IPv6 – The Future of the Internet

Submitted by:
Jennifer R. Lee
Athabasca University
Student #2634263

August 18, 2015
Summary
IPv6 has become the essential protocol of the Internet. Without IPv6, the Internet could not grow and evolve to connect more people and devices, resulting in billions of people deprived of new Internet services and applications on the drawing boards of today’s companies and in the imaginations of tomorrow’s entrepreneurs. This essay provides an overview of IPv6’s principles and key functionalities, including a technical explanation of how IPv6 works with related protocols such as Mobile IP and IPSec. As well, the background of IP and the deployment of IPv6 is discussed, accompanied by strong reasons for enterprises to embrace this new platform, allowing societies to continue evolving and connecting via the Internet.
IPv6 is the sixth version of the Internet Protocol (IP) and was designed initially to connect hosts across multiple networks. IP provides a way of moving a block of data (also known as a datagram) from one host machine to another through the Internet. The delivery of the datagrams are made possible by assigning an IP address to every host in the Internet. IP is the lowest layer protocol defined in the IP suite, runs on top of whatever protocols are in use in the physical network of a computer network (ie: Ethernet, X.25, token ring, serial, ATM, Frame Relay, wireless networks, etc.) and is an unreliable (connectionless) protocol. This means that datagrams sent from one host to another may not be delivered in the order in which they were sent, may be delivered more than once, or may not be delivered at all. (Umar, 2010)

IPv6, also known as the “next generation IP” (IPng), corrects this deficiency within the Internet and its networks, not only via providing a new addressing scheme to ensure datagram delivery, but also through improvements such as routing and network auto-configuration. (Umar, 2010)

The previously adopted version of IP, known as IPv4, had only 4.3 billion addresses available for use. With PCs, smartphones, tablets, gaming systems, and just about everything else connected to the Internet, the IPv4 system has become outdated. (Bradley, Tony, 2011) By the time IPv6 was more widely adopted in 2014, more than 4 billion devices had already been sharing IP addresses. (Carrol, Leigh-Ann, 2014)

The shortage was due to the IPv4 design and addressing scheme as it utilizes IP addresses which are 32 bits in length, commonly denoted as four decimal numbers separated by periods (ie: 12.345.223.2). The first part of the address showed which network the host resided on, and
the rest of the address shows where, within that network, that the host can be found. (Umar, 2010) As the Internet grows, it becomes more challenging to find hosts and mobile devices.

IPv6 uses 128-bit addresses, capable of creating 340 undecillion addresses (340 trillion trillion trillion possible IP addresses). (Bradley, Tony, 2011) It also looks completely different with eight groups of four letters and numbers separated by colons (ie: 2001:db8:1f70:999:de8:7648:6e8). The expanded addressing capacity enables trillions of addresses to support connectivity for a range of smart devices such as phones, household appliances, vehicles (The Internet Society, 2015), and smart watches. (Carrol, Leigh-Ann, 2014)

IPv6 works in a variety of ways with different devices. For example, in WLANs (wireless local area networks), IP addresses are assigned to devices via a network application protocol (software program known as DHCP - Dynamic Host Configuration Protocol) that runs on a network server, automatically assigning an IP address when a device that is connected to that server is turned on. (Umar, 2010) Another example, in cellular networks, assigned telephone numbers are used to locate cellular users, but are translated to IP addresses by cellular network providers. Thus, to use WLANs and cellular networks, there must be an abundance of IP addresses available to match demand. (Umar, 2010)

The “Mobile IP” protocol developed with IPv6 allows mobile devices (ie: PDAs and laptops) to maintain Internet connectivity while moving from one Internet attachment point to another. In Mobile IP, the IP addresses are assigned by Network Service Providers (NSPs), also known as Internet Access Providers (IAPs), and routing occurs to direct Internet traffic from one point
to another. Traffic is forwarded using a “care of” address, accomplished through an Internet router (an Internet gateway). Routers are software programs found inside dedicated computers and shuffle messages between physical networks. As the IP network grows it becomes complex, including the router’s role, as routers must understand the network topology, knowing how to get the message to the next router. Since routers are responsible for routing messages to a destination network (not to a destination host), it becomes a challenge if enterprises cannot present globally unique addresses to the Internet - resulting in messages not arriving at intended destinations. (Umar, 2010)

