INTERNET-DRAFT
Intended Status: Standards Track
Expires: April 30, 2015

X. Wei
Huawei Technologies

October 27, 2014

IP Address Management in DMM
draft-wei-dmm-address-management-00

Abstract

This document provides an IP address management solution for DMM network.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Copyright and License Notice

Table of Contents

1 Introduction

In DMM scenario, mobility anchors would be deployed in a distributed manner, and as specified in RFC7333 [RFC7333], one of the aims of DMM is to reduce the routing redundancy between mobile node and correspondent node, which means providing a more optimal communication path for application traffic between mobile node and correspondent node. To achieve routing optimization for specific application traffic, the basic idea is to make the traffic using IP address(s) anchored at current anchor, so that downlink traffic from correspondent node to mobile node will go directly to mobile node, but this routing optimization requirement brings a fact that mobile node has to change its IP address as it moving to a new anchor. Some application sessions can cope with the change of IP address either by application layer itself or by the function provided by other layers, e.g. transport layer; but for other application sessions, after IP address changed, the application session would be broken off totally. So it's reasonable to provide different network layer mobility support according to the need of application. This document provides a discussion on IP address management in DMM domain, which gives support to source IP address selection on mobile node side. A brief discussion of how end host chooses to use the IP address provided by network is also involved. Currently, the address management described in this document is not specific to certain DMM framework.

1.1 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 RFC 2119 [RFC2119].

2 IP Address Management

2.1 All application sessions prefer IP address consistency

In IP network, the nature of IP address acting as both "locator" and "identifier" results that the change of "location" would inevitably interrupt continuity of ongoing application session, no matter short-lived or long last one. There are mainly two different technical routes to eliminate the impacts of IP address change on application session continuity, the first one is keeping IP address unchanged during movement of host; the second one is allowing IP address change to happen and then using other methods to make the application session correctly finished, here are some examples of these methods:

(1) Deal with IP address change in process of a session Mobility

support could be provided by application layer or transport layer. When IP address change happens, specific signaling of application layer or transport layer could be used to add new IP address to the session and at the same time removing old IP address from the session.

(2) Restart a new session If there is no specific application layer signaling to deal with the change of IP address, the application could choose to restart a session when it finds the previous session failed. This method would only be used for short-lived session, e.g. DNS query/response session. Although, as discussed above, there are methods to cope with IP address change for application session, but from application's perspective, all these methods will bring in certain amount of "cost", and may import other negative impacts, e.g. signaling latency, packet losing, TCP slow start etc, in order to deal with the impact of IP address change. So we have to say that, all application sessions prefer to not change their IP address, the reason why they provide mechanisms to deal with IP address change is they have to do that, but not they willing to do that.

Another issue is that if application wants to make their traffic pass through an optimal path between MN and CN, it has to use an IP address anchored on the optimal path. So in order to get an overall good performance for application, there should be a tradeoff on whether to use a new IP address or not.

2.2 Address Management model

This sub-section provides a detailed description of suggested address

management model to satisfy the requirement of analysis result in sub-section 2.1.

2.2.1 Design Principles

The following are some design principles considered in design process of the address management model:

P1. Network SHOULD provide IP address consistency during the whole session lifetime for application that cannot bear IP address change.

P2. Providing opportunity for application session to use the new IP address after mobile node handover to a new anchor, but in order to limit IP address change frequency, application session SHOULD NOT changes its IP address each time after handover to a new anchor.

P3. Less IP addresses maintained by mobile node is preferred.

P4. Less requirements on mobile node side is preferred.

2.2.2 Anchor Deployment

Anchors are deployed in a distributed manner, and each one could assign its own prefix to mobile node.

Home anchor: A prefix's home anchor refers to the anchor which the prefix belongs to.

Foreign anchor: A prefix's foreign anchor refers to all of the other anchors that are not home anchor.

Current anchor: The anchor that mobile node currently attaches to.

2.2.3 Prefix Category

There are two kinds of prefixes: stable prefix and temporary prefix. DMM network will provide mobility support for both of these two kinds of prefix.

Stable prefix: Assigned by its home anchor, when mobile node hands over to a foreign anchor the stable prefix will be maintained by foreign anchors as long as the prefix is still being used by

application.

Temporary prefix: Assigned by its home anchor, temporary prefix usually has different valid lifetime values in home anchor's network and in foreign anchor's network (more shorter in foreign anchor's network), a foreign anchor only provide mobility support for temporary prefix for a specific period of time after which the temporary prefix will become invalid. In DMM domain, the anchors could set the valid lifetime of other anchors' temporary prefix to a predefined value.

Each anchor maintains at least one stable prefix and one temporary prefix for mobile node.

2.2.4 Anchor Action

Anchor advertises its own stable prefix and temporary prefix to the mobile node, and sets them as preferred prefix. If mobile node is hands over to current anchor from a previous anchor if prefix(es) of previous anchor is still used by application session of mobile node, then the current anchor will also advertise these prefixes from previous anchor, but set them as deprecated prefix. Current anchor sets valid lifetime value of temporary prefix of previous anchor to a specific value after which the prefix becomes invalid. When the cost of using previous temporary prefix is beyond a certain threshold (e.g. current anchor is certain hops away from home anchor), current

anchor could choose not advertise the temporary prefix to mobile node, and this will let the application session to select a new prefix to reduce routing redundancy.

2.2.5 IP Address Release

To reduce the number of IP addresses that mobile node must maintains, and contexts that network maintains for mobile node, there should be an effective IP address release mechanism for mobile node.

Triggers that could cause IP address to be released:

(1) Prefix valid Lifetime expiration.

(2) No traffic is transported using the IP address. For example, when

mobile node hands over to a new anchor, if there is no traffic transported on previous anchors' prefixes, the prefixes will be seen as invalid in current anchor's network. But there should be a special treatment for MN's public address which can be retrieved by others through DNS (e.g. when MN is a mobile server) , public address is a kind of stable address though current anchor could set it as a deprecated address, but it should not be released even when there is not traffic using it.

(3) Mobile node explicitly signals out that it wants to release certain IP address.

3 Source Address selection

Which IP address could be selected as source address depends on what IP addresses are provided by network. Based on the address management model discussed in this document, there are some simple source address selection criteria:

(1) New communication (e.g., the opening of a new TCP connection) should use a preferred address when possible.

(2) If an existing app session could cope with IP address changes, it could choose to use temporary address from temporary prefix. In a visit network, when MN's previous temporary address becomes invalid, a new temporary address from current anchor's temporary prefix will be selected.

(3) A deprecated stable address should be used only by applications that have been using it and would have difficulty switching to another address without a service disruption.

(4) For the session which is initialized by CN, the address in the

destination address field of packet from CN will be used as source address of outgoing packets. (This is mainly for the case of using MN's public address)

4 Security Considerations

TBD.

5 IANA Considerations

No.

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.

[RFC7333] H. Chan et al., Requirements for Distributed Mobility Management, RFC 7333, August 2014.

6.2 Informative References

Authors' Addresses

Xinpeng Wei
Xin-Xi Rd. No. 3, Haidian District,
Beijing, 100095, P. R. China
E-mail: weixinpeng@huawei.com