A Detail Comprehensive Review on IPv4-to-IPv6 Transition and Co-Existence Strategies

Priya Bali

M-Tech Student & Department of CSE & Delhi College of Technology & Management
Palwal, Haryana, India

***Abstract*— Internet Protocol version 4 (IPv4) addresses have been reported to be nearing exhaustion and the next generation Internet Protocol version 6 (IPv6) is gradually being deployed in the Internet. IPv6 provides a much larger address space, better address design and greater security, among other benefits. IPv6 deployment requires thorough and careful preparation to minimize network disruption and ensure that the benefits of IPv6 are obtained. Due to the drawbacks of IPv4,now these days IPv6 is extremely popular in organizations, companies and Internet service providers (ISP).For preventing the change from IPv4 to IPv6, three mechanisms will be used for a smooth transition from IPv4 to IPv6 with less effect on the network. These mechanisms are Tunnel, Dual-Stack and Translation. This paper discuss about IPV4 and IPV6 and use manual transition strategies and automatic of IPV6 and also compare their performances to show how these transition strategies affects network behavior.**

Index Terms— **IPv6, IPv4, 6to4 Tunnel, Manual Tunnel, Dual-Stack**

I. INTRODUCTION

With the exhaustion of available IPv4 address space at the IANA-to-RIR (Regional Internet Registry) level, it's only a matter of time before the RIRs exhaust, followed by ISP exhaustion. Enterprise organization will not be able to obtain IPV4 address space for new network during ISP exhaustion. Only IPV6 address space will be offered by them. IPV6 represents objective for IP address hungry organization and provide many features and increase in address space capacity is unique to IPV6. Increase in address space at cost of different address format and notation which affect network layer routing and application that display IP address. Organizations having IPV4 network they need to implement IPV6 faces many difficulties in finding impacts, planning transition and executing migration to IPV6. For attracting new customer via internet plan of organization should be complied documenting current environment and planned step to IPV6 deployment. While discussing IPV6 deployment, we discuss about initial state of IPV4 only network to which IPV6 node and Network are added and provide result in IPV6 only network. Most organization use above scenario and utilize both IPV4 and IPV6 for some time. So, migration word is use for migrating from IPV4 only network and combination IPV4-IPV6 network and suggest many strategies to implement that transition.

II. MIGRATION TECHNOLOGIES OVERVIEW

There are many applications for migration to IPV6. These technologies are discussed according to specific categories:-

i. ***Dual stack***: - It support both IPV6 and IPV4 on Network devices.
ii. ***Tunneling*****:** - Within IPV4 packet encapsulation of IPV6 packet for transmission over IPV4 network.
iii. ***Translation***: - Address translation of gateway device or translation of code in TCP/IP code of router.

A. Dual-Stack Approach:

It consist of implementation of both IPV4 and IPV6 protocol stack on the devices that needed access to both network layer technologies (including router) and end user devices. These devices would be configured with both IPV6 and IPV4 address and they got those addresses via method defined for protocol as enabled by administrators. For example, IPV6 address is auto-configured, while IPV4 address is obtain by DHCPV4.

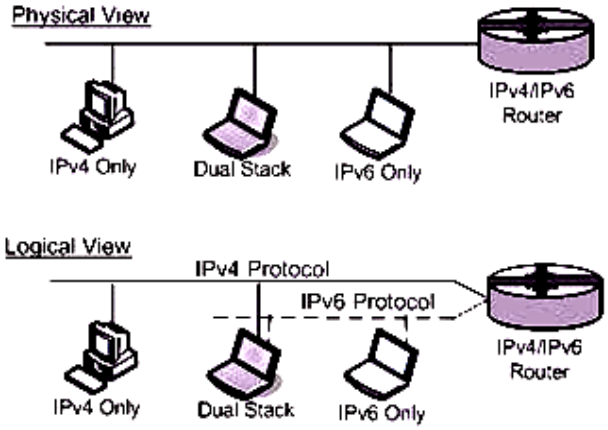

Figure 1: Dual-stacked Network Perspectives

ISSN: 2278 – 1323

With Dual stack approach implementation May changes with respect to extent of stack that is shared versus to each IP version what is unique. Using application, transport and Data Link Layer only network only Network Layer would be dualized. Other approach requires a separate network interface for IPV6 Vs IPV4 to span entire stack down to physical layer. This approach is desirable for benefits of layered protocol model in case of network servers with multiple applications. They support only one version in case of network server with multiple applications.

