Internet Engineering Task Force (IETF)
Request for Comments: 8818
Category: Informational
ISSN: 2070-1721

H. Chan, Ed.
CIHE
X. Wei
Huawei Technologies
J. Lee
Sejong University
S. Jeon
Sungkyunkwan University
CJ. Bernardos, Ed.
UC3M

October 2020

Distributed Mobility Anchoring

Abstract

This document defines distributed mobility anchoring in terms of the different configurations and functions to provide IP mobility support. A network may be configured with distributed mobility anchoring functions for both network-based or host-based mobility support, depending on the network's needs. In a distributed mobility anchoring environment, multiple anchors are available for mid-session switching of an IP prefix anchor. To start a new flow or to handle a flow not requiring IP session continuity as a mobile node moves to a new network, the flow can be started or restarted using an IP address configured from the new IP prefix anchored to the new network. If the flow needs to survive the change of network, there are solutions that can be used to enable IP address mobility. This document describes different anchoring approaches, depending on the IP mobility needs, and how this IP address mobility is handled by the network.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8818.

Table of Contents

1. Introduction

A key requirement in distributed mobility management (DMM) [RFC7333] is to enable traffic to avoid traversing a single mobility anchor far from an optimal route. This document defines different configurations, functional operations, and parameters for distributed mobility anchoring and explains how to use them to avoid unnecessarily long routes when a mobile node moves.

Other distributed mobility management documents already address source address selection [RFC8653] and control-plane and data-plane signaling [FPC-DMM-PROTOCOL]. A number of distributed mobility solutions have also been proposed, for example, in [DMM-DMA], [RFC8885], [DMM-WIFI], [DMM-ENHANCED-ANCHORING], and [STATELESS-UPLANE-VEPC].

Distributed mobility anchoring employs multiple anchors in the data plane. In general, control-plane functions may be separated from data-plane functions and be centralized but may also be co-located with the data-plane functions at the distributed anchors. Different configurations of distributed mobility anchoring are described in Section 3.1.

As a Mobile Node (MN) attaches to an access router and establishes a link between them, a /64 IPv6 prefix anchored to the router may be assigned to the link for exclusive use by the MN [RFC6459]. The MN

may then configure a global IPv6 address from this prefix and use it as the source IP address in a flow to communicate with its Correspondent Node (CN). When there are multiple mobility anchors assigned to the same MN, an address selection for a given flow is first required before the flow is initiated. Using an anchor in an MN's network of attachment has the advantage that the packets can simply be forwarded according to the forwarding table. However, after the flow has been initiated, the MN may later move to another network that assigns a new mobility anchor to the MN. Since the new anchor is located in a different network, the MN's assigned prefix does not belong to the network where the MN is currently attached.

When the MN wants to continue using its assigned prefix to complete ongoing data sessions after it has moved to a new network, the network needs to provide support for the MN's IP address and session continuity, since routing packets to the MN through the new network deviates from applying default routes. The IP session continuity needs of a flow (application) determine how the IP address used by this flow has to be anchored. If the ongoing IP flow can cope with an IP prefix/address change, the flow can be reinitiated with a new IP address anchored in the new network. On the other hand, if the ongoing IP flow cannot cope with such change, mobility support is needed. A network supporting a mix of flows both requiring and not requiring IP mobility support will need to distinguish these flows.

2. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

All general mobility-related terms and their acronyms used in this document are to be interpreted as defined in the Mobile IPv6 (MIPv6) base specification [RFC6275], the Proxy Mobile IPv6 (PMIPv6) specification [RFC5213], the Mobility Terminology document [RFC3753], and the DMM Current Practices and Gap Analysis document [RFC7429]. These include 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 terms and definitions:

IP session continuity: The ability to maintain an ongoing transport interaction by keeping the same local endpoint IP address throughout the lifetime of the IP socket despite the mobile host changing its point of attachment within the IP network topology. The IP address of the host may change after closing the IP socket and before opening a new one, but that does not jeopardize the ability of applications using these IP sockets to work flawlessly. Session continuity is essential for mobile hosts to maintain ongoing flows without any interruption [RFC8653].

Higher-layer session continuity: The ability to maintain an ongoing transport- or higher-layer (e.g., application) interaction by

keeping the session identifiers throughout the lifetime of the session despite the mobile host changing its point of attachment within the IP network topology. This can be achieved by using mechanisms at the transport or higher layers.

IP address reachability: The ability to maintain the same IP address for an extended period of time. The IP address stays the same across independent sessions, even in the absence of any session. The IP address may be published in a long-term registry (e.g., DNS) and is made available for serving incoming (e.g., TCP) connections. IP address reachability is essential for mobile hosts to use specific/published IP addresses [RFC8653].

IP mobility: The combination of IP address reachability and session continuity.

Anchoring (of an IP prefix/address): An IP prefix (i.e., Home Network Prefix (HNP)) or address (i.e., HoA) assigned for use by an MN is topologically anchored to an anchor node when the anchor node is able to advertise a route into the routing infrastructure for the assigned IP prefix. The traffic using the assigned IP address/prefix must traverse the anchor node. We can refer to the function performed by the IP anchor node as anchoring, which is a data-plane function.

Location Management (LM) function: A control-plane function that keeps and manages the network location information of an MN. The location information may be a binding of the advertised IP 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.

