A FRAMEWORK FOR DEPLOYING IPV6 AT HIGHER EDUCATION INSTITUTIONS

Shubair A. Abdullah

Department of Instructional and Learning Technology, Sultan Qaboos University
Muscat, Sultanate of Oman

ABSTRACT

Despite the fact that IPv6 was developed 30 years ago, its deployment within higher education institutions worldwide is still slow. While many have started transitioning from IPv4 to IPv6, a large number of them have deferred the transition due to the time needed to complete the transition, budget implications, and security issues. The main problem is how to deploy IPv6 without disrupting the teaching activities of academic departments. This paper introduces a phased framework for deploying IPv6 at the university campus networks of higher education institutions. The framework consists of three phases: preparation and assessment, perimeter network, and internal network. In addition to an independent phase to manage the security issues, a Venn diagram has been created to compare the proposed framework with a state-of-art framework. The results show that the proposed framework retains high value as a comprehensive IPv6 deployment framework at higher education institutions.

KEYWORDS

Higher Education Institution; IPv4/IPv4 transition; IPv4; IPv6

1. INTRODUCTION

On the Internet, data is transmitted via packets, blocks of data, similar to how a post office sends a letter. A person who wants to send a letter puts it in an envelope and types the recipient's address. Based on the address typed, the post office then delivers the letter. The routers deliver the packets based on the device destination address embedded in the packet. A single address is a unique Internet Protocol (IP) address assigned to a device to identify its exact identity and location. Currently, the packets are transmitted and delivered using IP version 4 (IPv4) that was first developed in 1981 [1]. IPv4 addresses are based on 32-bit identifiers, which can be used to create approximately 4.3 billion unique addresses. This number is very limiting when considering the global population and that one person could have more than one device connected to the Internet [2].

IPv6 is a new IP version developed in 1998 that employs a 128-bit address system [3]. It allows for an almost limitless number. Due to the imminent exhaustion of the IPv4 address space, the importance of IPv6 to the future of the Internet is now without question. On 3 February 2011, the Internet Assigned Numbers Authority (IANA) that manages address space globally announced the allocation of the last batch of IPv4 address blocks to the Regional Internet Registries (RIRs). This means that running out of the free pool of available IPv4 addresses in the RIR's designated areas can become a reality at any time [4]. Although there are some practical solutions, such as reusing and recycling unused IPv4 addresses by the ISPs and using the network address translation (NAT) devices that allow using IPv4 addresses privately behind the ISPs router, IPv4 must eventually be replaced with IPv6.

The biggest advantage over IPv4 is the address length. The 32-bit addresses in IPv4 have been increased to 128 bits in IPv6. In addition, the IPv6 has some other advantages over IPv4:

1. Reducing the size of IPv6 routing tables makes the IPv6 routing more efficient and hierarchical.
2. Simplifying the IPv6 packet headers makes the packet processing more efficient.
3. The directed data flows feature that is provided by the IPv6 multicast protocol reduces sending and receiving broadcast packets and allows for saving network bandwidth.
4. IPv6 Stateless Address Auto-configuration (SLAAC) mechanism simplifies the network configuration.
5. IPsec support in IPv6 is mandatory and not an optional add-on as in IPv4.

A University Campus Network (UCN) is a proprietary local area network (LAN) serving university administrative buildings, academic departments, academic halls, libraries, student centres, and other buildings associated with a university campus. Typically, a UCN offers high-speed connections capable of providing video, voice, and data services. It also provides computing resources for the academic curriculum and software applications, which may include video conferencing, email service, and students and staff related applications such as student registration, online learning, and HR management. UCN network administrators are in various stages of deploying IPv6 and facing different challenges [5]. The main challenge faced by higher education institutions (HEIs) is the deployment of IPv6 in a manner that does not disrupt the critical teaching and administrative activities dependent on the existing IPv4 infrastructure. Despite the IPv6 possesses advantages over IPv4, the transition from IPv4 to IPv6 has been slow-moving, particularly within HEIs, due to concerns over the time, budget, and technical challenges associated with this transition. This paper introduces a novel phased framework specifically designed for deploying IPv6 within the UCNs of HEIs. While previous studies have explored various aspects of IPv6 deployment, such as technical challenges and transition strategies [6], this study is unique in its comprehensive approach that not only addresses the technical transition from IPv4 to IPv6 but also focuses on minimizing disruption to academic and administrative activities, which are critical to HEIs. The proposed framework is distinguished by being the first to address the transition from IPv4 to IPv6 HEI environments. This paper aims at revealing the stages of IPv6 deployment across UCN. It also proposes a simple model to explain the effect relationships that are driving the UCN 's migration to IPv6. With regards to the evaluation, qualitative evidence of the framework’s effectiveness is provided.