Cellular network technology now relies on Mobile IPv6 to control handoffs (exchanges between cellular network providers). With Flash OFDM architecture, a 3G cellular network technology, radio routers act as base stations, IP routers route the IP traffic and media gateways convert IP to PSTN traffic. These components are simultaneously used to complete actions on behalf of the device, allowing for the device to be mobile (wireless). In this type of system, mobile devices (referred to as nodes) move between their “home network” and “foreign networks”, with their home agent intercepting packets (sent to the mobile node’s home address) and redirecting them to a “care-of-address” of the foreign agent (while the mobile node continues transmitting packets directly to the origin node within the cell). So as mobile devices move from one location to another and acquire new IP addresses, mobile IP shuffles the messages to the new IP addresses. (Umar, 2010)

Most homes and small business have only have one IP address on the Internet, assigned to the router that connects them to their ISP (Internet Service Provider). The router in turn issues IP addresses internally to devices attached to it, but must constantly track which traffic belongs
to which device, translating the IP address from the internal one to the public one. (Bradley, Tony, 2011). All of this activity taxes networks and devices when the supply of IP addresses fails to match demand.

Thus, the features with IPv6 are easier ISP switching, network control (Carrol, Leigh-Ann, 2014), and the ability to support a large range of next-generation network applications and services. (Das, Kaushik, 2008). Another is an inherent firewall, known as IPSec (IP Security). The newer large address space design, described above, allows for multiple levels of subnetting and address allocation from the Internet backbone to the individual subnets within an organization. This removes the need for address-conservation techniques (by re-using IP addresses) through NATs (Network Address Translators). (Das, Kaushik, 2008)

NATs modify network address information in IP datagram packet headers and remap one IP address space into another (Carrol, Leigh-Ann, 2014). NATs recycle IPv4 addresses but are a temporary solution (at the service provider level). Large scale NATs result in users sharing their IP address with hundreds of network neighbours simultaneously, reducing performance and capabilities for end users, and creating higher costs and management complexity for service providers. NATs are an issue with subscriber identity, creating implications for advertisers, content providers, and law enforcement who rely on location-based services. (The Internet Society, 2015)

Translating addresses via NATs does not provide the benefit of security. NATs require outgoing connections to be present before allowing incoming connections to succeed. (The Internet Society, 2015) Thus a huge improvement that arrives with IPv6 is the built-in security of IPSec
which is mandatory, part of the IPv6 protocol. The new “header extensions” in IPv6 ease the implementation of encryption, authentication, and Virtual Private Networks (VPNs). IPSec functionality is basically identical in IPv6 and IPv4, however within IPv6 IPSec can be utilized along the entire route (source to destination). (Das, Kaushik, 2008) The integrity and authenticity of IPv6 packets are ensured through encryption. Techniques aimed at preventing packet spoofing ensure Internet traffic gets to the correct destination without being intercepted (Bradley, Tony, 2011), providing VPN-like protection for standard Internet traffic. (Carrol, Leigh-Ann, 2014) Security in IPv4 is difficult in when NATs are present as they disrupted IP layer traceability and audit trails, and the use of address rewriting that NATs perform is considered by some security protocols to be a security violation. (The Internet Society, 2015)

IPv6 brings enhanced quality of service (QoS), required for applications like IP telephony, video/audio, interactive games or e-commerce. (The Internet Society, 2015) IPv6’s new header and extension header also make it easier to integrate future features and services without having to rewrite the protocol. (Das, Kaushik, 2008) Thus header overhead is minimized by moving non-essential fields and optional fields to extension headers, leading to efficient processing at intermediate routers.