When the MN is a Mobile Router (MR), the location information will also include the Mobile Network Prefix (MNP), which is the aggregate IP prefix delegated to the MR to assign IP prefixes for use by the Mobile Network Nodes (MNNs) in the mobile network.

In a client-server protocol model, secure (i.e., authenticated and authorized) location query and update messages may be exchanged between a Location Management client (LMc) and a Location Management server (LMs), where the location information can be updated or queried from the LMc. Optionally, there may be a Location Management proxy (LMp) between LMc and LMs.

With separation of control plane and data plane, the LM function is in the control plane. It may be a logical function at the control-plane node, control-plane anchor, or mobility controller.

It may be distributed or centralized.

Forwarding Management (FM) function: Packet interception and forwarding to/from the IP address/prefix assigned for use by 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 traffic indirection. With

separation of control plane and data plane, the FM function may split into an FM function in the data plane (FM-DP) and an FM function in the control plane (FM-CP).

FM-DP may be distributed with distributed mobility management. It may be a function in a data-plane anchor or data-plane node.

FM-CP may be distributed or centralized. It may be a function in a control-plane node, control-plane anchor, or mobility controller.

Home Control-Plane Anchor (Home-CPA or H-CPA): The Home-CPA function hosts the MN's mobility session. There can be more than one mobility session for a mobile node, and those sessions may be anchored on the same or different Home-CPA's. The Home-CPA will interface with the Home-DPA for managing the forwarding state.

Home Data-Plane Anchor (Home-DPA or H-DPA): The Home-DPA is the topological anchor for the MN's IP address/prefix(es). The Home-DPA is chosen by the Home-CPA on a session basis. The Home-DPA is in the forwarding path for all the mobile node's IP traffic.

Access Control-Plane Node (Access-CPN or A-CPN): The Access-CPN is responsible for interfacing with the mobile node's Home-CPA and with the Access-DPN. The Access-CPN has a protocol interface to the Home-CPA.

Access Data-Plane Node (Access-DPN or A-DPN): The Access-DPN function is hosted on the first-hop router where the mobile node is attached. This function is not hosted on a Layer 2 bridging device such as an eNode(B) or Access Point.

3. Distributed Mobility Anchoring

3.1. Configurations for Different Networks

We next describe some configurations with multiple distributed anchors. To cover the widest possible spectrum of scenarios, we consider architectures in which the control and data planes are separated. We analyze where LM and FM functions, which are specific sub-functions involved in mobility management, can be placed when looking at the different scenarios with distributed anchors.

3.1.1. Network-Based DMM

Figure 1 shows a general scenario for network-based distributed mobility management.

The main characteristics of a network-based DMM solution are:

* There are multiple data-plane anchors, each with an FM-DP function.

* The control plane may either be distributed (not shown in the figure) or centralized (as shown in the figure).

* The Control-Plane Anchor (CPA) and the Data Plane Anchor (DPA) may or may not be co-located. If the CPA is co-located with the distributed DPAs, then there are multiple co-located CPA-DPA instances (not shown in the figure).

* An IP prefix/address IP1 (anchored to the DPA with IP address IPa1) is assigned for use to an MN. The MN uses this IP1 address to communicate with CNs (not shown in the figure).

* The location management (LM) function may be co-located or split (as shown in the figure) into a separate server (LMs) and a client (LMc). In this case, the LMs may be centralized whereas the LMc may be distributed or centralized.

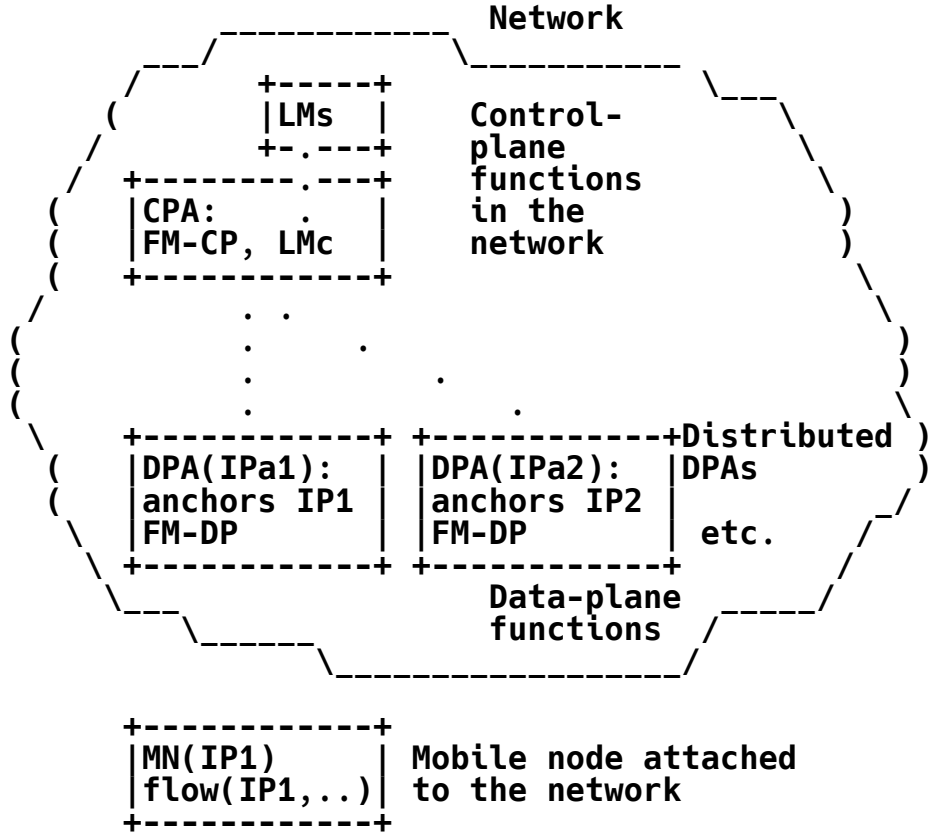
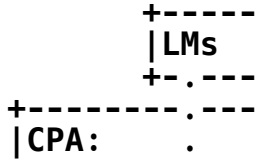