The rest of the paper is organized as follows: Section 2 provides background information and reviews the existing literature; the framework for deploying IPv6 is presented in Section 3. Section 4 presents the evaluation results and finally, the paper is concluded in Section 5.

2. LITERATURE REVIEW

The transition from IPv4 to IPv6 has been very slow all over the world. Google stats website continuously measures the availability of IPv6 connectivity among Google users. It shows that 23.39% of connectivity is of the IPv6 type until 31/6/2022 [7]. Some reasons behind this slow transition are related to the fact that replacing or upgrading the network infrastructure takes both time and a substantial budget. Other reasons are related to various technical and security issues because IPv6 does not provide a standardized solution to communicate with IPv4 systems. In addition, the transition process itself must be immune from malicious attacks. However, some HEIs have been affected by the general situation of the country in which they are located. In the US, UK, and Canada, which have a relative high level of IPv6 deployment, some HEIs started deployment early. Virginia Tech, for example, deployed IPv6 in a trial in 2004, and then

expanded the IPv6 throughout the campus [8]. In 2016, they reported that 82% of their network traffic used IPv6. Table 1 shows more examples.

Table 1. Examples of IPv6 early deployment in HEI.

Country	University	Starting year
UK	Imperial College London	2003
Canada	McGill University	2005
USA	University of Iowa	2005

Despite IPv6 deployment advancing markedly in these HEIs, it is still years away for many other HEIs as they continue to encounter several issues related to network security and sensitive data monitoring [9]. IPv4/IPv6 transition technical aspects and progress measuring has been the focus of many research [10]. With regards of deploying IPv6 in UCNs, the research has focused on some issues such as technical challenges of IPv6 deployment in UCNs [11] and showcase the IPv6 deployment process in UCNs [10]. In comparison, relatively little work has been published on producing a generic IPv4/IPv6 transition model. Like any new technologies, the modelling the diffusion of the Internet's transition to IPv6 has been extensively studied. Here in this section we only review a sample of representative works. For example, the work of Hovav et al. [12] modelled the IPv4 to IPv6 transition using a diffusion-based model. Their conclusion revealed that the success of IPv6 transition depends on the compatibility with the existing IPv4 standards. In addition, they also mentioned the external influences factors like regulation and investments. Another notable work presented by Joseph et al. [13]. They investigated the impact of converters on the IPv6 adoption and highlighted in their conclusion the efficiency of the convertors has an impact on the IPv6 adoption. A market model of two-side has been presented in the work of Nikkhah et al. [14]. In this model, the service providers connect their customers using different types of connectivity e. g. public IPv4/IPv6 and private IPv4 addresses. They confirmed the importance of the co-ordination among service providers in the IPv6 adoption process. In another study, Nikkhah et al. [15] they proposed a simple model of IPv6 adoption that could be applied by service providers, content providers and end-users. The work presented in this paper differs in the following from the reviewed works:

1. It focuses on higher education institutions and the technical services provided by their computer networks.
2. It is not assumed that the deployment of IPv6 requires high expenditures, but rather focuses on the efforts made by technical staff in higher education institutions.
3. It addresses the transition process in a technical way and sets a time frame for checking and upgrading network devices and computers, in addition to providing a detailed introduction to the security issue of the migration process to IPv6

3. METHODOLOGY

This section presents the proposed framework for UNC administrators to plan their IPv6 deployment. As shown in Figure 1, the approach consists of three phases: preparation and assessment, the perimeter network, and the internal network. The security policy creation will consist of synchronization of the aforementioned phases.

3.1. Preparation and Assessment Phase

This phase is used to plan and assess the personnel and network inventory in terms of hardware and software. It involves an assessment of the staff, a plan to select the best IPv6 address assignment and a method to choose the best internal routing protocol.

