Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Performance evaluation of simultaneous network configuration using dual stack and tunnel transition techniques: An enterprise level analysis

Abdul Basit, Rashid Hussain *

Faculty of Engineering Science and Technology, Hamdard University, Sharae Madinat Al-Hikmah, Karachi 74600, Pakistan

ARTICLE INFO

Article history:
Received 28 June 2016
Received in revised form
19 December 2016
Accepted 10 January 2017

Keywords:
IPv6-IPv4
Double stack
Tunneling

ABSTRACT

Exhausted IPv4 addresses space has impetus interest in the next generation of Internet Protocol IPv6. Internet Engineering Task Force (IETF) developed the IPv6 protocol that will replace the IPv4 version completely after a transition period, during which these two protocols will cohabit concurrently. However, these two protocols are incompatible; various transition mechanisms have been implemented to enable domains using the IPv4 protocol to communicate with those who use the IPv6 protocol. This research expounded the flexible migration from IPv4 to IPv6 environment involving coexistence network configurations, performance comparison of sending receiving IPv6 datagrams via dual stack and tunnel mechanisms. The authors have investigated both transition techniques for communication of IPv4/IPv6 datagrams simultaneously in an enterprise environment.

1. Introduction

The communication on the Internet mostly runs on IPv4 protocol. Simply because the huge number of computers, it is impossible to cover all in one fell swoop to IPv6 switch. This will certainly be a long-term process. That is, the operation of an IPv6 network must first be performed in parallel with the existing IPv4 network. During the transition must be ensured for all participants that they, regardless of its protocol version have full access to the network resources. So, IPv6 enable host should communicate with an IPv4 host, on the other hand it should also be possible that an IPv4 network to communicate with other IPv6 hosts. About to enable this, strategies have to be developed, the lightweight and flexible migration allow. For this reason, a new group called next generation transition (Ngtrans) was developed by the IETF in the Called life, which deals exclusively with the migration from IPv4 *to IPv6.*

1.1. Transitioning

In order to extend the usability of IPv6, number of transition techniques is available for the co-existence of IPv4 and IPv6 (Cui et al., 2014; 2013; Hadiya et al., 2013; Wu et al., 2013a; 2013b; Bagnulo et al., 2012). Recently reliable IPv6 packet delivery is investigated for mobile networks (Yan et al., 2015; Modares et al., 2016; Zhu et al., 2016). There are two major categories are being expounded based on the earlier research. In this research, three main strategies have been developed that should provide during the transition phase for error-free communication:

Dual-stack method: A network system that supports both an IPv4 and IPv6 stack. Dual IP stack is to equip a network device with a dual-stack protocol, assign an IPv4 address and an IPv6 address to the interface.

Tunneling method: To bridge an IPv4 network is the process of tunnling, the IPv6 datagram is packed into an IPv4 header, and vice versa. Tunnel is configured between two end routers which is connected local area network consisting IPv6 islands.

Translation method: translate IPv4 into IPv6 addresses and vice versa.

1.1.1. Dual-stack method

The Dual - stack - process works on two Stacks, for each protocol provided both protocol, versions use DNS to the name of the IP Addresses to communicate. The computer whose DNS Name resolution provides an IPv4 address to communicate over IPv4, an IPv6 address is assigned, finally over IPv6. Accordingly, IPv4-based applications in an IPv6 system will continue to run without restriction.

* Corresponding Author.
Email Address: rashid.hussain@hamdard.edu.pk (R. Hussain)
https://doi.org/10.21833/ijaas.2017.01.015

However, the terminal needed now post an IPv4 and an IPv6 address, which can lead to obstacles with respect to address shortage. For this reason, the dual stack transition Mechanism (DSTM) was founded only be assigned temporarily to the IPv4 numbers. DSTM header is shown in Fig. 1. During connection establishment, the DSTM terminal only one IPv6 address is assigned initially as shown in Fig. 2. If the unit now to contact an IPv4 system, it receives from a DHCPv6 server IPv4 number, which also makes a temporary record in the DNS optional.

