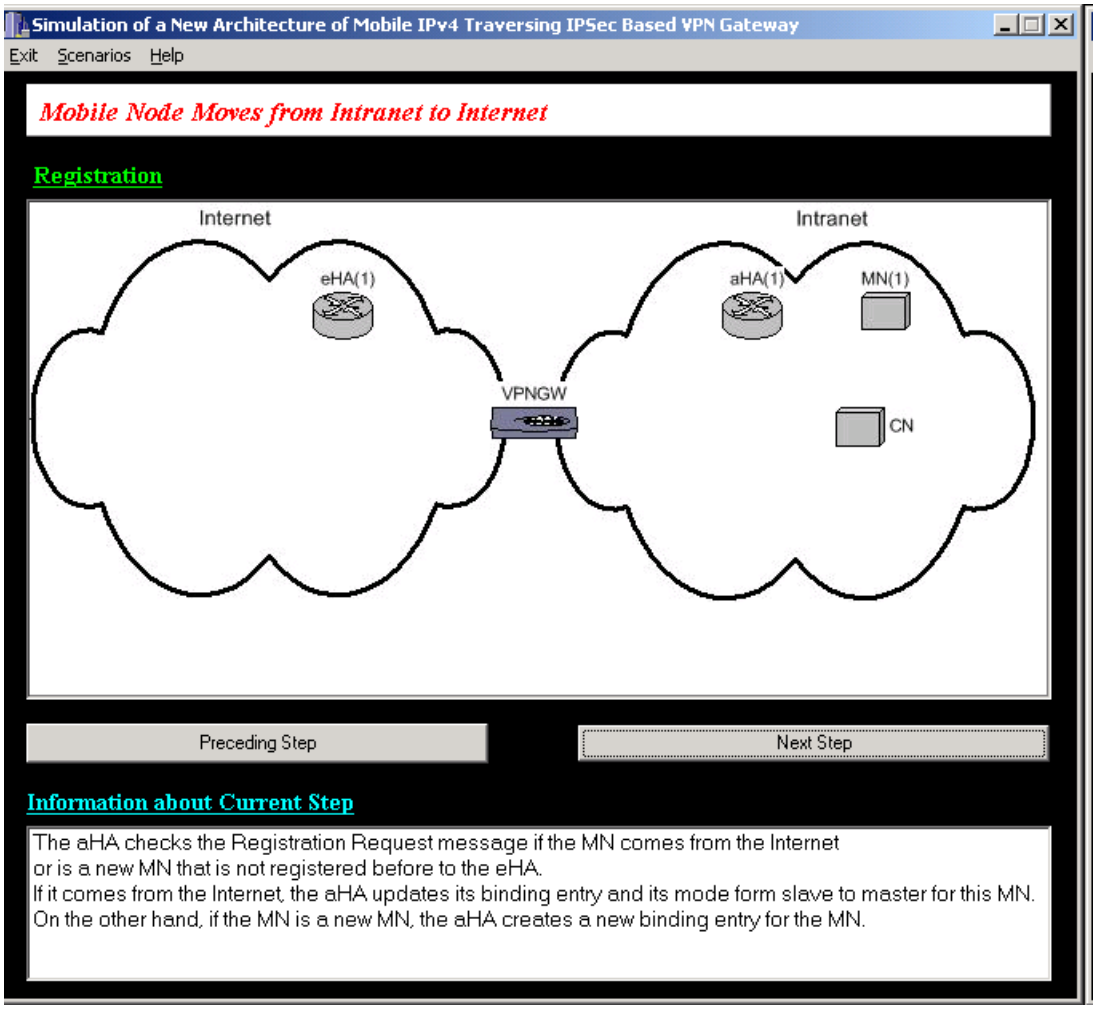

Figure A.9. Second step of registration in Intranet for the simulation example

- Third step of registration process in Intranet
    - This step is shown in Figure A.10.
    - The aHA sends a Registration Replay to the MN. It is assumed that the registration request is accepted.
    - The aHA informs the eHA about the MN.
    - The structure of datagram between the aHA and the VPN Gateway = IP(P):
        - Source IP address : IP address of aHA(1),
        - Destination IP address : IP address of eHA(1).
    - The structure of datagram between the VPN Gateway and the eHA = IP(AH(ESP(IP(P)))):
        - Source IP address : IP address of VPN Gateway,

- Destination IP address : IP address of eHA(1).

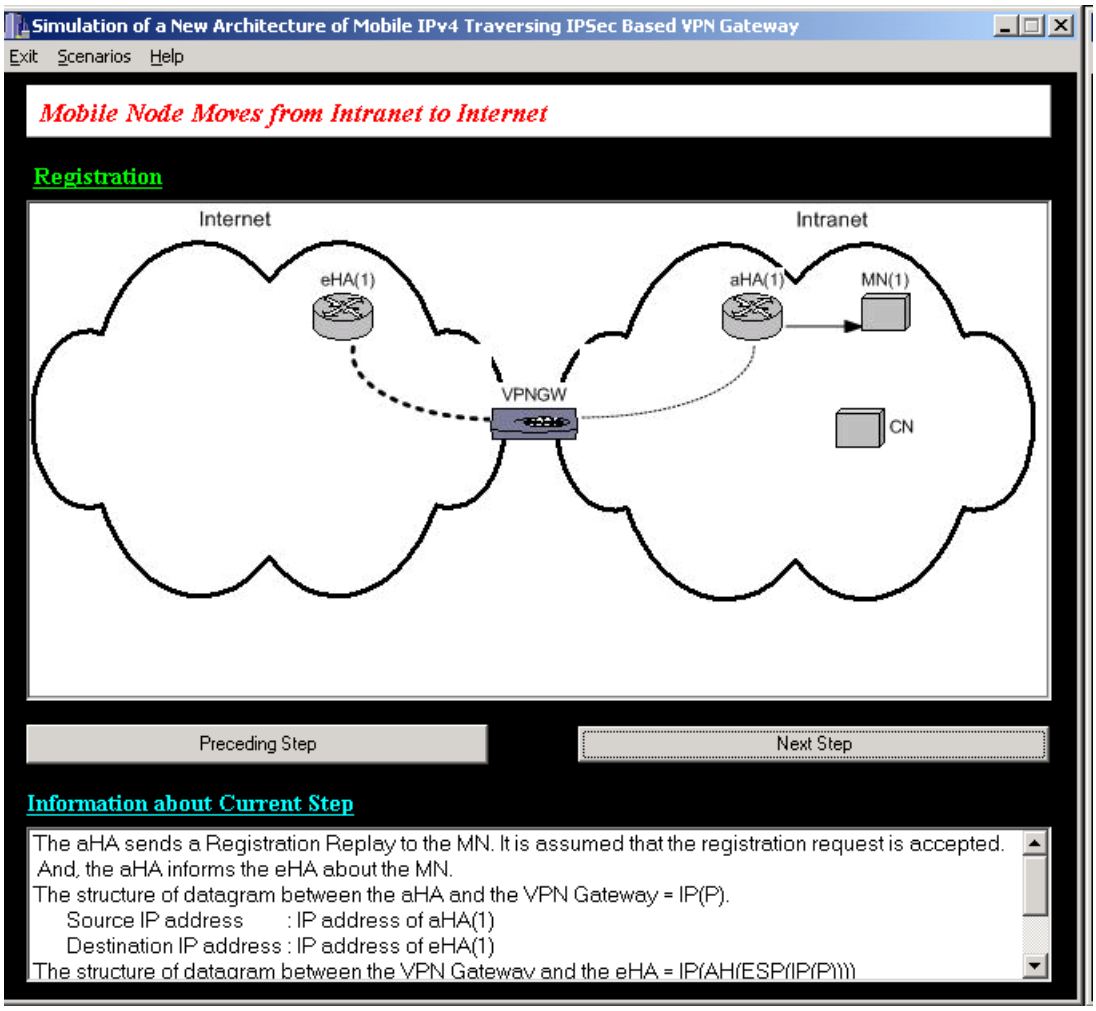

Figure A.10. Third step of registration in Intranet for the simulation example

- Fourth step of registration process in Intranet
    - This step is shown in Figure A.11.
    - The MN is ready to exchange user data.

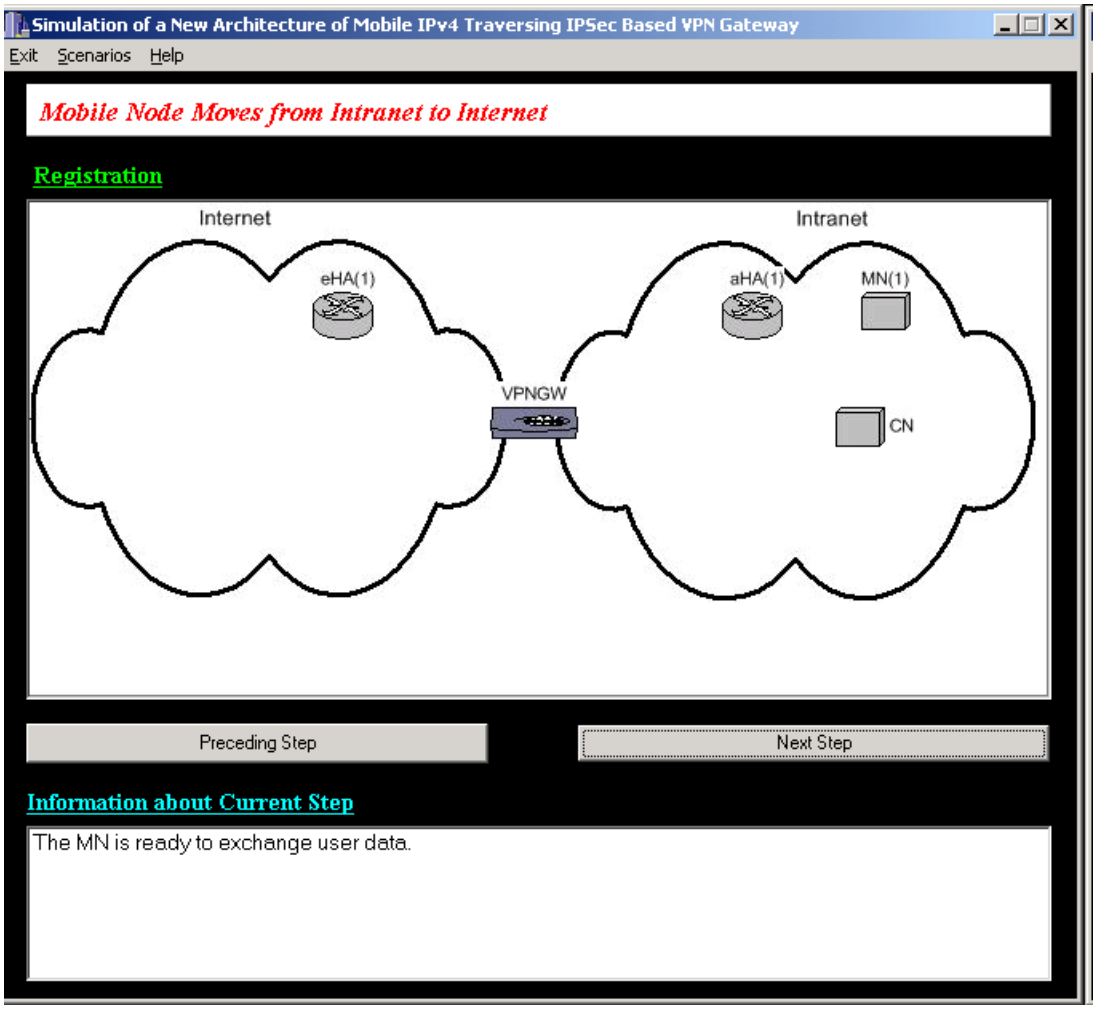

Figure A.11. Fourth step of registration in Intranet for the simulation example

- First step of routing process in Intranet
    - This step is shown in Figure A.12.
    - HSI = 0.
    - The MN sends an IP packet to the CN with following properties:
        - The structure of datagram = IP(P),
        - Source IP address : permanent IP address of MN,
        - Destination IP address : IP address of CN.

