I.J. Wireless and Microwave Technologies, **2023, 4, 11-17**
Published Online on August 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2023.04.02

IPv6 Migration Strategy Using Carrier Grade Network Address Translation

Dipti Chauhan*
Prestige Institute of Engineering Management & Research Indore, CSE
E-mail: diptichauhan09@gmail.com
ORCID iD: https://orcid.org/0000-0003-1665-7587

Received: 30 November, 2022; Revised: 19 January, 2023; Accepted: 03 March, 2023; Published: 08 August, 2023

Abstract: Due to the increased strain each new Internet-connected item puts on the IPv4 infrastructure, the emergence of additional Internet-connected places and devices has accelerated IPv4 exhaustion. Service providers have been obliged to invest in infrastructure to handle greater traffic due to unexpected growth in subscribers and linked IoT devices. Service providers are struggling to maintain growth and business continuity due to the expiration of IPv4 globally and the adoption of IPv6. There is strongly a need to address both a short-term solution for the maintenance of their current IPv4 address allocation and a long-term solution for a seamless transition to an IPv6 infrastructure, various service providers will need to design an address translation strategy. This paper presents a solution using CGNAT towards the migration of IPv6 networks. A general overview of the various parts needed to manage the depletion of IPv4 addressing and the engagement of full carrier grade network address translation solution is also discussed in this paper along with the different types of NAT.

Index Terms: CPE,NAT; NAT44; NAT64; NAT444; CGNAT.

1. Introduction

Initially, IP addresses were intended to be globally unique and reachable. The end-to-end architecture of the Internet is supported in large part by this attribute of the IP address. The aforementioned IP address architecture served as the foundation for nearly all Internet protocol designs up until recently, especially those that were below the application layer. However, the rapid expansion of the Internet during the 1990s not only warned of the threat of the depletion of IP address space but also immediately increased the need for IP addresses as the Internet connected a huge number of user networks and personal computers. The scarcity has been made more severe by the introduction of new Internet-connected places and new Internet-connected devices. The added devices placed an additional burden on the IPv4 infrastructure already in place. Such demand cannot be satisfied by using the standard IP address allocation procedure. To handle this sudden surge in demand, network address translation was put to use, and NAT products were produced fast to fulfil consumer demand. However, because NATs were not standardized prior to their widespread adoption, a variety of NAT products are available today, each with slightly varying functionality and technical specifications. Several solutions were proposed to extend the life of IPv4 addresses with its 32 bits, however by the late 1980s, it was clear that the internet's rapid use would eventually exhaust this huge pool of addresses [1]. For as long as this is even feasible, RIRs will only assign extremely limited blocks of new IP addresses, which will present providers with the issue of additional administrative expenses or, in the worst case scenario, the inability to launch new services.

The address space problem would be resolved by IPv6, which was intended to be the IPv4 successor protocol with 128 bits. By introducing a new address space with significantly more possible addresses, IPv6 eliminates the IP address scarcity. By providing a significantly bigger address space that enables each network resource to have a distinct genuine IP address, Internet Protocol version 6 (IPv6) eliminates the requirement for Network Address Translation. In this manner, IPv6 attacks the core issue for which Network Address Translation (NAT) offered a solution [2]. In addition, IPv6 offers many more advantages to service providers and end users than IPv4, including increased productivity, security, ease of use, and Quality of Service (QoS). As with IPv4 capabilities, many makers of business and consumer devices provide support for IPv6 network connectivity, IPv6 management, and IPv6 traffic handling. The switch from IPv4 to IPv6 cannot, however, be made instantly. A complete switchover is not feasible. As IPv6 was not designed to be backward compatible, therefore the issue of a restricted number of addresses per host persisted. This issue was addressed by the development of Carrier Grade NAT (CGNAT), which was primarily designed for service providers [3].

