Network Working Group A. Petrescu
Internet-Draft C. Janneteau
Intended status: Informational CEA LIST
Expires: September 8, 2011 N. Demailly
iXXi
March 7, 2011

Tunnel Type Change for Mobile IPv4 (TTC)
draft-petrescu-mip4-tuntype-change-00.txt

Abstract

The protocol Mobile IPv4 may use a number of encapsulation methods between an MN and its HA. The UDP method is used to perform NAT Traversal (if a NAT sits between MN and HA) whereas IP-in-IP method may be used if there is no NAT (CoA is a publicly routable address). Although these methods are individually specified, a mechanism for changing between one to another is not, which may lead to incoherent implementations.

This draft briefly presents the scenario of a MN performing a handover between private space (NAT) and public space (non-NAT), the implementation problem (type of tunnel can not be changed dynamically), and some potential solutions as textual modifications, better implementations, or protocol extensions.

Table of Contents

1. Requirements notation

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].

2. Introduction

Dynamically changing the type of a tunnel interface is an implementation difficulty which appeared during an experimentation of typical vehicular networks. The protocol Mobile IPv4 and extensions for traversal of NAT devices, as well as network mobility extensions are used.

In this draft we describe a scenario of a moving network in a public transportation vehicle. The vehicle successively connects to two different types of wireless access networks (WiFi and 3G+), by performing automatic handovers, without affecting the sessions run on passenger devices.

The problem arising in some existing implementations of Home Agent (not supporting dynamic change of the tunnel type) is further explained. Also, a brief analysis of RFC texts describing Mobile IPv4 and IP-in-UDP is performed, potentially giving way for a new mechanism for dynamic Tunnel Type Change to accommodate handovers between private and public space.

Several solutions are proposed to alleviate this problem. In one solution, only behaviour is modified (software implementation at MR and HA); in another, existing messages are exchanged differently (deletion prior to new registration); finally, a new message format may be proposed to solve this problem.

3. Scenario and Problem

The scenario relates to the use of Internet in vehicles of public transportation. A bus of the RATP public transportation agency of the City of Paris is equipped with special Routers and wireless access hardware. The bus offers stable WiFi access to passengers. While moving around, it successively connects to two different wireless access systems available on its trajectory: WiFi of operator Naxos (private space) and 3G+ of operator Orange (public space). The router equipment within the vehicle performs automatic handovers between these two wireless access systems, depending on coverage and signal strength. Thanks to the use of standard Mobile IP and software enhancements implemented in the Router, the connectivity events occuring on the Router are invisible to the passenger equipment; put simply, the sessions run by passengers are not affected by bus handovers.

In protocol terms, the scenario consists of a moving network changing attachment between a privately addressable IP space and a public space. We consider the co-located Care-of Address mode of Mobile IPv4 (not the Foreign Agent mode).

The moving network is managed by a Mobile Router (a kind of Mobile Node) and contains a Local Fixed Node playing the role of passenger equipment (e.g. an off-the-shelf laptop running Windows or MacOS). Although the LFN runs a typical TCP/IP stack, it does not run IP mobility software (LFN does not run Mobile IPv4). The MR runs the typical Mobile IPv4 protocol with NEMOv4 extensions.

The MR has two distinctive egress physical interfaces to connect to WiFi and to 3G+ networks respectively. The HA is placed in the Internet infrastructure and communicates with MR to establish tunnels of various types. LFN is deployed within the moving network and runs TCP/IP applications with the Correspondent Node.

The two relevant topologies for this scenario are illustrated in the following two figures. They depict a handover from public to private and from private to public, respectively.

```
             ----      /--------\      ----
            | HA |----| Internet |----| CN |
             ----      \--------/      ----    CN: Correspondent Node
                         /    \                HA: Home Agent
                        /     -----
                       /     | NAT |
                      /       -----
                     /           \
                  ----          ----
                 |SGSN|        | AR |
                  ----          ----
               3G+ |             | WiFi
           (public)               (private)

                     -------> handover

                     o  o
                 3G+ |  | WiFi
                    ------       -----         MN: Mobile Router with
                   |  MN  |     | LFN |            two egress interfaces
                    ------       -----        LFN: Local Fixed Node
                      |            |               In-vehicle
                      --------------
```

In the figure above we depict the handover from public space to private space.

```
             ----      /--------\      ----
            | HA |----| Internet |----| CN |
             ----      \--------/      ----   CN: Correspondent Node
                         /    \               HA: Home Agent
                        /      \
                      NAT       \
                      /          \
                    ----      ------
                   | AR |    | SGSN |
                    ----      ------
                WiFi |           | 3G+       private: address 10.x.y.z
           (private)               (public)  public:  90.z.u.t

                     -------> handover

                     o  o
                 WiFi|  |3G+
                    ------       -----        MN: Mobile Router with
                   |  MN  |     | LFN |           two egress interfaces
                    ------       -----       LFN: Local Fixed Node
                      |            |              In-vehicle
                      --------------
```

In this latter figure, the WiFi access offered by the Access Router is using a private address space. It uses DHCP to deliver IP Care-of Addresses which are non-routable in the Internet. On the other hand, the SGSN 3G+ wireless access offers IP addresses which are publicly routable in the Internet (public space).

