Bulletin of Electrical Engineering and Informatics
Vol. 9, No. 3, June 2020, pp. 1167~1175
ISSN: 2302-9285, DOI: 10.11591/eei.v9i3.2173

IPv6 campus transition: A Central Luzon State University case study

Marlon A. Naagas[1], Nemesio A. Macabale Jr[2], Thelma D. Palaoag[3]
[1,2]Central Luzon State University, Philippines
[3]University of the Cordilleras, Philippines

Article Info

Article history:

Received Oct 30, 2019
Revised Jan 7, 2020
Accepted Feb 21, 2020

Keywords:

IPv6
IPv6 campus model
IPv6 campus transition
IPv6 dual-stack model
IPv6 transition

ABSTRACT

Internet connections still use IPv4 as the primary address protocol and it is now facing exhaustion. However, academic institutions specifically in the Philippines should devise steps to address the exhaustion of IPv4. In this paper, this is brought to light as we present the IPv4 to IPv6 campus transition techniques to address the issue. The experiment is carried out in Central Luzon State University and is assessed if the university is able to adopt the IPv6 transition in their campus network. Two IPv6 transition mechanisms were implemented and tested. As a general result, it has been found out, through testbeds, that the dual-stack transition mechanism is more suitable than 6 to 4 tunnel broker. The results have also shown that 6 to 4 tunnel broker was outperformed by dual-stack transition mechanism in all areas and presents better performance. Additionally, results also showed that IPv4 presents slight advantages in terms of network performance than IPv6 with a very small percentage in difference, and this does mean that migration to IPv6 is possible without performance detriments. Furthermore, the results also provide a proof of concept for the university especially in the Philippines to consider IPv6 for future migration within their campus network.

Corresponding Author:

Marlon A. Naagas,
Central Luzon State University,
Science City of Munoz, NE, Philippines.
Email: manaagas@clsu.edu.ph

1. INTRODUCTION

The internet community was threatened by the fundamental resource scarcity issue of IPv4. Four out of five (APNIC, RIPE, LACNIC, ARIN) of the regional internet registries (RIRs) have run out of freely available IPv4 address space. The forecast of likely exhaustion dates for each RIR: ARIN reached IPv4 address exhaustion since 24 Sep-2015. The other pool depletion projections by other RIR: AFRINIC late-2019, LACNIC late-2019, RIPE NCC mid-2020 and APNIC by mid-2021 [1]. As a result, the internet engineering task force (IETF) developed IPv6 (internet protocol version 6) to address these limitations, along with several protocol improvements like network performances, ease-of-configuration, address length and network management issues [2].

Asia Pacific Network Information Center (APNIC) conducted a stakeholder's internet forum in the Philippines last 2014 [3]. The forum addressed the issues that the Internet industry in the Asia Pacific is at a critical point. It also stated that internet addresses using IPv4 has begun to run out, technology investors and stakeholders in the Philippines and the Asia Pacific are being urged to start their transition from IPv4 to IPv6 in order to maintain a scalable Internet for the region. The Philippines was in 55th place during

that time, but in the latest survey, the Philippines was placed 133rd in the recent world rankings of IPv6 users per country [4], and in google measurement, approximately 2.7% of the population uses IPv6 [5]. However, in the APNIC measurement, the Philippines scored 3.14% as IPv6 Capable and 3.05% prepared as of December 2019 [4]. As a solution, the Philippine government issued E.O. No. 893 that encourages the migration to IPv6 but was not taken seriously up until today. There's still no IPv4 and IPv6 transition mechanism framework established in the Philippines. The government has issued an executive order only to encourage but not force implementation.

The internet has become an important component in the academic institutions because of the vital role it plays in the gathering of information as well as means of communication. From anywhere in the world, the internet has made it possible to access wide range of information, such as research, journal article, papers, etc. It enables researchers, faculty, and students in this institution to spread learned facts to a wider audience around the globe [6]. Adopting the IPv6 protocol maintains competitiveness, interoperability, and growth that universities must become proactive in adopting this protocol. Most of the top universities in the world have taken steps in implementing IPv6 in their campus network operations. However, IPv6 is being adopted at a very slow pace in the Philippines because even major internet service providers (ISPs) doesn't provide IPv6 internet connectivity in their services. UP Diliman is one of the firsts to implement full-IPv6 connectivity from its core services down to its clients. This is the only university that participated in the IPv6 world launch day that was held in 2008 [7]. One question to ask, is Central Luzon State University next to UP Diliman in terms of IPv6 campus connectivity?

