An Integrated Secure Inter-mobility IPv4/IPv6 Address Translation Architecture for Corporate Networks

J. Amutha and S. Albert Rabara

***Abstract*—Next Generation Networks (NGN), the heterogeneous all-IP model with inherent capacity of providing next generation services as Always Best Connected (ABC), Anytime Anywhere with seamless mobility meriting the motto 'All over IP and IP over All' is effectively realized in IPv6 to supersede the current IPv4 protocol. Several initiatives have been made by researchers to integrate secure, inter-mobility and translation architecture together. But, not much progress has been reported in recent past. Hence, in this research, an Integrated Secure Inter-Mobility IPv4/IPv6 Address Translation Architecture for Corporate Networks has been proposed to achieve secure communication, inter-mobility between IPv4 and IPv6 networks and IP address translation with an IPv4/IPv6 Enabled Gateway Translator (IP46EGT). Network performance is evaluated and the generated results are tabulated and graphically presented.**

***Index Terms*—Addressing, mobility, NGN, security.**

I. Introduction

NGN is an IP-based integration of heterogeneous wired and wireless access networks into an All-IP Net-Era. All-IP networks basically apply the IP technology providing next generation services to any customer anywhere and at any time offering data, image, voice and video over the same network [1]. The network and service convergence on the IP-basis could prove to be an acceptable compromise towards the future and current interests of telecom companies [2]. Mobility management has emerged as the most challenging issue for the academia and industry because of the heterogeneous characteristics of IP-based networks [3]. "Achieving equitable communication for everyone" is one of the main strategic goals set by the International Telecommunication Union (ITU) to achieve mobility in NGN [4]. Internet Protocol version 6, IPv6 is a later version of IP suit, which has gained popularity as the primary network protocol for NGN that interconnects this heterogeneous network. Due to the escalating demand for IP addresses and growth of the global Internet, the transition from IPv4 to IPv6 becomes inevitable. In 2013 alone, 65 million IP addresses were consumed [5]. The rapidly developing countries, including China and India, suffer crunch in IP usage and therefore have reason to promote a more rapid transition in IPv6 [6]. Security issue is one of the primary considerations that need to be addressed. IPSec is compatible with current Internet standards in IPv4, but in IPv6, IPSec is defined as mandatory feature and the objective of improved security is to create routing changes that provide mobility in the network that are safe against all the various security threats [7].

Since the initiatives made by researchers to integrate secure, inter-mobility and translation architecture employing the transition and security mechanisms for corporate networks have been tardy, designing an integrated secure inter-mobility address translation architecture for corporate networks has become a felt need and a most challenging task. Hence, in this research work, an Integrated Secure Inter-Mobility IPv4/IPv6 Address Translation Architecture for Corporate Networks has been proposed to achieve secure communication, inter-mobility between IPv4 and IPv6 networks and IP address translation with an IPv4/IPv6 Enabled Gateway Translator (IP46EGT).

Manuscript received March 10, 2015; revised September 16, 2015.

The authors are with the Department of Computer Science, St.Joseph's College, Bharathidasan University, Tiruchirappalli, Tamil Nadu, India (e-mail: roniamutha@gmail.com, a_rabara@yahoo.com).

II. Review of Literature

Zhang *et al*. [8] proposed an Evolvable Locator/ID Separation Internet architecture (ELISIA), for IPv4/IPv6 transition, which combines the address mapping of IPv4/IPv6 (IVI) and Network Address Translation (NAT) system with its Locator/ID. Cui *et al*. [9] suggested 4over6 virtualization architecture for IPv4-IPv6 coexistence, using IPv4 embedded IPv6 prefixes for addressing. Jin *et al*. [10] realized an Xlat design which facilitates IPv4/IPv6 co-existence and transition based on the stateless NAT64 translator which uses the server port mapping method for address translation mechanism. Kafle *et al*. [11] proposed an architecture called HIMALIS (Heterogeneity Inclusion and Mobility Adaptation through ID/Locator Separation) for the future Internet which provides mobility through make-before-break and break-before-make type of seamless handover. Park *et al*. [12] addressed the need for global seamless handover between homogeneous or heterogeneous networks and emerged with the concept of Simple Mobility Management Protocol (SMMP). Shang *et al*. [13] dealt with an IPv4/IPv6 (IVI) based locator/id separation architecture for IPv4/IPv6 transition which supports inter-domain networking and host mobility. Choudhary *et al*. [14] presented a model named Policy Based Security Management (PBSM) for the secure deployment of the host-based security systems. Beck *et al*. [15] presented various algorithms and tools for the secure configuration of the firewalls.