Once connected on WiFi, the MR sends a Registration Request to HA indicating establishment of tunnel type encapsulation UDP (alternatively, the HA may detect the presence of NAT by simply comparing addresses in the RegReq message). To satisfy this request, the HA establishes a virtual interface whose type is IP-in-UDP, such that to ease the traversal of the intermediary NAT. Then, connecting on 3G+ provokes the MR to send a RegReq to HA, but this time demanding an encapsulation of type IP-in-IP (because if NAT is not present, the UDP encapsulation is not necessary).

The problem stems from the impossibility of the HA to dynamically change the encapsulation type of a virtual interface which is already established. Hence, the HA is not able to re-use the previously established tunnel and a new virtual interface needs to be established.

In practice (with some HA software implementation), this leads to HA not constructing the IP-in-IP virtual interface, or to build successively several interfaces for the same Home Address (whereas only one is needed). In other variations, the MR uses one single type of encapsulation which may encompass most types of access networks: e.g. it may righteously use IP-in-UDP encapsulation on private access networks and, unnecessarily, on public access networks as well. This constant use of IP-in-UDP encapsulation works ok on public space as well, but involves the use of additional bytes in the headers (compared to IP-in-IP) even though UDP is not needed on non-NAT networks.

In the reverse scenario, it is considered that the MR performs a handover from public space to private space (from 3G+ to WiFi, in other words from non-NAT to NAT). In this case, if there is no change in the type of tunnel - use IP-in-UDP - then the ongoing session may be interrupted.

In specification, when reading RFC5944 "Mobile IPv4", it is not clear whether or not the MN is allowed to request dynamically changing the type of a tunnel, once a registration is already present at the HA. The document does allow the use of various types of encapsulation (presumably when no registration present), but it is not clear whether a change in type is allowed, or forbidden, once a registration is already in place. Besides, RFC5944 does not specify the use of IP-in-UDP.

Encapsulation of type IP-in-UDP for NAT Traversal when using Mobile IP is described in RFC3519 "Mobile IP Traversal of Network Address Translation (NAT) Devices". This document focuses on the use of Mobile IP in domains exclusively using NAT. The document does mention the use of IP-in-UDP "when appropriate" which makes think that IP-in-UDP may be used alternatively (in a dynamic manner) with IP-in-IP encapsulation.

For example, RFC3519 states that: "When using simultaneous bindings, each binding may have a different type (i.e., UDP tunnelling bindings may be mixed with non-UDP tunnelling bindings)."

This may be interpreted as that the intention of RFC3519 is for HA to maintain simultaneously multiple tunnels for a unique Home Address (for example an IP-in-IP tunnel and a IP-in-UDP tunnel). If done, in some implementation, this leads to a difficulty of the forwarding algorithm to choose the outgoing interface, because the distinctive factor (Home Address) is the same for the two interfaces.

In another part of the document RFC3519, it is specified that the HA should decline a request to register IP-in-UDP tunnelling when the RegReq’s addresses match, unless MR uses the F(orce) flag (section 4.6, page 18). This behaviour may lead to a behaviour where the MR needs to re-require a registration (IP-in-IP this time) or, worse, insists on requesting IP-in-UDP although not behind NAT,

This is illustrated in the following message exchange diagram. Initially, the MR is connected on WiFi in private space, and performs a handover to 3G+ public space.

```
    MR                           HA
     |                           |
     |      RegReq UDP           |
     |-------------------------->|
     |      RegRep UDP           |
     |<--------------------------|
     |                           |
   --+- - - - - - - - - - - - - -+- Handover
     |                           |
     |     RegReq UDP            |
     |-------------------------->|
     |     RegRep Decline        |
     |<--------------------------|
     |?                          |
     |       RegReq IP-IP        |
     |-------------------------->|
     |       RegRep IP-IP        |
     |<--------------------------|
     |                           |
```

By RFC3519, the HA declines the request because it realizes MR is not really behind a NAT (the CoA and src addresses in RegReq match). However, it has no means to indicate to MR the reason of this declination. The only error code is "64 reason unspecified". Upon reception of this message, the MR is not able to decide whether the reason may be a memory exhaustion on HA, wrong security, or simply refusal to build IP-in-UDP when not behind NAT. Hence, it is difficult for MR to take appropriate action.

