INTERNET-DRAFT
Internet Engineering Task Force
Carl Williams, Editor
DoCoMo USA Labs

Issued:  March 1, 2002
Expires: September 7, 2002

# Localized Mobility Management Requirements for IPv6

**<draft-ietf-mobileip-lmm-requirements-01.txt>**

Status of This Memo



## Abstract

This document describes requirements for Localized Mobility Management (LMM) for Mobile IPv6.  These requirements are intended to guide the design of a protocol specification for LMMv6. Localized Mobility Management, in general introduces Local Mobility Agent functionality for proxying a Regional care of address that remains the same while the mobile node moves within a Local Mobility Domain, which reduces the binding update signaling latency and the signaling load outside the Local Mobility Domain. By its very nature LMM also serves as a mechanism to hide the Mobile Node's location from observers outside the administration domain (Local Mobility Domain).  The identified requirements are essential for localized mobility management functionality. They are intended to be used as a guide for analysis on the observed benefits over the identified requirements for architecting and deploying LMM schemes.

Table of Contents

1.0 Introduction .................................................... 2
2.0 Terminology ..................................................... 4
3.0 Requirements .................................................... 5
   3.1 Intra-domain mobility ........................................ 5
   3.2 Security ..................................................... 6
   3.3 Induced LMM functional requirement ........................... 6
   3.4 Scalability, Reliability, and Performance .................... 7
   3.5 Mobility Management Support .................................. 8
   3.6 Auto-configuration capabilities for LMM constituents.......... 9
   3.7 Interworking with IP routing infrastructure requirement....... 9
   3.8 Sparse routing element population requirement ................ 9
   3.9 Support for Mobile IPv6 Handover ............................ 10
   3.10 Simple network design requirement .......................... 10
   3.11 Location privacy and tracking support ...................... 10
   3.12 Stability .................................................. 10
   3.13 QoS Requirements ........................................... 10
4.0 Acknowledgments ................................................ 11
5.0 References ..................................................... 12
6.0 Author's Addresses ............................................. 12
7.0 Full Copyright Statement ....................................... 13

## 1.0 Introduction

In order to meet the demands of real-time applications and the expectations of future wireless users for service level quality similar to the one of wireline users, base mobility management in IP networks, and in particular Mobile IPv6 is facing a number of technical challenges in terms of performance and scalability. These manifest themselves as increased latencies in the control signaling between a Mobile Node and its peer entities, namely the Home Agent (HA) and its Corresponding Nodes (CNs).

### 1.1 Motivation

It is well established that real-time applications impose stringent requirements in terms of delay and packet loss.  From an IP mobility perspective any induced latency would cause these applications to experience noticeable degradation in quality as the mobile user transits within the same or over different internet (ISPs) or context (CSPs) service providers.  This is further exacerbated as the rate of transition of the MN (handoff) increases, between different such service or content providers manifested in form of provisioning (domains).  [1]

When a MN transits from its home domain to a foreign one, it is required to provide its Home Agent with its current mobility bindings that yield a reachable destination on the visiting domain.

The MN must send an inter-domain Binding Updates (BU) to notify both its HA and its communicating CN(s) about its movement that has caused attachment to a new Access Router (AR).  For large round-trip times (RTT) between the MN and its HA or CNs (in the order of 300-500 ms), the mobility management signaling is bound to introduce delays as well as potential packet loss in the forwarding of traffic through the HA tunnel (triangular routing) or through direct communication between the MN and the CN. [1]

Furthermore, for a high rate of handoff, the BU of the MN is soon to be rendered invalid; that will require new BUs to be generated at a much higher frequency by the MN and thus result in a signaling overhead for its peer communicating entities; this is bounded by the RTT between the MN and its peers (HA and CNs).

