ANALYSES OF THE MIGRATION TO INTERNET PROTOCOL VERSION SIX (IPv6)

by

Isizoh A.N.[1], Okechukwu O.P.[2], Ani A.A.[3]

1: Dept. of Electronic and Computer Engineering, Nnamdi Azikiwe University, Awka, Nigeria.

2: Dept. of Computer Science, Nnamdi Azikiwe University, Awka, Nigeria.

3: Dept. of Computer Engineering, Madonna University of Nigeria, Akpugo Campus, Enugu State, Nigeria

ABSTRACT

Due to recent concerns over the impending depletion of the current pool of Internet addresses version 4 and the desire to provide additional functionality for modern devices, an upgrade of the current version of the internet protocol (IP), has been defined. This new version, called Internet Protocol version 6 (IPv6), resolves unanticipated IPv4 design issues and takes the internet into the 21st Century. This paper describes the problems of the IPv4 Internet and how they were solved by IPv6, IPv6 addressing, the new IPv6 header and its extensions. It provides a foundation of Internet standards-based IPv6 concepts and is intended for network engineers.

1.0 INTRODUCTION

1.1 Background of Study

IP (short for Internet Protocol) specifies the technical format of packets and the addressing scheme for computers to communicate over a network. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

IP by itself can be compared to something like the postal system. It allows you to address a package and drop it in the system, but there's no direct link between you and the recipient. TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time (Behrouz, 2020).

Every device on the Internet is assigned an IP address for identification and location definition. With the rapid growth of the Internet after commercialization in the 1990s, it became evident that far more addresses than the IPv4 address space has available were necessary to connect new devices in the future. By 1998, the Internet Engineering Task Force (IETF) had formalized the successor protocol. IPv6 uses a 128-bit address, theoretically allowing 2^{128}, or approximately 3.4×10^{38} addresses. The actual number is slightly smaller, as multiple ranges are reserved for special use or completely excluded from use. The total number of possible IPv6 address is more than 7.9×10^{28} times as many as IPv4, which uses 32-bit addresses and provides approximately 4.3 billion addresses.

The two protocols are not designed to be interoperable, complicating the transition to IPv6. However, several IPv6 transition mechanisms have been devised to permit communication between IPv4 and IPv6 hosts (Bradner and Mankin, 2015).

Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4. IPv6 is the successor to Internet Protocol Version 4 (IPv4). It was designed as an evolutionary upgrade to the Internet Protocol and will, in fact, coexist with the older IPv4 for some time. IPv6 is designed to allow the Internet to grow steadily, both in terms of the number of hosts connected and the total amount of data traffic transmitted.

IPv6 provides other technical benefits in addition to a larger addressing space. In particular, it permits hierarchical address allocation methods that facilitate route aggregation across the Internet, and thus limit the expansion of routing tables (Thaler et al., 2019). The use of multicast addressing is expanded and simplified, and provides additional optimization for the delivery of services. Device mobility, security, and configuration aspects have been considered in the design of the protocol.

IPv6 addresses are represented as eight groups of four hexadecimal digits with the groups being separated by colons, for example 2001:0db8:0000:0042:0000:8a2e:0370:7334, but methods to abbreviate this full notation exist.

IPv6 provides a number of advanced features, and the massive increase in address space capacity is indisputably unique to IPv6 and represents the crowning objective for IP-address-hungry organizations. Unfortunately, this increase in address space comes at the cost of different address formats and notations, which affect not only network layer routing, but also applications that display IP addresses (Dowin, 2019).

Organizations with existing IPv4 networks needing to implement IPv6 face challenges in identifying impacts, planning the transition and executing the migration to IPv6. Given the common organizational reliance on external communications for attracting new customers via the Internet, supporting dedicated partner links, home-based employees and providing Internet access for email, web browsing, etc (Droms et al., 2021).

2.0 LITERATURE REVIEW

Internet Protocol Version 4 (IPv4) was the first publicly used version of the Internet Protocol (Mike Leber, 2020). IPv4 was developed as a research project by the Defense Advanced

Research Projects Agency (DARPA), a United States Department of Defense agency, before becoming the foundation for the Internet and the World Wide Web. It is currently described by IETF publication RFC 791 (September 1981), which replaced an earlier definition (RFC 760, January 1980). IPv4 included an addressing system that used numerical identifiers consisting of 32 bits (Mullins, 2021).

