# Analysis of IPv6/IPv4 Dual-Stack Transition Mechanism

**Surbhi Rani[1], Vandana[2]**

M-Tech Student[1,] Assit. Prof. [2] & Department of CSE
Delhi Institute of Technology, Management & Research
Faridabad, Haryana, India

***Abstract*—With the debilitation of the IPv4 addressing space rapidly approaching, it has become a high preference for enterprises, service providers, application developers, IP appliances manufacturers, and governments to start their preparations of IPv6. A smooth transition from IPv4 to IPv6 is difficult to attain. Thus various mechanisms are needed which assures stepwise, smooth and independent modifications to IPV6. Not only is the migration, combining of IPv6 is also needed into the available networks. The mechanisms (or solutions) can be categorized into three classes: tunnelling, dual stack and translation. The more favoured and most versatile way to prepare IPv6 in available IPv4 environments is Dual-Stack. IPv6 can be enabled whatever IPv4 is enabled by with the related features needed to build IPv6 highly available, routable and safe. In many cases, IPv6 is not enabled on a particular device or interface due to the presence of legacy hosts or applications which do not support IPv6. On the contrary, IPv6 may be enabled on devices and interfaces for which the support of IPv4 is no longer required. In this project the Dual-Stack migration technique is implemented by using GNS3 (Graphical Network Simulator) and CISCO routers. The procedure of this network is watched with the help of Wireshark (Packet analyser). The configuration integrates both, tunnelling and Dual-Stack techniques, which can be noted by catching the packets in the router interfaces.**

**Keywords: IPV6, IPv4, Dual-Stack, tunnelling, Wireshark**

## I. INTRODUCTION

The The current Layer 3 protocol is Internet Protocol version 4 (IPv4) employed on the most networks and Internet. IPv4 is preferred from more than 30 years and has been an in-built part of the Internet evolution. Originally it was described in RFC 760 (January 1980) and discussed by RFC 791 (September 1981). RFC 1819.ST was an observational resource reservation protocol proposed to supply quality of service (QoS) for real-time multimedia applications i.e. voice and video. ST is composed of two protocols— Stream Control Message Protocol (SCMP) and ST (Internet Stream Protocol). Internet Stream Protocol version 2 (ST-II or ST2) was not planned as a substitute for IPv4. The concept was that a multimedia application would utilize both protocols—IPv4 for the propagation of traditional packets and ST-II for packets transporting real-time data. Though it was never realized as IPv5, when encapsulated in IP, ST utilizes IP Protocol Number 5 (RFC 1700). In different words, though it was never carried out, the designation “IP version 5” was already specified.

## II. RELATED WORK

In [1], the myriad described IPv4/IPv6 existence technologies and talks about the outstanding features and benefits of each to support us to determine where a suggested technology choice builds the most sense. From a general view, the set of IPv4/IPv6 technologies can be categorized into three categories:
tunnelling - encapsulation of an IPv6 packet within an IPv4 packet for propagation over an IPv4 network or vice-versa; dual stack - implementation of both IPv4 and IPv6 protocols on network devices and translation - IP header, address, and/or port translation which is performed by gateway, host or network address translation (NAT) devices. The paper describes the application support of IPv6. At last it discusses about some service suppliers dual protocol schemes including a combination of techniques from multiple categories.

Internet has received decades of quick development, as the basis of the whole network the IPv4 also has grown. However, because of its own limits, it has been gradually disclosed various defects, so IPv6 planned by IETF as an option to IPv4. This paper discuss three main transition techniques: dual-stack (Dual Stack), tunnel (Tunnel), the address protocol conversion (NAT-PT) and the observational framework of the three techniques, which provide a useful support for IPv6 network design. [2]

IPv6 transition represents many issues to the Internet community, and many solutions have been suggested, involving tunnelling, dual stack and translation. Tunnelling provides support to "like-to-like" IP connectivity over an "unlike" network, whereas translation provide support to "like-to-unlike" IP interconnectivity. No central mechanism is available to deal with all possible scenarios. Because tunnelling can hold the end-to-end framework that the Internet is constructed on, the authors have demonstrated a tunnel-based model that resolves the transition issues in backbone and access networks with various tunnelling techniques. [3]



