Mobile IPv6 Extensions (mext)	C.P. Perkins
Internet-Draft	Tellabs
Intended status: Informational	Dapeng. Liu
	China Mobile
	Oct 28, 2011

DMM Comparison Matrix
draft-perkins-dmm-matrix-02

Abstract

Distributed Mobility Management (DMM) is proposed as a way to enable scalable growth of mobile core networks so that network service providers can meet new requirements for performance and reduced operational expenditures. This requires reconsideration of existing approaches within the IETF and elsewhere in order to determine which if any such approaches may be used as part of a DMM solution.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet- Drafts is at http://datatracker.ietf.org/drafts/current/.
Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

Copyright Notice

Table of Contents

1. Introduction

The goal of this document is to identify and compare known existing approaches for Distributed Mobility Management (DMM). Characterizations of each of the various methods selected for comparison are provided in a matrix form according to whether or not they meet certain criteria. Efforts within the IETF have been launched to find improved mobility management by decentralizing some or all of the traditional functions associated with mobility, including handovers, location management, identification, and so on.
The following abbreviations appear in this document:

MN: mobile node

HA: home agent

CN: correspondent node

FQDN: Fully Qualified Domain Name

The following approaches to mobility management are characterized:

Route optimization (RO): MN supplies Binding Updates directly to CN. [RFC3775]

Source address selection refinements (SAddrSel): MN picks source address appropriate for current point of attachment when launching an application.

Dynamically allocated home agent (DynHA): Mobility anchor for MN is allocated on demand.

Binding updates to CN even without HA (CN-wo-HA): Similar to RO, but does not require protocol signaling with home agent.

Transport protocol (Trans-Mob) : MN modifies transport (e.g., TCP, SCTP, DCCP, MPTCP) protocol parameters to change the IP address of transport connection endpoint

Local anchor (Anchor-Mob): Local mobility anchor (e.g., MAP in HMIP [RFC5380]) available for use by MN at its current point of attachment.

Dynamic DNS (DynDNS): When MN gets a new address, DNS is updated so that the MN's FQDN resolves to that new address.

The approaches listed above will be characterized according to the following criteria:

1. scalability: in # of nodes

2. specified?: whether there is a working group document specifying the approach

3. IPadd continuity: provides stable IP address

4. backhaul friendly: reduces burden on backhaul

5. app friendly: apps do not require new code

6. server-friendly: server state minimized, servers do not require new code

7. local routing: "local breakout" / "hairpinning" / local traffic routed locally

8. low signaling: not too much signaling required

2. Matrix Comparing Existing Approaches for DMM

The following matrix rates the approaches described in the the previous section according to the characteristics listed.

	RO	SAddr	DynHA	CN	Trans	Anchor	DynDNS	HIP/
		Sel		wo-HA	Mob	Mob	Mob	LISP
scalability	Y	Y	M	Y	Y	M	M	Y
specified?	Y	N	N	N	Y	Y	Y	Y
IPadd continuity	Y	N	N	Y	Y	Y	N	Y
backhaul friendly	Y	Y	Y	Y	Y	M	Y	M
app friendly	Y	N	Y	Y	N	Y	M	N/Y
server-friendly	M	Y	Y	Y	N	Y	Y	N/Y
local routing	Y	Y	M	Y	Y	N	Y	M
low signaling	N	Y	M	N	N	N	N	N

Table 1: Comparison Matrix [Legend: Y=Yes, N=No, M=Maybe]

3. Explanations for Matrix Entries

Most of the matrix entries are relatively self-evident. For instance, "Trans Mob" (Transport-based Mobility) approaches are rated as not "app friendly" because applications require changes in order to make use of the approach.
For approaches that are identified generically, it may be ambiguous whether or not they are properly specified in any working group document. Here, such approaches are characterized as specified if any particular approach in the generic family is specified. More detail may be needed in the future, in which case more columns or a new table may be needed.

3.1. Route Optimization

Mobile IPv6 supports route optimization and bi-directional tunneling. Using route optimization, the mobile node can send mobility signalling, and subsequently data packets, directly to the correspondent node. The following aspects of route optimization are characterized in the comparison matrix.

1. Scalability: Using route optimization, the signalling and data do not have to be sent through the centralized mobility anchor.