Dual-Stack deployment

During deployment of Dual stack devices, common network interface is share that implies operation of both IPV6 and IPV4 over same physical link. Routers supporting such links to be dual stacked are required by Dual Stacked devices. This approach is common during transition. This diagram can be modify beyond a physical LAN to multi hope network where routers route IPV4 packet among native IPV4 host and IPV6 packet among IPV6 capable host. These router support IPV4 and IPV6,RFC 4554 which is informational RFC describing a new approach using VLANs for supporting an overlay configuration without any need of immediate router upgrades, while routers would usually be among first IP element to be upgrade to support both protocols.

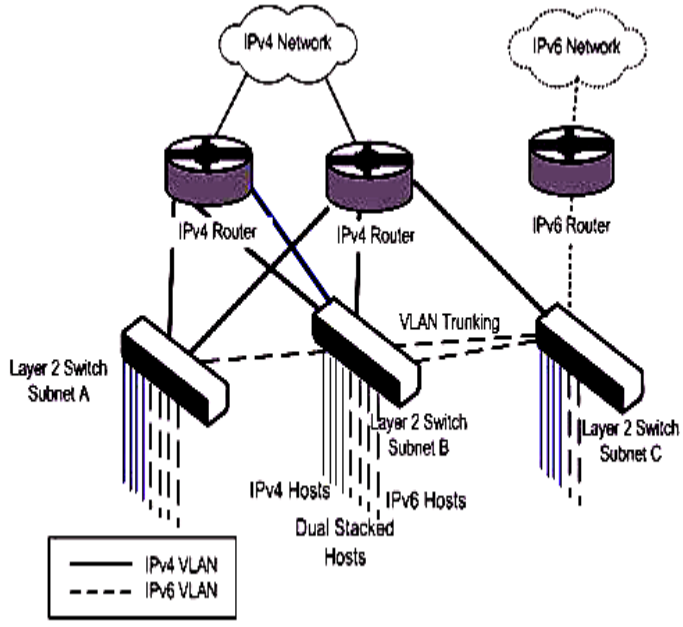

Figure 2: Dual-stacked VLAN Network

This approach on VLAN tagging to enable layer 2 switch to broadcast Ethernet frames having IPV6 payload to one or more IPV6 capable router switch ports can be configures as "IPV6 VLAN" to which its interfaces are connected this can be done by upgrading one router to support IPV6. Other dual stacked devices or IPV6 devices can be configured as member of VLAN and multiple VLAN.

B. Tunnelling Approaches

To support IPV6 over IPV4 and IPV4 over IPV6 tunnelling, many type of tunnelling technologies has been developed. These technologies are classified as automatic or configured. Automatic tunnels are created and torn down "on the fly" whereas configured tunnel are predefined. Firstly we will be reviewing some tunnelling basics, after that we will be discussing these tunnelling types. Tunnelling of IPV6 packets by an IPV4 network include prefixing each IPV6 packets with IPV4 headers. Due to this, tunnelled packet route over IPV4 routing infrastructure. Encapsulation is performed by router and entry node of tunnel. IPV4 address of source in IPV4 header is populated with IPV4 address of node and target address is that of tunnel endpoint. Protocol field of IPV4 header shows an encapsulated IPV6 packet, it is set to 41(decimal). The tunnel endpoint or exit node perform decapsulation to strip off IPV4 header and send the packet to destination by IPV6.

