ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 5, May 2016

Performance Analysis of IPv6 Dual-Protocol Stack and Tunnel Transition

Adarsh Misra[1], Harsha Chawla [2]

M-Tech Student[1], Assit. Prof.[2] & Department of CSE & NGF College of Engineering &Technology
Palwal, Haryana, India

Abstract:
IPv4/IPv6 transition rolls out several issues to the internet world. IETF introduces some transition mechanisms involving IP transition, dual IP stack and tunneling transition techniques. Depending on the migration technique from IPv4 to IPv6, the performance of three types of technique options, ISATAP tunneling, double-stack protocol and 6to4 tunneling mechanism are checked and examined. The result indicates there are some performance benefits on double stack protocol technique IPv6 ISATAP tunnel, IPv6 network than IPv4 and IPv6 6to4 tunnel network.

Index Terms: **double-stack protocol, IPv6, tunnel technique, throughput, round-trip delay**

I. INTRODUCTION

Because of IPv4 network suffering more and more issues, particularly the deficiency of network security flaws as well as address space, the next generation IPv6 network research is captured to be concentrated [1]. The IPv6 has eliminated IP address crisis, which explores IP addresses from 32-bit to 128-bit. There is restriction of compatibility between IPv4 and IPv6, thus, transition technique from IPv4 to IPv6 is studied broadly, primarily concentrates on dual stack technique and the tunnel technique two options. This paper explains the principle of transitional technique, builds a comparison and analysis by examining the performance of IPv6 depending on generally utilized transition technique [2][3].

Much work and care have been given to the transition to IPv6, and much work has already been begun on measuring the security significances during this time [3, 4]. However, the Internet has been suffered by various worms; it is required to explore the worms activities in IPv4-IPv6 dual-stack networks. The random address space scanning is the most famous technique applied by the worms to discover dangerous targets in IPv4 networks. The efficiency of this technique attributes to the 32-bit IPv4 address which permits the random-scanning worms to examine all possible hosts [5, 6]. It is normally considered that the IPv6 protocol can offer better security against these worms because of its 128-bit large address space, so that the possibility to attain a valid address in the IPv6 address space by random-scanning is very less. Hence, the transition from IPv4 to IPv6 is assumed as an efficient method to preventing worms from dispersing [7]. It is seen in this research paper that the dual-stack worm can gather the IPv6 addresses of all active hosts on the connection-local rapidly and efficiently, which result in accelerated worm dispersing on the IPv6 subnets. In actuality, those "isolated IPv6 islands" would really become the "hotbeds" for the dual-stack worm, particularly in the worm-propagation beginning phase. In another words, one infected host could infect all dangerous hosts on the same connection in a less time, while it may consider much higher time to infect the hosts in IPv4 networks with random-scanning technique. As a result, the deployment of IPv6 is not able to prevent the worm propagation as what was desired, but rather has opposite impact. However, it is risky to introduce a real worm into real networks, simulation and modeling are done to examine the features of the worm propagation and to inquire the defense mechanisms. In this research paper, the dual-stack worm is inquired by exploring its similar scanning mechanism to the self replicating natures of biological viruses.

II. LITERATURE SURVEY

Sheetal Borse et al. [1] : Here, in this paper authors discusses various techniques for migration of IPv4 to IPv6 protocol through dual stack mechanism in Local Area Network(LAN).For the implementation purposes, they used Packet Tracer version 6.0.1 software. Performance is analysed using the Ping connectivity and Round Trip Time (RTT) of

IPv4/IPv6 networks. After the simulation results, authors conclude that transition platform IPv4 based websites can be accessed and web page is displayed, yet, IPv6 based webpage can also be displayed unless the webpage is present at the server side.

Ali Albkerat et al. [2]: In this paper, authors analyzed the various IPv6 transition technologies. In their work authors compares the performance of IPv4 and IPv6 in order to show the effects of transition strategy on network behavior. In their work for performance evaluation, authors used the OPNET modeler that contains a WAN, a LAN, hosts and servers. After the simulation results, authors conclude that IPv6 has higher throughput. CPU utilization is lower for IPv4, IPv6 and dual stack than manual and 6to4 and also dual stack has less delay with TCP.

