NAT64 for Proxy Mobile IPv6
draft-sarikaya-behave-netext-nat64-pmip-00.txt

Abstract

This memo specifies how IPv6 only mobile nodes (MN) receiving
network-based mobility management using Proxy Mobile IPv6 (PMIPv6)
can communicate with IPv4 only servers. The protocol is based on
local mobility anchors maintaining a table similar to NAT64 and
linking it to the binding cache. This technique avoids the problems
encountered when NAT64 is used for mobile nodes. How IPv6 only
mobile nodes can receive multicast data from IPv4 only content
providers is also explained.

Status of this Memo

This Internet-Draft is submitted 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."

This Internet-Draft will expire on December 6, 2010.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the
document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal
Provisions Relating to IETF Documents
(http://trustee.ietf.org/license-info) in effect on the date of
publication of this document. Please review these documents
carefully, as they describe your rights and restrictions with respect
to this document. Code Components extracted from this document must
include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.

Table of Contents

1. Introduction .................................................. 3
2. Terminology .................................................. 3
3. Requirements .................................................. 3
4. Unicast Translation ............................................ 5
5. Multicast Translation .......................................... 5
6. Handover and Localized Routing ............................... 7
7. Extensions to Proxy Mobile IPv6 .............................. 8
   7.1. Multicast Extensions ...................................... 8
8. Security Considerations ....................................... 8
9. IANA Considerations ........................................... 9
10. Acknowledgements ............................................. 9
11. References ................................................... 9
   11.1. Normative References .................................. 9
   11.2. Informative references ................................. 10
Authors’ Addresses .............................................. 11
1. Introduction

With IPv4 address depletion on the horizon, many techniques are being standardized for IPv6 migration including NAT64 [I-D.ietf-behave-v6v4-xlate-stateful]. NAT64 together with DNS64 [I-D.ietf-behave-dns64] enables IPv6-only hosts to communicate with IPv4-only servers.

NAT64 is designed for fixed hosts. When used for mobile nodes several problems occur as described in [I-D.haddad-mext-nat64-mobility-harmful]. In this document we redesign NAT64 for network based mobility protocol called Proxy Mobile IPv6. The design uses DNS64 as is and integrates NAT64 operation with the binding cache of Proxy Mobile IPv6.

The document continues in Section 3 with a set of requirements on a solution for NAT64 for Proxy Mobile IPv6. In Section 4 the protocol design is presented, multicast translation is explained in Section 5 while handover and localized routing cases are covered in Section 6 for unicast. In Section 7 extensions to PMIPv6 are described.

2. Terminology

This document uses the terminology defined in [RFC5213], [I-D.ietf-behave-v6v4-xlate-stateful], [I-D.ietf-behave-dns64] and [RFC5844].

3. Requirements

NAT64 has two main problems if used for the mobile nodes: the first one is related to mobility and the second one is related to NAT keepalives. DNS64 may use the IPv6 prefix assigned to the NAT64 IPv6 interface in the domain in translating IPv4 address of the server to an IPv6 address. When the mobile node moves to a different domain the IPv6 prefix changes and as a result, the mobile node gets a different IPv6 address for the same correspondent host it was communicating before. However in Proxy Mobile IPv6, the mobile node is anchored at the local mobility anchor which receives packets reverse tunneled from the mobile node and sends them to their destinations. In this case the packets from the local mobility anchor will likely not reach their destination for properly translating into IPv4 packets and will get dropped [I-D.haddad-mext-nat64-mobility-harmful].

NAT64 protocol should enable host mobility. This requirement is met by redesigning NAT64 protocol so that the mobility anchor which keeps
track of the host’s mobility knows about all prefixes used.

NAT64 is a NAT device which keeps NAT table as the NAT state [RFC3519]. NAT state is soft state and it expires if it is not refreshed during a certain time interval. NAT keepalives sent by the host are used for this purpose. Mobile nodes go to sleep mode when inactive in which battery usage is minimized. However sending NAT keepalive messages may drain the mobile node’s battery because it has to cut short its sleep mode.