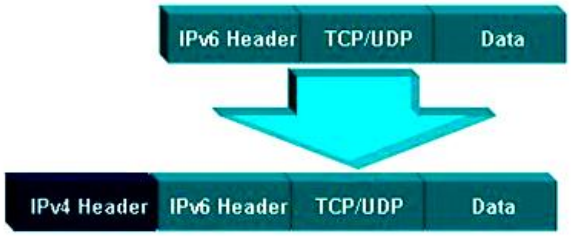

Figure 3: IPv6 over IPv4 Tunnelling

I. Tunnel types

There is different type of scenarios based on defined tunnel endpoint, while process of tunnelling is identical for all type of tunnels. Router- to –Router is most common configuration

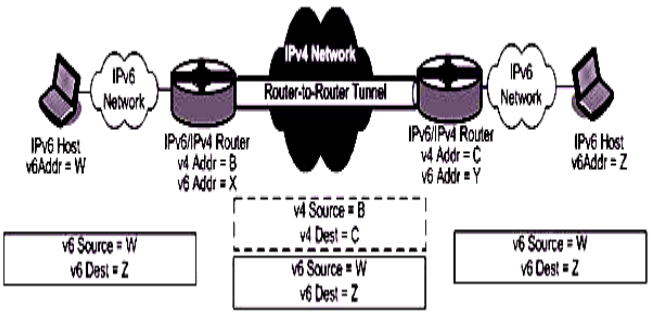

Figure 4: Router-to-Router Tunnel

In above diagram, Originating IPV6 host on the left side has an IPV6 address of W. A packet 3 destination for host at very far end of figure with Z's IPV6 address is sent to router. IPV6

ISSN: 2278 – 1323

packet is received by this router (with IPV6 address of X and IPV4 address of B). Router encapsulate IPV6 packet with header of IPV4, configured to tunnel packets target for network on which Z host resides. Router uses (B) IPV4 address as sender's IPV4 address and tunnel endpoint router as destination address. Packet is de-encapsulates by endpoint router stripping off IPV4 header and move the original IPV6 packet to destination (Z). Other tunnelling scenario's features an IPV6/IPV4 host cable of supporting both IPV4 and IPV6 protocol, tunnelling a packet to router that cause de-encapsulates the packet and move it by IPV6. The tunnelling mechanism is identical as in router- to- router case but tunnel endpoint are alike.

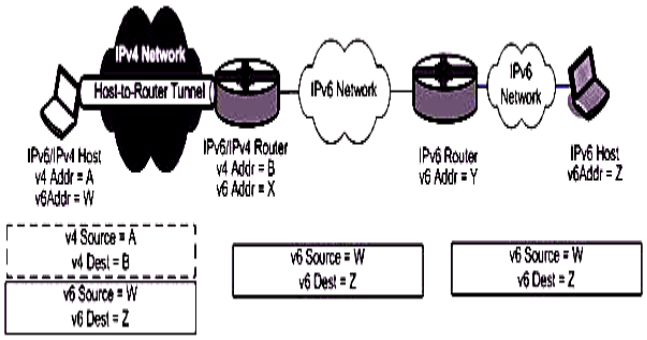

Figure 5: Host-to-Router Tunnelling Configuration

In Figure 6 router to host configuration is identical to router to router tunnelling originating IPV6 host in figure sends IPV6 packet to its local router which move it to a router closest to target. Tunnel IPV6 packet is configured over IPV4 to host by serving router.

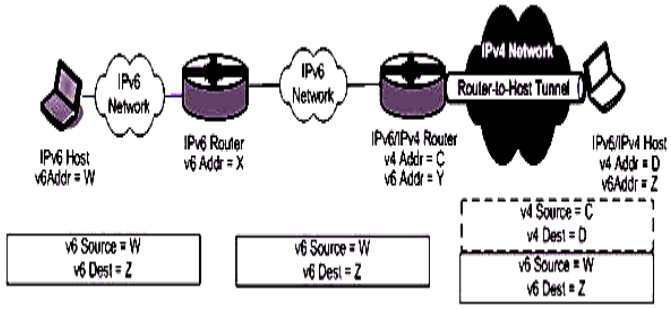

Figure 6: Router-to-Host Tunnel Configuration

Final tunnelling configuration is spans end to end from host to host. If infrastructure of routing has not been upgraded for supporting IPV6, This tunnelling configuration activates two IPV6/IPV4 hosts to communicate via tunnel over IPV4 network. In this example communication is IPV4 from end to end