Figure 1: Network-Based DMM Configuration

3.1.2. Client-Based DMM

Figure 2 shows a general scenario for client-based distributed mobility management. In this configuration, the mobile node performs Control-Plane Node (CPN) and Data-Plane Node (DPN) mobility functions, namely the forwarding management and location management (client) roles.



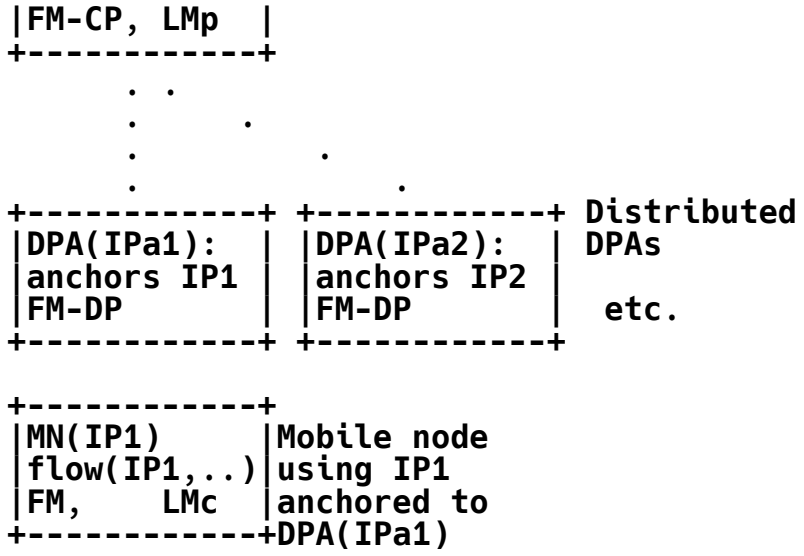


Figure 2: Client-Based DMM Configuration

4. IP Mobility Handling in Distributed Anchoring Environments: Mobility Support Only When Needed

IP mobility support may be provided only when needed instead of being provided by default. Three cases can be considered:

* Nomadic case: No address continuity is required. The IP address used by the MN changes after a movement and traffic using the old address is disrupted. If session continuity is required, then it needs to be provided by a solution running at Layer 4 or above.

* Mobility case with traffic redirection: Address continuity is required. When the MN moves, the previous anchor still anchors the traffic using the old IP address and forwards it to the new MN's location. The MN obtains a new IP address anchored to the new location and preferably uses it for new communications established while connected at the new location.

* Mobility case with anchor relocation: Address continuity is required. In this case, the route followed by the traffic is optimized by using some means for traffic indirection to deviate from default routes.

A straightforward choice of mobility anchoring is the following: the MN chooses, as a source IP address for packets belonging to an IP flow, an address allocated by the network the MN is attached to when the flow was initiated. As such, traffic belonging to this flow traverses the MN's mobility anchor [DMM-DMA] [RFC8885].

The IP prefix/address at the MN's side of a flow may be anchored to the Access Router (AR) to which the MN is attached. For example, when an MN attaches to a network (Net1) or moves to a new network (Net2), an IP prefix from the attached network is assigned to the MN's interface. In addition to configuring new link-local addresses, the MN configures from this prefix an IP address that is typically a dynamic IP address (meaning that this address is only used while the

MN is attached to this access router, so the IP address configured by the MN dynamically changes when attaching to a different access network). It then uses this IP address when a flow is initiated. Packets from this flow addressed to the MN are simply forwarded according to the forwarding table.

There may be multiple IP prefixes/addresses that an MN can select when initiating a flow. They may be from the same access network or different access networks. The network may advertise these prefixes with cost options [PREFIX-COST] so that the mobile node may choose the one with the least cost. In addition, the IP prefixes/addresses provided by the network may be of different types regarding whether mobility support is supported [RFC8653]. An MN will need to choose which IP prefix/address to use for each flow according to whether or not it needs IP mobility support, for example, using the mechanisms described in [RFC8653].

4.1. Nomadic Case

When IP mobility support is not needed for a flow, the LM and FM functions are not utilized so that the configurations in Section 3.1 are simplified as shown in Figure 3.

