DMM
Internet-Draft
Intended status: Informational
Expires: October 16, 2015

H. Chan
Huawei Technologies
J. Lee
Sangmyung University
S. Jeon
Instituto de Telecomunicacoes

April 14, 2015

Distributed Mobility Anchoring
draft-chan-dmm-distributed-mobility-anchoring-02

Abstract

This document defines the mobility management protocol solutions in the context of a distributed mobility management deployment. Such solutions consider the problem of assigning a mobility anchor and a gateway at the initiation of a flow. In addition, the mid-session switching of the mobility anchor in a distributed mobility management environment is considered.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

A key requirement in distributed mobility management [RFC7333] is to enable traffic to avoid traversing single mobility anchor far from the optimal route. Recent developments in research and standardization with respect to future deployment models call for far more flexibility in network function operation and management. For example, the work on service function chaining at the IETF (SFC WG) has already identified a number of use cases for data centers. Although the work in SFC is not primarily concerned with mobile networks, the impact on IP-based mobile networks is not hard to see as by now most hosts connected to the Internet do so over a wireless medium. For instance, as a result of a dynamic re-organization of service chain a non-optimal route between mobile nodes may arise if one relies solely on centralized mobility management. This may also occur when the mobile node has moved such that both the mobile node and the correspondent node are far from the mobility anchor via which the traffic is routed.

Recall that distributed mobility management solutions do not make use of centrally deployed mobility anchor. As such, a flow SHOULD be able to have its traffic changing from traversing one mobility anchor to traversing another mobility anchor as the mobile node moves, or when changing operation and management (OAM) requirements call for mobility anchor switching, thus avoiding non-optimal routes. This draft proposes distributed mobility anchoring solutions.

2. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL","SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

All general mobility-related terms and their acronyms used in this document are to be interpreted as defined in the Mobile IPv6 base specification [RFC6275], the Proxy Mobile IPv6 specification [RFC5213], and the DMM current practices and gap analysis [RFC7429]. This includes terms such as mobile node (MN), correspondent node (CN), home agent (HA), home address (HoA), care-of-address (CoA), local mobility anchor (LMA), and mobile access gateway (MAG).

In addition, this document uses the following term:

Home network of an application session (or of an HoA): the network that has allocated the IP address (HoA) used for the session identifier by the application running in an MN. An MN may be running multiple application sessions, and each of these sessions can have a different home network.

Anchoring Function (AF): allocation to a mobile node of an IP address, i.e., Home Address (HoA), or prefix, i.e., Home Network Prefix (HNP) topologically anchored by the advertising node. That is, the anchor node is able to advertise a connected route into the routing infrastructure for the allocated IP prefixes. This is a basic function of a mobility anchor. With separation of control plane and data plane, this function may reside in a control plane anchor. Then the anchor function performs the IP prefix or address allocation and the route advertisement for an IP anchor in the data plane.

Internetwork Location Management (LM) function: managing and keeping track of the internetwork location of an MN. The location information may be a binding of the IP advertised address/prefix, e.g., HoA or HNP, to the IP routing address of the MN or of a node that can forward packets destined to the MN. It is a control plane function.

In a client-server protocol model, location query and update messages may be exchanged between a Location Management client (LMc) and a Location Management server (LMs). With separation of control plane and data plane, this function may reside in a control plane anchor.

Forwarding Management (FM) function: packet interception and forwarding to/from the IP address/prefix assigned to the MN, based on the internetwork location information, either to the destination or to some other network element that knows how to forward the packets to their destination.

This function may be used to achieve indirection. With separation of control plane and data plane, FM may split into a FM function in the control plane (FM-CP), which may be a function in a control plane anchor or mobility controller, and a FM function in the data plane (FM-DP), which may be the function of a data plane anchor.

Security Management (SM) function: The security management function controls security mechanisms/protocols providing access control, integrity, authentication, authorization, confidentiality, etc. for the control plane and data plane.

This function resides in all nodes such as control plane anchor, data plane anchor, and mobile node.

3. Anchor Initiation and Switching

3.1. Anchoring function in network of attachment

The anchoring function of the IP address at MN’s side of a flow may be at the access router to which the MN is attached.

