Distributed Mobility Management: Current Practices and Gap Analysis

draft-ietf-dmm-best-practices-gap-analysis-02

Juan Carlos Zuniga (Editor) – Presenting
Dapeng Liu (Editor)
CJ. Bernardos
Pierrick Seite
H Anthony Chan

Current Status

- 02 version
  - Updated based on last IETF#87's discussion and comments on the ML.
- Comments resolution
  - Resolved all the comments received since IETF#87
  - Rewrote gap analysis section

Comments Resolution

Comments from Alper Yegin (2013-07-17):

[AY01]

It is typically the role of a connection manager to distinguish application capabilities and trigger the mobility support accordingly.

and

Multiple IP address management: ability of the mobile node to simultaneously use multiple IP addresses and select the best one (from an anchoring point of view) to use on a per-session/ application/service basis. Depending on the mobile node support, this functionality might require more or less support from the network side. This is typically the role of a connection manager.

I'm not sure if this is really a connection manager issue. This is more of a source address selection issue.

Proposed resolution:

OLD TEXT:

3. Mobility management should be realized by the preservation of the IP address across the different points of attachment during the mobility (i.e., provision of IP address continuity). IP flows of applications which do not need a constant IP address should not be handled by DMM. It is typically the role of a connection manager to distinguish application capabilities and trigger the mobility support accordingly. Further considerations on application management are out of the scope of this document.

NEW TEXT:

3. Mobility management should be realized by the preservation of the IP address across the different points of attachment during the mobility (i.e., provision of IP address continuity). IP flows of applications which do not need a constant IP address should not be handled by DMM. Typically, the a connection manager together with the operating system configure the source address selection mechanism of the IP stack. This might involve identifying application capabilities and triggering the mobility support accordingly. Further considerations on application management and source address selection are out of the scope of this document.

[AY02]

Mobility management and traffic redirection should only be triggered due to IP mobility reasons, that is when the MN moves from the point of attachment where the IP flow was originally initiated.

Mobility management and traffic redirection may also be triggered due to load balancing. Maybe we should acknowledge such non-mobility related triggers, and state that they are outside the scope of this document.

OLD TEXT:

4. Mobility management and traffic redirection should only be triggered due to IP mobility reasons, that is when the MN moves from the point of attachment where the IP flow was originally initiated.

NEW TEXT:

4. This document considers the use of mobility management and traffic redirection only within the context of IP mobility, that is when the MN moves to a point of attachment different from where the IP flow was originally initiated. Other mobility management and traffic re-direction triggers, due for instance to load balancing techniques, are outside the scope of this document.

[AY03]
Should we described the terms IP session continuity and IP address reachability? This document is solely focusing on the former, we should state that.

Proposed resolution:

This should be reflected in the requirements draft/charter. Current charter does not consider stable address reachability as a strict requirement.

[AY04]
When doing the gap analysis, we better break down the benefits we are seeking and evaluate existing solutions with respect to them (e.g., signaling reduction, use of most direct data-path, etc.). For example, regular use of HMIP helps with the former, but not the latter. But, using RCoA as source address helps with both (but it has other issues -- when MN moves outside the local domain).

Proposed resolution:

Add a new subsection where we provide an overview of the different analyzed existing solution and what benefits they provide (i.e., whether they meet the DMM requirements or not).

Comments from Jouni (2013-07-24):

[JK01]
In Section 4.2. it is stated:

"view using common and standardized protocols. Since WiFi is the most widely deployed wireless access technology nowadays, we take it as"

Do you have some data/reference to backup your claim?

Proposed resolution:

OLD TEXT:

4.2. IP flat wireless network

This section focuses on common IP wireless network architectures and how they can be flattened from an IP mobility and anchoring point of view using common and standardized protocols. Since WiFi is the most widely deployed wireless access technology nowadays, we take it as example in the following. Some representative examples of WiFi deployed architectures are depicted on Figure 1.

NEW TEXT:

4.2. IP flat wireless network

This section focuses on common IP wireless network architectures and how they can be flattened from an IP mobility and anchoring point of view using common and standardized protocols. We take WiFi an exemplary wireless technology, as it is widely known and deployed nowadays. Some representative examples of WiFi deployed architectures are depicted on Figure 1.

[JK02]
In Section 4.2.1. it is stated:

"at different point of attachment. However there is no mechanism
specified to enable an efficient dynamic discovery of available"

I would add a clarification here that there is no such mechanism available within IETF specifications. Other SDOs do have such mechanism(e.g. 3GPP).

