# Migrating from IPV4 to IPV6 in Jamaica

Christopher Udeagha ,School of Computing & Information Technology,
Faculty of Engineering& Computing, University of Technology
(UTech), Papine Campus, Jamaica.

## *Abstract*

***This paper will review the technological knowhow, especially, in areas of IPV6 applications by some local industries in Jamaica. The researchers will examine the limitations of internet protocol version 4 (IPv4), migrating from IPv4 to internet protocol, version 6 (IPv6), thebenefits and applications of IPv6. As knowledge continues to increase, so does technology and this will require more IP addresses spaces. IPv4 addresses are being depleted and this is making way for the transition into IPv6, which has 128 bits. The IPV6 will not only increase the number of IP addresses available but will also offer more efficient routing, better packet processing, improved IP securities, betterfragmentations, no packet congestion, no delay and hence no loss of packets.***

***This paper will also explain what these local industries have done, to achieve the green technique in computing, to migrate to IPV6.***

## *Keywords*

***IP; IPV4; IPV6; local industries; migrating; technology .***

## I INTRODUCTION

IPv4, according to Techopedia.com, is a connectionless protocol used in packet-switched layer networks such as Ethernet. IPv4 was designed to allocate approximately 4.3 billion addresses which at the beginning of the internet were considered more than enough. However, the sudden growth in internet users and its global use drastically increased the amount of devices needing authentic and unique IP addresses to communicate. Methods such as Network Address Translation (NAT) have been implemented to reduce the number of unique addresses needed by each device, yet the problems of IPV4 are still not resolved. However, IPv6 is the “new wave” which picks up the slack of IPv4.Many countries including Jamaica and the world at large can no longer continue to ignore IPV6. This study will educate us and the population at large about methods of migrating from IPv4 to IPv6 and the benefits of making such a transition by some

DOI: 10.5121/cncij.2019.041012 

local industries in Jamaica, such as digicel and flow through cable and wirelesscommunication (CWC) LTD of Jamaica.

The internet has experienced decades of rapid development, as the cornerstone of the entire network addresses need to be increased. With only 5.5% of IPv4 addresses available the cry for the turn to IPv6 could not be more imminent [1]. Today, with the explosive growth of the Internet, the number of network devices owned by each person is estimated to be 3.4 in 2020 and the requirements of IP addresses become much larger [2]. Not to mention network dependent initiatives like Cloud, 3G, Virtualization and BYOD are rapidly consuming the last remaining IPv4 addresses [4]. While IPv6 is considered to be a feasible solution due to its sufficient address space; the slow deployment of IPv6 and non-compatible structure of IPv6 and IPv4, makes the necessity of the transition from IPv4 to IPv6 a challenging one. By design, IPv6 cannot coexist with IPv4 networks creating challenges; yet on the other hand opportunities for the service providers. The current challenge for the IPv4 based business is to determine how to transition to IPv6 (Mill, 2012). Change from IPv4 to IPv6 is a planned procedure; significant players everywhere throughout the world have just begun the procedure. It is the high time to move towards IPv6, before the intense need emerges [4].

## II Background

This paper reviews the detail information to migrate from IPV4 to IPV6 by digicel and flow in Jamaica, benefits, potential issues interoperability issues and internet service providers (ISP).It examines the transitional techniques adopted by these companies to migrate from IPV4 to IPV6.
It is impossible to change the entire Internet infrastructure from IPv4 to IPv6 in an instant. As such, transitional mechanisms were applied by these local industries to migrate IPv4 to IPv6 [5]. Some of the transitional technologies adopted by these companies were; header translation, tunnelling and dual stack

A)HeaderTranslationTranslation mechanism is meant for communication between IPv4 and IPv6 network. Header translation is necessary when the majority of the Internet has transitioned to IPv6 but some systems still use IPv4 [6]. Basic mechanism behind the strategy is header translation due to which it is known as translation mechanism. Translation transition mechanisms function similarly to NAT in IPv4; routers translate between IPv4 and IPv6 addresses at network boundaries [6]. For example, a packet originating from IPv4 network, the translator would convert its header into IPv6 header before it is sent to IPv6 network and same process is done in inverse manner too [5]. In this technique, separate translator is required between both the networks; programming translators is a difficult task and sometimes high capacity translators may be required. It faces similar security issues as are faced in NAT because there is no end to end connectivity. On the other hand, it can be useful in some scenarios such as

if it is required to connect the IPv6 and IPv4 nodes independently then Translation Mechanism is the best choice [4].