ISSN: 2278 – 7798 

With the quick development of Internet, IPv4 protocol can no longer fulfil the requirements of users. This is primarily because of the restrictions of IPv4 in terms of routing, addresses and security. Correspondingly, IPv6 has the benefits of security, large address space, quality of Service, mobility and so on. Thus, IPv6 protocol has become the important mechanism for network development. However IPv6 and IPv4 are not compatible protocols, so a solution to transition is needed. In order to obtain stepwise and smooth transition, IETF encourages three types of transition techniques: dual stack, tunnelling and translation technology. This paper presents the principle of these transition techniques, definitely suggests a solution to seamless IPv6 transition based on translation and tunnelling techniques. At last, they implement two types of tunnel and deploy a IVI transition scheme. The experiment results indicate that the suggested solution is viable. [4]

## III. TRANSITION MECHANISMS

Here the transition to IPv6 requires to happen. For at least the predictable future, IPv6 and IPv4 will exist together and there is no switchover date or deadline to go from IPv4 to IPv6. The transition is assumed to take years. The Internet Engineering Task Force (IETF) has generated several tools, protocols and processes which help network administrators to migrate their networks to IPv6. These technologies can be categorized into three categories:

### A. *Dual-Stack*

A dual-stack device has total support for both IPv6 and IPv4. It can be a host, server, printer, router, or any device that can be deployed to provide support to both protocols. In the IPv4 world, this involves IPv4 addresses, Internet Control Message Protocol (ICMP) and Address Resolution Protocol (ARP) for IPv4.

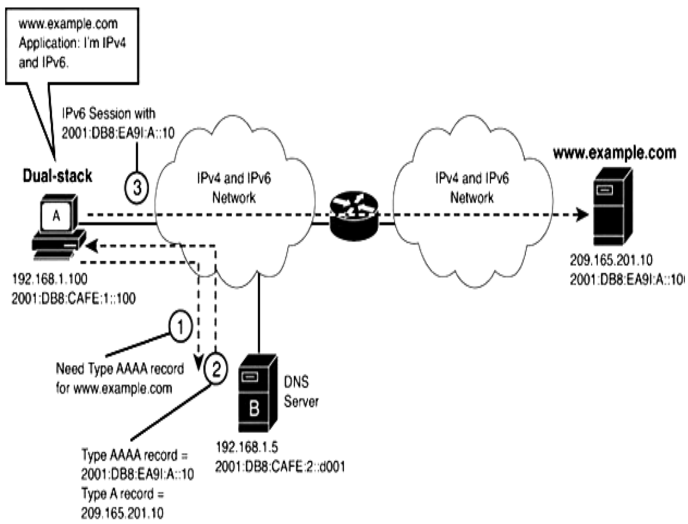


**Figure. 1 IPv4 Application Using the IPv4 Stack**

An IPv4 router provides support to IPv4 routing protocols i.e. Open Shortest Path First version 2 (OSPFv2) and Enhanced Interior Gateway Routing Protocol (EIGRP) and IPv4 static routes. IPv6 support involves IPv6 global uncast and link-local addresses, ICMPv6 operations involving Duplicate Address Detection (DAD) and Stateless Address Auto configuration (SLAAC). An IPv6 router requires propagating IPv6 packets by using static routes and IPv6 routing protocols i.e. EIGRP for IPv6 and OSPFv3. An IPv6 router sends ICMPv6 Router Advertisement messages and can perform translation or tunnelling techniques. During the communication with an IPv4 device, it acts as an IPv4-only device. During the communication with an IPv6 device, it behaves as an IPv6-only device.

### B. *Transition*

Other type of IPv4-to-IPv6 transition technique is tunneling. Similar to other transition schemes, tunneling should be taken as a temporary solution until original IPv6 can be utilized. A tunnel is not more than encapsulating the one IP packet inside another IP packet. A tunnel can be an IPv4 packet put in another IPv4 packet. One of the issues in combining IPv6 into the present IPv4 networks is the capability to transport IPv6 packets across IPv4-only networks. One manner to do this is to utilize a tunnel or, in IPv6, which is called Tunneling is a mechanism that permits devices in separated IPv6 networks to send IPv6 packets across the IPv4 network. [6] A tunnel has two kinds of protocols, a passenger protocol and a transport protocol. Overlay tunnels put IPv6 packets in IPv4 packets for delivery over an IPv4 infrastructure.