These addresses are typically displayed in quad-dotted notation as decimal values of four octets, each in the range 0 to 255, or 8 bits per number. Thus, IPv4 provides an addressing capability of 2^{32} or approximately 4.3 billion addresses. Address exhaustion was not initially a concern in IPv4 as this version was originally presumed to be a test of DARPA's networking concepts. During the first decade of operation of the Internet, it became apparent that methods had to be developed to conserve address space. In the early 1990s, even after the redesign of the addressing system using a classless network model, it became clear that this would not suffice to prevent IPv4 address exhaustion, and that further changes to the Internet infrastructure were needed (Savola and Haberman, 2018).

The last unassigned top-level address blocks of 16 million IPv4 addresses were allocated in February 2011 by the Internet Assigned Numbers Authority (IANA) to the five regional Internet registries (RIRs). However, each RIR still has available address pools and is expected to continue with standard address allocation policies until one /8 Classless Inter-Domain Routing (CIDR) block remains. After that, only blocks of 1024 addresses (/22) will be provided from the RIRs to a local Internet registry (LIR). As at September 2015, all of Asia-Pacific Network Information Centre (APNIC), the Réseaux IP Européens Network Coordination Centre (RIPE_NCC), Latin America and Caribbean Network Information Centre (LACNIC), and American Registry for Internet Numbers (ARIN) have reached this stage. This leaves African Network Information Center (AFRINIC) as the sole regional internet registry that is still using the normal protocol for distributing IPv4 addresses (Deering, 2013).

By the beginning of 1992, several proposals appeared for an expanded Internet addressing system and by the end of 1992 the IETF announced a call for white papers. In September 1993, the IETF created a temporary, ad-hoc *IP Next Generation* (IPng) area to deal specifically with such issues. The new area was led by Allison Mankin and Scott Bradner, and had a directorate with 15 engineers from diverse backgrounds for direction-setting and preliminary document review: The working-group members were J. Allard (Microsoft), Steve Bellovin (AT&T), Jim Bound (Digital Equipment Corporation), Ross Callon (Wellfleet), Brian Carpenter (CERN), Dave Clark (MIT), John Curran (NEARNET), Steve Deering (Xerox), Dino Farinacci (Cisco), Paul Francis (NTT), Eric Fleischmann (Boeing), Mark Knopper (Ameritech), Greg Minshall (Novell), Rob Ullmann (Lotus), and Lixia Zhang (Xerox).

The Internet Engineering Task Force adopted the IPng model on 25 July 1994, with the formation of several IPng working groups. By 1996, a series of RFCs was released defining Internet Protocol version 6 (IPv6), starting with RFC 1883 (Version 5 was used by the experimental Internet Stream Protocol.).

It is widely expected that the Internet will use IPv4 alongside IPv6 for the foreseeable future. Direct communication between the IPv4 and IPv6 network protocols is not possible; therefore, intermediary trans-protocol systems are needed as a communication conduit between IPv4 and IPv6 whether on a single device or among network nodes (Bradner and Mankin, 2015).

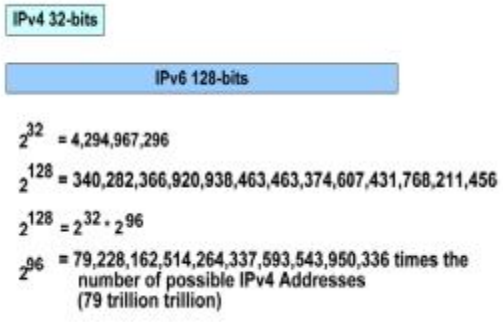
3.0 ANALYSIS OF INTERNET PROTOCOL VERSIONS 4 AND 6

3.1 IP Addressing

3.1.1 The Internet Protocol (IP):- It is the principal communications protocol in the internet protocol suite for relaying datagrams across network boundaries (Thaler et al., 2019). Its routing function enables internetworking, and essentially establishes the Internet.

