A New Scheme for a Mobile Node Seamless Mobility in Mixed Networks IPv4 and IPv6 Traversing NAT Routers

Bassam Naji Al-Tamimi, Rahmat Budiarto, and Mohd Adib Omar

***Abstract*—In the mobility environment, the interoperability between IPv4 and IPv6 networks is required due to the incompatibility that occurred in the headers of both IPv4 and IPv6 protocols. It is probable that a Mobile Node (MN) moves out of its home agent's domain towards a different IP domain IPv4/IPv6. This paper proposes a new scheme for mobile nodes that are connected with the home agent which is basically located behind Network Address Translation (NAT) to allow roaming of the MN throughout the IPv6 domains. MN would be able to communicate with its home agent despite its roaming throughout the IPv6 domain. Therefore, the proposed scheme is based on Teredo tunnel that allows clients behind NAT to utilize and get IPv6 services.**

***Index Terms*—Home agent, mobile node, NAT router, teredo tunnel.**

I. Introduction

The rapid growth of the Internet in the last few years has been exposing the limitation of the address space in the current Internet protocol version 4 (IPv4) [1]. The increasing of demand and consumption of IP addresses have led to anticipated exhaustion of the IPv4 addresses. To address this concern, the new Internet protocol version 6 (IPv6) [2] has developed by the Internet Engineering Task Force (IETF) to provide sufficient address space. Although many networks have been upgrading to support IPv6, there are many networks are still supporting IPv4 [3]. Since IPv6 has not yet been widely deployed and for cost constraints, various transition mechanisms [4] that is, (Dual stack, Translation, and Tunneling) have been defined to support the interoperability between IPv4 and IPv6. In mobility environment, the interoperability is required due to the incompatibility that occurred in the headers of both IPv4 and IPv6 protocols.

Over the past several years, wireless communications technology and mobile IP have become omnipresent and attracted much attention of various Research Development Centers and business trends due to its portability feature. In addition, the current deployment of wireless technology IEEE 802.11 will finally exceed the wired Ethernet to be used in as many sectors of life as available such as airports, Internet cafes, schools, and libraries. Hence, it is imperative that mobile nodes must constantly get connected with the home agent (HA) and be able to work and coexist within any IP infrastructure domain (IPv4/IPv6).

Manuscript received October 13, 2012; revised November 16, 2012.
Bassam Naji Al-Tamimi is with Universiti Sains Malaysi (e-mail: bnaa09_nu0186@student.usm.my)

Mobile IP was defined by IETF as a standard communication protocol. It was designed to enable mobile nodes to move from one position to another while maintaining connection with their home agents and permanent IP addresses [5]. As mentioned in Request for Comments [6], [7] respectively, the mobile IPv4 (MIPv4) can move between IPv4 subnets while maintaining connectivity. A mobile IPv6 (MIPv6) can also maintain connectivity while moving within the IPv6 subnets. Nonetheless, this paper does not concentrate on this subject that the essential issue of this paper aims to deal with the term of coexistence between heterogeneous network domains. More specifically, despite the movement of the mobile node towards the IPv6 networks, it has to be connected with its HA. It is taken into consideration that the HA of the mobile node is located behind NAT [8].

In terms of the coexistence, one of the existing methods of mobile interoperability was brought by [9]. As a matter of fact, this method was applied on MPLS networks (Multiprotocol Label Switching) in order to retain the connectivity between a mobile node and its HA, as well as with a Correspondent Node (CN).

MPLS network supports the backbone solution for high-speed IP packet forwarding and enhanced scalability. In addition, the MPLS network provides Quality-of-Service for MIPv4 and MIPv6. While the initial MPLS effort was focused on IPv4, the core technology of MPLS was extended to support IPv6 protocol as in Fig. 1.