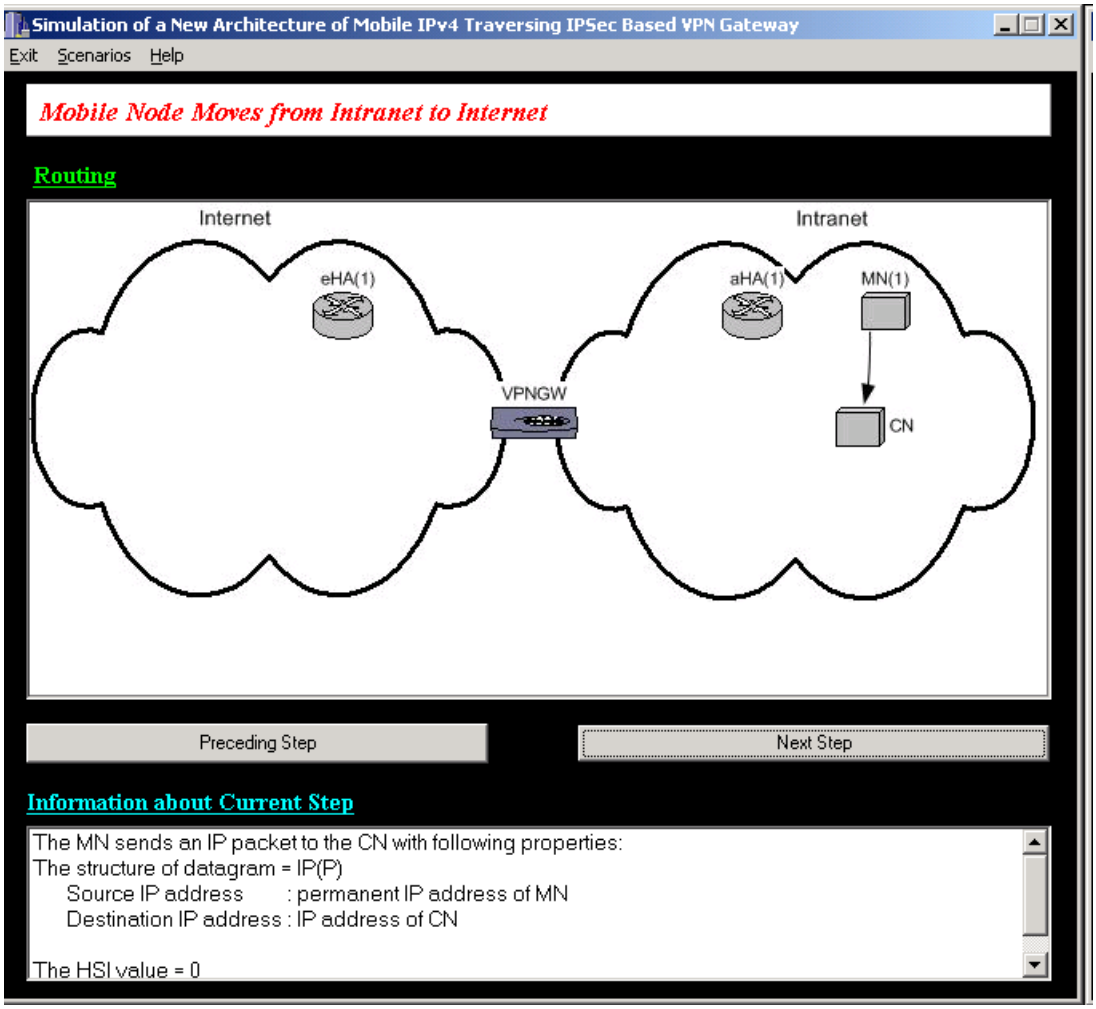

Figure A.12. First step of routing in Intranet for the simulation example

- Second step of routing process in Intranet
    - This step is shown in Figure A.13.
    - HSI = 0.
    - The CN sends an IP packet to the MN with the following properties:
        - The structure of datagram = IP(P),
        - Source IP address : IP address of CN,
        - Destination IP address : permanent IP address of MN.

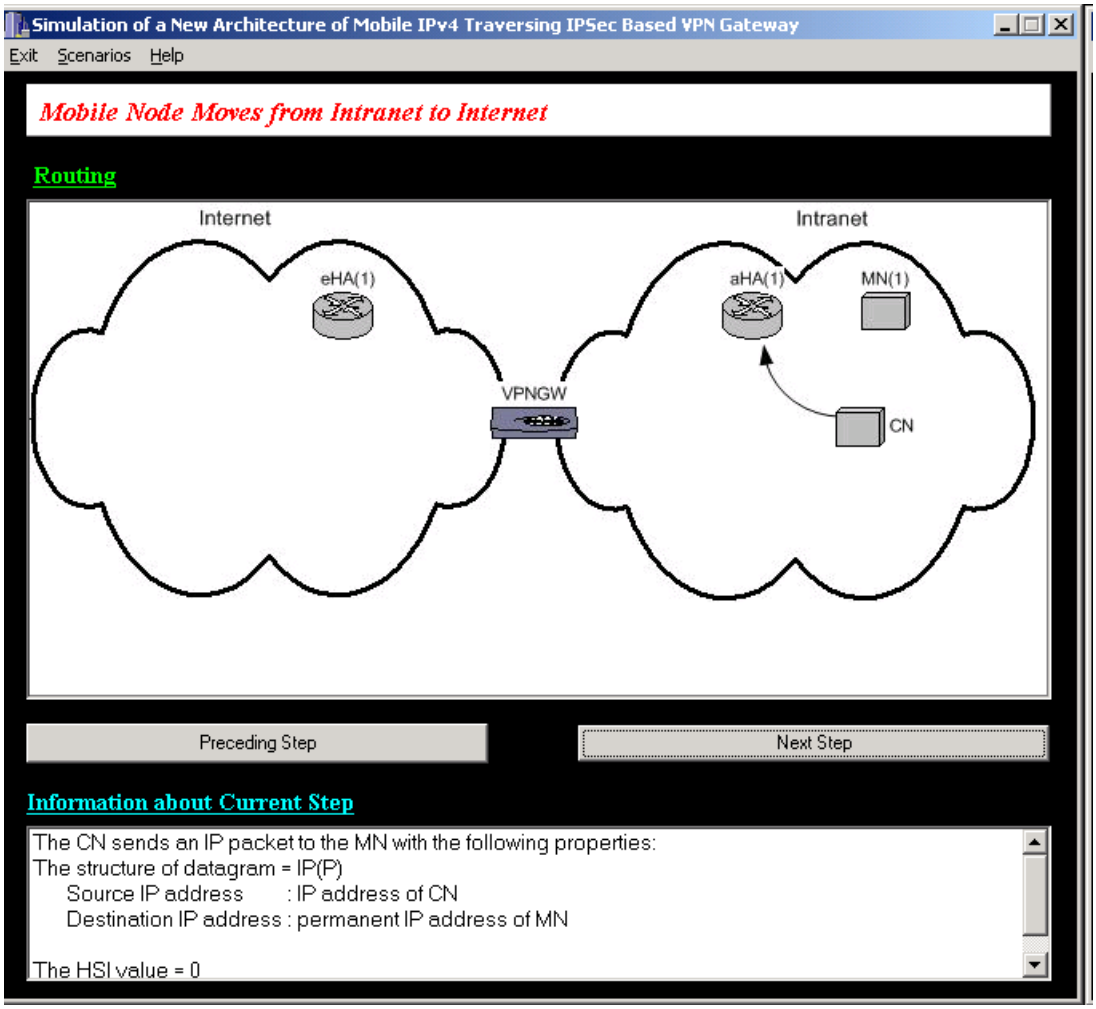

Figure A.13. Second step of routing in Intranet for the simulation example

- Third step of routing process in Intranet
    - This step is shown in Figure A.14.
    - HSI = 1.
    - The aHA encapsulates (IP in IP encapsulation) the received packet with the following properties:
        - The structure of datagram = IP(IP(P)),
        - Source IP address of outer datagram : IP address of CN,
        - Destination IP address of outer datagram : care-of address of MN.

