Problem Statement for Network-based Localized Mobility Management
(draft-ietf-netlmm-nohost-ps-04.txt)

Status of this Memo

Abstract

Localized mobility management is a well understood concept in the IETF with a number of solutions already available. This document looks at the principal shortcomings of the existing solutions, all of which involve the host in mobility management, and makes a case for network-based local mobility management.

Contributors

Gerardo Giaretta, Kent Leung, Katsutoshi Nishida, Phil Roberts, and Marco Liebsch all contributed major effort to this document. Their names are not included in the authors' section due to the RFC Editor's limit of 5 names.

Table of Contents

1.0 Introduction

Localized mobility management has been the topic of much work in
the IETF. The experimental protocols developed from previous work,
namely FMIPv6 [1] and HMIPv6 [2], involve host-based solutions that
require host involvement at the IP layer similar to or in addition
to that required by Mobile IPv6 [3] for global mobility management.
However, recent developments in the IETF and the WLAN
infrastructure market suggest that it may be time to take a fresh
look at localized mobility management.

Firstly, new IETF work on global mobility management protocols that
are not Mobile IPv6, such as HIP [4] and MOBIKE [5], suggests that
future wireless IP nodes may support a more diverse set of global
mobility protocols. While it is possible that existing localized
mobility management protocols could be used with HIP and MOBIKE,
some would require additional effort to implement, deploy, or in
some cases even to specify in a non-Mobile IPv6 mobile environment.

Secondly, the success in the WLAN infrastructure market of WLAN
switches, which perform localized management without any host stack
involvement, suggests a possible paradigm that could be used to
accommodate other global mobility options on the mobile node while
reducing host stack software complexity expanding the range of
mobile nodes that could be accommodated.

This document briefly describes the general local mobility problem
and scenarios where localized mobility management would be
desirable. Then problems with existing or proposed IETF localized
mobility management protocols are briefly discussed. The network-
based mobility management architecture and a short description of
how it solves these problems is presented. A more detailed
discussion of goals for a network-based, localized mobility
management protocol and gap analysis for existing protocols can be
found in [6]. Note that IPv6 and wireless links are considered to
be the initial scope for a network-based localized mobility
management, so the language in this document reflects that scope.
However, the conclusions of this document apply equally to IPv4 and
wired links where nodes are disconnecting and reconnecting.

1.1 Terminology

Mobility terminology in this draft follows that in RFC 3753
[7], with the addition of some new and revised terminology
given here:

  Local Mobility (revised)
    Local Mobility is mobility over an access network. Note
    that, although the area of network topology over which the
    mobile node moves may be restricted, the actual geographic
    area could be quite large, depending on the mapping between
    the network topology and the wireless coverage area.

  Localized Mobility Management

    Localized Mobility Management is a generic term for any
    protocol that maintains the IP connectivity and reachability
    of a mobile node for purposes of maintaining session
    continuity when the mobile node moves, and whose signaling
    is confined to an access network.

  Localized Mobility Management Protocol

    A protocol that supports localized mobility management.

  Global Mobility Management Protocol

    A Global Mobility Management Protocol is a mobility protocol
    used by the mobile node to change the global, end-to-end
    routing of packets for purposes of maintaining session
    continuity when movement causes a topology change and thus
    invalidates a global unicast address of the mobile node.
    This protocol could be Mobile IP [1][13] but it could also
    be HIP [4] or MOBIKE [5].

  Global Mobility Anchor Point

    A node in the network where the mobile node maintains a
    permanent address and a mapping between the permanent
    address and the local temporary address where the mobile
    node happens to be currently located. The Global Mobility
    Anchor Point may be used for purposes of rendezvous and
    possibly traffic forwarding.

  Intra-Link Mobility

    Intra-Link Mobility is mobility between wireless access
    points within a link. Typically, this kind of mobility only
    involves Layer 2 mechanisms, so Intra-Link Mobility is often
    called Layer 2 mobility. No IP subnet configuration is
    required upon movement since the link does not change, but
    some IP signaling may be required for the mobile node to

confirm whether or not the change of wireless access point
also resulted in the previous access routers becoming
unreachable. If the link is served by a single access

point/router combination, then this type of mobility
is typically absent. See Figure 1.