This study aims to answer the question by implementing suitable IPv6 transition mechanisms based on existing university network specifications of Central Luzon State University (CLSU). This study will have a huge contribution in the IPv6 community especially in the academic sectors in the Philippines once it is fully implemented. This study will enable other State Universities and Colleges (SUC) to follow the track of UP Diliman and CLSU and for them to also consider future migration to IPv6 within their campus network operation.

2. CAMPUS IPv6 TRANSITION TECHNIQUES

Many IPv6 transition techniques have been proposed by the IETF. T. Chown of the University of Southampton proposed an IPv6 campus transition technique [8] that considers and analyzes the specific scenario of IPv6 transition and implementation in a large department of a university campus network. Transition to IPv6 campus cannot be implemented overnight. Proper planning and design are needed before commencing the implementation phase. The transition process should be performed phase by phase due to operating costs, utilities and changing factors that should be considered by an organization before initiating the transition process [9]. Hence, the choice of appropriate IPv6 transition mechanisms can make sure that the transition process goes smoothly. Proper testing procedures are the fundamental requirement in order to test the IPv6 transition mechanism before implementing in the actual network [10].

IETF released RFC 4057 in 2005. The RFC defines the scenarios in deploying IPv6 in enterprise networks. This RFC is beneficial to the network administration team to know the IPv6 transition strategy used within the enterprise network. These IPv6 transition "scenarios" will also be described in this document. It is stated in this document that it is impossible to define every possible enterprise scenario that will be applied to IPv6 adoption and transition. It is appropriate for an organization or enterprise to select the best technique that is suitable to support their network requirements. It is also mentioned in the document that any attempt to define a default or a one-size-fits-all scenario simply won't work [11].

- Dual-stack: The primary technique for transitioning to IPv6 is the dual-stack approach. This migration technique provides complete support for running both Internet Protocols IPv4 and IPv6 at the same time in both hosts and routers. The Nodes support both protocol stacks (IPv4 and IPv6) that work in parallel and allow the end device or router to operate via either protocol.
- Tunneling: Another transitioning technique for IPv6. It allows the movement of a packet from network to another different network. It involves allowing the IPv6 network to be sent across an IPv4 network through encapsulation. This technique encapsulates an IPv6 packet into an IPv4 packet so that it can be delivered over IPv4-only networks [12]. Different types of Tunneling strategies have been developed and it can be configured manually or automatically such as IPinIP, GRE, 6to4, Teredo, ISATAP, 6rd, MPLS and others. However, this study only discussed 6 to 4 Tunnel Broker because it is more suitable for rapid deployment where an IPv6 is not supported by an ISP in their location.
- Translation: Network address translation (NAT) is an old method in IPv4, it refers to the translation of an IP address from public address into private address space. IPv6 also uses the same translation technique as defined in RFC 2765 and RFC 2766 which is the network address translation-port translation (NAT-PT) and is now substituted by NAT64. However, many benefits to network address translation

(NAT) has been identified, but the primary benefit of this technique is only to "amplify" available address space which is not needed in the IPv6 environment. IPv6 was designed to make NAT unnecessary [13-15].

3. CAMPUS NETWORK SET-UP AND TRANSITION IMPLEMENTATION

This study adopts "Scenario 1" of the IPv6 enterprise network scenarios [11] of RFC 4057, where the IPv6 network is to be deployed in parallel with the existing IPv4 network. We ensure that the university's existing IPv4 network infrastructure is not interrupted during the implementation stage and IPv6 has an equivalent or better than the IPv4 network infrastructure. We also deployed IPv6 pervasively in the wired and wireless networks of the university. This new network will become an enabler for the faculty, developer and researchers to encourage them to experience and develop new applications that focuses on IPv6.

The network performance testing focused on two important statistics: First, TCP throughput measurement. Second, UDP connection-UDP throughput, jitter, and packet loss. Packet loss is defined as the time it takes for a packet to traverse between two hosts on a network. Jitter is the difference or change in the delay over time. Jitter calculations are continuously computed by the server, as specified by RTP in RFC 1889 [16-17]. Each of these statistics is important in measuring the performance of computer networks and will be analyzed for both IPv4 and IPv6 transition mechanisms.

3.1. Campus preparation and network specification

The existing network of CLSU is consisted of an IPv4 network with around 20 subnets and the current network design is using internetwork or a hierarchical network model that combines edge-core router down to the core to access switches' functionality in central devices. The main routing and switching equipment are all IPv6 and VLAN capable. The main site deployed IPv6 dual-stack to support its users along with its teaching and research needs. The goal is for IPv6 to enable the network using wired and wireless such that the whole operation is dual-stack. Tunneling using 6 to 4 Tunnel Broker is also tested and implemented, this technique applies to the University that doesn't have an IPv6 internet connection due to lack of IPv6 capability of the internet service provider (ISP) in the Philippines.

