IPv6

Jose Chaverra Say

ICTN 4060 - 601

Dr. Phil Lunsford

April 15, 2014

IPv6

1. Introduction

The Internet Protocol (IP) is the most widely used network protocol. IPv4 is a well-established protocol and, since its publication in 1981, only a few changes have been made to it. For many years it proved to be an efficient way to interchange data over a computer network. Ironically, IPv4's success is at the same time its own executioner. The expansion of the Internet around the world and the consequent hunger for internet presence will exhaust any world-wide availability of IPv4 addresses by July 2014. The Network Address Translator (NAT) is an educated way to incorporate more devices to the global network that the nominal capacity.

Soon after IPv4 was development, several security issues were raised. The industry moved towards security add-ons, and several protocols have been added to the TCP/IPv4 suite to meet the security requirements. However, their implementation is not mandatory since they were developed as different protocols, not as a set.

The IPv6 protocol emerged as a more effective solution to the addressing problem than the NAT used in IPv4, and as a built-in security suite. IPv6 can hold about $7.9 * 10^{28}$ times as many IP addresses as IPv4, totaling 2^{128} IPv6 addresses. Thus, the growth rate of devices connected to the Internet leads the experts to believe that IPv6 addresses will not be exhausted in this century. This new version of the Internet Protocol includes a mandatory security layer, quality of service capabilities, larger address space, compatibility with jumbograms, and multicast/anycast/unicast capabilities. The design of the header keeps open possibilities to add more security or capabilities to the protocol.

2. Why a new protocol?

About a decade after IPv4 publication, in the early 90s, concerns about exhaustion of address space began to arise. By 1995, one quarter of the total IPv4 addresses were leased, and by 2002, this number rose to two-thirds. Finally, by July 2014, all the IPv4 addresses world-wide will be depleted. One of the first attempts to solve the deficit in IP addresses was the Network Address Translator (NAT), a mechanism that uses a large set of IPv4 addresses for internal traffic and a small pool of IPv4 addresses for external usage. However, this mechanism creates some weaknesses in security since it significantly complicates the network topology and reduces VPN configuration options.

Geographic distribution of IPv4 addresses also affects the perception of the problem. North America, with a reduced population has 32% of all IPv4 addresses while the Asia / Pacific / Australia region only has 22% of the total IPv4 addresses as we can see in the figure 1. Thus, IPv6 is not perceived as an urgent matter in the US while it is vital in Asia.

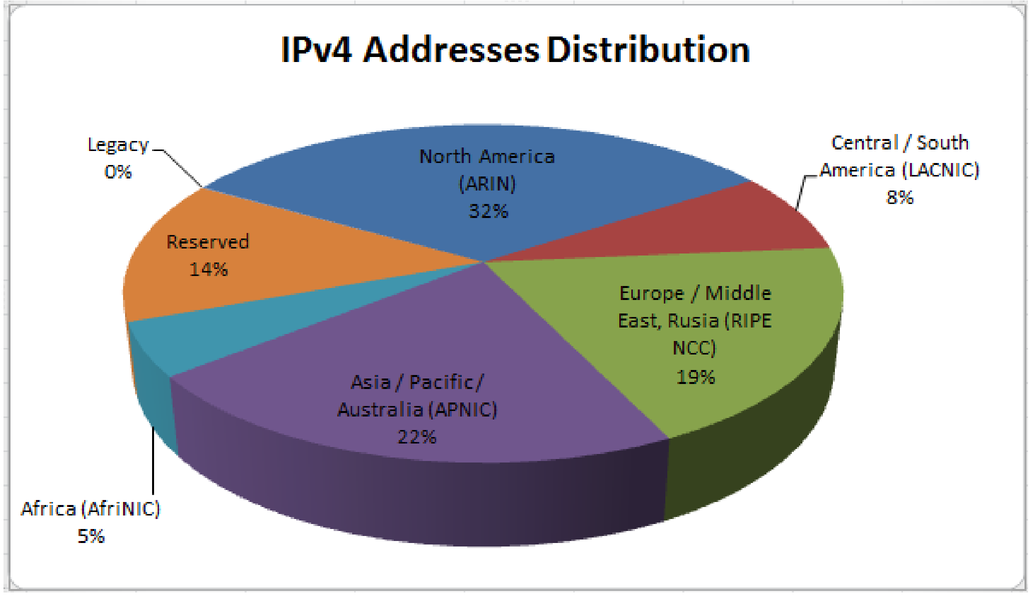

Figure 1: IPv4 addresses, geographic distribution

In addition, the intense usage of the Internet turned data integrity and confidentiality into an issue. An additional protocol, IPsec, was created as an option to the TCP/IPv4 suite to reduce security risks. However, IPSec is not mandatory in IPv4, and it is difficult to IPSec and NAT to coexist. In IPv4, IPSec is a solution to security, but it is a challenge to address space. Thus, IPv6 comes to be a solution for the exhausted addresses and security issues faced in the IPv4 networks as well as an improvement to the administrative workload and, very important nowadays, to the effectiveness of supporting mobile devices.