Thus, IPv6 achieves end-to-end security, mobile communications, quality of service (QoS), and simplified system management. (Das, Kaushik, 2008)

The challenges in IPv6 are added performance overhead, increased complexity and some complications with IPSec. (Carrol, Leigh-Ann, 2014) Also, with network needs and businesses differing, IPv6 transition strategies and related costs can include operational costs (ie: staff
training) and one-time administrative costs (ie: adding IPv6 to management databases and upgrade documentation processes). Organisations running in-house customized software may experience upgrade costs (ie: IPv6 configuration testing). (The Internet Society, 2015)

The switch from IPv4 to IPv6 is still in progress as IPv4 naturally phases out. NATs are still used as IPv4 and IPv6 run as parallel networks, exchanging data via special gateways because the software and routers on the networks must be upgraded to support IPv6. (Parr, Ben, 2011) This can result in the use of “tunneling”, creating an IPv6 tunnel through an IPv4 packet. Thus, “tunnel brokers” exist to provide IPv6 tunnels to sites or end users over IPv4, and vice versa. (Tunnel Brokers, n.d.)

IPv4 has lasted over 3 decades despite some challenges. IP was introduced in 1969 to support file transfers and emails between less than 100 DARPA (Defence Advanced Research Projects Agency) researchers on very slow networks (300 bps or less) that existed circa 1970. (Umar, 2010) Briefly, IPv4 was followed by IPv5 (referred to as Internet Stream Protocol) in the 1980s, but not widely deployed because it was an experimental protocol.

In 1998, anticipating the shortage of IP addresses, the Internet Engineering Task Force (IETF), an global group concerned with developing technical standards for the evolving Internet, published the first basic IPv6 protocol. In 2004, IETF added the Mobile IPv6 specifications. (The Internet Society, 2015)

On January 12, 2011, “World IPv6 Day” was announced as a readiness-testing and publicity event to raise awareness, sponsored and organized by the Internet Society with the key support
of Facebook, Google, Yahoo, Akamai Technologies, and Limelight Networks. (World IPv6 Day, n.d.) Testing deployment readiness can be a “chicken and egg” issue, as websites can’t test effectively without the networks and equipment vendors being ready and vice versa. (The Internet Society, 2015) The objective: test IPv6 on a global scale. It came at the right time because in February 2011, the last block of the 4.3 billion IPv4 addresses were assigned from the global supply, meaning no remaining IPv4 address space existed for distribution. Then, only 12 percent of businesses had started planning for the transition with six percent indicating they had no awareness of IPv6 at all. (Daigle, 2012)

The testing event started at 00:00 UTC on June 8, 2011 and ended 23:59 the same day. The real world effects of IPv6 became known as 400+ industry participants (ISPs, hardware makers, operating system vendors and web companies) enabled IPv6 on their main websites for 24 hours and began to officially prepare their services for IPv6 to ensure a successful transition before address space ran out. (World IPv6 Day, n.d.)

Impact varied depending on hardware, Internet service and Web services that individuals were trying to access. Rare cases of broken IPv6 connectivity occurred due to misconfigured or misbehaving equipment (e.g., home routers) or software (e.g., firewalls), impacting approximately one Internet user in every 2,000. (The Internet Society, 2015) Early results indicated the day passed according to plan without significant problems for participants. Facebook even left their developer site IPv6-enabled. However, more work had to be done before IPv6 could consistently be implemented. (World IPv6 Day, n.d.)
McGill University was one of the few universities worldwide to be IPv6-compatible on World IPv6 Day. McGill, a leading research university based in Montreal, Quebec, wanted to demonstrate that they were ready to support IPv6 as a component of an overall network modernization effort. They chose to implement the IPv6 Gateway™ feature, built into the F5® BIG-IP® Local Traffic Manager™. By taking advantage of features in the F5 products that McGill already owned, they saved time and money and proved to their management that they could to support IPv6. (Canadian University Gets Ready for IPv6 with Easy-to-deploy F5 Solution, 2012)