Philippine Research, Education, and Government Information Network or PREGINET is the primary internet service provider (ISP) of CLSU, allocated /127 IPv6 prefix and/30 for IPv4 point to point link for the WAN connection, see Figure 1. Also, PREGINET provides a routed IPv6 /56 prefix for the university LAN. The university offers a /64 prefix and makes its prefix allocations for every subnet in the university. Using /56 prefix there are 256/64 subnets allotted to the university to play with. The implemented IPv6 addressing plan for the university is Dual-Stack migration in which IPv4 and IPv6 network co-existed.

3.2. Design and implementation of network topology

3.2.1. Multi-layer dual-stack model

Multi-layer dual-stack model is the primary model in our campus design. This model combines the multi-layer architecture to a dual-stack IPv6 transition model. The multi-layer model is a useful high-level model for designing reliable network infrastructure and it breaks the complex problem of network design into smaller and more manageable areas [18, 19]. Core layer: Referred to as the network backbone and it provides connectivity to the university distribution and access layer for the local area network connectivity. It also provides fast transport between distribution switches within the university local area network. Distribution layer: serves as the communication point between the access layer and the core. Access layer: Provides end-users access to the network. Figure 1 shows the dual-stack campus model.

In addition, most of the current IPv4 migration for internal networks use a private IPv4 address space for local area network (LAN) devices and network access translation (NAT) at the edge router to translate a private address to a globally routable public IPv4 address. This is a common transition for most local area network implementation and is partly responsible for having IPv4 public addresses alive until this year. However, there are a lot of complications and problems with address translation (NAT), but IPv6 uses a different technique and eliminates these problems and complications. One of the new methods IPv6 uses is DHCPv6 with the prefix delegation option (sometimes referred to as DHCPv6-PD or DHCPv6 prefix delegation), which provides a mechanism for automated delegation of a globally routable IPv6 prefix from a provider's router to a customer's premises router using DHCPv6. DHCPv6-PD was described in RFC 3633 [20].

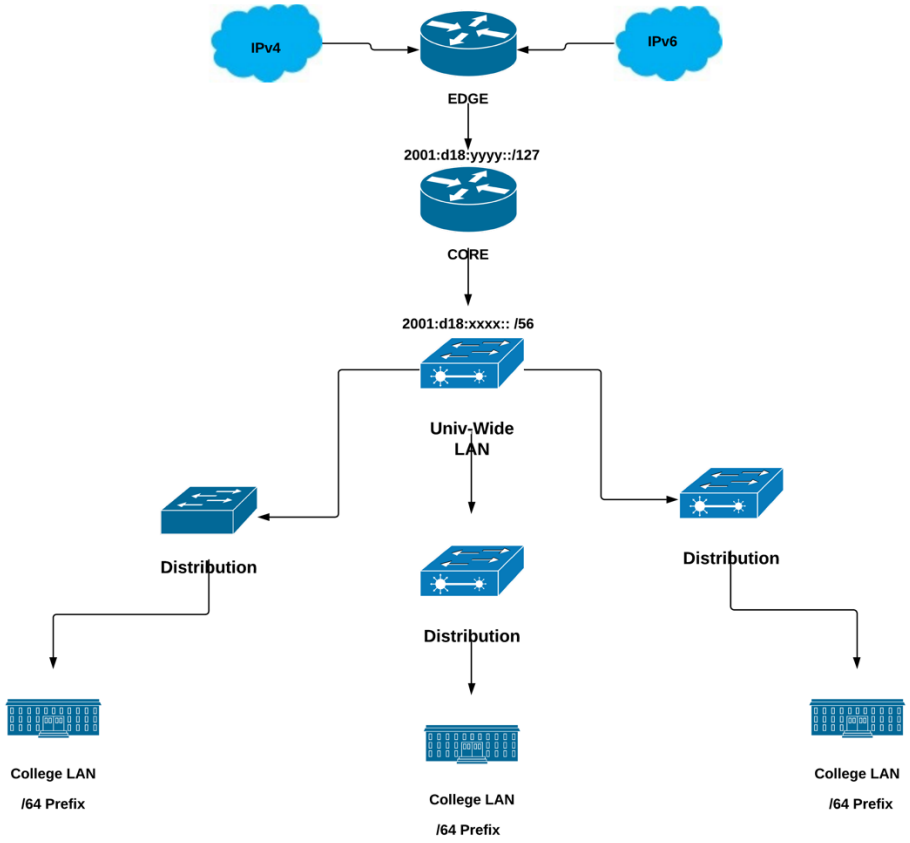

Figure 1. Multi-layer IPv6 campus DUAL-STACK model

Our model adopts these concepts and as shown in Figures 1 and 2, there are two routers involved in this design: Core Router, this is the router that acts as the DHCPv6 client, requesting the prefix(es) to be assigned. Edge router, this is the router that acts as the DHCPv6 server, responding to the requesting router's IPv6 prefix request. The DHCPv6 message exchange between the core router and edge router. Although this is similar to a state full DHCPv6 message exchange, you can see the differences in the SOLICIT and REPLY messages, see Figure 2.