Network Address Translator (NAT) is a technique is used to address reuse is a simple approach to control the demand for IP addresses until the long-term solutions are ready. This approach takes use of the fact that only a tiny fraction of hosts in a stub domain are ever engaged in inter-domain communication. Stub domain simply handles traffic coming from or going to hosts in the domain. In fact, most hosts (if not all) never communicate with one another outside of their stub domain. As a result, when external communications are necessary, just a portion of the IP networks address within the stub domain need to be transformed into global IPv4 addresses which can be adopted globally. A deterministic NAT feature of CGNAT lowers the amount of monitoring required by mapping particular private IP addresses to public IP addresses. With the inclusion of IP Policy Enforcement Manager, carriers will be able to connect CGNAT settings to service plans with destination-aware policies and knowing more about what users are doing on the network.

In 1998, the IPv6 protocol was made a draft standard as a replacement for IPv4 and a long-term solution to IPv4 address exhaustion. It took the Internet Engineering Task Force (IETF) 19 years to proclaim this protocol an internet standard, despite the fact that it offered a 128-bit address space (a total of $3.4 * 10^{38}$ addresses, or over 340 trillion addresses) [4]. The ojective of this research paper is that-

1. To understand about the need of using NAT for migration strategy.
2. To understand about various NAT Schemes- like NAT 666, NAT 44 etc.
3. Understanding about the deploymeny of CGNAT mechanism in the network.

Rest of the paper is structured as follows: Section II discusses about the deployment Mechanisms for various NAT technology, Section III discusses about the benefits of NAT mechanism, and section IV discusses about the migration approach for IPv6 protocol, Section V concludes the paper.

2. Standard NAT and IPv4 Addresses

Within the internal networks, end users and devices can use any IP address available from the pool of private IP addresses. Multiple organizations may have same private IP address internally, however when connected to outside network they may require a unique public IP address for communication. The ability of NAT44 to translate several Private IP addresses to a single Public IP address is another helpful feature. This is feasible because Applications rarely use all the available ports on any Private IP address. For the conversion of private IP into public IP, organizations are using Network Address Translation (NAT) service to transport internal hosts to outside hosts [5]. When routing is done between IPv4 networks, a mechanism known as NAT44 is used to translate network addresses from IPv4 to IPv4 addresses. A NAT table is maintained at edge router for mapping of addresses. The fig 1 depicts a Customer Premises Equipment (CPE) gateway that uses NA.T to convert private addresses to public addresses is shown below.

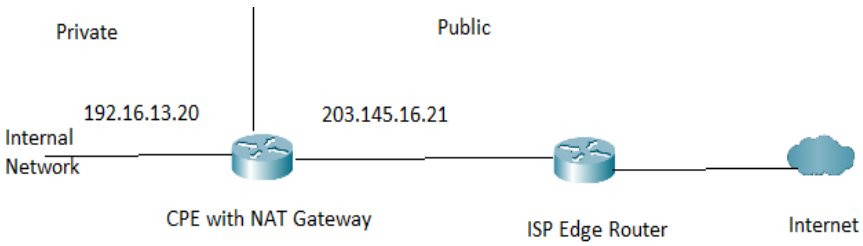

Fig. 1. CPE Gateway

Converting private IP addresses to public IP addresses using standard network address translation: Consumer and enterprise solutions functioned properly with conventional NAT, which converts a number of internal addresses in stub domains to a single global public address and vice versa. However, NAT implementations eventually included home and mobile networks in addition to commercial networks. The issue of internet IPv4 exhaustion grew urgent as each customer CPE or mobile device needed a public IP address and as consumer usage quickly rose. The implementation of NAT44 on the ISM platform supports the following Layer 4 protocols.

1. The UDP (IP Protocol 17) port number and IPv4 address (four bytes each) are translated simultaneously.
2. The TCP (IP Protocol 6) port number and IPv4 address (four bytes each) are translated simultaneously.
3. The ICMP (IP Protocol 1) - ICMP Identifier field (2 bytes) is used as a (fake) Layer 4 port in the echo request and echo response messages.
4. The Call ID field (2 bytes) of GRE, which is used with IP Protocol 47 and PPTP ALG, is used as a (fake) Layer 4 port.

