Network Working Group
Request for Comments: 4830
Category: Informational

J. Kempf, Ed.
DoCoMo USA Labs

April 2007

Problem Statement for Network-Based Localized Mobility Management (NETLMM)

Status of This Memo

Copyright Notice

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.

Table of Contents

1. Introduction

Localized mobility management has been the topic of much work in the IETF. The experimental protocols developed from previous works, namely Fast-Handovers for Mobile IPv6 (FMIPv6) [13] and Hierarchical Mobile IPv6 (HMIPv6) [18], involve host-based solutions that require host involvement at the IP layer similar to, or in addition to, that required by Mobile IPv6 [10] for global mobility management. However, recent developments in the IETF and the Wireless LAN (WLAN) infrastructure market suggest that it may be time to take a fresh look at localized mobility management.

First, new IETF work on global mobility management protocols that are not Mobile IPv6, such as Host Identity Protocol (HIP) [16] and IKEv2 Mobility and Multihoming (MOBIKE) [4], 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 specify in a non-Mobile IPv6 mobile environment.

Second, 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 are 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 [11]. 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 document follows that in RFC 3753 [14], with the addition of some new and revised terminology given here:

WLAN Switch

A WLAN switch is a multiport bridge Ethernet [8] switch that connects network segments but also allows a physical and logical star topology, which runs a protocol to control a collection of 802.11 [6] access points. The access point control protocol allows the switch to perform radio resource management functions such as power control and terminal load balancing between the access points. Most WLAN switches also support a proprietary protocol for inter-subnet IP mobility, usually involving some kind of inter-switch IP tunnel, which provides session continuity when a terminal moves between subnets.

Access Network

An access network is a collection of fixed and mobile network components allowing access to the Internet all belonging to a single operational domain. It may consist of multiple air interface technologies (for example, 802.16e [7], Universal Mobile Telecommunications System (UMTS) [1], etc.) interconnected with multiple types of backhaul interconnections (such as Synchronous Optical Network (SONET) [9], metro Ethernet [15] [8], etc.).

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, thus invalidating a global unicast address of the mobile node. This protocol could be Mobile IP [10] [17], but it could also be HIP [16] or MOBIKE [4].

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. 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., Generic Tunneling Protocol (GTP), Cellular IP, Hawaii, etc.) and the routers form a standard IP routed network (e.g., OSPF, Intermediate System to Intermediate System (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 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.