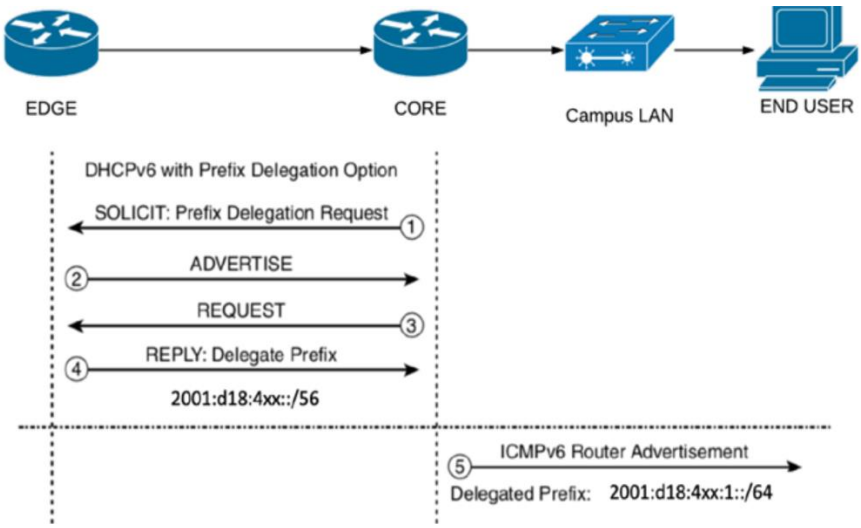

Figure 2. DHCPv6 with prefix delegation migration

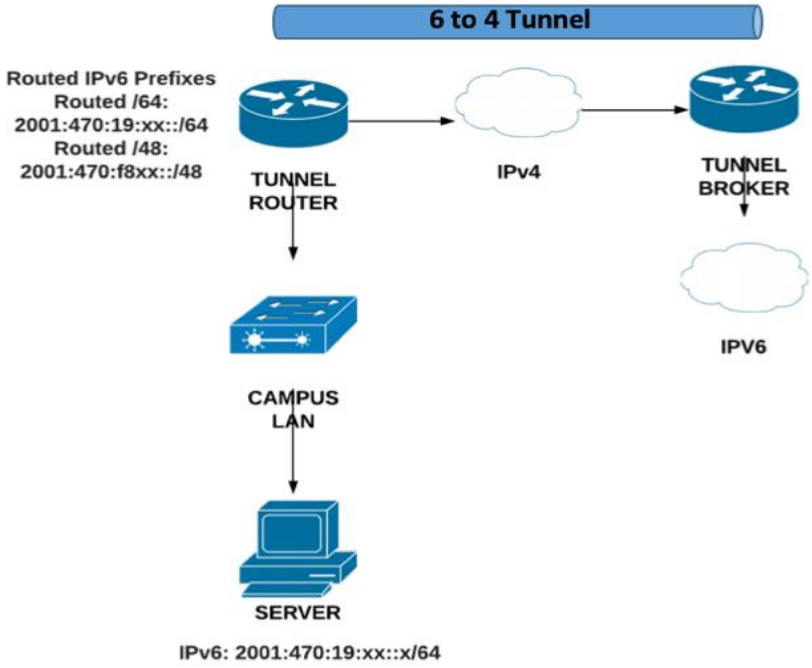

Figure 3. IPv6 campus tunnel model

3.2.2. 6 to 4 tunnel broker

Hurricane electric (HE.net or HE) Tunnel Broker is the main tunneling migration technique we used. This technique enables to reach the IPv6 internet by tunneling over existing IPv4 connections from IPv6 enabled host and will provide you a routed IPv6 space with a prefix of /48 or /64 free in charge [21]. The design goal of 6 to 4 tunnel broker is to give an idea to our fellow state universities and colleges (SUC) that it is possible to implement or deploy an IPv6 network even without native IPv6 internet connectivity in their location especially in the Philippines where major ISPs doesn't offer IPv6 in their major services. Figure 3 shows the network topology for 6 to 4 tunneling using a router enabled tunnel broker.