3.1.1. Training

Training HEI staff is important and the courses should be selected carefully. The courses may include IPv6 addressing and subnetting, IPv6 routing protocols, IPv6 services, IPv6 and IPv4 transition techniques, and IPv6 security. Some staff groups i.e., the IPv6 implementation group and the operations group will have practical duties that must take more focus. It is recommended that this training be given by teachers from the departments of computer science or computer engineering.

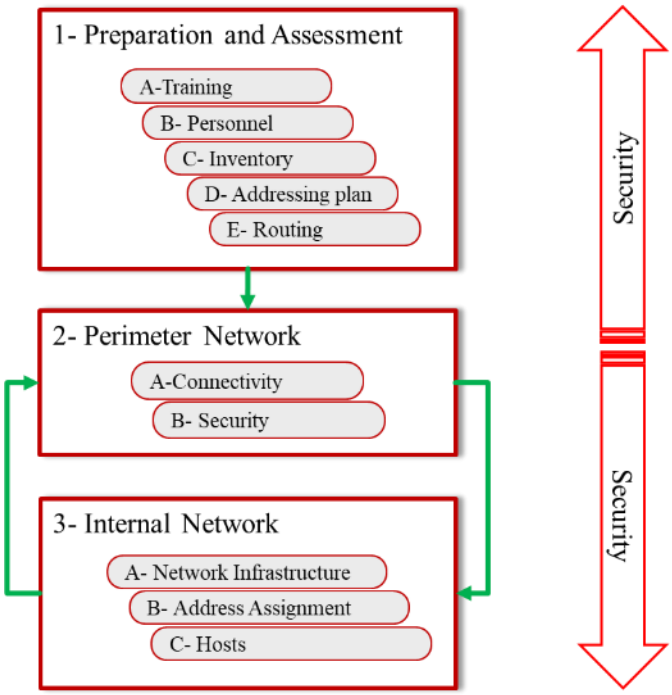

Figure 1. IPv4/IPv6 Transition Phased Approach.

3.1.2. Personnel

The personnel are appointed and assigned the tasks of IPv6 deployment. The formation of the team might include (1) Transition Project Manager to organize the work; (2) Executive Sponsor to ensure the interests of the HEI in the transition; (3) Transition Project Consultant to offer technical expertise, analyse the transition progress, assist in delegating tasks to each team member, and test and tweak each phase of the transition; and (4) Network Administrators, Security Professionals, and Technicians to perform the implementation.

3.1.3. Inventory

The equipment inventory could be decided by the transition team, but it has to achieve basic objectives such as identifying the level of readiness of UCN software and hardware, determining the efforts required to move academic functional services towards supporting IPv6, and identifying which equipment is needed for programming codes or firmware has to be upgraded to be IPv6 ready. The actions needed to achieve these objectives include data collection about the network topology, equipment, and firmware versions. In addition, data must be collected regarding the OS, firmware, middleware, and academic applications (internally developed and purchased).

3.1.4. Addressing Plan

A site as a logical concept refers to an entity that has well-defined boundaries. These boundaries are most typically based on site location or based on site function. Another logical concept is the intra-site. Intra-site is a subnet within the aforementioned well-defined boundaries of a site. Since these specifications can be applied to the UCN, we can consider that the UNC is a site. An example of UNC site is show in Figure 2 and explains how best to implement an IPv6 addressing plan. The UCN site showed in the figure includes four modules: edge, campus, data centre, and infrastructure module.

