Research Journal of Applied Sciences, Engineering and Technology 14(8): 299-309, 2017
DOI:10.19026/rjaset.14.4954
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: January 30, 2017 Accepted: April 11, 2017 Published: August 15, 2017

Research Article

A Prototype and Roadmap for Transition to IPv6 with Performance Evaluation

Eman H. Khudhair and Imad J. Mohammed
Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq

Abstract: The migration from IPv4 to IPv6 can not be achieved in a brief period, thus both protocols co-exist at certain years. IETF Next Generation Transition Working Group (NGtrans) developed IPv4/IPv6 transition mechanisms. Since Iraq infrastructure, including universities, companies and institutions still use IPv4 protocol only. This research article tries to highlight, discuss a required transition roadmap and extend the local knowledge and practice on IPv6. Also, it introduces a prototype model using Packet tracer (network simulator) deployed for the design and implementation of IPv6 migration. Finally, it compares and evaluates the performance of IPv6, IPv4 and dual stack using OPNET based on QoS metrics such as throughput, delay and point to point utilizationas the key performance metrics for network with address allocation and router configuration supported by Open Shortest Path First (OSPF) routing protocol. In addition it compares dual-stack to the tunneling mechanism of IPv6 transition using OPNET. The results have shown that IPv6 network produces a higher in throughput, Response time and ethernet delay, but little difference in packet dropped, additionaly the result in TCP delay, Point to point utilization shows small values compared to dul-stack networks, The worst performance is noted when 6 to 4 tunneling is used, tunneling network produces a higher delay than other scenarios.

Keywords: IPv4, IPv6, IPv4 to IPv6 transition mechanism, OPNET, prototype simulation

INTRODUCTION

IPv6 is developed by the Internet Engineering Task Force (IETF) as the next-generation network layer protocol, overcoming the nagging problems in IPv4. IPv6 works more effective, secure, scalable and routable than IPv4 (Deering and Hinden, 1998). The primary reason for a new version of the Internet Standard protocol was going to improve the address space. IPv6 was designed with a 128bit address structure, enough to label every molecule on the surface of the earth with a unique address. Unlike IPv4, IPSec support has become a requirement in the IPv6 header. Payload identification for QoS handling by routers is currently maintaining the Flow Label field in the IPv6 packet header. Fragmentation support has recently been moved from routers to the sending hosts. The IPv6 header is not packed with a checksum and does not have any options included in the header, but instead introduces expansion headers. IPv6 requires no manual configuration or DHCP (Dynamic Host Configuration Protocol) that becomes important as the number of nodes increases (Saklani and Dimri, 2013). It has recently been widely believed that IPv6 is the most experienced and feasible solution for the next-generation Internet. To enable the transition between IPv4 and IPv6, IETF proposed three transition mechanisms to be able to run both 1IPv4 and IPv6 at exactly the same time. These are:

The 1Dual Stack Transition Mechanism (DSTM): Is one of the very most forthright means by which IPv4 and IPv6 can talk to each other. DSTM allows a client in the IPv6 network to talk to an IPv4 host. As the name indicates, dual stacking involves the implementation of stacks in both IPv4 and IPv6 clients. This implies the host can decide when an interconnection should be produced using IPv4 or IPv6 (Bi *et al*., 2007). Both hosts and routers must support dual stacks and become configured in parallel. When IPv4 communicates with IPv4, DSTM uses the IPv4 network, so when IPv6 communicates with IPv6, it uses IPv6. The advantages of the dual stack are; low cost and already supported in all devices and modern OSs. Easy to implement alternatively, the disadvantages of the dual stack are; two routing tables, Additional memory space and CPU power and two firewall sets of policies (Mulchandani *et al*., 2013).

The tunneling 1mechanism: Is an additional strategy that allows the transition of packages from IPv4 to IPv6. The concepts behind this tunneling are known as

Corresponding Author: Eman H. Khudhair, Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq

encapsulation and decapsulation. Encapsulation can be used when an IPv4 header transfers IPv6 packages from source to destination in an IPv4 network. On the other hand, de-capsulation maybe used when the IPv4/IPv6 router or host receives an IPv4 datagram that is addressed to one of its own IPv4 addresses or even to a multicast group address. Packets are confirmed by verifying their source and also destination addresses. There are different types of Tunneling Mechanisms: -6 to 4 Transition Mechanism, Static Tunneling,Teredo, (ISATAP) Intra-Site Automatic Tunnel Addressing Protocol (Mulchandani *et al*., 2013). The advantage of tunneling is; configure tunnel endpoints only, no additional management and simple deployment. Alternatively, the disadvantages of Tunneling are; take additional time and CPU power, creation of the tunnel could be expensive, the breakdown of the tunnel will certainly fail the network (Tatipamula *et al*., 2004).

Translation 1mechanisms: Translation mechanism refers the direct change of IP protocols; it always requires translators that could translate particular IPv4 address to particular IPv6 address.This makes a break in the end to end network as NAT. In this mechanism the router can be used as a translation communicator and also solve network interoperability problems. Over the other side, disadvantages of Translation are; limitations just like IPv4 NAT, slow to translate IP address and also harder to manage on a larger scale (Tatipamula *et al*., 2004).