4. EVALUATION AND ANALYSIS OF RESULTS

Several testing were done to evaluate network performance. IPERF was the primary network throughput testing tool used in this study. To perform the TCP network stress testing, different sets of testing parameters were used, and this includes the combination of both windows size [22], parallel streams with a payload of 512MB sent to the server. This test generates 10 streams instead of the default of 1 and it also sends TCP payload of 512MB for 180 seconds. This duly noted that while increasing the number of streams may improve your overall throughput, there is a point of diminishing returns [23]. However, the same parameters were set in UDP performance testing except for windows size, in addition, the rate of speed with which the data is transferred was set to 100Mbps. TCP and UDP functions differently, TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent whereas UDP doesn’t guarantee the delivery of the data but with has the advantage of being faster than TCP.

Table 1 and Figure 4 presents a summary of the TCP throughput measurement result. The result shows that the dual-stack on both LAN and WAN migration is much better in all areas against 6 to 4 tunnel broker. In the dual-stack performance testing (LAN), IPv4 has a slight advantage against IPv6 in terms of time, transfer and bandwidth utilization [24]. 5120 Mbytes of the payload were sent in the maximum bandwidth of 346 Mbits/Seconds within 124 seconds. However, 5120 Mbytes of the payload were also transmitted in the maximum bandwidth of 339 Mbits/Seconds within 126 seconds of transmission time for IPv6. The IPv6 is 2 seconds slower than the IPv4 protocol in the Local Area Network environment. However, in the WAN (online) environment IPv4/IPv6 dual-stack and 6 to 4 tunnel were also evaluated. IPv4 also has a slight advantage in all areas versus IPv6 and 6 to 4 tunnel broker. As a result, both payloads were delivered within 180-181.9 seconds but the server only received 346 (IPv4), 343 (IPv6) and 232 MBytes in the maximum bandwidth of 16.1, 15.9, and 10.7 Mbits/Seconds respectively, see Figure 4. The results also have shown that 6 to 4 tunnel broker was outperformed by dual-stack transition mechanism.

Table 1. Summary of TCP throughput measurement

Metric	Dual-stack (DS)				6 to 4 Online	Unit
	LAN		WAN (online)			
	IPv4	IPv6	IPv4	IPv6		
Time	124	126	180	180	181.9	Secs
Transfer	5120	5120	346	343	232	Mbytes
Bandwidth	346	339	16.1	15.9	10.7	Mbits/S

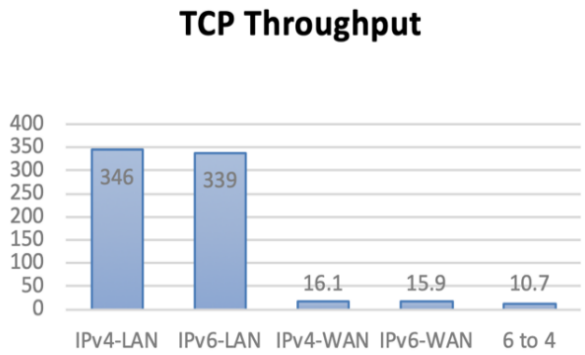

Figure 4. TCP throughput

Table 2 and Figure 5 presents the summary of throughput measurement results for UDP. The quality of a link in UDP was tested in jitter (latency variation or RTT) and datagram loss. As mentioned, UDP packets are sent without any checks but with the advantage of being faster than TCP however, one disadvantage is that there is no guarantee that the datagrams or packets sent would reach their destination. Table 2 shows that dual-stack is superior in terms of bandwidth utilization against 6 to 4 tunneling during the test. IPv4/IPv6 dual-stack achieved 362 and 340 Mbits/Seconds throughput under local area network setup while 16.7 and 12.88 Mbits/Seconds throughput achieved under WAN or online dual-stack setup. This proved that the 6 to 4 tunneling has the poorest performance in terms of throughput and that it only achieved 11.42 Mbits/Seconds.

Table 2. Summary of UDP throughput, jitter, and loss measurement

Metric	Dual-stack (DS)				6 to 4 Online	Unit
	LAN		WAN (online)			
	IPv4	IPv6	IPv4	IPv6		
Time	121.8	129.6	44.1	44.1	44.0	Sec
Transfer	5248	5247	87.5	68.45	59.98	Mbytes
Bandwidth	362	340	16.7	12.88	11.42	Mbits/S
Jitter	0.227	0.217	8.03	9.48	9.69	Ms
Total Loss	0.31	1.309	83	87.2	88.4	%

