ISSN No:-2456-2165

Analysis and Optimization of IPv4 and IPv6 Transition Technologies

Amusu Mary Iniobong, Akinrinlola Ibitoye Akinfolajimi & Odesanya Oluwafunsho Idowu
Department of Computer Science, Lagos State Polytechnic, Ikorodu, Lagos, Nigeria

Abstract:- IPv4 has reached the end of its addressable space, necessitating the deployment and execution of IPv6 protocols. Although IPv6 significantly increases addressable space in comparison to IPv4, IPv4 has not been completely phased out due to the difficulty and cost of phasing out the protocol. As such, IPv4 and IPv6 must coexist. As a result, there is a need for research into transition mechanisms that enable standards to communicate with one another. This research examined many research publications, studied transition technologies and their performance in test circumstances, compared technologies using measurement metrics, and made inferences about the selection of transition technologies. Additionally, it discusses several transition mechanisms, their advantages and disadvantages as measured by various metrics, and how these mechanisms might be adjusted.

Keywords:- *IPv4, IPv6, Addressable Spaces, Transition Mechanisms.*

I. INTRODUCTION

As IPv6 adoption increases, it is critical that network operators transition to single-stack IPv6 core and access networks to simplify network design and operation. The IPv4 address space is rapidly approaching exhaustion, necessitating the development of a new and evolving protocol to address the address space shortage. This is why the new IPv6 protocol was designed, which provides a larger address pool due to its usage of 128-bit address sizes. This means that there are many more addresses available than there are Internet-connected devices, ensuring IPv6's future viability and enabling considerable advancements in internet technology. Additionally, IPv6 eliminates the need for Network Address Translators (NAT), as each device is issued a unique IP address. Among the main enhancements built into IPv6 are address auto-configuration, enhanced security, increased Quality of Service (QoS), and a new header format [3]. Due to this limitation of address space, organizations have recognized the need to migrate their networks to IPv6.

Because IPv6 and IPv4 are incompatible protocols, network users are unable to connect across networks. As a result, a transition mechanism(s) is required to provide a smooth migration and to allow IPv6 hosts to traverse across IPv4 networks or connect to IPv4 hosts. The following are the transition conditions stated by the original IPv6 specification's designers (RFC 1752):

- Is it straightforward to update IPv4 hosts to IPv6 without causing network disruption, and can this be accomplished without requiring an upgrade of other routers or hosts on the network?
- When adding new IPv6 hosts, no dependencies on other hosts or routing infrastructure exist.
- Both IPv4 and IPv6 addresses can be used concurrently without requiring all nodes to be upgraded simultaneously.
- Similar to installing new IPv6 nodes, upgrading IPv4 infrastructure to IPv6 requires minimal planning.

There have been a variety of suggested and widely used transition technologies, including dual stack and tunnel techniques. Due to the prevalence of IPv4-based Internet services, it is critical to understand that the shift from IPv4 to IPv6 may take years, which implies both protocols will coexist [11].

The IPv4 (Internet Protocol version four) and IPv6 (Internet Protocol version six) are the fourth and sixth version of the Internet Protocol standard based internet working methods. IPv4 was first deployed in 1982 on SATNET (Atlantic Satellite Network) and uses a 32-bit addressing system.

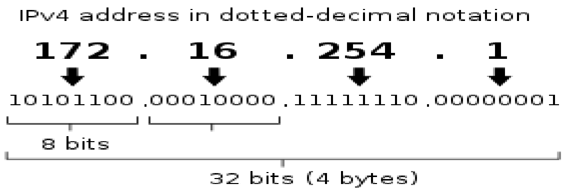

Fig. 1: IPv4 Address [1]

The Internet address space, which is maintained by the Internet Assigned Numbers Authority (IANA) and five regional Internet registries (RIRs), was exhausted in 2011 when the final 4.3 billion addresses were formally allocated, resulting in the launch of IPv6.

The Internet Engineering Task Force (IETF) created IPv6 as a replacement for IPv4. In 2017, it became a full internet standard. Unlike its predecessor, IPv6 has a 128-bit addressing system and cannot interact directly with the IPv4 Standard.