2.1 Network Address Translation of a Carrier-Grade (CGNAT)

The way NAT is implemented by service providers allows several subscribers to form a single global IP address. The service provider NAT is a carrier grade NAT since it scales to several million NAT translations (CGN) [6]. In CGN, just the source address port translation is necessary for packets that travel from inside the network to outside; destination address port translation is not necessary. CGN can be used in conjunction with broadband access aggregation or independently, similar to traditional NAT. Layer 4 Redirect and subscriber services like traffic classes coexist alongside CGN in Intelligent Services Gateway (ISG) capabilities. As a result, service providers including ISPs, broadband cable, and mobile operators quickly needed a technology to meet both specific performance and feature needs as well as to stretch the restricted pool of Public IP addresses even further [7]. While managing IPv4 address depletion and preparing migration strategy to IPv6, CGNAT provides seamless IPv4 connection and handles a large number of concurrent sessions. A few application-layer gateways that are functional include large scale NAT, port control protocol (PCP), NAT64/DNS64, NAT 444, 464xlat, endpoint-independent mapping, address/port persistence, filtering (EIM/EIF), hair pinning, PIM-DM. It also have many application-layer gateways like RTSP, FTP, PPTP, SIP FTPS, FTP over TLS, and many more. The following fig 2 depicts the deployment of CGNAT-

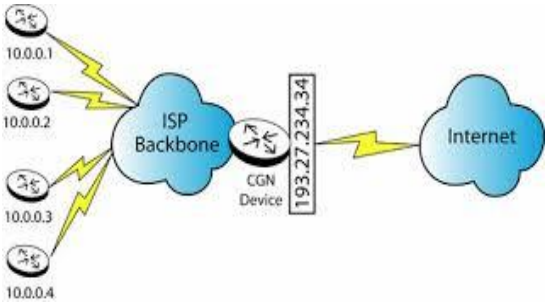

Fig. 2. CGNAT for Service Providers

2.2 NAT44 and NAT444 CGNAT Common Deployment Scenarios for Service Providers

An additional layer for address translation is provided by CGNAT device which functions as to translate a private IP into public IP address in addition to the services provided by conventional NAT. ISPs can preserve their public IP addresses by processing customer traffic through the service provider's IP network and catering to clients or organizations that have their own private IPv4 networks, numerous locations, or devices. CGNAT is defined as follows and is typically used in NAT 444 scenarios:

- Customer's private IPv4 network address (ISP).
- For internet connectivity, use your ISP's public IPv4 network address to connect to their private IPv4 network. (Customer) Private IPv4 to (ISP) Private IPv4 network address. The following fig 3 depicts the address translation scheme for private to public IP address-

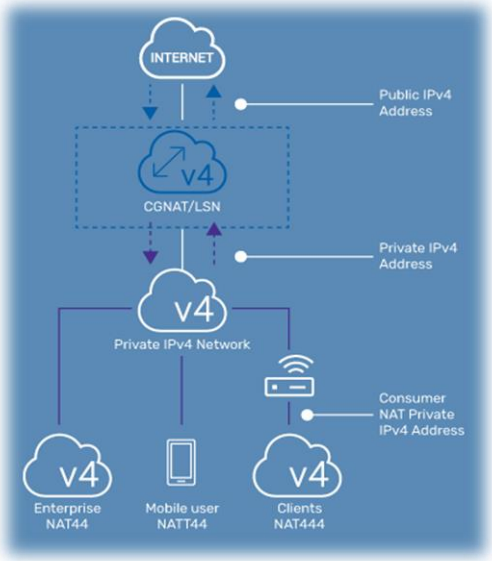

Fig. 3. Private to public address mapping

2.3 Common Deployment Scenarios for NAT44 and NAT444

The fig 4 below illustrates the implementation of NAT444 (private, private, public), with three client networks sharing a single public IPv4 address and three external IPv4 addresses that are private to the ISP and share the same internal IPv4 address space.