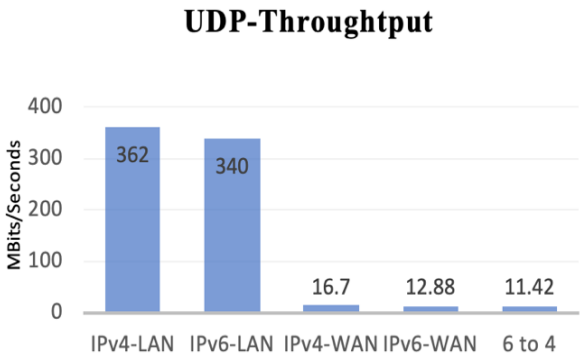

Figure 5. UDP throughput

Table 2 also shows that the dual-stack LAN transition mechanism has a huge advantage in all areas of test parameters. The test also shows that dual-stack LAN has a low network latency and datagram loss (see Table 2, Figures 6 and 7) with the average latency of 0.227ms, 0.217ms and .31%, 1.3% datagram loss for both IPv4 and IPv6 respectively. However, the test also shows (see Table 2 and Figures 8 and 9) that there are too much network latency (jitter) and datagram loss using WAN transmission in both IPv4/IPv6 dual-stack wan and 6 to 4 tunnel with the latency average of 8.03ms, 9.48ms and 9.69ms and average datagram loss of 83%, 87.2%, and 88.4%. The test also shows that IPv6 under dual-stack WAN has a slight advantage versus 6 to 4 tunnel broker.

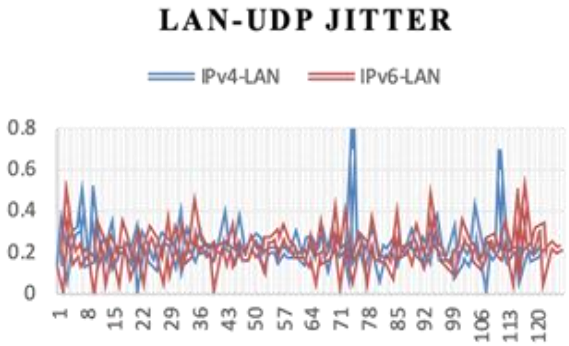

Figure 6. LAN-UDP jitter

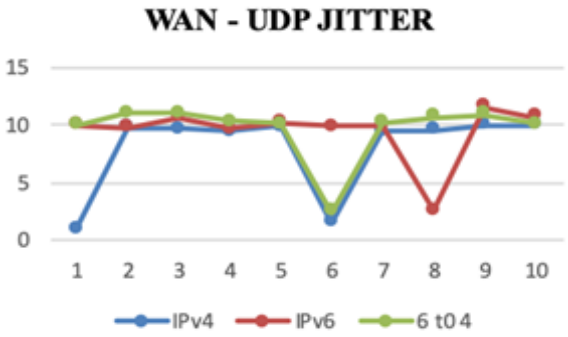

Figure 7. WAN-UDP jitter

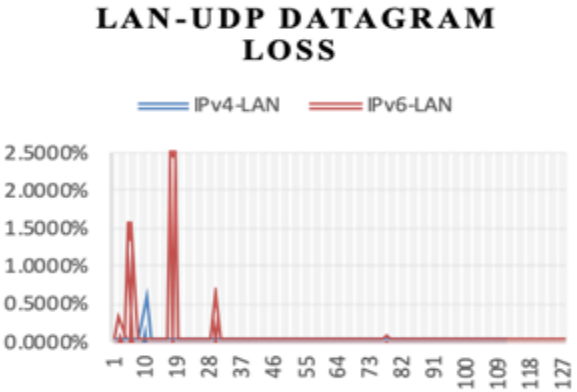

Figure 8. LAN-UDP datagram loss

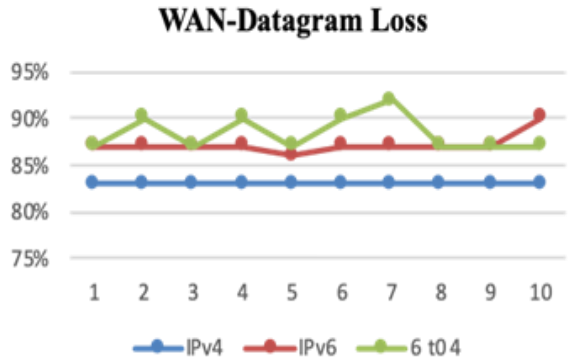

Figure 9. WAN-UDP datagram loss

Furthermore, IPv6 WAN and IPv6 6 to 4 tunnel broker (online) were only measured because the purpose of 6 to 4 tunneling is to enable the network to reach the IPv6 internet by tunneling over existing IPv4 connections from IPv6 enabled host or router to one of the tunnel broker IPv6 routers [25-26]. In short, the 6 to 4 tunnel broker only provides an IPv6 internet connection to the IPv4 internet users that want to experience IPv6 internet in their network. However, the tunnel is more suitable if IPv6 internet is not available in the ISP services in your location.

