International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 02 | May-2015 www.irjet.net p-ISSN: 2395-0072

IPv4 to IPv6 Network Migration and Coexistence

A.Chandra[1], K. Lalitha[2]

[1] *Assistant Professor, Department of CSSE, Sree Vidyanikethan Engg. College, Tirupati, Andhra Pradesh, India*

[2] *Assistant Professor(SL), Department of CSSE, Sree Vidyanikethan Engg. College, Tirupati, Andhra Pradesh, India*

Abstract - *The Internet Assigned Numbers Authority (IANA) finally exhausted the IPv4 address space which made to push forward IPv6. As the existing setup is on IPv4 it had become inevitable to go a transition phase. During this transition phase both IPv4 and IPv6 will exist, due the technical differences both are not compatible. Therefore it is necessary to provide the inter communication ability of IPv4 to IPv6. We focus on the difficulties in transition from IPv4-IPv6 and performance evaluation during inter operation. It is important to consider the migration process, Transition mechanisms and the inter operation of IPv4 and IPv6 networks.*

Keywords: IPv4-IPv6 Transition, transition mechanisms, heterogeneous network connectivity, threats, tunneling, performance evaluation.

1. INTRODUCTION

Internet protocol follows certain technical rules for communication among computers over a network. The widely used first version of internet protocol for most of today's internet traffic is IPv4. IPv4 header is depicted in Fig.1. It has four billion IP addresses even it is lot of IP addresses it is no more sufficient. The second version of internet protocol IPv6 is a newer numbering system with a large pool of IP addresses. IPv4 cover 4,294,967,296 addresses whereas 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses are covered by IPv6. Fig.2. shows a simplified header of Ipv6. The technical functionality of both versions remains same and will operate simultaneously in future. Today's most networks that use IPv6 support both versions of IP. The challenging issues in deployment of IPv6 are migration and tunneling techniques. It is highly difficult to replace existing IPv4 infrastructure with IPv6 rather a coexistence may be possible.

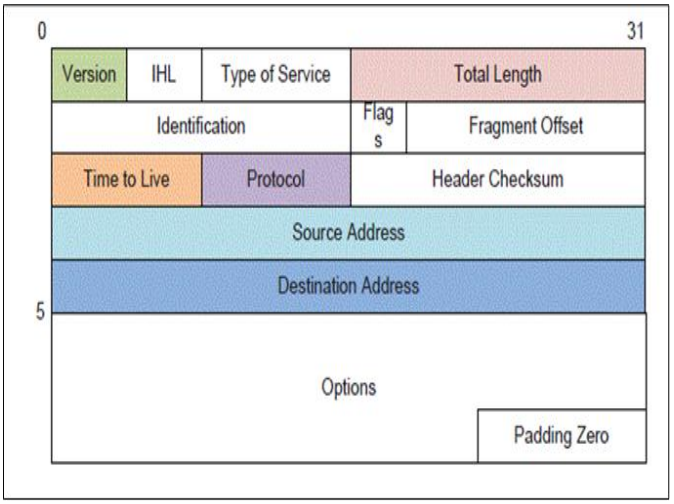

Fig-1: IPv4 Header

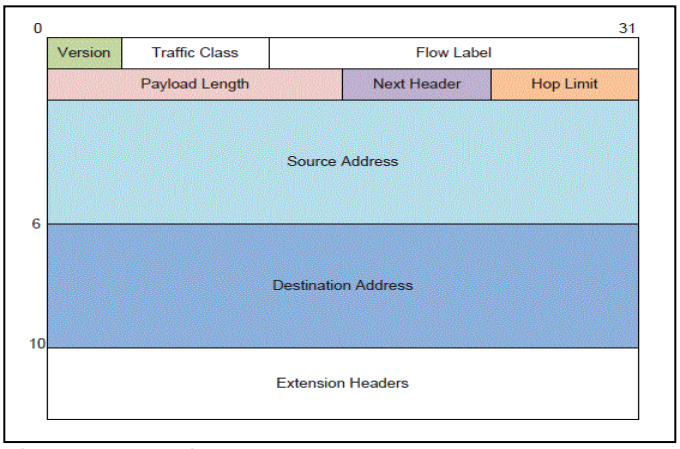

Fig-2: IPv6 Header

The key differences between IPv4 and IPv6 are, in IPv6 header length is eliminated as the length of the header is fixed. The function of service type field is taken over by priority and flow label fields. Total length field is eliminated and is replaced by payload length field. The fragmentation extension header includes identification, flag and offset fields. The TTL field is called hop limit, protocol field is replaced by next header. As the checksum is provided by upper layers it is not needed and hence eliminated. Options fields are implemented in extension headers.