Proposed resolution:

OLD TEXT:

agents by a single mobile node. This deployment model could be exploited by a mobile node to meet assumption #4 and use several anchors at the same time, each of them anchoring IP flows initiated at different point of attachment. However there is no mechanism specified to enable an efficient dynamic discovery of available anchors and the selection of the most suitable one.

NEW TEXT:

agents by a single mobile node. This deployment model could be exploited by a mobile node to meet assumption #4 and use several anchors at the same time, each of them anchoring IP flows initiated at different point of attachment. However there is no mechanism specified by the IETF to enable an efficient dynamic discovery of available anchors and the selection of the most suitable one. Note that some of these mechanisms have been defined outside the IETF (e.g., 3GPP).

[JK03]
Furthermore, around the bulleted list for the MIPv6 RO discussion, I would mention that nothing prevents a MN to use its CoA directly when communicating CNs on the same link or anywhere in the internet. Of course there is no mobility in that case but it is a valid scenario to mention IMHO (and also part of our charter). I recon the HMIPv6 text mentions at least the use of RCoA already.

Proposed resolution:

OLD TEXT:

> Notwithstanding these considerations, the RO mode does offer the possibility of substantially reducing traffic through the Home Agent, in cases when it can be supported on the relevant correspondent nodes.

NEW TEXT:

> Notwithstanding these considerations, the RO mode does offer the possibility of substantially reducing traffic through the Home Agent, in cases when it can be supported on the relevant correspondent nodes. Note that a mobile node can also use its CoA directly [RFC5014] when communicating with CNs on the same link or anywhere in the Internet, although no session continuity support would be provided by the IP stack in this case.

[JK04]
In Section 4.2.2. where the text describes RFC6463, I would also reference to RFC6097 since that has quite a bit of text regarding the discovery procedure of the LMA.

Proposed resolution:

OLD TEXT:

An interesting extension that can also be used to facilitate the deployment of network-based mobility protocols in a distributes mobility management environment is the LMA runtime assignment [RFC6463]. This extension specifies a runtime local mobility anchor assignment functionality and corresponding mobility options for Proxy Mobile IPv6. This runtime local mobility anchor assignment takes place during the Proxy Binding Update / Proxy Binding Acknowledgment message exchange between a mobile access gateway and a local mobility anchor. While this mechanism is mainly aimed for load-balancing purposes, it can also be used to select an optimal LMA from the routing point of view. A runtime LMA assignment can be used to change the assigned LMA of an MN, for example in case when the mobile node does not have any session active, or when running sessions can survive an IP address change.

NEW TEXT:

An interesting extension that can also be used to facilitate the deployment of network-based mobility protocols in a distributes mobility management environment is the LMA runtime assignment [RFC6463]. This extension specifies a runtime local mobility anchor assignment functionality and corresponding mobility options for Proxy Mobile IPv6. This runtime local mobility anchor assignment takes place during the Proxy Binding Update / Proxy Binding Acknowledgment message exchange between a mobile access gateway and a local mobility anchor. While this mechanism is mainly aimed for load-balancing purposes, it can also be used to select an optimal LMA from the routing point of view. A runtime LMA assignment can be used to change the assigned LMA of an MN, for example in case when the mobile node does not have any session active, or when running sessions can survive an IP address change. Note that several possible dynamic local mobility anchor discovery solutions can be used, as described in [RFC6097].

[JK05]
While I found Section 4.2. good in general I was somehow expecting to see text regarding MOBIKE (RFC4555). We can safely assume MOBIKE is probably the most deployed client mobility enabling technology out there today.

Proposed Resolution: add text for MOBIKE

There other host-based approaches standardized within the IETF that can be used to provide mobility support. For example MOBIKE [RFC4555] allows a mobile node encrypting traffic through IKEv2 [RFC5996] to change its point of attachment while maintaining a Virtual Private Network (VPN) session. The MOBIKE protocol allows updating the VPN Security Associations (SAs) in cases where the base connection initially used is lost and needs to be re-established. The use of the MOBIKE protocol avoids having to perform an IKEv2 re- negotiation. Similar considerations to those made for Mobile IPv6 can be applied to MOBIKE; though MOBIKE is best suited for situations where the address of at least one endpoint is relatively stable and can be discovered using existing mechanisms such as DNS.

[JK06]
In Section 4.3. it says:

"GPRS Tunnelling Protocol (GTP) [3GPP.29.060] is a network-based mobility protocol specified for 3GPP networks (S2a, S2b, S5 and S8 interfaces)."

