Address Resolution Technique of Packet Transmission

[1]CHANDAN KUMAR PANDA, *Gandhi Institute of Excellent Technocrats, Bhubaneswar, India*

[2]SANGRAM SAHU, *BRM League of Institution, Bhubaneswar, Odisha, India*

***Abstract*—**Packet transfer via address resolution has been the mainstay of Internet communication via packet transmission between computer networks. In comparison to IPv4, packet transmission was implemented in both IPv4 and IPv6, with the attention gradually shifting to IPv6 because IPv6 has a 128-bit address space and supports billions of IP addresses. Before packets are sent to their final destination, packet transmission involves the mapping of multiple addresses among computers on the network. And it's here that address resolution comes in. Direct Mapping and Dynamic Binding, which is the most often used method, are used to resolve IPv6 packets. The study will concentrate on a direct mapping technique using a new methodology called as direct dynamic neighbor. However, the study will concentrate on the Direct mapping strategy, as well as a novel methodology known as direct dynamic neighbor, which is a combination of Dynamic Binding and Direct mapping methods for sending packets in the same network. Packet transmission will be greatly improved with the new approach, as packets can be transmitted straight to their destination. In order to determine the efficacy of each methodology, the research will compare the techniques of each approach briefly. Other areas to compare include packet transmission for each technique, as well as the number of steps each method takes to send a packet from source to ultimate destination.

Keywords: Direct mapping, Dynamic binding, Neighbor Discovery Protocol, Packets Transmission, Direct Dynamic Neighbor

I. INTRODUCTION

Packet transmissions are carried out using Internet Protocols (IPs), especially IPv4 and the more recently adopted IPv6, as one of the primary means of sending data between network machines. Before packets are dispatched to their final destinations, the procedures for packet transmissions map IP and MAC addresses among machines using address resolution. Direct mapping and dynamic binding are two methods for implementing packet transmission procedures. The process of sending packets takes longer with dynamic binding because it necessitates the use of a protocol to send back and forth Neighbor Discovery (ND) messages such as Neighbor Solicitation (NS) and Neighbor Advertisements (NA) to resolve addresses before packets are sent, resulting in time and packet delivery efficiency delays [1].].

With Direct Mapping in IPv6, the destination's physical address (receiving computer) is already known thanks to the IPv6 Interface Identifier, which eliminates multiple discussions before packets are sent to their final destination with the help of the Neighbor Discovery Protocol (NDP). TCP/IP is responsible for packet transmission over networks because it resolves both IP addresses and physical MAC addresses of network computers through an address resolution procedure that maps one host network to another to validate linkages and communication [2]. When a network computer wants to send a packet or datagram to another network host, for example, Address resolution algorithms [3] link the IP address to the specific physical address of the intended receiver. Direct mapping's main task is to map IP addresses to physical addresses, such as a computer's MAC address, in order to provide faster access times and efficient packet delivery to specific hosts. In order to deliver packets, Direct mapping and Dynamic binding employ the ND protocol to discover link nodes, link layer addresses of various nodes, and check for availability of routers within the discovery range [3]. With the introduction of the IPv6 Interface Identifier, a built-in interface embedded in the IPv6 protocol that ensures direct transmission of packets to final destinations because the receiving computer's destination MAC address has already been built in, the issues of direct mapping approach of transmitting packets have become simpler.

Because NDP nodes function by exchanging messages via ICMPv6 (Internet Control Message Protocol v6), which is part of ICMPv6 packet with NDP specified fields, encapsulated by IPv6 header as well as link laye, its main purpose is to help solve addresses and physical MAC addresses as well as discover all neighbouring routers within the same link to transmit packets because NDP nodes functions by exchanging messages via ICMPv6 (Internet Control Message Protocol v6) To enable fast and convenient transmission, the research will develop a Direct Dynamic Neighbor (DDN) algorithm for resolving addresses before packets are sent, which is derived from the best aspects of direct mapping, dynamic binding, and NDP. DDN, a proposed new technology, will speed up the process.

