Current Status of Mobile Internet Protocol Version 4 and its security issues

Ms. Susanna S Henry, Dr. V. Santhosh Kumar

Computer Science, Birla Institute of Technology & Science, Pilani
Dubai Campus,
Dubai International Academic City
P. O. Box No. 345055, Dubai, UAE

Computer Science, Birla Institute of Technology & Science, Pilani
Dubai Campus,
Dubai International Academic City
P. O. Box No. 345055, Dubai, UAE

Abstract

Many consumers have moved from stationary personal computers to cellular mobile devices. These mobile devices permit change of location while staying connected to the network. To sustain stable communication with the receiver, Mobile Internet Protocol (Mobile IP) was developed. Mobile IP is intended to afford absolutely automated and non interactive reconfiguration at any point. Mobile IP is considered to be a routing protocol thus solving the primary problem of routing IP packets to mobile nodes, which is a first step in providing mobility on the internet. Mobile IP is a secure, robust, and medium-independent protocol whose scaling properties make it applicable throughout the entire Internet. Mobile IP has two versions, Mobile IPv4 and Mobile IPv6.This paper analysis the current status of Mobile IPv4 which is on the verge of exhaustion and announces the urgent need to upgrade IP layer to Mobile IPv6.

Keywords: *Mobile IP, Number Resource Organization (NRO), Internet Assigned Numbers Authority (IANA), Regional Internet Registry (RIR), Internet Engineering Task Force (IETF).*

1. Introduction

Mobile IP is the Internet standard for allowing users to seamlessly roam among wireless networks. Using Mobile IP, applications such as Internet telephony, media streaming and virtual private networking can be supported without service interruption when users move across network boundaries. Mobile IP has a very specialized purpose of allowing IP packets to be routed to mobile nodes that potentially changes its location very rapidly. Mobile IP provides an efficient and scalable mechanism for mobility within the Internet. It is designed to help organizations easily enable their customers to benefit from seamless mobility between different networks in the entire Internet-connected world [11]. Internet users require host mobility with a flexible and seamless connection in order to connect internet at anywhere and anytime. In order to satisfy the requirement of internet users' mobility, IETF standardized Mobile IP that supports uninterrupted internet services on mobile hosts at IP layer. MIPv4 is proposed for supporting mobility in current IPv4 networks [1].

In section 2 of this paper, Current status of Mobile IPv4 is discussed along with few of its security issues are been analyzed, these issues have solutions which in fact has certain amount of risks involved, there are few issues in Mobile IPv4 that do not have solutions, thus due to all these reasons there is an urgent need to shift IP layer to Mobile IPv6. In the later part of this paper, advantages of Mobile IPv6 and proposed deployment mechanism for Mobile IPv6 are given.

2. Current status of Mobile IPv4.

Twenty years ago, the fastest Internet backbone links were 1.5Mbps. Today we argue whether that's fast enough minimum to connect home users. In 1993, 1.3 million machines were connected to the Internet. By this past summer, that number had risen to 769 million and this only counts systems that have DNS names. The notion of a computer that is *not* connected to the Internet is patently absurd these days. But all of this rapid progress is going to slow

down in the next few years. The Internet will soon be sailing in very rough seas, as it's about to run out of addresses, needing to be gutted and reconfigured for continued growth in early half of the 2011 and beyond. Originally, the idea was that this upgrade would happen quietly in the background, but over the past few years, it has become clear that the change from the current Internet Protocol version 4, which is quickly running out of addresses, to the new version 6 will be quite a messy affair [4]. The current status of IPv4 address is given in figure 1.

Fig: 1. IPv4 address as of January 2010

Figure 1 shows the IPv4 address space with used (red boxes), unusable (brown boxes) and free spaces (blue box).