June 6, 2012 was the official “World IPv6 Launch”, resulting in IPv6 being permanently enabled on all participating sites. The event was billed as “this time, it's for real”. (World IPv6 Day, n.d.) In 2014 it was reported that IPv6 connectivity had more than tripled with Google users, set to become the dominant protocol by 2018. Today, tens of thousands of websites are using IPv6. (Carrol, Leigh-Ann, 2014)

For enterprises to deploy IPv6, an abundance of support and information exists. IPv6 benefits from over a decade of development, thus the core standards have been stable for years, deployed in both research and operational contexts. (The Internet Society, 2015) In Canada, CANARIE (Canada’s Advanced Research and Innovation Network) and BCNET (the Shared IT Services Organization for Higher Education in British Columbia) provide universities and colleges with free access to an IPv6 Community Lab to help prepare their networks for upgrades to IPv6. (CANARIE and BCNET helping Canadians get ready for IPv6 transition, 2012)
However, it has been said that “there is no business case” for deploying IPv6 with companies viewing it as an expense with no associated increase in revenue, or they believe they can get by with interim workarounds like NAT. The fact is that the long-term overall cost of not deploying IPv6 is more costly to both companies looking to grow and to the Internet as a whole. Therefore, enterprises should have IPv6 on their strategic roadmap and deploy it soon if they have not already. (Daigle, 2012)

Deploying IPv6 prevents increased costs in the long-term (in workarounds, buying networking gear, buying more IPv4 addresses), prevents disruption to websites (risking accessibility problems to websites and Internet-connected locations and services), facilitates global growth, avoids diminishing experiences for customers and/or access to supply chains, and helps a firm remain competitive. The only long-term solution is to adopt IPv6. (Daigle, 2012)

Those who run IT services should plan for IPv6 as with any major service upgrade, do an audit of current IPv6 capabilities and readiness, assess the level of IPv6 technical knowledge within staff and make plans for staff development and training that supports IPv6 implementation. Examine those services that will lose business if only accessible to IPv4-users and make them a priority for IPv6 capability (ie: plan to implement an IPv6-enabled front-end Web server immediately, before converting the internal network). Removing obstacles to enabling IPv6 includes identifying those legacy systems that cannot be upgraded and choosing a solution (such as an application-level proxy that can support both IPv4 and IPv6 for the remaining lifetime of the legacy system). Firms can plan upgrades and purchases in advance to be proactive, rather than discovering at a late stage that a key system dependency is not IPv6 capable. Contact vendors to find out about IPv6 support in their current products and future
releases and ask your ISP about their plans with IPv6 (if not already supported). (The Internet Society, 2015)

Much was learned during the IPv6 conversion in Mexico with Axtel, a large cellular network. Their biggest challenge was establishing IPv6 as the main technology, the easiest was preparing the documentation. Otherwise, IPv6 deployment and implementation was very straightforward. The Axtel team learned in retrospect that they should have consulted their different equipment providers for insight, talked to another provider that had already implemented IPv6 to learn more and get support from their providers (with hands-on experience), and should have had IPv6 support years before even starting the project, simply by instituting a policy of required functionality in all their network and IT equipment requirements. (Fuentes, 2014)

To conclude, IPv6 is a fascinating new protocol that ensures we can grow as a global society. It comes with a host of challenges, but the benefits are greater. Enterprises that have not switched over from IPv4 should take the advice of Eric Vyncke, Distinguished System Engineer at Cisco: “When an enterprise wants to deploy IPv6 they need to do it in a secure way. They have all the tools right now. The biggest threat is the lack of education and training regarding basic security because IPv6 is already there in your IPv4 network… your network is running IPv6 already – so do it.” (Carrol, Leigh-Ann, 2014)
Bibliography


