Transparent Mobility in Mobile IPv6: An experience report

Author: Rodolfo Kohn, Senior Software Engineer at Motorola, Global Software Group in Argentina. rodolfo.kohn@motorola.com

Topics: Distributed Systems – Communications and Networks.

Workshop: Distributed and Parallel Processing.

Abstract

The publication of Mobile IPv6 RFC 3775 by the IETF is a breakthrough in the data communications industry to achieve the technology convergence required by ubiquitous mobile devices. MIPv6 not only brings the possibility of innovative distributed applications and services for mobile devices but also allows a transparent use of existing distributed applications even when they have been designed and developed for non-mobile platforms. This work document describes the experience gained by testing a chat application for IPv6 [3], designed and developed for a desktop computer, on a mobile device running Mobile IPv6. The description is focused on the fundamentals of the transparent mobility property: during the tests, the device was moving from one network to a different one without affecting the applications' TCP connections.

Introduction

The availability of wireless technologies yielded new distributed applications involving highly mobile devices such as cell phones, PDA's, badges, wireless sensors and various forms of robots. A major hinder for these technologies can be identified though: while a data service is being used, a device can move only as long as it remains attached to the same link-layer technology, and in most cases to the same network, unless some application-layer solution is provided. To improve mobility among heterogeneous access networks, the necessity of technology convergence appears and is addressed by different types of solutions. This necessity is tackled by the Cooperative Network working group (CoNet) of the Wireless World Research Forum (WWRF) in its envisaged Beyond-3G systems [14].

Mobile IP is a home-based solution [1] for mobile devices. It lets a device roam over different networks, possibly involving different technologies, in a transparent way to the upper-layer protocols and applications. Among other possibilities, this would permit a cell phone connected to a GPRS network switch to an 802.11 home network and from there to the local Internet connection while all established IP connections are maintained.

Highly mobile devices usually have low cost and powerful processors with the capacity of running sophisticated applications at the lowest possible price. The availability of Mobile IP in these devices adds a wide range of services that could not be imagined otherwise and opens the way to new concepts in the telecommunications market. However, in a world with every small device connected to the Internet and the capability of establishing end-to-end peer communications, the large address space of IPv6 [3] turns out to be a primary necessity.

Since mobility is entirely managed at the network layer, it is transparent for transport and applications layers. This allows running the already existing distributed applications using BSD sockets and IPv6 in mobile devices with no porting costs. This paper describes how this is possible based on the work and experience realized in [12].

An IPv6 Internet should not be a surprise at this moment. Currently a number of organizations worldwide are preparing the field for an organized deployment of IPv6 [3]. In many countries IPv6 tests are being carried out with vendors and service providers. According to [13] the Department of Defense of United States has announced plans to migrate its existing Global Information Grid Network to IPv6 by 2008. Having an IPv6 Internet there is only one step to Mobile IPv6 and consequently these new purportedly innovative applications and services will be possible. Many applications will be ported from IPv4 to IPv6. Furthermore, the interest to port IPv6 applications to mobile environments will arise.

Mobile IPv6

Mobile IP is a protocol specified by the IETF Network Working Group in the RFC 3344 [9]. It brings up a mobility solution based on the IPv4 protocol. Mobile IPv6 is a protocol published by the Internet Engineering Task Force (IETF) in the RFC 3775 [2].

Mobile IPv6 allows nodes to roam throughout the IPv6 Internet while still reachable by any other node.

An IP address identifies not only a node interface but also the network the interface is attached to. Usually, if a node attaches to a different network it will have to change its IP address, otherwise it will not be able to receive any datagram delivered to it from another network and probably also in the same network. Ingress filtering is another hinder when it comes to send a datagram to a node in a different network. As an alternative, host-specific routes can be propagated by the routers throughout the Internet but this is not a scalable solution.

Besides, other hinders appear regarding host location:

- The host cannot be accessed by another host that knows its old address and any datagram sent outside the current network could be dropped by some router.
- When the host is in a foreign network, any DNS server storing the host address must be updated and every cache entry for this host throughout Internet must be removed before the host can be accessed.

Last but not least, if the host moves from one network to the other, any existing connection that is based on the IP address, like a TCP connection, will be broken.

Mobile IPv6 has been designed to bring mobility capability to an Internet connected host. In MIPv6 the following principal elements can be identified:

- Mobile Node (MN): the node that is capable of moving away from the home network.
- Home Agent (HA): router that has location information for a mobile node that is away from home and tunnels any datagram received in the home network to the mobile node.
- Correspondent Node (CN): a node communicating with the MN.