Sheryl Radley et al. [3] : Here authors present the evaluation and study of the Transition Techniques addressed on IPv4-IPv6 . In their work authors aimed at a comparative study on the three transition techniques such as softwire mesh which supports dual stack, NAT444 which supports translation and IPv6 rapid Development mechanism in tunnelling mechanism. For the simulation purpose, authors used NS-2 simulator. After the simulation result, authors conclude that effective way of transition is IPv6 Rapid Development method. The tunnelling mechanism shows a higher throughput value when compared to the other two mechanisms.

Febby Nur Fatah et al. [4]: In this paper authors analysed the performance of Dual Stack IPv4-IPv6 system in university network by using of jitter and delay period in interconnection. In their work, authors calculated the jitter and delay period by transferring different files with different size. For performance analysis, technique used by authors is the method by direct measurement of performance on the model or network prototype. After the implementation, authors conclude that Dual Stack system is most trustworthy implementation for migration of IPv4 to IPv6 system. Also IPv6 system is more stable and there is less jitter than IPv4.

III. TRANSITION MECHANISM

A. Dual-stack protocol:

In dual-stack, all routers/hosts manage both protocol IPv6 and IPv4 stacks. Dual stack routers/hosts are capable to interact with not only IPv6 system, but also IPv4 system. The dual stack hosts utilize IPv6 address while interacting with IPv6 hosts, and utilize the IPv4 address while interacting with IPv4 hosts. Applications select between using IPv4 or IPv6 with the application choosing the right address depending on the kind of IP traffic and specific needs of the communication.

B. Tunnel Mechanism

Another transition to IPv6 is utilizing tunnel mechanism. The element of this method is to encapsulate IPv6 datagram into IPv4 by dual-stack protocol routers while IPv6 datagram entering IPv4 network, and to build the IPv6 packet become part of IPv4 packet. Then IPv6 packets begin transition within IPv4 tunnel network. At the time of the IPv4 datagram leaves the IPv4 network tunnel, the dual-stack routers will send data, the actual IPv6 packet, to the IPv6 protocol stack. The essence of tunnel mechanism is IPv6 packets will be encapsulated in IPv4 packets, utilizing the available interaction issues between. IPv4, IPv4 transmission path as IPv6 data link layer, can be consider as a point to point virtual connection.

1) 6to4 Tunnel Mechanism

The core concept of 6to4 tunnel technique is that site address prefix consist IPv4 tunnel port address, a mapping generated between IPv6 address of intra-site hosts and IPv4 address of site border routers, and directly utilizes IPv4 address of site border router as part of IPv6 address prefix of intra-site hosts.

2) ISATAP tunneling Mechanism

Intra-site Automatic Tunnel Addressing Protocol (ISATAP) is targeted for the intra-site scope. With ISATAP, the intra-site IPv4 network is seen as a link layer for IPv6 and other nodes in the intra-site network are seen as strong IPv6 routers/hosts. An ISATAP address is made with its own interface identifier. After that, the ISATAP hosts can link each other through the IPv6-in-IPv4 tunnel with ISATAP address.

IV. IPV6 TO IPV4 AUTOMATIC TUNNELING MECHANISM

Automatic tunneling means to a tunnel configuration that does not require direct management. An automatic IPv*6 to IPv4* tunnel enables an isolated IPv6 domain to be linked over an IPv4 network and then to a remote IPv6 networks. This tunnel handles the IPv4 infrastructure as a virtual non broadcast connection, so the IPv4 address inserted in the IPv6 address is utilized to determine the other end of the tunnel. The inserted IPv4 address can easily be extracted and the entire IPv6 packet provided over the IPv4 network, hidden in an IPv4 packet. No configured tunnels are needed to forward packets among *6to4*- capable IPv6 sites anywhere in IPv4 Internet. Fig 5 illustrates the *6to4* address format structure. The prefix field (FP) value is 0x001, which determines global unicast address. The Top-Level

Aggregation identifier field (TLA) is allocated by the IANA for the IPv*6 to IPv4* technique. Thus, the IPv6 address prefix is 2002::/16 and the 32 bits after 2002::/16 show the IPv4 address of the gateway machine of the network in question. The packets hence know the way to any other network. The *6to4* technique is the most broadly extensively utilized automatic tunnelling mechanism [14]. It involves a technique for allocating an IPv6 address prefix to a network node with a global IPv4 address.

