MN IP reachability for the DMM
draft-xiong-dmm-ip-reachability-01

Abstract

   In distributed mobility management (DMM) environment, the mobile node
   (MN) has more than one IP addresses and can use different IP address
   to communicate with different hosts.

   When a new correspondent node (CN) initials an IP session with MN,
   the CN needs to find and select one of the MN's IP addresses to
   provide best performance (e.g. with low delay) for the IP session.

   This draft analyses the existing mechanisms for IP reachability in a
   distributed mobility management environment, and identifies the key
   procedures or enhancements to support the routing-optimized IP
   reachability in a distributed mobility management environment.

Status of this Memo

Copyright and License Notice

Table of Contents

1. Introduction

In distributed mobility management (DMM) environment, the mobile node (MN) has more than one IP addresses and can use different IP address to communicate with different hosts. When a new correspondent node (CN) initials an IP session with MN, the CN needs to find and select one of the MN's IP addresses to best (e.g. with low delay) for the IP session.

This draft analyses the existing mechanisms for IP reachability in a distributed mobility management environment, and identifies the key procedures or enhancements to support the routing-optimized IP reachability in a distributed mobility management environment. This draft tries to find out whether there are technical issues blocking the current existing IP reachability mechanism to be routing-optimized in a distributed mobility management environment, then try to find out how to change or enhance the current existing IP reachability mechanism to be routing-optimized if there are some technical issues. This draft does not define or provide new IP reachability mechanism for the distributed mobility management environment but can provide some guidance to define new IP reachability mechanisms for the distributed mobility management environment.

Currently, there are two main IP reachability solutions to find and select of MN's IP Addresses, one is DDNS[RFC 2136]-based solution that MN registers its new IP address to a DDNS server, and CN obtains the MN's new IP address info from the DDNS server, and then initials an IP session to the MN. The other is Application Server Register-based solution that MN and CN both register their new IP addresses and ports info to the same application server for a given service or application, e.g., MSN messenger and there are three sub-methods for CN to obtain the MN's IP address info and initial an IP session to the MN, which are P2P mode, server central mode, and combined mode.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

this draft introduces the following terms.

MR: Mobile Router

CN: Correspondent Node

DDNS: Distributed DNS

GUID: Global Unique ID

P2P: Peer To Peer

[3](#). Problem Statement

In distributed mobility management (DMM) environment, the mobile node
(MN) has more than one IP addresses to communicate with other hosts.
The MN initials a new IP session with a new CN via the MN's latest IP
address and the IP path between the MN and CN are routing-
optimized[I-D.ietf-dmm-requirements].However, when a new
correspondent node(CN) initials a new IP session with the MN, the CN
doesn't know how to choose the MN's latest IP address to ensure the
IP path between the CN and the MN is routing-optimized. so the IP
reachability in the distributed mobility management is how a new CN
finds out and chooses the MN's latest IP address to initial a new
routing-optimized IP session with the MN.

As described in figure 1, firstly the MN attaches to the MR1 and
address IP1 is allocated to the MN by the MR1, then the MN initials a
new IP session with the CN1 through the MR1 via the address IP1.after
the MN moves to the MR2 and IP2 is allocated to the MN by the MR2,the
MN initials another new IP session with CN2 using IP2, at the same
time, the IP session between the MN's IP1 and CN1 are kept
continuity, after that, a new CN3 wants to initial a new IP session
with the MN, the IP reachability issue needs to be solved: How the
CN3 to get the MN's latest IP address to ensure the new IP session
between the CN3 and the MN is routing-optimized ?

```
            +----+              +----+        +----+
            |CN1 |              |CN2 |        |CN3 |
            +--+-+              +--+-+        +--+-+
           IP1 |                   |IP2          |
               |                   |             |
            +--+--+     IP1     +---+-+     ? ---+
            | MR1 +-----------+ MR2 |
            +--+--+              +-+-+-+
               |                  | |
               |IP1            IP1| |IP2
               |                  | |
             +-+--+     move     ++-+-+
             | MN | ---------- | MN |
             +----+              +----+
```
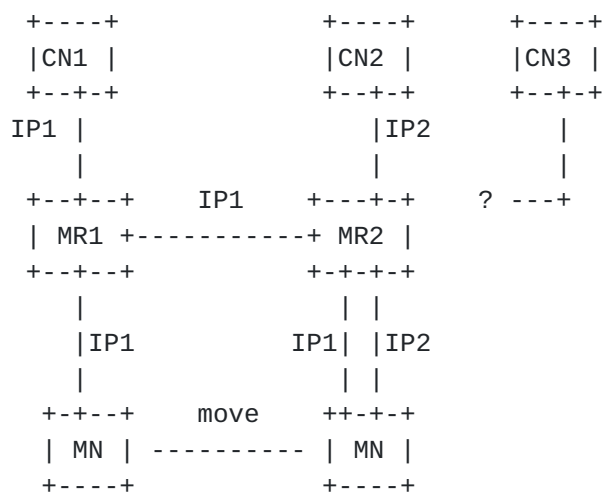
Figure 1: MN routing with multiple IP addresses

