NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PERFORMANCE ANALYSIS OF THE MOBILE IP PROTOCOL (RFC 3344 AND RELATED RFCS)

by

Chin Chin Ng

December 2006

Thesis Co-Advisors: George W. Dinolt
J. D. Fulp

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Performance Analysis of the Mobile IP Protocol (RFC 3344 and Related RFCs)			**5. FUNDING NUMBERS**
6. AUTHOR(S) Chin Chin Ng			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Mobile IP defines the mechanisms and protocol behaviors necessary to facilitate the seamless flow of traffic to a mobile host that roams from its normal home network. Of particular interest in this research, is how this capability might support the relatively rapid roaming of a wirelessly connected host. This research is focused on isolating and analyzing the constituent components of the Mobile IP protocol for the purpose of identifying any component(s) that may be improved upon, or may be exploited by an attacker intent on denying or delaying proper handoff service.

14. SUBJECT TERMS Mobility, Mobile IP, Mobile Node, Home Agent, Foreign Agent, Care-of Address, Home Address, Home Network, Foreign Network, Handoff			**15. NUMBER OF PAGES** 148
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

PERFORMANCE ANALYSIS OF THE MOBILE IP PROTOCOL (RFC 3344 AND RELATED RFCS)

Chin Chin Ng
Civilian, Singapore Defence Science & Technology Agency
B.S., National University of Singapore, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
December 2006

Author: Chin Chin Ng

Approved by: George W. Dinolt
Thesis Co-Advisor

J. D. Fulp
Thesis Co-Advisor

Peter J. Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Mobile IP defines the mechanisms and protocol behaviors necessary to facilitate the seamless flow of traffic to a mobile host that roams from its normal home network. Of particular interest in this research, is how this capability might support the relatively rapid roaming of a wirelessly connected host. This research is focused on isolating and analyzing the constituent components of the Mobile IP protocol for the purpose of identifying any component(s) that may be improved upon, or may be exploited by an attacker intent on denying or delaying proper handoff service.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABRREVIATIONS

ACK	Acknowledgment
ARP	Address Resolution Protocol
BSS	Basic Service Set
BSSID	BSS Identifier
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CTS	Clear to Send
DHCP	Dynamic Host Configuration Protocol
DoS	Denial-of-Service
ESS	Extended Service Set
FHAE	Foreign-Home Authentication Extension
GRE	Generic Routing Encapsulation
HMAC	Keyed-Hash Message Authentication Code
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IOS	Internetwork Operating System
IP	Internet Protocol
ITU	International Telecommunication Union
LAN	Local Area Network
LLC	Logical Link Control
MAC	Media Access Control
MAC	Message Authentication Code
MAN	Metropolitan Area Network
MD5	Message-Digest algorithm 5
MFAE	Mobile-Foreign Authentication Extension
MHAE	Mobile-Home Authentication Extension
MSDU	MAC Service Data Unit
NTP	Network Time Protocol
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
PS	Power-Save
QoS	Quality of Service
RF	Radio Frequency
RFC	Request For Comments
RTS	Request to Send
SPI	Security Parameter Index
TCP	Transmission Control Protocol
TTL	Time-to-Live
UDP	User Datagram Protocol

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Being able to see through this thesis research marks a major achievement for me, and I would like to take the opportunity to express my sincere gratitude to many who have participated to make this feat possible.

I would to thank my thesis advisors, J. D. Fulp and Dr. George W. Dinolt, for their patience and guidance; during the initial “discovery” of an appropriate thesis topic, to the process of “registration” with a thesis proposal, and finally “routing” to reach the destination of completing this thesis. I am indeed grateful to J. D., for the time and effort spent in the numerous brainstorming sessions. J. D. has served well as an advisor, mentor, and friend. I am equally grateful to Dr. Dinolt, for his understanding and encouragement, especially during the times when things do not “auto-magically” happen, and failure is considered an acceptable result.

I would also like to thank all the lecturers and professors who have taught me in the Information Assurance track specialization, imparting their invaluable knowledge to make me well-equipped and competent to handle my future IA posting.

It was not an easy task to get back to the routine of study and exams, especially in a foreign environment where I have never previously been to. I am grateful to my fellow Singapore comrades, for their camaraderie and support in helping me adapt “seamlessly”. Special thanks go to Yu Loon, Harry and Han Chong, for their constant support and interesting insights, ever since the team’s involvement in Mobile IP.

I would like to thank my sponsor – the Singapore Defence Science & Technology Agency; and my superiors, Eugene Chang and Tan Ah Tuan; for their faith in me, giving me this opportunity to pursue my postgraduate study.

I am grateful to Kay Lee from Cisco Systems Singapore, for his friendship and support to enable me to achieve this “near impossible” feat.

Most importantly, I would like to share the success of this completion with my mother; my constant role model, and has always been lending a listening ear to my sorrow and joy.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND AND MOTIVATION

1. Growth of Mobile Computing

The explosive growth of the Internet has triggered an increased reliance on network computing. Most organizations today have sophisticated networks that are connected to the Internet. The major benefit reaped from such a networked environment is the ability for an employee to virtually work from anywhere at any time. This in turn had led to a steady rise in the number of telecommuters and the mobile workforce. Coupled with the increase in the number of mobile users is the evolution of mobile device technology such as notebook computers, personal digital assistants and cell phones to facilitate mobility. The combination of these three forces – increased reliance on network computing, a growing mobile workforce, and the evolution in mobile device technology – drives the need for mobile computers to communicate seamlessly with other computers, be they fixed or mobile.

2. Problems Introduced by Mobility

Internet routing plays an important role for the delivery of an Internet Protocol (IP) packet from a source to its destination. The Internet Protocol standard specified in Request For Comments (RFC) 791 [1] describes routing of IP packets to be based upon destination address. By consulting its routing table, each network node is able to make forwarding decisions based only upon the destination address field within the IP packet header. For maintainability and scalability reasons, routing decisions are typically made based upon the network-prefix of the IP destination address, rather than the entire host-specific IP address. Every host on the same IP network would have an identical network-prefix. When a node moves, it will have to change its network-prefix (i.e. IP address) to reflect its new network of residence to the routing infrastructure in order to ensure continued packet delivery service with other networked nodes.

The Transmission Control Protocol (TCP), specified in RFC 793 [2] and User Datagram Protocol (UDP), specified in RFC 768 [3] are two widely used transport layer protocols employed in the operation of the Internet. TCP is a connection-oriented protocol providing reliable data communications to higher application layers. TCP uses

port identifiers to identify the separate data/application streams that it may handle. A TCP socket is uniquely identified by the concatenation of its IP address with the TCP port identifier, and a TCP connection is uniquely identified by the pair of sockets at both ends. A TCP connection will drop if any one of the four parameters, namely, source IP address, source port, destination IP address and destination port, were to change. Thus, any ongoing communications initiated by a mobile mode would be terminated and have to be re-established were it to change its IP address.

It is apparent from the foregoing that the desired functionality of mobility presents two conflicting requirements. The mobile node's IP address needs to change according to the node's point-of-attachment to facilitate continued packet delivery; yet existing connections require a mobile mode to retain its original IP address for session continuity.

3. Mobility Explained

The term mobility is often used synonymously with nomadicity. For the purpose of clarifying the benefits brought about by Mobile IP as specified in RFC 3344 [4], it is important to distinguish between the two. According to [5], nomadicity refers to the ability of users moving from one location to another and initiating communications. Such movement, however, would require a user to terminate and restart sessions and applications as a result of the move. Users are thus responsible for establishing a new connection wherever they go. Mobility, on the other hand, does not require the user to terminate and re-initiate a connection in order to move from one location to another. All connections are automatically maintained despite the change in location. The relocation from one network to another takes place without any user intervention. In this thesis, the term "roam" will be used synonymously with the notion of mobility presented above.

4. Issues with Mobile IP

Despite the benefits brought about by Mobile IP, there are some technical challenges introduced by Mobile IP that need to be overcome before it is deemed worthy of widespread adoption. Two of the dominant technical challenges are identified and briefly described next, which serve to set the stage for the purpose of this research.

a. TCP Performance

As described in [6], the TCP congestion control mechanism interprets the cause of the majority of lost segments and acknowledgments to be the result of

congestion. This assumption is valid for most of the operational Internet, but does not necessarily hold true for the mobile environment, where lost segments and acknowledgments can be expected to occur due to the required handoff protocol traffic and processing taking place when a mobile node roams. Moreover, transmission over the error-prone radio-frequency medium in a wireless mobile environment is the likely cause for majority of the lost packets and acknowledgments. The combination of these two factors – mobility and the wireless environment over which mobile nodes communicate – can severely degrade the performance of TCP.

b. Security

The mode of operations in a mobile computing environment differs from that of an ordinary computing environment. In most scenarios, mobile nodes are connected via wireless means, which are particularly susceptible to active and passive attacks. Moreover, the ability for a mobile node to roam to virtually anywhere on the Internet introduces unprecedented risks, in which IP packets meant for the mobile node could potentially be subjected to Denial-of-Service (DoS) and traffic redirection attacks if the Mobile IP registration process was not authenticated.

B. RESEARCH METHODOLOGY AND ORGANIZATION

1. Primary Research Question

- Will the Mobile IP protocol described in RFC 3344 (and related RFCs) provide sufficiently quick and sufficiently reliable handoffs to support the relatively rapid roaming of connected wireless (IEEE 802.11) hosts?

2. Subsidiary Research Questions

- What is the goal of Mobile IP?
- What constitutes a Mobile IP handoff?
- What are the constituent functional components underlying the Mobile IP protocol that facilitates the roaming of the mobile host?
- What is the basic protocol functionality used by IEEE 802.11 to associate and disassociate wireless hosts?

- How would a test lab network be architected and instrumented so as to best measure time/performance statistics for each of the constituent functional components?
- What are the test cases that should be employed to generate the data that will be used for performance analysis?
- Which of the protocol's constituent parts are good candidates for test data collection?
- Does the collected data provide any insights regarding how the mobile handoff of wireless (IEEE 802.11) clients may be done more quickly? If so, what are they and how should they be adjusted for quicker, more seamless, handoffs?
- Does the collected data provide any insights regarding how the mobile handoff of wireless (IEEE 802.11) clients might be vulnerable to DoS or traffic redirection type attacks?

3. Assumptions

The operation of the Mobile IP protocol is built upon the basics of computer networking and IP routing. This thesis report assumes that the reader has the necessary background to understand the contents presented herein. It is not the intent of this thesis report to describe computer networking and IP routing at length. Readers can refer to [7] and [8] for a more thorough treatment of the topic.

4. Scope

Mobile IP defines the mechanisms and protocol behaviors necessary to facilitate the seamless flow of traffic to a mobile host that roams from its normal home network. Of particular interest in this research, is how this capability might support the relatively rapid roaming of a wirelessly connected host. This research is focused on isolating and analyzing the constituent components of the Mobile IP protocol for the purpose of identifying any component(s) that may be improved upon, or may be exploited by an attacker intent on denying or delaying proper handoff service.

The scope of this research involves setting up a controlled environment to demonstrate the operations of Mobile IP version 4 to support the roaming of a wirelessly connected host. The setup shall be configured based on existing Cisco hardware and software available within the campus. Performance statistics for the constituent functional components that facilitate the roaming of the mobile host shall be collected

and analyzed for the performance and security ramifications associated with the mobile handoff of wireless (IEEE 802.11) clients.

5. Chapter and Appendix Overview

This thesis is comprised of the following chapters and appendices:

Chapter I: Introduction – This chapter introduces the driving factor for mobility and recognizes the need for Mobile IP to support mobility. Issues concerned with Mobile IP are briefly described to set the stage for the focus of this research.

Chapter II: Operations of Mobile IP Version 4 – This chapter discusses the salient points of RFC 3344 [4] and presents the essential functional components in order to facilitate the performance measurements and analysis identified in this research.

Chapter III: IEEE 802.11 Protocol Primer – This chapter outlines the basic operation for the IEEE 802.11 wireless environment in an infrastructure mode, used in the instrumented lab setup in this research.

Chapter IV: Setting Up the Mobile IP Test Environment – This chapter describes the topological design and architecture, considerations, test plan, data collection and collation strategy for collecting and analyzing the performance statistics.

Chapter V: Results and Findings – This chapter presents the performance statistics for the Mobile IP handoff components, analyzes the results and identifies potential candidates for performance fine-tuning. The chapter discusses the types of applications that can be supported by Mobile IP, and concludes with a brief discussion on the security ramifications associated with Mobile IP.

Chapter VI: Conclusions – This chapter summarizes the conclusion, discusses the major challenges and recommends potential areas for future research.

Appendix A: Configuration Setup – This section documents the configuration details of the respective components for the Mobile IP test environment identified in Chapter IV.

Appendix B: Test Results – This section includes the detailed test results that were collected and collated by conducting the respective test cases identified in Chapter IV.

THIS PAGE INTENTIONALLY LEFT BLANK

II. OPERATIONS OF MOBILE IP VERSION 4

A. INTRODUCTION

The Mobile IP protocol was originally defined as a standard in RFC 2002 [9] by the Internet Engineering Task Force (IETF) in October 1996. Since then, a number of additional RFCs have proposed enhanced functionality and clarified the original standards. The core Mobile IP protocol has been updated and is currently defined in RFC 3344 [4]. RFC 3344 serves as the main source of reference for the concepts described in this chapter, with additional references taken from [5], [6] and [10] to provide appropriate clarifications and illustrations.

This chapter will describe the constituent functional components underlying the Mobile IP protocol, namely, Agent Discovery, Registration and Routing. Having understood the functional components, it will be appropriate to explain what constitutes a Mobile IP handoff. The chapter then concludes by presenting the security considerations, as well as how the Mobile IP protocol addresses some of these issues.

1. Goals and Assumptions

The Mobile IP protocol was designed to meet the following goals:

- A mobile node must be able to communicate with other nodes after changing its physical point-of-attachment to the Internet without changing its IP address.
- A mobile node must be able to communicate with other nodes that do not implement the Mobile IP functionality.
- Introduction of the Mobile IP protocol must not expose the mobile node to any new security threats over and above those current threats faced by fixed nodes that are connected to the Internet.
- Due to the resource constraints imposed on a mobile node, administrative messages sent over the physical link by which a mobile node is directly attached to the Internet should be kept minimal in size and number.

The developers of the Mobile IP protocol also made two fundamental assumptions, namely

- Mobile nodes will generally not change their physical point-of-attachment more frequently than once per second;

- Routing of IP unicast packets is based only upon the destination address field within the IP packet header.

2. New Architectural Entities and Terminology

Mobile IP defines three new architectural entities that are used to implement its mobility functionality. The relationships among these architectural entities are illustrated in Figure 1.

a. Mobile Node

A mobile node can either be a host or a router that changes its physical point-of-attachment to the Internet without changing its IP address, yet maintaining any ongoing communications with other nodes on the Internet using its constant IP address.

b. Home Agent

A router on a mobile node's home network that maintains up-to-date location information about the mobile node and tunnels IP packets for delivery to the mobile node when it is away from its home network.

c. Foreign Agent

A router on a mobile node's visited network that provides Mobile IP services to the mobile node while it is registered. The foreign agent is capable of offering one or more of its IP addresses as a care-of address; in which case the foreign agent will serve to de-tunnel and deliver IP packets to the mobile node that were tunneled by the mobile node's home agent. The foreign agent may assist the mobile node in informing its home agent of its current care-of address; and may serve as a default router for routing traffic from the registered mobile node.

Besides identifying the functional entities, the following terminology is commonly used to describe the concepts underlying the operations of Mobile IP.

d. Authentication Extension

An authentication extension is appended to the end of a registration message that contains relevant security information to authenticate and protect the integrity of the registration process. The concept of the authentication extension will be described in detail under the *Security Considerations* of this chapter.

e. Authorization-enabling Extension

An authorization-enabling extension refers to the use of an authentication extension that facilitates the acceptance of a registration request or reply message by the recipient of the message.

f. Care-of Address

A care-of address signifies the termination point of a tunnel established by a mobile node's home agent, for IP packets to be forwarded to the mobile node when it is away from its home network. The Mobile IP protocol uses two different types of care-of address: a foreign agent care-of address is an IP address of a foreign agent with which the mobile node is registered; a co-located care-of address is an externally obtained local IP address from the mobile node's current point-of-attachment.

g. Correspondent Node

A correspondent node is a peer node with which a mobile node is currently communicating. A correspondent node can either be a fixed or mobile node.

h. Foreign Network

A foreign network is any network other than the mobile node's home network.

i. Home Address

A home address is an IP address that is assigned to the mobile node either statically by a network administrator, or dynamically via the Dynamic Host Configuration Protocol (DHCP) [11] for some configurable leased period. This address remains constant when the mobile node changes its point-of-attachment to the Internet.

j. Home Network

A home network has a network-prefix that matches the mobile node's home address. IP packets destined for the mobile node will be routed to the mobile node's home network for delivery to the mobile node.

k. Mobility Agent

A mobility agent refers to either a home agent or a foreign agent.

l. Mobility Binding

A mobility binding refers to the association of a mobile node's home address with a care-of address, along with the remaining lifetime of that association. Mobility bindings are maintained at the mobile node's home agent.

m. Mobility Security Association

A mobility security association refers to a collection of security contexts that exist between a pair of nodes, which may be applied to Mobile IP protocol messages that are exchanged between them. The concept of the mobility security association will be described in detail under the *Security Considerations* of this chapter.

n. Tunnel

A tunnel is the path followed by an IP packet while it is encapsulated. A tunnel is established between the mobile node's home agent and the mobile node's care-of address. IP packets destined for the mobile node will be encapsulated by the home agent upon entering this tunnel, and decapsulated by the tunnel end-point for correct delivery to the mobile node. The concept of tunneling will be described in detail under the *Routing* section of this chapter.

o. Visited Network

A visited network is a foreign network to which the mobile node is currently attached.

p. Visitor List

A visitor list refers to the list of mobile nodes visiting a foreign network, and is maintained by the foreign agent serving that foreign network.

Figure 1 illustrates the relationships among the architectural entities and the corresponding Mobile IP terminology.

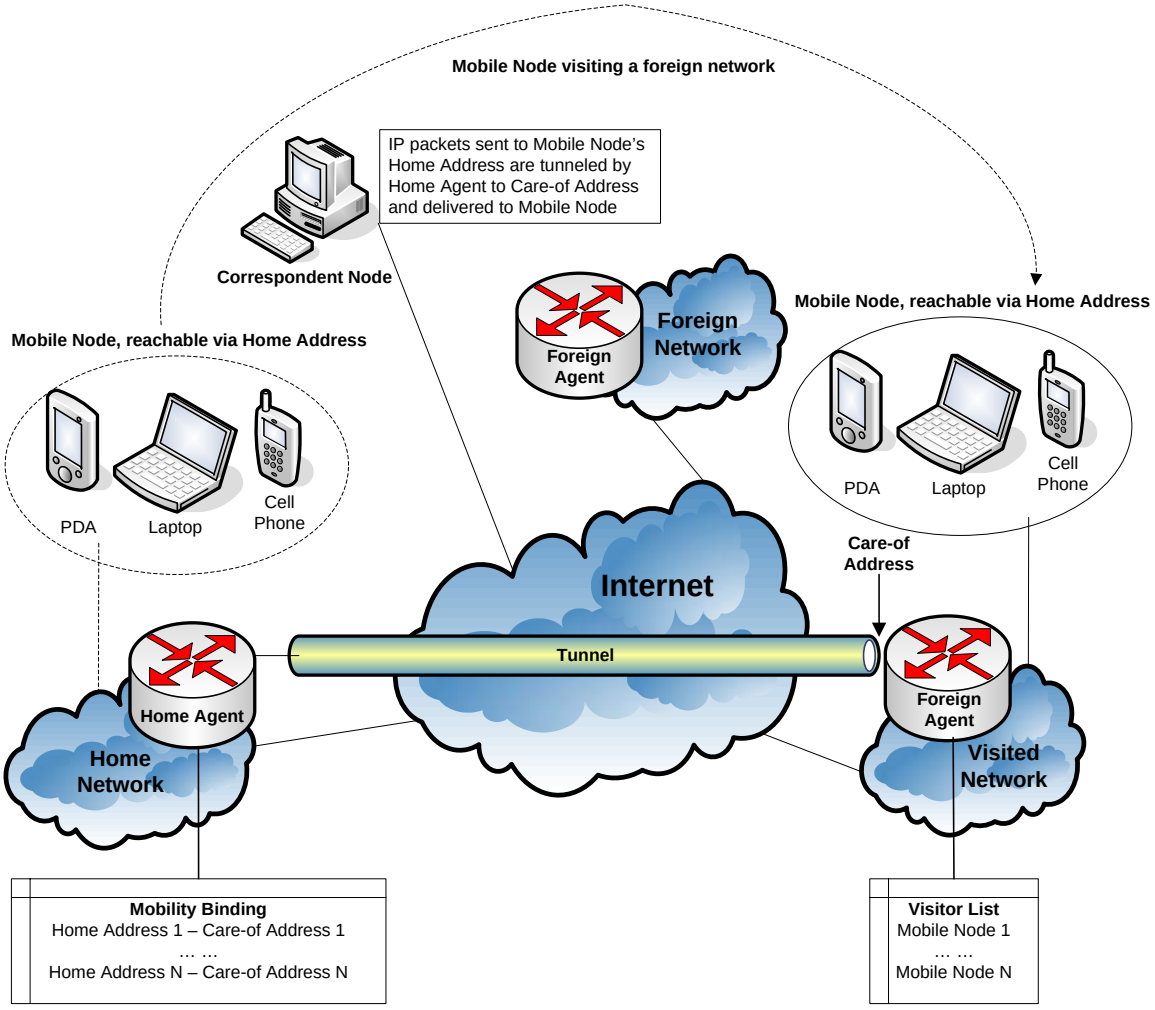


Figure 1. Mobile IP Entities and Relationships (After: [5] & [6]).

3. Protocol Overview

An overview of the operation of the Mobile IP protocol is described in Figure 2. Details of each component will be explored in greater detail in the subsequent sections.

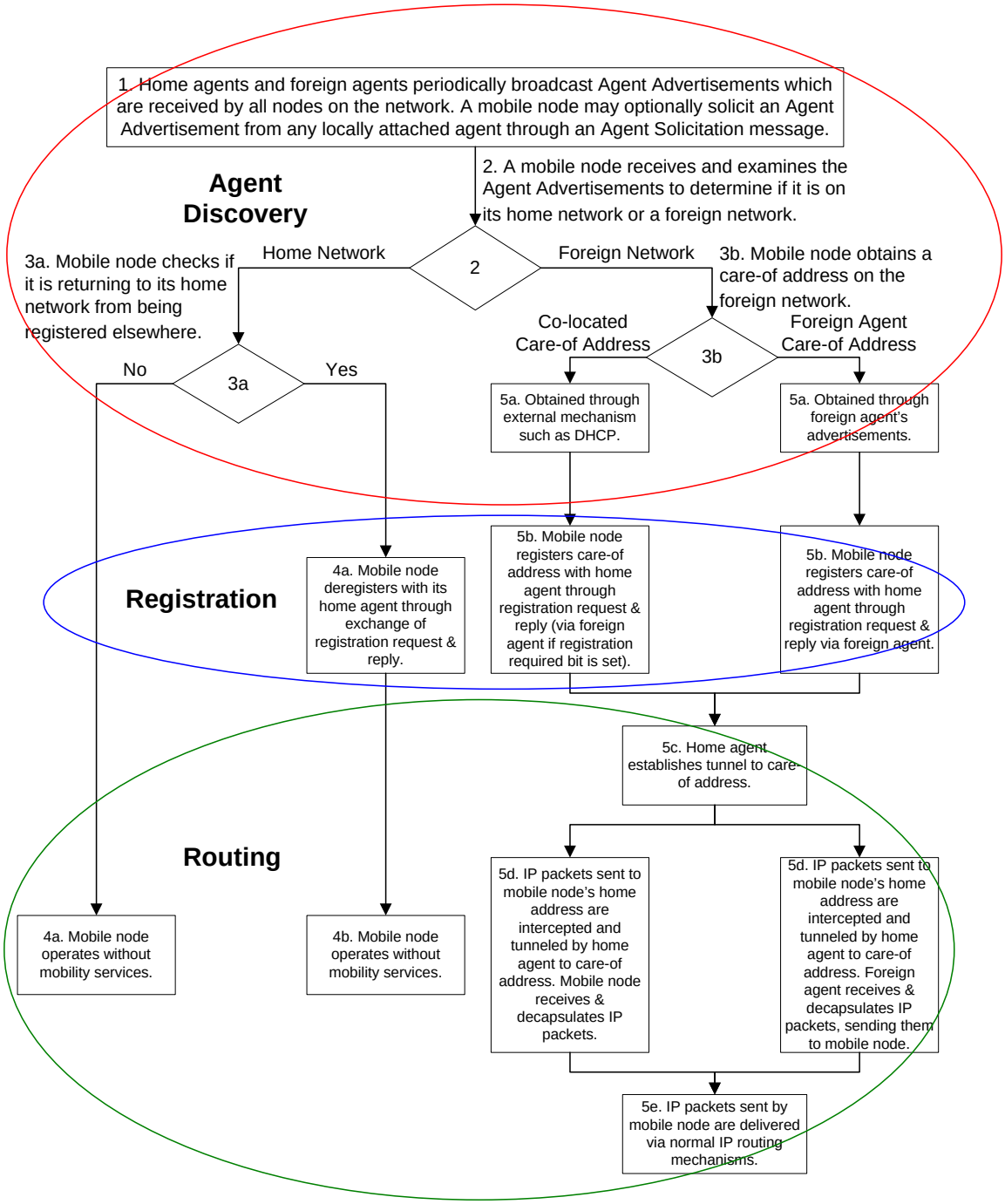


Figure 2. Overview of Mobile IP Operation.

B. AGENT DISCOVERY

Agent discovery is the process by which a mobile node determines whether it is currently connected to its home network or to a foreign network, thereby allowing the mobile node to detect if it has moved from one network to another. In the case where the mobile node has moved to a foreign network, the process of agent discovery will also facilitate its obtainment of a care-of address.

1. Agent Advertisement

Agent advertisements are periodically transmitted by home agents and foreign agents to advertise their offered Mobile IP services on a network. Mobile nodes make use of these advertisements to determine their current or possibly new point-of-attachment to the Internet. An agent advertisement message is in fact an Internet Control Message Protocol (ICMP) [12] router advertisement [13] that has been extended to carry a mobility agent advertisement extension and other optional extensions. Figure 3 shows such an agent advertisement message, with Table 1 describing its corresponding fields.

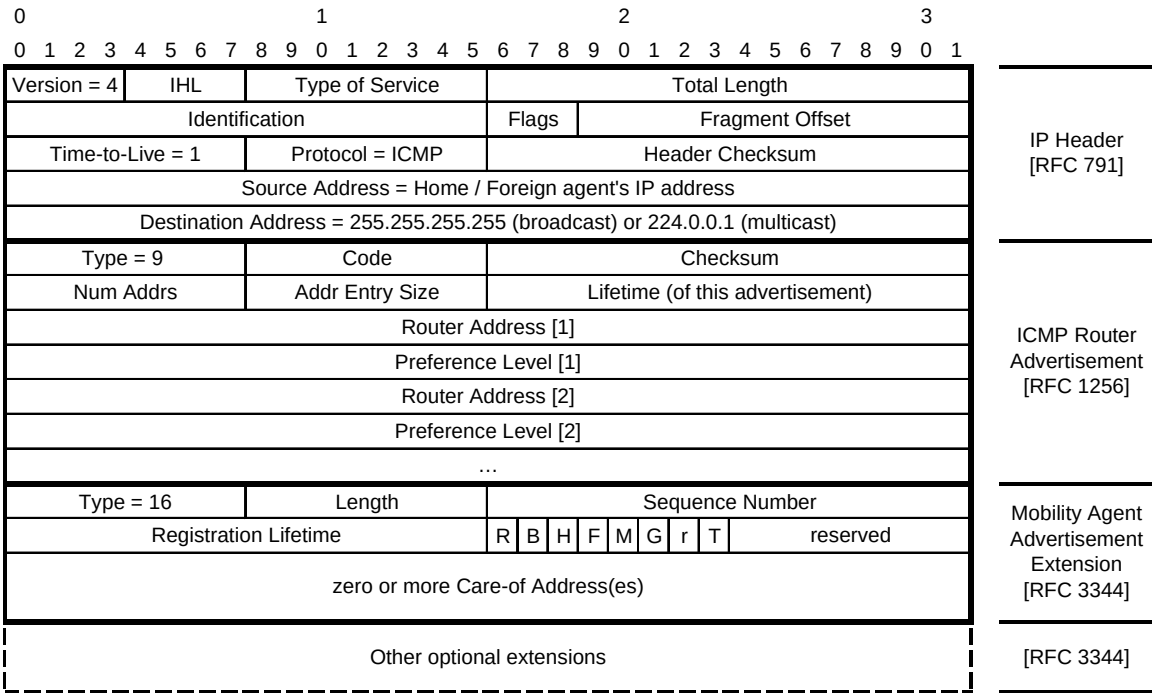


Figure 3. Agent Advertisement Message (After: [4] & [6]).

Field	Description
IP Header	
Time-to-Live	The TTL for all agent advertisements must be set to 1.
ICMP Header	
Type	A type field of 9 identifies the ICMP message as an adverstisement.
Code	Mobile IP home agents and foreign agents use the value of 16 to prevent any nodes other than mobile nodes to use them as routers. A value of 0 allows nodes on the network to use them as routers.
Lifetime	Indicates how frequently this agent sends advertisement. The lifetime field is used primarily for move detection.
Num Addrs	Reflects the number of router address / preference level pairs that are listed in this advertisement, and the corresponding number of bytes each pair occupies.
Addr Entry Size	
Mobility Agent Advertisement Extension	
Type	A type field of 16 identifies the extension as a mobility agent advertisement extension.
Length	Gives the number of bytes in the data portion of the extension, which is equivalent to 6 + 4 * number of care-of addresses advertised, where 6 accounts for number of bytes in the Sequence Number, Registration Lifetime, flags and reserved fields.
Sequence Number	The count of agent advertisement messages sent since the agent was last initiated. An agent must use the number 0 for its first advertisement after booting. Each subsequent advertisement must use the sequence number that is one greater than the previous, with the exception that the sequence number 0xffff must be followed by sequence number 256 to indicate a rollover in sequence number.
Registration Lifetime	The longest lifetime (measured in seconds) that this agent is willing to accept in any registration request. This field has no relation to the Lifetime field within the ICMP router advertisement portion of the agent advertisement.
R	Registration required. Registration with this foreign agent is required even when a co-located care-of address is used. An agent advertisement must not have the 'R' bit set if the 'F' bit is not set.
B	Busy. The foreign agent will not accept registrations from additional mobile nodes. An agent advertisement must not have the 'B' bit set if the 'F' bit is not set.
H	Home agent. This agent offers service as a home agent on the network where this agent advertisement is sent.
F	Foreign agent. This agent offers service as a foreign agent on the network where this agent advertisement is sent.
M	Minimal encapsulation. This agent supports receiving tunneled IP packets that use minimal encapsulation [14].
G	GRE encapsulation. This agent supports receiving tunneled IP packets that use GRE encapsulation [15].
r	Set as zero; ignored on reception.
T	Foreign agent supports reverse tunneling [16].
reserved	Set as zero; ignored on reception.
Care-of Address (es)	The advertised foreign agent care-of address(es) provided by this foreign agent. An agent advertisement must include at least one care-of address if the 'F' bit is set.
Other Optional Extensions	
-	Other optional extensions include the prefix-length extension and one-byte padding extension.

Table 1. Agent Advertisement Message Fields.

2. Agent Solicitation

Agent solicitations are sent by mobile nodes to force any agents on the network to immediately respond with an agent advertisement, without having to wait for the next periodic transmission of agent advertisements. An agent solicitation message is identical to the ICMP router solicitation message [13] with the restriction that the IP Time-To-Live (TTL) field must be set to one. A type field of value 10 identifies the ICMP message as a solicitation message. An agent solicitation message is shown in Figure 4.

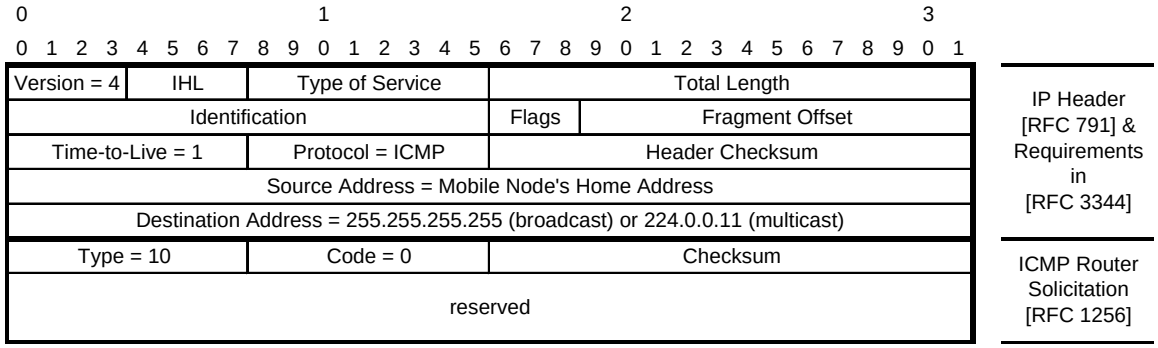


Figure 4. Agent Solicitation Message (After: [4] & [6]).

3. Move Detection

Mobile nodes are responsible for engaging in the continuous process of move detection, which is the act of monitoring changes in available paths into the network at large. Two primary mechanisms are provided for mobile nodes to detect when they have moved from one network to another.

a. Move Detection Using Lifetime

A mobile node uses the lifetime field in the ICMP header of an agent advertisement message to determine if it has moved. Figure 5 illustrates such a move detection process using the lifetime field.

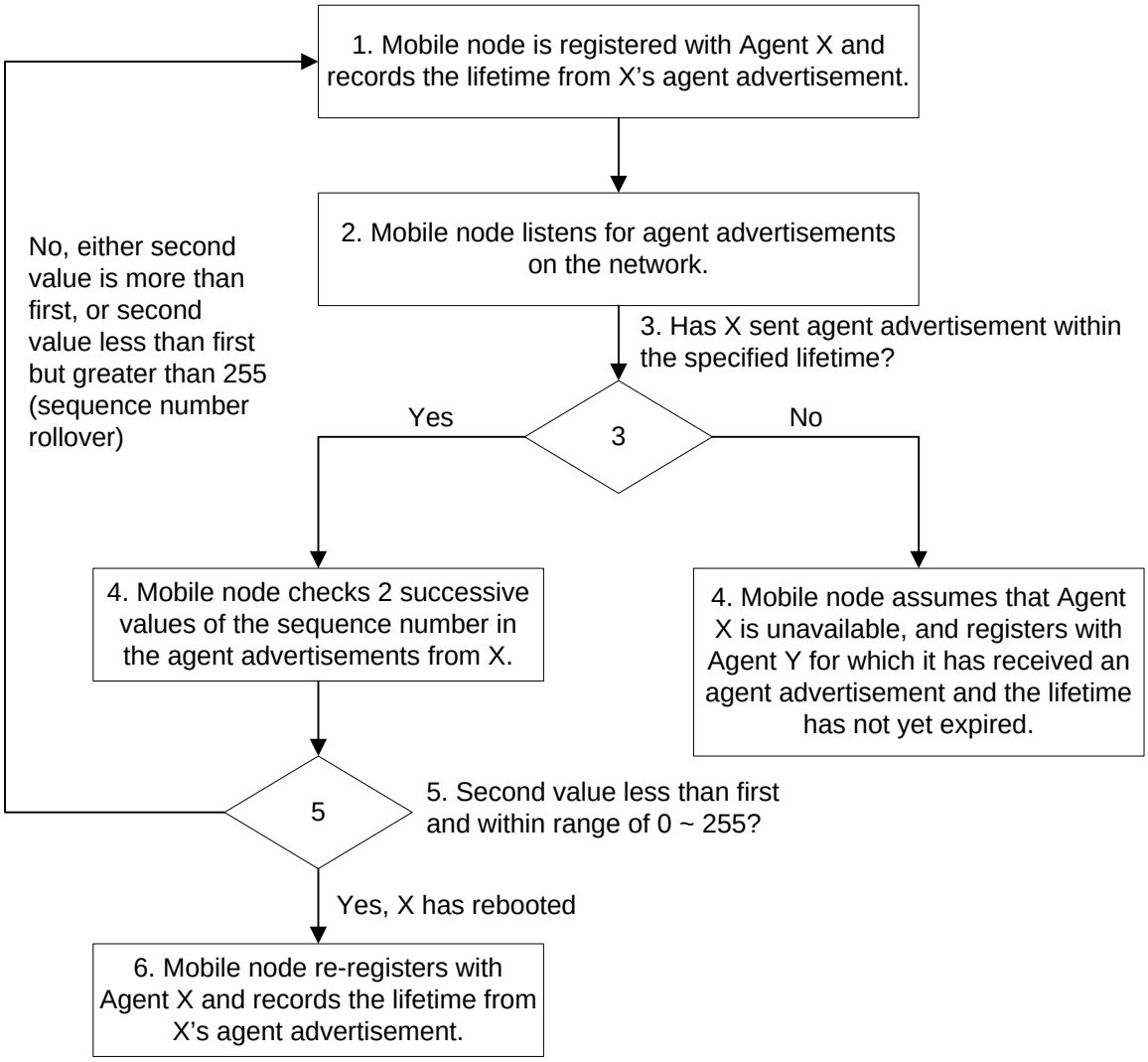


Figure 5. Move Detection using Lifetime.

b. Move Detection Using Network Prefix

A mobile node uses the network address based on the network prefixes specified in the prefix-length extension of an agent advertisement message to determine if a newly received agent advertisement was received from the same network as the mobile node's current care-of address. If the network addresses differ, the mobile node concludes that it has moved and will proceed to register with the new foreign agent that sent this agent advertisement. If the network addresses are the same, the mobile node concludes that it has not moved. The mobile node will not need to register with this new foreign agent unless it has not received an advertisement within the specified lifetime from its currently registered foreign agent. Thus, this method of move detection still relies on the

first method of move detection using lifetime to check for the availability of the mobile node's current foreign agent. Moreover, move detection using a network prefix can only be used if all agent advertisements include the prefix-length extensions and the mobile node knows the network prefix of its current care-of address (for the case of co-located care-of address). Figure 6 illustrates the move detection mechanism using network prefix.