III. Proposed Architecture

The proposed unique architecture is designed to integrate the two independent IP versions IPv4 and IPv6, by mutually permitting one version of IP mobile nodes to roam into

doi: 10.18178/ijfcc.2015.4.5.408

another version of IP networks. Therefore IPv4 networks communicate with IPv6 mobile nodes, and IPv6 networks communicate with IPv4 mobile nodes. This is achieved by designing a novel translator namely an IPv4/IPv6 Enabled Gateway Translator (IP46EGT) which is simulated in the form of a PC-Emulator. Fig. 1 illustrates the diagrammatic representation of the proposed architecture.

The IP46EGT translates IPv4 address into IPv6 address and IPv6 address into IPv4 address. When an IPv6 node communicates with an IPv4 host in the IPv4 network, the translated IPv6 source prefix is configured in the IP46EGT which detects the destination address of the IPv6 packet. If this prefix is the same as the configured prefix, the address mapping takes place and converts the IPv6 address to IPv4 address. Mobility header includes Mobile IP and Mobile IPv6 for managing mobility as it roams in different networks. If an IPv6 mobile node V6 from an IPv6 network roams into an IPv4 network, V6 is referred to as V6'. Similarly if an IPv4 mobile node V4 from an IPv4 network roams into an IPv6 network, then V4 is referred to as V4'.

Virtual Private Network (VPN) is incorporated in the proposed architecture to provide secure data transmission between the VPN mobile node and the network. The PC-Emulator in the architecture generates a New Secret Key (NSKG) which is the Cryptographically Generated Address (CGA) for every communication. The NSKG is a combination of the four-digit random number (SKG) and the last two bit positions of the source client node MAC address(MSKG) that is, NSKG = SKG + MSKG. The NSKG is sent to the source and destination to establish an authentication between the mobile node and the server which provides the end-to-end security. Load balancer balances traffic over multiple connections, which ensures the availability of the network and improves the overall performance of the availability of the applications. The proposed architecture consists of three major processes, namely: Neighbor Discovery, Obtaining Binding Address and Registration Procedure.

A. Neighbor Discovery

When an IPv4/IPv6 mobile node moves into the IPv6/IPv4 network, the mobile node in IPv6/IPv4 network uses neighbor discovery protocol to find the neighboring routers to forward packets. The IPv6 neighbor discovery contains five Internet Control Message Protocol (ICMP) packet types namely: a pair of Router Solicitation and Advertisement messages, a pair of Neighbor Solicitation and Advertisement messages, and a Redirect message. ICMPv6 allows a mobile node to discover the address of operational routers on the network through router solicitation and router advertisement messages of type 133 and of type 134 respectively. Similarly, ICMPv4 allows a mobile node to discover the address of the operational routers on the network through router advertisement and router solicitation messages of type 9 and of type 10 respectively. Both ICMPv4 and ICMPv6 are compatible with each other. Router Advertisement (RA) allows routers to perform DHCPv6 / stateless address configuration. The IPv4 mobile node (V4') after entering into the IPv6 network other than its home network, in order to obtain a new binding address, starts searching for the DNS agent and receives IPv6 router advertisement message of type 134. The IPv4 mobile node identifies that it is not in the IPv4 network. Hence, IPv6 router sends a RA message of type 134 in IPv6 network through ICMPv6 protocol. The IPv4 mobile node (V4'), on entering into the IPv6 network, sends a router solicitation message of type 10 through ICMPv4 protocol. IPv4 mobile node (V4') in the IPv6 network turns client to the IPv6 router which, after receiving a router solicitation message of type 10, replies to IPv4 mobile node (V4').

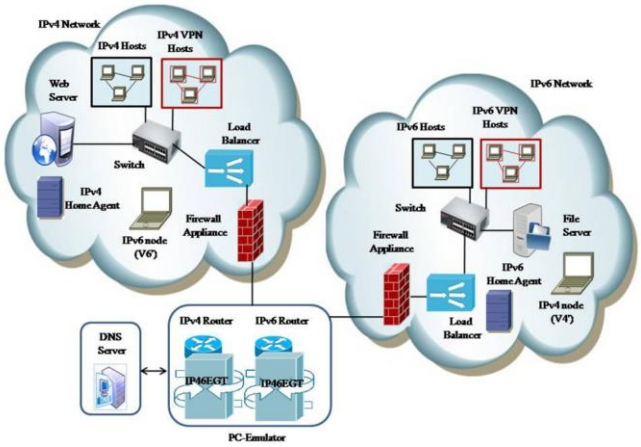

Fig. 1. Proposed IPv4/IPv6 enabled gateway translator (IP46EGT) translation architecture.

