Mobile IP Administration Guide

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303-4900
U.S.A.

Part Number 806-4042–10
June 2000

Copyright 2000 Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, California 94303-4900 U.S.A. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, docs.sun.com, AnswerBook, AnswerBook2, and Solaris are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

Federal Acquisitions: Commercial Software–Government Users Subject to Standard License Terms and Conditions.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2000 Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, Californie 94303-4900 Etats-Unis. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées du système Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, docs.sun.com, AnswerBook, AnswerBook2, et Solaris sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REPONDRE A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.

Contents

Preface

The *Mobile IP Administration Guide* provides information about configuring and managing the Mobile IP framework installed in your Solaris™ operating environment. This book assumes that you have already installed the SunOS™ 5.8 operating system, and you have set up any networking software that you plan to use. The SunOS 5.8 operating system is part of the Solaris product family, which includes the Solaris Common Desktop Environment (CDE). The SunOS 5.8 operating system is compliant with AT&T's Unix® System V, Release 4 operating system.

Note - The Solaris operating environment runs on two types of hardware, or platforms: SPARC™ and IA. The Solaris operating environment runs on both 64-bit and 32-bit address spaces. The information in this document pertains to both platforms and address spaces unless called out in a special chapter, section, note, bullet, figure, table, example, or code example.

Who Should Use This Book

This book is intended for anyone who administers one or more systems that run the Solaris 8 release. To use this book, you should have one to two years of UNIX® system administration experience. Attending UNIX system administration training courses might be helpful, if you lack the experience.

How This Book Is Organized

Chapter 1 provides an overview of Mobile IP.

Chapter 2 describes conceptual information about the Solaris implementation of Mobile IP.

Chapter 3 describes how to configure the various Mobile IP parameters using the Mobile IP configuration file. This chapter also provides other useful procedures related to Mobile IP.

Glossary provides definitions of key Mobile IP terms.

Related Books

For useful information about Mobile IP, refer to the following documents:

- Perkins, Charles E. *Mobile IP Design Principles and Practices*. Massachusetts, 1998, Addison-Wesley Publishing Company.
- *RFC 2002* from the Internet Engineering Task Force (IETF). Available online at [`http://ietf.org/rfc.html`].
- Solomon, James D. *Mobile IP The Internet Unplugged*. New Jersey, 1998, Prentice-Hall, Inc.

Ordering Sun Documents

Fatbrain.com, an Internet professional bookstore, stocks select product documentation from Sun Microsystems, Inc.

For a list of documents and how to order them, visit the Sun Documentation Center on Fatbrain.com at `http://www1.fatbrain.com/documentation/sun`.

Accessing Sun Documentation Online

The docs.sun.com[SM] Web site enables you to access Sun technical documentation online. You can browse the docs.sun.com archive or search for a specific book title or subject. The URL is `http://docs.sun.com`.

What Typographic Conventions Mean

The following table describes the typographic changes used in this book.

TABLE P–1 Typographic Conventions

Typeface or Symbol	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories; on-screen computer output	Edit your `.login` file. Use `ls –a` to list all files. `machine_name% you have mail.`
`AaBbCc123`	What you type, contrasted with on-screen computer output	`machine_name%` **`su`** `Password:`
AaBbCc123	Command-line placeholder: replace with a real name or value	To delete a file, type **`rm`** *filename*.
AaBbCc123	Book titles, new words or terms, or words to be emphasized	Read Chapter 6 in *User's Guide*. These are called *class* options. Do *not* save changes yet.

Shell Prompts in Command Examples

The following table shows the default system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

TABLE P–2 Shell Prompts

Shell	**Prompt**
C shell prompt	`machine_name%`
C shell superuser prompt	`machine_name#`
Bourne shell and Korn shell prompt	`$`
Bourne shell and Korn shell superuser prompt	#

CHAPTER 1

Overview of Mobile IP

Mobile IP (Internet Protocol) enables the transfer of information to and from mobile computers, such as laptops and wireless communications. The mobile computer can change its location to a foreign network and still access and communicate with and through the mobile computer's home network. The Solaris implementation of Mobile IP supports only IPv4.

Introduction

Current versions of the Internet Protocol (IP) assume that the point at which a computer attaches to the Internet or a network is fixed and its IP address identifies the network to which it is attached. Datagrams are sent to a computer based on the location information contained in the IP address.

If a mobile computer, or *mobile node*, moves to a new network while keeping its IP address unchanged, its address does not reflect the new point of attachment. Consequently, existing routing protocols cannot route datagrams to the mobile node correctly. In this situation, you must reconfigure the mobile node with a different IP

address representative of its new location, which is a cumbersome process. Thus, under the current Internet Protocol, if the mobile node moves without changing its address, it loses routing; but if it does change its address, it loses connections.

Mobile IP solves this problem by allowing the mobile node to use two IP addresses: a fixed *home address* and a *care-of address* that changes at each new point of attachment. Mobile IP enables a computer to roam freely on the Internet or an organization's network while still maintaining the same home address. Consequently, computing activities are not disrupted when the user changes the computer's point of attachment to the Internet or an organization's network. Instead, the network is updated with the new location of the mobile node. See *Glossary* for definitions of terms associated with Mobile IP.

The following figure illustrates the general Mobile IP topology.

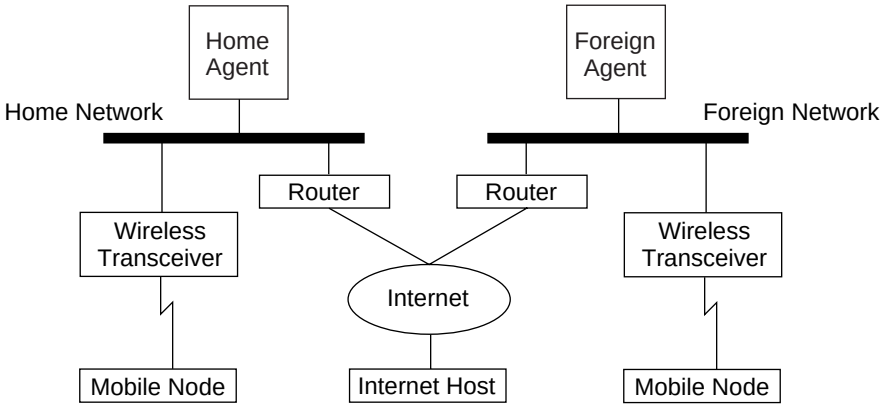

Figure 1–1 Mobile IP Topology

Using the previous illustration's Mobile IP topology, the following scenario shows how a datagram moves from one point to another within the Mobile IP framework.

1. The Internet host sends a datagram to the mobile node using the mobile node's home address (normal IP routing process).
2. If the mobile node is on its home network, the datagram is delivered through the normal IP process to the mobile node. Otherwise, the home agent picks up the datagram.
3. If the mobile node is on a foreign network, the home agent forwards the datagram to the foreign agent.
4. The foreign agent delivers the datagram to the mobile node.
5. Datagrams from the mobile node to the Internet host are sent using normal IP routing procedures. If the mobile node is on a foreign network, the packets are delivered to the foreign agent. The foreign agent forwards the datagram to the Internet host.

In the case of wireless communications, the illustrations depict the use of wireless transceivers to transmit the datagrams to the mobile node. Also, all datagrams

between the Internet host and the mobile node use the mobile node's home address regardless of whether the mobile node is on a home or foreign network. The care-of address is used only for communication with mobility agents and is never seen by the Internet host.

Mobile IP Functional Entities

Mobile IP introduces the following new functional entities:

- **Mobile Node (MN)**–Host or router that changes its point of attachment from one network to another.
- **Home Agent (HA)**–Router on a mobile node's home network that intercepts datagrams destined for the mobile node, and delivers them through the care-of address. The home agent also maintains current location information for the mobile node.
- **Foreign Agent (FA)**–Router on a mobile node's visited network that provides routing services to the mobile node while the mobile node is registered.

How Mobile IP Works

Mobile IP enables routing of IP datagrams to mobile nodes. The mobile node's home address always identifies the mobile node, regardless of its current point of attachment to the Internet or an organization's network. When away from home, a care-of address associates the mobile node with its home address by providing information about the mobile node's current point of attachment to the Internet or an organization's network. Mobile IP uses a registration mechanism to register the care-of address with a home agent.

The home agent redirects datagrams from the home network to the care-of address by constructing a new IP header that contains the mobile node's care-of address as the destination IP address. This new header then encapsulates the original IP datagram, causing the mobile node's home address to have no effect on the encapsulated datagram's routing until it arrives at the care-of address. This type of encapsulation is also called *tunneling*. After arriving at the care-of address, each datagram is de-encapsulated and then delivered to the mobile node.