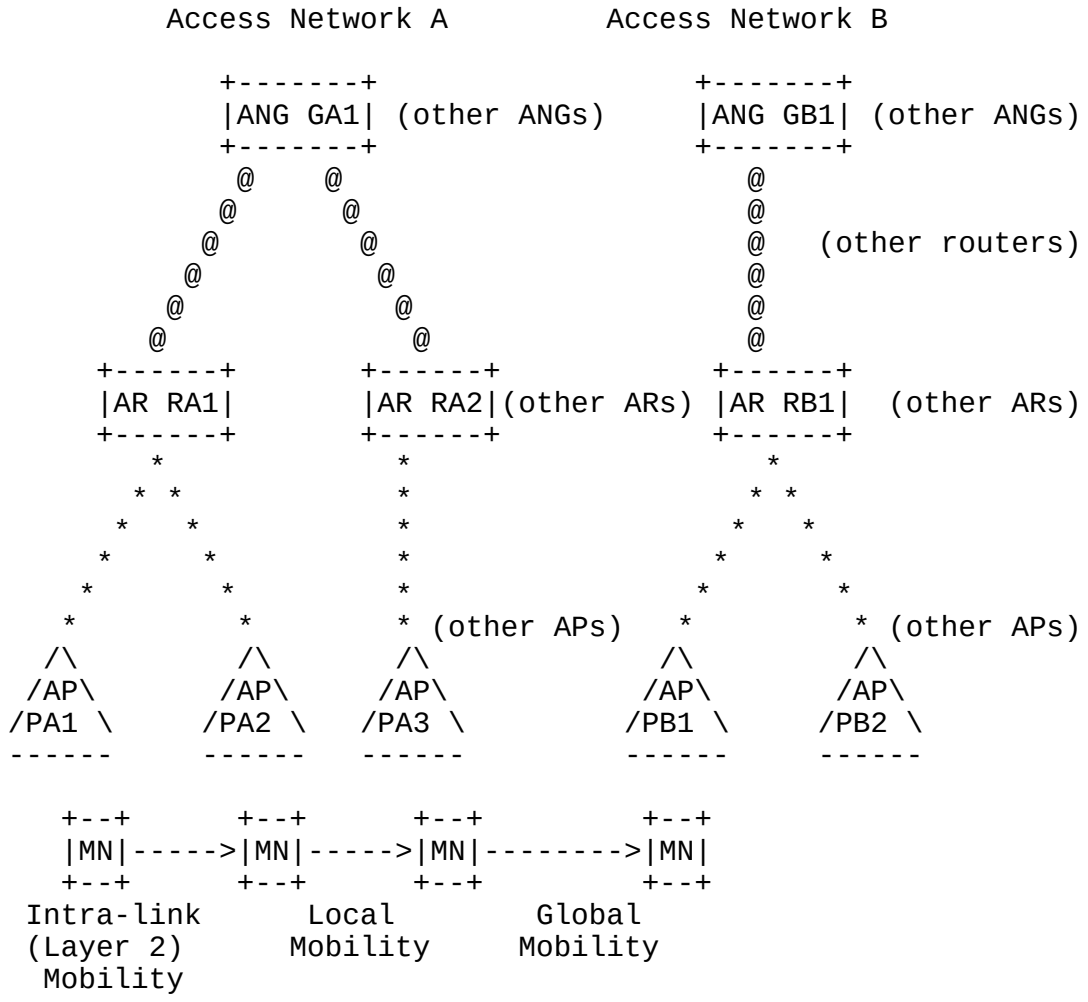

Figure 1. Scope of Local and Global Mobility Management

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:

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. 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 campus WLAN deployment, in which the geographical span of the campus, distribution of buildings, availability of wiring in buildings, etc. preclude deploying all WLAN access points as part of the same IP subnet. WLAN Layer 2 mobility could not be used across the entire campus.

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 WLAN switches that coordinate 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 [7] and Super 3G/3.9G [2], 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) [5] and Bluetooth [3]. 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 [11] 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 [5] and Bluetooth [3], 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. Problems with Existing Solutions

Existing solutions for localized mobility management fall into two 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, for example, 802.11 [6].

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 vendors' equipment.

3) Because the solutions are based on Layer 2 routing, they may not scale up to a metropolitan area or local province, particularly when multiple kinds of link technologies are used in the backbone.

5. Advantages of Network-based Localized Mobility Management

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. The advantages that this solution has over 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.

RFC 4831 [11] discusses a reference architecture for a network-based, localized mobility protocol and the goals of the protocol design.

6. Security Considerations

Localized mobility management has certain security considerations, one of which -- the need for security from access network to mobile node -- was discussed 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 that is equivalent to what is needed for routing information security, and security between the host and network that is 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 [11].

7. Informative References

[1] 3GPP, "UTRAN Iu interface: General aspects and principles", 3GPP TS 25.410, 2002, http://www.3gpp.org/ftp/Specs/html-info/25410.htm.

[2] 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.

[3] Bluetooth SIG, "Specification of the Bluetooth System", November, 2004, available at http://www.bluetooth.com.

[4] Eronen, P., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", RFC 4555, June 2006.

[5] IEEE 802.15 WPAN High Rate Alternative PHY Task Group 3a (TG3a), http://www.ieee802.org/15/pub/TG3a.html.

[6] IEEE, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications", IEEE Std. 802.11, 1999.

[7] IEEE, "Amendment to IEEE Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems - Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands", IEEE Std. 802.16e-2005, 2005.

[8] IEEE, "Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications", IEEE Std. 802.3-2005, 2005.

[9] ITU-T, "Architecture of Transport Networks Based on the Synchronous Digital Hierarchy (SDH)", ITU-T G.803, March, 2000.

[10] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[11] Kempf, J., Ed., "Goals for Network-Based Localized Mobility Management (NETLMM)", RFC 4831, April 2007.

[12] Koodli, R., "IP Address Location Privacy and Mobile IPv6: Problem Statement", Work in Progress, February 2007.

[13] Koodli, R., "Fast Handovers for Mobile IPv6", RFC 4068, July 2005.

[14] Manner, J. and M. Kojo, "Mobility Related Terminology", RFC 3753, June 2004.

[15] Metro Ethernet Forum, " Metro Ethernet Network Architecture Framework - Part 1: Generic Framework", MEF 4, May, 2004.

[16] Moskowitz, R. and P. Nikander, "Host Identity Protocol (HIP) Architecture", RFC 4423, May 2006.

[17] Perkins, C., "IP Mobility Support for IPv4", RFC 3344, August 2002.

[18] Soliman, H., Castelluccia, C., El Malki, K., and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", RFC 4140, August 2005.

8. Acknowledgements

The authors would like to acknowledge the following for particularly diligent reviewing: Vijay Devarapalli, Peter McCann, Gabriel Montenegro, Vidya Narayanan, Pekka Savola, and Fred Templin.

9. Contributors

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

Editor’s Address

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

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.