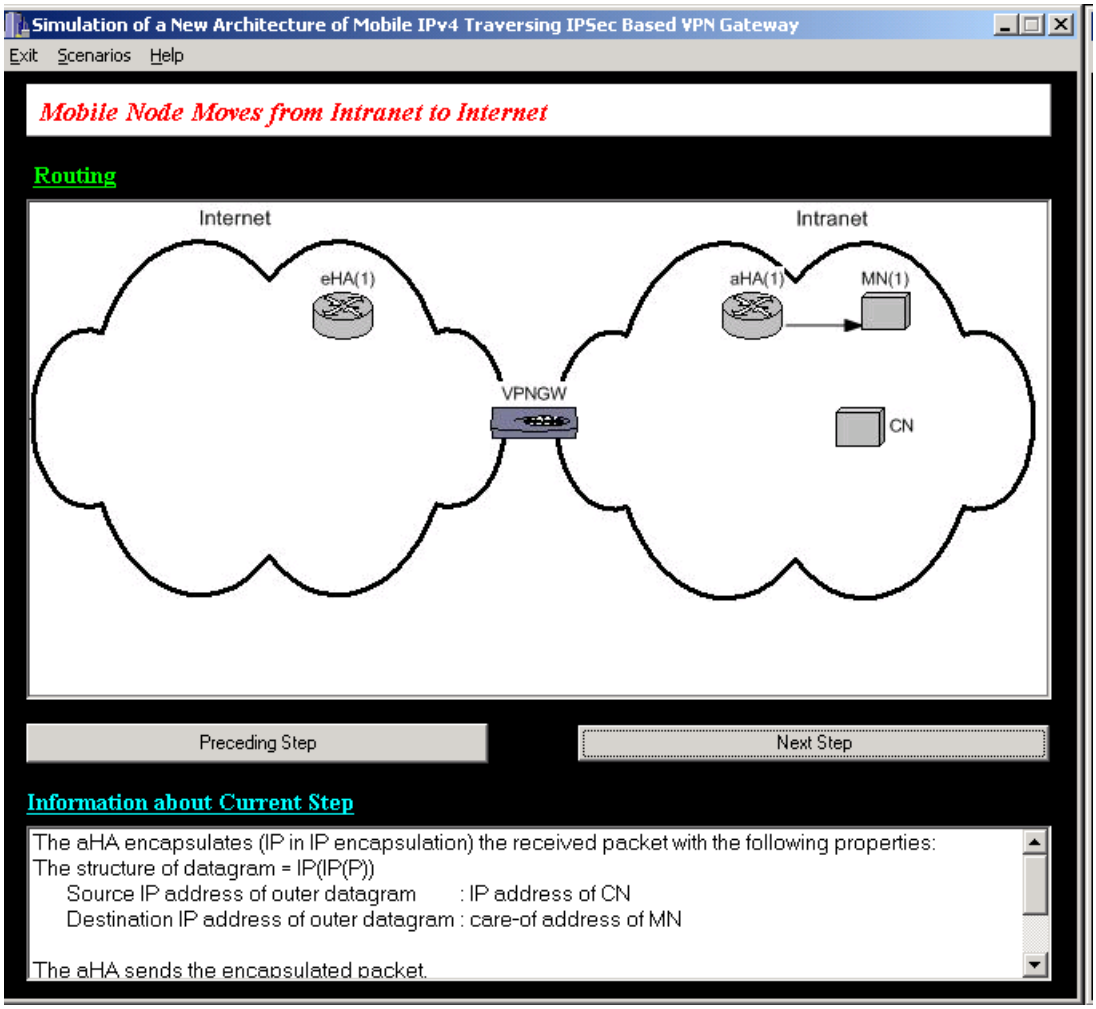

Figure A.14. Third step of routing in Intranet for the simulation example

- Fourth step of routing process in Intranet
    - This step is shown in Figure A.15.
    - The MN receives the encapsulated packet.
    - The MN decapsulates the tunneled datagram and processes the original datagram

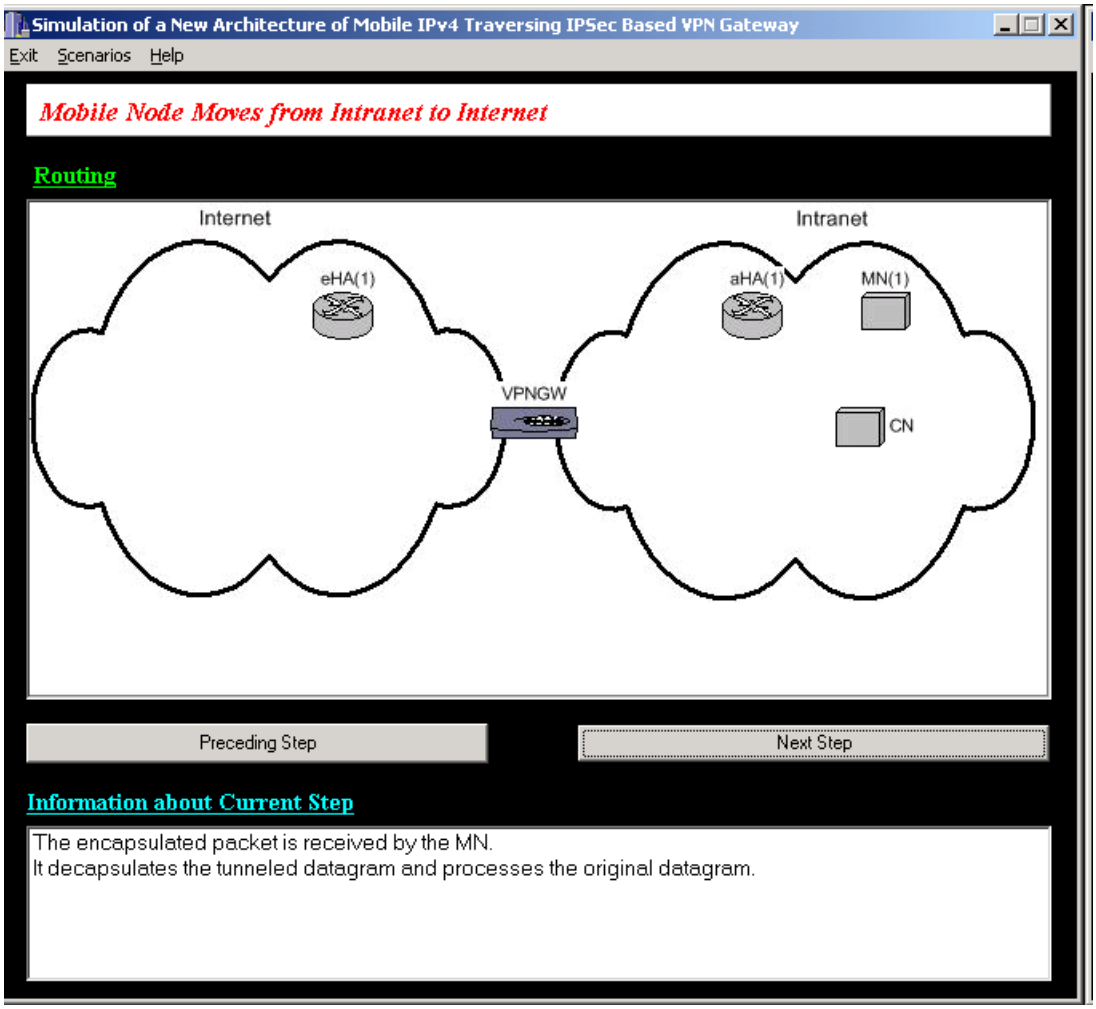

Figure A.15. Fourth step of routing in Intranet for the simulation example

- Network change step
    - This step is shown in Figure A.16.
    - The MN moves from the Intranet to the Internet.

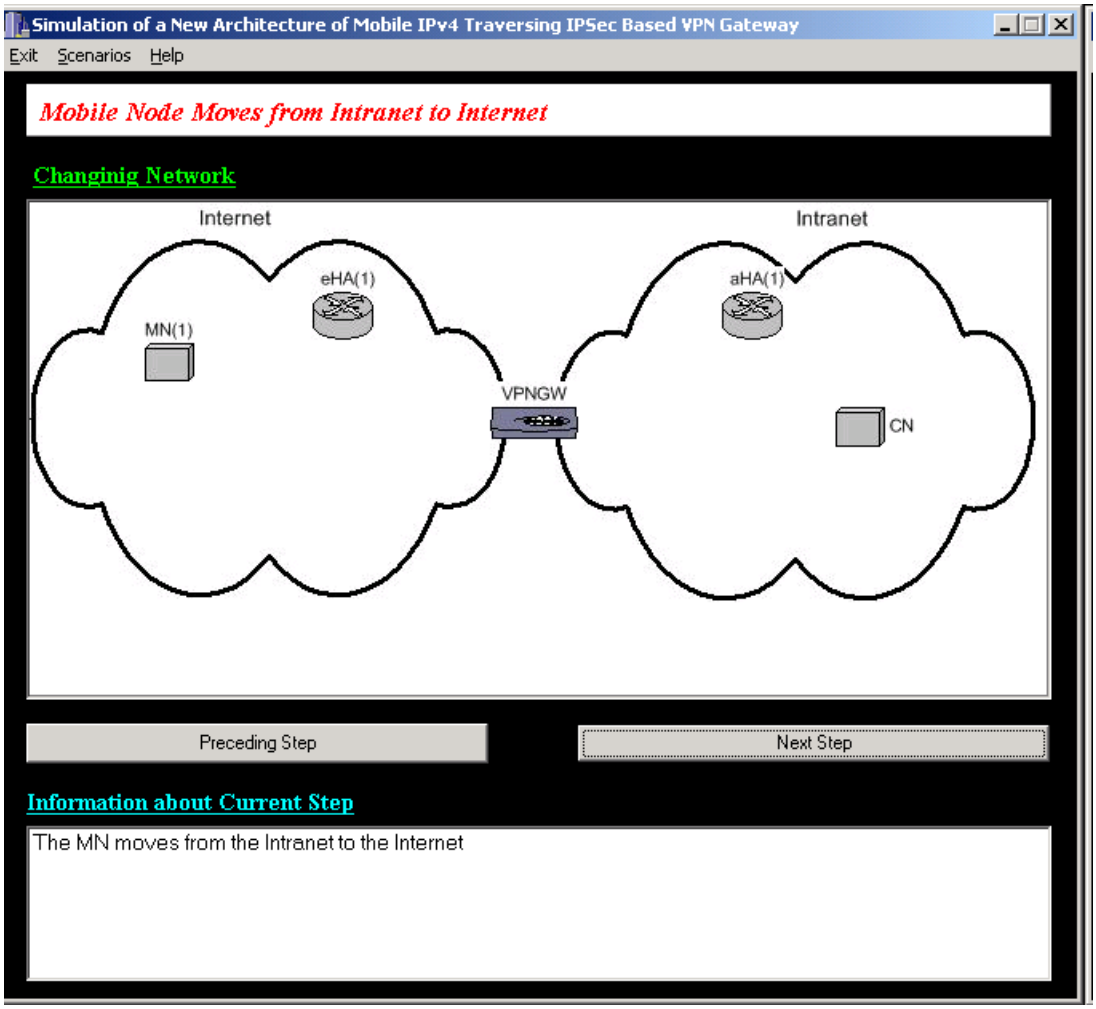

Figure A. 16. Network change step for the simulation example

- Network detection step
    - This step is shown in Figure A.17.
    - The MN detects network change, the change from the Intranet to the Internet.
    - Then the MN changes its mode from normal mode to secure mode.