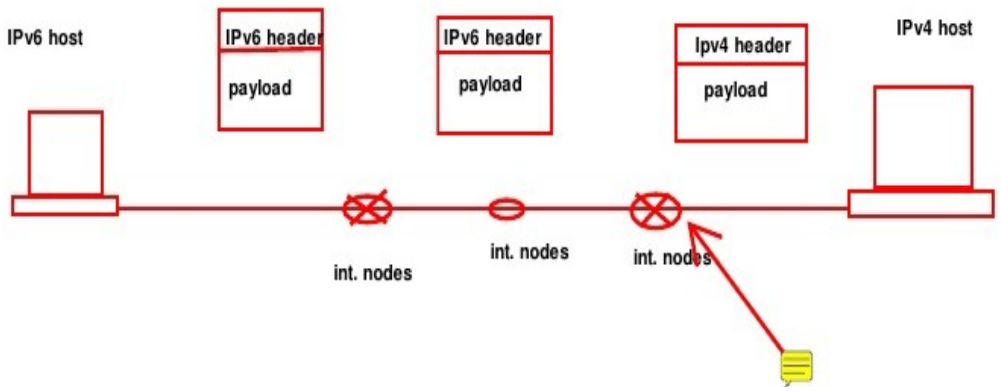


**Figure 1: Header translation technique**

**B) Tunnelling**

Tunnelling is a strategy used when two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4 [5]. Configured tunnelling of IPv6 over IPv4 is a procedure for creating point-to-point tunnels by encapsulating IPv6 packets within IPv4 headers to transport them over IPv4 routing infrastructures. In most deployment situations, the IPv6 routing infrastructure will ultimately be designed overtime. Although the IPv6 infrastructure is being deployed, the present IPv4 routing infrastructure can remain functional and can be used to carry IPv6 traffic. Tunnelling provides an approach to develop an existing IPv4 routing infrastructure to carry IPv6 traffic. IPv6/IPv4 hosts and routers can tunnel IPv6 datagrams over regions of IPv4 routing topology by encapsulating them within IPv4 packets [3]. The widely used tunnelling mechanisms include IPv4/IPv6 configured tunnel, 6to4, ISATAP, Silkroad, Teredo, Tunnel Broker, TSP, DSTM, etc.[6].

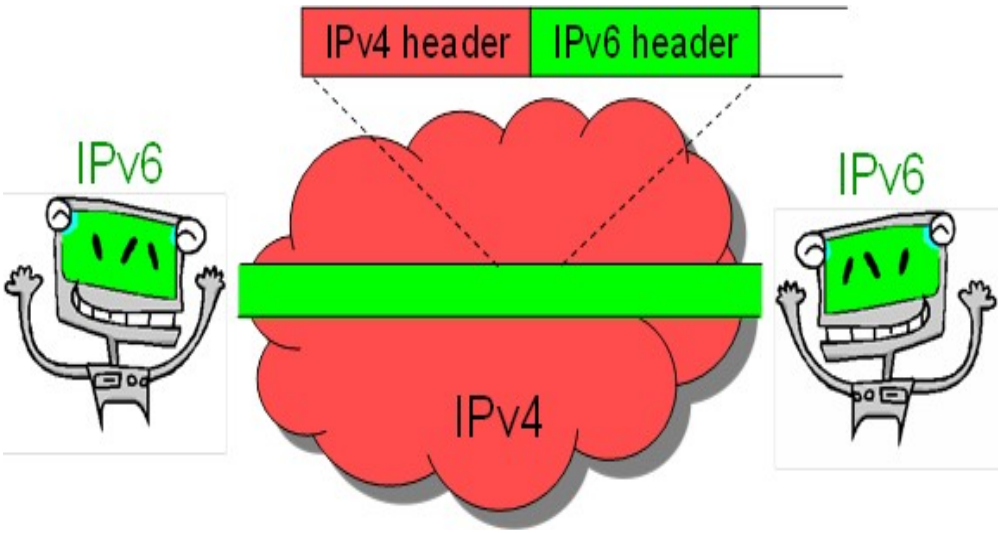


**Figure 2: The transitional technique in tunnelling**

**C) Dual Stack**

Dual IP layer (also known as dual stack) is a technique for providing complete support for both Internet protocols -- IPv4 and IPv6 -- in hosts and routers. A dual stack network is a network in which all of the nodes are both IPv4 and IPv6 enabled. Because the nodes support both protocols, IPv6/IPv4 nodes may be configured with both IPv4 and IPv6 addresses. IPv6/IPv4 nodes use IPv4 mechanisms (e.g., DHCP) to acquire their IPv4 addresses, and IPv6 protocol mechanisms (e.g., stateless address auto configuration and/or DHCPv6) to acquire their IPv6 addresses. As a straightforward IPv6 transition solution, deploying a dual-stack network is popular among many Internet service providers (ISPs) [6]. However, this solution cannot really support interoperation between IPv4 and IPv6 networks. In addition, managing a dual-stack network is complicated and expensive. Hence, the research community is focusing on other solutions that can support the interoperation between two heterogeneous protocols. Such solutions can be broadly classified into two categories, translation and tunnelling. In both of them, state is essential because it keeps necessary information including binding between IPv4 and IPv6 addresses, transport-layer protocol and IDs (i.e., TCP/UDP ports or Internet Configuration Message Protocol IDs), and so on [3].

