IPv4 is not Sufficient For The Next 30 Years

Oct 8, 2004

Abstract

The potential implementation of IPv6 has become an important issue that will inevitably reshape Internet technology. There are widely differing views on the urgency of the need to switch from IPv4 to IPv6. The proponents of IPv4 claim that the current protocol is sufficient to keep the Internet going for the next 30 years. This paper looks at features of IPv4 andIPv6 and it argues that, in view of the unquestionable limitations of IPv4 and the nature of upcoming technologies, IPv6 will replace IPv4 much sooner than 30 years.

1. Introduction

The Internet as we have known it in the past several years has been running relatively smoothly with IPv4. In spite of this, the noise about IPv6 has been picking up intensity over the past few years. Some people predict that IPv6 will be implemented in the coming half a decade as a matter of necessity. Others consider the implementation of IPv6 prior to 2030 a matter of luxury. Considering that the Internet has become a part of everyday life in our society, it is worth having a closer look at the two extreme positions. To understand the background of the divergent views, we will look at brief histories of IPv4 and IPv6.

2. Background

Based off of RFC 789, IPv4 was first published in 1981. Since its introduction to the networking world, IPv4 has proven to be a robust, scalable protocol that survived the growing demands of technology with considerable ease. While this aspect of IPv4 had been well considered since its inception, the designers of IPv4 did not foresee the limitations of the protocol as networks expanded.

Once the Internet got popular among academic institutions, and eventually the public, the demand for IP addresses grew exponentially. In 1985 1/16th of total IP addresses had been allocated. Between 1990 and 2000, the IP allocation had gone up from 1/8th to half. IPv4 has 4.2x10*9, or 4.2 billion possible addresses. The actual number of addresses available for use is actually even less. The current culture of distribution of addresses limits the number available to a few hundred million as a result of addresses being reserved for multicast, experimental, etc.

Over time, when it became apparent that the pool of available addresses was rapidly shrinking, in order to circumvent the growing but unsatifiable demand for IP addresses, the use of Network Address Translation (NAT) was introduced. NAT allows a single device, such as a router, to act as an agent between the Internet (or "public network") and a local (or "private") network. This means that only a single, unique IP address is required to represent an entire group of computers[1].

This issue of limited addresses in IPv4 forms the backbone of the case against it. Even with the implementation of NAT, and other efforts like PPP/DHCP address sharing, classless interdomain routing, and other address reclamation practices, sooner or later IPv4 will still eventually run out of addresses.

There were also other unforeseen complications in IPv4 due to expansion of the network, for example expansive routing tables - most routing tables currently maintain as many as 48,000 different routes[2]. As a

[1] Jeff, Tyson, How Network Address Translation Works
[2] Introduction to IPv6, The New Internet Protocol

result of an attempt to conserve addresses, among many other negative side effects, IPv4 has lost transparency, robustness, unique addressing and the end-to-end communication model.

Naturally, one of the major changes IPv6 makes over IPv4 is addressing. IPv6 increased the number of possible addresses to 3.4x10*38. Addresses will have 128 bits. They are assigned to interfaces, which can in turn pass them down the hierarchy.

Like IPv4 topology, there are there types of addresses in IPv6. Unicast, Multicast, and Anycast. In general IPv6 borrows ideas heavily from IPv4. However, at times the implementation of ideas we are familiar with in IPv4, such as the use of local addresses and subletting, may take a slightly different turn in IPv6.

An outstanding advantage of IPv6 is that with reasonable address allocation policy, the possibility of addresses becoming exhausted is implausible, making things like NAT no longer necessary. Also since IPv4 has the embedded means for auto-configuration, IPv4 features like DHCP will become obsolete. This will make the job of networking managements significantly less complicated.

As a result of enabling all devices to be uniquely addressed from a single address pool, IPv6 allows for coherent end-to-end packet delivery by the network. This in turn allows for the deployment of end-to-end security tools for authentication and encryption and it also allows for true peer-to-peer applications.

In addition, IPv6 implements a policy of RIPE-NCC, ARIN, APNIC, LACNIC registries where prefixes are allocated such that they enable a hierarchy of routers. This is considered a significant benefit in the new design. So each packet is equipped with optional headers that are not examined or processed by any router on the packet's path. This simplifies the routing process and the need for expansive routing tables is reduced.

