Design and Implementation of Mobile IPv6 Data Communication in Dual Networks

Chaman Singh[1] , Sanjeev Kumar[2], Sanjeev Kumar[3] and K.L.Bansal[4]

[1] Department of Computer Application, Govt. P.G. College, Chamba
Affiliated to H.P.University , Shimla , Himachal Pradesh 176310, India

[2]Department of Journalism and Mass Communication, Govt. P.G. College, Chamba
Affiliated to H.P.University , Shimla , Himachal Pradesh 176310, India

[3]Department of Physics, Govt. P.G. College, Chamba
Affiliated to H.P.University , Shimla , Himachal Pradesh 176310, India

[4] Department of Computer Science, H.P.University, Shimla
Himachal Pradesh 171005, India

Abstract

Dual Stack Mobile IPv6 is an extension of Mobile IPv6 to support mobility of devices irrespective of IPv4 and IPv6 Networks. This is implemented by combining different modules. IPv4 private networks are behind Network Address Translation (NAT) devices. So, to bypass the Binding Update and Binding Acknowledgment by NAT, we need to encapsulate it in User Datagram Protocol (UDP) Packets. So, the Dual Stack Mobile IPv6 should support NAT Traversal and Detection. With the support of NAT Detection and Traversal Module in Dual Stack Mobile IPv6, the mobile node is able to move freely from IPv6 Network to IPv4 Network or vice-versa. The main objective of not breaking the connectivity at the time of switching from one network to other is accomplished by NAT Module in Dual Stack Mobile IPv6.

Keywords: *Dual Stack, Network Address Translation, Detection, Tunnelling, Home Agent, Mobility.*

1. Introduction

IPv6 is introduced generally to resolve the address space issues and also provides several advanced features. Dual Stack Mobile IPv6 is an extension of Mobile IPv6 to support mobility of devices irrespective of IPv4 and IPv6 network. The application interface is required to exchange mobility information with Mobility subsystem [1]. Mobile IPv6 (MIPv6) is a protocol developed as a subset of Internet Protocol version 6 (IPv6) [2] to support mobile connections. MIPv6 [3] allows a mobile node to transparently maintain connections while moving from one subnet to another. The Mobile IPv6 protocol takes care of binding addresses between Home Agent (HA) and Mobile Node (MN). It also ensures that the Mobile Node is always reachable through Home Agent. Each mobile node is always identified by its home address [4], regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about its current point of attachment to the Internet. The protocol provides for registering the care-of address with a home agent. The home agent sends datagram's destined for the mobile node through a tunnel to the care-of address. After arriving at the end of the tunnel, each datagram is then delivered to the mobile node. Currently, two mobility management protocols are defined for IPv4 and IPv6. Deploying both in a dual stack mobile node introduces a number of problems. This has been improved [5]. Mobile IPv6 uses IP Security (IPSec) to protect signaling between the home agent and the mobile node [6] [22]. Generic Packet Tunneling [7] Specifies a method and generic mechanisms by which a packet is encapsulated and carried as payload within an IPv6 packet. The forwarding path between the source and destination of the tunnel packet is called an IPv6 tunnel. The technique is called IPv6 tunneling. The current Mobile IPv6 [3] and Network Mobility [8] [21] specifications support IPv6 only. These extend those standards to allow the registration of IPv4 addresses and prefixes, respectively, and the transport of both IPv4 and IPv6 packets over the tunnel to the Home Agent. [9] Allows the Mobile Node to roam over both IPv6 and IPv4, including the case where Network Address Translation is present on the path between the mobile node and its home agent. Middle Boxes [10], such as Firewalls and Network

Address Translators (NAT) [11], are an important component for a majority of Internet Protocol (IP) [5] networks today. Current IP networks are predominantly based on IPv4 [5] technology, and hence various firewalls as well as Network Address Translators have been originally designed for these networks. NAT's are necessary to overcome the IPv4 address space limitations of many network domains.

A network address translator a box that interconnects a local network to the public internet, where the local network runs on a block of private IPv4 addresses [12]. In the original design of the internet architecture, each IP address was defined to be globally unique and globally reachable. In contrast, a private IPv4 address is meaningful only within the scope of the local network behind a NAT and as such, the same private address block can be reused in multiple local networks [20] , as long as those networks do not directly talk to each other. Instead, they communicate with each other and with the rest of internet through NAT boxes. Mobile IPv6 (MIPv6) [15] is a protocol developed as a subset of Internet Protocol veMyon 6 (IPv6) to support mobile connections. The impact to IPv4, which changes IP address semantics, provide ample evidence , since now coming time MIPv6 are in progress so need of network address translation traversal and detection on Dual Stack implementation of mobile IPv6 [16]. NEPL (NEMO Platform for Linux) [17] is a freely available implementation of DSMIPv6 for Linux platform. The original NEPL release was based on MIPL (Mobile IPv6 for Linux) [18]. Without the support of NAT Detection and Traversal module in DSMIPv6, the mobile node will not be able to move freely from IPv6 network to IPv4 network or vice-versa. Connectivity also breaks at the time of switching from one network to other will be accomplished by this research.