3. What is IPv6?

In 1998, the Internet Engineering Task Force (IETF) published the standard specification of the IPv6 in the Request for Comment (RFC) 2460. This protocol uses 128-bit addresses, totaling about $3.4*10^{38}$ (equivalent to 2^{128}) addresses, instead of the $4.29*10^{9}$ (equivalent to 2^{32}) total addresses allowed with the 32-bits IPv4 system. Comparatively, IPv6 ‘s addressing system allows about $7.92*10^{28}$ addresses per each IPv4 address or about 15 billion times the total IPv4 addresses per cm^{2} of the Earth’s surface. The new header has several improvements over the one in the previous protocol including flow label (QoS Management), next header, Hop limit, and source and destination address (128-bit each). Furthermore, the protocol provides security, quality of service, auto configuration, and better internet routing than IPv4.

Considering the enormous amount of new addresses, the old decimal-dotted system used in IPv4 for addressing is not effective in the new version of the protocol. IPv6 addresses are represented by 8 hexadecimal, 16-bits long fields that are separated by colon. A technique called zero compression leads to replace contiguous zeroes in an IPv6 address by double colons. According to Khaldoun Batiha, a Ph.D in Computer Engineering at Venitsia University, Ukraine, the Mixed Notation, a third method to express an IPv6 address, “has the first 96 bits in colon hexadecimal notation and the last 32 bits in dotted decimal” (436).

With the longer address system, a new IP header is required to accommodate all the possibilities. When compared with the IPv4 header, there are new fields in the IPv6 header, some fields have been removed, and others have been changed in a way that the new header is 40 bytes long or double the size of the IPv4 header without options (Figure 1).

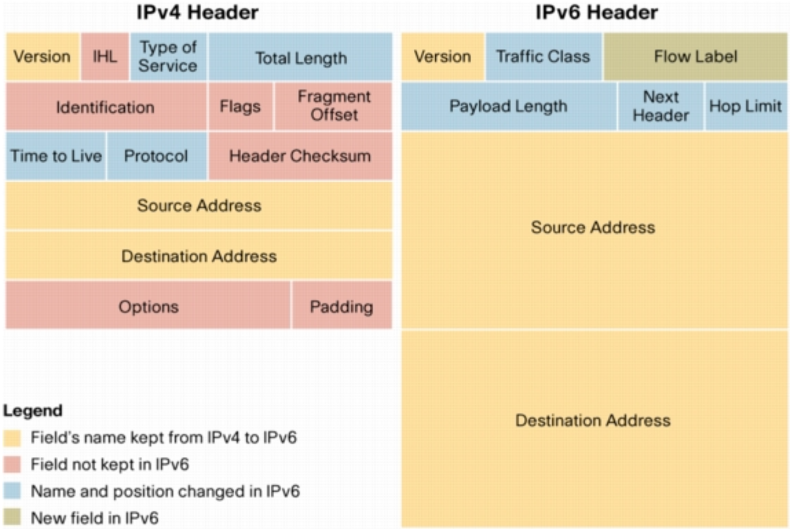

Figure 2:

IPv4 & IPv6 Headers (From Cisco.com)

This new header contains a 4-bit field for version (filled with the binary representation of the number 6), an 8-bits field for traffic class that is used to give priority to certain kinds of packets in a flow(QoS), a 20-bits field called flow label used for a source to mark packets that belong to the same flow of data, a Payload Length field of 16-bits that specifies the length of the message to be transmitted, an 8-bits field to identify the next header type, an 8-bits Hop Limit field that decreases its value by one unit by each node it passes through, a 128-bit field to the source IPv6 address, and a 128-bits field to the IPv6 destination address. An extension header is added only if it is needed, and it is connected to the original IPv6 header by the next header field. If more than one extension header is added, they are arranged by its importance for all nodes (IPv6 header, Hop-by-Hop Options header, Destination Options header, Routing header, Fragment header, etc.). A very important capability is that every extension header should include a next header field and it is not necessary to read each extension header in every node. This process of adding as many extension headers as necessary is called Header Chaining.