4. Solutions as Specification and Implementation Changes

It is possible that the specifications of Mobile IPv4 and NAT Traversal to be improved. It may be possible to be more precise in the textual descriptions to cover cases of handover from public to private addressing space. For example, one would specify that the HA stores the current type of a tunnel, receives a RegReq, compares the tunnel type received to the current, and if change is needed then the current tunnel is deleted and a new one is built.

It is also possible that implementation behaviours on HA and MR are simply rendered more intelligent. They can implement this behaviour (dynamically change the tunnel type) without needing any new bit in the message formats, hence no protocol extensions.

5. Trivial Protocol Solution

Protocol solutions include new uses of existing messages, or the addition of new bits in existing message formats and suggest new protocol behaviour upon reception of these new bits or when generating them.

A trivial solution to address this problem is to request deletion prior to constructing a tunnel of type different than the existing. This means that the MR must detect the change in access (from private to public, or vice-versa) and first send a Registration Request which demands a de-registration of the current binding Home Address - Care-of Address. It then immediately sends a Registration Request for the creation of a new binding, with the new tunnel type.

This solution has been tested successfully with an HA implementation which exhibited the said problem of changing the tunnel type.

In the following figure we illustrate a message exchange showing first a Registration Request with type UDP when the MR is attached on private space WiFi, followed by a de-registration, and then by a new Registration with tunnel type IP-in-IP.

```
        MN                           HA
         |                           |
         |      RegReq UDP           |
         |-------------------------->|
         |      RegRep UDP           |
         |<--------------------------|
         |                           |
         |                           |
       --+- - - - - - - - - - - - - -+- Handover
         |                           |
         |     RegReq UDP delete     |
         |-------------------------->|
         |     RegRep UDP            |
         |<--------------------------|
         |                           |
         |       RegReq IP-IP        |
         |-------------------------->|
         |       RegRep IP-IP        |
         |<--------------------------|
         |                           |
```

6. Tunnel Type Change

A more advanced mechanism - Tunnel Type Change - consists in defining new options in the Registration Request indicating that this is a type-changing registration (the type of the tunnel must change), as illustrated in the following figure:

```
          MN                          HA
           |                          |
           |       RegReq UDP         |
           |------------------------->|
           |       RegRep UDP         |
           |<-------------------------|
           |                          |
           |                          |
         --+- - - - - - - - - - - - - +- Handover
           |                          |
           |     RegReq TTC IP-IP     |
           |------------------------->|
           |     RegRep TTC IP-IP     |
           |<-------------------------|
           |                          |
```

This message exchange is obviously shorter than the trivial mechanism presented in the previous section.

This method requires extensions to the HA software: the HA would have to be able to interpret new fields in the RegReq message and eventually generate new reply codes. If we allow modifications to be performed on the HA (assume a software implementation effort), then it is reasonable to assume that easier implementation would be to modify locally the HA (instead of generating new kinds of messages): maintain local logic triggering a deletion followed by creation of a new tunnel. It is a subject of further investigation to balance the trade-offs between local implementation and message extension.

7. Security Considerations

The SPI used for protecting Registration Request could be used for protecting also the same message extended for Tunnel Type Change.

8. Acknowledgements

The experimentations were performed during the project SEAMLESS funded by ANR (Agence Nationale pour la Recherche) of France, lasting between 2008 and 2011. The bus vehicle was kindly provided by Regie Autonome des Transports Parisiens (RATP - leader mondial pour le transport public) for several test sorties between September 2010 and January 2011. The 3G+ access by Orange was a typically billed data subscription whereas the WiFi access was kindly provided by Naxos for test purposes.

9. Normative References

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

Authors' Addresses

Alexandru Petrescu
CEA LIST
Communicating Systems Laboratory, Point Courrier 94
Gif-sur-Yvette,   F-91191
France

Phone: +33 169089223
Email: alexandru.petrescu@cea.fr

Christophe Janneteau
CEA LIST
Communicating Systems Laboratory, Point Courrier 94
Gif-sur-Yvette,   F-91191
France

Phone: +33 169089182
Email: christophe.janneteau@cea.fr

Nicolas Demailly
iXXi
1 Avenue Montaigne, Immeuble Central 4
Noisy-le-Grand F-93160
France

Email: nicolas.demailly@ixxi.biz