### C. *Translation*

Network Address Translation (NAT) is a known method in IPv4, generally employed to translate between private addresses and public IPv4 address space. NAT64 easily provides access between IPv4-only and IPv6- only networks. Address Family Translation (AFT) or simply translation, provides communications between IPv4-only and IPv6-only networks and hosts. AFT performs IP address and header translations between these two network layer protocols [7]. Similar to other transition mechanisms, translation is not a long-term technique and the finest aim should be native IPv6. However translation provides two major benefits over tunnelling:

i. Translation offers a means for slow and smooth transition to IPv6.
ii. Content providers can provide services easily to IPv6 Internet subscribers.

NAT64 is the substitute for NAT-PT, Network Address Translation – Protocol Translation, as described in RFC 6144, model for IPv4/IPv6 Translation. Cisco prefers not using NAT-PT, supporting its substitute NAT64. NAT-PT has been viewed depreciated by IETF due to its tight association with Domain Name System (DNS) and general restriction in translation. These causes are described in RFC 4966, causes to Move the Network Address Translator - Protocol Translator



ISSN: 2278 – 7798 

(NAT-PT) to Historic Status. IETF suggested NAT64 as the replacement to NAT-PT.

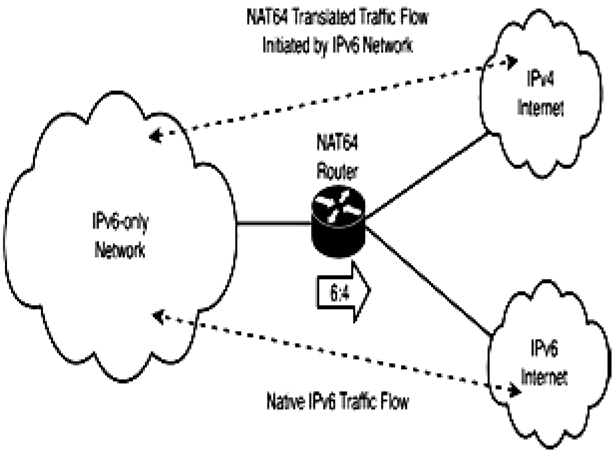


**Figure. 2 IPv6-only Networks Accessing IPv4 and IPv6 Internet**

## IV. IMPLEMENTATION AND RESULTS

For The network diagram in Fig 3 indicates the Dual-Stack implemented configuration, in which R1 and R2 are two Dual-Stack routers. The router R2 is set up only with IPv4 stack.

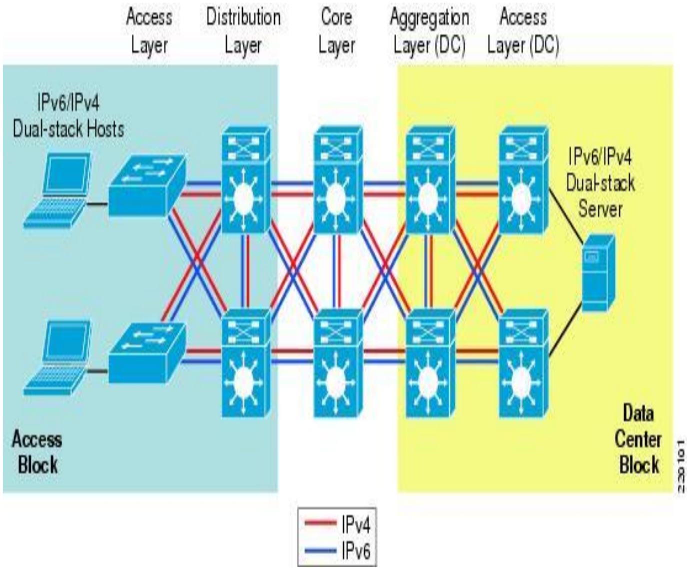


**Figure. 3 Dual-Stack enabled network**

The Network addresses are also indicated close their respective networks. A Tunnelling strategy is required when we are needed of linking IPv6 Domains through IPv4 Clouds. 6to4 Tunnelling is deployed in this network to obtain connectivity between the IPv6 networks. It is a point-to-multipoint tunnel. The destination IPv4 address of the tunnel is decided by the destination IPv6 address of the packet. 6to4 tunnels need a relationship between the IPv6 network address or prefix and IPv4 tunnel addresses. The IPv6 address is opposite engineered by the IPv4 tunnel address by using the format 2002: tunnel-IPv4-address::/48. This permits a single tunnel to be generated that has several destinations - a point-to-multipoint tunnel.