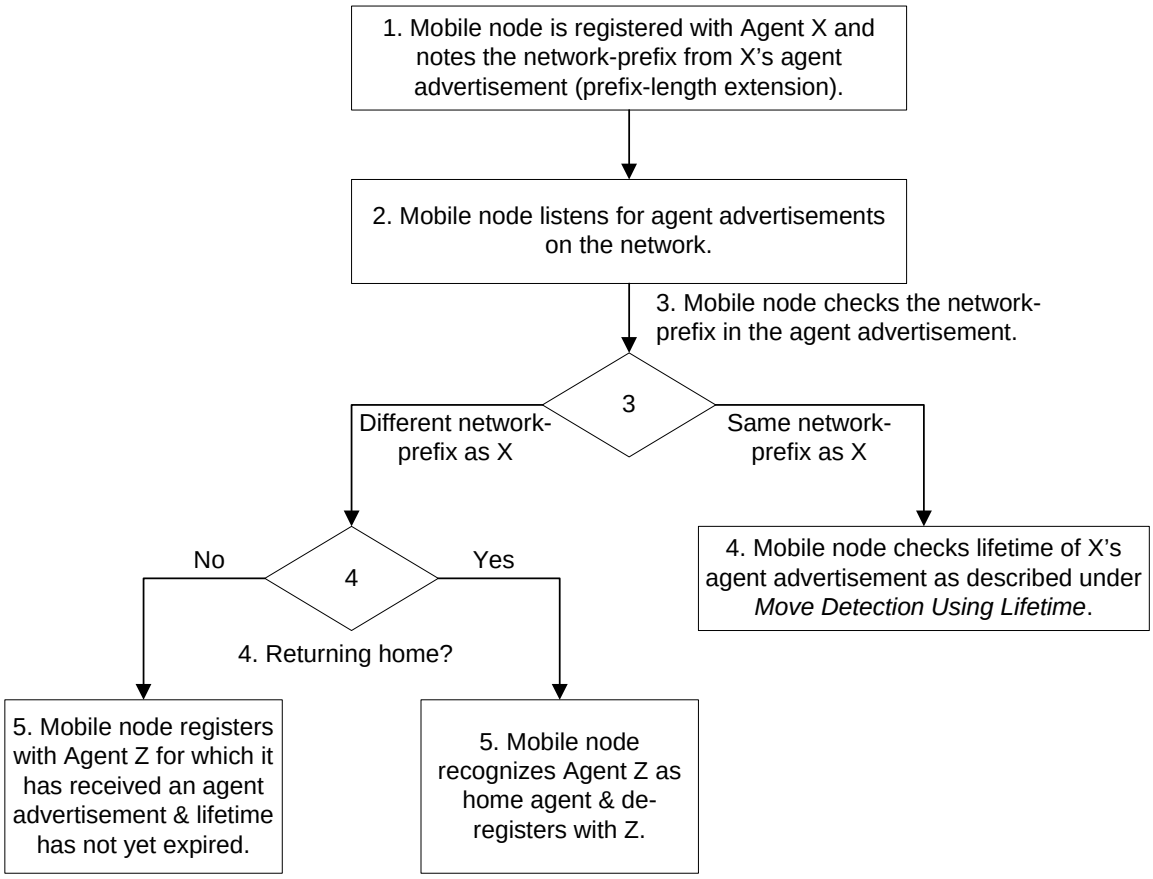


Figure 6. Move Detection using Network Prefix.

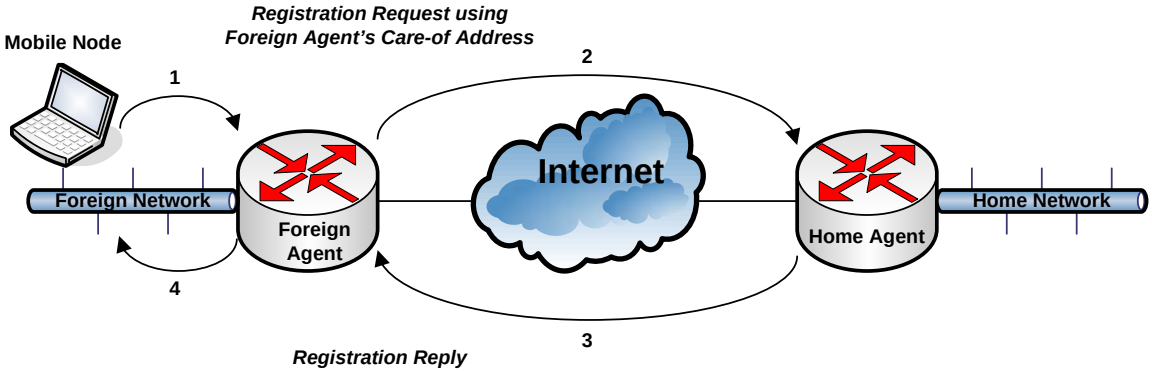
C. REGISTRATION

Mobile IP registration is the process that mobile nodes use to communicate their current reachability information to their home agents, so that IP traffic destined for the mobile nodes can be delivered to them when they are away from their home network. A mobile node uses the registration process to:

- Request forwarding services when visiting a foreign network;
- Inform its home agent of its current care-of address(es);
- Renew a registration which is due to expire;
- De-register when it returns home.

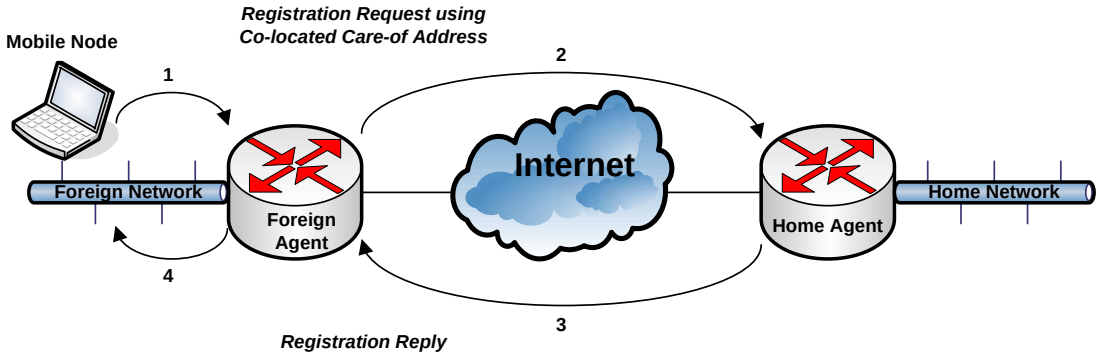
1. Registration Overview

The Mobile IP registration process comprises mainly the exchange of two messages, a registration request and a registration reply, using UDP [3]. A registration involves an exchange of a registration request and a registration reply between a mobile node and its home agent. Depending on the registration options and the type of care-of address used by the mobile node, a foreign agent may be involved in the registration process. Figures 7 – 10 depict the four scenarios under which registration could take place.



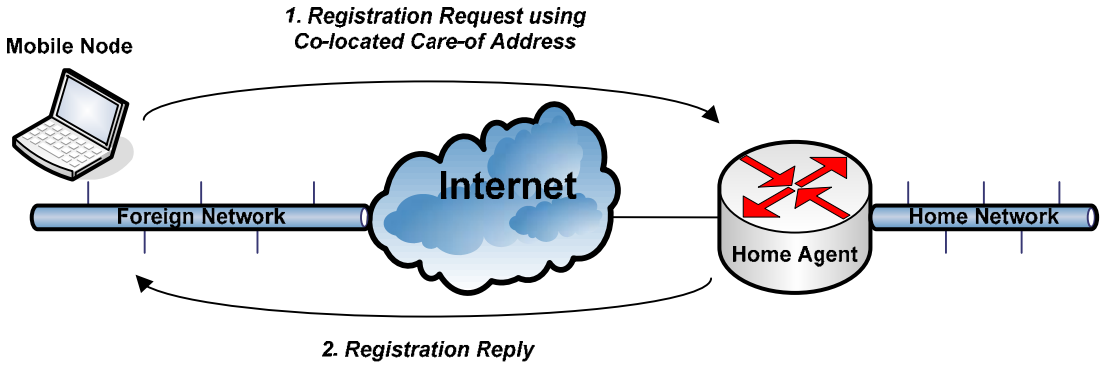
1. Mobile node sends a registration request using foreign agent's care-of address (obtained from agent advertisement) to foreign agent.
2. Foreign agent processes the registration request and relays it to home agent (if foreign agent supports requested services).
3. Home agent sends a registration reply to foreign agent to grant or deny the request.
4. Foreign agent processes the registration reply and relays it to the mobile node.

Figure 7. Registration using Foreign Agent's Care-of Address (After: [4] & [6]).



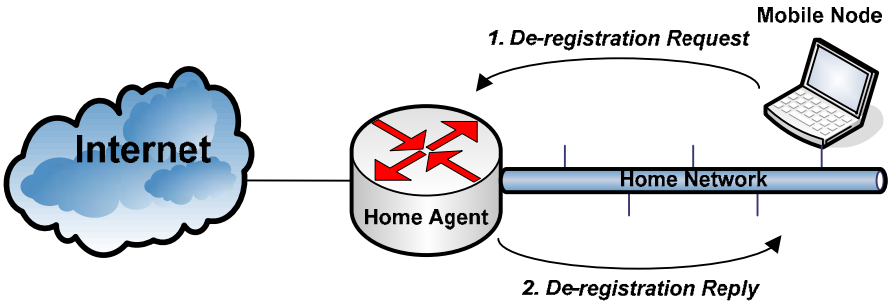
1. Mobile node sends a registration request using co-located care-of address to foreign agent (agent advertisement received on the foreign network where mobile node resides has “Registration Required” bit set).
2. Foreign agent processes the registration request and relays it to home agent (if foreign agent supports requested services).
3. Home agent sends a registration reply to foreign agent to grant or deny the request.
4. Foreign agent processes the registration reply and relays it to the mobile node.

Figure 8. Registration via Foreign Agent using Co-located Care-of Address (After: [4] & [6]).



1. Mobile node sends a registration request using co-located care-of address to the home agent.
2. Home agent sends a registration reply to the mobile node, granting or denying the request.

Figure 9. Direct Registration using Co-located Care-of Address (After: [4] & [6]).



1. Mobile node detects that it has returned to its home network and sends a registration request to de-register with its home agent.
2. Home agent sends a registration reply to the mobile node, granting or denying the request.

Figure 10. De-registration upon Returning Home (After: [4] & [6]).

2. Registration Request

A mobile node initiates the registration process by sending a registration request message. A mobile node registers with its home agent so that its home agent can create a mobility binding (when the mobile node relocates to another network) or modify an existing mobility binding (when the mobile node renews a registration which is about to expire) for that mobile node. Figure 11 shows a registration request message, with Table 2 describing its corresponding fields.

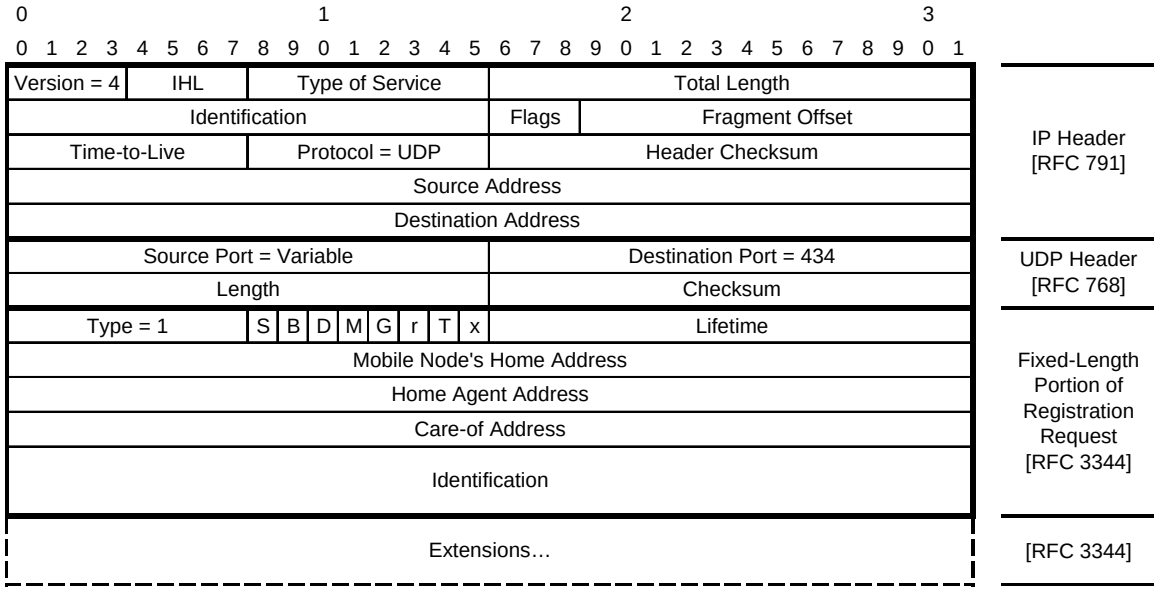


Figure 11. Registration Request Message (After: [4] & [6]).

Field	Description
IP Header	
Source Address	*Mobile Node* : If a co-lcated care-of address is used, IP source address must be the care-of address. If it does not have a home address, IP source address is set to 0.0.0.0. Otherwise, IP source address must be its home address. *Foreign Agent* : Interface address from which the request is forwarded to home agent.
Destination Address	*Mobile Node:* 1. If it has discovered the agent with which it is registering through other means where the IP address is unknown, the "All Mobility Agents" multicast address of 224.0.0.11 must be used. Subsequent request is then sent to the agent's unicast address. 2. If it is registering with a foreign agent, address of the foreign agent (obtained from agent advertisement) must be used. 3. If it is registering directly with its home agent and knows the home agent's unicast IP address, this will be used as destination address. Otherwise, it uses dynamic home agent address resolution to determine the IP address of its home agent by setting the address field to the home network's subnet-directed broadcast. *Foreign Agent* : Copied from home agent field within the received registration request.
Time-to-Live	IP TTL field must be set to 1 if the IP destination address is set to the "All Mobility Agents" multicast address.
UDP Header	
Source Port	Variable.
Destination Port	A value of 434 is reserved for Mobile IP registration messages.
Fixed-Length Portion of Registration Request	
Type	A type field of 1 identifies message as a registration request.
S	Simultaneous bindings. Mobile node is requesting that the home agent retains its prior mobility bindings, otherwise home agent deletes any previous bindings and replaces with new binding specified in registration request.
B	Broadcast datagrams. If the 'B' bit is set, mobile node is requesting that the home agent tunnels to it any broadcast IP packets it receives on the home network.
D	Decapsulation by mobile node. If the 'D' bit is set, the mobile node will perform its own decapsulation of IP packets that are sent to the care-of address, i.e., mobile node is using a co-located care-of address.
M	Minimal encapsulation. If the 'M' bit is set, the mobile node requests that its home agent use minimal encapsulation [14] for IP packets tunneled to the mobile node.
G	GRE encapsulation. If the 'G' bit is set, the mobile node requests that its home agent use GRE encapsulation [15] for IP packets tunneled to the mobile node.
r	Set as zero; ignored on reception.
T	Mobile node is requesting for reverse tunneling [16] service.
x	Set as zero; ignored on reception.
Lifetime	The number of seconds remaining before the registration is considered to be expired. A value of 0 indicates a request for deregistration.
Home Address	IP address of the mobile node if it is known, otherwise set to 0.0.0.0.
Home Agent	IP address of the mobile node's home agent if it is known, otherwise set to home network's subnet-directed broadcast.
Care-of Address	IP address for the end of the tunnel established by the home agent, set to value of particular care-of address that mobile node wishes to (de)register. This value is set to mobile node's home address if it wishes to de-register all care-of addresses.
Identification	A 64-bit number that is constructed by the mobile node for matching registration requests with registration replies, and for protecting against replay attacks of registration messages.
Extensions	
-	The fixed-length portion of the registration request is followed by one or more extensions that are described in the subsequent sections of this chapter. An authorization-enabling extension must be included in all registration requests.

Table 2. Registration Request Message Fields.

3. Registration Reply

A registration reply is generated by a home agent or foreign agent in response to a registration request initiated by a mobile node. A registration reply message contains the necessary codes to inform the mobile node about the status of its request, along with the lifetime that is granted by the home agent, which may be smaller than the requested lifetime. Figure 12 shows a registration reply message, with Table 3 describing its corresponding fields.

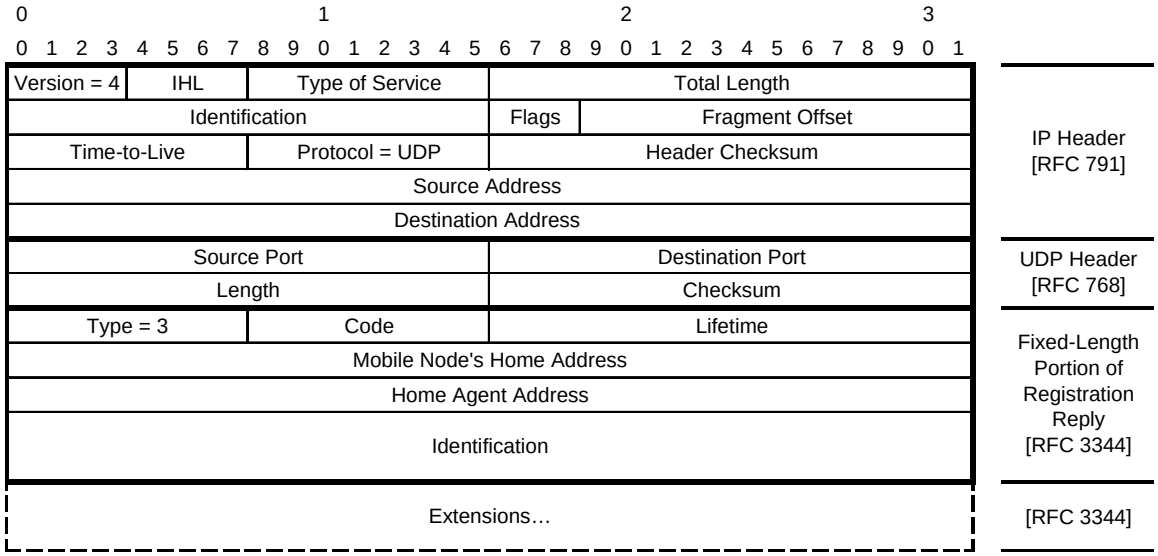


Figure 12. Registration Reply Message (After: [4] & [6]).

Field	Description
IP Header	
Source Address	*Foreign agent* : Copied from IP destination address of registration request. If "All Agents Multicast" address was used, interface address from which reply is sent must be used. *Home agent* : Copied from IP destination address of registration request. If a multicast or broadcast address was used, home agent's unicast IP address is used for this field.
Destination Address	*Foreign agent:* If it generates a registration reply to reject the request and the home address field in request is not 0.0.0.0, home address is used as the destination address. If it is relaying a reply from the home agent and the home address field is not 0.0.0.0, home address is used as the destination address. Otherwise, the destination address is set to 255.255.255.255. *Home agent* : Copied from IP source address of registration request.
UDP Header	
Source Port	A value of 434 is reserved for Mobile IP registration messages.
Destination Port	Copied from UDP source port of the registration request.
Fixed-Length Portion of Registration Reply	
Type	A type field of 3 identifies message as a registration reply.
Code	A value indicating the result of the registration request.
Lifetime	If code field indicates that the registration was accepted, the lifetime field is set to the number of seconds remaining before the registration is considered to be expired. A value of 0 indicates that the mobile node has been de-registered. If the code field indicates that the registration was denied, the contents of the lifetime field are unspecified and must be ignored upon reception.
Home Address	IP address of the mobile node.
Home Agent	IP address of the mobile node's home agent.
Identification	A 64-bit number used for matching registration requests with registration replies, and for protecting against replay attacks of registration messages. Value is computed based on the identification field from the mobile node's registration request, and on the style of replay protection used in the security context between the mobile node and its home agent. Details will be covered under the *Security Considerations* section of this chapter.
Extensions	
-	The fixed-length portion of the registration reply is followed by one or more extensions that are described in the subsequent sections of this chapter. An authorization-enabling extension must be included in all registration replies returned by the home agent.

Table 3. Registration Reply Message Fields.

4. Mobile Node's Role

A mobile node will register with its home agent by sending registration requests whenever it detects that there is a change in its network connectivity. This enables the home agent to create or update mobility bindings for the mobile node when it is away from home, as well as delete the mobile node's mobility bindings when it returns home. A mobile node will re-register with its foreign agent if it detects that the foreign agent has rebooted, or when its current registration lifetime is about to expire.

A mobile node receives registration replies from the home agent and/or the foreign agent in response to its registration requests. Registration replies indicate if a registration request was accepted, or if it was denied by the home agent or foreign agent.

A mobile node performs validity checks for received registration replies to determine if it should accept or discard the reply. Figure 13 illustrates the process of handling a registration reply that is received by a mobile node.

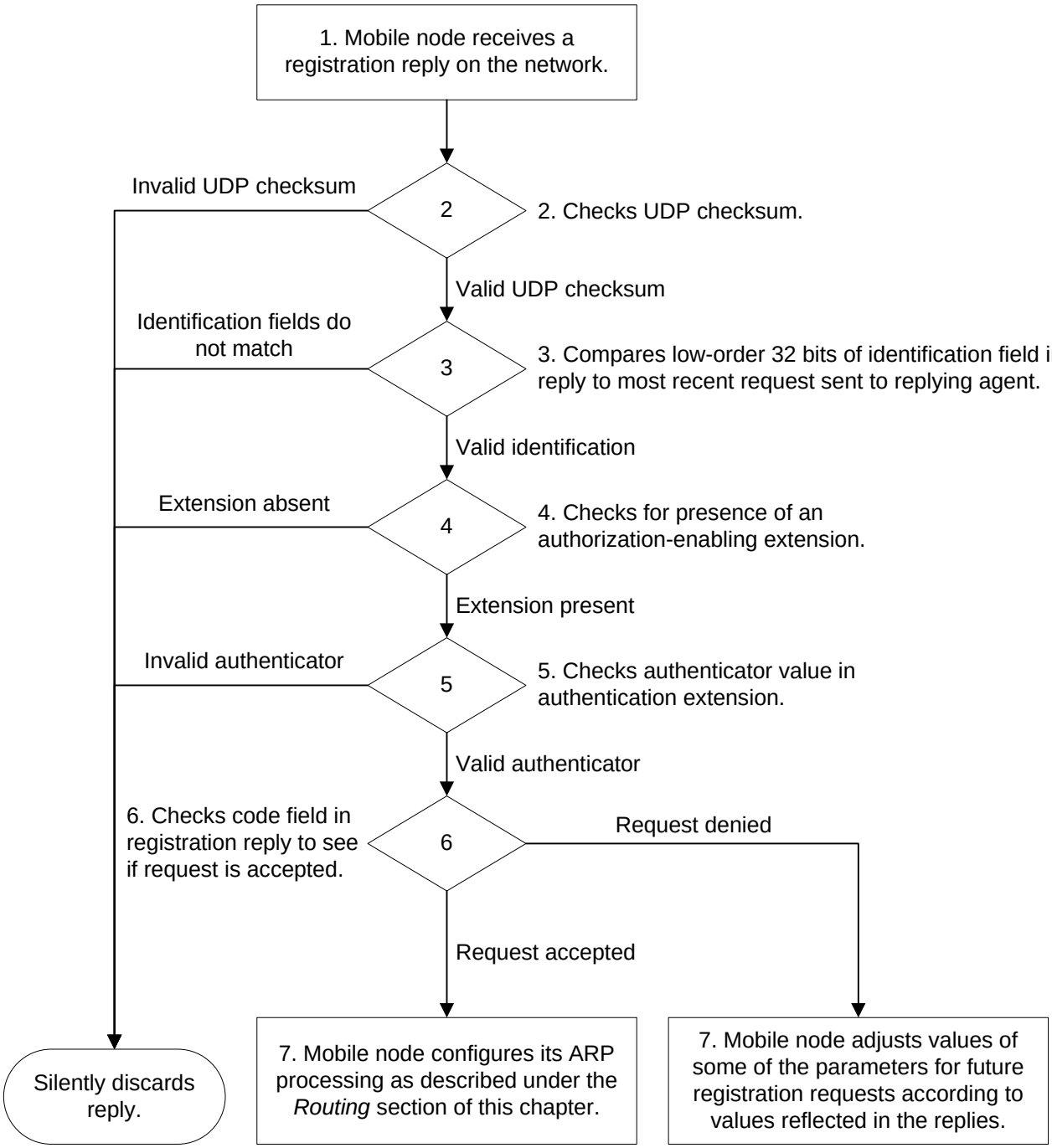


Figure 13. Processing a Registration Reply received by a Mobile Node.

5. Foreign Agent's Role

A foreign agent plays mostly a passive, "middleman", role in the Mobile IP registration process. A foreign agent relays registration requests and replies between the mobile node and its home agent. It will only generate a registration reply if it could not support the services requested by the mobile node. In the case where the foreign agent's care-of address is used in the registration process, the foreign agent will be responsible for decapsulating IP packets sent by the home agent for delivery to the mobile node.

Every foreign agent maintains a visitor list to capture each pending or current registration request it processes for a mobile node. The foreign agent may delete any pending registration request if it has been pending for more than seven seconds. Optionally, the foreign agent may also share mobility security associations with home agents or mobile nodes, in which case the appropriate authentication extensions must be included and processed when relaying such registration requests and replies. Figures 14 and 15 describe the process of handling registration requests and replies received by the foreign agent.

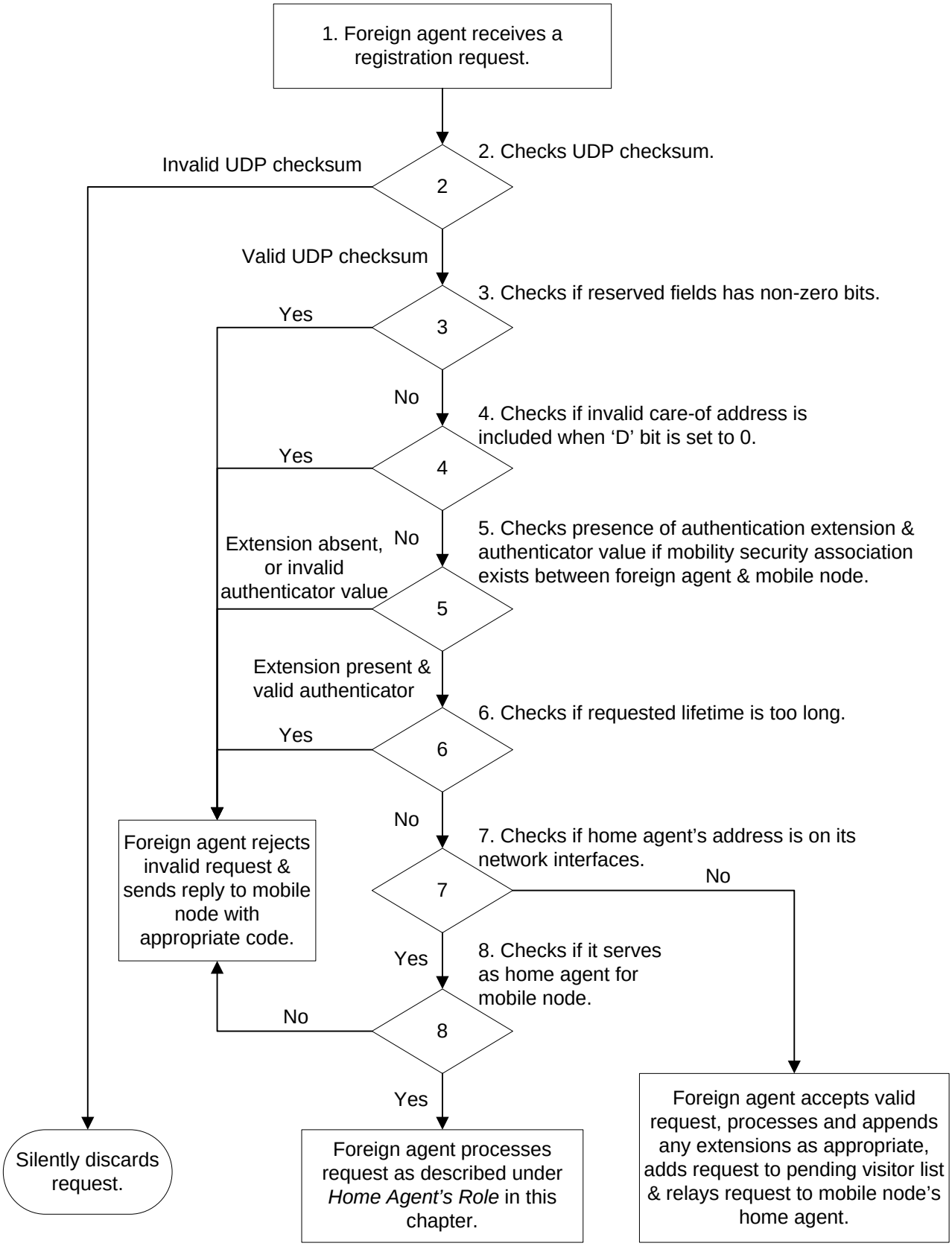


Figure 14. Processing a Registration Request received by a Foreign Agent.

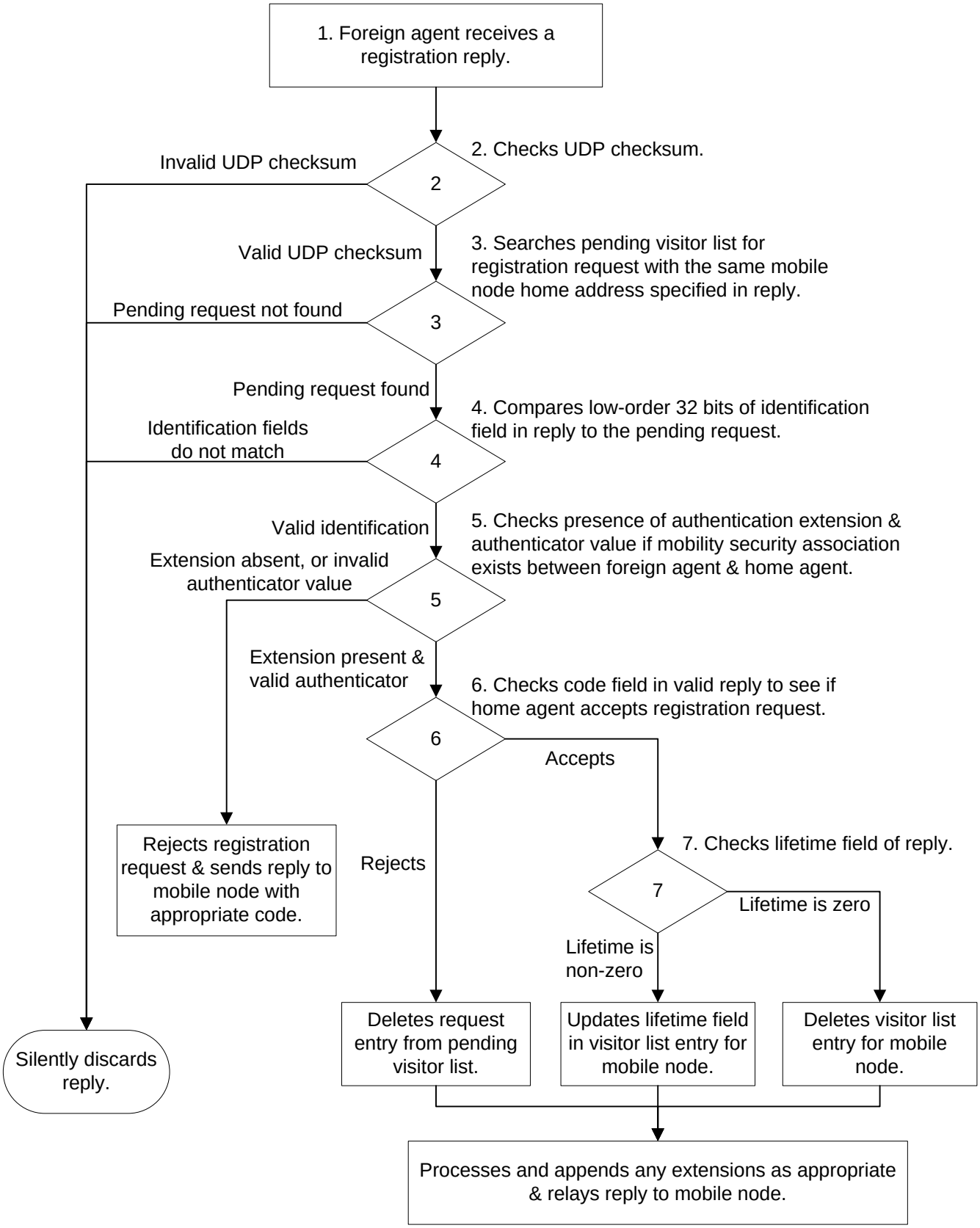
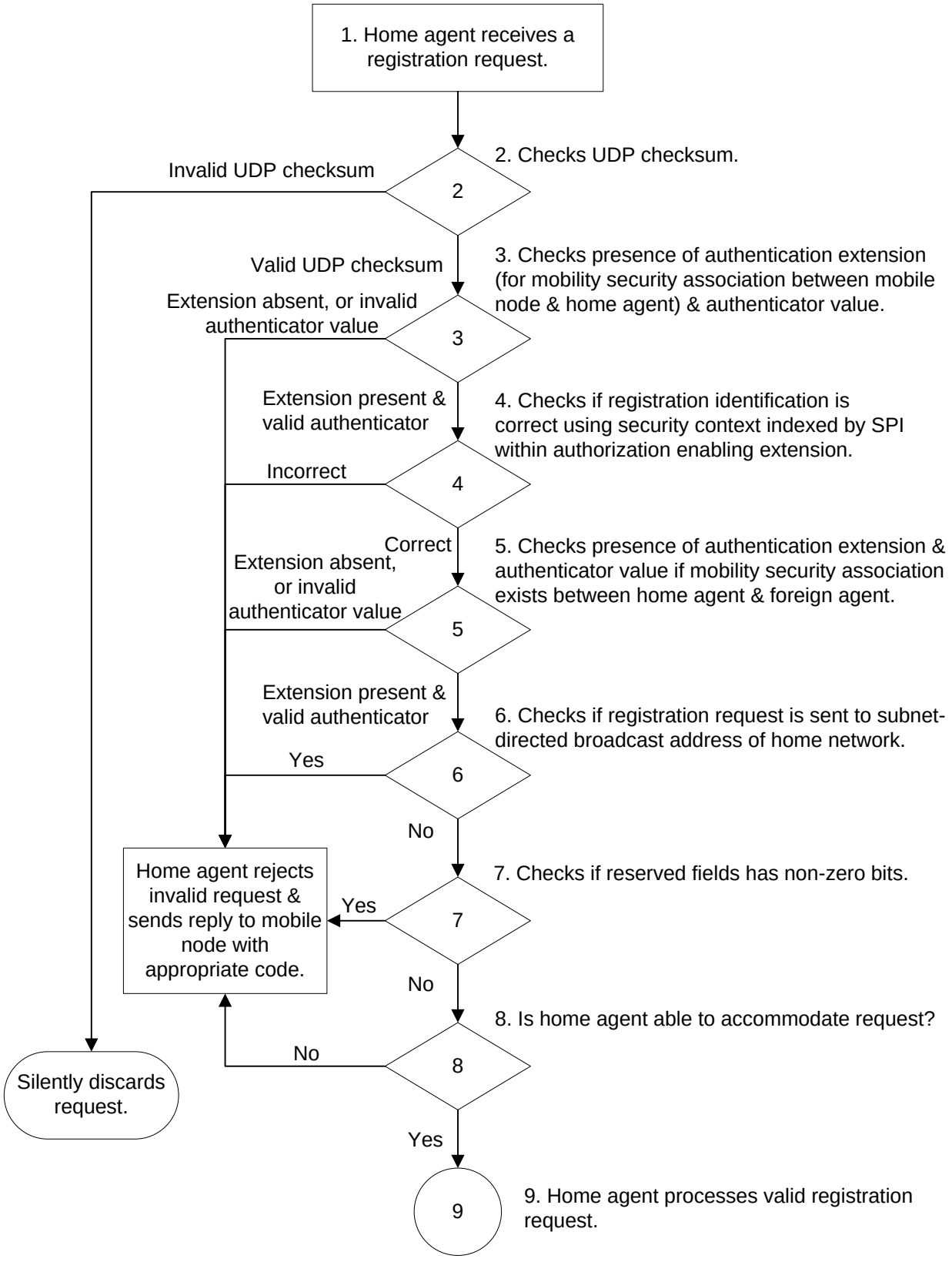


Figure 15. Processing a Registration Reply received by a Foreign Agent.

6. Home Agent's Role

A home agent plays a crucial role in the Mobile IP registration process. A home agent receives registration requests from the mobile node, updates its record of mobility bindings for the mobile node, and generates appropriate registration reply in response to each request. Every home agent maintains a list of mobility bindings for each mobile node that it serves as home agent.

To ensure the authenticity of a registration request in order to prevent against malicious DoS or traffic redirection types of attacks, all mobile nodes that will be served by a home agent must have been previously identified and configured with the appropriate mobility security associations with the home agent. Optionally, the home agent may also maintain mobility security associations with foreign agents, in which case the appropriate authentication extensions must be included and processed when responding to such registration requests and generating the corresponding registration replies. Figure 16 describes the process of handling a registration request that is received by a home agent.


1. Home agent receives a registration request.
2. Checks UDP checksum.
Invalid UDP checksum
2
Valid UDP checksum
3. Checks presence of authentication extension (for mobility security association between mobile node & home agent) & authenticator value.
Extension absent, or invalid authenticator value
3
Extension present & valid authenticator
4. Checks if registration identification is correct using security context indexed by SPI within authorization enabling extension.
Incorrect
4
Correct
5. Checks presence of authentication extension & authenticator value if mobility security association exists between home agent & foreign agent.
Extension absent, or invalid authenticator value
5
Extension present & valid authenticator
6. Checks if registration request is sent to subnet-directed broadcast address of home network.
Yes
6
No
Home agent rejects invalid request & sends reply to mobile node with appropriate code.
7. Checks if reserved fields has non-zero bits.
Yes
7
No
8. Is home agent able to accommodate request?
No
8
Silently discards request.
Yes
9
9. Home agent processes valid registration request.

