DMM Requirements
draft-ietf-dmm-requirements

H. Anthony Chan, h.a.chan@ieee.org; Dapeng Liu, liudapeng@chinamobile.com; Pierrick Seite, pierrick.seite@orange-ftgroup.com; Hidetoshi Yokota, yokota@kddilabs.jp; Jouni Korhonen, jouni.korhonen@nsn.com; Charles E. Perkins, charliep@computer.org; Melia Telemaco, telemaco.melia@alcatel-lucent.com; Elena Demaria, elena.demaria@telecomitalia.it; Jong-Hyouk Lee, jh.lee@telecom-bretagne.eu; Kostas Pentikousis k.pentikousis@huawei.com; Tricci So, tso@zteusa.com; Carlos J. Bernardos, cjbc@it.uc3m.es; Peter McCann, PeterMcCann@huawei.com; Seok Joo Koh, sjkoh@knu.ac.kr; Wen Luo, luo.wen@zte.com.cn; Sri Gundavelli sgundave@cisco.com; Marco Liebsch, liebsch@neclab.eu; Carl Williams, carlw@mcsr-labs.org; Seil Jeon, seiljeon@av.it.pt; Sergio Figueiredo, sfigueiredo@av.it.pt; Stig Venaas, stig@venaas.com; Luis Miguel Contreras Murillo, lmcm@tid.es; Juan Carlos Zuniga, JuanCarlos.Zuniga@InterDigital.com; Slexandru Petrescu, alexandru.petrescu@gmail.com; Georgios Karagiannis, g.karagiannis@utwente.nl; Julien Laganier, jlaganier@juniper.net; Wassim Michel Haddad, Wassam.Haddad@ericsson.com; Dirk von Hugo, Dirk von Hugo, Dirk.von-Hugo@telekom.de; Ahmad Muhana, amuhanna@awardsolutions.com

Status

- Draft-ietf-dmm-requirements-03
- Edited PS1, PS3, REQ2,
- Added REQ7, PS8
- Comments seem to have converged, seem ready for last call

- Draft-ietf-dmm-requirements-02
- Changes based on discussions in IETF84
- Also minor improvements in text: improve clarity, avoid long sentences
- Uploaded and sent each requirement in separate email to solicit further comments.
- Received no suggested changes

- Draft-ietf-dmm-requirements-01
- Discussed extensively in IETF 84

draft-ietf-dmm-requirements-03

Changes to 03

REQ1: Distributed deployment draft-ietf-dmm-requirements-03

- REQ1:
- Motivation
- PS1: Non-optimal routes: added multicast example
- PS2: Non-optimality in Evolved Network Architecture
- PS3: Low scalability of centralized route and mobility context maintenance change route to tunnel
- PS4: Single point of failure and attack

REQ1: Distributed deployment draft-ietf-dmm-requirements-03

- PS1: Non-optimal routes:
- Routing via a centralized anchor often results in a longer route. The problem is manifested, for example, when accessing a local server or servers of a Content Delivery Network (CDN), or when receiving locally available IP multicast or sending IP multicast packets.
- PS3: Low scalability of centralized tunnel management and mobility context maintenance
- Setting up tunnels through a central anchor and maintaining mobility context for each MN therein requires more resources in a centralized design, thus reducing scalability. Distributing the tunnel maintenance function and the mobility context maintenance function among different network entities can increase scalability.

REQ2: Transparency to Upper Layers when needed draft-ietf-dmm-requirements-03

- REQ2: Rephrase
- Motivation
- PS5: Wasting resources to support mobile nodes not needing mobility support
- PS6: Mobility signaling overhead with peer-to-peer communication

REQ2: Transparency to Upper Layers when needed draft-ietf-dmm-requirements-03

- REQ2: Transparency to Upper Layers when needed DMM solutions MUST provide transparent mobility support above the IP layer when needed. Such transparency is needed, for example, when, upon change of point of attachment to the Internet, an application flow cannot cope with a change in the IP address. However, it is not always necessary to maintain a stable home IP address or prefix for every application or at all times for a mobile node.