2.0 The Local Mobility Problem

The local mobility problem is restricted to providing IP mobility
management for mobile nodes within an access network. The access
network gateways function as aggregation routers. In this case,
there is no specialized routing protocol (e.g. GTP, Cellular IP,
Hawaii, etc.) and the routers form a standard IP routed network
(e.g. OSPF, IS-IS, RIP, etc.). This is illustrated in Figure 1,
where the access network gateway routers are designated as "ANG".
Transitions between service providers in separate autonomous
systems or across broader topological "boundaries" within the same
service provider are excluded.

Figure 1 depicts the scope of local mobility in comparison to
global mobility. The Access Network Gateways (ANGs) GA1 and GB1 are
gateways to their access networks. The Access Routers (ARs) RA1 and
RA2 are in access network A, RB1 is in access network B. Note that
it is possible to have additional aggregation routers between ANG
GA1 and ANG GB1 and the access routers if the access network is
large. Access Points (APs) PA1 through PA3 are in access network A,
PB1 and PB2 are in access network B. Other ANGs, ARs, and APs are
also possible, and other routers can separate the ARs from the
ANGs. The figure implies a star topology for the access network
deployment, and the star topology is the primary one of interest
since it is quite common, but the problems discussed here are
equally relevant to ring or mesh topologies in which ARs are
directly connected through some part of the network.

As shown in the figure, a global mobility protocol may be necessary
when a mobile node (MN) moves between two access networks. Exactly
what the scope of the access networks is depends on deployment
considerations. Mobility between two APs under the same AR
constitutes intra-link, or Layer 2, mobility, and is typically
handled by Layer 2 mobility protocols (if there is only one AP/cell
per AR, then intra-link mobility may be lacking). Between these two
lies local mobility. Local mobility occurs when a mobile node moves
between two APs connected to two different ARs.

Global mobility protocols allow a mobile node to maintain
reachability when the MN's globally routable IP address changes. It
does this by updating the address mapping between the permanent
address and temporary local address at the global mobility anchor
point, or even end to end by changing the temporary local address
directly at the node with which the mobile node is corresponding. A
global mobility management protocol can therefore be used between
ARs for handling local mobility. However, there are three well-