For example, when an MN attaches to a network (Net1) or moves to a new network (Net2), it is allocated an IP prefix from that network. It configures from this prefix an IP address which is typically a dynamic IP address. It then uses this IP address when it starts a new flow. Packets to the MN in this flow are simply forwarded according to the forwarding table.

In this example, the flow may have terminated before the MN moves to a new network. Otherwise, the flow may close and then restart using a new IP address configured in the new network.

The security management function in the IP anchoring node at a new network must assign a valid IP prefix to a mobile node. In the example, the security management function in the node anchoring address IP2 assigns the valid IP prefix for the mobile node.

```
 Net1                                                  Net2
 +--------------+                                      +--------------+
 |AR1:          |                                      |AR2:          |
 |RA(IP1)       |                                      |RA(IP2)       |
 +--------------+                                      +--------------+
 +--------------+                                      +--------------+
 |MN(IP1):      |                 or                   |MN(IP2):      |
 |flow(IP1,...) |                                      |flow(IP2,...) |
 +--------------+                                      +--------------+
```

Figure 1. Anchoring function in network of attachment. MN is attached to AR1 in Net1 where it has initiated a flow using IP1 or has moved to AR2 in Net2 where it initiates a new flow using IP2.

3.2. Anchoring Function not in network of attachment

The anchoring function of the IP address at MN’s side of a flow may not be at the access router to which the MN is attached.

An example when an MN moves to a new network is as follows. The MN has an ongoing session which was initialized in a prior network (Net1) of attachment using an IP address belonging to the network where it was initialized as described in Section 3.1. When the flow is unable to change its IP address it may continue to use its original IP address so that the anchoring function of the IP address is not in the current network of attachment but in the network where the original IP address belongs. Mobility support is needed to enable the flow to use this original IP address.

The security management function in the anchoring node at a new network must assign a valid IP prefix to a mobile node. The security management function must allow the mobile node to receive or send data packets with an IP address configured at a prior network of attachment of the mobile node. Note that nowadays access networks deploy ingress filtering so that the mobile node may not receive or send data packets with the previously configured IP address without the security management function's interaction with ingress filtering.

```
Net1                                                    Net2
+--------------+                                        +--------------+
|AR1:          |                                        |AR2:          |
|RA(IP1)       |                                        |RA(IP2)       |
+--------------+                                        +--------------+
                                                        +--------------+
                                                        |MN(IP2):      |
                                                        |flow(IP1,...) |
                                                        +--------------+
```

Figure 2. Anchoring function not in network of attachment. MN attached to AR2 in Net2 has a flow(IP1,...) using IP1, which belongs to Net1.

3.3. Keeping an IP address

After the MN moves with an ongoing session to the new network (Net2), it obtains a new IP address or prefix from the new network. However, the ongoing session which was initialized in a prior network of attachment is using an IP address belonging to the network where it was initialized as described in Section 3.1. IP mobility is needed to use the original IP address for session continuity.

```
Net1                                                   Net2
+--------------+                                       +--------------+
|AR1:          |                                       |AR2:          |
|RA(IP1)       |                                       |RA(IP2)       |
+--------------+                                       +--------------+
+..............+                                       +--------------+
.MN(IP1):      .                move                   |MN(IP1,IP2):  |
.flow(IP1,...) .              =======>                 |flow(IP1,...) |
+..............+                                       +--------------+
```

Figure 3. Keeping an IP address. MN with ongoing flow using IP1 in Net1 has moved to Net2 and the flow needs to continue using IP1 to preserve session continuity.

The use of IP address belonging to the network of attachment whenever a new flow is initiated as described in Section 3.1 and to keep the IP address as the MN moves to a new network are described in [I-D.seite-dmm-dma].

3.4. Changing the IP address

With the MN in the example in Section 3.1 it may be desirable to change to a flow using the new IP address configured in the new network. The packets of this flow may then follow the forwarding table without requiring IP layer mobility support. Yet such a change in flow may be using a higher layer mobility support which is not in the scope of this document to change the IP address of the flow.

