Navigating the Transition: Address Depletion of IPv4 and Transition to IPv6

Dalal Arafeh

Table of Contents

1. Abstract

The global internet infrastructure is critically constrained by the exhaustion of IPv4 addresses, a problem that has become increasingly urgent since the American Registry for Internet Numbers (ARIN) depleted its IPv4 address pool in 2015. The IPv4 protocol, initially designed with a 32-bit address space for a limited number of organizations, is unable to support the exponential growth of internet-connected devices such as mobile phones, PCs, and IoT devices. Mitigation strategies like Network Address Translation (NAT), Classless Inter-Domain Routing (CIDR), and address reclamation have provided temporary relief but are insufficient for long-term scalability. IPv6 provides a comprehensive solution with about 3.4 x 10^38 addresses and a 128-bit address space, which ensures safeguarding for the booming internet ecosystem. However, the transition from IPv4 to IPv6 is fraught with technical challenges, primarily due to the incompatibility between the two protocols. Dual-stack allows devices to run both IPv4 and IPv6 simultaneously, providing a gradual transition path. Tunneling methods, such as 6to4 and ISATAP, enable IPv6 packets to be transmitted over existing IPv4 infrastructure. Translation techniques, including NAT64/DNS64, allow IPv6-only devices to communicate with IPv4-only systems.

According to a United Nations survey, the global population is projected to reach 7 billion by 2050, with approximately 70% residing in urban areas (United Nations). This rapid urbanization, with many people migrating from rural to urban areas daily, highlights the critical need for a robust and scalable internet addressing system, which IPv6 aims to provide. This white paper examines the technical contrasts between IPv4 and IPv6, emphasizing IPv6's benefits like larger address capacity, streamlined header format, and enhanced support for QoS and multicast. By comparing IPv4 with IPv6, the white paper aims to empower network engineers with insights and resources for managing the transition to a sustainable IPv6 internet.

2. *Problem Statement*

The global internet infrastructure has long been plagued by the depletion of IPv4 addresses. In 2015, an important turning point in the history of the internet occurred when the American Registry for Internet Numbers (ARIN) ran out of IPv4 addresses. Even earlier, in 2011, Microsoft bought 666,624 IPv4 addresses from Nortel Networks after recognizing the impending shortage (Rosoff). This trend continues as four out of five Regional Internet Registries (RIRs) exhausted their available IPv4 space. APNIC exhausted its available IPv4 space on April 15th, 2011 (APNIC), followed by RIPE on September 14th, 2012 (RIPE NCC), LACNIC on June 10th, 2014 (LACNIC), and ARIN on September 24th, 2015 (ARIN).

Originally, IPv4 was designed as an experimental protocol for a limited number of organizations, and it was not intended to handle the current boom of internet-connected devices. The depletion of Ipv4 addresses has been exacerbated by the proliferation of mobile devices, PCs, and other numerous IP-dependent technologies. The inevitable depletion happened in spite of creative solutions like Network Address Translation (NAT), recovering unused address space, and port address translation. On February 3, 2011, the "class A" block, the last block of IPv4 addresses, was distributed by the Internet Assigned Number Authority (IANA), marking the end of IPv4 resources and the transition to IPv6 (ARIN).

The Internet Engineering Task Force (IETF) and other stakeholders have been preparing for this transition. IPv6, approximately 3.4×10^{38} addresses, provides a sustainable solution for address depletion. IPv4, a 32-bit address protocol, was adequate for the early internet, which was mostly used by desktop computers. The rapid growth of the internet, especially in regions such as Asia, Africa, and Latin America, underscores the need for transitioning to IPv6. Countries like Japan are leading this transition with projects the NTT backbone and Seychelles achieving the significant milestone of deploying 100% Ipv6 throughout the whole digital infrastructure including The Seychelles Internet Exchange Point (Sey-IX).

Public IPv4 addresses have become relatively scarce, forcing many users and organizations to use Network Address Translation (NAT) to map a single public IPv4 address to multiple IPv4 addresses. While NAT facilitates the reuse of private address space, it contradicts the original internet design principle of ensuring each node possesses a unique and globally reachable address. This limitation restricts true end-to-end connectivity for various network applications.

Currently, the internet is made up of native IPv4, native IPv6, and dual IPv4/IPv6 networks (D. Shalini Punithavathani and Sankaranarayanan K). Unfortunately, IPv4 and IPv6 are mutually incompatible protocols, preventing their coexistence. When both IP versions are available and internet users wish to connect without any limitations, a transition mechanism becomes required (Charlene). In the past, IPv6-based networks were implemented independently. But now, there have been efforts towards interconnecting these IPv6's across the broader IPv4 network. In order to fully understand the transition from IPv4 to IPv6, it is essential to compare and contrast these two protocols. This comparison will highlight the technical differences, advantages, and challenges associated with each protocol.