IPv6 Tunnel Broker: The IPv6 Tunnel Broker offers an automatic configuration facility for IPv6 over IPv4 tunnels to subscribers linked to the IPv4 Internet [15]. IPv4 connectivity between the subscriber and the service supplier is needed.

I. The subscriber contacts Tunnel Broker and performs the registration mechanism.
II. The subscriber contacts Tunnel Broker again for authorization and offering configuration information (operating system, IP address, IPv6 support software, etc.).
III. Tunnel Broker sets up the network side end-point, user terminal and the DNS server.
IV. The tunnel is active and the subscriber is linked to IPv6 networks.

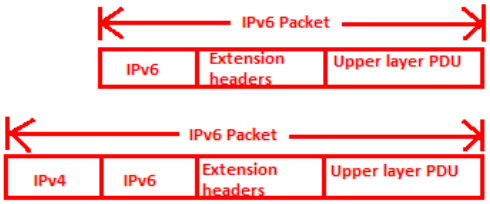


Figure 1: *6over4* Address Link Layer Identifier

V. IPv4/IPv6 Translation Mechanism

The basic service of translation in IPv4/IPv6 transition is to translate IP packets. Many translation techniques depend on the SIIT (Stateless IP/ICMP Translation algorithm) algorithm [16]. The SIIT algorithm is utilized as a basis of NAT-PT (Network Address Translation-Protocol Translation) and the BIS (Bump In the Stack) techniques,

1. Bump-In-the-Stack Mechanism: BIS mechanism (RFC 2767) involves a translator module and a TCP/IPv4 protocol module, which Contain three bump components and is layered above an IPv6 module (Fig 6) [17]. Packets from IPv4 applications propagate into the TCP/IPv4 protocol module. The detected packets are translated into IPv6 packets and then sent to the IPv6 protocol module. The three bump components are the extension name resolver, which analyzes DNS lookups to find whether the peer node is IPv6- only; the address mapper, which assigns a local IPv4 address to the IPv6 peer and caches the address mapping; and the translator, which interprets packets between IPv6 and IPv4 protocol.

2. Network Address Translation-Protocol Translation: The NAT-PT technique is a stateful IPv4/IPv6 translator [18][19]. NAT-PT nodes are at the boundary between IPv4 and IPv6 networks. Every node manages a globally routable IPv4 addresses pool, which are dynamically allocated to IPv6 nodes when sessions are started throughout the IPv4/IPv6 boundary. This technique permits native IPv6 nodes and applications to interact with native IPv4 applications and nodes, and vice versa. The fundamental NAT-PT function does not snoop packet payloads, and the application may thus be unknown of it. Thus, the NAT-PT technique is based on ALG agents that permit an IPv6 node to interact with an IPv4 node and vice versa for particular applications. The NAT-PT technique is an interoperability solution that requires no modification or additional software, i.e. dual stacks, to be installed on any of the end subscriber nodes, either the IPv6 or the IPv4 network. This technique implements the needed interoperability functions within the core network, building interoperability between nodes easier to maintain and quicker to manifest. Tunneling mechanisms as represented in fig 2 are more suitable as compared to dual stack and translation mechanisms. Tunnels are utilized to carry one protocol inside another. Most access network works over IPv4 [13]. Subscribers of these networks might require to get linked to IPv6 internet. Thus, ISP should offer IPv6 access over IPv4 only network, which could be obtained through IPv6 over IPv4 tunnel. These tunnels consider IPv6 packets and encapsulate them in IPv4 packets to be forwarded across network portions that haven't yet been upgraded to IPv6 [10].