3.1.2 Internet Protocol version 4 (IPv4):- It is the fourth version in the development of the Internet Protocol (IP) Internet, and routes most traffic on the Internet, it is a 32-bit long address of four bytes separated by colon(:), dot(.).

3.1.3 Internet Protocol version 6 (IPv6):- It is the sixth version in the development of the Internet Protocol (IP) Internet, and routes most traffic on the Internet, it is a 128-bit long address of sixteen bytes separated by colon(:).



The table 1 shows the differences between IPv4 and IPv6.

Table 1: Differences between IPv4 and IPv6

S/N	IPv4	IPv6
1.	Source and destination addresses are 32 bits (4 bytes) in length.	Source and destination addresses are 128 bits (16 bytes) in length.
2.	They are binary numbers represented in decimals.	They are binary numbers represented in hexadecimals.
3.	IP-Sec support is only optional.	In-built IP-Sec support.
4.	Broadcast messages are available.	Broadcast messages are not available. Instead a link-local scope "All nodes" multicast IPv6 address (FF02::1) is used for broadcast similar functionality.
5.	Manual configuration of IPv4 addresses or DHCP is required to configure IPv4 addresses.	Auto-configuration of addresses is available.
6.	Packet fragmentation is done by routers and sending hosts.	Packet fragmentation is done by sending hosts only.
7.	Address Resolution Protocol (ARP) uses broadcast ARP Request frames to resolve an IPv4 address to a link layer address.	ARP Request frames are replaced with multicast Neighbor Solicitation messages. For more information, see "Neighbor Discovery."

3.3 IPv6 Features

IPv6 is an Internet Layer protocol for packet-switched internetworking and provides end-to-end datagram transmission across multiple IP networks, closely adhering to the design principles developed in the previous version of the protocol, Internet Protocol Version 4 (IPv4). IPv6 was first formally described in Internet standard document RFC 2460, published in December 1998. In addition to offering more addresses, IPv6 also implements features not present in IPv4. It simplifies aspects of address assignment (stateless address autoconfiguration), network renumbering, and router announcements when changing network connectivity providers. It simplifies processing of packets in routers by placing the responsibility for packet fragmentation into the end points. The IPv6 subnet size is standardized by fixing the size of the host identifier portion of an address to 64 bits to facilitate an automatic mechanism for forming the host identifier from link layer addressing information (MAC address). Network security was a design requirement of the IPv6 architecture, and included the original specification of IPsec (Mullins, 2021).

IPv6 does not specify interoperability features with IPv4, but essentially creates a parallel, independent network. Exchanging traffic between the two networks requires translator gateways employing one of several transition mechanisms, such as NAT64, or a tunneling protocol like 6to4, 6in4, or Teredo.

3.4 IPv6 Address Syntax

IPv4 addresses are represented in dotted-decimal format. This 32-bit address is divided along 8-bit boundaries. Each set of 8 bits is converted to its decimal equivalent and separated by periods. For IPv6, the 128-bit address is divided along 16-bit boundaries, and each 16-bit block is converted to a 4-digit hexadecimal number and separated by colons.

The resulting representation is called colon-hexadecimal (Deering, 2013).

The following is an IPv6 address in binary form:

00100000000000010000110110111000000000
00000000000001011110011011
00000010101010100000000011111111111111
11000101000100111000010110 10

The 128-bit address is divided along 16-bit boundaries:

0010000000000001 0000110110111000
0000000000000000 0010111100111011
0000001010101010 0000000011111111
1111111000101000 1001110001011010

Each 16-bit block is converted to hexadecimal and delimited with colons. The result is:

2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A

IPv6 representation can be further simplified by removing the leading zeros within each 16-bit block. However, each block must have at least a single digit. With leading zero suppression, the address representation becomes:

2001:DB8:0:2F3B:2AA:FF:FE28:9C5A

3.4.1 Compressing Zeros

Some types of addresses contain long sequences of zeros. To further simplify the representation of IPv6 addresses, a contiguous sequence of 16-bit blocks set to 0 in the colon hexadecimal format can be compressed to "::", known as *double-colon*.