3. *Background*

3.1 *IPv4 Address Exhaustion and Mitigation Techniques*

3.1.1 *Network Address Translation (NAT)*

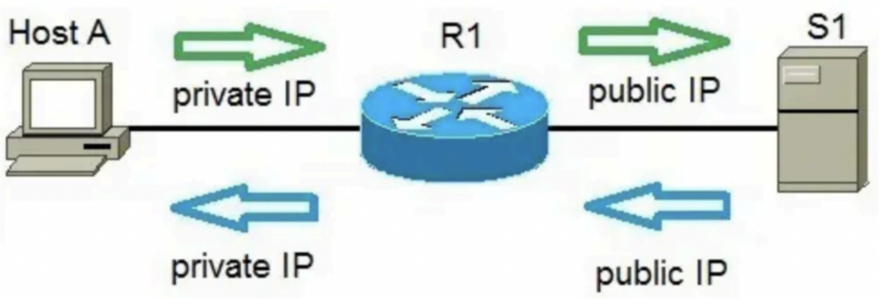


Figure 1: NAT CCNA Diagram (CCNA).

NAT allows multiple devices on a local network to share a single public IPv4 address. Port Address Translation (PAT) involves replacing the source IP addresses and ports of outgoing packets from devices within the local network with the router's public IP address and unique port number. The router's translation table keeps a log of which port belongs to which device, making sure the packets are correctly routed to the intended device based on their port numbers. When incoming packets reach the router's public IP address, the router checks their destination ports and refers to the translation table to find the matching private IP address and port, forwarding the packets accordingly. NAT can become a performance bottleneck, especially in high-traffic environments (Rocío Cerón).

3.1.2 *Classless Inter-Domain Routing (CIDR)*

Traditionally, IP addresses were managed through classful addressing, which imposed rigid allocations. CIDR, however, introduces variable length subnet masking (VLSM) to customize the balance between network and host address bits, allowing for more efficient use of IP addresses. CIDR works by organizing IP addresses into blocks with shared network prefixes, denoted by CIDR notation, and routers route data packets based on these prefixes. CIDR improves routing table efficiency but increases the complexity of routing decisions (AWS).

3.1.3 *Address Reclamation*

This process involves locating and retrieving IP addresses that are either inactive or unused to guarantee effective distribution of the limited IPv4 address space. By reclaiming these addresses, organizations are able to manage their IP resources, postpone the need for further allocations, and even sell subnets on the open market. Among the methods include dispersing address ranges, eliminating duplicate IP blocks, and carrying out IP address audits to identify and utilize dormant addresses (IPTrading).

Feature	*IPv4*	*IPv6*
Address Size	32-bit number	128-bit number
Number of Addresses	2^{32}~ 4.29 billion	2^{128}~ 340 undecillion
DNS	(A) records	(AAAA) records
Header Size	20 bytes	40 bytes
Fragmentation	Preformed by routes	Preformed by source device
Broadcasting	Supports broadcasting	No broadcasting, uses multicast and anycast
Routing Table Size	Larger due to address space exhaustion and NAT	Smaller, more efficient with hierarchical addressing
Configuration Methods	Manual, DHCP	SLAAC, DHCPv6, manual (HPE)
Packet Forwarding	Routers use ARP for MAC address resolution	Routers use Neighbor Discovery Protocol (NDP)
ICMP	ICMP for error reporting and diagnostics	ICMPv6 for error reporting, diagnostics, Neighbor Discovery, Router Solicitation (Meena)
QoS (Quality of Service)	ToS field, less granular	Flow labels, Traffic Class field, more granular (GeeksforGeeks)
Routing Protocols	RIP, OSPF, BGP, EIGRP	RIPng, OSPFv3, MP-BGP, EIGRP (IPCisco)
Private Addressing	RFC 1918 private addresses	Unique Local Addresses (ULAs) (Jain and Dalal)
Renumbering	Manual	Supports renumbering
Compatibility	Not directly compatible with IPv6, requires dual-stack or tunneling	Compatible with IPv4 through dual-stack or tunneling
IPv4-IPv6 Interoperability	Dual-stack, tunneling, translation mechanisms required	Dual-stack, tunneling, translation mechanisms available

Table 1: Comparing features of IPv4 and IPv6.