Tunnels can be generated where there are IPv6 islands distinguished by an IPv4 ocean, which will be the norm during the early phases of the transition to IPv6. After that there will be IPv4 islands that will require to be bridged across an IPv6 ocean. Tunnels are categorized as: manual and dynamic [1]. Manually configured IPv6 tunneling needs configuration at both tunnel ends, whereas dynamic tunnels are generated automatically depending on the routing and packet destination address. Dynamic tunneling mechanisms simplify management as compared with statically configured tunnels, but static tunnels build traffic information existed for every endpoint, offering additional security against

injected traffic [15]. Many tunneling mechanisms are Automatic tunneling utilizing IPv4 Compatible address, 4 over 6 tunneling, 6 over 4 tunneling, 6 in 4 tunneling, 6 to 4 tunneling, terado, Intrasite, Automatic tunneling Addressing Protocol (ISATAP) and IPv6 Rapid Development (6rd). With dynamic tunnels it isn't easy to track who is interacting over the transient tunnels and the tunnel destination end point is not known.

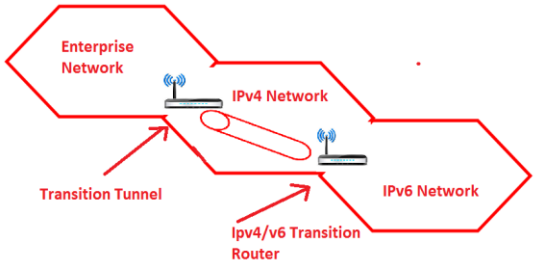
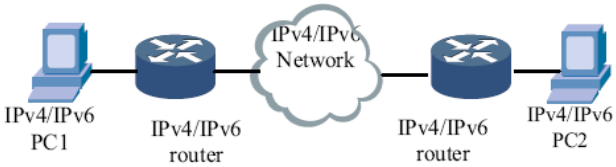


Fig 2: Tunneling Mechanism

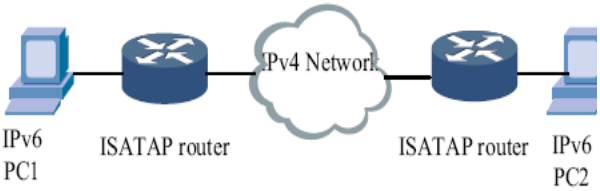
VI. PERFORMANCE TEST DESIGN AND ANALYSIS

In this paper, the round-trip delay and throughput are examined by the comparison of IPv6 to IPv4 network performance as well as IPV6 network performances under those three techniques above. Depending on test results, IPV6 network performance benefit is proved. In Fig 3, PC1 and PC2 are examined transmitter and recipient operating with Windows operation system. Because of restricted resource, routers are modeled with high-performance PC. Selecting active testing mechanism, that is, forwarded particular strength data packets from PC1 to PC2 over the network to analyze [8].

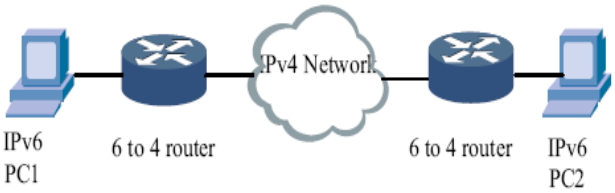
A. Testing structure



(a) Dual stack protocol



(b) ISATAP tunnel mechanism



(b) 6to4 tunnel mechanism

Figure 3 Testing Structure

B. Test analysis

1) Throughput test: Throughput is described as the amount of packet data that is transferred over the whole path per time unit. The throughput is computed from the formula T=P/L where T shows the throughput, P shows the transferred data size, and L shows the time cost in transfer. TCP protocol is utilized in the throughput analyze, examine data packet's payload size from 64 bytes to 1408 bytes, and every group's result considers the average value of 10 times test. Fig 2 presents comparison result of IPv4 and IPv6 network throughput under the dual-stack protocol. Fig 3 represents dual stack IPv6 network throughput comparison between ISATAP tunnel technique and 6to4 tunnel technique.