The IPv6 Identifier [6] is used to transport packets in the network and to ensure packet transmission efficiency as the destination for the receiving host. In terms of time and efficiency, the results will compare the novel technique to Dynamic binding..

II. Related study

When opposed to dynamic binding, previous research has shown that packet transmission in IPv6 is substantially more efficient in transmitting packets in direct mapping. Kozirok [7] looked at converting and mapping MAC addresses, EUI-64, and IPv6 Interface Identifiers. Neighbor Discovery (ND) protocol enables the discovery of link nodes, link layer addresses of various nodes, and search for availability routers within the discovery range in order to deliver packets, according to studies on IPv6 packet transmission through direct mapping and dynamic binding. Kim et al. [12] explored how Neighbor Discovery works in any network, with the main goal of resolving IP addresses and physical addresses, as well as locating all nearby routers inside the same link, in order to improve network performance. The major goal of Neighbor Discovery, according to Kim et al [12], is to resolve IP addresses and physical addresses, as well as to discover any nearby routers inside the same link so that packets can be sent. Based on the MAC 48 bits or EUI-64 address of the hosts' interface, ND may automatically generate the interface Identifier. ND nodes also exchange messages using ICMPv6 (Internet Control Message Protocol v6), which is part of an ICMPv6 packet that contains ND-specified fields and is encapsulated by IPv6 and link layer headers. Link-local addresses, global unicast addresses, and multicast addresses are among the numerous types of addresses contained in IPv6 source and destination address fields, according to Narten et al [6]. Next-hop determination in ND is defined by Hines [14] as an algorithm for mapping and determining the IP ultimate destination address before forwarding the packet to the IP address of the destination neighbour. In other words, the technique resolves the mapping between an IP destination address and the traffic neighbor's IP address. For the Next hop neighbour mentioned for forwarding packets, the ND node stores a Destination Cache for already mapped IPv6 addresses of recently transmitted packets.

.

III. MATERIALS AND METHODS

The procedures needed for this research are simulations of how IPv6 packets are transmitted directly from source to destination and how addresses are resolved through DDN before a packet is transmitted. The methodology proposes a new transmission algorithm for IPv6 packets. The algorithm intends to apply some of the functions of ND mechanisms in transmitting packets such as neighbor cache and to conform to direct mapping approach as well. So the new DDN algorithm uses Interface Identifiers in IPv6 because it has lower 64 bits embedded with 48 bits MAC addresses through EUI 64 mapping which have source destination already embedded so transmission can take place without many network negotiations. The IPv6 Interface Identifier, MAC address, network topology, simulation of nodes were implemented in the same network [10]. The DDN technique for packet Transmission used IEEE EUI-64, a protocol for converting MAC 48-bit addresses to IPv6 lower 64-bit addresses. Furthermore, the new algorithm employed Interface Identifiers in IPv6 because it has lower 64-bit embedded MAC addresses with 48-bit MAC addresses using EUI-64 mapping, which specifies the final destination where packets are to be transmitted. Because the EUI-64 has 15 ones and zeros in the centre for the data connection layer, as well as the network layer filled in with the network address [11].

The following are the processes for implementing DDN for address resolution before packet transmission:

• Only one of multiple NDP message types, Neighbor cache, was kept to support the new DDN method, while others, such as Neighbor Solicitation, were dropped (NS)

Because link layer addresses are encoded as IPv6 lower 64-bit Interface Identifiers and have a destination target of packets to be transmitted, it is prudent to keep track of network information via some NDP mechanism for reference and security purposes, which is why only Neighbor Cache was chosen out of the many NDP message types. Figure 1 displays an elaborative method of how DDN packets are sent and explains the process flow of the proposed algorithm DDN. Using the suggested DDN, the number of packet transmission channels is minimised. According to Figure 1, the proposed DDN technique only has to obtain the required destination MAC address from the Neighbor cache and broadcast it. All that is required of the proposed DDN technique is to obtain the required destination MAC address from the Neighbor cache and transmit the packet to its final destination. The time it takes to send the packet is reduced since no address resolutions are necessary, and no ND messages such as NS and NA are exchanged. Because the destination address has already been encoded as part of the IPv6 Interface Identifier ID, the packet is sent to its final destination significantly faster. Because the lengthier stages used in Dynamic binding to deliver packets have been eliminated, packets can now be sent at a faster pace.