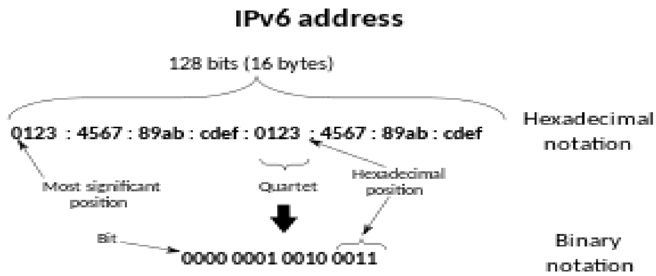

Fig. 2: IPv6 Address [1]

IPv4 addresses are 32bits in quad-dotted notation, represented as decimal values of four octets, ranging from 8bit to 32bit per number. The early 1990s overhaul of the system utilizing a classless network architecture did not prevent the address system from exhausting. The IANA allocated the final unassigned address blocks to the RIRs in February 2011. In 2019, RIPE NCC (Réseaux IP Européens Network Coordination Centre) reached its official IPv4 address allocation limit. When compared to IPv4, IPv6 offers the following benefits: auto-configuration, improved multicast routing, simplified administration, flow labeling, built-in authentication and privacy support, and more. Changing from one addressing scheme to the other can be problematic, necessitating the use of both addressing schemes concurrently. This is referred to officially as Transition Technologies.

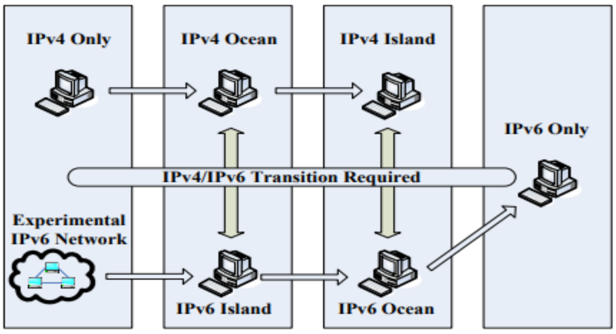

Fig. 3: Transitioning from IPv4 and IPv6 [2]

Transitioning technologies aid in the resolution of issues such as the requirement for scalable routing tables, the delay associated with the defragmentation process in intermediary devices, and NAT (Network Address Translation) translation. When a network is transitioned, the following approaches are typically used: Dual Stack, Encapsulation, Single Translation, and Double Translation.

A. Dual Stack Transition Mechanism (DSTM)

The Dual Stack Transition System (DSTM) is a mechanism for communicating and interoperating across IPv6 and IPv4 networks. A dual stack device is one that has a network interface capable of communicating with both IPv4 and IPv6. Dual stack requires both devices to support both IP versions and to be capable of handling both concurrently. While it is effective, it is not appropriate for big networks.

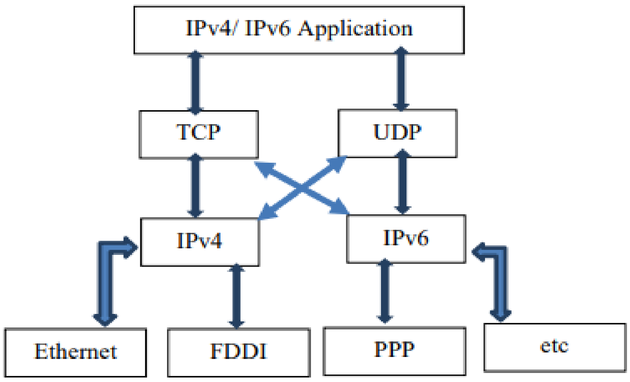

Fig. 4: Dual Stack Transition [6]

A. Encapsulation

Encapsulation is a transition method that uses the header of another domain to encapsulate packets arriving from a specific domain between the two domains. After being received, the encapsulated packets are de-encapsulated between the two domains. A formal description is that the transition mechanisms in this category encapsulate packets arriving from IPvX-specific domains using the IPvY header at the boundary between IPvX- and IPvY-specific domains. Then, at the boundary between an IPvY-specific domain and another IPvX-specific domain, the IPvY-encapsulated packets are de-encapsulated before being received by the nodes of the latter domain [8]. Manual Tunneling, 6to4, Teredo, ISATAP, 6rd, Tunnel Broker, DS-Lite, MAP-E, and Lw4o6 are only a few of them.

B. Unified Translation

Single Translation employs a process known as reverse translation. It converts packets originating from a specific domain to packets heading to that domain and vice versa at the domain boundary. NAT-PT, SIIT, and Stateful NAT64 are all examples, as is DNS64.