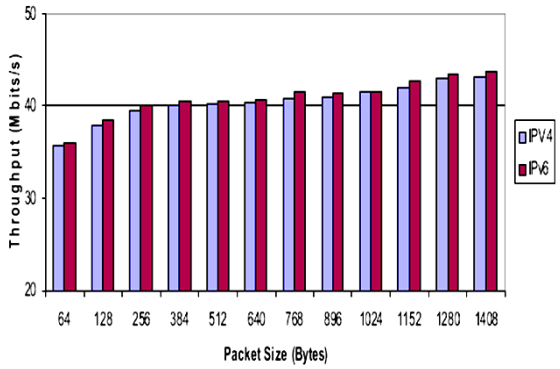


Figure 4: IPv6 and IPv4 network throughput comparison

In Fig 4, in dual-stack technique, TCP/IPv6 throughput increases along with the packet payload size increasing, and represents larger volume as compared to TCP/IPv4 throughput under the similar situation. Fig 4 is also depends on the similar test situation, throughput of 6to4 and ISATAP tunnel technique appear similar. But throughput of dual-stack technique is more than the other two.

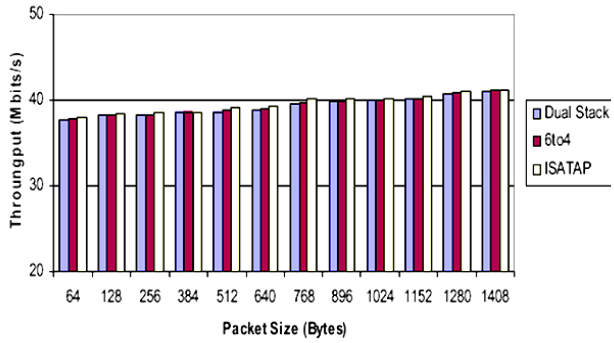


Figure 5: IPv6 throughput comparison on three transition mechanism

IV. CONCLUSION

Depending on analysis transition technique of the dual stack protocol, IPv6, 6 to 4 tunneling technique and ISATAP tunnel network performance are studied and examined depending on program implemented by our group. In general, results show that dual stack protocol IPv6 network has better performance as compared to 6 to 4 technique, dual stack protocol IPv4 and ISATAP technique.

REFERENCES

[1] Grosse, E. and Lakshman, Y. (2003). Network processors applied to IPv4/IPv6 transition, IEEE Network, 17(4), pp.35-39.

[2] Ali, A. (2012). Comparison study between IPv4 & IPv6, International Journal of Computer Science Issues (IJCSI), 9(3), pp.314-317

[3] Batiha, K. (2013). Improving IPv6 Addressing Type and Size, International Journal of Computer Networks & Communications (IJCNC), 5(4), pp.41-51

[4] I. Parra, J. (2014). Comparison of IPv4 and IPv6 Networks Including Concepts for Deployment and Interworking, INFOTECH Seminar Advanced Communication Services (ACS), pp.1-13

[5] Sailan, M., Hassan, R. and Patel, A. (2009). A comparative review of IPv4 and IPv6 for research test bed, Proceedings of International Conference on Electrical Engineering and Informatics (ICEEI '09), Malaysia, pp.427-433.

[6] Ahmad, N. and Yaacob, A. (2012). IPSec over Heterogeneous IPv4 and IPv6Networks: Issues and Implementation, International Journal of Computer Networks & Communications (IJCNC), 4(5), pp. 57-72

[7] Arafat, M., Ahmed, F. and Sobhan, M. (2014). On the Migration of a Large Scale Network from IPv4 to IPv6 Environment, International Journal of Computer Networks & Communications (IJCNC), 6(2), pp.111-126.

[8] Wu, P., Cui, Y., Wu, J., Liu, J. and Metz, C. (2013). Transition from IPv4 to IPv6: A state-of-the-art survey, IEEE Communications Surveys & Tutorials, 15(3), pp.1407--1424.

[9] Wu, Y. and Zhou, X. (2011). Research on the IPv6 performance analysis based on dual-protocol stack and Tunnel transition, Proceedings of the 6th International Conference on Computer Science & Education (ICCSE), pp.1091--1093.