The security management function in the IP anchoring node at a new network must assign a valid IP prefix to a mobile node.

```
Net1                                                   Net2
+--------------+                                       +--------------+
|AR1:          |                                       |AR2:          |
|RA(IP1)       |                                       |RA(IP2)       |
+--------------+                                       +--------------+
+..............+                                       +--------------+
.MN(IP1):      .                move                   |MN(IP2):      |
.flow(IP1,...) .              =======>                 |flow(IP2,...) |
+..............+                                       +--------------+
```

Figure 4. Changing the IP address. MN running a flow using IP1 in Net1 changes to running a flow using IP2 in Net2.

3.5. Moving the IP address

The anchoring function may move without changing the IP address of the flow.

```
Net1                                                    Net2
+..............+                                        +--------------+
.              .                  move                  |AR2:          |
.RA(IP1)       .                =======>                |RA(IP2,IP1)   |
+..............+                                        +--------------+
+..............+                                        +--------------+
.MN(IP1):      .                  move                  |MN(IP2,IP1):  |
.flow(IP1,...) .                =======>                |flow(IP1,...) |
+..............+                                        +--------------+
```

Figure 5. Moving the IP address. MN with flow using IP1 in Net1 continues to run the flow using IP1 as it moves to Net2.

As an MN with an ongoing session moves to a new network, the flow may preserve session continuity by moving the original IP address to the new network. An example is in the use of BGP UPDATE messages to change the forwarding table entries as described in [I-D.mccann-dmm-flatarch] and also for 3GPP Evolved Packet Core (EPC) network in [I-D.matsushima-stateless-uplane-vepc]. Another example is in the case where Net1 and Net2 both belong to the same operator network with separation of control and data planes ([I-D.liu-dmm-deployment-scenario] and [I-D.matsushima-stateless-uplane-vepc]), where the controller may send to the switches/routers the updated information of the forwarding tables with the anchoring function of the original IP prefix/address at AR1 moved to AR2 in the new network. Then the anchoring function which was advertising the prefix in the original network will need to move to the new network. As the anchoring function in the new network advertises the prefix of the original IP address in the new network, the forwarding tables will be updated so that packets of the flow will be forwarded according to the updated forwarding tables.

The security management function must allow that the anchoring function in the new network configures the original IP prefix/address used by the mobile node at the previous (original) network. As the configured original IP prefix/address is to be used in the new network, the security management function must allow the anchoring function to advertise the prefix of the original IP address and also allow the mobile node to send and receive data packets with the original IP address.

3.6. Indirection of a flow

As an MN with an ongoing session moves to a new network, the flow may use the original IP address for session continuity by using indirection. Here the location management information may be kept as a binding of the original IP address to a new forwarding address, whereas the Forwarding management function may then use this binding to forward the flow.

In Figure 6, the location management information kept in the original network is the binding of the original IP address to an IP address in the new network.

```
                             Net3
                             +--------------+
                             |AR3:          |
                            /|RA(IPcn)      |
                           / +--------------+
  Net1                    /  +--------------+           Net2
  +--------------+       /   |CN(IPcn): flow|           +--------------+
  |flow(IP1,...) |      /    |(IPcn,IP1,...)|           |flow(IP1,...) |
  |--> AR2       |     /     +--------------+           |-->MN         |
  |              |    /                                 |              |
  |IP1<->IPar2   |   /                                  |              |
  |--------------|  /                                   |--------------|
  |AR1:          |<-                                    |AR2(IPar2):   |
  |RA(IP1)       | ------------------------------------>|RA(IP2)       |
  +--------------+                                      +--------------+
  +..............+                                      +--------------+
  .MN(IP1):      .                 move                 |MN(IP1,IP2):  |
  .flow(IP1,...) .               =======>               |flow(IP1,...) |
  +..............+                                      +--------------+
```

Figure 6. Indirection of a flow. After MN has moved from Net1 to Net2, Location Information function in Net1 keeps a binding of IP1 to IP of AR2, and Routing Management function in Net1 forwards the packets of the flow(IP1,...) to Net2.