The following illustration shows a mobile node residing on its home network, Network A, before the mobile node moves to a foreign network, Network B. Both networks support Mobile IP. The mobile node is always associated with its home network by its permanent IP address, `128.226.3.30`. Though Network A has a

home agent, datagrams destined for the mobile node are delivered through the normal IP process.

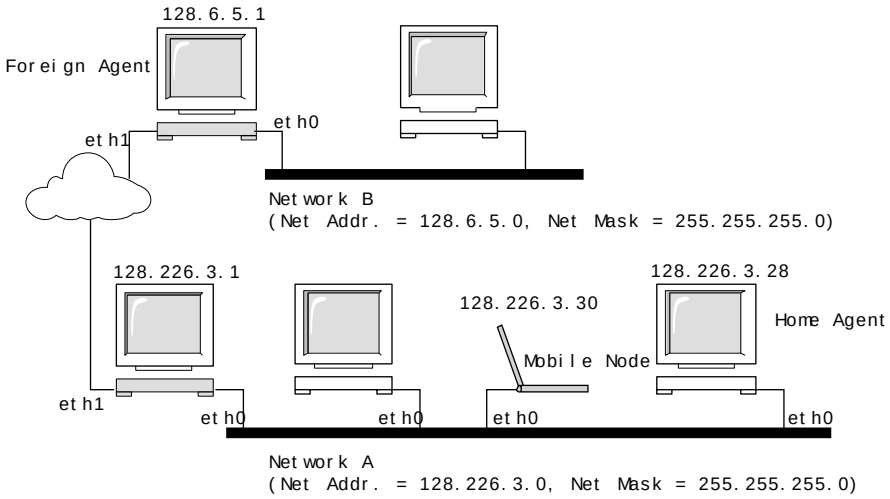

Figure 1–2 Mobile Node Residing on Home Network

The following illustration shows the mobile node moving to a foreign network, Network B. Datagrams destined for the mobile node are intercepted by the home agent on the home network, Network A, encapsulated, and sent to the foreign agent on Network B. Upon receiving the encapsulated datagram, the foreign agent strips off the outer header and delivers the datagram to the mobile node visiting Network B.

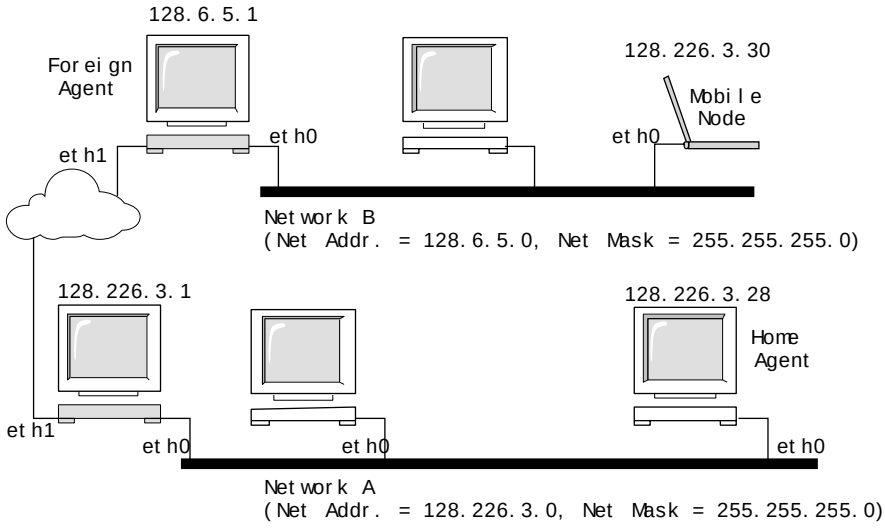

Figure 1–3 Mobile Node Moving to a Foreign Network

The care-of address might belong to a foreign agent, or might be acquired by the mobile node through Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol (PPP). In the latter case, a mobile node is said to have a co-located care-of address.

The mobile node uses a special *registration* process to keep its home agent informed about its current location. Whenever a mobile node moves from its home network to a foreign network, or from one foreign network to another, it chooses a foreign agent on the new network and uses it to forward a registration message to its home agent.

Mobility agents (home agents and foreign agents) advertise their presence using *agent advertisement* messages. A mobile node can optionally solicit an agent advertisement message from any locally attached mobility agents through an *agent solicitation* message. A mobile node receives these agent advertisements and determines whether they are on its home network or a foreign network.

When the mobile node detects that it is located on its home network, it operates without mobility services. If returning to its home network from being registered elsewhere, the mobile node *deregisters* with its home agent.

Care-of Addresses

Mobile IP provides the following alternative modes for the acquisition of a care-of address:

- A foreign agent provides a *foreign agent care-of address* through its agent advertisement messages. In this case, the care-of address is an IP address of the foreign agent. The foreign agent is the endpoint of the tunnel and, on receiving tunneled datagrams, de-encapsulates them and delivers the inner datagram to the mobile node. In this mode, many mobile nodes can share the same care-of address. This sharing reduces demands on the IPv4 address space and can also save bandwidth, because the forwarded packets, from the foreign agent to the mobile node, are not encapsulated. Saving bandwidth is important on wireless links.
- A mobile node acquires a *co-located care-of address* as a local IP address through some external means, which the mobile node then associates with one of its own network interfaces. The address might be dynamically acquired as a temporary address by the mobile node, such as through DHCP. The address might also be owned by the mobile node as a long-term address for its use only while visiting some foreign network. When using a co-located care-of address, the mobile node serves as the endpoint of the tunnel and performs de-encapsulation of the datagrams tunneled to it.

Co-located care-of address enables a mobile node to function without a foreign agent, for example, in networks that have not yet deployed a foreign agent.

If a mobile node is using a co-located care-of address, the mobile node must be located on the link identified by the network prefix of this care-of address. Otherwise, datagrams destined to the care-of address are undeliverable.

Agent Discovery

A mobile node uses a method known as agent discovery to determine the following information:

- When the node has moved from one network to another
- Whether the network is the node's home or a foreign network
- What is the foreign agent care-of address offered by each foreign agent on that network

Mobility agents transmit *agent advertisements* to advertise their services on a network. In the absence of agent advertisements, a mobile node can solicit advertisements. This is known as *agent solicitation*.

Agent Advertisement

Mobile nodes use agent advertisements to determine their current point of attachment to the Internet or to an organization's network. An agent advertisement

is an Internet Control Message Protocol (ICMP) router advertisement that has been extended to also carry a mobility agent advertisement extension.

A foreign agent can be too busy to serve additional mobile nodes. However, a foreign agent must continue to send agent advertisements. This way, mobile nodes that are already registered with it will know that they have not moved out of range of the foreign agent and that the foreign agent has not failed.

Agent Solicitation

Every mobile node should implement agent solicitation. The mobile node uses the same procedures, defaults, and constants for agent solicitation, as specified for ICMP router solicitation messages.

The rate at which a mobile node sends solicitations is limited by the mobile node. The mobile node can send three initial solicitations at a maximum rate of one per second while searching for an agent. After registering with an agent, the rate at which solicitations are sent is reduced, to limit the overhead on the local network.

Mobile IP Registration

When the mobile node receives an agent advertisement, the mobile node registers through the foreign agent, even when the mobile node might be able to acquire its own co-located care-of address. This feature enables sites to restrict access to mobility services. Through agent advertisements, mobile nodes detect when they have moved from one subnet to another.

Mobile IP registration provides a flexible mechanism for mobile nodes to communicate their current reachability information to their home agent. The registration process enables mobile nodes to perform the following tasks:

- Request forwarding services when visiting a foreign network
- Inform their home agent of their current care-of address
- Renew a registration that is due to expire
- Deregister when they return home

Registration messages exchange information between a mobile node, a foreign agent, and the home agent. Registration creates or modifies a mobility binding at the home agent, associating the mobile node's home address with its care-of address for the specified lifetime.

The registration process also enables mobile nodes to:

- Register with multiple foreign agents

- Deregister specific care-of addresses while retaining other mobility bindings
- Discover the address of a home agent if the mobile node is not configured with this information

Mobile IP defines the following registration processes for a mobile node:

- If a mobile node is registering a foreign agent care-of address, the mobile node registers using that foreign agent.
- If a mobile node is using a co-located care-of address, and receives an agent advertisement from a foreign agent on the link on which it is using this care-of address, the mobile node registers using that foreign agent (or another foreign agent on this link).
- If a mobile node uses a co-located care-of address, the mobile node registers directly with its home agent.
- If a mobile node returns to its home network, the mobile node deregisters with its home agent.

