Mobility in IPv6

Bruno Maia, João Miranda
Faculdade de Engenharia
Universidade do Porto

I. Abstract

This paper deals with mobility related issues in the upcoming version 6 of the IP protocol. Aiming at better understanding the enhancements for mobility support implemented in IPv6, a test setting was implemented with several mobility scenarios. The analysis focused on describing the protocol inner-works and comparison with current mobility support in IPv4.

II. Introduction

IPv6 represents a real turning point for mobile computing. In fact, because IPv6 has been completely redesigned, since its conception it has foreseen the need to effectively support mobile computing and has not been bound, in the choice of solutions, by requirements of compatibility with past versions. A growing number of Internet users don't work at their office desks anymore but work while traveling. Clearly, the requirement to provide support for mobility in IPv6 is a matter of primary importance.

A. Overview of Mobile IPv6

Mobile IPv6 requires the exchange of additional information. All new messages used in Mobile IPv6 are defined as IPv6 Destination Options. The Options are used in IPv6 to carry additional information that needs to be examined only by a packet's destination node.
The following four new Destination Options are defined in Mobile IPv6:

- Binding Update – this option is used by a mobile node (MN) to inform its home agent (HA) or any other correspondent node (CN) about its current care-of-address (COA).
- Binding Acknowledgment – this option is used to acknowledge the receipt of a Binding Update, if an acknowledgement was requested.
- Binding Request – this option is used by any node to request a MN to send a Binding Update with the current COA.
- Home Address – this option is used in a packet sent by a MN to inform the receiver of this packet about the MN home address. If a packet with the Home Address option is authenticated then the Home Address option must also be covered by this authentication.

The Mobile IPv6 specification describes the protocol in terms of the following three conceptual data structures:

- Binding Cache – every IPv6 node has a Binding Cache which is used to hold the bindings for other nodes. If a node receives a Binding Update, it will add this binding to its Binding Cache. Every time when sending a packet, the Binding Cache is searched for an entry. In case there is an entry the packet is sent to COA of the CN using a routing header.
- Binding Update List – every MN has this data structure which is used to store information about each Binding Update sent by this MN for which the lifetime has not yet expired. It contains all Binding Updates sent to any (mobile or stationary) CNs and to its HA.
- Home Agents List – for each home link a node serves as HA it generates a list, which contains information about all other home agents on this link. The information in this list is learned from unsolicited multicast Router Advertisements, which are sent by all home agents, and which have the home agent bit set if the sender serves as HA on that link. The information about all other home agents is used by the Dynamic Home Agent Discovery mechanism.

B. Mobile IPv6 Operation

The mechanisms of Mobile IPv6 will be explained using the scenario shown in Figure 1. This scenario shows three links and three systems. On link A resides a router which offers home agent service. This link is also the home link of a MN. This MN has just moved from link A to link B. Additionally there is CN link C. This node may be mobile or stationary.

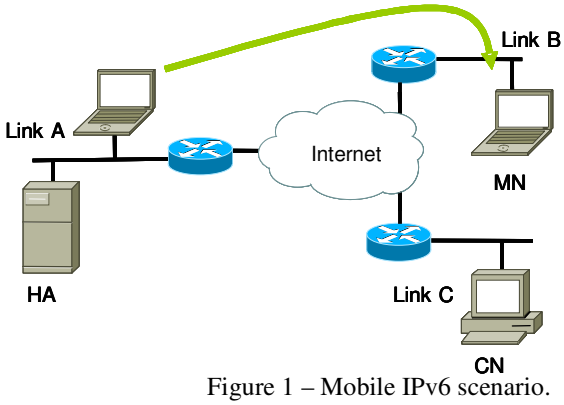

Figure 1 – Mobile IPv6 scenario.