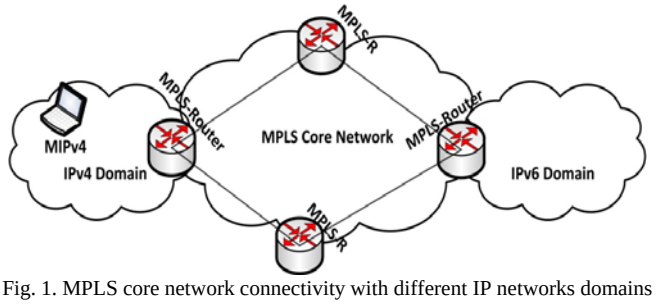

Fig. 1. MPLS core network connectivity with different IP networks domains

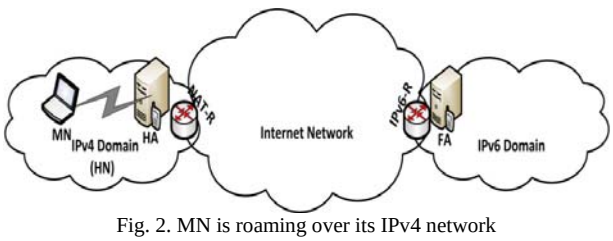

Fig. 2. MN is roaming over its IPv4 network

Nowadays, many existing IPv4 networks are still unable to support MPLS technology due to many reasons, including impossibility of upgrading all router devices to support this technology in a short time and the concern of the high cost of

MPLS routers. Moreover, it is unreasonable to restrict the movement of mobile nodes within the MPLS networks. Thus, this paper aims to realize the possibility of an mobile node movement in the IPv6 network domains, since its HA is essentially operated and attached within the IPv4 network that relies over the NAT router as elaborated in Fig. 2.

This paper mainly focuses on introducing a model that enables Mobile nodes to maintain its connectivity on the IPv6 network domain taking into account that the IPv4 home agents are located behind NAT. This paper is organized as follows. It begins with an overview of the IP Mobility support for IPv4/IPv6, Mobility over tunneling mechanism, Proposed Model, Signaling Cost and finally Conclusion.

II. IP Mobility Support for IPv4/IPv6

In [6], [7] the mobility support and its solutions have been described in details.

A. Mobile IPv4

Mobile IPv4 (MIPv4) is the most common solution for mobility on the current IPv4 Internet [6]. IETF has developed a MIPv4 to provide the Internet connectivity to mobile devices and users that are attached along with the Internet. MIPv4 introduces three functional entities: Mobile Node (MN), Home Agent (HA), and Foreign Agent (FA). The MN can change its attachment point without changing its permanent IP address (Home Address).

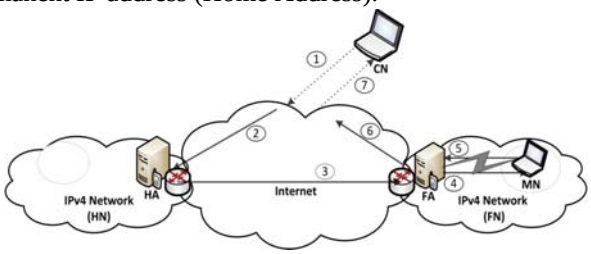

Fig. 3. The components of a Mobile IPv4 network and an MN movement

When a mobile node moves out from its home link, it receives a temporary address called Care-of Address (CoA) via the foreign agent. This CoA is not a permanent address. It has to be changed when the MN moves among different foreign networks. The MN is associated with this address to be an identified node within the visited network. In addition, it provides information regarding its attachment point.

The registration process between the MN and its HA initializes by providing the HA with a new CoA. This process is performed through two registration ways: either through a FA or directly from the MN to its HA. Through the registration request message, the HA can realize that its MN has moved to a foreign network. Hence, the HA is able to redirect all the intercepted packets that are destined to the MN via the usage of a new CoA. When a correspondent node (CN) sends packets to the MN, it will absolutely use the permanent address of the MN. These packets normally arrive to the MN's home agent. Then, it will intercept and tunnel them to the MN over the foreign network.

B. Mobile IPv6

Mobile IPv6 (MIPv6) [7] has inherited a number of features from Mobile IPv4 and offers many other improvements over Mobile IPv4.

Route optimization capability is embedded in all MIPv6 nodes rather than being added as an optional extension with MIPv4. Route optimization [10] has been proposed to provide the MN with the capability to avoid the problem which is called the triangle routing problem for any of its CNs. This problem occurs when the MN is apart from its HA. The CN will not be aware of the MN's current location. Therefore, the CN must tunnel the packets through the MN's HA in an indirect path. While the MN can tunnel the packets to the CN directly by updating a CN of a MN's new CoA using a Binding Update message (BU), a CN can forward the packets directly to a MN without the need for the HA to redirect the packets.