3.2 *IPv4 and IPv6 Header*

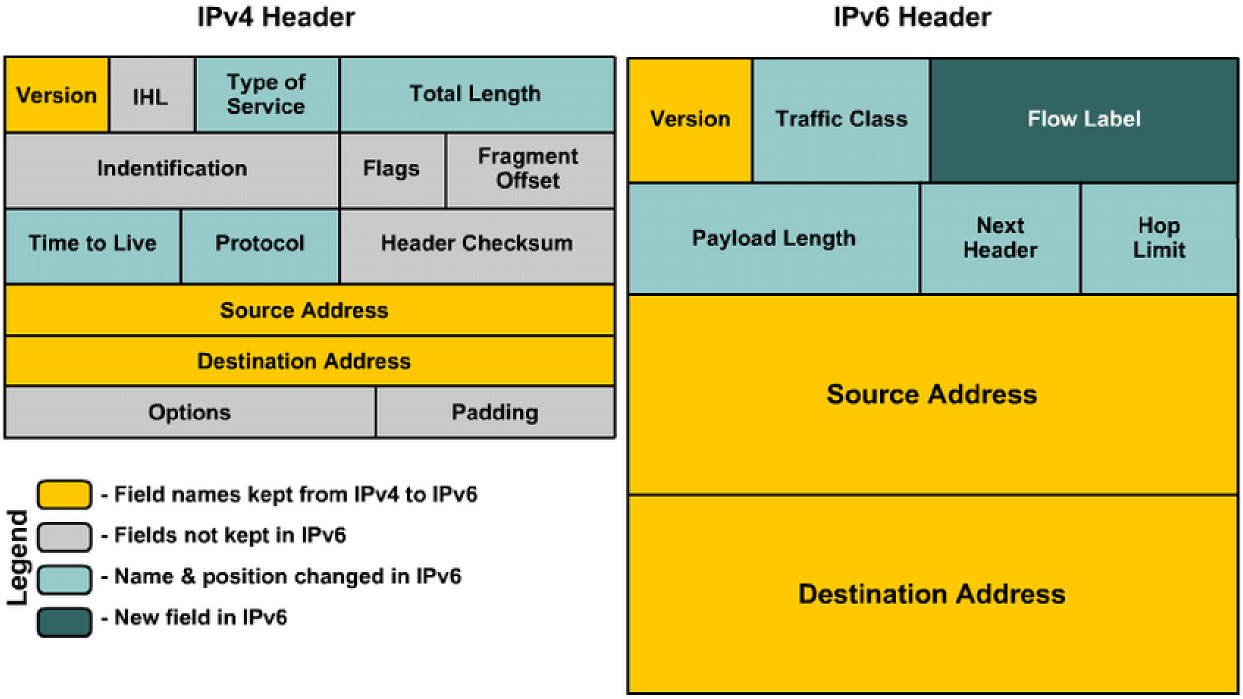


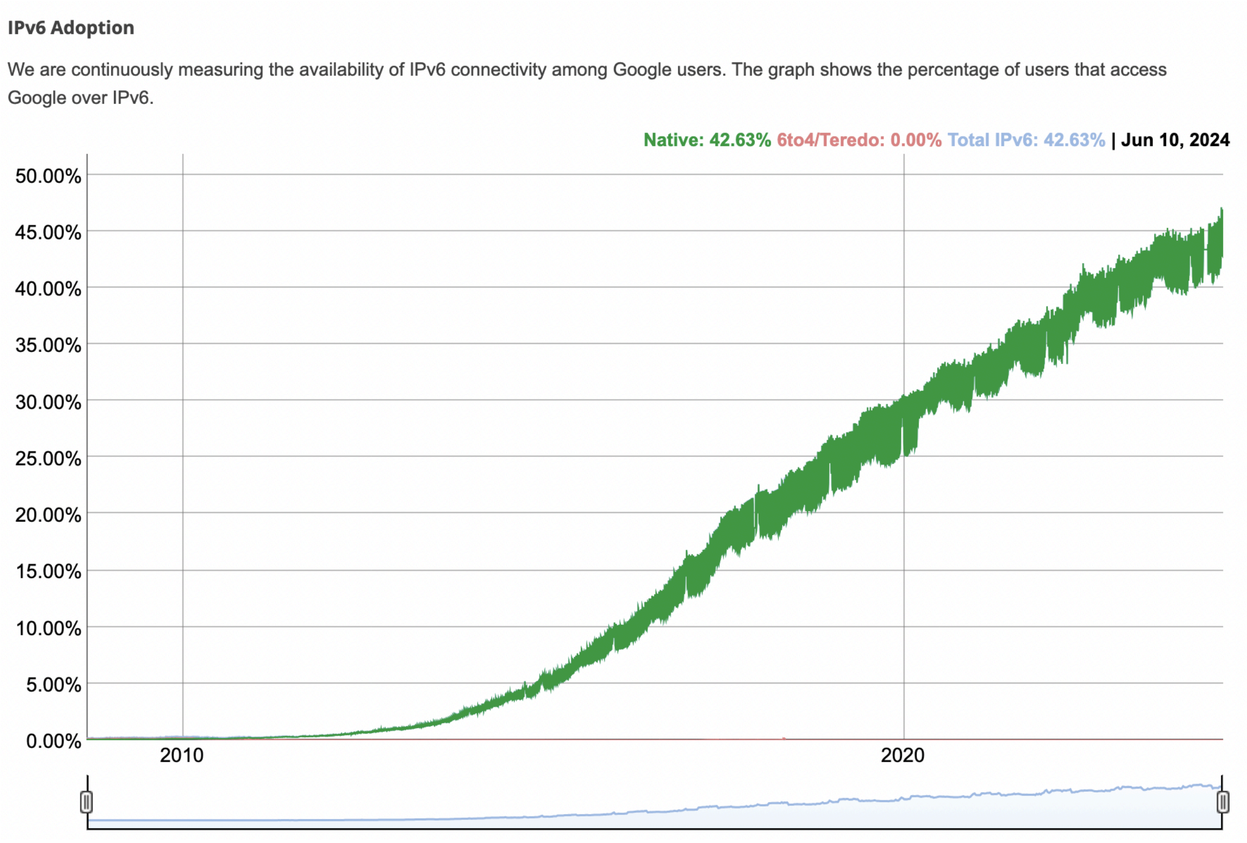
Figure 2: Comparison of IPv4 and IPv6 header structure (Qureshi).

The IPv4 header is characterized by a variety of fields, each with a specific function, leading to a more complex and variable-length structure. This complexity can introduce inefficiencies in packet processing. Key fields in the IPv4 header include the Version field (4 bits) identifying the IP version as 4, and the Internet Header Length (IHL) field (4 bits) specifying the length of the header. The Type of Service field (8 bits) is used to assign priority and QoS parameters to packets. The Total Length field (16 bits) denotes the entire packet size, including header and data. IPv4 also incorporates fields like Identification, Flags, and Fragment Offset (collectively 32 bits) for managing fragmentation. The Time to Live (TTL) field (8 bits) ensures packets do not circulate indefinitely, decrementing with each hop until it reaches zero, prompting the packet to drop. The Protocol field (8 bits) indicates the type of protocol in the payload, such as TCP or UDP. The Header Checksum field (16 bits) is used for error-checking the header. The Source Address and Destination Address fields (32 bits each) specify the sender and receiver addresses. The Options and Padding fields (variable length) provide additional functionalities, though they are less commonly used (Network Academy).