Home Agent Registration

As soon as a MN detects that it has moved from one link to another and it has discovered a new default router (by monitoring Router Advertisement or sending Routing Solicitation messages), a MN performs (stateful or stateless) address autoconfiguration. It uses this new formed address as its COA. The prefix of this COA is the prefix of the link being visited by the mobile node. All packets addressed to this COA will reach the MN on the current link. The mobile node registers its COA with its HA on the home link. Therefore the MN send a packet to its HA containing a "Binding Update" destination option. The HA registers this binding and returns a packet with a "Binding Acknowledgement" destination option to the MN.

Triangle Routing

Now the HA intercepts any packets addressed to the MN's home address. Therefore it uses proxy Neighbour Discovery. Proxy Neighbour Discovery means that the HA multicasts a Neighbour Advertisement onto the home link on behalf of the MN. This advertises the HA own link layer address for the MN home address. The HA replies Neighbour Solicitations on behalf of the MN. Each intercepted packet is tunnelled to the registered COA of the MN using IPv6 encapsulation. If the MN sends packets to any other node, it sends packets directly to the destination. The mobile node sets the source address of this packet to the COA and includes a "Home Address" destination option. Because the home address is static, this allows every CN the transparent use of the COA. If a MN communicates with a CN while being away from home, packets are routed from the CN to the HA, from the HA to the MN and from the MN to the CN. This routing is called Triangle Routing.

Route Optimization

To avoid triangle routing a MN can send Binding Updates to any CN. This allows IPv6 CN to cache the current COA and send packets directly to a mobile node. Any IPv6 node sending a packet first checks its Binding Cache for this destination address. If there is an entry, it will send the packet to the mobile node using a routing header (rather than IPv6 encapsulation). The route specified by this routing header has two hops. The first is the COA and the second is the home address of the MN. This results in the packet being directly sent to the COA of the MN. The MN receives this packet and forwards it internally (through the loop back interface) to the next hop specified in the routing header. The next hop is the home address of the MN, therefore this packet will be "looped back" inside the mobile node. Afterwards the packet will be processed in the same way as if the MN was at home. If the Binding Cache has no entry, this packet will be sent normally. Then this packet is routed to the specified network and received by the CN. In case the CN is a mobile node which is away from home, this packet will be intercepted by the HA on the home link and tunnelled to the MN. MNs can detect when a CN has no Binding Cache entry for its COA by noticing the packet tunnelled from the HA coming from this CN. It can now send a Binding Update in response to this CN, optimizing this route.

III. Simulation

A. *Scenario*

Simulation scenario was set as described in figure 2. Some changes were introduced to the setting specified as only two MNs were used. Addressing was not subject to change. Nodes' network points of attachment were occasionally changed so as to allow packet logging at the hubs using promiscuous mode probing nodes.

Ethereal and *libcap* were used to analyze and capture traffic. Mobility scenarios tested are described by green arrows which indicate the different roaming movements performed.

Central router was already configured, IPv6 enabled and running the radvd, which was set to advertise in all interfaces and the router was set not to act as a HA.

Ethernet switches shown were actually two VLANs in the same switch.

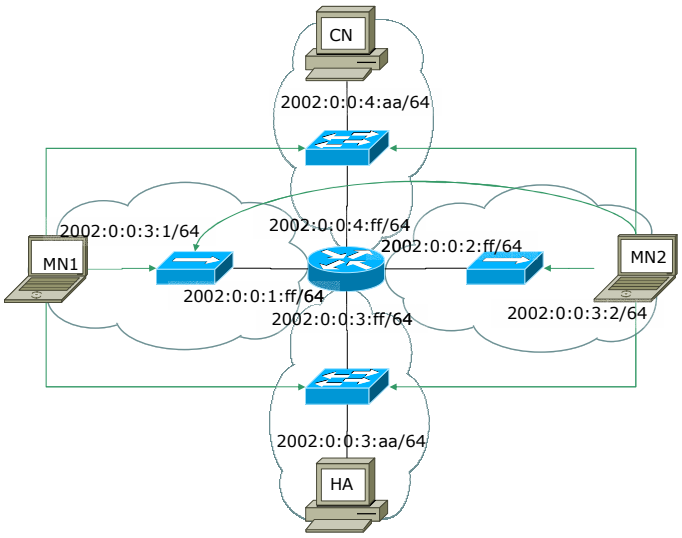

Figure 2 – Simulation scenario.