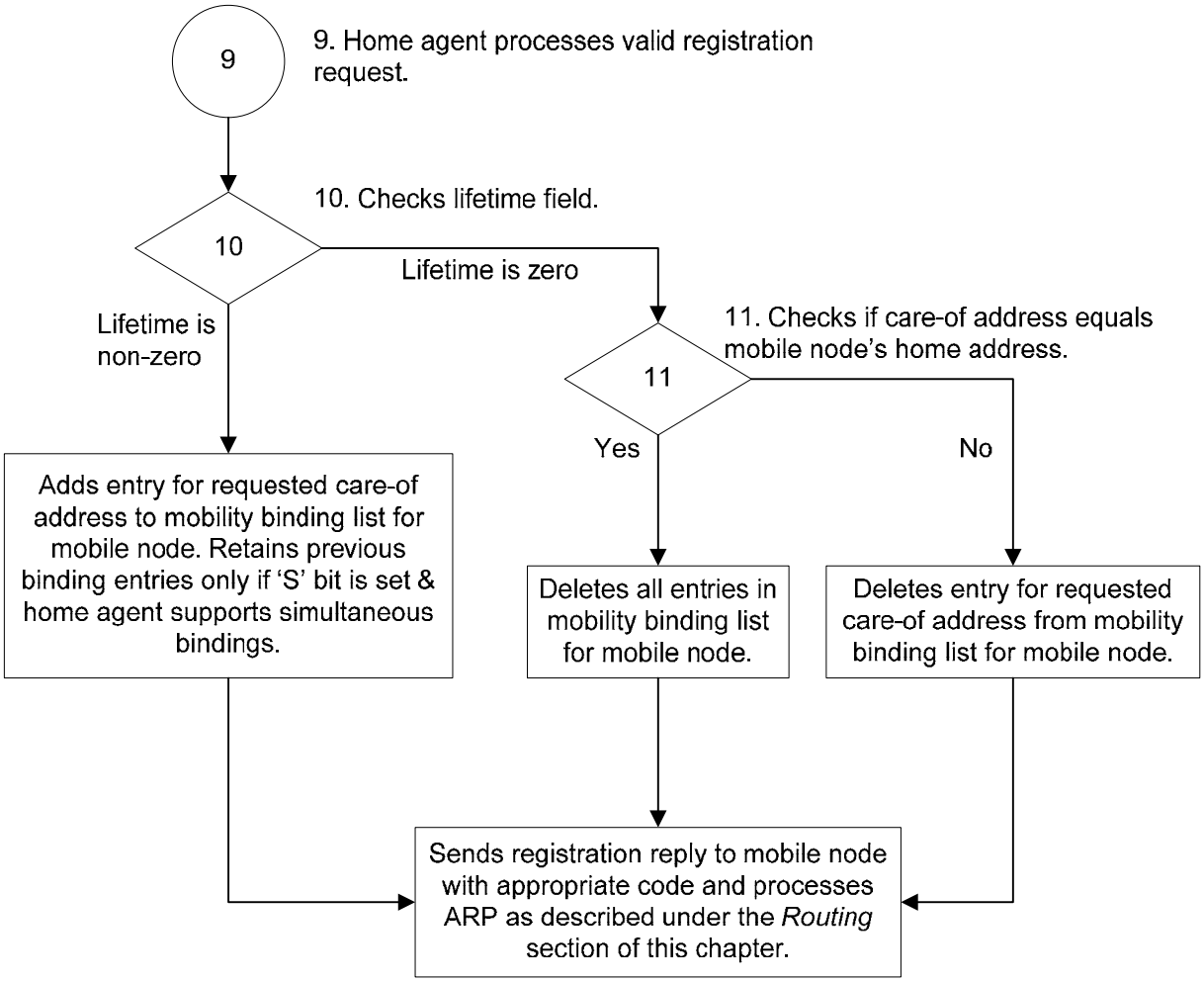


Figure 16. Processing a Registration Request received by a Home Agent.

D. ROUTING

Once the mobile node discovers its current location through agent discovery and communicates this information to its home agent via the registration process, routing is the next process that must take place to facilitate the delivery of IP packets to and from the mobile node.

1. Tunneling

As highlighted at the beginning of this chapter, one of the major goals of Mobile IP is for a mobile node to keep its IP address constant when it roams from network to network, at the same time maintaining ongoing communications with correspondent nodes. Supporting this with traditional routing protocols would require the propagation of host routes for each mobile node, which is clearly not robust and scaleable. Instead, the

approach adopted by Mobile IP is protocol tunneling, where host routes are inserted in at most two devices, i.e., the home agent and foreign agent, and single-hop logical links, or tunnels, are established from the home agent to the edge of the foreign network where the mobile node currently resides. The tunnel endpoint in the foreign network can either be a foreign agent's care-of address, or a mobile node's co-located care-of address. The home agent then forwards IP packets to the mobile node using this tunnel. Figure 17 depicts these two different tunnel options that can be established by a home agent.

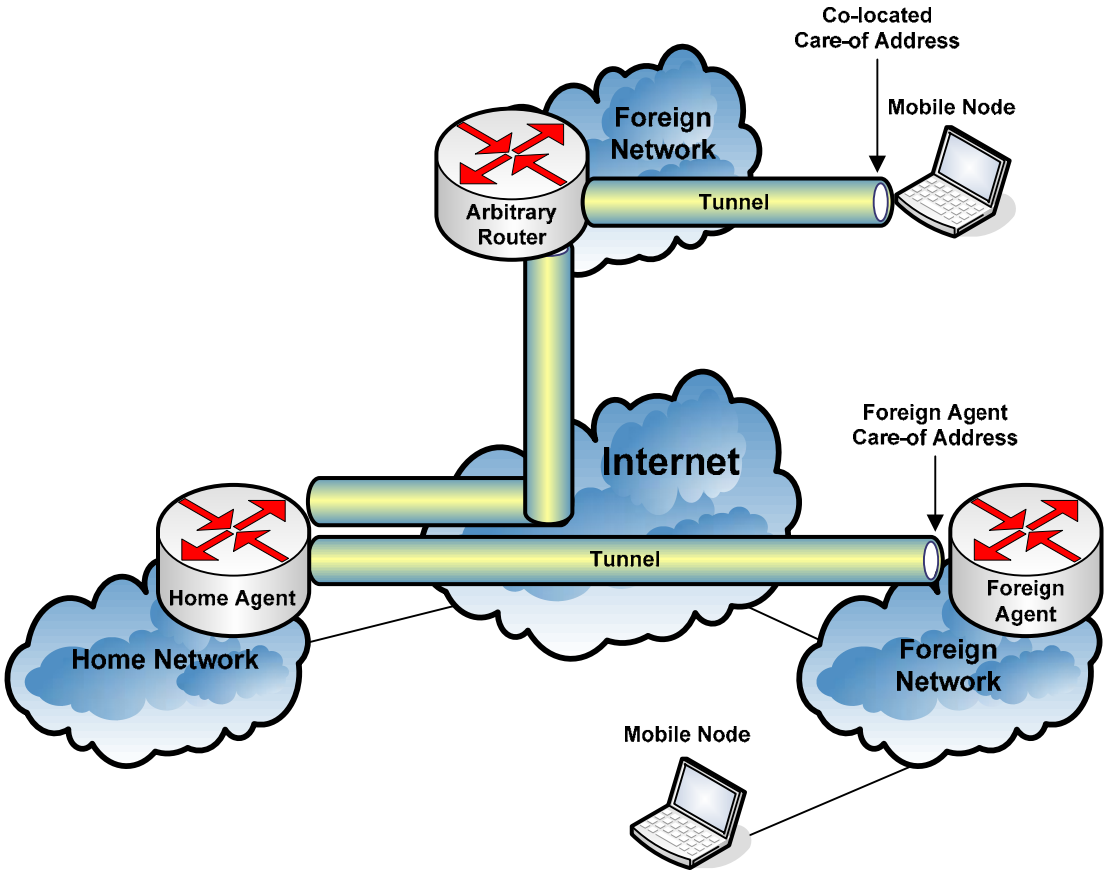


Figure 17. Tunnels established by a Home Agent (After: [6]).

Mobile IP uses IP-in-IP encapsulation [17] as the default tunneling protocol to deliver IP packets via the tunnel established by the home agent. An IP packet is encapsulated as payload in another IP packet, with the tunnel endpoints reflected in the source and destination address fields of the new IP header. The home agent encapsulates IP packets destined for the mobile node and sends them across the tunnel. Upon leaving the tunnel, the encapsulated IP packet is decapsulated either by the foreign agent for

delivery to the mobile node; or by the mobile node for delivery to its higher application layers. Each home agent, foreign agent, and mobile node using a co-located care-of address must be able to support IP-in-IP encapsulation, with optional support for minimal encapsulation [14] and Generic Routing Encapsulation (GRE) [15].

2. Triangle Routing

A mobile node operates without the support of mobility services when it is connected to its home network. IP packets sent to and from the mobile node are routed via the standard routing mechanisms. When the mobile node roams to a foreign network and is registered away from home, its home agent intercepts IP packets destined to the mobile node[1] and tunnels them to the mobile node's registered care-of address. At the care-of address, the foreign agent decapsulates and delivers the IP packets to the mobile node; or the mobile node performs its own decapsulation. IP packets sent by the mobile node on the foreign network are routed via the standard routing mechanisms to its correspondent node. Consequently, an asymmetric routing path, commonly referred to as triangle routing illustrated in Figure 18, is established for delivery of IP packets to and from a mobile node when it is away from its home network.

[1] IP unicast packets destined for the mobile node. A home agent will only forward IP broadcast packets to a mobile node if the mobile node has set the 'B' bit in its registration request. If a foreign care-of address is used, the home agent needs to first encapsulate the IP broadcast packet into an IP unicast packet addressed to the mobile node prior to tunneling it to the foreign agent (i.e., nested encapsulation). The foreign agent will then decapsulate and send the unicast encapsulated packet to the mobile node. Such nested encapsulation is not required if a mobile node uses a co-located care-of address.

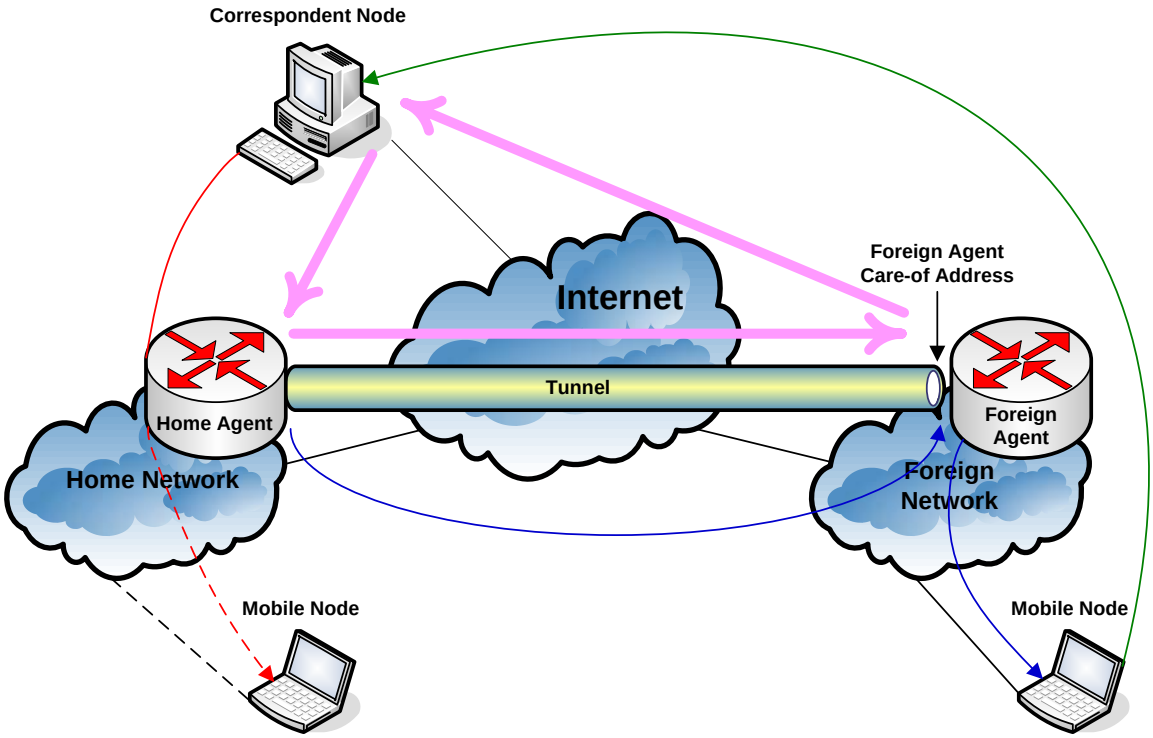


Figure 18. Triangle Routing (After: [5]).

3. ARP and its Variants

Besides tunneling, Address Resolution Protocol (ARP) [18] and its variants are used in a Mobile IP environment[2] to ensure proper delivery of IP packets to and from a mobile node. ARP is used when a node wishes to resolve (discover) a target node's Ethernet link-layer address from its IP address.

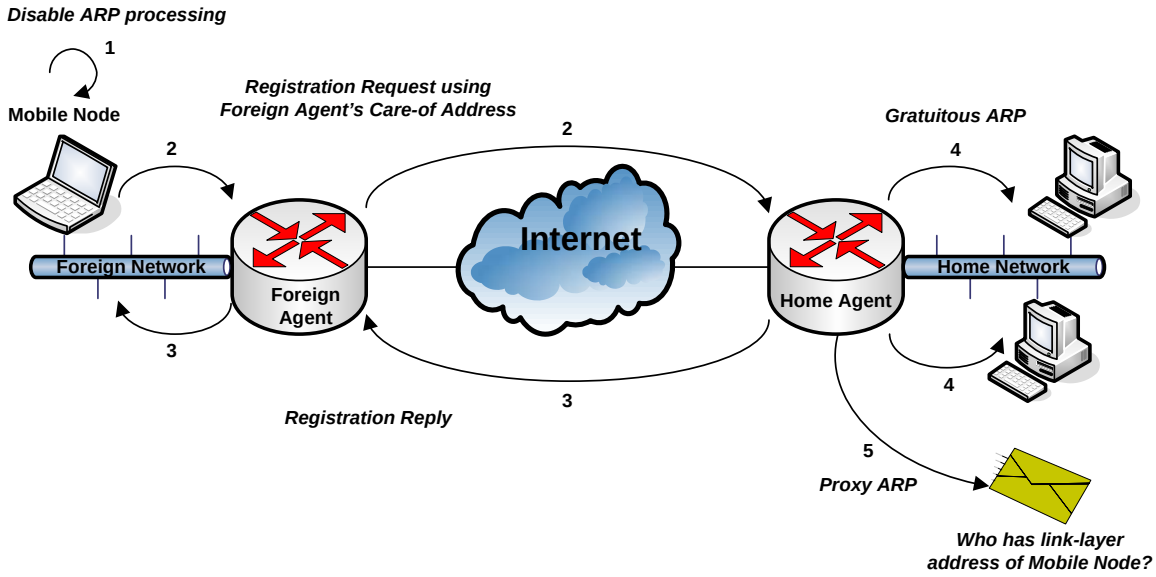
A proxy ARP [19] is an ARP reply sent by a node, i.e., the proxy, on behalf of another node that is unable to respond to its own ARP requests. The recipient of this reply will then associate the proxy node's link-layer address with the IP address of the original target node.

A gratuitous ARP [8] is an ARP packet sent by a node to cause other nodes to spontaneously update an entry in their ARP cache, to immediately reflect the change in link-layer address associated with the IP address advertised in the ARP packet. A gratuitous ARP uses either an ARP request or ARP reply packet. Both the ARP sender and target protocol addresses are set to the IP address of the cache entry to be updated,

[2] This section is applicable to all home networks that use ARP for address resolution.

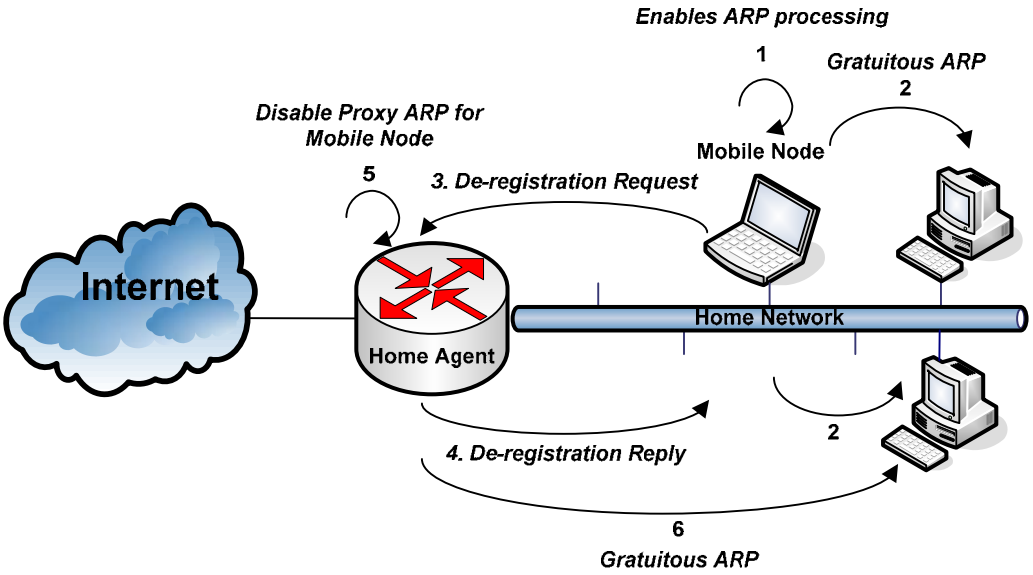
and the ARP sender hardware address is set to the link-layer address to be reflected in the updated cache entry. The target hardware address is also set to the same link-layer address if an ARP reply packet is used.

To ensure the correct operation of the Mobile IP protocol, it is important for the use of ARP, proxy ARP, and gratuitous ARP to adhere to a specific sequence when a mobile node roams away from home or when it returns home. Figures 19 and 20 illustrate the use of ARP and its variants for the scenario when a mobile node leaves its home network; and the scenario when the mobile node returns to its home network.



1. Mobile node disables its own processing of any ARP requests it may subsequently receive that request link-layer address corresponding to its home address (except when necessary to communicate with foreign agents on visited networks).
2. Mobile node transmits its registration request.
3. Home agent accepts registration request & sends reply.
4. Home agent sends gratuitous ARP to all nodes on the home network by setting its link-layer address as that for the mobile node's home address.
5. Home agent uses proxy ARP to reply to ARP requests that it receives on the home network, requesting for the mobile node's link-layer address.

Figure 19. ARP Operation when a Mobile Node leaves its Home Network.



1. Mobile node re-enables its own processing of any ARP requests it may subsequently receive that request link-layer address corresponding to its home address.
2. Mobile node performs a gratuitous ARP for itself.
3. Mobile node transmits its de-registration request.
4. Home agent accepts de-registration request & sends reply.
5. Home agent stops using proxy ARP to reply to ARP requests that it receives on the home network, requesting for the mobile node's link-layer address.
6. Home agent uses mobile node's link-layer address to send gratuitous ARP on behalf of mobile node to all nodes on the home network.

Figure 20. ARP Operation when a Mobile Node returns to its Home Network.

E. MOBILE IP HANDOFF

In order for a mobile node to roam from one network to another and continue its ongoing communications with other correspondent nodes, it must be able to perform move detection through agent discovery and register its new location with its home agent through the registration process. Routing information is then updated to facilitate the delivery of IP traffic to the mobile node. Since Mobile IP is a layer 3 protocol, a change in routing to facilitate the continued delivery of IP traffic to the mobile node is considered a Mobile IP handoff.

There are three scenarios in which a Mobile IP handoff can be initiated, namely, when a mobile node leaves it home network, when a mobile node roams from one foreign network to another foreign network, and when a mobile node returns to its home network. In addition to using agent discovery, a mobile node may rely on link-layer mechanisms to

decide that it has moved to a different network. One such mechanism is the wireless link-layer handoff that will be described in the next chapter.

F. SECURITY CONSIDERATIONS

The Mobile IP registration procedure is potentially vulnerable to Denial-of-Service (DoS) and traffic redirection types of attacks, as a malicious user could masquerade as a mobile node and send bogus registration requests to the mobile node's home agent, resulting in tunneling of the mobile node's IP packets to the malicious user. To prevent against such attacks, the Mobile IP protocol requires that all registration messages between the mobile node and its home agent be authenticated. Specifically, RFC 3344 [4] states that

> Registration messages between a mobile node and its home agent MUST be authenticated with an authorization-enabling extension, e.g., the Mobile-Home Authentication Extension.

1. Authentication Extensions

Authentication extensions are used by the Mobile IP protocol to provide peer authentication and message integrity. An authentication extension is appended to the end of a registration request or reply message that contains relevant security information to authenticate and protect the integrity of the registration process. An authentication extension that facilitates the acceptance of a registration request or reply message by a recipient of the message is also referred to as an authorization-enabling extension. Figure 21 depicts the authentication extension that follows after a registration request or reply message, and Table 4 describes its corresponding fields.

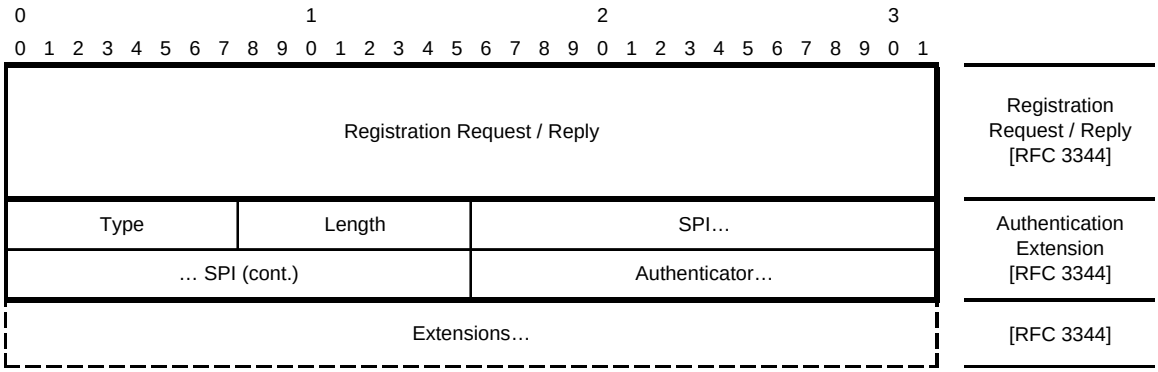


Figure 21. Authentication Extension (After: [4]).

Field	Description
Authentication Extension	
Type	Mobile-Home Authentication Extension has a value of 32. Mobile-Foreign Authentication Extension has a value of 33. Foreign-Home Authentication Extension has a value of 34.
Length	4 bytes (for SPI) plus number of bytes in the Authenticator.
SPI	4 bytes Security Parameter Index.
Authenticator	Variable length.

Table 4. Authentication Extension Fields.

The Mobile IP protocol uses three authentication extensions to protect its registration request and reply messages, namely, the mobile-home authentication extension, mobile-foreign authentication extension and foreign-home authentication extension.

a. Mobile-Home Authentication Extension (MHAE)

The mobile-home authentication extension must be present in all registration requests initiated by the mobile node, as well as all registration replies generated by the home agent.

b. Mobile-Foreign Authentication Extension (MFAE)

The mobile-foreign authentication extension must be included in registration requests and replies whenever a mobility security association exists between the mobile node and foreign agent.

c. Foreign-Home Authentication Extension (FHAE)

The foreign-home authentication extension must be included in registration requests and replies whenever a mobility security association exists between the foreign agent and home agent.

2. Security Association

Mobile IP entities must first share a security relationship in order to use an authentication extension. The security relationship is predefined using a set of parameters configured into each node, which are collectively known as a security context. A security context identifies the encryption algorithm and mode, the shared key used by a pair of nodes, and the method of replay protection used. A specific security context in an authentication extension is identified by a four byte Security Parameter Index (SPI). A

group of one or more security contexts that are shared with a peer node is referred to as a security association.

a. Encryption Algorithm and Mode

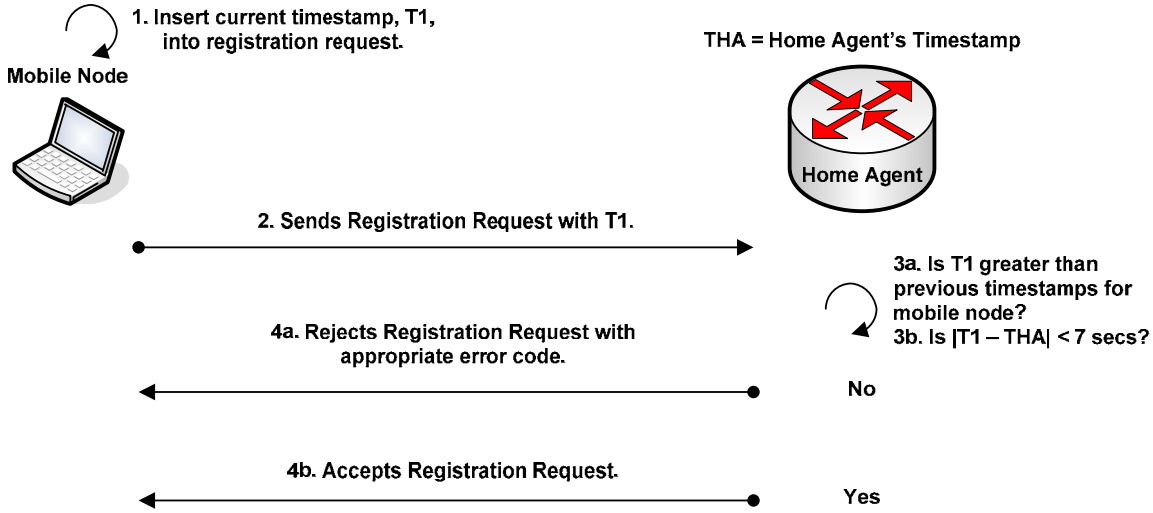
The authenticator value computed for each authentication extension is a Message Authentication Code (MAC), which is a unique fingerprint for each registration message. HMAC-MD5 [20] is the default algorithm used to compute a 128-bit message digest of the registration message. The computed authenticator value will protect the registration request or reply data, all prior extensions in their entirety, as well as the type, length and SPI of the authentication extension. The SPI within any of the authentication extensions defines the security context that is used to compute the authenticator value and must be used by the recipient to verify the received value.

b. Shared Key

The authenticator value is computed using a key that is shared between a pair of nodes. The sender of the message uses the shared key to compute the authenticator value (i.e., the MAC) and places it in the authentication extension. The recipient uses the same shared key to compute the authenticator over the received registration message, compares the result to the authenticator value in the authentication extension, and accepts the authentication only if the two values match. The default key used for HMAC-MD5 in the Mobile IP registration process is 128 bits long and is represented as a 32-character hexadecimal string. In order for keyed MD5 authentication to be useful, the 128-bit key must be both secret, i.e., known only to communicating peers, and pseudo-random.

c. Replay Protection

To prevent the replay of captured registration requests by a malicious user, the Mobile IP registration process offers two methods of replay protection. All mobile nodes and home agents must implement timestamp-based replay protection, with optional support for replay protection based on nonce. Figures 22 and 23 illustrate the use of the replay protection mechanisms based on timestamp and nonce.



1. Mobile node inserts current timestamp into registration request by setting the identification field to a 64-bit value formatted as specified by the Network Time Protocol (NTP) [21]. Identification value must be greater than that used by previous registration requests, as the home agent uses this as a sequence number.
2. Mobile node sends the registration request to its home agent.
3. Home agent checks timestamp value in identification field:
a. Is it greater than all previously accepted timestamps for mobile node?
b. Does it fall within the allowable range from the home agent's current timestamp?
4a. If either of the checks in 3 fails, the home agent rejects the registration request by sending a reply with an appropriate error code.
4b. Home agent accepts the registration request only if the timestamp value passes the checks in 3.

Figure 22. Replay Protection using Timestamp (After: Ref. [5]).

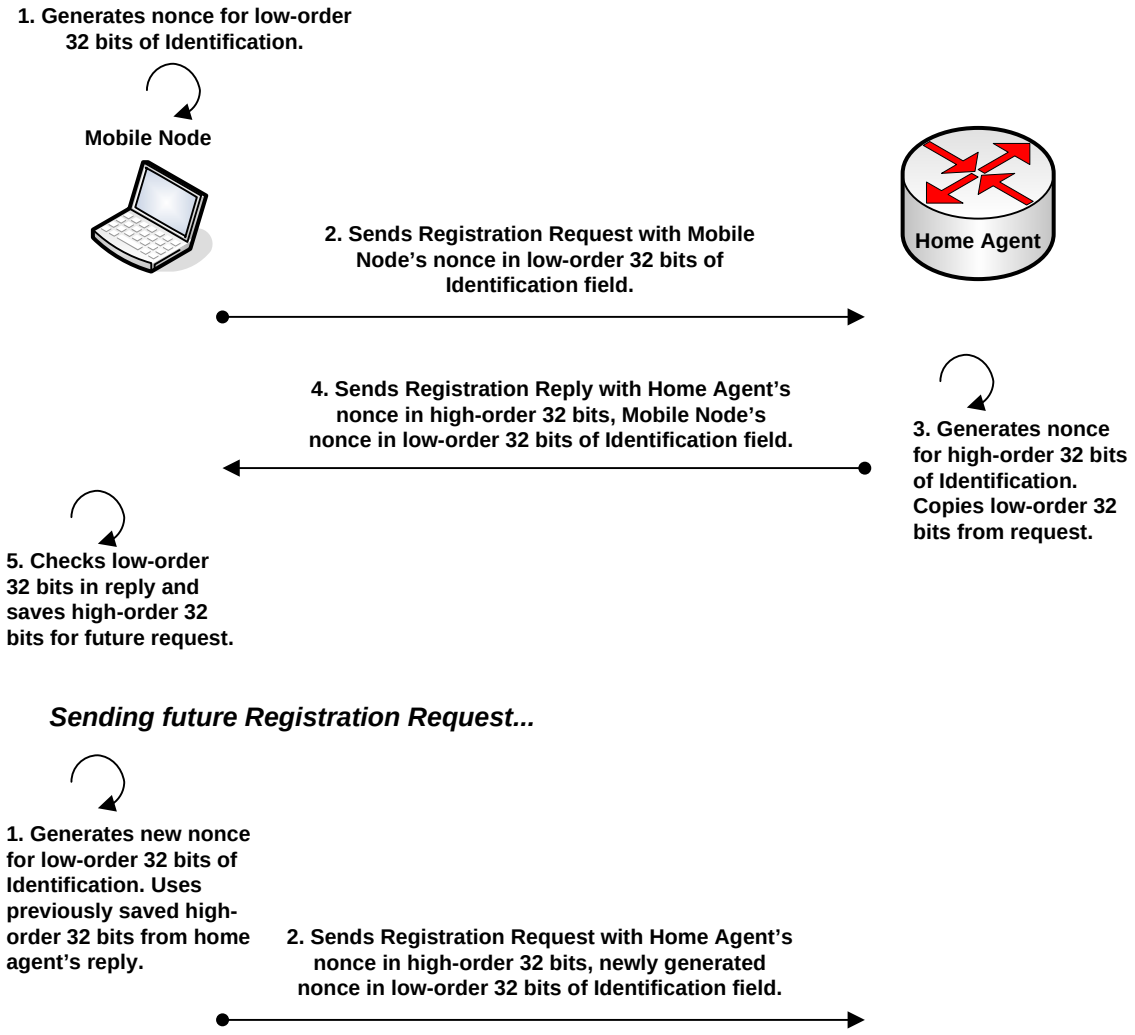


Figure 23. Replay Protection using Nonce.

3. IP Spoofing

IP spoofing enables a malicious user to gain unauthorized access to networked resources by assuming the IP address of an authorized network node [22]. This is possible since the IP standard defines routing of IP packets to be based only upon destination address [1]. To protect against IP spoofing, many routers that are connected to the Internet implement ingress filtering, where IP packets whose source address appears to be topologically incorrect are dropped.

Mobile IP relies on the standard routing based on destination address in order for a mobile node to retain its IP address when it roams away from its home network. As a mobile node's home address will be considered topologically incorrect when it is

connected to a foreign network, IP packets originated from the mobile node in the foreign network may potentially be dropped. To support the proper operation of Mobile IP in such an environment, a mobile node may request the use of reverse tunneling [16] during registration with its home agent. In this case, IP packets sent by the mobile node will be reverse-tunneled back to the home agent for delivery to the destination.

4. Open Areas of Concern

a. Key Management

The Mobile IP protocol uses keyed MD5 as its authentication mechanism. This requires the management of shared secret keys between peer nodes that have a security association. As key distribution is difficult in the absence of a network key management protocol, registration messages exchanged with the foreign agent do not need to be authenticated. This will potentially subject the registration process to traffic redirection attacks in which a malicious node can masquerade as a foreign agent and send bogus agent advertisements.

b. ARP Usage

As described under the *Routing* section of this chapter, gratuitous ARP is used to force recipients of the ARP packet to spontaneously update their ARP cache for the broadcast entry. Since the use of ARP is not subjected to any form of authentication, attackers can potentially exploit this vulnerability to poison the ARP cache [23] and result in malicious traffic redirection.

THIS PAGE INTENTIONALLY LEFT BLANK

III. IEEE 802.11 PROTOCOL PRIMER

A. INTRODUCTION

Wireless networking is often associated with mobility. Wireless data networks free users from the tethers of an Ethernet cable at a desk, allowing users to roam freely and stay connected to the network. Several wireless technologies are available for the purpose of data transmission; however, the wireless technology based on the IEEE 802.11 standard [24] is the most popular and widely adopted wireless method for networking computers. It is thus appropriate to give an overview of how the IEEE 802.11 protocol operates, so as to appreciate its integration with the Mobile IP protocol to provide seamless mobility when a user wirelessly roams from one network to another.

This chapter will briefly describe the IEEE 802.11 nomenclature and design, highlighting the two types of network modes available for an IEEE 802.11 environment. The chapter will then introduce the fundamental building blocks underlying an IEEE 802.11 infrastructure mode network, followed by the basics of operation of this mode. The chapter will conclude with an analysis of what constitutes a “link layer handoff”, and how this handoff integrates with the mobility mechanisms of the Mobile IP protocol.

It is not the intent of this chapter to describe the operations of the IEEE 802.11 standard at length. Sufficient details will be covered to set the stage for the focus of this research. Readers can refer to [25] and [26] for a more thorough treatment on the IEEE 802.11 operations and security ramifications. These same two references have also served as the main source of information for the concepts illustrated in this chapter.

B. IEEE 802.11 NOMENCLATURE AND DESIGN

Before delving into the operations of the IEEE 802.11 protocol, it is appropriate to describe the nomenclature and design of IEEE 802.11 wireless networks, in order to facilitate understanding of the concepts underlying the IEEE 802.11 operation.

1. Physical Components

IEEE 802.11 networks are comprised of four major physical components, namely, distribution system, access points, wireless medium and stations. Figure 24 depicts the relationship among these four components.

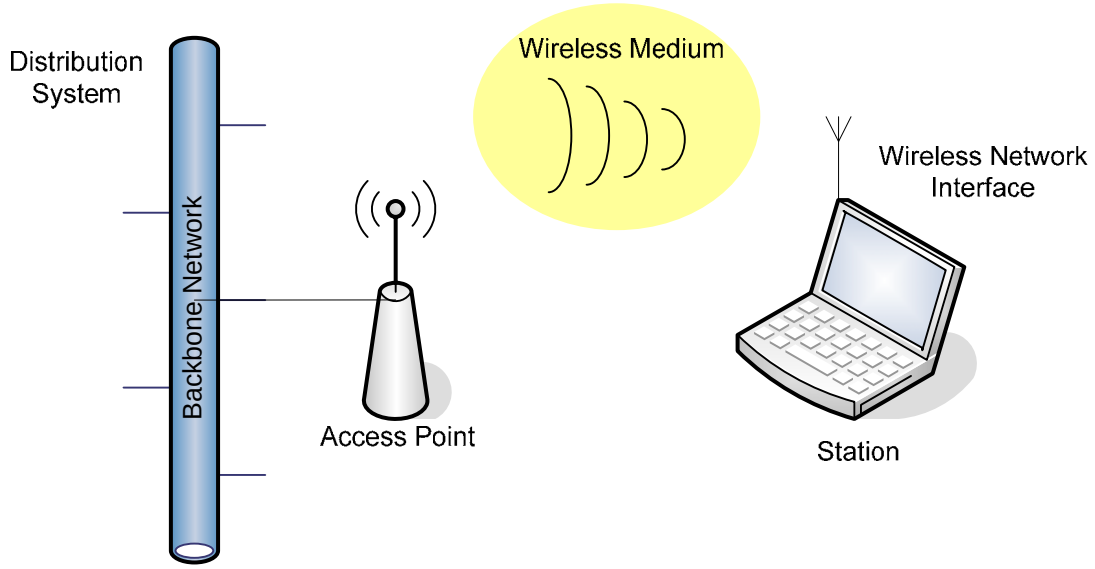


Figure 24. Components of an IEEE 802.11 Network (After: Ref. [25]).

a. Distribution System

A distribution system is typically a backbone network that is used to connect multiple access points servicing a large coverage area. The distribution system is used to transmit frames[3] from one access point to another access point, or any other network destination—wired or wireless.

b. Access Point

An access point performs the wireless-to-wired bridging function, so as to convert frames received on an IEEE 802.11 wireless network into other type of frames as appropriate for delivery in the wired environment.

c. Wireless Medium

The IEEE 802.11 standard uses a wireless medium to transmit frames from one location to another. Several physical layers have been defined in the standard;

[3] A frame refers to a Protocol Data Unit (PDU) at layer 2, i.e., the Data Link layer, of the Open Systems Interconnection (OSI) reference model.

however, the more popular wireless medium in use today is a portion of the radio frequency (RF) range of the electromagnetic spectrum.

d. Stations

Stations are simply computing devices with wireless network interfaces. Depending on the usage scenario, stations can range from portable handheld devices to desktop computers with wireless network interfaces.

2. Types of Networks

IEEE 802.11 supports two types of network modes, specifically, independent mode and infrastructure mode.

a. Independent Mode

Stations in an independent network mode communicate directly with each other, and thus, must be in direct communication range with all the participating stations. Typically, independent network mode is used to setup a wireless network for a small number of stations to serve a specific purpose within a short time-frame. Because of the small size, short duration, and explicit purpose, independent network mode is sometimes referred to as ad-hoc network mode. Figure 25 illustrates a wireless network setup based on the independent mode.