These registration processes involve the exchange of registration requests and registration reply messages. When registering using a foreign agent, the registration process takes the following steps, which the subsequent illustration depicts:

1. The mobile node sends a registration request to the prospective foreign agent to begin the registration process.
2. The foreign agent processes the registration request and then relays it to the home agent.
3. The home agent sends a registration reply to the foreign agent to grant or deny the request.
4. The foreign agent processes the registration reply and then relays it to the mobile node to inform it of the disposition of its request.

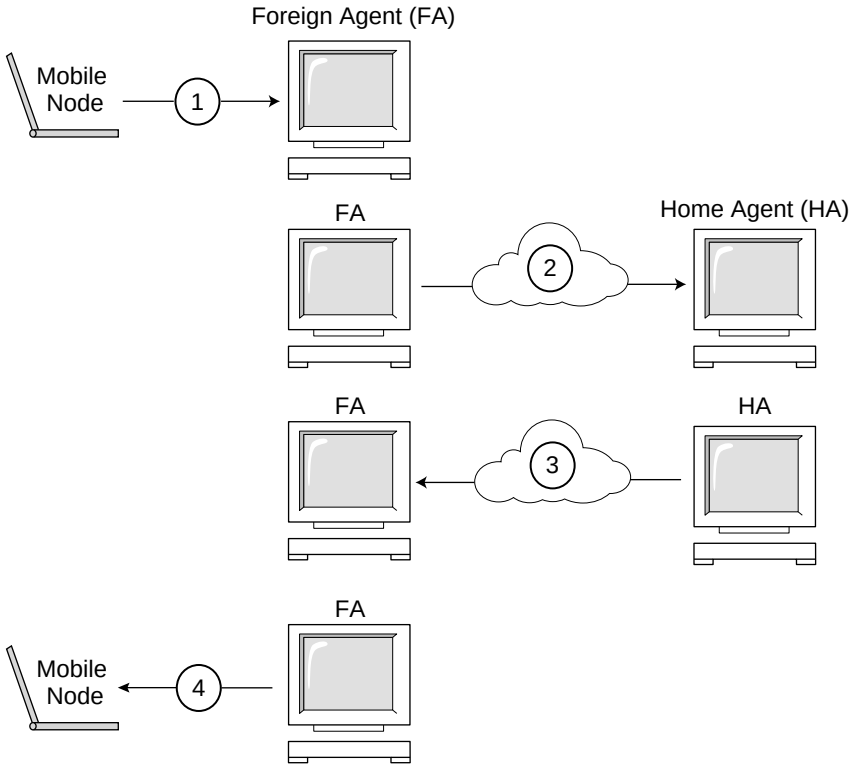

Figure 1–4 Mobile IP Registration Process

When the mobile node registers directly with its home agent, the registration process requires only the following steps:

- The mobile node sends a deregistration request to the home agent.
- The home agent sends a registration reply to the mobile node, granting or denying the request.

Network Access Identifier (NAI)

AAA servers, in use within the Internet, provide authentication and authorization services for dial-up computers. These services are likely to be equally valuable for mobile nodes using Mobile IP when the nodes are attempting to connect to foreign domains with AAA servers. AAA servers identify clients by using the Network Access Identifier (NAI). A mobile node can identify itself by including the NAI in the Mobile IP registration request.

Since the NAI is typically used to identify the mobile node uniquely, the mobile node's home address is not always necessary to provide that function. Thus, it is possible for a mobile node to authenticate itself, and be authorized for connection to the foreign domain, without even having a home address. To request that a home

address be assigned, a message containing the mobile node NAI extension can set the home address field to zero in the registration request.

Mobile IP Message Authentication

Each mobile node, foreign agent, and home agent supports a mobility security association between the various Mobile IP components, indexed by their security parameter index (SPI) and IP address. In the case of the mobile node, this address is its home address. Registration messages between a mobile node and its home agent are authenticated with the Mobile-home authentication extension. In addition to Mobile-home authentication, which is mandatory, you can use the optional Mobile-foreign agent and Home-foreign agent authentications.

Mobile Node Registration Request

A mobile node registers with its home agent using a *registration request* message so that its home agent can create or modify a mobility binding for that mobile node (for example, with a new lifetime). The foreign agent can relay the registration request to the home agent. However, if the mobile node is registering a co-located care-of address, then the mobile node can send the registration request directly to the home agent.

Registration Reply Message

A mobility agent returns a *registration reply* message to a mobile node that has sent a registration request message. If the mobile node is requesting service from a foreign agent, that foreign agent receives the reply from the home agent and subsequently relays it to the mobile node. The reply message contains the necessary codes to inform the mobile node about the status of its request, along with the lifetime granted by the home agent, which can be smaller than the original request. The registration reply can also contain a dynamic home address assignment.

Foreign Agent Considerations

The foreign agent plays a mostly passive role in Mobile IP registration. A foreign agent adds all registered mobile nodes to its visitor table. It relays registration requests between mobile nodes and home agents, and, when it provides the care-of address, de-encapsulates datagrams for delivery to the mobile node. It also sends periodic agent advertisement messages to advertise its presence.

Home Agent Considerations

Home agents play an active role in the registration process. The home agent receives registration requests from the mobile node (perhaps relayed by a foreign agent), updates its record of the mobility bindings for this mobile node, and issues a suitable registration reply in response to each. The home agent also forwards packets to the mobile node when the mobile node is away from its home network.

Dynamic Home Agent Discovery

In some cases, the mobile node might not know its home agent address when the mobile node attempts to register. If the mobile node does not know its home agent address, the mobile node can use dynamic home agent address resolution to learn the address of its home agent. In this case, the mobile node sets the home agent field of the registration request to the subnet-directed broadcast address of the mobile node's home network. Each home agent that receives a registration request with a broadcast destination address rejects the mobile node's registration by returning a rejection registration reply. By doing so, the mobile node can use the home agent's unicast IP address indicated in the rejection reply when the mobile node next attempts registration.

Routing Datagrams to and From Mobile Nodes

This section describes how mobile nodes, home agents, and foreign agents cooperate to route datagrams to and from mobile nodes that are connected to a foreign network.

Encapsulation Types

Home agents and foreign agents support tunneling datagrams using one of the available encapsulation methods (IP in IP Encapsulation, Minimal Encapsulation, or Generic Routing Encapsulation). Mobile nodes that use a co-located care-of address can receive tunneled datagrams using any encapsulation type.

Unicast Datagram Routing

When registered on a foreign network, the mobile node chooses a default router using the following rules:

- If the mobile node is registered using a foreign agent care-of address, then the mobile node chooses its default router from among the router addresses advertised in the ICMP router advertisement portion of that agent advertisement message. The mobile node can also consider the IP source address of the agent advertisement as another possible choice for the IP address of a default router.
- If the mobile node is registered directly with its home agent using a co-located care-of address, then the mobile node chooses its default router from among those advertised in any ICMP router advertisement message that it receives. The chosen default router network prefix must match the mobile nodes externally obtained care-of address. If the mobile node's externally obtained care-of address matches the IP source address of the agent advertisement under the network prefix, the mobile node can also consider that IP source address as another possible choice for the IP address of a default router.

Broadcast Datagrams

When a home agent receives a broadcast datagram, it does not forward the datagram to any mobile nodes in its mobility binding list. However, the home agent does forward the datagram if a mobile node has requested forwarding of broadcast datagrams. For each registered mobile node, the home agent forwards received broadcast datagrams to the mobile node; the method depends on how the configuration of the home agent specifies categories of broadcast datagrams forwarded to mobile nodes.

Multicast Datagram Routing

To receive multicasts, a mobile node joins the multicast group in one of the following ways:

- If a multicast router exists on the visited subnet, the mobile node uses this local multicast router. If the mobile node is using a co-located care-of address, it uses this address as the source IP address of its Internet Group Management Protocol (IGMP) messages. Otherwise, it uses its home address.
- If the mobile node's home agent is a multicast router, the mobile node can join groups using a bidirectional tunnel to its home agent. The mobile node tunnels IGMP messages to its home agent. The home agent then forwards multicast datagrams down the tunnel to the mobile node.

A mobile node that sends datagrams to a multicast group also has the following options:

- Send directly on the visited network
- Send through a tunnel to its home agent

Multicast routing depends on the IP source address. Therefore, a mobile node that sends multicast datagrams directly on the visited network uses a co-located care-of address as the IP source address. Similarly, a mobile node that tunnels a multicast datagram to its home agent uses its home address as the IP source address of both the multicast datagram and the encapsulating datagram. This second option assumes that the home agent is a multicast router.

Security Considerations

In many cases, mobile computers use wireless links to connect to the network. Wireless links are particularly vulnerable to passive eavesdropping, active replay attacks, and other active attacks.

