J. Kempf,
Editor
K. Leung
P. Roberts
K. Nishida
G. Giaretta
M. Liebsch

Internet Draft
Document: draft-kempf-netlmm-nohost-ps-01.txt

Expires: July, 2006 January, 2006

Problem Statement for IP Local Mobility
(draft-kempf-netlmm-nohost-ps-01.txt)

Status of this Memo

Abstract

In this document, the well-known problem of localized mobility management for IP link handover is given a fresh look. After a short discussion of the problem and a couple of scenarios, the principal shortcomings of existing solutions are discussed.

Table of Contents

1.0 Introduction

Localized mobility management has been the topic of much work in the IETF for some time, and it may seem as if little remains to be said on the topic.
The experimental protocols developed from previous work, namely FMIPv6 [1] and HMIPv6[2], involve host-based solutions that mimic to a greater or lesser extent the approach taken 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. Secondly, the success in the WLAN infrastructure market of WLAN switches, which perform localized mobility management without any host stack involvement, suggests a possible design paradigm that could be used to accommodate other global mobility management options on the mobile node while reducing host stack software complexity and expanding the range of mobile nodes that could be accommodated.

This document briefly describes the local mobility problem and a few scenarios where localized mobility management would be desirable. Then, it describes the two most serious problems with existing protocols: the requirement for host stack support, and the complex security interactions required between the mobile node and the access network. More detailed requirements and gap analysis for existing protocols can be found in [6].

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:

IP Link
A set of routers, mobile nodes, and wireless access points that share link broadcast capability or its functional equivalent. This definition covers one or multiple access points under one or several access routers. In the past, such a set has been called a subnet, but this term is not strictly correct for IPv6, since multiple subnet prefixes can be assigned to an IP link in IPv6.

Access Network (revised)

An Access Network consists of following three components: wireless or other access points, access routers, access network gateways which form the boundary to other networks and may shield other networks from the specialized routing protocols (if any) run in the Access Network; and (optionally) other internal access network routers which may also be needed in some cases to achieve a specialized routing protocol.

Local Mobility (revised)

Local Mobility is mobility over a restricted area of the network topology. 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 protocols dealing with IP mobility management confined within the access network. Localized mobility management signaling is not routed outside the access network, although a handover may trigger Global Mobility Management signaling. Localized mobility management protocols exploit the locality of movement by confining movement related changes to the access network.

Global Mobility Protocol
A Global Mobility Protocol is a mobility protocol used by the mobile node to change the global, end-to-end routing of packets when movement causes a topology change and thus invalidates a global unicast address on the local IP link currently in active use by the mobile node. The Global Mobility Protocol allows the mobile node to maintain a mapping between a permanent rendezvous or home address and a temporary care-of address for rendezvous with nodes that want to initiate a connection, and it may also provide direct routing through the rendezvous node and/or optimized routing directly between correspondent nodes and the local address. Typically, this protocol will be Mobile IPv6 [1] but it could also be HIP [4] or Mobike [5] (Note: although Mobike is not considered a mobility management protocol in general, for purposes of this document, it will be so considered because it manages the address map and routing between a fixed VPN endpoint address and a changing local address).

Global Mobility Anchor Point
A node in the network where the mobile node has its fixed home address that maintains the mapping between the home address and care-of address for purposes of rendezvous and possibly traffic forwarding. For Mobile IPv6 [1], this is the home agent. For HIP [4], this is the rendezvous server. For Mobike [5], this is the VPN tunnel gateway in the home

network.

Intra-Link Mobility

Intra-Link Mobility is mobility between wireless access points within an IP Link. Typically, this kind of mobility only involves Layer 2 mechanisms, so Intra-Link Mobility is often called Layer 2 mobility. No IP link 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 a change of IP link. If the IP link consists of 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. An access network consists of a group of access routers connected to wired or wireless access points on the downlink side and a wired IP core through one or more aggregation routers on the side that is routed toward the border router and the Internet. The aggregation routers function as an access network gateway, although in this case, there is no specialized routing protocol and the routers function as a standard IP routed network. This is illustrated in Figure 1, where the aggregation routers are designated as "AggR". 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 Aggregation Routers AggR A1 and B1 are gateways to the access network. The Access Routers AR A1 and A2 are in Access Network A, B1 is in Access Network B. Note that it is possible to have additional aggregation routers between AggR A1 and AggR B1 and the access routers if the access network is large. Access Points AP A1 through A3 are in Access Network A, B1 and B2 are in Access Network B. Other Aggregation Routers, Access Routers, and Access Points are also possible. 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 access routers are directly connected through some part of the network.

```
        Access Network A         Access Network B

            +--------+               +--------+
            |AggR A1| (other AggRs)  |AggR B1| (other AggRs)
            +--------+               +--------+
             @    @                     @
            @      @                    @
           @        @                   @
          @          @                  @
         @            @                 @
        @              @                @
     +-----+       +-----+            +-----+
     |AR A1|       |AR A2|(other ARs) |AR B1|  (other ARs)
     +-----+       +-----+            +-----+
```

```
                 *             *                   *
                * *            *                  * *
               *   *           *                 *   *
              *     *          *                *     *
             *       *         *               *       *
            *         *        * (other APs) *         * (other APs)
           /\          /\       /\            /\          /\
          /AP\        /AP\     /AP\          /AP\        /AP\
         / A1 \      / A2 \   / A3 \        / B1 \      / B2 \
         ------      ------   ------        ------      ------

          +--+      +--+      +--+          +--+
          |MN|----->|MN|----->|MN|-------->|MN|
          +--+      +--+      +--+          +--+
```