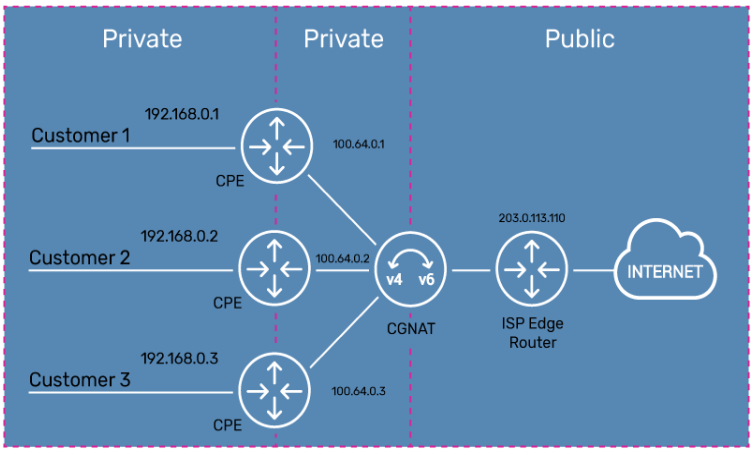

Fig. 4. NAT 444 (PPP)

2.4 NAT64:

This is one method for converting IPv6 addresses to IPv4 addresses. For its duty as an IPv4 and IPv6 translator, the NAT64 gateway would require one IPv4 address and IPv6 network segment address at the minimal with 32-bit address space. The main goal of NAT64 is to enable successful transmission between an IPv6-only client and an IPv4-only server. This goal is achieved in conjunction with DNS64. Using static or manual bindings, NAT64 can also be used by IPv4-only clients connecting to IPv6-only servers. A records are used in IPv4 name resolution to convert names to numbers. The identical procedure on IPv6 uses AAAA records. When utilizing NAT64, the translation engine will switch between AAAA and A records [8]. There are two different types of NAT64 transitions, Stateless and Stateful. State is not kept in stateless NAT64, so each IPv6 user needs their own dedicated IPv4 address. It's quite challenging to implement this NAT64 option because we are in the IPv4 depletion period. Utilizing stateless NAT64 only has benefits when there are few IPv6 addresses available (NAT46). States are kept in NAT64 stateful. All private users with various port numbers share a single IP address. For all IPv6 users in that LAN to contact a public IPv4 server, a single IPv4 address is used with various port numbers. Fig 5 depicts the scenario for Nat 64.

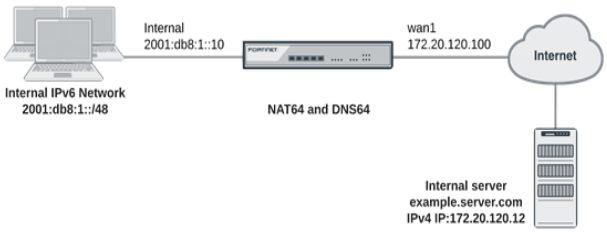

Fig. 5. NAT 64 (PPP)

2.5 NAT 46:

When dual stack and IPv6 tunneling solutions are not an option, the Network Address Translation 46 (NAT 46) functionality enables IPv4 hosts to connect to IPv6 internet. This solves the IPv4 to IPv6 connectivity issue. The IPv4 host to IPv6 internet connectivity problem is solved by NAT46. When an IPv4 host tries to connect to a server, it first sends a DNS type A query packet. This is changed to type AAAA query by the NAT 46 router [9] . NAT 46 pulls the IPv6 address from the answer packet when it receives the query response. From the configd NAT 46 pool, an IPv4 address is assigned, and the retrieved IPv6 address is bound to the assigned IPv4 address. The IPv4 host receives a DNS answer for its IPv4 address. Using a configd NAT 46 IPv6 prefix, packets coming from IPv4 hosts have their source address transformed. Utilizing pool address binding generated during DNS packet flow, the target IPv4 address is converted to an IPv6 address. Since no sessions are maintained, there is no cap on the total number of private IPv4 addresses that can be provided. Up to 40,000 IPv6 hosts should be able to be represented by a single IPv4 pool address.