Of course, change *does* manage to happen. We went from 10Mbps to 10Gbps Ethernet, from wired to wireless, and from a Web that was barely able to show blinking text to one running all manners of applications. But the reason we were able to change all of these technologies is that they happen either above or below the Internet Protocol in the network stack. Changing the Internet Protocol means changing *all* hosts and *all* routers. It became obvious that the 32-bit addresses in the existing Internet Protocol were too small to allow for continued growth of the Internet. So far in the world only 6, 7, or even 10 billion people have received the 4.3 billion possible different addresses (with 3.7 billion that are actually usable). The question surely aroused here is … What now?

The Number Resource Organization (NRO) announced that the free pool of available IPv4 addresses is now fully depleted. On Monday, 31 January 2011, the Internet Assigned Numbers Authority (IANA) allocated two blocks of IPv4 address space to Asia Pacific Network Information Centre (APNIC), the Regional Internet Registry (RIR) for the Asia Pacific region, which triggered a global policy to allocate the remaining IANA pool equally between the five RIRs. After allocating those blocks, it means that there are no longer any IPv4 addresses available for allocation from the IANA to the five RIRs. Raúl Echeberría, Chairman of the Number Resource Organization (NRO) stated “This has been an historic event in the history of the Internet, and one we have been anticipating for quite some time”.

The only saving grace is that the IETF started its IP next generation (IPng) effort, which eventually produced IPv6, very early, giving us nearly 20 years between the moments that IPv6 was first standardized in 1995 and the moment that the IPv4 addresses run out, probably 2012. The bad news is that those 20 years are almost up [4].

The Number Resource Organization warned Monday that the number of available IPv4 addresses had slipped below 10 percent, with one service predicting that the available addresses will expire in a bit more than a year. In 2008, worldwide organizations began warning that the number of IPv4 addresses was slowly expiring, predicting that they would expire at the end of 2010 or early 2011. That seems to be holding true, with one algorithm predicting that the central registry will run out of IP blocks [5].

According to a forecasting site operated by Geoff Huston, who is an adjunct research fellow at the Centre for Advanced Internet Architectures at

Swinburne University of Technology in Australia. Europe is next to run out of IPv4addresses. In 2013, it will be North America's turn to watch its Internet registry run out of IPv4 addresses, according to Huston's forecast. Africa and Latin America will face the same in 2014 [8].

2.1 Mobile IPv4 protocol Security Issues and solutions with risks involved:

Issue 1: Ingress filtering:

Packets may be neglected and removed from Internet Service Provider by any router. Many routers implement security policies that do not allow forwarding of packets that have a Source Address which appears topologically incorrect. The internal network of ISP never constitutes of packet's IP address. This kind of problem is stated as Ingress Filtering. Considering MIPv4, mobile node uses source address as home IP address from Foreign Internet service Provider, which is different when compared to the address of internet service provider network [9].

Solution:

The solution for this issue of Ingress filtering is given by reverse tunneling, whereby the Foreign Agent address is supplied instead of that of the Mobile Node, the base Mobile IP uses encapsulation to tunnel the packet from Correspondent Host to Care of Address of Mobile Node. Here Generic Routing Encapsulation (GRE) is a default protocol employed for tunneling. By using this protocol encapsulation is avoided in MIPv4 and tunneling techniques are applied for private and public networks, but this solution ahs a risk involved, it creates privacy issue.

Issue 2: Authentication:

Main reason for authentication is to confirm the characteristics of message designer. Confirmation is supplied in an extension which composes of message digest, security parameter index, length and type of extension used. Message digest utilizes 128 bits for estimation. Considering Mobile IPv4, we have to keep the consistency with previous Mobile IPv4 executions. Present executions should cooperate with Hashing for Message Authentication (HMAC MD5) using prefix suffix form mode [10].

Solution:

Use of Internet Protocol security on Mobile IP is one of the solutions for the issue of authentication. Encapsulation is utilized to forward packets to Mobile nodes. Keeping the consistency with previous Mobile IPv4 executions and cooperate Hashing for Message Authentication (HMAC MD5) in Present executions using prefix suffix form mode gets added up with beginning and end part of data for authentication. But this is too risky.