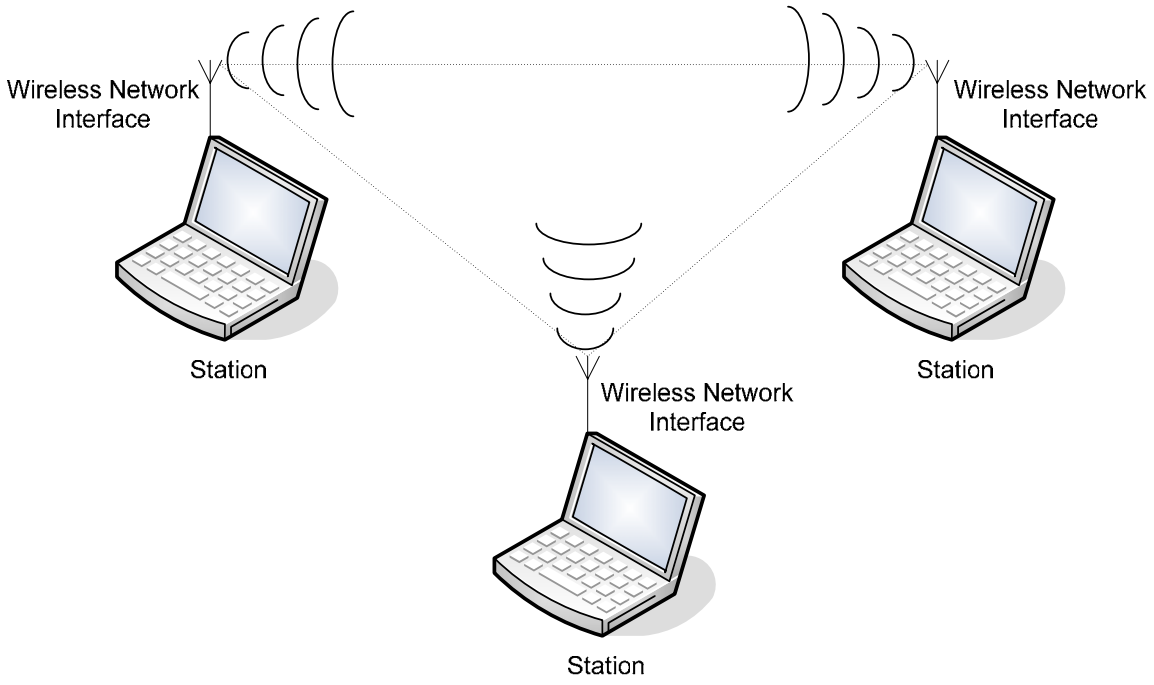


Figure 25. Wireless Network in Independent Mode (After: Ref. [25]).

b. Infrastructure Mode

The main distinction between an infrastructure network mode and an independent network mode is the presence of an access point. Access points are used for all wireless communications between stations in an infrastructure network mode. Transmission of a frame from one station to another station requires two hops: first, the source station transmits the frame to the access point; next, the access point transmits the frame to the destination station. Stations in an infrastructure network mode will only need to stay within communication range with the access point. Figure 26 illustrates a wireless network setup based on the infrastructure mode.

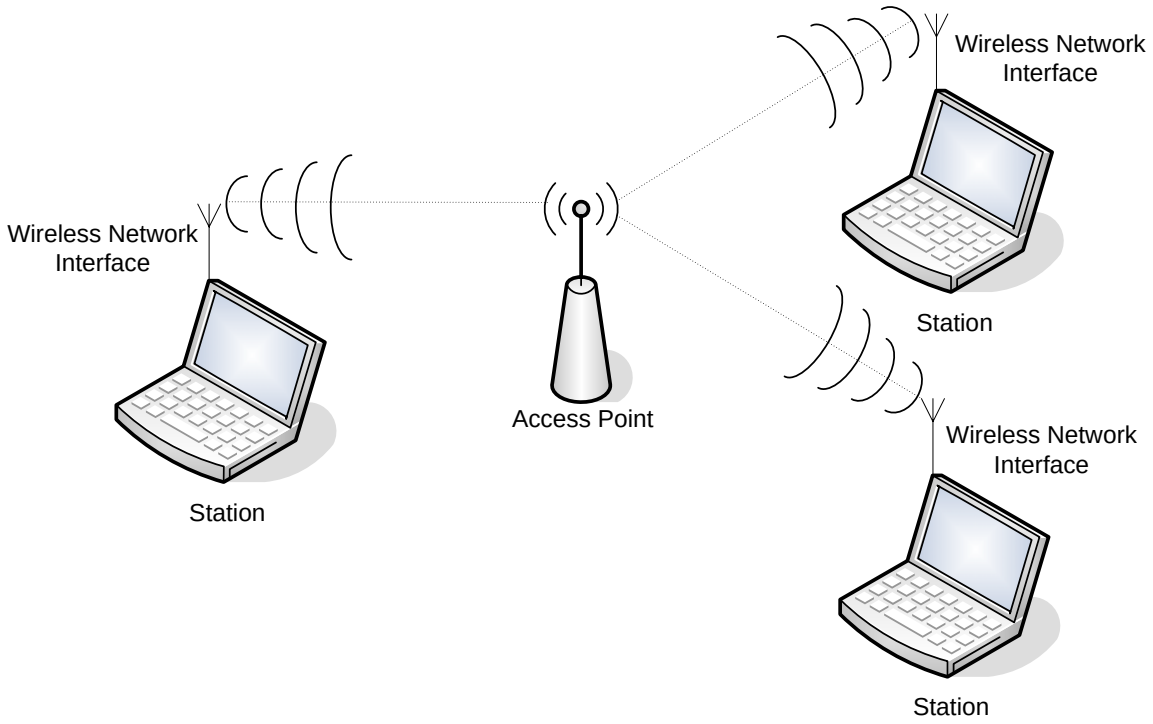


Figure 26. Wireless Network in Infrastructure Mode (After: Ref. [25]).

3. Building Blocks for Wireless Network in Infrastructure Mode

As stated in the earlier section, wireless networks configured using the independent mode are typically short-lived and service only a small group of users. Infrastructure mode is; however, the appropriate mode for creating a more permanent and scalable wireless networking infrastructure to service a larger group of users. Moreover, wireless networks configured based on the infrastructure mode will interoperate

seamlessly with the Mobile IP environment, and were thus adopted for the lab setup described in the next chapter.

a. Basic Service Set (BSS)

The fundamental building block for an IEEE 802.11 wireless network in infrastructure mode is the Basic Service Set (BSS). Stations within a BSS are serviced by an access point, and they compete for the same, shared wireless medium. Each BSS is assigned a BSS Identifier (BSSID), which corresponds to the Media Access Control (MAC) address of the wireless interface in the access point servicing the BSS. Figure 27 shows the notion of a BSS.

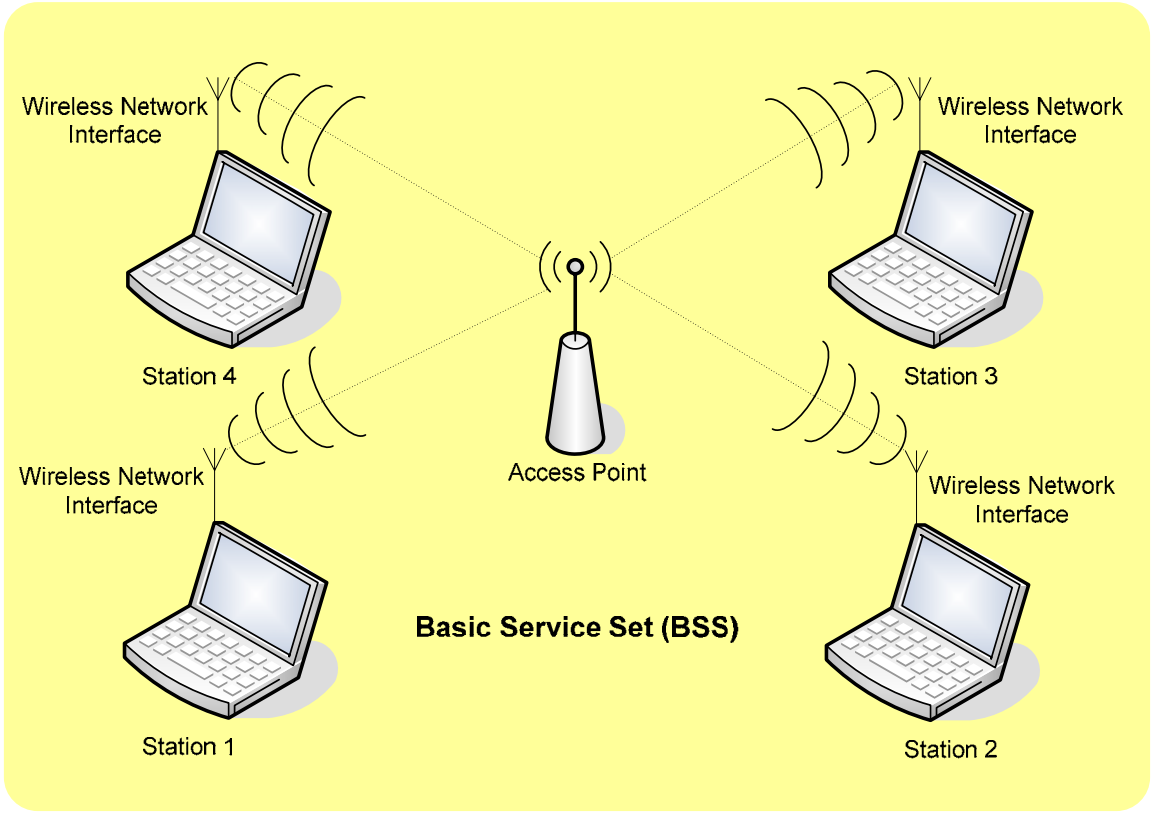


Figure 27. Basic Service Set (BSS) (After: Ref. [25]).

b. Extended Service Set (ESS)

BSS can only provide service coverage up to a certain area size, beyond which, the IEEE 802.11 standard allows for wireless networks of arbitrarily large size to be created by interconnecting different BSSs to form an Extended Service Set (ESS). An ESS typically utilizes the distribution system to connect the various BSSs, as depicted in Figure 28.

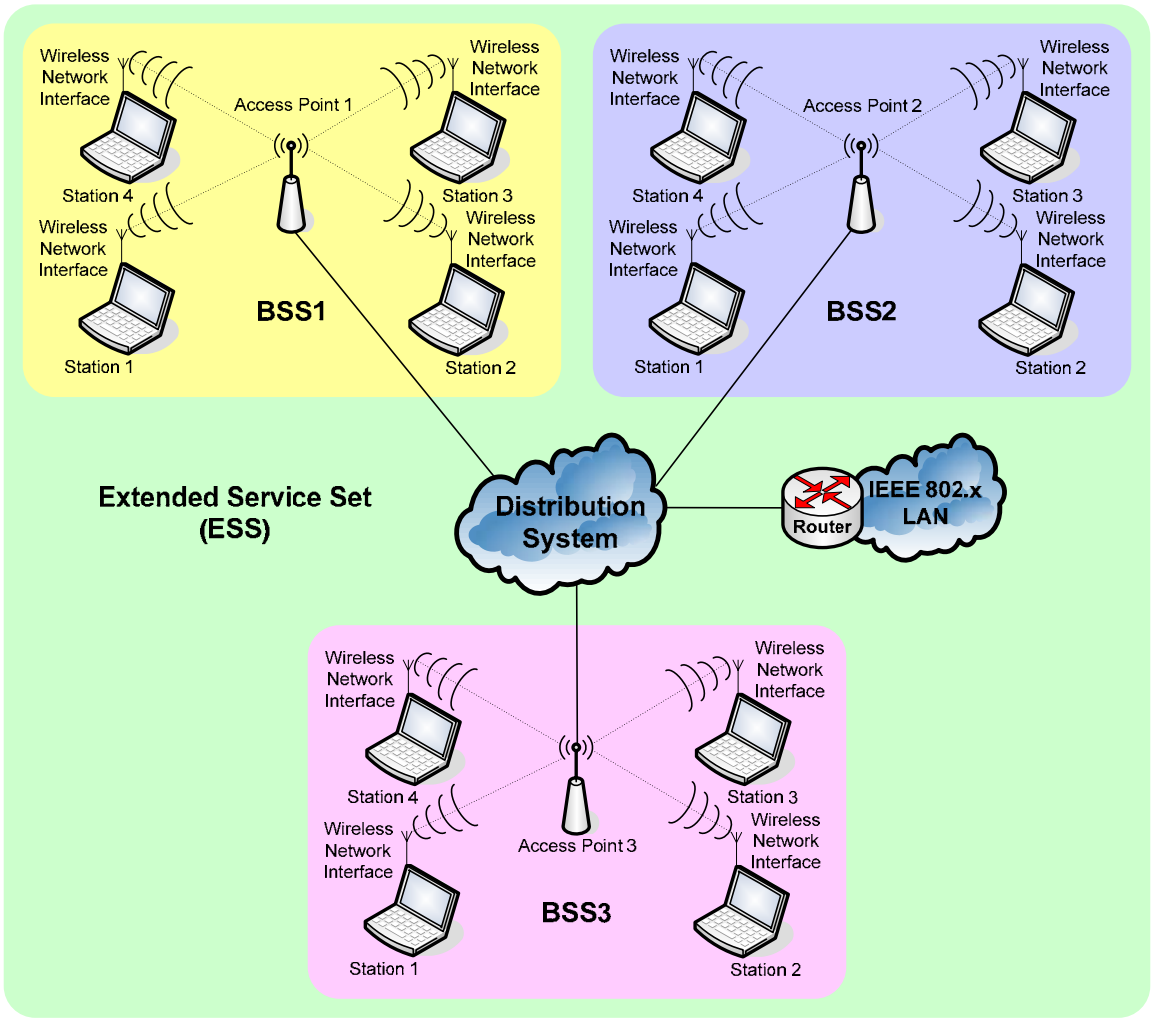


Figure 28. Extended Service Set (ESS) (After: Ref. [27]).

C. IEEE 802.11 NETWORK OPERATIONS

IEEE 802.11 standard is a member of the IEEE 802 family [28], which specifies a series of standards for Local Area Network (LAN) and Metropolitan Area Network (MAN) technologies. IEEE 802 standards address the two lowest layers of the Open Systems Interconnection (OSI) reference model, the physical and data link[4] layers. IEEE 802.2 standard [29] specifies a common link layer, i.e., the Logical Link Control (LLC) layer, which can be used by any lower layer LAN technology. IEEE 802.11 standard can be considered as another LAN technology that utilizes the IEEE 802.2 / LLC encapsulation. The IEEE 802.11 standard includes specification for both the physical and Media Access Control (MAC) layers. The relationships among the various components of the IEEE 802 family are illustrated in Figure 29.

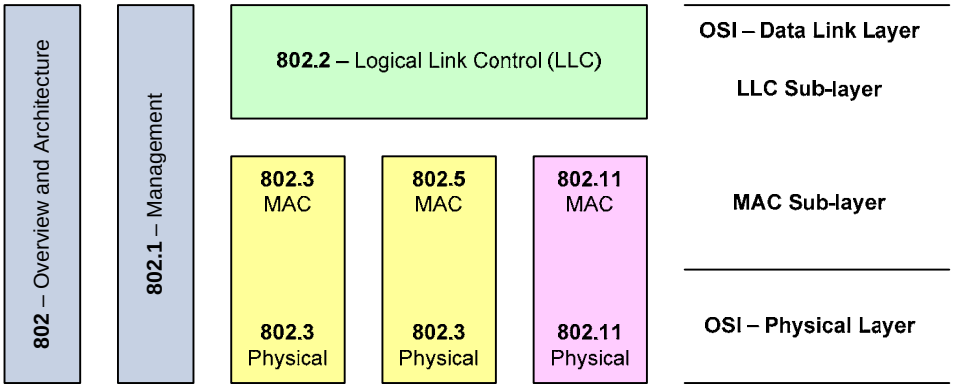


Figure 29. IEEE 802 Network Technology Family Tree (After: Ref. [25] & [28]).

1. Network Services

The IEEE 802.11 standard offers nine network services: three of the services are used for data transmission; the remaining six services are used for management operations to track the current location of stations for correct frame delivery. Table 5 summarizes the network services that are described in the IEEE 802.11 standard.

[4] The Data Link layer of the OSI reference model is further divided into two sub-layers: the Logical Link Control (LLC) sub-layer; and the Media Access Control (MAC) sub-layer.

Service	Type	Description
Distribution	Data transmission	An access point uses the distribution service to deliver a frame to its destination.
Integration	Data transmission	The distribution system uses the integration service to deliver a frame to an IEEE 802 LAN outside the wireless network.
Association	Management operation	Stations are required to register, or associate, with an access point in order to send or receive frames in the BSS served by the access point. The registration information is also used by the distribution system to determine which access point to use for frame delivery to a station.
Reassociation	Management operation	When a station moves between BSSs within an ESS, it will evaluate the signal strength and may change the access point with which it is currently associated. A station initiates a reassociation with a new access point whenever the signal conditions indicate that this new association is beneficial. After reassociation is complete, the distribution system updates its location records to reflect the access point to use for frame delivery to the station.
Disassociation	Management operation	Stations may use the disassociation service to terminate an existing association. Any location records stored within the distribution system will be removed when stations invoke this service. Stations will no longer be attached to the BSS once disassociation is complete.
Authentication	Management operation	An access point uses authentication to determine the identity of the station prior to establishing association with the station.
Deauthentication	Management operation	Deauthentication terminates an authenticated relationship, along with its existing association.
Privacy	Management operation	The privacy service provides protection against potential eavesdropping over the wireless network.
MSDU Delivery	Data transmission	Stations use the MAC Service Data Unit (MSDU) delivery service to deliver data to the recipient.

Table 5. IEEE 802.11 Network Services (After: Ref. [25]).

2. IEEE 802.11 Framing

IEEE 802.11 framing is much more elaborate than the traditional Ethernet framing in a wired environment, as the use of the wireless medium requires additional management features and corresponding frame types to provide reliable data delivery service. Three frame types are employed to support the operations of the IEEE 802.11 protocol, namely, data frames, control frames, and management frames.

a. Data Frames

Data frames are used to transmit data from station to station. Data frames carry higher-level protocol data in the frame body. Different types of data frames exist,

depending on whether the frames are used for contention-based service or contention-free service[5]. As contention-free service is not widely implemented, this section will focus only on frames used for contention-based service. Table 6 lists the data frames used for contention-based service.

Frame Type	Carries Data?	Description
Data	Yes	Frames of the data sub-type are used solely for the purpose of moving the frame body from one station to another.
Null	No	Null frames are used by the stations to inform the access point of changes in power-saving status. The access point will then need to buffer frames for the station when the station sleeps.

Table 6. IEEE 802.11 Data Frames.

b. Control Frames

Control frames are used to administer access to the wireless medium. Control frames work in conjunction with data frames to provide reliable data delivery from station to station. Table 7 lists the control frames provided by the IEEE 802.11 protocol.

Frame Type	Function	Description
Request to Send (RTS)	Carrier sensing using CSMA/CA	An RTS frame is sent by a station whenever it has a unicast frame to transmit. The RTS frame serves to reserve the wireless medium for transmission, at the same time preventing any stations hearing the RTS frame from sending more frames.
Clear to Send (CTS)	Carrier sensing using CSMA/CA	A CTS frame is sent by the access point in response to an RTS. Similar to the RTS frame, the CTS frame serves to prevent any stations in the vicinty from sending more frames.
Acknowledgment (ACK)	Positive acknowlegment	ACK frames are used for the positive acknowledgment of any unicast frames sent in the wireless medium.
Power-Save Poll (PS-Poll)	Power savings option	When a station wakes from a power-saving mode, it sends a PS-Poll frame to the access point to retrieve any frames buffered for it when it was in power-saving mode.

Table 7. IEEE 802.11 Control Frames.

c. Management Frames

Management frames are used to perform supervisory functions, so as to facilitate a station's ability to gain access to a wireless network in order to send and

[5] IEEE 802.11 supports contention-based service and contention-free service. Contention-based service functions analogously to the traditional Ethernet's Carrier Sense Multiple Access with Collision Detection (CSMA/CD) [30], where stations need to compete for the shared medium in order to transmit data. (IEEE 802.11 uses Carrier Sense Multiple Access with Collision Avoidance, i.e., CSMA/CA, for this purpose.) Contention-free service, on the other hand, ensures that the medium is granted to a station for data transmission without any contention.

receive data. A station needs to go through a three-step procedure when it first initiates data transmission in a wireless network: first, the station needs to search for a compatible wireless network to use for access, i.e., scanning; next, the wireless network must authenticate the station intending to connect to the network, i.e., authentication; and finally, a station needs to be associated with an access point in order to start sending and receiving data on the wireless network, i.e., association. Table 8 describes the different management frames provided by the IEEE 802.11 protocol.

Frame Type	Function	Description
Beacon	Scanning	An access point uses beacon frames to announce the existence of the wireless network for which it serves. Beacon frames are transmitted at regular intervals to enable stations to find and identify a network, as well as to allow stations to configure the necessary parameters for joining the network.
Probe Request	Scanning	A station uses a probe request frame to scan an area for any existing wireless networks.
Probe Response	Scanning	An access point sends a probe response frame to respond to a probe request. The same access point that sends beacon frames is responsible for responding to probe requests.
Authentication	Authentication	A station exchanges authentication frames with an access point in order to authenticate itself to the access point.
Deauthentication	Authentication	A station uses deauthentication frames to terminate an existing authentication relationship with an access point.
Association Request	Association	After a station has identified a compatible network and authenticated itself to the network, it will attempt to join the network by sending an association request frame.
Association Response	Association	An access point checks the parameters in the received association request and verifies that they match the parameters of the network the access point is serving, before it responds with an association response.
Reassociation Request	Association	A station sends a reassociation request frame when it moves from one BSS to another BSS; or when it leaves the coverage area of an access point temporarily and rejoins later.
Reassociation Response	Association	An access point uses the reassociation response frame in reply to a reassociation request.
Disassociation	Association	A station uses a disassociation frame to terminate an existing association relationship with the access point.

Table 8. IEEE 802.11 Management Frames.

3. Operation of the IEEE 802.11 Protocol in Infrastructure Mode

The previous sections describe the network services and framing provided by the IEEE 802.11 protocol. It is now appropriate to summarize the rudiments of the IEEE 802.11 operation in infrastructure mode, illustrated in Figure 30.

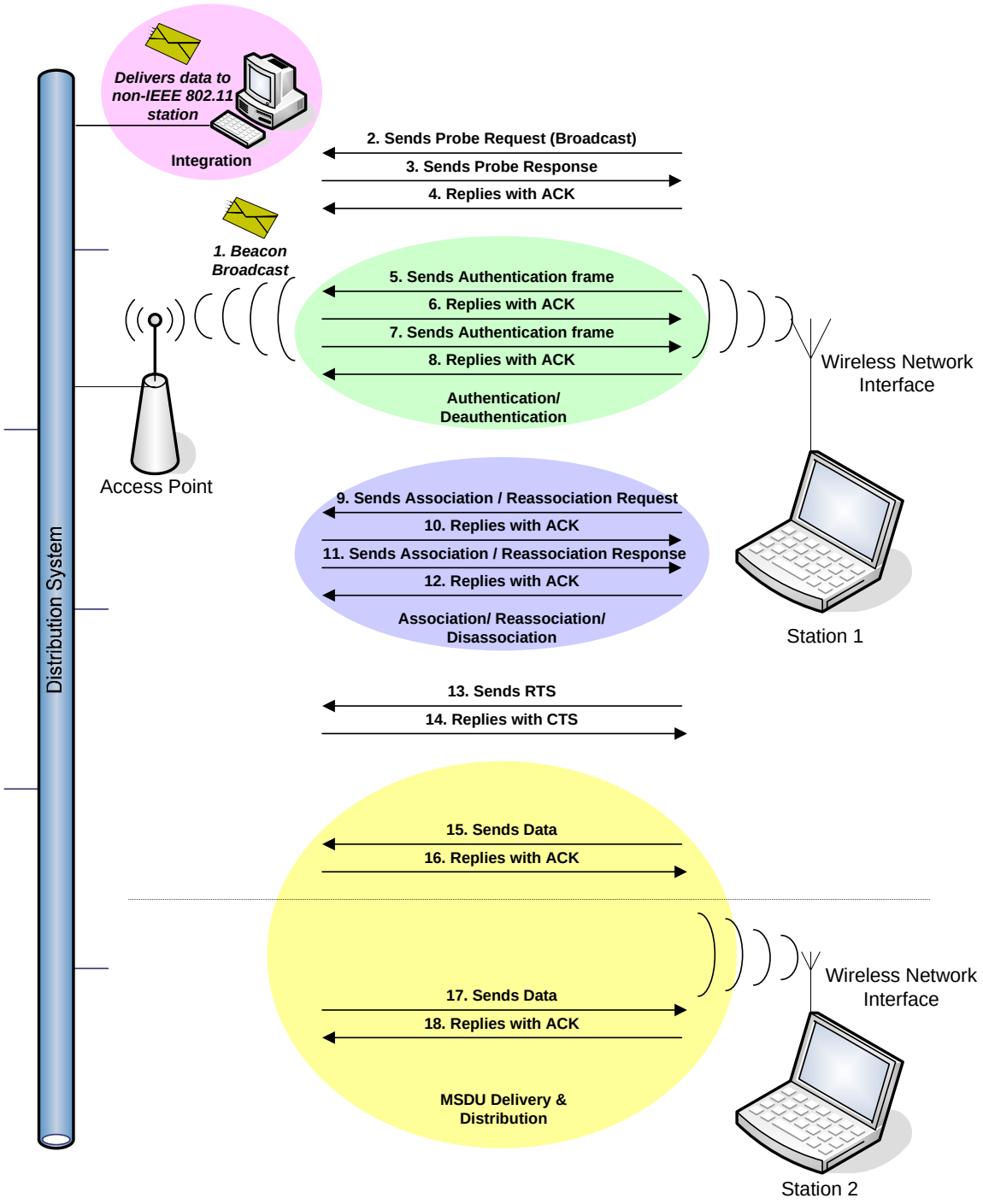


Figure 30. Operation of the IEEE 802.11 Protocol in Infrastructure Mode.

D. MOBILITY SUPPORT

As mentioned in the beginning of this chapter, wireless networking is often associated with mobility. Stations can move and remain connected to the wireless network, and they can transmit data while moving. Mobility can result in one of the three transition scenarios, namely, no transition, BSS transition, and ESS transition.

1. No Transition

When stations move within the same service coverage area offered by an access point, i.e., stations move within the same BSS, there is no need for any transition to take place, as stations will still be associated with the same access point.

2. BSS Transition

BSS transition occurs when a station moves from one BSS to another BSS within the same ESS. IEEE 802.11 provides link layer mobility, in which the station reassociates with the access point of the BSS it has moved to, before it continues to send and receive data. Figure 31 depicts a BSS transition.

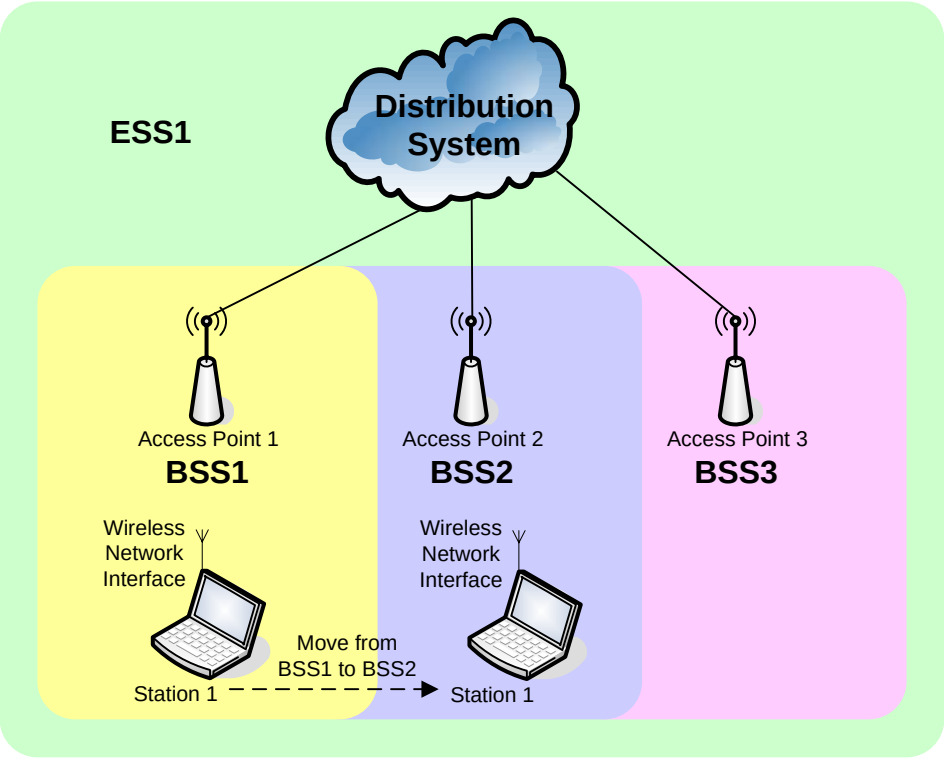


Figure 31. BSS Transition (After: Ref. [25]).

3. ESS Transition

ESS transition occurs when a station moves from one ESS to another; i.e., the station moves from one network to another. As IEEE 802.11 offers only link layer mobility, higher layer connections will be disrupted as a result of this move. Specifically, the move to a new network typically requires a station to obtain a new IP address as appropriate on the new, destination network. This is the scenario in which Mobile IP is required to offer network mobility, working hand-in-hand with the IEEE 802.11 link layer mobility to provide a seamless transition from one ESS to another ESS. Figure 32 shows such an ESS transition.

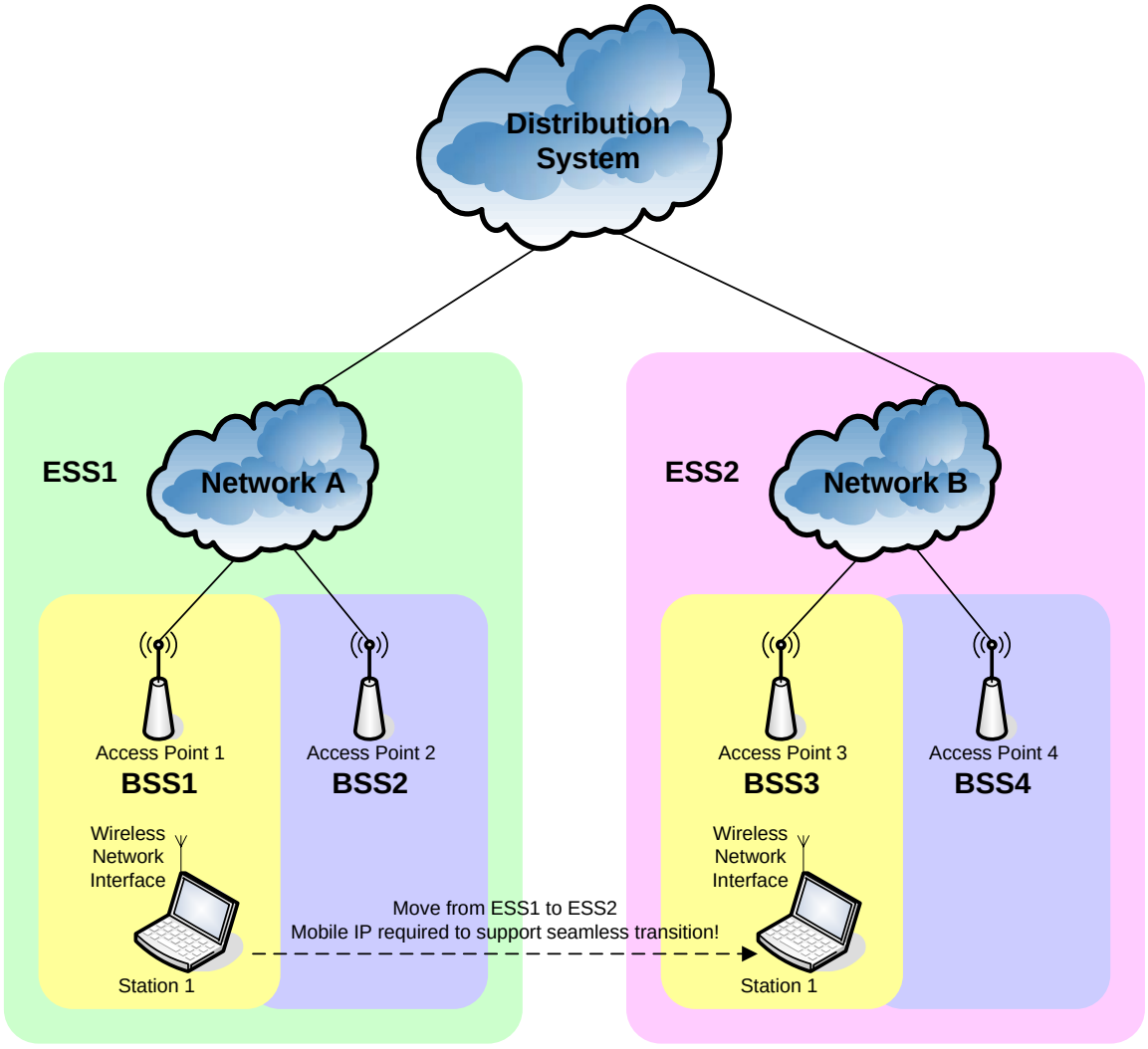


Figure 32. ESS Transition (After: Ref. [25]).

E. IEEE 802.11 LINK LAYER HANDOFF

The three different transition scenarios discussed in the previous section support the mobility of a station in a wireless environment. To continue data transmission in a new BSS—whether or not the station has also crossed an ESS boundary—the station will need to go through the process of scanning, authentication, and reassociation in the new destination BSS. This three-step process corresponds to a link layer handoff, in which the association of the station is transferred between access points. Figure 33 summarizes the exchanges corresponding to a link layer handoff.

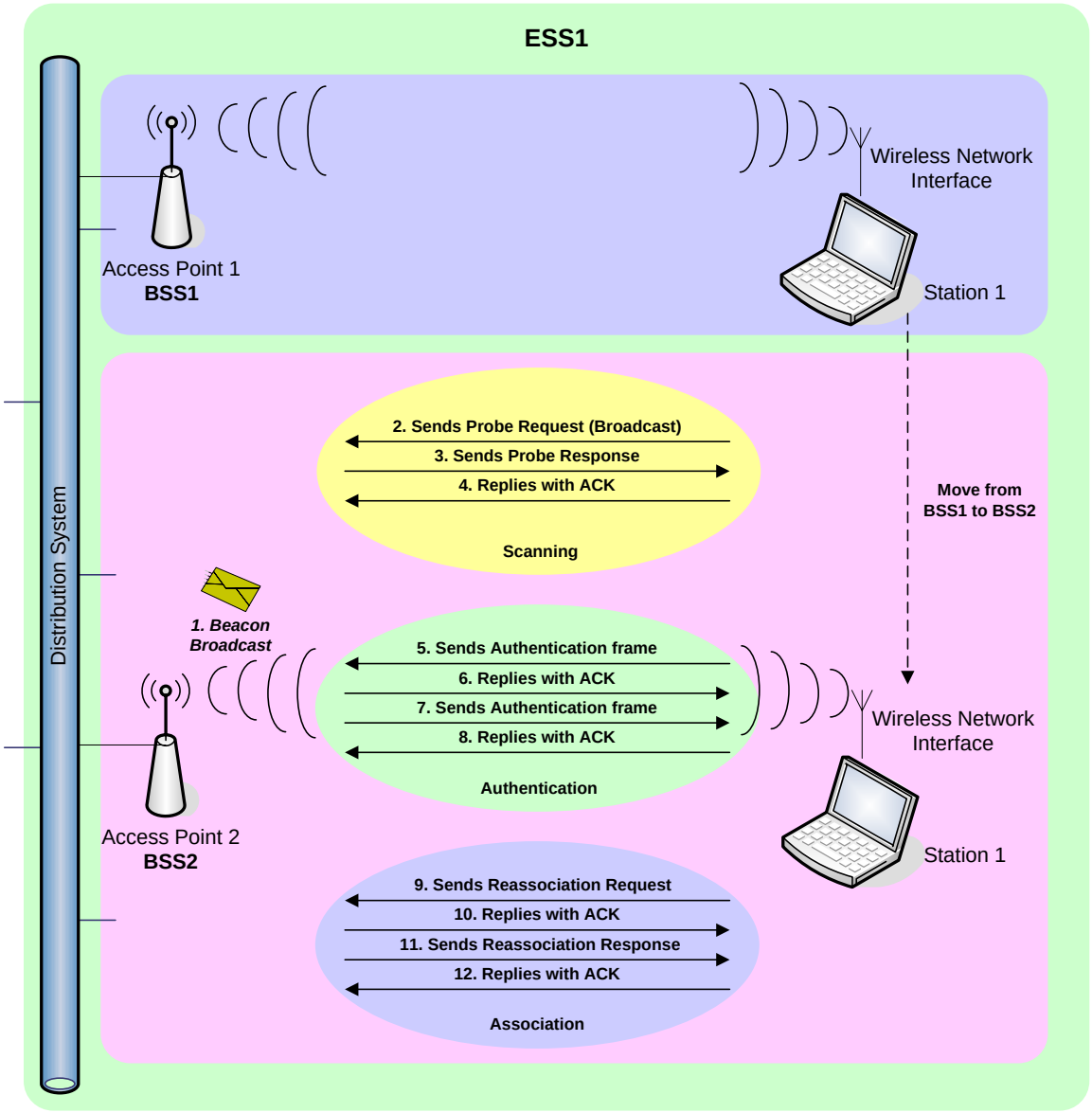


Figure 33. IEEE 802.11 Link Layer Handoff.

IV. SETTING UP THE MOBILE IP TEST ENVIRONMENT

A. INTRODUCTION

With an appreciation of the operations of the Mobile IP protocol and IEEE 802.11 nomenclature and network operations, this chapter will describe the considerations for devising a test setup to demonstrate the operations of Mobile IP version 4, to support the roaming of an IEEE 802.11 wirelessly connected host. The chapter will give an overview of the topological design, elaborating on the hardware and software requirements, along with any constraints and restrictions. After which, the chapter will briefly outline the test plan for collecting the performance statistics. Finally, the chapter will conclude by explaining the methodology for data collection and collation.

B. REFERENCE ARCHITECTURE

Setting up a Mobile IP environment that supports the roaming of an IEEE 802.11 wirelessly connected host entails two parts, namely, the Mobile IP network, and the IEEE 802.11 wireless network.

1. Considerations

It is the intent of this research to setup a controlled environment in order to collect performance statistics for the constituent components underlying the handoff mechanisms involved in the operation of Mobile IP. Statistics collected from this controlled environment will then be used as a nominal "best-case" benchmark. As such, it becomes crucial to architect a test setup that is as "clean" as possible. In order to minimize the introduction of unnecessary "noise" into the data, a minimalist configuration will be adopted. Thus, all unnecessary services will be turned off to preclude having their resource demands skew the data.

2. Setting up the IEEE 802.11 Wireless Network in Infrastructure Mode

a. Topological Design

Two ESSs will be configured in the wireless network to demonstrate an ESS transition, in which Mobile IP is required to provide the handoff. A single BSS will be setup within each ESS, so as to ensure that the BSS transition will also correspond to an ESS transition (i.e., there will be one BSS per ESS). This will minimize any potential

overhead that might otherwise result when a wireless mobile node encounters a BSS transition within an ESS, and then an ESS transition when it roams across to the next ESS. Put another way, a BSS transition will force an ESS transition as well.