## 1.2 Principles of LMM

To alleviate the above mentioned mobility issues, extensions to the Mobile IPv6 protocol are proposed to minimize or at best, eliminate frequent mobility management signaling (BUs) to its HA and its peer CNs, caused by frequent change of care-of address. This is achieved by introducing Localized Mobility Management Agents (LMM agents) into the visited domain with functionality similar to a HA.  Thus, control messages are either localized (regional) or global signals. Localized signals are those that are bound within a single administrative domain and generally targeted towards the LMM agent(s) whereas global signals are those that are communicated across different administrative domains with their destination the true peers of the MN. With the introduction of regional control messages the signaling load of the MNs corresponding HA and CNs is reduced as long as the MN stays within the administrative domain. [1]

As it has been pointed out, the main issues behind LMMs is to eliminate frequent Binding Updates to both HA and CN entities. This is done introducing a level of indirection by assigning two care-of addresses to each MN: one on-link care-of address (LCoA), and one regional care-of address.  The change of the on-link CoA is visible (mobility-local) only within the visited domain for the purpose of mobility.  The regional care-of address is visible to those peer entities outside the local domain (mobility-global) and it changes when the MN moves between different administrative domains.

## 1.3 Consideration points for LMM design

Having provided some motivation and brief summary of the underlying principles of LMM, it is important to enumerate goals for LMM.

Goals for LMM:

- reduce the signaling induced by changes in the point of attachment due to the movement of a host; this is the fundamental reason for introducing localized mobility management extensions to core Mobile IPv6.

- provide a mechanism whereby the mobile nodes location is hidden from observers outside the administration domain.

- reduce the usage of air-interface and network resources for mobility;

- avoid or minimize the changes of, or impact to the Mobile Node, Home Agent or the Correspondent Node;

- avoid creating single points of failure;

- simplify the network design and provisioning for enabling LMM capability in a network;

- allow progressive LMM deployment capabilities.

Identifying a solid set of requirements that will render the protocol internals, for some LMM scheme, robust enough to cater for the aforementioned considerations becomes essential in designing a widely accepted solution.  The remainder of this document present a set of requirements that encompass essential considerations for the design of an LMM scheme.  It is with this foundation that we can seek to ensure that the resulting LMM solution will best preserve the fundamental philosophies and architectural principles of the Internet in practice today.

## 2.0 Terminology

See [2] for additional terminology.

Administrative Domain A collection of networks under the same administrative control and grouped together for administrative purposes. [2]

Local Mobility        The movement of an IP device without requiring a change to its routable IP address seen by the CN or HA. Although its point of attachment may change during the move, the IP addresses used to reach the device (both its home and globally visible routable IP address) do not change.

| | |
|---|---|
| Local Mobility Agent (LMA) | A Mobile Node uses Local Mobility Agent as a local Home Agent while roaming within a Local Mobility Domain. The LMA proxy Regional CoA, receives all packets on behalf of the Mobile Node and will encapsulate and forward them directly to its current address. |
| Local Mobility Domain | A Local Mobility Domain contains one or more IP subnets, networks, or Administrative Domains. Within the Local Mobility Domain, the globally visible routable IP address assigned to a Mobile Host or Mobile Router serving a Mobile Network does not change. |
| Localized Mobility Management (LMM) | A method of moving an IP device without requiring a change to its routable IP address seen by its peers, namely the MN's HA and its CNs, in order to restrict the signaling area, thus possibly reducing the amount of signaling. |
| Strong Authentication | Techniques that permit entities to provide evidence that they know a particular secret without revealing the secret. [3] |

## 3.0 LMM Requirements

This section describes the requirements of a LMM solution for Mobile IPv6. Only Mobile IPv6 based requirements are described here.

## 3.1 Intra-domain mobility

LMM is introduced to minimize the signaling traffic to the Home Agent and/or Correspondent Node(s) for intra-domain mobility (within an Administrative Domain). This is the fundamental reason for introducing localized mobility management extensions to core Mobile IPv6.

In the LMM infrastructure a Correspondent Node or Home Agent outside the administration domain MUST always be able to address the mobile host by the same IP address, so that from the point of view of hosts outside the administration domain, the IP address of the mobile host remains fixed regardless of any changes in the Mobile Node's subnet.

It is not the intent or goal for LMM to enter the intra-subnet (intra AR) mobility problem space. See [4] for more information on this specific problem space.

## 3.2 Security

**3.2.1 LMM protocol MUST provide for "security provisioning" within the respective administration domain.**

The security of exchanging LMM specific information and signaling MUST be ensured.  Security provisioning includes protecting the integrity, confidentiality, and authenticity of the transfer of LMM specific information within the administration domain.  If applicable, replay protection MUST exist mutually between the LMM agents.