MIPL Mobile IPv6 package was already installed and preconfigured in all nodes which were IPv6 enabled. Configuration was pretty straightforward, only addresses and type of node had to be changed. Minimum and maximum default values for number of free tunnels were used (6 and 9). Unicast traffic for link-local addresses was set to be tunnelled in both the HA and the MNs.

Interfaces' addresses and routing tables were configured in all nodes using the scripts provided. MIPL package was started via *init.d* script, which inserts the MIPL module in the kernel. *mipdiag* tool was used to checks status – binding cache, binding cache, binding update list and MN information (COA and HA addresses). All data logged with *mipdiag used in a script*, ethereal and *ping6* is included in annex 1.

We focused our analysis in understanding the Mobile IPv6 messages being exchanged so as to be able to accurately describe the process. Round-trip times were measured using *ping6* but won't be presented in this report as they were pretty constant, whatever the location of the MN. Changes introduced were more accountable to using hubs then to the slight overhead introduced by the Destination and Routing Headers. As MIPv6 allows Route Optimization and only rarely tunnels traffic, overhead induced and extra hops path will not, in our opinion, be matters of concern. *Traceroute6* data isn't referred due to inconsistent behaviour and difficulty by the authors in interpreting its results – rather different from the IPv4 corresponding tool. This fault was overtaken since all traffic could be analyzed in detail with *Ethereal.*

B. Roaming tests

MN from home to foreign network and back

This scenario was intended to test connectivity while ICMPv6 Echo Request/Reply traffic was being exchanged between MN and the CN. Roundtrip times were gathered, no notable delays were noticed besides that expected by changing from switch to hub (full-duplex collision free to half-duplex with contention). Roaming procedure was very smooth, with fast automatic address configuration and Binding Updates.

Traffic was logged using *Ethereal* only on the MN. Later the same scenario was performed again with one node acting as an *Ethereal* probe, logging traffic in the Home Network – the point was to log ICMPv6 Proxy Neighbour Advertisement messages (sent by the HA when the MN leaves its home network) and Neighbour Advertisement messages with the Override flag set (sent by the MN when it arrives at its home network), ICMPv6 Router Advertisements from the HA and eventually tunnelled packets from the HA or from the MN in reverse tunnelling.

Some unexpected ICMPv6 redirect messages were also logged. These appeared to be ICMPv6 messages (echo reply/request and mobility related). They came from the HA and indicated the next-hop address (target address) to be the home network router (2000:0:0:3:ff/64). Though, some of the messages were sent while the MN was still in the home network, which is rather strange as it seems the MN was using the HA as its next-hop towards the CN, without tunnelling. The authors couldn't find any good explanation to this behaviour, as the MN had a valid route to the CN in its routing table and HA's Router Advertisement hadn't the Router Address flag set.

MN between two foreign networks, including the CN's network, and back home

In this test we were able to check the mobile's response in roaming between different foreign networks, once again while ICMPv6 Echo Request/Reply was being exchanged with CN. Roam timing, Binding Update and Neighbour Discovery messages, Return Routability procedure and roundtrip times were logged. Special attention focused on understanding the Return Routability procedure (Home and Care of Test messages were analyzed). This provides a mean to check the validity of the MN's COA and to build a 'security association' between the MN and the CN allowing the exchange of 'authenticated' Binding Update messages. Mobility

detection via Router Advertisement/Solicitation messages proved effective in detecting the roaming swiftly.

Both MNs roaming while exchanging ICMPv6 Echo Request/Reply messages

This is perhaps the most demanding scenario in what concerns mobility, as both nodes act at the same time as CN and MN. Special focus was taken on the IPv6 header and extension headers (both Destination and Routing are used at the same time) and the protocol reliability in frequent roaming movements. With both MNs in foreign networks, packets exchanged carry only COA address in the IPv6 header, the routing extension header bears the corresponding MN home address and the destination options extension header bears the sender MN home address. Binding Updates also double in number.