III. Mobility over Tunneling Mechanism

Tunneling mechanisms [4] are used to transport the packets that are related to the same type of the network layer protocol among a network that uses different types of network layer protocols. For instance, IPv6 packets can be encapsulated within the IPv4 packet and then tunnel them over the Internet (IPv4 routing infrastructure) to a distant IPv6 network, and vice versa. Obviously, the proposed method which is based on Teredo tunnel enables a HA that is located behind NAT to utilize the IPv6 services and remain reachable with the mobile nodes that are roaming over the IPv6 network domains. Since other tunnels such as 6to4 and ISTAP are typically unable to function best through the NAT router as illustrated in [10].

Moreover, with the current deployment and the rapid development of IPv6, it is extremely reasonable to assume that a mobile node could move out of its IPv4 home network that is located behind NAT to a foreign IPv6 network domain. A mobile node would not be able to retain or establish the connectivity with its HA unless the HA obtains the IPv6 address. This potentially turns out to be one of the biggest obstacles that may face the rapid deployment of Mobile IP. The tunneling must be applied to avoid such a problem as shown in Fig. 4.

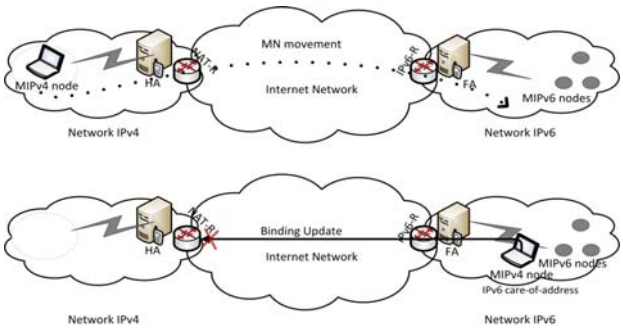

Fig. 4. Modeling the two cases

IV. The Proposed Model

This section describes the proposed model. As illustrated in Fig. 5, the proposed method architecture is mainly based on the integration of three essential elements:

1) IPv4 Network based on NAT router. MIPv4 network contains mobile node, home agent, and NAT router on its border where mobile node will in turn move to the IPv6 network.
2) IPv6 Network. It contains an IPv6 router as a FA which periodically broadcasts router advertisement messages.
3) Teredo Server. Its purpose is to provide the HA with the IPv6 address.

In short, applying this proposed method allows the mobile node to efficiently move to any IPv6 network and keep the connection with its home agent.

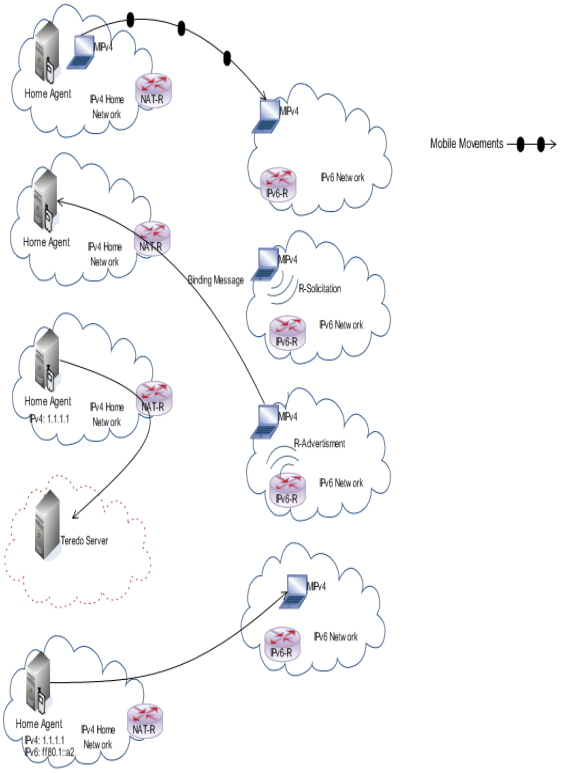

Fig. 5. The proposed model steps

V. Modification Mechanisms for a Mobile Node and a Home Agent

The modification mechanisms for a mobile node and a home agent are discussed in detail below:

A. Mechanism for a Mobile Node

In Fig. 2, the mobile node modification mechanism is illustrated when it is going to be roaming over an IPv6 network.