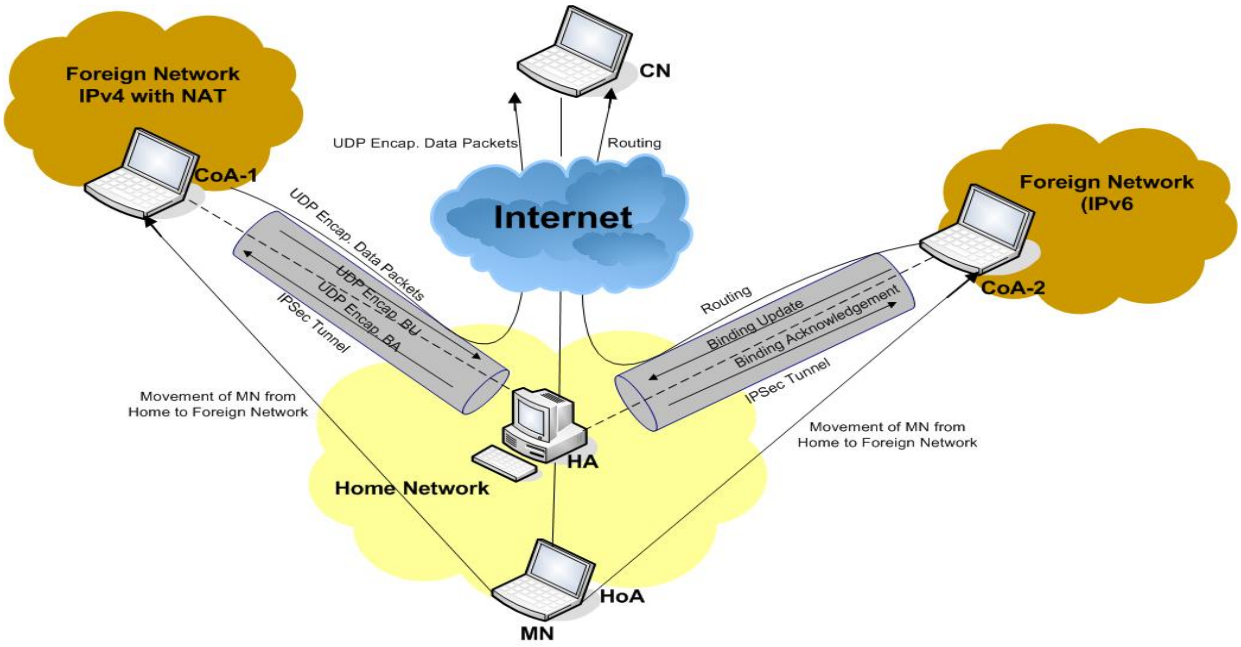

Figure 1:- Basic Function of Dual Stack Mobile IPv6

2. Dual Stack Implementation of Mobile IPv6

First, NEPL (NEMO Platform for Linux) [17] is a freely available implementation of DSMIPv6 for Linux platform. The original NEPL release was based on MIPL (Mobile IPv6 for Linux) [18]. In Figure-1: Basic Operation of DSMIPv6, all Mobile Nodes (MN) has a fixed address, called a Home Address (HoA), assigned by Home Agent. When the Mobile Node moves to other networks, it gets Care-of Address (CoA) from foreign network. Mobile Node sends a Binding Update (BU) message to its Home Agent. Then Home Agent replies to the Mobile Node with a Binding Acknowledgement (BA) message to confirm the request. When Mobile Node is moved to any foreign network all packets sent to the Home Agent will be IPSec encrypted. A bi-directional tunnel is established between the Home Agent and the Care of address of the Mobile Node after the binding information has been successfully

exchanged. DSMIPv6 extends the MIPv6 and NEMO [6] Basic Support standards to allow mobile nodes to roam in both IPv6 [23] and IPv4-only networks. The following features are supported by the DSMIPv6 Architecture:-

1. The mobile node can register an IPv6/IPv4 Care of address to its Home Agent and so roam in IPv6-only networks and IPv4-only networks by the use of IPv6 and IPv6-in-IPv4 tunnels between the Node and its Home Agent.
2. A Network Address Translation Detection and Traversal Mechanism allow the Mobile Node to communicate with its Home Agent even though it uses an IPv4 private address as a Care of address. The signaling messages are always UDP encapsulated in IPv4 network. However, when the Mobile Node is located behind a NAT, data traffic is also encapsulated in UDP.
3. Securing the signaling packets between Home Agent and Mobile Node when Mobile Node is moved to foreign network and Session management on movement from one foreign link to another.

3. Solution Description

Solution is an extension to the existing NEPL solution provided by Nautilus [17]. We validated DSMIPv6 functionality as per the requirements provided against the draft, along with other IETF standards. We took the baseline architecture implementation from the Nautilus6 which uses Linux platform. The below mentioned steps are taken by us to achieve the requirements:-

1. Setup DSMIPv6 Test Lab using Kernel 2.6.28.2 and UMIP veMyon 0.4. In order to test the basic functionality between Home Agent and Mobile Node according to [3] the Test Bed has been setup.
2. Code change in MIP6 Daemon and Linux kernel and also applied the open source patches/packages .The Routing Advertisement daemon (radvd), IPSec daemon (strongswan) and Web Server (httpd) daemon has been configured on Home Agent.
3. The Mobile Node is configured with IPSec daemon (strongswan). Mobile Node gets IPv6 address whenever it is moved to any IPv6 foreign network through the radvd server running on the router.
4. When Mobile Node is moved to IPv4 network, it gets configured with IPv4 Care of address from the DHCP server running on IPv4 Router. In IPv4 network, DHCP is configured on the private network behind router. The network behind IPv4 router can be public or private.