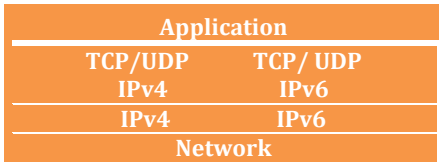

Fig. 1: DSTM Header

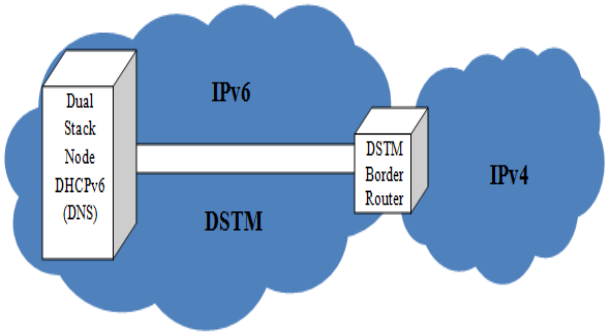

Fig. 2: DSTM connectivity

Limitations of Dual stack method:

1. Full network software update necessary to set up two separate Protocol Stacks
2. Parallel routing table exist (more memory and CPU power) - Routing protocols must be configured separately
3. Various commands for both protocols
4. DNS resolver must be capable of dissolving both types of addresses

1.1.2. Tunneling methods

With the dual-stack method simple IPv6 packets are sent over an IPv6 system. However, if the IPv6 path is interrupted by an IPv4 network, an exchange is no longer possible. For this purpose, the tunneling method has been developed by which the IPv6 packet is encapsulated in the IPv4 route to the associated header and is unpacked at the IPv4/v6-Knoten again (Cui et al., 2013; Hadiya et al., 2013; Wu et al., 2013b; Chen and Li, 2013). General Tunneling means the sending of wrapped packages. During the first phase of the migration, the IPv6 packets encapsulated in IPv4 packets as shown in Fig. 3, and later when all routers are added to IPv6 stack, can also IPv4 Transmitted information of the IPv6 packet over IPv6 routes - packets as payload as shown in Fig. 4 and Fig. 5.

Case Scenario A: Tunneling Technique**:** By tunneling technique, IPv6 is a virtual link between two IPv6 nodes established. Thus, IPv6 devices can exchange IPv4 network data. In the Example as shown in Fig. 5, Host A sends the IPv6 packet to router R1. Router R1 receives the packet that is addressed to B, tunnel encapsulates it in an IPv4 header and transmits in an IPv4 tunnel to Router R2. R2 is the tunnel exit point. Router R2 encapsulates the packet and sends it in the original form to Host B.

Fig. 3: Tunnel IPv4 header with IPV6Payload

Fig. 4: Tunnel IPv6 header with IPv4 Payload

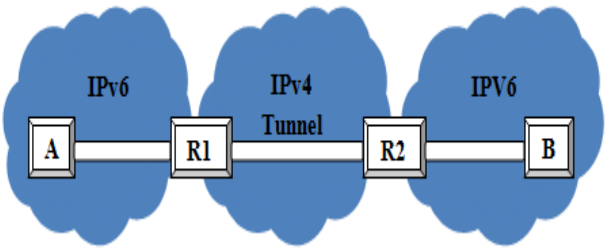

Fig. 5: Tunnel exit point receives

A tunnel always referred to a network path on which an IPv6 packet is sent over an IPv4 network infrastructure. During the transition phase, the tunneling technology can be used in the following cases:

Router to Router: IPv6/IPv4 router, connected to the IPv4 infrastructure to enable IPv6 Packets with each tunnel

Host to Router: IPv6/IPv4 hosts can send IPv6 packets to an IPv6/IPv4 routerIPv4 infrastructure tunnel as shown in Fig. 6.

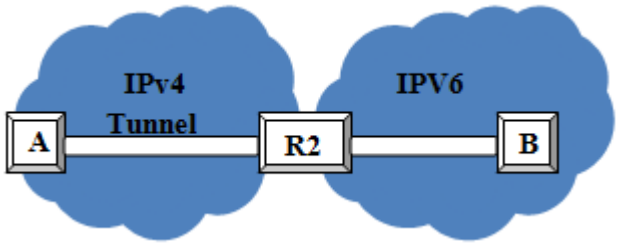

Fig. 6: Host to router

Host to Host: IPv6/IPv4 hosts that are connected by IPv4 infrastructure IPv6 packets are tunneled between themselves as shown in Fig. 7.

Router-to-Host: IPv6/IPv4 routers can tunnel using an IPv4/IPv6 host to achieve through IPv4 infrastructure as shown in Fig. 8.

Configured Tunneling: In the first two tunneling techniques–between two routers as between host router as shown in Fig. 6. Tunnel is configured between two end routers which is connected to networks consisting IPv6 islands. When packet is sent to tunnel then 6to4 transition mechanism occurs. IPv6 packet is encapsulated into IPv4 packet and this encapsulated is routed via IPv4 huge

network. Packet reach to destination where IPv4 header is separated from encapsulated packet and remaining IPV6 packet is routed towards host on Local area network of IPv6. In this technique tunnel end points are configured manually, this tunnel is called “configured tunneling".