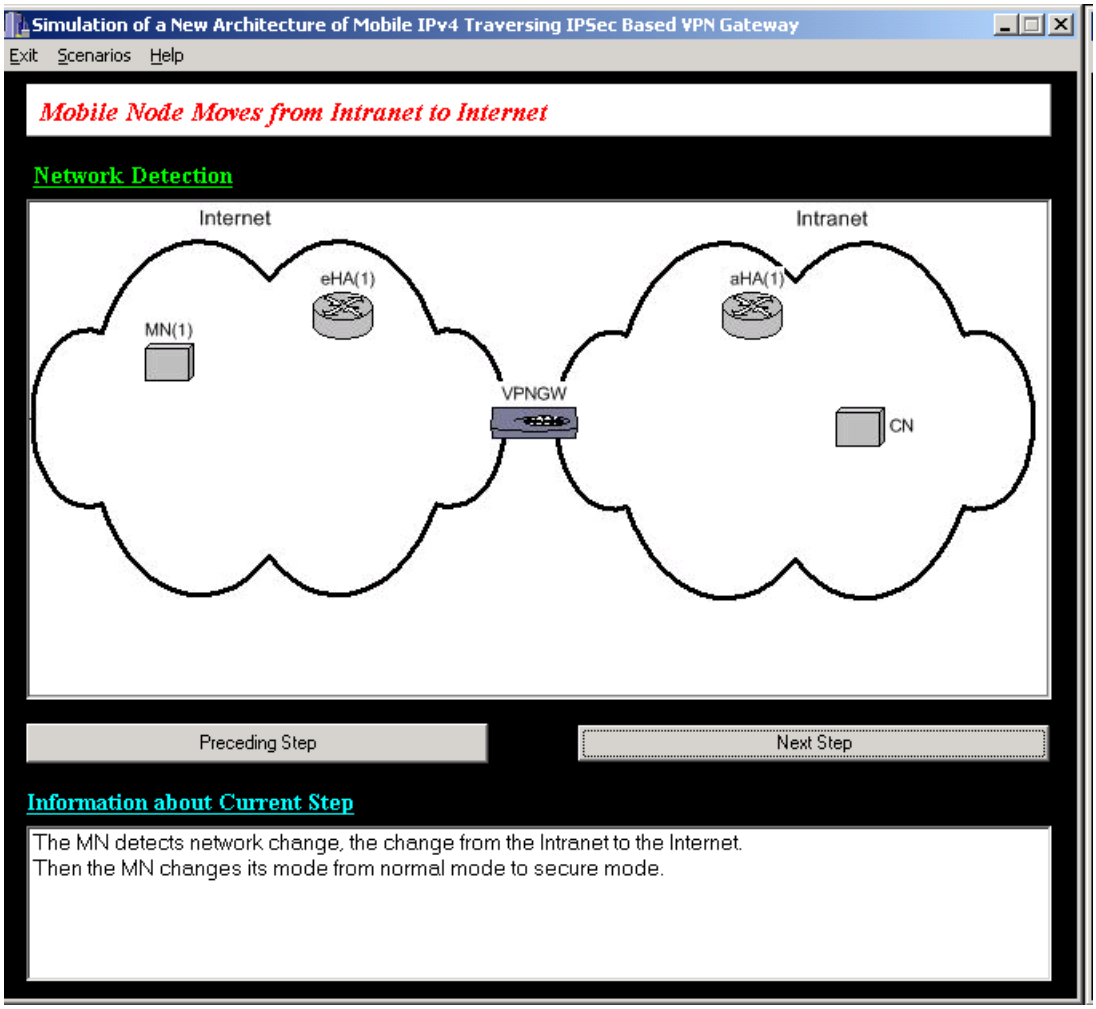

Figure A.17. Network detection step for the simulation example

- First step of agent discovery process in Internet
    - This step is shown in Figure A.18.
    - The eHA or any FA broadcasts Agent Advertisements messages.
    - Agent Advertisements are periodically transmitted as multicasts or broadcasts to each link on which a node is configured to perform as a home agent, a foreign agent, or both. This allows a mobile node that is connected to such a link to determine whether any agent is present and, if so, their respective identities (IP addresses) and capabilities.

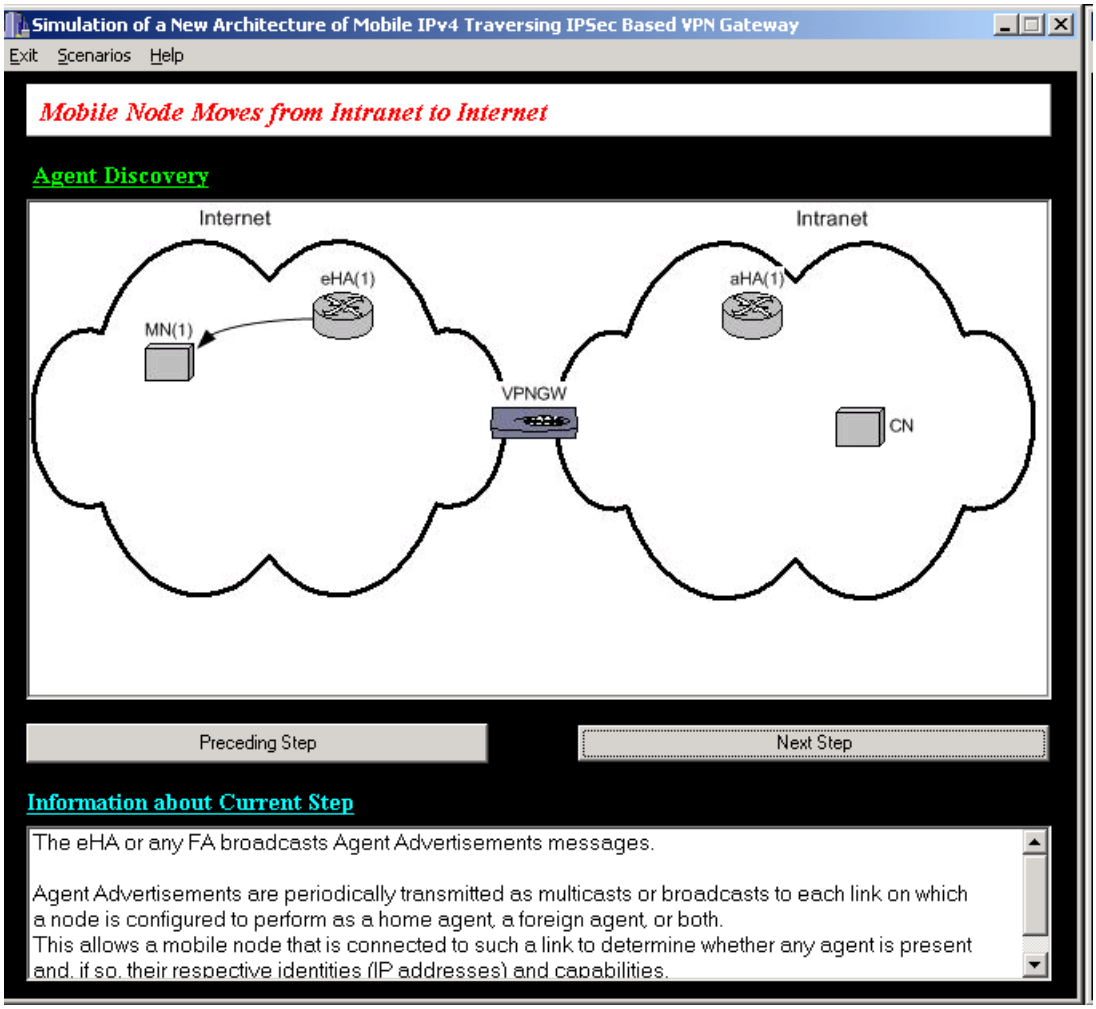

Figure A.18. First step of agent discovery in Internet for the simulation example

- Second step of agent discovery process in Internet
    - This step is shown in Figure A.19.
    - The MN receives an Agent Advertisement message that is sent by the eHA or any FA.
    - The MN detects whether it has moved from one link to another.
    - The MN obtains a care-of address when connected to a new link.

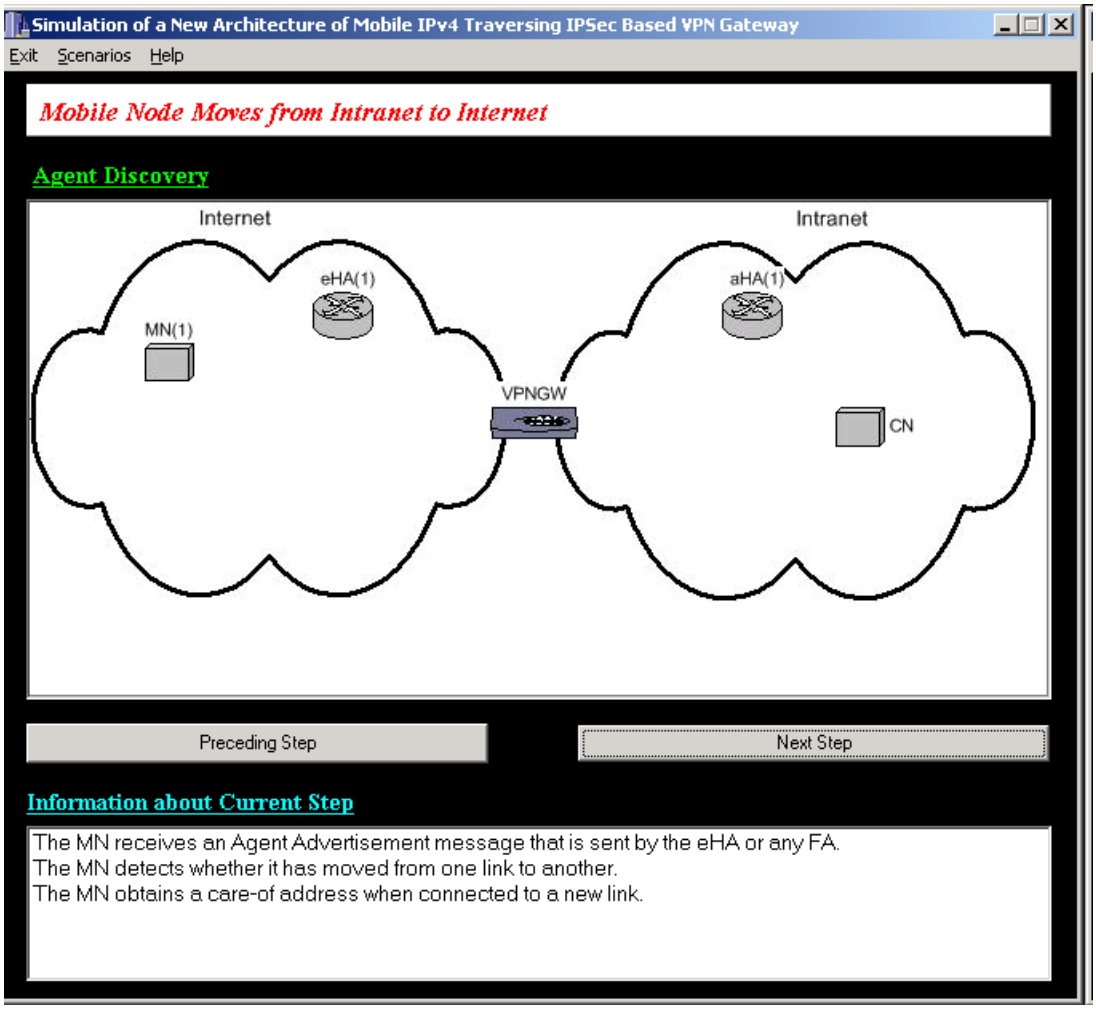

Figure A.19. Second step of agent discovery in Internet for the simulation example

- First step of registration process in Internet
    - This step is shown in Figure A.20
    - The MN sends a Registration Request message to the eHA.
    - A Registration Request message is sent by a mobile node to update its state (binding entry) information on the eHA and the aHA.