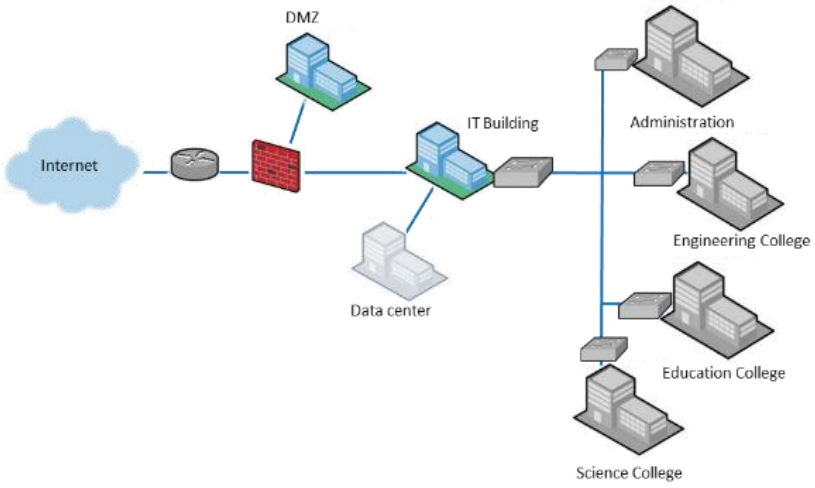

Figure 2. IPv4/IPv6 Transition Phased Approach

- **Edge Network**: The edge network is located in the IT building and consists of a head-end router with a single WAN link from the service provider (ISP). Behind the head-end router, a firewall has segments to the demilitarized zone (DMZ) and to the campus network segments. The edge network includes the domain name server (DNS), email server, web server, and Virtual Private Network (VPN) for remote access. Also provided by the Internet connection (an ISP WAN connection) are a Firewall and Intrusion Detection System (IDS).
- **Campus Network**: The campus network consists a distribution switch connected to the data center and has fiber runs to switches in other buildings. The IT building houses the IT departments and the data center. The administration building houses the administrative departments. Several Virtual LANs (VLAN) incorporated by the campus network include: Ethernet network, wireless network, internal users, guests (spans the site), and voice-over IP (VoIP) for telephone calls.
- **Data Center Network**: the data center network includes typical top-of-rack switches. The data center network includes two components, a storage network and a private cloud.
- **Infrastructure Network**: the infrastructure network includes elements such as loopback and management interfaces, point-to-point interfaces, and guest wireless networks.

In IPv6, a subnet is part of an IPv6 address that consists of an IPv6 global prefix and subnet identifier. Addressing plans in IPv6 are about defining and assigning subnets based on the site structure of the UCN. The source of the IPv6 global prefix is the first concern when addressing a plan. Two types of global prefix sources exist: Provider Independent (PI) prefixes obtained from a regional Internet registry i.e. RIPE NCC, and Provider Aggregate (PA) prefixes obtained from a local Internet registry i.e. ISP.

The typical setup for UCN subnets is /64, that is 48 bits for the global prefix and 16 bits for the subnets within the UCN. To accommodate future expansions in the number of sites, however, a /44 global prefix is used. Assuming 2001:db8:11a0::/44 is the global prefix , Table 2 shows the global routable prefix of the site IPv6 address.

Table 2. The global routable prefix of the IPv6 addresses for the site (UCN)

Organization Prefix	Site IPv6	Description
2001:db8:11::/44	:a0	Main campus
	:a1 to :af	Future use

3.1.5. Implementation of Addressing Plan

The structure of intra-sites subnet is a group of subnets hierarchically arranged. The following steps define the subnets for the intra-sites:

Step1: Primary modules of intra-site

Within the main campus, the first level of hierarchy will be assigned to the primary modules. There are four modules: the edge, the campus, the data center, and the infrastructure. Thus, two bites are enough to represent the primary module, however, one nibble (2^4=16 primary modules) will be reserved to cover any future expansion. Table 3 shows the results of step 1.

Step 2: Segments

The second level of hierarchy will be assigned to the segments within the module. One nibble (24=16 segments) will be reserved to cover any future expansion. Table 4 shows the second step implementation of addressing for the module of Campus.

Step 3: Departments

The third level of hierarchy will be assigned to the various departments within the segment. Two nibbles (2^8=256 departments) will be reserved to cover any future expansion. Table 5 shows the three step implementation of addressing the segment of Engineering.

Step 4: VLANs

The fourth level of hierarchy will be assigned to the VLANs within the department. One nibble (24=16 VLANS) will be reserved to cover any future expansion. Table 6 shows the fourth step implementation of addressing for the department of Computers.

Table 3. The global routable prefix of the IPv6 addresses for the site (UCN)

Intra-site	Module	Description
2001:db8:11 a0::/48	:0	Reserved
	:1	Edge
	:2	Campus
	:3	Data center
	:4	Infrastructure
	:5 to :f	Future use

Table 4 Implementation of IPv6 addressing for the module of Campus.