Though Mobile IP cannot reduce or eliminate this vulnerability, Mobile IP can authenticate the Mobile IP messages. The default algorithm used is MD5, with a key size of 128 bits. The default operational mode requires that this 128–bit key precede and succeed the data to be hashed. The foreign agent also supports authentication using MD5 and key sizes of 128 bits or greater, with manual key distribution. Mobile IP can support more authentication algorithms, algorithm modes, key distribution methods, and key sizes.

Tunneling can be a significant vulnerability, especially if registration is not authenticated. Also, the Address Resolution Protocol (ARP) is not authenticated, and can potentially be used to steal another host's traffic.

CHAPTER 2

Managing Mobile IP

This chapter describes the components provided with the Solaris implementation of Mobile IP. To use Mobile IP, you must first configure the Mobile IP configuration file using the parameters and commands described in the following sections.

Overview of the Solaris Mobile IP Implementation

The mobility agent software incorporates home agent and foreign agent functionality. The Solaris Mobile IP software does not provide a client mobile node. Only the agent functionality is provided. Each network with mobility support should have at least one static (non-mobile) host running this software. The following RFC functions are supported in the Solaris implementation of Mobile IP:

RFC 2002	(Agent only) IP Mobility Support
RFC 2003	IP Encapsulation within IP

RFC 2794	Mobile IP Network Access Identifier Extension for IPv4

The base Mobile IP protocol (RFC 2002) does not address the problem of scalable key distribution and treats key distribution as an orthogonal issue. The Solaris Mobile IP software utilizes only manually configured keys, specified in a configuration file.

The functionality in the following IETF drafts are also supported in the Solaris implementation of Mobile IP:

- **draft-ietf-mobileip-challenge-09.txt** – Mobile IP Challenge/Response Extensions
- **draft-ietf-mobileip-vendor-ext-09.txt** – Mobile IP Vendor/Organization-Specific Extensions

The following RFC functions are not supported in the Solaris implementation of Mobile IP:

RFC 1700	General Routing Encapsulation
RFC 1701	General Routing Encapsulation
RFC 2004	Minimal Encapsulation Within IP
RFC 2344	Reverse Tunneling for Mobile IP

In addition, the Solaris implementation of Mobile IP does not support the forwarding of multicast or broadcast traffic to a mobile node visiting a foreign network.

See `mipagent`(1M) man page for additional information.

Mobile IP Configuration File

The `mipagent` command reads configuration information from the `/etc/inet/mipagent.conf` configuration file at startup. Mobile IP uses the `/etc/inet/mipagent.conf` configuration file to initialize the Mobile IP mobility agent. When configured and deployed, the mobility agent issues periodic router advertisements and responds to router discovery solicitation messages as well as Mobile IP registration messages.

See the `mipagent.conf`(4) man page for a description of file attributes and the `mipagent`(1M) man page for a description of its usage.

Configuration File Format

The Mobile IP configuration file consists of sections. Each section has a unique name and is enclosed in square brackets. Each section contains one or more labels. You assign values to the labels using the following format:

```
[Section_name]
      Label-name = Value-assigned
```

"Configuration File Sections and Labels" on page 31 describes the section names, labels, and possible values.

Sample Configuration Files

The default Solaris installation provides the following sample configuration files in the `/etc/inet` directory:

- `mipagent.conf-sample`–Contains a sample configuration for a Mobile IP agent that provides both foreign and home agent functionality.
- `mipagent.conf.fa-sample`–Contains a sample configuration for a Mobile IP agent that provides only foreign agent functionality.
- `mipagent.conf.ha-sample`–Contains a sample configuration for a Mobile IP agent that provides only home agent functionality.

These sample configuration files contain sample mobile node address and security settings. Before you can implement Mobile IP, you must create a configuration file with the name `mipagent.conf` and place it in the `/etc/inet` directory. This file contains the configuration settings that satisfy your Mobile IP implementation requirements. You can also choose one of the sample configuration files, modify it with your addresses and security settings, and copy it to `/etc/inet/mipagent.conf`.

"How to Create the Mobile IP Configuration File" on page 45 shows the procedures to perform.

`mipagent.conf-sample` File

The following listing shows the sections, labels, and values contained in the `mipagent.conf-sample` file. "Configuration File Sections and Labels" on page 31 describes the syntax, sections, labels, and values.

```
[General]
   Version = 1.0    # version number for the configuration file. (required)

[Advertisements hme0]
   HomeAgent = yes
   ForeignAgent = yes
   PrefixFlags = yes
   RegLifetime = 200
   AdvLifetime = 200
   AdvFrequency = 5
   AdvertiseOnBcast = yes

[GlobalSecurityParameters]
   MaxClockSkew = 300
   HA-FAauth = yes
   MN-FAauth = yes
   Challenge = no
   KeyDistribution = files

[Pool 1]
   BaseAddress = 10.68.30.7
   Size = 4

[SPI 257]
   ReplayMethod = none
   Key = 11111111111111111111111111111111

[SPI 258]
   ReplayMethod = none
   Key = 15111111111111111111111111111111

[Address 10.1.1.1]
   Type = node
   SPI = 258

[Address mobilenode@sun.com]
   Type = node
   SPI = 257
   Pool = 1

[Address Node-Default]
   Type = node
   SPI = 258
   Pool = 1

[Address 10.68.30.36]
   Type = agent
   SPI = 257
```

Example–`mipagent.conf.fa-sample` File

The following listing shows the sections, labels, and values contained in the `mipagent.conf.fa-sample` file. “Configuration File Sections and Labels” on page 31 describes the syntax, sections, labels, and values. The `mipagent.conf.fa-sample` file shows a configuration that provides only foreign

agent functionality. This sample file does not contain a `Pool` section, because pools are used only by a home agent. Otherwise, this file is the same as the `mipagent.conf-sample` file.

```
[General]
   Version = 1.0    # version number for the configuration file. (required)

[Advertisements hme0]
   HomeAgent = no
   ForeignAgent = yes
   PrefixFlags = yes
   RegLifetime = 200
   AdvLifetime = 200
   AdvFrequency = 5
   AdvertiseOnBcast = yes

[GlobalSecurityParameters]
   MaxClockSkew = 300
   HA-FAauth = yes
   MN-FAauth = yes
   Challenge = no
   KeyDistribution = files

[SPI 257]
   ReplayMethod = none
   Key = 11111111111111111111111111111111

[SPI 258]
   ReplayMethod = none
   Key = 15111111111111111111111111111111

[Address 10.1.1.1]
   Type = node
   SPI = 258

[Address mobilenode@sun.com]
   Type = node
   SPI = 257
   Pool = 1

[Address Node-Default]
   Type = node
   SPI = 258
   Pool = 1

[Address 10.68.30.36]
   Type = agent
   SPI = 257
```

Example–`mipagent.conf.ha-sample` File

The following listing shows the sections, labels, and values contained in the `mipagent.conf.ha-sample` file. “Configuration File Sections and Labels” on page 31 describes the syntax, sections, labels, and values. The

`mipagent.conf.ha-sample` file shows a configuration that provides only home agent functionality. Otherwise, this file is the same as the `mipagent.conf-sample` file.

```
[General]
   Version = 1.0    # version number for the configuration file. (required)

[Advertisements hme0]
   HomeAgent = yes
   ForeignAgent = no
   PrefixFlags = yes
   RegLifetime = 200
   AdvLifetime = 200
   AdvFrequency = 5
   AdvertiseOnBcast = yes

[GlobalSecurityParameters]
   MaxClockSkew = 300
   HA-FAauth = yes
   MN-FAauth = yes
   Challenge = no
   KeyDistribution = files

[Pool 1]
   BaseAddress = 10.68.30.7
   Size = 4

[SPI 257]
   ReplayMethod = none
   Key = 11111111111111111111111111111111

[SPI 258]
   ReplayMethod = none
   Key = 15111111111111111111111111111111

[Address 10.1.1.1]
   Type = node
   SPI = 258

[Address mobilenode@sun.com]
   Type = node
   SPI = 257
   Pool = 1

[Address Node-Default]
   Type = node
   SPI = 258
   Pool = 1

[Address 10.68.30.36]
   Type = agent
   SPI = 257
```

Configuration File Sections and Labels

The Mobile IP configuration file contains the following sections:

- `General` (Required)
- `Advertisements` (Required)
- `GlobalSecurityParameters` (Optional)
- `Pool` (Optional)
- `SPI` (Optional)
- `Address` (Optional)

The `General` and `GlobalSecurityParameters` sections contain information relevant to the operation of the Mobile IP agent and can appear only once in the configuration file.