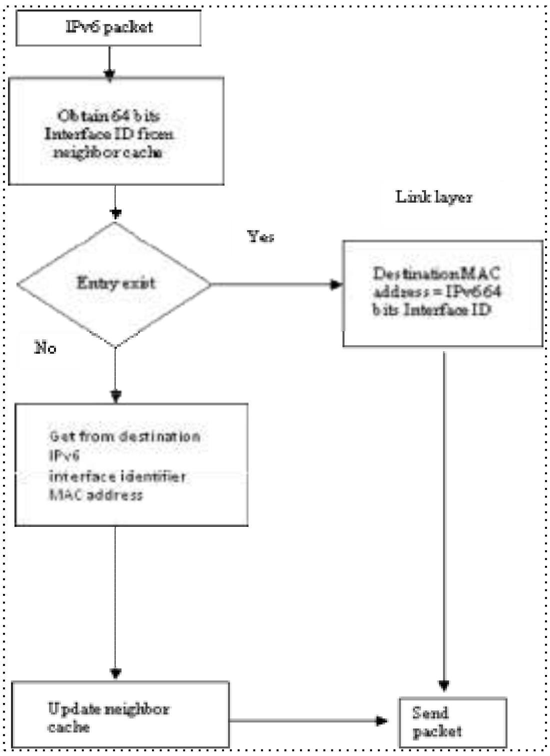

Figure-1: Algorithm of DDN for link layer

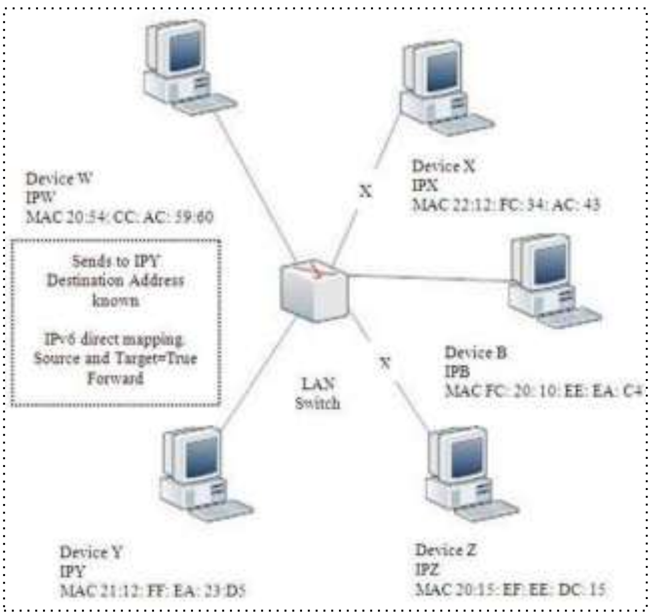

Figure-2: Proposed DDN for address resolution

This section explains how the proposed DDN algorithm sends the packets. In DDN Whenever a packet arrives from a higher protocol say, TCP/IP, the algorithm verifies the destination address for packet to be sent if it does not have any previous information stored in the Neighbor Cache. If so, the destination address is extracted from IPv6 Interface Identifier which already has the destination MAC address of the receiving host before the packet is sent. If the destination is already known because there have been previous communications among source and receiving hosts, and the information is already stored in the Neighbor Cache, the information needed to send the packet is retrieved from the Neighbor Cache before packet is transmitted to destination.

Figure 2 illustrates this, that is, when Device W intends to transmit a packet to Device Y, after applying the required NDP mechanism proposed for the DDN algorithm, the packet is transmitted from Device W to Device Y and not to Devices Z, B and X because devices Z, B and X do not have the destination MAC address that Device W wants. Also, when Device W wants to send packet to Device Y for the second time the transmission information will be retrieved from the Neighbor cache because it had stored information from earlier communication. Transmission protocols such as switches are obliged to send the packet because the destination is already resolved through the Direct mapping approach of the lower bits of IPv6 Interface Identifier ID and the DDN applied both technique functions to send packet. Thus, by using the new DDN the packet transmission steps in DDN are significantly reduced. It is possible because with the DDN, the source address and destination MAC address are already known and resolved in IPv6 Interface Identifier so the packet can be transmitted easily without having to pass through many routes as seen when using Dynamic binding approach.