4. Modules Representation in Dual Stack Mobile IPv6

MIPL (Mobile IPv6 for Linux) [24] is an open-source implementation of the Mobile IPv6 standard for the GNU/Linux operating system. MIPv6 is a user space for Mobile Node and Home Agent which aims at providing the necessary changes to MIPL in order to run on the latest kernels.Figure-2: Block Diagram of MIPv6 shows the internal data flow between two major components i.e. Home Agent and Mobile Node. Both of these two components consist of several helper modules which are also shown in this figure. This section describes IPv4 address assignment mechanism used by DSMIPv6.DHCP DNA module is used to obtain IPv4 address from the DHCP server running on IPv4 network.

4.1 DNA / DHCP Module

Module describes IPv4 address assignment mechanism used by DSMIPv6. When Mobile Node moves to IPv4 FL (Foreign Link) and its egress interface becomes enabled, Mip6d code in Mobile Node listens for Router Advertisement message, and since it does not receives Router Advertisement message in IPv4 FL, it gets timeout and sends Router Solicitation message (that will request the router to generate the Router Advertisement message immediately rather than at there next scheduled time), and Mobile Node wait for some time interval for Router Advertisement message before repeating the same procedure of sending Router Solicitation message. Meanwhile after sending Router Solicitation message, mip6d daemon will check the presence of DHCP server on the Egress interface link of Mobile Node by sending the DHCP discover message and wait for DHCP offer packet. Since the DHCP server is running on the IPv4 FL, it gets the IPv4 address from DHCP server and then mip6d code maps IPv4 address to IPv6 address, which is further used as Care of address. Mip6d daemon sets the default route on Mobile Node figure 3.

4.2 Movement Detection Modules

Describe Movement Detection in DSMIPv6 implementation. The movement of a mobile node away from its home link is transparent to transport and higher-layer protocols and applications. Describe Movement Detection in DSMIPv6 implementations. The Movement detection uses Neighbor Unreachablility Detection [13] to detect when the default router is no longer bi-directionally reachable, in which case the mobile node must discover a new default router (usually on a new link). However, this

detection only occurs when the mobile node has packets to send. When the mobile node detects handover, it expire the previous routers and Care-of-Address (es) and selects a new default router as a consequence of Router Discovery, and then performs Prefix Discovery with that new router to form new care-of address (es). It then registers its new primary care-of address with its home agent. After updating its home registration, the mobile node then updates associated mobility bindings in correspondent nodes. It triggers a movement event and then detects that Mobile Node is in foreign network. Route is modified and Home Address which was previously assigned to the physical interface is now moved to the tunnels. This is handled in 'mn.c'.