LITERATURE REVIEW

In Tahir *et al*. (2006) Reviewed the execution of DSTM over their IPv6 test-bed (6Net) in University Utara Malaysia (UUM). Additionally, explain our experience of configuring 6Net. 6Net is the initial IPv6 test-bed in UUM as well as has become a platform for an IPv6 research study in UUM. In Govil *et al*. (2008) examined imperatives, different techniques and standards require for abnormal state similarity smooth transition and interoperation amongst IPv4 and IPv6 by removing the imperatives. In Che and Lewis (2010) investigated the purposes behind the slow rate of progress and additionally the debate, argument encompassing the interest for IPv6 technology. The issues, identifying with IPv4-to-IPv6 relocation, re-tended to, from where individual arrangements proposed alongside basic leadership roles.This study does not focus on IPv6's contribution to wireless and mobile networks; attention is placed on its deployment in the Internet backbone and enterprise networks. In Sumara *et al*. (2014) provided the very important theoretical principles of IPv6 which solve the problem of IP addressing and also give attention to IPv6 address format, routing and three mechanisms of migration to IPv6 network: Dual Stack, Tunneling and translation using network simulator (called Packet tracer). Also, it focused on network migration from IPv4 to IPv6 for seeable future trend. In Kalwar *et al*. (2015) introduced a survey with two fold. Firstly, to highlight the issues related to the move from IPv4 to IPv6. Also, to discover the move component that can be given flawlessly to end clients where they will have the capacity to utilize all the administrations of IPv4. Keeping in mind the end goal to accomplish the said destinations a reproduced test bed has been sent at Mehran University of Engineering and Technology (MUET), Jamshoro, Pakistan. The reason for existing is to handle the issues and difficulties that are prone to be confronted amid the move from IPv4 to IPv6. GNS3 and Wireshark are utilized for reproduction and DSTM has been picked as the move component for the proving ground. DSTM permit both conventions to run all the while and the outcomes demonstrate that it additionally gives consistent move from IPv4 to IPv6.

MATERIALS AND METHODS

In our prototype, the migration process to achieved through the following phases:

Planning forIPv6 deployment (roadmap): This phase discusses how to create a migration process. However, each network has its own specifications; therefore a specific migration plan must be created for each case. In some cases, the plan seems similar to the one proposed here, but in other cases may be requires some modifications depending on the type of the network and its requirements. The following explains these steps:

Survey of the 1prevailing network facilities (equipment): How about the devices in the organization and which equipment has to be upgraded or changed. An intensive inventory of the network can be an essential initial step to any type of network implementation planning. The network inventory includes all aspects that IPv6 will address (Main *et al*., 2015). Table 1 lists the affected components with a short description.

Cost: discusses and highlights the expense of migration from IPv4 to IPv6. Cost estimation of IPv6 transition can help IPv6 migration faster. The cost model may contain many components such as (Arifin *et al*., 2006):

- Network Software, Network Hardware and operating system costs.
- Training costs and unpredictable (Unstable) costs.

Security 1and knowledge plan: Participant listed the data that must be provided to the technological team. The IT staff training consists of major topics like the organizational benefits associated with IPv6, its technical requirements, safety and security considerations over IPv4 IPv4 to IPv6 transition mechanisms (Mudziwepasi and Scott, 2014), which can be:

Table 1: Affected components

Components	Description
Hardware	Every piece of equipment and software must support the new protocol. Many of the hardware pieces acquired over the years do not have IPv6 support, because when they were bought there was no knowledge about IPv6. So this equipment must be replaced without affecting the network's performance
IP Addressing	There must be an addressing plan for IPv6 just like in IPv4. However, the difference in the size of the addresses makes it unfeasible for some companies to create an addressing plan manually.
Routing protocols	All the major routing protocols have their version for IPv6 but with the changes made to the protocols, are the ones used still the best solutions
Security	Firewalls and Intrusion systems must support IPv6. The security of the network must be at least equal to the one for IPv4
Service and applications	All type of services and applications in the network must be upgraded or replaced if they do not have IPv6 support.

- Configuring (setting up) IPv6 1addressing
- 1Enable IPv6 routing and also configuring IPv6 on the 1safety and security appliance.

Methodology: There are basically two ways to deploy IPv6 (Mudziwepasi and Scott, 2014):

Core to Edge: IPv6 is applied first in the routers forming the central (core) of the network. Usually uses dual stack interfaces and progressively expands towards the edge of the network. The dual stack methodology has the advantage of implementing first where it is easiest, as most core routers software either already supports IPv6 or can support it with a simple upgrade.

Edge to core: IPv6 is implemented first at the edge of the network and then expanded toward the central (core).

Identify transition 1mechanism: Because IPv6 and IPv4 address types are different (Yousafzai *et al*., 2015), we should permit the two protocols to talk to each other using one of the IETF transition mechanisms described in below Section.

Test-bed network 1and final implementation: The IT department should create a platform to test a scenario as close to the real one as possible using network simulation or part of the real network. This step is essential because a migration plan is much more reliable if it is based on a carefully defined test-bed. The test-bed and the migration plan may be elaborated together, this way it is possible to realize almost immediately if the recommendations written are viable or should be replaced.