**3.2.2 LMM protocol MUST provide for the security provisioning to be disabled.**

In certain environments the security within the administration domain may not be necessary, or it may be preferred to minimize the LMM protocol overhead. This feature would be used at the network operator's own risk.

**3.2.3 LMM protocol MUST NOT interfere with the security provisioning that exists between the Home Agent and the Mobile Node.**

**3.2.4 LMM protocol MUST NOT interfere with the security provisioning that exists between the Correspondent Node and the Mobile Node.**

**3.2.5 LMM protocol MUST NOT introduce new security holes or the possibility for DOS-style attacks.**

**3.2.6 An LMM scheme MUST provide support for security at the level associated with routing.  LMM SHOULD also ensure** that the network be able to maintain topological confidentiality from visiting mobile nodes.  That is to say that the LMM scheme in use SHOULD NOT reveal the visited network's topology to the Mobile Node.

## 3.3 Induced LMM functional requirements

**3.3.1 Any Localized Mobility Management protocol MUST NOT inject any additional functionality over base IPv6 Mobility [6] at the** Home Agent or any of its peer CNs.  Thus, the LMM framework MUST NOT add any modifications or extensions to the Correspondent Node(s) and Home Agent. It is essential to minimize the involvement of the Mobile Node in routing beyond what is in the basic MIPv6 protocol. Preferences, load balancing, and other complex schemes requiring heavy mobile node involvement in the mobility management task SHOULD BE avoided.

**3.3.2 Non-LMM-aware routers, hosts, Home Agents, and Mobile Nodes**

**MUST be able to interoperate with LMM agents.**

**3.3.3 The LMM framework MUST NOT increase the number of messages between the mobile host and the respective Correspondent Node(s) and Home** Agent. Indeed, the LMM framework MUST minimize the global signaling between the MN and its peers. The amount of regional signaling MUST NOT surpass the amount of global signaling that would have otherwise occurred if LMM were not present.

### 3.4 Scalability, Reliability, and Performance

**3.4.1 The LMM complexity MUST increase at most linearly with the size of the local domain and the number of Mobile Nodes.**

**3.4.2 Any Localized Mobility Management protocol MUST assure that that LMM routing state scales at most linearly with the number** of Mobile Nodes registered, and that the increase in routing state is confined to those ARs/ANRs involved in implementing the LMM protocol at hand. This would involve MIP-specific routing state as binding caches in addition to standard routing table host routes. While host routes cannot be eliminated by any mobility management protocol including base IP mobility, any LMM protocol MUST keep the number of host routes to a minimum.

**3.4.3 The LMM framework MUST NOT create single points of failure in the network. The current access router would be excluded from** this requirement.

**3.4.4 The LMM framework MUST NOT interfere with the Mobile IPv6 performance of a mobile host communications with a Correspondent** Node(s).

#### 3.4.5 Scalable expansion of the network

The LMM framework MUST allow for scalable expansion of the network and provide for reasonable network configuration with regard to peering, inter-administrative domain connectivity, and other inter-administrative domain interoperability characteristics of interest to wireless ISPs. The LMM framework MUST NOT introduce any additional restrictions in how wireless ISPs configure their network, nor how they interconnect with other networks beyond those introduced by standard IP routing. In addition, the amount of regional signaling MUST NOT increase as the Local Domain expands in size.

### 3.4.6 Resilience to topological changes

The LMM protocols MUST be topology-independent.  The LMM protocols MUST be able to adapt to topological changes within the domain.  The topological changes may include the addition or removal/failure of LMM agents or that of changes in the routing of the local domain over which the LMM scheme is applied.

### 3.4.7 Header or Tunneling overhead

Any additional header or tunneling overhead caused by LMM MUST be reduced on the radio link by compression.  The transfer of compressor state on movement SHOULD be possible so as not to introduce any perceived service disruption.

Candidate LMM designs that require additional header overhead for tunnels MUST be reviewed by the ROHC working group to determine if the header compressor can be restarted from transferred compressor context when handover occurs without requiring any full header packet exchange on the new link.

### 3.4.8 Optimized signaling within the administrative domain

By its very nature, LMM reintroduces triangle routing into Mobile IPv6 in that all traffic must go through the LMM agent. There is no way to avoid this. The LMM framework SHOULD be designed in such a way as to reduce the length of the unwanted triangle leg.