Because of the close proximity of the entire setup, the ESS transition will be simulated by cutting off the power supply to one of the access points serving the BSS-ESS pair. This will "force" an ESS transition to take place, in which the mobile node will have to reassociate with the access point in the other BSS-ESS pair in order to continue its data transmission. Figure 34 illustrates such a wireless network that will be setup.

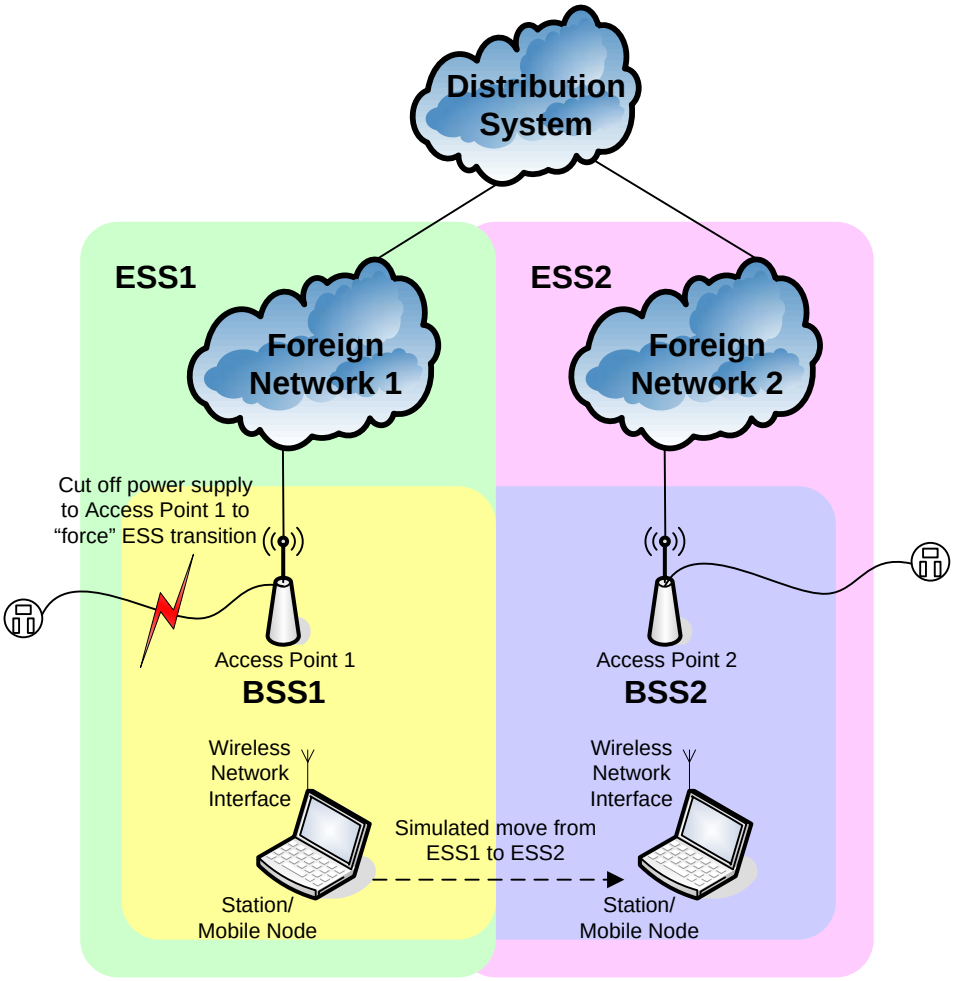


Figure 34. IEEE 802.11 Wireless Network in Devised Setup.

b. Network Service

Table 9 lists which wireless protocol services will (and will not) be utilized during the data collection. As previously mentioned, the intent will be to only involve essential services so as to collect the "best case" data.

Service	Configured? / Used?
Distribution	Yes
Integration	Yes
Association	Yes
Reassociation	Yes
Disassociation	No
Authentication	Yes, however, setup will use the open-system authentication option.
Deauthentication	No
Privacy	No
MSDU Delivery	Yes

Table 9. IEEE 802.11 Network Services Used for the Devised Setup.

c. Hardware and Software Requirements

Table 10 summarizes the list of hardware and software that will be required for setting up the IEEE 802.11 wireless network.

Component	Description
Hardware Requirements	
Access Point 1	Linksys Wireless Network Access Point (Model: WAP11 ver.2.2)
Access Point 2	Dell TrueMobile 1170 Wireless Base Station (Model: WLGW2011)
Wireless Network Interface	Cisco Aironet 340 series 11Mbps Wireless LAN Adapter (Model: AIR-PCM340)
Station / Mobile Node	Dell Latitude C640 laptop
Software Requirements	
Operating System for Station / Mobile Node	Microsoft Windows XP Professional Service Pack 2 (with driver support for Cisco Aironet 340 series 11Mbps Wireless LAN Adapter)

Table 10. Hardware and Software Requirements for IEEE 802.11 Wireless Setup.

3. Setting up the Mobile IP Version 4 Network

a. Topological Design

A home network and two foreign networks will be setup and interconnected to form a Mobile IP network. Each network is serviced by a router that is configured with the corresponding mobility agent service to function either as a home agent or foreign agent. A correspondent node will be connected to the home network,

maintaining ongoing communications with the mobile node in order to demonstrate the Mobile IP handoff process taking place while a mobile node is still in the process of exchanging data in a connection-oriented (TCP) communication session. Figure 35 depicts the Mobile IP network that will be setup.

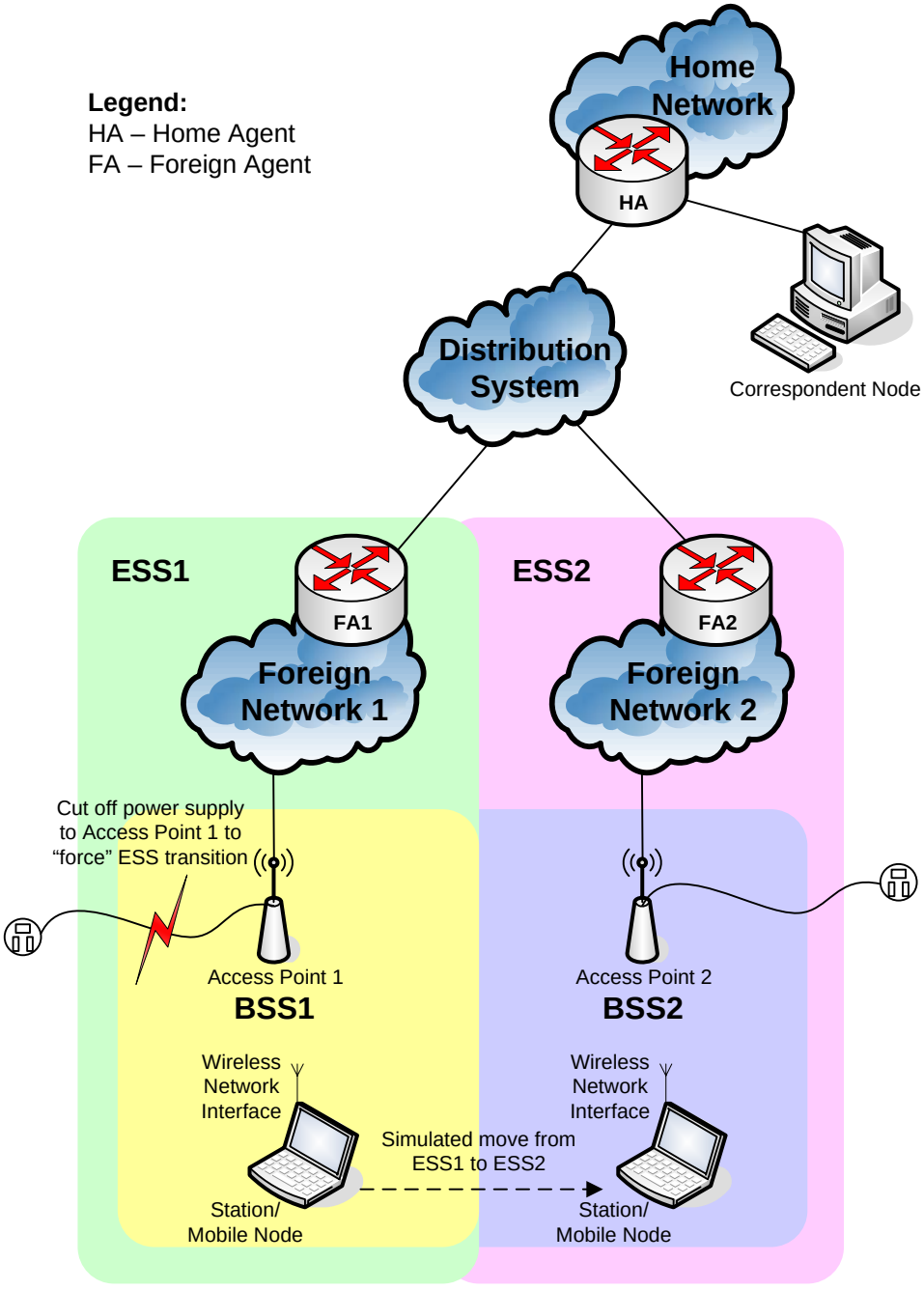


Figure 35. Mobile IP Version 4 Network in Devised Setup.

b. Network Services

To minimize any unnecessary network traffic and exchanges, services that are not required to support the collection of the performance statistics will be disabled. This includes the configuration of static routes to eliminate exchanges of routing information that take place when employing dynamic routing protocols. Table 11 summarizes the list of network services that will be configured / used for the Mobile IP network, along with their intended purpose.

Network Service	Purpose
Mobile IP Services	To configure the appropriate home agent or foreign agent services at the respective routers.
Static Routes	To enable a node to determine the path for data delivery from the source to destination. Static routes will be configured to minimize routing exchanges that result from the configuration of dynamic routing protocols.
DHCP Service	DHCP service is enabled at the home agent to dynamically assign an IP address for the mobile node when it is at its home network.
NTP Service	To synchronize the time among the home agent and foreign agents to facilitate Mobile IP registration, as well as data collation.

Table 11. Network Services Configured for the Mobile IP Version 4 Network of the Devised Setup.

c. Hardware and Software Requirements

The Mobile IP network will be setup using Cisco hardware and software. To fully support the operation of the Mobile IP protocol, the version of the Cisco Internetwork Operating System (IOS)[6] image that is used by the router has to meet specific software requirements [31]. Use of this version of the IOS image; however, places certain restrictions on the type of Cisco routers that can be deployed. Table 12 details the list of hardware and software requirements for the setup of the Mobile IP network.

[6] Cisco IOS image functions as the operating system for all Cisco routers.

Component	Description
Hardware Requirements	
Home Agent	Cisco 2621XM router with 128MB RAM and 32MB Flash
Foreign Agent 1	Cisco 2651XM router with 128MB RAM and 32MB Flash
Foreign Agent 2	Cisco 2651XM router with 128MB RAM and 32MB Flash
Distribution System	CentreCOM 100Base-Tx IEEE 802.3 12-port stackable hub (Model: MR912TX) to interconnect the 3 routers
Correspondent Node	Desktop computer with Ethernet network interface
Station / Mobile Node	Dell Latitude C640 laptop
Software Requirements	
Home Agent	Cisco IOS image for 2621XM router (with Advanced IP Services) version 12.4.1a
Foreign Agent 1	Cisco IOS image for 2651XM router (with Advanced IP Services) version 12.4.1a
Foreign Agent 2	Cisco IOS image for 2651XM router (with Advanced IP Services) version 12.4.1a
Correspondent Node	Operating System: Microsoft Windows 2000 Professional Service Pack 4 Tools/Utilities: Netcat listener (for data transfer via TCP)
Station / Mobile Node	Operating System: Microsoft Windows XP Professional Service Pack 2 Tools/Utilities: Netcat (for data transfer via TCP) Mobile Node Software: Cisco Mobile Client version 2.0.14

Table 12. Hardware and Software Requirements for the Mobile IP Network Setup.

C. TEST PLAN

After establishing the reference architecture for setting up the Mobile IP test environment, this section will deal with the considerations for coming up with the appropriate test cases to collect the performance statistics corresponding to the Mobile IP handoff process.

1. Traffic Considerations

There are three main types of application traffic that are carried by IP, namely, data, voice and video. Supporting the transmission of relatively inelastic (gaps in delivery are problematic) voice and video traffic over IP demands much more performance from the underlying network than does the transmission of elastic static data (e.g., textual files or single photos). Quality of Service (QoS) [32] mechanisms are required to guarantee a certain throughput level such that the voice and video traffic can be transmitted within an acceptable amount of network delay and packet loss.

Adopting a minimalist configuration would provide the necessary quality of service that is required to support voice and video traffic, since the network bandwidth in

this setup would be solely dedicated to the test traffic whose performance statistics are being measured. Considering that most voice and video traffic is carried over UDP (i.e., a connectionless protocol that has no notion of "maintaining a session") [33], a decision is necessary regarding what type of traffic to use during testing. One obvious option is to test with streaming data that employs a connectionless protocol (i.e., employs UDP). The competing option is to test with non-streaming data that employs a connection-oriented protocol (i.e., employs TCP). The latter will be chosen as it places a more "stringent" demand on the network layer to maintain a session, and is thus the better choice for conducting the Mobile IP handoff test cases. In order to demonstrate that session continuity is maintained when a mobile node roams from one network to another network, data will be transmitted via an established TCP session using netcat. The correspondent node will initiate a netcat listener on TCP, and the mobile node will transmit a large file over the established TCP session while roaming from one network to the other network[7].

2. Mobile IP Handoff Considerations

As described in Chapter 2, there are three scenarios in which a Mobile IP handoff can take place; namely, when a mobile node leaves its home network, when a mobile node roams from one foreign network to another foreign network, and when a mobile node returns to its home network. Since the Mobile IP setup will be configured based on the Cisco IOS mobility services and Cisco Mobile Client software, the products' features will have to be taken into consideration when determining the handoff scenarios that can be implemented in this setup.

a. Cisco IOS Mobility Services

Cisco IOS mobility services support configuration for two types of home networks: physical home networks and virtual home networks [5]. A physical home network allows a mobile node to attach itself directly to the home network; in which case, all Mobile IP functionality for the mobile node will become inactive, and IP traffic will be delivered via the normal routing mechanisms. The disadvantage with the use of the

[7] In theory, the Mobile IP handoff performance results should be identical regardless of whether the correspondent node or the mobile node initiates the data transfer. It is recommended however, that collecting the handoff performance results for the scenario where the correspondent node initiates the data transfer to the mobile node be considered as an area for future research.

physical home network is that the mobile node will not be able to register with the home agent if the home agent's network interface serving the physical home network is down.

A virtual home network is analogous to a loopback interface, in which a virtual network will always be available and not susceptible to any physical failures. Virtual home networks are used in the scenario in which the mobile nodes will never be physically connected to the home networks. Thus, use of a virtual home network implies that a mobile node will only roam from foreign network to foreign network, without the need for it to return to its home network.

b. Cisco Mobile Client Software

Based on the default configuration of the Cisco Mobile Client software [34], mobility services would still be enabled when a mobile node is connected to its home network. In this scenario, the mobile node will attempt to register itself with the home agent using a co-located care-of address, issued by the DHCP service that is configured at the home network. Thus, use of the default configuration supports the use of virtual home network, where the mobile node at its home network is treated just like any other foreign network, except that a co-located care-of address is used in place of a foreign agent's care-of address.

To disable all mobility services when the mobile node is connected to its home network, the Cisco Mobile Client software offers a "pass-through" mode, in which the mobile node will use a DHCP-advertised item to detect that it has returned to its home network. In this scenario, the mobile node will initiate a de-registration process with its home agent, and obtain an IP address assigned by the home network's DHCP service. The Cisco Mobile Client will cease to participate in the delivery of IP traffic, handing over the responsibility to the mobile node's underlying operating system. As a result, session continuity will break with the change in IP address. The pass-through mode is typically used in circumstances in which triangle routing and tunneling are not desired. Thus, use of the pass-through mode work hand-in-hand with the notion of physical home network; the only disadvantage being the disruption in session continuity when a mobile node roams away from home, and when a mobile node returns home.

c. Mobile IP Handoff Test Cases

With the considerations of the product features and resulting constraints described in the previous sections and summarized in Figure 36, the test cases that will be adopted for the purpose of this research will correspond to the scenario when a mobile node roams from one foreign network to another foreign network. The scenarios when a mobile node roams away from home and when it returns home will not be used, as the way in which these are implemented deviate from RFC 3344's recommendation [4].

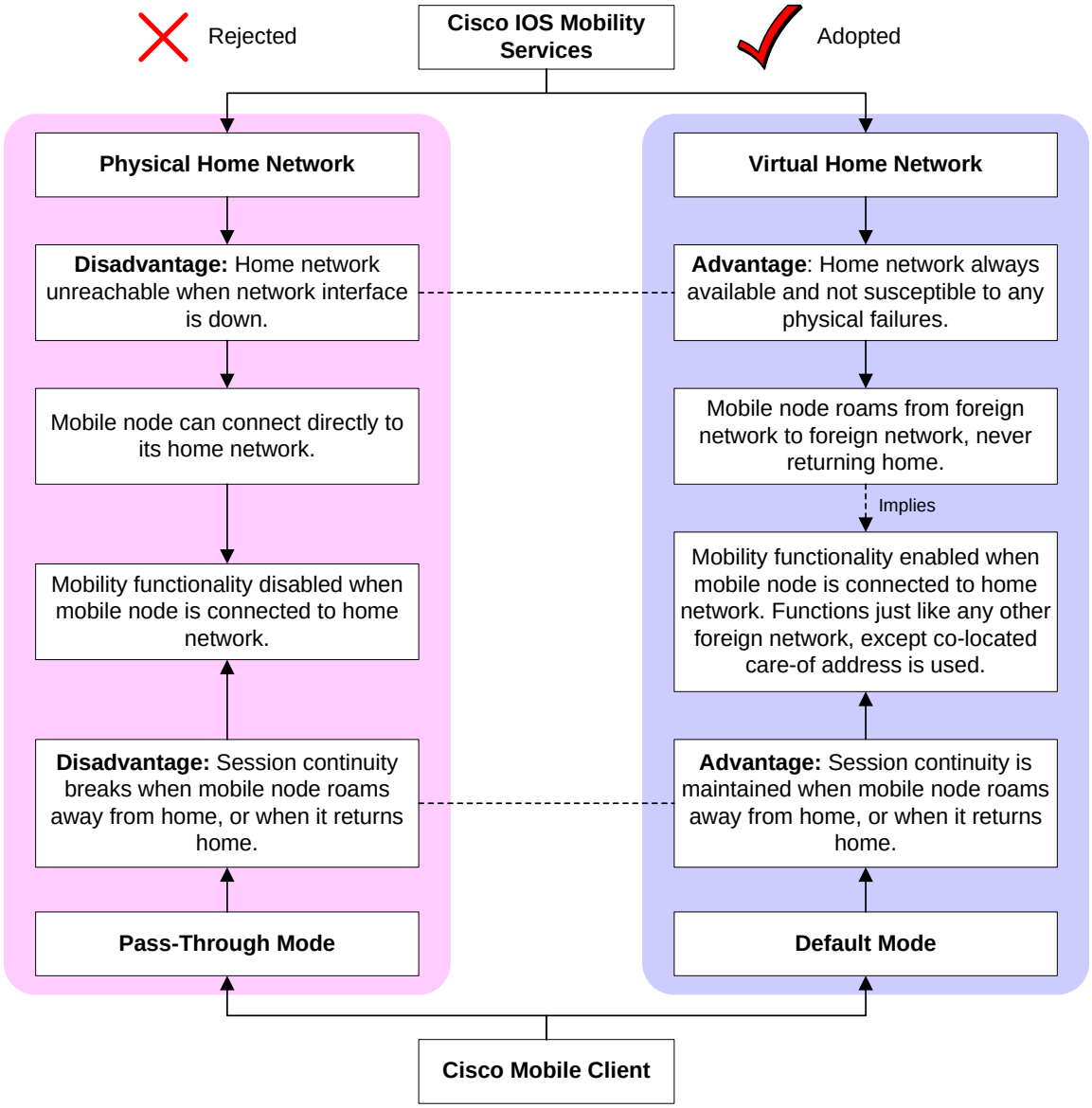
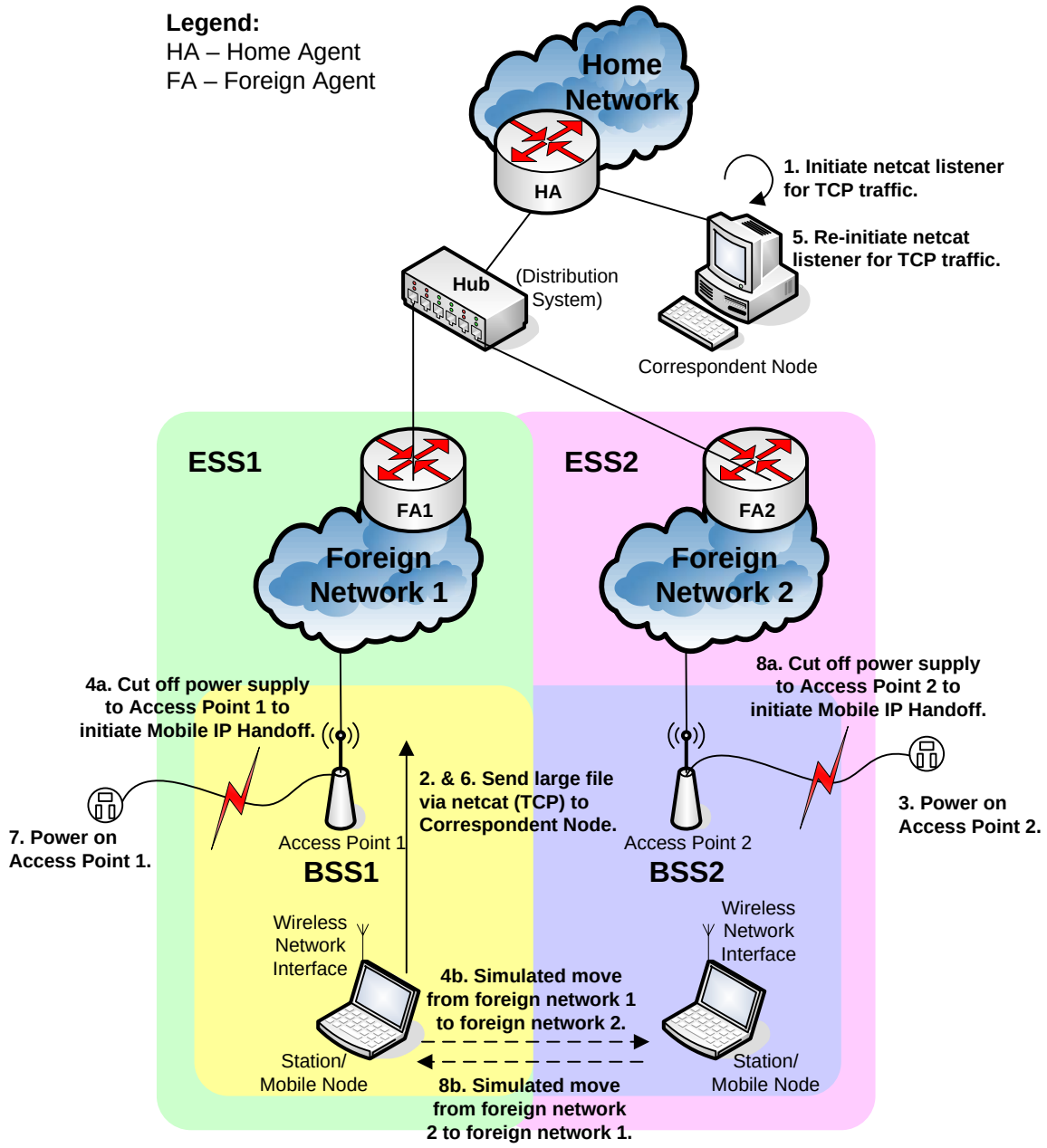


Figure 36. Considerations Underlying the Use of Cisco Mobile IP Products.

Figure 37 illustrates the test procedure for carrying out the Mobile IP handoff test cases, in which a set of measurements will be taken for the handoff occurring when the mobile node roams from foreign network 1 to foreign network 2; and another set of measurements taken for the handoff occurring when the mobile node roams from foreign network 2 to foreign network 1.



Notes:
Steps 1 to 4 correspond to roaming from foreign network 1 to foreign network 2.
Steps 5 to 8 correspond to roaming from foreign network 2 to foreign network 1.

Figure 37. Mobile IP Handoff Test Procedure.

3. Care-of Address Considerations

As highlighted in Chapter 2, Mobile IP supports two types of care-of address: foreign agent care-of address, and co-located care-of address. The Cisco Mobile Client software offers support for these two types of care-of address [34]. Table 13 outlines the considerations and usage scenarios for the different care-of addresses.

Care-of Address	Usage Scenario	Adopted in Test Case?
Co-located Care-of Address	1. Used in the default mode when a mobile node attempts registration with its home agent when it is at its home network. IP address issued by the DHCP service configured on the home network is used as the co-located care-of address.	1. No, test cases are based on the scenario when a mobile node roams from one foreign network to another foreign network.
	2. Used in a foreign network, in which DHCP service is enabled, and a foreign agent is present. The mobile node will register its DHCP-assigned address as the co-located care-of address with the foreign agent.	2. No, use of co-located care-of address still requires the presence of a foreign agent.
	3. Used in a foreign network where no foreign agent is present. Co-located care-of address is configured statically using a locally routable address.	3. No, co-located care-of address has to be pre-configured. Session continuity will break when mobile node roams from network to network.
Foreign Agent Care-of Address	Used in the scenario in which a foreign agent is present in the network where the mobile node is visiting.	Yes

Table 13. Considerations and Usage Scenarios for Care-of Addresses.

D. DATA COLLECTION AND COLLATION METHODOLOGY

Upon identifying the test cases and outlining the test procedure, data collection and collation is the next process that must take place in order to gather the performance statistics for the Mobile IP handoff process.

1. Candidates for Data Collection

As mentioned in Chapter 2, a change in routing to facilitate the continued delivery of IP traffic to the mobile node is considered a Mobile IP handoff; the process involves move detection using agent discovery, registration, and updating of the routing information. In addition to using agent discovery to detect that the mobile node has moved, RFC 3344 [4] states that

> The mobile node MAY use link-layer mechanisms to decide that its point of attachment has changed.

The specific link-layer technology that is appropriate in this context will be the IEEE 802.11 wireless link-layer handoff mechanism that was described in Chapter 3. Integrating the link-layer handoff mechanism with the Mobile IP handoff mechanism, Figure 38 illustrates the constituent components corresponding to the handoff process that is required to facilitate an IEEE 802.11 wirelessly connected host to roam from one network to another network.

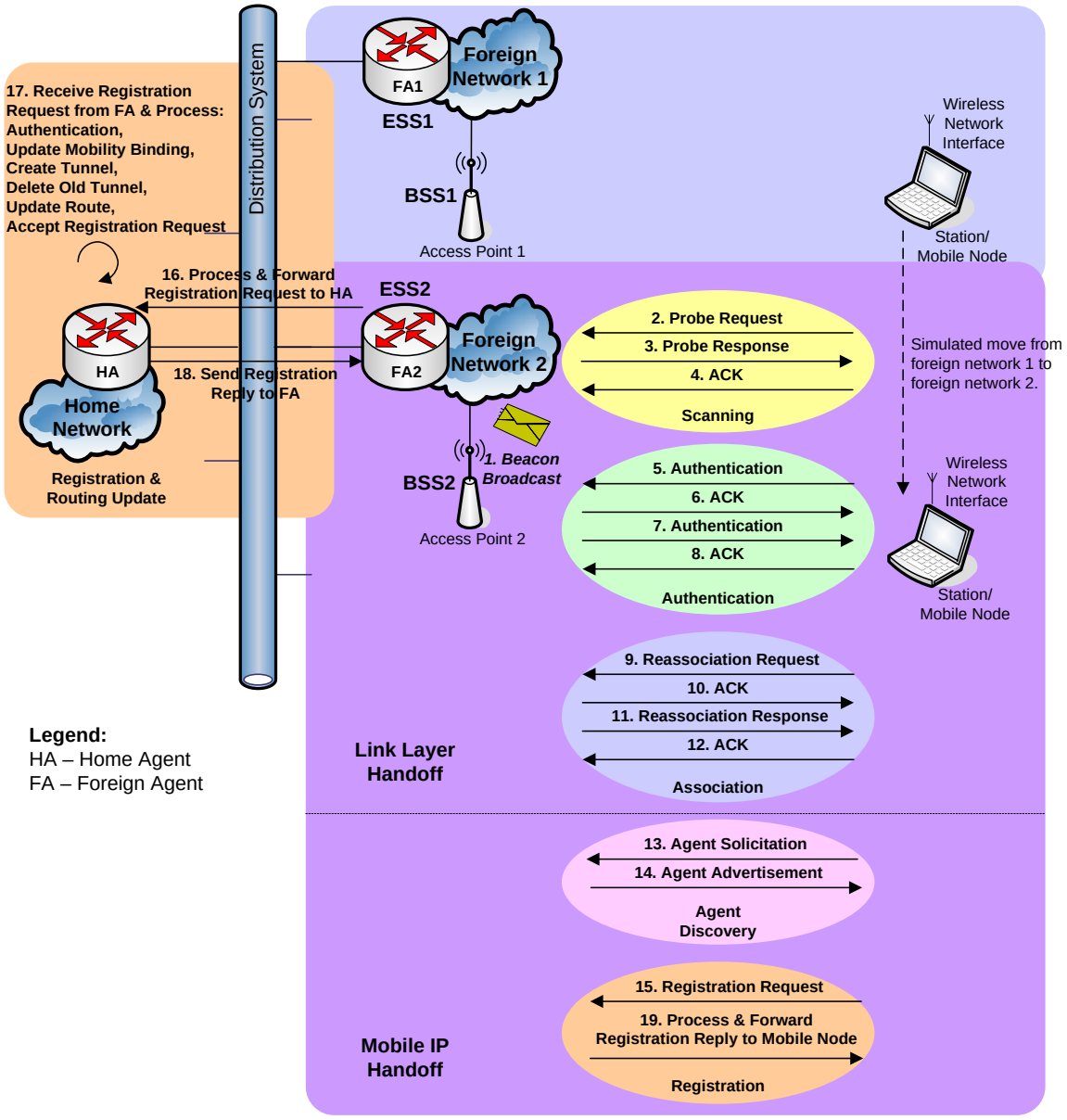


Figure 38. Constituent Components for the Mobile IP Handoff Process.

2. Data Collection Instrumentation

To facilitate the data collection process, the reference architecture derived in the earlier section of this chapter was instrumented to include strategic points for data collection. Figure 39 depicts the resulting instrumented setup, with Table 14 detailing the list of hardware and software that is required to support the data collection process. The detailed component configuration for the instrumented setup can be found in Appendix A of this report.

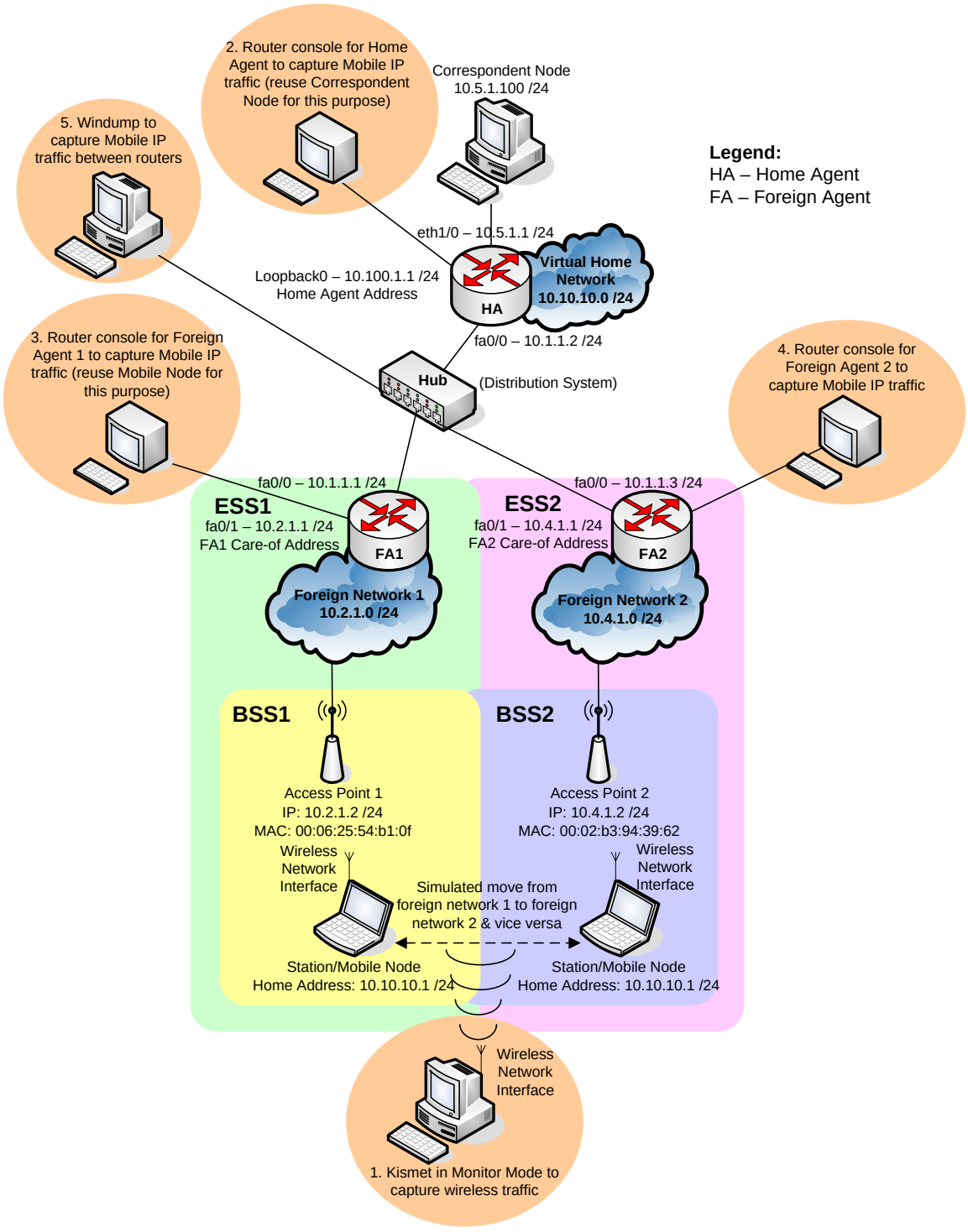


Figure 39. Mobile IP Setup with Data Collection Points.

Hardware	Software	Purpose
Desktop computer with wireless network interface (in monitor mode)	Kismet	To capture wireless traffic.
Desktop computer (reuse Correspondent Node)	Hyper Terminal for router console	To capture Mobile IP traffic processed by the Home Agent.
Laptop computer (reuse Mobile Node)	Hyper Terminal for router console	To capture Mobile IP traffic processed by Foreign Agent 1.
Laptop computer	Hyper Terminal for router console	To capture Mobile IP traffic processed by Foreign Agent 2.
Desktop computer with Ethernet network interface	Windump	To capture Mobile IP traffic exchanged among the 3 routers.

Table 14. Hardware and Software Requirements for Data Collection.

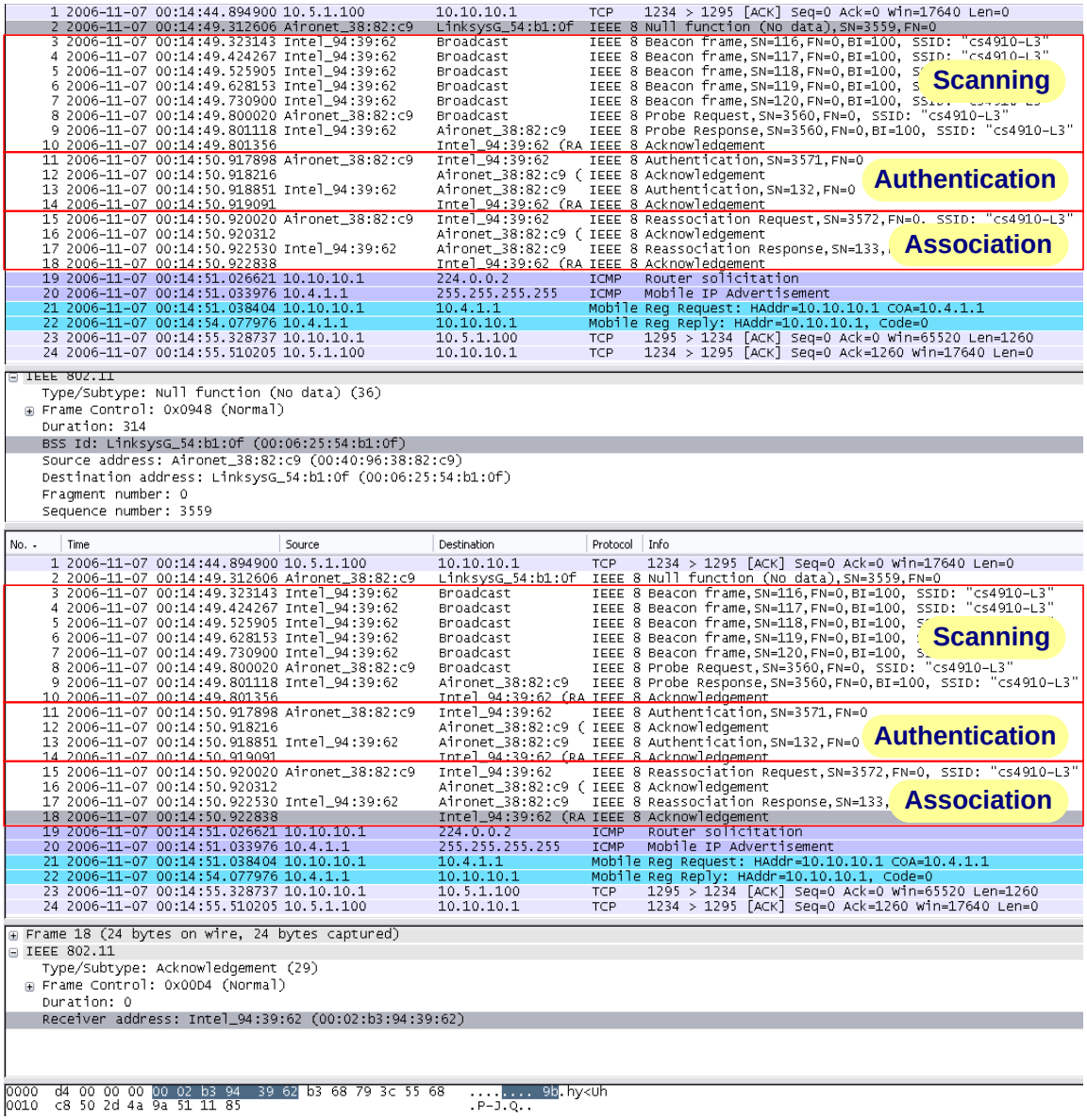
3. Data Collation

Having collected the data using the instrumented setup described in the previous section, data collation must take place in order to assimilate the data that was collected from the different sources. This section will describe the specific information that will be collected from the various data collection points, and the methodology for collating all the information to derive the performance statistics corresponding to the constituent components underlying the Mobile IP handoff process.

a. Kismet

Kismet [35] plays a crucial role in the entire data collection process. The IEEE 802.11 wireless traffic captured by Kismet will enable one to delineate the link layer handoff components from the Mobile IP handoff components. The Kismet output gives a rough order of magnitude for the time taken for the Mobile IP registration process. The identification field in the captured registration request and reply message is then used to index into the corresponding home agent and foreign agent router debug logs to provide a finer resolution in the processing of the registration request and reply message by the respective routers. Figure 40 shows the information that can be derived from the Kismet output[8], along with the methodology for computing the performance statistics corresponding to the constituent components.