Further risks as concern to authentication in Mobile IPv4 is given in the tabular form

Issue	Risk
a. Optional authentication of registration messages between Mobile Node and Foreign Agent. b. No authentication of Foreign Agent Advertisement message.	Risk of hostile Foreign Agent masquerading on as a legitimate Foreign agent which presents a denial-of-service threat.
Use of Address Resolution Protocol (ARP) and proxy ARP.	There is no ARP authentication, thus Home network gets vulnerable to Mobile Node traffic stealing by hostile network.

Table 1: Authentication

Issue 3: Authorization:

During the connection with the node, the operator of the association has to determine who is the connector and kind of network source used. This kind of issue is known as authorization.

The related security issues and risks for MIPV4 protocol:

Issue	Risk
Silent beyond, including a Foreign Agent registration.	a. Fails to address how Foreign Agent, or Default router, ascertains legitimacy of visiting MN. b. Leaves authorization implementation up to developers without providing any guidelines.

Table2: Authorization

Solution:

Registration key is one of the solutions for the issue of authorization. Authorization in MIPv4 is method established to supply security between Foreign Agent and Mobile Node. The constraint in this solution is that registration of Mobile Node with Foreign Agent is required.

Issue 4: Encryption key distribution:

The précised non repudiation, integrity, and authentication are obtained by some method which involves allocation, discussion and distribution of key among receivers and senders. Mobile Internet protocol should encourage for key administration process [11].

Solution:

Mobile internet protocol is supplied with an extension. This explains how Mobile Node, Foreign networks and Home Networks employ confidential key or public key. Secure Scalable Authentication (SSA) is employed which require further modifications for authentication expansion to adapt distinct sizes and types of digital Signatures when utilized by Mobile IPv4.The above given issues are solved in Mobile IPv4 but each issue discussed has several risks involved. There are few issues that are not solved in Mobile IPv4, they are as follows

2.2 Issues that are not solved in Mobile IPv4

Issue 5: Triangular routing problem: This is main unsolved problem presently faced by Mobile IPv4. Basic concept behind this routing problem is: Mobile Node needs to transmit the packet to an additional node within the network. The distance between the Receiver and Mobile Node's Home Network is significantly more to send the packets. Therefore all the packets are sent to Home Network. This is why the packets are first sent to Home agent via Internet. After this they are tunneled to the Foreign Agent again through internet. The most favorable way is transferring packets precisely to Mobile Node by neglecting the Home Agent. For the reason that message is sent from Mobile node to Correspondent Node and from Correspondent node to Home Agent, this process is known as triangle routing. As there is a single router from transmitter to Mobile Node and then Home Agent, there is a noticeable problem. Triangular routing interrupts the transmission of packets to Mobile Node.

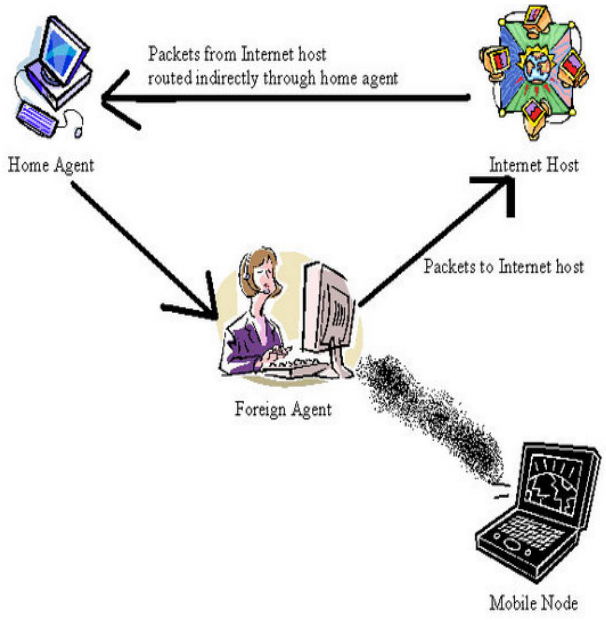

Figure 2: Triangular Routing Problem

In figure 2, the packets from Internet Host are routed indirectly through the home agent. These packets are

further passed to the foreign agent. Figure 2 shows the presence and role of mobile node as discussed in the Triangular Routing Problem.

