Mobile IP Working Group
INTERNET-DRAFT
Expires December 1999

Eva Gustafsson, Ericsson, Editor

June 1999

Annika Jonsson, Ericsson
Elisabeth Hubbard, Telia
Jonas Malmkvist, Telia
Anders Roos, Telia

Requirements on Mobile IP from a Cellular Perspective
<draft-ietf-mobileip-cellular-requirements-02.txt>

Status of this memo

This document is a submission by the Mobile IP Working Group of the Internet Engineering Task Force (IETF). Comments should be submitted to the mobile-ip@standards.nortelnetworks.com mailing list. Distribution of this memo is unlimited.

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/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at
http://www.ietf.org/shadow.html.

Abstract

The increasing interest in Mobile IP as a potential macro-mobility solution for cellular networks leads to new solutions and extensions to the existing protocol. As part of this work, there is a need to gather the requirements on Mobile IP from a cellular perspective. This draft lists a set of requirements on Mobile IP for use in cellular networks, for instance IMT-2000, and relates the requirements to proposed solutions.

Table of contents

1. Introduction

Recently, there has been an increasing interest in Mobile IP as a potential future mobility standard, common to cellular systems and the Internet as a whole [3][16][17]. The benefits of adopting a common mobility solution would include independence of access network technologies and common solutions for fixed and wireless networks.

The purpose of this document is to state the requirements on Mobile IP as a potential macro-mobility solution for future cellular networks. In particular, we consider third generation mobile systems fulfilling the requirements from ITU for International Mobile Telecommunications - 2000 (IMT-2000). The Universal Mobile Telecommunication System (UMTS) and the Enhanced Data rates for GSM Evolution (EDGE), which both evolve from the GSM/GPRS standard, as well as Cdma 2000, are such IMT-2000 systems.

Parts of the requirements presented in this document are specific for Mobile IP in cellular networks, while others consider mobile users in general. However, we have chosen to include all kinds of requirements necessary for a cellular operator to deploy Mobile IP. In the following, the term Mobile IP refers to both Mobile IPv4 [20] and Mobile IPv6 [18].

We start in Section 2 with some general, system-level requirements for IP mobility in cellular networks. Then we list more specific requirements in Section 3 through Section 10. Section 11 concludes the document.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [6].

2. General considerations

This section describes some general considerations and requirements on a system using Mobile IP. Note that these requirements are not specific requirements on the Mobile IP protocol, but point out important aspects on a system level.

To allow Mobile IP to be a mobility solution which supports many different kinds of access networks/technologies, Mobile IP functionality shall be independent of the access network technology. For Mobile IP to be deployed in future cellular networks, it needs to interwork with, or operate in co-existence with, existing protocols in the cellular networks.

Considering a migration from Mobile IPv4 to Mobile IPv6, there may be mobile nodes which are upgraded and mobile nodes which are not. Similarly, there may be home and/or visited networks supporting Mobile IPv4, and others supporting Mobile IPv6. Such a scenario must be supported. Mobile nodes supporting Mobile IPv6 must also be able to communicate with mobile nodes supporting Mobile IPv4.

Mobile IP provides authentication of the signalling messages [18][20]. For security reasons, such as keeping the current location of a user unknown to other users, it should also be possible to provide encryption of the Mobile IP signalling. In Mobile IPv4, this may be implemented through, for instance, IPSec tunnels and security associations established on a permanent basis inside and between different administrative domains. It should also be possible to provide encryption of the traffic. A solution is to employ IPSec together with Mobile IPv4, as suggested in [27]. For Mobile IPv6, use of IPSec is included in the protocol [18].

Emerging Internet quality-of-service (QoS) mechanisms are expected to enable wide-spread use of real-time services between stationary nodes, for instance voice over IP and videoconferencing. There will be a demand for using the same kind of services when being mobile. Promising a certain level of QoS to a mobile user is generally difficult, since there may not be enough resources available in the part of the network that the mobile node is moving into. However, when network resources allow, there should be mechanisms to handle QoS for mobile users, particularly in case of handover and route optimization [23]. The differences between stationary and mobile nodes making use of QoS mechanisms should also be minimized, and network operators should not need to employ different QoS platforms for stationary and mobile users. The emerging QoS architectures, Differentiated Services and Integrated Services [4][5][24][25], do not consider mobile nodes. Additions or changes may be needed.

QoS mechanisms enforce a differentiated sharing of bandwidth among services and users. Thus, there must be mechanisms available to identify traffic flows with different QoS attributes, and to make it possible to charge the users accordingly.