[8] Wireshark Network Protocol Analyzer [36] was used to analyze the dump file captured by Kismet.

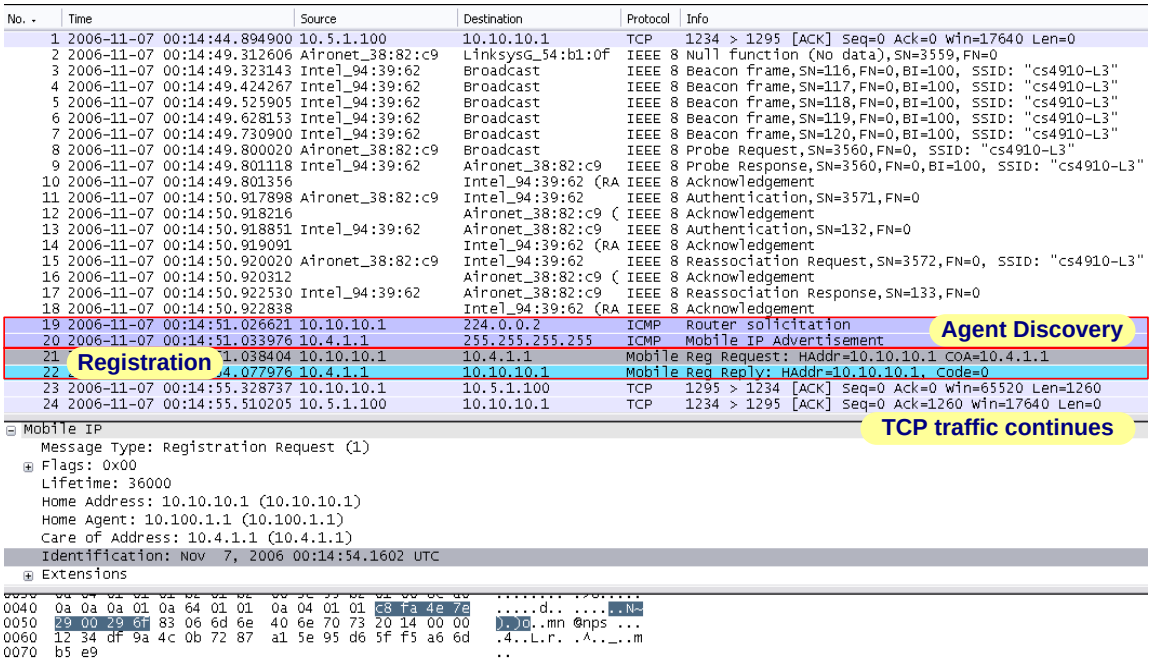


Frame 2 corresponds to the last frame sent by Access Point 1 (i.e., BSS ID: 00:06:25:54:b1:0f) prior to power shutdown. Due to the close proximity of the setup, the last frame received by the wireless mobile node from Access Point 1 (in a real-world scenario) can be assumed to be the same as the last frame transmitted by Access Point 1 prior to power shutdown. The time taken for the constituent components of the link-layer handoff is thus given by:

Scanning = Time at Frame 10 – Time at Frame 2

Authentication = Time at Frame 14 – Time at Frame 10

Association = Time at Frame 18 – Time at Frame 14



Frame 19 to frame 20 correspond to move detection using agent discovery. Frame 21 to frame 22 correspond to the Mobile IP registration process. Value in the Identification field of the registration request / reply message is used to index into the respective home agent and foreign agent router debug logs to provide a finer resolution of the registration process. The time taken for the constituent components of the Mobile IP handoff is thus given by:

Move Detection using Agent Discovery = Time at Frame 21 – Time at Frame 18

The time taken for the registration process and update in routing information is derived from the data collated at the router logs.

Figure 40. Information Derived from Kismet Output.

b. Router Debug Log

In order to capture the Mobile IP traffic that is processed by the home agent and foreign agent, the routers' debug mode for Mobile IP traffic will need to be enabled. The debug traffic that will be generated can then be logged using Hyper Terminal's screen capture function.

Each handoff test case requires the data collation from two router logs; namely, the home agent router log, and the foreign agent router log. The specific foreign agent router log to use depends on whether the mobile node is roaming from foreign network 1 to foreign network 2, or from foreign network 2 to foreign network 1. If the mobile node is roaming from foreign network 1 to foreign network 2, the appropriate foreign agent router log to examine will be that of foreign agent 2's router log, since the mobile node will initiate the registration process with its home agent via foreign agent 2. Likewise logic can be applied when the mobile node roams from foreign network 2 to

foreign network 1. Figure 41 displays the collated router log for both the home agent and foreign agent when the mobile node roams from foreign network 1 to foreign network 2.

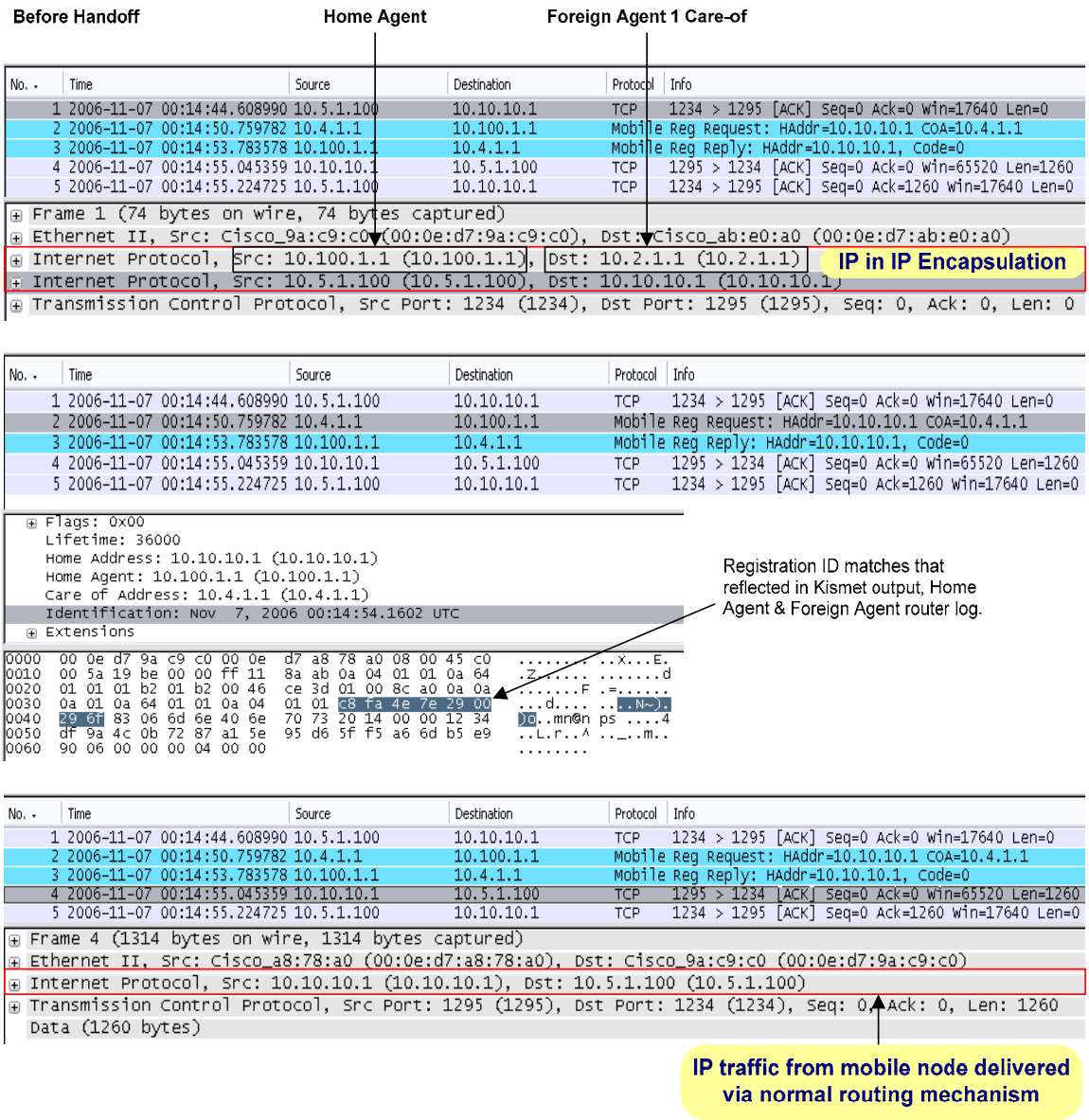
```
Router Debug Log of Foreign Agent 2
Nov  7 00:14:49.705: MobileIP: ParseRegExt type NAI(131) addr 7C53ECC end 7C53EEA
Nov  7 00:14:49.705: MobileIP: ParseRegExt skipping 6 to next
Nov  7 00:14:49.705: MobileIP: ParseRegExt type MHAE(32) addr 7C53ED4 end 7C53EEA
Nov  7 00:14:49.705: MobileIP: ParseRegExt skipping 20 to next
Nov  7 00:14:49.705: MobileIP: FA rcv registration for MN mn@nps on FastEthernet0/1 using COA
10.4.1.1 HA 10.100.1.1 lifetime 36000 options sbdmg-t- identification C8FA4E7E2900296F
Nov  7 00:14:49.705: MobileIP: Registration request byte count = 82
Nov  7 00:14:49.709: MobileIP: FA queued MN mn@nps in register table
Nov  7 00:14:49.709: MobileIP: Visitor registration timer started for MN mn@nps, lifetime 7
Nov  7 00:14:49.709: MobileIP:  Adding UDP Tunnel req extension
Nov  7 00:14:49.709: MobileIP: FA forwarded registration for MN mn@nps to HA 10.100.1.1

Router Debug Log of Home Agent
Nov  7 00:14:49.715: MobileIP: HA 158 rcv registration for MN mn@nps on FastEthernet0/0 using
HomeAddr 10.10.10.1 COA 10.4.1.1 HA 10.100.1.1 lifetime 36000 options sbdmg-t- identification
C8FA4E7E2900296F
Nov  7 00:14:49.715: MobileIP: NAT not detected SRC:10.4.1.1 COA: 10.4.1.1
Nov  7 00:14:49.715: MobileIP: UDP Tunneling not enabled
Nov  7 00:14:49.715: MobileIP: Authenticating MN mn@nps using SPI 1234
Nov  7 00:14:49.715: MobileIP: Authentication algorithm HMAC-MD5 and 16 byte key
Nov  7 00:14:49.715: MobileIP: Authentication algorithm HMAC-MD5 and truncated key
Nov  7 00:14:49.719: MobileIP: Authentication algorithm HMAC-MD5 and 16 byte key
Nov  7 00:14:49.719: MobileIP: Authenticated MN mn@nps using SPI 1234 and 16 byte key
Nov  7 00:14:49.719: MobileIP: Name for local pool is mn@nps
Nov  7 00:14:49.719: MobileIP: Flow 10.10.10.1 already exists
Nov  7 00:14:49.719: MobileIP: Route opt bindupdate entry not created: No SA for 10.2.1.1
Nov  7 00:14:49.719: MobileIP: Mobility binding for MN mn@nps updated - tunnel changed
Nov  7 00:14:49.723: MobileIP: Tunnel0 (IP/IP) created with src 10.100.1.1 dst 10.4.1.1
Nov  7 00:14:49.723: MobileIP: MN mn@nps Delete tunnel route 10.10.10.1/255.255.255.255 via gateway
10.2.1.1
Nov  7 00:14:49.723: MobileIP: Deleted Tunnel1 src 10.100.1.1 dest 10.2.1.1
Nov  7 00:14:49.727: MobileIP: MN mn@nps Insert route for 10.10.10.1/255.255.255.255 via gateway
10.4.1.1 on Tunnel0
Nov  7 00:14:49.731: MobileIP: Stopping LineProtoTimer for Tunnel0
Nov  7 00:14:49.731: MobileIP: swif coming up Tunnel0
Nov  7 00:14:52.731: MobileIP: Roam timer started for MN mn@nps using 10.10.10.1, lifetime 36000
Nov  7 00:14:52.731: MobileIP: HA accepts registration from MN mn@nps
Nov  7 00:14:52.731: MobileIP: Dynamic and Static Network Extension Length 0 - 0
Nov  7 00:14:52.731: MobileIP: Composed mobile network extension length:0
Nov  7 00:14:52.731: MobileIP: Authentication algorithm HMAC-MD5 and 16 byte key
Nov  7 00:14:52.731: MobileIP: MN mn@nps MHAE added to MN mn@nps using SPI 1234
Nov  7 00:14:52.731: MobileIP: MN mn@nps - HA sent reply to 10.4.1.1

Router Debug Log of Foreign Agent 2
Nov  7 00:14:52.734: MobileIP: ParseRegExt type NAI(131) addr 7C53108 end 7C5312E
Nov  7 00:14:52.734: MobileIP: ParseRegExt skipping 6 to next
Nov  7 00:14:52.734: MobileIP: ParseRegExt type MHAE(32) addr 7C53110 end 7C5312E
Nov  7 00:14:52.734: MobileIP: ParseRegExt skipping 20 to next
Nov  7 00:14:52.734: MobileIP: ParseRegExt type UDPTUNREPE(44) addr 7C53126 end 7C5312E
Nov  7 00:14:52.734: Parsing UDP Tunnel Reply Extension - length 6
Nov  7 00:14:52.734: MobileIP: ParseRegExt skipping 6 to next
Nov  7 00:14:52.738: MobileIP: FA rcv accept (0) reply for MN mn@nps on FastEthernet0/0 using HA
10.100.1.1 lifetime 36000
Nov  7 00:14:52.738: MobileIP: Update visitor table for MN mn@nps
Nov  7 00:14:52.738: MobileIP: FA route add 10.10.10.1 successful. Code = 0
Nov  7 00:14:52.738: MobileIP: Visitor timer started for MN mn@nps, lifetime 36000
Nov  7 00:14:52.738: MobileIP: Reply in for MN mn@nps using 10.10.10.1, accepted
Nov  7 00:14:52.738: MobileIP: registration reply byte count = 78
Nov  7 00:14:52.738: MobileIP: FA forwarding reply to MN mn@nps (10.10.10.1 mac 0040.9638.82c9)
Nov  7 00:14:52.742: MobileIP: FA dequeued MN mn@nps from register table
```

Registration ID in both router logs matches that reflected in the Kismet output, i.e., C8 FA 4E 7E 29 00 29 6F.

Figure 41. Collated Router Logs for Home Agent and Foreign Agent.

c. Windump

Windump [37] is used to capture traffic that is exchanged among the home agent and foreign agents. Windump plays a passive role in the data collection process. It serves to validate the exchange of registration request and reply messages that occurred between the home agent and foreign agent. In addition, the output from Windump[9] will demonstrate that IP traffic destined for the mobile node is indeed tunneled by the home agent to the foreign agent's care-of address. IP traffic originating from the mobile node is delivered via normal routing mechanisms, as illustrated in Figure 42.



[9] Wireshark Network Protocol Analyzer [36] was used to analyze the dump file captured by Windump.

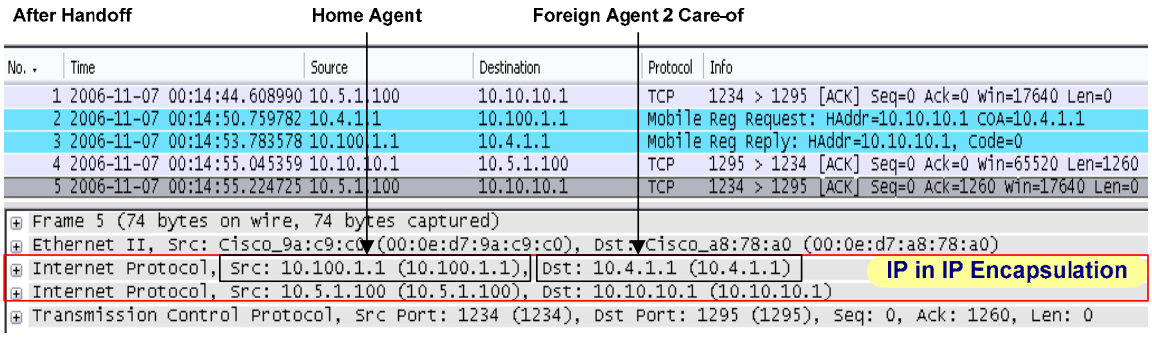


Figure 42. Windump Output.

4. Putting Everything Together

With the knowledge of how the performance statistics for the constituent components corresponding to the handoff process will be measured, Figure 43 summarizes the data collection and collation methodology that will be adopted for the purpose of this research.

As indicated in Figure 43, there is an inherent limitation in which the time of transmission from the mobile node to the foreign agent; and the time of transmission from the foreign agent back to the mobile node, could not be measured using the existing instrumentation. Since transmission of the RF signal travels approximately at the speed of light, subjected to some variability with temperature, pressure and humidity conditions and the distances are very short (several meters at most), the time of transmission for these two scenarios is negligible and will be ignored when computing the performance statistics for the Mobile IP handoff process.

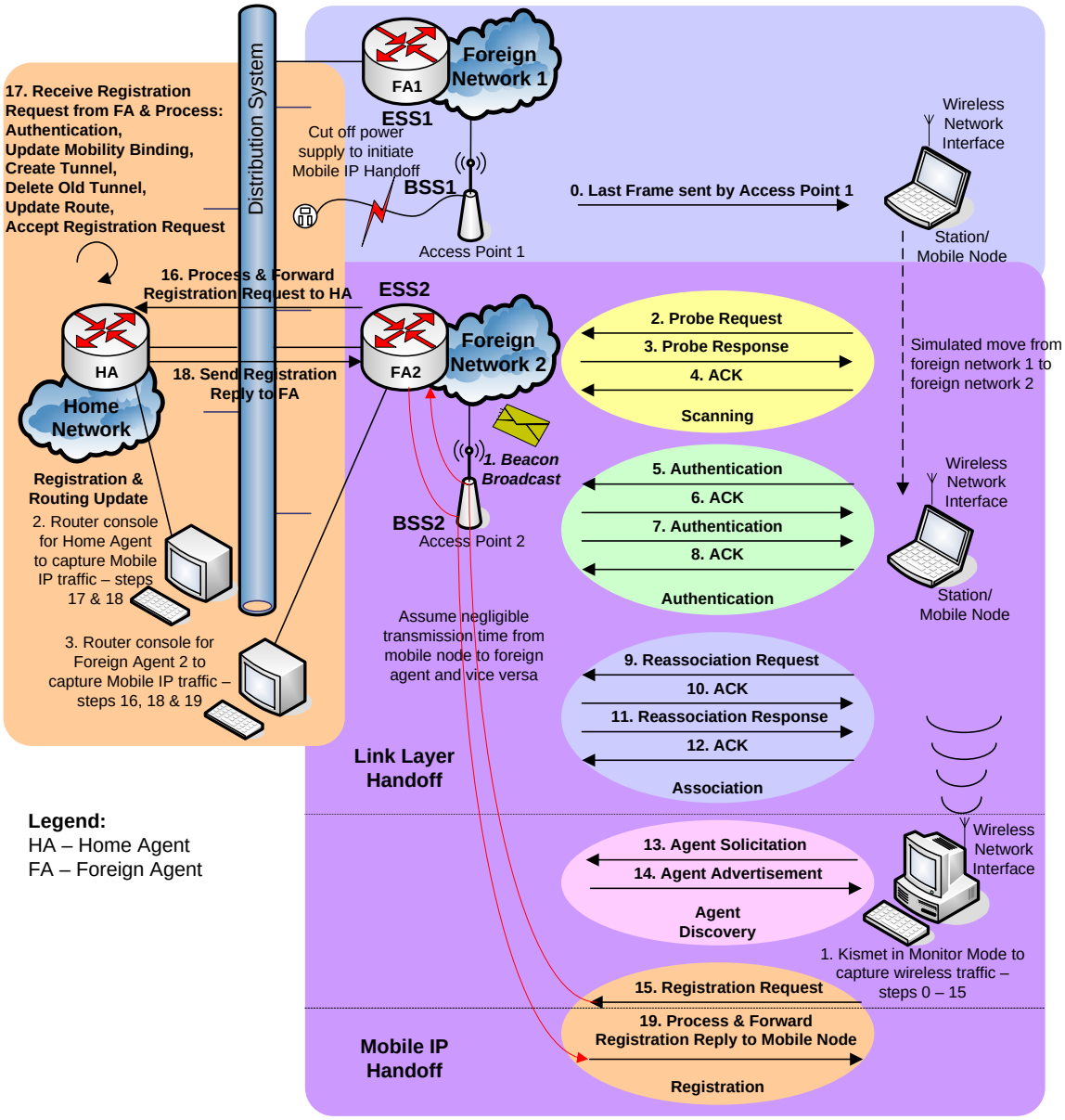


Figure 43. Summary of the Data Collection and Collation Methodology.

THIS PAGE INTENTIONALLY LEFT BLANK

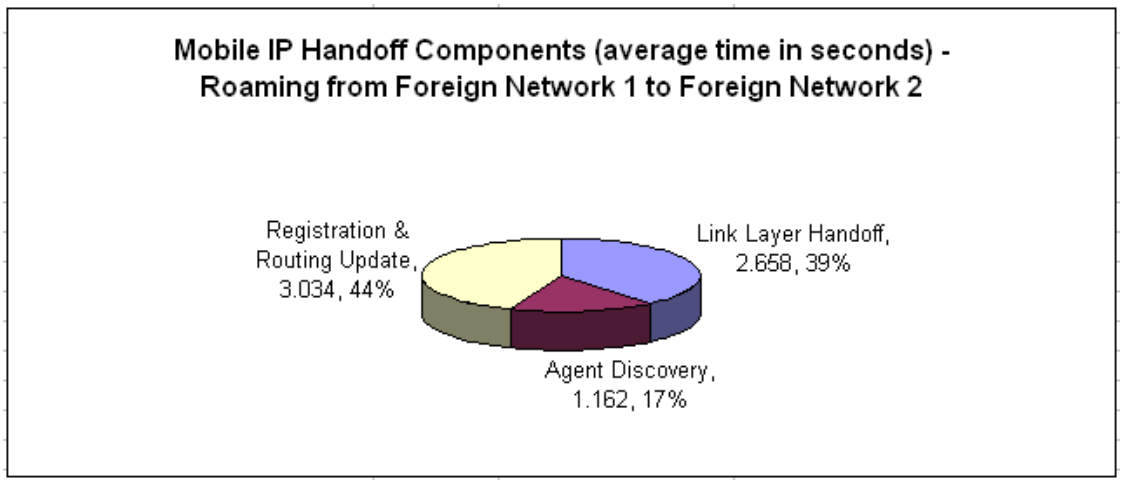
V. RESULTS AND FINDINGS

A. INTRODUCTION

Using the Mobile IP test setup and data collection and collation methodology described in Chapter 4, a total of 63 test cases were carried out to gather the performance statistics relating to the Mobile IP handoff process. The chapter will present a summary of the performance statistics that were derived for the constituent components underlying the Mobile IP handoff process. After which, we will give an analysis of the results obtained and recommend the types of applications that Mobile IP can support. Finally, we conclude the chapter by briefly discussing the components of the handoff process that can potentially be exploited by attackers intent on delaying or denying the handoff service.

B. MOBILE IP HANDOFF PERFORMANCE STATISTICS

Out of the 63 test cases that were conducted, 31 of them correspond to the scenario where the mobile node roams from foreign network 1 to foreign network 2; and the remaining 32 correspond to the scenario where the mobile node roams from foreign network 2 back to foreign network 1. The performance statistics for the constituent components underlying the Mobile IP handoff process in each scenario were tabulated and averaged over the number of test cases that were conducted. Figure 44 shows the results that were obtained for the scenario where the mobile node roams from foreign network 1 to foreign network 2; and Figure 45 shows the corresponding results for the scenario where the mobile node roams from foreign network 2 back to foreign network 1. The results for the individual test cases can be found in Appendix B of this report.



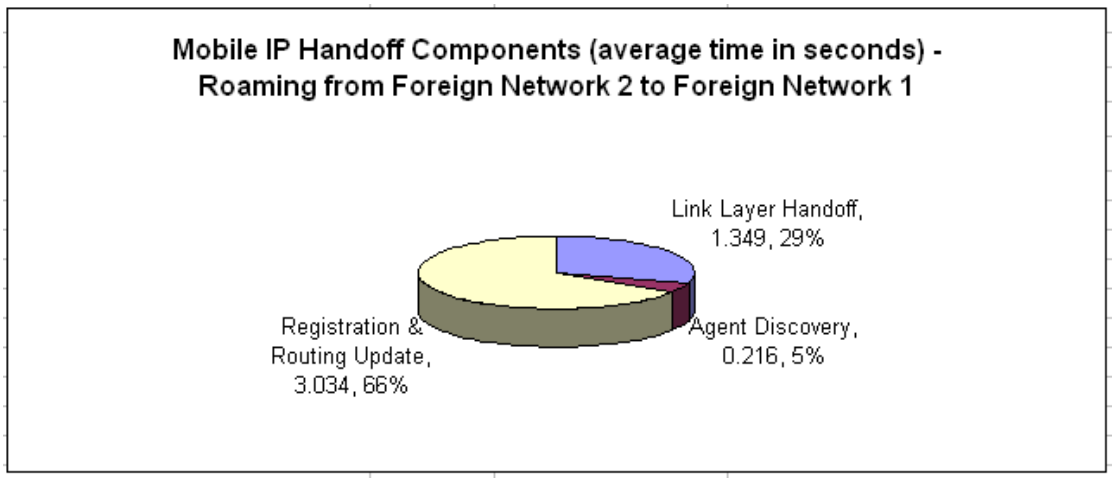
Mobile IP Handoff Components (average time in seconds)	
Link Layer Handoff	2.658
Agent Discovery	1.162
Registration & Routing Update	3.034
	6.854

Mobile IP Handoff Components (standard deviation)	
Link Layer Handoff	4.912
Agent Discovery	4.077
Registration & Routing Update	0.002

Link Layer Handoff Components (average time in seconds)	
Scanning	1.406
Authentication	1.156
Association	0.096
	2.658

Registration & Routing Update Components (average time in seconds)	
Foreign Agent's Processing of Registration Request	0.003
Foreign Agent - Home Agent Transmission Delay (for Registration Request)	0.005
Authentication	0.004
Update Mobility Binding & Create Tunnel	0.006
Delete Old Tunnel & Update Route	0.005
Home Agent Accepts Registration Request & Sends Registration Reply	3.003
Home Agent - Foreign Agent Transmission Delay (for Registration Reply)	0.005
Foreign Agent's Processing of Registration Reply	0.003
	3.034

Figure 44. Mobile IP Handoff Performance Statistics for Roaming from Foreign Network 1 to Foreign Network 2.



Mobile IP Handoff Components (average time in seconds)	
Link Layer Handoff	1.349
Agent Discovery	0.216
Registration & Routing Update	3.034
	4.599

Mobile IP Handoff Components (standard deviation)	
Link Layer Handoff	3.016
Agent Discovery	0.525
Registration & Routing Update	0.002

Link Layer Handoff Components (average time in seconds)	
Scanning	0.250
Authentication	1.091
Association	0.008
	1.349

Registration & Routing Update Components (average time in seconds)	
Foreign Agent's Processing of Registration Request	0.003
Foreign Agent - Home Agent Transmission Delay (for Registration Request)	0.005
Authentication	0.004
Update Mobility Binding & Create Tunnel	0.006
Delete Old Tunnel & Update Route	0.005
Home Agent Accepts Registration Request & Sends Registration Reply	3.003
Home Agent - Foreign Agent Transmission Delay (for Registration Reply)	0.005
Foreign Agent's Processing of Registration Reply	0.003
	3.034

Figure 45. Mobile IP Handoff Performance Statistics for Roaming from Foreign Network 2 to Foreign Network 1.

C. RESULTS ANALYSIS

Using the results that were described in the previous section, a component analysis was performed to evaluate the performance statistics for the three main components constituting the Mobile IP handoff, namely, move detection using link layer handoff and agent discovery, registration and updating of routing information.

1. Registration and Routing Update

The "Registration and Routing Update" component appears to be the main cost driver for the Mobile IP handoff process. The standard deviation for this component is very low, having only a value of 0.002; implying that the average time computed for the registration and routing update process is fairly accurate with little variance.

Further analysis of the subcomponents underlying the "Registration and Routing Update" component reveals the pre-processing by the home agent prior to accepting the registration request (i.e., the "Home Agent Accepts Registration Request and Sends Registration Reply" subcomponent) to be the main contributor of the overall processing delay. Since the time measurement for this subcomponent is already at its "atomic" level, with the router debug log offering no further breakdown in processing of this subcomponent, one would probably need to examine the IOS software that is written for the Mobile IP registration processing in order to fine-tune the performance parameters.

2. Move Detection Using Link Layer Handoff

The next contributor to the processing delay of the Mobile IP handoff process is the "Link Layer Handoff" component that is used for move detection. It was observed that the link layer handoff performance was roughly 100% faster for the scenario where the mobile node roams from foreign network 2 to foreign network 1, compared to the scenario where the mobile node roams from foreign network 1 to foreign network 2. The unintentional use of different brand/model of access points for the two foreign networks has led to the variability of the data that was collected for the two handoff scenarios.

Further analysis of the performance statistics for the "Link Layer Handoff" subcomponents seemed to indicate that the scanning process was the main cause for the variance in the two sets of readings. As the same wireless adaptor was used for the

mobile node, an obvious deduction is that the default scanning parameters[10] used for the access point in foreign network 1 outperformed those used for the access point in foreign network 2. Thus, the scanning parameters for the access point in foreign network 2 could potentially be fine-tuned for better performance[11].

The standard deviation for the "Link Layer Handoff" component is higher than the computed average for both the scenarios. The high deviation value could possibly be attributed to the nature of the wireless medium, which is unreliable and highly susceptible to noise and interference from the surrounding environment. Considering the constraints of space and the physical location where the test cases were conducted, RF interference from the neighboring equipment could possibly have affected the readings.

3. Move Detection Using Agent Discovery

The third contributor of the processing delay for the Mobile IP handoff process is the "Agent Discovery" component used for move detection. A similar observation was made for the performance of this component, in that the results for the scenario when the mobile node roams from foreign network 2 to foreign network 1 were better than the scenario when the mobile node roams from foreign network 1 to foreign network 2.

As the exchange of agent solicitation and agent advertisements in the agent discovery process takes place via the access point, one could reasonably deduce that the default control parameters for the channel acquisition and carrier-sensing maintenance functions differ for the two access points, and could be adjusted accordingly[12]. In addition, the standard deviation derived for the "Agent Discovery" component is higher than its computed average, the reason for this could possibly be attributed to the unreliable nature of the wireless medium, as described in the preceding section.

---

[10] It was the intent of this thesis research to use the default parameters for the IEEE 802.11-compliant access points so as to gather a set of readings that could be used as baseline for performance fine-tuning.

[11] The scanning parameters can only be fine-tuned if the specific access point provides an option for changing such parameters. Otherwise, the fine-tuning can only take place at the time of manufacture of the access point.

[12] Again, these control parameters can only be adjusted if the access point has made provisions for changing such settings.

4. Candidates for Performance Fine-tuning

Having analyzed the performance statistics for the constituent components underlying the Mobile IP handoff process, Table 15 provides a summary of the parameters that are potential candidates for performance fine-tuning.

Mobile IP Handoff Component	Applicable in which Roaming Scenario?	Subcomponent / Parameter	Suggested Improvements
Registration & Routing Update	Foreign network 1 to 2 & Foreign network 2 to 1	Home Agent Accepts Registration Request & Sends Registration Reply subcomponent	Examine the router IOS software that is handling the registration processing for possible code optimization so as to improve the performance for this component.
Link Layer Handoff	Foreign network 1 to 2	Scanning parameters	Adjust the scanning parameters of the access point in foreign network 2 to match those of the access point in foreign network 1 (if it is feasible). Otherwise, use the same brand/model as the access point in foreign network 1.
Agent Discovery	Foreign network 1 to 2	Control parameters for channel acquisition and carrier-sensing	Adjust the control parameters of the access point in foreign network 2 to match those of the access point in foreign network 1 (if it is feasible). Otherwise, use the same brand/model as the access point in foreign network 1.

Table 15. Summary of Potential Candidates for Performance Fine-tuning for the Mobile IP Handoff Process.

D. APPLICATION SUPPORT

After analyzing the performance statistics for the Mobile IP handoff process to support the roaming of an IEEE 802.11 wirelessly connected host, it is appropriate at this juncture to examine the different types of traffic requirements in order to determine the applications that can be supported by Mobile IP.

1. Data

As described in Chapter 4, the test cases were conducted based on data transmission over an established TCP session, so as to demonstrate that the session continuity is indeed maintained when the mobile node roams from one foreign network to another foreign network. Since Mobile IP was shown to support data transmission of connection-oriented TCP traffic, which places a more "stringent" requirement on the network layer in order to maintain a session; Mobile IP should have no problems supporting connectionless protocols such as UDP. As a result, a variety of applications that utilize either TCP or UDP as the underlying transport protocol, and which are not time-sensitive in nature, can be supported by Mobile IP.

2. Voice

To support voice requirements, the International Telecommunication Union (ITU) has recommended a set of values for the maximum round trip delay that can be tolerated by a voice system, and the perceived quality of the voice channel at these values [38]. Table 16 lists the recommendations that are defined in ITU-T G.113.

G.113 Delay Specification	
0 to 150 msec	acceptable to most applications
150 to 400 msec	acceptable for international connections
> 400 msec	acceptable for public network operation

Table 16. ITU-T G.113 Delay Specification for Voice System (From: Ref. [38]).

In addition to the ITU-T G.113 Voice Quality Specification shown in Table 16, ITU-T G.114 recommends an end-to-end delay of not more than 150 milliseconds for good voice quality [39]. As depicted in Figure 46; however, there are scenarios in which an end-to-end delay of more than 150 milliseconds will be encountered. Although the

ITU-T G.114 recommendation would categorize such delays as being outside the acceptable range of voice quality, many conversations occur daily over satellite links that consistently exceed the 150 millisecond limit due to the distance (~22,300 miles) of geosynchronous satellites above the Earth's surface. We cannot establish a hard upper limit on "acceptable" delay as voice quality is also subjectively based on what an individual user will accept and use.

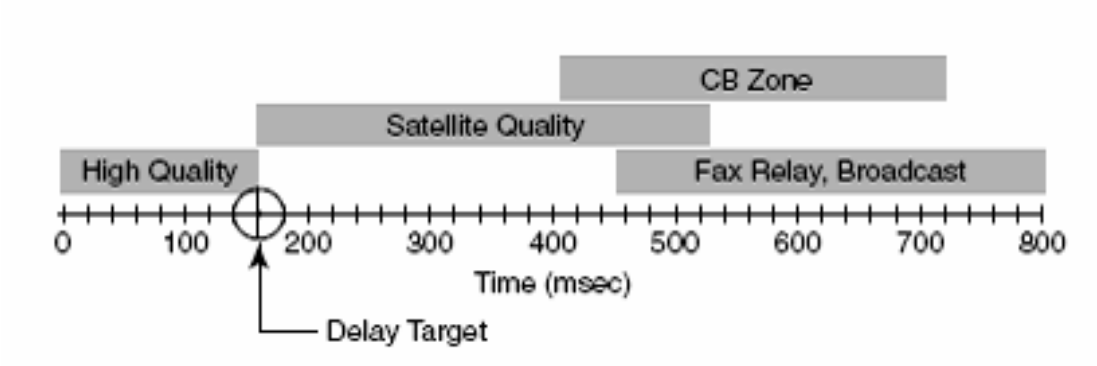


Figure 46. End-to-End Delay in ITU-T G.114 Specification (From: Ref. [39]).

Given the recommended values that are reflected in Table 16 and Figure 46, it will be optimal to keep the maximum round trip delay to less than 150 milliseconds to support most voice applications and maintain a consistent level of good voice quality. Tests conducted by the University of Maryland indicated that an access point probe occurs every 250 to 400 milliseconds [38]. These values match the computed average that was obtained from the Mobile IP handoff test cases conducted for the scenario when the mobile node roams from foreign network 2 to foreign network 1: the scanning subcomponent of the link layer handoff took 0.250 seconds. It is apparent that the scanning subcomponent alone has already exceeded the maximum round trip delay that can be tolerated by most voice applications. An ongoing effort to improve the performance of the link layer handoff in a wireless environment is currently addressed by the IEEE 802.11e (QoS) task group [40].

After addressing the performance issue relating to the link layer handoff, the Mobile IP protocol will need to provide support for the proper handling of QoS related traffic at its mobility agents and intermediate nodes, so that QoS sensitive IP services can

be supported over Mobile IP. RFC 3583 [41] describes the requirements for an IP QoS mechanism for its satisfactory operation with Mobile IP, and recommends that

> The expectation is that the appropriate working group will use this requirements document to provide a QoS solution for Mobile IP.

Therefore, both the IEEE 802.11 link layer handoff performance and Mobile IP's support for QoS traffic will need to be addressed, before the Mobile IP handoff process can be used to support the roaming of an IEEE 802.11 wirelessly connected host that is supporting voice applications.

3. Video

Video applications can be categorized into two main types: interactive video applications such as videoconferencing, and "store-and-forward" video applications such as video streaming. According to [42], real-time IP applications such as videoconferencing and voice-over-IP have an upper bound end-to-end latency requirement of not more than 150 milliseconds. Thus, the same voice requirements that were described in the preceding section will apply in order for Mobile IP to be able to support interactive video applications.