IPv6 also introduces a new concept in the implementation of Anycast addresses. Anycast addresses are Unicast addresses assigned to many interfaces. A packet to an Anycast address is delivered to the nearest interface with a valid Anycast address. If the interface is found to be busy, it is passed on to the next possible interface. This is a simple load balancing system built directly into IPv6. It also provides the experimental feature that allows provider selection.

There is also improved resource allocation in IPv6. IPv6 enables the labeling of packets belonging to a particular traffic flow for which the sender requests special handling. The use of a new 20-bit field in the IP header called the Flow Label proves a feature abundantly available to support Quality of Service (QoS). For example, if a certain machine sends ping messages and another downloads a file, the download process, which will create a data stream, will have a higher priority than a simple ICMP data. This facilitates support of specialized traffic for some applications, such as real-time audio and video.

Just about every operating system released since 2000 is IPv6 compatible. IPv6 in turn has the support built into it that allows it to communicate directly with current IPv4 addressing system currently in existence.

There is very little doubt that IPv6 will eventually replace IPv4. The question is how urgent the need for this transition is, and what factors determine the urgency.

3. The Address Space Issue

It is a certainty that IPv4 will run out of IP addresses to allocate. The big question is: when will it run out? According to some predictions, by now it should have run out. In April 2004, excluding some 6 percent is reserved and another 6 percent is used for multicast, 31% [3]of IP addresses were still not yet allocated. If we continue with the current trend of growth for Internet, assuming a continuation of the current utilization efficiency levels, and assuming a continuing balance between public address utilization and various forms of address compression, then IPv4 may survive well into the late 2020s.

[3] Hain, Tony, The Current Reality Behind The Promise, 2004

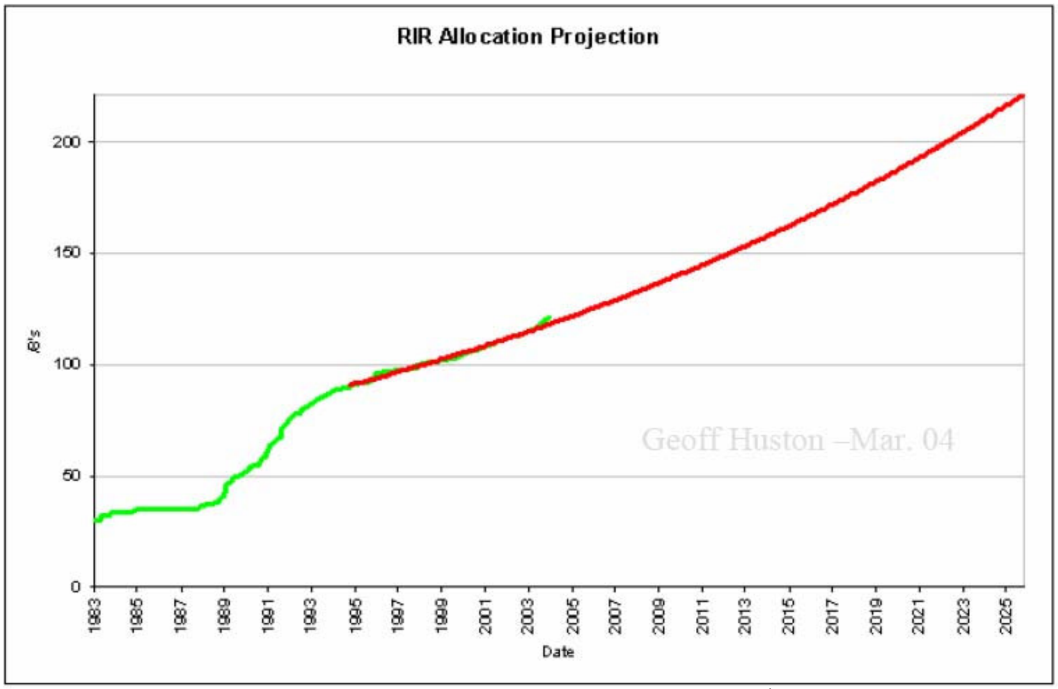

Figure 1: Ongoing analysis of IPv4 trends[4]

Figure 2 shows expected growth in demand for addresses. It assumes that there will be no disruption in the trend of demand for addresses. However, in reality, various events can easily disrupt this trend. The history of the Internet, as can be seen in the periods 1983 – 1993, in Figure 2, has had an unstable progression. By 1993, when the Internet boom took over, the need for addresses also increased by many folds. Given the nature of technology in today's world, it would be laughable to predict anything beyond, at most, five years from now.