It is well known that mobile nodes are more complex to handle than stationary ones. Even so, the extra handling of mobile nodes should be based on the same basic mechanisms as the stationary ones, rather than on separate mechanisms. Among these basic mechanisms are (i) an Authentication, Authorization, Accounting (AAA) infrastructure; (ii) QoS and policy control; and (iii) directory services and gateway services like IP telephony.

As more and more users become mobile, the need for a uniform service delivery across various access technologies increases. Ultimately, the user should not need to know what kind of access technology is in use at a particular moment. When bandwidth and other network capabilities allow, IP-based services should appear the same, independently of the access technology. Moreover, a normal user will try to employ the most efficient access, considering capacity and cost, which means that changes of access technology can be expected during active sessions. Thus, the change of access technology should be as smooth and transparent to the user as possible.

These are general considerations and requirements; some of them may apply to Mobile IP and some may be fulfilled through other protocols and solutions. The following sections address more specific requirements on Mobile IP, in order to provide solutions satisfactory for operators as well as end users.

3. Authentication

The authentication of a mobile node or user can be performed at different locations and be based upon different parameters. We may also consider two phases of the authentication procedure: (i) full or initial authentication; and (ii) subsequent authentications. Full authentication is performed when the existing security associations are insufficient, for instance at initial registration, or when a mobile node requests a new home agent. Subsequent authentications are performed when a mobile node changes its point of attachment, within or between administrative domains, or to renew bindings before they are timed out.

The Mobile IP protocol specifies authentications to be performed at the home agent, and the identifications to be based on the home IP address of the mobile node [18][20]. However, additional solutions and extensions, mainly to Mobile IPv4, have introduced identification and authentication based on the Network Access Identifier (NAI) [1][2][8][9][10][11][12][21]. Basing the authentication on the IP address means that it is the host that is authenticated, while

authentication based on the NAI enables authentication of the mobile user. The latter alternative would lessen the connection between a specific user and a specific host, and provide a secure way for dynamic allocation of IP addresses. Thus, the full authentication must be based on a unique user identity, for example the NAI.

For reasons of subscription handling and charging, the full authentication must always be performed at the home domain or by the home operator, that is, where the user is subscribed. Such authentication procedures have been suggested for Mobile IPv4 in [8][10], and may, for instance, be performed through AAA functionality. Full authentication may not be performed at the home agent, since the home agent may be dynamically allocated.

Once a mobile node is connected to a visited network, performing subsequent authentications at the home domain could result in significant signalling delay. To minimize the signalling delay, and to reduce the signalling between the visited and the home network, it should be possible to perform subsequent authentications in the visited network, as described in [8].

Finally, since the Mobile IP protocol is independent of the access network technology, Mobile IP authentication should be independent of the authentication for the access medium, for instance the radio resources. A separation of the authentication procedures is motivated by the fact that radio resources are scarce, and an access network operator may not want to allow Mobile IP signalling until the access network in itself has accepted to provide resources for a mobile node. Also, different access networks with, for instance, radio-based or fixed access, experience different types of security threats, and may address them differently.

The requirements for the authentication procedure are:

1. There MUST be a generic Mobile IP authentication procedure, specifying full and subsequent authentication, as well as authentication for registration requests or binding updates generated on behalf of a mobile node.

2. Full authentication MUST be performed with the home network, the home administrative domain or with the home operator of the mobile user.

3. There MUST be a unique user identity for full authentication.

4. It SHOULD be possible to perform subsequent authentication locally at the visited network.

5. Mobile IP SHOULD use the same AAA infrastructure as stationary Internet nodes.

4. Registration requests generated on behalf of a mobile node

There may be cases when a mobile node does not support Mobile IP signalling. If so, the signalling between the mobile node and its network access point/foreign agent could be handled by lower-level functionality in the access network. Then, the access point/foreign agent could generate a registration request or binding update on behalf of the mobile node. This was described for Mobile IPv4 in [9] as surrogate registrations.

For reasons of backward compatibility with existing systems, it must be possible to implement Mobile IP without introducing Mobile IP signalling in the terminal. Registration requests/binding updates generated on behalf of a mobile node provide such a solution. They also provide a means to minimize the signalling over the radio link. Lastly, secure full and subsequent authentication for registration requests/binding updates generated on behalf of a mobile node must be ensured according to the generic authentication procedure for Mobile IP.

