

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, cjb@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@telekom.de; Ahmad Muhana, amuhanna@awardsolutions.com; Byoung-Jo Kim, macsbug@research.att.com; Hassan Aliahmad, hassan.aliahmad@orange.com

Issue tracker status

- ◆ Issue tracker: <http://tools.ietf.org/wg/dmm/trac/query?status=new&status=assigned&status=reopened&component=requirements>
- ◆ 40 tickets with valuable comments and suggested changes were submitted by Jouni, Byoung-Jo, Hassan, and Charlie
- ◆ Additional help from Perrick, Seil, Jong-Heouk
- ◆ Resolved most tickets in -04, -05,
- ◆ Resolving remaining tickets in -06

Major changes

- ◆ Draft-ietf-dmm-requirements-04, -05, -06
- ◆ Pulled out problem statements into a separate section 4 (with corresponding change in the outline of the draft in the last paragraph of the Introduction section).
- ◆ Major revision in REQ6: security consideration
- ◆ Major revision in REQ07: multicast

draft-ietf-dmm-requirements-06

Changes to 03

Ticket #34(Charles):

- ◆ The problem statement clauses should be located in an initial section. Each problem statement should have a motivation.
- ◆ A motivation is inserted to each REQ where the motivation was missing.

Ticket #38(Charles):

- ◆ Section 4.1
- ◆ REQ1: IP mobility, network access and routing solutions provided by DMM MUST enable distributed deployment for mobility management of IP sessions so that traffic does not need to traverse centrally deployed mobility anchors and thus can be routed in an optimal manner.
- ◆ Changed “IP session” to “flows”
- ◆ REQ1: IP mobility, network access and routing solutions provided by DMM MUST enable distributed processing for mobility management of some flows so that traffic does not need to traverse centrally deployed mobility anchors and thereby avoid nonoptimal routes.

Ticket #39(Charles):

- ◆ Section 1 Introduction:
- ◆ Change:
- ◆ "Notions of localization and distribution of local agents have been introduced to reduce signaling overhead."
- ◆ to:
- ◆ "Notions of localization and distribution of local agents have been introduced to reduce signaling overhead at the centralized routing anchor point."

Ticket #40(Charles):

- ◆ Section 1 Introduction:
- ◆ Change “Gateway selection mechanism” to “A gateway selection mechanism”
- ◆ REQ4: missing motivation
- ◆ Added:
- ◆ Motivation: Reuse of existing IETF work is more efficient and less error-prone.
- ◆ REQ4: no problem statement supporting REQ4:
- ◆ Added: This requirement attempts to avoid the need of new protocols development and therefore their potential problems of being time-consuming and error-prone.

Ticket #40(Charles):

- ◆ Section 1 Introduction:
- ◆ Change “is also taking the” to “also takes”
- ◆ However assigning a gateway anchor node from a visited network in roaming scenario has until recently been done and are limited to voice services only.
- ◆ Delete “However”
- ◆ Issues such as charging and billing require solutions beyond the mobility protocol.
- ◆ Delete: “Issues such as”

Ticket #40(Charles):

- ◆ Section 1 Introduction:
- ◆ When demand exceeds capacity, both traffic offloading and CDN mechanisms could benefit from the development of mobile architectures with fewer levels of routing hierarchy introduced into the data path by the mobility management system.
- ◆ Delete “When demand exceeds capacity,”

Ticket #40(Charles):

- ◆ Section 1 Introduction:
- ◆ This trend towards so-called "flat networks" is reinforced by a shift in user traffic behavior. In particular, there is an increase in direct communications among peers in the same geographical area.
- ◆ Change to:
- ◆ This trend towards so-called "flat networks" works best for direct communications among peers in the same geographical area.

Ticket #40(Charles):

- ◆ Section 3.1
- ◆ Version -03: In centralized mobility management, the mapping information between the persistent node identifier and the **changing** IP address of a mobile node (MN) is kept at a single mobility anchor.
- ◆ Version -05: In centralized mobility management, the mapping information between the persistent node identifier and the **locator** IP address of a mobile node (MN) is kept at a single mobility anchor.

Ticket #40(Charles):

- ◆ Section 3.1
- ◆ Version -03: In particular, Gateway GPRS Support Node (GGSN) and Serving GPRS Support Node (SGSN) in the 3GPP UMTS hierarchical network, and the Packet data network Gateway (P-GW) and Serving Gateway (S-GW) in the 3GPP EPS network, **respectively**, act as anchors in a hierarchy.
- ◆ Version -05: In particular, **the** Gateway GPRS Support Node (GGSN), Serving GPRS Support Node (SGSN) and Radio Network Controller (RNC) in the 3GPP GPRS hierarchical network, and the Packet Data Network Gateway (P-GW) and Serving Gateway (S-GW) in the 3GPP EPS network **all** act as anchors in a hierarchy.

