Adopting IPv6 in the Enterprise

LoyCurtis Smith

East Carolina University

Abstract

Despite efforts to extend IPv4 addressing with the introduction of private IP addressing, network address translation (one private IP to one public IP conversion), and port address translation (many private IPs to one public IP conversion), the world is still en route to an inevitable path. IPv4 will eventually be completely exhausted. This inevitable depletion lead to the inception of IPv6, which provides an immense amount more IP addresses per person than its predecessor as well as many other features. While IPv6 presents solutions to some of the design flaws of IPv4, it still has yet to be completely adopted worldwide. In the recent years it has slowly started becoming mandatory for particular entities to adopt this protocol. With this mandatory push towards its adoption it is imperative that it is known what all the adoption encompasses. Opposed to IPv4, IPv6 has built in security, its address space is composed of 128 bits instead of 32 bits, it has hexadecimal characters for the much longer addressing format, and etc. This paper will provide an in-depth analysis of the adoption of IPv6. It will do so by describing IPv6 and discussing its features in comparison with IPv4 as well as discussing the advantages, disadvantages, and obstacles organizations may face with its adoption.

Introduction

Since its deployment by the Internet Engineering Task Force (IETF) in 1981, Internet Protocol version 4 (IPv4) has been the main addressing standard. According to request for comment (RFC) 791, IPv4 has been the means of transporting datagrams from one system to another through an interconnected set of networks (i.e. the Internet) (Postel). Due to the expected expansion of the Internet and the increase of the amount of devices connecting to it, the 2^{32} (4,294,967,296) unique addresses that the Internet protocol offered were expected to one day become completely exhausted. The foresight of this evident exhaustion of Internet Protocol version 4 addresses in the early 1990s lead to the creation of Internet Protocol version 6 (IPv6) by IETF in 1998 (Das). According to Neal Leavitt in his article titled "IPv6: Any Closer to Adoption?" it was predicted by the chief scientist of the Asia-Pacific Network Information Centre (APNIC), Geoff Huston, that the exhaustion dates for IPv4 Address would be as follows:

- 12 February 2012 for European Networks
- 25 July 2013 for African Networks
- 17 December 2013 for US, Canada, and some Caribbean Islands
- 9 April 2014 for Latin American and other parts of the Caribbean (Levitt).

The initial intent of Internet Protocol Next Generation (IPV6) was to address the address space exhaustion of IPv4 as well as the many other shortcomings to include security. It has been nearly 20 years since its creation and it has yet to become to main Internet protocol. Engineers have been able to extend the use of its predecessor through the use of network address translation (NAT), private IP addressing, and port address translation (PAT). However despite these efforts we are on the last leg of the IPv4 address space. The adoption of IPv6 has been ramping up

slowly within recent years. Due to the inevitable exhaustion of IPv4 and the increased adoption of IPv6 it is imperative that one becomes familiar with this protocol. In order to assist with this familiarization this paper will be providing an in-depth analysis of the adoption of IPv6. It will do so by defining IPv6, discussing its features, providing a brief comparison with IPv4, as well as discussing the advantages, disadvantages, and obstacles organizations may face with its adoption.

What is IPv6?

Internet Protocol version 6, which is also referred to as Internet Protocol Next Generation (IPng), is the successor of IPv4 that addresses its addressing limitations and its lack of security. IPv6 is a 128-bit IP addressing protocol that the IETF began engineering in the early 1990s to address the addressing and security limitations, as well as performance, ease-of-configuration, and network management issues (Hermann-Seton). The first RFC, RFC 1883, for this protocol was published December 1995 by the IETF and has since been replaced by RFC 2460.

Ipv6 Features

IPv6 has a myriad of features that causes it to be a phenomenal protocol. There are many important Ipv6 features that a network professional will need to familiarize themselves with. The main characteristic that should be known is that an IPv6 address is composed of 128 bits, which allows it to offer a substantial amount more IP addresses for Internet usage. This section will cover most of the Internet Protocol Version 6 features that will provide a good understanding of what all it encompasses and what all must be considered when deploying it.

Expanded Addressing Capabilities
New Header Format
Improved Multicast Addressing

Efficient and Hierarchical Addressing and Routing Infrastructure
Security
Mobile Phone Network Support (MobileV6)
Stateless & Stateful Address Auto-Configuration
Neighbor Discover Protocol
Extensibility
Improved QoS Support

Table 1: IPv6 Features

Table 1 displays characteristics of Ipv6. As can be seen in the table IPv6 has the following features: expanded addressing capabilities, new header format, improved multicast addressing, an efficient and hierarchical addressing and routing infrastructure, security, mobile phone network support (MobileV6), stateless and stateful address auto-configuration, neighbor discover protocol, extensibility, and improved QoS support. The descriptions of the features are as follows:

- **Expanded Addressing Capabilities:** in IPv6 the IP address size is increased to 128 bits, to support more levels of addressing hierarchy, a much greater number of addressing nodes (Deering & Hinden). The 128-bit addressing space allows for 2^{128} (3.4×10^{38} or 340,282,366,920,938,463,463,374,607,431,768,211,456) total unique addresses (Shiranzaei & Khan).
- **New Header Format:** the IP header has been streamlined to minimize header overhead. The Ipv4 header checksum has been removed, which allows for faster router packet handling performance (Green). In addition the fragmentation fields and the IP options have been moved out of the base header, the header length field has been eliminated, the length field excludes the Ipv6 header, and the alignment was changed to 64 bits. The following revisions have also take place the time to live (TTL) hop limit, the protocol next header, and the precedence & type of service (TOS) traffic class (Hain).

- **Improved Multicast Addressing:** multicast support has been improved in Ipv6. Ipv6 uses the Multicast Listener Discover (MLD) protocol to allow nodes to join multicast groups. MLD is an integral part of Internet Group Management Protocol version 6 (ICMPv6) (Podermanki).
- **Efficient and Hierarchical Addressing and Routing Infrastructure:** The global addresses in Ipv6 used on the Ipv6 portion of the Internet create an efficient, hierarchical, and summarizable routing infrastructure that addresses common occurrence of multiple levels of Internet service providers (Ipv6 features).
- **Security:** Ipv6 is able to bind a public signature key to an Ipv6 address, which results in a Cryptographically Generated Address (CGA). CGA makes spoofing attacks harder and allows for messages to be signed with the owner's private key (Ipv6 Security). IP Security (Ipsec) is mandatory. It provides authenticity, integrity, confidentiality. Ipsec also provides traffic security services through the use of authentication header (AH) and Encapsulating Security Payload (ESP) (Kent & Seo).
    - **Mobile Phone Network Support (MobileV6):** the mobile IP protocol keeps continuity of communication between mobile nodes, without changing their IP address when connecting to other network access points (Xiaorong & Shizhun). This protocol allows for Ipv6 nodes to cache the binding of a mobile node's home address with its care-of (remote) address, and to send any packets destined for that node to its care-of address (Perkins & Johnson).
    - **Stateless & Stateful Address Auto-Configuration:** Ipv6 has the ability to obtain an IP address through stateful auto-configuration, which uses DHCP server, and stateless

auto-configuration, which does not utilize a DHCP server to assign and IP Address (Hermann-Seton). It is considered the Plug-N-play feature.

- **Neighbor Discovery Protocol (NDP):** in Ipv6 nodes use NDP to do the following: determine the link-layer addresses for neighbors known to reside on attached links and to quickly purge cached values that become invalid, to find neighboring routers that are willing to forward packets on their behalf. Finally, nodes use the protocol to actively keep track of which neighbors are reachable and which are not, and to detect changed link-layer addresses (Narten, Nordmark, Simpson, & Soliman).
- **Extensibility:** Ipv6 offers extension headers that can be placed between the Ipv6 header and the upper-layer header in the packet. The 6 extension headers offered are:
    - **Routing Header** -. Used to mandate a specific routing. Similar Ipv4 source routing options.
    - **Authentication Header (AH)** – Provides authentication and integrity.
    - **Encapsulating Security Payload (ESP) Header** – Provides authentication and encryption.
    - **Fragmentation Header** – Similar to Ipv4 fragmentation options.
    - **Destination Options Header** – contains a set of options to be processed by the final destination node. (ex: MobileV6).
    - **Hop-by-Hop Options Header** – A set of options needed by routers to perform certain management or debugging functions (Hermann-Seton).
- **Improved QoS Support –** Ipv6 introduces the Flow Label**,** which assists in traffic identification. The flow label allows routers to identify and provide special handling for packets that belong to a flow. A flow is a series of packets between a source and

destination. Because the traffic is identified in the Ipv6 header, support for QoS can be easily achieved even when the packet payload is encrypted with IPsec (Ipv6 features).

Comparison with IPv4

As earlier stated IPv6 was designed for the sole purpose of address the design flaws of IPv4. This section intends on comparing IPv4 and its successor IPv6 by stating the main differences between the two. Table 2 shows the main differences between IPv4 and IPv6.

IPv4	IPv6
32-bit Addressing Space	**128-bit Addressing Space**
Broadcast Addresses	**Built-In encryption and Authentication (IPsec)**
Manual configuration	**Auto-configuration**
Uses NAT	**Anycast Addressing**
No Inherent Security or Authentication	**Flow Label Field (Improved QoS)**
Options integrated in header fields	**Improved Header**
	Improved Multicast Addressing

Table 2: Ipv4 and IPv6 Comparison

In table 2 it can be seen that there are several differences between the two protocols. The main differences are the address space, IPv6 no longer uses broadcast addresses