IV. Evaluation

DDN as illustrated in Figure 2 has the capability to reduce the transmission time of packets as well as sending the packet to the final destination directly by avoiding various protocol negotiations, and that only the essential transmission mechanisms in sending packets are needed. The evaluation of the proposed DDN was evaluated by the following:

- Latency/Delay.
- Efficiency.

Latency is analyzed in terms of time, i.e. the time taken for the packet to reach receiving host destination. The overall latency also should improved due to shortened transmission routes the packets travel when the new algorithm DDN is used because it eliminated routes which are not necessary for the packets to reach their final destination. The proposed methodology will also be measured by efficiency where each steps of transmission from the source to targeted destination will be estimated to determine a safe delivery of packets. Figure 2 shows packet steps from A to B.

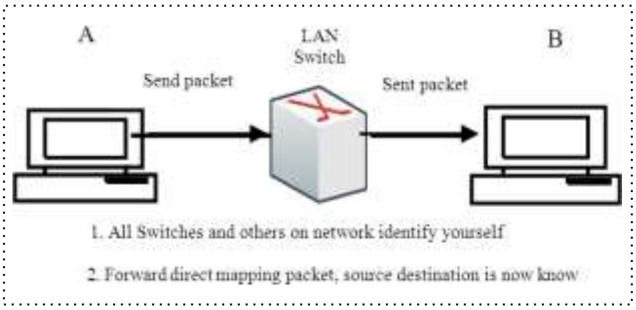

Figure-3: Switch Packet Transmission steps in DDN

When the network is enabled, Host A sends a message to Switches X on the network to identify themselves with all the necessary network information comprising of the source and destination of computers, routers, addresses, layers among others for the packets to be forward. With this information, Host A can send a packet to Host B more conveniently and less time is spent in transmitting packets and negotiations. As seen at Figure 3, packet transmission in DDN consumes lesser time and the packet is transmitted efficiently to the receiving host destination because the transmission routes are much shorter. And by applying the IEEE EUI64, IPv6 Interface Identifier with lower 64 bits that has the source and destination MAC addresses already encoded packets can be transmitted much easily and faster. Packet algorithm for DDN is marked as IPv6 64-bit Interface Identifier so Direct mapping packets do not have to be subjected to various negotiations in resolving addresses as in dynamic binding, but only have to send packets to the recommended routes to the target destination, because the destination MAC address is already known from the initial stage through IPv6 Interface Identifier lower 64 bits.

The proposed DDN was implemented in NS-2 simulation network which was a distinct event scheduling simulator used for developing networks and it included simulation for routing, unicast, multicast protocols used for network wired implementation. The DDN was implemented in the NS-2 simulator, Windows Operating System, Toshiba Computer with 4GB RAM, Toshiba computer and 250GB hard disk drive.

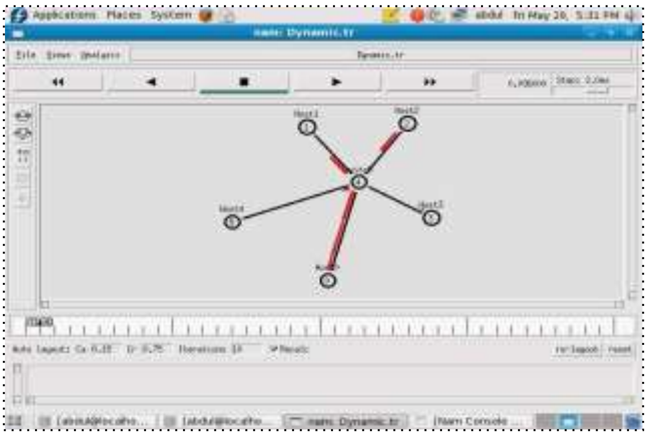

Figure-4: Dynamic binding transmissions

In the dynamic transmission mode, Figure 4, host 0 intends to send packet to host 3, and the procedures are made of two stages as follows:

- Since the MAC destination address is not known, the sending host 0 multicast to all the hosts namely 1, 2, 3, 5 and wait for responses on destination MAC addresses
- Once the sending host 0 received the MAC (destination address) from lower protocols, packets are transmitted through the network to intended host recipient, in this case host 3.