known problems involved in using a global mobility protocol for
every movement between ARs. Briefly, they are:

```
          Access Network A          Access Network B

             +-------+                 +-------+
             |ANG GA1| (other ANGs)    |ANG GB1| (other ANGs)
             +-------+                 +-------+
              @     @                     @
               @       @                  @
                @         @               @    (other routers)
                 @         @              @
                  @          @            @
                   @           @          @
            +------+        +------+          +------+
            |AR RA1|        |AR RA2|(other ARs) |AR RB1|  (other ARs)
            +------+        +------+          +------+
               *               *                 *
              * *              *               * *
             *   *             *              *   *
            *     *            *             *     *
           *       *           *            *       *
          *         *        * (other APs)  *          * (other APs)
         /\         /\        /\            /\          /\
        /AP\       /AP\      /AP\          /AP\        /AP\
       /PA1 \     /PA2 \    /PA3 \         /PB1 \      /PB2 \
       ------     ------    ------         ------      ------


         +--+       +--+       +--+          +--+
         |MN|----->|MN|----->|MN|--------->|MN|
         +--+       +--+       +--+          +--+
       Intra-link     Local        Global
       (Layer 2)     Mobility     Mobility
        Mobility
```
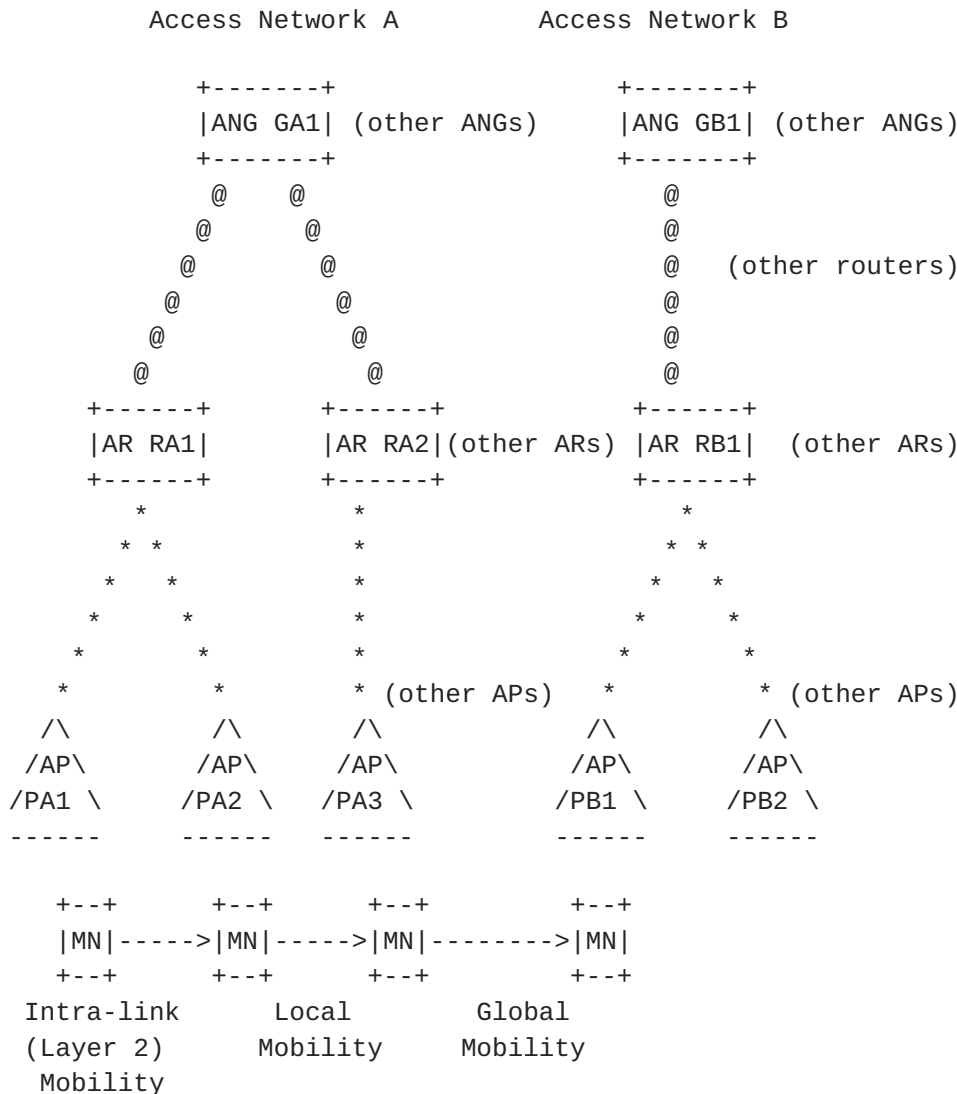
        Figure 1. Scope of Local and Global Mobility Management

1) Update latency. If the global mobility anchor point and/or
   correspondent node (for route optimized traffic) is at some
   distance from the mobile node's access network, the global
   mobility update may require a considerable amount of time.
   During this time, packets continue to be routed to the old
   temporary local address and are essentially dropped.
2) Signaling overhead. The amount of signaling required when a
   mobile node moves from one last hop link to another can be
   quite extensive, including all the signaling required to
   configure an IP address on the new link and global mobility
   protocol signaling back into the network for changing the
   permanent to temporary local address mapping. The signaling
   volume may negatively impact wireless bandwidth usage and real
   time service performance.
 3) Location privacy. The change in temporary local address as the

mobile node moves exposes the mobile node's topological
location to correspondents and potentially to eavesdroppers. An
attacker that can assemble a mapping between subnet prefixes in
the mobile node's access network and geographical locations can
determine exactly where the mobile node is located. This can

expose the mobile node's user to threats on their location
privacy. A more detailed discussion of location privacy for
Mobile IPv6 can be found in [12].

These problems suggest that a protocol to localize the management
of topologically small movements is preferable to using a global
mobility management protocol on each movement to a new link. In
addition to these problems, localized mobility management can
provide a measure of local control, so mobility management can be
tuned for specialized local conditions. Note also that if localized
mobility management is provided, it is not strictly required for a
mobile node to support a global mobility management protocol since
movement within a restricted IP access network can still
be accommodated. Without such support, however, a mobile node
experiences a disruption in its traffic when it moves beyond the
border of the localized mobility management domain.

3.0 Scenarios for Localized Mobility Management

There are a variety of scenarios in which localized mobility
management is useful.

3.1 Large Campus

One scenario where localized mobility management would be
attractive is a large campus wireless LAN deployment. Having a
single broadcast domain for all WLAN access points doesn't scale
very well. Also, sometimes parts of the campus cannot be covered
by one VLAN for other reasons (e.g., some links are other than
802.3).