When a mobile node moves out from its home link, it has to send back a registration request called a Binding Update Message with MIPv6 to its HA in order to redirect and forward the intercepted packets to its current position. Fig. 6, illustrates this operation as proposed in this paper. The following steps provide further clarifications:

1) When mobile node realizes that it begins traversing away from its home network, it will start sending Router Solicitation (RS) messages.
2) Upon receiving the Router Advertisement (RA) message, it would get subjected to a prefix check to identify whether the visited network is based on IPv4 or IPv6 infrastructure.
3) In case a visited network is IPv4, the mobile node sends a binding update message to its HA in order to register its new CoA. On the other side, if a visited network is IPv6, the mobile node sends a binding update message attached with Requesting Teredo IPv6 address (BUMR-TIPv6). Consequently, the mobile node remains waiting for the acknowledgment message from its HA that contains a new Teredo IPv6 address. After that, the mobile node will maintain its connectivity with its HA until it is switched to another available network through its movement.

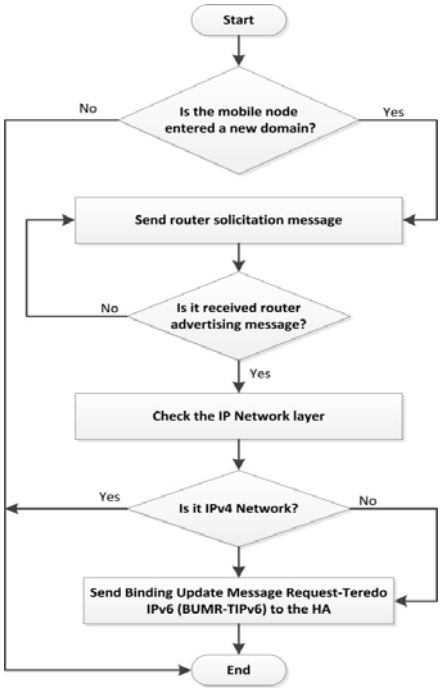

Fig. 6. Modification of MN

B. Mechanism for a Home Agent

The proposed method, shown in Fig. 7, elaborates its operational steps to be implemented in the HA that is working behind NAT. Once the HA received a BU message from its MN, the packet will be subjected to an examination process. The purpose of this process is to verify from two possibilities in terms of the MN's movement. The first possibility comprises roaming the MN within its HA network. Consequently, nothing will change since the MN remains connected within its HA over its domain. The second possibility comprises the movement of the MN away of its HA network towards either IPv4 network or IPv6 network. In case of moving towards the IPv4 network, the process will allow the MN to perform its registration between the FA and its HA in accordance to its ordinary procedure. On the other side, in terms of IPv6 network, the process will check whether the MN in the IPv6 network has already sent the BUMR-TIPv6 within its initiated requested packet or not. If the BUMR-TIPv6 is already sent, then the proposed method (algorithm) will check if the Teredo tunnel is activated or not. If it is not activated, the HA will perform the Teredo qualification procedure. Then, the process will check whether the HA is qualified to get Teredo address. If it is qualified, the HA will send RS to closest Teredo server in

order to get Teredo address, and then the HA forwards its new IPv6 address to the MN. If the HA is not qualified the MN will lose the connection with its HA until it returns to its domain.

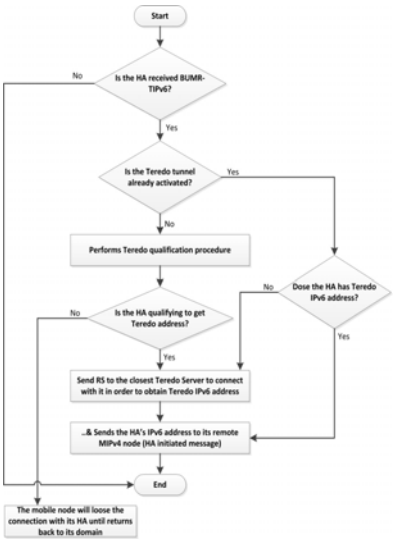

Fig. 7. Modification of HA

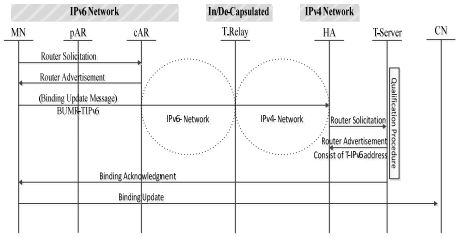

Fig. 8. Signaling procedure between the MN over an IPv6 Network and its HA

VI. Signaling Cost

This section shows the signaling procedure of our proposed scheme. Fig. 4, illustrates the signaling cost that is needed for the registration between mobile node that is roaming over an IPv6 network and its HA which is located on an IPv4 network. The Teredo relay as shown in the Fig. 8, encapsulate and decapsulate packets between IPv4 and IPv6 networks. Teredo IPv6 registration process between the HA and Teredo server increases the signaling cost but it will always happened once HA request Teredo address. When the mobile node moves in the IPv6 network then the signaling message will be increased to accomplish the binding between the mobile node and its HA. Once the Teredo tunnel of the HA is already activated then the process of Teredo binding (Qualification procedure) will not take place again.