The requirements for registration requests generated on behalf of a mobile node are:

1. It MUST be possible to employ Mobile IP in a network without introducing Mobile IP signalling in the terminal.

5. Private networks

Since private networks are an important part of the communication network structure, Mobile IP must support private networks and private address spaces. A proposed solution for Mobile IPv4 is to support private address spaces through proxy home and foreign agents [8]. This solution also supports hierarchical foreign agents within a network. Such a hierarchy may be valuable in order to improve handover performance. It may also be important for security reasons, since it allows the existence of agents without direct connection to external agents, that is, agents external to for instance a private network. Another solution for IP mobility support across routing realms is suggested in [26]. Lastly, since most private networks are protected by firewalls, Mobile IP must provide a means for signalling and traffic to pass these firewalls.

Larger private networks may provide their own home agents, but there is also the case where one operator provides a home agent which is shared by several smaller private networks. Then, a mobile node may want access to a private network which is not its home network. In this case, we recognize a need for, for instance, the VPN Identifier Extension in the registration request [9]. The NAI of a mobile user points out the home network of the user and the VPN Identifier Extension points out the final destination of the tunnel.

The requirements for support of private networks are:

1. Support of private address spaces MUST be included in Mobile IPv4.

2. Mobile IP MUST provide a means for signalling and traffic to pass through firewalls.

3. Mobile IP MUST provide a means for a mobile node, or an agent generating registration requests or binding updates on behalf of a mobile node, to request access to a network which is not the home network of the mobile node.

6. Reverse tunnelling

The Mobile IPv4 protocol, as specified in [20], is built on the concept of triangular routing. Reverse tunnelling has been suggested as an addition to Mobile IPv4, to support topologically correct reverse tunnels [19]. Reverse tunnelling may also be valuable to provide location privacy, both for Mobile IPv4 and Mobile IPv6. For reasons of security and charging, it must be possible for a network operator to employ reverse tunnelling, and to refuse mobile nodes, or agents generating registration requests or binding updates on behalf of mobile nodes, which do not request reverse tunnelling when required. It must also be possible to employ encryption of the traffic with reverse tunnelling. Lastly, it should be possible to choose how to employ reverse tunnelling: all the way to the home agent, or to a firewall or gateway between the mobile node, or foreign agent, and the home agent.

The requirements for reverse tunnelling are:

1. It MUST be possible to employ reverse tunnelling together with Mobile IP.

2. For Mobile IPv4, a network operator MUST be able to refuse mobile nodes, or agents generating registration requests/binding updates on behalf of mobile nodes, which do not request reverse tunnelling.

7. Route optimization

New access techniques are expected to give users significantly more bandwidth than today, which will lead to more traffic in the backbone networks. Thus, it is important to minimize the load on the backbone, as well as the delay, through efficient routing. In the Mobile IPv4 protocol, datagrams destined to a mobile node are sent to its home address and are tunnelled by the home agent to the current care-of address [20]. Route optimization is a suggested addition, which allows correspondent nodes to send datagrams directly to a mobile node [23][22]. In order to minimize the delay, and to optimize the utilization of network resources, it must be possible for an operator

to employ route optimization. Especially, this would improve the performance for two mobile nodes located in a visited network, which are communicating with each other. For Mobile IPv6, route optimization is included in the protocol.

The authentication procedure for route optimization must be according to the generic authentication procedure for Mobile IP, and there must be a secure way to distribute information of the current address of a mobile node. If requested, encryption must also be available for the traffic. Integrated and differentiated services [4][5][24][25] do not always handle the change from triangular to optimized routing in a smooth way, and Mobile IP extensions or changes may be needed. Lastly, choosing the optimal route, with respect to the number of hops, may result in a lower level of quality of service. In order to maintain a negotiated quality of service, the quality-of-service mechanisms may need to interact with the route optimization mechanisms.

The requirements for route optimization are:

1. It MUST be possible to employ route optimization together with Mobile IP.

8. Dynamic home address assignment

In many IPv4 networks, including home networks of mobile nodes, addresses are assigned dynamically. Dynamic address assignment provides a means to better utilize the IP addresses in a network. It must be possible to assign an address to a mobile node, which belongs to a home network that usually employs dynamic address assignment. Furthermore, if the home agent is dynamically assigned, the home address needs to be dynamically assigned as well, since the home address must belong to the same sub-network as the home agent [20]. The latter requirement applies to Mobile IPv6 as well as to Mobile IPv4. A solution for dynamic home address assignment for Mobile IPv4 was proposed in [11][12].

