



HP-UX Mobile IPv4

A.02.01

White Paper

March 2003

Legal Notices

The information in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty

A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

HEWLETT-PACKARD DEVELOPMENT COMPANY L.P.
20555 S.H. 249
Houston, Texas 77070

Use of this document and any supporting software media supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and back-up purposes only. Resale of the programs, in their present form or with alterations, is expressly prohibited.

Copyright Notice

Copyright © 1997-2003 Hewlett-Packard Development Company L.P. All rights reserved.

Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under the copyright laws.

Additional Copyright Notice and Disclaimer

Copyright © 1995, 1996 Carnegie Mellon University. All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation is hereby granted (including for commercial or for-profit use), provided that both the copyright notice and this permission notice appear in all copies of the software, derivative works, or modified versions, and any portions thereof, and that both notices appear in supporting documentation, and that credit is given to Carnegie Mellon University in all publications reporting on direct or indirect use of this code or its derivatives.

THIS IMPLEMENTATION OF MOBILE IP IS EXPERIMENTAL AND IS KNOWN TO HAVE BUGS, SOME OF WHICH MAY HAVE SERIOUS CONSEQUENCES. CARNEGIE MELLON PROVIDES THIS SOFTWARE IN ITS "AS IS" CONDITION, AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Carnegie Mellon encourages (but does not require) users of this software to return any improvements or extensions that they make, and to grant Carnegie Mellon the rights to redistribute these changes without encumbrance.

Contents

The Mobile Internet	1
Mobility for Internet Protocol (IPv4).....	2
<i>How Mobile IP Works</i>	<i>2</i>
<i>Roles</i>	<i>2</i>
The Role of the Mobile Node.....	2
The Role of the Foreign Agent.....	2
The Role of the Home Agent.....	2
How a Mobile Node Receives Packets.....	3
How a Mobile Node Sends Packets.....	3
<i>Agent Advertisements</i>	<i>4</i>
<i>Agent Solicitations.....</i>	<i>4</i>
<i>How a Mobile Node gets the Care-of Address</i>	<i>4</i>
<i>Location Updates - Registering the COA.....</i>	<i>5</i>
<i>Deregistering the Care-of Address.....</i>	<i>5</i>
HP-UX Mobile IPv4	6
<i>Product Features</i>	<i>6</i>
IP Mobility Support for IPv4 [RFC 3344]	6
IP Encapsulation and Tunneling.....	6
Reverse Tunneling [RFC 3024].....	6
Route Optimization	7
AAA Support.....	8
Mobile Node Authentication	8
Dynamic Key Generation and Distribution.....	10
Dynamic Home Address Allocation.....	10
Dynamic Home Agent Allocation	10
References	11
For more Information	12

THE MOBILE INTERNET

The increasing popularity of mobile devices, such as PDAs, handhelds, and digital cellular phones, is beginning to change our perceptions of the Internet. A need has been generated to allow users to attach to any domain convenient to their current location. Convenient access to the Internet anytime and anywhere will help free users from the ties that bind them to their desktops. A mobile networking environment has the potential not just to extend that flexibility but to fundamentally change the way the world communicates across administrative boundaries and geographical constraints. Users may now begin to enjoy the convenience of seamless and continuous connectivity to the Internet.

MOBILITY FOR INTERNET PROTOCOL (IPv4)

Mobile nodes were not considered when the Internet Protocol (IPv4) was designed. Then and now, a node's IP address, which indicates its point of attachment to the Internet, is assumed to remain unchanged for the duration of a session.

Mobile IP, a standard proposed by the Internet Engineering Task Force (IETF), was designed to solve this problem by allowing the mobile node to use two IP addresses: a fixed Home Address and a Care-of Address (COA) that changes at each new point of attachment to the Internet.

How Mobile IP Works

Mobility Support for IPv4 defines a protocol that allows transparent routing of IP datagrams to Mobile Nodes as they move about from one domain to another on the Internet. When a Mobile Node moves into a foreign network, its computing activities are not disrupted. Instead, all the needed reconnection occurs automatically and without user interaction.