*Wireshark captures and Results*

The Fig 4 indicates the Wireshark capture built in the Ethernet link between the Routers R2 and R3.

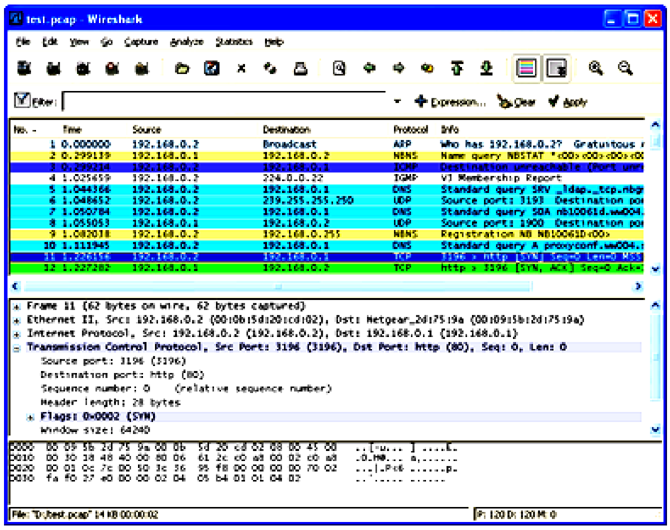

**Figure. 4 Wireshark capture of ICMP packets**

We can view that the ICMP message consists both, IPv6 and IPv4 fields in its packet. The data inside these fields are analyzed in the fig. 5 and 6.

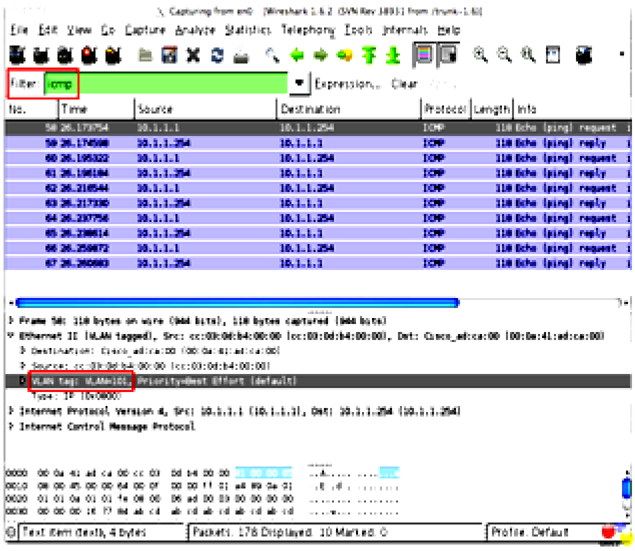

**Fig 5 IPv4 field analysis**

The primary contents to be observed in the IPv4 field are the Source and Destination addresses and Protocol Type. The Protocol field in the IPv4 header shows the Network layer at the destination host, to which Protocol this packet relates to.


ISSN: 2278 – 7798 

Protocol 41 introduces the encapsulation of IPv6 packets inside the IPv4. [9]

The Ping is done to the host in 2001:DB8:0:3::/64 network from the host in 2001:DB8:0:1::/64 network. But we can view that the Source and Destination addresses observed by the Wireshark are the IPv4-only interfaces of the Routers R1 and R3, which are the two end-points of the 6to4 Tunnel.

The analysis of the IPv6 field is indicated in the fig below. The primary content to be observed in IPv6 is its Source and Destination addresses.

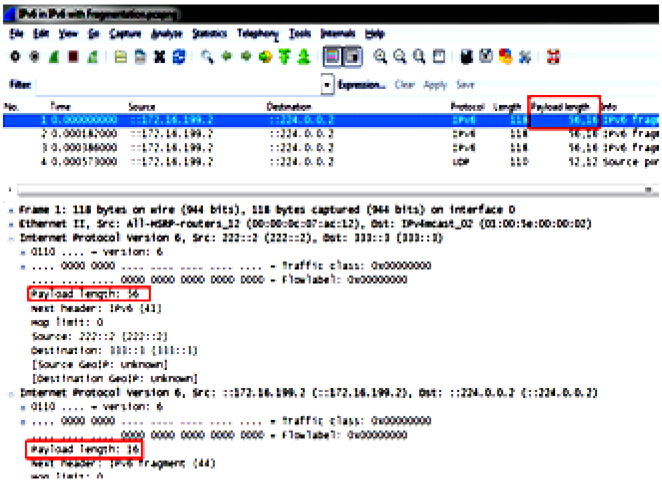


**Figure. 6 IPv6 field analyses**

The Source and Destination addresses in IPv6 describe the actual end-to-end addresses of the communicating hosts.

