DMM Working Group   S. Jeon
Internet-Draft   Sungkyunkwan University
Intended status: Standards Track   S. Figueiredo
Expires: March 15, 2018   Altran Research
                                                            Y. Kim
                                                Soongsil University
                                               J. Kaippallimalil
                                                            Huawei
                                               September 11, 2017

        Use Cases and API Extension for Source IP Address Selection
              draft-sijeon-dmm-use-cases-api-source-07.txt

Abstract

   This draft specifies and analyzes the expected cases regarding the
   selection of a proper source IP address and address type by an
   application in a distributed mobility management (DMM) network. It
   also proposes a new Socket API to address further selection issues
   with three source IP address types defined in the on-demand mobility
   API draft.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Applications to select source IP address type in a mobile node (MN)
need to consider IP session continuity and/or IP address
reachability. [I-D.ietf-dmm-ondemand-mobility], defines three types
of source IP addresses based on mobility management capabilities:
fixed IP address, session-lasting IP address, and non-persistent IP
address. Based on the address type requested by the application, the
MN configures a proper source IP address. However, the source IP
address type itself in a socket request may not be enough to convey
all the requirements of an application. For example, more than one
IP address of the same type requested may be available. It may be
that as a result of mobility the MN can potentially obtain new IP

prefixes from different serving networks belonging to different
subnets. This draft categorizes and analyzes use cases that an MN is
likely to encounter. In addition, this draft proposes an extension
that allows the application to express its preferences when more than
one source address of a type is present.

2. Use Cases and Analysis

This section outlines use cases where an application on the MN tries
to obtain a source IP address.

2.1. Application has no specific IP address type requirement or address preference

Applications such as text-based web browsing or information service,
e.g. weather and stock information, as well as legacy applications
belong to this category. Many applications use short-lived Internet
connections with no requirements for session continuity or IP address
reachability. Assigning a non-persistent IP address can be thus
considered as default for MNs. However, it is subject to address
assignment policy of a network operator. The suggested flag,
IPV6_REQUIRE_NON-PERSISTENT_IP, defined in
[I-D.ietf-dmm-ondemand-mobility] can used for expressing its
preference to the IP stack.

2.2. Application has specific IP address type requirement and address preference

This category is for an application requiring IP session continuity
with different granularity of IP address reachability. This case may
be further divided in three sub-cases with regard to IP address type
availability and/or address selection.

2.2.1. Case 1: there is no configured IP address based on a requested type in the IP stack, but there is a further selection
preference by the application

Once an IP address is requested by an application regardless of any
source IP address type defined in [I-D.ietf-dmm-ondemand-mobility],
the network stack will configure an IP address after obtaining an IP
prefix based on the requested source IP address type from the current
serving gateway.

2.2.2. **Case 2: there are one or more IP addresses configured with a
        requested type in the IP stack, and no selection preference by**
        the application

   This is the same as Case 1 described above, except the existence of
   more than one configured IP addresses belonging to the requested IP
   address type in the IP stack, e.g. due to different address
   assignment policy by an operator.

   When a non-persistent IP address is requested, if an application
   requests a non-persistent IP address to the IP stack, the IP address
   is obtained from the serving IP gateway as the previous one is not
   maintained across gateway changes.

   When a session-lasting IP address is requested, an expected sequence
   can be described as follows;

   1. The MN has one or more session-lasting IP addresses configured in
   the IP stack.

   2. If an application requests a session-lasting IP address to the IP
   stack, it will try to use an existing session-lasting IP address as
   it is already configured in the IP stack. If there are multiple
   available session-lasting IP addresses, the default address selection
   rules will be applied [RFC6724], e.g. with scope preference, longest
   prefix matching, and/or so on. The best-matched IP address among
   them will be selected and assigned to the application.

   3. Subsequently, the MN moves to another serving network, and the
   previous (mobile) sessions are still in use. A new application
   requests a session-lasting IP address with flag,
   IPV6_REQUIRE_SESSION_LASTING_IP to the IP stack. The selection of
   the session-lasting IP address follows the same procedure as
   described in Step 2.

   When a fixed IP address is requested, it will follow the same
   procedure with session-lasting IP address request as described.

2.2.3. **Case 3: there are one or more IP addresses with a requested type
        configured in the IP stack, but there is a further selection**
        preference by the application

   Assume that there are one or multiple applications with session-
   lasting IP address running. A newly initiated application might get
   one of the session-lasting IP addresses being used, not initiating a
   protocol procedure, i.e. DHCP or SLAAC for a new session-lasting IP
   address to the network. On the contrary, the IP stack might try to
   get a new session-lasting IP address from the current serving gateway

by default. Acquiring a new session-lasting IP address may take some
time (due to the exchange with the network) while using an existing
one is instantaneous. On the other hand, using the existing one
might yield less optimal routing. For example, the use of the IP
address with an existing one configured might provide a suboptimal
routing path as a result of a handover. This situation might not be
preferred by newly initiated applications because the application
incurs the costs of IP mobility even though the MN has not moved from
the current serving network. Eventually, the new session is served
by a remote IP mobility anchor with mobility management functions,
though the MN has not moved yet.