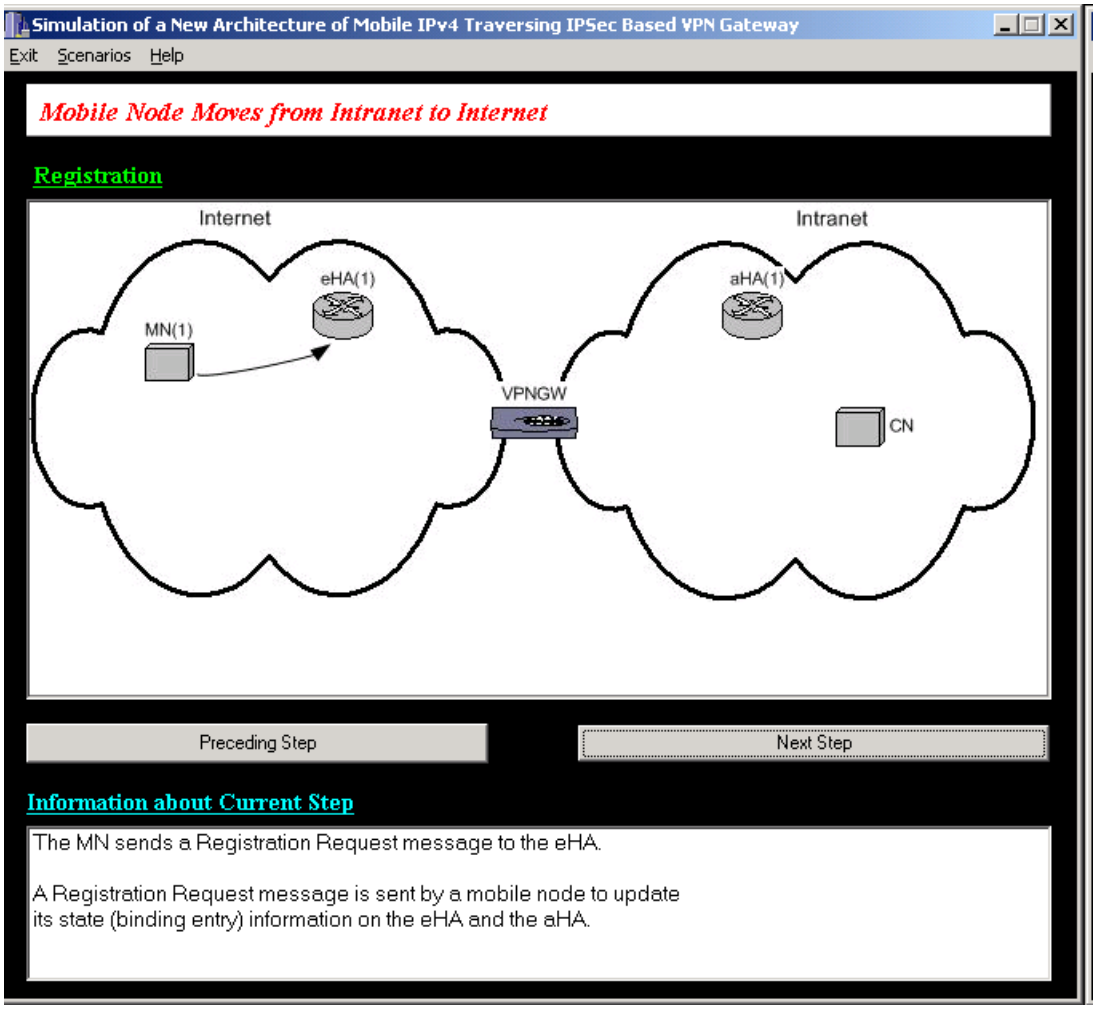

Figure A.20. First step of registration in Internet for the simulation example

- Second step of registration process in Internet
    - This step is shown in Figure A.21.
    - The eHA checks the Registration Request message if the MN comes from the Intranet or is a new MN that is not registered before to the aHA.
    - If the MN comes from the Intranet, the eHA updates its binding entry and its mode form slave to master for this MN.
    - if the MN is a new MN, the eHA creates a new binding entry for the MN.
    - The eHA changes its state form slave (passive) to master (active) in this scenario.

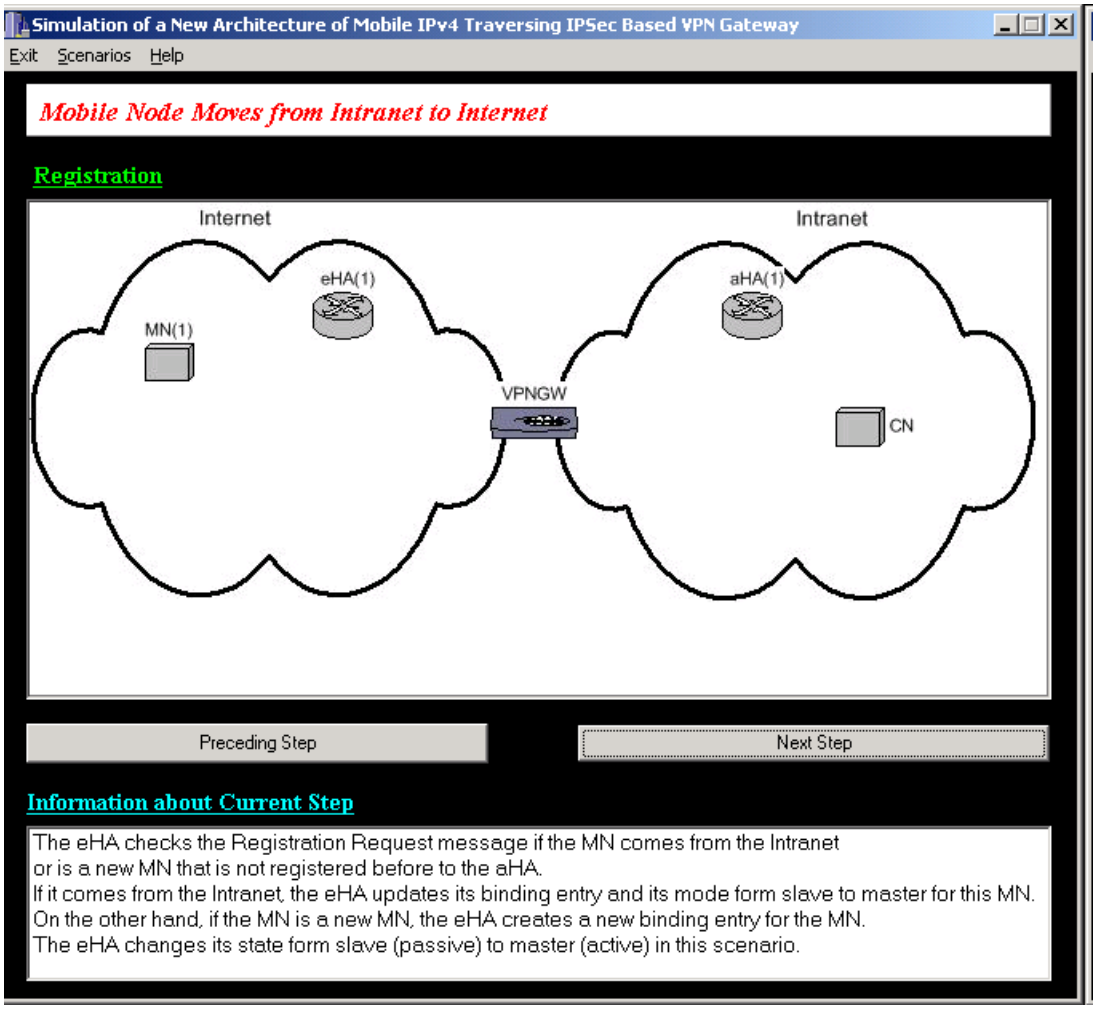

Figure A.21. Second step of registration in Internet for the simulation example

- Third step of registration process in Internet
    - This step is shown in Figure A.22.
    - The eHA sends a Registration Replay to the MN. It is assumed that the registration request is accepted.
    - The eHA informs the aHA about the MN.
    - The structure of datagram between the aHA and the VPN Gateway = IP(P),
        - Source IP address : IP address of eHA(1),
        - Destination IP address : IP address of aHA(1).
    - The structure of datagram between the VPN Gateway and the eHA = IP(AH(ESP(IP(P)))),
        - Source IP address : IP address of eHA(1),

- Destination IP address : IP address of VPN Gateway.

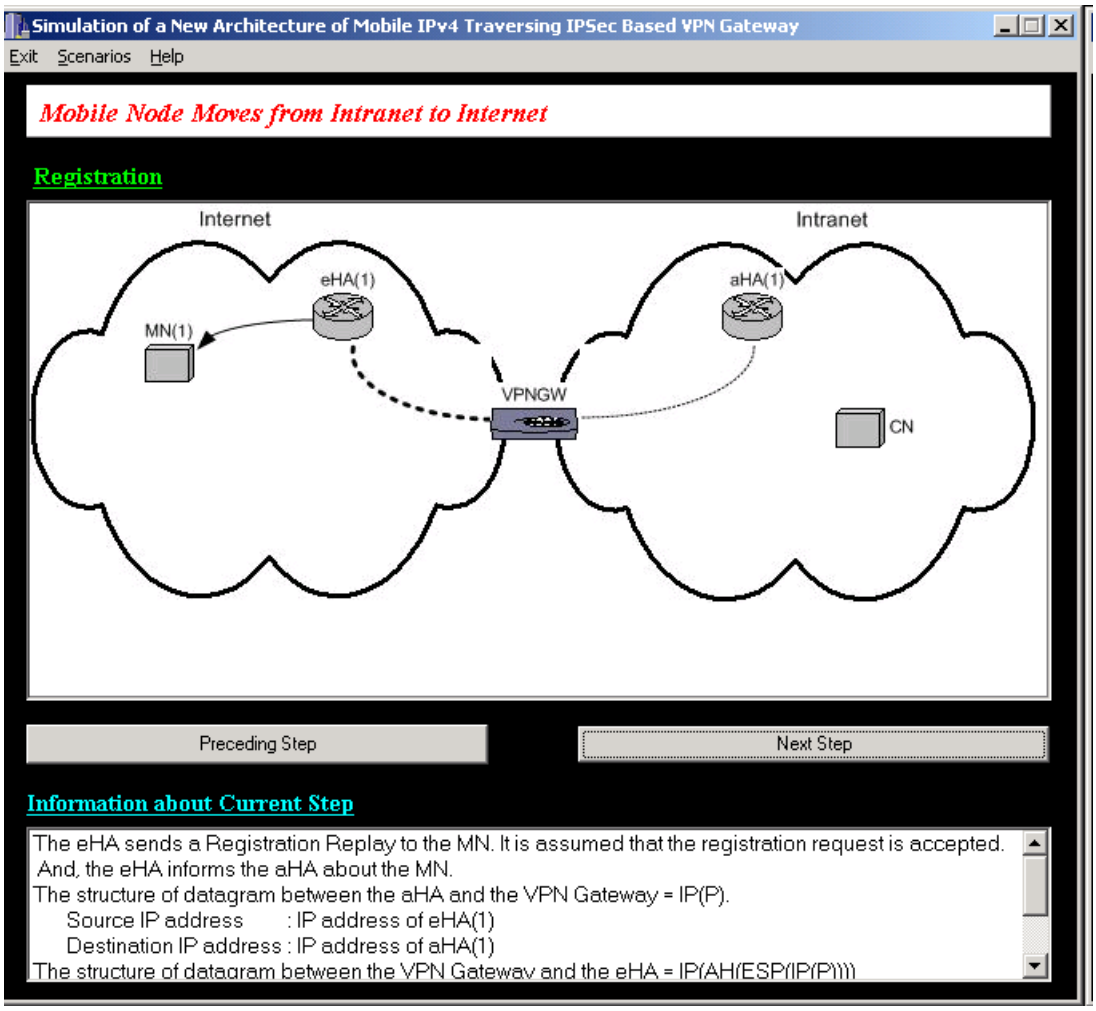

Figure A.22. Third step of registration in Internet for the simulation example

- Fourth step of registration process in Internet
    - This step is shown in Figure A.23.
    - The MN is ready to exchange user data.