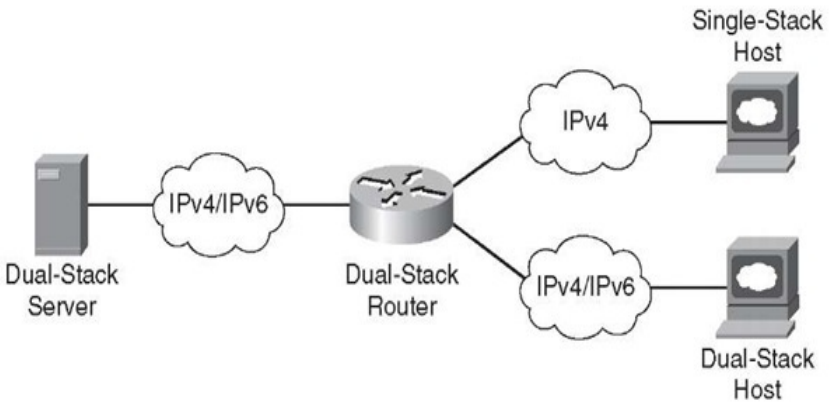


**Figure 3: The dual stack transitional technique.**

## III POTENTIAL ISSUES

Even though the IPv6 introduction is a miraculous idea the IPv4 to IPv6 transition is encountering multiple challenges. These challenges and potential issues could be prudent to monitor and could influence the course of the transition. Pace adoption, consumer demand, no flag date, IPv6 transition methods and security are a few of the named challenges that are being surveyed to this date. Pace adoption speaks on the slow movement of the IPv6 transition. Little content is available, connectivity is limited, backbone services were not always abundant, IPv4 devices are embedded, and there is a lack of IPv6 exchange points[8].

Consumer demand for the protocol is low [9]. There is consumer demand for Internet access regardless of whether IPv4 or IPv6. Public Internet services are generally reachable today via IPv4, so there is no perceived need by consumers to run IPv6 [10]. Consumers have devices such as cameras, TVs or game consoles that may only be IPv4 enabled. If the Internet service provider for these devices migrate to the IPv6 protocol, the service provider risks upsetting consumers whose equipment may no longer work properly on the new protocol [9].

Another challenge for the transition is that there is no set achievement date. Unlike the transition from NCP to Ipv4 previously, there is no hard and fast date for this new transition therefor there is no urgency in achieving the success for the transition which makes it even harder to fully implement. Ipv6 is not backward compatible which means that ipv6 networks are not directly interconnected with ipv4 protocols 10. This means there will be a big issue where ipv4 devices should communicate with ipv6 devices.

Lastly the most talked about challenge is the security aspect in the ipv6 protocol. Security infrastructure, in the vast majority of cases, is not ready, especially if Security is left to the final stages of implementation [10]. There is much less experience with IPv6 than with IPv4 and IPv6 implementations are less mature than their IPv4 counterparts which means security products like firewalls, NIDS, etc. have less support for IPv6 than for IPv4 [8].

The complexity of the resulting network is expected to increase during the transition/co-existence period, increased use of NATs, increased use of tunnels, use of other transition/co-existence technologies and Lack of well-trained human resources are also expected to result from the transition.

## IV INTEROPERABILITY ISSUE

In light of the immense differences between the protocol formats, interoperability cannot exist between IPv4 and IPv6. An ISP is needed to create an independent yet parallel network. This requires overlap features to enable operation on both networks and to allocate necessary bandwidth for both platforms [11]. In addition, dual-protocol stacks have been implemented in modern computer operating systems to access both networks.

Moreover, an upgrade is needed for the complete range of devices to support IPv6 features to allocate shared resources. Since IPv4 and IPv6 protocols are not compatible, they run their individual addressing and routing systems [12]. Without additional mechanisms, the two types of networks cannot communicate.

However, in reality, IPv4 and IPv6 networks are mixed together because it is the users who decide when to switch to IPv6. Regardless of whether a user has IPv4 or IPv6 access, they still want to communicate with each other irrespective of platform. This requires an artificial inter-operability between protocols in the interest of network connectivity in heterogeneous networks.
Internet Service Providers & Internet Content Providers

Providing IPv6 users with accessibility to IPv4 services has been one of the most challenging tasks during the IPv4/IPv6 transition. Some protocols contain IP addresses in the application layer, resulting in incompatibilities in traversing the network-layer translators. The transition to IPv6 for Internet Content Providers (ICPs) cannot be done at one stroke because of the difficulty both in upgrading infrastructures and in updating all the content to be IPv6-compatible.