VII. Conclusion

In this paper, we have proposed an integrated method for the mobility support. The essential issue of this paper aimed to address the concern of the coexistence between IPv4/IPv6 networks when the mobile node moves in an IPv6 network in particular. This paper has proposed two modification methods which comprise a mobile node modification method and its HA modification method. The modification of mobile node is proposed to examine the prefix of the router advertisement message and check whether a visited network is based on IPv4 or IPv6 infrastructure. As well as, it sends back a binding update message attached with BUMR-TIPv6 to its HA. The modification of HA is proposed to request IPv6 address from the Teredo server.

References

[1] *Internet Protocol: In Request for Comments RFC 791*, Internet Engineering Task Force, 1981.
[2] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," in Request for Comments RFC 2460, Internet Engineering Task Force, 1998.
[3] W. Jianping, C. Yong, L. Xing, X. Mingwei, and M. Chris, 4over6 Transit Solution Using IP Encapsulation and MP-BGP Extensions, in *Request for Comments RFC 5747*, *Tsinghua University and Cisco Systems*, Inc., March 2010.
[4] R. Gilligan and E. Nordmark, Transition Mechanisms for IPv6 Hosts and Routers, in *Request for Comments RFC 289*3, Internet Engineering Task Force, 2000.
[5] C. Perkins, "IP mobility support," in Request for Comments RFC 2002, Mobile IP Working Group, 1996.
[6] C. E. Perkins, "IP mobility support for IPv4," in Request for Comments 3220, Internet Engineering Task Force, 2002.
[7] D. Johnson, C. E. Perkins, and J. Arkko, "Mobility support in IPv6," in Request for Comments 3775, Internet Engineering Task Force, 2004.
[8] K. Egevang and P. Francis, "The IP Network Address Translator (NAT)," In RFC1631, May 1994.
[9] H. T. Cong, C. N. Ngoc, T. N. Duc, and H. T. Dinh, "Interoperability between Mobile IPv4 and Mobile IPv6 based on MPLS core network," in *Advanced Communication Technology, the 9th International Conference*, 2007.
[10] C. E. Perkins and D. B. Johnson, "Route optimization in Mobile IP," in *Internet Draft*, Internet Engineering Task Force, 2001.
[11] D. J. Hoagland, *The Teredo Protocol: Tunneling Past Network Security and Other Security Implications*, Symantec Principal Security Researcher Symantec Advanced Threat Research, 2007.

Bassam N. Al-Tamimi received the B.Sc., degree in Computer Sciences from University Science and Technology, Sana'a, Yemen in 2005 and M.Sc., degree in Distributed Computing and Networks from Universiti Sains Malaysia (USM), Pulau Penang, Malaysia in 2009. Currently, he is a PhD candidate at the School of Computer Sciences, Universiti Sains Malaysia. His main research interests include Wireless & Mobile Communications, Next Generation Networks including IPv4/IPv6 Network Security and Computer Network Protocols.

Rahmat Budiarto received his B.Sc., degree from Bandung Institute of Technology in 1986, M.Eng., and Dr.Eng., in Computer Science from Nagoya Institute of Technology in 1995 and 1998 respectively. Currently, he is a professor at school of computer sciences, UUM. He is the director of InterNetWorks Research Lab, UUM. His research interest includes Next Generation Network including IPv6 and smart networks, Intelligent Network Monitoring System & Security, Intelligent Systems for Data Mining and Knowledge Discovery Using Evolving Connectionist Systems, and Brain Modeling. He was the chairman of Security Working Group of APAN.

Mohd. Adib Omar completed his BSc. (Artificial Intelligence) and MSc. (Computer Networks) in Computer Science from American University, Washington DC, USA in 2006 and 2007 respectively. He received his PhD in Collaborative Computing from Universiti Sains Malaysia, in 2009. He is currently a senior lecturer at School of Computer Sciences, Universiti Sains Malaysia. His research interests include Wireless Networks, Collaborative and Service Computing, Distributed and Parallel Computing, and Information Security.