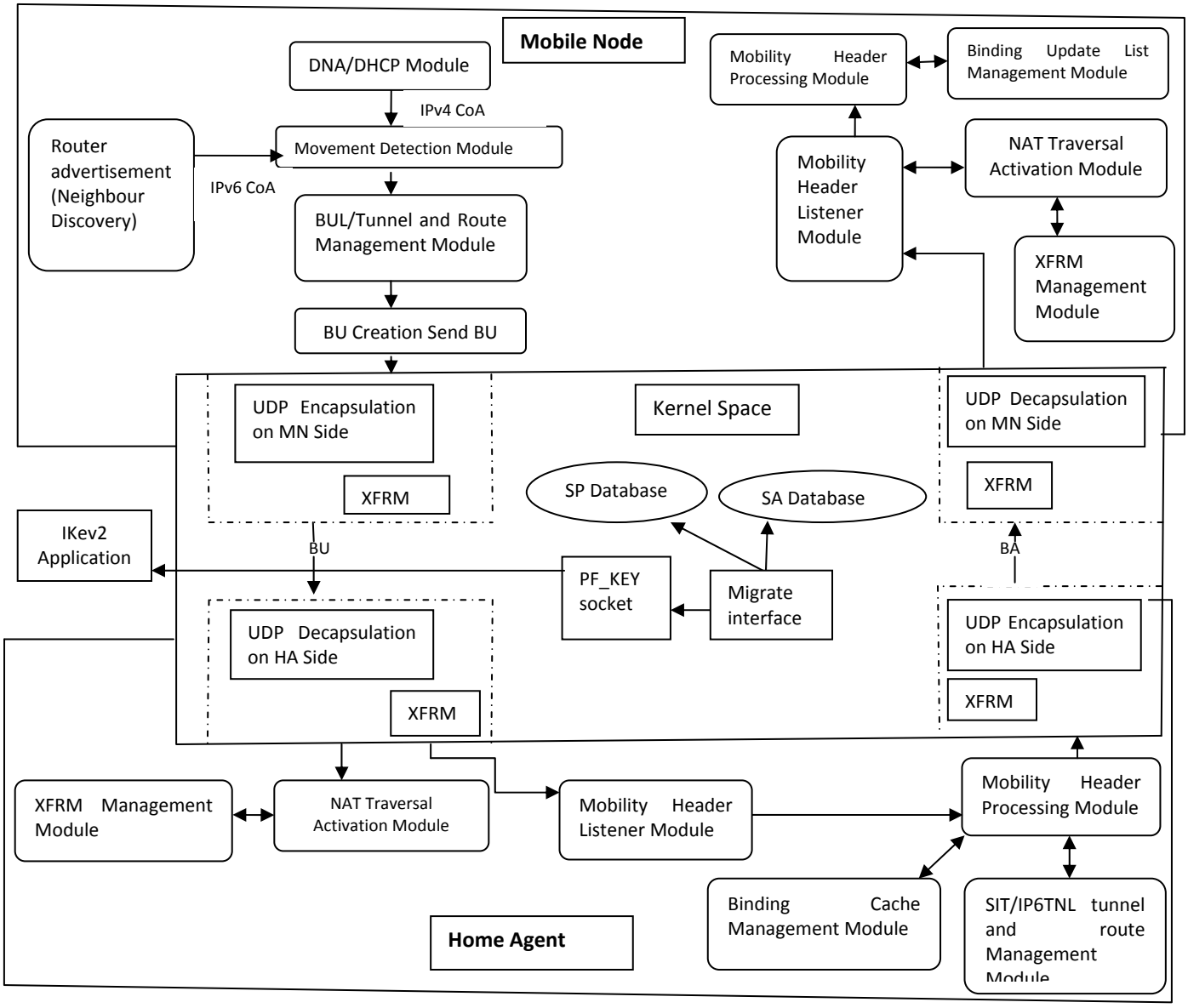

Figure 2: MIPL for Home Agent and Mobile Node

4.3 Binding Management Modules

Describe Binding Management in DSMIPv6 implementation. When a Mobile Node moves between different networks, it is essential that binding update messages are sent to that node's Home Agent and Correspondent Nodes as soon as possible, in order to facilitate a fast handoff. Mobile Nodes therefore cannot rely on the soft state timeout mechanism used in binding caches to refresh stale bindings maintained by Correspondent Nodes (typical binding lifetimes are of the order of minutes).

