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

Issued: October 2003
Expires: April 2004

Localized Mobility Management Requirements
<draft-ietf-mobileip-lmm-requirements-04.txt>

Status of This Memo

Abstract

This document describes requirements for Localized Mobility Management (LMM) for Mobile IP and Mobile IPv6 protocols. These requirements are intended to guide the design of a protocol specification for LMM. Localized Mobility Management, in general, introduces enhancements to Mobile IPv4 and Mobile IPv6 to reduce the amount of latency in binding updates sent to the Home Agent and, for route-optimization, Correspondent Nodes, upon Care of Address change. In addition, LMM seeks to reduce the amount of signaling over the global Internet when a mobile node traverses within a defined local 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

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, IP based mobility management is facing a number of
technical
challenges in terms of performance and scalability [4, 5, 6].
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).

In the base Mobile IP protocol [3], movement between two subnets requires that the Mobile Node obtain a new Care of Address in the new subnet. This allows the Mobile Node to receive traffic on the new subnet. In order for the routing change to become effective, however, the Mobile Node must issue a binding update (also known in Mobile IPv4 as a Home Agent registration) to the Home Agent so that the Home Agent can change the routing from the previous subnet to the new subnet. The binding update establishes a host route on the Home Agent between the Mobile Node's Home Address and its new Care of Address. In addition, if route optimization is in use [3], the Mobile Node may also issue binding updates to Correspondent Nodes
to
allow them to send traffic directly to the new Care of Address rather than tunneling their traffic through the Home Agent.

Traffic destined for the Mobile Node is sent to the old Care of Address and is, effectively, dropped until the Home Agent processes the MIPv6 Binding Update or MIPv4 Home Agent Registration. If the Mobile Node is at some geographical and topological distance away

from the Home Agent and Correspondent Nodes, the amount of time involved in sending the binding updates may be greater than 100 hundred milliseconds. This latency in routing update may cause some packets for the Mobile Node to be lost at the old Access Router.
Recently, Mobile IP has been extended by certain local mobility mechanisms, aiming to alleviate the above performance limitations; they are identified as hierarchical/regional or more generically Localized Mobility Management (LMM). LMM schemes allow the Mobile Node to continue receiving traffic on the new subnet without any change in the Home Agent or Correspondent Node binding. The latency involved in updating the Care of Address bindings at far geographical and topological distances is eliminated or reduced until such time as the Mobile Node is in a position to manage the latency cost.

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; reduction in signaling delay will minimize packet loss and possible session loss;

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

- reduce the processing overhead at the peer nodes, thereby improving protocol scalability;

- 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

Please also see [7] for mobility terminology used in this document.

3.0 LMM Requirements

This section describes the requirements for a LMM solution. The requirements are relevant to both Mobile IPv4 and Mobile IPv6.

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 a Local Coverage Area). 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.

3.2 Security

3.2.1 LMM protocol MUST provide for "security provisioning" within the respective local coverage area.

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 NOT interfere with the security provisioning that exists between the Home Agent and the Mobile Node.

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

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

3.3 Induced LMM functional requirements

3.3.1 Any Localized Mobility Management protocol MUST NOT inject any additional functionality over base Mobility [2, 3] 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 MIP and 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 introduce additional 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 basic IP mobility 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

The LMM framework MUST not prevent header compression from being applied.
It is recommended that andidate LMM designs that require additional header overhead for tunnel 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 Local Coverage Area

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.

NOTE: It is not required that a LMM scheme specify LMM agents as
part
of its solution.

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 IP and Mobile IPv6

specification [2, 3]. Indeed, the LMM framework SHOULD decrease
the
amount of latency or amount of packet loss that exists with the core mobility protocols.

3.5.2 The LMM framework MUST NOT increase the amount of service disruption that already exists with the core mobility specifications.

Again, the LMM framework SHOULD decrease the amount of service disruption that already exists with the core mobility protocols.

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 mobility specifications [2, 3]. 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 mobility specifications [2, 3].

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 in the case of Mobile IPv6 [3], 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 carrierÆs 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 IPv4 or 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 IPv4 or Mobile IPv6 handover algorithms. LMM and the Mobile IP or 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 IP or Mobile IPv6 handoff schemes that simplify the implementation or deployment of LMM or Mobile IP 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 Stability

LMM MUST avoid any forwarding loops.