On the other hand, video streaming applications demand a less stringent requirement on the end-to-end network delay. Depending on the application's buffering capabilities, "non-interactive" video content can be pre-downloaded and stored in the application's buffer prior to playback. Such a mechanism will "convert" the real-time requirement to a non real-time one; treating video streaming just like any other transmission of elastic static data. Thus, Mobile IP should have no problems supporting non-interactive video streaming applications.

E. SECURITY RAMIFICATIONS

The implementation of security measures often comes at the cost of performance. In architecting the Mobile IP setup to gather performance statistics for the constituent components underlying the handoff, minimal security-related services were configured for both the IEEE 802.11 wireless network and Mobile IP network. As a recap, Table 17 shows the security-related services that were enabled for the setup.

Service	Configured? / Used?
IEEE 802.11 Security-Related Services	
Authentication	Open-system authentication was configured.
Privacy	No
Mobile IP Security-Related Services	
Authentication Extension	The Mobile-Home Authentication Extension (MHAE) was configured.
Reverse Tunneling	No

Table 17. Security-Related Services Configured for the Mobile IP Setup.

The Mobile IP setup, in its most primitive configuration, can be exploited by an attacker intent on denying or delaying proper handoff service. Specifically, the following section will describe the handoff components that are potentially vulnerable to attacks launched by a malicious user.

1. Link Layer Handoff

Link layer handoff comprises mainly the scanning, authentication and association subcomponents. The use of the default authentication protocol, i.e., open system authentication, for the IEEE 802.11 wireless network that was setup essentially offers no authentication, as there is no control over who can associate with the access point [26]. Thus, any malicious user can potentially exploit the “identification and authentication vulnerability” to gain unauthorized access to the wireless network that is served by the access point.

The management frames that are used in the link layer handoff process do not offer any form of integrity protection. Coupled with the fact that link layer MAC addresses can be easily forged, an attacker can potentially launch a man-in-the-middle attack [26] against the IEEE 802.11 wireless network, as illustrated in Figure 47.

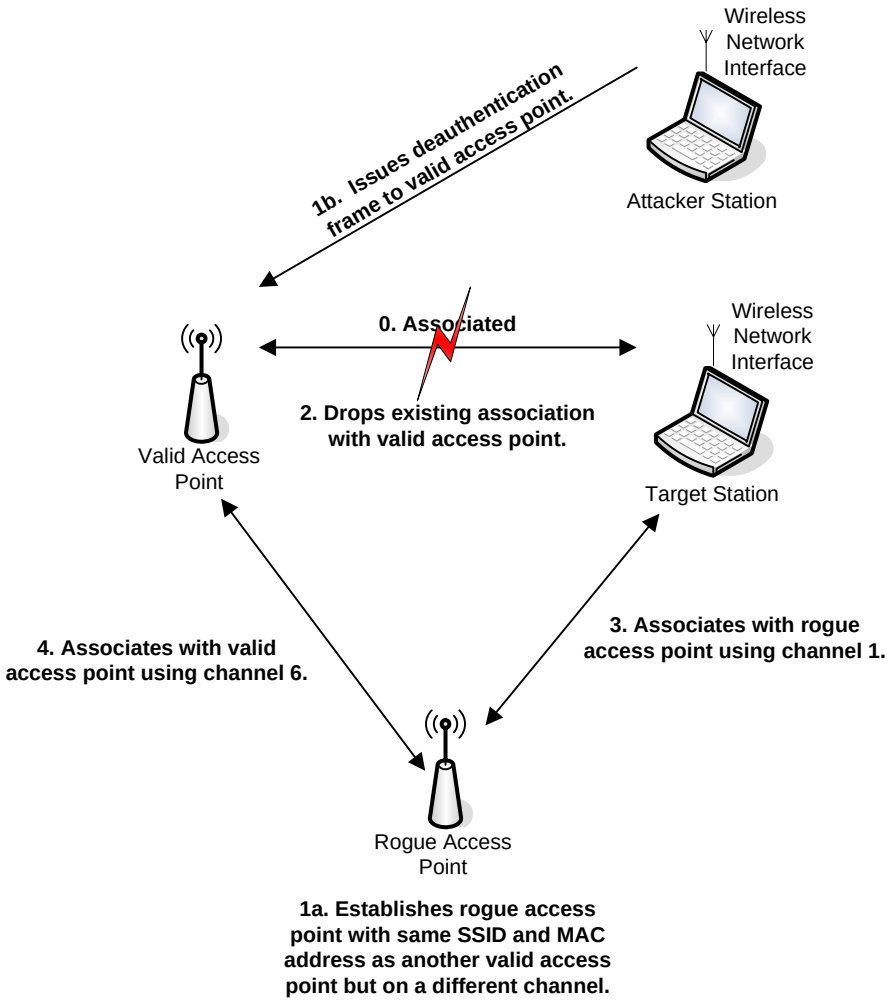


Figure 47. Example Man-in-the-Middle Attack for the IEEE 802.11 Wireless Network (After: Ref. [26]).

Exploiting the “lack of integrity protection vulnerability” of the management frames, denial-of-service attacks can also be launched against the IEEE 802.11 wireless network [26]. Figure 48 and Figure 49 illustrate two possible denial-of-service attacks that can be launched by an attacker.

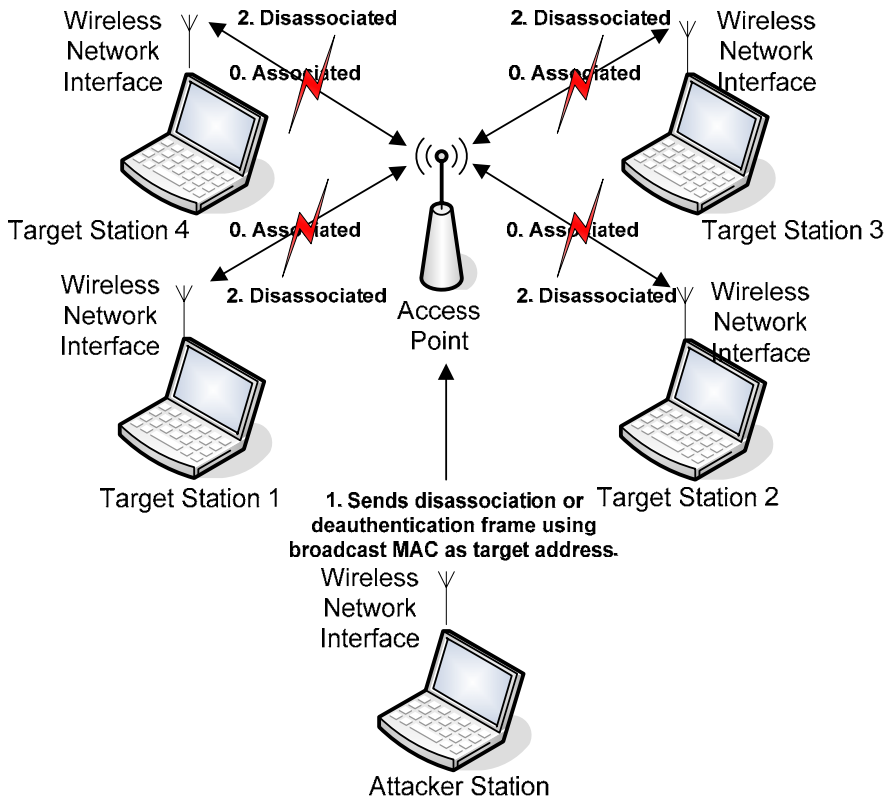


Figure 48. Denial-of-Service Attack Using Deauthenticaton / Disassociation Frame.

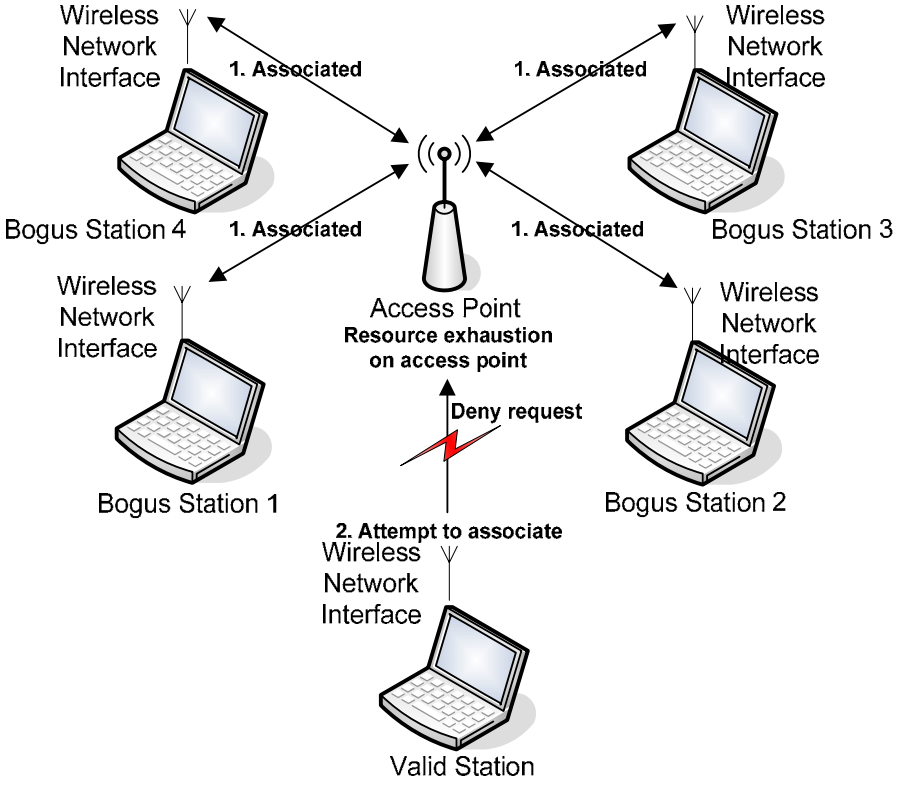


Figure 49. Denial-of-Service Attack Using Resource Exhaustion.

2. Agent Discovery

As described in Chapter 2, RFC 3344 [4] requires that all the registration messages between the mobile node and its home agent be authenticated. Because of key management challenges, registration messages relayed by the foreign agent will only be authenticated if an optional mobility security association exists between the mobile node and foreign agent; and if an optional mobility security association exists between the foreign agent and home agent. This is a potential vulnerability that can be exploited by an attacker to launch a denial-of-service or traffic redirection type of attack. A bogus foreign agent can be configured to respond to the mobile node's agent solicitation with its agent advertisement, resulting in IP traffic destined for the mobile node to be tunneled to the bogus foreign agent's advertised care-of address, as depicted in Figure 50.

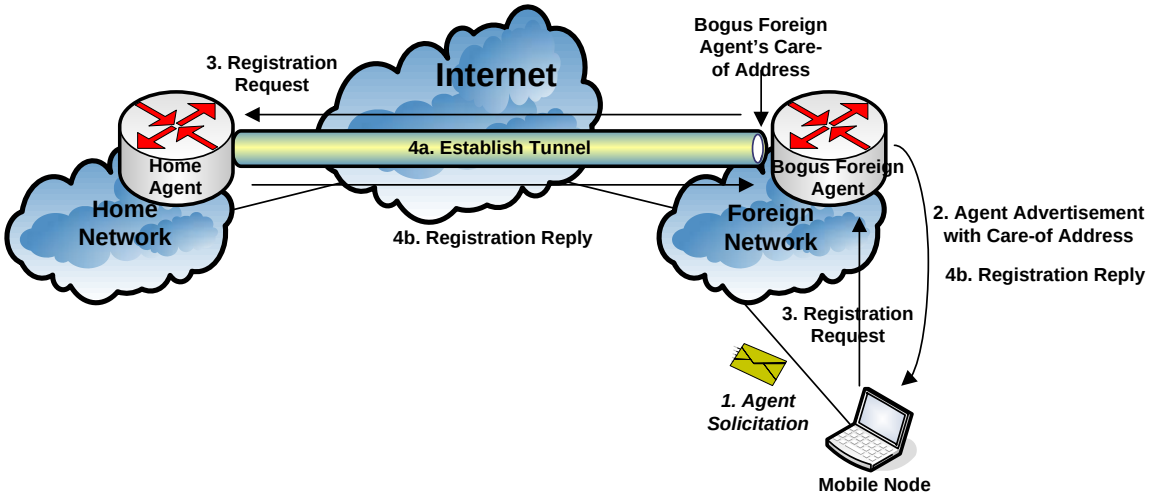


Figure 50. Registration via a Bogus Foreign Agent.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS

The Mobile IP protocol specified in RFC 3344 [4] defines the mechanisms and protocol behaviors that are necessary to facilitate the seamless flow of traffic to a mobile host that roams away from its normal home network. The main objective of this research was to explore how this capability could be utilized to support the relatively rapid roaming of an IEEE 802.11 wirelessly connected host. Specifically, this research was focused on isolating and analyzing the constituent components underlying the Mobile IP protocol for the purpose of identifying the cost drivers that may be improved upon, and recognizing the vulnerabilities that may be exploited by an attacker intent on denying or delaying proper handoff service.

A reference architecture was devised and adopted to demonstrate the operations of the Mobile IP protocol to support the roaming of an IEEE 802.11 wirelessly connected host in a controlled environment. Thereafter, a test plan was formulated, describing the appropriate test cases and test procedure for collecting the performance statistics. Having identified the potential candidates for data collection, the Mobile IP setup was instrumented to facilitate the gathering of the performance statistics. Data collected from the different sources were then collated and analyzed to determine the performance statistics corresponding to the constituent components underlying the handoff process.

Based on the results that were obtained, suggestions were made to fine-tune the appropriate parameters to possibly improve the performance of the different cost drivers. Using the traffic requirements for different types of applications as a reference, it was concluded that Mobile IP should have no problems supporting data and non-interactive video traffic. Further enhancements to the Mobile IP protocol and IEEE 802.11 standard will be required in order to support real-time traffic such as voice and interactive video applications.

The security ramifications for the Mobile IP setup were briefly discussed. A malicious user could potentially exploit the IEEE 802.11 wireless link layer mechanism, and the Mobile IP agent discovery process, to launch denial-of-service, man-in-the-middle, and traffic redirection types of attacks. As the main purpose of this thesis

research was to gather the performance statistics for the constituent components underlying the Mobile IP handoff process, a minimalist configuration was adopted, with minimal security-related services enabled. Thus, this is a potential area that would call for further research.

A. MAJOR CHALLENGES

The journey taken to reach this final stage of the thesis research was not a smooth sailing one. One of the major challenges encountered was to be able to work within the confines of existing hardware and software in order to devise an appropriate setup that could be used to gather the performance statistics. More often than not, due to equipment age and peculiarities, a lot of time and effort were spent troubleshooting problems that were not of direct relation to Mobile IP. One would frequently need to think out-of-the-box and come up with innovative solutions in order to work within the existing boundaries.

Despite the fact that vendor documentation were made available for the configuration of the Mobile IP setup, these were "component-based" information that offered a "silo" view of how Mobile IP operates. Coupled with the fact that there were no common deployable scenarios that utilized both the mobile client software with the Mobile IP service-enabled routers, one could not reference existing deployments when problems were encountered. As a result, a significant amount of time and effort were expended on trial-and-error sessions in order to find the "correct mix" for the setup to work.

The physical location where the Mobile IP setup was situated also posed a challenge to the data collection process. As the IEEE 802.11 standard operates in a frequency band that is shared by other industrial, scientific and medical equipment [25], its operations are highly susceptible to RF interferences from its neighboring equipment. Having the setup located at a research lab with a significant amount of equipment and ongoing activity was not exactly an ideal environment for the collection of "baseline" performance statistics. The workaround was to collect the data at the "silent hours" of the day, where the surrounding environment has relatively less activity taking place.

The instrumented Mobile IP setup relied on different equipment for data collection, which had led to the need for collation of multiple data sources in order to determine the performance statistics for the handoff components. The process of manual data collation is tedious and error-prone, and does not favor scalability. In addition, due to the different time-precisions that are used by the various data collection equipment, the accuracy of the collated data could only be as accurate as the equipment with the least time-precision. Going forward, it is recommended that an automated tool be considered to collect and collate data from the respective authoritative sources to address accuracy and scalability concerns.

B. RECOMMENDATIONS FOR FUTURE RESEARCH

Working within the confines of existing hardware and software, the performance statistics were gathered based on a set of vendor-specific products. As described under the *Result Analysis* section of the previous chapter, the main cost driver for the Mobile IP handoff process was the "Registration and Routing Update" component. The test cases conducted using the current setup were based on a "black-box" approach, with one having no minute information on the exact processing that took place when the home agent decided to accept a registration request. Going forward, this is an area that will call for further research. Specifically, one will want to analyze all the constituent components underlying the registration and routing update process, compare that against the recommendations given in RFC 3344 [4], and suggest the appropriate enhancements to improve the performance of the "Registration and Routing Update" component. Additionally, one may want to determine the relationship between the handoff performance and the router's internal processing, i.e., if a better handoff performance will "stress" the router, resulting in slower processing of other network traffic, and vice versa.

As it was the intent of this research to collect the "best-case" performance statistics from a relatively "clean" environment using a minimalist configuration, it will be of interest to explore the effect of network load on the router's processing of Mobile IP related traffic. Consequently, one will then be able to determine if the router's software processing is sufficient to meet the performance requirements of a "real-world"

scenario, and recommend possible improvements such as offloading the processing to dedicated hardware component.

The unintentional use of different brands/models of access points has introduced variability in the results obtained for the link-layer handoff performance. It will be useful to conduct the test cases using a variety of access points (with the option to configure the scanning and control parameters) to determine the "best-case" link-layer performance that can be obtained, and recommend the corresponding set of scanning and control parameters that will provide the desired link-layer performance.

A decision was made to conduct the test cases based on "static" data transfer over an established TCP session to demonstrate that the session is indeed "maintained" when a mobile node roams from one network to another. To facilitate data collection and collation, the mobile node was the party initiating the data transfer to the correspondent node in the current setup. It will be constructive to conduct the same "static" data transfer over TCP with the correspondent node initiating the data transfer to the mobile node, to determine if there will be any variations in the performance statistics associated with the handoff process. In addition, it will be worthwhile to gather the performance statistics for test cases conducted based on streaming of "non-interactive" voice and video over a UDP session, to facilitate comparison against the results obtained for supporting TCP traffic.

The main objective of this research was to conduct a performance analysis of the Mobile IP protocol to support the relatively rapid roaming of an IEEE 802.11 wirelessly connected host. As a result, minimal security-related services were supported. Knowing that a potentially vulnerable network will be subjected to active and passive attacks, ultimately affecting its performance, the security ramifications would justify the need for further research. Specifically, the two areas that would need to be addressed would be the protection of the IEEE 802.11 link layer handoff mechanism, and the protection of the Mobile IP registration process that takes place via a foreign agent. Addressing these two areas will also provide further insights on how the performance may be affected through the configuration of the security-related services.

As was highlighted in the previous section, the current mechanism for collecting and collating data is a manual process that is tedious, error-prone, not scaleable, and can

only be as accurate as the measuring device with the least time-precision. In order to support the identified areas for future research, it will be of immediate interest and relevance to devise an automated mechanism to collect and collate the data from the respective authoritative sources to address accuracy and scalability concerns.

Last but not least, the topic on mobility, and its support for IP applications, branches out into many facets; ranging from micro-mobility to macro-mobility [38], seamless integration with cellular networks, support for mobile ad-hoc networking, QoS and traffic engineering considerations for supporting real-time traffic, operational considerations for military command and control, varying boundaries and the security ramifications, and much more. The scope for each of these areas would justify a separate research on its own. Needless to say, the analysis conducted and recommendations provided as a result of this thesis research have only addressed a tip of the iceberg.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A – CONFIGURATION SETUP

This appendix serves to document the configuration details of the respective components that were used to setup the Mobile IP test environment as illustrated in Figure 39.

A. MOBILITY AGENT

A mobility agent refers to a home agent or foreign agent. A home agent and two foreign agents were configured in the Mobile IP test environment. It is not the intent of this appendix to describe the step-by-step procedure for router configuration. Rather, this section will only list the running configuration for the three respective routers. Readers can refer to [5] and [43] for a more thorough treatment on how to configure IP mobility services for the routers. Similarly, readers can also refer to [44] and [45] for enabling the DHCP and NTP services on these routers.

1. Home Agent

The running configuration for the home agent is shown in Figure 51.

```
!
! Last configuration change at 10:20:58 UTC Mon Nov 20 2006
! NVRAM config last updated at 12:46:18 UTC Mon Nov 20 2006
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C2621XM_HomeAgent
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 errors
!
no aaa new-model
!
resource policy
!
no network-clock-participate slot 1
no network-clock-participate wic 0
ip subnet-zero
!
!
no ip dhcp use vrf connected
ip dhcp excluded-address 10.3.1.1 10.3.1.9
ip dhcp excluded-address 10.3.1.251 10.3.1.255
!
ip dhcp pool HomeNet                    DHCP Configuration
   network 10.3.1.0 255.255.255.0
   default-router 10.3.1.1
!
!
ip cef
no ip ips deny-action ips-interface
!
!
interface Loopback0
 ip address 10.100.1.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 10.1.1.2 255.255.255.0
 duplex auto
 speed auto
!
```

```
interface FastEthernet0/1
 ip address 10.3.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Ethernet1/0
 ip address 10.5.1.1 255.255.255.0
 half-duplex
!
interface Ethernet1/1
 no ip address
 shutdown
 half-duplex
!
interface Ethernet1/2
 no ip address
 shutdown
 half-duplex
!
interface Ethernet1/3
 no ip address
 shutdown
 half-duplex
!
router mobile
!
ip classless
ip route 10.2.1.0 255.255.255.0 10.1.1.1
ip route 10.4.1.0 255.255.255.0 10.1.1.3
!
!
no ip http server
no ip http secure-server
ip mobile home-agent
ip mobile bindupdate retry 1
ip mobile virtual-network 10.10.10.0 255.255.255.0
ip mobile host nai mn@nps static-address 10.10.10.1 virtual-
network 10.10.10.0 255.255.255.0
ip mobile secure host nai mn@nps spi 1234 key hex
12345678123456781234567812345678 algorithm hmac-md5
!
```

Home Agent Configuration

```
!
no cdp run
!
!
!
control-plane
!
!
line con 0
 session-timeout 180
 logging synchronous
line aux 0
line vty 0 4
 login
!
ntp clock-period 17179470                          NTP Configuration
ntp server 10.1.1.1 key 1234 source FastEthernet0/0
!
end
```

Figure 51. Home Agent's Running Configuration.

2. Foreign Agent

Figure 52 and Figure 53 show the running configuration for the two foreign agents.

```
!
! Last configuration change at 10:40:03 UTC Mon Nov 20 2006
! NVRAM config last updated at 12:46:51 UTC Mon Nov 20 2006
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C2651XM_ForeignAgent1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
no network-clock-participate slot 1
no network-clock-participate wic 0
ip subnet-zero
!
!
no ip dhcp use vrf connected
!
!
ip cef
no ip ips deny-action ips-interface
!
!
interface Loopback0
 no ip address
!
interface FastEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
!
```

```
interface FastEthernet0/1
 ip address 10.2.1.1 255.255.255.0
 ip mobile foreign-service
 ip irdp
 ip irdp maxadvertinterval 4
 ip irdp minadvertinterval 3
 ip irdp holdtime 9
 speed auto
 half-duplex
!
interface Serial0/1
 no ip address
 shutdown
!
interface Serial0/2
 no ip address
 shutdown
!
interface Serial0/3
 no ip address
 shutdown
!
router mobile
!
ip classless
ip route 10.5.1.0 255.255.255.0 10.1.1.2
ip route 10.100.1.0 255.255.255.0 10.1.1.2
!
no ip http server
no ip http secure-server
ip mobile foreign-agent care-of FastEthernet0/1
!
no cdp run
!
control-plane
!
dial-peer cor custom
!
line con 0
 session-timeout 180
 logging synchronous
line aux 0
line vty 0 4
 login
!
ntp authentication-key 1234 md5 062E2E1E7847041C 7
ntp trusted-key 1234
ntp source FastEthernet0/0
ntp master 6
!
end
```

Foreign Agent Configuration

NTP Configuration

Figure 52. Foreign Agent 1's Running Configuration.

```
!
! Last configuration change at 10:39:18 UTC Mon Nov 20 2006
! NVRAM config last updated at 12:47:26 UTC Mon Nov 20 2006
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C2651XM_ForeignAgent2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
no network-clock-participate slot 1
no network-clock-participate wic 0
ip subnet-zero
!
!
no ip dhcp use vrf connected
!
!
ip cef
no ip ips deny-action ips-interface
!
!
interface FastEthernet0/0
 ip address 10.1.1.3 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
!
```

```
interface FastEthernet0/1
 ip address 10.4.1.1 255.255.255.0
 ip mobile foreign-service
 ip irdp
 ip irdp maxadvertinterval 4
 ip irdp minadvertinterval 3
 ip irdp holdtime 9
 speed auto
 half-duplex
!
interface Serial0/1
 no ip address
 shutdown
!
interface Serial0/2
 no ip address
 shutdown
!
interface Serial0/3
 no ip address
 shutdown
!
router mobile
!
ip classless
ip route 10.5.1.0 255.255.255.0 10.1.1.2
ip route 10.100.1.0 255.255.255.0 10.1.1.2
!
!
no ip http server
no ip http secure-server
ip mobile foreign-agent care-of FastEthernet0/1
!
no cdp run
!
control-plane
!
line con 0
 session-timeout 180
 logging synchronous
line aux 0
line vty 0 4
 login
!
ntp clock-period 17207990
ntp server 10.1.1.1 key 1234 source FastEthernet0/0
!
end
```

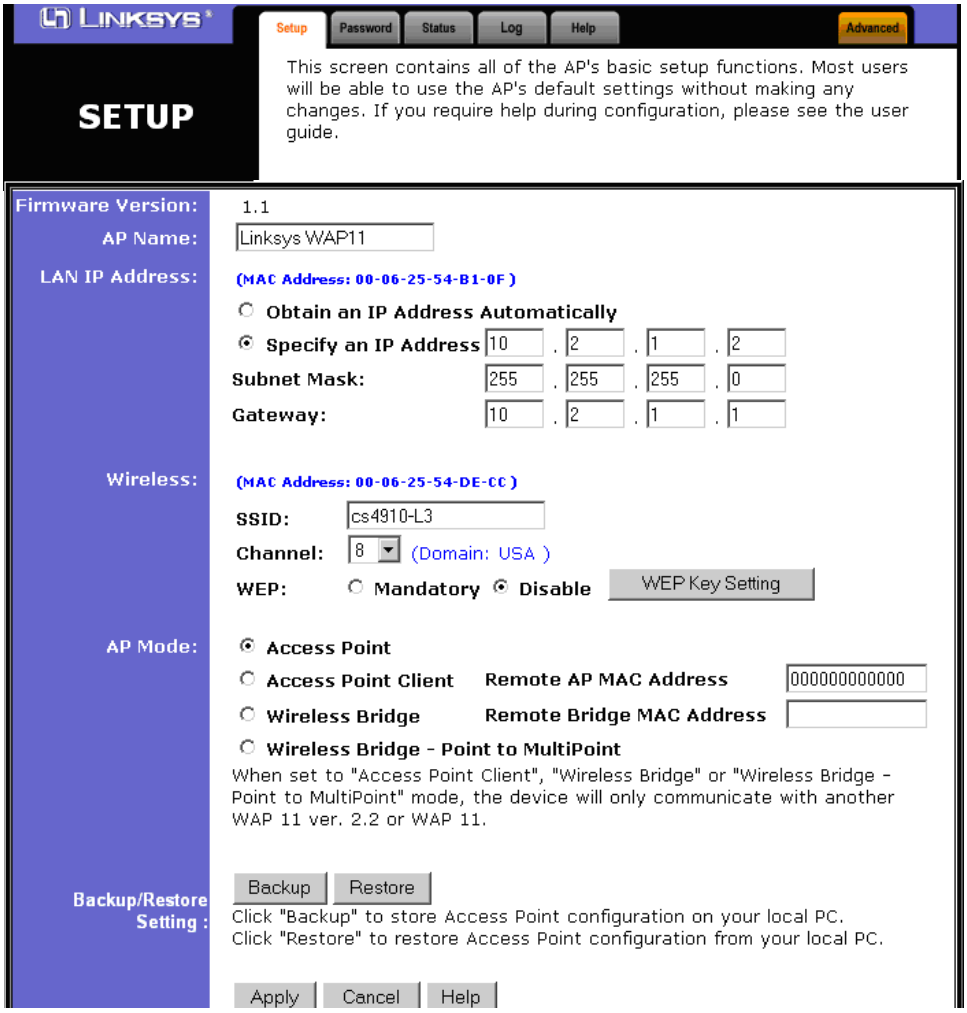
Foreign Agent Configuration

NTP Configuration

Figure 53. Foreign Agent 2's Running Configuration.

B. ACCESS POINT

Two ESSs, corresponding to the two foreign networks, were configured for the Mobile IP setup. As described in Chapter 4, each of the ESSs has a single BSS, which is served by an access point. Figure 54 and Figure 55 list the configuration for access point 1 and access point 2 respectively. Readers can refer to [46] for the detailed user guide for access point 1, and [47] for the user guide for access point 2.



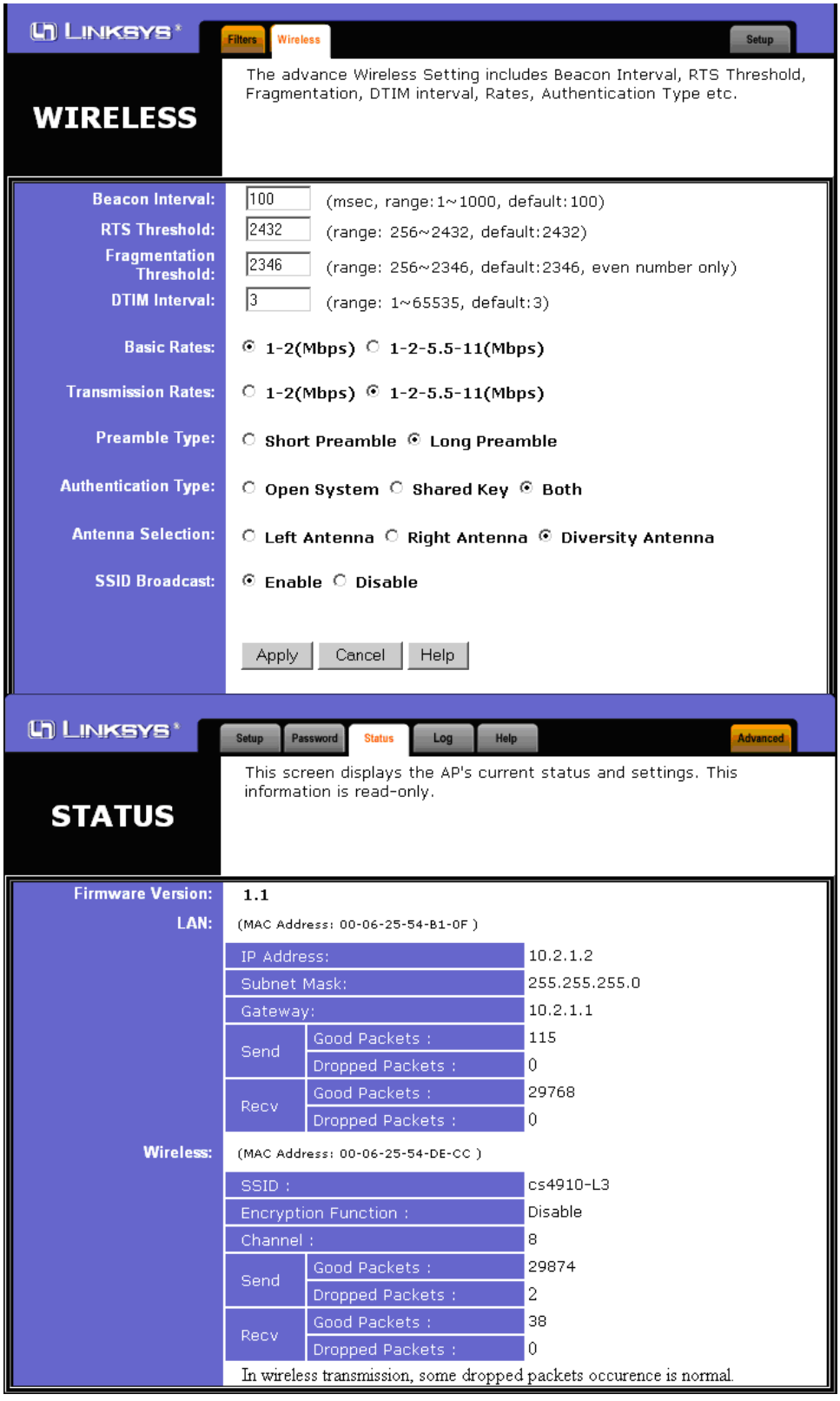


Figure 54. Access Point 1's Configuration.

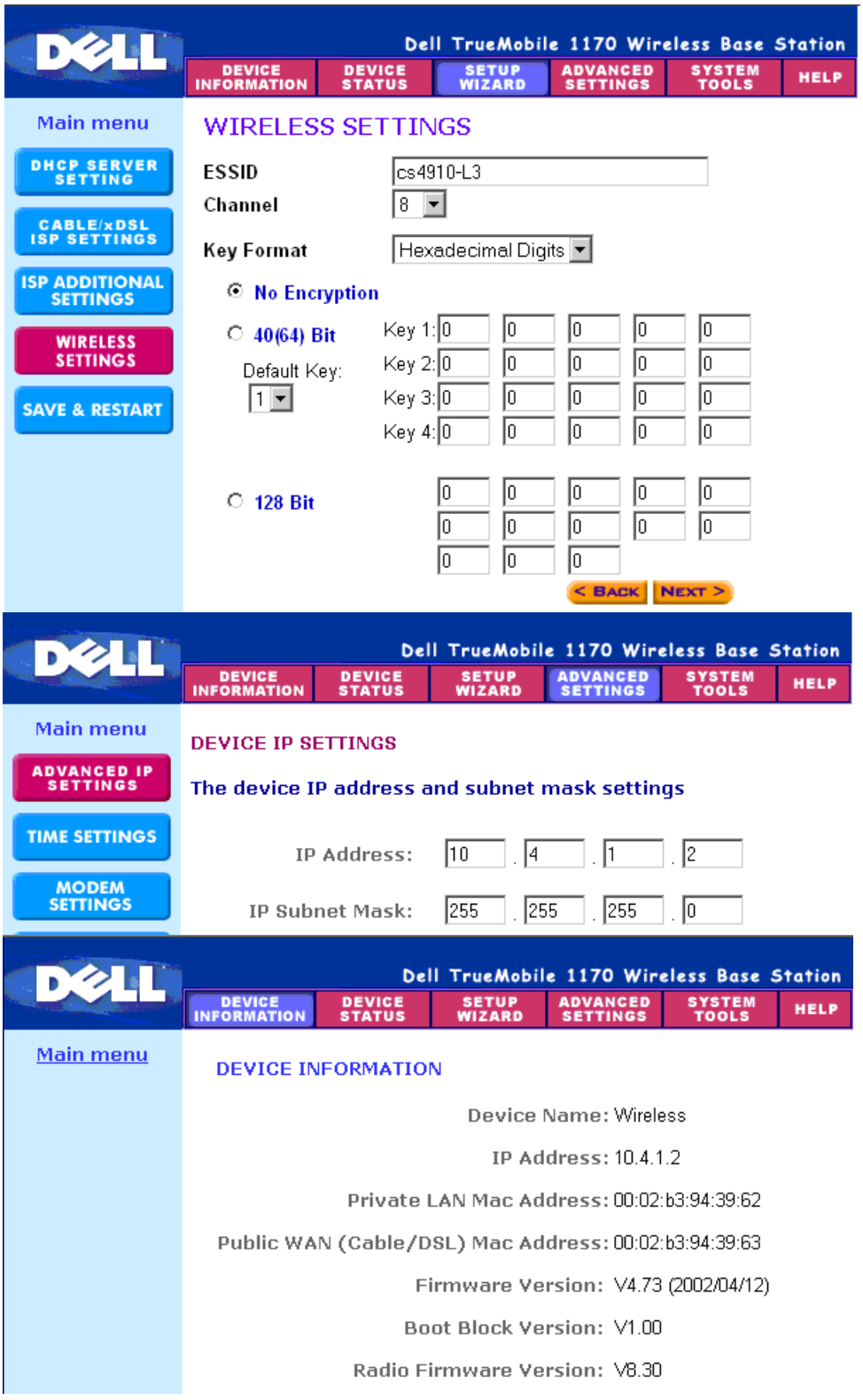
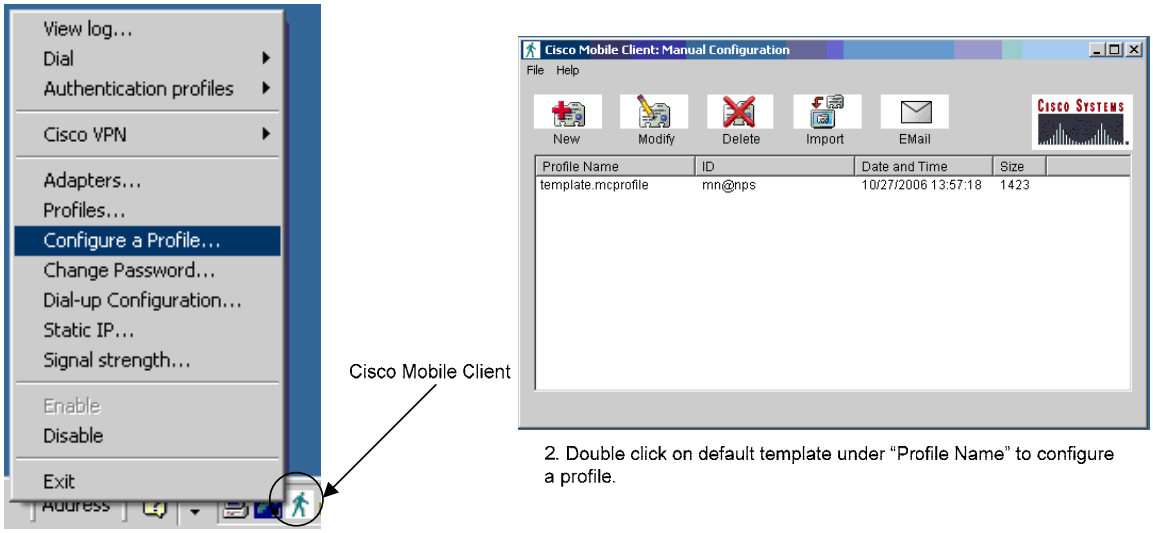


Figure 55. Access Point 2's Configuration.