Configrations and performance evaluation: The configuration and performance evaluation of the prototype (IPv6 transition) passes through two phases; in phase I two experiments are applied (Dual stack, Native IPv6) using Packet Tracer for the prototype validation. Dual-stack (IPv6/IPv4) remains the accepted industry direction for the introduction of IPv6. Our proposed strategy for IPv6 deployment follows the dual-stack approach, allowing both IPv4 and IPv6 addresses to co-exist until the transition to native IPv6 can achieve complete. This approach makes sure that the transition occurs with minimal impact on customers. The use of dual stack ensure our customers have the current functionality of IPv4 always available to them even while they start deploying IPv6 in their systems. The transition from IPv4 to IPv6 is a known issue which the industry will have to manage over the coming years. The transition takes time as it will require IPv6 support by an industry end-to-end eco-system, including CPE, modems/home gateways, networks, systems (OSS/BSS, tools), content and applications. Figure 1 shows the Dual-stack supports both protocols in parallel within one network. While during Phase II two experiments are applied in OPNET to measure and compare the performance of IPv6, IPv4, dual-stack and 6to4 Tunneling networks, according to QoS parameters (point to point utilization, throughput, Response time, Packet dropped and delay).

Experiment 1: (Dual-stack): This experiment introduces a prototype configuration and implementation of Dual Stack transition mechanism using packet tracer (version 6.3). The used topology shown in Fig. 2. The network topology composes three routers 2811, eight generic switches and clients (six computers, three laptops and four servers) configured in the simulator.

Dual stack IP address scheme:

Dual stack configuration: For example, R1 router configured using an IP address scheme of Table 2 as follows:

R1 (config) # interface fast ethernet 0/0
R1 (config-if) # IP address 192.168.2.1 2551.255.255.0
R1 (config-if) # ipv6 address 2000:8::8/64
R1 (config-if) #no shutdown
R1 (config) # interface fastet1hernet0/1
R1 (config-if) # IP address1 192.168.4.1 255.255.255.0
R1 (config-if) # ipv6 address 2000:9::9/64
R1 (config-if) #no 1shutdown
R1 (config) #interface serial 1/0
R1 (config-if) # IP address 192.168.1.2 255. 1255.255.0
R1 (config-if) #ipv6 address 12001::40/64
R1 (config-if) #no shutdown
Enable OSPF for IPv4 as follows:
R1(config)#router 1ospf process--id
R1(config-router)# network 192.168.2.1 1area 0

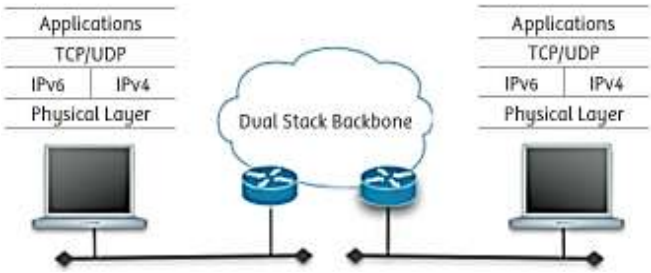

Fig. 1: Dual-stack supports both protocols in parallel

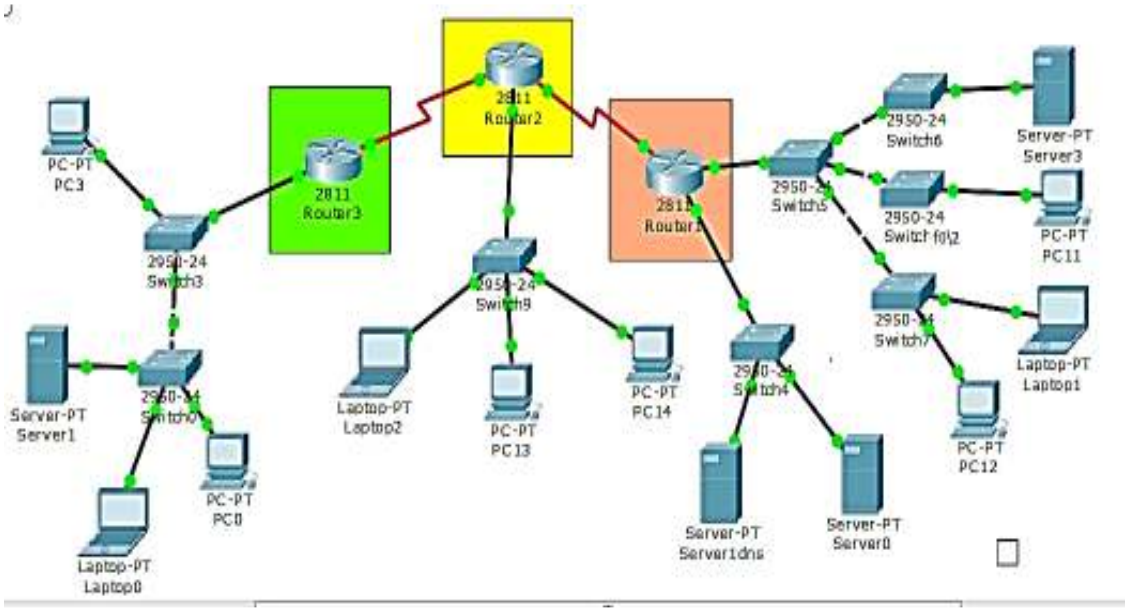

Fig. 2: The network topology

Table 2: Dual stack IP address

Router	Interface	IPv4Address	IPv6 Address
R1	F 0/0	192.168.2.1	2000:8::8/64
	F 0/1	192.168.4.1	2000:9::9/64
	S 1/0	192.168.1.2	2001::40/64
R2	F 0/0	192.168.10.1	2000:7::7/64
	S 1/0	192.168.1.1	2001::50/64
	S 1/1	192.168.6.1	2001:2::40/64
R3	F 0/0	192.168.12.1	2000:6::6/64
	S 1/0	192.168.6.2	2001:2::30