4. IPv6 Features

- Efficient Addressing and Routing infrastructure: Understanding routing as the process of forwarding packets between different connected networks, the 128-bits address source and 128-bits address destination allow IPv6 routers to have a more efficient routing table. According to Amer AbuAli, Associate professor of the Faculty of Information Technology at Philadelphia University, “on the IPv6, backbone routers have much smaller routing tables, corresponding to the routing infrastructure of Top-Level Aggregators” (585).
- Stateless and Stateful Address Configuration: IPv6 can work with or without DHCP Servers. The RFC 4862 frame the IPv6 Stateless Address Configuraion: When not DHCP Servers are enabled in the network, the Neighbor Discovery Protocol (NDP) provides information to a plug-and-play auto configuration. Hosts use the link-local address auto configuration with information about their MAC addresses and the advertising from local routers. If a node detects that its tentative address in not unique, auto configuration stops and manual configuration is required for that specific node. Thus, IPv6 routers advertise themselves periodically using the rules defined in the NDP.
- Quality of Service (QoS): The Flow Label field in the IPv6 header defines how to handle traffic and guarantee end-to-end information integrity. However, QoS benefits are a battlefield between different authors. While for some authors “IPv6 QoS is neither better nor worse than IPv4 QoS. It follows the same architectural models and faces the same inherent challenges”

(Batiha 439), for other the 20-bits flow label in the IPv6 header can be used to request special handling by the IPv6 routers. This capability is still experimental and not all routers are able to process the flow label field.

- Security: In IPv6, supporting IPsec is not optional. Under the RFC4301, IPSec is mandatory in all the IPv6 nodes. Furthermore, the Security Architecture for the Internet Protocol (RFC 2401) frames the IPSec security features of IPv6: IP Authentication Header (RFC 2402) uses MD5 (RFC2403) and SHA (RFC 2404) as authentication algorithms, and IP Encapsulating Security Payload (RFC 2406) uses DES CBC (RFC2405) as encryption algorithms, the key management is done through ISAKMP (RFC 2408) and IKE (RFC 2409) . However, an intermediate step is necessary to negotiate security associations; Domain of Interpretation (RFC 2407) ensures proper communication with ISAKMP.

  Thus, IPSec acts as the first security front and all the protocols that form IPSec act in the network layer. The built-in security in IPv6 addresses DoS attacks, replay attacks, man-in-the middle attacks, spying, sniffers, data modification, identity spoofing by ensuring authentication and data encryption, and preventing replaying old packets. The security architecture relies on authenticating the header and encrypting the payload using key interchange algorithms based on Diffie Hellman Key-Exchange.

  There are two different modes available for the IPSec, transport and tunnel mode depending on the topology of the connection.

- Multicast: Multicast support is mandatory in IPv6. With this feature, it is possible to send packets to multiple destinations. However, IPv6 multicast is different from IPv4 broadcast (not supported in IPv6) since in multicast the packets are sent to a defined pool of addresses while in broadcast the packets are sent to all addresses in the subnet.

- Neighbor Node Interaction: The Internet Control Message Protocol version 6 (ICMPv6) adds new capabilities to IPv6 over IPv4 Address Resolution Protocol (ARP), ICMPv4 Router discovery and ICMPv4 Redirect. ICMPv6 allows the Neighbor Discover Protocol (NDP). Using NDP, a host can discover neighbor routers, addresses, address prefixes, etc. The NDP allows routers to advertise themselves about their configuration parameters and "better next-hop address to forward packets for a specific destination" (Batiha 440). Using NDP hosts can identify if another host is still reachable and they can resolve link-layer address of a neighbor node.
- Mobility: With Mobile IPv6, a mobile node (device) can move through different links keeping its home address, and packets should be routed to the mobile node no matter its current point of access to the Internet. However, Mobile IPv6 can manage link interchange in a homogeneous media (Ethernet segments, for example), but not across a heterogeneous media.
- Extensibility: Adding as many extension headers as is necessary, IPv6 can be extended to new features. This contrasts to the limited 40-bits options for IPv4.
- Anycast: A single host can send a message to anyone of a group of hosts sharing the same anycast address, usually to the nearest one.
- Jumbograms: A jumbogram is defined as an IPv6 packet with a payload that exceeds the 65,535 octets and only works links with link-MTU (Maximum Transmission Unit) larger than 65,535 octets. Larger payloads mean that the ratio of payload-length to header-length is higher, resulting in less wasted bandwidth. The standard payload size is defined by the 16-bit payload length field in the IPv6 headers. However, the Jumbo Payload option makes possible

transmission of packets with sizes up to 4,294,967,295bits (4GB) since this option has a 32-bit payload length field. Jumbograms can be used with TCP and with a modified version of UDP specified in the RFC2675.