IPv6 is designed to minimize the impact on layering protocols, instead improving upon the IPv4 header by simplifying its structure and adding features to meet the needs of modern networks. IPv4 contains fields such as Internet Header Length (IHL), Identification, Flags, Fragment Offset, and Header Checksum, which impacts the speed at which routers process routes and forward packets. These fields have been omitted in IPv6. The Version field (4 bits) identifies the IP version as 6. The Traffic Class field (8 bits) replaces the IPv4 Type of Service field, specifying packet priority and quality of service parameters. The Flow Label field (20 bits) is a new addition, used to designate packet sequences for routers to handle differently. In contrast to the IPv4 Total Length field, which also contains the header, the Payload Length field (16 bits) indicates the length of the data component only, excluding the header.

Similar to the IPv4 Protocol field but with more options for extension headers, the Next Header field (8 bits) indicates the type of the next header or upper-layer protocol. The Hop Limit field (8 bits), equivalent to the IPv4 TTL field, limits the packet's hops. The IPv6 header leaves out the checksum field, which saves processing cost because error-checking is taken care of by upper-layer transport protocols like TCP and UDP and link-layer protocols. An important improvement over IPv4's constrained 32-bit addresses is the greatly increased address space provided by the Source Address and Destination Address fields (128 bits each). IPv6 adds Extension Headers, which are handled independently of the main header and enable optional capabilities without compromising packet processing speed (Network Academy).

3.3 *IPv6 Adoption*



IPv6 Adoption

We are continuously measuring the availability of IPv6 connectivity among Google users. The graph shows the percentage of users that access Google over IPv6.

Figure 3: Google Statistics IPv6 Adoption.