In this case, the campus is divided into separate last hop links
each served by one or more access routers. This kind of deployment
is served today by wireless LAN switches that co-ordinate IP
mobility between them, effectively providing localized mobility
management at the link layer. Since the protocols are proprietary
and not interoperable, any deployments that require IP mobility
necessarily require switches from the same vendor.

3.2 Advanced Cellular Network

Next generation cellular protocols such as 802.16e [8] and Super
3G/3.9G [9] have the potential to run IP deeper into the access
network than the current 3G cellular protocols, similar to today's
WLAN networks. This means that the access network can become a
routed IP network. Interoperable localized mobility management can
unify local mobility across a diverse set of wireless protocols all
served by IP, including advanced cellular, WLAN, and personal area
wireless technologies such as UltraWide Band (UWB) [10] and

Bluetooth [11]. Localized mobility management at the IP layer does
not replace Layer 2 mobility (where available) but rather
complements it. A standardized, interoperable localized mobility
management protocol for IP can remove the dependence on IP layer
localized mobility protocols that are specialized to specific link

technologies or proprietary, which is the situation with today's 3G protocols. The expected benefit is a reduction in maintenance cost and deployment complexity. See [6] for a more detailed discussion of the goals for a network-based localized mobility management protocol.

3.3 Picocellular Network with Small But Node-Dense Last Hop Links

Future radio link protocols at very high frequencies may be constrained to very short, line of sight operation. Even some existing protocols, such as UWB and Bluetooth, are designed for low transmit power, short range operation. For such protocols, extremely small picocells become more practical. Although picocells do not necessarily imply "pico subnets", wireless sensors and other advanced applications may end up making such picocellular type networks node-dense, requiring subnets that cover small geographical areas, such as a single room. The ability to aggregate many subnets under a localized mobility management scheme can help reduce the amount of IP signaling required on link movement.

4.0 Problems with Existing Solutions

Existing solutions for localized mobility management fall into three classes:

1) Interoperable IP level protocols that require changes to the mobile node's IP stack and handle localized mobility management as a service provided to the mobile node by the access network,
2) Link specific or proprietary protocols that handle localized mobility for any mobile node but only for a specific type of link layer, namely 802.11 running on an 802.3 wired network backhaul.

The dedicated localized mobility management IETF protocols for Solution 1 are not yet widely deployed, but work continues on standardization. Some Mobile IPv4 deployments use localized mobility management. For Solution 1, the following are specific problems:

1) The host stack software requirement limits broad usage even if the modifications are small. The success of WLAN switches indicates that network operators and users prefer no host stack software modifications. This preference is independent of the lack of widespread Mobile IPv4 deployment, since it is much easier to deploy and use the network.
2) Future mobile nodes may choose other global mobility management protocols, such as HIP or MOBIKE. The existing localized mobility management solutions all depend on Mobile IP or derivatives.

3) Existing localized mobility management solutions do not support
   both IPv4 and IPv6.
4) Existing host-based localized mobility management solutions
   require setting up additional security associations with network
   elements in the access domain.

Market acceptance of WLAN switches has been very large, so Solution 2 is widely deployed and continuing to grow. Solution 2 has the following problems:

1) Existing solutions only support WLAN networks with Ethernet backhaul and therefore are not available for advanced cellular networks or picocellular protocols, or other types of wired backhaul.
2) Each WLAN switch vendor has its own proprietary protocol that does not interoperate with other vendor's equipment.
3) Because the solutions are based on layer 2 routing, they may not scale up to a metropolitan area, or local province.

Having an interoperable, standardized localized mobility management protocol   that is scalable to topologically large networks, but requires no host stack involvement for localized mobility management is a highly desirable solution. Mobility routing anchor points within the backbone network maintain a collection of routes for individual mobile nodes. The routes point to the ARs on which mobile nodes currently are located. Packets for the mobile node are routed to and from the mobile node through the mobility anchor point. When a mobile node moves from one AR to another, the ARs send a route update to the mobility anchor point. While some mobile node involvement is necessary and expected for generic mobility functions such as movement detection and to inform the AR about mobile node movement, no specific mobile node to network protocol will be required for localized mobility management itself.