Similarly, the IPv6 mobile node (V6') after entering into the IPv4 network other than its home network, in order to obtain a new binding address, starts searching for the network prefix as it receives IPv4 RA message of type 9 through stateless address autoconfiguration. The IPv6 mobile node identifies that it is not in the IPv6 network. Hence, IPv4 router sends an RA message of type 9 in the IPv4 network through ICMPv4 protocol. The IPv6 mobile node (V6'), on entering into the IPv4 network, sends a router solicitation message of type 133 through ICMPv6 protocol. IPv6 mobile node (V6') in the IPv4 network turns a client to the IPv4 router which, after receiving a router solicitation message of type 133, replies to IPv6 mobile node (V6'), by providing its address.

B. Obtaining IPv4 and IPv6 Binding Address

Whenever a mobile node roams into the network which is IPv4 or IPv6, it is labeled with a new temporary address called Binding Address (BAdd). The IPv6 mobile node (V6') which roams in the IPv4 foreign network obtains a binding address called V6BAdd. The V6' sends an IPv4 router solicitation request message, in response to the corresponding IPv6 mobile node receives the 32-bit IPv4 router address. This 32-bit IPv4 address is converted to its corresponding IPv6 address which is in hexadecimal format and is assigned to the 33rd to 64th bit position of the network part of the IPv6 address. The first 16-bit is assigned with the format prefix as 2001. The 17th to 32nd bit position is assigned with FFFF representing IPv4-mapped IPv6 address. The last 65th to 128th bit position is generated by the MAC address which represents the interface identifier of the V6' node. This IPv6 address in the IPv4 network is the IPv6 Cryptographically Generated Binding Address (V6CGBAdd).

Similarly, the IPv4 mobile node (V4') which roams in the IPv6 foreign network obtains a binding address called

V4BAdd. The V4' sends an IPv6 router solicitation request message and in response the corresponding roaming IPv4 mobile node receives the 128-bit IPv6 router address. The IP46EGT extracts the 32-bits from the 33rd to 64th bit position of the network part of the IPv6 address and converts them to its corresponding IPv4 address which is in decimal format. The remaining bit positions are assigned with zeroes representing IPv4-compatible IPv6 address. The generated IPv4 address in IPv6 network is the IPv4 Cryptographically Generated Binding Address (V4CGBAdd). The V6CGBAdd / V4CGBAdd and the mobile node's IPv6 / IPv4 home address are assigned in the IPv6 / IPv4 address pool of the IP46EGT, while the V6' / V4' sends a binding update message to its HAv6/ HAv4 respectively. After the generation of the binding address, the IPv6/ IPv4 mobile node in the IPv4/IPv6 network performs Duplicate Address Detection (DAD) in order to prevent multiple nodes from using the same address simultaneously. On successful return of DAD, the V6CGBAdd / V4CGBAdd is recorded into the IPv4/IPv6 Enabled Gateway Translator (IP46EGT) and the registration process occurs.

C. Registration Procedure

The registration procedure is performed to inform its IPv4/ IPv6 home agent about its binding address. After receiving the BU message of V4'or V6', the corresponding home agent creates two binding cache entries, one for V4CGBAdd or V6CGBAdd and another for the corresponding mobile node's home address (HAv4/HAv6). The binding cache entries on HAv4 is initiated by a DNS query in which the prefix is added to the IPv4 home agent to form IPv6 home agent and the binding update message which is generated by the IPv4 mobile node which roams in IPv6 network will be sent to the IP46EGT. But, the binding cache entries on HAv6 is initiated by a DNS query which will be sent to the IP46EGT directly. The IP46EGT searches its address pool, which generates the mapped address of the IPv4/IPv6 home address, records a mapping between the PC-Emulator and the mobile node home agent address by converting the mobile nodes home agent HAv4/HAv6 address as the IPv6/IPv4 mapped address.

IV. Experimental Study

The main focus of the experimental study is to test the functionality of the IPv4/IPv6 address translation architecture with respect to IPv4/IPv6 addressing, inter-mobility between IPv4 and IPv6 nodes and to measure the performance of these mechanisms on a network. The testing process is carried out in the lab environment using a virtual topology. The performance of the proposed system is investigated in terms of data loss rate, throughput, and latency analysis. The results of the study are tabulated and presented graphically.