Extension Header Types and Options: The header of IPv4 is comprised of two parts. Apart from 20 bytes of

fixed part it is also having a maximum of 40 bytes variable part is available, which can be used for network testing and debugging. Fig.3. classifies various options used in IPv4. Similarly for IPv6 have fixed 40 byte base header and optional six extension headers and data from the upper layers upto 65,535 bytes of information. Extension header types of IPv6 is shown in Fig.4.

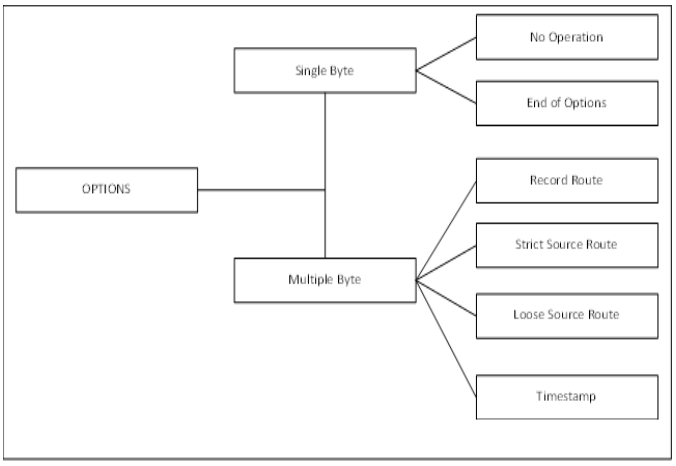

Fig-3: Taxonomy of options in IPv4

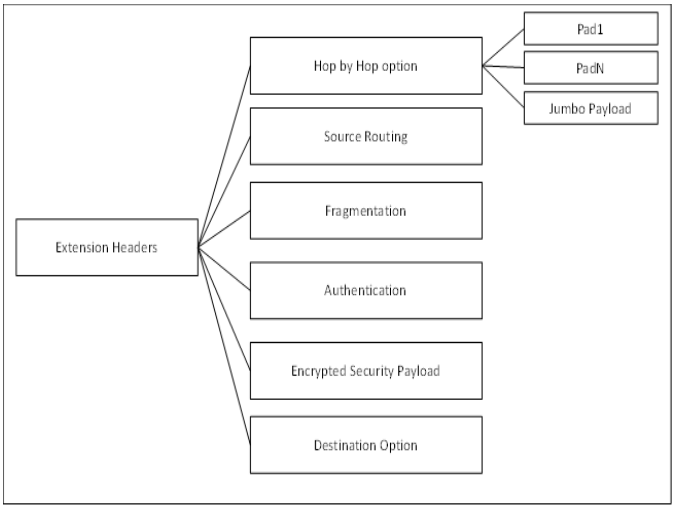

Fig-4: Extension header types in IPv6

Primary differences between the IPv4 and IPv6 extension headers are, the no-operation and end-of-options in IPv4 are replaced by Pad1 and PadN options in IPv6. Record route options and time stamp options are not implemented in IPv6. The fragmentation fields in the base header section of IPv4 have moved to the fragmentation extension header in IPv6.

Security threats in IPv4 and IPv6 network: Despite of security implementation in new IPv6 protocol, vulnerabilities still exist. Many attacks in IPv4 networks are not suppressed by appearance of new IPv6 Protocols. They still affect both the networks. Certain attack, application layer attack, flooding attack, rogue devices and man-in-the middle attack are common in the both the network architectures [1].

1.1 Security Threats Specific to IPv6 [2]:

Reconnaissance: A larger attack, in which an intruder uses reconnaissance attacks to gather some essential data of the victim network that can be misused later in further attacks. An intruder can use scanning techniques or passive data mining for attack. IPv6 networks are more resistant than IPv4 networks for this kind of attack. Some types of multicast addresses used in IPv6 networks that can help an intruder to identify and attack some resources in the targeted network.