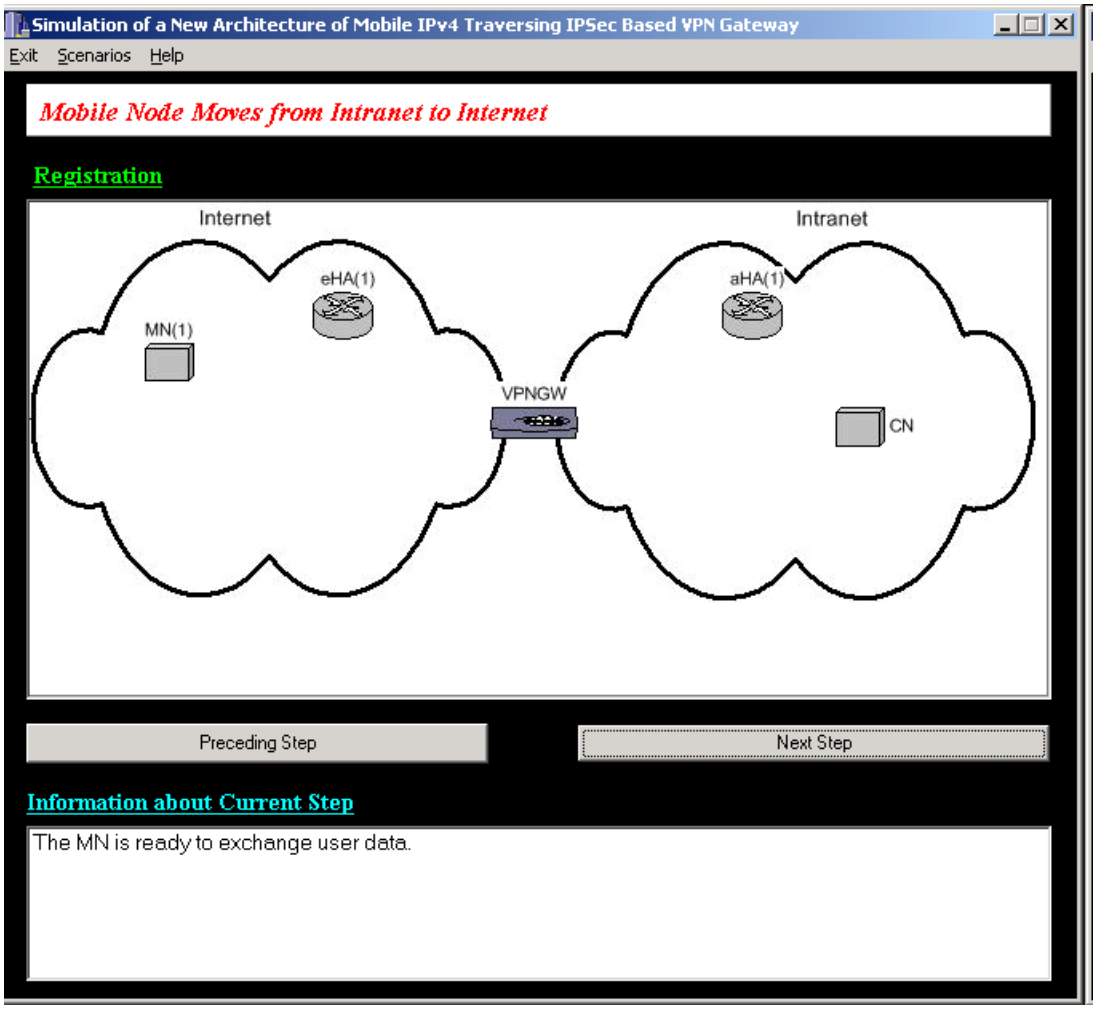

Figure A.23. Fourth step of registration in Internet for the simulation example

- First step of routing process in Internet
    - This step is shown in Figure A.24.
    - HSI = 2,1.
    - The MN sends a datagram in an IPSec tunnel to the VPN Gateway.
    - The structure of datagram = IP(AH(ESP(IP(P)))),
        - Source IP address : care-of address of MN,
        - Destination IP address : IP address of VPN Gateway.

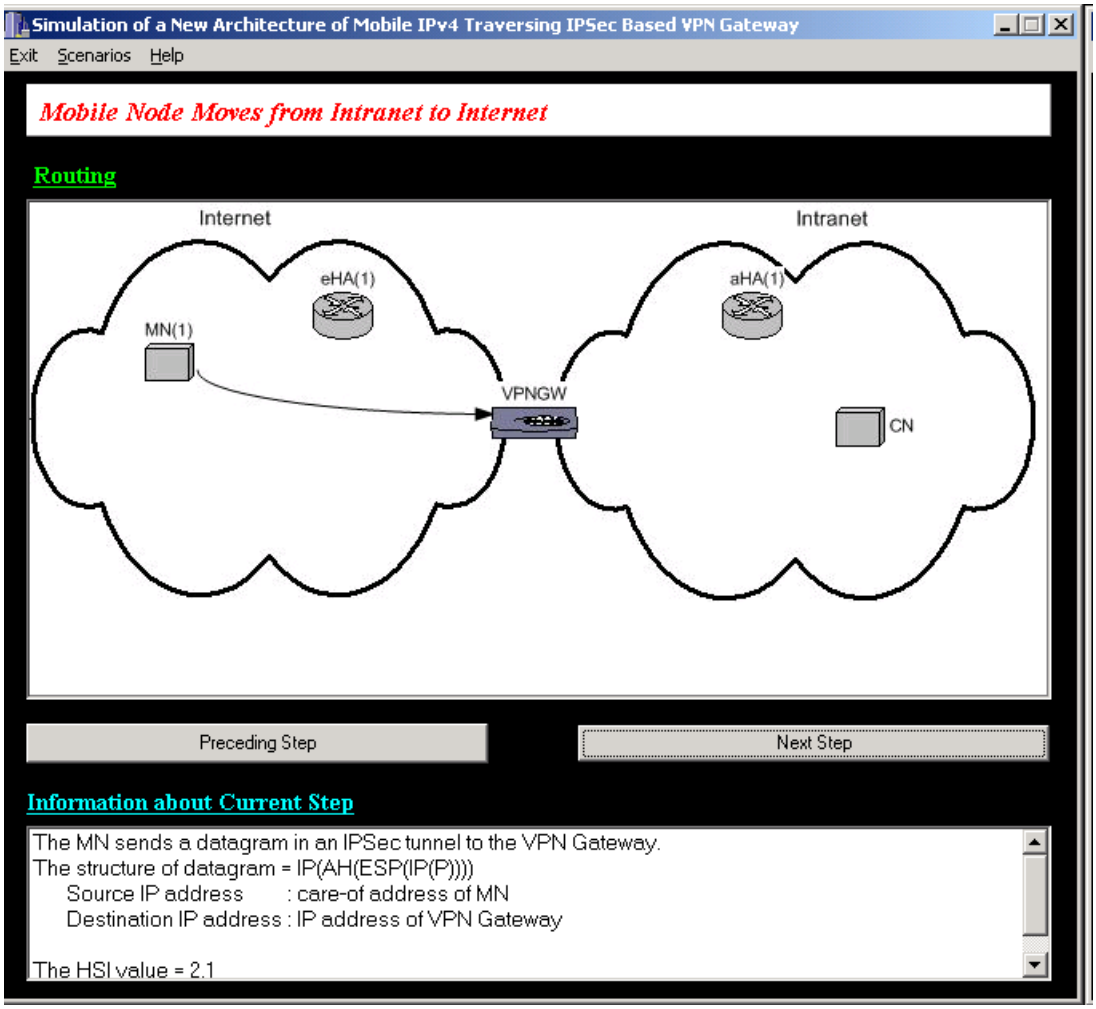

Figure A.24. First step of routing in Internet for the simulation example

- Second step of routing process in Internet
    - This step is shown in Figure A.25.
    - HSI = 0.
    - The VPN Gateway receives the datagram and decapsulates it from the IPSec tunnel.
    - The VPN Gateway sends the inner datagram to the CN.
    - The CN receives the datagram.
    - The structure of datagram = IP(P),
        - Source IP address : permanent IP address of MN,
        - Destination IP address : IP address of CN.

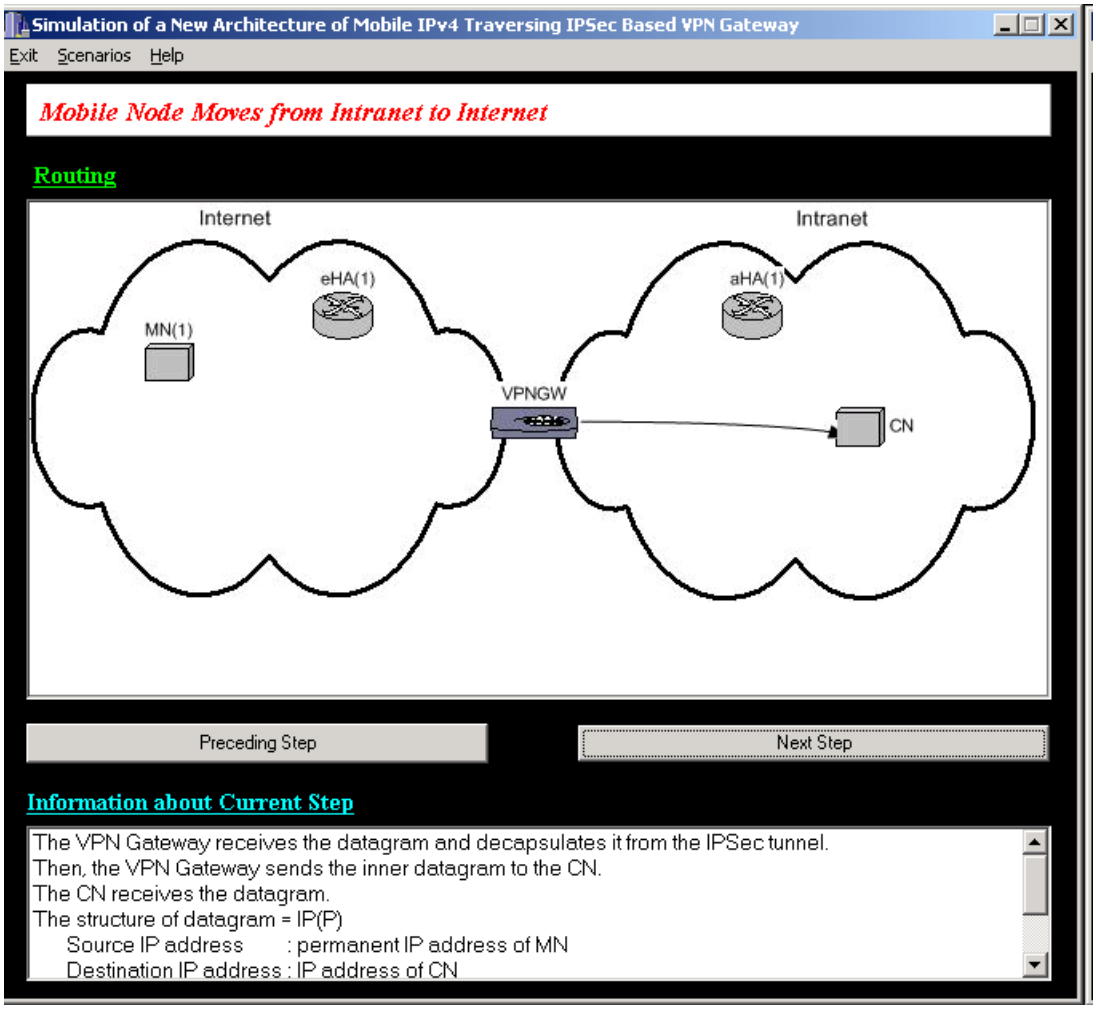

Figure A.25. Second step of routing in Internet for the simulation example

- Third step of routing process in Internet
    - This step is shown in Figure A.26.
    - HSI = 0.
    - The CN creates and sends an IP packet to the MN with the following properties:
        - The structure of datagram = IP(P),
        - Source IP address : IP address of CN,
        - Destination IP address : permanent IP address of MN.
    - The aHA receives the datagram.