While 29.060 is about GTP, for the above referenced interfaces 29.281 and 29.274 are probably more appropriate.

Proposed resolution:

(update references)

OLD TEXT:

> GPRS Tunnelling Protocol (GTP) [3GPP.29.060] is a network-based mobility protocol specified for 3GPP networks (S2a, S2b, S5 and S8 interfaces). Similar to PMIPv6, it can handle mobility without requiring the involvement of the mobile nodes. In this case, the mobile node functionality is provided in a proxy manner by the Serving Data Gateway (SGW), Evolved Packet Data Gateway (ePDG), or Trusted Wireless Access Gateway (TWAG).

NEW TEXT (also update the actual refs):

> GPRS Tunnelling Protocol (GTP) [3GPP.29.060] [3GPP.29.281] [3GPP.29.274] is a network-based mobility protocol specified for 3GPP networks (S2a, S2b, S5 and S8 interfaces). Similar to PMIPv6, it can handle mobility without requiring the involvement of the mobile nodes. In this case, the mobile node functionality is provided in a proxy manner by the Serving Data Gateway (SGW), Evolved Packet Data Gateway (ePDG), or Trusted Wireless Access Gateway (TWAG).

[JK07]

"A Local IP Access (LIPA) and Selected IP Traffic Offload (SIPTO) enabled network [3GPP.23.829] allows offloading some IP services at"

I would say referencing to e.g. 23.401 on LIPA/SIPTO is more Appropriate these days, since the TR23.829 is somewhat left behind and the LIPA/SIPTO functionality is part of the main stage-2 specs already.

Proposed resolution:

(update references)

OLD TEXT:

A Local IP Access (LIPA) and Selected IP Traffic Offload (SIPTO) enabled network [3GPP.23.829] allows offloading some IP services at the local access network, above the Radio Access Network (RAN) or at the macro, without the need to traverse back to the PGW (see Figure 6.

NEW TEXT (also update the actual refs):

A Local IP Access (LIPA) and Selected IP Traffic Offload (SIPTO) enabled network [3GPP.23.401] allows offloading some IP services at the local access network, above the Radio Access Network (RAN) or at the macro, without the need to traverse back to the PGW (see Figure 6.

[JK08]
I found Section 4 in general quite nice. However, I was somehow Expecting to see a bit of text of WiMAX. Or can we safely state that no IPv6 deployments ever took place in WiMAX? Anyway, at least a reference to WiMAX would be nice, since they spent quite a bit of time developing both CMIPv6 and PMIPv6 functionality into their architecture.

Proposed resolution:

Add some short text in Section 4.2 (before 4.2.1, just before the last paragraph "Existing IP mobility protocols can also be deployed...") to mention WiMAX.

NEW TEXT:

Although we have adopted in this section the example of WiFi networks, there are other IP flat wireless network architectures specified, such as WiMAX [REFs], which integrates both host and network-based IP mobility functionality.

[JK09]
In Section 4.3. I would reference to 3GPP TS29.303 and say something about 3GPP's heavy use of DNS as the "gateway location database" and how that is used to discover gateways with both topological and gateway collocation in mind

Proposed resolution

Add text:

> The 3GPP architecture specifications also provide mechanisms to allow discovery and selection of gateways [3GPP.29.303]. These mechanisms enable taking decisions taking into consideration topological location and gateway collocation aspects, using heavily the DNS as a "location database".

[JK10]
In Section 5. it is stated:

"o The dynamic anchor relocation needs to ensure that IP address continuity is guaranteed for sessions that need it at the relocated anchor. This for example implies having the knowledge"

Since our charter _allows_ solutions where mobility is used "when needed"
that fact should be reflected above. Even if there is mobility supported
only locally within a limited area, it might meet the requirements from
the MN or the application point of view i.e. when the MN or the application
does not care about a "full longstanding mobility" to be provided.

Proposed resolution:

OLD TEXT:

- The dynamic anchor relocation needs to ensure that IP address continuity is guaranteed for sessions that need it at the relocated anchor. This for example implies having the knowledge of which sessions are active at the mobile node, which is something typically known only by the MN (namely, by its connection manager). Therefore, (part of) this knowledge might need to be transferred to/shared with the network.