For example, the link-local address of AA80:0:0:0:2DA:0DCC:FA6A:004C can be compressed to AA80::2DA:0DCC:FA6A:004C. The multicast address FF02:0:0:0:0:0:0:2 can be compressed to FF02::2.

Zero compression can only be used to compress a single contiguous series of 16-bit blocks expressed in colon hexadecimal notation. You cannot use zero compression to include part of a 16-bit block. For example, you cannot express FF02:30:0:0:0:0:0:5 as FF02:3::5. The correct representation is FF02:30::5.

To determine how many 0 bits are represented by the "::", you can count the number of blocks in the compressed address, subtract this number from 8, and then multiply the result by 16. For example, in the address FF02::2, there are two blocks (the "FF02" block and the "2" block.) The number of bits expressed by the "::" is 96 (96 = (8 – 2)×16).

Note that zero compression can only be used once in a given address. Otherwise, you could not determine the number of 0 bits represented by each instance of "::".

3.5 Types of IPv6 Addresses

Unicast

Address of a single interface. One-to-one delivery to single interface.

Multicast

Address of a set of interfaces. One-to-many delivery to all interfaces in the set.

Anycast

Address of a set of interfaces. One-to-one-of-many delivery to a single interface in the set that is closest.

4.0 COMPARISON OF IPV6 WITH IPV4

On the Internet, data is transmitted in the form of network packets. IPv6 specifies a new packet format, designed to minimize packet header processing by routers. Because the headers of IPv4 packets and IPv6 packets are significantly different, the two protocols are not interoperable. However, in most respects, IPv6 is an extension of IPv4. Most transport and application-layer protocols need little or no change to operate over IPv6; exceptions are application protocols that embed Internet-layer addresses, such as FTP and NTP, where the new address format may cause conflicts with existing protocol syntax. Figure 1 shows IPv6 and IPv4 network with dual-stack router.

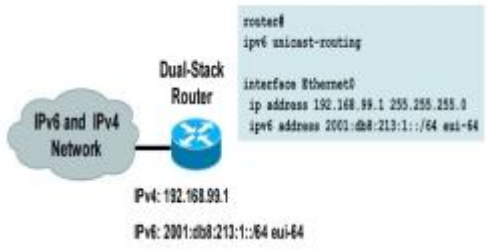


Figure 1: IPv6 and IPv4 network with dual-stack router

4.1 Larger address space

The main advantage of IPv6 over IPv4 is its larger address space. The length of an IPv6 address is 128 bits, compared with 32 bits in IPv4. The address space therefore has 2^{128} or approximately 3.4×10^{38} addresses.

In addition, the IPv4 address space is poorly allocated, with approximately 14% in 2011, of all available addresses utilized. While these numbers are large, it was not the intent of the designers of the IPv6 address space to assure geographical saturation with usable addresses. Rather, the longer addresses simplify allocation of addresses, enable efficient route aggregation, and allow implementation of special addressing features. In IPv4, complex Classless Inter-Domain Routing (CIDR) methods were developed to make the best use of the small address space.

The standard size of a subnet in IPv6 is 2^{64} addresses, the square of the size of the entire IPv4 address space. Thus, actual address space utilization rates will be small in IPv6, but network management and routing efficiency are improved by the large subnet space and hierarchical route aggregation.

Renumbering an existing network for a new connectivity provider with different routing prefixes is a major effort with IPv4. With IPv6, however, changing the prefix announced by a few routers can in principle renumber an entire network, since the host identifiers (the least-significant 64 bits of an address) can be independently self-configured by a host.

4.2 Multicasting

Multicasting, the transmission of a packet to multiple destinations in a single send operation, is part of the base specification in IPv6. In IPv4 this is an optional although commonly implemented feature. IPv6 multicast addressing shares common features and protocols with IPv4 multicast, but also provides changes and improvements by eliminating the need for certain protocols. IPv6 does not implement traditional IP broadcast, i.e. the transmission of a packet to all hosts on the attached link using a special *broadcast address*, and therefore does not define broadcast addresses. In IPv6, the same result can be achieved by sending a packet to the link-local *all nodes* multicast group at address ff02::1, which is analogous to IPv4 multicasting to address 224.0.0.1. IPv6 also provides for new multicast implementations, including embedding rendezvous point addresses in an IPv6 multicast group address, which simplifies the deployment of inter-domain solutions.