4. Solutions Analysis

Currently, there are two main IP reachability solutions to find and
select of MN's latest IP Address, one is DDNS[RFC 2136]-based
solution that MN registers its new IP address to a DDNS server, and
CN obtains the MN's latest IP address info from the DDNS server. The
other is Application Server Register-based solution that MN and CN
both register their latest IP address and ports info to the same
application server for a given service or application, then the CN
obtains the MN's latest IP address info from the application server.

4.1 Solution1 Analysis: DDNS server-based solution

In this solution, each MN has a global unique ID (GUID), e.g. FQDN
[RFC4703] , and a DDNS server stores the MN's latest IP address with
the MN's GUID.As described in figure 2, when the MN attaches to MR1
and gets an IP address IP1 from the MR1, the MN registers its latest
IP address i.e. IP1,and MN's GUID to the DDNS server. The MN initials
a new IP session with CN1 via its latest IP address IP1, after the MN
moves and attaches to the MR2, and gets a new IP address IP2 from the
MR2, the MN immediately refreshes its DDNS registration with its
latest IP address IP2 and the same MN GUID to the DDNS server, If the
MN initials a new IP session with the new CN2, the MN uses its latest
IP address IP2 to setup the IP session to the CN2 to ensure the new
IP session is routing-optimized. At the same time, the IP session
between the MN's IP1 and CN1 are kept IP session continuity via the
distributed mobility management procedure.

If a new CN3 initials a new IP session with the MN, firstly CN3 has
to requests the MN's IP address from DDNS server with the MN GUID,
and DDNS Server responses with the registered MN's IP address, then
the CN3 directly initials to setup a new IP session to the MN with
the retrieved MN's IP address. If the retrieved MN's IP address is
the latest IP address of the MN, then the new IP session between the
CN3 and MN is routing-optimized, otherwise, it is not. So the key
requirement for the DDNS-based IP reachability solution is that the
MN needs to register its latest IP address to the DDNS server.

But the DNS cache mechanism to improve the DNS query speed makes the
things more complex. For example, after the CN3 has got the MN IP
address IPx from the DDNS Server with the MN GUID, the CN3 usually
caches the IPx with MN GUID with a defined timer, if before the timer
expires, the MN has refreshed the DDNS server with its new latest IP
address IPy and the CN3 initials another new IP session, the CN3
still uses the cached IPx to setup the new IP session, this new IP
session is not routing-optimized, for the DDNS-based IP reachability
solution either the CN3 disable its DNS cache function or the DDNS
server indicates that the DNS response can't be cached or is with a

very short validate time (e.g. 200ms).

It seems that the DDNS-based IP reachability solution is very simple
and workable in the distributed mobility management, but there still
needs some additional functions or mechanism to support for this
solution:

1) There needs a mechanism/procedure to allocate a permanent GUID for
each MN, currently, not each GUID is allocated for a MN permanently.
In the mobile telecommunication system, e.g. 3GPP system, a global
unique MSISDN (Mobile Station Integrated Services Data Network) is
allocated to each mobile node.

2) A reliable DDNS Server is needed for the MN to register its latest
IP address and for the CN to query the MN's latest IP address.