The packets of the flow(IP1, IPcn, ...) from the CN to the MN will first be forwarded to AR1 in the original network. Here, using the binding of IP1 to an IP address in the new network, the forwarding management function may forward these packets to the new network such as by encapsulating them with a header destined to the new network.

In a host-based mobility management solution such as [I-D.bernardos-dmm-cmip] the address in the new network may be the MN itself.

In a network-based mobility management solution such as [I-D.bernardos-dmm-pmip], [I-D.sarikaya-dmm-for-wifi], and [Paper-Distributed.Mobility.PMIP], the address in the new network may be an access router to which the MN is attached in the new network. The access router may then forward the packet to the MN at L2, which may use Software-Defined Networking as described in [I-D.sarikaya-dmm-for-wifi].

In general, indirection is invoked only when needed. The flow can use the IP address belonging to the network of attachment where the flow is initialized as described in [I-D.seite-dmm-dma].

The security management function in the IP anchoring node must ensure that the forwarding management function establishes a secure session anchoring with a relevant node. The security management function in the end communication nodes (i.e., mobile node and correspondent node) may be used to ensure a secure data plane between them. For both cases (i.e., establishments of secure session anchoring and secure data plane), existing security protocols such as IKE, IPsec, TLS may be invoked by the security management function.

3.7. Changing indirection of a flow

Forwarding the packets of an ongoing session from CN’s network via the original network to MN’s new network is not necessarily optimal. The route can be more direct by forwarding these packets directly from CN’s network to MN’s new network.

Here, the location information in the original network may be copied to CN’s network. The packets of the flow(IP1, IPcn, ...) from the CN to the MN are first intercepted at the access router of CN. Then using the binding of IP1 to an IP address in the new network, the forwarding management function in CN’s network may forward these packets directly to the new network ([Paper-Distributed.Mobility.PMIP]) such as by encapsulating them with a header destined to the new network.

To change the indirection of a flow, the relevant context with regard to MN should be delivered from AR1 in Net1 to AR3 (CN’s anchor) in Net3 (CN’s network), while AR2 should be notified of the change of indirection to receive packets directly forwarded by AR3. Existing IP mobility signaling messages such as Proxy Binding Update (PBU) and Proxy Binding Acknowledgment (PBA) can be used for the both communications with as little option extensions as possible. When a packet from the CN has reached AR3, AR3 encapsulates the packet with a tunnel header specified with IP address of CN’s anchor as outer source IP and AR2’s IP address as outer destination IP. For transparent packet delivery operation in the perspective od AR2, CN’s anchor needs to forward packets encapsulated with a tunnel header specified with AR1’s IP address as outer source IP and AR2’s IP address as outer destination IP.

The security management function in the IP anchoring node must ensure that the forwarding management function re-establishes a secure session anchoring with a relevant node during mid-session. The security management function in the end communication nodes may be used to ensure a secure data plane between them during mid-session. For both cases (i.e., re-establishments of secure session anchoring and secure data plane), existing security protocols such as IKE, IPsec, TLS may be invoked by the security management function.

```
                             Net3
                             +--------------+
                             |flow(IP1,...) |
                             |--> AR2       |
                         y..>|              |
                        p.   |IP1<->IPar2   |
                       o.    |--------------|
                      c.     |AR3:          |
                      .      |RA(IPcn)      |\
                     .       +--------------+ \
  Net1              .        +--------------+  \        Net2
  +--------------+           |CN(IPcn): flow|   \       +--------------+
  |flow(IP1,...) |           |(IPcn,IP1,...)|    \      |flow(IP1,...) |
  |--> AR2       |           +--------------+     \     |-->MN         |
  |              |                                 \    |              |
  |IP1<->IPar2   |                                  \   |              |
  |--------------|                                   \  |--------------|
  |AR1:          |                                    ->|AR2(IPar2):   |
  |RA(IP1)       |                                      |RA(IP2)       |
  +--------------+                                      +--------------+
  +..............+                                      +--------------+
  .MN(IP1):      .                 move                 |MN(IP1,IP2):  |
  .flow(IP1,...) .               =======>               |flow(IP1,...) |
  +..............+                                      +--------------+
```

Figure 7. Changing indirection of a flow. Location Information function and Routing Management function in Net2 are copied to Net3, so that the Location Information function in Net3 keeps a binding of IP1 to IP of AR2, and the Routing Management function in Net3 forwards the packets of the flow(IP1,...) to Net2.