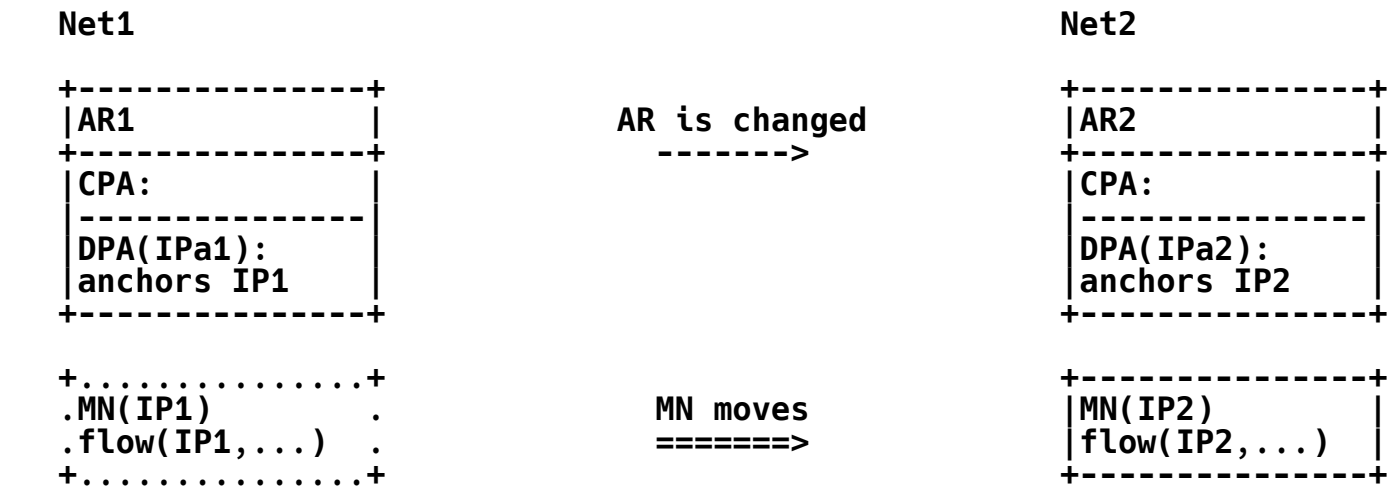


Figure 3: Changing to a New IP Address/Prefix

When there is no need to provide IP mobility to a flow, the flow may use a new IP address acquired from a new network as the MN moves to the new network.

Regardless of whether or not IP mobility is needed, if the flow has not terminated before the MN moves to a new network, the flow may subsequently restart using the new IP address assigned from the new network.

When IP session continuity is needed, even if an application flow is ongoing as the MN moves, it may still be desirable for the application flow to change to using the new IP prefix configured in the new network. The application flow may then be closed at the IP level and then be restarted using a new IP address configured in the new network. Such a change in the IP address used by the application

flow may be enabled using a higher-layer mobility support that is not in the scope of this document.

In Figure 3, a flow initiated while the MN was using the IP prefix IP1, anchored to a previous access router AR1 in network Net1, has terminated before the MN moves to a new network Net2. After moving to Net2, the MN uses the new IP prefix IP2, anchored to a new access router AR2 in network Net2, to start a new flow. Packets may then be forwarded without requiring IP-layer mobility support.

An example call flow is outlined in Figure 4. An MN attaches to AR1, which sends a router advertisement (RA) including information about the prefix assigned to the MN, from which the MN configures an IP address (IP1). This address is used for new communications, for example, with a correspondent node (CN). If the MN moves to a new network and attaches to AR2, the process is repeated (the MN obtains a new IP address, IP2, from AR2). Since the IP address (IP1) configured at the previously visited network is not valid at the current attachment point, any existing flows have to be reestablished using IP2.

Note that in these scenarios, if there is no mobility support provided by Layer 4 or above, application traffic would stop.