C. Concurrent Translation

Double Translation is a type of transition mechanism that converts packets from one IPvX-specific domain to packets that pass through the network operator's IPvY-specific core domain and then to another IPvX-specific domain. The first translation occurs at the boundary of the first IPvX domain and the IPvY core domain, whereas the second occurs at the boundary of the IPvY core domain and the second IPvX domain [8]. 464XLAT and MAP-T are two examples of these processes.

The majority of performance analysis of transition approaches is conducted using industry-standard performance indicators such as Round Trip Time (RTT), Throughput, CPU Utilization, Packet Loss, and Latency.

- Throughput is the rate at which data is transferred from a source. It is used to determine a network's performance. The higher the throughput, the more performance in the network.
- Round Trip Time (RTT), also known as Round Trip Delay, is the time it takes for a signal to be sent and confirmed as received.
- CPU utilization is a measure of a computer's performance. It refers to the amount of time the CPU spends processing data.
- Packet Loss happens when one or more data packets are not delivered to their intended destination.
- Latency is a term that refers to the time it takes for data to travel through a network.

II. REVIEW OF RELATED WORKS

This section evaluates various researches on IPv6 and identifies areas that deserve additional research. Despite IPv6's embryonic state, it has become a subject of much research; yet, there are still gaps in knowledge, some of which may have been generated by this research paper.

A. A Survey of IPv6 Transition Technologies' Performance Analysis

This research examines several papers on transition technologies using multiple measures, discusses research findings on the technologies, and provides advice for feasible technique. The research explored the many classifications of transition technologies, including their disadvantages, and demonstrated a performance analysis of the various transition technologies, identifying the best and worst performing technologies based on the measuring criteria. The article concluded that selecting the optimal technology for migrating is a difficult subject, and the solution varies according to the situation and type of network. Finally, the report offered principles for standardized benchmarking technologies. [8]

B. Performance Analysis of IPv6 Transition Technologies and Transition Methods

This article examined the performance of IPv6 transition technologies through the use of mathematical models for transition strategies. The performance research was conducted on a real network environment with a single user and varying the number of users while measuring RTT and throughput. Dual Stack, Manual Tunneling, ISATAP, and 6to4 were used in the experiment. Manual Tunneling and 6to4 performed best in terms of throughput and RTT, whereas Dual Stack had the lowest throughput and highest RTT. [7]

C. Performance Analysis of Three IPv6-IPv4 Transition Mechanisms: Dual Stack, Tunneling, and Translation

This article examined the performance of three IPv6 security and header format transition techniques. The research analyzed the performance of Dual Stack, 6to4 and NAT-PT using packet tracer as a simulator. The research employed measures to determine delay, throughput, and packet loss. At the conclusion of the research, 6to4 had the best performance, with the lowest latency, the least packet loss, and the maximum throughput. NAT-PT performed the worst on these measures. Due to the packet tracer's limitations, this research's comparison analysis is limited to a few application layer services. [6]

D. Evaluation of IPv4/IPv6 Transition Techniques

This research article compares the performance of the most widely used tunneling and dual stacking techniques. Three automatic tunneling protocols were evaluated for tunneling: 6to4, 6rd, and ISATAP. Additionally, native IPv4 and IPv6 were compared to ascertain the differences and modifications brought about by the new protocol. The experiment was conducted in GNS3 and included a variety of performance measurement methodologies, including RTT, throughput, packet loss, and CPU utilization. The research produced performance graphs and charts illustrating the test bed's outcomes. It established that Dual Stack and Sixth are superior approaches. Additionally, the article analyzed native IPv6 and IPv4 using the same metrics and concluded that IPv6 performed significantly better than IPv4. [4]

E. Benchmarking Tools for Analytical Performance Evaluation of Native IPv6 and Several Tunneling Techniques

This article compares the performance of several tunneling techniques, including ISATAP, 6to4, 6rd, and Teredo. The research analyzes performance using a client/server model and Iperf, which is based on the client/server model. Cisco 2811 was used, along with Cisco IOS version 15.1 (4) M6. The research found that ISATAP performed the best of the tunneling approaches, while Teredo performed the least well, however there was no difference in performance between ISATAP, 6to4, and 6rd. [5]