5. IPv6 / IPv4 transition mechanisms

Both IPv4 and IPv6 are called to coexist for a long period of time until IPv6, or a new protocol, completely replaces IPv4. Since they are not compatible protocols, transitional mechanisms are necessary during the provisional time in which both protocol are used. The Internet Engineering Task Force (IETF) attacked this incompatibility problem from three approaches: dual-stack, tunneling and translation mechanisms.

The dual-stack mechanism's specification in the IETF RFC2893 states that, during the transitional period, network nodes should include both IPv4 and IPv6 protocols stacked in parallel. Thus, "IPv4 applications use IPv4 stack and IPv6 application use the IPv6 stack" (Punithavathani 111). Almost every one of the modern Operating Systems (OS) and network devices include dual IP protocol stacks.

Tunneling mechanisms allow IPv6 and IPv4 to be bridged. There are three accepted tunneling mechanisms to ensure communication across IPv4 and IPv6 networks:

- IPv6 over IPv4 mechanism basically inserts an IPv4 address in the link-layer identifier part of the IPv6 address, then uses local multicast to define an IPv4 version of ND. This mechanism is effective when isolated IPv6 Islands (IPv6 domain) are present in an IPv4 ocean.
- IPv6 Tunnel Broker is defined by the IETF RFC 3053 and requires IPv4 connectivity between the final user and the tunnel broker service provider. In this mechanism, the tunnel broker works like a virtual ISP, allocating IPv6 address block to users and sets up IPv6/IPv4 tunnels for the final users.

- IPv6 to IPv4 Automatic Tunneling Mechanism uses a technique similar to IPv6 over IPv4 and allows isolated IPv6 domains to communicate over an IPv4 network but it does not require manual management. According to Punithavathani, Registrar at Anna University Tirunelveli, India, "the embedded IPv4 address can easily be extracted and the whole IPv6 packet delivered over the IPv4 network, encapsulated in an IPv4 packet" (112)
- A fourth tunneling mechanism is called Teredo and is an IPv6 tunneling over UDP service. However, it relies in UDP to transmit data, making this tunneling mechanism limited to certain applications.

The third approach to solving the incompatibility between the two IP versions is two translations mechanisms.

- Bump-In-the-Stack (BIS) allows an IPv6 host to communicate with other IPv6 hosts using IPv4 applications. Under the IETF RFC 2767, BIS includes a translator module divided in Extension Name Resolver, Address Mapper and the translator itself layered above IPv6. The Extension Name Resolver determines if a node is IPv6 only by examining the DNS lookup. The Address Mapper keeps an IPv4 address spool and issues one of those when the resolver or the translator requests it.
- Network Address Translation-Protocol Translation (NAT-PT) as well as BIS uses a pool of IPv4 addresses for assignment to IPv6 nodes dynamically. This protocol can be used as traditional NAT-PT (v6 network to access hosts in v4 networks) or Bi-Directional NAT-PT (connections are established in both directions v6-to-v4 and v4-to-v6). According to the RFC 2766, "a fundamental assumption for NAT-PT is only to be use when no other native IPv6 or IPv6 over IPv4 tunneled means of communication is possible" (Tsirtsis 2).

5. Conclusion

IPv4 is progressively being replaced with IPv6 and, in the future IPv4 will disappear completely off the Internet, but the transitional period is predicted to be long. Since these two protocol suites are not interoperable by themselves, they should interoperate by transitional mechanisms. The advantages of IPv6 include the enormous amount of addresses that it can handle, larger payloads, built-in security protocol, options for Quality of Service, and auto configuration options with NDP, the integrated mobile IP and the multicast, unicast/anycast/multicasts ways to reach one or more hosts. Furthermore, the extensibility is, probably, the feature that will keep IPv6 as the predominant Internet Protocol for many coming years.

IPv6 is not a totally secure protocol (or set of protocols), but it presents several security improvements when compared to IPv4. By authenticating the header, encrypting the payload, and adding a field for a next header, IPv6 provides a security baseline for network transmission.