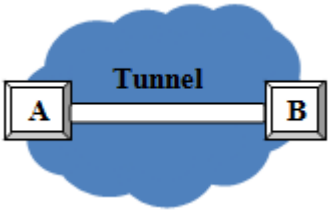

Fig. 7: Host to host

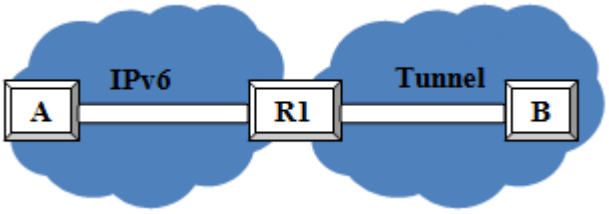

Fig. 8: Router-to-host

Automatic Tunneling: In the last two tunneling technique between two hosts and between one router one host, the IPv6/4 packets are tunneled to its destination host. In this situation, IPv4-compatible IPv6 addresses are configured in automatic IPv4 compatible tunnels. IPv4-compatible IPv6 addresses are IPv6 unicast addresses that have zeros in the high-order 96 bits of the address, and an IPv4 address in the low-order 32 bits as shown in Fig. 9. The tunnel destination is automatically determined by the IPv4 address. Here, IPv4 address refers to automatically generated tunnel destination, these tunnel techniques are called "automatic tunneling".

The IPv4-compatible IPv6 address is formed by filling the first 12 bytes of the IPv6 Address with zeros as shown in Fig. 9.

An IPv4 address (tunnel endpoint), simply by removing the first 96 bits are generated from the IPv6 address, as shown in Fig. 10.

Compatible Address	
96 Bit	32 Bit
0:0:0:0:0:0	IPv4 Addresses

Fig. 9: IPv4 compatible address

3 Bit	13 Bit	32 Bit	16 Bit	64 Bit
FP 001	TLA 0x0002	IPv4 Address	SLA ID	Interface ID

Fig. 10: IPv6 address; an example

Case Scenario B: 6to4 approach**:** Automatic tunnel configuration tunnel set up directly between the communication end points that it, the two at the computer communication involved need one official, globally valid IPv4 Address, which is undesirable in terms of potential address space scarce. Furthermore, it is this method can only be used for dual-stack hosts, since each of the hosts for the construction and Transport of an IPv6-supporting IPv4 packet's responsibility. All of these problems tries to solve the referred to as 6to4 approach (Hadiya et al., 2013; Chen and Li, 2013; Cui et al., 2012).

Here only an IPv4 address for tunneling the entire network is required per IPv6 network. The automatic configuration of the tunnel to the destination network is kept. However, it is the Use of a tailored this method Tunneling Router necessary (Castelli, 2002) (Fig. 11).

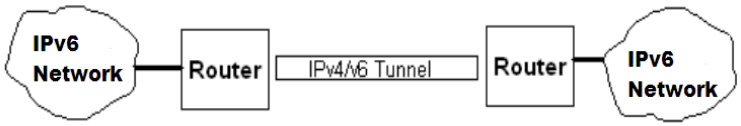

Fig. 11: 6to4 method

Each end node with a unique IPv4 address, a unique IPv6 Assigned prefix

The packages will be shipped by a boarder router (router specifically for the 6to4 process oriented) to the standing in the prefix IPv6 address forwarded

The computers need in this configuration, only the IPv6 protocol stack -. Provided no communication with the IPv4 world is necessary.

The router must be IPv6 capable logically. 6to4 tunnel for automatic configuration in a particular format for the IPv6 prefix of the network is used as shown in Fig. 11. It contains the IPv4 address of the responsible for the tunneling router (Fig. 12).

IPv4 addresses	212.204.101.210: 0xD4.0Xcc.0x65.0XD2
IPv4 compatible IPv6 addresses	0:0:0:0:0:0:D4CC:65D2
Generated from IPv6 addresses	::212.204.101.210::D4CC:65D2

Fig. 12: Format of 6 to 4 Prefix

FP: 001 shows that this is an aggretable Global Unicast Address. TLA: 0x0002-reserved value for the identification of addresses on the 6to4Standard. The next 32 bits after the prefix consist of IPv4 address (gateway address). There remain: 16 bits for subnets

(2 ^{16}) and 64 bits for computer (2 ^{64}) as shown in Fig. 12.

The derivation of IPv6 addresses of IPv4 addresses shown in the as shown in Fig. 13.