Moreover, to complete the IPv6 migration process, Traffic Flow was also used. Traffic flow provides real-time visibility into network bandwidth performance [27]. As shown in Figure 10, 41.1% of IPv6 traffic was recorded. This is a good sign that the new IPv6 network migration has worked properly and 41.1% of the university clients are IPv6 capable and IPv6 ready. This also concluded that CLSU is ready to become a campus of the future.

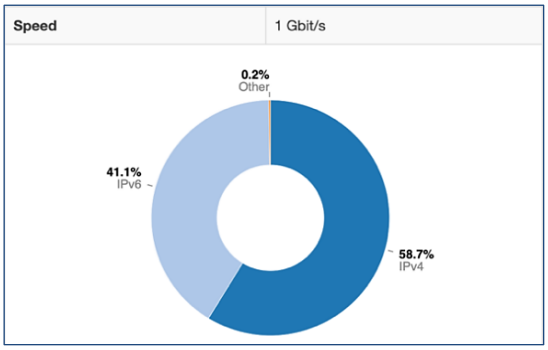

Figure 10. CAMPUS IPv6 utilization

5. CONCLUSION

Due to the deterioration of IPv4 addresses, IPv6 has become a necessity to accommodate the growing number of users especially in the field of academic institutions. The migration from IPv4 to IPv6 protocol in the university requires a long period of time to be implemented. The process requires IPv4 and IPv6 running in one network and IPv6 transition mechanism is needed to enable both protocols to communicate. Proper planning and a suitable choice of transition mechanism can avoid any interferences to the current campus network during the deployment stage.

In general, the testbed results found that the Dual-Stack transition mechanism is more suitable than a 6 to 4 tunnel broker. The results also showed that the 6 to 4 Tunnel Broker was outperformed by the dual-stack transition mechanism in all areas and presents better performance, however, the 6 to 4 tunnel broker is best suited in locations that don't have access to native IPv6 internet connectivity. In addition, the results showed that IPv4 presents a slight advantage in performance than IPv6. The difference is due to the IPv6 header length, which is higher than that of an IPv4 (IPv4 header is 32 bit long while the source and destination addresses of IPv6 header are 128 bits long). Furthermore, the results also showed that after the deployment, the traffic flows captured 41.1% of IPv6 traffic along the network. This is a good sign for us because this indicates that almost half of CLSU user devices are running on IPv6 network and were able to access IPv6 websites. With the provision of IPv6 in the campus network, this allows future development in terms of research, teaching, and collaboration with other universities, and in general, enhances the strength of the school which is of utmost importance. However, IPv6 is still in its early stage; it has lots of bugs and security issues that is still needed to be fixed. Our future research will focus on the IPv6 security issues specifically in the campus network migration.

ACKNOWLEDGEMENTS

We would like to acknowledge the support of CLSU, UP EEEI-PRIME and ASTI-DOST SCIMIX Project for allowing us to use their infrastructures and imparting their knowledge that has helped us finished this research. Also, this research has been funded by the Commission of Higher Education (CHED)-K 12 scholarship program, Republic of the Philippines.

REFERENCES

[1] G. Huston, "Addressing 2018 | APNIC Blog," *APNIC Blog*, 2019. [Online], Available at: https://blog.apnic.net/2019/01/30/addressing-2018/.
[2] The Government of Hong Kong Special Administrative Region, "IPv6 SECURITY," 2011. [Online], Available at: https://www.infosec.gov.hk/english/technical/files/ipv6s.pdf.
[3] A. Mulingbayan, "International perspective on Philippine internet development," *APNIC: Presentation*, 2014.
[4] "Use of IPv6 for Philippines (PH)," APNIC LABS, 2019. [Online], Available at: https://stats.labs.apnic.net/ipv6/PH.
[5] "Google `IPv6," Google, 2019, [Online], Available at: https://www.google.com/intl/en/ipv6/statistics.html.
[6] G. Singh and P. Rakesh, "Use of internet for research and educational activities by research scholars: A study of D.S.B. campus of Kumaun University-Nainital," *Int. J. of Eng. and Manag. Sci.*, vol. 4, no. 2, pp. 193-199, 2013.
[7] K. Babaran, "UP Diliman: A shift from IPv4 to IPv6," PREGINET Pilipinas, 2011, [Online], Available: http://pregi.net/media/news/up-diliman-a-shift-from-ipv4-to-ipv6/.
[8] T. Chown, "IPv6 campus transition scenario description and analysis," *IETF Tools*, 2006.