The advantages that this solution has over the Solutions 1 and 2 above are as follows:

1) Compared with Solution 1, a network-based solution requires no localized mobility management support on the mobile node and is independent of global mobility management protocol, so it can be used with any or none of the existing global mobility management protocols. The result is a more modular mobility management architecture that better accommodates changing technology and market requirements.
2) Compared with Solution 2, an IP level network-based localized mobility management solution works for link protocols other than Ethernet, and for wide area networks.

5.0 IANA Considerations

There are no IANA considerations in this document.

6.0 Security Considerations

Localized mobility management has certain security considerations,

one of which - need for access network to mobile node security -
was touched on in this document. Host-based localized mobility
management protocols have all the security problems involved with
providing a service to a host. Network-based localized mobility

management requires security among network elements equivalent to
what is needed for routing information security, and security
between the host and network equivalent to what is needed for
network access, but no more. A more complete discussion of the
security goals for network-based localized mobility management can
be found in [6].

7.0 References

7.1 Informative References

[1] Koodli, R., editor, "Fast Handovers for Mobile IPv6," RFC
    4068, July, 2005.
[2] Soliman, H., Castelluccia, C., El Malki, K., and Bellier. L.,
    "Hierarchical Mobile IPv6 Mobility Management," RFC 4140,
    August, 2005.
[3] Johnson, D., Perkins, C., and Arkko, J., "Mobility Support in
    IPv6," RFC 3775.
[4] Moskowitz, R., and Nikander, P., "Host Identity Protocol (HIP)
    Architecture", RFC 4423, May, 2006.
[5] Eronen, P., editor, "IKEv2 Mobility and Multihoming Protocol
    (MOBIKE)", Internet Draft, work in progress.
[6] Kempf, J., editor, "Goals for Network-based Localized Mobility
    Management", Internet Draft, work in progress.
[7] Manner, J., and Kojo, M., "Mobility Related Terminology", RFC
    3753, June, 2004.
[8] IEEE, "Air Interface for Mobile Broadband Wireless Access
    Systems", 802.16e, 2005.
[9] 3GPP, "3GPP System Architecture Evolution: Report on Technical
    Options   and   Conclusions",   TR   23.882,   2005,
    http://www.3gpp.org/ftp/Specs/html-info/23882.htm.
[10] http://www.ieee802.org/15/pub/TG3a.htm
[11] Bluetooth SIG, "Specification of the Bluetooth System",
    November, 2004, available at http://www.bluetooth.com.
[12] Koodli, R., "IP Address Location Privacy and Mobile IPv6:
    Problem Statement", Internet Draft, work in progress.
[13] Perkins, C., editor, " IP Mobility Support for IPv4", RFC
    3220, August, 2002.

8.0 Acknowledgements

9.0 Author's Addresses

    James Kempf

DoCoMo USA Labs

     181 Metro Drive, Suite 300
     San Jose, CA 95110
     USA
     Phone: +1 408 451 4711
     Email: kempf@docomolabs-usa.com

     Kent Leung
     Cisco Systems, Inc.
     170 West Tasman Drive
     San Jose, CA 95134
     USA
     EMail: kleung@cisco.com

     Phil Roberts
     Motorola Labs
     Schaumberg, IL
     USA
     Email: phil.roberts@motorola.com

     Katsutoshi Nishida
     NTT DoCoMo Inc.
     3-5 Hikarino-oka, Yokosuka-shi
     Kanagawa,
     Japan
     Phone: +81 46 840 3545
     Email: nishidak@nttdocomo.co.jp

     Gerardo Giaretta
     Telecom Italia Lab
     via G. Reiss Romoli, 274
     10148 Torino
     Italy
     Phone: +39 011 2286904
     Email: gerardo.giaretta@tilab.com

     Marco Liebsch
     NEC Network Laboratories
     Kurfuersten-Anlage 36
     69115 Heidelberg
     Germany
     Phone: +49 6221-90511-46
     Email: marco.liebsch@ccrle.nec.de

10.0   IPR Statements

   The IETF takes no position regarding the validity or scope of any
   Intellectual Property Rights or other rights that might be claimed
   to pertain to the implementation or use of the technology described
   in this document or the extent to which any license under such

rights might or might not be available; nor does it represent that
it has made any independent effort to identify any such rights.
Information on the procedures with respect to rights in RFC
documents can be found in BCP 78 and BCP 79.

11.0   Disclaimer of Validity

12.0   Copyright Notice