3) There still needs a way (out scope of this draft) for a CN to
acquire the MN GUID and the MN registered-DDNS server address before
the CN wants to initial a new IP session to the MN.

```
                   +------------+____Req_____+----+

                   | DNS Server |____Res_____|CN3 |
                   +-----+------+             +--+-+
                  /      /\        \             #
                 /      /  \        \            #
            +-+--+     /    \    +--+-+           #
            |CN1 |    /      \   |CN2 |           #
            +--+-+   /        \  +--+-+           #
           IP1 #   /          \ IP2#             #
              # /              \   #          to IPx
           +--++-+  Tunnel    ++--+-+
           | MR1 +==========+ MR2 |
           +--+--+              ++--+-+
              #                  #   #
           IP1   #            IP1#  # IP2
              #                  #   #
           +-+--+     move      +--+-+
           | MN | --------->  | MN |
           +----+              +----+
```
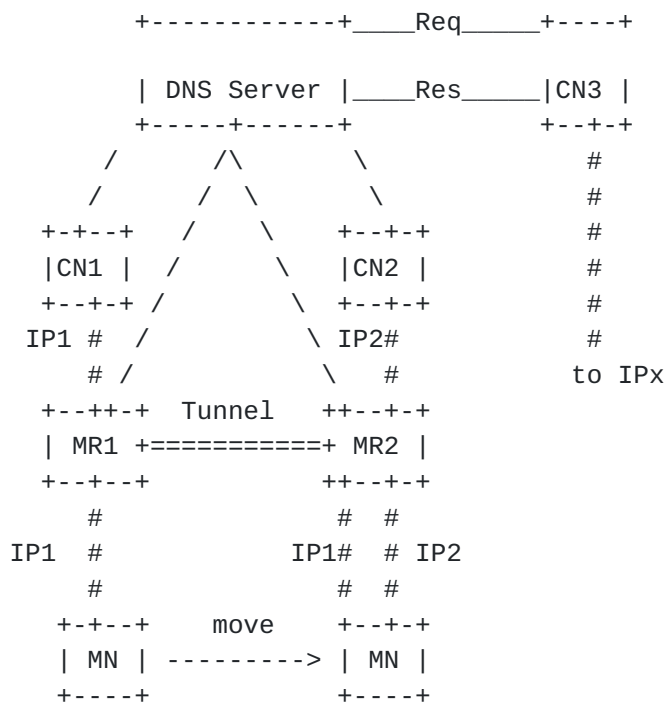
                Figure 2: MN's IP reachability with DDNS server

[4.2](#) Solution2 Analysis : Application Server Registration-based solution

In this solution, for an application or service, e.g., MSN Messenger,
the MN and the CN both register their IP address and (TCP/UDP) port
info to the same (virtual or physical) application server. After

moving and attaching to a new MR, the MN gets a new and latest IP
address from the new MR, the MN refreshes its registration with its
new IP address and port info to the application server immediately or
some time later again depended on the application status of the MN.
There are three mode for the CN to initial a new IP session with the
MN, which is including P2P mode[RFC 5694], Server central mode and
Combined mode.

4.2.1 **P2P mode**

   As described in figure 3, firstly the CN3 has registered its IP
   address and Port info to the same application server as the MN. If
   the CN3 wants to initial a new IP session with the MN, the CN3 sends
   "service request to the MN" message to the application server. In
   this request message, the MN is identified by the application-
   specific ID, e.g. Messenger Name of the MN. The application server
   searches and finds out the MN application context indexed by the MN's
   application ID and gets the MN's registered IP address and port info
   and responses the MN registered IP address and port info to the CN3,
   then the CN3 directly setup a new IP session to the MN by connecting
   to the retrieved MN's IP address and port info. When the MN moves and
   attaches to a new MR2 and get a new IP address IP2 from the MR2, the
   MN can immediately refreshes the application server with the new IP
   address IP2 even when the established IP session between the CN3 and
   the MN is still running and the IP session continuity is kept.

   However, a lot of applications have a separate user plane and control
   plane, i.e. a different IP + Port is used for the application's user
   plane and control plane respectively. For example, the MN can
   register IP1+Port1 for the control plane and dynamically allocates
   IP2+Port2 for the user plane with a host (e.g. SIP/WebRTC/IMS
   service), or the MN can register the IP2+Port1 for the control plane
   and dynamically allocates IP2+Port2 for the user plane with a host.
   For Application Server Registration-based P2P mode, it is required
   that the MN registers the same latest IP address and port number for
   the control plane.

   It seems that the Application Server Registration-based P2P solution
   is almost the same as the DDNS-based solution, As described in the
   DDNS-based solution, the CN needn't to cache the retrieved MN IP
   address and Port info, if the CN wants to initial another new IP
   session with the MN, the CN just request the application server and
   gets the MN's latest registered IP address and port info from the
   application server.

   Based on the above description, it can found out that the Application
   Server Registration-based solution has more advantages than the DDNS-

based solution:

1)In DDNS-based solution, there needs a mechanism/procedure to
allocate a permanent GUID for each MN. In Application Server
Registration-based solution, the MN (also the CN) is assigned a
unique ID by the application server.