R1(config-router)# network 192.168.4.1 1area 0
R1(config-router)# network 192.168.1.2 1area 0
Enable OSPF for IPv6 as follows:
R1(config)# ipv6 unicast--1routing
R1(config) # ipv6 router 1ospf 1
R1(config-rtr) # router--1id 1.1.1.1
R1(config-rtr) # exi
R1(config)# interface fastethernet0/0
R1(config-router)#ipv61address 2000:8::8/64
R1(config)# interface fastethernet0/1
R1(config-router)#ipv61address 2000:9::/64
R1(config)# interface serial 1/0
R1(config-router)#ipv61address 2001::40/64
R1(config-router)#ipv61ospf 1 area 0

Similar to R1configuration, suitable IPs and OSPF configured for R2 and R3.

Figure 3 and 4 shows the verification using "ping" command, in this validation of the link tests we didn't get any destination unreachable echo request

Experiment 2: (Native IPv6): In this experiment, the implementation of Native IPv6 network using Packet Tracer (version 16.3) is discussed. The topology used is shown in Fig. 2.

Native IPv6 Address1Scheme:

Configuration: The IPv6 configuration steps for router R1based on the IP address scheme (Table 3) looks like:
For example, R1 router configured using IPv6 address scheme appears in Table 3 as follows:
R1(config)# interface fastethernet0/0
R1(config-if)# ipv6 address 2000:8::8/64
R1(config-if)#no shutdown
R1(config)# interface fastethernet0/1
R1(config-if)# ipv6 address 12000:9::9/64
R1(config-if)#no shutdown
R1(config)#interface serial 1/0

IOS Command Line Interface

```
Router>
Router>en
Router#pi
Router#ping 2001::50

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::50, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms

Router#ping 2000:8::8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2000:8::8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/17/51 ms

Router#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/11 ms

Router#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/9/20 ms

Router#
```

Fig. 3: Router to router communication result

Command Prompt

```
    Minimum = 1ms, Maximum = 22ms, Average = 9ms

PC>ping 192.168.12.3

Pinging 192.168.12.3 with 32 bytes of data:

Reply from 192.168.12.3: bytes=32 time=2ms TTL=126
Reply from 192.168.12.3: bytes=32 time=1ms TTL=126
Reply from 192.168.12.3: bytes=32 time=2ms TTL=126
Reply from 192.168.12.3: bytes=32 time=3ms TTL=126

Ping statistics for 192.168.12.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 2ms

PC>ping 2000:6::9

Pinging 2000:6::9 with 32 bytes of data:

Reply from 2000:6::9: bytes=32 time=2ms TTL=126
Reply from 2000:6::9: bytes=32 time=1ms TTL=126
Reply from 2000:6::9: bytes=32 time=12ms TTL=126
Reply from 2000:6::9: bytes=32 time=1ms TTL=126

Ping statistics for 2000:6::9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 12ms, Average = 4ms

PC>
```

Fig. 4: Client communication result

R1(config-if)#ipv6 address1 2001::40/64
R1(config-if)#no shutdown

IP Routing (OSPF) 1Configuration: OSPFv3 enabled in IPv6 network for router R1. The configuration steps are similar to the described steps of Experiment 1 (Dual-stack) But

- Similar to R1 configuration, 1suitable IPs and OSPFv3 1configured for R2 and R3.

RESULTS AND VERIFICATION

Figure 5 and 6 shows the verification using "ping" command, Pings is successful and connections are established. In this validation of the link tests we didn't get any destination unreachable echo request.

Experiment 3: Performance 1evaluation using OPNET: The network topology configured using three scenarios; IPv4, IPv6 and Dual Stack.Each of them modeled using OPNET.The total runtime for every scenario is 60 minutes.The used topology of the three scenarios is shown in Fig. 7. It composes eight work stations, two servers, two gateway routers, two switches, Ethernet 100baseT and PPP_DS3 communication links between routers established. Voice and Email are two modeled applications activated during each tested scenario. And further more enable IP Routing (OSPF) Configuration; OSPF enabled in IPv4 network, OSPFv3 enabled in IPv6 network and in Dual-Stack permit both of them. Individual simulation run employed for the sake of comparison and performance evaluation.

The following QoS metrics used in our performance evaluation:

Throughput: Is defined as the average date packet transferred through a network and is usually measured in bits per second (bits/Sec) (Shah and Parvez, 2014).

Table 3: Native IPv6 address

Router	Interface	IPv6 Address
R1	F 0/0	2000:8::8/64
	F 0/1	2000:9::9/64
	S 1/0	2001::40/64
R2	F 0/0	2000:7::7/64
	S 1/0	2001::50/64
	S 1/1	2001:2::40/64
R3	F 0/0	2000:6::6/64
	S 1/0	2001:2::30

Fig. 5: Router to router result (IPV6)

