

## Roaming Support in Mobile IP

### [1.](#) Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

To view the list Internet-Draft Shadow Directories, see <http://www.ietf.org/shadow.html>.

The distribution of this memo is unlimited. It is filed as <[draft-ietf-roamops-mobileip-02.txt](#)>, and expires December 1, 1999. Please send comments to the authors.

### [2.](#) Copyright Notice

Copyright (C) The Internet Society (1999). All Rights Reserved.

### [3.](#) Abstract

[RFC 2002](#) describes the framework for Mobile IP, while [RFC 2290](#) describes how a mobile node and a peer negotiate the appropriate use of Mobile IP over a PPP link. [RFC 2477](#) describes the roaming architecture as well as criteria for evaluation of roaming protocols, which include reconciliation between roaming and mobile IP.

This document describes the relationship between the roaming

architecture and mobile IP and describes how support for secure roaming may be provided within Mobile IP, while requiring only minimal changes to the Mobile IP protocol.

## [4.](#) Introduction

[RFC 2002](#) [7] describes the framework for Mobile IP, while [RFC 2290](#) [8] describes how a mobile node and a peer negotiate the appropriate use of Mobile IP over a PPP link, through use of the IPCP IP Address and Mobile-IPv4 Configuration Options. [RFC 2477](#) [6] describes the roaming architecture as well as, which include reconciliation between roaming and mobile IP.

This document describes the relationship between the roaming architecture and mobile IP and describes how support for secure roaming may be provided within Mobile IP, while requiring only minimal changes to the Mobile IP protocol.

### [4.1.](#) Requirements language

In this document, the key words "MAY", "MUST", "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [4].

### [4.2.](#) Overview

The architectural framework for Internet roaming, described in [6], permits a roaming user to make use of the facilities of multiple Internet Service Providers while maintaining a formal account relationship with only one. This framework makes use of the Network Access Identifier (NAI), defined in [9], in order to identify the roaming user, as well as to permit the location of the home authentication server. The home authentication server is located either via static configuration or via lookup of the SRV record, following the procedure described in [RFC 2052](#) [18].

Within the roaming architecture the roaming user typically does not maintain a pre-existing relationship with the local provider. As a result, unless certificate-based authentication is used between the roaming user and the local provider, it is necessary for the the local provider to contact the home authentication server in order to validate the user's identity.

When certificate-based authentication is used between the roaming user and the local provider, as described in [11], the local provider is able

to determine whether the user possesses the private key corresponding to the offered certificate, and thus authentication by the home provider is not required.

Where it is necessary for the local provider to contact the home authentication server, it is desirable for that communication be secured using public key certificates, as supported in IKE [16]-[17]. Since the local provider and home server typically do not maintain a pre-existing relationship, without public key certificate support it is typically necessary for one or more proxies to act as intermediaries in order to reduce the shared secret management problem. As noted in [10] the introduction of proxies creates a number of security problems and therefore is undesirable.

#### 4.3. Scenarios

This document discusses roaming within Mobile IP, based on the following scenarios:

1. The mobile node supports certificate-based authentication with the foreign agent.
2. The mobile node does not support certificate-based authentication with the foreign agent, nor does it share a secret with the foreign agent. However, the mobile node does share a secret with the home agent. In this scenario, the foreign agent contacts the home authentication server in order to validate the mobile node's identity.
3. PPP-based connectivity is established at layer 2 prior to Mobile IP foreign agent discovery and Mobile Node Registration. In this scenario, it cannot be assumed that a prior relationship exists between the mobile node and the foreign agent. This scenario may support any authentication mode type supported by PPP, including CHAP and Extensible Authentication Protocol (EAP), which includes support for certificate-based authentication. Where certificate-based authentication is used, the foreign agent will be able to validate the mobile node's identity without contacting the home authentication server. Where another means of authentication is used, it will typically be necessary for the foreign agent to contact the home authentication server.

In all scenarios it is assumed that the mobile node is operating with a co-located care of address. However, it is not assumed that the foreign agent and home agent have a pre-existing relationship and therefore it cannot be assumed that a shared secret exists between the parties. As a result, roaming support within Mobile IP does not make use of the Foreign Agent-Home Agent authentication extension.

---

## [5.](#) Support for roaming within Mobile IP

### [5.1.](#) Support for certificate-based roaming in Mobile IP

In this scenario, it is assumed that the Mobile Node and Home Agent have a security association, but that there is no security association between the Foreign Agent and the Home Agent. An IPSEC security association is negotiated between the Mobile Node and the Foreign Agent, so that the Mobile Node-Foreign Agent authentication extension is not needed.

