DMM Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 04, 2014

A. Yegin
K. Kweon
J. Lee
J. Park
Samsung

July 03, 2013

On Demand Mobility Management
draft-yegin-dmm-ondemand-mobility-00

Abstract

Applications differ with respect to whether they need IP session continuity and/or IP address reachability. The network providing the same type of service to any mobile host and any application running on the host yields inefficiencies. This document describes a solution for taking the application needs into account in selectively providing IP session continuity and IP address reachability on a per-socket basis.

Table of Contents

1. Introduction

In the context of Mobile IP [RFC5563][RFC6275][RFC5213][RFC5944], following two attributes are defined for the IP service provided to the mobile hosts:

IP session continuity: The ability to maintain an ongoing IP session by keeping the same local end-point IP address throughout the session despite moving among different IP networks. The IP address of the host may change between two independent IP sessions, but that does not jeopardize the IP session continuity. IP session continuity is essential for mobile hosts to maintain ongoing IP sessions without any interruption.

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

Mobile IP is designed to provide both IP session continuity and IP address reachability to mobile hosts. Architectures utilizing these protocols (e.g., 3GPP, 3GPP2, WIMAX) ensure that every one of the mobile hosts attached to the compliant networks enjoy these benefits. Every application running on each one of those mobile hosts is

subjected to the same treatment with respect to the IP session continuity and IP address reachability.

It should be noted that in reality not every application may need those benefits. IP address reachability is required for applications running as servers (e.g., a camera mounted on a bus). But, a typical client application (e.g., web browser) does not necessarily require IP address reachability. Similarly, IP session continuity is not required for all types of applications either. Applications performing brief communication (e.g., DNS client) can survive without having IP session continuity support.

Achieving IP session continuity and IP address reachability by using Mobile IP incur some cost. This solution forces the mobile host's IP traffic to traverse a centrally-located router (Home Agent, HA), which incurs additional transmission latency and use of additional network resources, adds to the network CAPEX and OPEX, and decreases the reliability of the network with the introduction of a single point of failure [I-D.ietf-dmm-requirements]. Therefore, IP session continuity and IP address reachability should be used selectively.

Furthermore, even when an application needs IP session continuity, it may be able to satisfy that need by using a solution above the IP layer, such as MPTCP [RFC6824], SIP mobility [RFC3261], or an application-layer mobility solution. Those higher-layer solutions are not subject to the same issues that arise with the use of Mobile IP since they can utilize the most direct data path between the end-points. But, if Mobile IP is being applied to the mobile host, those higher-layer protocols are rendered useless because their operation is inhibited by the Mobile IP. Since Mobile IP ensures the IP address of the mobile host remains fixed (despite the location and movement of the mobile host), the higher-layer protocols never detect the IP-layer movement and never engage in mobility management.

This document proposes a solution where the applications running on the mobile host can indicate whether they need IP session continuity or IP address reachability. The IP stack on the mobile host, in conjunction with the network, would provide the required type of IP service. It is for the benefit of both the users and the network operators not to engage an extra level of service unless it is absolutely necessary. So it is expected that applications and networks compliant with this specification would utilize this solution to use network resources more efficiently.

2. Notational Conventions

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].

3. Solution

3.1. Types of IP Addresses

Three types of IP addresses are defined with respect to the mobility management.

- Home Network Anchored Address

This is what standard Mobile IP provides with a Home Address (HoA). The mobile host is configured a HoA from a centrally-located Home Network. Both IP session continuity and IP address reachability are provided to the mobile host with the help of a router in the Home Network (Home Agent, HA). This router acts as an anchor for the IP address of the mobile host.

- Access Network Anchored Address

This type of IP address provides IP session continuity but not IP address reachability. It is achieved by ensuring that the IP address used at the beginning of the session remains usable despite the movement of the mobile host. But the IP address may change after the end of ongoing IP sessions, therefore it does not exhibit persistence.

The IP address is allocated by a serving IP gateway. When the mobile host moves to another network, the previously serving gateway becomes an anchor gateway and starts treating the IP address as a Home Address with the help of the received binding updates. A tunnel is established between the anchor gateway and the current care-of address of the mobile host (whether configured on the host itself [RFC5944][RFC6275], or on the serving gateway [RFC5213][RFC5563]) for ensuring the session continuity using the same IP address.

- Unanchored Address

This type of IP address provides neither IP session continuity nor IP address reachability. The IP address is obtained from the serving IP gateway and it is not maintained across gateway changes. In other words, the IP address may be released and replaced by a new IP address when the IP gateway changes due to the mobile host’s mobility.

Applications running as servers at a published IP address require Home Network Anchored Address. Long-standing applications (e.g., an SSH session) may also require this type of address. They could use Access Network Anchored Address, but that can produce sub-optimal results if the mobile host ends up far from the anchor gateway. Enterprise applications that connect to an enterprise network via virtual LAN require Home Network Anchored Address.

Applications with short-lived transient IP sessions can use Access Network Anchored Address. For example: Email client, web browser, calendar, app store client, etc.

Applications with very short IP sessions, such as DNS client and instant messengers, can utilize Unanchored Address. Even though they could very well use Home or Access Network Anchored Addresses, the transmission latency would be the minimum when an Unanchored Address is used.

3.2. Granularity of Selection

The IP address type selection is made at per-socket granularity. Different parts of the same application may have different needs. For example, control part of the application may require Home Network Anchored Address in order to stay reachable, whereas data part of the application may be satisfied with Access Network Anchored Address.