The same processes can be applied for all the other hosts as well whenever each host wants to send packet to each other. There are two stages of sending packet before a packet is sent to a target destination; first instance is to resolve the target destination through address resolution and second is to send packet.

Figure 5 describes how the packet is sent to targeted destinations after the hosts have exchanged messages and target or destination address are received. Finally the packet is sent to receiving host 3 as seen in the Figure 5 below.

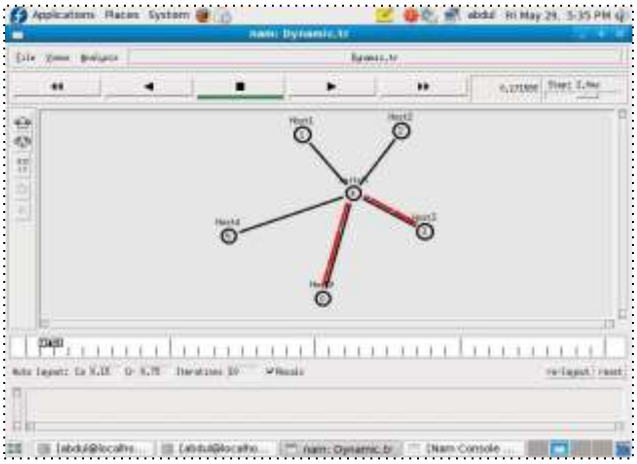

Figure-5: Dynamic binding targeted destination

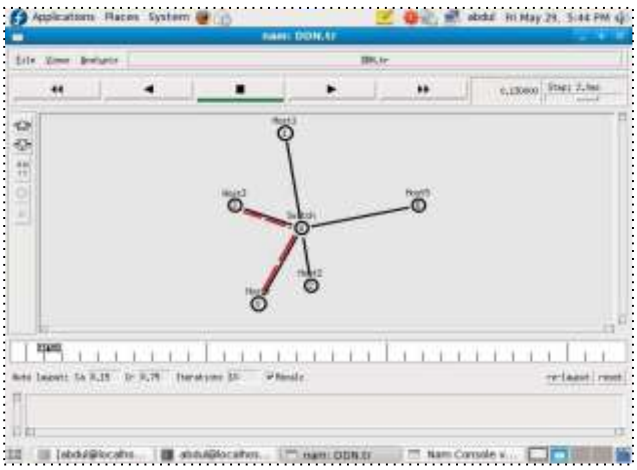

Figure-6: DDN direct mapping transmission

Figure 6 describes the simulation for direct mapping results. The concept of DDN is straightforward as the algorithm extracts the best features from dynamic binding and direct mapping to send a packet. Packets are transmitted directly to final destinations without having to do multicasting to lower protocols for resolving addresses but instead they are sent directly to target destination address because of IPv6 Interface Identifier. In the Figure 6, host 0 sends packets to host 3 directly to destination through the switch because destination address is established through IPv6 Interface Identifier. If hosts 0 or 3 decided to send a packet to each other next time, the process would be even faster because the destination addresses for each packet in formations are already stored in the Neighbor Cache. Moreover two steps are needed to send a packet in the DDN approach.

V. RESULTS

Results were obtained for both DDN direct mapping and dynamic binding using the NS-2 Simulator and on five network computers with the performance criteria being latency and efficiency on packets delivery. The results are presented in Figures 7-9.