In certificate-based roaming, the Mobile Node creates an IPSEC security association with the Foreign Agent. For the IKE negotiation to be carried out, the Mobile Node **MUST** obtain a co-located care-of-address from the mobile node (used as the source address for IKE) and **MUST** discover the IP address of the Foreign Agent (used as the destination address for IKE). If the IP address of the Foreign Agent cannot be obtained then the IKE negotiation cannot be carried out since the destination address for the IKE negotiation cannot be the all-mobility-agents multicast address, 224.0.0.11. During the IKE negotiation, user-based certificates **MUST** be used in order for the Mobile Node to prove its identity to the Foreign Agent. Machine-based certificates **MUST NOT** be used since they do not demonstrate that the Mobile Node's identity corresponds to the NAI that will be used by the Foreign Agent to bill for services.

In order to permit the mobile node to make a claim of identity as well as to validate that claim, the Mobile Node includes in the Registration Request the NAI extension described in [\[12\]](#). The realm portion of the NAI is used by the Foreign Agent to locate the home agent via a lookup of the mobileip-agent.udp.realm SRV record, following the procedure described in [RFC 2052](#) [\[18\]](#). Note that the NAI extension provided by the Mobile Node **MUST** correspond to the identity provided in the IKE negotiation.

The Registration Request also **MUST** include the Mobile Node-Home Agent authentication extension. Since the Mobile Node and Foreign Agent create an IPSEC security association there is no need for an alternative security association and the Mobile Node-Foreign Agent authentication extension **MUST NOT** be included.

When the Foreign Agent receives the Registration Request, it may or may not negotiate an IPSEC security association with the Home Agent prior to forwarding the Registration Request to the Home Agent. Note that the home agent may not have access to the secret shared with the mobile node and therefore may not be able to validate the Mobile Node-Home Agent

authentication extension on its own without help from a central authentication server. This can be achieved via use of the RADIUS protocol and the MN-Registration attribute described below.

Please note that in mobile IP, certificate based roaming provides only stronger authentication but does not reduce latency. Unlike dialup-roaming, it is generally not possible for the Foreign Agent to avoid contact with the Home Agent, even if it has already authenticated the Mobile Node. This is because the Mobile Node will still need to register its co-located care-of-address with the Home Agent, and the Foreign Agent will need to be aware of the outcome of the Registration Request. Thus in Mobile IP roaming, certificate-based authentication does not save any round-trips.

## [5.2](#). Support for shared secret-based roaming in Mobile IP

In this scenario, it is assumed that the Mobile Node and Home Agent share a security association, but that no security association exists between the Mobile Node and Foreign Agent. Since an IPSEC security association is negotiated between the Foreign Agent and the Home Agent, there is no need for the Foreign Agent-Home Agent authentication extension.

In order to permit the user to make a claim of identity as well as to validate that claim, the Mobile Node Registration Request includes the NAI extension described in [\[12\]](#), as well as the Mobile Node-Home Agent authentication extension. Since the Mobile Node and Foreign Agent typically do not have a security association, the Mobile Node-Foreign Agent authentication extension is not included.

Since in shared-secret based roaming there is no IPSEC negotiation between the Mobile Node and the Foreign Agent, there is no requirement that the Mobile Node obtain a co-located care of address. This allows the Foreign Agent to re-use the care-of-address if it desires.

When the Foreign Agent receives the Registration Request, it negotiates an IPSEC security association with the Home Agent. The Foreign Agent locates the home agent from the realm portion of the NAI via a lookup of the mobileip-agent.udp.realm SRV record, following the procedure described in [RFC 2052](#) [\[18\]](#).

As part of the IKE negotiation, the Foreign Agent and Home Agent will authenticate using certificates from a mutually trusted party (the roaming association). The foreign agent will subsequently bill this trusted party for the resources consumed by the mobile node. Note that this security association may be reused by the Foreign Agent for handling of additional Mobile Nodes using the same Home Agent.

INTERNET-DRAFT

Roaming Support in Mobile IP

25 June 1999

The IPSEC-protected Mobile IP registration message sent by the Foreign Agent to the Home Agent MUST provide for integrity protection and authenticity via the ESP null transform. The Mobile IP Registration Response serves to validate the identity of the Mobile Node both to the Home Agent and to the Foreign Agent, and therefore provides assurance to the Foreign Agent that it will be able to provide service.