Issue 6: Non-repudiation:

Message Recipient should have a chance to confirm the message created by sender. Which means the message sender will not be capable of rejecting the created message. This is done in wireless network. This kind of issue is known as Non repudiation.

The related security issues and risks for MIPV4 protocol: Non-repudiation

Issue	Risk
Foreign Agent visitor list entries do not record the actual duration of the Mobile Node visit nor the amount of time spent in the network or resources consumed in the network.	There is no mechanism for logging visiting Mobile Node's resource consumption, thus the owner or operator of visited network would not be able to track network resource utilization.
The Foreign Agent must delete a Mobile Node Visitor List entry when the Foreign Agent receives a valid registration reply.	a. Once a Mobile Node Visitor List entry is deleted, there is no longer any record of a Mobile Node's visit. b. There is no mechanism or approach, for logging Mobile Nodes who have visited and left Foreign Agent's network

Table3: Non-Repudiation

Issue 7: Location privacy

Basic purpose of location privacy is to keep secret about Mobile Nodes location. Location of present real attachment of sender to network is secured from other receivers by the message sender.

The related security issues and risks for MIPv4 protocol is given in the following tabular form

Location Privacy.

Traffic analysis on wireless link	Only viable protection against a traffic analysis attack on wireless links can serve the purpose.

Table 4: Location Privacy

Issue 8: Minimize the number of required trusted entities:

The amount of necessary agents like Home agent and Foreign Agent must be reduced. While minimizing the number of trusted entities there is a requirement of improvement in the security.

3. Proposed Solution

Based on the several analyses done, we come to the conclusion in this paper that Mobile IPv4 is on the verge of exhaustion and it is proposed that IP layer be shifted to the next version of Mobile IP that is Mobile IPv6. This paper will give you few expert comments about Mobile IPv6 from various expert members of Internet Society.

One of the official representatives from the five Regional Internet Registry (RIRs) states that "The future of the Internet is in IPv6. All Internet stakeholders must now take definitive action to deploy IPv6".

Rod Beckstrom, President and Chief Executive Officer of Internet Corporation for Assigned Names and Numbers (ICANN) said "This is truly a major turning point in the on-going development of the Internet; nobody was caught off guard by this, the Internet technical community has been planning for

IPv4 depletion for quite some time. But it means the adoption of IPv6 is now of paramount importance, since it will allow the Internet to continue its amazing growth and foster the global innovation we've all come to expect."

Elise Gerich, Vice President of Internet Assigned Numbers Authority (IANA) said , "IPv6 is the "next generation" of the Internet Protocol, providing a hugely expanded address space and allowing the Internet to grow into the future. "Billions of people worldwide use the Internet for everything from sending tweets to paying bills. The transition to IPv6 from IPv4 represents an opportunity for even more innovative applications without the fear of running out of essential Internet IP addresses."

Adoption of IPv6 is now vital for all Internet stakeholders. The Regional Internet Registry (RIRs) have been working with network operators at the local, regional, and global level for more than a decade to offer training and advice on IPv6 adoption and ensure that everyone is prepared for the exhaustion of IPv4 [5].

While IPv4 and IPv6 are very much alike to users and applications; "on the wire," the protocols are completely separate and don't interact. The advantage of IPv6 is that there is no need to change existing IPv4 infrastructure—IPv6 is simply added as a new protocol. All the limitations and mistakes that are part of IPv4 are left behind. Right around this point in the story, many system administrators start becoming very uncomfortable about the transition to IPv6: they can't just set up a big Dynamic Host Configuration Protocol (DHCPv6) for IPv6 server that logs all address assignments. Ten years ago, this difference between IPv4 and IPv6 may have been met with a can-do attitude. But the peculiarities of IPv4 are now so ingrained and the memories remain of the multi-protocol world that existed during the last decades of the previous century, that the lack of similarity between IPv4 and IPv6 could be a real stumbling block today [4].