We can conceive of many reasons why the demand for IP addresses may increase. For example, due to the imitations in NAT and its inability to support emerging popular applications, we may see a surge in address take up rates. There is a growing buzz for peer-to-peer applications. We are also seeing a boom in wireless technology. There are rising expectations for third-generation (3G) large radius services being combined with consumer devices, control systems, identification systems, and various other forms of embedded dedicated function devices[5]. There is talk of internet-enabled devices, ranging from handheld devices, automobiles, and household appliances to airplanes, which can all potentially exert increased demand on the pool of IPv4-based Internet addresses

4. The IPv6 Myth

Given the long list of improvements IPv6 has over its predecessor, and the foreseeable Internet address crunch in IPv4, a question arises as to why people are not rushing to implement IPv6. There are two classless of reason to explain this. One is that there is a halo of myth surrounding IPv6, which does not offer much to impress, especially when considered in comparison to IPv4. We will discuss here some such myths.

4.1. IPv6 Is More Secure

[4] Hain, Tony, The Current Reality Behind The Promise, 2004
[5] Huston, Geoff, Exposing 9 Myths About IPv6, 2003

IPv4 does provide come with the mandatory support for Authentication and Encapsulating Security Payload extension headers. However the presence of this extension does not mean mandatory utilization of it. IPv4 also has the same feature as an add-on. Should anybody require using this security measure, it is not clear that the IPv6 advantage in ease of implementation has an overwhelming advantage over IPv4.

There is some difference between security features in the two protocols. IPv4 caters to authentication in environments in the face of various forms of deployed active middleware such as NAT. IPv6 on the other hand was designed keeping in mind that arrangements such as NAT will be obsolete as result of its deployment. Therefore it is more concerned with peer-to-peer authentication and transport security at the protocol level.

It is important to note that IPv6 paves the path to end-to-end security, which takes it Internet a different direction than the approach taken by IPv4, which concentrated on peripheral security. This gives the user a new direction from which to approach security. But it is still not clear that there is any advantage, solely based on the issue of security, for moving from one protocol to another.

4.2. IPv6 and Improves Mobility

IPv6 is also believed to be mobile friendly. If one looks at this claim from the perspective of countless existing and upcoming mobile gadgets, it is indisputably true that the increased address fields in IPv6 cater to accommodate the expanding market. But this essentially ties the topic of mobility to the question of how soon will IPv4 run out of addresses rather than technology associated with it.

However, if the issue of mobility is one concerned with the actual technology to support mobility, then once again IPv6 fails to impress in comparison to IPv4. Mobile IP refers to the mobility aspect of IP that allows nodes to move to different networks all over the world while maintaining upper layer connectivity[6]. IPv4 was created at the time when mobile devices were non-existent. However, Mobile IPv4 (MIPv4) was designed as an extension to the base IPv4 protocol to support mobility.

In fact, new security threats are introduced in IPv6, which have been largely responsible for blocking the standardization of Mobile IPv6. The biggest vulnerability, Binding Updates (BUs), can result in various types of attacks, including False Binding Update, Man-in-the-Middle and Denial-of-Service attacks. There have been proposals to secure MIPv6 Binding Updates, including integration of IPSec into MIPv6, Purpose Built Keys (PBK) and a new IETF Mobile IPv6 security draft, Mobility Support in IPv6.

Various difficulties impede the acceptance of solutions offered for the Binding Update problem. IPSec requires too much processing from the IPv6 end devices. IPSec also depends on technologies like PKI, which are not widely deployed. PBK not only comes with limitations in providing a lightweight method to authorize Binding Updates, but it also does not offer as much security as IPSec. Other solution variations, such as Mobility Support in IPv6 by IETF, are in developmental stages.