`General` Section

The `General` section contains only one label: the version number of the configuration file. The `General` section has the following syntax:

```
[General]
     Version = 1.0
```

`Advertisements` Section

The `Advertisements` section contains the `HomeAgent` and `ForeignAgent` labels, as well as other labels. You must include a different `Advertisements` section for each interface on the local host that provides Mobile IP services. The `Advertisements` section has the following syntax:

```
[Advertisements Interface-name]
     HomeAgent = <yes/no>
     ForeignAgent = <yes/no>
     .
     .
```

Typically, your system has a single interface (`le0`, `hme0`, and so on) and supports both home agent and foreign agent operations. If this is the case, say for `hme0`, then the `yes` value is assigned to both the `HomeAgent` and `ForeignAgent` labels as follows:

```
[Advertisements hme0]
     HomeAgent = yes
     ForeignAgent = yes
     .
     .
```

The following table describes the labels and values that you can use in the `Advertisements` section.

TABLE 2–1 `Advertisements` Section Labels and Values

Label	Value	Description
`HomeAgent`	`yes` or `no`	Determines if mipagent provides home agent functionality.
`ForeignAgent`	`yes` or `no`	Determines if mipagent provides foreign agent functionality
`PrefixFlags`	`yes` or `no`	Specifies if advertisements include the optional prefix length extension.
`RegLifetime`	`n`	The maximum lifetime value accepted in registration requests, in seconds.
`AdvLifetime`	`n`	The maximum length of time that the advertisement is considered valid in the absence of further advertisements, in seconds.
`AdvFrequency`	`n`	Time between two consecutive advertisements, in seconds.

`GlobalSecurityParameters` Section

The `GlobalSecurityParameters` section contains the `maxClockSkew`, `HA-FAauth`, `MN-FAauth`, `Challenge`, and `KeyDistribution` labels. This section defines the security parameters. The `GlobalSecurityParameters` section has the following syntax:

```
[GlobalSecurityParameters]
     MaxClockSkew = n
     HA-FAauth = <yes/no>
     MN-FAauth = <yes/no>
     Challenge = <yes/no>
     KeyDistribution = files
```

The Mobile IP protocol provides message replay protection by allowing timestamps to be present in the messages. If the clocks differ, the home agent returns an error to the mobile node with the current time and the mobile node can re-register using the current time. You use the `MaxClockSkew` label to configure the maximum number of seconds that differ between the home agent and the mobile node's clocks. The default value is 300 seconds.

The `HA-FAauth` and `MN-FAauth` labels enable or disable the requirement for home-foreign and mobile-foreign authentication, respectively. The default value is disabled. You use the `challenge` label so that the foreign agent issues challenges to the mobile node in its advertisements. The label is used for replay protection. The default value is disabled here, also.

The following table describes the labels and values that you can use in the `GlobalSecurityParameters` section.

TABLE 2–2 `GlobalSecurityParameters` Section Labels and Values

Label	Value	Description
`MaxClockSkew`	`n`	The number of seconds that mipagent accepts as a difference between its own local time and the time found in registration requests.
`HA-FAauth`	`yes` or `no`	Specifies if HA-FA authentication extensions must be present in registration requests and replies.
`MN-FAauth`	`yes` or `no`	Specifies if MN-FA authentication extensions must be present in registration requests and replies.
`Challenge`	`yes` or `no`	Specifies if the foreign agent includes challenges in its mobility advertisements.
`KeyDistribution`	`files`	Must be set to files.

Pool Section

Mobile nodes can be assigned dynamic addresses by the home agent. The dynamic address assignment is done within the mipagent independently of DHCP. You can create an address pool that can be used by mobile nodes requesting a home address. Address pools are configured through the Pool section in the configuration file.

The Pool section contains the BaseAddress and Size labels. The Pool section has the following syntax:

```
[Pool Pool-identifier]
     BaseAddress = IP-address
     Size = size
```

Note - If you use a Pool identifier, then it must also exist in the mobile node's Address section.

You use the Pool section to define address pools that can be assigned to the mobile nodes. You use the BaseAddress label to set the first IP address in the pool. You use the Size to specify the number of addresses available in the pool.

For example, if IP Addresses 192.168.1.1 through 192.168.1.100 are reserved in pool 10, the Pool section has the following entry:

```
[Pool 10]
     BaseAddress = 192.168.1.1
     Size = 100
```

Note - Address ranges should not encompass the broadcast address. For example, you should not assign BaseAddress = 192.168.1.200 and Size = 60, because this range encompasses the broadcast address 192.168.1.255.

The following table describes the labels and values used in the Pool section.

TABLE 2–3 Pool Section Labels and Values

Label	Value	Description
BaseAddress	n.n.n.n	First address in the address pool
Size	n	Number of addresses in the pool

TABLE 2–3 `Pool` Section Labels and Values *(continued)*

`SPI` Section

Because the Mobile IP protocol requires message authentication, you must identify the security context using a Security Parameter Index (SPI). You define the security context in the `SPI` section. You must include a different `SPI` section for each security context defined. A numerical ID identifies the security context. The Mobile IP protocol reserves the first 256 SPIs. Therefore, you should use only SPI values greater than 256. The SPI section contains security-related information, such as shared secrets and replay protection.

The `SPI` section also contains the `ReplayMethod` and `Key` labels. This section defines the security contexts. The `SPI` section has the following syntax:

```
[SPI SPI-identifier]
     ReplayMethod = <none/timestamps>
     Key = key
```

Two communicating peers must share the same SPI identifier. You must configure them with the same key and replay method. You specify the key as a string of hex digits. The maximum length is 16 bytes. For example, if the key is 16 bytes long, and contains the hex values `0` through `f`, the key string might look like:

```
Key = 0102030405060708090a0b0c0d0e0f10
```

Keys must have an even number of digits (corresponding to the two digits per byte representation).

The following table describes the labels and values that you can use in the SPI section.

TABLE 2–4 `SPI` Section Labels and Values

Label	Value	Description
`ReplayMethod`	`none` or `timestamps`	Specifies the type of replay authentication used for the SPI.
`Key`	`x`	Authentication key in hexadecimal.

Address Section

The Solaris implementation of Mobile IP enables you to configure mobile nodes in one of three methods. Each method is configured in the Address section. The first method follows the traditional Mobile IP protocol, and requires that each mobile node have a home address. The second method enables a mobile node to be identified through its Network Access Identifier (NAI). The last method enables you to configure a *default* mobile node, which can be used by any mobile node that has the proper SPI value and related keying material.

Mobile Node With a Home Address

The Address section for a mobile node with a home address contains the Type and SPI labels that define the address type and SPI identifier. The Address section has the following syntax:

```
[Address address]
     Type = <agent/node>
     SPI = SPI-identifier
```

You must include an Address section in a home agent's configuration file for each mobile node supported. Mobile nodes have the Type label set to node.

If Mobile IP message authentication is required between the foreign and home agent, you must include an Address section for each peer with which an agent needs to communicate. Mobility agents have the Type field set to agent.

The SPI value that you configure must represent an SPI section that is present in the configuration file.

The following table describes the labels and values that you can use in the Address section for a mobile node with a home address.

TABLE 2–5 Address Section Labels and Values—Mobile Node With a Home Address

Label	Value	Description
Type	node or agent	Specifies that the entry is for a mobile node or a mobility agent.
SPI	n	Specifies the SPI value for the associated entry.

Mobile Node Identified by its NAI

The `Address` section for a mobile node identified by its NAI contains the `Type`, `SPI`, and `Pool` labels. The NAI parameter enables you to identify mobile nodes through their NAI. The `Address` section, using the NAI parameter, has the following syntax:

```
[Address NAI]
     Type = Node
     SPI = SPI-identifier
     Pool = Pool-identifier
```

In order to make use of pools, you identify mobile nodes through their NAI. The `Address` section permits you to configure an NAI, as opposed to a home address. An NAI uses the format `user@domain` format. You use the `Pool` label to specify which address pool to use in order to allocate the home address to the mobile node.

The following table describes the labels and values that you can use in the `Address` section for a mobile node identified by its NAI.

TABLE 2–6 `Address` Section Labels and Values—Mobile Node Identified by its NAI

Label	Value	Description
`Type`	`node`	Specifies entry for a mobile node.
`SPI`	`n`	Specifies SPI value for the associated entry.
`Pool`	`n`	Allocates the pool from which an address is assigned to a mobile node.

You must have corresponding `SPI` and `Pool` sections for the `SPI` and `Pool` labels defined in an `Address` section with a mobile node identified by its NAI, as shown in the following illustration.