## V. CONCLUSION

Nowadays, lots of researches and works have been carried out on IPv6 and its related challenges, and there is yet a long way to go. IPv4 and IPv6 must exist together for some number of years, and their coexistence must be easily understandable to end users. If an IPv4-to-IPv6 migration is successful, end users should not even note it. Dual stacking is the favored solution in various scenarios. The dual-stacked device can operate equally with IPv6 devices, IPv4 devices, and other dual stacked devices. Tunnels can be generated where there are IPv6 islands isolated by an IPv4 ocean, which is the norm in these former stages of the migration to IPv6. To understand and experiment the role which IPv6 will play in the future, it is significant for us to develop experience with the IPv6 technology. Through our attempt in generating a Dual-Stack network by using GNS3 have permitted us to formulate expertness and become technically adequate with IPv6 technology in an academic environment. It can enhance our knowledge regards the IPv4 to IPv6 migration and transition. We have also been capable to find the basic of IPv6 technology and implementation of migration techniques. It also provided us the chances to understand and test the IPv6 technology before any real implementation time comes. This project could be employed to other organizational setting which proposes to implement IPv6 in their network interconnection.

## REFERENCES


[1] Dooley, M. and Rooney, T. (2013) ‘IPv4/IPv6 Co-Existence Technologies’, IPv6 Deployment and Management, Wiley-IEEE Press, First Edition

[2] Li XiaoHong (2013) ‘The Research of Network Transitional Technology fromIPv4 to IPv6’, Digital Manufacturing and Automation (ICDMA), 2013 Fourth International Conference, Qingdao, pp. 1507 – 1509

[3] Carpenter. B and Moore. K (2001) ‘Connection of IPv6 Domains via IPv4 Clouds’, IETF RFC: 3056

[4] Cui Yong, Dong Jiang, Wu Peng, Wu Jianping, Metz Chris, Lee Yiu L. and Durand Alain (2013) ‘Tunnel-Based IPv6 Transition’, Internet Computing, IEEE (Volume: 17, Issue: 2), pp. 62 – 68

[5] Chris Sanders (2011) ‘Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems’, No Starch Press, Second Edition

[6] Aazam, M., Syed, A.M., Shah, S.A.H., Khan, I. and Alam, M. (2011) ‘Evaluation of 6to4 and ISATAP on a test LAN’, Computers & Informatics (ISCI), 2011 IEEE Symposium, Kuala Lumpur, pp. 46 – 50

[7] Arkko. J and Baker. F (2011) ‘Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment’, IETF RFC: 6180

[8] Heping Hou, Qin Zhao and Yan Ma (2010) ‘Design and implementation of a solution to smooth IPv6 transition’, Advanced Intelligence and Awareness Internet (AIAI 2010), 2010 International Conference, Beijing, China, pp. 157 – 161

[9] Huitema. C (2001) ‘An Anycast Prefix for 6to4 Relay Routers’, IETF RFC: 3086

[10] Joseph Davies (2013), ‘Understanding IPv6’, Microsoft Press, Third Edition

[11] Chakraborty, K., Dutta, N. and Biradar, S.R. (2009) ‘Simulation of IPv4-to-IPv6 Dual Stack Transition Mechanism (DSTM) between IPv4 hosts in integrated IPv6/IPv4 network’, Computers and Devices for Communication, 2009. CODEC 2009. 4th International Conference, Kolkata, pp. 1 – 4

[12] Rick Graziani (2013) ‘IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6’, Cisco Press, First Edition

[13] Shirasaki. Y, Miyakawa. S, Yamasaki. T and Takenouchi. A (2005) ‘A Model of IPv6/IPv4 Dual Stack Internet Access Service’, IETF RFC: 4241




ISSN: 2278 – 7798 