The data from Google statistics measures the percentage of users accessing Google services via IPv6. The adoption of IPv6 has been steadily increasing over the years, starting from nearly 0% in 2009 and reaching 42.63% by 2024. The green shading represents the native IPv6 connectivity, indicating that the majority of IPv6 traffic is handled without the need for transition mechanisms such as 6to4 or Teredo, both of which remain at 0%. Native IPv6 is preferred because it directly supports IPv6 traffic without needing additional translation or encapsulation, keeping things simple and avoids any delays or complications that can come with additional steps in the network (S.J.M. Steffann et al.).

4. Solution

4.1 *Dual-Stack*

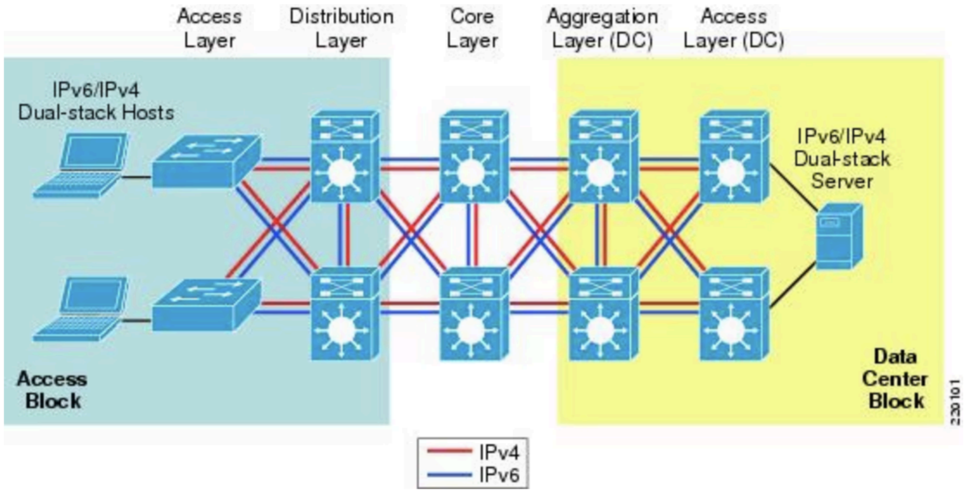


Figure 3: Cisco Dual-Stack Model Example.

The dual-stack approach allows hosts and applications to use either IPv4, IPv6, or both concurrently. Dual-stack does not require translating between IPv4 and IPv6 addresses; it supports both protocols independently. Key RFCs detailing dual-stack mechanisms include RFC4241, RFC4213, RFC6555, and RFC305. Depending on the network architecture, Dual-stack devices can handle IPv4 and IPv6 connections using either a single network interface or multiple interfaces. Each IP stack manages its own addressing configuration, routing table, and protocols independently (LACNIC).

Dual stack requires configuring both IPv4 and IPv6 addresses for end hosts, CPEs, and routers. IPv4 supports IPoE, static addressing, DHCPv4, or PPPoE. IPv6 offers static assignment, SLAAC, Prefix+EUI-64, DHCPv6/DHCPv6-PD. Dual-stack deployment includes two methods: native and tunneling. In native mode, hosts and routers independently operate IPv4 and IPv6 stacks. Tunneling encapsulates IPv6 with IPv4, enabling dual-stack over existing IPv4 networks. The Happy Eyeballs algorithm (RFC8305) helps hosts prioritize faster responding connections between IPv4 and IPv6. The main advantage of dual stack is avoiding complex tunneling or translation techniques. It allows the continued use of IPv4 while gradually introducing IPv6, making the transition smoother. Most operating systems and applications already support IPv6, facilitating its deployment (LACNIC).

4.2 *Tunneling*

6to4 tunneling allows IPv6 packets to traverse an IPv4 network, facilitating IPv6 connectivity over existing IPv4 infrastructure. This method is intended for situations where users need access to IPv6-based services via networks that do not support IPv6. To set up a 6to4 tunnel, a global IPv4 address is required for the tunnel interface, which serves as the foundation for generating the 6to4 IPv6 address. Secondly, a dual-stack relay server is necessary to handle routing between IPv4 and IPv6 interfaces bidirectionally. This server is essential for routing packets effectively between the two protocols. Lastly, The 6to4 IPv6 address is derived directly from the corresponding IPv4 address (IP2Location).