Internet society announces 6 June 2012 as the World IPv6 launch day. IPv6 is the new net address system that replaces the current protocol IPv4. Web companies participating in the event have pledged to enable IPv6 on their main websites from that date. The Internet Society, which made the announcement, said the day represented "a major milestone" in the deployment of the standard. Facebook, Google, Microsoft Bing and Yahoo are the inaugural web firms involved. Google, Yahoo, Microsoft Bing and Facebook are among the companies switching-on IPv6 versions of their websites for the one day trial. The technology is gradually being introduced because the world is running out of older IPv4 addresses as more devices come online.

IPv4 conceived in early 1980s is typically made up of 32 bits, written as 12 digits, e.g. 112.233.189.123.That gives a maximum of around 4.3 billion addresses. The rapid growth in PCs, smart phones and other internet connected devices means those addresses are close to being used up, with an estimated 80 million still to be allocated. IPv6 is a 128bit system, written in hexadecimal (base 16 counting using numbers and letters), e.g. 21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A.
The system gives a maximum of 340 undecillion possible addresses (1 undecillion = 10 followed by 35 zeros in the British numbering system). The additional capacity, argue proponents of IPv6, will be needed to cater to the so-called "internet of things" where devices such as TVs, fridges and home heating systems are connected to the net.

Companies and home users may need new networking equipment. However the transition is likely to take years. For users with an ordinary domestic internet connection, the changeover may involve upgrading their hardware."A lot of routers at the moment are already capable of supporting IPv6. What they need is a firmware update," explained Richard Fletcher, chief operating officer at Plusnet, a UK internet service provider (ISP) "ISPs should ship new routers or offer those updates. We are making sure all our fiber routers are ready for IPv6" [6].

3.1 Comparison of Mobile IPv4 with Mobile IPv6 in terms of TCP Traffic.

Here we compare and evaluate the TCP performance of Mobile IPv4 and Mobile IPv6 networks in the present scenario. It is proved that the amount of transmitted TCP packets in MIPv4 network is more than that in MIPv6 network. However, total packet sequence numbers of TCP are nearly same with each

other in MIPv4 and MIPv6 networks. This result comes from that TCP packets in MIPv4 network are retransmitted or dropped more than that in MIPv6 network. It is proved that TCP performance in Mobile IPv6 network outperforms Mobile IPv4 network in terms of amount of dropped packets and lasting the connection. There is no need to deploy special routers as "Foreign Agents", as in Mobile IPv4. Mobile IPv6 operates in any location without any special support required from the local router. Most packets sent to a mobile node while away from home in Mobile IPv6 are sent using an IPv6 routing header rather than IP encapsulation, reducing the amount of resulting overhead compared to Mobile IPv4 [2].

3.2 Advantages of IPV6

In 2008, barely any of the Internets had moved to IPv6, IPv6 addresses add an additional level to the IP address, providing enough IP address for all devices for the foreseeable future. Number Resource Organization (NRO) stated “Today the shift is becoming more pronounced” [5].

Mobile IPv6 is decoupled from any particular link layer, as it uses IPv6 Neighbor Discovery instead of Address Resolution Protocol (ARP). This also improves the robustness of the protocol. The use of IPv6 encapsulation (and the routing header) removes the need in Mobile IPv6 to manage "tunnel soft state". The dynamic home agent address discovery mechanism in Mobile IPv6 returns a single reply to the mobile node. The directed broadcast approach used in IPv4 returns separate replies from each home agent.