V. Performance Analysis

Network performance of the IP46EGT translator is evaluated using the Ixia tool. This tool measures bandwidth and response time to measure the data loss rate, throughput and latency analysis between IPv6 and IPv4 hosts.

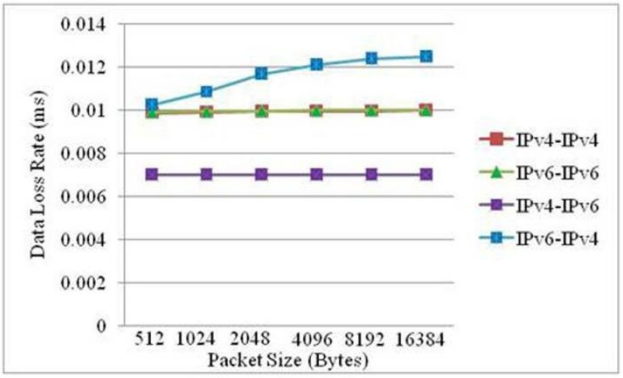

Fig. 2. Data loss rate analysis.

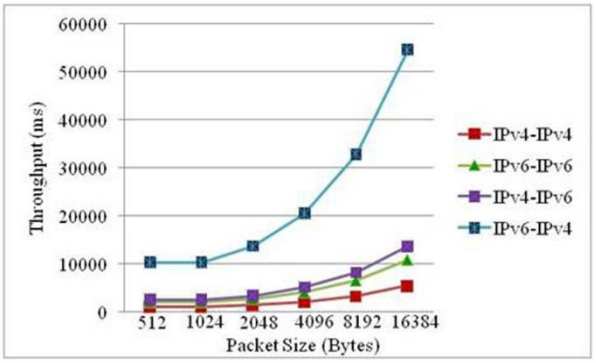

Fig. 3. Throughput analysis.

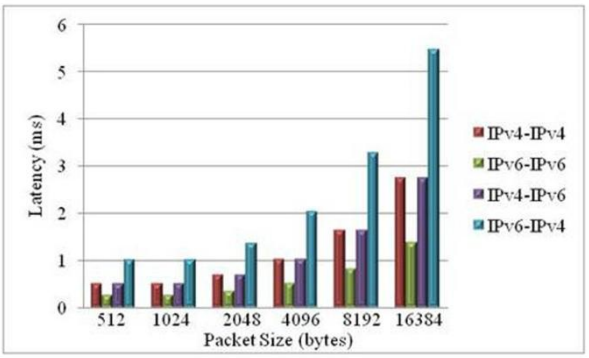

Fig. 4. Latency analysis.

A. Data Loss Rate Analysis

Data Loss rate is the ratio between the number of bytes received at the receiving node to the total number of bytes transferred from the source node. In the data loss rate analysis, the packet size is varied in the range (512, 1024….16384 in bytes), to measure the corresponding change in the data loss rate. Fig. 2 depicts the data loss rate analysis between IPv4 and IPv6 communications.

B. Throughput Analysis

Throughput is defined as the amount of packet data that is transmitted over the entire path per time unit. The throughput generally increases with the size of the packets. The maximum throughput is reached for the largest packet sizes. From the graph in Fig. 3, it is observed that the packets transmission from IPv4 to IPv6 exhibits the best throughput performance and maximum throughput is reached for the larger packet sizes both in IPv4 and IPv6.

C. Latency Analysis

Latency analysis is measured by varying the packet size

from 512 bytes to 16384 bytes (512, 1028, ..16384 bytes). Fig. 4 indicates that the delay for the IPv4 to IPv6 communication is less or same when compared with IPv4 to

IPv4 communication. However the delay in IPv6 to IPv4 communication is higher when compared with IPv6 to IPv6 communication due to the routing table size.

VI. Conclusion

The proposed Integrated Secure Inter-Mobility IPv4/IPv6 Address Translation Architecture for Corporate Networks is designed to integrate two independent IP networks by an IPv4/IPv6 built-in security Enabled Gateway Translator (IP46EGT). IP46EGT provides connectivity between IPv4 and IPv6 networks by stateless address configuration mechanism which is simulated in the form of PC-Emulator. The proposed architecture is tested and the results are tabulated and graphically presented.

References

[1] A. Quintero and S. L. Alaoui. "A mobility management model based on users' mobility profiles for IPv6 networks," *Computer Communication*, Elsevier, vol. 30, no. 1, pp. 66-80, December 2006.