NEW TEXT:

- The dynamic anchor relocation needs to ensure that IP address continuity is guaranteed for sessions that need it and while needed (in some scenarios, the provision of mobility locally within a limited area might be enough from the mobile node or the application point of view) at the relocated anchor. This for example implies having the knowledge of which sessions are active at the mobile node, which is something typically known only by the MN (e.g., by its connection manager). Therefore, (part of) this knowledge might need to be transferred to/shared with the network.

[JK11]

"o Dynamic discovery and selection of anchors. There might be more than one available anchor for a mobile node to use. Currently, there is no efficient mechanism that allows to dynamically discover the presence of nodes that can play the role of anchor, discover their capabilities and allow the selection of the most suitable one."

Within 3GPP TS29.303 makes that possible and is deployed.

Proposed resolution:

OLD TEXT:

- Dynamic discovery and selection of anchors. There might be more than one available anchor for a mobile node to use. Currently, there is no efficient mechanism that allows to dynamically discover the presence of nodes that can play the role of anchor, discover their capabilities and allow the selection of the most suitable one.

NEW TEXT:

- Dynamic discovery and selection of anchors. There might be more than one available anchor for a mobile node to use. Currently, there is no efficient mechanism specified by the IETF that allows to dynamically discover the presence of nodes that can play the role of anchor, discover their capabilities and allow the selection of the most suitable one. Note that there are 3GPP mechanisms providing this functionality defined in [3GPP.23.303].

Comments from Georgios Karagiannis (2013-08-01):
==========

[GK01]
The current version of the draft is not using the requirements defined in the requirements draft to identify
the gaps on existing mobility protocols.

In my opinion it is important to use these requirements in order to identify the gaps.

Proposed resolution:

Refer to the requirements in the new subsection that includes the summary table
(to be added to address [AY04]).

Comments from Alex Petrescu (2013-08-01):
==========

[AP01]
1. The Route Optimization feature of Mobile IPv6 does not support
mobile network prefixes - it only works for a full /128 Home Address. There is a security problem in extending the RR tests for
prefixes. But if done, it will allow direct communications from an
LFN in the moving network to an arbitrary Correspondent Node in the
Internet.

Proposed resolution:

OLD TEXT:

- The RO mode is only supported by Mobile IPv6. There is no route optimization support standardized for the NEMO protocol, although many different solutions have been proposed.

NEW TEXT:

- The RO mode is only supported by Mobile IPv6. There is no route optimization support standardized for the NEMO protocol because of the security problems posed by extending return routability tests for prefixes, although many different solutions have been proposed.

[AP02]

2. Anchoring a Mobile Node's Home Address at multiple points may be a very good goal, but one wonders whether it could be achieved within useful limits. An IP address is typically valid at a single point in the Internet. Anchoring it at more places involves the use of route updates or of tunnelling. It is a question whether this could be achieved within measurable and advantageous limits, compared to changing the IP address, or prefer still anchor at remote HA.

Proposed resolution:

The decision on whether anchoring at
multiple points vs anchoring at a remote HA
is solution space specific. Nothing prevents
a solution to perform this decision on a per-application
basis.

[AP03]

3. Simultaneous use of multiple interfaces at a same mobile router is something that is not supported by Mobile IPv6 today (although it does support multiple Care-of Addresses). If done, it allows bandwidth augmentation (i.e. add 10 cellular interfaces to a Mobile Router deployed in a bus, and thus multiply the bandwidth by ten) for all kinds of applications.

Proposed resolution:

May not be in scope for the gap analysis.

The New Section 5

- http://tools.ietf.org/html/draft-ietf-dmm-best-practices-gap-analysis-02#section-5

- Analysis based on each requirement

Gap Summary 1/2

- Anchor Selection
  - Existing solutions only provide an optimal initial anchor assignment, a gap being the lack of dynamic anchor change/new anchor assignment. Neither the HA switch nor the LMA runtime assignment allow changing the anchor during an ongoing session.
  - While existing network-based DMM practices may allow to deploy multiple LMAs and dynamically select the best one, this requires to still keep some centralization in the control plane, to access on the policy store (as defined in RFC5213).

Gap Summary 2/2

- Anchor Selection
  - Currently, there is no efficient mechanism specified by the IETF that allows to dynamically discover the presence of nodes that can play the role of anchor, discover their capabilities and allow the selection of the most suitable one.

- Address selection/management for MN
  - The mobile node needs to simultaneously use multiple IP addresses, which requires additional support which might not be available on the mobile node's stack, especially for the case of network-based solutions.

Next Steps

- Will generate a new version correcting some editorial issues
  - Clarification of Summary Table
  - Update references
- Other comments?