Note that the home agent may not have access to the secret shared with the mobile node and therefore may not be able to validate the Mobile Node-Home Agent Authentication Extension on its own without help from a central authentication server. This can be achieved via use of the RADIUS protocol and the MN-Registration attribute described below.

### 5.3. Support for PPP-based roaming in Mobile IP

The steps involved in negotiating mobile access to the Internet while roaming between PPP-based mobile IP providers are as follows:

1. The mobile node connects to the foreign agent via PPP, and authenticates via LCP, identifying itself via the Network Access Identifier (NAI), described in [\[9\]](#). The NAI provides the local ISP with the information necessary to contact the home authentication server.
2. The foreign agent then sends a RADIUS Access-Request to the home authentication server, and receives a RADIUS Access-Reply. Based on the Access-Reply, the foreign agent will grant access to the mobile node, or will terminate the conversation. Note that since the RADIUS conversation takes place in LCP, while mobile IP configuration takes place in IPCP, an Access-Accept if sent must include the authorization information required to assist the foreign agent in negotiating use of Mobile IP with the mobile node.
3. The mobile node will indicate its preference for a foreign care-of-address or a co-located care of address via use of the IP Address and Mobile-IPv4 Configuration Options in IPCP, as described in [\[8\]](#). If a co-located care-of-address is preferred, this will typically be indicated by setting the IP Address option to zero, and the Mobile-IPv4 Configuration option to the Home Address. If a foreign agent care-of-address is preferred, this will typically be indicated by sending only a Mobile-IPv4 Configuration option with the Home Address.
4. The Foreign Agent will respond to the mobile node's Configure-Request as described in [\[8\]](#). If the NAS is not Mobile-IP capable, then it will respond with a Configure-Reject. If the mobile node has requested a co-

located care-of-address, and the foreign agent can comply, it will typically reply with a Configure-NAK including an IP Address Option set to the co-located care-of-address or home address, depending on whether

INTERNET-DRAFT

Roaming Support in Mobile IP

25 June 1999

the mobile node is attached via a foreign link or home link.

If the foreign agent only supports a foreign agent care-of-address, it will typically reply with a Configure-NAK including an IP Address Option set to zero. If the mobile node has requested a foreign agent care-of-address, and the foreign agent is Mobile-IP capable, then the foreign agent MUST reply with a Mobile-IPv4 Configuration Option set to the Home Address indicated by the mobile node.

As noted in [8], the foreign agent need not know the mobile node's Home Address beforehand in order to decide how to reply. This information is not useful because if the Home Address expected by the foreign agent did not match that provided by the mobile node, there would be no way to correct the problem, since as described in [8] a Configure-NAK is undefined for the Mobile-IPv4 Configuration Option.

5. The IPCP negotiation concludes and the mobile node now has access to the Internet.

6. The foreign agent sends a RADIUS Accounting Start packet to the RADIUS accounting server.

7. The Foreign Agent sends an agent advertisement on the PPP link.

8. The mobile node sends a Registration Request and receives a Reply. As noted in [8], the mobile node must receive an agent advertisement before registering on a foreign link since even if the mobile node is using a colocated care-of-address, the foreign agent may wish to enforce a policy requiring registration. Note that in this registration the Mobile Node SHOULD include the NAI extension even though the Foreign Agent has already learned this by other means. The NAI MUST correspond to that used in the PPP authentication.

In order to carry out the IPCP negotiation described above, the NAS requires the following information:

a. Whether the mobile node is authorized to do mobile IP. This is indicated by the Mobile-IP-Configuration Attribute defined below. Since the mobile node may not always wish to do mobile IP, Mobile IP authorization should not be interpreted as requiring mobile IP. Similarly, the mobile node may not always contact an ISP that is Mobile-



IP capable, and as a result, while a home server may include Mobile-IP-Configuration attribute in the Access-Accept, this attribute may be stripped by a local ISP proxy.

b. Whether a co-located care-of-address is available for assignment to the mobile node if requested. This is indicated by the inclusion or absence of a Framed-IP-Address attribute in the Access-Accept. When a

Mobile-IP-Configuration attribute is present, the absence of a Framed-IP-Address attribute should be interpreted as indicating that a co-located care-of-address MUST NOT be assigned. If a Framed-IP-Address attribute is included along with a Mobile-IP-Configuration attribute, then a co-located care-of-address MAY be assigned. As described in [2], a co-located care-of-address may assigned statically or dynamically.

