International Journal of Core Engineering & Management
Volume-6, Issue-07, 2020 ISSN No: 2348-9510

BEYOND IPV4: WHY ENTERPRISES AND SERVICE PROVIDERS MUST EMBRACE IPV6 FOR THE FUTURE OF NETWORKING

Nikhil Bhagat, Principal Network Engineer
Independent Scholar, Network Engineering
Aurora, Colorado, USA
nikhil.bhagat90@gmail.com

Abstract

With the increase in evolution of internet and its capacity needs, the limitations of IPv4 have surfaced. Rapid growth in connected smartphones, IoT devices, and other smart devices have taken up all the available IPv4 address space, leaving enterprises and service providers in search of alternatives. IPv6, which was coined as a long-term solution for IPv4, offers far more addresses and several other advantages such as better network performance, security, and simplified routing. This paper covers how IPv4 has changed, its limitations, and the ever-increasing struggles that those organizations who continue to leverage it still experience. The paper discusses how IPv6 overcomes these limitations by removing Network Address Translation (NAT), allowing true end-to-end connectivity as well as adding mandatory security measures with IPsec. Additionally, this paper describes why enterprises and service providers should embrace IPv6, focusing on the long-term advantages of scale, cost reduction, and network efficiencies. It also describes the migration strategies like dual stack deployment and tunneling that could allow a seamless transition from IPv4 to IPv6. By considering these aspects, this paper has made a strong case for why IPv6 should be viewed not just as a technical necessity, but as a strategic need for organizations seeking to future proof their networks.

Index Terms – ***IPv4, IPv6, Migration Strategies, Dual-Stack, Tunneling, Network Address Translation.***

I. INTRODUCTION

The Internet Protocol (IP) plays a key role in making the internet work, defining special addresses used for devices to send messages over networks. IPv4 has been the internet connectivity core since its launch to allow communication across devices around the globe [1]. Yet the explosive increase of internet traffic, devices, and apps has consumed up the IPv4 addresses available and there are a growing demand for a more scalable and secure protocol. IPv6, which was created to replace the shortcomings of IPv4, offers an alternative with its large address space and richer features [2]. Nevertheless, IPv6 adoption is still lagging in enterprises and service providers because of migration barriers, cost and interoperability. This paper attempts to show why IPv6 should be taken seriously and will examine the value of the change and outline solutions to facilitate its smooth implementation.

II. EVOLUTION OF IPV4 ADDRESSES IN NETWORKING

IPv4 was introduced in 1981 as a member of the TCP/IP protocol suite that standardized communication over computers networks [3]. IPv4 provides 32-bit address space and approximately 4.3 billion individual addresses [3]. By the time it was devised, that number was considered enough to link the entire world. But the growth that followed, with devices from laptops to smartphones, IoT appliances to smart home systems, has far exceeded what had been envisioned.

Back in the early years of the internet, network address translation (NAT) was a way to extend the life of IPv4 addresses [4]. As NAT enabled many computers on a private network to use the same single public IP address, it alleviated the address crisis in the near future. NAT came with its own challenges though, from end-to-end communication challenges to security and performance issues.