2) In DDNS-based solution, a reliable DDNS Server is needed for the
MN to register its latest IP address and for the CN to query the MN's
latest IP address. In Application Server Registration-based solution,
the Application server is always available for the MN and the CN.

3)In DDNS-based solution, there still needs a way (out scope of this
draft) for a CN to acquire the MN GUID and the MN registered-DDNS
server address before the CN wants to initial a new IP session to the
MN. In Application Server Registration-based solution, the MN and the
CN can be included in each other's buddy list or can be found out
each other by the search function of the application.

```
                 +------------+____Req_____+----+
                 |   Server   |____Res_____|CN3 |
                 +-----+------+            +--+-+
                /      /        \              #
               /      /          \             #
           +-+--+    /          +--+-+          #
           |CN1 |   /           |CN2 |          #
           +--+-+  /            +--+-+          #
           IP1 #  /              IP2#           #
              # /                  #          to IPx
           +--++-+   Tunnel  ++--+-+
           | MR1 +==========+ MR2 |
           +--+--+          ++--+-+
              #              #  #
           IP1  #         IP1#  # IP2
              #              #  #
           +-+--+    move    +--+-+
           | MN | ---------> | MN |
           +----+           +----+
```
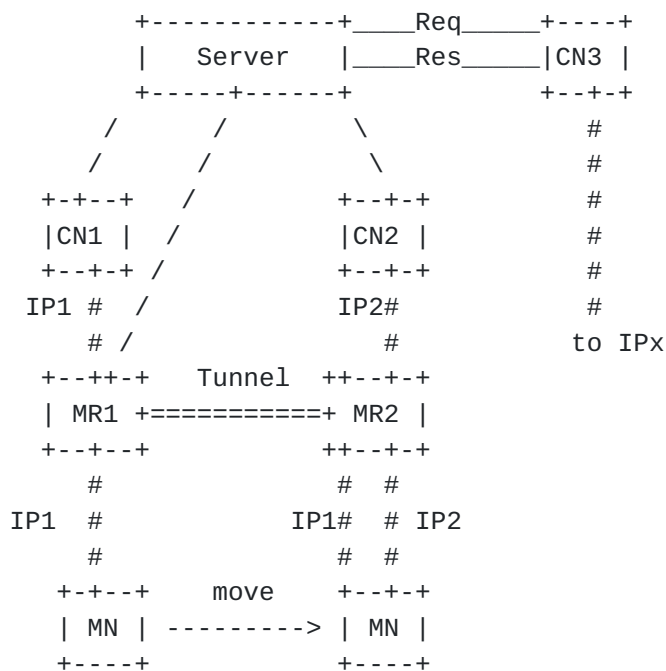
   Figure 3: MN's reachability with Server Registration by P2P mode

4.2.2 Server Central mode

As described in figure 4, firstly the CN3 has registered its IP
address and Port info to the same application server as the MN. If
the CN3 wants to initial a new IP session with the MN, the CN3 sends

"Service Request to the MN" message to the application server. In
this request message, the MN is identified by the application-
specific ID, e.g. Messenger Name of the MN. The application server
responses the server's IP address and port info to the CN3, the CN3
initiate a new IP session to the received the application server's IP
address and the port info. At the same time, the application server
searches and finds out the MN application context indexed by the MN's
application ID, and gets the MN's registered IP address and port info
and initiates a new IP session to the MN via the MN's registered IP
address and port info. After both the IP session between the CN3 and
the Server and the IP session between the application server are
established, and the application server forwarding the application
data between the two IP sessions, the communication between the CN3
and the MN is established. From the CN3 side, it thinks it setups a
new IP session with the MN, and for the MN side, it thinks a new IP
session is established with the CN3, in fact, the IP session is not
directly established, the application server acts as an application
proxy for the CN3 and the MN's IP session. So this method of
establishing a new IP session between the CN and the MN is named as
Application Server Registration-based server central solution.