4. Security Considerations

TBD

5. IANA Considerations

This document presents no IANA considerations.

6. Contributors

This document is an attempt to harmonize the different distributed mobility solutions in a number of other drafts. These drafts cited in this document are the work of their many authors/co-authors. While some of them have taken the work to jointly write this document, others have contributed at least indirectly by writing these drafts. The latter include Carlos J. Bernardos, Philippe Bertin, Hui Deng, Fabio Giust, Dapeng Liu, Satoru Matushima, Peter McCann, Antonio de la Oliva, Behcet Sarikaya, Pierrick Seite, Li Xue, and Ryuji Wakikawa.

7. References

7.1. Normative References

[I-D.bernardos-dmm-cmip]
Bernardos, C., Oliva, A., and F. Giust, "An IPv6 Distributed Client Mobility Management approach using existing mechanisms", draft-bernardos-dmm-cmip-03 (work in progress), March 2015.

[I-D.bernardos-dmm-pmip]
Bernardos, C., Oliva, A., and F. Giust, "A PMIPv6-based solution for Distributed Mobility Management", draft-bernardos-dmm-pmip-04 (work in progress), March 2015.

[I-D.liu-dmm-deployment-scenario]
Liu, V., Chan, A., and H. Deng, "Distributed mobility management deployment scenario and architecture", draft-liu-dmm-deployment-scenario-03 (work in progress), March 2015.

[I-D.matsushima-stateless-uplane-vepc]
Matsushima, S. and R. Wakikawa, "Stateless user-plane architecture for virtualized EPC (vEPC)",

draft-matsushima-stateless-uplane-vepc-04 (work in progress), March 2015.

[I-D.mccann-dmm-flatarch]
McCann, P., "Authentication and Mobility Management in a Flat Architecture", draft-mccann-dmm-flatarch-00 (work in progress), March 2012.

[I-D.sarikaya-dmm-for-wifi]
Sarikaya, B. and L. Xue, "Distributed Mobility Management Protocol for WiFi Users in Fixed Network", draft-sarikaya-dmm-for-wifi-01 (work in progress), October 2014.

[I-D.seite-dmm-dma]
Seite, P., Bertin, P., and J. Lee, "Distributed Mobility Anchoring", draft-seite-dmm-dma-07 (work in progress), February 2014.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC6241] Enns, R., Bjorklund, M., Schoenwaelder, J., and A. Bierman, "Network Configuration Protocol (NETCONF)", RFC 6241, June 2011.

[RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

[RFC7333] Chan, H., Liu, D., Seite, P., Yokota, H., and J. Korhonen, "Requirements for Distributed Mobility Management", RFC 7333, August 2014.

[RFC7429] Liu, D., Zuniga, JC., Seite, P., Chan, H., and CJ. Bernardos, "Distributed Mobility Management: Current Practices and Gap Analysis", RFC 7429, January 2015.

7.2. Informative References

[Paper-Distributed.Mobility.PMIP]
Chan, H., "Proxy Mobile IP with Distributed Mobility Anchors", Proceedings of GlobeCom Workshop on Seamless Wireless Mobility, December 2010.

[Paper-Distributed.Mobility.Review]

Chan, H., Yokota, H., Xie, J., Seite, P., and D. Liu, "Distributed and Dynamic Mobility Management in Mobile Internet: Current Approaches and Issues", February 2011.

Authors' Addresses

H Anthony Chan
Huawei Technologies
5340 Legacy Dr. Building 3
Plano, TX 75024
USA

Email: h.a.chan@ieee.org

Jong-Hyouk Lee
Sangmyung University
708 Hannuri Building
Cheonan 330-720
Korea

Email: jonghyouk@smu.ac.kr

Seil Jeon
Instituto de Telecomunicacoes
Campus Universitario de Santiago
Aveiro 3810-193
Portugal

Email: seiljeon@av.it.pt