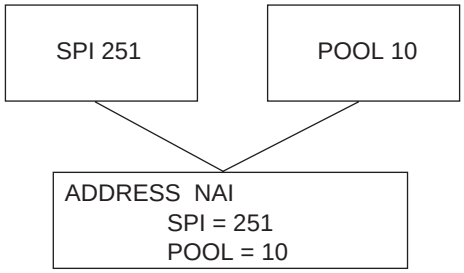

Figure 2–1 Corresponding SPI and Pool Sections for Address Section With Mobile Node Identified by its NAI

Default Mobile Node

The `Address` section for a default mobile node contains the `Type`, `SPI`, and `Pool` labels. The `Default-Node` parameter enables you to permit all mobile nodes to get service if they have the correct SPI (defined in this section). The `Address` section, using the `Default-Node` parameter, has the following syntax:

```
[Address Default-Node]
     Type = Node
     SPI = SPI-identifier
     Pool = Pool-identifier
```

The `Default-Node` enables you to reduce the size of the configuration file; otherwise, each mobile node requires its own section. However, the `Default-Node` does pose a security risk. If a mobile node is no longer trusted for any reason, you need to update the security information on all trusted mobile nodes. This task can be very tedious. However, you can use the `Default-Node` in networks that consider security risks unimportant.

The following table describes the labels and values that you can use in the `Address` section for a default mobile node.

TABLE 2–7 `Address` Section Labels and Values—Default Mobile Node

Label	Value	Description
`Type`	`node`	Specifies entry for a mobile node.
`SPI`	`n`	Specifies SPI value for the associated entry.
`Pool`	`n`	Allocates the pool from which an address is assigned to a mobile node.

You must have corresponding `SPI` and `Pool` sections for the `SPI` and `Pool` labels defined in the `Address` section with a default mobile node, as shown in the following illustration.

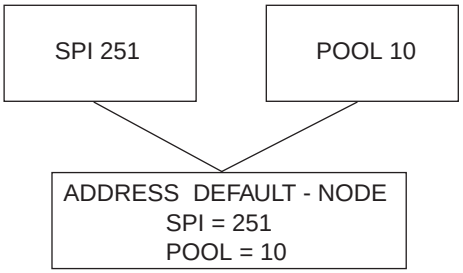

Figure 2–2 Corresponding SPI and Pool Sections for Address Section With a Default Mobile Node

Configuring the Mobility IP Agent

You can use the `mipagentconfig` command to configure the mobility agent. This command enables you to create or modify any parameter in the `/etc/inet/mipagent.conf` configuration file. Specifically, you can change any setting, and add or delete mobility clients, pools, and SPIs. The `mipagentconfig` command has the following syntax:

```
# mipagentconfig <command> <parameter> <value>
```

The following table describes the commands that you can use with `mipagentconfig` to create or modify parameters in the `/etc/inet/mipagent.conf` configuration file.

TABLE 2–8 `mipagentconfig` Commands

Command	Description
`add`	Used to add advertisement parameters, security parameters, SPIs, and addresses to the configuration file
`change`	Used to change advertisement parameters, security parameters, SPIs, and addresses in the configuration file
`delete`	Used to delete advertisement parameters, security parameters, SPIs, and addresses from the configuration file
`get`	Used to display current settings in the configuration file

See the `mipagentconfig`(1M) man page for a description of command parameters and acceptable values. “Modifying the Mobile IP Configuration File” on page 49 provides procedures that use the `mipagentconfig` command.

Mobile IP Mobility Agent Status

You can use the `mipagentstat` command to display a foreign agent’s visitors list and a home agent’s binding table. The following examples show the type of information displayed when using this command. To display the foreign agent visitor list, you use the `mipagentstat` command’s `–f` option. To display the home agent binding table, you use the `mipagentstat` command’s `–b` option. The following examples show typical output when using these options.

EXAMPLE 2–1 Foreign Agent Visitor List

```
Mobile Node     Home Agent     Time Granted    Time Remaining

foobar.xyz.com  ha1.xyz.com    600             125
10.1.5.23       10.1.5.1       1000            10
```

EXAMPLE 2–2 Home Agent Binding Table

```
Mobile Node     Foreign Agent  Time Granted    Time Remaining

foobar.xyz.com  fa1.tuv.com    600             125
10.1.5.23       123.2.5.12     1000            10
```

See `mipagentstat`(1M) command for more information about the command's options. "Displaying Mobility Agent Status" on page 57 provides procedures that use the `mipagentstat` command.

Mobile IP State Information

Upon shutdown, the `mipagent` daemon stores internal state information in `/var/inet/mipagent_state`. This happens only when the `mipagent` provides services as a home agent. This state information includes the list of mobile nodes being supported as a home agent, their current care-of addresses, and remaining registration lifetimes. If the `mipagent` program is terminated (for maintenance) and restarted, `mipagent_state` is used to recreate as much of the mobility agent's internal state as possible in an effort to minimize service disruption for mobile nodes that might be visiting other networks. If `mipagent_state` exists, it is read immediately after `mipagent.conf` every time `mipagent` is started or restarted.

`snoop` Extensions for Mobile IP

Mobile IP extensions have been added to the `snoop`(1M) command to identify Mobile IP traffic on the link. See the `snoop`(1M) man page for more information.

The following example shows the output of `snoop` running on the mobile node, `mip-mn2`.

EXAMPLE 2–3 Output From `snoop` Command

```
mip-mn2# snoop
Using device /dev/hme (promiscuous mode)
  mip-fa2 -> 224.0.0.1    ICMP Router advertisement (Lifetime 200s [1]:
{mip-fa2-80 2147483648}), (Mobility Agent Extension), (Prefix Lengths),
(Padding)
  mip-mn2 -> mip-fa2   Mobile IP reg rqst
```

(Continuation)

```
mip-fa2 -> mip-mn2   Mobile IP reg reply (OK code 0)
```

This example shows that the mobile node received one of the periodically sent mobility agent advertisements from the foreign agent, `mip-fa2`. Then `mip-mn2` sent a registration request to `mip-fa2`, and in response, received a registration reply. The registration reply indicates that the mobile node successfully registered with it's home agent.

CHAPTER 3

Deploying Mobile IP

This chapter provides procedures for modifying, adding, deleting, and displaying parameters in the Mobile IP configuration file. This chapter also shows you how to display mobility agent status.

Configuring the Mobile IP Configuration File

When you configure the `mipagent.conf` file for the first time, you need to perform the following tasks:

1. Depending on your organization's host's requirements, determine what functionality your Mobile IP agent will provide:
   - Foreign agent functionality only
   - Home agent functionality only
   - Both foreign and home agent functionality
2. Create the `/etc/inet/mipagent.conf` file and enter the settings you require using the procedures described in this section. You can also copy one of the following files to `/etc/inet/mipagent.conf` and modify it according to your requirements:
   - For foreign agent functionality, copy `/etc/inet/mipagent.conf.fa-sample`.
   - For home agent functionality , copy `/etc/inet/mipagent.conf.ha-sample`.
   - For both foreign agent and home agent functionality, copy `/etc/inet/mipagent.conf-sample`.
3. You can reboot your system to invoke the boot script that starts the `mipagent` daemon. You can also start `mipagent` by typing the following command on a command line:

```
# /etc/inet.d/mipagent start
```

Configuring the Mobile IP Configuration File Task Map

The following table provides a brief description of the tasks described in this section.

TABLE 3–1 Configuring the Mobile IP Configuration File Task Map

Task	Description	For Instructions, Go to ...
Creating the Mobile IP configuration file	Involves creating the `/etc/inet/mipagent.conf` file or copying one of the sample files	"How to Create the Mobile IP Configuration File" on page 45
Configuring the `General` section	Involves entering the version number into the `General` section of the Mobile IP configuration file	"How to Configure the `General` Section" on page 46
Configuring the `Advertisements` section	Involves adding labels and values or changing them in the `Advertisements` section of the Mobile IP configuration file	"How to Configure the `Advertisements` Section" on page 46
Configuring the `GlobalSecurityParameters` section	Involves adding labels and values or changing them in the `GlobalSecurityParameters` section of the Mobile IP configuration file	"How to Configure the `GlobalSecurityParameters` Section" on page 47
Configuring the `Pool` section	Involves adding labels and values or changing them in the `Pool` section of the Mobile IP configuration file	"How to Configure the `Pool` Section" on page 47
Configuring the `SPI` section	Involves adding labels and values or changing them in the `SPI` section of the Mobile IP configuration file	"How to Configure the `SPI` Section" on page 48
Configuring the `Address` section	Involves adding labels and values or changing them in the `Address` section of the Mobile IP configuration file	"How to Configure the `Address` Section" on page 48

▼ How to Create the Mobile IP Configuration File

1. **Become superuser on the system where you want to enable Mobile IP.**

2. **Depending on your preference, do one of the following substeps.**

   a. **In the `/etc/inet` directory, create an empty file named `mipagent.conf`.**

   b. **From the following list, copy the sample file that provides the functionality you want to the file `/etc/inet/mipagent.conf`.**

      - `/etc/inet/mipagent.conf.fa-sample`
      - `/etc/inet/mipagent.conf.ha-sample`

- /etc/inet/mipagent.conf-sample

3. **Add or change configuration parameters in the** /etc/inet/mipagent.conf **file according to your configuration requirements. The remaining procedures in this section describe the steps that you perform.**

▼ How to Configure the General Section

If you copied one of the sample files, you can omit this procedure because the sample file contains this entry.