The 6to4 IPv6 address is formed by embedding an IPv4 address within an IPv6 address structure. As defined by RFC 3056. The first 16 bits of a 6to4 IPv6 address are always 2002 in hexadecimal. The subsequent 32 bits of a 6to4 IPv6 address represent the embedded IPv4 address, followed by 16 bits allocated for the IPv6 subnet. The relay server, equipped with both IPv4 and IPv6 interfaces, manages the routing of packets between IPv6 and IPv4 networks. When a 6to4 packet arrives at the IPv4 interface of the relay server, the IPv6 payload is extracted and then forwarded to the IPv6 network. Conversely, packets arriving at the IPv6 interface with a destination address prefix of 2002::/16 are encapsulated and transmitted over the IPv4 network. Encapsulation inserts IPv6 packets into IPv4 packets using protocol type 41, indicating an encapsulated IPv6 payload. This enables IPv6 traffic to flow smoothly through IPv4 networks (IP2Location).

Packet Tracer commands to create and configure a tunnel interface with an IP address

```
Router1> enable
Router1# configure terminal
Router1(config)# interface Tunnel X
Router1(config-if)# tunnel source <source-interface>
Router1(config-if)# tunnel destination <destination-ip>
Router1(config-if)# tunnel mode ipv6ip
Router1(config-if)# ipv6 address <ipv6-address/prefix-length>
Router1(config)# ipv6 route <remote-ipv6-network/prefix-length> Tunnel X
Router1(config-if)# end
Router1# copy running-config startup-config
```

```
Router2> enable
Router2# configure terminal
Router2(config)# interface Tunnel X
Router2(config-if)# tunnel source <source-interface>
Router2(config-if)# tunnel destination <destination-ip>
Router2(config-if)# tunnel mode ipv6ip
Router2(config-if)# ipv6 address <ipv6-address/prefix-length>
Router2(config)# ipv6 route <remote-ipv6-network/prefix-length> Tunnel X
Router2(config-if)# end
Router2# copy running-config startup-config
```

4.3 *Translation*

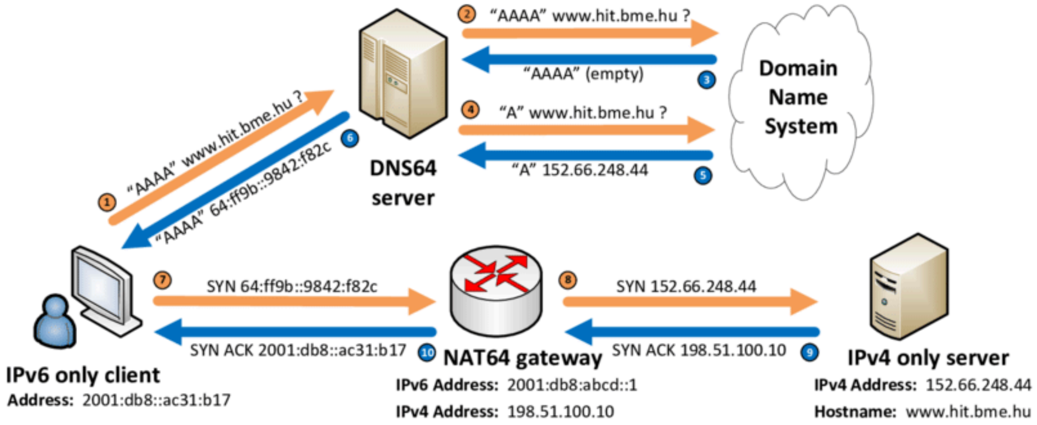


Figure 4: The functionality of the DNS64+NAT64 solution involves an IPv6-only client communicating with an IPv4-only server (Lencse).

NAT64/DNS64 translation is utilized in environments with mixed IPv4 and IPv6 networks, supporting IPv4 resources while IPv6 adoption is limited. This mechanism enables IPv6 clients to reach IPv4 resources by dynamically translating address formats and adjusting DNS responses as needed.

According to RFC 6036, at least 30% of operators intend to run some type of translator, typically NAT64/DNS64, making NAT64 deployment and operation guidance essential. The distinction between NAT64 Carrier Grade NAT (NAT64-CGN) and NAT64 server Front End (NAT64-FE) lies in their location and functionality. NAT64-CGN, placed in an ISP network, enables IPv6 subscribers to access IPv4 Internet services, with the ISP managing the IPv6 side but having limited control over the IPv4 Internet side. On the other hand, NAT64-FE, typically in a content provider or data center network, allows full control over the IPv4 network within the data center but has limited influence over the external IPv6 network. Stateful NAT64 is preferred for efficient sharing of public IPv4 addresses, maximizing address utilization. In contrast, stateless NAT64 offers better transparency but requires coordination with Address plus Port (A+P) processes to manage IPv4 address shortages. DNS64 is recommended for use with stateful NAT64. DNS64 generates synthetic AAAA replies when services provide only A records, allowing applications to access IPv6 networks via mechanisms like 464XLAT (Chen et al.)