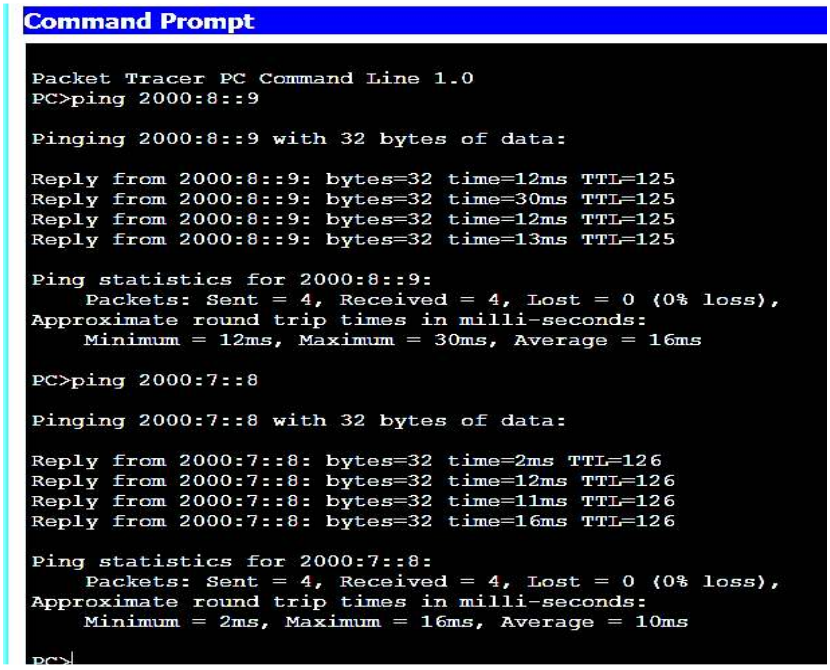

Fig. 6: Client communication result (IPV6)

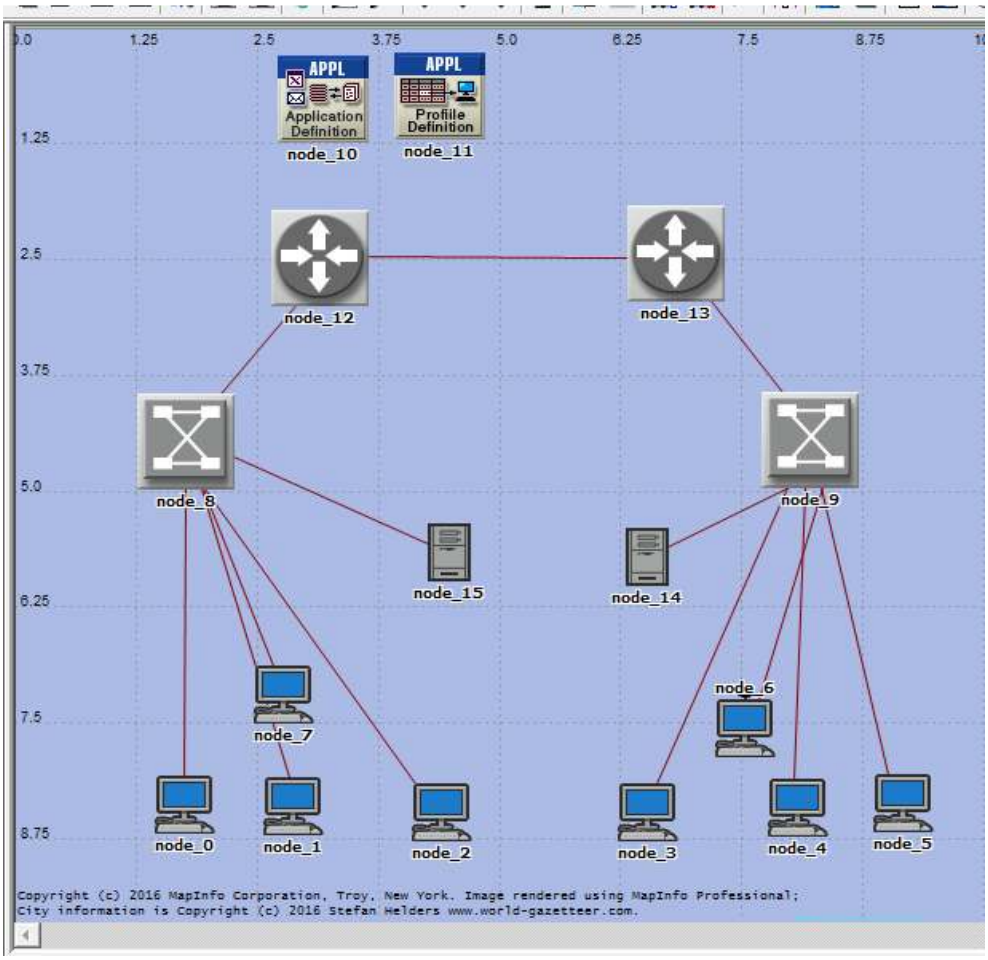

Fig. 7: Network topology using OPNET

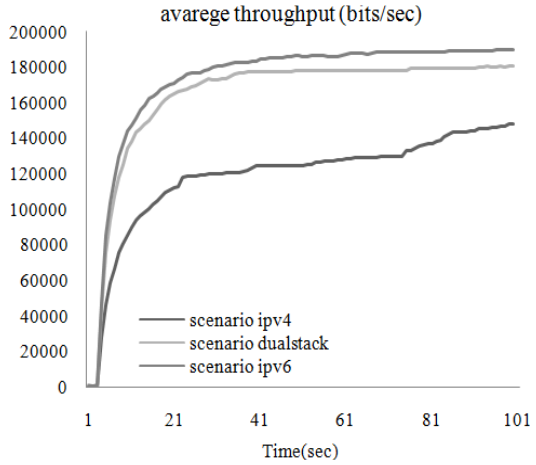

Fig. 8: Traffic throughput (IPv4, Dual stack, IPv6)