Ticket #40(Charles):

- ◆ Section 3.1
- ◆ Figure 1
- ◆ Change “UMTS, 3GPP EPS” to “3G GPRS, 3GPP EPS”

- ◆ Section 3.1, 3.2
- ◆ Figure 1 and Figure 2
- ◆ Center figure captions

Ticket #40(Charles):

- ◆ Section 3.2
- ◆ Version -03: Mobility management functions may also be distributed to multiple networks as shown in Figure 2, so that a mobile node in any of these networks may be served by a **closeby** mobility function (MF).
- ◆ Version -05: Mobility management functions may also be distributed to multiple networks as shown in Figure 2, so that a mobile node in any of these networks may be served by a **nearby** mobility function (MF).

Ticket #40(Charles):

- ◆ Section 3.2
- ◆ Version -03: A distributed mobility management scheme for **future** flat IP-based mobile network architecture
- ◆ Version -05: A distributed mobility management scheme for flat IP-based mobile network architecture

Ticket #40(Charles):

- ◆ Version -03: Section 4: this section **states** the requirements **as follows**:
- ◆ Version -05: Section 5: this section **identifies** the **following** requirements:
- ◆ Version -03: Distributed **deployment**
- ◆ Version -05: Distributed **processing**

Ticket #40(Charles):

- ◆ Version -03: REQ1: IP mobility, network access and routing solutions provided by DMM MUST enable distributed deployment for mobility management of **IP sessions** so that traffic does not need to traverse centrally deployed mobility anchors and **thus can be routed in an optimal manner.**
- ◆ Version -05: REQ1: IP mobility, network access and routing solutions provided by DMM MUST enable distributed processing for mobility management of **some flows** so that traffic does not need to traverse centrally deployed mobility anchors and **thereby avoid nonoptimal routes.**

Ticket #40(Charles):

- ◆ Version -03: REQ1:
- ◆ This requirement addresses problems PS1, PS2, PS3, and PS4 **in the following**.
- ◆ Version -05: REQ1:
- ◆ This requirement addresses problems PS1, PS2, PS3, and PS4 **in Section 4**.

Ticket #40(Charles):

- ◆ Version -03: PS3:
- ◆ 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, thus reducing scalability. Distributing the tunnel maintenance function and the mobility context maintenance function among different network entities can increase scalability.
- ◆ Version -05: PS3:
- ◆ Setting up tunnels through a central anchor and maintaining mobility context for each MN **usually** requires more **concentrated** resources in a centralized design, thus reducing scalability. Distributing the tunnel maintenance function and the mobility context maintenance function among different network entities **with proper signaling protocol design** can increase scalability.

Ticket #40(Charles):

- ◆ Version -03: PS4:
- ◆ Centralized anchoring may be more vulnerable to single points of failures and attacks than a distributed system..
- ◆ Version -05: PS4:
- ◆ Centralized anchoring **designs** may be more vulnerable to single points of failures and attacks than a distributed system.

Ticket #40(Charles):

- ◆ Version -03: REQ3 Motivation:
- ◆ This requirement **is to be inline with** the general orientation of IETF work. DMM deployment is foreseen in mid- to long-term horizon, when IPv6 is expected to be far more common than today. It is also unnecessarily complex to solve this problem for IPv4, as we will not be able to use some of the IPv6-specific features/tools...
- ◆ Version -05: REQ3 Motivation:
- ◆ This requirement **conforms to** the general orientation of IETF work. DMM deployment is foreseen in mid- to long-term horizon, when IPv6 is expected to be far more common than today.
- ◆ This requirement avoids the unnecessarily complexity in solving the problems in Section 4 for IPv4, which will not be able to use some of the IPv6-specific features..

Ticket #40(Charles):

- ◆ Version -03: REQ5
- ◆ 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..
- ◆ Version -05: REQ5
- ◆ 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 **co-exist** with a network or mobile hosts/routers that do not support DMM protocols.

Ticket #40(Charles):

- ◆ Version -03: REQ5
- ◆ 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.
- ◆ Version -05: REQ5
- ◆ Motivation: (a) to preserve backwards compatibility so that existing networks and hosts are not affected and continue to function as usual, and (b) enable inter-domain operation if desired.