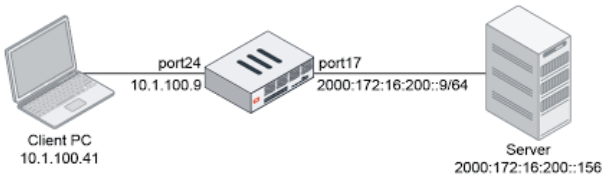

Fig. 6. NAT 46

2.6 SNAT:

By assigning remote users/systems a public Internet Protocol (IP) address, the network address translation (NAT) technique known as secure network address translation (SecureNA or SNAT) provides private network security. Using a single IP address, it allows multiple computers connected to a private local area network (LAN) to access the Internet. Routers and modems employ secure NAT to connect many users on a LAN or local network to the Internet. In a SNAT-based network, each computer has its own IP address, but every device is connected to the same local SNAT device, router, or modem. The SNAT-configd router replaces the originating IP address when submitting a request with its own IP address. When sending a request, the SNAT-configd router substitutes its IP address for the originating IP address. The SNAT-configd source IP address, rather than the device's actual IP address, is what the destination device sees when it gets the packet from the local device. This permits numerous devices to utilize the same IP address while protecting the internal network from exposure to external networks.

3. Benefits of using Carrier Grade NAT

In order to preserve IPv4 addresses and facilitate the transition to IPv6, CGNAT enables network scalability. Even with the escalating connectivity demands from customers and devices, bridging IPv4 and IPv6 helps to ensure that new and old applications are easily reachable. Worldwide IPv4 address allocations have been exhausted. The number of IPv4 addresses available globally has reached its limit, hence service providers must switch to IPv6. While implementing newer IPv6 apps and devices, service providers must manage IPv4 devices and content. IPv6 migration techniques must accommodate the coexistence of both IPv4 and IPv6 devices and content because they are incompatible with each other. End-to-end networking was the guiding philosophy behind the creation of IP. Application protocols can therefore anticipate direct communication between hosts without the need for middle systems to alter the packet headers or payload. NAT can disrupt communications since it at the very least updates IP addresses and occasionally changes other protocol headers and payloads. By incorporating the following capabilities, Carrier Grade NAT (CGNAT) addresses this issue as well as others related to employing classical NAT at scale:

• To address the issue of NAT servers severing communications, application level gateway (ALG) was created. ALGs intelligently alter required application protocol headers and payloads based on proxy server technology to comply with the protocol being routed by the NAT.

Transparent NAT connectivity is provided via Endpoint Independent Mapping (EIM), Endpoint Independent Filtering (EIF), and hair pinning. EIM and EIF traffic, as well as protocols that must hairpin, or loop their traffic back inside, are not permitted by conventional NAT implementations.

Demands on a Large Scale for Service Providers: The crucial performance, reliability, and management needs of carrier networks, major companies, higher education institutions, and ISPs necessitate significantly more advanced carrier grade NAT (CGNAT) features than those needed by consumer and small business networks.

• Performance - Carrier Grade NAT systems need to be able to handle millions of concurrent network connections.

• High Availability - Carrier Grade NAT solutions must be highly high available 24 hours a day, 7 days a week, without causing user service interruptions.

• Scale-out - Operator systems must have the ability to scale dynamically, providing more throughput as needed without affecting with the existing networks. In the event of any component failures, this necessitates session preservation and seamless failover.

• Central Management - For centralized logging, large-scale NAT and carrier-grade NAT solutions must be able to integrate with the main CNM platforms and DevOps infrastructures.

Advanced logging - Since every Internet-connected device creates a high number of sessions, keeping track of all of those sessions generates a massive amount of log messages. For carrier grade NAT solutions, advanced logging techniques like port batching, zero-logging, and compact logging are necessary, as well as filtering to obtain relevant, practical insights.

• Security - CGNAT deployments must have extremely thorough security measures in place as well as safeguards against threats like Distributed Denial of Service (DDoS) attacks directed against CGNAT pools.

• User Quota system - To ensure equitable resource distribution among customers in ISP and Mobile Network Provider (MNP) environments, the ability of an administrator to restrict the number of TCP and UDP ports that a single user may use is essential. External attackers could easily compromise other subscribers' connectivity if it isn't managed.