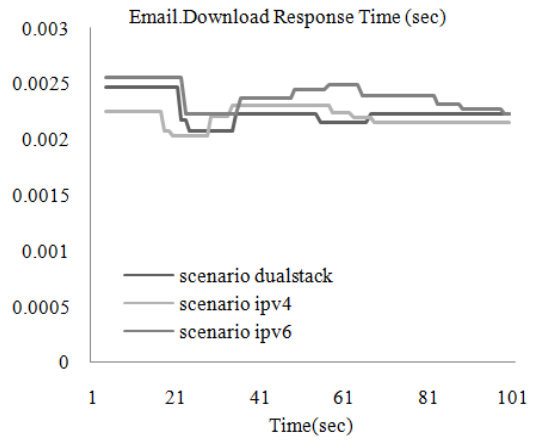

Fig. 9: Response time (IPv4, Dual stack, IPv6)

Figure 8 shows Throughput evaluation among IPv6, IPv4 and dual-stack. IPv6 has high throughput compared to other two cases.

The application 1Response time:represent elapsed time 1between sending a request and receiving the response packet for the application. Figure 9 shows the Email download response time. The IPv6 has higher response time than dual stack and IPv4 scenarios.

Ethernet delay: Represents an end to end delay of all data packets received by all the stations. Figure 10 shows a comparison of average Ethernet delay. The notice is that IPv4 has a greater delay than both Dual stack and IPv6. On the routing level, IPv6 always add the time to transfer the extra 128-160 bits to each hop in the network compared to IPv4.

TCP delay 1(in seconds): Suffered by the TCP layers represents the delay of data packets in the complete network and measured from the time the source TCP layer sends an application data packet to the time that's received by the TCP layer at the destination node (Shah

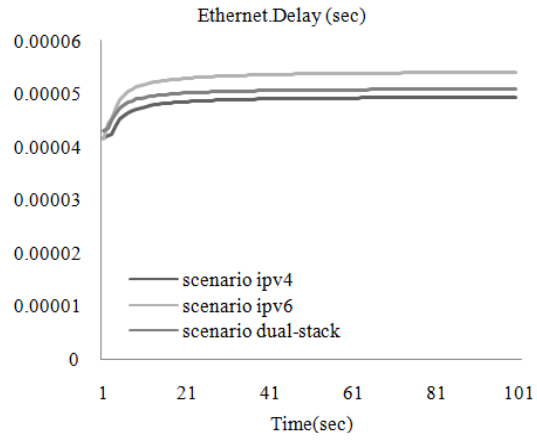

Fig. 10: Traffic ethernet delay (IPv4, Dual stack and IPv6)

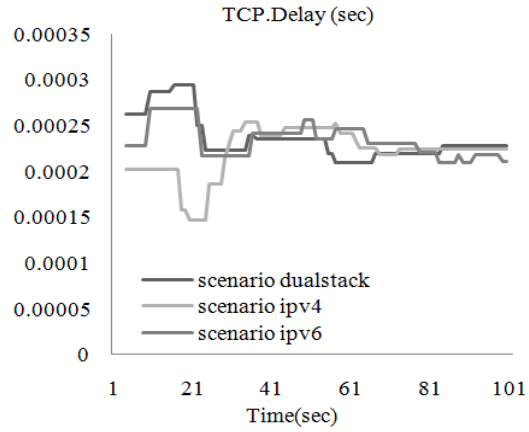

Fig. 11: TCP delay (IPv4, Dual stack and IPv6)

and Parvez, 2014). Figure 11 represents a plot of TCP delay against time for the dual-stack, IPv6 and IPv4. In the tested WAN network, TCP delay suffered by IPv4 was quite low as compared with dual stack and IPv6 network.

Point to point 1utilization: represents the percentage of a link's bandwidth that is being consumed by network traffic. Figure 12 shows the evaluation of utilization.

Packet drop or loss: Takes place when one or more packets traveling on a network fail to reach the destination due to overwhelmig and cannot allow extra packets at that time. Due to packet drop, the destination has to inform the sender to re-send the dropped packet and this adds to the traffic and may cause network congestion. Figure 13 shows a comparison among IPv4, Dual stack and IPv6 network in terms of average packet dropped. They are compattive as behavior.

Table 4 summarizes the average value per Scenario based on throughput, Ethernet delay and TCP delay, Point to point utilization, Response time and Packet dropped. The results have shown that IPv6 network

Table 4: Average values of simulation

Scenarios materials	IPv4	Dual stack	IPv6
Throughput (bits/sec)	149081	165535	168409
Ethernet delay (ms)	0.0482	0.0512	0.0520
TCP delay(ms)	0.2202	0.2362	0.2337
Point to point utilization	0.1468	0.1674	0.1671
Response time	0.002200	0.002243	0.002389
Packet drop	0.2343	0.23822	0.23823