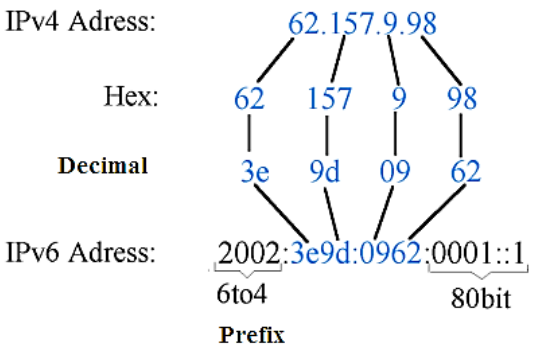

Fig. 13: Derivation of IPv6 addresses of IPv4 addresses

1.1.3. Translation method

The last method for the transition of the protocols is the translation process and is based on the translation of addresses. In this protocol translation must be taken to ensure that this does not affect the application layer, otherwise the applications need to be modified.

Stateless IP / ICMP Translator (SIIT): The SIIT method is suitable for communication between IPv4-only and IPv6-only Systems. By the use of SIIT can be prevented that both Protocol stacks must be placed on the machine. The IPv4 side is from the IPv6 Host addressed by an IPv4-mapped address. The spa located on the IPv6 side Translator, which optionally translates the IP and ICMP messages to the respective IP protocol receives an additional IPv4 address assigned to the IPv4 side obtains an IPv4 mapped address in the format 0 :: FFFF.abcd On the basis of the address can thus decide whether a translation is necessary.

Network Address Translation - Protocol Translation (NAT - PT): In contrast to the SIIT method it needs a dedicated computer here, the Addresses converts. The address conversion is similar to the SIIT, only the IPv4 Address assigned to the first packet of a session. This has the advantage that the Addresses can be exploited efficiently. The IPv6 computer addresses the IPv4 Computer by mean of prefix: wxyz, a router then ensures that all packets with the prefix go to the NAT-PT. The address of an incoming packet is in analogy with the prefix expanded. The communication between the two endpoints is mandatory on the Proxy running, because the address translation must be made for each packet. From this the main problem is this procedure: The proxies are heavily loaded with a lot of traffic. With load balancing, the problem could also be collected.

Probable Migration History

- Once routers are added to the IPv6 stack, IPv6-in-IPv4 tunnels be removed
- IPv6 will be established in addition to IPv4 on the Internet
- IPv4 will be routed for many years on the Internet
- IPv4-in-IPv6 tunnel to later IPv4 over IPv6 islands topologies

Several studies have been conducted for co-existence of IPv4 and IPv6 and transition to IPv6 including; A framework for uninterrupted connectivity using novel stack support for secure IPv6 vehicular communications (Hong, 2013) ISP-level address sharing to connect multiple customers with single IPv4 address using NAT444 and DS-Lite (Santa et al., 2014), Tunnel –based framework for IPv6 transitions in backbone and access networks (Cui et al., 2014), Network layer virtualization for IPv4-IPv6 coexistence for addressing schema, layer 3 routing and packet forwarding (Cui et al., 2012), Implementing security and privacy of network-layer and transport-layer address for IPv6 network (Sheng et al., 2013). Enhanced IP solution for IPv4 addresses depletion without modifications in-path routers (Dunlop et al., 2012). Requirements for configuring an IPv4 over IPv6 networks using the Dynamic Host Configuration Protocol (DHCP) (Cui et al., 2014), Survey on recent internet design such as: mobility, multihoming, multipath, and network scalability issues (Chimiak et al., 2014). Research on the IPv6 performance analysis based on dual-protocol stack and tunnel transition (Campista et al., 2014). IPv4-to-IPv6 transition by allowing communication among unmodified IPv6 and IPv4 nodes (Bagnulo et al., 2012). Key challenges in IPv4-IPv6 tunneling and translation techniques (Wu et al., 2013a), Highlight the reasons behind slow convergence of IPv6 and evaluates the performance of two transition techniques 6to4 and configured tunnel (Hadiya et al., 2013), three major transition technologies: dual-stack (Dual Stack), tunnel (Tunnel), the address protocol conversion (NAT-PT) focusing on future IPv6 network design (Wu and Zhou, 2011), Extensive survey of IP Based internet protocols, standards and it connectivity with WSNs. Sheng et al. (2013) surveyed the mainstream tunneling and translation mechanisms raised since 1998, especially the new mechanisms proposed recently, capturing the aspects of technical principles, pros and cons, scenarios and applicability (Wu et al., 2013a) 4over6 virtualization architecture that virtualizes IPv4-only networks over IPv6-only networks (Cui et al., 2012). Performance of three kinds of mechanism options, double-stack protocol, ISATAP tunneling and 6to4 tunneling technique are analysed and tested (Chen and Li, 2013).