NAT keepalives should be avoided for the mobile nodes. This requirement is met by integrating NAT64 state with binding cache that the mobility anchor creates for the mobile node in order to keep track of its mobility. NAT64 state is refreshed automatically when the mobile node’s binding cache entry is refreshed and in case of Proxy Mobile IPv6, Mobile Access Gateway refreshes it not the mobile node so no battery consumption is needed.

While resolving issues of NAT64 related to mobility, it is desirable to keep compatibility with fixed hosts. This requirement is met by reusing DNS64 for mobile nodes as well.

NAT64 translates IPv6 packet into IPv4 packet and vice versa and the translation algorithm is defined in [I-D.ietf-behave-v6v4-xlate]. However translation algorithm is deficient in that IPv6 extension headers (except fragmentation header) and IPv4 options are not translated. Proxy Mobile IPv6 uses extension header in registration signaling using PBU/PBA messages. PBU/PBA are exchanged between MAG and LMA and not between mobile node and correspondent node. Because of this the deficiency is avoided.

The behaviour of IPv4-only or dual stack mobile nodes using network based mobility protocol Proxy Mobile IPv6 is specified in [RFC5844]. However this document does not specify how IPv6-only mobile nodes can access IPv4-only servers. Hence this specification complements [RFC5844].

NAT64 is designed for unicast communication, the translation algorithm is defined in [I-D.ietf-behave-v6v4-xlate] does not translate multicast packets. IPv6 only hosts receiving multicast data from IPv4 only servers is not covered.

For many applications multicast communication for mobile nodes is a requirement. This requirement is met by designing a multicast translation scheme for Proxy Mobile IPv6. This technique applies to any source multicast.
4. Unicast Translation

When forwarding packets sent by the mobile node, the local mobility anchor first checks the Source Address field in the binding cache. A further check is made if the destination address’s prefix matches Pref64. In case of a match, IPv6-only flag in the binding cache entry for the mobile node is set if it was not set already.

LMA generates an IPv4 packet and sends it to the destination IPv4-only server from its IPv4 interface. We assume that IPv4 interface address is 203.0.113.1 as in [I-D.ietf-behave-v6v4-xlate-stateful]. As in [I-D.ietf-behave-v6v4-xlate-stateful], LMA selects an available source port, e.g. 2000 which becomes IPv4 packet source port and creates a "NAT state" of

<MN source address, IPv6 source port> <---> <IPv4 Interface address, IPv4 source port>

This state is linked to the binding cache entry for MN. In generating IPv4 packet, destination IPv4 address is derived from the last 32 bits of destination address of IPv6 packet, e.g. 192.0.2.1 and destination port of IPv6 packet is set to the destination port of IPv4 packet. IPv6 packet is translated into an IPv4 packet following the algorithm presented in [I-D.ietf-behave-v6v4-xlate].

When forwarding any subsequent packets for the same session corresponding to <MN source address, source port>, LMA finds the corresponding entry in the NAT table and creates the corresponding IPv4 packet using this entry. The above procedure is repeated only when a new session is started by MN.

When LMA receives a packet addressed to its IPv4 interface it searches the NAT table for the corresponding MN IPv6 source address and port. For example the tuple <203.0.113.1, 2000> would match the network-specific prefix (NSP) of 2001:FF00::/64 and the source port of 1500. LMA creates an IPv6 packet from IPv4 packet using this information. IPv4 packet is translated into an IPv6 packet following the algorithm presented in [I-D.ietf-behave-v6v4-xlate]. Next LMA fetches MN’s binding cache entry and finds the MAG MN is associated with. LMA encapsulates IPv6 packet and sends it to the MAG.