Routing Header Related Threats: Routing headers can be used to avoid access controls based on destination addresses can produce some security problems. There is a possibility that an intruder sends a packet to a publicly accessible address with a routing header containing address on the victim network. Then the publicly accessible host will forward the packet to a destination address stated in the routing header which may cause a threat.

Fragmentation Related Threats: In IPv6 protocol specification packet fragmentation by intermediate nodes is not allowed. The minimal packet size for IPv6 network is 1280 octet, it is highly recommended to discard all packets less than 1280 octets due to security reasons. By sending a large number of small fragments an attacker can cause an overload of reconstruction buffers on the target system potentially implying system to crash. To avoid such problems it is a recommends security practice to limit the total number of fragments and their allowed arrival rate.

ICMPv6 and multicast related Security Threats: In IPv6 networks neighbor discovery and path discovery are dependent on some types of ICMPv6 messages like packets too big and parameter problem must be allowed for proper network operation which is also sent to multicast addresses, this fact is misused by an attacker, where he can cause multiple responses targeted at the victim.

Transition Mechanisms Related Security Issues: It is very important for network designers and administrators to understand security implications of implications of transition mechanisms in order to apply proper security mechanisms such as firewalls and intrusion detection mechanisms.

2. TRANSITION MECHANISMS

As IPv6 is being came to existence it is evident that methods of upgrading the internet is essential. It involves lot of cost, so gradual transitions are evolved which may take a decade happen. In literature several transition mechanisms are proposed they are Dual Stack, DTI and

Bump-in-Dual Stack, NAT protocol translator, Stateless IP/ICMP Translator, Assignment of IPv4 Global Addresses to IPv6 hosts, Tunnel Broker, 6 to 4 transition mechanism and IPv6 in IPv4 Tunneling. In these mechanisms Dual Stack is easy to implement however complexity increases due to both infrastructures and the cost is higher due to more complex stack. DNS issues and single point failure are the drawbacks of NAT protocol. Tunnel broker suffers from authentication and scaling issues [4].

IPv6 to IPv4 translation mechanisms allows interconnection between IPv6 hosts connected over IPv4 Infrastructure. IPv6 over IPv4 tunneling mechanism allows to connect isolated IPv6 networks over IPv4 network.

IPv6 to IPv4 Translation: The IPv6 nodes connected to an IPv4 network. The IPv6 datagrams are encapsulated and sent on an IPv4 network without any knowledge of IPv6 protocol the Fig. 5. illustrates the process. By using the translation scheme it is possible to support IPv6, by installing both IPv4 and IPv6 on the end nodes without changing the IPv4 infrastructure [3].

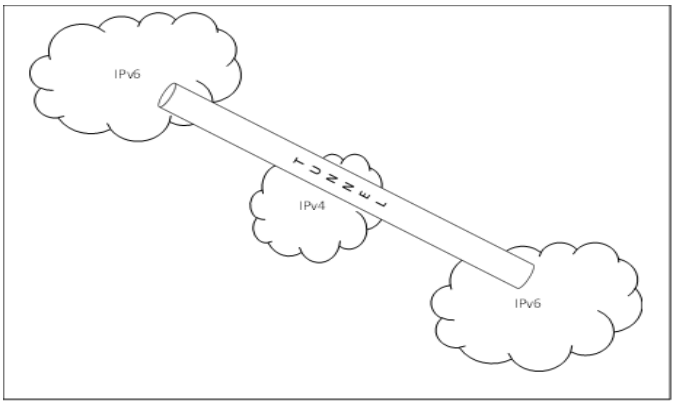

Fig-5. Tunneling

IPv6 over IPv4 Tunneling: The working mechanism of this technique is depicted in Fig.6. An edge router is employed to which the external nodes are connected. These routers create a tunnel to handle encapsulation and de-encapsulation of IPv6 packets over the existing IPv4 network. In this mechanism edge routers support dual stacks and creates a tunnel prior to transmission. Tunnels can be established dynamically as required [3].