[9] P. Wu, Y. Cui, J. Wu, J. Liu, and C. Metz, "The transition from IPv4 to IPv6: A State-of-the-art survey," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 1407-1424, 2013.
[10] Z. Wang and W. Xu, "Exploration of IPv6 network construction on campus," *7th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1-4, 2011.
[11] J. Bound, "IPv6 enterprise network scenarios-RCF 4057," *Network Working Group*, pp. 1-17, 2005
[12] F. Siddika, Md. A. Hossen, and S. Saha, "Transition from IPv4 to IPv6 in Bangladesh: The competent and enhanced way to follow," *International Conference on Networking, Systems and Security*, pp. 174-179, 2017.
[13] F. Baker, X. Li, C. Bao, and K. Yin, "Framework for IPv4/IPv6 translation-RFC 6144," *Internet Engineering Task Force (IETF)*, pp. 1-31, 2011.
[14] G. Van de Velde et al, "Local network protection for IPv6-RFC 4864," *Networking Working Group*, pp. 1-36, 2007
[15] J. Arkko and F. Baker, "Guidelines for using IPv6 transition mechanisms during IPv6 deployment-RFC 6180," *Internet Engineering Task Force (IETF)*, pp. 1-20, 2011.
[16] V. J. D. Barayuga and W. E. S. Yu, "Study of packet level UDP performance of NAT44, NAT64 and IPv6 using Iperf in the context of IPv6 migration," *Int.Conference on IT Convergence and Security (ICITCS)*, pp.1-6, 2014.
[17] Q. Li, T. Qin, X. Guan, and Q. Zheng, "Empirical analysis and comparison of IPv4-IPv6 traffic: A case study on the campus network," *18th IEEE International Conference on Networks (ICON)*, pp. 395-399, 2012.
[18] Cisco Networking Academy, "Cisco networking academy connecting networks companion guide: Hierarchical network design-Hierarchical network design overview (1.1)," *Cisco press*, 2014.
[19] M. A. Naagas, E. L. Mique Jr., T. D. Palaoag, and J. S. Dela Cruz, "Defense-through-deception network security model: Securing university campus network from DOS/DDOS attack," *Bulletin of Electrical Engineering and Informatics*, vol. 7, no. 4, pp. 593-600, 2018.
[20] O. Troan and R. Droms, "IPv6 prefix options for dynamic host configuration protocol (DHCP) version 6-RFC 3633," *Network Working Group*, pp. 1-19, 2002
[21] A. Durand, P. Fasano, I. Guardini, and D. Lento, "IPv6 tunnel broker-RFC 3053," *Netw. Work. Group*, pp. 1-13, 2001
[22] V. Jacobson, R. Braden, and D. Borman, "TCP extensions for high performance-RFC 1323," *Netw. Work. Group*, pp. 1-37, 1992
[23] T. T. Zhang, J. Chen, H. Y. Wei, and J. Y. Jiang, "A research on IPv6/IPv4-based network performance test," *International Workshop on Information and Electronics Engineering (IWIEE)*, vol. 29, pp. 1573-1577, 2012.
[24] K. el Khadiri, O. Labouidya, N. Elkamoun, and R. Hilal, "Performance evaluation of IPv4/IPv6 transition mechanisms for real-time applications using OPNET modeler," *Int. J. of Adv. Comp. Sci. and Appl.*, vol. 9, no. 4, pp. 387-392, 2018.
[25] S. Frankel, R. Graveman, J. Pearce, and M. Rooks, "Guidelines for the secure deployment of IPv6," *NIST Special Publication-800-119*, 2010
[26] A. Risdianto and R. Rumani, "IPv6 Tunnel Broker implementation and analysis for IPv6 and IPv4," *6th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*, pp. 139-144, 2011.
[27] A. Zakari, M. Musa, G. Bekaroo, S. A. Bala, I. A. T. Hashem, and S. Hakak, "IPv4 and IPv6 protocols: A Comparative performance study," *IEEE 10th Control and System Graduate Research Colloquium (ICSGRC)*, pp. 1-4, 2019.

BIOGRAPHIES OF AUTHORS

Marlon A. Naagas is an Assistant Professor, former Department Chairman of Information Technology Department of Central Luzon State University. He is also a former Network Engineer in CLSU, former Network Consultant of DOST PCIEERD – CLSU Bayanihanets Project. He is a CISCO Cyber Security Scholarship Awardee, CISCO Certified Network Associate in Cyber Security Operations (CCNA - CyberOps).

Dr. Nemesio A. Macabale Jr. received his Ph.D. in electrical and electronics engineering from the University of the Philippines, Quezon City, Philippines in 2013. He is currently a professor at the Department of Information Technology and the Director of the Information Systems Institute, Central Luzon State University, Science City of Munoz, Philippines.

Dr. Thelma D. Palaoag received her Doctorate Degree in Information Technology (DIT) from the University of the Cordilleras, Baguio City, Philippines. She is a Professor and Research Coordinator of the College of Information Technology and Computer Science, University of the Cordilleras.