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; Costas 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; Byoung-Jo Kim, macsbug@research.att.com; Hassan Aliahmad, hassan.aliahmad@orange.com
Issue tracker status


♦ All 40 tickets closed right after Berlin meeting in version 08
Resolved additional email comments in August 2013

Requirements does not restrict whether to distribute or centralize in the control plane

Included individual draft on prefix coloring
Resolved new email comments in November

REQ1 is revised

Motivation of REQ6 on Security consideration is shortened
Next step
Backup
♦ REQ1

♦ IP mobility, network access and routing solutions provided by DMM MUST enable distributed processing for mobility management so that traffic can avoid traversing single mobility anchor far from the optimal route.
REQ6 No change. Only shortened the motivation.

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 control, integrity, authentication, authorization, 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.