Although demanding, this test posed no such threat for MIPv6, no noticeable delays induced in roaming even when performed simultaneous. Only two nodes were being used, though.

IV. Analysis

A. Roaming speed and reliability

MIPL IPv6 mobility implementation proved to be much faster then the previous Dynamics Mobile IPv4. Detection of roaming to foreign networks was very fast, almost unnoticed in *ping6* reports (only a few packets lost). Home network detection was also very satisfactory. Both performed much better than Dynamics' Hierarchical IPv4 and probably with some L2 hint would be sufficient for cellular mobility in WLANs.

Protocol reliability is much improved compared to Dynamics, although MIPL sometimes mysteriously stopped altogether and only restarting (removing and inserting the module again via the *init.d* script provided) would get things back on track. This seemed to be related to frequent network changes, perhaps causing the Return Routability procedure to fail. However, during roaming operations, usually only some (5 to 10) packets got lost (especially due to the Routing Extension with the MN's home address and ICMPv6 processing by the HA when messages cannot reach the MN).

B. Overhead and trough output

IPv6 introduces considerable overhead due to the much larger addresses, though it cunningly reduces it in usual traffic as most of the options in the IPv4 header were stripped down to optional headers in IPv6. Mobile IPv6 uses at least one of these optional headers – destination options and/or routing. However the impact of this somewhat larger overhead wasn't noticed, in comparison to MIPv4. Perhaps because, even without this large addresses, MIPV4 had to tunnel (IP on IP was used) at least half of the traffic.

Through output was considerable improved by several features in IPv6. As IPv6 rarely uses tunnelling, extra node processing at the HA is eliminated. Route optimization is possible with every IPv6 node - no more persistent triangle routing. There is no FA, no processing or decapsulation (if selected) at this extra node – no registration either.

C. Security

This simulation didn't focus on security and certainly no attack was carried out. However by studying the protocol security mechanisms, the major improvements to IPv4 become clear. All Mobility messages are now authenticated (IPSec AH), some of them (between HA and MN) can even be encrypted (IPSec ESP). Even a mechanism – Return Routability – was conveyed to verify Care-of Addresses and allow security associations between MN and the CNs receiving Binding Updates. Of course, many of these improvements are also due to the much welcomed mandatory support of IPSec in IPv6. One key aspect to mention is, although safe it is not at all cumbersome, no security configurations were left to the user in this mode.

V. Conclusion

IPv6 is indeed a very powerful protocol and a trustworthy successor of IPv4. In this small test we were able to realise its potential from address and route autoconfiguration, mobility support and security features. Sometimes, IPv6 nodes started to talk to each other as soon as we plugged them, only via their auto-configured link-local addresses.

The authors hope all this IPv6's paraphernalia speeds up its real world deployment as the benefits clearly outweigh the difficulties engaged at a replacing a very large IPv4 infrastructure and know-how.

Future MIPv6 will certainly benefit a lot from early implementations like MIPL's and when integrated with L2 technologies might present themselves as good alternatives to conventional cellular communications systems, whether they are based on UMTS (3GPPP2 and accepted by ETSI) or WLAN.

VI. References

[1] Deering, Hinden, Internet Protocol, Version 6 (IPv6) Specification, RFC2460, IETF

[2] Arkko, Johnson, Perkins, Mobility Support in IPv6, draft-ietf-mobileip-ipv6-21.txt Internet Draft – work in progress

[3] William Stallings, IPv6: The New Internet Protocol

[4] Johnson, Perkins Mobility Support in IPv6, 1996

[5] Manuel Ricardo, IPv6, Comunicações Móveis, DEEC, FEUP, 2003

[6] Manuel Ricardo, IP móvel v6, Comunicações Móveis, DEEC, FEUP, 2003