IT field seems like it is moving towards wireless transmission, many mobile devices are added to digital networks every day. IPv6 is very efficient to handling mobile devices as long as the transmission occurs in a homogeneous media. Furthermore, the 128-bits addressing system is capable of managing the expansion of mobile devices in the next decades.

There are many challenges in data security, transmission speed, availability, and device interconnection and reachability that only IPv6 can possibly address for a reasonable period of time. New threats and challenges could lead the industry to adopt a new protocol, or set of protocols, but for now, IPv6 is the best tool we have to manage data transmission over a computer network.

Works Cited

AbuAli, Amer, Ismail Shayeb, Khaldoun Batiha, and Haifa Aliudos. "The Benefits of Using Internet Protocol Version 6 (IPv6)." *International Review on Computers & Software* 5.6 (Nov2011): 583-87. *Academic Search Alumni Edition*. Web. 7 Mar. 2014. <http://ehis.ebscohost.com.ezproxy.cfcc.edu/ehost/detail?sid=eddba19c-f779-454b-98d8-77edebc8c127%40sessionmgr110&vid=1&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=70136721>.

Batiha, Khaldoun, Khaled Batiha, and Amer AbuAli. "THE NEED FOR IPv6." *International Journal of Academic Research* 3.3 (May 2011): 431-48. *Academic Search Alumni Edition*. Web. 27 Feb. 2014. <http://ehis.ebscohost.com.ezproxy.cfcc.edu/ehost/detail?sid=a24234b4-5eac-4ea7-8ffe-cefa327b8720%40sessionmgr111&vid=5&hid=109&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=69707623>.

Borman, D., S. Deering, and R. Hinden. "RFC 2675 - IPv6 Jumbograms." *IETF Tools*. Aug. 1999. Web. 27 Mar. 2014. <http://tools.ietf.org/html/rfc2675>.

Dawood, Harith. "IPv6 Security Vulnerabilities." *ESBCOHost*. International Journal of Information Security Sciense. Dec2012, Vol. 1 Issue 4, p100-105. 6p. Web. 01 Apr. 2014 < http://eds.a.ebscohost.com.jproxy.lib.ecu.edu/ehost/detail?vid=4&sid=124f83cb-9ffe-410f-bb61-7aa2888b45d1%40sessionmgr4005&hid=4102&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=88128446>

Deering, S., and R. Hinden. "RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification." *IETF Tools*. Dec. 1998. Web. 01 Apr. 2014. <http://tools.ietf.org/html/rfc2460>.

Huitema, C. "RFC 4380 - Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)." *IETF Tools*. Feb. 2006. Web. 02 Apr. 2014. <http://tools.ietf.org/html/rfc4380>.

"IPv6 Extension Headers Review and Considerations." *Cisco*. Oct. 2006. Web. 01 Apr. 2014. <http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html>.

“IPv6 Quality-of-Service Capabilities” *Oracle*. N.P., 2010. Web. 01 Apr. 2014 <http://docs.oracle.com/cd/E19683-01/817-0573/chapter1-25/index.html>

Johnson, D., C. Perkins, and J. Arkko. "Mobility Support in IPv6." *Internet Engineering Task Force*. June 2004. Web. 1 Apr. 2014. <http://www.ietf.org/rfc/rfc3775.txt>.

Punithavathani, D. Shalini, and K. Sankaranarayanan. "IPv4/IPv6 Transition Mechanisms." *European Journal of Scientific Research* 34.1 (Jul2009): 110-24. *Academic Search Alumni Edition*. Web. 7 Mar. 2014. <http://ehis.ebscohost.com.ezproxy.cfcc.edu/ehost/detail?sid=4af1345d-7ecb-44f7-be25-4185c1b6e684%40sessionmgr12&vid=1&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=44066165>.

Thomson, S., T. Narten, and T. Jinmei. "RFC 4862: IPv6 Stateless Address Autoconfiguration." *IPv6 Stateless Address Autoconfiguration*. Internet Engineering Task Force (IETF), Sept. 2007. Web. 03 Apr. 2014.

Tsirtsis, G., and P. Srisuresh. "RFC 2766 - Network Address Translation - Protocol Translation (NAT-PT)." *IETF Tools*. Feb. 2000. Web. 01 Apr. 2014. <http://tools.ietf.org/html/rfc2766>.

Tsuchiya, K., H. Higuchi, and Y. Atarashi. "RFC 2767 - Dual Stack Hosts Using the Bump-In-the-Stack Technique (BIS)." *IETF Tools*. Feb. 2000. Web. 02 Apr. 2014. <http://tools.ietf.org/html/rfc2767>.