If a server-central mode IP session between MN and CN1 is established
via the MN's IP1 when the MN attaches to the MR1, after the MN moves
and attaches to a new MR2 and get a new IP address IP2 from the MR2,
the MN can't immediately refreshes the registration to the
application server with the new IP address IP2 if there is a
established IP session for the MN, otherwise the established server-
central mode IP session between CN1 and MN is interrupted. So if the
CN3 wants to initiate a new server-central mode IP session to the MN,
the new IP session is established via the MN's old IP1 instead of the
new IP2, so the new IP session isn't routing optimized. However, for
the application with a separate user plane and control plane, the MN
can't immediately refreshes the registration to the application
server with the new IP address IP2 if there is a established IP
session for the MN , but the MN can dynamically allocates IP2+Port2
for the user plane with the CN3,i.e. that the new IP session with CN3
are combined with IP1+Port1 in control plane and IP2+Port2 in user
plane, in this method, the new IP session is partly routing-optimized
between the application server and the MN. Because the Application
Server Registration-based server central solution can't provide
routing optimization or only provide partly routing optimization, it
is not preferred method to establish an IP session in a distributed
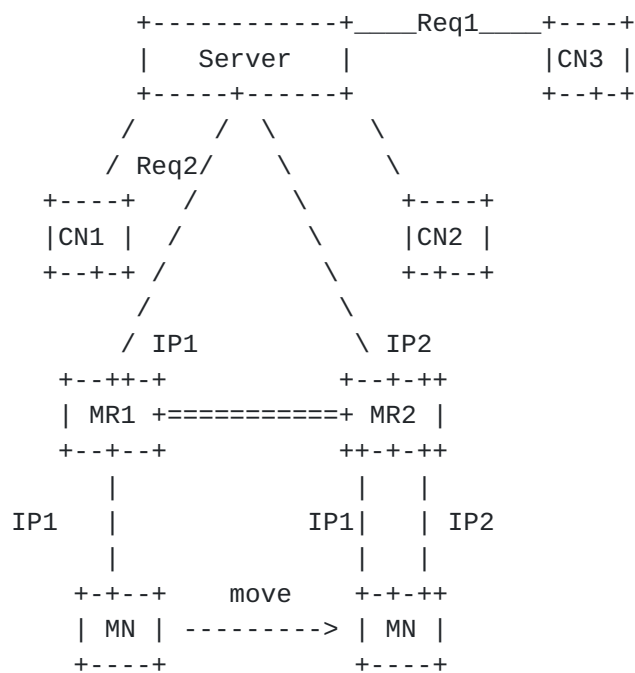mobility management environment.

```
                   +------------+____Req1____+----+
                   |   Server   |            |CN3 |
                   +-----+------+            +--+-+
                  /     / \       \
                 / Req2/   \       \
            +----+   /       \     +----+
            |CN1 |  /         \    |CN2 |
            +--+-+ /           \   +-+--+
                 /             \
                / IP1           \ IP2
            +--++-+             +--+-++
            | MR1 +===========+ MR2 |
            +--+--+             ++-+-++
               |                |  |
         IP1   |            IP1 |  | IP2
               |                |  |
            +-+--+    move     +-+-++
            | MN | --------->  | MN |
            +----+             +----+
```

               Figure 4: MN's reachability with Server Registration by
                             Server central mode

4.2.3 Combined mode

The Application Server Registration-based Combined mode is using the
Server Central mode to discover the MN's control plane IP and port
info and using P2P mode to establish the user plan IP session. As
described in figure 5, firstly the CN3 has registered its IP address
and Port info to the same application server as the MN. If the CN3
wants to initial a new IP session with the MN, the CN3 sends "Service
Request to the MN" message to the application server (in this control
plane). In this request message, the MN is identified by the
application-specific ID, e.g. Messenger Name of the MN. Then the
application server forwards the request message to the MN based on
the MN's registration information (in the MN's control plane),the MN
responses to the application server with MN's user plane IP and Port
info and the application server forwards the MN's responses to the
CN3, the CN3 initiate a new IP session for the user plane data and
keeps the control IP session with the application server and the MN.

If a Combined mode user plane IP session between MN and CN1 is
established via the MN's IP1 when the MN attaches to the MR1, after
the MN moves and attaches to a new MR2 and get a new IP address IP2
from the MR2, the MN can't immediately refreshes the registration to
the application server with the new IP address IP2 if there is a
established IP session for the MN, otherwise the established server-
central mode IP session between CN1 and MN is interrupted. So if the
CN3 wants to initiate a new combined mode IP session to the MN, the