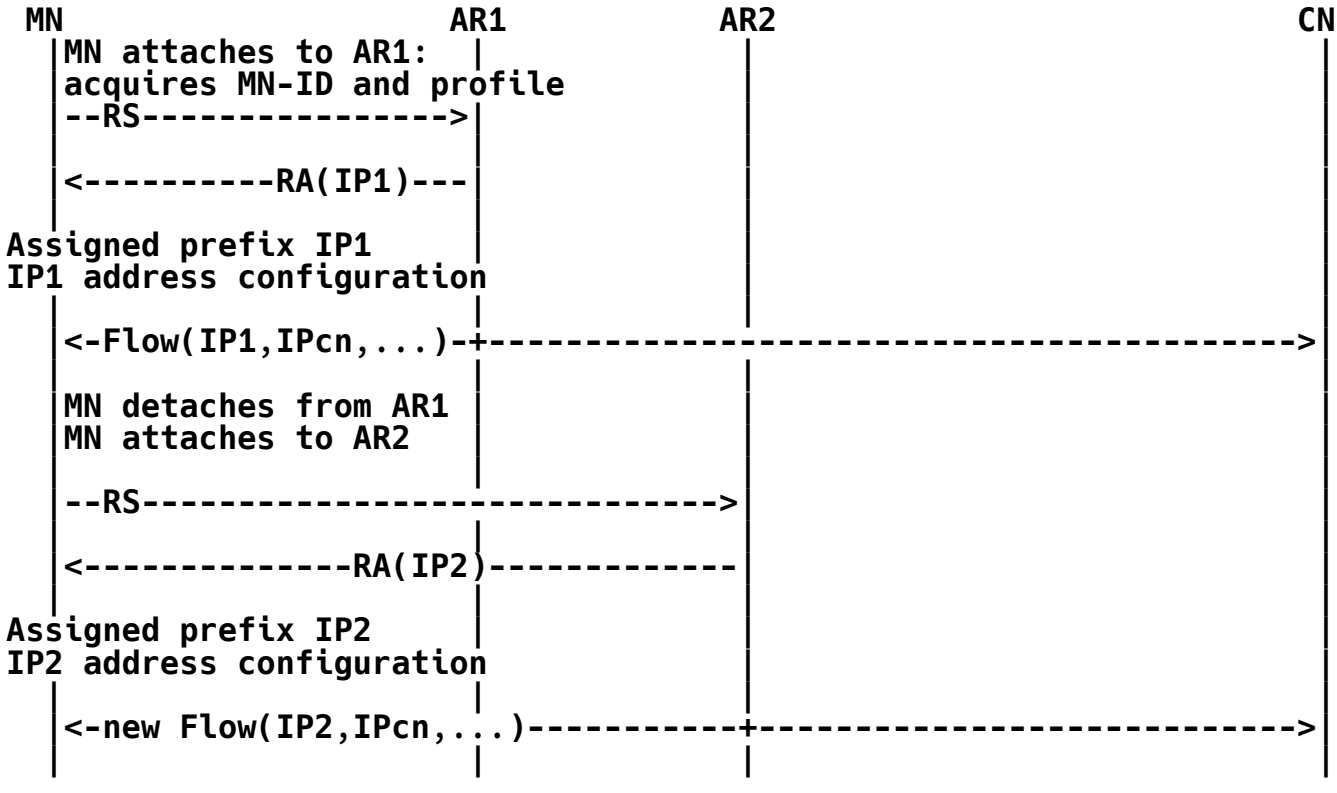


Figure 4: Restarting a Flow with New IP Prefix/Address

4.2. Mobility Case with Traffic Redirection

When IP mobility is needed for a flow, the LM and FM functions in Section 3.1 are utilized. There are two possible cases: (i) the mobility anchor remains playing that role and forwards traffic to a

new locator in the new network, and (ii) the mobility anchor (data-plane function) is changed but binds the MN's transferred IP address/prefix. The latter enables optimized routes but requires some data-plane node that enforces traffic indirection. We focus on the first case in this section. The second case is addressed in Section 4.3.

Mobility support can be provided by using mobility management methods, such as the approaches surveyed in the following academic papers: [IEEE-DISTRIBUTED-MOBILITY], [PMIP-DMA], and [DMM-MOBILE-INTERNET]. After moving, a certain MN's traffic flow may continue using the IP prefix from the prior network of attachment. Yet, some time later, the application generating this traffic flow may be closed. If the application is started again, the new flow may not need to use the prior network's IP address to avoid having to invoke IP mobility support. This may be the case where a dynamic IP prefix/address, rather than a permanent one, is used. Packets belonging to this flow may then use the new IP prefix (the one allocated in the network where the flow is being initiated). Routing is again kept simpler without employing IP mobility and will remain so as long as the MN, which is now in the new network, does not move again to another network.

An example call flow in this case is outlined in Figure 5. In this example, the AR1 plays the role of the FM-DP entity and redirects the traffic (e.g., using an IP tunnel) to AR2.