REQ7: Flexible multicast distribution draft-ietf-dmm-requirements-03

- Requirement for multicast added:

- REQ7: Flexible multicast distribution
- Motivation
- PS8: Duplicate multicast traffic

REQ7: Flexible multicast distribution draft-ietf-dmm-requirements-03

- REQ7: Flexible multicast distribution
- DMM should enable multicast solutions in flexible distribution scenario. This flexibility enables different IP multicast flows with respect to a mobile host to be managed (e.g., subscribed, received and/or transmitted) using multiple endpoints.
- Motivation: The motivation of this requirement is to consider multicast early so that solutions can be developed to overcome performance issues in multicast distribution scenario. The multicast solution may therefore avoid having multicast-capable access routers being restricted to manage all IP multicast traffic relative to a host via a single endpoint (e.g., regular or tunnel interface), which would lead to the problems described in PS1 and PS6.
- PS8: Duplicate multicast traffic
- IP multicast distribution over architectures using IP mobility solutions (e.g. RFC6224) may lead to convergence of duplicated multicast subscriptions towards the downstream tunnel entity (e.g. MAG in PMIPv6). Concretely, when multicast subscription for individual mobile nodes is coupled with mobility tunnels (e.g. PMIPv6 tunnel), duplicate multicast subscription(s) is prone to be received through different upstream paths. This problem may also exist or be more severe in a distributed mobility environment.

draft-ietf-dmm-requirements-02

Past changes to 02

REQ1: Distributed deployment draft-ietf-dmm-requirements-02

- REQ1:
- Motivation
- PS1: Non-optimal routes
- PS2: Non-optimality in Evolved Network Architecture
- PS3: Low scalability of centralized route and mobility context maintenance
- PS4: Single point of failure and attack

REQ2: Transparency to Upper Layers when needed draft-ietf-dmm-requirements-02

- Minor improvements in text: improve clarity, avoid long sentences
- REQ2:
- Motivation
- PS5: Wasting resources to support mobile nodes not needing mobility support – Rephrase based on comments at IETF84
- O-PS1: Mobility signaling overhead with peer-to-peer communication – Revise to clarify

REQ2: Transparency to Upper Layers when needed draft-ietf-dmm-requirements-02

- PS5: IP mobility support is not always required, and not every parameter of mobility context is always used. For example, some applications do not need a stable IP address during a handover to maintain IP session continuity. Sometimes, the entire application session runs while the terminal does not change the point of attachment.
- O-PS1: Wasting resources when mobility signaling (e.g., maintenance of the tunnel, keep alive, etc.) is not turned off for peer-to-peer communication. Peer-to-peer communications have particular traffic patterns that often do not benefit from mobility support from the network. Thus, the associated mobility support signaling (e.g., maintenance of the tunnel, keep alives, etc.) wastes network resources for no application gain. In such a case, it is better to enable mobility support selectively.

REQ3: IPv6 deployment draft-ietf-dmm-requirements-02

- Minor improvements in text: improve clarity, avoid long sentences
- REQ3
- Motivation

REQ5: Compatibility draft-ietf-dmm-requirements-02

- Re-ordered sentences, rephrase to remove trusted networks
- The DMM solution MUST be able to co-exist with existing network deployments and end hosts. For example, depending on the environment in which DMM is deployed, DMM solutions may need to be compatible with other deployed mobility protocols or may need to interoperate with a network or mobile hosts/routers that do not support DMM protocols. Furthermore, a DMM solution SHOULD work across different networks, possibly operated as separate administrative domains, when allowed by the trust relationship between them.
- Motivation: The motivations of this requirement are (1) to preserve backwards compatibility so that existing networks and hosts are not affected and continue to function as usual, and (2) enable inter-domain operation if desired.

REQ6: Security considerations draft-ietf-dmm-requirements-02

- REQ6: Added examples of security aspects
- Motivation

REQ6: Security considerations draft-ietf-dmm-requirements-02

- DMM protocol solutions MUST consider security aspects, including confidentiality and integrity. Examples of aspects to be considered are authentication and authorization mechanisms that allow a legitimate mobile host/router to use the mobility support provided by the DMM solution; signaling message protection in terms of authentication, encryption, etc.; data integrity and confidentiality; opt-in or opt-out data confidentiality to signaling messages depending on network environments or user requirements.