The Future of IPv6

Vavruska, Ryan
Computer Science
University of Massachusetts - Lowell
Lowell, USA
ryan_vavruska@student.uml.edu

***Abstract*—While IPv6 was invented 26 years ago, IPv4 still remains the more commonly used version of internet protocoling. With the growth of the internet however, the number of available addresses available to the world is dwindling day-by-day. With this, the need to swap standardizing IPv6 as the go-to addressing standard is becoming more and more needed. In this paper I will describe the implementation of IPv4 and IPv6 and discuss the benefits of each version as well as their shortcomings. The paper will primarily focus on why the internet is taking so long to switch to using IPv6, as today only about a third of the internet supports IPv6. It will also discuss the problem that IPv6 was trying to solve over IPv4, focusing as well on a performance comparison between the two versions. Through research it can be found that IPv6 is much better than IPv4 when it comes to performance, so why is IPv4 still more commonly used to this day?**

I. Introduction

When the internet was invented, there was a need to figure out how to route and address packets so that they can travel across networks and arrive at the desired destination. This led to the invention of the internet protocol (IP). When data is communicated across networks, the data is divided into packets and embedded in these packets is IP information. This information tells routers that exist where to send the packet. Every device that connects to the internet is given its own IP address, this is typically done with a series of parent and local networks. For instance, your home network typically will have a single IP address, and every device in your home connects to that router and is assigned an address that is local to your network. When the data arrives at your own router, your router pushes the data to the correct device on your network.

Throughout the years many versions of Internet Protocol have existed, with IPv4 being the main version of addressing used today. IPv4 was introduced in 1981 and included with it a 32-bit address space. This sums up to around 4.3 billion addresses that can be assigned in the world. With the amount of internet devices, and the increasing amount of people that are becoming connected to the internet day-by-day it is no surprise that the limited number of addresses introduced a scaling problem that needed to be solved.

With IPv4, most networks nowadays also include IPv6 side-by-side with devices often having both addresses assigned to them. IPv6 was introduced in 1995 and includes a 128-bit address space. This sums up to 2î28 unique addressed that can be assigned to devices across the world. These addresses are represented in a series of four characters separated by colons. The address is split into two parts, with the first 64 bits representing the network component, which is used for routing. With the second half of the address, the node component representing the physical address or MAC address of the device.

With IPv6 having existed for 26 years, in this paper I will present why IPv4 is still the more commonly used version of internet protocol to this day and what needs to change for IPv6 become more commonly used.

II. Discussion

The primary way to compare the two version of internet protocol, IPv4 and IPv6, is to first look at the performance difference between the two versions. The primary gain in performance between the two versions is that IPv6 does not use network-address translation (NAT). Network address translation is how multiple local addresses are mapped to a public one before transferring information. This is done by the router and with IPv4 comes a range of reserved addresses that are used by devices on a local network that is then mapped to a single public address. This is primarily used to deal with the shortage of public IP addresses that exist in the 32-bit IPv6 address space. Consider an environment where a company with thousands of employees all utilize the same network. Without NAT, each of the devices on the company's network would take up its own IPv4 address. With the amount of address availability with IPv6, there is so longer a need to translate these addresses since each device can reliably be given its own address. The ability to remove NAT increases routing and traffic performance by removing a step in the data translation process.

A. Header changes

The IPv6 header differs much from the IPv6 header which also helps increase performance in the routing process. With the size of the header being constant now, with the option for extension headers given their necessity. The header of IPv6 is defined to be 40 bytes of data, with a lot of fields that were contained in IPv6 being moved to the extension headers. The routing process with these header changes is much more streamlined because the routers no longer need to process useless data that was contained in the extra fields of the IPv4 header and can instead ignore the existence of the extension headers in their entirety, instead focusing solely on moving the packet to its destination. [2]

B. Quality of Service

Another key feature of IPv6 is that Quality of Service can be naively implemented using the flow label of the IPv6 header. Quality of Service is a feature that is commonly used to prioritize certain kinds of packets, allowing data that requires more frequent communication to essentially skip the line when it comes to their transmission. For example, packets containing text can be often have more delay in between them, since the priority of the text being transmitted in real time is usually not necessary. The is opposed to the transmission of voice of video packets. In a world where people are often streaming video at all times of the day, packets containing audio or video data have a much greater need to be transported so the media can be played in real-time.