[2] V. I. Tikhonov, P. P. Vorobiyenko, and A. S. P. Odesa, "Integrated telecommunication technology for the Next Generation Networks," in *Proc. ITU Kaleidoscope Academic Conference*, 2013, pp. 1-7.

[3] B. R. Chandavarkar and G. R. M. Reddy, "Survey paper: Mobility management in heterogeneous wireless networks," *Procedia Engineering*, vol. 30, pp. 113- 123, 2012.

[4] L. Lehmann, "Accessibility support for persons with disabilities by total conversation service mobility management in Next Generation Networks," presented at ITU-T Kaleidoscope Academic Conference, 2011.

[5] S. L. Levin and S. Schmidt. "IPv4 to IPv6: Challenges, solutions and lessons," *Telecommunications Policy*, Elsevier, vol. 38, no. 11, pp. 1059-1068, December 2014.

[6] A. Henten and R. Tadayoni, "Transition from IPv4 to IPv6," *CMI Working Paper*, vol. 2, 2013.

[7] H. Modares, A. Moravejosharieh, H. Keshavarz, and R. Salleh, "Protection of binding update message in Mobile IPv6," presented at IEEE UKSim-AMSS 6th European Modelling Symposium, 2012.

[8] H. Zhang, X. Li, and C. Bao, "An evolvable locator/ID separation internet architecture (ELISIA)," presented at IEEE International Conference on Networking, Architecture and Storage, 2013.

[9] Y. Cui, P. Wu, M. Xu, J. Wu, Y. L. Lee, A. Durand, and C. Metz, "4over6: Network layer virtualization for IPv4-IPv6 coexistence," *IEEE Network*, vol. 26, pp. 44-48, 2012.

[10] R. Jin, C. Bao, and X. Li, "Provide IPv4 service using pure IPv6 server with stateless NAT64 translator," presented at IEEE International Conference on Networking, Architecture and Storage, 2014.

[11] V. P. Kafle, Y. Fukushima, and H. Harai, "New mobility paradigm with ID/Locator Split in the Future Internet," presented at IEEE Consumer Communications and Networking Conference (CCNC 2014): Mobility Management in the Networks of the Future World, 2014.

[12] J. T. Park, S. M. Chun, J. H. Choi, and S. M. Lee, "Simple mobility management protocol for global seamless handover," presented at IEEE IEEE International Workshop on Personalized Networks, 2012.

[13] W. Shang, C. Bao, and X. Li, "IVI-based locator/ID separation architecture for IPv4/IPv6 transition," presented at IEEE International Conference on Networking, Architecture, and Storage, 2012.

[14] A. R. Choudhary and A. Sekelsky, "Securing IPv6 network infrastructure: A new security model," presented at 2010 IEEE Conf., 2010.

[15] F. Beck, O. Festor, I. Chrisment and R. Droms, "Automated and secure IPv6 configuration in Enterprise networks," presented at IEEE International Conference on Network and Service Management – CNSM, 2010.

J. Amutha was born on August 31, 1981 in Kanyakumari District, Tamil Nadu, India. She got the B.Sc. degree in computer science from Manonmaniam Sundaranar University, Tirunelveli in 2002. Subsequently, she obtained the M.Sc. degree in computer science from Bharathiar University, Coimbatore in 2004. She received her M.Phil degree in computer science from the Madurai Kamaraj University, Madurai in the year 2005. She worked as an assistant professor for 8 ½ years in three colleges: Jayaraj Annapackiam College, Theni District, Arul Anandar College, Madurai and St.Joseph's College, Tiruchirappalli. Currently, she is doing her research in the area of computer networks and security in the Department of Computer Science, St. Joseph's College, Tiruchirappalli, Tamil Nadu, India. She has published her research articles in various journals and attended variouss workshops, seminars and conferences.

S. Albert Rabara was born on July 31, 1962 in Tamil Nadu, India. He obtained his B.Sc. degree and M.Sc. degree in physics from Madurai Kamaraj University, Madurai in the year 1983 and 1985 resspectively. He received his Ph.D degree in the field of computer science from Bharathidasan University, Tiruchirappalli in 2001. He started his carrier as an assistant professor in the Department of Computer Science, St. Joseph's College, Tiruchirappalli since 1989. Currently, he is working as an associate professor in the Department of Computer Science, St.Joseph's College (Autonomous), affiliated to Bharathidasan University, Tiruchirappalli. An expert in the field of information and communication technology and security, he is a consultant for several colleges in Tamil Nadu. He has 27 years of teaching and research experience and guided nine Ph.D scholars.