F. IPv6 Analysis through Transition Technologies and Security Attacks

IPv6 delivers more address space, improved address design, and increased security than IPv4 does, according to these academics. Different transition strategies, such as dual stack networks, tunnels, and translation technologies, can be utilized to migrate from IPv4 to IPv6. Network security is a critical component of all of this and hence deserves specific attention. This article compares and contrasts two transition technologies: dual stack and tunnel. Cisco Packet Tracer and GNS3 are used to implement both technologies. Additionally, their work analyzed IPv6 security issues in order to identify the most common vulnerabilities and security difficulties encountered throughout the switch. Finally, the authors created and implemented dual stack, automated, and manual tunneling transition mechanisms, analyzing performance and comparing it to native IPv4 and IPv6 networks using the Riverbed Modeler simulation tool. [9]

G. Consider the Advantages and Disadvantages of IPv6 Transition Technologies for IPv4 as-a-Service

Numerous IPv6 transition solutions have been developed to deliver IPv4-as-a-Service (IPv4aaS) to clients of ISPs with an IPv6-only access and/or core network. Each of these technologies has a number of pros and disadvantages, and based on the network operator's existing topology, capabilities, strategy, and other preferences, one of these technologies may be the most suited solution. This study investigates the five most widely used IPv4aaS technologies from a variety of perspectives in order to offer network operators with an easy-to-use reference for determining the technology that best meets their objectives. Additionally, five potential IPv4aaS solutions were explored, and the following IPv6 transition technologies were analyzed, with some of their most significant properties described. [10]

- 464XLAT [RFC6877]
- Dual Stack Lite [RFC6333]
- lw4o6 (Lightweight 4over6) [RFC7596]
- MAP-E [RFC7597]
- MAP-T [RFC7599]

III. METHODOLOGY AND RESULTS

This research is conducted in the form of a survey and analysis of various transition technologies and their short comings. According to a survey of transition strategies, the following techniques are the most widely used and optimized, with few drawbacks. Table 3.1 below summarizes the research papers reviewed, as well as the methods, metrics, and traffic generation techniques employed in the articles.

Research Papers	Test Method	Transition Technologies	Metrics	Traffic Generation Method
[7]	Real test-bed Simulation (GNS3& OPNET)	Dual Stack Manual Tunneling ISATAP 6to4	Round Trip Time (RTT) and Throughput	Poison Distribution by MATLAB
[6]	Simulation (Packet Tracer)	Dual Stack 6to4 NAT-PT	Latency, Throughput and Packet Loss	Packet Tracer PDU Generator
[4]	Simulation (GNS 3)	Dual Stack 6to4 ISATAP 6rd	RTT, Throughput and CPU Usage	GNS 3 Packet generator
[5]	Real test-bed	ISATAP 6to4 6rd Teredo	RTT and Throughput	Propriety for RTT and Iperf for Throughput

Table 1: Methods used in the Research papers under survey

IV. RESULTS

In [4], the table below is the result of the analysis simulated on GNS3 simulator.

Transition Techniques	Throughput	CPU Utilization	Packet Loss
6to4	70.1Mbs	11-12%	230.9ms
ISATAP	71.96Mbs	11-13%	221.95ms
6rd	84.4Mbs	10-12%	196.8ms
Dual Stack	82.2Mbs	17-19%	175.2ms

Table: 2 Comparative Analysis of Transition Techniques [4]

The test-bed of this analysis consist of four Cisco 7200 series routers and used OSPFv3 as routing protocol. Dual Stack according to this analysis performed the best with the highest CPU utilization and the lowest packet loss. Although from this table Dual Stack performed best it has a major limitation and high latency and these results in Happy Eyeballs. Happy Eyeballs also known as Fast Fallback is an algorithm which makes dual stack application able to connect users using IPv4 and Ipv6 to connect to the internet it addresses the problem of unresponsive networks commonly associated with Dual Stack. However, even with the optimization Dual Stack is still complicated as both protocols are expected to be in order, making it vulnerable to security threats.

Sookun et al. [4] evaluated Teredo, 6to4, ISATAP, and 6rd using benchmarking tools. The test-bed used Cisco 2811 with the Cisco IOS version 15.1(4) M6 and showed the results in tables. ISATAP performed the best in terms of throughput and RTT while Teredo had the worst performance of the tuning techniques.