Intra-link   Local   Global
Mobility   Mobility   Mobility

Figure 1. Scope of Local and Global Mobility Management

As shown in the figure, a global mobility protocol is 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 access points under the same access router constitutes Intra-link mobility, and is typically handled by Layer 2 mobility protocols (if there is only one access point/cell per access router, then intra-link mobility may be lacking). Between these two lies local mobility. Local mobility occurs when a mobile node moves between two access points connected to two different access routers.

Global mobility protocols allow a mobile node to maintain reachability when a change between access routers occurs, by updating the address mapping between the home address and care-of address at the global mobility anchor point, or even end to end by changing the care-of address directly at the correspondent node. A global mobility management protocol can therefore be used between access routers for handling local mobility. However, there are three well-known problems involved in using a global mobility protocols for every transition between access routers. Briefly, they are:

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 which time packets continue to be routed to the old care-of address and are essentially dropped.
2) Signaling overhead. The amount of signaling required when a mobile node moves from one IP 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 home to care-of address mapping. The signaling volume may negatively impact wireless bandwidth usage and real time service performance.
3) Location privacy. The change in care-of 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.

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 IP link move. 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 attractive.

3.1 Large Campus with Diverse Physical Interconnectivity

One scenario where localized mobility management would be attractive is for a campus wireless LAN deployment in which parts of the campus are connected by links that are other than 802.3 or in which it is not possible to cover the campus by one VLAN. In this case, the campus is divided into separate IP 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 UWB and Bluetooth. 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 requirements for localized mobility management.

3.3 Picocellular Network with Small But Node-Dense IP 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 power, short range operation. For such protocols, extremely small picocells become more practical. Although picocells do not necessarily imply "pico IP links", 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 IP 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 host 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.
3) Use of a standard IGP such as OSPF or IS-IS to distribute host routes, and updating the host routes when the mobile node moves.

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 likely to be 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) Security for the existing localized mobility management solutions requires complex security associations with network elements for no improvement in security over what is available if localized mobility management is not used. In addition to the additional signaling required to set up these security associations, provisioning a mobile node with credentials for roaming to all the access networks where the mobile node might end up may prove difficult, acting as a barrier to deployment.

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.

Solution 3 has the following problems:

1) Each router in the localized mobility management domain is required to maintain a host route table and to search the host route table for routing each packet, limiting the memory and processing power scalability.
2) After handover, until host routes propagate back along the current path of traffic to the localized mobility management domain border, traffic packets for the mobile node are sent to the old router, causing the packets to drop. Since IGPs typically propagate routing updates through

flooding, the delay in host route propagation also limits the topological span of the localized mobility management domain.

3) Rapid movement by the mobile node faster than the rate at which flooding can propagate host routes could lead to a cascading series of host route messages that never stabilize.

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.

5.0 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. Existing localized mobility management solutions increase the need for mobile node to access network signaling and provisioning of the mobile node with credentials without increasing the security beyond what is available if no localized mobility management solution is used. A more complete discussion of the security requirements for localized mobility management can be found in [6].

6.0 Author Information

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

7.0 Informative References

[1] Koodli, R., editor, "Fast Handovers for Mobile IPv6," RFC 4068, July, 2005.
[2] Soliman, H., editor, "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., Nikander, P., Jokela, P., and Henderson, T., "Host Identity Protocol", Internet Draft, work in progress.
[5] Kivinen, T., and Tschopfening, H., "Design of the MOBIKE Protocol", Internet Draft, work in progress.
[6] Kempf, J., Leung, K., Roberts, P., Giaretta, G., Liebsch, M., and Nishita, K.., "Requirements and Gap Analysis for 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.

8.0 IPR Statements

9.0 Disclaimer of Validity

10.0 Copyright Notice

11.0 Changes in 01 (remove before publication)

- Added "revised" to those definitions in Section 1.1 that are revised from RFC 3753.

- Changed "mobile host" to "mobile node" where the wireless device was meant, to avoid confusion about whether mobile routers are supported.

- Added discussion in Section 4 of problems involving using a standard IGP for host route distribution.