At the same time most of the operating systems on user devices have supported IPv6 and the number of global IPv6 users has been increasing in recent years. Google reports that over 12% of

their users are using IPv6 by July 2016, most of which are using native IPv6 rather than legacy tunnels [5]. Moreover, due to the shortage of IPv4 address resources on Internet Service Providers (ISPs), more and more newly built networks will become IPv6-only instead of dual-stack to save IPv4 addresses. Therefore, bridging the gap between IPv6 users and IPv4 services is an important task in IPv4/IPv6 transition.

## V OTHER INTERNET PROTOCOL (IP) VERSIONS

1. IP v 1-3 defined and replaced
2. IP v4 - current version
3. IP v5 - streams protocol
4. IP v6 - replacement for IP v4
5. During development it was called IPng
6. Next Generation

## VI WHY CHANGING IP VERSIONS

1. Address space exhaustion
2. Two level addressing (network and host) wastes space
3. Network addresses used even if not connected to Internet
4. Growth of networks and the Internet
5. Extended use of TCP/IP
6. Single address per host
7. Requirements for new types of service

## VII BENEFITS OF IPV6

IPv6 was primarily designed to solve the problem of IPv4 address exhaustion by increasing the address space from 32b to 128b. The address itself is split into a 64b network identifier and a 64b host identifier using /64 subnet masks for all networks. Allocation of /48 prefixes to end customers allows for 65536 /64 subnets, each of which can more than accommodate the entire IPv4 address space [7]. Moreover, there are other improvements compared to IPv4 than just an expanded address space. Other enhancements include but aren't restricted to:

**1 More Efficient Routing** - IPv6 reduces the size of routing tables and makes routing more efficient and hierarchical.

**2 More Efficient Packet Processing** - IPv6's simplified packet header makes packet processing more efficient. Compared with IPv4, IPv6 contains no IP-level checksum, so the checksum does not need to be recalculated at every router hop [13].

**3 Directed Data Flows** - IPv6 supports multicast rather than broadcast. Multicast allows bandwidth-intensive packet flows (like multimedia streams) to be sent to multiple destinations simultaneously, saving network bandwidth [12].

**4 Simplified Network Configuration** - Address auto-configuration (address assignment) is built in to IPv6. A host can generate its own IP address by appending its link-layer (MAC) address to the 64 bits of the local link prefix [12].

**5 Support for New Services** - By eliminating Network Address Translation (NAT), true end-to-end connectivity at the IP layer is restored, enabling new and valuable services. Peer-to-peer networks are easier to create and maintain, and services such as VoIP and Quality of Service become more robust [12].

**6 Security IPsec** - provides confidentiality, authentication and data integrity, is baked into in IPv6. Because of their potential to carry malware, IPv4 ICMP packets are often blocked by corporate firewalls, but ICMPv6, the implementation of the Internet Control Message Protocol for IPv6, may be permitted because IPsec can be applied to the ICMPv6 packets [12].

## VIII STRUCTURE OF IPV6

An Ipv6 PDU known as a packet has the following general form [14]:

### A) 1Pv6 Extension Header

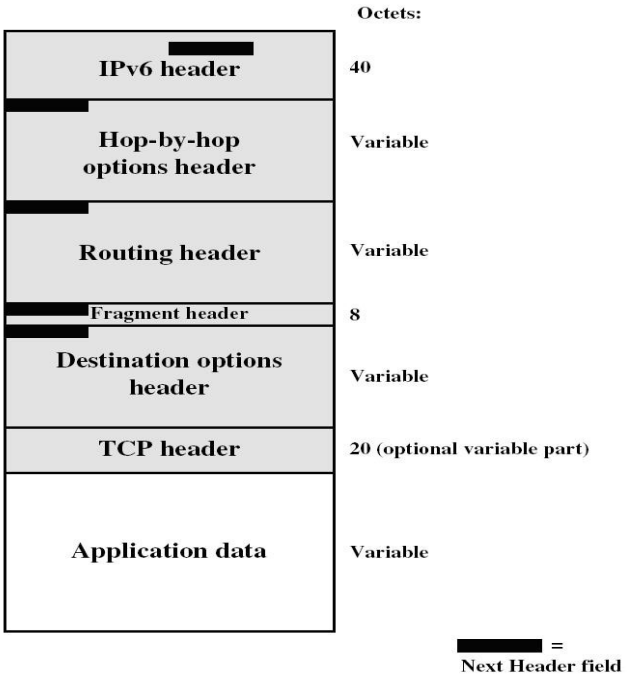


**Figure 4: IPV6 packet with extension header containing a TCP segment**

### B) Extension Headers

- **Hop-by-Hop Options-** Options to be processed at each hop
- **Routing -** Similar to v4 source routing; extended routing
- **Fragment** – contains fragmentation and reassembly information
- **Authentication** – provides packet integrity and authentication
- **Encapsulating security payload header**- Provides security
- **Destination options header** – Contains optional information to be examined by the destinationnode.