Module	Segment	Description
2001:db8:11 a0:2::/52	:0	Reserved
	:1	Engineering
	:2	Education
	:3	Science
	:4	IT
	:5 to :f	Future use

Table 5 Implementation of IPv6 addressing for the segment of Engineering.

Segment	Department	Description
2001:db8:11 a0:22::/60	:00	Reserved
	:01	Computer
	:02	Electricity
	:03	Electronic
	:04	Mechanic
	:05 to :ff	Future use

Table 6 Implementation of IPv6 addressing for the department of Computers.

Department	VLAN	Description
2001:db8:11 a0:221::/64	**:0**	Reserved
	:1	Wired
	:2	Wireless
	:3	Internal
	:4	Guest
	:5	VoIP

3.1.6. Routing

There are four IPv6 IGP (Interior Gateway Protocol) routing protocols: Routing Information Protocol next-generation (RIPng), an Open Shortest Path First version 3 (OSPFv3), Enhanced Interior Gateway Routing Protocol (EIGRP), and Intermediate System–to–Intermediate System (IS-IS). The most common routing protocols are RIPng and OSPFv3. The processes and operations of the IPv6 routing protocols are basically the same as in IPv4. The main difference is in the authentication process; where the IPv4 routing protocols use MD5 features while the IPv6 routing protocols use the authentication features provided by the IPsec. The IPv6 routing protocols are not much different than their IPv4 counterparts. Therefore, it would be beneficial to continue using the same protocol family that is being used for IPv4.

3.2. Perimeter Network Phase

A perimeter network consists of Internet accessible services such as web and email services along with edge routers and firewalls. Since the UCN will communicate with IPv4 networks, edge routers are needed to adopt tunnels or NAT64 translation [16]. Another option available is dual-stack, which adopts both protocols IPv4 and IPv6. Employing either option should be decided based on the interests of the HEI. The security part involves implementing three security techniques: filtering, monitoring, and logging. With regards to online learning environments, sophisticated and modern tools should be used in implementing these techniques to eliminate outside intruders. The tools may include stateful firewalls, anti-spoofing tools, and an ingress access control list (ACL). The monitoring covers specifically the access path to the learning

management systems servers. Logging the outside users' activities at the edge router helps in detecting unusual behaviour. Their privacy and the confidentiality shall be observed in all circumstances.

3.3. Internal Network Phase

This phase is closely related to the previous phase and the team might have to move back to integrate the overall tasks. The internal network consists of devices and peripherals of the faculty, students, and employees as well as HEI management and academic related applications. The network infrastructure covers deploying IPv6 on the network infrastructure's devices plus the wireless access points (WAP) that offers UCN services wirelessly in the student centers, teaching halls and scientific laboratories, administrative buildings, etc. With regards to the IPv6 addresses assignment, the dynamic host configuration protocol (DHCPv6) is recommended to control the addresses in UCN. Adopting DHCPv6 addressing method enables a clearer understanding of the segments of the UCN. The host deals with deploying IPv6 on the end-user devices, PC, laptops, and mobile devices. The good news is that most OSes support IPv6 today, but there is a need to investigate the default status of IPv6. For example, Windows 10 and OS support the basic IPv6 features by default, while Linux needs little configuration in case of using IPv6 auto stateless assignment. Attention should be paid to the software that is specially developed for the HEI, such as student registration and grading database management systems. The modifications might be to the middleware tools, which are used to enable database management systems to communicate with the databases, i.e. Open Database Connectivity (ODBC) and ActiveX Data Objects (ADO.NET).

3.4. The Security Policy

The security policy is crucial for HEI enterprise networks since they deal with both faculty and students' data which are highly sensitive and important data. Securing the UCN endeavours will never end, the security policy needed to be built, implemented, and constantly optimized. Knowledge of IPv6 is the best security measure. Therefore, it is important to assess the transition team's knowledge to determine the need for temporary consultants. The security policy includes the following aspects:

1. Similarities between IPv4 and IPv6 attacks: this helps to apply the same malware mitigation techniques of IPv4 in IPv6. In general, malwares that attack online learning systems and database systems i.e., cross scripting and SQL injection might be mitigated using same techniques of IPv4 protocol.
2. Specific Security Issues for IPv6: this helps to decide which IPv6 security feature to be enabled like IPSec and RA-Guard.
3. The severity level when implementing dual-stack, IPv4 and IPv6 together: this will help to decide the intrusion detection systems (IDS) and types of firewall that need to be purchased.
4. Inspection of the security vendors worldwide: companies such as Palo Alto Networks are producing devices with up-to-date built-in mitigation techniques.