If the application is allowed to further define its preference for an
optimally routed, this situation can be avoided. See Section 3 for
the proposed flag.

2.3. Gaps in the consistency with the default address selection

The need of an indication mechanism can be sought in the consistency
with the former IETF standards. For example, in [RFC6724] where
default behavior for IPv6 is specified, without a proper indication
mechanism, following conflicts are expected to happen. In Rule 6 in
[RFC6724], it is said that the matching label between source address
of an IPv6 host and destination address is preferred among the
combinations between other source addresses and destination address,
where the label is a numeric value representing policies that prefer
a particular source address prefix for use with a destination address
prefix in [RFC6724]. In Rule 8 in [RFC6724], it is said that the
longest matching prefix between source address of an IPv6 host and
destination address is preferred among the combinations between other
source addresses and destination address. Following Rules 6 and 8
may result in the selection of a source IP address with which packets
that are sub-optimally routed.

3. Indications for expressing address preference requirement

When an application prefers a new IP address of the requested IP
address type, additional indication flags should be delivered through
the socket API interface.

To obtain an address that supports dynamic mobility using session-
lasting IP address, a new address preference flag needs to be
defined. The flag should be simple and useful while aligned with the
three types of IP addresses. The objective of the hereby presented
address preference flag is letting the IP stack check whether it has
an available IP address assigned from the current serving network
when the flag is received by an initiated application. If not, it

will trigger the IP stack to get a new IP address from the current
serving network. We call it "ON_NET" property.

If the application requests an IP address with ON_NET flag set in the
socket request, the IP address returned by the stack should conform
to the address preference requirement. This should be the case even
though other session-lasting IP addresses, not belonging to the
current serving network are available. If there are multiple
session-lasting IP addresses matched with ON_NET property, the
default source address selection rules will be applied.

IPV6_XX_SRC_ON_NET

/* Require (or Prefer) an IP address based on a requested IP address
type as source, assigned from the current serving network, whatever
it has been assigned or should be assigned */

This flag aims to express the preference to check an IP address,
being used by an application, previously assigned from the current
serving network and to use it or to get an IP address from the
current serving network, as well as enabling differentiated per-flow
anchoring where an obtained session-lasting IP address might be used
for all initiated session-lasting IP applications. The use of the
flag can be combined together with the three types of IP address
defined in [I-D.ietf-dmm-ondemand-mobility].

In [I-D.mccann-dmm-prefixcost], it proposes that the Router
Advertisement signaling messages communicate the cost of maintaining
a given prefix at the MN's current point of attachment. The
objective is to make a dynamic and optimal decision of address
assignment and release, i.e. when to release old addresses and assign
new ones. The proposed ON_NET property may present a way to deliver
a prefix decision for an application, specifically from a routing
distance point of view, to the IP stack.

4. IANA Considerations

This document makes no request of IANA.

5. Security Considerations

T.B.D.

6. Acknowledgements

We would like to thank Danny Moses, Marco Liebsch, Brian Haberman,
Sri Gundavelli, Alexandru Petrescu for their valueable comments and
suggestions on this work.

7. References

7.1. Normative References

   [RFC6724] Thaler, D., Ed., Draves, R., Matsumoto, A., and T. Chown,
              "Default Address Selection for Internet Protocol Version 6
              (IPv6)", RFC 6724, DOI 10.17487/RFC6724, September 2012,
              <https://www.rfc-editor.org/info/rfc6724>.

7.2. Informative References

   [I-D.ietf-dmm-ondemand-mobility]
              Yegin, A., Moses, D., Kweon, K., Lee, J., Park, J., and S.
              Jeon, "On Demand Mobility Management", draft-ietf-dmm-
              ondemand-mobility-12 (work in progress), July 2017.

   [I-D.mccann-dmm-prefixcost]
              McCann, P. and J. Kaippallimalil, "Communicating Prefix
              Cost to Mobile Nodes", draft-mccann-dmm-prefixcost-03
              (work in progress), April 2016.

Authors' Addresses

   Seil Jeon
   Sungkyunkwan University
   2066 Seobu-ro, Jangan-gu
   Suwon, Gyeonggi-do
   Korea

   Email: seiljeon@skku.edu

   Sergio Figueiredo
   Altran Research
   2, Rue Paul Dautier
   Velizy-Villacoublay 78140
   France

   Email: sergio.figueiredo@altran.com

   Younghan Kim
   Soongsil University
   369, Sangdo-ro, Dongjak-gu
   Seoul 156-743
   Korea

   Email: younghak@ssu.ac.kr

John Kaippallimalil
Huawei
5340 Legacy Dr., Suite 175
Plano, TX   75024
USA

Email: john.kaippallimalil@huawei.com