The IPv6 standard recommends that, when multiple extension headers are used, the IPv6 headers appear in the following order[14]:

1. **IPv6 header**: mandatory, must always appear first
2. **Hop-by-hop options header**
3. **Destination Options header:** For options to be processed by the first destination that appears in the IPv6 Destination address field plus subsequent destinations listed in the routing header.
4. **Routing header**
5. **Fragment header**
6. **Authentication header**
7. **Encapsulating Security payload header**
8. **Destination Options header:** For options to be processed only by the final destination of the packet.

### C) IPV6 Address Structure

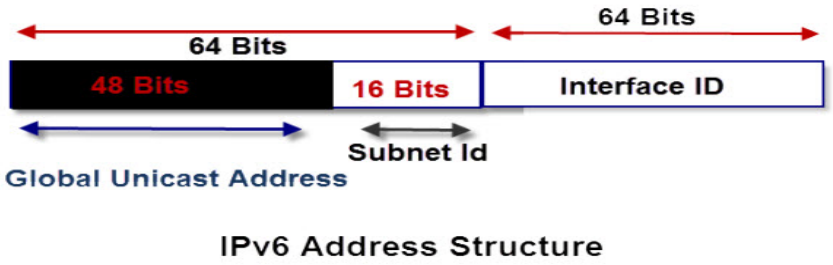


**Figure 5: IPV6 address structure.**

### The IPv6 Address structure contains the following:

1. 128 bits long
2. Assigned to individual interfaces on nodes ( Nodes include both routers and hosts)
3. Single interface may have multiple unicast addresses; but any of the uni-cast addresses associated with a given interface on a node may uniquely identify that node.
4. Three types of address
5. Unicast-single interface
6. Anycast
7. Set of interfaces (typically different nodes)
8. Delivered to any one interface
9. the “nearest”
10. Multicast

11. Set of interfaces
12. Delivered to all interfaces identified

## D) IPV6 Header

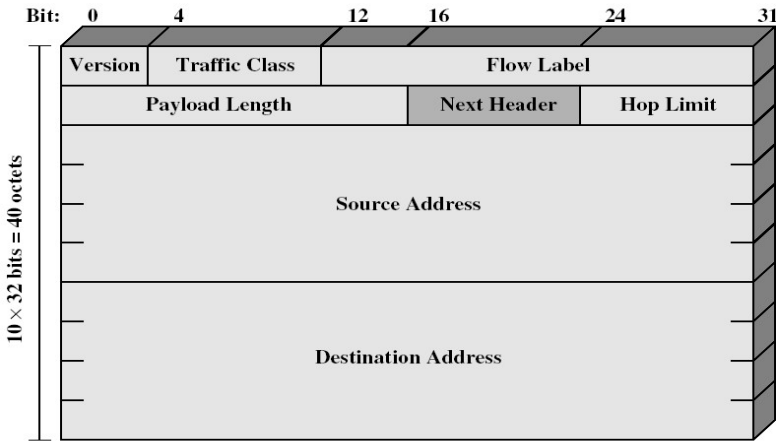


**Figure 6: IPV6 header with 40 octets**

## E) Scope of IPV6 Unicast Addresses [15]

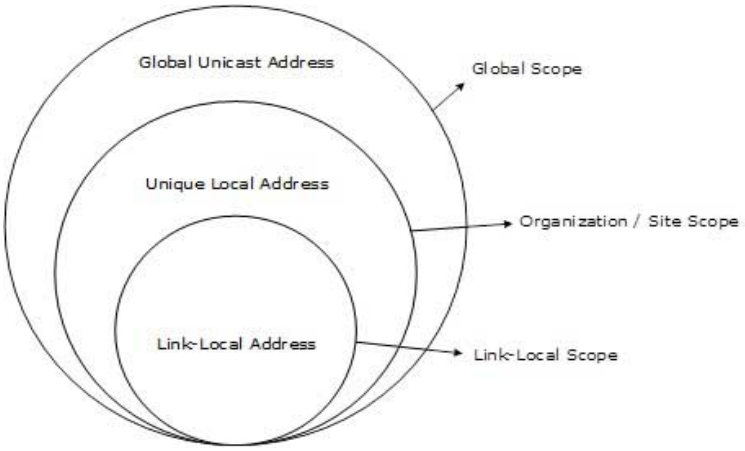


**Figure 7: IPV6 unicast address scope**

The Unicast addresses are globally unique and recognizable, but are not routed over the internet, limiting their scope to the organization's boundary.