Roles

The Role of the Mobile Node

A MN is responsible for detecting change in network connectivity and acquiring a care-of address. It initiates the process of informing its Home Agent of its current Care-of Address. Mobile Nodes using collocated Care-of Address also need to perform tunneling and encapsulation of packets.

The Role of the Foreign Agent

A Foreign Agent relays location updates and acknowledgments between the Home Agent and Mobile Node. If it is also the Care-of Address for the Mobile Node, the Foreign Agent forwards encapsulated packets destined to the Mobile Node. The Foreign Agent generally serves the Mobile Node as its default router.

The Role of the Home Agent

A Home Agent processes and coordinates mobility services for the Mobile Node. The Home Agent receives location updates from the Mobile Node, and acknowledges the updates with the result. The Home Agent receives packets that arrive on the network destined for a Mobile Node that it serves and tunnels them to the Mobile Node's Care-of Address.

How a Mobile Node Receives Packets

When the Mobile Node is not attached to its home network, the Home Agent receives all packets destined for the Mobile Node's home address. The Home Agent encapsulates the original IP packet and directs it to the Mobile Node's Care-of Address. When the packet arrives at the Care-of Address, the original IP packet is extracted and delivered to the Mobile Node. This encapsulation is also called tunneling.

How a Mobile Node Sends Packets

Tunneling is generally not required when the Mobile Node sends a packet. The Mobile Node transmits an IP packet with its Home Address as the source IP address. The packet is routed through the Mobile Node's default router in the foreign network.

In networks that do source IP address checking, reverse tunneling may be desirable. With reverse tunneling, packets from the Mobile Node are encapsulated by the Care-of Address and sent to the Home Agent. The HA decapsulates these packets and routes them to the original destination.

Figure 1.1 shows the data path of an IP packet from a Correspondent Node to a Mobile Node.

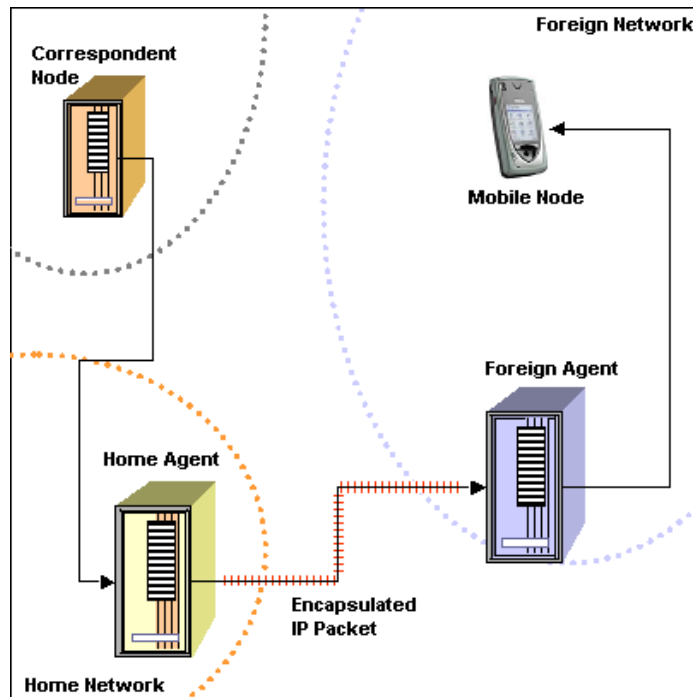


Figure 1.1 Data path of an IP packet sent from a Correspondent Node to a Mobile Node

Agent Advertisements

Home Agents and Foreign Agents, at regular intervals (every few seconds), broadcast on their subnet, messages known as Agent Advertisements. The Agent Advertisement is designed as an extension of the already existing ICMP router advertisement [RFC 1256] message. The agent advertisement conveys the following information:

- Whether the agent is a Home Agent or a Foreign Agent.
- A list of available Care-of Addresses (in case of the Foreign Agents).