The requirements for dynamic home address assignment are:

1. Dynamic home address assignment MUST be included in Mobile IP.

9. Temporary home

According to Mobile IP, as specified in [18][20], the home agent is allocated in the home network. However, mobile users may have a need for a temporary home, not necessarily through a home agent assigned in the home network. The need could be to have an anchor point for some period of time, and the most optimal solution, considering routing performance and signalling delay, would be to have a home agent dynamically assigned in the visited network.

It must be possible for a mobile node, or an agent generating registration requests/binding updates on behalf of a mobile node, to request and obtain a dynamically assigned home agent in the home network or in the visited network. It should also be possible for a mobile node which has obtained a dynamically assigned home agent in a visited network, to keep this home agent when moving to another network.

The requirements for a temporary home solution are:

1. It MUST be possible for a mobile node, or an agent generating registration requests/binding updates on behalf of a mobile node, to request and be assigned a dynamic home agent in the home network.

2. It SHOULD be possible for a mobile node, or an agent generating registration requests/binding updates on behalf of a mobile node, to request and be assigned a dynamic home agent in the visited network.

3. A mobile node which has been assigned a dynamic home agent in a visited network SHOULD be able to keep this home agent when moving to another network.

10. Handover performance

Mobile IPv4, as specified in [20], does not guarantee seamless/loss-less handover between different foreign agents within the same administrative domain. The existing solution may be acceptable for non-delay-sensitive and loss-tolerant applications, but needs to be improved in order to support for instance real-time applications.

There have been suggestions on how to improve the handover performance, in terms of making the signalling procedure faster [8][13][14][15][23]. However, the handover performance still needs to be improved in order to support real-time applications, or to support loss-less handover.

When a mobile node supporting Mobile IPv6 changes care-of address, it is able to generate binding updates to its home agent, to its previous default router and to its correspondent nodes [18]. However, the radio is a scarce resource, and transmission of multiple simultaneous binding updates may not be feasible.

11. Conclusions

This draft provides a list of requirements on Mobile IP for use in cellular networks. Beside the general requirements on functionality and security, there are specific requirements on authentication, address assignment, routing and issues providing interworking with existing cellular solutions.

All the requirements provided in this draft may not be necessary in a first step of introducing Mobile IP in cellular networks. However, we believe that they all need to be considered to eventually support all various demands from different operators and end users.

12. Intellectual property considerations

Ericsson has a patent US 5708655 which might be relevant to the issues considered in this document. If access to this patent should become necessary for implementing any standard or standards proposal based on this document, Ericsson is willing to license this patent and any foreign counterparts on fair and reasonable terms and conditions to anybody for such use. If somebody asking for such a license from Ericsson owns or controls a patent also necessary for implementing the standard, Ericsson consider fair and reasonable terms and conditions to include a grant back license on such patent and any foreign counterparts. For the avoidance of doubt Ericsson supports the handling of IPR issues according to RFC 2026 [7].

13. Acknowledgements

The authors would like to thank Henrik Basilier, Martin Korling, Lars Westberg, Anders Herlitz, Yuri Ismailov, Ulf Olsson, Conny Larsson and Georg Chambert at Ericsson and Thomas Eklund at SwitchCore for their valuable comments.

14. References

[1] B. Aboba: "Support for Mobile IP in Roaming", Internet draft (expired), draft-ietf-roamops-mobileip-01.txt, March 1998.

[2] B. Aboba, M. Beadles: "The Network Access Identifier", RFC 2486, January 1999.

[3] C.B. Becker, B. Patil, E. Qaddoura: "IP Mobility Architecture Framework", Internet draft (work in progress), draft-ietf-mobileip-ipm-arch-00, February 1999.

[4] Y. Bernet, et al.: "A Framework for Differentiated Services", Internet draft (work in progress), draft-ietf-diffserv-framework-02, February 1999.

[5] S. Blake, Editor: "An Architecture for Differentiated Services", RFC 2475, December 1998.

[6] S. Bradner: "Key words for use in RFCs to Indicate Requirements Levels", RFC 2119, March 1997.

[7] S. Bradner: "The Internet Standards Process -- Revision 3", RFC 2026, October 1996.

[8] P.R. Calhoun, G. Montenegro, C.E. Perkins: "Mobile IP Regionalized Tunnel Management", Internet draft (expired), draft-ietf-mobileip-reg-tunnel-00.txt, November 1998.