## IX SIDE BY SIDE COMPARISM OF IPV4 AND IPV6 [16]

| | IPv4 | IPv6 |
|---|---|---|
| **Invention** | 1981 | 1999 |
| **Address length** | 4 bytes<br>32 bits | 16 bytes<br>128 bits |
| **No. of addresses** | $2^{32} \approx 4.2$ billion<br>(Less than a single IP address per person on the planet) | $2^{128} \approx 340$ trillion trillion trillion |
| **Address format** | Dotted decimal notation:<br>192.168.10.1 | Hexadecimal notation:<br>2001:0db8:85a3:0000:0000:8a2e:0370:7334 |
| **Packet size** | 576 bytes required<br>fragmentation optional | 1280 bytes required<br>no fragmentation |
| **Packet header** | includes options up to 40 byte | extension headers used for optional data |
| | include checksum | does not include checksum |
| **Address configuration** | Manual or via Dynamic Host Configuration Protocol (DHCP) | Manual, via Stateless address autoconfiguration (SLAAC), or via DHCPv6 |
| **Security features** | Security is dependent on applications, and the Internet Protocol Security (IPSec) is optional | IPSec is built into the IPv6 protocol |
| **Interoperability & mobility** | Very constrained interoperability and mobility | Designed to provide interoperability and mobility capabilities |

**Table 1:Side by side comparism of IPV4 and IPV6**

## X ANALYSIS OF FINDINGS FROMTHE LOCAL INDUSTRIES IN JAMAICA

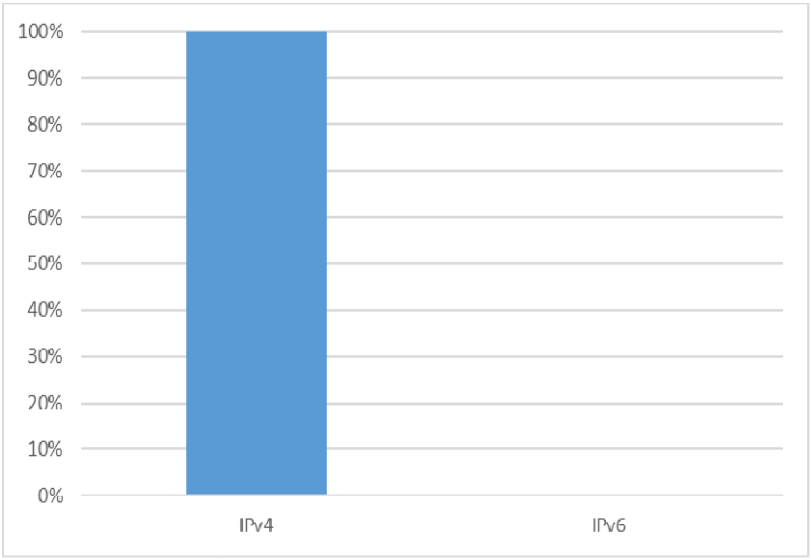


**Figure 8: Bar Chart showing the percentage of the Internet Protocols being utilized by CWC Jamaica to offer services to Jamaica.**

Currently, Cable &Wireless Communications LTD, Jamaica is solely using IPv4 to transmit data to its customers. As the chart above shows, 100% of their services are operated on IPv4 infrastructure. Even with the depletion of IPv4 addresses, the company has been sufficiently able to carry out their services with little to no limitations. As of now they see no problem with using IPv4 as the mechanisms they have employed have curtailed any issues they would have encountered. However, the IPv4/IPv6 compatible at their core and the international edge of their network. The graph below gives a representation of IPV4/IPV6 core edge compatibility.