Every node has a fixed IPv6 address, called home address, by which it can be identified. It is the identifier.

In the typical scenario when a MN is visiting a foreign network it listens to the Router Advertisements [4] sent out by the routers attached to the same link, it detects that it is away from the home network and, using stateless address auto-configuration [5], it forms its own care-of address stemmed from its hardware address and a network prefix advertised by the routers (stateful address auto-configuration is also possible). After checking the new auto-configured address is unique in the link to which it is attached, the device sends a Binding Update (BU) to its Home Agent which in turn updates its binding cache in order to maintain the new locator, the care-of address. The MN also sends BU's to any CN which has an entry for the MN in its binding cache. When a node sends out a datagram destined to a MN that is away from home, the datagram is routed to its home address; there, the HA, acting as a proxy for the MN, intercepts the datagram and

obtains the current care-of address – the locator - of the MN from its binding cache, then it tunnels the datagram directly to the MN which de-tunnels it at the IP layer and passes it to the higher layers. This process is depicted in Figure 1 by lines blue and red.

In Mobile IPv6 the MN can communicate with a CN in two different modes: Bidirectional Tunneling –line red in Figure 1 - and Route Optimization (if the CN supports Mobile IPv6) – line magenta in Figure 1 -. With route optimization the shortest communication path can be used.

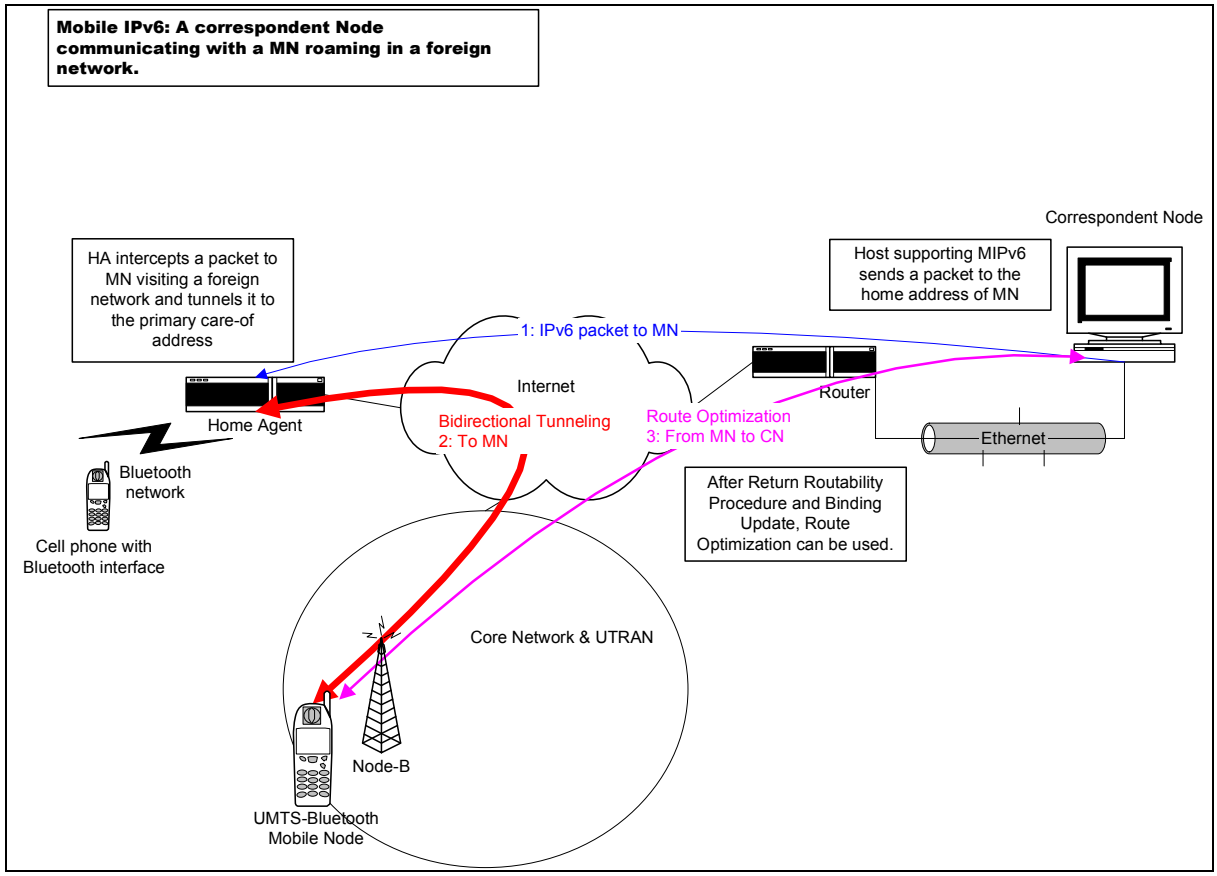

Figure 1 - Typical MIPv6 scenario

While the IPv6 home address is the identifier of the node's interface, its care-of address is the locator used to reach a node wherever it is attached to the Internet. The node's identifier can be