C. Security Changes

There are also security benefits from employing IPv6. IPv6 employs IP security (IPSec) as part of its protocol suite. It is completely standardized and while it is also employed as an optional feature of IPv4, IPv6 requires IPSec as part of its implementation. IPSec provides end-to-end security, meaning that data is secured starting at its origin all the way to its destination. In its implementation, IPSec utilizes authentication header and encapsulating security payload header to secure packets. They can be used separately or together in two modes. In tunnel mode, the protocol is applied to the entire packet, and is needed to ensure security over the packet. The other mode is transport mode, where the security is only applied to the transport layer in the form of an IPv6 header. The authentication header provides data integrity and secure for the entire packet. This is done providing a means to ensure that a packet came from the address provided in the source address of the header. It also ensures that the contents of the packet have not been modified during transit. If either the source address or packet contents have been modified, the packet is dropped and not accepted as valid when it reaches its destination. Meanwhile, the encapsulating security payload header provides confidentiality and data integrity to the payload. The confidentiality of the packet refers to the confidence that nobody has seen the contents of the packet other than the routers and the one who the content is intended for. [2]

D. Address Labeling

While the addresses of IPv6 prove to be much longer than those of IPv4 given their nature there are several ways that they can be shortened to improve readability. The main method that these addresses are shortened is done by the removal of leading zeros. For example, if you have an address that was 2601:189:0000: 0000: 0000:0000:53c2:c02d, the address could be shortened to 2601:189::53c2:c02d. The shortening is done by employing a double colon, which can be used a single time in an IPv6 address, with the assumption being that the area in the address where the double colon is positioned contains several octal of zeroes.

E. Why not swap today?

The main reason that the world still uses IPv4 as its format of data communication, despite all the benefits is provides, is the complexity and cost of swapping to the newer format. The two formats are not backwards compatible and require infrastructure changes to continue to use the old format, if one was to swap completely over to IPv6. With NAT solving the primary problem on address scarcity, more and more people are reluctant to switch over to the newer version. Most people would rather to continue to use the old format rather than incur the possibility of breaking things as they transition to the newer one. While all major modern day operating systems support the two systems, the scope required to swap networking over to the new format is often seen as not worth the gain. Certain organizations, such as the Massachusetts Institute of Technology have almost completely swapped over to using IPv6 as of 6 years ago. The organization concluded that it had roughly 8 million excess IPv4 addresses that were not being used allocated to them and decided that it would be better to sell these addresses to help fund the transition to IPv6 rather than continuing to use the now more outdated format.

III. Analysis

In a paper by Abubakar et al. they do a comparative study of performance between sending video and audio between the two protocol versions. They conducted a series of studies in a controlled test bed environment. This environment was then used to compare throughput, jitter and packet loss of voice and video using both protocols. A wireless LAN network was employed where four different payloads were sent containing data. When it came to audio, both IPv4 and IPv6 performed similarly, with the only notable difference being that IPv4 contained a small amount more jitter in comparison to its IPv6 counterpart.

When translating video, the different between the two are much more comparable, with IPv6 having a higher throughput percentage as well as a lower amount of jitter when compared to IPv6. In terms of packet loss, IPv6 also had a smaller amount. This behavior was consistent amount different video codecs being used, with H 264, MJPEG, FLY and AVI being the codecs used in the experiment. In the conclusion of their paper Abubaker et al. conclude that in general IPv6 contains better performance than IPv4 and affirmed the need for IPv6 being mainlined by IT systems going forward. [1]

IV. Conclusion

While more and more organizations are slowly transitioning to using IPv6 the likelihood of a greater wide-spread adoption of the format in the distant future is highly unlikely. Most western and European countries do not see the transition to IPv6 a priority and thus the transition has not seen much movement on a larger scale. One country however, who has set the goal of running entirely on IPv6 by 2030 is China, with plans to push for faster adoption across the nation in the coming years. Without similar government initiative in the western world, the swap to primarily using IPv6 is unlikely.

One day that may change; but, until then, it is likely that IPv4 will continue to be the go-to standard for addressing for many years to come.

REFERENCES

[1] Zakari, Abubakar & Musa, Maryam & Bekaroo, Girish & Bala, Surayya & Hashem, Ibrahim & Hakak, Saqib. (2019). IPv4 and IPv6 Protocols: A Comparative Performance Study. 1-4. 10.1109/ICSGRC.2019.8837050.

[2] Hermann-Seton, Penny, Security Features in IPv6, https://www.sans.org/white-papers/380/

[3] Paul, Henry & Bakon, Kinn. (2016). A STUDY ON IPv4 and IPv6: THE IMPORTANCE OF THEIR CO-EXISTENCE. International Journal of Information Systems and Engineering. 4. 97-106. 10.24924/ijise/2016.11/v4.iss2/97.106.

[4] Internet Protocol Version 6 (IPv6), https://www.ibm.com/docs/en/zos/2.3.0?topic=ipv6-internet-protocol-version-6, 04 12 2022

[5] Internet Protocol Version 4 (IPv4), https://www.ibm.com/docs/en/zos/2.3.0?topic=ipv6-internet-protocol-version-4-ipv4, 04 12 2022

[6] What is quality of service?, https://www.juniper.net/us/en/research-topics/what-is-qos.html, 04 12 2022