4. Challenges for adopting NAT

Network address translators, sometimes known as NAT devices, are widely used nowadays. Their quick ascent to widespread adoption did not follow any deliberate strategy. Instead, it was fueled by the internet's continuing expansion and the shrinking IPv4 address space as a result. In addition to its obvious benefits, such as IP address reuse and the concealment of internal network topologies, NAT technology also has several significant disadvantages. NAT was not created with emerging technologies and protocols in mind because it was intended to be a temporary technology. In order to solve these problems, those protocols must incorporate some sort of intelligence. The difficulties encountered during NAT implementation are listed below.

1. No specific deployment specifications: The IETF opposed defining NAT behaviour because doing so would only promote its use. They only considered this technology to be a "temporary solution." As a result, the initial specification was kept at a broad level. However, this forced each NAT implementer to decide locally how the NAT should act in particular situations. Users benefit from a network that has an active device that is widely deployed but does not have consistent implementations and, in the worst instances, behaves non-deterministically. This has made it extremely difficult to deploy some internet-based apps, like voice-based ones.

2. IP Packet Fragmentation and Out-of-Order delivery NAT devices lack consistent response to IP packet fragmentation as they depend on the TCP/UDP header of the each incoming frame for translation. They try attempt to place the IP packet back together as if they're the end devices/host and can only perform the Network address translation afterwards. Naturally, if the reassembled packet is too large to be transmitted alone, the NAT will then have to further fragment it. Instead of attempting to reassembly packets, other NAT devices are based on a packet fragment translation state that chooses how additional fragments must be translated [10].

3.Peer-to-peer communication: Peer-to-peer communication is not supported by NAT in cases where an outside initiator is involved. Since the internal addresses used by an enterprise are private behind the NAT, they cannot be relayed over the internet. As a result, the external device is unable to initiate a session with the device protected by NAT by sending any packets. It means that peer-to-peer voice-based systems cannot be operated properly in a NAT environment. To tackle this limitation, a protocol needs to implement a special solution.

4. IPSEC: For data integrity, IPSEC (Internet Protocol Security) employs a cryptographic hash value. However, NAT modifies the IP packet, rendering such integrity tests useless. However, NAT Traversal, sometimes known as NAT-T, offers a solution. In essence, NAT-T [11] detects the presence of any NAT devices that may be present between two hosts and encapsulate IPsec traffic in a second UDP that may be used on a non-IPsec port.

5. Migrating Strategy towards IPv6

In December 1998, the IETF proposed IPv6 as a draft standard to address the IPv4 exhaustion problem. Complete adoption took place in July 2017. Since its introduction, IPv6 usage has increased gradually across devices, service provider networks, and content providers, despite notable regional variances per country. A significantly bigger address space provided by Internet Protocol version 6 (IPv6), which enables each network resource to have a distinct genuine IP address, eliminating the requirement for Network Address Translation [12]. In this approach, IPv6 gets to the heart of the issue that NAT attempted to address. Mobile carriers, ISPs, and device manufacturers have pushed adoption of IPv4 and IPv6, which are supported by the more recent iterations of mobile devices (4G/5G). All of the major web content providers, including Google, Alexa, Facebook, Yahoo, YouTube, and others, have adopted IPv6. Due to the associated costs, businesses have generally been hesitant to use IPv6, however acceptance is accelerating. Due to the large number of websites, devices, and networks that are still primarily IPv4-based, the majority of service providers, educational institutions, and businesses must support IPv4 and IPv6 connectivity for their users and subscribers even though their own networks have fully migrated to IPv6. This hybrid environment has led to the development of a number of technologies that facilitate the process of transition and permit communication between IPv4 and IPv6 devices, networks, and Internet destinations [13]. These systems either convert between IPv4 and IPv6 addresses or wrap communication to allow it to travel over the incompatible network.