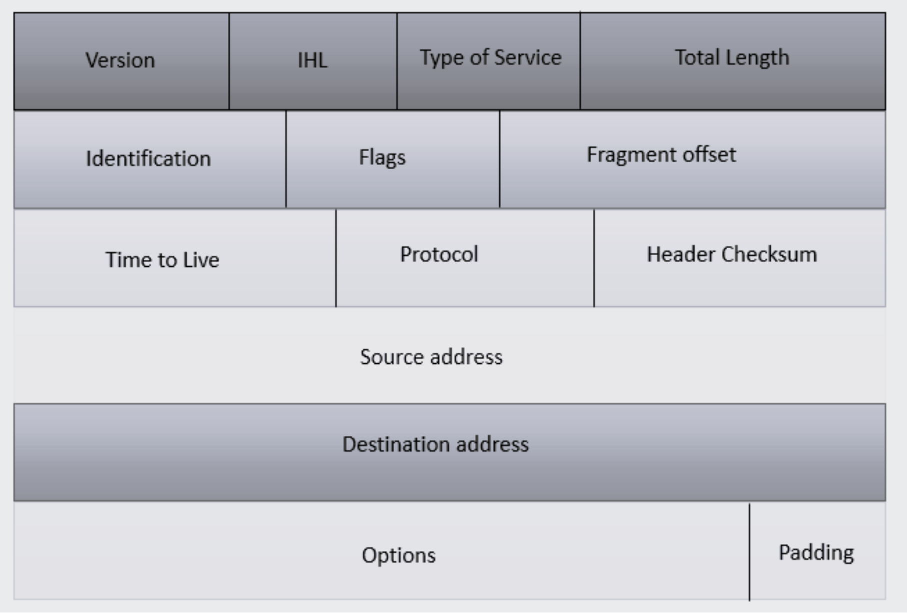

Fig. 1. IPv4 packet header [5]

As the internet expanded, there was even more uncertainty about the IPv4 sustainability. Regional internet registries (RIRs) started rationing IP addresses allocations and IPv4 address exhaustion finally became a reality in 2011. IPv4's limits were starting to emerge, and a successor that could scale with the future of the internet was on the horizon.

III. CHALLENGES WITH IPV4 AS THE INTERNET CONTINUES TO EXPAND

The IPv4 bottleneck doesn't stop with the address scarcity. As the internet stretches ever wider, several challenges have appeared that impact performance, security, and scalability of IPv4-based networks:

A. Address Exhaustion in IPv4

One of IPv4's biggest challenges is its limited address space. IPv4 is limited to 4.3 billion addresses, which does not allow for an increase in the number of devices that need unique IPs. Because of the lack of address space, we have to excessively rely on protocols such as NAT which creates complexity and degrades true end-to-end connectivity [2].

B. Network Complexity

For those that can't use IPv4 but want a workaround, companies use techniques like private addressing and NAT. Even though it is effective in delaying the addressing problem, these solutions are too costly to scale. Also managing a massive network using IPv4 needs excessive planning, complex subnetting, and the use of dynamic IP allocation protocols like DHCP [6].

C. Security Issues

IPv4 wasn't built with security in mind. Security protocols such as IPsec are possible but not mandatory, and require additional complex configuration. While NAT can potentially extend IPv4's lifecycle, it can also impede security protocols that needs true end-to-end connectivity [7].

D. Performance Limitations

The larger and more complex the networks, the more overhead that is involved with managing IPv4 networks. NAT translation, for example, adds latency, slowing performance on massive scale. IPv4's reliance on workaround solutions can also introduce inefficiencies that negatively affect the network speed and availability.

IV. INTRODUCTION TO IPV6

IPv6 was created by the Internet Engineering Task Force (IETF) as a long-term solution to address future problems with IPv4, which was launched in 1998 with a 128-bit address space that can hold up to 340 undecillion (3.41038) unique addresses [8]. This expansion ensures IPv6 is able to support an ever-increasing number of devices with internet connectivity for years to come. Besides its massive address space, IPv6 provides many additional benefits to networks for efficiency, security and performance. These features include:

A. Simplified Addressing

IPv6 does not require NAT and provides true end-to-end device communication. It also makes address assignment easy with automatic configurations such as Stateless Address Autoconfiguration (SLAAC) [9].

B. Enhanced Security

In contrast to IPv4, IPv6 is security optimized. IPsec is an integral part of IPv6, and it is the standard used to send messages encrypted and authenticated between hosts.

C. Improved Routing Efficiency

IPv6 reduces the size of routing tables with the Hierarchical Addressing Architecture of IPv6. It allows for more efficient routing, which decreases the strain on routers and improves network performance.