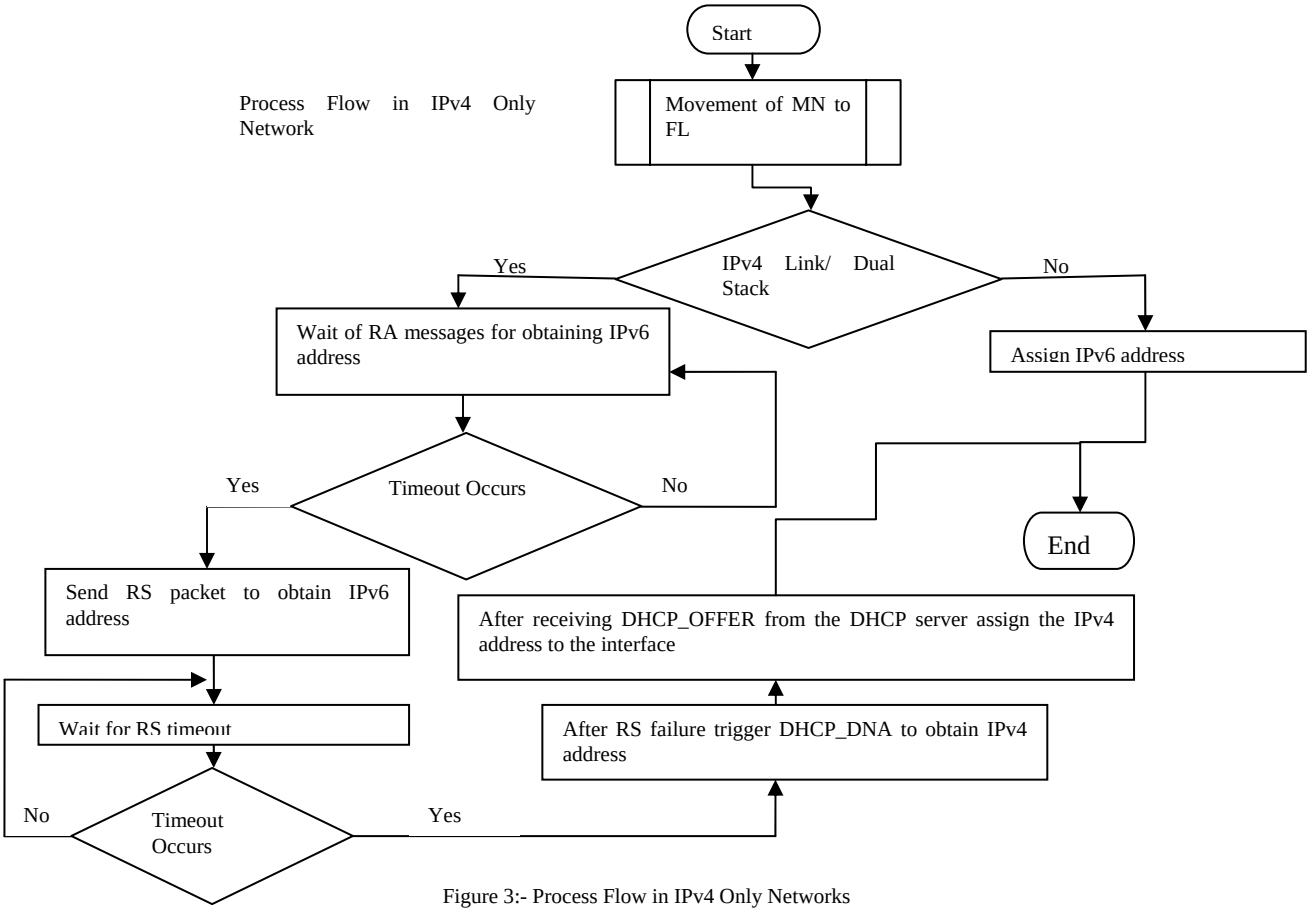

Figure 3:- Process Flow in IPv4 Only Networks

An additional data structure, the binding update list, is therefore kept by Mobile Nodes, which maintains state on any Correspondent Nodes or Home Agents. And in Home Agent mobile IPv6 binding cache maps home addresses to the current care-of addresses for each mobile node. This allows the home agent to tunnel traffic to the mobile node at its current location, and allows a correspondent node to send packets directly to a mobile node at its current location. Binding Management Module is classified as:

1. Binding Update List
2. Binding Cache

Binding Update: When Mobile Node moves to any Foreign Link, Mip6d code in Mobile Node initiate binding update functionality after configuring Care of address either from Router Advertisement message received in IPv6 or Dual stack FL or from DHCP server in IPv4 FL on the egress interface of Mobile Node. After Mobile Node configures Care of address on its egress interface, it creates BUL which consists of information about Mobile Node's Home Address, Care of address, CN address, life time and delay time of this binding message in seconds and set of various flag.

Binding Update List format is as follows:
== BUL_ENTRY ==
Home address 2001: x: x: x: x: x: x: x Care-of addresses 2001: x: x: x: x: x: x: x
CN address 2001: x: x: x: x: x: x: x Lifetime = 32, delay = 1500
Flags: IP6_MH_BU_HOME
IP6_MH_BU_ACK IP6_MH_BU_TLV

When Mip6d code in Mobile Node creates BUL successfully, it send Binding Update message to Home Agent to register the new Care of address of Mobile Node to Home Agent. So that Home Agent gets updated with current Care of address of Mobile Node.

Binding Cache: Mip6d code in Home Agent received Binding Update message sent by Mobile Node when it moves to any Foreign Link or when it directly boots in IPv6/IPv4 FL. Home Agent process BU by performing DAD (dynamic address discover)[14] and latter parse Binding Update message. After paMyng the binding update message Home Agent creates or updates its Binding Cache entry. Binding Cache entry consists of

Mobile Node's Home Address, Mobile Node's Care of address, its local address, lifetime and sequence no.

Binding Cache entry format is as follows:

== BC_ENTRY ==

HoA 2001: a: b: 0:0:0:0:1 status registered CoA 2001: a: d: 1:20c:29ff:fea0:4026 flags AH-- Local 2001: a: b: 0:0:0:0:1000 Lifetime 23 / 32 sequence 3435 Unreach 0 / 959299 retry -2

After updating its Binding Cache entry, the mip6d code creates devices to tunnel traffic to Mobile Node. Mip6d code in Home Agent creates and send Binding Acknowledgment message to Mobile Node so that Mobile Node gets acknowledged that it's new Care of address gets successfully registers with Home Agent. When Mobile Node receives Binding Acknowledgment message, mip6d code in Mobile Node parses the BA packet and update the BUL entry. It checks for various options set in BA and proceed accordingly. If NAT is detected between Mobile Node and Home Agent, it set xfrm policies/states to UDP Encapsulate IPv6/IPv4 data traffic to bypass NAT. Mip6d daemon sets the callback function to resend the BA, once lifetime of BUL entry is expired. And finally set the binding update timer to decrease the lifetime of BUL entry. When Mobile Node moves back from any FL to Home Link, Mip6d code in Mobile Node sends Binding Update message with lifetime set as zero to Home Agent to indicate that it as returned to Home Link mip6d code in Mobile Node deletes corresponding BUL entry. On Home Agent side Mip6d code receives BU message with lifetime set as zero, it indicate that Mobile Node moved to Home Link, so it deletes corresponding Binding Cache entry and send Binding Acknowledgment back to Mobile Node.

4.4 Route and Tunnel Management Modules

Tunnel and Route Management module figure 4 is mainly responsible for tunneling, when mobile node changes from IPv6 to IPv6, IPv6 to IPv4 and vice versa network. This module configures sit and ip6tnl interface via IOCTL system call which in turns performs the task at kernel level. Route Management handles the return rout-ability with CN. Some data structures are being used between some of the important functions in Tunnel Management module. Some user land data structures used in various routines in tunnel management module. Some data structures used in various routines in tunnel management module.