♦ **Edit the** /etc/inet/mipagent.conf **file and add the following lines.**

```
[General]
     Version = 1.0
```

Note - The /etc/inet/mipagent.conf file must contain the preceding entry.

"General Section" on page 31 provides descriptions of the labels and values used in this section.

▼ How to Configure the Advertisements Section

♦ **Edit the** /etc/inet/mipagent.conf **file and add or change the following lines using the values required for your configuration.**

```
[Advertisements Interface-name]
     HomeAgent = <yes/no>
     ForeignAgent = <yes/no>
     PrefixFlags = <yes/no>
     RegLifetime = n
     AdvLifetime = n
     AdvFrequency = n
```

Note - You must include a different `Advertisements` section for each interface on the local host that provides Mobile IP services.

"`Advertisements` Section" on page 31 provides descriptions of the labels and values used in this section.

▼ How to Configure the `GlobalSecurityParameters` Section

♦ **Edit the `/etc/inet/mipagent.conf` file and add or change the following lines using the values required for your configuration.**

```
[GlobalSecurityParameters]
     MaxClockSkew = n
     HA-FAauth = <yes/no>
     MN-FAauth = <yes/no>
     Challenge = <yes/no>
     KeyDistribution = files
```

"`GlobalSecurityParameters` Section" on page 32 provides descriptions of the labels and values used in this section.

▼ How to Configure the `Pool` Section

♦ **Edit the `/etc/inet/mipagent.conf` file and add or change the following lines using the values required for your configuration.**

```
[Pool Pool-identifier]
     BaseAddress = IP-address
     Size = size
```

"`Pool` Section" on page 34 provides descriptions of the labels and values used in this section.

▼ How to Configure the SPI Section

♦ **Edit the /etc/inet/mipagent.conf file and add or change the following lines using the values required for your configuration.**

```
[SPI SPI-identifier]
     ReplayMethod = <none/timestamps>
     Key = key
```

Note - You must include a different SPI section for each security context deployed.

"SPI Section" on page 35 provides descriptions of the labels and values used in this section.

▼ How to Configure the Address Section

♦ **Edit the /etc/inet/mipagent.conf file and add or change the following lines using the values required for your configuration.**

■ **For mobile node with a home address or for an agent**

```
[Address address]
     Type = <agent/node>
     SPI = SPI-identifier
```

■ **For mobile node identified by its NAI**

```
[Address NAI]
     Type = Node
     SPI = SPI-identifier
     Pool = Pool-identifier
```

■ **For default mobile node**

```
[Address Default-Node]
     Type = Node
     SPI = SPI-identifier
     Pool = Pool-identifier
```

"Address Section" on page 36 provides descriptions of the labels and values used in this section.

Modifying the Mobile IP Configuration File

This section shows you how to modify the Mobile IP configuration file using the mipagentconfig(1M) command. It also shows you how to display the current settings of parameter destinations.

"Configuring the Mobility IP Agent" on page 39 provides a conceptual description of the mipagentconfig(1M) command's usage. You can also review the mipagentconfig(1M) man page.

Modifying the Mobile IP Configuration File Task Map

TABLE 3–2 Modifying the Mobile IP Configuration File Task Map

Task	Description	For Instructions, Go to ...
Modifying the General section	Uses the mipagentconfig change command to change the value of a label in the General section of the Mobile IP configuration file	"How to Modify the General Section" on page 50
Modifying the Advertisements section	Uses the mipagentconfig change command to change the value of a label in the Advertisements section of the Mobile IP configuration file	"How to Modify the Advertisements Section" on page 51

TABLE 3–2 Modifying the Mobile IP Configuration File Task Map *(continued)*

Task	Description	For Instructions, Go to ...
Modifying the `GlobalSecurityParameters` section	Uses the `mipagentconfig change` command to change the value of a label in the `GlobalSecurityParameters` section of the Mobile IP configuration file	"How to Modify the `GlobalSecurityParameters` Section" on page 51
Modifying the `Pool` section	Uses the `mipagentconfig change` command to change the value of a label in the `Pool` section of the Mobile IP configuration file	"How to Modify the `Pool` Section" on page 52
Modifying the `SPI` section	Uses the `mipagentconfig change` command to change the value of a label in the `SPI` section of the Mobile IP configuration file	"How to Modify the `SPI` Section" on page 52
Modifying the `Address` section	Uses the `mipagentconfig change` command to change the value of a label in the `Address` section of the Mobile IP configuration file	"How to Modify the `Address` Section" on page 53
Adding or deleting parameters	Uses the `mipagentconfig add` or `delete` commands to add new parameters, labels, and values or delete existing ones in any of the sections of the Mobile IP configuration file	"How to Add or Delete Configuration File Parameters" on page 54
Displaying the current settings of parameter destinations	Uses the `mipagentconfig get` command to display current settings of any section of the Mobile IP configuration file	"How to Display Current Parameter Settings in the Configuration File" on page 55

▼ How to Modify the `General` Section

1. **Become superuser on the system where you want to enable Mobile IP.**

2. **On a command line, type the following command for each label that you want to modify in the `General` section.**

```
# mipagentconfig change <label> <value>
```

The following example shows how you might change the version number (in the future) in the configuration file's `General` section.

EXAMPLE 3–1 Changing Parameters in the `General` Section

```
# mipagentconfig change version 2
```

▼ How to Modify the `Advertisements` Section

1. **Become superuser on the system where you want to enable Mobile IP.**

2. **On a command line, type the following command for each label that you want to modify in the `Advertisements` section.**

```
# mipagentconfig change adv device-name <label> <value>
```

For example, if you wanted to change the agent's advertised lifetime to 300 seconds for device `le0`, use the following command to make this change.

```
# mipagentconfig change adv le0 AdvLifetime 300
```

The following example shows how you might change other parameters in the configuration file's `Advertisements` section.

EXAMPLE 3–2 Changing Parameters in the `Advertisements` Section

```
# mipagentconfig change adv le0 HomeAgent yes
# mipagentconfig change adv le0 ForeignAgent no
# mipagentconfig change adv le0 PrefixFlags no
# mipagentconfig change adv le0 RegLifetime 300
# mipagentconfig change adv le0 AdvFrequency 4
```

▼ How to Modify the `GlobalSecurityParameters` Section

1. **Become superuser on the system where you want to enable Mobile IP.**

2. **On a command line, type the following command for each label that you want to modify in the `GlobalSecurityParameters` section.**

```
# mipagentconfig change <label> <value>
```

For example, if you wanted to enable home agent and foreign agent authentication, use the following command to make this change.

```
# mipagentconfig change HA-FAauth yes
```

The following example shows how you might change other parameters in the configuration file's `GlobalSecurityParameters` section.

EXAMPLE 3–3 Changing Parameters in the `GlobalSecurityParameters` Section

```
# mipagentconfig change MaxClockSkew 200
# mipagentconfig change MN-FAauth yes
# mipagentconfig change Challenge yes
# mipagentconfig change KeyDistribution files
```

▼ How to Modify the `Pool` Section

1. **Become superuser on the system where you want to enable Mobile IP.**

2. **On a command line, type the following command for each label that you want to modify in the `Pool` section.**

```
# mipagentconfig change Pool Pool-identifier <label> <value>
```

For example, if you wanted to change the base address to `192.168.1.1` and size to `100` of Pool `10`, use the following commands to make this change.

EXAMPLE 3–4 Changing Parameters in the `Pool` Section

```
# mipagentconfig change Pool 10 BaseAddress 192.168.1.1
# mipagentconfig change Pool 10 Size 100
```

▼ How to Modify the `SPI` Section

1. **Become superuser on the system where you want to enable Mobile IP.**

2. **On a command line, type the following command for each label that you want to modify in the `SPI` section.**

```
# mipagentconfig change SPI SPI-identifier <label> <value>
```

For example, if you wanted to change the key for `SPI 257` to `5af2aee39ff0b332`, use the following command to make this change.

```
# mipagentconfig change SPI 257 Key 5af2aee39ff0b332
```

The following example shows how you might change the `ReplayMethod` label in the configuration file's SPI section.