3.12 Quality of Service requirements

3.12.1 The LMM MUST have the ability to coexist with QoS schemes to hide the mobility of the MN to its peer by avoiding end-to-end QoS signaling.

3.12.2 The LMM MUST have the ability to coexist with QoS schemes to facilitate the new provisioning of both uplink and downlink QoS after a handoff.

4.0 Security Considerations

This document does not generate any additional security considerations.

5.0 Acknowledgments

Thank you to all who participated in the LMM requirement discussion on the Mobile IP working group alias. First, the editor wishes to recognize Theo Pagtzis's 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. Special thanks also to Gabriel Montenegro, John Loughney, Alper Yegin, Alberto Lopez Toledo, and Madjid Nakhjiri for providing input to the draft in its preliminary stage and many other comments they had. Thanks to the LMM requirement analysis design team: Hesham Soliman, Erik Nordmark, Theo Pagtzis, James Kempf, and Jari Malinen.

Additional comments on the LMM requirements were received from: Charlie Perkins, Muhammad Jaseemuddin, Tom Weckstr, Jim Bound, Gopal Dommety, Glenn Morrow, Arthur Ross, Samita Chakrabarti, Karim El-Malki, Phil Neumiller, Behcet Sarikaya, Karann Chew, Michael Thomas, Pat Calhoun, Bill Gage, Vinod

Choyi, John Loughney, Wolfgang Schoenfeld, David Martin, Daichi Funato, Ichiro Okajima, Jari Malinen, Kacheong Poon, Koshimi Takashi, and Cedric Westphal.

An LMM requirement analysis of this body of work was completed by a number of members of the Mobile IP working group and published in [1] below.

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

6.0 References

Normative References

[1] T. Pagtzis, C. Williams, P. Kirstein, C. Perkins and A. Yegin, "Requirements for Localised IP Mobility Management", Proceedings of IEEE Wireless Communications and Networking Conference (WCNC2003), Louisiana, New Orleans, March 2003.

[2] Perkins, C., "IP Mobility Support for IPv4," RFC3344, August 2002.

[3] David B. Johnson, Charles Perkins, J. Arkko, "Mobility Support in IPv6", Work in Progress, June 2003.

[4] G. Karlsson, ôQuality Requirements for Multimedia Network Servicesö, Proceedings of Radiovetenskap ach kommunikation, June 1996, pp. 96-100.

[5] T. Kurita, S. Iai, and N. Kitawaki, ôEffects of transmission delay in audiovisual communicationsö, Electronics and Communications in Japan, Vol 77, no 3, pp. 63-74, 1995.

[6] Y. Wang, M. Claypool, and Z. Zuo, ôAn Empirical Study of RealVideo Performance Across the Internetö, in Proceedings of ACM SIGCOMM Internet Measurement Workshop, Nov. 2001.

[7] J. Manner, M. Kojo, ôMobility Related Terminologyö, Work in Progress, April 2003.

Informative References

[8] R. Koodli. (Editor), "Fast Handovers for Mobile IPv6"; Work in Progress; October 2003.

[9] Soliman, H., Castelluccia, C., El-Malki, K., Bellier L.,
ôHierarchical Mobile Ipv6 mobility management (HMIPv6)ö,
Work in progress, June 2003.

Appendix A - LMM requirements and HMIPv6

HMIPv6 was evaluated as a localized mobility management protocol, and that it was mostly found to satisfy the requirements put forth in this document. This section details one exception with some explanation.

Exception 1:

One LMM requirement that needs further clarification with respect to HMIPv6 is the requirement that states that LMM should not introduce additional single points of failure. The HMIPv6 Mobility Anchor Point (MAP) is a new single point of failure. Proposals for HMIPv6 MAP replication can be optionally incorporated in order to avoid this new single point of failure. Such proposals can also be applied to the base Mobile IPv6 specification to also allow for Home Agent failover as well.

Author Address

Carl Williams
MCSR Labs
3790 El Camino Real
Palo ALto, CA 94306 USA
phone: +1 650 279 5903
email: carlw@mcsr-labs.org

Full Copyright Statement