4. EVALUATION

For the evaluation purposes, a comparison between the presented framework and a state-of-the-art framework has been conducted. The method proposed by Li & Li [17] was selected for the comparison. This framework was chosen for comparison because, to the best of the author's knowledge, no other comprehensive frameworks for IPv6 deployment in HEIs have been published. In addition, it represents the most relevant and advanced approach currently available,

making it an appropriate benchmark for assessing the proposed framework's effectiveness. By comparing it with this state-of-the-art model, this sections aims to highlight both the strengths and areas of improvement in the proposed approach. The Venn diagram [18] was used to show all possible similarities and differences, as in Figure 3. The overlap area contains the similarities. It shows the two methods have an analysis of basic needs in terms of staff, software, and equipment. Both methods aim to deploy IPv6 in HEI and UCNs. The differences are shown in the non-overlapped areas. In terms of staff, the proposed framework details training courses while the scheme has a limited reference to the training. The proposed framework has detailed transition plans for perimeter and internal networks along with software and hardware inventory, addressing, and routing recommendations while selected scheme has analysed the address types and demonstrated the risk of applying tunnelling.

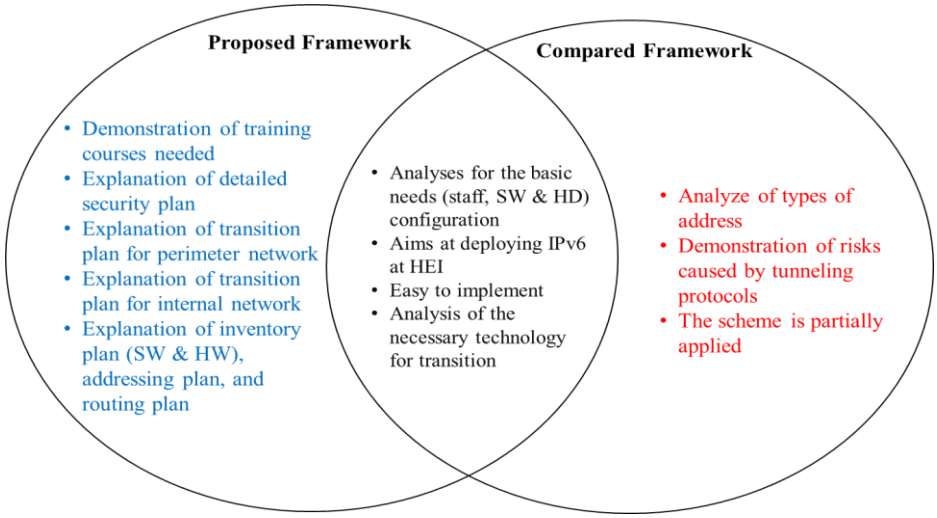

Figure 3. Comparison of the proposed framework against Li & Li's scheme.

This is the most important difference, which could be considered in favour of the proposed framework. However, the selected scheme has been partially applied at the campus network.

5. CONCLUSION

Many HEIs have started deploying IPv6 protocol over their UCNs, and they are currently in various stages of deployment. A large number of HEIs have deferred transition due to the time needed to complete the transition, budget implications, and security issues. The main challenge is how to deploy IPv6 without negatively impacting the teaching tasks of academic departments. In this paper, a new framework for deploying IPv6 at HEI was introduced to help UCN's network administrators have a comprehensive understanding of the transition. The framework consisted of three phases: preparation and assessment, the perimeter network, and the internal network, while the security policy creation and adoption was intended to synchronize all phases. A comparison was conducted against a state-of-the-art framework for the purpose of evaluation. The results showed that the proposed framework possesses high value as a comprehensive IPv6 deployment framework at HEIs.

REFERENCES

[1] A. Shiranzaei and R. Z. Khan, "A comparative study on IPv4 and IPv6," *Int. J. Adv. Inf. Sci. Technol. (IJAIST)*, vol. 33, pp. 6–19, 2015.