Backup slides

Changes to 03

Section 5.6 – REQ6: Security considerations ticket #29, #27, (closed, Byoung-Jo)

- ◆ A DMM solution MUST not introduce new security risks or amplify existing security risks against which the existing security mechanisms/protocols cannot offer sufficient protection.
- ◆ Motivation: Various attacks such as impersonation, denial of service, man-in-the-middle attacks, and so on, may be launched in a DMM deployment. For instance, an illegitimate node may attempt to access a network providing DMM. Another example is that a malicious node can forge a number of signaling messages thus redirecting traffic from its legitimate path. Consequently, the specific node is under a denial of service attack, whereas other nodes do not receive their traffic. Accordingly, security mechanisms/protocols providing access confidentiality, etc. can be used to protect the DMM entities as they are already used to protect against existing networks and existing mobility protocols defined in IETF. In addition, end-to-end security measures between communicating nodes may already be used when deploying existing mobility protocols where the signaling messages travel over the Internet. For instance, EAP-based authentication can be used for network access security, while IPsec can be used for end-to-end security. When the existing security mechanisms/protocols are applied to protect the DMM entities, the security risks that may be introduced by DMM MUST be considered to be eliminated. Else the security protection would be degraded in the DMM solution versus in existing mobility protocols.
- ◆ Section 6: Security Considerations: Please refer to Session 5.6.

Ticket #27(closed, Byoung-Jo):

- ◆ REQ6: Security consideration.
- ◆ The requirements described here may give the impression that DMM excludes ephemeral security for the purpose of routing to the correct entities, but not necessarily tied to service authorizations or identities. Also, protection requirements beyond what current ISPs deal with for their access routers seem unnecessary. DMM's own security should be limited to risks that DMM adds to the access network, not the whole access network security.

Ticket #29 (closed, Byoung-Jo):

- ◆ REQ6: Security consideration.
- ◆ Related to Ticket #27, "access network security" is confusing here, as it often means allowing access to the network to begin with. DMM must assume that is already done at least in the lower layer or even IP layer. It may or may not offer DMM service to anyone or only to authorized devices/users. I think DMM must cover the situation where the service is offered to anything that asks for it, while ensuring the packets are not redirected to wrong directions.

Section 5.7 – REQ7: Multicast ticket #22(Closed, Jouni)

- ◆ DMM SHOULD consider multicast early so that solutions can be developed not only to provide IP mobility to keep IP multicast sessions when it is needed, but also to avoid network inefficiency issues in multicast traffic delivery (such as duplicate multicast subscriptions towards the downstream tunnel entities). The multicast solutions should therefore avoid restricting the management of all IP multicast traffic to a single host through a dedicated (tunnel) interface on multicast-capable access routers.
- ◆ Motivation: Existing multicast deployment have been introduced after completing the design of the reference mobility protocol, then optimization and extensions have been followed by "patching-up" procedure, thus leading to network inefficiency and non-optimal routing. The multicast solutions should therefore be required to consider efficiency nature in multicast traffic delivery.

Ticket #22(Closed, Jouni):

- ◆ Ticket #22(Jouni):
- ◆ 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 problem described in PS1 or PS6.

Tickets #1,2,3,4 (Closed, Jouni)

- ◆ Ticket #1 (closed, Jouni): abstract:
 - change cellular network to traditional wireless network
- ◆ Ticket #2 (closed, Jouni): abstract:
 - change compatible with to may co-exist with
- ◆ Ticket #3 (closed, Jouni):
 - deleted unused references, moved RFC2119 language from Section 2 to the front.
- ◆ Ticket #4 (closed, Jouni): Section 1
 - Make following bulleted list:
 - a centralized mobility anchor providing global reachability and an always-on experience to the user;
 - extensions to the base protocols to optimize handover performance while users roam across wireless cells; and
 - extensions to enable the use of heterogeneous wireless interfaces for multi-mode terminals (e.g. smartphones).

Ticket #5 (closed, Jouni):

◆ Section 1

➤ Change:

➤ The presence of the centralized mobility anchor allows a mobile node to remain reachable when it is not connected to its home domain.

➤ To

➤ The presence of the centralized mobility anchor allows a mobile node to remain reachable after it has moved to a different network.

Ticket #6 (closed, Jouni):

◆ Section 1

- Change:
- Compared with a distributed approach, a centralized approach is likely to have several issues or limitations affecting performance and scalability, which require costly network dimensioning and engineering to resolve.
- To
- Compared with a distributed approach, a centralized approach is likely to have several issues or limitations affecting performance and scalability, which require costly network engineering to resolve.