In IPv4 it is very difficult for an organization to get even one globally routable multicast group assignment, and the implementation of inter-domain solutions is arcane. Unicast address assignments by a local Internet registry for IPv6 have at least a 64-bit routing prefix, yielding the smallest subnet size available in IPv6 (also 64 bits). With such an assignment it is possible to embed the unicast address prefix into the IPv6 multicast address format, while still providing a 32-bit block, the least significant bits of the address, or approximately 4.2 billion multicast group identifiers. Thus, each user of an IPv6 subnet automatically has available a set of globally routable source-specific multicast groups for multicast applications.

4.3 Stateless address autoconfiguration (SLAAC)

IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the Neighbor Discovery Protocol via Internet Control Message Protocol version 6 (ICMPv6) router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet Layer configuration parameters.[15]
If IPv6 stateless address auto-configuration is unsuitable for an application, a network may use stateful configuration with the Dynamic Host Configuration Protocol version 6 (DHCPv6) or hosts may be configured manually using static methods.

4.4 Network-layer security
Internet Protocol Security (IPsec) was originally developed for IPv6, but found widespread deployment first in IPv4, for which it was re-engineered. IPsec was a mandatory specification of the base IPv6 protocol suite, but has since been made optional.

4.5 Simplified processing by routers
In IPv6, the packet header and the process of packet forwarding have been simplified. Although IPv6 packet headers are at least twice the size of IPv4 packet headers, packet processing by routers is generally more efficient, because less processing is required in routers. This furthers the end-to-end principle of Internet design, which envisioned that most processing in the network occurs in the leaf nodes.
The packet header in IPv6 is simpler than the IPv4 header. Many rarely used fields have been moved to optional header extensions.
IPv6 routers do not perform IP fragmentation. IPv6 hosts are required to either perform path MTU discovery, perform end-to-end fragmentation, or to send packets no larger than the default Maximum transmission unit (MTU), which is 1280 octets.

The IPv6 header is not protected by a checksum. Integrity protection is assumed to be assured by both the link layer or error detection and correction methods in higher-layer protocols, such as TCP and UDP. In IPv4, UDP may actually have a checksum of 0, indicating no checksum; IPv6 requires a checksum in UDP. Therefore, IPv6 routers do not need to recompute a checksum when header fields change, such as the time to live (TTL) or hop count.
The *TTL* field of IPv4 has been renamed to *Hop Limit* in IPv6, reflecting the fact that routers are no longer expected to compute the time a packet has spent in a queue.

4.6 Mobility
Unlike mobile IPv4, mobile IPv6 avoids triangular routing and is therefore as efficient as native IPv6. IPv6 routers may also allow entire subnets to move to a new router connection point without renumbering.

4.7 Options extensibility
The IPv6 packet header has a minimum size of 40 octets. Options are implemented as extensions. This provides the opportunity to extend the protocol in the future without affecting the core packet structure. However, recent studies indicate that there is still widespread dropping of IPv6 packets that contain extension headers.

4.8 Jumbograms
IPv4 limits packets to 65,535 (2^{16}–1) octets of payload. An IPv6 node can optionally handle packets over this limit, referred to as jumbograms, which can be as large as 4,294,967,295 (2^{32}–1) octets. The use of jumbograms may improve performance over high-MTU links. The use of jumbograms is indicated by the Jumbo Payload Option header.

4.9 Privacy

Like IPv4, IPv6 supports globally unique IP addresses by which the network activity of each device can potentially be tracked. The design of IPv6 intended to re-emphasize the end-to-end principle of network design that was originally conceived during the establishment of the early Internet. In this approach each device on the network has a unique address globally reachable directly from any other location on the Internet.

Network prefix tracking is less of a concern if the user's ISP assigns a dynamic network prefix via DHCP. Privacy extensions do little to protect the user from tracking if the ISP assigns a static network prefix. In this scenario, the network prefix is the unique identifier for tracking and the interface identifier is secondary.