Agent Solicitations

The Mobile Node may also broadcast or multicast an Agent Solicitation message. Any Home Agent or Foreign Agent that receives the agent solicitation message responds with an Agent Advertisement.

How a Mobile Node gets the Care-of Address

A Mobile Node, when attaching to a foreign network, must acquire a Care-of Address on that network. There are two ways of achieving this:

1. **Foreign Agent Care-of Address:** A Foreign Agent Care-of Address is a Care-of Address acquired by the Mobile Node from a Foreign Agent's advertisement broadcast. The foreign Care-of Address is registered with the Home Agent and the Foreign Agent serves as the endpoint in the tunnel for encapsulated packets sent from the Home Agent to the Mobile Node.
2. **Co-located Care-of Address:** A co-located Care-of Address is a Care-of Address acquired by the Mobile Node as a local IP address through some external means, such as DHCP [RFC2131], that the Mobile Node then associates with one of its own network interfaces. When using a co-located Care-of Address, the Mobile Node serves as the endpoint of the tunnel and performs decapsulation of datagrams tunneled to it.

Location Updates - Registering the COA

When a Mobile Node attaches to a new foreign network, it sends a Registration Request to its Home Agent to register its Care-of Address. If the Mobile Node is using a Foreign Agent Care-of Address, the Registration Request is sent via the Foreign Agent. The Registration Request includes an extension with a cryptographic authentication value (HMAC-MD5 or keyed MD5). The Mobile Node calculates the authentication value based on fields in the Registration Request and a static key (shared secret key) that is specified on both the Home Agent and the Mobile Node.

The Home Agent authenticates the Mobile Node's Registration Request by calculating its own authentication value and comparing it with the authentication value from the Mobile Node. After the Home Agent authenticates the Registration Request, it sends a Registration Reply message to the Mobile Node. The Registration Reply also includes a lifetime for the registration.

Deregistering the Care-of Address

A Mobile Node, upon returning to its home network or upon session termination, sends the Home Agent a Mobile IP Registration Request message for deregistration. The Home Agent removes its mobility binding for the Mobile Node. Deregistration with the Foreign Agent occurs automatically when the registration lifetime expires.

HP-UX MOBILE IPv4

HP-UX Mobile IPv4 runs on HP-UX 11i and provides mobility support for mobile devices as they roam about from one network to another on the Internet. Version A.02.01 is designed for a wide-ranging commercial deployment of Mobile IP that requires AAA (Authentication, Authorization, and Accounting) services and support.

Product Features

The following are the salient features of the HP-UX Mobile IPv4 product.

IP Mobility Support for IPv4 [RFC 3344]

HP-UX Mobile IPv4 provides mobile nodes, the ability to roam through the Internet while maintaining their home address and network connection. HP-UX Mobile IPv4 allows transparent routing of IP datagrams to these mobile nodes as they migrate from their home network to other networks.

IP Encapsulation and Tunneling

When the mobile node is away from its home network, the Home Agent receives all packets destined for the Mobile Node's home address. The Home Agent encapsulates each packet in a new packet. The destination address of this encapsulated packet is set to the Mobile Node's Care-of Address. This is called IP Encapsulation.

This encapsulated packet is then routed to the Mobile Node's Care-of Address. When this encapsulated packet arrives at the Mobile Node's Care-of Address, the original IP packet is extracted (or decapsulated) and the original packet is routed to the Mobile Node.

This use of encapsulation and decapsulation of a datagram is frequently referred to as tunneling the datagram, and the encapsulator and decapsulator are then considered to be the endpoints of the tunnel.

Reverse Tunneling [RFC 3024]

A Mobile Node, when communicating with a Correspondent Node, typically sends packets directly back to the Correspondent Node. With reverse tunneling, the IP packet is encapsulated in a new packet with the destination address set to the Home Agent. The Home Agent decapsulates the tunneled datagram and routes it to the original destination.