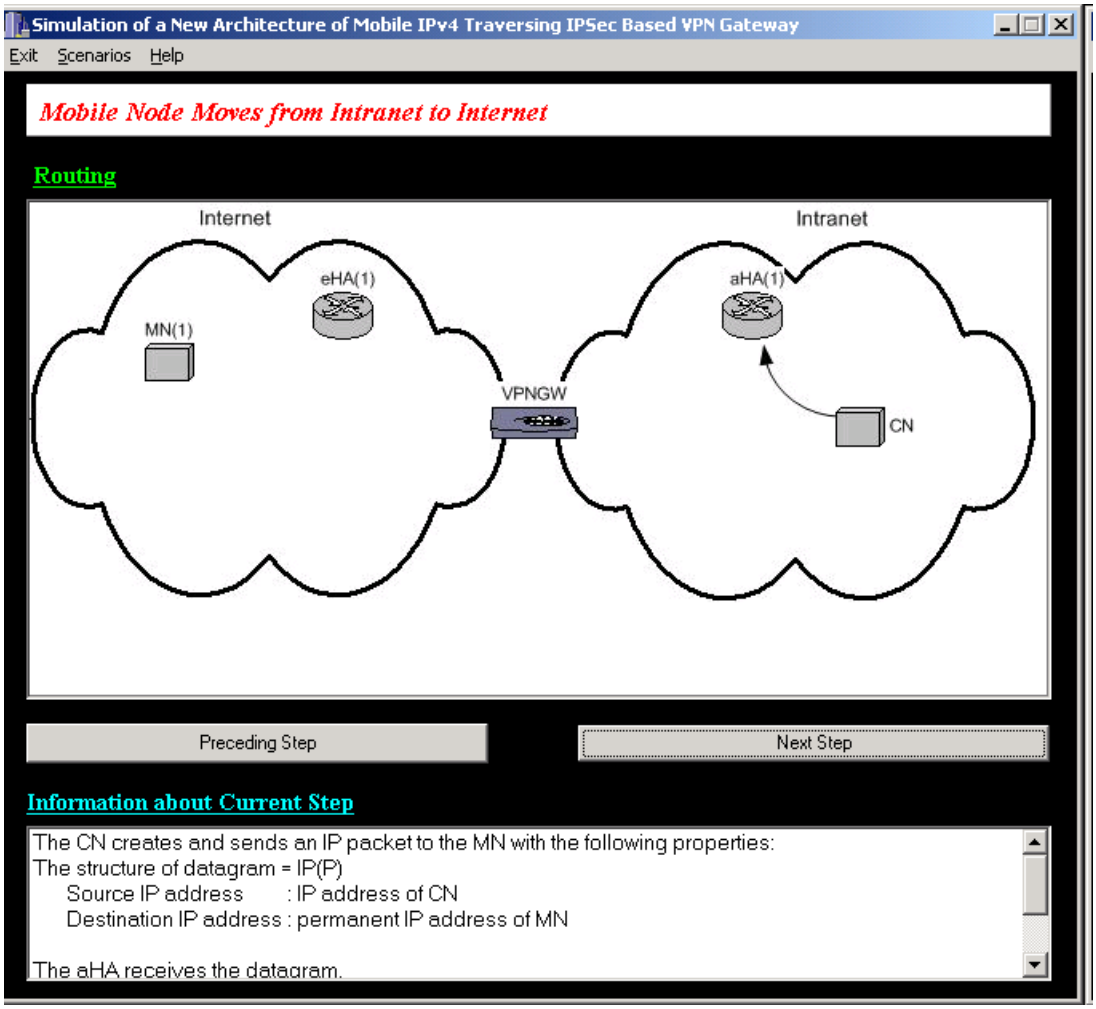

Figure A.26. Third step of routing in Internet for the simulation example

- Fourth step of routing process in Internet
    - This step is shown in Figure A.27.
    - HSI = 1.
    - The aHA encapsulates (IP in IP encapsulation) the received packet with the following properties:
        - The structure of datagram = IP(IP(P)),
        - Source IP address of outer datagram : permanent IP address of MN,
        - Destination IP address of outer datagram : IP address of eHA.
    - The aHA sends the encapsulated packet.
    - The VPN Gateway receives the datagram.

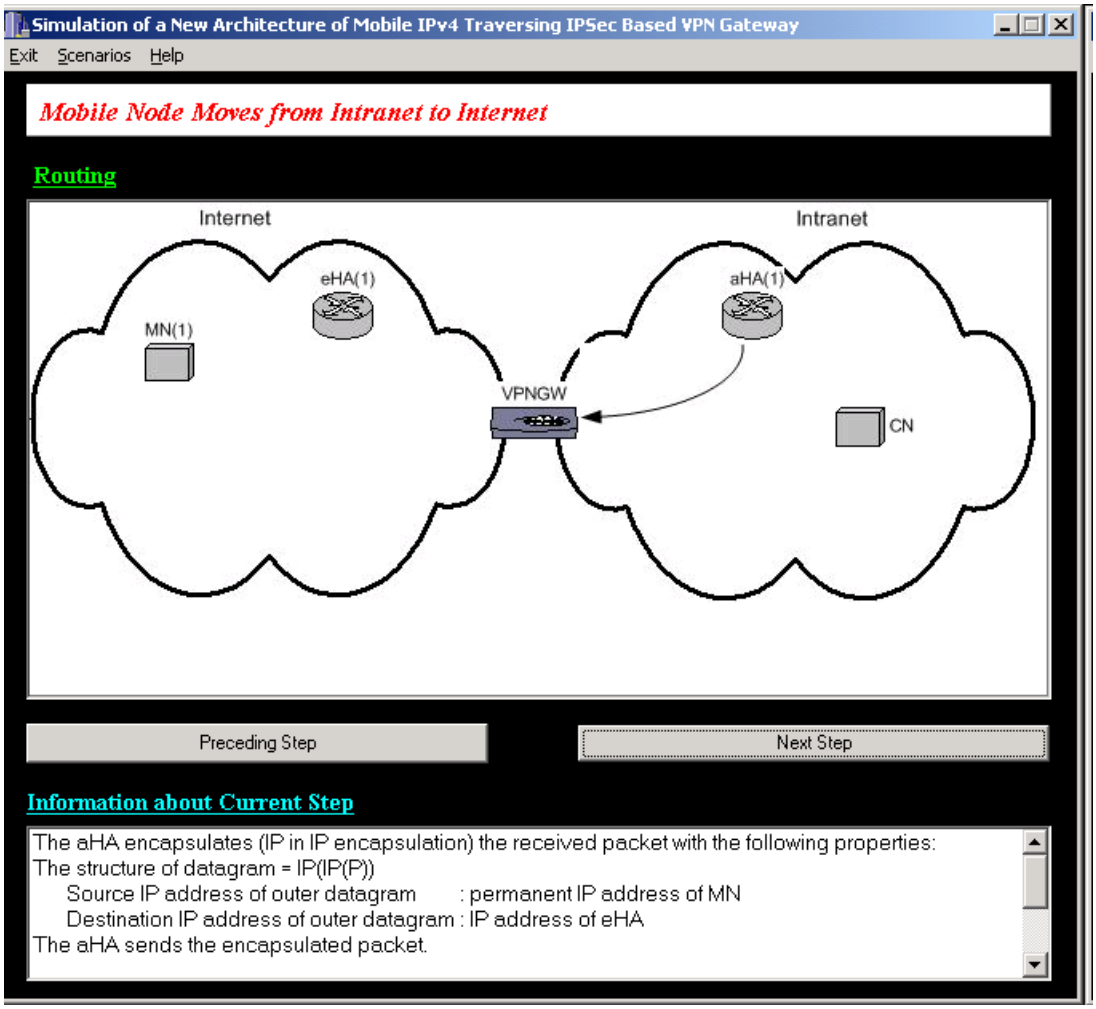

Figure A.27. Fourth step of routing in Internet for the simulation example

- Fifth step of routing process in Internet
    - This step is shown in Figure A.28.
    - HSI = 3,1.
    - The VPN Gateway encapsulates the received datagram in an IPSec tunnel with the following properties:
        - The structure of datagram = IP(AH(ESP(IP(IP(P))))),
        - Source IP address of outer datagram : IP address of VPN Gateway,
        - Destination IP address of outer datagram : permanent IP address of MN,
        - The VPN Gateway sends the encapsulated datagram.
        - The eHA receives the datagram.