The LMM design SHOULD not prohibit optimal placement of LMM agents to reduce or eliminate additional triangle routing introduced by LMM.

### 3.5 Mobility Management Support

The following LMM requirements pertain to both inter-domain and intra-domain hand-off.

**3.5.1 The LMM framework MUST NOT increase the amount of latency or amount of packet loss that exists with the core Mobile IPv6 specification [6].**
Indeed, the LMM framework SHOULD decrease the amount of latency or amount of packet loss that exists with the core Mobile IPv6.

**3.5.2 The LMM framework MUST NOT increase the amount of service disruption that already exists with the core Mobile IPv6 specification.**
Again, the LMM framework SHOULD decrease the amount of service disruption that already exists with the core Mobile IPv6.

**3.5.3 The LMM framework MUST NOT increase the number of messages between the mobile host and the respective Correspondent Node(s) and Home** Agent as is in the core Mobile IPv6 specification. The LMM framework SHOULD decrease the number of messages between the mobile host and the respective Correspondent Node(s) and Home Agent as is in the core Mobile IPv6 specification.

### 3.6 Auto-configuration capabilities for LMM constituents

It is desirable that in order to allow for simple incremental deployment of an LMM scheme, the local mobility agents MUST require minimal (if any) manual configuration. This plug-and-play feature could make use of IPv6 auto-configuration mechanisms, even though most likely other automatic configurations will be needed (such as, for example, learning about adjacent LMM agents). Auto-configuration also facilitates the network to dynamically adapt to general topological changes (whether planned or due to link or node failures).

### 3.7 LMM inter-working with IP routing infrastructure requirement

The LMM framework MUST NOT disrupt core IP routing outside the local domain.

### 3.8 Sparse routing element population requirement

Any LMM protocol MUST be designed to be geared towards incremental deployment capabilities; the latter implies that the LMM scheme itself imposes minimum requirements on the carriers network. Incremental deployment capabilities for an LMM protocol signifies that an initial set of sparse LMM agents can populate the administration domain of a network provider and operate sufficiently. In addition, any LMM scheme MUST be compatible with any additional deployment of LMM agents in future infrastructure expansions; that is to say, allow progressive LMM deployment capabilities.

It is for this reason that the LMM framework MUST NOT require that all routing elements be assumed to be LMM-aware in the signaling interactions of an LMM protocol. The LMM framework MUST BE supported, at the very minimum, by a sparse (proper subset) LMM agent population that is co-located within the routing topology of a single administration domain.

### 3.9 Support for Mobile IPv6 Handover

Since one of the primary goals of LMM is to minimize signaling during handover, an LMM solution MUST be available for the standardized Mobile IPv6 handover algorithms.  LMM and the Mobile IPv6 handover algorithms MUST maintain compatibility in their signaling interactions for fulfilling complementary roles with respect to each other.

This requirement SHOULD NOT be interpreted as ruling out useful optimizations of LMM and Mobile IPv6 handoff schemes that simplify the implementation or deployment of LMM or Mobile IPv6 handoff.

### 3.10 Simple Network design requirement

LMM SHOULD simplify the network design and provisioning for enabling LMM capability in a network and allow progressive LMM deployment capabilities.

### 3.11 Location privacy and tracking support

The LMM framework MUST allow for location privacy for the MN.  The LMM framework MAY provide efficient and scalable location tracking on behalf of a MN.

### 3.12 Stability

LMM MUST avoid any routing loops.

### 3.13 Quality of Service requirements

#### 3.13.1 The LMM MUST have the ability to interwork with the QoS schemes to hide the mobility of the MN to its peer

by avoiding end-to-end QoS signaling.

#### 3.13.2 The LMM MUST have the ability to interwork with the QoS schemes to facilitate the new provisioning of both uplink

and downlink QoS after a handoff.