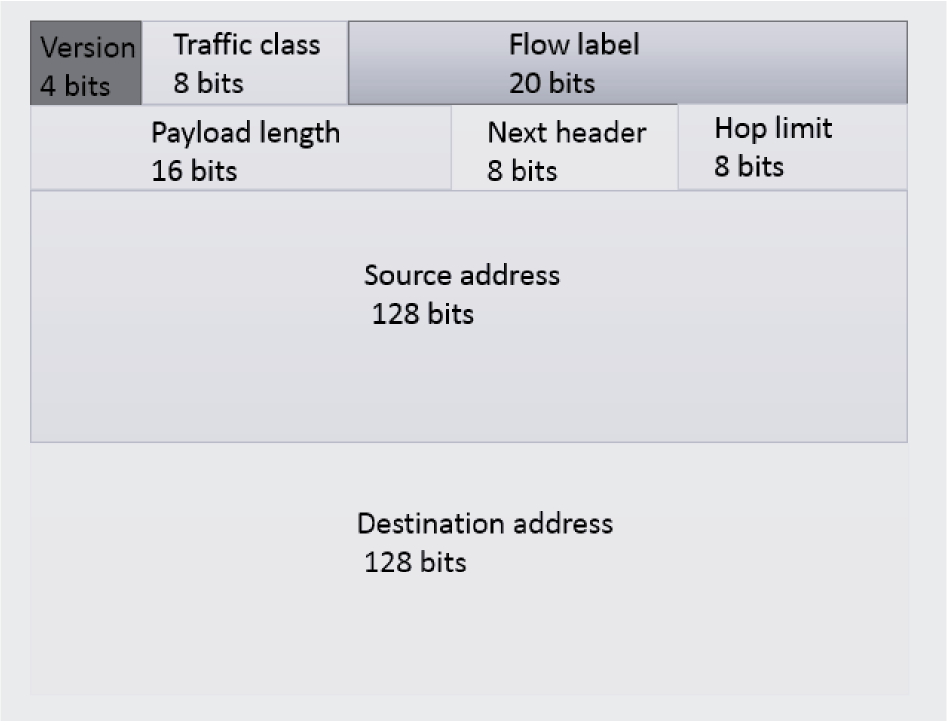

Fig. 2. IPv6 packet header [10]

V. HOW IPV6 CAN SOLVE IPV4 ISSUES

IPv6 corrects many of the problems of IPv4 in its own right:

A. Address Exhaustion

With the massive address space, it allows, IPv6 bypasses NAT and gives all devices a unique IP address of their own. This not only prevents address exhaustion but makes managing networks much easier by not requiring a workaround, such as private addressing [2].

B. Network Simplicity

Through the NAT elimination, IPv6 reduces the network's complexity. They talk directly to each other, and features such as SLAAC eliminate manual configuration or DHCP management so that network management and scaling are efficient.

C. Built-in Security

IPv6 requires IPsec which provides a robust layer of security for all communications. With IPv6, the organizations do not have to deploy additional security controls for end-to-end encryption and authentication.

D. Performance Improvements

IPv6's routing performance and simplified addressing structure reduces the overhead associated with large networks [11]. This means lower latency and more performance, particularly when deploying on a large scale.

VI. WHY SHOULD ENTERPRISES AND SERVICE PROVIDERS ADOPT IPV6?

The enterprise and the service provider can benefit immensely from IPv6 for various reasons, among them:

A. Future-Proofing

With the continuous growth in internet connected devices, IPv4 will never be economically sustainable. Businesses and service providers moving to IPv6 will have more space to manage future expansion without the constraints of address exhaustion [12].

B. Cost Savings

Moving to IPv6 can save substantial amounts of money over the long-term. There may be upfront costs to invest in hardware, software upgrades, and staff training but IPv6 efficiencies can cover these in the long term. As it eliminates NAT and other workarounds from managing networks, IPv6 frees IT teams of cumbersome administrative work.

Enterprises and service providers can expect fewer technical issues with address exhaustion, easier routing and more efficient address handling in IPv6, which means lower costs as network administrators won't be having to spend more time diagnosing address issues and managing complex configurations [13]. Besides, enhanced speed from IPv6 networks can help businesses perform better – especially for businesses with high-density, low-latency communications for their core applications.