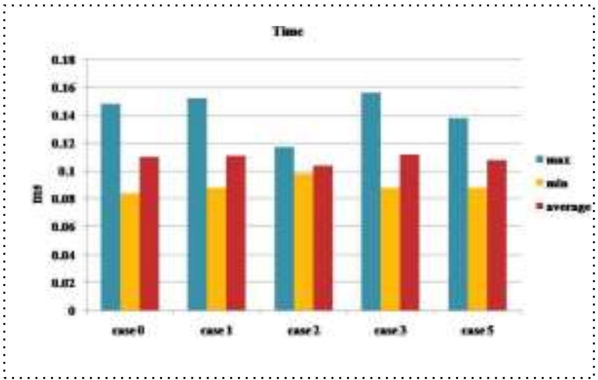

Figure-7: dynamic binding time

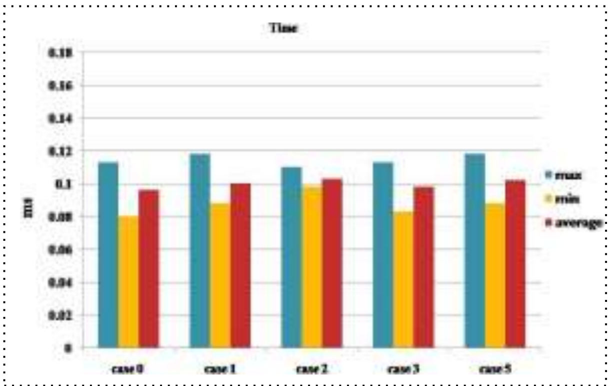

Figure-8: DDN direct mapping time

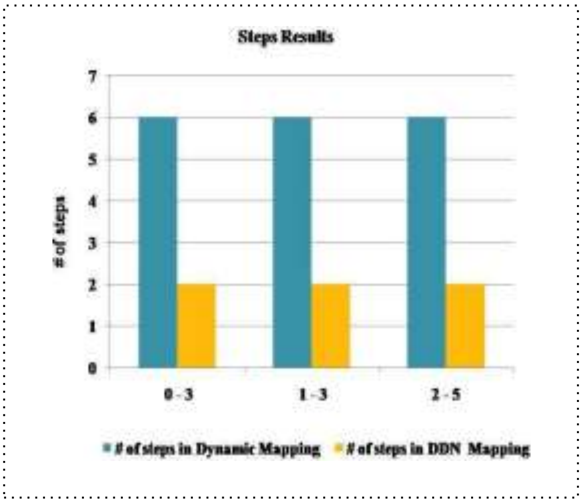

Figure-9: Number of steps

VI. DISCUSSION

The histogram in Figure 7 reports the maximum, minimum and average time of dynamic binding. The highest average time recorded for sending packet is Case 3 which is 0.112ms and the lowest in Case 2 at 0.104ms. On the other hand Figure 8 reports the maximum, minimum and average time of sending packet in DDN. The highest average time is recorded for sending packet is Case 2 which is 0.103ms and the lowest in Case 0 at 0.096ms. Comparing the average times recorded for both approaches it can be seen that it took more time to send a packet in Dynamic binding than in Direct Mapping using the DDN approach. This is performance is repeated for Case 0 where the dynamic average time was 0.110ms while that of DDN Case 0 was 0.096ms.

Figure 9, illustrates the efficiency rate between both methods when packets were sent. Efficiency here was measured by the number of steps each sending host transmitted a packet to a target destination. This was mainly the path packets traveled on the network. The more paths the packets had to travel, the longer time it would take for a packet to reach its destination. In view of the long procedures involved, a packet may not reach its destination because of time outs or undue delays or poor traffic that might cause the data to lose its efficiency. The less transmission paths were involved, the better the efficiency of the packet to reach its destination. And with the new algorithm, the paths of packet were significantly reduced.

In Figure 9, the number of steps for dynamic packet were from hosts 0-3, 1-3, 2-5, and it involved 6 steps each for each case before a packet reached a final destination. At the same time using the proposed DDN for the same cases, it involved only 2 steps before a packet reached its final destination. The results implied that it took more steps for the packets to be processed and sent in Dynamic Binding than in Direct Mapping, using our proposed algorithm DDN. In the longer procedures of dynamic binding as illustrated in Figures 7- 9 the packets had to wait for negotiations on how to resolve the addresses.