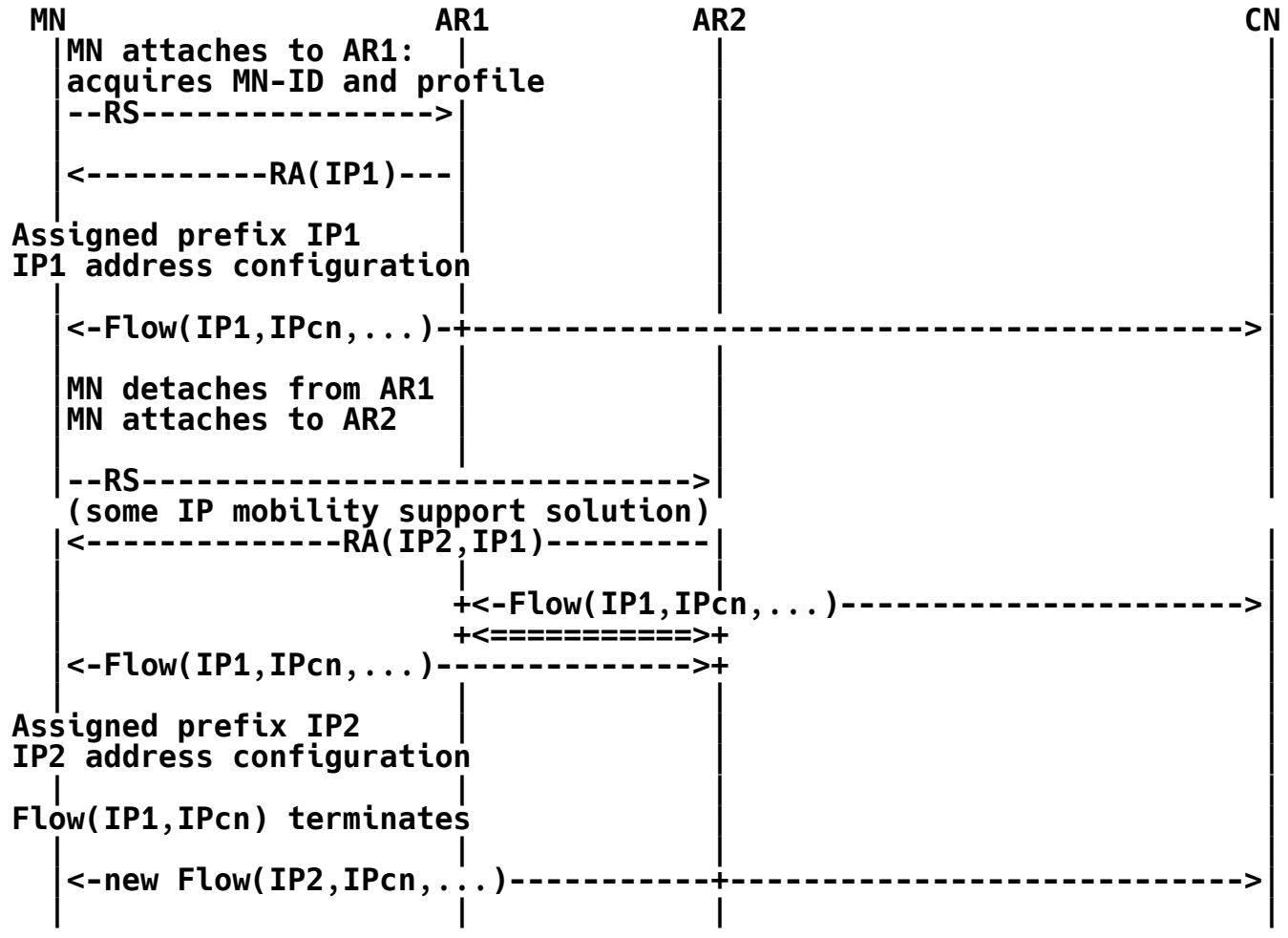


Figure 5: Flow Using IP Prefix from Home Network after MN has Moved

Another solution could be to place an FM-DP entity closer to the CN network to perform traffic steering to deviate from default routes (which will bring the packet to AR1 per default routing). The LM and FM functions are implemented as shown in Figure 6.

Figure 6: Anchor Redirection

Multiple instances of DPAs (at access routers), which are providing IP prefixes to the MNs, are needed to provide distributed mobility anchoring in an appropriate configuration such as those described in Figure 1 (Section 3.1.1) for network-based distributed mobility or in Figure 2 (Section 3.1.2) for client-based distributed mobility.

4.3. Mobility Case with Anchor Relocation

We focus next on the case where the mobility anchor (data-plane function) is changed but binds the MN's transferred IP address/prefix. This enables optimized routes but requires some data-plane node that enforces traffic indirection.

IP mobility is invoked to enable IP session continuity for an ongoing flow as the MN moves to a new network. The anchoring of the IP address of the flow is in the home network of the flow (i.e., different from the current network of attachment). A centralized mobility management mechanism may employ indirection from the anchor in the home network to the current network of attachment. Yet, it may be difficult to avoid using an unnecessarily long route (when the route between the MN and the CN via the anchor in the home network is significantly longer than the direct route between them). An alternative is to move the IP prefix/address anchoring to the new network.

The IP prefix/address anchoring may move without changing the IP prefix/address of the flow. The LM function in Figure 1 of

Section 3.1.1 is implemented as shown in Figure 7.

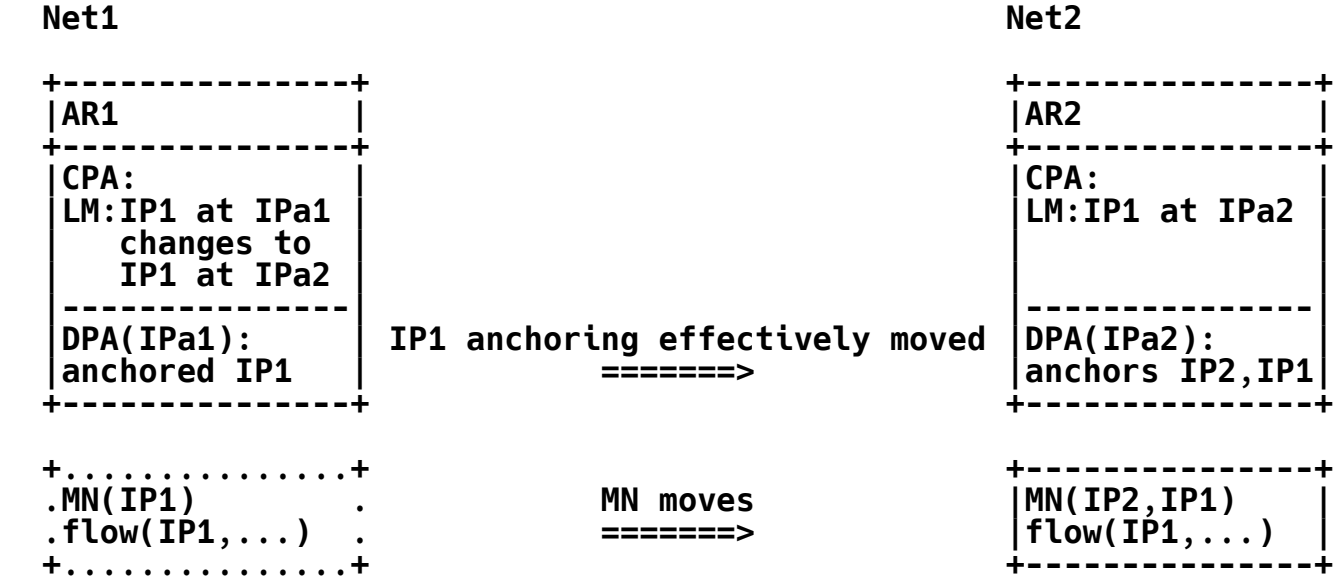


Figure 7: Anchor Relocation

As an MN with an ongoing session moves to a new network, the flow may preserve IP session continuity by moving the anchoring of the original IP prefix/address of the flow to the new network.