Ticket #7 (closed, Jouni):

- ◆ Section 1
- ◆ the availability of multi-mode devices and the possibility
Moreover, the availability of multiple-interface host and the of using several network interfaces simultaneously have motivated the possibility of using several network interfaces simultaneously have development of even more protocol extensions to add more capabilities motivated the development of even more protocol extensions to add and to combine IP multicasting to the base protocol.
 - Change: “multi-mode devices” to “multiple interface host”
 - Delete “and to combine IP multicasting”
 - Change “base protocol” to “mobility management protocol”

Ticket #9 (closed, Jouni):

◆ Section 1

- (e.g. 3GPP work items LIPA/SIPTO [TS.23829])
- Change
- TS.23829
- to
- TS.23.401
- with corresponding change in the list of references

Ticket #10 (closed, Jouni):

◆ Section 1

- Distributed mobility management in a truly flat mobile architecture would anchor the traffic closer to the point of attachment of the user, overcoming the suboptimal route stretch of a centralized mobility scheme.
- delete “, overcoming the suboptimal route stretch of a centralized mobility scheme”

Ticket #11(closed, Jouni):

◆ Section 1

➤ Corrected punctuation “.” to “.”

Ticket #12(closed, Jouni):

◆ Section 1

- mobility can be provided selectively, thus simplifying the context maintained in the different nodes of the mobile network
- Change
- mobility can be provided selectively
- To
- mobility support could be provided selectively
- Change “simplifying the context maintained in the different nodes of the mobile network” to “reducing the amount of context maintained in the network”

Ticket #13(closed, Jouni):

◆ Section 1

- Change “The DMM charter” to “The distributed mobility management (DMM) charter”
- Change “(HA, LMA)” to (e.g., HA, LMA)”
- Change “it can avoid the establishment of non-optimal tunnels between two topologically distant anchors.” to “it can avoid the unnecessary establishment of mechanisms to forward traffic from an old to a new mobility anchor.”

Ticket #14(closed, Jouni):

◆ Section 3.1

- Change “changing IP address” to “locator IP address”
- Change “UMTS network” to “GPRS network”
- Added “Radio Network Controller (RNC)” into the hierarchy in both text and in Figure 1.
- Change “UMTS, 3GPP SAE” to “3G GPRS, 3GPP EPS” in Figure 1

Ticket #15(closed, Jouni):

◆ Section 3.2

- Change: "In other words, such mobility management systems are centralized in both the control plane and the data plane." to "In other words, such mobility management systems are centralized in both the control plane and the data plane (mobile node IP traffic)."

Ticket #16(closed, Jouni): REQ1

- Added
- (Existing route optimization is only a host-based solution. On the other hand, localized routing with PMIPv6 addresses only a part of the problem where both the MN and the CN are located in the PMIP domain and attached to a MAG, and is not applicable when the CN is outside the PMIP domain.)

Ticket #17(closed, Jouni):

- ◆ REQ2 ... upon change of point of attachment to the Internet network
 - Change “Internet” to “network”
- ◆ PS5: Wasting resources to provide mobility support to nodes that do not need such support
 - Change “Wasting” to “Unnecessarily reserving”
- ◆ PS6: (e.g., maintenance of tunnel, keep alive, etc.)
 - Change “keep alive” to “keep alive signaling”
- ◆ PS6: (e.g., maintenance of tunnel, keep alives, etc.)
 - Change “keep alives” to “keep alive signaling”

Ticket #18(closed, Jouni):

- ◆ REQ5 Motivation:
- ◆ Change list indices from (1), (2) to (a), (b) to be consistent with the earlier indices in the draft.

Ticket #19(closed, Jouni):

- ◆ PS7: Complexity problem ...
- ◆ Change to "Deployment with multiple mobility solutions: There are already many variants and extensions of MIP. Deployment of new mobility management solutions can be challenging, and debugging difficult, when they must co-exist with solutions already in the field."

Ticket #20(closed, Jouni):

- ◆ REQ6: Security consideration
- ◆ Suggest editorial change.
- ◆ Superceded by ticket #29, which rewrites REQ6 entirely.

Ticket #21(closed, Jouni):

- ◆ REQ6: Security consideration
- ◆ Suggest editorial change.
- ◆ Superceded by ticket #29, which rewrites REQ6 entirely.
- ◆ REQ6 Motivation: As signaling messages may travel over the Internet, end-to-end security could be required.
- ◆ Change to: “end-to-end security measures between communicating nodes may already be used when deploying existing mobility protocols where the signaling messages travel over the Internet.

Ticket #22(closed, Jouni):

- ◆ REQ7:
- ◆ This requirement addresses the problems PS1 and PS8.
- ◆ Change to:
- ◆ “This requirement addresses the problems PS1 and PS8 described in Section 4.”

Ticket #24, 25(closed, Jouni):

- ◆ Security consideration section
- ◆ The text in this section is deleted in version 06, which refers to the security consideration under REQ6.

Ticket #26(closed, Byoung-Jo):

- ◆ REQ2: Transparency to Upper Layers when needed.
- ◆ Suggest time limit on transparency.
- ◆ Closed after email discussion