Reverse tunneling is useful for installations with ingress filtering (filters that check inbound packets for topologically correct source addresses). With reverse tunneling, the packet leaving the foreign network will have a topologically correct source address, because the source address in the outermost IP header will be an address from the foreign network (the Care-of Address) instead of the Mobile Node's home address.

Route Optimization

HP-UX Mobile IPv4 facilitates the routing of datagrams directly from the Correspondent Node to the Mobile Node's Care-of Address without going through the Mobile Node's home network. This improves the data transmission rates between the Correspondent Node and Mobile Node and reduces congestion in the home network.

Normally, packets from the Correspondent Node to the Mobile Node are sent through the Home Agent (and through the Mobile Node's home network). When Route Optimization is used, the Home Agent sends an authenticated message to the Correspondent Node with the Mobile Node's current Care-of Address. This message informs the Correspondent Node to form a route optimization tunnel to the Mobile Node's Care-of Address.

AAA SUPPORT

In a Mobile IPv4 environment, remote nodes and users may visit networks outside their home domain. Administrators in the networks being visited may want to use AAA (Authentication, Authorization, and Accounting) to restrict or grant access to local resources.

HP-UX Mobile IPv4 is designed for wide-ranging commercial deployment of Mobile IP that requires AAA services and support. This version supports the use of AAA servers using the Diameter protocol to authenticate Mobile Nodes and authorize access.

The HP-UX Mobile AAA Server (T1428BA) is an Authentication, Authorization, and Accounting (AAA) server based on the Diameter Base Protocol and Diameter Mobile IPv4 Application IETF specifications. These protocols define a standard for information exchange that allows Diameter servers to deliver AAA services to Mobile IP agents.

More information on HP-UX Mobile AAA Server (T1428BA) can be found at: <http://docs.hp.com/hpux/pdf/T1428-90008.pdf>.

HP-UX Mobile IPv4 supports the following basic features when used with AAA Diameter servers:

Mobile Node Authentication

Mobile IPv4 AAA authentication is based on user authentication. A Mobile Node is identified using a Network Access Identifier and this information along with AAA user authentication information is included in the registration requests. There are different types of AAA user authentication. Many of them are based on a security key or password that is shared between both the AAA server and the Mobile Node.

The AAA server that authorizes and authenticates a Mobile Node is known as the Node's AAA Home server (AAAH). The AAAH authenticates and authorizes users. When a Mobile Node uses a Foreign Agent Care-of Address, the Foreign Agent must also have a relationship configured with an AAA server in the foreign network. This AAA server is known as the AAA Foreign Agent server (AAAF). The AAAF receives AAA requests from Foreign Agents and forwards them to the appropriate AAAH based on the Mobile Node user NAI [RFC 2794]. Fig 1-2 shows how Mobile Node authentication takes place in an AAA environment.