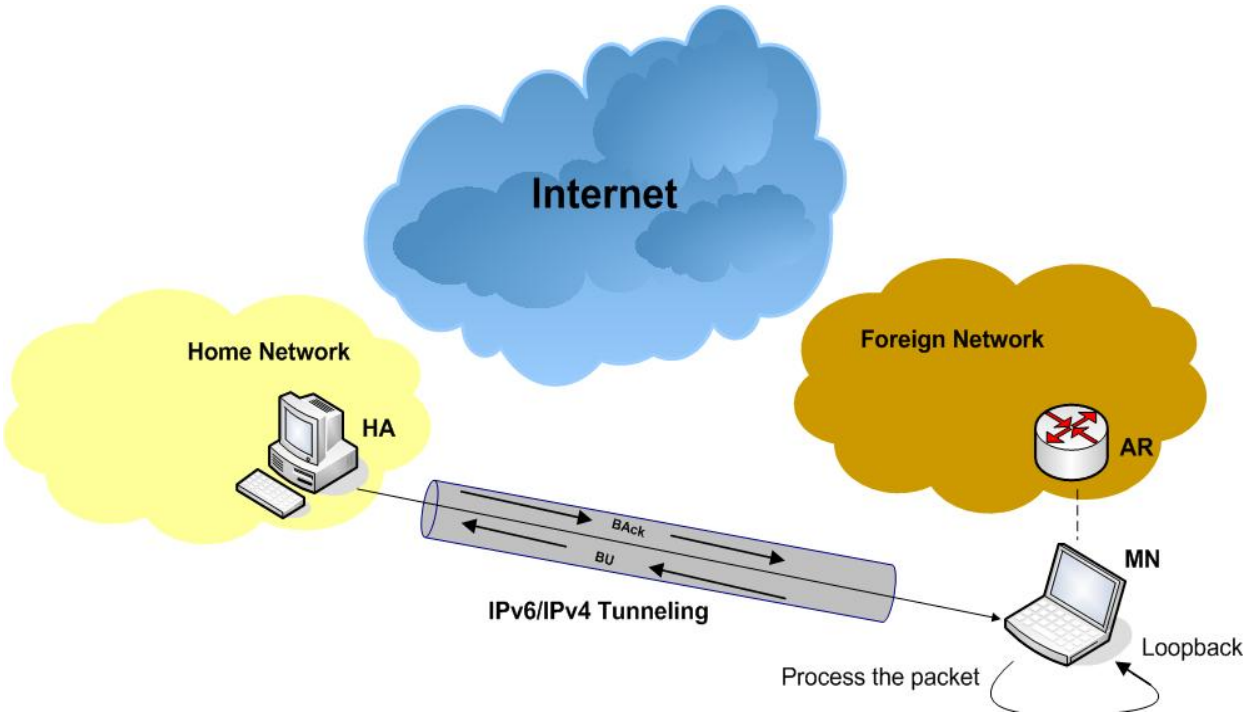

Figure 4 : Tunnel and Route

4.5 XFRM and IPSEC Management Modules

XFRM [15] is a packet transformation framework residing in the Linux kernel. It performs operations on IP packets such as inserting, modifying headers, UDP encapsulation and de-capsulation. DSMIPv6 XFRM module will take the advantage of existing IPSEC transformation and defines a simple UDP encapsulation scheme. IPSEC module is responsible for interaction with IKE through MIGRATE messages. IPSec will be used to protect the following traffic between Home Agent and Mobile Node.

1. BU/BA messages.
2. Mobile prefix sollicitation and advertisement messages.
3. Normal traffic between Mobile Node and Home Agent.
4. All tunneled normal traffic between Mobile Node and correspondent Node.

In Mip6d, the Mobile Node and the Home Agent uses IPsec Security Associations in transport mode to protect BU/BA messages, since the MN may change its attachment point to the Internet, it is necessary to update its endpoint address of the IPsec SAs. This indicates that corresponding entry in IPsec databases (Security Policy and SA databases) should be updated when Mobile Node performs movements. IPSec is used to protect the following traffic between Home Agent and Mobile Node. When Mobile Node move in FL a new Care of address is assign to it by FL network. After detecting the movement following steps are taken to create IPSec tunnel.

1. Mip6d issues a PF_KEY MIGRATE message to the PF_KEY socket. The operating system validates the message and checks if corresponding security policy entry exists in SPD. When the message is confirmed to be valid, the target SPD entry is updated according to the MIGRATE message. If there is any target SA found that is also target of the update, those should also be updated.
2. After the MIGRATE message is successfully processed inside the kernel, it will be sent to all open PF_KEY sockets. The IKE daemon receives the MIGRATE message from its PF_KEY socket and updates its SPD and SAD images. The IKE daemon may also update its state to keep the IKE session alive. After that ESP protected BU is send with K–bit set.

Mobile IPv6 specifies a flag named Key Management Mobility Capability bit (K-bit) in Binding Update (BU) and Binding Acknowledgement (BA) messages, which indicates the ability of IKE sessions to survive movement. When both the Mobile Node and Home Agent agree to use this functionality, the IKE daemons dynamically update the IKE session when the Mobile Node moves. The following methods are used.

4.6 NAT Detection and Traversal Modules

NAT (Network Address Translation (figure 5)) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. In DSMIPv6 the mip6d daemon should bypass NAT, when Mobile Node is behind NAT' ed device in IPv4 FL. NAT detection is done when the initial Binding Update message is sent from the mobile node to the home agent. When located in an IPv4-only foreign link, the mobile node sends the Binding Update message encapsulated in UDP (User Datagram Protocol) and IPv4; this is handled in xfrm.c file. The mip6d daemon adds xfrm policy/state for UDP encapsulation for BU packet. When the home agent receives the encapsulated Binding Update, it compares the IPv4 address of the source address field in the IPv4 header with the IPv4 address included in the IPv4 care-of address option. If the two addresses match, no NAT device is in the path. Otherwise, a NAT is detected in the path and the NAT detection option is included in the Binding Acknowledgement. The Binding Acknowledgement, and all future packets, is then encapsulated in UDP and IPv4. Note that the home agent also stores the port numbers and associates them with the mobile node's tunnel in order to forward future packets. This is handled in ha.c file. The mip6d daemon adds the xfrm polices/states for UDP encapsulation of BA and IPv6/IPv4 data traffic. Upon receiving the Binding Acknowledgement with the NAT detection option, the mobile node sets the tunnel to the home agent for UDP encapsulation. Hence, all future packets to the home agent are tunneled in UDP and IPv4. If no NAT device is detected in the path between the mobile node and the home agent then IPv4/IPv6 data traffic is not UDP encapsulated. A mobile node will always tunnel the Binding Updates in UDP when located in an IPv4-only network. Essentially, this process allows for perpetual NAT detection. Similarly, the home agent will encapsulate Binding Acknowledgements in a UDP header whenever the Binding Update is encapsulated in UDP. This is handled in mn.c and xfrm .c file. The mip6d daemon adds xfrm polices/states for UDP encapsulation of IPv6/IPv4 data traffic, when NAT is detected between Mobile Node and Home Agent.