6. Conclusion

In an ideal world, everyone would already be utilizing dual stack or native IPv6. But that is not the case, and IPv4 will continue to exist for a very long time. Whether you like it or not, there will be a requirement to translate between the two while both protocols are in use. Large service provider, enterprise, and higher education network deployments

of CGNAT or LSN have been successful for many years. Carrier Grade NAT (CGNAT) offers a tried-and-true way to leverage current IPv4 investment while providing subscribers and users with a seamless migration path to IPv6 when combined with the IPv6 migration technologies previously identified in a strong CGN solution. Carrier Grade NAT (CGNAT) has a number of features that enable it to successfully handle large-scale carrier deployments while overcoming the constraints of regular NAT. Service providers can now manage IPv4 depletion and preservation while preparing for IPv6 migration by sharing their limited public IPv4 address across a large number of expanding users thanks to carrier grade NAT. The solution with CGNAT will solve the IPv6 adoption problem and make our internet more secure and better place for consumers.

References

[1] Chauhan, D., & Sharma, S. (2014). A survey on next generation Internet Protocol: IPv6. Int. J. Electron. Ind. Eng.(IJEEE), ISSN, 2(2), 125-128.

[2] Al-hamadani, A. T. H., & Lencse, G. (2021). A survey on the performance analysis of IPv6 transition technologies. Acta Technica Jaurinensis, 14(2), 186-211.

[3] Dawadi, B. R., Rawat, D. B., Joshi, S. R., & Manzoni, P. (2022). Towards Smart Networking with SDN Enabled IPv6 Network. arXiv preprint arXiv:2203.01528.

[4] Hinden, R., & Deering, S. (2003). Internet protocol version 6 (IPv6) addressing architecture (No. rfc3513).

[5] Kivinen, Tero, et al. Negotiation of NAT-Traversal in the IKE. No. rfc3947. 2005.

[6] Dawadi, B. R., Rawat, D. B., Joshi, S. R., & Manzoni, P. (2022). Towards Smart Networking with SDN Enabled IPv6 Network. arXiv preprint arXiv:2203.01528.

[7] Radu, R., & Hausding, M. (2020). Consolidation in the DNS resolver market–how much, how fast, how dangerous?. Journal of Cyber Policy, 5(1), 46-64.

[8] Marian, C. V. (2021, May). DNS Records Secure Provisioning Mechanism for Virtual Machines automatic management in high density data centers. In 2021 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom) (pp. 1-5). IEEE.

[9] Fukuda, K., Aharen, Y., Sato, S., & Mitamura, T. (2022, April). Characterizing DNS query response sizes through active and passive measurements. In NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium (pp. 1-6). IEEE.

[10] Chauhan, D., Jain, J. K., & Sharma, S. (2016, December). An end-to-end header compression for multihop IPv6 tunnels with varying bandwidth. In 2016 Fifth international conference on eco-friendly computing and communication systems (ICECCS) (pp. 84-88). IEEE.

[11] Nam, T. S., Van Thuc, H., & Van Long, N. A High-Throughput Hardware Implementation of NAT Traversal for IPSEC VPN.

[12] Chauhan, D., & Sharma, S. (2015). Addressing the Bandwidth issue in End-to-End Header Compression over IPv6 tunneling Mechanism. International Journal of Computer Network and Information Security, 7(9), 39-45.

[13] Chauhan, D., Jain, J. K., & Bahad, P. (2021). PERFORMANCE EVALUATION OF 802.11 A/G WIRELESS NETWORKS WITH IP6HC. Journal of Management Information and Decision Sciences, 24, 1-7.

Authors' Profiles

Dr. Dipti Chauhan is presently holding the position of Professor in the Department of Computer Science & Engineering, at PIEMR Indore. She completed her Ph.D. from Maulana Azad National Institute of Technology, Bhopal, Madhya Pradesh, India in the area of Next generation networks & IPv6. She has received a fellowship from the Ministry of Human Resource Development (MHRD). She is IPv6 Certified Gold and Silver Network Engineer from the IPv6 forum, University Sains Malaysia. Her Research Areas include Data Mining & Warehousing, Artificial Intelligence, Machine Learning, Data Science, Next Generation Networks, and the Internet of Things.

How to cite this paper: Dipti Chauhan, "IPv6 Migration Strategy Using Carrier Grade Network Address Translation", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.13, No.4, pp. 11-17, 2023. DOI:10.5815/ijwmt.2023.04.02