In IPv4 the effort to conserve address space with network address translation (NAT) obfuscates network address spaces, hosts, and topologies. In IPv6 when using address auto-configuration, the Interface Identifier (MAC address) of an interface port is used to make its public IP address unique, exposing the type of hardware used and providing a unique handle for a user's online activity.

It is not a requirement for IPv6 hosts to use address auto-configuration, however. Yet, even when an address is not based on the MAC address, the interface's address is globally unique, in contrast to NAT-masqueraded private networks. Privacy extensions for IPv6 have been defined to address these privacy concerns, although Silvia Hagen describes these as being largely due to "misunderstanding". When privacy extensions are enabled, the operating system generates random host identifiers to combine with the assigned network prefix. These ephemeral addresses are used to communicate with remote hosts making it more difficult to track a single device.

Privacy extensions are enabled by default in Windows (since XP SP1), OS X (since 10.7), and iOS (since version 4.3). Some Linux distributions have enabled privacy extensions as well.

In addition to the "temporary" addresses mentioned above, there are also "stable" addresses: Interface Identifiers are generated such that they are stable for each subnet, but change as a host moves from one network to another. In this way it is difficult to track a host as it moves from network to network, but with-in a particular network it will always have the same address (unless the state used in generating the address is reset and the algorithm is run again) so that network access controls and auditing can be potentially be configured.

Privacy extensions do not protect the user from other forms of activity tracking, such as tracking cookies or browser fingerprinting.

Figure 2 shows IPV6 packet format.

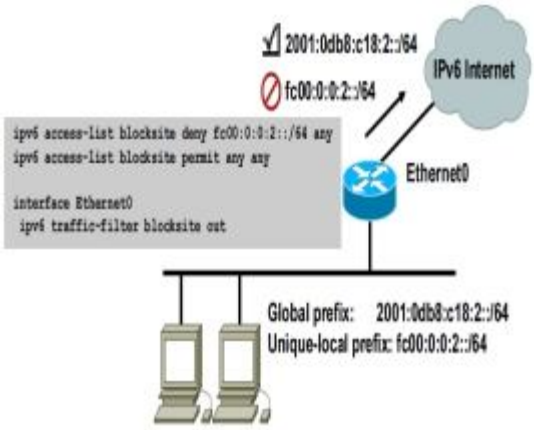


Figure 2: IPv6 Packet Format

4.10 IPv6 packet header

An IPv6 packet has two parts: a header and payload. The header consists of a fixed portion with minimal functionality required for all packets and may be followed by optional extensions to implement special features.

The fixed header occupies the first 40 octets (320 bits) of the IPv6 packet. It contains the source and destination addresses, traffic

classification options, a hop counter, and the type of the optional extension or payload which follows the header. This *Next Header* field tells the receiver how to interpret the data which follows the header. If the packet contains options, this field contains the option type of the next option. The "Next Header" field of the last option, points to the upper-layer protocol that is carried in the packet's payload.

Extension headers carry options that are used for special treatment of a packet in the network, e.g., for routing, fragmentation, and for security using the IPsec framework.

Without special options, a payload must be less than 64KB. With a Jumbo Payload option (in a *Hop-By-Hop Options* extension header), the payload must be less than 4 GB.

Unlike with IPv4, routers never fragment a packet. Hosts are expected to use Path MTU Discovery to make their packets small enough to reach the destination without needing to be fragmented.

5.0 MIGRATION MECHANISMS AND DEPLOYMENT

5.1 Migration Mechanisms

Pv6 is not foreseen to supplant IPv4 instantaneously. Both protocols will continue to operate simultaneously for some time. Therefore, some IPv6 transition mechanisms are needed to enable IPv6 hosts to reach IPv4 services and to allow isolated IPv6 hosts and networks to reach each other over IPv4 infrastructure.

Many of these transition mechanisms use tunneling to encapsulate IPv6 traffic within IPv4 networks. This is an imperfect solution, which reduces the maximum transmission unit (MTU) of a link and therefore complicates Path MTU Discovery, and may increase latency. Tunneling protocols are a temporary solution for networks that do not support native dual-stack, where both IPv6 and IPv4 run independently.