4.3. IPv6 Offers Better QoS

Another belief about IPv6 is that it comes equipped with features for better QoS. The claim is usually based on the fact that IPv6 comes with a 20-bit flow label in its packet header. Indeed, there is an advantage to the capability but as far as the feature presenting an advantage over IPv4, both protocols come quipped with an 8-bit traffic class field which utilizes 6-bits to differentiate

---

[6] Sudanthi, Sudha, Mobile IPv6, 2003

services by code points. This information is made available to an Integrated Service packet classifier in both protocols. As for the extended 20-bit flow label in IPv6, it is yet clear what practical application it can serve in large-scale networks.

4.4. IPv6 Supports Auto-Configuration

IPv6 does have an embedded system for auto-configuration. IPv4 users are also accustomed to this feature though the widespread use of DHCP. Again this does not bring much into the table for people who are already using IPv4 and have established systems for auto-configuration.

In fact there is some lingering doubt in the way IPv6 does its auto-configuration which, in its current specification gives the capability to uniquely identify a device and potentially trace its activity. In IPv6, 64 out of the 128 bits of an address are created during auto-configuration. When the interface identifier, which is the first 64-bits of the IPv6 address, is created from the 48-bit MAC address the MAC address must be expanded to create a 64-bit sequence. This interface identifier derived from the network interface MAC address, which does not change, is then appended to the remainder of the IPv6 address[7].

During Auto-configuration, a machine discovers neighbors through Neighbor Discovery, which in turn allows a device to send router solicitation messages instead of waiting for routers and other devises to initiate communication. The device then receives the network prefix from the router and this value combined with the 64-bit interface identifier to make up the complete 128-bit IPv6 address. This poses a serious privacy glitch and without resolution plans to fully implement IPv6 could meet strong resistance from privacy advocacy groups. Several solutions have been suggested, including the use of DHCP, which is borrowed from IPv4, and RFC 3401, which offers the capability to create new addresses utilizing a random number instead of the factory-assigned serial number. Some of the privacy concerns of IPv6 have been resolved through RFC 3401, but further considerations of privacy issues in IPv6 are essential to the success of its Internet-wide deployment.

5. Other Considerations Before Implementing IPv6

One reason why there is not a rush to implement IPv6 is that it does not present any operational advantage over IPv4 for networks that are already well established with IPv4. In fact, as discussed in the previous section, IPv6, which has not yet been fully tested, may introduce new uncertainties.

> *An essential characteristic of [IPv6] was that of an evolutionary refinement of the IPv4, rather than a revolutionary departure from IPv4 to an entirely different architectural approach.*[8]*.*

A great characteristic of IPv6 is that it pledges a fluid transition from IPv4. Ironically, this very characteristic also makes IPv6 currently less favorable. Businesses' view of the IPv4-to-IPv6 transition issue is, "IPv6 is IP …and if a carrier is getting revenue from IPv4 there is no reason he can't get revenue from the same way"[9]. Alas, the reverse is also true As far as users who are currently on IPv4 are concerned, in the absence of signs of imminent address shortage; there is very little advantage in taking up IPv6.

Another drawback to the transition process of IPv6 is that it costs money- the immediate reward for switching from IPv4 does not add up to the expense of adopting IPv6. IPv4 users, from the backbone carriers down, are being urged to abandon a functional protocol, to replace it by a similar protocol which promises pretty much the same functionalities, albeit with greater simplicity and efficiency.

---

[7] Scott, Kevin The Next Internet Privacy in Internet Protocol Version 6 (IPv6), 2004
[8] Huston, Geoff How Did IPv6 Come About, Anyway? , 2003
[9] IPv4 - Scaling the Internet, Driving New Services, 2004

On a good note, it is expected that the cost of running IPv6 will decrease with time since it is expected that the work associated with network management and address allocation is going to be much simpler. Convincing businesses of the long terms benefits of IPv6 remains as one of the challenges.

In addition, there is some disadvantage in being among the first to switch to IPv6, as there will be in being the last to remain with IPv4. Much of the equipment in major backbones and ISPs is already IPv6-capable. It has already been mentioned that most post-2000 operating systems being released with IPv6 capability. Some countries are even beginning to see consumer electronics that are only IPv6 capable. Yet, there are still a lot of hardware and software in the network, which are currently functioning smoothly with IPv4, but are far from being IPv6 compatible. Some machines are simply too old. There are also pockets of technologies, such as in the broadband router sector many small routers, which are not IPv6 capable[10]. Such pockets of technologies being left behind can unnecessarily slow down the transition to IPv6.