2. Materials and methods

Before going further, it is necessary to present the prototype serving as reference for the tests that follow. The following diagram was thought to be able to put into practice the concepts discovered during the research phase. The simulation software (GNS3,

Oracle Virtual Box and Wireshark) running smoothly on below system requirements:

- System Intel Cori3-Cor i5 (3MB -6MB Cache)
- RAM = 6GB
- Hard Drive = 500GB

The network consists of:

- Router R1(Cisco 2691)
- Router R2(Cisco 3660)
- Router R3(Cisco 3700)
- PC IPv6(Windows 7) Connected By Oracle Virtual Box
- PC IPv4(Windows XP) Connected By Oracle Virtual Box

All explanations below are based on the following diagram. However, another more schema specific is often presented in order to identify the factors to be taken into account.

2.1. Simultaneous network configuration dual stack and tunnel

For implementation Cisco based GNS3 (0.8.6) network simulator is used to simulate network. The network consists of following entities (Fig. 14):

- Router R1(Cisco 3640) using s0/0, Fa1/0,Fa2/0
- Router R2(Cisco 3640) using s0/0, s0/1
- Router R3(Cisco 3640) using s0/0, Fa1/0,Fa2/0
- Router R4(Cisco 3745) using s1/0, s1/1, Fa0/0,Fa0/1
- Router R5(Cisco 3640) using s0/1, s0/2
- Router R6(Cisco 2691) using s1/0, Fa0/0,Fa0/1
- Six PC's

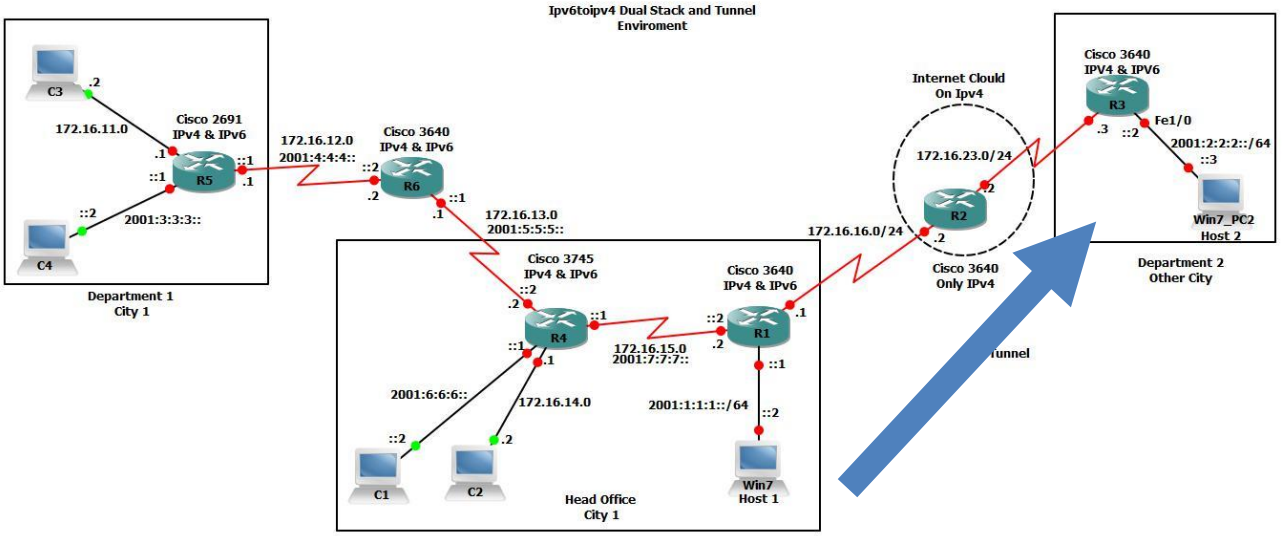

Fig. 14: Simultaneous network configuration dual stack and tunnel

Above mentioned configuration is representing an enterprise environment where a head office is connected to its other department 1in same city via few routers, while connected to department 2 located in other city via IPv4 cloud. Network consist of Five dual stack routers R1,R4,R5,R6 which are connected R3 via only IPv4 supported router R2. These routers are representing Cisco 3640, Cisco3745 and Cisco 2691 functionality while running on IOS. R1 and R3 have IPv6 networks on fast Ethernet Fe1/0 ports while router R2 have two serial ports consist of IPv4 address. Here Router R2 is representing huge IPv4 network, between two small IPv6 networks. Serial Interfaces S0/0 of (R1), S0/0-S0/1 (R2) and S0/0 of R3 are configured on IPv4 address, including networks 172.16.16.0/24 and 172.168.23.0/24 respectively. These interfaces route data packets through EIGRP routing protocol while end routers contain Fast Ethernet1/0, include networks 2001:1:1:1::/64 and 2001:2:2:2::/64 route data packets through OSPF v3 and EIGRP both protocols. In Fig. 14 blue arrow mark is representing tunnel between head office and department 2 which is located in other city.