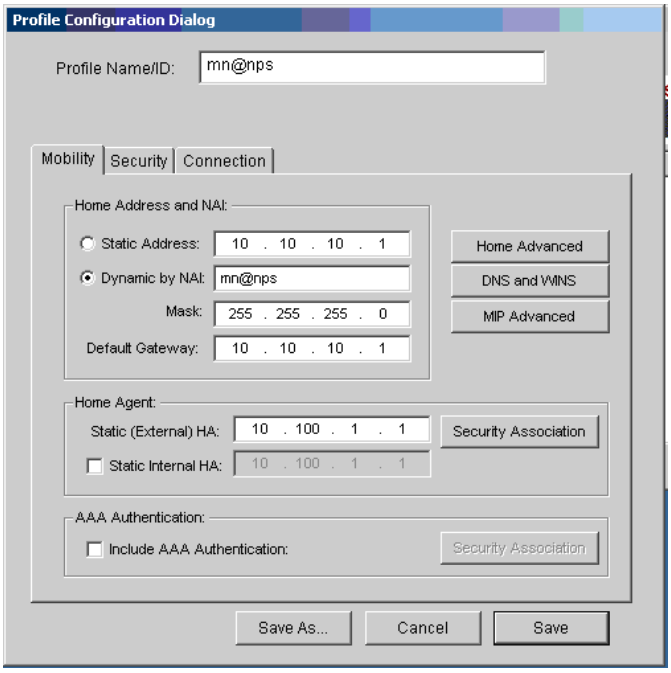
C. MOBILE NODE

The Cisco Mobile Client version 2.0.14 software was used to enable the station to function as a mobile node. Figure 56 briefly describes the steps that are required to configure the mobile node, and Figure 57 illustrates the status of the Cisco Mobile Client when the mobile node roams from one foreign network to another foreign network. Readers can refer to [34] for a more thorough treatment on how to configure the Cisco Mobile Client software.

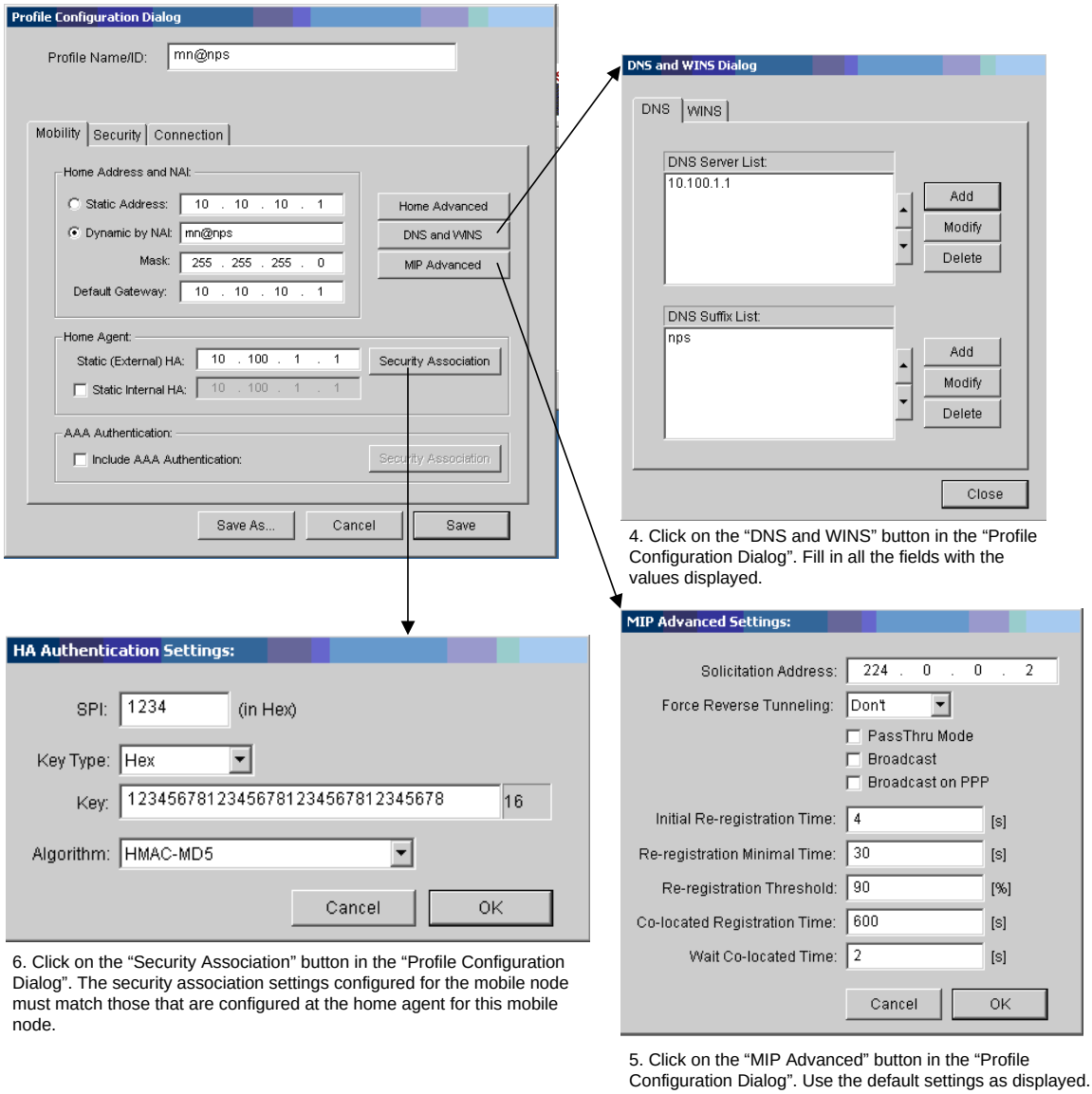
1. Right click on Cisco Mobile Client & Select "Configure a Profile…"



2. Double click on default template under "Profile Name" to configure a profile.



3. The "Profile Configuration Dialog" appears. Fill in all the fields with the values displayed.



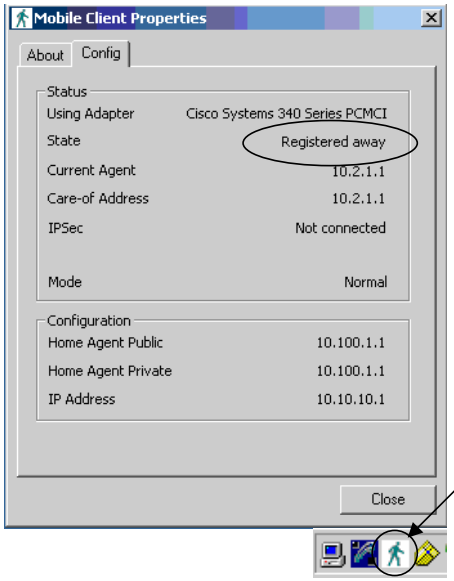
4. Click on the “DNS and WINS” button in the “Profile Configuration Dialog”. Fill in all the fields with the values displayed.

6. Click on the “Security Association” button in the “Profile Configuration Dialog”. The security association settings configured for the mobile node must match those that are configured at the home agent for this mobile node.

5. Click on the “MIP Advanced” button in the “Profile Configuration Dialog”. Use the default settings as displayed.

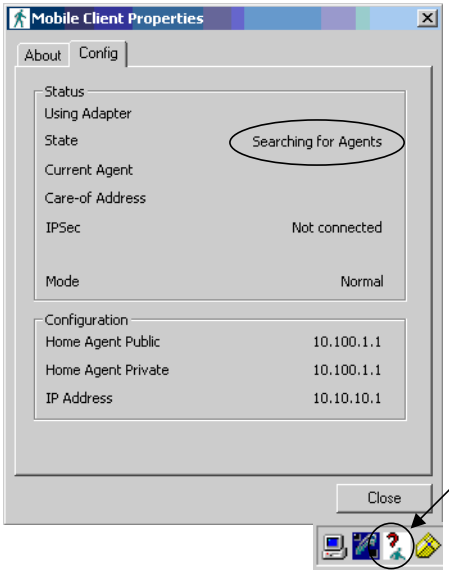
Figure 56. Mobile Node’s Configuration.

1. Double click on Cisco Mobile Client to get "Mobile Client Properties" dialog box.



2a. Select "Config" tab. The dialog box shows the mobile node being connected to foreign network 1 and is "registered away".

2b. Note status of Cisco Mobile Client.



3a. The mobile node roams to foreign network 2. The dialog box shows the mobile node "searching for agents".

3b. Note status of Cisco Mobile Client.

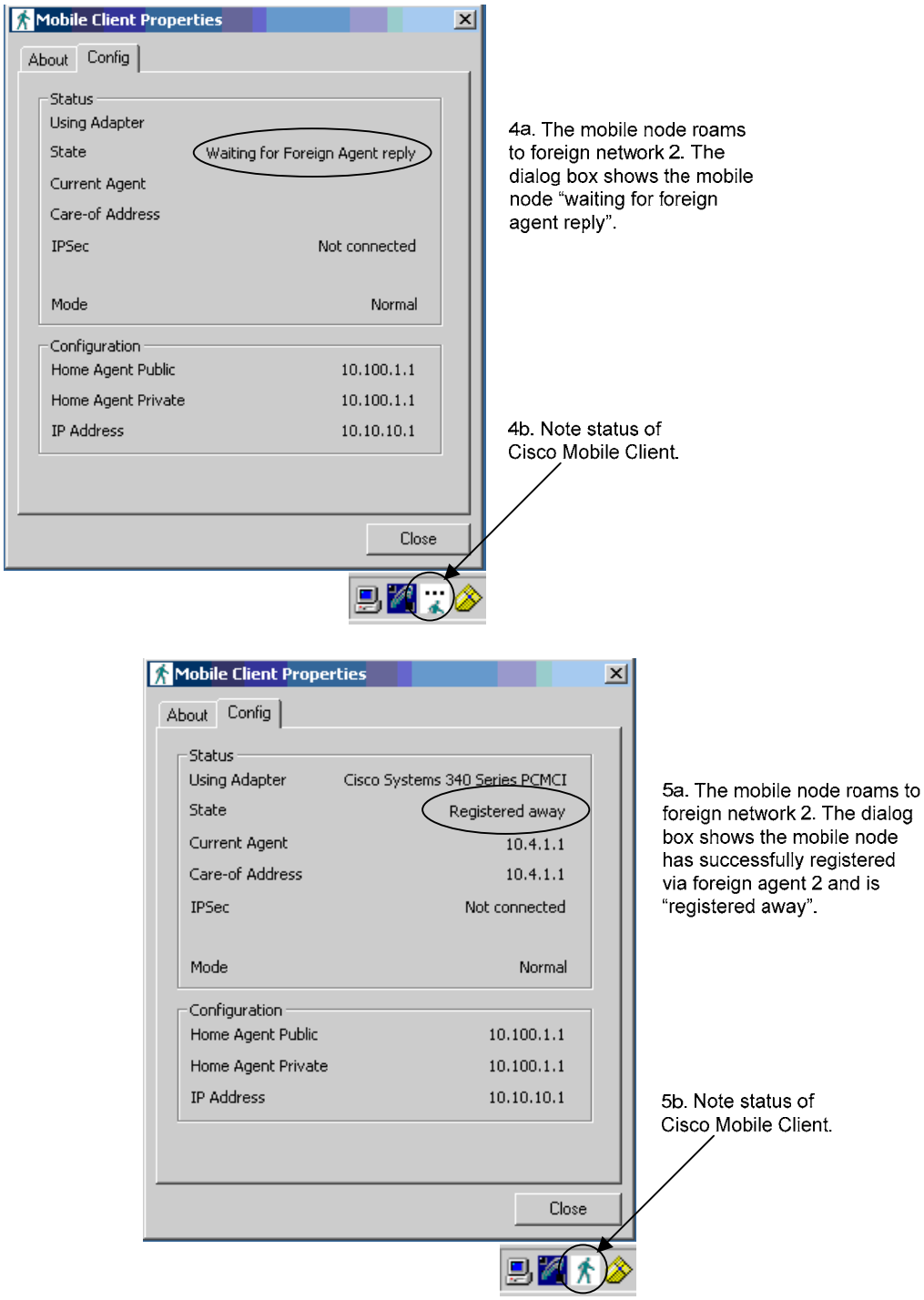


Figure 57. Cisco Mobile Client in Operation.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B – TEST RESULTS

This appendix details the collated results for the individual test cases that were used to derive the summary statistics shown in Figure 44 and Figure 45.

A. ROAMING FROM FOREIGN NETWORK 1 TO FOREIGN NETWORK 2

The collated results for the individual test cases conducted for the scenario when the mobile node roams from foreign network 1 to foreign network 2 are detailed in Tables 18, 19 and 20.

Data Set	Move Detection		Registration & Routing Upate	Total
	Link Layer Handoff	Agent Discovery		
1	2.948	0.049	3.032	**6.029**
5	0.404	0.101	3.033	**3.539**
7	0.088	0.066	3.033	**3.186**
9	0.394	0.089	3.033	**3.516**
11	0.456	22.196	3.037	**25.690**
13	9.042	2.133	3.032	**14.207**
17	1.027	5.504	3.033	**9.565**
21	2.254	0.113	3.033	**5.400**
23	23.331	0.020	3.033	**26.385**
27	0.080	0.049	3.033	**3.162**
31	1.334	0.048	3.033	**4.415**
35	1.171	0.043	3.037	**4.251**
37	0.171	0.072	3.037	**3.280**
39	1.699	0.065	3.033	**4.797**
41	1.895	0.087	3.033	**5.015**
43	0.672	0.119	3.041	**3.832**
45	2.487	0.020	3.033	**5.540**
47	0.096	0.078	3.041	**3.214**
49	4.959	0.022	3.033	**8.014**
51	0.667	0.064	3.037	**3.768**
53	0.019	0.103	3.033	**3.155**
57	14.496	0.010	3.037	**17.543**
59	6.577	1.006	3.032	**10.615**
63	0.887	0.061	3.033	**3.981**
65	1.610	0.116	3.033	**4.759**
67	1.224	0.047	3.033	**4.304**
69	0.307	0.061	3.037	**3.404**
P51	0.121	0.066	3.033	**3.220**
P23	0.950	0.047	3.033	**4.030**
P19	0.945	3.455	3.033	**7.433**
P11	0.087	0.114	3.033	**3.235**
Total	82.397	36.025	94.060	**212.483**
Average	2.658	1.162	3.034	**6.854**

Table 18. Detailed Test Results for Mobile IP Handoff Components (in Seconds) – Roaming from Foreign Network 1 to Foreign Network 2.

Data Set	Link Layer Handoff			Total
	Scanning	Authentication	Association	
1	0.057	0.204	2.687	**2.948**
5	0.370	0.032	0.002	**0.404**
7	0.078	0.002	0.008	**0.088**
9	0.007	0.379	0.008	**0.394**
11	0.022	0.399	0.036	**0.456**
13	0.530	8.462	0.050	**9.042**
17	0.020	0.998	0.009	**1.027**
21	1.770	0.465	0.020	**2.254**
23	23.218	0.104	0.009	**23.331**
27	0.073	0.005	0.002	**0.080**
31	0.610	0.721	0.003	**1.334**
35	0.796	0.372	0.003	**1.171**
37	0.162	0.005	0.004	**0.171**
39	0.008	1.683	0.009	**1.699**
41	0.522	1.366	0.007	**1.895**
43	0.099	0.570	0.003	**0.672**
45	1.664	0.818	0.006	**2.487**
47	0.086	0.007	0.003	**0.096**
49	4.611	0.340	0.007	**4.959**
51	0.249	0.416	0.002	**0.667**
53	0.008	0.006	0.005	**0.019**
57	2.727	11.751	0.018	**14.496**
59	3.578	2.981	0.018	**6.577**
63	0.221	0.661	0.005	**0.887**
65	0.489	1.118	0.004	**1.610**
67	0.644	0.576	0.003	**1.224**
69	0.091	0.213	0.002	**0.307**
P51	0.114	0.006	0.001	**0.121**
P23	0.226	0.721	0.003	**0.950**
P19	0.492	0.439	0.015	**0.945**
P11	0.061	0.004	0.022	**0.087**
Total	43.600	35.822	2.975	**82.397**
Average	1.406	1.156	0.096	**2.658**

Table 19. Detailed Test Results for Link Layer Handoff Components (in Seconds) – Roaming from Foreign Network 1 to Foreign Network 2.

Data Set	Registration & Routing Upate								Total
	FA's Process-ing of RRQ	FA - HA Trans-mission Delay (for RRQ)	Authenti-cation	Update Mobility Binding & Create Tunnel	Delete Old Tunnel & Update Route	HA Accepts RRQ & Sends RRP to FA	HA - FA Trans-mission Delay (for RRP)	FA's Process-ing of RRP	
1	0.004	0.005	0.004	0.004	0.008	3.000	0.003	0.004	**3.032**
5	0.000	0.005	0.004	0.008	0.004	3.004	0.004	0.004	**3.033**
7	0.004	0.003	0.004	0.004	0.008	3.000	0.006	0.004	**3.033**
9	0.004	0.006	0.004	0.004	0.004	3.003	0.008	0.000	**3.033**
11	0.004	0.003	0.004	0.008	0.004	3.004	0.005	0.005	**3.037**
13	0.000	0.004	0.004	0.008	0.004	3.004	0.004	0.004	**3.032**
17	0.004	0.000	0.008	0.004	0.004	3.004	0.005	0.004	**3.033**
21	0.004	0.004	0.004	0.004	0.008	3.000	0.005	0.004	**3.033**
23	0.004	0.005	0.004	0.004	0.004	3.004	0.004	0.004	**3.033**
27	0.004	0.002	0.004	0.008	0.004	3.004	0.007	0.000	**3.033**
31	0.000	0.004	0.004	0.008	0.004	3.004	0.005	0.004	**3.033**
35	0.004	0.003	0.004	0.004	0.008	3.004	0.006	0.004	**3.037**
37	0.004	0.004	0.004	0.008	0.004	3.004	0.005	0.004	**3.037**
39	0.000	0.007	0.004	0.004	0.008	3.000	0.006	0.004	**3.033**
41	0.004	0.005	0.004	0.004	0.004	3.004	0.004	0.004	**3.033**
43	0.004	0.002	0.008	0.004	0.004	3.008	0.007	0.004	**3.041**
45	0.004	0.005	0.004	0.004	0.008	3.000	0.004	0.004	**3.033**
47	0.000	0.017	0.004	0.004	0.004	3.004	0.004	0.004	**3.041**
49	0.000	0.005	0.004	0.008	0.004	3.004	0.004	0.004	**3.033**
51	0.004	0.004	0.004	0.008	0.004	3.004	0.005	0.004	**3.037**
53	0.000	0.007	0.004	0.004	0.004	3.004	0.006	0.004	**3.033**
57	0.004	0.004	0.004	0.008	0.004	3.004	0.005	0.004	**3.037**
59	0.000	0.007	0.004	0.004	0.004	3.004	0.005	0.004	**3.032**
63	0.004	0.002	0.004	0.008	0.004	3.004	0.007	0.000	**3.033**
65	0.004	0.006	0.004	0.004	0.004	3.004	0.007	0.000	**3.033**
67	0.004	0.004	0.004	0.004	0.004	3.004	0.005	0.004	**3.033**
69	0.004	0.004	0.004	0.008	0.004	3.004	0.005	0.004	**3.037**
P51	0.004	0.004	0.004	0.004	0.008	3.000	0.005	0.004	**3.033**
P23	0.005	0.005	0.004	0.004	0.008	3.000	0.003	0.004	**3.033**
P19	0.004	0.005	0.004	0.004	0.004	3.004	0.004	0.004	**3.033**
P11	0.004	0.002	0.004	0.008	0.004	3.004	0.007	0.000	**3.033**
Total	0.093	0.143	0.132	0.172	0.156	93.099	0.160	0.105	**94.060**
Average	0.003	0.005	0.004	0.006	0.005	3.003	0.005	0.003	**3.034**

Table 20. Detailed Test Results for Registration and Routing Update Components[13] (in Seconds) – Roaming from Foreign Network 1 to Foreign Network 2.

[13] Legend: FA refers to Foreign Agent. HA refers to Home Agent. RRQ refers to Registration Request. RRP refers to Registration Reply.

B. ROAMING FROM FOREIGN NETWORK 2 TO FOREIGN NETWORK 1

The collated results for the individual test cases conducted for the scenario when the mobile node roams from foreign network 2 to foreign network 1 are detailed in Tables 21, 22 and 23.

Data Set	Move Detection		Registration & Routing Upate	Total
	Link Layer Handoff	Agent Discovery		
2	0.402	0.106	3.037	**3.544**
4	0.880	0.075	3.033	**3.988**
6	0.056	0.099	3.033	**3.188**
8	0.067	0.054	3.033	**3.154**
12	0.905	2.847	3.033	**6.785**
14	0.015	0.087	3.037	**3.139**
16	1.654	0.117	3.033	**4.804**
18	0.271	0.042	3.033	**3.346**
22	1.809	0.474	3.033	**5.316**
26	0.889	0.079	3.037	**4.005**
28	11.032	0.017	3.037	**14.086**
30	0.069	0.056	3.037	**3.162**
32	4.759	0.664	3.033	**8.456**
34	1.115	0.063	3.033	**4.211**
36	0.072	0.096	3.033	**3.201**
38	0.162	0.097	3.033	**3.292**
40	0.063	0.027	3.033	**3.124**
42	0.070	0.040	3.037	**3.147**
44	0.679	0.105	3.033	**3.817**
46	13.494	0.024	3.033	**16.552**
48	0.083	0.090	3.033	**3.206**
50	0.690	1.050	3.037	**4.776**
52	0.479	0.075	3.037	**3.591**
54	0.209	0.047	3.033	**3.289**
56	0.745	0.096	3.033	**3.873**
58	0.136	0.060	3.033	**3.230**
60	0.066	0.078	3.033	**3.176**
62	0.755	0.044	3.033	**3.832**
64	0.068	0.043	3.033	**3.144**
66	0.126	0.047	3.033	**3.206**
68	1.162	0.052	3.033	**4.247**
70	0.191	0.052	3.037	**3.280**
Total	43.169	6.905	97.092	**147.166**
Average	1.349	0.216	3.034	**4.599**

Table 21. Detailed Test Results for Mobile IP Handoff Components (in Seconds) – Roaming from Foreign Network 2 to Foreign Network 1.

Data Set	Link Layer Handoff			Total
	Scanning	Authentication	Association	
2	0.006	0.392	0.004	**0.402**
4	0.050	0.827	0.003	**0.880**
6	0.049	0.004	0.003	**0.056**
8	0.060	0.004	0.003	**0.067**
12	0.214	0.682	0.009	**0.905**
14	0.005	0.004	0.006	**0.015**
16	0.426	1.128	0.100	**1.654**
18	0.141	0.126	0.003	**0.271**
22	1.795	0.011	0.003	**1.809**
26	0.296	0.590	0.003	**0.889**
28	0.005	11.015	0.011	**11.032**
30	0.062	0.005	0.003	**0.069**
32	0.007	4.750	0.003	**4.759**
34	0.005	1.108	0.003	**1.115**
36	0.064	0.005	0.003	**0.072**
38	0.070	0.090	0.003	**0.162**
40	0.056	0.004	0.003	**0.063**
42	0.062	0.005	0.003	**0.070**
44	0.320	0.356	0.003	**0.679**
46	3.091	10.401	0.003	**13.494**
48	0.073	0.004	0.005	**0.083**
50	0.023	0.662	0.005	**0.690**
52	0.012	0.464	0.003	**0.479**
54	0.201	0.005	0.003	**0.209**
56	0.131	0.611	0.003	**0.745**
58	0.129	0.005	0.003	**0.136**
60	0.058	0.004	0.003	**0.066**
62	0.095	0.658	0.003	**0.755**
64	0.060	0.005	0.003	**0.068**
66	0.115	0.007	0.003	**0.126**
68	0.260	0.846	0.055	**1.162**
70	0.060	0.128	0.003	**0.191**
Total	8.001	34.906	0.262	**43.169**
Average	0.250	1.091	0.008	**1.349**

Table 22. Detailed Test Results for Link Layer Handoff Components (in Seconds) – Roaming from Foreign Network 2 to Foreign Network 1.

Data Set	Registration & Routing Upate								Total
	FA's Process-ing of RRQ	FA - HA Trans-mission Delay (for RRQ)	Authenti-cation	Update Mobility Binding & Create Tunnel	Delete Old Tunnel & Update Route	HA Accepts RRQ & Sends RRP to FA	HA - FA Trans-mission Delay (for RRP)	FA's Process-ing of RRP	
2	0.004	0.003	0.004	0.008	0.004	3.004	0.006	0.004	**3.037**
4	0.005	0.006	0.004	0.004	0.004	3.004	0.006	0.000	**3.033**
6	0.000	0.007	0.004	0.004	0.008	3.000	0.006	0.004	**3.033**
8	0.004	0.004	0.004	0.004	0.008	3.000	0.005	0.004	**3.033**
12	0.000	0.006	0.004	0.004	0.008	3.004	0.007	0.000	**3.033**
14	0.004	0.004	0.004	0.008	0.004	3.004	0.005	0.004	**3.037**
16	0.004	0.005	0.004	0.004	0.008	3.000	0.004	0.004	**3.033**
18	0.000	0.006	0.004	0.008	0.004	3.004	0.003	0.004	**3.033**
22	0.004	0.006	0.004	0.004	0.004	3.003	0.004	0.004	**3.033**
26	0.004	0.003	0.004	0.008	0.004	3.004	0.006	0.004	**3.037**
28	0.004	0.003	0.004	0.008	0.004	3.004	0.006	0.004	**3.037**
30	0.004	0.004	0.004	0.004	0.008	3.004	0.005	0.004	**3.037**
32	0.004	0.005	0.004	0.004	0.008	3.000	0.004	0.004	**3.033**
34	0.004	0.002	0.004	0.008	0.004	3.004	0.003	0.004	**3.033**
36	0.004	0.002	0.004	0.008	0.004	3.003	0.004	0.004	**3.033**
38	0.000	0.005	0.004	0.008	0.004	3.004	0.004	0.004	**3.033**
40	0.000	0.008	0.004	0.004	0.004	3.003	0.006	0.004	**3.033**
42	0.004	0.004	0.004	0.008	0.004	3.004	0.005	0.004	**3.037**
44	0.004	0.001	0.008	0.004	0.004	3.004	0.004	0.004	**3.033**
46	0.004	0.006	0.004	0.004	0.008	3.000	0.007	0.000	**3.033**
48	0.000	0.005	0.004	0.004	0.008	3.004	0.004	0.004	**3.033**
50	0.004	0.005	0.004	0.004	0.008	3.004	0.004	0.004	**3.037**
52	0.004	0.005	0.004	0.008	0.004	3.004	0.004	0.004	**3.037**
54	0.004	0.003	0.004	0.008	0.004	3.003	0.007	0.000	**3.033**
56	0.004	0.005	0.004	0.004	0.008	3.000	0.004	0.004	**3.033**
58	0.000	0.006	0.004	0.008	0.004	3.004	0.003	0.004	**3.033**
60	0.000	0.007	0.004	0.004	0.008	3.000	0.006	0.004	**3.033**
62	0.000	0.008	0.004	0.004	0.004	3.004	0.005	0.004	**3.033**
64	0.000	0.007	0.004	0.004	0.004	3.004	0.006	0.004	**3.033**
66	0.004	0.004	0.004	0.004	0.008	3.000	0.005	0.004	**3.033**
68	0.004	0.004	0.004	0.004	0.004	3.004	0.005	0.004	**3.033**
70	0.004	0.003	0.004	0.008	0.004	3.004	0.006	0.004	**3.037**
Total	0.089	0.152	0.132	0.180	0.176	96.092	0.159	0.112	**97.092**
Average	0.003	0.005	0.004	0.006	0.005	3.003	0.005	0.003	**3.034**

Table 23. Detailed Test Results for Registration and Routing Update Components[14] (in Seconds) – Roaming from Foreign Network 2 to Foreign Network 1.

[14] Legend: FA refers to Foreign Agent. HA refers to Home Agent. RRQ refers to Registration Request. RRP refers to Registration Reply.

LIST OF REFERENCES

[1] Postel, J., *Internet Protocol*, RFC 791, September 1981.

[2] Postel, J., *Transmission Control Protocol*, RFC 793, September 1981.

[3] Postel, J., *User Datagram Protocol*, RFC 768, August 1980.

[4] Perkins, C., *IP Mobility Support for IPv4*, RFC 3344, August 2002.

[5] Raab, S. and Chandra, M. W., *Mobile IP Technology and Applications: Real-world solutions for Mobile IP configuration and management*, 1st ed., pp.3-143 & 183-204, Cisco Press, Indiana, June 2005.

[6] Solomon, J. D., *Mobile IP: The Internet Unplugged*, 1st ed., pp.1-153 & 273-300, Prentice Hall, New Jersey, 1998.

[7] Socolofsky, T. and Kale, C., *A TCP/IP Tutorial*, RFC 1180, January 1991.

[8] Stevens, W. R., *TCP/IP Illustrated, Volume 1: The Protocols*, 1st ed., pp. 62-63, Addison-Wesley, Massachusetts, 1994.

[9] Perkins, C., *IP Mobility Support*, RFC 2002, October 1996.

[10] Mondal, A. S., *Mobile IP: Present State and Future*, 1st ed., pp. 3-107 & 196-202, Kluwer Academic / Plenum Publishers, New York, 2003.

[11] Droms, R., *Dynamic Host Configuration Protocol*, RFC 2131, March 1997.

[12] Postel, J., *Internet Control Message Protocol*, RFC 792, September 1981.

[13] Deering, S., *ICMP Router Discovery Messages*, RFC 1256, September 1991.

[14] Perkins, C., *Minimal Encapsulation within IP*, RFC 2004, October 1996.

[15] Farinacci, D., Li, T., Hanks, S., Meyer, D. and Traina, P., *Generic Routing Encapsulation (GRE)*, RFC 2784, March 2000.

[16] Montenegro, G., *Reverse Tunneling for Mobile IP, revised*, RFC 3024, January 2001.

[17] Perkins, C., *IP Encapsulation within IP*, RFC 2003, October 1996.

[18] Plummer, D. C., *An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*, RFC 826, November 1982.

[19] Postel, J., *Multi-LAN Address Resolution*, RFC 925, October 1984.

[20] Krawczyk, H., Bellare, M. and Canetti, R., *HMAC: Keyed-Hashing for Message Authentication*, RFC 2104, February 1997.

[21] Mills, D.L., *Network Time Protocol (Version 3): Specification, Implementation and Analysis*, RFC 1305, March 1992.

[22] Tanase, M., *IP Spoofing: An Introduction*, Online: http://www.securityfocus.com/infocus/1674, Last Accessed: October 2006.

[23] Nachreiner, C., *Anatomy of an ARP Poisoning Attack*, Online: http://www.watchguard.com/infocenter/editorial/135324.asp, Last Accessed: October 2006.

[24] LAN/MAN Standards Committee of the IEEE Computer Society, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, ANSI/IEEE Standard 802.11, 1999 Edition (R2003).

[25] Gast, M. S., *802.11 Wireless Networks: The Definitive Guide*, 1st ed., pp. 1-85 & 114-139, O'Reilly & Associates, Inc., California, 2002.

[26] Edney, J. and Arbaugh, W.A., *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*, 1st ed., pp. 51-65 & 311-336, Addison-Wesley, Massachusetts, 2005.

[27] Singh, G., *CS4130 – Wireless Mobile Computing: Wireless LANs*, NPS Lecture Notes, Summer 2006.

[28] LAN/MAN Standards Committee of the IEEE Computer Society, *IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture*, IEEE Standard 802, 2001 Edition.

[29] LAN/MAN Standards Committee of the IEEE Computer Society, *Part 2: Logical Link Control*, ANSI/IEEE Standard 802.2, 1998 Edition (R2003).

[30] LAN/MAN Standards Committee of the IEEE Computer Society, *Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*, IEEE Standard 802.3, 2005 Edition.

[31] Cisco Systems, Inc., *Cisco IOS IP Mobility Configuration Guide, Release 12.4*, Online: http://www.cisco.com/application/pdf/en/us/guest/products/ps6350/c2001/ccmigration_09186a0080789b48.pdf, Last Accessed: December 2006.

[32] Shenker, S., Partridge, C. and Guerin, R., *Specification of Guaranteed Quality of Service*, RFC 2212, September 1997.

[33] Wong, K.D., Dutta, A., Burns, J., Jain, R. and Young, K., *Merging IP and Wireless Networks: A Multilayered Mobility Management Scheme for Auto-configured Wireless IP Networks,* IEEE Wireless Communications, October 2003, Online: http://www1.cs.columbia.edu/~dutta/research/ieee-wireless-imm.pdf, Last Accessed: December 2006.

[34] Cisco Systems, Inc., *Cisco Mobile Client User Guide Release 2.0*, Online: http://www.cisco.com/application/pdf/en/us/guest/products/ps6527/c2001/ccmigration_09186a00806674d8.pdf, Last Accessed: November 2006.

[35] *Kismet*, Online: http://www.kismetwireless.net, Last Accessed: December 2006.

[36] *Wireshark*, Online: http://www.wireshark.org, Last Accessed: December 2006.

[37] *WinDump: tcpdump for Windows*, Online: http://www.winpcap.org/windump, Last Accessed: December 2006.

[38] Texas Instruments, *Including VoIP over WLAN in a Seamless Next-Generation Wireless Environment*, Web ProForum Tutorials, The International Engineering Consortium, Online: http://www.iec.org/online/tutorials/acrobat/ti_voip_wlan.pdf, Last Accessed: November 2006.

[39] Cisco Systems, Inc., *VoIP: An In-Depth Analysis*, Online: http://www.ciscopress.com/articles/article.asp?p=606583&seqNum=1&rl=1, Last Accessed: December 2006.

[40] LAN/MAN Standards Committee of the IEEE Computer Society, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements*, IEEE Standard 802.11e, 2005 Edition.

[41] Chaskar, H., *Requirements of a Quality of Service (QoS) Solution for Mobile IP*, RFC 3583, September 2003.

[42] Wainhouse Research, *A Technical FAQ: Frequently Asked Questions About Voice and Video over IP Networks*, January 2003, Online: http://www.wainhouse.com/files/papers/wr-faq-ip-conf.pdf, Last Accessed: November 2006.

[43] Cisco Systems, Inc., *Cisco IOS IP Mobility Command Reference, Release 12.4T*, Online: http://www.cisco.com/application/pdf/en/us/guest/products/ps6441/c2001/ccmigration_09186a00804c69cc.pdf, Last Accessed: November 2006.

[44] Cisco Systems, Inc., *Cisco IOS IP Configuration Guide: Configuring DHCP*, Online: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfdhcp.pdf, Last Accessed: November 2006.

[45] Cisco Systems, Inc., *Configuring a Cisco Router to be an NTP Server*, Online: http://www.cisco.com/univercd/cc/td/doc/product/netsec/secmgmt/asdmhelp/5_0procs/conf-ips/ntpserv.pdf, Last Accessed: November 2006.

[46] Linksys, A Division of Cisco Systems, Inc., *WAP 11 – Instant Wireless Network Access Point*, Online: http://www.linksys.com/servlet/Satellite?childpagename=US%2FLayout&packedargs=page%3D2%26cid%3D1115416835852%26c%3DL_Content_C1&pagename=Linksys%2FCommon%2FVisitorWrapper&SubmittedElement=Linksys%2FFormSubmit%2FProductDownloadSearch&sp_prodsku=1121194967244, Last Accessed: November 2006.

[47] Dell Inc., *Dell TrueMobile 1170 Wireless Base Station User's Guide*, Online: http://support.dell.com/support/edocs/comm/1h824/en/index.htm, Last Accessed: November 2006.

BIBLIOGRAPHY

1. Cisco Systems, Inc., *Introduction to Mobile IP*, Online: http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/moblip/mobil_ip.pdf, Last Accessed: November 2006.

2. Cisco Systems, Inc., *Cisco Mobile IP White Paper*, Online: http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/mbxul_wp.pdf, Last Accessed: November 2006.

3. Cisco Systems, Inc., *Cisco IOS Local-Area Mobility – A Cisco IOS Software Solution to Business Needs to Enable Mobility Within the Enterprise Network*, Online: http://www.cisco.com/warp/public/cc/pd/iosw/ioft/lam/tech/lamso_wp.pdf, Last Accessed: November 2006.

4. Cisco Systems, Inc., *Mobile IP, Release 12.0(1)T*, Online: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/mobileip.pdf, Last Accessed: November 2006.

5. Cisco Systems, Inc., *Cisco IOS IP and IP Routing Configuration Guide: Configuring Mobile IP*, Online: http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt1/1cdmobip.pdf, Last Accessed: November 2006.

6. Cisco Systems, Inc., *Cisco Mobile Client for Windows 2000, XP*, Online: http://www.cisco.com/application/pdf/en/us/guest/products/ps6744/c1650/cdccont_0900aecd8035da89.pdf, Last Accessed: November 2006.

7. Cisco Systems, Inc., *Mobile Networking Technology*, Online: http://www.ceenet.org/workshops/lectures2004/Gaetan_Feige/CEE_NET.ppt, Last Accessed: November 2006.

8. Zhou, H., Mutka, M.W. and Ni, L.M., *IP Address Handoff in the MANET*, IEEE INFOCOM 2004, Online: http://www.ieee-infocom.org/2004/Papers/50_4.PDF, Last Accessed: November 2006.

9. Blondia, C., Casals, O., Cerdà, L., Wijngaert, N., Willems, G. and Cleyn, P. D., *Performance Comparison of Low Latency Mobile IP Schemes*, Online: http://www.pats.ua.ac.be/publications/2003/WiOpt03_final.pdf, Last Accessed: November 2006.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. George W. Dinolt
   Naval Postgraduate School
   Monterey, California

4. J. D. Fulp
   Naval Postgraduate School
   Monterey, California

5. Gurminder Singh
   Naval Postgraduate School
   Monterey, California

6. John H. Gibson
   Naval Postgraduate School
   Monterey, California

7. Thomas H. Hoivik, TDSI Coordinator
   Naval Postgraduate School
   Monterey, California

8. Yeo Tat Soon, Director, Temasek Defence Systems Institute (TDSI)
   National University of Singapore
   Singapore

9. Tan Lai Poh, Temasek Defence Systems Institute (TDSI)
   National University of Singapore
   Singapore

10. Tan Sian Boon, Human Resource Department
    Defence Science & Technology Agency
    Singapore

11. Eugene Chang
    Defence Science & Technology Agency
    Singapore

12. Tan Ah Tuan
Defence Science & Technology Agency
Singapore

13. Chua Kay Lee
Cisco Systems Singapore
Singapore

14. Ng Chin Chin
Defence Science & Technology Agency
Singapore