5.1.1 Dual IP Stack Implementation

Dual-stack (or *native dual-stack*) IP implementations provide complete IPv4 and IPv6 protocol stacks in the same network node. This facilitates native communications between nodes using either protocol. The method is defined in RFC 4213.

This is the most desirable IPv6 implementation during the transition from IPv4 to IPv6, as it avoids the complexities of tunneling, such as security, increased latency, management overhead, and a reduced PMTU. However, it is not always possible, since outdated network equipment may not support IPv6.

Dual-stack software design is a transitional technique to facilitate the adoption and deployment of IPv6. However, it might introduce more security threats as hosts could be subject to attacks from both IPv4 and IPv6. It has been argued that dual-stack could ultimately overburden the global networking infrastructure by requiring routers to deal with IPv4 and IPv6 routing simultaneously.

5.1.2 Tunneling

Many current Internet users do not have IPv6 dual-stack support, and thus cannot reach IPv6 sites directly. Instead, they must use IPv4 infrastructure to carry IPv6 packets. This is done using a technique known as *tunneling*, which encapsulates IPv6 packets within IPv4, in effect using IPv4 as a link layer for IPv6.

IP protocol 41 indicates IPv4 packets which encapsulate IPv6 datagrams. Some routers or network address translation devices may block protocol 41. To pass through these devices, UDP packets may be used to encapsulate IPv6 datagrams. Other encapsulation schemes, such as AYIYA or Generic Routing Encapsulation, are also popular.

Conversely, on IPv6-only Internet links, when access to IPv4 network facilities is needed, tunneling of IPv4 over IPv6 protocol occurs, using the IPv6 as a link layer for IPv4.

5.1.3 Automatic Tunneling

Automatic tunneling refers to a technique by which the routing infrastructure automatically determines the tunnel endpoints. Some automatic tunneling techniques are below.

6to4 is recommended by RFC 3056. It uses protocol 41 encapsulation. Tunnel endpoints are determined by using a well-known IPv4 anycast address on the remote side, and embedding IPv4 address information within IPv6 addresses on the local side. 6to4 is the most common tunnel protocol currently deployed.

Teredo is an automatic tunneling technique that uses UDP encapsulation and can allegedly cross multiple NAT nodes.[53] IPv6, including 6to4 and Teredo tunneling, are enabled by default in Windows Vista[54] and Windows 7. Most Unix systems implement only 6to4, but Teredo can be provided by third-party software such as Miredo.

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) uses the IPv4 network as a virtual IPv6 local link, with mappings from each IPv4 address to a link-local IPv6 address. Unlike 6to4 and Teredo, which are *inter-site* tunneling mechanisms, ISATAP is an *intra-site* mechanism, meaning that it is designed to provide IPv6 connectivity between nodes within a single organization.

5.1.4 Configured and Automated Tunneling (6in4)

6in4 tunneling requires the tunnel endpoints to be explicitly configured, either by an administrator manually or the operating system's configuration mechanisms, or by an automatic service known as a tunnel broker; this is also referred to as *automated tunneling*. Configured tunneling is usually more deterministic and easier to debug than automatic tunneling, and is therefore recommended for large, well-administered networks. Automated tunneling provides a compromise between the ease of use of automatic tunneling and the deterministic behavior of configured tunneling.

Raw encapsulation of IPv6 packets using IPv4 protocol number 41 is recommended for configured tunneling; this is sometimes known as 6in4 tunneling. As with automatic tunneling, encapsulation within UDP may be used in order to cross NAT boxes and firewalls.

5.1.5 Proxying and Translation for IPv6-only Hosts

After the regional Internet registries have exhausted their pools of available IPv4 addresses, it is likely that hosts newly added to the Internet might only have IPv6 connectivity. For these clients to have backward-compatible connectivity to existing IPv4-only resources, suitable IPv6 transition mechanisms must be deployed.

One form of address translation is the use of a dual-stack application-layer proxy server, for example a web proxy.

NAT-like techniques for application-agnostic translation at the lower layers in routers and gateways have been proposed. The NAT-PT standard was dropped because of criticisms; however, more recently, the continued low adoption of IPv6 has prompted a new standardization effort of a technology called NAT64.