[9] P.R. Calhoun, G. Montenegro, C.E. Perkins: "Tunnel Establishment Protocol", Internet draft (expired), draft-ietf-mobileip-calhoun-tep-01.txt, March 1998.

[10] P.R. Calhoun, C.E. Perkins: "DIAMETER Mobile IP Extensions", Internet draft (expired), draft-calhoun-diameter-mobileip-01.txt, November 1998.

[11] P.R. Calhoun, C.E. Perkins: "Mobile IP Dynamic Home Address Allocation Extension", Internet draft (expired), draft-ietf-mobileip-home-addr-alloc-00.txt, November 1998.

[12] P.R. Calhoun, C.E. Perkins: "Mobile IP Network Access Identifier Extension", Internet draft (work in progress), draft-ietf-mobileip-mn-nai-02.txt, May 1999.

[13] M. Chuah, A. Yan, Y. Li: "Distributed Registrations Enhancements to Mobile IP", Internet draft (expired), draft-chuali-mobileip-dremip-00.txt, October 1997.

[14] K. El Malki, N.A. Fikouras: "Fast Handoff Method for Real-Time Traffic over Scaleable Mobile IP Networks", Internet draft (work in progress), draft-elmalki-mobileip-fast-handoffs-00.txt, March 1999.

[15] S.F. Foo, K.C. Chua: "Regional Aware Foreign Agent (RAFA) for Fast Local Handoffs", Internet draft (expired), draft-chuafoo-mobileip-rafa-00.txt, November 1998.

[16] E. Gustafsson, A. Herlitz, A. Jonsson, M. Korling: "UMTS/IMT-2000 and Mobile IP/DIAMETER Harmonization", Internet draft (expired), draft-gustafsson-mobileip-imt-2000-00.txt, November 1998.

[17] T. Hiller, Editor: "3G Wireless Data Provider Architecture Using Mobile IP and AAA", Internet draft (work in progress), draft-hiller-3Gwireless-00.txt, March 1999.

[18] D.B. Johnson, C. Perkins: "Mobility Support in IPv6", Internet draft (expired), draft-ietf-mobileip-ipv6-07.txt, November 1998.

[19] G. Montenegro: "Reverse Tunneling for Mobile IP", RFC 2344, May 1998.

[20] C. Perkins, Editor: "IP Mobility Support", RFC 2002, October 1996.

[21] C.E. Perkins, P.R. Calhoun: "Mobile IP Challenge/Response Extensions", Internet draft (work in progress), draft-ietf-mobileip-chal-02.txt, May 1999.

[22] C. Perkins, D.B. Johnson: "Registration Keys for Route Optimization", Internet draft (expired), draft-ietf-mobileip-regkey-00.txt, November 1997.

[23] C. Perkins, D.B. Johnson: "Route Optimization in Mobile IP", Internet draft (work in progress), draft-ietf-mobileip-optim-08.txt, February 1999.

[24] S. Shenker, J. Wroclawski: "General Characterization Parameters for Integrated Service Network Elements", RFC 2215, September 1997.

[25] S. Shenker, J. Wroclawski: "Network Element Service Specification Template", RFC 2216, September 1997.

[26] W.T. Teo, Y. Li: "Mobile IP extension for Private Internets Support (MPN), Internet draft (work in progress), draft-teoyli-mobileip-mvpn-02.txt, February 1999.

[27] J.K. Zao, M. Condell: "Use of IPSec in Mobile IP", Internet draft (expired), draft-ietf-mobileip-ipsec-use-00.txt, November 1997.

15. Addresses

The working group can be contacted via the current chairs:

Erik Nordmark
Sun Microsystems, Inc.
17 Network Circle
Menlo Park, California 94025
USA

nordmark@sun.com

Basavaraj Patil
Nortel Networks Inc.
2201 Lakeside Blvd.
Richardson, TX. 75082-4399
USA

bpatil@nortelnetworks.com

Questions about this memo can be directed to:

Eva Gustafsson, Annika Jonsson
Ericsson Radio Systems AB
Network and Systems Research
SE-164 80 Stockholm
SWEDEN

{eva.m.gustafsson | annika.jonsson}@era.ericsson.se

Elisabeth Hubbard, Jonas Malmkvist, Anders Roos
Telia Research AB
Network Research
Vitsandsgatan 9
SE-123 86 Farsta
SWEDEN

{elisabeth.a.hubbard | jonas.x.malmkvist | anders.g.roos}@telia.se