EXAMPLE 3–5 Changing Parameters in the `SPI` Section

```
# mipagentconfig change SPI 257 ReplayMethod timestamps
```

▼ How to Modify the `Address` Section

1. **Become superuser on the system where you want to enable Mobile IP.**

2. **On a command line, type the following command for each label that you want to modify in the `Address` section.**

```
# mipagentconfig change addr [NAI | IPaddr | node-default] <label> <value>
```

See "`Address` Section" on page 36 for a description of the three configuration methods (NAI, IP address, and node-default).

For example, if you wanted to change the SPI of IP address `10.1.1.1` to `258`, use the following command to make this change.

```
# mipagentconfig change addr 10.1.1.1 SPI 258
```

The following example shows how you might change other parameters provided in the sample configuration file's `Address` section.

EXAMPLE 3–6 Changing Parameters in the `Address` Section

```
# mipagentconfig change addr 10.1.1.1 Type agent
# mipagentconfig change addr 10.1.1.1 SPI 259
# mipagentconfig change addr mobilenode@abc.com Type node
# mipagentconfig change addr mobilenode@abc.com SPI 258
# mipagentconfig change addr mobilenode@abc.com Pool 2
# mipagentconfig change addr node-default SPI 259
# mipagentconfig change addr node-default Pool 3
# mipagentconfig change addr 10.68.30.36 Type agent
# mipagentconfig change addr 10.68.30.36 SPI 260
```

▼ How to Add or Delete Configuration File Parameters

1. **Become superuser on the system where you want to enable Mobile IP.**

2. **On a command line, type the appropriate command for each label that you want to add or delete for the designated section.**

   For the `General` section use:

   ```
   # mipagentconfig [add | delete] <label> <value>
   ```

   For the `Advertisements` section use:

   ```
   # mipagentconfig [add | delete] adv device-name <label> <value>
   ```

   Note - You can `add` an interface by typing:

   ```
   # mipagentconfig add adv device-name
   ```

   In this case, default values are assigned to the interface (for both foreign agent and home agent).

   For the `GlobalSecurityParameters` section use:

   ```
   # mipagentconfig [add | delete] <label> <value>
   ```

   For the `Pool` section use:

   ```
   # mipagentconfig [add | delete] Pool Pool-identifier <label> <value>
   ```

   For the `SPI` section use:

```
# mipagentconfig [add | delete] SPI SPI-identifier <label> <value>
```

For the `Address` section use:

```
# mipagentconfig [add | delete] addr [NAI | IPaddr | node-default] \
<label> <value>
```

Note - Be careful that you do not create identical Advertisements, Pool, SPI, and Address sections.

For example, if you wanted to create a new address pool, say Pool 11, that has a base address of `192.167.1.1` and a size of `100`, use the following commands.

EXAMPLE 3–7 Adding a New Pool and Parameters

```
# mipagentconfig add Pool 11 BaseAddress 192.167.1.1
# mipagentconfig add Pool 11 size 100
```

Or you might want to delete a particular security parameter. The following example shows you how to delete `SPI 257`.

EXAMPLE 3–8 Deleting an SPI

```
# mipagentconfig delete SPI 257
```

▼ How to Display Current Parameter Settings in the Configuration File

You can use the `mipagentconfig get` command to display current settings associated with parameter destinations.

1. **Become superuser on the system where you want to enable Mobile IP.**

2. **On a command line, type the following command for each parameter for which you want to display settings.**

```
# mipagentconfig get [<parameter> | <label>]
```

For example, if you wanted to display the advertisement settings for the `le0` device, use the following command.

```
# mipagentconfig get adv le0
```

This causes the following results to display (for example).

```
[Advertisements le0]
   HomeAgent = yes
   ForeignAgent = yes
```

The following example shows the results of using the `mipagentconfig get` command with other parameter destinations.

EXAMPLE 3–9 Using the `mipagentconfig get` Command

```
# mipagentconfig get MaxClockSkew
      [GlobalSecurityParameters]
         MaxClockSkew=300

# mipagentconfig get HA-FAauth
      [GlobalSecurityParameters]
         HA-FAauth=no

# mipagentconfig get MN-FAauth
      [GlobalSecurityParameters]
         MN-FAauth=no

# mipagentconfig get Challenge
      [GlobalSecurityParameters]
         Challenge=no

# mipagentconfig get Pool 10
      [Pool 10]
         BaseAddress=192.168.1.1
         Size=100

# mipagentconfig get SPI 257
      [SPI 257]
         Key=11111111111111111111111111111111
         ReplayMethod=none

# mipagentconfig get SPI 258
      [SPI 258]
         Key=15111111111111111111111111111111
         ReplayMethod=none

# mipagentconfig get addr 10.1.1.1
      [Address 10.1.1.1]
         SPI=258
         Type=agent
```

(continued)

(Continuation)

```
# mipagentconfig get addr 192.168.1.200
      [Address 192.168.1.200]
         SPI=257
         Type=node
```

Displaying Mobility Agent Status

You can use the `mipagentstat` command to display a foreign agent's visitors list and a home agent's binding table. "Mobile IP Mobility Agent Status" on page 40 provides a conceptual description of the `mipagentstat` command. You can also review the `mipagentstat`(1M) man page.

▼ How to Display Mobility Agent Status

1. **Become superuser on the system where you want to enable Mobile IP.**

2. **On a command line, type the following command.**

```
# mipagentstat <option>
```

You can use the following options:

`–f`	Shows the list of active mobile nodes in the foreign agent's visitor list.
`–b`	Shows the list of active mobile nodes in the home agent's binding table.

For example, to show the visitor list for all mobile nodes registered with the foreign agent, use the following command.

```
# mipagentstat -f
```

This causes the following results to display (for example).

```
Mobile Node     Home Agent     Time Granted    Time Remaining
                                 (in secs)       (in secs)
     foobar.xyz.com  ha1.xyz.com    600             125
     10.1.5.23       10.1.5.1       1000            10
```

Glossary

This glossary contains only definitions of new terms found in this book and are not in the Global Glossary. For definitions of other terms, see the Global Glossary at `http://docs.sun.com:80/ab2/coll.417.1/GLOBALGLOSS/@Ab2TocView`.

address pool — A set of addresses designated by the home network administrator for use by mobile nodes that need a home address.

agent advertisement — A message periodically broadcasted by home agents and foreign agents to advertise their presence on any attached link.

agent discovery — The process by which a mobile node determines if it has moved, its current location, and its care-of address on a foreign network.

bidirectional tunnel — A tunnel that can transmit datagrams in both directions.

binding table — A home agent table that associates a home address with a care-of address, including remaining lifetime and time granted.

care-of address — A mobile node's temporary address used as a tunnel exit point when the mobile node is connected to a foreign network.

foreign network — Any network other than the mobile node's Home Network.

Generic Routing Encapsulation (GRE) — An optional form of tunneling that can be supported by home agents, foreign agents, and mobile nodes. GRE enables a packet of any network-layer protocol to be encapsulated within a delivery packet of any other (or same) network-layer protocol.

home address — An IP address assigned for an extended period to a mobile node. The address remains unchanged when the node is attached elsewhere on the Internet or an organization's network.

home network	A network having a network prefix matching that of a mobile node's home address.
IP in IP encapsulation	The Internet-standard protocol for tunneling IPv4 packets within IPv4 packets.
MD5	An iterative cryptographic hash function used for message authentication.
Minimal encapsulation	An optional form of IPv4 in IPv4 tunneling that can be supported by home agents, foreign agents, and mobile nodes. Minimal Encapsulation has 8 or 12 less bytes of overhead than does IP in IP Encapsulation.
mobile node	A host or router that can change its point of attachment from one network to another while maintaining all existing communications, using its IP home address.
mobility agent	Either a home agent or a foreign agent.
mobility binding	The association of a home address with a care-of address, along with the remaining lifetime of that association.
mobility security association	A collection of security measures, such as an authentication algorithm, between a pair of nodes, which are applied to Mobile IP protocol messages exchanged between the two nodes.
node	A host or a router.
Network Access Identifier (NAI)	Used to uniquely identify the mobile node in the format of user@domain.
registration	The process by which a mobile node registers its care-of address with its home agent when it is away from home.
Security Parameter Index (SPI)	An integer that specifies the row in the SADB (security associations database) that a receiver should use to decrypt a received packet.
tunnel	The path followed by a datagram while it is encapsulated.
Virtual Private Network	A single, secure, logical network that uses tunnels across a public network such as the Internet.

visited network A network other than a mobile node's home network, to which the mobile node is currently connected.

visitor list The list of mobile nodes visiting a foreign agent.

Index

G

H

I

K

M

N

P

R

S

T

U

V

W