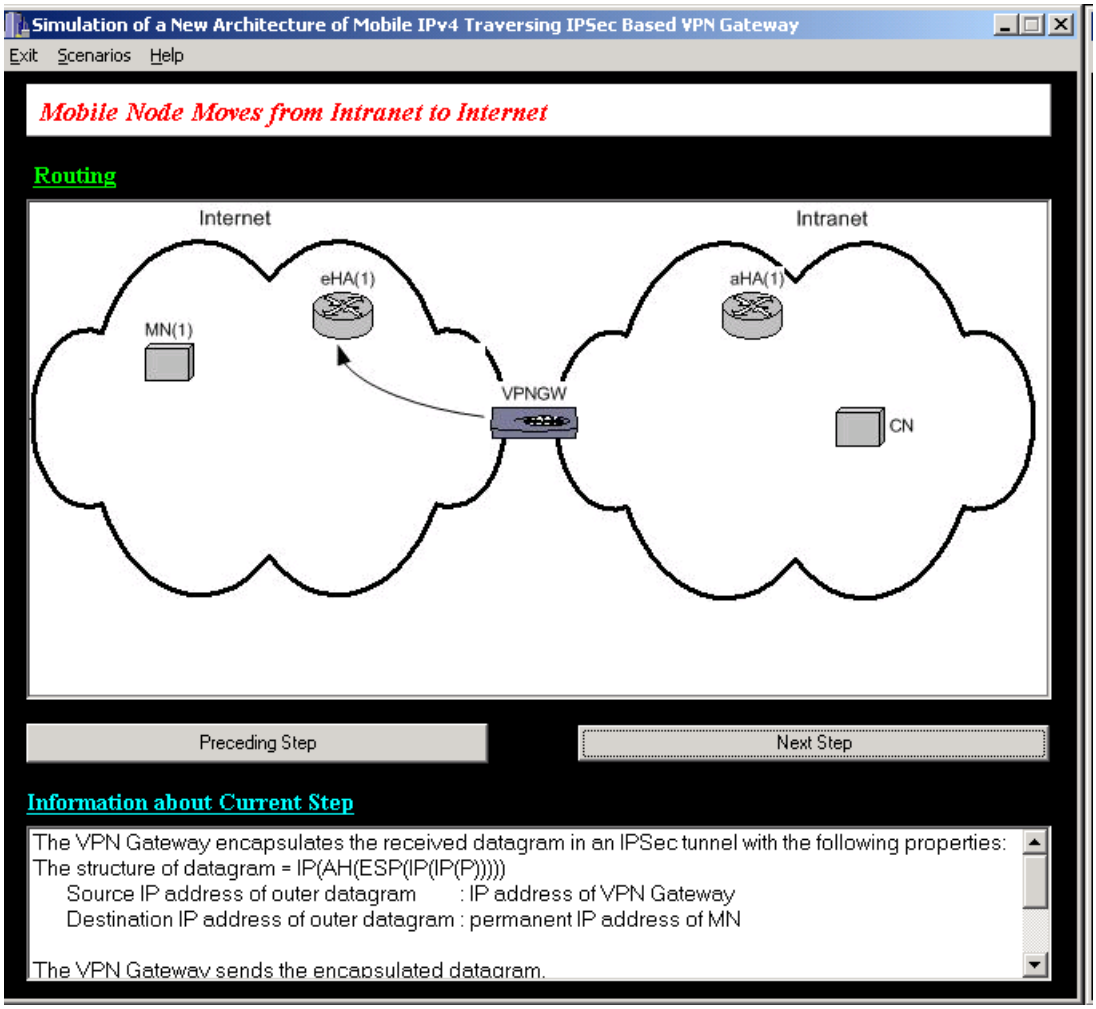

Figure A.28. Fifth step of routing in Internet for the simulation example

- Sixth step of routing process in Internet
    - This step is shown in Figure A.29.
    - HSI = 4,1.
    - The eHA encapsulates (IP in IP encapsulation) the received packet with the following properties:
        - The structure of datagram = IP(IP(AH(ESP(IP(IP(P)))))),
        - Source IP address of outer datagram : IP address of eHA,
        - Destination IP address of outer datagram : care-of address of MN.
        - The eHA sends the encapsulated datagram.
        - The MN receives the datagram.

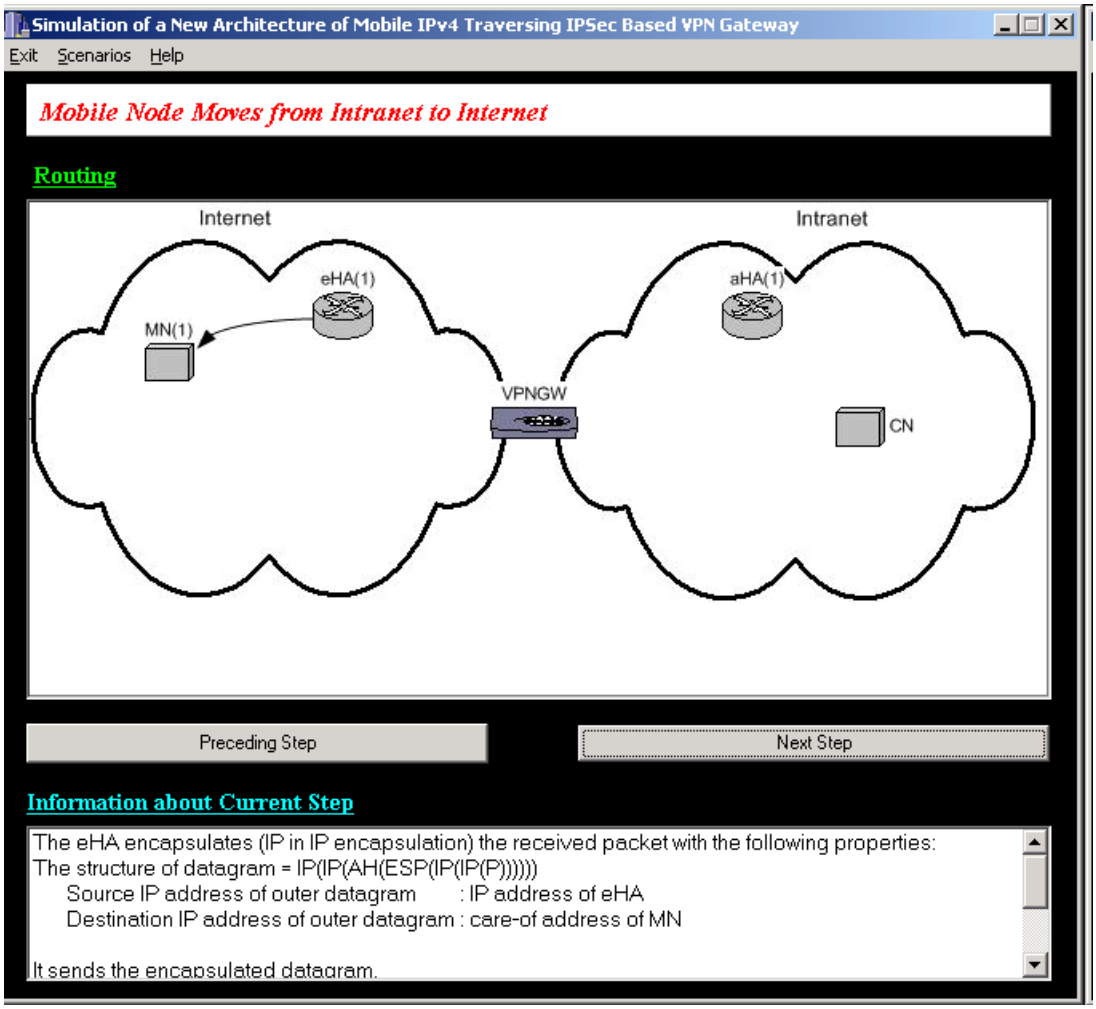

Figure A.29. Sixth step of routing in Internet for the simulation example

- Seventh step of routing process in Internet
    - This step is shown in Figure A.30.
    - The MN decapsulates the original datagram form the IPSec tunnel and from Mobile IP tunnels.

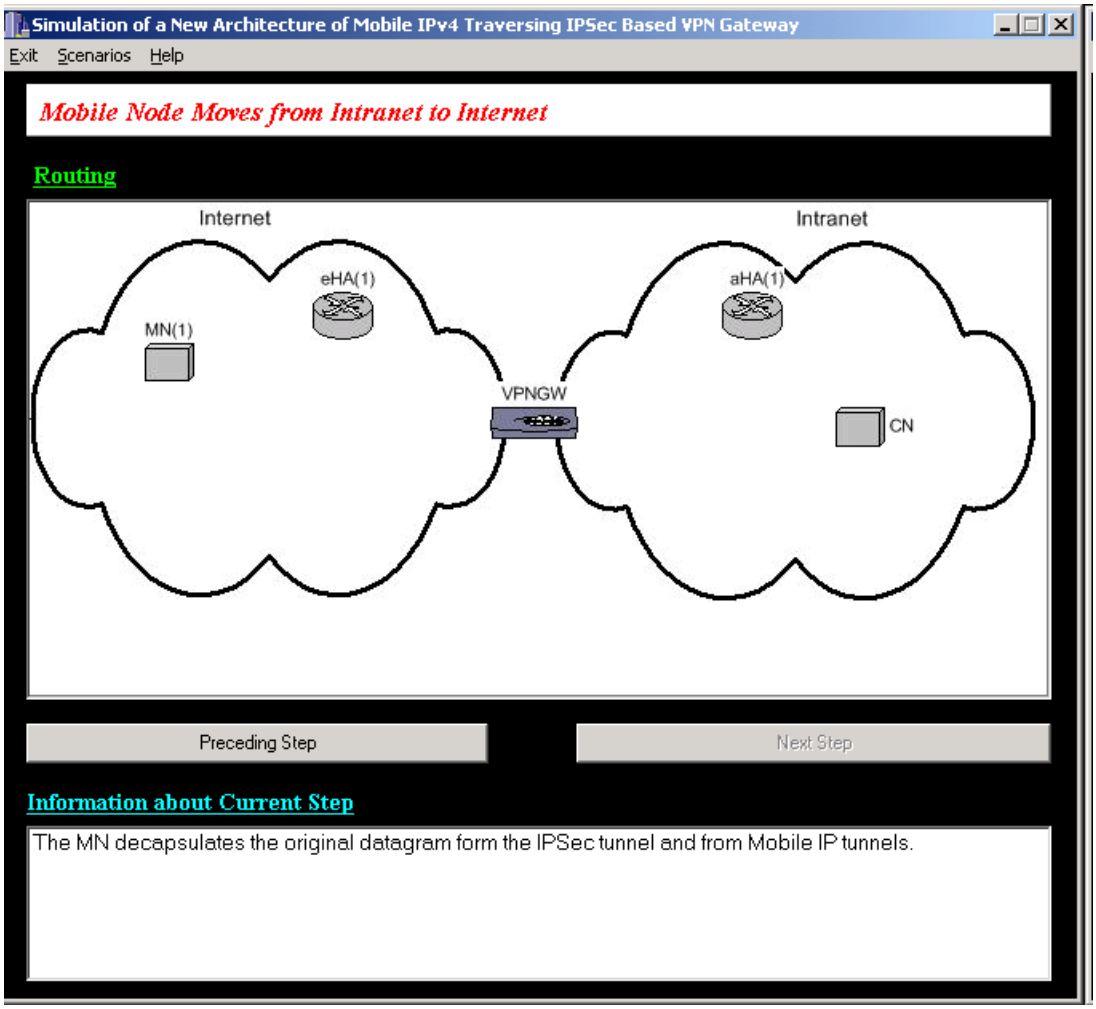

Figure A.30. Seventh step of routing in Internet for the simulation example

BIOGRAPHY

Şerif Bahtiyar was born in Omurtag (Bulgaria) in 1977. He received the B.Sc. degree in control and computer engineering from Istanbul Technical University in 2001. He has been working as a researcher in National Research Institute of Electronics and Cryptology (TÜBİTAK UEKAE) since 2001.

His research interests include computer networks, next generation Internet, security, mobility, distributed operating systems, parallel programming and intelligent systems.