IPv6 also means low-capex capital expenditure (CAPEX) for service providers in the long run [14]. ISPs with IPv4 typically want to invest in a complicated infrastructure to support NAT and maintain address availability. IPv6 eliminates this, so service providers are able to distribute resources more effectively and scale services with less restriction on available IP addresses.

C. Improved Security in IPv6

One of the major benefits of IPv6 is that it includes security by default. While IPv4 considers security as an optional extra, IPv6 was built for security from the beginning. The IPsec (Internet Protocol Security) requirement was made mandatory in IPv6 for extra protection by encryption and authentication. With IPsec, you can transmit information securely across the network without fear of interceptions or manipulations.

IPsec can be implemented; however, it is seldom deployed for IPv4 networks since it is complex and requires configuration [15]. For IPv6, IPsec is seamlessly implemented, making security embedded in the protocol. It's especially relevant for business and service providers who deal with highly confidential information, such as banking details, health data, and business secrets. IPv6's default security mechanisms add an additional layer of security for organizations to stay compliant with regulations and reduce cybersecurity vulnerabilities.

D. Better Performance

There are many improvements over IPv4 in IPv6 to optimize the performance of the network. One of the main enhancements is routing scalability. IPv6 has a more hierarchical and converged address space which reduces the size of routing tables and makes routing easy. This accelerates the processing of data packets and takes less pressure off routers which means fewer latency and faster performance on the network.

In addition, IPv6 removes the requirement of NAT which is a source of latency and slowness in large networks. NAT involves translating private to public IP addresses and adds overhead in each network transaction. IPv6 eliminates NAT, so that devices communicate directly end-to-end instead of between each other which speeds up and reduces network latency [16]. This in turn for providers gives the ability to provide faster and reliable internet connections and for enterprises can receive improved internal communication and critical applications performance.

E. Better Support for IoT and Emerging Technologies

This Internet of Things (IoT) is a huge part of future internet expansion as billions of devices will be interconnected in the coming years. IPv4 cannot cope with IoT devices with sophisticated throttling mechanisms such as NAT and that slows down scalability and leads to network inefficiencies. IPv6, because of its huge address space is well-suited to the IoT deployment, allowing direct connectivity for each device and easier communication.

IPv6 is also compatible with newer technologies like 5G, cloud and edge computing as well as other emerging technologies like IoT [17]. These platforms need scalable low-latency and high-security networks that IPv6 provides. IPv6-adopting enterprises and service providers will be in a better position to accommodate these advances and stay on the front lines of a dynamic technological world.

F. Regulatory Compliance and Global Adoption

IPv6 is being encouraged and required by governments and regulators worldwide with IPv6 being an increasingly popular technology in countries around the world. For instance, the US federal government has policies on how agencies should migrate to IPv6, and countries such as China are taking significant steps to introduce IPv6 into their networks [18]. Companies and service providers that deploy IPv6 will not only meet these new guidelines but also experience greater interoperability with worldwide networks.

Additionally, with more companies adopting IPv6 the IPv4 only business is at risk of being pushed aside. In an IPv6 trend that grows rapidly, companies that remain behind could experience compatibility problems, deterioration of performance and a lack of access to some services. With IPv6, enterprises and service providers can ensure that they are able to remain connected with global networking standards without causing interruption to their services.

VII. MIGRATION STRATEGIES FOR ENTERPRISES AND SERVICE PROVIDERS TO IPV6

The migration of IPv4 to IPv6 is an essential but challenging undertaking that needs careful planning, resource allocation and technical knowledge. Even though IPv6 provides a host of benefits – from an address space that's basically limitless to new security improvements – it presents its own challenges in technical and operational terms. For enterprises and service providers, a migration plan should take into account the specific network architecture, device support, and service need. Below are some of the most widely applied migration strategies that the organizations can use to implement IPv6 — dual stack deployment, tunneling, translation, training and support:

A. Dual-Stack Deployment

Dual stack is probably the most common and widespread IPv6 migration technique. In this way, IPv4 and IPv6 protocols are deployed together on the same network infrastructure. Each network device (router, switch, and end-user system) has both IPv4 and IPv6 addresses [19]. This approach lets companies still accommodate IPv4 traffic but gradually transition to IPv6. The beauty of dual stack deployment is that you can migrate over time. Service providers and enterprises do not need to completely rebuild their network at once, avoiding service disruption and compatibility risks. They can deploy IPv6 on a one-by-one basis, with isolated sections of the network, apps or services. This option is especially beneficial for organizations with large, complex networks, because it gives the organization a chance to evaluate IPv6 performance and compatibility before diving into a full transition.

However, dual stack deployment also comes with some disadvantages. It takes extra resources such as more processing power in network devices and adds complex routing configurations to run two protocols at the same time. Network engineering departments have to deal with IPv4 and IPv6 networks and it can become complex to administer. In spite of all these issues, dual stack is still a preferred strategy in most companies due to the flexibility and low risk.

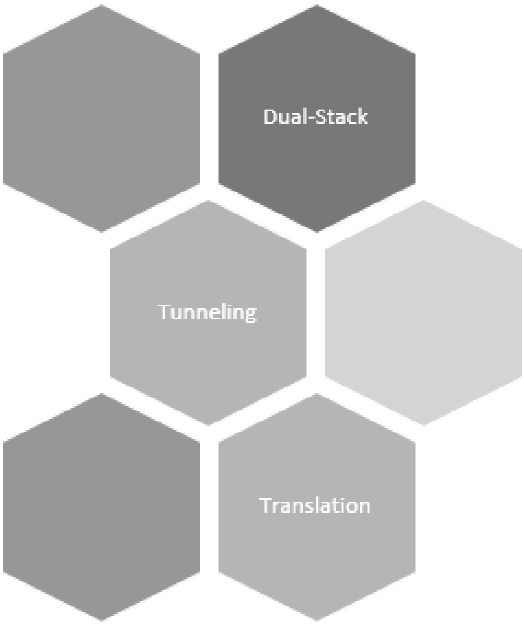

Fig. 3. IPv4 to IPv6 migration strategies

B. Tunneling migration strategy

Tunneling is another great approach for IPv6 migration. With tunneling, the IPv6 traffic gets wrapped into IPv4 packets to be delivered through a known IPv4 network. This is useful especially for those companies that have IPv6 islands within an overall IPv4 network or who wish to evaluate IPv6 traffic prior to fully adopting IPv6.

Tunneling can be performed through various tunnels including 6to4, Teredo, or ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) [20]. Each approach has their use cases and limitations, but they all provide the same basic thing: IPv6 communication in an IPv4 environment.

For instance, 6to4 tunneling would send IPv6 traffic through an IPv4 network without requiring you to specify a tunnel. This is especially important for those businesses who want to implement IPv6 on-demand without deploying new infrastructure. Teredo, meanwhile, is a tunneling protocol used on behind NAT (Network Address Translation) devices to help ensure IPv6 packets can be routed through even if NAT is applied.

Tunneling can be considered as a temporary step during migration and not a long-term solution. It has the added overhead of encapsulation, and this can negatively impact the network speed. What's more, tunneling doesn't give you all the features of a native IPv6 deployment — for example routing efficiency and security. Therefore, companies need to treat tunneling as a bridge not a long-term solution.

C. Translation migration strategy

During the migration, companies also have to frequently ensure IPv4 and IPv6 network interoperability. This is particularly true for businesses and carriers with legacy IPv4-only systems or those that must engage with IPv4-only partners or customers. This is where translation tools such as NAT64 or DNS64 come in. The translation technology NAT64 (Network Address Translation 64) translates IPv6 addresses into IPv4 addresses and allows devices with IPv6 to exchange address information with systems with IPv4 [19]. Similarly, DNS64 works by consolidating AAAA records for IPv6 addresses, which allows IPv6 hosts to convert domain names for IPv4-only services. These techniques allow communication between the two address spaces to flow easily, thus ensuring continuity of service throughout the migration [20].