One way to accomplish such a move is to use a centralized routing protocol, but such a solution may present some scalability concerns and its applicability is typically limited to small networks. One example of this type of solution is described in [BGP-ATN-IPS]. When an MN associates with an anchor, the anchor injects the MN's prefix into the global routing system. If the MN moves to a new anchor, the old anchor withdraws the /64 and the new anchor injects it instead.

5. Security Considerations

As stated in [RFC7333], "a DMM solution MUST support any security protocols and mechanisms needed to secure the network and to make continuous security improvements". It "MUST NOT introduce new security risks".

There are different potential deployment models of a DMM solution. The present document has presented three different scenarios for distributed anchoring: (i) nomadic case, (ii) mobility case with traffic redirection, and (iii) mobility case with anchor relocation. Each of these cases has different security requirements, and the actual security mechanisms depend on the specifics of each solution/ scenario.

As general rules, for the first distributed anchoring scenario (nomadic case), no additional security consideration is needed, as this does not involve any additional mechanism at Layer 3. If session connectivity is required, the Layer 4 or above solution used to provide it MUST also provide the required authentication and security.

The second and third distributed anchoring scenarios (mobility case) involve mobility signaling among the mobile node and the control-plane and data-plane anchors. The control-plane messages exchanged between these entities MUST be protected using end-to-end security associations with data-integrity and data-origination capabilities. IPsec [RFC8221] Encapsulating Security Payload (ESP) in transport mode with mandatory integrity protection SHOULD be used for protecting the signaling messages. Internet Key Exchange Protocol Version 2 (IKEv2) [RFC8247] SHOULD be used to set up security associations between the data-plane and control-plane anchors. Note that in scenarios in which traffic indirection mechanisms are used to relocate an anchor, authentication and authorization mechanisms MUST be used.

Control-plane functionality MUST apply authorization checks to any commands or updates that are made by the control-plane protocol.

6. IANA Considerations

This document has no IANA actions.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3753] Manner, J., Ed. and M. Kojo, Ed., "Mobility Related Terminology", RFC 3753, DOI 10.17487/RFC3753, June 2004, <https://www.rfc-editor.org/info/rfc3753>.

[RFC5213] Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, DOI 10.17487/RFC5213, August 2008, <https://www.rfc-editor.org/info/rfc5213>.

[RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, DOI 10.17487/RFC6275, July 2011, <https://www.rfc-editor.org/info/rfc6275>.

[RFC7333] Chan, H., Ed., Liu, D., Seite, P., Yokota, H., and J. Korhonen, "Requirements for Distributed Mobility Management", RFC 7333, DOI 10.17487/RFC7333, August 2014, <https://www.rfc-editor.org/info/rfc7333>.

[RFC7429] Liu, D., Ed., Zuniga, JC., Ed., Seite, P., Chan, H., and CJ. Bernardos, "Distributed Mobility Management: Current Practices and Gap Analysis", RFC 7429, DOI 10.17487/RFC7429, January 2015, <https://www.rfc-editor.org/info/rfc7429>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC

2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8221] Wouters, P., Migault, D., Mattsson, J., Nir, Y., and T. Kivinen, "Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 8221, DOI 10.17487/RFC8221, October 2017, <https://www.rfc-editor.org/info/rfc8221>.

[RFC8247] Nir, Y., Kivinen, T., Wouters, P., and D. Migault, "Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 8247, DOI 10.17487/RFC8247, September 2017, <https://www.rfc-editor.org/info/rfc8247>.

7.2. Informative References

[BGP-ATN-IPS]
Templin, F., Saccone, G., Dawra, G., Lindem, A., and V. Moreno, "A Simple BGP-based Mobile Routing System for the Aeronautical Telecommunications Network", Work in Progress, Internet-Draft, draft-ietf-rtgwg-atn-bgp-06, 30 June 2020, <https://tools.ietf.org/html/draft-ietf-rtgwg-atn-bgp-06>.

[DMM-DMA] Seite, P., Bertin, P., and J. Lee, "Distributed Mobility Anchoring", Work in Progress, Internet-Draft, draft-seite-dmm-dma-07, 6 February 2014, <https://tools.ietf.org/html/draft-seite-dmm-dma-07>.

[DMM-ENHANCED-ANCHORING]
Kim, Y. and S. Jeon, "Enhanced Mobility Anchoring in Distributed Mobility Management", Work in Progress, Internet-Draft, draft-yhkim-dmm-enhanced-anchoring-05, 8 July 2016, <https://tools.ietf.org/html/draft-yhkim-dmm-enhanced-anchoring-05>.

[DMM-MOBILE-INTERNET]
Chan, H., Yokota, H., Xie, J., Seite, P., and D. Liu, "Distributed and Dynamic Mobility Management in Mobile Internet: Current Approaches and Issues", Journal of Communications, Vol. 6, No. 1, February 2011.