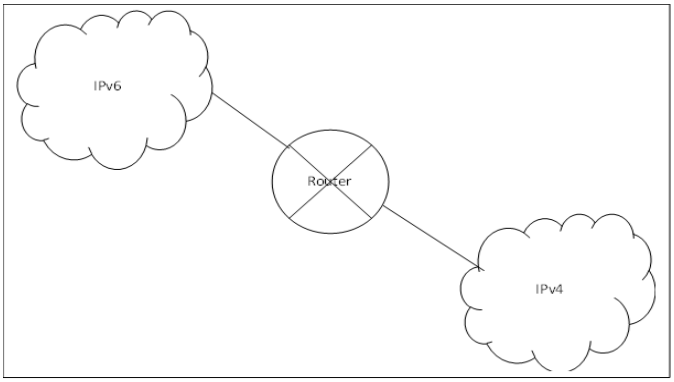

Fig-6: Translation

3. PERFORMANCE EVALUATION OF IPv4 AND IPv6

To calculate the performance of the IPv4 and Ipv6 protocols, first of all consideration has been made over bandwidth utilization, delay, throughput and round trip time performance metrics. Different procedures have been adopted to calculate the performance of these protocols stack. All these experiments conducted within the 60 seconds interval. Every test performs many times so that gets reliable outcomes. In point-to-point connection oriented test where more than two computers are linked from end to end directly by utilizing Unshielded Twisted Pair Ethernet cable.

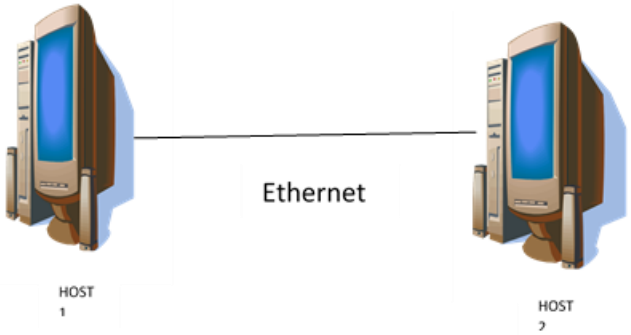

Fig -7: Point to Point connection

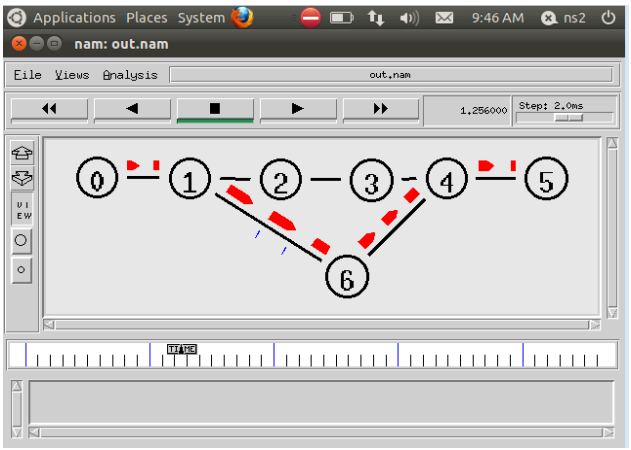

Fig-8. NS2 Simulation

In Fig.7. point-to-point connection oriented test where more than two computers are linked from end to end

directly by utilizing Unshielded Twisted Pair Ethernet cable. A network host is a computer connected to a computer network. A network host may offer information resources, services, and applications to users or other nodes on the network. A network host is a network node that is assigned a network layer host address. On the both machines operating systems and IPv4 and IPv6 protocols stack are stack are installed. The IP has been configured implemented by using NS2 [5]. After performing the experiments, the diagram explains that both working process of both protocol stack IPv4 and IPv6 under the platform of Linux is very narrowly and closely. Fig shows the connection between the required hosts via twisted pair Ethernet cable.

In the Fig.8. nodes arranged within the infrastructure are of IPv4 and IPv6. The data packets are passed through these nodes and bandwidth utilization, delay and throughput are calculated which determines the performance of IPv4 and IPv6.The data is estimated and plotted in the form of graphs. The Fig.8. shows the flow of packets from node0 to node5 via node6. The Fig.9. and Fig.10. shows the difference in the band utilization and delay respectively in IPV4 and IPV6 infrastructures. In the below shown graph(Fig.9.) x-axis denotes the size of the data packet passing through and y-axis denotes the bandwidth utilization. In the case of Fig.10. x-axis denotes the packet size which is similar in both the cases and y-axis denotes the delay in both the cases.