## 6. RADIUS attributes

### 6.1. MN-Registration attribute

#### Description

This Attribute requests validation of the Mobile Node Registration. It MAY be included in an Access-Request packet.

A summary of the MN-Registration Attribute format is shown below. The fields are transmitted from left to right.

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Type      |      Length      |      Flags      |      Registration
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Registration...
+---+---+---+---+---+---+---+---+---+---+---+---+

```

Type

? for MN-Registration

Length

varies

Flags

The flags, which indicate the authenticators whose validation is requested, are encoded as follows:

```

0 1 2 3 4 5 6 7 8
+---+---+---+---+
|M|F|H|R|R|R|R|R|
+---+---+---+---+

```

INTERNET-DRAFT

Roaming Support in Mobile IP

25 June 1999

M = Mobile Node-Foreign Agent  
 F = Foreign Agent-Home Agent  
 H = Home Agent-Mobile Node  
 R = reserved

If the flag is set for a particular authenticator, the appropriate extension **MUST** be included in the enclosed Mobile IP registration packet. If the indicated extension is missing, then the RADIUS server **MUST** return an Access-Reject.

## Registration

The entire contents of the Mobile IP registration packet, including IP/UDP headers, registration request, and extensions.

## Discussion

The MN-Registration attribute is designed to allow the foreign or home agent to validate the authenticators enclosed in the Mobile IP registration message. Allowing this validation to be carried out by an authentication server alleviates the need for the Foreign Agent or Home Agent to maintain its own authentication database.

## [6.2.](#) Mobile-IP-Configuration attribute

### Description

This Attribute indicates whether a user is authorized to do Mobile IP. It **MAY** be included in Access-Accept, or Accounting-Request packets.

A summary of the Mobile-IP-Configuration Attribute format is shown below. The fields are transmitted from left to right.

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```



- [6] Aboba, B, Zorn, G., "Criteria for Evaluating Roaming Protocols", [RFC 2477](#), January 1999.
- [7] Perkins, C., "IP Mobility Support", [RFC 2002](#), October 1996.
- [8] Solomon, J., Glass, S., "Mobile-IPv4 Configuration Option for PPP IPCP", [RFC 2290](#), February 1998.

Aboba

Standards Track

[Page 10]

---

INTERNET-DRAFT

Roaming Support in Mobile IP

25 June 1999

- [9] Aboba, B, Beadles, M. A., "The Network Access Identifier", [RFC 2486](#), January 1999.
- [10] Aboba, B., Vollbrecht, J., "Proxy Chaining and Policy Implementation in Roaming", [RFC 2607](#), June 1999.
- [11] Aboba, B., "Certificate-based Roaming", Internet Draft (work in progress), [draft-ietf-roamops-cert-01.txt](#), April 1999.
- [12] Calhoun, P. R., Perkins, C., "Mobile IP Network Access Identifier Extension", Internet draft (work in progress), [draft-ietf-mobileip-mn-nai-02.txt](#), May 1999.
- [13] Atkinson, R., Kent, S., "Security Architecture for the Internet Protocol", [RFC 2401](#), November 1998.
- [14] Kent, S., Atkinson, R., "IP Authentication Header", [RFC 2402](#), November 1998.
- [15] Kent, S., Atkinson, R., "IP Encapsulating Security Payload (ESP)", [RFC 2406](#), November 1998.
- [16] Harkins, D., Carrel, D., "The Internet Key Exchange (IKE)", [RFC 2409](#), November 1998.
- [17] Piper, D., "The Internet IP Security Domain of Interpretation of ISAKMP", [RFC 2408](#), November 1998.
- [18] Gulbrandsen A. and P. Vixie, "A DNS RR for specifying the location of services (DNS SRV)", [RFC 2052](#), October 1996.

## [8.](#) Acknowledgements

Thanks to Jim Solomon of Motorola and Pat Calhoun of Sun Microsystems for useful discussions of this problem space.

## 9. Authors' Addresses

Bernard Aboba  
Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052

Phone: 425-936-6605  
EMail: [bernarda@microsoft.com](mailto:bernarda@microsoft.com)

Aboba

Standards Track

[Page 11]

---

INTERNET-DRAFT

Roaming Support in Mobile IP

25 June 1999

## 10. Full Copyright Statement

Copyright (C) The Internet Society (1999). All Rights Reserved.  
This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English. The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns. This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."

## 11. Expiration Date

This memo is filed as <[draft-ietf-roamops-mobileip-02.txt](#)>, and expires December 1, 1999.

Aboba

Standards Track

[Page 12]