Translation tools are good for making things compatible, but they aren't free of limitations. For example, NAT64 can create latency and complicate network management due to an extra overhead of addresses and protocol headers translation. Also, translation is not the solution for long-term; it doesn't solve IPv6 scalability and performance advantage but rather it is only a short-term bridge that allows organizations to transition until IPv6 takes over.

D. Training and Support

IPv6 migration is not only a technical challenge, it's also an organizational one. Among the biggest considerations for a seamless migration, making sure network engineering and security teams are properly informed on IPv6 architecture, setup, and troubleshooting is essential. There are many new features and operating models introduced with IPv6, like address autoconfiguration (SLAAC), neighbor discovery, IPv6 security features, like IPsec. Enterprises need to fund IPv6-related training courses for their network admins, engineers, and staff to gain the skills [21]. The training should be in both theory (IPv6 and IPv4) and practical experience (deploying and operating IPv6 networks). The training can also consist of vendor or standards organization certification courses that provide certification for IPv6 proficiency.

Further, businesses must provide the proper vendor support throughout the migration cycle. This includes working with network equipment vendors, ISPs and software developers to ensure compatibility and seamless integration. Most vendors offer IPv6 transition services for enterprises and service providers to manage the challenges of migrating – offering tools, consulting and technical assistance.

E. Phased Migration and testing

Regardless of what strategies are used, it is recommended for service providers and enterprises to use a phased migration model. Businesses and providers must start by choosing ineffective segments or services of the network for IPv6 deployment [22]. This gives them an opportunity to validate IPv6 capabilities and interoperability before scaling it into critical infrastructure. By migration progressively, issues can be fixed on a small scale with minimum impact to service.

It is during this phase, that organizations also have to perform thorough interoperability and stress tests for IPv6 and IPv4 devices to be able to work in conjunction. Such testing could be stress tests, performance tests, and security tests to ensure that the IPv6 network is strong enough.

VIII. CONCLUSION

Whether you want to switch to IPv6 or IPv4, IPv6 is an important strategic upgrade for business organizations and service providers that want their network to be secure for the future. As the demand for access to the internet grows globally, the limitations of IPv4 – primarily, the running out of addresses – makes it extremely difficult to scale, secure and make a network efficient. IPv6 with its vastly expanded address space and functionality provide a solution to all these issues, allowing enterprises to scale to the ever-increasing devices and services.

IPv6 has many other benefits that merely increase the address pool. It increases routing performance, makes managing networks easier with autoconfiguration and adds IPsec. For businesses and service providers, adopting IPv6 not only solves the existing network issues but prepares for future challenges of IoT, cloud services, and next-generation applications which will need the new agility and flexibility that IPv6 offers.

Yet, the IPv6 migration takes preparation, technical skills, and organizational commitment. There are possible options for gradual adoption, such as dual stack deployment, tunneling, translation, which will make IPv4 infrastructure easily adaptable to IPv6 without introducing significant change. In addition to that, investing in training and support is essential to make the move seamlessly and keep the network up-to-date.

As a conclusion, IPv6 isn't just an architectural evolution; it's a critical step for organizations wanting to stay relevant in an increasingly interconnected world. The advantages of IPv6, ranging from scale, performance, and security, makes it mandatory for businesses and ISPs to implement it. When properly managed and prepared, IPv6 migration will leave businesses well-prepared for the future of the internet.