When an IPv6-only host initiates a DNS query to resolve a domain name to an IP address, it typically requests an AAAA record, which contains the IPv6 address of the target node. If the target node is IPv4-only, AAAA record does not exist. DNS64 intervenes by querying for the A record when an IPv6-only host requests resolution of a domain name. Upon obtaining the A record (which contains the IPv4 address), DNS64 generates a synthetic AAAA record. This synthetic record retains the original owner name but embeds an IPv6 address derived from the IPv4 address. DNS64 constructs IPv6 addresses by combining a fixed prefix (Pref64::/n) with the IPv4 address. For DNS64 to function correctly, both the DNS64 server and the IPv6/IPv4 translator must use the same Pref64::/n prefix. This consistency ensures that both can generate identical IPv6 representations of IPv4 addresses. Packets addressed to the synthetic IPv6 address are routed to an IPv6/IPv4 translator. This translator, using the matching Pref64::/n prefix, converts IPv6 packets into IPv4 packets, allowing communication with IPv4-only servers on the network. The prefixes used in DNS64 can be of two types. The Well-Known Prefix (64:ff9b::/96) is universally recognized and reserved for representing IPv4 addresses in the IPv6 address space. The Network-Specific Prefix (NSP) is assigned by organizations for their specific networks, allowing them to create IPv6 representations of IPv4 addresses within their network. DNS64 can be used in three locations. In authoritative servers, the server synthesizes AAAA records for an IPv4-only client in its zone. In recursive name servers, these servers serve end hosts by synthesizing AAAA records and passing them back to IPv6-only clients. In end hosts, the DNS64 function is built into the end host's resolver, allowing it to synthesize AAAA records if they are unavailable (Matthews et al.).

5. Conclusion

The limited address space of IPv4 has already shown its constraints, which will only become more pronounced as the number of internet-connected devices continues to surge. The 32-bit architecture of IPv4, a relic of the early internet, is fundamentally misaligned with the demands of our hyper-connected, data-driven society. By clinging to IPv4, we perpetuate a fragmented internet architecture, burdened by administrative overhead and security vulnerabilities. IPv6 offers a sustainable solution to address depletion. As early as 2011, the world began to witness significant signs of this scarcity, prompting organizations and stakeholders to prepare for a substantial transition to IPv6. The potential of IPv6 is especially obvious when it comes to future technologies such as Mobile IP: this will enable users to access the Internet anywhere in the world using only one IP address.

Moving forward, it is imperative for network engineers and organizations to prioritize the adoption of IPv6. This involves not only implementing dual-stack configurations and tunneling solutions but also ensuring that infrastructure and applications are IPv6-ready. By doing so, the global internet can support the increasing number of connected devices and the expanding digital ecosystem. This transformation aims to optimize network performance and get ready for the next wave of internet development, which will be fueled by IoT, smart cities, and next-generation mobile networks, rather than just increasing address capacity.

Works Cited

APNIC. "APNIC IPv4 Address Pool Reaches Final /8." *Apnic.net*, 2024, conference.apnic.net/news-archives/2011/final-8/. Accessed 14 June 2024.

ARIN. "ARIN IPv4 Free Pool Reaches Zero." *Arin.net*, 24 Sept. 2015, www.arin.net/vault/announcements/20150924/. Accessed 14 June 2024.

AWS. "What Is CIDR? - CIDR Blocks and Notation Explained - AWS." *Amazon Web Services, Inc.*, 2023, aws.amazon.com/what-is/cidr/#:~:text=A%20CIDR%20IP%20address%20appends,2%2C%20is%20the%20network%20address. Accessed 14 June 2024.

CCNA. "What Is NAT (Network Address Translation)? - Study CCNA." *Study CCNA*, 26 Jan. 2016, study-ccna.com/what-is-nat/. Accessed 14 June 2024.

Charlene. "How to Achieve IPv4 and IPv6 Coexistence: Dual Stack or MPLS Tunnel? | FS Community." *Knowledge*, 2020, community.fs.com/article/how-to-achieve-ipv4-and-ipv6-coexistence-dual-stack-or-mpls-tunnel.html. Accessed 14 June 2024.

Chen, Gang, et al. "RFC 7269: NAT64 Deployment Options and Experience." *IETF Datatracker*, 2014, datatracker.ietf.org/doc/html/rfc7269. Accessed 14 June 2024.