Since the effect of route optimization is to reduce traffic through the home network, scalability is improved. Moreover, route optimization can reduce the effect of the home agent as a single point of failure.

2. Specified: RFC 3775 specifies the route optimization mode of MIPv6.

3. IP address continuity: In MIPv6 route optimization mode, the mobile node still uses the same home address as the bi-directional tunnel mode. RO mode supports IP address continuity.

4. backhaul friendly: In RO mode, the data can send directly to the CN. Data do not need to send through centralized moblity anchor, thence RO is backhaul friendly.

5. app friendly: RO mode does not require application changing, so it is application friendly.

6. server-friendly: RO mode requires the server (i.e., CN) to also support Mobile IP RO mode. In this sense, RO is not server friendly.

7. local routing: In RO mode, the data is forwarded directly between MN and CN, it thence can support local routing.

8. low signaling: MIPv6 RO mode use the return routability procedure. which requires more signalling than MIPv6 bi-directional tunnel mode.

3.2. Source address selection refinements

Source address selection refinements (SAddrSel): MN picks source address appropriate for current point of attachment when launching an application.

1. Scalability: Since the MN can pick a local source address, packets to/from the MN do not have to traverse the home network, improving scalability and reducing delay.

2. Specified: see [RFC3484]

3. IP address continuity: If the MN uses a local source address, IP address continuity is likely to be violated when MN moves to a new network where that address is no longer addressable.

4. backhaul friendly: Since packets do not have to traverse the home network, this solution is more backhaul friendly.

5. app friendly: since applications are likely to require changes in order to make the address selection, this solution is less

app-friendly. If source addresses are selected without involvement of the application, this effect would be eliminated.

6. server-friendly: The source address selection by the application does not involve the server.

7. local routing: Using a local source address enables local routing for local services and communication partners.

8. low signaling: This solution does not impose any signaling signaling requirement, unless the address selection algorithm requires policy management by the operator.

3.3. Dynamically allocated home agent

Dynamically allocated home agent (DynHA): Mobility anchor for MN is allocated on demand.
Scalability: If the network supports dynamically allocated home agents, the mobile node can choose the nearest home agent. Other mobile nodes can use different home agents. But when changing location, home agent may not be able to change accordingly. The mechanism for associating home agents to mobile nodes can vary, and different algorithms have different scalability characteristics; some may be more scalable than others. Method relying on anycast addresses for home agents are among the more scalable approaches.
Specified: RFC 3775 specifies dynamic home agent address discovery and dynamic home prefix discovery. But it does not support changing home agent afterwards. If the MN selected a new home agent, it is likely that existing communications through the previous home agent would be disrupted.
IP address continuity: When mobile node changes location, it may choose a new home agent, but home address would also need to change accordingly, making IP address continuity unlikely.
backhaul friendly: The mobile node can choose the nearest home agent, in this sense, it is backhaul friendly.
app friendly: application does not need to change to support dynamically allocated home agent. So it is app friendly.
server-friendly: server does not need to change to support dynamically allocated home agent, so it is server friendly.
Local routing: When mobile node selects the nearest home agent, it can support local routing through that home agent.
Low signaling: Dynamic discovery and assignment of a home agent may need additional signaling.

3.4. Binding updates to CN even without HA

Binding updates to CN even without HA (CN-wo-HA): Similar to route optimization, but does not require protocol signaling with home agent.

1. Scalability: yes, same as for route optimization.

2. Specified: Internet drafts exist, but no working group document.

3. IP address continuity: yes, same as for route optimization.

4. backhaul friendly: yes, same as for route optimization.

5. app friendly: yes, same as for route optimization.

6. server-friendly: no, same as for route optimization.

7. local routing: yes, same as for route optimization.

8. low signaling: no, same as for route optimization.

3.5. Transport protocol Mobility

Transport protocol (Trans-Mob): MN modifies transport (e.g., TCP, SCTP, DCCP, MPTCP) protocol parameters to change the IP address of transport connection endpoint. In many ways, such approaches resemble CN-wo-HA except that the signaling occurs at a different layer of the protocol stack (namely, at the transport layer instead of the network layer).