## 4.0 Acknowledgments

Thank you to all who participated in the LMM requirement discussion on the Mobile IP working group alias.  First, I want to recognize Theo Pagtzis's (University College London) work on LMM requirement analysis. Theo has contributed significantly to the LMM discussion on the mailing list and at IETF working group meetings and has provided text for various requirements and the text for the introduction detailing motivation and basic LMM principles.  Theo's work on requirement analysis will be published soon (see [1] below). Special thanks also to John Loughney (Nokia), Alper Yegin (DoCoMo USA Labs) and Madjid Nakhjiri (Motorola) for providing input to the draft in its preliminary stage.  As editor of the draft a small team was put together to work with me on LMM requirement analysis: Hesham Soliman (Ericsson), Erik Nordmark (Sun), Theo Pagtzis (UCL), James Kempf (DoCoMo USA Labs), and Jari Malinen (Nokia).

Many other working group members have participated in the requirement analysis of LMM for IPv6.  This included writing requirements listed in this document as well as providing insight into requirement analysis.  This made my job as editor of this document quite easy. Members who contributed are:
Charlie Perkins (Nokia), Theo Pagtzis (University College London), Muhammad Jaseemuddin (Nortel), Tom Weckstr (Helsinki University), Jim Bound (Compaq),  Erik Nordmark (Sun), James Kempf (DoCoMo USA Labs), Gopal Dommety (Cisco), Glenn Morrow (Nortel), Arthur Ross (IEEE), Samita Chakrabarti (Sun), Hesham Soliman (Ericsson),

Karim El-Malki (Ericsson), Phil Neumiller (Telocity), Behcet Sarikaya (Alcatel), Karann Chew (University of Surrey), Michael Thomas (Cisco), Pat Calhoun (Black Storm Networking), Bill Gage (Nortel Networks), Vinod Choyi (Alcatel), John Loughney (Nokia), Wolfgang Schoenfeld (GMD IPSI), and David Martin (Nextel).  Recent comments received by Atsushi Takeshita (DoCoMo USA Labs), Daichi Funato (DoCoMo USA Labs), Youngjune Gwon (DoCoMo USA Labs),  Ichiro Okajima (NTT DoCoMo), Jari Malinen (Nokia), and Koshimi Takashi (NTT DoCoMo).  Thanks to Cedric Westphal (Nokia) for a thorough reviewing of the draft.

In addition special thanks to the Mobile IP working group chairs for their input as well as capturing and organizing the initial set of requirements from the discussions, Phil Roberts (Magisto) and Basavaraj Patil (Nokia).

## 5.0 References

[1]            Theo Pagtzis, "Requirements for Localized Mobility Management in IPv6 Networks"; Paper in Submission;

Work In Progress, November 2001.

[2] Manner, J. et al; "Mobility Related Terminology"; draft-manner-seamoby-terms-02.txt; Work In Progress; July 2001.

[3] J.J. Tardo and K. Alagappan, "SPX: Global Authentication Using Public Key Certificates." In Proc IEEE Symp. Research in Security and Privacy.  IEEE CS Press, 1991.

[4] Roberts, P., "Local Subnet Mobility Problem Statement"; draft-proberts-local-subnet-mobility-problem-01.txt; Work In Progress; May 2001.

[5] Perkins, C., "IP Mobility Support". IETF, Request for Comments (RFC) 2002, October 1996.

[6] David B. Johnson, Charles Perkins, "Mobility Support in IPv6"; draft-ietf-mobileip-ipv6-14.txt; July 2001.

[7] Tsirtsis, G. (Editor), "Fast Handovers for Mobile IPv6"; draft-ietf-mobileip-fast-mipv6-00.txt; a work in progress; February 2001.

[8] Loughney, J. (Editor), "SeaMoby Micro Mobility Problem Statement"; draft-ietf-seamoby-mm-problem-01.txt; a work in progress; February 2001.

## 6.0 Authors' Addresses

The working group can be contacted via the current chairs:

Basavaraj Patil
Nokia Corporation
6000 Connection Drive
Irving, TX 75039
USA

Phone:  +1 972-894-6709
EMail:  Raj.Patil@nokia.com
Fax :  +1 972-894-5349

Phil Roberts
Megisto Systems
20251 Century Blvd
Suite 120
Germantown Maryland, 20874-1191

EMail:  proberts@megisto.com

Questions about this memo can also be directed to:

Carl Williams
DoCoMo Communications Laboratories USA, Inc.
181 Metro Drive, Suite 300
San Jose, CA 95110
USA
phone: +1 408 451 4741

fax:   +1 408 573 1090
email: carlw@docomolabs-usa.com

## 7.0 Full Copyright Statement