[2] K. G. Coffman and A. M. Odlyzko, “Growth of the Internet,” in *Optical Fiber Telecommunications IV-B*, Elsevier, 2002, pp. 17–56.
[3] S. Deering and R. Hinden, “Internet protocol, version 6 (IPv6) specification,” RFC 2460, Dec. 1998.
[4] P. Richter, M. Allman, R. Bush, and V. Paxson, “A primer on IPv4 scarcity,” *ACM SIGCOMM Comput. Commun. Rev.*, vol. 45, no. 2, pp. 21–31, 2015.
[5] S. L. Levin and S. Schmidt, “IPv4 to IPv6: Challenges, solutions, and lessons,” *Telecomm. Policy*, vol. 38, no. 11, pp. 1059–1068, 2014.
[6] Z. Ashraf, A. Sohail, S. A. Latif, A. Hameed, and M. Y. Malik, "Challenges and Mitigation Strategies for Transition from IPv4 Network to Virtualized Next-Generation IPv6 Network," *International Arab Journal of Information Technology*, vol. 20, no. 1, pp. 78-91, 2023.
[7] “IPv6 Adoption,” Google Stats, 2022. [Online]. Available: https://www.google.com/intl/en/ipv6/statistics.html. Accessed: Jul. 15, 2022.
[8] S. Groat, M. Dunlop, R. Marchany, and J. Tront, “IPv6: nowhere to run, nowhere to hide,” in *2011 44th Hawaii International Conference on System Sciences*, 2011, pp. 1–10.
[9] S. Zander and X. Wang, “Are we there yet? IPv6 in Australia and China,” *ACM Trans. Internet Technol.*, vol. 18, no. 3, pp. 1–20, 2018.
[10] J. Czyz, M. Allman, J. Zhang, S. Iekel-Johnson, E. Osterweil, and M. Bailey, “Measuring IPv6 adoption,” in *Proceedings of the 2014 ACM Conference on SIGCOMM*, 2014, pp. 87–98.
[11] K. S. Mudziwepasi and M. S. Scott, “Exploring technical deployments of IPv6 on university LANs,” *Int. J. Comput. Sci. Issues*, vol. 11, no. 1, pp. 187–193, 2014. [Online]. Available: http://www.ijcsi.org/papers/IJCSI-11-1-2-187-193.pdf.
[12] A. Hovav, R. Patnayakuni, and D. Schuff, “A model of Internet standards adoption: the case of IPv6,” *Inf. Syst. J.*, vol. 14, no. 3, pp. 265–294, 2004.
[13] D. Joseph, N. Shetty, J. Chuang, and I. Stoica, “Modeling the adoption of new network architectures,” in *Proceedings of the 2007 ACM CoNEXT Conference*, 2007, pp. 1–12.
[14] M. Nikkhah and R. Guérin, “Migrating to IPv6—The role of basic coordination,” in *2014 IFIP Networking Conference*, 2014, pp. 1–9.
[15] M. Nikkhah and R. Guérin, “Migrating the internet to IPv6: An exploration of the when and why,” *IEEE/ACM Trans. Netw.*, vol. 24, no. 4, pp. 2291–2304, 2015.
[16] S. A. Abdulla, “Survey of security issues in IPv4 to IPv6 tunnel transition mechanisms,” *Int. J. Secur. Networks*, vol. 12, no. 2, pp. 83–102, 2017.
[17] B. Li and Z. Li, “The design of IPv6’s transitional scheme in university,” in *AIP Conference Proceedings*, 2017, vol. 1839, no. 1, p. 020219.
[18] H. A. Kestler, A. Müller, T. M. Gress, and M. Buchholz, "Generalized Venn diagrams: a new method of visualizing complex genetic set relations," *Bioinformatics*, vol. 21, no. 8, pp. 1592-1595, 2005.

AUTHOR

Shubair Abdulla received his BSc degree in computer science from Basra University in 1994, and his MSc and PhD degrees in computer science from University Sains Malaysia (USM) in 2007 and 2014 respectively. He is working as assistant professor at Sultan Qaboos University, Oman, Muscat currently. His research interests include data mining, network security, and fuzzy inference systems.