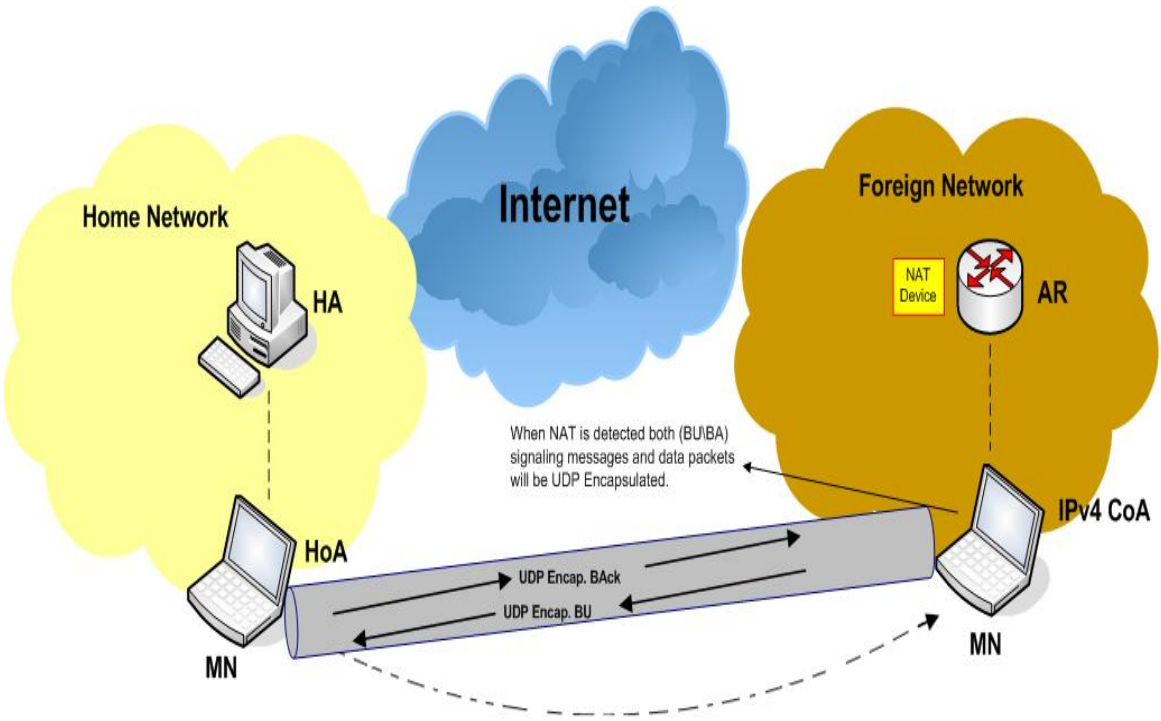

Figure-5: NAT Detection/Traversal

4.7 Mobility Listener Modules

The Mobility Header is an extension header used by mobile nodes, correspondent nodes, and home agents in all messaging related to the creation and management of bindings. The Mobility Header is identified by a Next Header value of 135 in the immediately preceding header. Header is used to carry various messages. A mobile node uses the Home Test Init message to initiate the return rout-ability procedure and request a home keygen token from a correspondent node. The Home Test Init message uses the MH Type value 1. The Home Test message is a response to the Home Test Init message, and is sent from the correspondent node to the mobile node. The Home Test message uses the MH Type value 3.A mobile node uses the Care-of Test Init message to initiate the return rout-ability procedure and request a care-of keygen token from a correspondent node. The Care-of Test Init message uses the MH Type value 2.The Care-of Test message is a response to the Care-of Test Init message, and is sent from the correspondent node to the mobile node. The Care-of Test message uses the MH Type value 4. The Binding Update message is used by a mobile node to notify their nodes of a new care-of address for itself. The Binding Update uses the MH Type value 5.The Binding Acknowledgement is used to acknowledge receipt of a Binding Update. The Binding Acknowledgement has the MH Type value 6.The Binding Refresh Request message requests a mobile node to update its mobility binding. The Binding Refresh Request message uses the MH Type value 0.The Binding Error message is used by the correspondent node to signal an error related to mobility, such as an inappropriate attempt to use the Home Address destination option without an existing binding. The Binding Error message uses the MH Type value 7.