5. Multicast Translation

In this section we specify how mobile node can receive IPv4 multicast data from IPv4-only content provider based on currently adopted base solution for supporting multicast in Proxy Mobile IPv6
IPv6-only mobile node will join IPv4 multicast group by sending MLD Membership Report message to MLD Proxy which is located at the mobile access gateway. Mobile node will use synthesized IPv6 address of IPv4 multicast group address, e.g. a /96 prefix used for any source multicast called IPV6_TRASM_ADDRESS prefix followed by a.b.c.d, IPv4 multicast group address. IPV6_TRASM_ADDRESS prefix takes the form of FFxx::/96, it is non-SSM prefix [I-D.venaas-behave-mcast46]. Multicast router at the local mobility anchor receives an aggregate join message from the mobile access gateway for the group IPV6_TRASM_ADDRESS prefix:a.b.c.d.

Each local mobility anchor is assigned a unique IPV6_TRASM_ADDRESS prefix. Mobile nodes can learn this value by means out of scope with this document. With this, mobile node can easily create an IPv6 multicast address from the IPv4 group address a.b.c.d that it wants to join.

Local mobility anchor as multicast anchor checks the group address and recognizes IPV6_TRASM_ADDRESS prefix. It next checks the last 32 bits is an IPv4 multicast address in range 224/8 - 239/8. If all checks succeed, local mobility anchor joins a.b.c.d using IGMP on its IPv4 interface.

When local mobility anchor receives multicast data for the group a.b.c.d, it first obtains the IPv6 address IPV6_TRASM_ADDRESS prefix: a.b.c.d and then checks to see if it has any outgoing interfaces towards the mobile access gateway which happens when at least one mobile node is subscribed to this address. Local mobility anchor will then translate IPv4 multicast data packet into an IPv6 multicast data packet. The destination address is IPv6 group address IPV6_TRASM_ADDRESS prefix:a.b.c.d and source address is local mobility anchor’s IPv6 interface address. IPv4 payload is copied into IPv6 payload.

Multicast translation described in this section is mobile node agnostic. Local mobility anchor gets Multicast Listener Discovery messages from the proxy instance in one of the mobile access gateways when the membership database of the mobile access gateway changes. For the local mobility anchor it is sufficient to know if there is at least one member in the corresponding downstream Multicast Listener Discovery proxy instance and because of this local mobility anchor does not need to consult its binding cache.
6. Handover and Localized Routing

In Proxy Mobile IPv6 mobile node is always at home, i.e. its home address does not change even if it moves. If the move is within the same domain served by the same DNS64 entity the mobile node can continue to send/receive packets with IPv4 only server and the protocol defined in Section 4 can be used for translating IPv6 packets into IPv4 and vice versa.

If MN moves to a domain where DNS64 entity changes MN initiates communication with IPv4-only server, it gets a different synthetic AAAA RR with a different IPv6 address of the destination. MN sends its IPv6 packet to the local MAG which tunnels it to MN’s LMA.

LMA checks the source address (mobile node’s home address) in the binding cache for any entry with IPv6-only flag set. Next destination address’s prefix is checked in a list of Pref64’s that are supported. In case of a match, LMA continues to create an IPv4 packet as described in Section 4. In addition LMA also removes all NAT table entries matching MN source address since MN is no longer using the same Pref64. If IPv6-only flag is not set then this is the first packet sent to a new IPv4-only server. LMA processes this packet as described in Section 4.

The effect of handover on multicast translation depends on how IPv6_TRASM_ADDRESS prefix is configured. Mobile node may get a different IPv6_TRASM_ADDRESS prefix locally after moving to a new mobile access gateway. Mobile node sends a join request (Multicast Listener Discovery Report message) with a new multicast group address. Local mobility anchor adds this group address to its membership database. Local mobility anchor MUST add the new IPv6_TRASM_ADDRESS prefix to the multicast prefix table.

Localized routing in PMIPv6 is used to avoid reverse tunneling every packet to local mobility anchor by enabling the MAG to directly send the packets to another MAG where the correspondent node for this mobile node is associated [I-D.ietf-netext-pmip6-lr-ps]. The other MAG may be connected to a different LMA.