MN's uses the old and shared control plane IP session with CN1 to
provide the MN's user plane IP2+Port2 info to the CN3, then the new
user plane IP session between the CN3 and MN is established via the
MN's latest IP2.In Combined method, the new user plane IP session is
routing-optimized but the control plane is not routing optimized, and
because the traffic in the control plane is some minor, so the
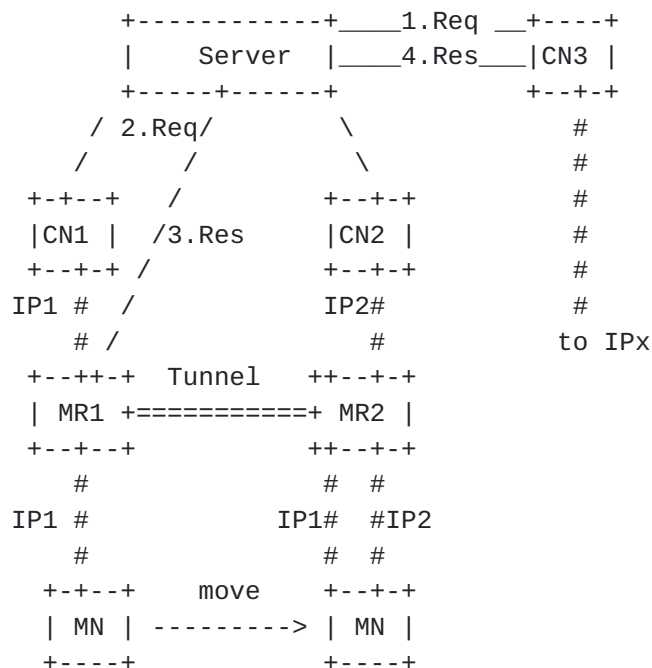control plane's non-routing optimization can be ignored.

```
                +------------+____1.Req __+----+
                |    Server  |____4.Res___|CN3 |
                +-----+------+            +--+-+
               / 2.Req/         \              #
              /      /           \             #
         +-+--+    /           +--+-+           #
         |CN1 |   /3.Res       |CN2 |           #
         +--+-+ /              +--+-+           #
         IP1 #  /              IP2#             #
            # /                  #           to IPx
         +--++-+  Tunnel    ++--+-+
         | MR1 +==========+ MR2 |
         +--+--+            ++--+-+
            #                #  #
         IP1 #            IP1#  #IP2
            #                #  #
          +-+--+    move     +--+-+
          | MN | ---------> | MN |
          +----+            +----+
```
  Figure 5: MN's reachability with Server Registration by Combined mode

4.3 Analysis Summary

Based on the above analysis, most of the current IP reachability
solution can be used in a distributed mobility management
environment. The main conclusion are: 1)The DDNS-based and
Application Server Registration-based P2P mode solution can provide
IP session routing optimization if the MN refreshes the registration
of the DDNS/application server immediately after the latest IP
address is allocated to the MN.

2)The Application Server Registration-based Combined mode solution
can provide user plane IP session routing optimization and the
control plane isn't routing optimized if the MN provides the latest
IP address for the user plane IP session. Since the traffic of the
control plane is minor, so the Application Server Registration-based
Combined mode solution is regard as a good routing optimization
solution.

   3)The Application Server Registration-based Server central solution
   can't provide routing optimization or only provide half segmentation
   routing optimization between the application server and the MN, so
   this method should not be used.

   This draft only analyzes the current well-known IP reachability
   methods without considering the special DMM framework or DMM
   protocols or any special application (e.g. broadcast or multicast).
   The draft needs to be updated with new and good IP reachability
   methods or after DMM protocols are defined or some special
   applications are supported in the DMM environment.

5. Security Considerations

   Security related issues are not considered in current document.

6. IANA Considerations

   None

7. References

7.1 Normative References

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC2136] Vixie, P., Ed., Thomson, S., Rekhter, Y., and J. Bound,
              "Dynamic Updates in the Domain Name System (DNS UPDATE)",
              RFC 2136, April 1997.

   [RFC4703] Stapp, M. and B. Volz, "Resolution of Fully Qualified
              Domain Name (FQDN) Conflicts among Dynamic Host
              Configuration Protocol (DHCP) Clients", RFC 4703, October
              2006.

   [RFC5694] Camarillo, G., Ed., and IAB, "Peer-to-Peer (P2P)
              Architecture: Definition, Taxonomies, Examples, and
              Applicability", RFC 5694, November 2009.

7.2 Informative References

   [I-D.ietf-dmm-requirements] Chan, A., Liu, D., Seite, P., Yokota, H.,

and J. Korhonen, "Requirements for Distributed Mobility
Management", draft-ietf-dmm-requirements-14 (work in
progress),February 2014.

Authors' Addresses

Chunshan Xiong
Huawei Technologies
BeiQing Road No.156
HaiDian District , Beijing   100095
China

Email: sam.xiongchunshan@huawei.com

Jianning Liu
Huawei Technologies
BeiQing Road No.156
HaiDian District , Beijing   100095
China

Email: liujianning.liu@huawei.com