5.2 Deployment

The 1993 introduction of Classless Inter-Domain Routing (CIDR) in the routing and IP address allocation for the Internet, and the extensive use of network address translation (NAT) delayed IPv4 address exhaustion. The final phase of exhaustion started on 3rd February 2011. However, despite a decade long development and implementation history as a Standards Track protocol, general worldwide deployment of IPv6 is increasing slowly. As at September 2013, about 4% of domain names and 16.2% of the networks on the Internet have IPv6 protocol support.

IPv6 has been implemented on all major operating systems in use in commercial, business, and home consumer environments. Since 2008, the domain name system can be used in IPv6. IPv6 was first used in a major world event during the 2008 Summer Olympic Games, the largest showcase of IPv6 technology since the inception of IPv6. Some governments including the Federal government of the United States and China have issued guidelines and requirements for IPv6 capability.

In 2009, Verizon mandated IPv6 operation and deprecated IPv4 as an optional capability for cellular (LTE) hardware.

As at 2014, IPv4 still carried more than 99% of worldwide Internet traffic. The internet exchange in Amsterdam is the only big exchange which publicly showed the IPv6 traffic percentage, which as of November 2015 was tracking at about 1.2%, growing at about 0.3 percentage points per year. As of 31 December 2015, the percentage of users reaching Google services with IPv6 reached 10.0% for the first time, growing at about 4.3 percentage points per year, although varying widely by region.

As at 18 April 2015, deployment of IPv6 on web servers also varied widely, with over half of web pages available via IPv6 in many regions, with about 16% of web servers supporting IPv6.

6.0 CONCLUSION AND RECOMMENDATION

6.1 Conclusion

Numerous IPv4-to-IPv6 transition mechanisms have been devised to readily enable the migration.

Leading router and operating system vendors already support IPv6, as well as various transition implementations. However, bringing it all together into a comprehensive migration plan for your network can be a daunting task. BT Diamond IP offers a number of services to assist with IPv6 readiness assessments, transition strategy analysis, migration plan development and execution and ongoing operations support. BT Diamond IP also offers its market-leading IP Address Management (IPAM) solution IP Control, the world's first integrated IPv4-to-IPv6 address management solution.

6.2 Recommendation

The migration from IPv4 to IPv6 is of great advantage to the present day (Jet age), talking about the vast availability of address spaces, security guarantee and abolishment of Network Address Translation (NAT).

REFERENCES

1. Behrouz A. Forouzan (2020), "Data Communications and Networking", Fifth Edition, McGraw-Hill International Edition, Pp. 73-91.
2. Bradner S., Mankin A. (2015), "The Recommendation for the IP Next Generation Protocol", Daaty Cookies Publishers, Scotland, PP. 17-33.
3. Thaler D., Handley M., Estrin D. (2019), "The Internet Multicast Address Allocation Architecture", Antar Drew Network Conference, USA, Pp. 24-58.
4. Droms J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney (2021), "Dynamic Host Configuration Protocol for IPv6 (DHCPv6), IECCE Conference, Canada, Pp. 65-79 (Proposed Standard).
5. Mc Dowin (2019), "IPv6 Address Allocation and Assignment Policy", RIPE NCC Publications, USA, Pp. 4-12.
6. Mike Leber (2020), "Global IPv6 Deployment Progress Report", Hurricane Electric, London, Retrieved on 19th October 2022.
7. Mullins Robert (2021), "Shadow Networks: An Unintended IPv6 Side Effect", Duwell Publications, Canada, Pp. 12-19.
8. Savola P., Haberman B. (2018), "Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address", Networking Conference Paper, Australia.

9. Deering S. (2013), “Host Extensions for IP Multicasting”, Internet World Conference, India, Pp. 3-9.
10. www. Google, internet protocol version 6, retrieved on 24th April, 2023.
11. www. Google, Network Mobility (NEMO) Basic Protocol Support, retrieved on 17th June, 2023.
12. www. Google, Unicast-Prefix-based IPv6 Multicast Addresses retrieved on 6th May, 2023.
.
Generation Computer Systems, 11:375-80.
Zhu N, Yu Z, Kou C. (2020), “A New Deep Neural Architecture Search Pipeline for Face Recognition”, IEEE Access, 8:91303-10.