4. Proposed IPv6 Deployment mechanism

The Cisco Systems has designed and developed some types of routers such as provider edge (PE) routers or Virtual Private Networks provider edge (VPE) routers that support IPv4 and IPv6. All of them create an environment on which IPv4 nodes can connect to other IPv4 nodes, IPv6 nodes can connect to other IPv6 nodes or few of IPv6 nodes can connect to IPv4 nodes. However, there is no solution for mobile IP nodes. As concerned above, a mobile IPv6 node can keep communication with other IPv6 nodes when migrating in IPv6 network. But it hasn't connected to another mobile IPv4 node yet. There are a lot of limit and difficulty when deploying a real IPv6-and-IPv4 network. It is harder to create and keep connection between mobile IPv4 and mobile IPv6 node. Solutions are researched, discussed and simulated. So, it is said that the trend of mobile IP mechanisms is solving the problem.

How can a mobile IPv6 connect and keep communication with an IPv4 node while moving from network to network and vice versa? Mobile IPv4 and Mobile IPv6 can perform separately with high performance. However, when co-exist, they make many troubles. Mobile IPv6 can be deployed on Multi Protocol Label Switching (MPLS) core network with reliable data transfer procedures. Advanced mechanisms of MPLS such as traffic management and flow control guarantee QoS requirements of IPv6 end users. Because label switching routers map labels and switch datagram at layer two which is independent on IP layer, many IP-based services can be developed on MPLS network. Many researches about transferring data between IPv4 nodes and IPv6 nodes rely on these features of MPLS. Some acceptable solutions are proposed such as using dual-stacks routers, virtual private networks (VPN) and network address translation (NAT). The next step of these researches is bringing out solutions of transferring data between mobile IPv4 nodes and mobile IPv6 nodes on MPLS core network to prepare for the replacement of IPv4 devices by IPv6 devices in future [3].

The key to a successful IPv6 transition is compatibility with the large installed base of IPv4 hosts and routers. Maintaining compatibility with IPv4 while deploying IPv6 will streamline the task of transitioning the Internet to IPv6. This specification defines two mechanisms that IPv6 hosts and routers may implement in order to be compatible with IPv4 hosts and routers. The mechanisms in this document are designed to be employed by IPv6 hosts and routers that need to interoperate with IPv4 hosts and utilize IPv4 routing infrastructures. We expect that most nodes in the Internet will need such compatibility for a long time to come, and perhaps even indefinitely.

The mechanisms specified here are:

1) Dual IP layer (also known as dual stack): A technique for providing complete support for both Internet protocols -- IPv4 and IPv6 -- in hosts and routers.

2) Configured tunneling of IPv6 over IPv4: A technique for establishing point-to-point tunnels by encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 routing infrastructures.

The mechanisms defined here are intended to be the core of a "transition toolbox" -- a growing collection of techniques that implementations and users may employ to ease the transition. The tools may be used as needed. Implementations and sites decide which techniques are appropriate to their specific needs. This paper defines the basic set of transition mechanisms, but these are not the only tools available.

Techniques Used in the Transition

1) Dual IP Layer Operation: The most straightforward way for IPv6 nodes to remain compatible with IPv4 only nodes is by providing a complete IPv4 implementation. IPv6 nodes that provide complete IPv4 and IPv6 implementations are called “IPv6/IPv4 nodes". IPv6/IPv4 nodes have the ability to send and receive both IPv4 and IPv6 packets. They can directly interoperate with IPv4 nodes using IPv4 packets, and also directly interoperate with IPv6 nodes using IPv6 packets.

Even though a node may be equipped to support both protocols, one or the other stack may be disabled for operational reasons. Here we use a rather loose notion of "stack". A stack being enabled has IP addresses assigned, but whether or not any particular application is available on the stacks is explicitly not defined. Thus, IPv6/IPv4 nodes may be operated in one of three modes:

i. With their IPv4 stack enabled and their IPv6 stack disabled.

ii. With their IPv6 stack enabled and their IPv4 stack disabled.

iii. With both stacks enabled.