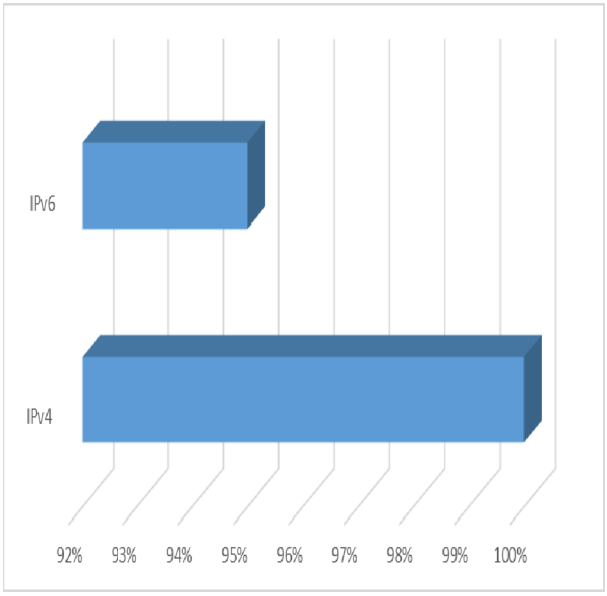


**Figure 9: Graph shows CWC Jamaica's IPv4/IPv6 compatibility at core and edge devices.**

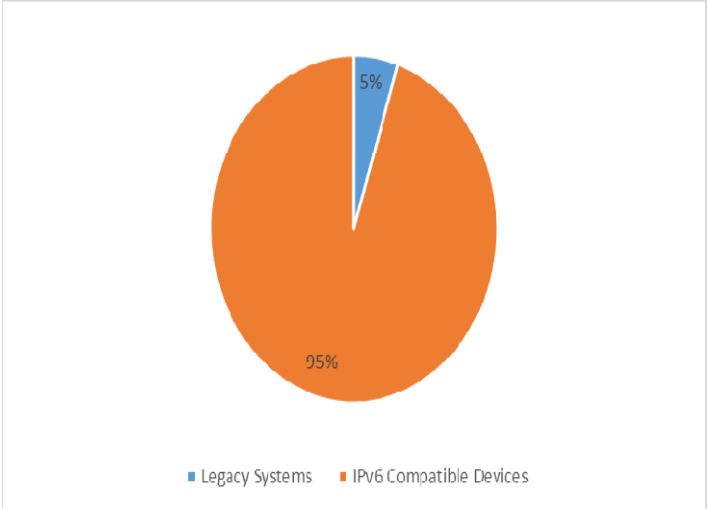


**Figure 10: Pie Chart showing CWC Jamaica's hardware compliance towards IPv6 compatibility.**

From the information we gathered, CWC Jamaica claim to be 95% ready or better when it comes on to their hardware being compatible for IPv6. Mr Pink of CWC, did mention that there is however a few old equipment that will be replace and upgraded in short order.

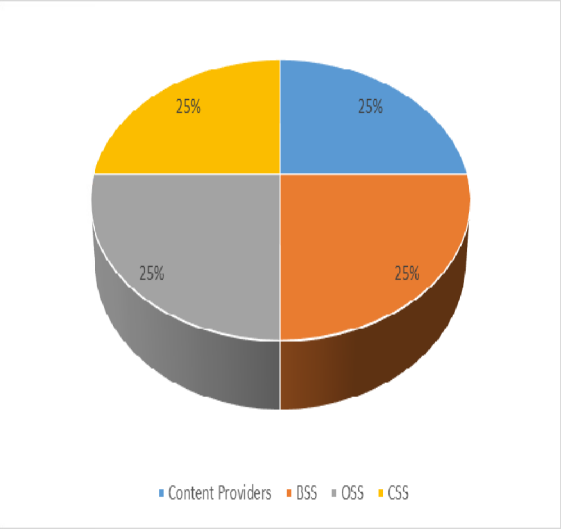


**Figure 11: Pie Chart showing the challenges faced by CWC in their transition to IPv6.**

CWC Jamaica broke down the biggest challenges they face in transitioning to IPv6 into four categories. The first challenge highlighted is that the large content providers such as Google, Facebook, Netflix, YouTube and others are slowly migrating.

Only 40% of America's traffic is on IPv6, if there were to migrate to IPv6 then they fear that only 40% of the internet's content would be available to their users. The other challenges include their Business Support Systems (BSS), Operations Support (OSS) System and Customer Service Systems (CSS) which accounted for the other 75% of their transitioning challenge. Other local industry such as digicel is yet to consider migrating to IPV6, because many of their customers still operate at platform of IPV4.

## XI SECURITY CONCERNS, POTENTIAL RISK AND MITIGATION TECHNIQUES REGARDING IPV6 TRANSITION IN JAMAICA

| Security Concerns | Potential Risks | Mitigation Techniques |
|---|---|---|
| Elimination of NAT | Hackers being able to pinpoint a specific machine within an organization | Educating employees and end users. |
| Device bypass via tunnelled traffic | Internal contents are shielded from transit network, removing the ability to use certain traffic control features. | Dual Stack where you can, tunnel where you must. |
| Lack of IPv6 training/education | Spending more time and money on security further down the road to plug security holes. | Invest time and money in IPv6 security training upfront before deploying. |
| Security policies in IPv4 and IPv6 | Weak IPv6 security knowledge would produce weak IPv6 security policies. | Depth of IPv6 security policies should equate to that of their IPv4 counterparts but much wider. |

**Table 2: Table showing security concerns, potential risk and mitigation techniques regarding IPv6 transition in Jamaica.**

The table gives summarization of the security concerns being thought out by CWC Jamaica. Elimination of NAT will drastically increase the number of public addresses being routed on the internet. Due to the nature of tunnelling, packets can make their way inside the network without proper authentication as contents are concealed.