5. Conclusions

This paper is one of the earliest attempts in the community to investigate the problems and impacts when middle boxes, especially NAT devices are placed in Dual stack Mobile IPv6are implemented in computer laboratory. With the support of modules in DSMIPv6, the mobile node is able to move freely from IPv6 network to IPv4 network or vice-versa. It accomplishes the main objective of not breaking the connectivity at the time of switching from one network to other. The transition from IPv4 to IPv6 will be time consuming process, so there will be time, when both IPv4 and IPv6 networks will be there and there will be always being scope for further development.

Acknowledgments

The authors would also like to express their sincere thanks to Mr. Manish Jamwal for his worthy Help and support for This Work.

References

[1]. T.Momoseetal, The Internet Engineering Task Force, July 2005 “The application interface to exchange mobility information with Mobility subsystem”, Internet Drafts draft-momose-mip6-mipsock-00.
[2]. Vida, R. and L. Costa, Eds., RFC 3810, June 2004. "Multicast Listener Discovery VeMyon 2 (MLDv2) for IPv6".
[3]. Perkins, C., RFC 3344, August 2002. "IP Mobility Support for IPv4".
[4]. Johnson, D., Perkins, C., and J. Arkko, RFC 3775, June 2004. "Mobility Support in IPv6".
[5]. G.Tsirtsis, Qualcomm, H. Soliman, Elevate Technologies, [RFC 4977], August 2007. “Dual Stack Mobility”.
[6]. Arkko, J., Devarapalli, V. and F. Dupont, RFC 3776, June 2004. "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents".
[7]. Conta, A. and S. Deering, RFC 2473, December 1998. "Generic Packet Tunneling in IPv6 Specification".
[8]. F Ralf Spenneberg, ipsec-howto, 2003-08-18.
[9]. Soliman, Ed., Elevate Technologies, November 3, 2008. Mobile IPv6 Support for Dual Stack Hosts and Routers draft-ietf-mext-nemo-v4traversal-06.txt.
[10]. B. Carpenter and S. Brim. Middleboxes: Taxonomy and Issues. RFC 3234, Internet Engineering Task Force, February 2002.
[11]. K. Egevang and P. Francis. The IP Network Address Translator (NAT). RFC 1631, Internet Engineering Task Force, May 1994.
[12]. Y.Rekhter et al, “Address allocation for private Internets” RFC 1918, 1996.
[13]. J. Rosenberg et al., “STUN: Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NATs),” RFC 3489, 2003.
[14]. Rosenberg, R. Mahy, and P. Matthews, “Traversal Using Relays around NAT (TURN),” draft-ietf-behave-turn-08, 2008.
[15]. C. Huitema, “Teredo: Tunnelling IPv6 over UDP through Network Address Translations (NATs),” RFC 4380, 2006.
[16]. K.L.Bansal, Chaman Singh, “Dual Stack Implementation of Mobile IPv6 Software Architecture”, IJCA- Volume 25, No 9, July 2011.
[17]. NEPL (NEMO Platform for Linux) how to, June 24th, 2009.
[18]. MIPL (Mobile Ipv6 for Linux), how to, 2004-4-20.
[19]. K.L.Bansal, Chaman Singh, “NAT Traversal and Detection on Dual Stack Implementation of Mobile IPv6”, IJCA-Volume 29, No 7, September2011.
[20]. L Cao, G J Qi, S F Tsai, M H Tsai, A D Pozo, T S Huang, et al.” Multimedia Information Networks in Social Media“ in Social Network Data Analytics -2011.
[21]. Mark S. Taylor, Willium Waung and Mohsen Banan, “Imternetwork Mobility – The CDPD Approach”,Prentice Hall PTR Upper Saddle River NJ 07458ISBN-0-13-209963-5.
[22]. Christian Huitema, “IPv6- The New Internet Protocol”, Prentice Hall PTR Upper Saddle River NJ 07458 ISBN 0-13-241936-X.
[23]. Scott O. Bradner, Allison Mankin ,” IPng Internet Protocol Next Generation” Addison-Wesley IPng Series-Massachusetts 01867. ISBN 0-201-63395-7.
[24]. Viktor T.Toth ,” Linux:-A Network Solution for Your Office”, Sams Publication,USA ISBN 0-672-31628-5.

Chaman Singh is working as Assistant Professor Cum HOD Department of Computer Application, Govt. P.G. College, Chamba Himachal Pradesh University Shimla India. He received Master of Computer Application from Department of Computer Science H.P.University. He also qualified UGC-NET-2006 and Doctor of Philosophy in Computer Science is Under Submission from H.P.University. Having more then 4 years of working experience in Development, Teaching and Networks.

Sanjeev Kumar is working as Assistant Professor Cum HOD Department of Journalism and Mass Communication, Govt. P.G. College, Chamba Himachal Pradesh University Shimla India. He received Master of Philosophy in Journalism and Mass communication from H.P.University. Having more then 3 years of working experience in Teaching and Communication.

Sanjeev Kumar is working as Assistant Professor in Department of Physics Govt. P.G. College, Chamba Himachal Pradesh University Shimla India. He received Master of Philosophy in Physics from Punjabi University Patiala. Having more then 6 years of working experience in Physics and Teaching.

Dr. K.L. Bansal is working as Associate Professor in Department of Computer Science , H.P.University Shimla Himachal Pradesh. Received MCA from P.U. Chandigarh and Ph.D. from H.P.University Shimla Himachal Pradesh India. More then 15 year of experience in Teaching and Guidance.