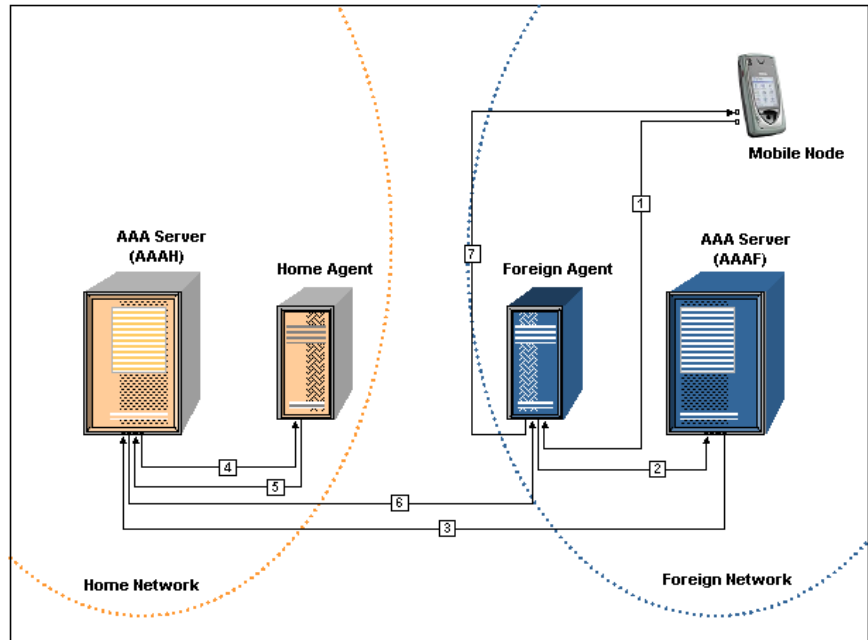


Fig 1-2. Mobile Node Authentication

1. Mobile Node sends a registration request message to the Foreign Agent.
2. The Foreign Agent sends a Diameter AA-Mobile Node Request (AMR) message to the local AAA Server (AAAF) that includes the Mobile IP registration request in it.
3. The AAAF forwards the AMR message to the AAA Server (AAAH) in the home network.
4. The AAAH builds a Diameter Home Agent MIP Request (HAR) message from the information in the AMR and forwards it to the Home Agent. The HAR includes the Mobile IP registration request.
5. The Home Agent processes the HAR message and sends a Diameter Home Agent MIP Answer (HAA) message to the AAAH. The HAA includes the Mobile IP registration reply.
6. The AAAH processes the HAA and builds a Diameter AA-Mobile Node Answer (AMA) message from the information in the HAA and sends it to the Foreign Agent. The AMA includes the Mobile IP Registration Reply.
7. The Foreign Agent processes the Registration Reply and then sends it to the Mobile Node.

Dynamic Key Generation and Distribution

The Diameter Mobile IPv4 protocol allows for the FA to request the AAAH server to generate dynamic keys for authenticating messages between the following entities:

- Mobile Node and Home Agent
- Mobile Node and Foreign Agent
- Home Agent and Foreign Agent

Use of dynamically generated keys increases packet security. Using different keys makes it more difficult for someone examining network packets to determine a key's value.

The AAAH encrypts keys for the Mobile Node using the AAA key or password for the Mobile Node user. While keys for the Home Agent and Foreign Agent are not encrypted by the AAA protocol, the AAA messages sent between AAAH and Home Agent and AAAF and Foreign Agent containing security keys can be protected by other mechanisms, such as IPSec. Messages sent between the AAAH and AAAF containing security keys can be encrypted using security features provided by the AAA infrastructure.

Dynamic Home Address Allocation

The Base Mobile IP protocol allows a Mobile Node to be configured without a home address. Home addresses for such mobile nodes are dynamically allocated during registration process. HP-UX Mobile IPv4 Home Agents support dynamic home address allocation for AAA Mobile Nodes. The Home Agent dynamically allocates addresses from a pool or range of IP addresses.

Dynamic Home Agent Allocation

HP-UX Mobile IPv4 Home Agent supports dynamic Home Address allocation for requests authenticated by the AAAH server. This feature is to support Nodes that do not know their Home Agent. Home Agent allocation can be done along with Home Address allocation if required.

REFERENCES

Mobile IP technology is built around drafts and specifications proposed by IETF. This version of HP-UX Mobile IPv4 software supports the following IETF specifications:

- RFC 3344 - IP Mobility Support for IPv4
- RFC 2003 - IP Encapsulation within IP
- RFC 3024 - Reverse Tunneling for Mobile IP
- RFC 2794 - Mobile IP Network Access Identifier
- RFC 3012 - Mobile IP Challenge/Response Extensions
- RFC 1256 - ICMP Router Discovery Messages
- Route Optimization in Mobile IP, Draft 11: draft-ietf-mobileip-optim-11.txt
- Diameter Base Protocol, Draft 8: draft-ietf-aaa-diameter-08.txt
- Diameter Mobile IPv4 Application, Draft 8: draft-ietf-aaa-diameter-mobileip-08.txt
- AAA Registration Keys for Mobile IP, Draft 10: draft-ietf-mobileip-aaa-key-10.txt.

FOR MORE INFORMATION

Visit [Mobile IPv4 documentation](#) on `docs.hp.com` for more information.