The new DDN algorithm, on the other hand, in showed that fewer steps were needed, that is, 2 steps were involved before the packets were sent from host 0 to 3, 1 to 3 and among others (Figure 9). So the chances of the packets reaching its destination were much higher in the direct DDN approach than the dynamic binding as the destination was already known in the algorithm. This reason accounted for the reduction to the two steps employed in the direct approach. Figure 9 also shows a higher number of steps, e.g. 6 for each in Dynamic binding than direct approach, and it led to more utilization of resources.

VII. CONCLUSION

The study introduces DDN, a new technique based on the IPv6 Interface Identifier model that provides improved direct mapping and dynamic binding functions. Because there were fewer agreements processes involved in transmitting packets, the DDN exhibited significant improvements in packet delivery when compared to dynamic binding. Figures 7-9 show that the DDN technique delivered the packets to their respective end destinations quickly. There is a need for quicker packet transmission with the new IPv6 technology, and DDN has the ability to give a platform for future consideration into new packet transmissions.

REFERENCES

[1] Crawford, M., Narten, T. and Thomas, S., Transmission of IPv6 Packets over Token Ring Networks, IETF RFC 2470, December 1998; [Accessed 2nd March, 2009], Availabl from Website: http://tools.ietf.org/html/rfc2470.

[2] Davies, J. (2008). Understanding IPv6, 2nd Edition, Microsoft Press,USA.

[3] Kozirok, C.M. (2005). The TCP/IP Guide: A Comprehensive, Illustrated Internet Kindle Edition, No Starch Press,St Louis.

[4] Beck, F., Cholez, T., Festor, O. and Chrisment, I. (2007). Monitoring the Neighbor Discovery Protocol, The Global Information Technology, IEEE, pp. 57-57.

[5] Chen, E., Thiam, T. H., Issac, B. and Nguan, T. H. (2006). Analysis of IPv6 Network, 4th Student Conference on Research and Development, IEEE,pp. 11-15.

[6] Narten, T., Nordmark, E., Simpson, W. and Soliman, H., Neighbor Discovery for IP Version 6 (IPv6), IETF RFC 4861, September 2007; [Accessed 2nd April,2009], Availabl from Web site:www.rfc-editor.org/rfc/rfc4861.txt.

[7] Kozirok, C.M.(2005). The TCP/IP Guide: A Comprehensive, Illustrated Internet Kindle Edition, No Starch Press,St Louis**.**

[8] Hinden, R. and Deering, S., Internet Protocol Version 6 (IPv6) Addressing Architecture, IETF RFC 3513, April 2003; [Accessed 2nd March,2009], Available from Web site: http://www.ietf.org/rfc/rfc3513.txt.

[9] Murugesan, R. K., Budiarto, R., and Ramadass, S. (2008). Performance Improvement of IPv6 Packet Transmission through Address Resolution using direct mapping, First International Conference Distributed Framework and Applications, IEEE, pp. 164-169

[10] Gilligan, R. and Nordmark, E., Transition Mechanisms for IPv6 Hosts and Routers, IETF RFC 2893, August 2000; [Accessed 7th March,2009], Available from Website: http://www.ietf.org/rfc/rfc2893.txt

[11] Tulloch, M. (2006). TCP/IP Networking Understanding TCP/IP is fundamental to computer networking nowadays, 2nd edition ,Tata McGraw-Hill,New York**.**

[12] Kim, J.M., Park, I.K., Yu, J.W. and Park, J.-H. (2004). Design and implementation of IPv6 Neighbor discovery protocol supporting security function, The 6th International Conference on Advanced Communication Technology, IEEE, pp. 323 – 326**.**

[13] Huang, H. and Ma, J. (2000). IPv6 – Future Approval Networking, International Conference on Communication Technology Proceedings, IEEE, Vol. 2, pp. 1734-1739

[14] Hines, A. (2004). Neighbour Discovery in IPv6. [Accessed 3rd February,2009], Available from Web site: http://wwwcs.uni-paderborn.de/cs/ag madh/WWW/Teaching/2004SS/AlgInternet/Submissions/17-neighbour-discovery-protocol-in-IPv6.pdf