obtained from a names service given a human friendly name, as in DNS while Mobile IPv6 provides the location service providing the current primary care-of address given the identifier.

After the MN has been located, datagram exchange can be performed with bidirectional tunneling, Mobile IP in IPv4, or with Route Optimization, available in Mobile IPv6.

The way a MN detects it has moved to other network is by listening to Router Advertisement sent out by routers and HA's. The ICMPv6 Router Advertisement is extended to include Mobility Agent Advertisement information and possibly a Prefix-Length extension.

L3 Handover is defined by [2] as the process by which a node detects a change in the on-link subnet prefix, possibly because of a change of the subnet to which it is attached, this requires a change in the care-of address and consequently the sending of binding updates to the HA and the CN's. L2 Handover is the process by which the mobile node changes from one link-layer connection to another [2]. An L2 Handover can be a horizontal handover when the same interface is used and the link-layer connection changes or a vertical handover when the interface changes, for example when a device moves from a connection to a GPRS radio access network to a WLAN 802.11 connection. A vertical handover usually implies an L3 handover.

After the MN's having detected it is at a new network and having obtained the new care-of address, it must send a Binding Update to the HA to update the primary care-of address. A security association is maintained between the MN and the HA. Once this process is finished, the MN whether to send BU's to the CN's with which it is connected with Route Optimization, in some cases it might prefer to receive datagrams from specific CN's at the old care-of address. Before updating a care-of address at the CN, a process called Return Routability must be performed for security reasons.

All mobility management is transparent for the higher layers because Mobile IPv6 does all it works at the network layer under the IP protocol. Thus, an application can run regardless of the mobile node's being at the home network or the mobile node's roaming at a visiting network: a TCP

connection towards the permanent Home Address can be maintained alive and a FTP client, for example, can download a large file while the node is roaming; also, a potentially mobile UDP server is always reachable at its Home Address.

Current Mobile IPv6 implementations

Currently a number of different Mobile IPv6 implementations are available:

- Livsix, an open source implementation for Linux. It has been ported to a number of different platforms. The author has ported LIVSIX to the microprocessor ColdFire [11] with uClinux, useful for embedded systems. http://www.enrl.motlabs.com/livsix [6][7][8][10]
- Cisco Mobile IP, for Cisco IOS, http://www.cisco.com/warp/public/732/Tech/mobile/ip
- Monarch, for FreeBSD, from Rice University http://www.monarch.cs.cmu.edu/mobile_ipv6.html
- MIPL, for Linux, from Helsinki University of Technology http://www.mipl.mediapoli.com
- Treck Inc., for embedded systems and RTOS, http://www.treck.com
- Others.

Transparent Mobility

The work described in [12], shows the advantages of LIVSIX [10] – a MIPv6 implementation – porting by the author from a Linux Desktop PC platform to a mobile platform with a small, cheap and powerful microprocessor: ColdFire M5272C3 [11] running uClinux. That document described a Testbed used to perform all the tests, shown in Figure 2. In the Testbed there is a PC acting as Home Agent in Network1 and another PC acting as Router between the home network (Network1) and a foreign network (Network2). During these tests, board EB2 was moved from Network1, the

home address, to Network2 while there was a chat session established between EB2 and EB1 along with the corresponding TCP connection. The chat application kept working and all the chat sessions were maintained normally. [12] Contains all logs from the applications and from the Ethernet frames obtained with Ethereal.