Lack of IPv6 education is another concern as it is a fairly new technology and technicians may not have sufficient knowledge of the protocol. Lastly, security policies for IPv6 must have greater depth and width when compared to IPv4.

## XII IPV6 IN THE CARIBBEAN AND LATIN AMERICA

Trinidad is among the top 20 countries using IPv6 withabout 20,860users accessing IPv6 content. Other countries include Bolivia, Brasil, Ecuador and Perú

## XIII CONCLUSION

The transition from IPv4 to IPv6 in Jamaica will be a timely and costly one as both hardware and software must merge in order for compatibility to be nurtured which will take a substantial amount of resources and development and which will also take an extensive amount of time and money.

IPv6 will take over from IPv4 as IP addresses are running out which will invocate IPv6 being the main IP protocol [2]. IPv6 is slowly but surely gaining popularity and being more global. The benefits which it proposes can be seen as one that will shape the future into a better one for everyone providing more flexibility and features [13].

Concurrence of the two adaptations (IPv4 and IPv6) will not happen for quite a while and it is important to break down different system situations. The author found that each change procedure amongst IPv4 and IPv6 involves some security risk.

This implies that crossing over between conventions is required; all the same guaranteeing against security dangers, thus complicating the procedure considerably. Regardless of these difficulties, relocating to IPv6 is important because of the restricted IPv4 address space.

Based on the table 1 above, IPV6 will provide trillions and trillions address spaces as against billions of address spaces provided by IPV4 in Jamaica.

In Jamaica, with increase in populations and with corresponding increase in computers and cellular devices used in primary, secondary and tertiary institutions, it will be advisable for the local internet service providers (ISP) such as digicell and flow to consider migration to IPV6. Migrating to IPV6, will also be a solution to the forthcoming logistic hub of Jamaica.

Among all, additional investigation is required to deal with this migration and to recognize issues and answers for a smooth transitio

## REFERENCES

[1] E.I. Editors, (2010), November 8).Plan for IPV6 beforeIPV4 Addresses Run Out. Retrieved from Enterprise Innovation: www.enterpriseinnovation.net

[2] N.Gilligan, (2005). Basic Transition Mechanisms for IPv6 Hosts and Routers.

[3] M. M. Bhuiyan, (2015). An Efficient Approach of Converting an IPv4 Network to IPv6 Network through Dynamic Enhance Interior Gateway Routing Protocol.

[4] S.Kalwar, N. Bohra, & A. A. Memon, (2015). A survey of transition mechanisms from IPv4 to IPv6 — Simulated test bed and analysis. 2015 Third International Conference on Digital Information, Networking, and Wireless Communications (DINWC), 30-34. doi:10.1109/dinwc.2015.7054212

[5] F.Siddika, M. A.Hossen, & S. Saha, (2017). Transition from IPv4 to IPv6 in Bangladesh: The competent and enhanced way to follow. 2017 International Conference on Networking, Systems and Security (NSysS), 174-179. doi:10.1109/nsyss.2017.7885821

[6] T.Peter, H.Pavol& D. Lukas, (2016). Implementation and evaluation of IPv6 to IPv4 transition mechanisms in network simulator 3. 2016 International Conference on Systems, Signals and Image Processing (IWSSIP), 1-4. doi:10.1109/iwssip.2016.7502745

[7] T. D. Hoang, (2015). Deployments of IPV6 over IPV4 Network Infrastructure

[8] F.Gont (2011). Results of a Security assessment of the internet protocol version 6 ( ipv6 ). DEEPSEC 2011 Conference (p. 8/41). Fernando Gont.

[9] R.Cannon (2010).Potential Impacts on Communications from. Federal Communications Commission, 15-25.

[10] J.C. Smith, (2011). IPv6 Security Basics.SMU School of engineering, 20-28.

[11] A.S. Ahmed, R. Hassan,&N. E. Othman,(2014). Security threats for IPv6 transition strategies: A review. 2014 4th International Conference on Engineering Technology and Technopreneuship (ICE2T), 83-88. doi:10.1109/ice2t.2014.7006224

[12] L Hong, (2014). Modeling and Analysis of IPv4 to IPv6 Address

[13] E.Durda, & A. Buldu, (2010).IPV4/IPV6 Security and Threat Comparisons.Procedia Social and Behavioral Sciences 2, 5 7-5288.