1. Scalability: yes, same as for CN-wo-HA.

2. Specified: no, same as for CN-wo-HA.

3. IP address continuity: The point of such approaches is, basically, to eliminate the need for IP address continuity. So, while IP address continuity is not provided, this should not be considered a demerit of transport mobility approaches. It would be better to compare approaches based on "session continuity" instead of "IP address continuity".

4. backhaul friendly: yes, same as for CN-wo-HA.

5. app friendly: yes (typically), same as for CN-wo-HA.

6. server-friendly: no, same as for CN-wo-HA.

7. local routing: yes, same as for CN-wo-HA.

8. low signaling: MIPv6 RO mode use the return routability procedure. which requires more signalling than MIPv6 bi-directional tunnel mode.

3.6. Local anchor

Local anchor (Anchor-Mob): Local mobility anchor (e.g., MAP in HMIP [RFC5380]) available for use by MN at its current point of attachment.

1. Scalability: The mobile node signals the nearest anchor. MNs in other networks can use different anchors. Scalability is improved because the signaling path between the mobile node and its local anchor is shorter. Moreover, local mobility anchors

offload work from any remote mobility anchor such as the home agent.

2. Specified: HMIP[RFC5380]

3. IP address continuity: In conjunction with Mobile IPv6 as a macro mobility protocol, IP address continuity is enabled.

4. backhaul friendly: The mobile node can choose the nearest local anchor; in this sense, it is backhaul friendly.

5. app friendly: application does not need to change to support dynamically allocated home agent. So it is app friendly.

6. server-friendly: server does not need to change to support local mobility anchor, so it is server friendly.

7. Local routing: Generally, the use of a local anchor does not necessarily improve local routing; additional functionality would need to be designed or included with the local anchor.

8. Low signaling: Additional signaling is required for the mobile node to insert new bindings at the local anchor.

3.7. HIP/LISP

HIP: Host Identity Protocol(RFC 4423); LISP: Locator/ID Separation Protocol.

1. Scalability: HIP/LISP are both location/indentification separation protocol. Both HIP/LISP can support large scale deployment in HIP/LISP domain. But when a node running HIP/LISP needs to communicate with other hosts that are not located in the HIP/LISP domain, another mechanism is needed.

2. HIP is specified in RFC 4423[RFC5380]. LISP is specified in [I-D.ietf-lisp].

3. IP address continuity: HIP/LISP both use host indentification for addressing. The host can use a stable IP address for identification and addressing, thence HIP/LISP can support IP address continuity.

4. backhaul friendly: HIP/LISP both use routing address for packet routing; there is no centralized anchor point in the data plane. But for communication to other hosts which are not located in the HIP/LISP domain, a gateway function is needed and the data traffic is constrained to travel through the gateway.

5. app friendly: LISP does not require application modification. HIP may require application modification [RFC 6317].

6. server-friendly: For mobile nodes, HIP may require server modifications; LISP does not require server modification.

7. Local routing: For communication within the HIP/LISP domain, HIP/LISP can support local routing since the routing is based on routing prefix instead of host indentification and there is no centralized anchor point.

8. Low signaling: HIP/LISP need new signaling in the host/network to support its function.

4. Security Considerations

This document does not have any security considerations.

5. IANA Considerations

This document does not have any IANA actions.

6. References

[I-D.ietf-lisp]	Farinacci, D, Fuller, V, Meyer, D and D Lewis, "Locator/ID Separation Protocol (LISP)", Internet-Draft draft-ietf-lisp-16, November 2011.
[RFC3484]	Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", RFC 3484, February 2003.
[RFC3775]	Johnson, D., Perkins, C. and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.
[RFC4423]	Moskowitz, R. and P. Nikander, "Host Identity Protocol (HIP) Architecture", RFC 4423, May 2006.
[RFC5380]	Soliman, H., Castelluccia, C., ElMalki, K. and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", RFC 5380, October 2008.

Appendix A. Acknowledgements

This document has benefitted from discussions with the following people, in no particular order: Seok Joo Koh, Jouni Korhonen, Julien Laganier, Dapeng Liu, Telemaco Melia, Pierrick Seite

Authors' Addresses

Charles E. Perkins Perkins Tellabs Phone: +1-408-421-1172 EMail: charliep@computer.org

Dapeng Liu Liu China Mobile Phone: +86-123-456-7890 EMail: liudapeng@chinamobile.com