6. Eventual Transition from IPv4 to IPv6

Considering the transition to IPv6 is inevitable, there are some pointers worth mentioning, which indicate that the transition will happen sooner than later.

I. The rush to switch to IPv6 on IPv4 Dooms Day will not benefit anyone. It makes better sense to gradually work towards IPv6 in terms of testing the new technology as well as preserving the continuity of business.

II. As mentioned in a previous section, there is an increasing demand for IPv6 from 3G devices and peer-to-peer applications. Much of this world is driven by the demand and supply for services. As the demand for IPv6 rises, companies will start picking up on the new technology to accommodate evolving customer needs.

III. Recently Japan, China and Korea, at times in collaboration, started implementing IPv6 at larger scales. These countries either have a culture of picking up new technologies, like Japan, or are going through a record growth in networking, like China, a trend that is expected to increase in the coming years. Other countries will soon want to keep at par with these nations so that when IPv4 addresses eventually run out, they will enter the realm of the new Internet with the same level IPv6 maturity.

7. Conclusion

Unless, for some unforeseeable reason, interest in Internet technology takes a significant downturn, IPv4 will not be sufficient for the next 30 years. If current trends of IP address allocation continue without disruption, IPv4 may continue to for another 20-25 years. This is highly unlikely given how strongly technology is embedded in today's society, and the rate at which new technologies are being introduced. There is growing interest in many devices that call for the implementation of IPv6.

Despite all these indicators towards IPv6, it is still understandable that users are reluctant to take up on IPv6 because i) it has no overpowering capability that does not have a functional counterpart in IPv4 and if it is not urgently needed, and if it costs money, later is better than sooner ii) it has barely ever been tested at large scale. However, these are difficulties society faces with every new implementation of technology. If we can learn from our experience with IPv4, from which IPv6 borrows many positive qualities, we can expect that IPv6 will also have the enduring qualities like robustness and scalability that will help it weather growing demands of technology.

Even though the current seemingly lethargic response from IPv4 users towards the new technology, steps taken by nations like Japan, China and Korea are going to help accelerate the transition of Internet towards IPv6. We can expect more tangible movement towards IPv6 in the coming years.

---

[10] Chirgwin, Richard, Juniper's Ipv6 Advocate Tests Mythology, 2003

References

1. Huston, Geoff, How Did IPv6 Come About, Anyway?, The Internet Protocol Journal (IPJ), Volume 6, No. 2, June, 2003
2. IPv6 - Scaling the Internet, Driving New Services, http://hs247.com/modules.php?name=News&file=article&sid=224 , 2004
3. Chirgwin, Richard, Juniper's Ipv6 Advocate Tests Mythology, http://www1.commsworld.com.au/NASApp/cs/ContentServer?pagename=commsworld/home&var_el=art&art_id=1034683451310&var_sect=NEWS&from=home , 2003
4. Scott, Kevin The Next Internet Privacy in Internet Protocol Version 6 (IPv6) , http://www.sans.org/rr/papers/44/1397.pdf, 2004
5. Jeff, Tyson, How Network Address Translation Works, http://computer.howstuffworks.com/nat.htm
6. An Introduction to IPv6: The *New* Internet Protocol, http://www.raiden.net/techhelp/intro-ipv6.htm
7. Hain, Tony, The Current Reality Behind The Promise, http://usipv6.unixprogram.com/North_American_IPv6_Summit_2004/Thursday/PDFs/Tony_Hain.pdf, 2004
8. Hubert Feyrer, Introduction to IPv6, http://www.onlamp.com/pub/a/onlamp/2001/05/24/ipv6_tutorial.html, 2001
9. Huston, Geoff, IPv4 - How long have we got?, http://www.potaroo.net/ispcolumn/2003-07-v4-address-lifetime/ale.html, 2003
10. Huston, Geoff, Exposing 9 Myths About IPv6, The Internet Protocol Journal (IPJ), Volume 6, No. 2, June, 2003
11. Sudanthi, Sudha, Mobile IPv6, http://www.giac.org/practical/GSEC/Sudha_Sudanthi_GSEC.pdf, 2003
12. Fernandez, David, Addressing and Routing in IPv6, http://www.ipv6-es.com/02/docs/david_fernandez_1.pdf, 2002
13. History of TCP, http://student.ing-steen.se/IPv4/TCP-IP.pdf