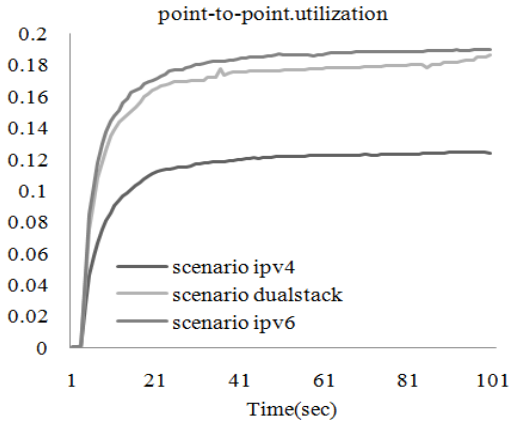

Fig. 12: Point to point utilization (IPv4, Dual stack, IPv6)

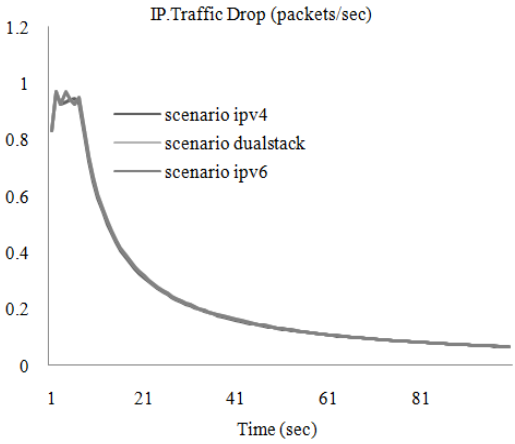

Fig. 13: Packet dropped (IPv4, Dual stack, IPv6)

produces a higher in throughput, Response time and ethernet delay, but little difference in packet dropped, additionaly the result in TCP delay, Point to point utilization shows small values compared to dul-stack networks due to the some reasons such as IPv6 have been designed for faster packet processing and larger packet size. This enables it to transfer more data beside better forwarding capability than IPv6 transitioning networks. It affects the throughput positively. Packet fragmentation process performed in IPv6 by the host only makes its performance better. The large IPv6 header size (40 bytes for IPv6 vs. 20 bytes for IPv4) contributes in packets delay difference. Hence, the implementation of IPv6 introduces concerns which are related to expanded packet headers.

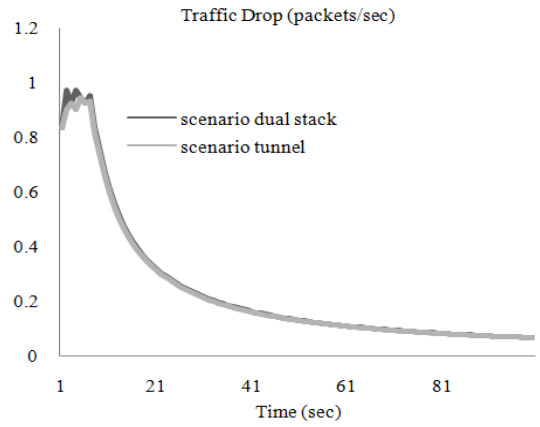

Fig. 14: Traffic drop (6 to 4 tunneling, dual stack)

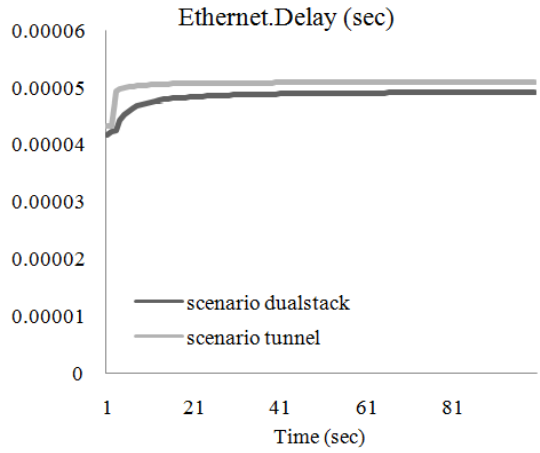

Fig. 15: Ethernet delay (6 to 4 tunneling, dual stack)

Experiment 4: It compares and evaluates the network topology (Fig. 7) using dual stack and 6to4 tunnel based on QoS parameters such as traffic drop, ethernet delay, response timeand throughput using Email and voice. Figure 14 to 17 depict the comparison results.

The average of each calculated value is shown in Table 5 for simplification. Analyzing Table 5, notice that 6 to 4 Tunneling yields lower throughput and less packet drop, but higher delay than the dual stack. This is obvious due to presence of two protocols in the dual stack and encapsulation/decapsulation delays when tunneling is used.

CONCLUSION

Current paper focused on Transition to IPv6 mechanisms. Dual Stack is the easiest and most suitable

Table 5: Average values of simulation in Exp4

Scenario materials	6to4 tunneling	Dual stack
Packet dropped	0.23304	0.23822
Ethernet delay	0.0566	0.0512
Response time	0.002276	0.002243
Throughput	127168	165535

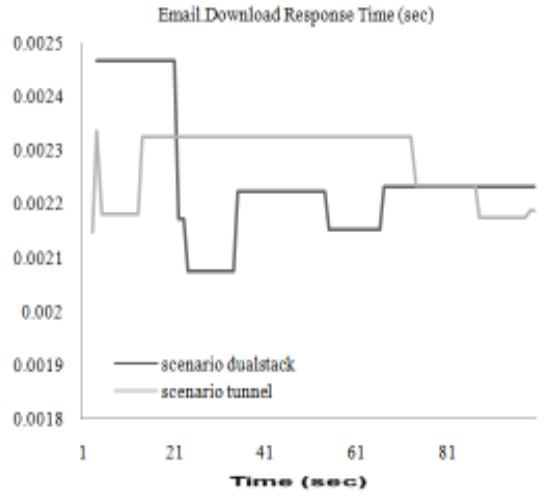

Fig. 16: Response time (6 to 4 tunneling, dual stack)