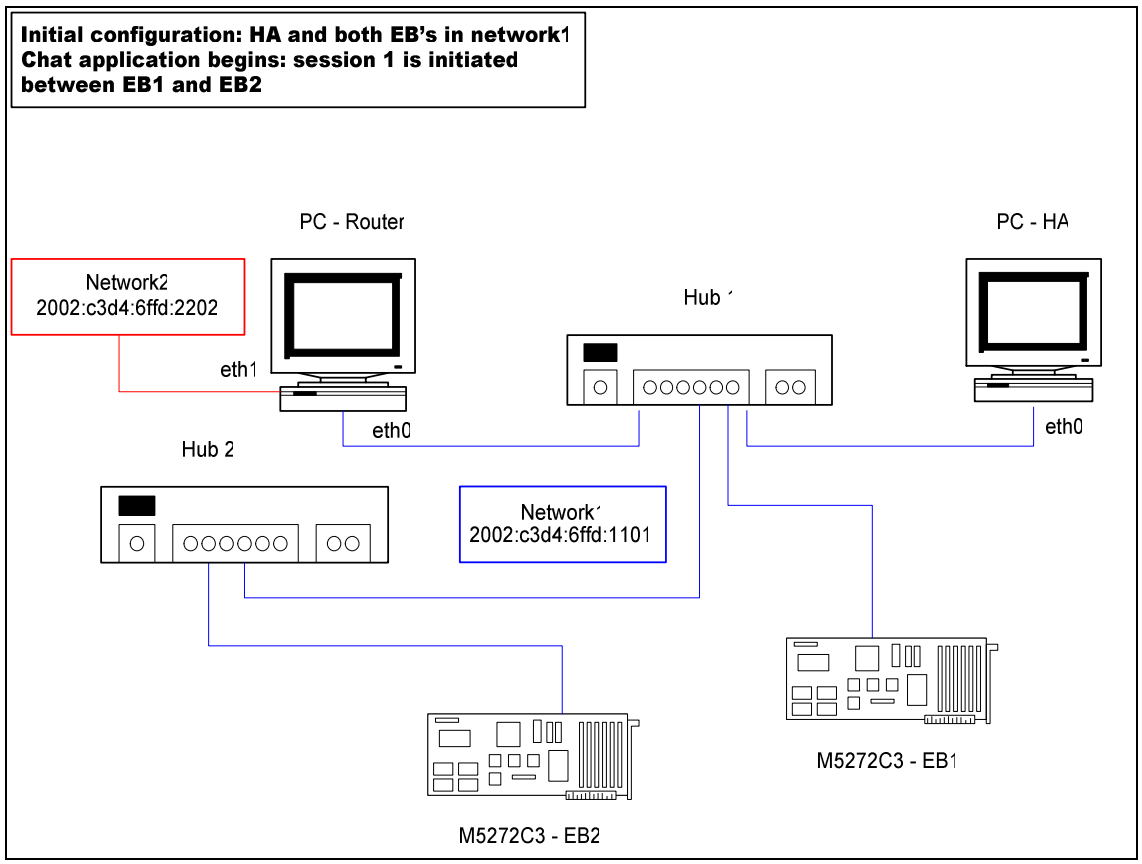

Figure 2 - Testbed

How the location service is managed in MIPv6 has already been explained, so it can be understood how a mobile node is contacted the first time and how it informs the HA that it has moved to another network in order to be reached when needed, further details can be found in [2]. Then it is necessary to explain the fact of mobility being transparent to higher layers after a connection and a session have been established. To achieve this transparency usually it is essential that, at layer four,

protocols see the same source and destination addresses they saw when a connection was established. This is the case for TCP: if any address changes, then a socket will be no longer valid and it will be closed probably as reset by peer. Regarding UDP, although a connection is not established an application might need to send a response to a UDP packet received and this response will be sent to the source address of the received packet.

In Route Optimization, addresses remain the same for upper-layer protocols due to the following reasons:

- MIPv6 adds an extension header to IPv6 called Type 2 Routing Header. This header is used in IPv6 datagrams sent from the correspondent node to the mobile node. While the IPv6 Destination Address is the MN's care-of address (locator), type 2 routing header contains the MN's home address (identifier). Thus, the datagram is directly routed to the MN. When the MN receives the datagram, it retrieves the home address from the type 2 routing header and uses it as the final destination address in the IP layer. In this way beyond the IP layer, the care-of address is not known, only the home address is managed in a received datagram.
- IPv6 defines a Destination Option extension header which contains options to be processed by the destination node. MIPv6 adds a new destination option called Home Address option. This option contains the home address of the node sending a packet so that when a correspondent node receives a datagram that uses the care-of address as the IPv6 Source Address, MIPv6 obtains the home address and the IP layer uses the home address as the Source Address. This option is used also for packets sent to the Home Agent.