In above network head office has been linked with other department 1 via dual stack routers within the organization. In Fig. 14, other routers running on Dual Stack mode except R2. Duals stack network include two dual protocol support routers R1, R3 and one only IPv4 support router R2. These routers contain IOS of Cisco 3640 series. Two hosts, Host1 (C1) and Host2 (C3) PCs are representing IPv6 (2001:3:3:3::/64 and 2001:6:6:6::/64) Networks with subnets and performing routing with OSPfv3 protocol for IPv6 packets although Two hosts, Host1 (C2) and Host2 (C4) PCs are representing IPv4 (172.16.11.0/24 and 172.16.14.0/24) Networks with subnets and performing routing with EIGRP protocol for IPv4 packets. All routers are running on EIGRP and OSPFv3 both protocols for IPv4 packets through IPv4 network and IPv6 packet via IPv6 network.

After configuration of above network all systems have connectivity while within the city and outside the city for IPv6 protocol.

2.2. Simultaneous dual stack and tunnel configuration results and performance comparison

In Fig. 15 and Fig. 16 echo ping request and echo ping reply. Fig. 15 is showing ping response to system via tunnel, in below trace sequence is starting from 291 that representing heavy data packet including extra 20 bytes header of IPv4, that require more calculation for router and much delay response. In contrast Fig. 16 dual stack system response is providing less sequence number 4 due to no extra header, in result repose time of dual stack is much quicker than tunnelling.