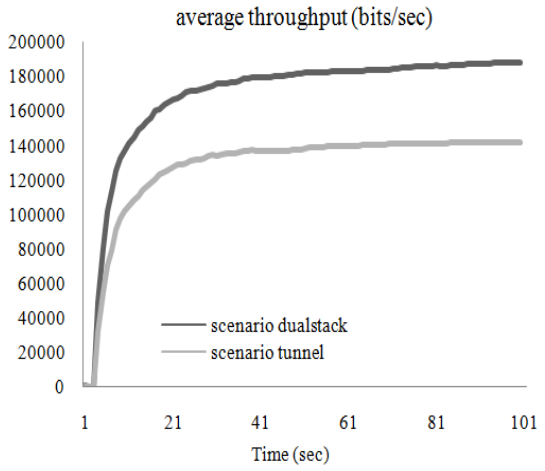

Fig. 17: Traffic throughput (6 to 4 tunneling, dual stack)

method for IPv4 and IPv6 to coexist and most probably to be the next phase in a network's evolution. It introduced a prototype, configuration and implementation of dual Stack and native IPv6 network using Packet Tracer. The paper also demonstrated three scenarios implemented, tested and evaluated according to QoS metrics (IPv4, Dual-Stack and native IPv6 using OPNET. The statistics obtained from simulation shows that the performance of native IPv6 (utilization) is much better than other scenarios. Further more IPv6 has faster packet processing and forwarding capability than transitioning networks. Using TCP, the Dual Stack delay appears more than TCP delay using native IPv6 due to the presence of two protocols. The worst performance is noted when 6 to 4 tunneling is used, tunneling network produces a higher delay than other scenarios due to increased processing time and tunneling overhead. This study also introduced roadmap guidelines for IPv6 transition.

REFERENCES

Arifin, A.H., D. Abdullah, S.M. Berhan and R. Budiarto, 2006. An economical IPv4-to-IPv6 transition model: A case study for university network. Int. J. Comput. Sci. Netw. Secur., 6(11): 170-178.

Bi, J., J. Wu and X. Leng, 2007. IPv4/IPv6 transition technologies and univer6 architecture. Int. J. Comput. Sci. Netw. Secur., 7(1): 232-243.

Che, X. and D. Lewis, 2010. Ipv6: Current deployment and migration status. Int. J. Res. Rev. Comput. Sci., 1(2): 22-29.

Deering, S. and R. Hinden, 1998. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460 (Draft Standard), Internet Engineering Task Force,<draft-ietf-ipngwg-ipv6-spec-v2-01.txt>Updated by RFCs 5095, 5722, 5871, 6437, 6564.

Govil, J., J. Govil, N. Kaur and H. Kaur, 2008. An examination of IPv4 and IPv6 networks: Constraints and various transition mechanisms. Proceeding of the IEEE Southeastcon, pp: 178-185.

Kalwar, S., N. Bohra and A.A. Memon, 2015. A survey of transition mechanisms from IPv4 to IPv6 — Simulated test bed and analysis. Proceeding of the 3rd International Conference on IEEE Digital Information, Networking and Wireless Communications (DINWC), pp: 30-34.

Main, A., N.A. Zakaria and R. Yusof, 2015. Organisation readiness factors towards IPv6 migration: Expert review. Proc. Soc. Behav. Sci., 195: 1882-1889.

Mudziwepasi, S.K. and S.M. Scott, 2014. Exploring technical deployments of IPv6 on university LANs. Int. J. Comput. Sci. Issue., 11(1(2): 187-193.

Mulchandani, C., K. Mistry, P. Chawan and A. Shetty, 2013. Transition from IPV4 to IPV6. Int. J. Electron. Commun. Eng. Technol., 4: 169-176.

Saklani, A. and S.C. Dimri, 2013. Technical comparison between IPv4 & IPv6 and migration from IPv4 to IPv6. Int. J. Sci. Res., 2(7): 52-55.

Shah, J.L. and J. Parvez, 2014. An examination of next generation IP migration techniques: Constraints and evaluation. Proceeding of the International Conference on IEEE Control, Instrumentation, Communication and Computational Technologies (ICCICCT), pp: 776-781.

Sumara, S.K., A.B. Bavarva and S.A.V. Shrivastava, 2014. Design concept and simulation of migration from present IPv4 network to future IPv6 network using three transition mechanisms. Int. J. Eng. Res. Technol., 3(4): 1396-1400.

Tahir, H.M., A. Taa and N.B.M. Nasir, 2006. Implementation of IPv4 over IPv6 using dual stack transition mechanism (DSTM) on 6iNet. Proceeding of the IEEE 2nd International Conference on Information and Communication Technologies, 2: 3156-3162.

Tatipamula, M., P. Grossetete and H. Esaki, 2004. IPv6 integration and coexistence strategies for next-generation networks. IEEE Commun. Mag., 42(1): 88-96.

Yousafzai, M.M., N.E. Othman and R. Hassan, 2015. Toward IPv4 to IPv6 migration within a campus network. J. Theor. Appl. Inform. Technol., 77(2): 209-217.