[10] Chen, J., Chang, Y. and Lin, C. (2004). Performance investigation of IPv4/IPv6 transition Mechanisms, Proceedings of the 6th International Conference on Advanced Communication Technology, pp.545--550

[11] Narayanan, A., Mohideen, M. and Raja, M. (2012). IPv6 Tunnelling Over IPV4, International Journal of Computer Science Issues (IJCSI), 9(2), pp.599-604.

[12] Xiaodong, Z. and others, (2009). Research on the Next-generation Internet transition technology, Proceedings of Second International Symposium on Computational Intelligence and Design (SCID '09), pp.380-382

[13] A. Law, W. Kelton, and W. Kelton, Simulation modelin and analysis. McGraw-Hill New York, 1991, vol. 2.

[14] Y. Wang, S. Ye, and X. Li, "Understanding Current IPv6 Performance: A Measurement Study," in 10th IEEE Symposium on Computer Communications, Jun. 2005.

[15] X. Zhou, R. E. Kooij, H. Uijterwaal, and P. van Mieghem, "Estimation of Perceived Quality of Service for Applications on IPv6 Networks," in ACM PM2HW2N'06, Oct. 2006.

[16] D. P. Pezaros, D. Hutchison, F. J. Garcia, R. D. Gardner, and J. S. Sventek, "Service Quality Measurements for IPv6 Inter-networks," in 12th IEEE IWQoS, Jun. 2004.

[17] T.-Y. Wu, H.-C. Chao, T.-G. Tsuei, and Y.-F. Li, "A Measurement Study of Network Efficiency for TWAREN IPv6 Backbone," International Journal of Network Management, vol. 15, no. 6, pp. 411–419, Nov. 2005.

[18] K. Cho, M. Luckie, and B. Huffaker, "Identifying IPv6 Network Problems in the Dual-Stack World," in ACM SigComm Network Troubleshooting Workshop, Sep. 2004.

[19] S. Zeadally and L. Raicu, "Evaluating IPv6 on Windows and Solaris," IEEE Internet Comput., vol. 7, no. 3, pp. 51–57, May/Jun. 2003.

[20] R. Sargent, "Verification and validation of simulation models," in Proceedings of the 37th conference on Winter simulation. Winter Simulation Conference, 2005, pp. 130–143

[21] A. Law, "Statistical analysis of simulation output data: the practical state of the art," in Simulation Conference, 2007 Winter. IEEE, 2008, pp. 77–83.

[22] OPNET, Modeler Release, 14th ed. [Online]. Available: http://www.opnet.com/solutions/network_rd/modeler.html

[23] K. Salah, P. Calyam, and M. Buhari, "Assessing readiness of IP networks to support desktop

videoconferencing using OPNET," Journal of Network and Computer Applications, vol. 31, no. 4, pp. 921–943, 2008.

[24] J. Moy, "OSPF Version 2," RFC 2328 (Standard), Internet Engineering Task Force, Apr. 1998, updated by RFC 5709 [Online]. Available: http://www.ietf.org/rfc/rfc2328.txt

[25] R. Coltun, D. Ferguson, J. Moy, and A. Lindem, "OSPF for IPv6," RFC 5340 (Proposed Standard), Internet Engineering Task Force, Jul. 2008. [Online]. Available: http://www.ietf.org/rfc/rfc5340.txt

[26] P. Chimento and J. Ishac, "Defining Network Capacity," RFC 5136 (Informational), Internet Engineering Task Force, Feb. 2008. [Online]. Available: http://www.ietf.org/rfc/rfc5136.txt

[27] K. Salah, P. Calyam, and M. Buhari, "Assessing readiness of IP networks to support desktop videoconferencing using OPNET," Journal of Network and Computer Applications vol. 31, no. 4, pp. 921–943, 2008.

[28] O. Balci, "Principles and techniques of simulation validation, verification, and testing," in Simulatio Conference Proceedings, 1995. Winter. IEEE, 2002, pp 147–154.

[29] K. Pawlikowski, H. Jeong, J. Lee et al., "On credibility o simulation studies of telecommunication networks," IEE Communications Magazine, vol. 40, no. 1, pp. 132–139, 2002.