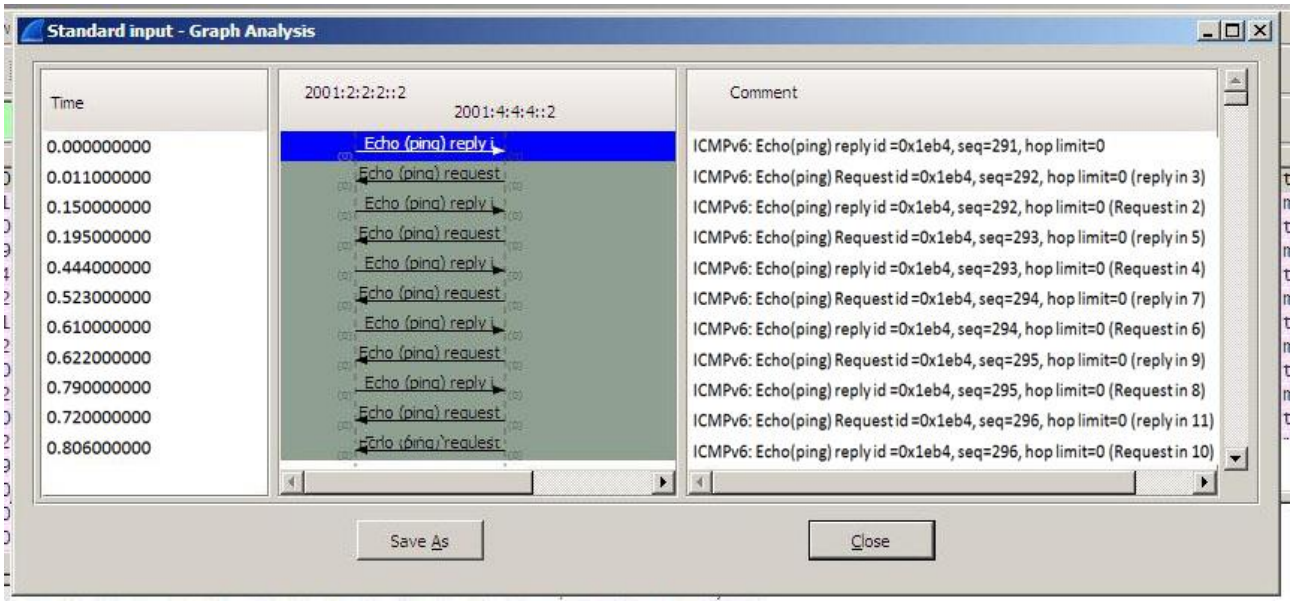

Fig. 15: Ping delay on system through tunnel by Wireshark

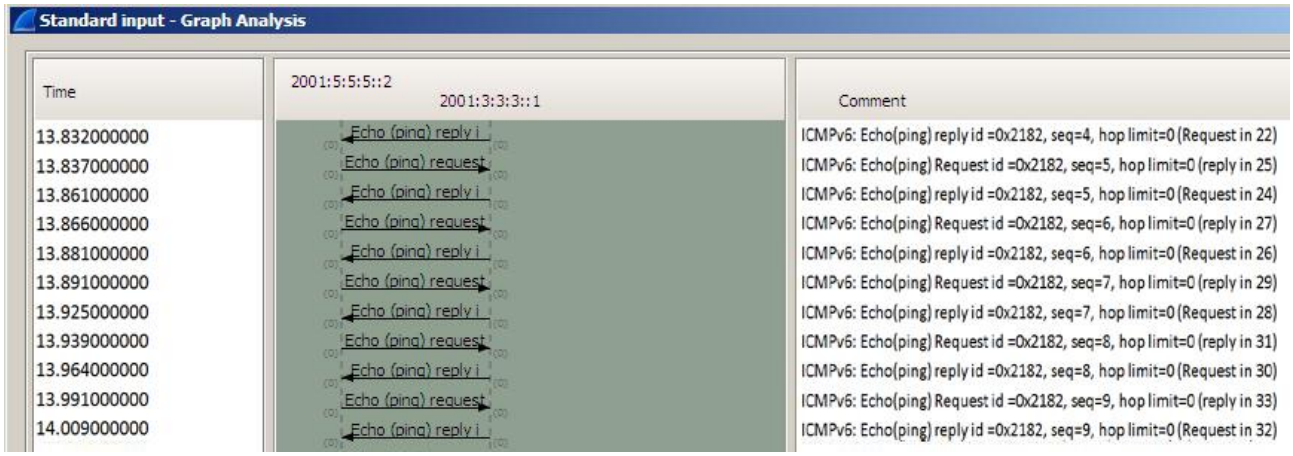

Fig. 16: Ping delay on system by dual stack by Wireshark

In Fig. 17 and Fig. 18 round trip time has been tested with following inputs.

No Of Packets = 1024
Datagram Size = 100
Time out = 2 Sec
Extended Commands = No
Sweep range of size = No

After sending ping request to IPv6 systems via tunnel and dual stacks routes. Fig. 17 is showing round trip response of 1024 data packets with datagram size 100 from R5 to IPv6 system host 2. Due to tunnel encapsulation present between R1 and R3 the round trip time is (Min=12ms, Avg=109ms, Max=432ms) which is much greater round trip time in comparison of dual stack response (Min=0, Avg=32ms, Max=176ms), comparison is being shown in Table 1, testing results can be observed in Fig. 17 and Fig. 18.

3. Conclusion

In Dual Stack, router do not encapsulates or decapsulates the packets, as a result fast and efficient data rate can be possible, it has been concluded that dual stack method is useful for small networks.

In future there is a need of developing more efficient and reliable transition mechanisms, which could reduce the size and complications of the data packets and could condense the routing tables. when all devices on entire networks have unique global IP and NAT technology has been removed than peer to peer communication will become more efficient and reliable, The devices will be able to communicate and translate global and private

address easily, While application such as video conferencing, IP telephony, other needful applications will be have much higher performance.

Table 1: Delay response of dual stack and tunnel transition method

Transition Method	Minimum Delay	Maximum Delay	Average Delay
Dual Stack	0 ms	176 ms	32 ms
Tunnel	12 ms	432 ms	109 ms