REFERENCES

1. C. Lynch, "The Transition from TCP/IP to OSI," [Online]. Available: https://example.com.
2. L. Ladid, "IPv6 on everything: the new Internet IPv6 helps network architects address the IP address shortage, security, QoS, multicast and management," Network World, vol. 25, no. 14, pp. 35-40, July 2010.
3. P. L. Metzger and W. A. Simpson, "Network Working Group," IETF, RFC 1332, May 1992. [Online]. Available: https://www.rfc-editor.org/rfc/rfc1332.txt.
4. Mattern and C. Floerkemeier, "From the Internet of Computers to the Internet of Things," Informatik-Spektrum, vol. 33, no. 2, pp. 107-121, Apr. 2010.
5. "IPv4 Header Structure and Fields Explained," Computer Networking Notes, [Online]. Available: https://www.computernetworkingnotes.com/networking-tutorials/ipv4-header-structure-and-fields-explained.html.
6. L. J. Cox, L. Ricciulli, R. Woundy, W. Will, X. Zhou, and X. Zhou, "Managing the last eights: three ways forward for IPv6," Journal of Internet Technology, vol. 13, no. 5, pp. 215-225, Oct. 2015. [Online]. Available: https://xzhou@indiana.edu.

7. S. Bellovin, "Security problems in the TCP/IP protocol suite," Computer Communications Review, vol. 19, no. 2, pp. 32-48, Apr. 1989.
8. "RFC 2460: Internet Protocol, Version 6 (IPv6) Specification," IETF, Dec. 1998. [Online]. Available: https://www.rfc-editor.org/rfc/rfc2460.txt
9. S. Thomson and T. Narten, "IPv6 Stateless Address Autoconfiguration," IETF, RFC 2462, Dec. 1998. [Online]. Available: https://www.rfc-editor.org/rfc/rfc2462.txt.
10. "IPv6 Header Structure Format and Fields Explained," Computer Networking Notes, [Online]. Available: https://www.computernetworkingnotes.com/networking-tutorials/ipv6-header-structure-format-and-fields-explained.html.
11. M. V. Vineeth and R. Rejimoan, "Evaluating the performance of IPv6 with IPv4 and its distributed security policy," International Journal of Computer Applications, vol. 96, no. 1, pp. 32-40, June 2014.
12. O. Babatunde and O. Al-Debagy, "A Comparative Review Of Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6)," International Journal of Computer Science and Information Security, vol. 11, no. 3, pp. 65-72, Mar. 2013.
13. K. Zorbadelos, "Towards IPv6 only: A large scale lw4o6 deployment (rfc7596) for broadband users," Internet Research, vol. 25, no. 4, pp. 675-690, Aug. 2015.
14. I. Farrer, G. Lencse, R. Patterson, H. Lee, and J. Palet, "Pros and Cons of IPv6 Transition Technologies for IPv4aaS," IEEE Communications Magazine, vol. 54, no. 2, pp. 152-158, Feb. 2016.
15. R. Oppliger, "Security at the Internet layer," IEEE Internet Computing, vol. 5, no. 3, pp. 48-56, May-June 2001.
16. V. G. Cerf, "2012 Isn't the End of the World," IEEE Internet Computing, vol. 15, no. 1, pp. 96-99, Jan.-Feb. 2011.
17. H. Zhou, "Strategy and study of the transition technologies from IPv4 to TPv6," IEEE Transactions on Network and Service Management, vol. 12, no. 1, pp. 123-132, Mar. 2015.
18. A. S. Frankel, R. Graveman, A. J. Pearce, M. Rooks, F. Scholl, G. Raines, P. Jones, and R. P. Johnson, "NIST Special Publication (SP) 800-119, Guidelines for the Secure Deployment of IPv6," National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, Dec. 2010.
19. I. Hsieh and S. Kao, "Managing the Co-Existing Network of IPv6 and IPv4 under Various Transition Mechanisms," IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 95-104, May 2017.
20. S. Narayan and S. Tauch, "IPv4-v6 configured tunnel and 6to4 transition mechanisms network performance evaluation on Linux operating systems," International Journal of Network Security & Its Applications, vol. 12, no. 3, pp. 50-62, May 2014.
21. M. Tufail, "IP v6 - An opportunity for new service and network features," IEEE Communications Magazine, vol. 54, no. 7, pp. 112-119, July 2016.
22. S. E. Frankel, R. Graveman, J. A. Pearce, and M. Rooks, "Guidelines for the secure deployment of IPv6," National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, Dec. 2010.