NAT64 for PMIPv6 is supported at the local mobility anchor not at the mobile access gateway so it would not work when localized routing is used. Since NAT64 assumes that MN is communicating with IPv4-only servers these servers are not expected to be associated with any mobile access gateway in the domain. This means that no trigger can be found to initiate localized routing for communication between the mobile node and IPv4-only server.
7. Extensions to Proxy Mobile IPv6

Binding cache entry contains the following new entry:

A flag indicating whether or not this mobile node is IPv6-only node.

IPv6-only flag is set after receiving the first IPv6 packet containing a synthetic IPv6 address. This flag is used to connect the binding cache with the NAT table.

Local mobility anchor keeps a NAT table for IPv6-only mobile nodes communicating with IPv4-only servers. NAT table contains at a minimum entries for associating MN source address, IPv6 source port to the corresponding IPv4 interface address of the local mobility anchor and source port information.

MN source address in the NAT table MUST correspond to a binding cache entry with IPv6-only flag set.

Local mobility anchor has a table of NAT64 prefixes, Pref64 that are supported in PMIPv6 domain and its roaming partners. For each Pref64, local mobility anchor keeps a 32-bit suffix which is concatenated to the prefix. The resulting 96-bit value is concatenated with IPv4 address of the destination IPv4-only server to obtain the synthesized IPv6 address.

If the Well-Known Prefix is used this table contains 64:FF9B::/96. In this case there is no associated suffix.

7.1. Multicast Extensions

Multicast anchor at the local mobility anchor MUST support at least one IPV6_TRASM_ADDRESS prefix. Multicast anchor at the local mobility anchor MUST support IGMP on its IPv4 interface.

Local mobility anchor has a table of IPV6_TRASM_ADDRESS prefixes. This table normally contains a single entry, i.e. the local prefix value. It may be populated by more entries in case of handover as described in Section 6. The entries are kept as soft-state and removed after a period of no activity.

8. Security Considerations

For IPv4-only or dual stack mobile nodes security considerations stated in [RFC5844] apply. This document specifies additional procedures PMIPv6 for the case of IPv6-only mobile nodes which are not covered in [RFC5844]. Security considerations for IPv4 interface
of the local mobility anchor is similar to [I-D.ietf-behave-v6v4-xlate-stateful] and the considerations stated there apply.

9. IANA Considerations

None.

10. Acknowledgements

TBD.

11. References

11.1. Normative References


[I-D.ietf-behave-v6v4-xlate-stateful]

[I-D.ietf-behave-dns64]

[I-D.ietf-behave-v6v4-xlate]


11.2. Informative references


[I-D.haddad-mext-nat64-mobility-harmful]
Haddad, W. and C. Perkins, "A Note on NAT64 Interaction with Mobile IPv6",
draft-haddad-mext-nat64-mobility-harmful-01 (work in progress), April 2010.

[I-D.ietf-netext-pmip6-lr-ps]
Liebsch, M., Jeong, S., and W. Wu, "PMIPv6 Localized Routing Problem Statement",
draft-ietf-netext-pmip6-lr-ps-02 (work in progress), January 2010.


[I-D.venaas-behave-mcast46]

[I-D.ietf-multimob-pmipv6-base-solution]
Schmidt, T., Waehlisch, M., and S. Krishnan, "Base Deployment for Multicast Listener Support in PMIPv6 Domains",
draft-ietf-multimob-pmipv6-base-solution-02 (work in progress), May 2010.
Authors’ Addresses

Behcet Sarikaya
Huawei USA
1700 Alma Dr. Suite 500
Plano, TX  75075

Phone: +1 972-509-5599
Email: sarikaya@ieee.org

Frank Xia
Huawei USA
1700 Alma Dr. Suite 500
Plano, TX  75075

Phone: +1 972-509-5599
Email: xiayangsong@huawei.com