IPv6/IPv4 nodes with their IPv6 stack disabled will operate like IPv4-only nodes. Similarly, IPv6/IPv4 nodes with their IPv4 stacks disabled will operate like IPv6-only nodes. IPv6/IPv4 nodes may provide a configuration switch to disable either their IPv4 or IPv6 stack.

2) Configured Tunneling Mechanisms: In most deployment scenarios, the IPv6 routing infrastructure will be built up over time. While the IPv6 infrastructure is being deployed, the existing IPv4 routing infrastructure can remain functional and can be used to carry IPv6 traffic. Tunneling provides a way to utilize an existing IPv4 routing infrastructure to carry IPv6 traffic. Tunneling can be used in a variety of ways:

i. Router-to-Router. IPv6/IPv4 routers interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves. In this case, the tunnel spans one segment of the end-to-end path that the IPv6 packet takes.

ii. Host-to-Router. IPv6/IPv4 hosts can tunnel IPv6 packets to an intermediary IPv6/IPv4 router that is reachable via an IPv4 infrastructure. This type of tunnel spans the first segment of the packet's end-to-end path.

iii. Host-to-Host. IPv6/IPv4 hosts that are interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves. In this case, the tunnel spans the entire end-to-end path that the packet takes.

iv. Router-to-Host. IPv6/IPv4 routers can tunnel IPv6 packets to their final destination IPv6/IPv4 host. This tunnel spans only the last segment of the end-to-end path.

Configured tunneling can be used in all of the above cases, but it is most likely to be used router-to-router due to the need to explicitly configure the tunneling endpoint [7].

5. Conclusions

In this paper, we have proposed a solution for the problem of IPv4 address exhaustion; the proposed solution is to shift IP layer to Mobile IPv6. There are several IPv6 Deployment mechanisms suggested by many researchers. One of the IPv6 Deployment mechanisms is emphasized in this paper as given in [7]. There is an urgent need for further work on this proposal to ease the current problem of IPv4 address exhaustion.

References:

[1]. R.Gunasundari and S.Shanmugavel, Performance Comparison of Mobile IPv4 and Mobile IPv6 Protocols in Wireless Systems, First International Conference on Communications Systems and Networks (COMSNETS) 5-10 Jan, 2009, pp. 1 – 8.

[2]. Sujeong Chang, Jaehyung Park, Yonggwan Won, Mijeong Yang, and Min Young Chung, Performance Comparison of TCP Traffic over Mobile IPv4 and IPv6 Networks and a Mobile Network Deployment Approach, First International Conference on Computer and Information technology (CIT) 21-23 Sept. 2005, Page(s): 469 – 473.

[3]. Nguyen Ngoc Chan and Tran Cong Hung, Mechanisms of Mobile IP in delivering packets and its trends for changing from IPv4 to IPv6, Ninth International Conference on Advanced Communication Technology, 12-14 Feb. 2007, Vol. 2, pp. 1027 – 1032.

[4]. Iljitsch van Beijnum, ARS Technica, September 29, 2010.

[5]. Montevideo, Number Resource Organization (NRO), 3 February, 2011.

[6]. BBC News Technology, 7 June 2011.

[7]. E. Nordmark and R. Gilligan, Network Working Group, Request for Comments: 4213, Obsoletes: 2893, October 2005.

[8]. Stephen Lawson, Info World, January 03, 2012.

[9]. Ulrike Meyer, Hannes Tschofenig and Georgios Karagiannis, On the Security of the Mobile IP Protocol Family, University of Twente Publications, Proceedings of 1st IEEE Workshop on Enabling the Future Service-Oriented Internet, Workshop of GLOBECOM 2007, 26-30 Nov 2007.

[10]. Chakchai So-In, Mobile IP Survey, Mobile IP IETF, Request for Comments and Internet Drafts, 2006, pp. 1-29.

[11]. Karri Huhtanen, Advanced Course on Networking, Mobile IP, Tampere University of Technology, 2010.