In case bidirectional tunneling is used instead of route optimization, a mobile node will receive an IP packet destined to its home address inside another IP packet intended to it care-of address, MIPv6 will de-tunnel it and IPv6 layer will get the inner packet.

Thus, the source and destination addresses do not change for upper-layers.

Since the packets traveling through the networks have the correct IPv6 address they have not been dropped by the router which knew where to forward them. When route optimization is available, packets sent by the MN have the care-of address as the source address, and packets received have the care-of address as the IPv6 destination address. The same occurs in case of bidirectional tunneling.

The chat application uses BSD sockets to achieve a peer-to-peer communication with TCP. The common BSD functions for IPv6 domain sockets are used:

- `socket(AF_INET6, SOCK_STREAM, 0)`
- **connect**
- **write**
- **read**
- **bind**
- **listen**
- **accept**

Sockets are set as non-blocking since at the test time, blocking sockets were not perfectly working.

It is possible to establish a number of concurrent sessions with different nodes. During the tests, there were only two mobile nodes as shown in Figure 2, and all the sessions were established between these two nodes.

From the description above, it can be easily inferred that there is no reason for the TCP sockets to be affected, so the sessions, in the application layer, were not affected.

Conclusions

An IPv6 application can be ported from a non-mobile platform to a mobile platform running MIPv6 without any code change. This is possible because mobility is entirely managed at the network layer and it is transparent for upper-layers. The main benefit of MIPv6 is the

technology convergence. With this protocol, a mobile device, like a PDA, a mobile phone, mobile router, or a robot, will be able to roam among different link-layer networks with no need to modify the already running IPv6 applications.

It is true that the gradual transition from an IPv4 to an IPv6-Internet requires a porting cost but this cost will be afforded sooner or later. Once an application has been ported to IPv6 it will be able to run on MIPv6 with no extra cost.

Finally, it is possible to affirm that not only MIPv6 will open the opportunity to develop a wide range of innovative applications and services for ubiquitous mobile devices but it will also provide the benefits of real ubiquity to existing IPv6 applications.

References

[1] Tanenbaum A. S., Van Steen M., "Distributed Systems, Principles and Paradigms," Prentice Hall, 2002.

[2] Johnson D., Perkins C., Arkko J., "Mobility Support in IPv6," IETF RFC 3775, June 2004.

[3] Deering S., Hinden R., "Internet Protocol, Version 6 (IPv6) Specification," IETF RFC 2460, Dec. 1998.

[4] Narten T., Nordmark E., Simpson W., "Neighbor Discovery for IP Version 6 (IPv6)," IETF RFC 2461, Dec. 1998.

[5] Thomson S., Narten T., "IPv6 Stateless Address Autoconfiguration," IETF RFC 2462, Dec. 1998.

[6] Petrescu A., Riou E, "HOWTO use a LIVSIX box as a router, A guide to LIVSIX routing configuration," http://www.enrl.motlabs.com/livsix, May 2003.

[7] Petrescu A., Riou E, "IPv6 Applications over LIVSIX. A guide to the IPv6 applications which are running over LIVSIX," http://www.enrl.motlabs.com/livsix, Feb. 2003.

[8] Petrescu A., Riou E, "The LIVSIX mobility HOWTO, A detailed guide to LIVSIX mobility configuration and use http://www.enrl.motlabs.com/livsix", Jan. 2003.

[9] Perkins C., "IP Mobility Support for IPv4," IETF RFC 3344, Aug. 2002.

[10] http://www.enrl.motlabs.com/livsix

[11] 68K/ColdFire web site:

http://e-www.motorola.com/webapp/sps/site/homepage.jsp?nodeId=03M0ylgrpxN

[12] Kohn Rodolfo, "Ubiquigeneous Networking, A Distributed Networking Application Over Mobile Embedded Devices," Thesis document for Magister In Data Networks, Universidad Nacional de La Plata, http://journal.info.unlp.edu.ar/postgrado/tesis/TesisREDES.html, Dec. 2004.

[13] Bound Jim and Ladid Latif (Editors), "NAv6TF NTIA IPv6 RFC Response," http://www.nav6tf.org/documents/NAv6TF_Response_NTIA_IPv6_RFC_FINAL.pdf, March 2004.

[14] Politis, C.; Oda, T.; Dixit, S.; Schieder, A.; Lach, H.-Y.; Smirnov, M.I.; Uskela, S.; Tafazolli, R.; "Cooperative Networks for the Future Wireless World," IEEE Communications Magazine, vol.42, no.9, Sept. 2004, pp. 70-79.