3.3. On Demand Nature

At any point in time, a mobile host may have any mixture of IP addresses configured. Zero or more Unanchored, zero or more Access Network Anchored, and zero or more Home Network Anchored IP addresses may be available on the IP stack of the host. The mixture may be as a result of the host policy, or as a result of the application demand.

If an IP address of the requested type is not available, then the IP stack shall attempt to configure one. For example, a host may not always have a Home Network Anchored IP address available as this is rarely used. In case an application requests one, then the IP stack shall make an attempt to configure one using Mobile IP. If Mobile IP is not available to the host, or if its operation fails, then the IP stack shall fail the associated socket request. In case of successful Mobile IP operation, a Home Network Anchored IP Address gets configured on the mobile host. If another socket requests a Home Network Anchored IP address at a later time, then the same IP address may be served to that socket as well. When the last socket using the requested IP address is closed, the IP address may be released.

The following are matters of policy, which may be dictated by the host itself, the network operator, or the compliant network architecture:

- The initial set of IP addresses configured on the host at the boot time.

- Permission to grant various types of IP addresses to a requesting application.

- Determination of a default address type when an application does not make any explicit indication, whether it already supports the required API or it is a legacy application.

3.4. Conveying the Selection

The selection of the address type is conveyed from the applications to the IP stack in a way to influence the source address selection algorithm [RFC6724].

The current source address selection algorithm operates on the available set of IP addresses when selecting an address. According to the proposed solution, if the requested type IP address is not available at the time of the request, then the IP stack shall make an attempt to configure one such IP address. The selected IP address shall be compliant with the requested IP address type, whether it is selected among available addresses or dynamically configured. In the absence of a matching type (because it is not available and not configurable on demand), the source address selection algorithm shall return an empty set.

A Socket API-based interface for enabling applications to influence the source address selection algorithm is described in [RFC5014]. That specification defines IPV6_ADDR_PREFERENCES option at the IPPROTO_IPV6 level. That option can be used with setsockopt() and getsockopt() calls to set and get address selection preferences.

Furthermore, that RFC also specifies two flags that relate to IP mobility management: IPV6_PREFER_SRC_HOME and IPV6_PREFER_SRC_COA. These flags are used for influencing the source address selection to prefer either a Home Address or a Care-of Address.

Unfortunately, these flags do not satisfy the aforementioned needs due to the following reasons, therefore new flags are proposed in this document:

- Current flags indicate a "preference" whereas there is a need for indicating "requirement". Source address selection algorithm does

not have to produce an IP address compliant with the "preference" , but it has to produce an IP address compliant with the "requirement".

- Current flags influence the selection made among available IP addresses. The new flags force the IP stack to configure a compliant IP address if none is available at the time of the request.

- The Home vs. Care-of Address distinction is not sufficient to capture the three different types of IP addresses described in Section 2.1.

The following new flags are defined in this document and they shall be used with Socket API in compliance with the [RFC5014]:

IPV6_REQUIRE_HOME_ANCHORED /* Require Home Anchored address as source */

IPV6_REQUIRE_ACCESS_ANCHORED /* Require Access Anchored address as source */

IPV6_REQUIRE_UNANCHORED /* Require Unanchored address as source */

More than one of these flags may be set on the same socket. In that case, an IP address compliant with any one of them shall be selected.

When any of these new flags is used, then the IPV6_PREFER_SRC_HOME and IPV6_PREFER_SRC_COA flags, if used, shall be ignored.

These new flags are used with setsockopt()/getsockopt(), getaddrinfo(), and inet6_is_srcaddr() functions [RFC5014]. Similar with the setsockopt()/getsockopt() calls, getaddrinfo() call shall also trigger configuration of the required type IP address, if one is not already available. When the new flags are used with getaddrinfo() and the triggered configuration fails, the getaddrinfo() call shall ignore that failure (i.e., not return an error code to indicate that failure). Only the setsockopt() shall return an error when configuration of the requested type IP address fails.

Application of this solution to IPv4 is TBD.

4. Security Considerations

The setting of certain IP address type on a given socket may be restricted to privileged applications. For example, a Home Anchored IP Address may be provided as a premium service and only certain applications may be allowed to use them. Setting and enforcement of such privileges are outside the scope of this document.

5. IANA Considerations

TBD

6. References

6.1. Normative References

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

[RFC5014] Nordmark, E., Chakrabarti, S., and J. Laganier, "IPv6 Socket API for Source Address Selection", RFC 5014, September 2007.

[RFC6724] Thaler, D., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", RFC 6724, September 2012.

6.2. Informative References

[I-D.ietf-dmm-requirements] Chan, A., Liu, D., Seite, P., Yokota, H., and J. Korhonen, "Requirements for Distributed Mobility Management", draft-ietf-dmm-requirements-05 (work in progress), June 2013.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

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

[RFC5563] Leung, K., Dommety, G., Yegani, P., and K. Chowdhury, "WiMAX Forum / 3GPP2 Proxy Mobile IPv4", RFC 5563, February 2010.

[RFC5944] Perkins, C., "IP Mobility Support for IPv4, Revised", RFC 5944, November 2010.

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

[RFC6824] Ford, A., Raiciu, C., Handley, M., and O. Bonaventure, "TCP Extensions for Multipath Operation with Multiple Addresses", RFC 6824, January 2013.

Authors' Addresses

Alper Yegin
Samsung
Istanbul
Turkey

Email: alper.yegin@partner.samsung.com

Kisuk Kweon
Samsung
Suwon
South Korea

Email: kisuk.kweon@samsung.com

Jinsung Lee
Samsung
Suwon
South Korea

Email: js81.lee@samsung.com

Jungshin Park
Samsung
Suwon
South Korea

Email: shin02.park@samsung.com