Fig. 17: Ping response time in sec on system through tunnel

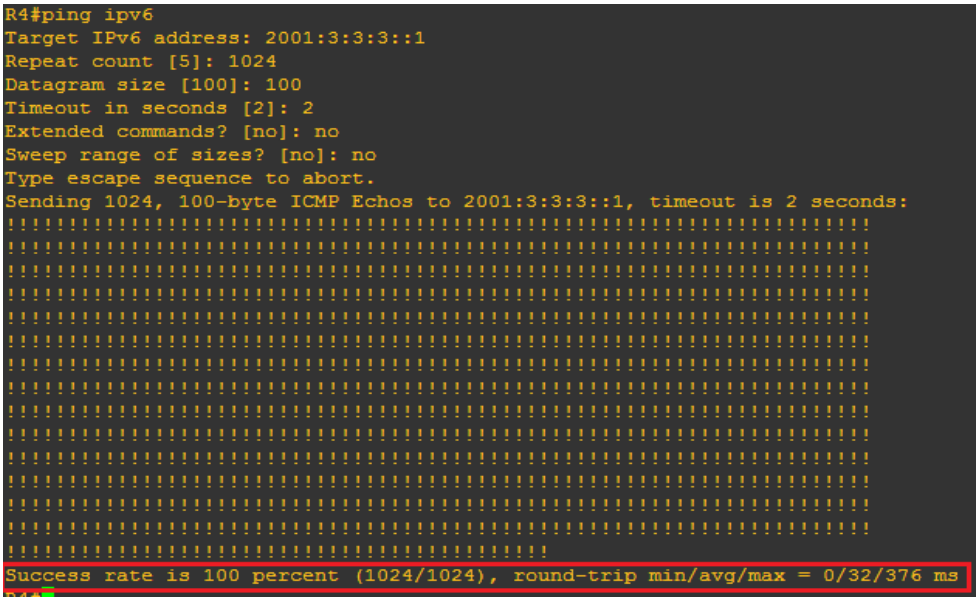

Fig. 18: Ping response time in second on system by dual stack

Acknowledgments

We would like to thank research conducted by Cisco USA, GNS3 (0.8.2) network simulator and to the Graduate School of Engineering Sciences and Information Technology, Hamdard University for their logistic support and services. This work is inspired by research Implementation of IPv6/IPv4 Dual-Stack Transition Mechanism by Niranjan Ravi, Muppidathi, Manoranjan Periyasamy of PSNACET, Dindigul, Tamil Nadu and India.

References

Bagnulo M, García-Martínez A, and Van Beijnum I (2012). The NAT64/DNS64 tool suite for IPv6 transition. IEEE Communications Magazine, 50(7): 177-183.

Campista MEM, Rubinstein MG, Moraes IM, Costa L HM, and Duarte OCM (2014). Challenges and research directions for the future internetworking. IEEE Communications Surveys and Tutorials, 16(2): 1050-1079.

Castelli MJ (2002). Network consultants handbook. Cisco Press, Indianapolis, USA.

Chen WE and Li SH (2013). Client-based internet protocol version 4-internet protocol version 6 translation mechanism for session initiation protocol multimedia services in next generation networks. IET Networks, 2(3): 115-123.

Chimiak WJ, Patton ST, and Janansky S (2014). Enhanced IP: IPv4 with 64-Bit Addresses. Computer, 47(2): 62-69.

Cui Y, Dong J, Wu P, Wu J, Metz C, Lee YL, and Durand A (2013). Tunnel-based IPv6 transition. IEEE Internet Computing, 17(2): 62-68.

Cui Y, Sun Q, Xu K, Wang W, and Lemon T (2014). Configuring IPv4 over IPv6 Networks: Transitioning with DHCP. IEEE Internet Computing, 18(3): 84–88.

Cui Y, Wu P, Xu M, Wu J, Lee YL, Durand A, and Metz C (2012). 4over6: Network layer virtualization for IPv4-IPv6 coexistence. IEEE Network, 26(5): 44-48.

Dunlop M, Groat S, Urbanski W, Marchany R, and Tront J (2012). The blind man's bluff approach to security using IPv6. IEEE Security and Privacy, 10(4): 35-43.

Hadiya D, Save R, and Geetu G (2013). Network performance evaluation of 6to4 and configured tunnel transition mechanisms: An empirical test-bed analysis. In 2013 6th International Conference on Emerging Trends in Engineering and Technology, IEEE: 56-60.

Hong LX (2013). The research of network transitional technology fromIPv4 to IPv6. In Digital Manufacturing and Automation (ICDMA), 2013 Fourth International Conference, IEEE: 1507-1509.

Modares H, Moravejosharieh A, Lloret J, and Salleh RB (2016). A survey on proxy mobile IPv6 handover. IEEE Systems Journal, 10(1): 208-217.

Santa J, Pereniguez-Garcia F, Bernal F, Fernandez PJ, Marin-Lopez R, and Skarmeta AF (2014). A framework for supporting network continuity in vehicular ipv6 communications. IEEE Intelligent Transportation Systems Magazine, 6(1): 17-34.

Sheng Z, Yang S, Yu Y, Vasilakos AV, McCann JA, and Leung KK (2013). A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities. IEEE Wireless Communications, 20(6): 91-98.

Wu P, Cui Y, Wu J, and Li M (2013). Tunnel concentrator placement for traffic optimization in IPv4-IPv6 coexisting networks. In 2013 IEEE International Conference on Communications Workshops (ICC). IEEE: 1309-1313.

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 and Tutorials, 15(3): 1407-1424.

Wu Y and Zhou X (2011). Research on the IPv6 performance analysis based on dual-protocol stack and Tunnel transition. In 2011 6th International Conference on Computer Science and Education (ICCSE). 47(2): 1091-1093.

Yan Z, Wang HC, Park YJ, and Lee X (2015). Performance study of the dual-stack mobile IP protocols in the evolving mobile internet. IET Networks, 4(1): 74-81.

Zhu YH, Chi K, Tian X, and Leung VC (2016). Network coding-based reliable IPv6 packet delivery over IEEE 802.15. 4 Wireless Personal Area Networks. IEEE Transactions on Vehicular Technology, 65(4): 2219-2230.