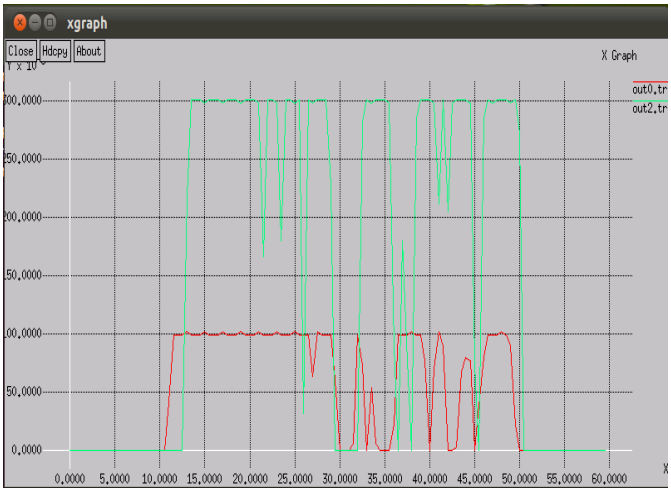

Fig-9: Performance analysis of band width

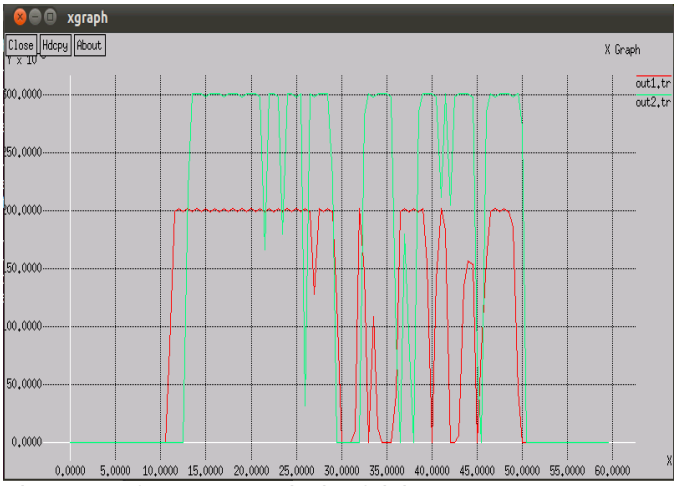

Fig-10: Performance analysis of delay

From the experiment it can be concluded that band width utilization is comparatively better in IPv6 protocol than IPv4. Delay is less in IPv6 than IPv4. IPv6 will have better performance, however it is migration is not easy it involves lot of cost, replacement existing infrastructure should be gradual.

4. CONCLUSION AND FUTURE WORK

Internet is the global system with the interconnection of networks. For browsing the internet, a system need to be identified in the network. This identification can be done with an IP address given to the system. The IP is a numerically assigned label that is used for the identification of the system and IPv4 is the presently used addressing format. Due to the limitations of IPv4 the generation tends to migrate to the advanced version of IP called IPv6. To enhance the migration both the IP's are analyzed. The expanded addressing capacity of IPv6 will enable the trillions of new Internet addresses needed to support connectivity for a huge range of smart devices. IPv6 brings enhanced quality of service for several new applications.

REFERENCES

[1] Peng Wu, Yong Cui, Jianping Wu, Jiangchuan Liu, Chriz Metz "Transition from IPv4 to IPv6 :A State of the Art Survey," IEEE Communications Surveys and Tutorials, Vol.15, 2013.

[2] Emre Durdagi, Ali Buldu "IPv4/IPv6 Security and Threat Comparisons procedia social and behavioral sciences," Elsevier 5285-5291, 2010.

[3] Peng Wu, Yong Cui, Mingwei Xu, Jianping Wu, Xing Li, Chriz Metz, Shengling Wang "PET: Prefixing, Encapsulation and Translation for IPv4-IPv6 Coexistence" IEEE Communication Society, Globecom Proceedings, 2010.

[4] M. Mehran Arshad Khan, Yahya Saeed, Nadeem Asif , Tahir Abdullah, Shahbaz Nazeer, Afzal

Hussain "Network Migration and Performance Analysis of IPv4 and IPv6," European Scientific Journal ISSN: 1857-7881 2012.

[5] The network simulator. ns-2 http://www.isi.edu/nsnam/ns.

BIOGRAPHIES

Mr. A.Chandra received his B.Tech degree in Computer Science and Engineering from JNT University, Hyderabad. He had his M.Tech from JNTUA, Anantapur. His research interests are image processing, computer networks and network security. Presently he is working as Assistant professor in the Department of Computer Science and Systems Engineering, Sree Vidyanikethan Engineering College, A.Rangampet, Tirupati.