In [6], Dual Stack, 6to4 and NAT-PT were analyzed using Cisco Packet Tracer and ICMP packets being transferred. The results were represented with charts of each performance metric. The results were then deduced in the table below.

Transition Techniques	Throughput	Packet Loss	Latency
Dual Stack	Medium	Medium	Medium
6to4	High	Low	Low
NAT-PT	Low	High	High

Table 3: Analysis of Transition Techniques [6]

From the table, NAT-PT performed the poorest while 6to4 had better performance.

In [7], the table below shows the result of the analysis carried out.

Transition Techniques	Throughput (Bytes/s)	RTT (ms)
Dual Stack	845	77.1
Manual Tunnel	991	65.3
ISATAP	938	70.3
6to4	951	70.5

Table 4: Analysis of Transition Techniques [7]

From the table, Dual Stack has the lowest average throughput in bytes and the highest RTT (maximum delay). This research shows Manual Tunnel has the best performance in terms of throughput and RTT.

V. DISCUSSION

As the survey indicates, no transition technique is optimal for all network environments and circumstances. As a result, the adoption of transition technology is critical. The conclusions drawn from the analysis of transition technologies are strongly dependent on a variety of variables, among which are the following:

- The tools used in the test i.e. the simulator and software equipment.
- The type of test.
- The number of iterations in the test
- The network topology.

These elements contribute significantly to the experiment's outcome but are not exhaustive. Thus, depending on the parameters listed above, the optimal transition technique may change.

VI. CONCLUSION

Numerous transition strategies for communication between IPv4 and IPv6 have been developed throughout the years. These technologies have limitations in certain areas that have been optimized numerous times. This has contributed in mitigating the impact of issues with communication between IPv4 and IPv6 prior to the full adoption of IPv6. This report reviewed previous research, assessed transition technologies and their performance in test circumstances, comparing technologies using measurement metrics and drawing conclusions on the selection of transition technologies.

REFERENCES

[1.] https://www.google.com/url?sa=i&url=https%3A%2F%2Fcommons.wikimedia.org [1]

[2.] Mahadevan, V., Ali, A. (2010). Why is IPV4 still in existence? [2]

[3.] Fatah, F.N., & Suhendra, A. (2013). Performance Measurements Analysis of Dual Stack. Proceedings of The Conference on Advances in Information Technology (pp. 100-107). [3]

[4.] Sookun, Y., Bassoo, V. (2016). Performance analysis of IPv4/IPv6 transition techniques. In 2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech) (pp. 188-193). IEEE.[4]

[5.] Sans, F., Gamess, E. (2013). Analytical performance evaluation of native IPv6 and several tunneling techniques using benchmarking tools. In 2013 XXXIX Latin American Computing Conference (CLEI) (pp. 1-9). IEEE.[5]

[6.] Hossain, M. A., Podder, D., Jahan, S., Hussain, M. (2016). Performance Analysis of Three Transition Mechanisms between IPv6 Network and IPv4 Network: Dual Stack, Tunneling and Translation. International Journal of Computer (IJC), 20(1), 217-228.[6]

[7.] Altangerel, G., Tsogbaatar, E., Yamkhin, D. (2016). Performance analysis on IPv6 transition technologies and transition method. In 2016 11th International Forum on Strategic Technology (IFOST) (pp. 465-469). IEEE.[7]

[8.] Al-hamadani, A. T. H., Lencse, G. (2021). A Survey on the performance analysis of IPv6 transition technologies. Acta Technica Jaurinensis. [8]

[9.] Alzaid, W. Issac, B. (2016). Analysis of IPv6 through Implementation of Transition Technologies and Security Attacks. International Journal of Business Data Communications and Networking. 12. 36-62. 10.4018/IJBDCN.2016010103. [9]

[10.] Lencse, G., Martinez, J. P., Howard, L., Patterson, R., Farrer, I. (2020). Pros and cons of IPv6 transition technologies for IPv4aaS. active Internet Draft, 2020.[cited 2019-11-15] URL https://tools. ietf. org/id/draft-lmhp-v6opstransition-comparison-02. html. [10]

[11.] Hassan, R., & Ahmed, A. S. (2013). Avoiding Spoofing Threat in IPv6 Tunnel by Enhancing IPSec. International Journal of Advancements in Computing Technology, 5(5), 1241–1250.[11]