[DMM-WIFI] Sarikaya, B. and L. Li, "Distributed Mobility Management Protocol for WiFi Users in Fixed Network", Work in Progress, Internet-Draft, draft-sarikaya-dmm-for-wifi-05, 30 October 2017, <https://tools.ietf.org/html/draft-sarikaya-dmm-for-wifi-05>.

[FPC-DMM-PROTOCOL]
Matsushima, S., Bertz, L., Liebsch, M., Gundavelli, S., Moses, D., and C. Perkins, "Protocol for Forwarding Policy Configuration (FPC) in DMM", Work in Progress, Internet-Draft, draft-ietf-dmm-fpc-cpdp-14, 22 September 2020, <https://tools.ietf.org/html/draft-ietf-dmm-fpc-cpdp-14>.

[IEEE-DISTRIBUTED-MOBILITY]
Lee, J., Bonnin, J., Seite, P., and H. A. Chan, "Distributed IP mobility management from the perspective of the IETF: motivations, requirements, approaches, comparison, and challenges", IEEE Wireless Communications, vol. 20, no. 5, pp. 159-168, October 2013.

[PMIP-DMA] Chan, H., "Proxy mobile IP with distributed mobility anchors", IEEE Globecom Workshops Miami, FL, 2010, pp. 16-20, December 2010.

[PREFIX-COST]
McCann, P. and J. Kaippallimalil, "Communicating Prefix Cost to Mobile Nodes", Work in Progress, Internet-Draft, draft-mccann-dmm-prefixcost-03, 11 April 2016, <https://tools.ietf.org/html/draft-mccann-dmm-prefixcost-03>.

[RFC6459] Korhonen, J., Ed., Soininen, J., Patil, B., Savolainen, T., Bajko, G., and K. Iisakkila, "IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS)", RFC 6459, DOI 10.17487/RFC6459, January 2012, <https://www.rfc-editor.org/info/rfc6459>.

[RFC8653] Yegin, A., Moses, D., and S. Jeon, "On-Demand Mobility Management", RFC 8653, DOI 10.17487/RFC8653, October 2019, <https://www.rfc-editor.org/info/rfc8653>.

[RFC8885] Bernardos, CJ., de la Oliva, A., Giust, F., Zúñiga, JC., and A. Mourad, "Proxy Mobile IPv6 Extensions for Distributed Mobility Management", RFC 8885, DOI 10.17487/RFC8885, October 2020, <https://www.rfc-editor.org/info/rfc8885>.

[STATELESS-UPLANE-VEPC]
Matsushima, S. and R. Wakikawa, "Stateless user-plane architecture for virtualized EPC (vEPC)", Work in Progress, Internet-Draft, draft-matsushima-stateless-uplane-vepc-06, 21 March 2016, <https://tools.ietf.org/html/draft-matsushima-stateless-uplane-vepc-06>.

Acknowledgements

The work of Jong-Hyouk Lee was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2020-2015-0-00403) supervised by the IITP (Institute for Information & communications Technology Planning & Evaluation).

Contributors

Alexandre Petrescu and Fred Templin had contributed to earlier draft versions of this document regarding distributed anchoring for hierarchical networks and for network mobility, although these

extensions were removed to keep the document within reasonable length.

This document has benefited from other work on mobility support in SDN networks, on providing mobility support only when needed, and on mobility support in enterprise networks. These works have been referenced. While some of these authors have taken the work to jointly write this document, others have contributed at least indirectly by writing these works. The latter include Philippe Bertin, Dapeng Liu, Satoru Matushima, Pierrick Seite, Jouni Korhonen, and Sri Gundavelli.

For completeness, some terminology from draft-ietf-dmm-deployment-models-04 has been incorporated into this document.

Valuable comments have been received from John Kaippallimalil, ChunShan Xiong, Dapeng Liu, Fred Templin, Paul Kyzivat, Joseph Salowey, Yoshifumi Nishida, Carlos Pignataro, Mirja Kuehlewind, Eric Vyncke, Qin Wu, Warren Kumari, Benjamin Kaduk, Roman Danyliw, and Barry Leiba. Dirk von Hugo, Byju Pularikkal, and Pierrick Seite have generously provided careful review with helpful corrections and suggestions. Marco Liebsch and Lyle Bertz also performed very detailed and helpful reviews of this document.

Authors' Addresses

H. Anthony Chan (editor)
Caritas Institute of Higher Education
2 Chui Ling Lane, Tseung Kwan O
N.T.
Hong Kong

Email: h.a.chan@ieee.org

Xinpeng Wei
Huawei Technologies
Xin-Xi Rd. No. 3, Haidian District
Beijing, 100095
China

Email: weixinpeng@huawei.com

Jong-Hyouk Lee
Sejong University
209, Neungdong-ro, Gwangjin-gu
Seoul
05006
Republic of Korea

Email: jonghyouk@sejong.ac.kr

Seil Jeon
Sungkyunkwan University

2066 Seobu-ro, Jangan-gu
Suwon, Gyeonggi-do
Republic of Korea

Email: seiljeon.ietf@gmail.com

Carlos J. Bernardos (editor)
Universidad Carlos III de Madrid
Av. Universidad, 30
28911 Leganes, Madrid
Spain

Phone: +34 91624 6236
Email: cjbc@it.uc3m.es
URI: http://www.it.uc3m.es/cjbc/