GeeksforGeeks. "Internet Protocol Version 6 (IPv6) Header." *GeeksforGeeks*, GeeksforGeeks, 21 Sept. 2017, www.geeksforgeeks.org/internet-protocol-version-6-ipv6-header/. Accessed 14 June 2024.

HPE. "Configuring an IPv6 Global Unicast Address." *Hpe.com*, 2017, techhub.hpe.com/eginfolib/networking/docs/routers/vsr1000/cg/5200-3156_l3-ip-svcs_cg/content/478552078.htm. Accessed 14 June 2024.

IP2Location. "What Is 6to4 Tunneling? | IP2Location.com." *IP2Location.com*, 3 May 2019, blog.ip2location.com/knowledge-base/what-is-6to4-tunneling/. Accessed 14 June 2024.

IPCisco. "IPv6 Routing Protocols | RIPng | OSPFv3 | EIGRP | MP-BGP4 ⋆ IpCisco." *IPCisco*, 2022, ipcisco.com/lesson/ipv6-routing-protocols/. Accessed 14 June 2024.

IPTrading. “A Deep Dive into IPv4 Address Reclamation Strategies | IP Trading.” *IP Trading*, 6 Feb. 2024, iptrading.com/blog/a-deep-dive-into-ipv4-address-reclamation-strategies-with-iptrading/. Accessed 14 June 2024.

Jain, Ujjwal, and Rohit Dalal. “Using IPv6 Unique Local Addresses, or ULA, in Google Cloud.” *Google Cloud Blog*, Google Cloud, 19 Jan. 2023, cloud.google.com/blog/products/networking/using-ipv6-unique-local-addresses-or-ula-in-google-cloud. Accessed 14 June 2024.

LACNIC. “Dual Stack.”

---. “Phases of IPv4 Exhaustion.” *Lacnic.net*, 2024, www.lacnic.net/1039/2/lacnic/phases-of-ipv4-exhaustion. Accessed 14 June 2024.

Lencse, Gabor. “Fig. 7. The Operation of the DNS64+NAT64 Solution: An IPv6 Only Client...” *ResearchGate*, ResearchGate, 2016, www.researchgate.net/figure/The-operation-of-the-DNS64-NAT64-solution-an-IPv6-only-client-communicates-with-and-IPv4_fig3_299405560. Accessed 14 June 2024.

Matthews, Philip, et al. “RFC 6147: DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers.” *IETF Datatracker*, 2024, datatracker.ietf.org/doc/html/rfc6147. Accessed 14 June 2024.

Meena. “How Does ICMP Work in IPv6? - a Practical Demonstration - Luminisindia.com.” *Luminisindia.com*, 2020, luminisindia.com/it-networking-blog/163-how-does-icmp-work-in-ipv6-a-practical-demonstration. Accessed 14 June 2024.

Network Academy. “IPv4 vs IPv6 - Understanding the Differences.” *NetworkAcademy.io*, 2020, www.networkacademy.io/ccna/ipv6/ipv4-vs-ipv6. Accessed 14 June 2024.

Qureshi, Ashad. “Fig 1.1: Comparison of IPv4 and IPv6 Header Structure.” *ResearchGate*, ResearchGate, 2020, www.researchgate.net/figure/Comparison-of-IPv4-and-IPv6-header-structure_fig1_339722884. Accessed 14 June 2024.

RIPE NCC. “RIPE NCC Begins to Allocate IPv4 Address Space from the Last /8.” *RIPE Network Coordination Center*, 14 Sept. 2012, www.ripe.net/publications/news/ripe-ncc-begins-to-allocate-ipv4-address-space-from-the-last-8/. Accessed 14 June 2024.

Rocío Cerón. “NAT: What It Is and How It Works in Our Network -.” *Pandora FMS*, 3 Apr. 2024, pandorafms.com/en/it-topics/what-is-nat/. Accessed 14 June 2024.

Rosoff, Matt. “Microsoft: Paid $11 Apiece for Internet Addresses.” *Business Insider*, Insider, 24 Mar. 2011, www.businessinsider.com/microsoft-just-bought-600000-internet-addresses-for-12-apiece-2011-3 . Accessed 14 June 2024.

S.J.M. Steffann, et al. “RFC 7059: A Comparison of IPv6-Over-IPv4 Tunnel Mechanisms.” *IETF Datatracker*, 2024, datatracker.ietf.org/doc/rfc7059/. Accessed 14 June 2024.

United Nations. “68% of the World Population Projected to Live in Urban Areas by 2050, Says UN | United Nations.” *United Nations*, United Nations, 2022, www.un.org/uk/desa/68-world-population-projected-live-urban-areas-2050-says-un. Accessed 14 June 2024.