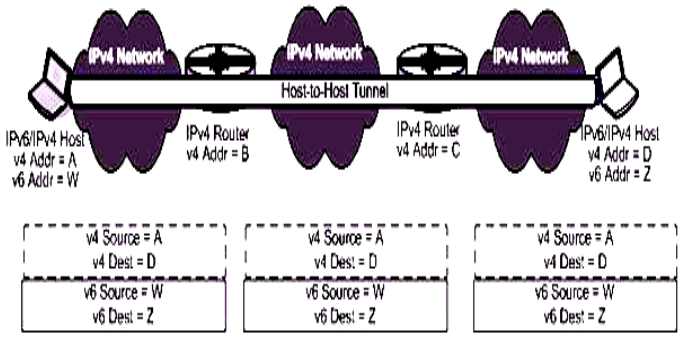

Figure 7: Host-to-Host Tunnel Configuration

III. LITERATURE REVIEW

In [2] Authors investigate a dual stack worm which can spread over IPV4 - IPV6 Dual Stack Network. Two level scanning strategies are applied by this worm to find the target in Dual Stack Network. After simulation Result, they find that worm spread much faster in IPV4-IPV6 Dual Stack Network than in pure IPV4.Worm defenses is consider in future internet construction. In [3] Authors designed and simulated network by using OPNET Modeler to study different translation schemes. After simulation Result, they find that network performance varied across different mechanisms. Result shows that IPV6 has higher throughput than IPV4 Dual stack 6 to 4, manual tunnel mechanism. In [4] Authors study about common transition technologies that facilitate co-existence of both IPV4 & IPV6 address. They use different scenarios for migrating to IPV6.These scenarios falls within one of 3 transitional technology categories native dual stack tunnelling and translation. Based on the result of this research paper, Native Dual Stack Technology should be considered by companies for their deployment. It can be done on technologies that allow IPV4 host to communicate with IPV6 host and services are needed. In [5] Authors survey on importance of IPV6 and reason to deploy IPV6 and they discuss standards and techniques which are require for interoperation between two protocol. Dual stack architecture, Tunnelling mechanism, Translation Device is use for supporting both protocol. Authors conclude that IPV6 provide great advantage as compare to IPV4. We must implement IPV6 for future use. In [6] Authors analysed performance of Dual stack IPV4 - IPV6 system in university network by using jitter and delay period. They calculate jitter and delay period by transferring various files with different size. Result shows average of Jitter period is around size transfer. Result of this research shows that Dual stack system is reliable implementation for migration of IPV4 to IPV6 system. To increase the performance of IPV6 Connection, in further research we can use multiple header compression schemes that have been design overtime to decrease header size. It will increase performance of IPV6. In [7] Authors analysed a series of transition mechanism over multiprotocol.

ISSN: 2278 – 1323

IV. CONCLUSION:

Based on our interviews and research, native Dual-Stack is the technology that companies should consider for their deployment. It keeps both IPv4 and IPv6 running at the same time. When the network is fully transitioned to IPv6, operators can stop supporting IPv4. The two protocols must be supported until native IPv6 is the only protocol in use. The cost of operation for Dual-Stack is more than single stack for operators because they have to support both stacks. If it is difficult for operators to move directly to native IPv6, then they can go implement transition technologies. According to our findings, the next best transition technology to deploy in the network is NAT64. Some of the companies are planning to run NAT64 in their network and then move to native IPv6 when all the applications and content is available on IPv6. If the SP's access network is not IPv6 ready, then they should plan to deploy 6rd in their network. NAT444 allows customers to run IPv4 services after the exhaustion of IPv4 addresses. However, this is not a viable long-term solution. Additionally, the implementation of NAT 444 will require investment in a NAT logging infrastructure.

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.

ISSN: 2278 – 1323