How Long Will IPv4 Stand?

Abstract

Since the first time IPv4 was described in IETF publication RFC 791 (September 1981), it has been widely deployed as a Internet Layer protocol and served as the core standard of internetworking methods. Although in nearly 30 years IPv4 has been remarkably resilient in spite of its age, due to unexpected fast development of the Internet, many unforeseen problems emerged, stemming from the nature of IPv4 architecture. One of the most urgent issues is the IPv4 address exhaustion, which was noticed in the early 1990s. By 1996 a series of RFCs were released defining IPv6, which meant to answer the call for "IP Next Generation". Although it's still not a perfect protocol, it is equipped with many new features to overcome the vital limitations of its predecessor. However, the transition of IPv6 is undergoing really slowly in the past twenty years. People prefer turning to new techniques which ease the issues presented by IPv4 rather than running into the new age of IPv6 Internet. In this paper, we intend to compare IPv4 and IPv6 key difference, discuss the reasons that the transition didn't progress as expected, and why IPv4 will still stand in the near future.

1. Introduction

As early as 1990s, one decade after the release of IPv4 standards, it had been noticed and predicted that the architecture design of IPv4 wouldn't be able to keep pace with the fast increasing needs of Internet. "IP Next Generation" was called for to eliminate the limitations of IPv4 and clear the way of Internet development. Through almost 20 years' propagandizing, IPv6 transition is still undergoing slowly, even until the born of IPv9, which brings the possibilities that a direct deployment of IPv9 will force the skip of IPv6 transition.

IPv4's status is vitally shaken by its well known IP address exhaustion problem. It uses classful address scheme, which creates IP address waste when an organization or enterprise don't use all of the IP addressing space allocated to it, especially when the allocated address is class A. Therefore NAT technique was created to help the enterprises whose allocated IP address space cannot meet their needs. NAT boxes allow them to use a relatively small amount of addresses form the globally unique IP address space for external traffic, and use another set of local-area network IP addresses for internal traffic. By doing this, their greatly increased internal addressing space can meet all their needs for addresses.

Of course the new generations of IP protocols (IPv6 or even IPv9) don't only intend to solve the addressing space issue but also to improve on the deficiencies of IPv4, such as communication encryption and multi-media data transmission. But in the current IPv4 protocol, options to enhance communication security and data transmission quality are also available. Only they're mandatory, but just extendable optional functions.

After a product is commercialized, technical wise advancements alone are not sufficient to propel the revolution in the industry. IP protocol backed Internet presents a similar situation. Economy wise considerations greatly affect the Internet protocol transition process. IPv6 is not back compatible, so all the routers should upgraded or replaced. Clearly ISPs don't want to take on the responsibilities and cost to make the change happens if the profit potentials cannot be guaranteed by new IPv6 Internet services. So current NAT solution, which is external cost to ISPs, seems like a preferable option. Also other non-traditional concerns affect the process, such the technology status concerns.

We begin in Section 2 with a brief overview of some critical limitations of IPv4, describing the reasons and motivations for the new generation of IP protocols. Section 3 describes IPv6 implementations and the strategies they use to overcome the IPv4 generation shortcomings. Section 4 presents counter arguments against IPv6 transition, and why current IPv4 can still support the Internet development, and why it favors the interests of ISPs, companies and even countries. Finally Section 5 concludes paper that IPv4 will stand beyond 2011.

2. IPv4 Protocol Deficiencies

By considering the existence time of IPv4, it should be acknowledged that it has been working really well. So there must be convincing reasons that motivate the notion to replace it. Among many issues existing in IPv4, two most urgent and critical issues are discussed in this section, address exhaustion and communication security.

2.1 Address Exhaustion

IPv4 uses 32 bit value (i.e. four bytes) to present an IP address. It has theoretical address space of about 4 billion IP addresses. Because of its unideal "Classful" Addressing strategy, the current address allocation efficiency is quite low, only no more than 5 percent of the addresses are fully utilized. Large portion of the already allocated addresses, especially class A addresses, are unused and hence wasted.

Because not all the enterprises have the internal network big enough to utilize all the addresses they got allocated. But the amount of addresses left available to allocate is small.

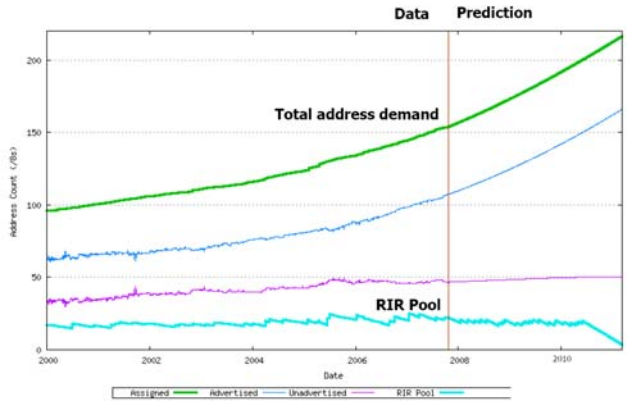

Figure 1

Figure 1 is The IPv4 consumption model built by Geoff Huston. According to his prediction model on 22nd October 2007, IANA allocates its last IPv4 /8 to an RIR on the 22nd May 2010, and RIR's IPv4 address pool exhausts in 2012. The affects of 3G, digital home network, and sensor network etc are not considered in this model. Take mobile phone for instance, in order to evolve into the 3G age, almost all the mobile phone manufacturers ask ICANN to assign an IP address of every phone they make.

In late 1970s when IPv4 addressing space was designed, no one ever expected IPv4 addresses could be consumed in such a high rate. Because of the development of Internet and the explosion of the number of machines and devices got connected to the Internet, actually as early as 1992 the IPv4 address resources already reached the alarm point.

2.2 Security

At the beginning of Internet the parties got connected were mostly research and development institutions, and the researchers in them knew each other's reputations. Also their close relationships with military and government guaranteed security over the internet. More importantly, for a long time, people thought security issue was not crucial in the lower layers of network protocols, and the security responsibilities should be handed over to application layer. Under most circumstances, IPv4 is designed with least security options. So privacy and certification operations should be performed by applications to provide secure communications.

3. IPv6 Enhancements

IPv6 designers built the new protocol on the foundation of IPv4. Time proved best parts were kept, and improvements were made on the parts with shortcomings, and others that affect performance and functions were eliminated. Furthermore, new functions were added to meet the modern Internet needs. This section presents the enhancements made to overcome the deficiencies present in IPv4 protocol.

3.1 Addressing Space

The primary motivation for creating IPv6 was to rectify the addressing problems in IPv4. Comparing to IPv4, the most attractive feature of IPv6 is its huge addressing space. An IPv6 address has 128 bits, which is four times the length of IPv4 address. If we do the math every square meter of the earth surface can get 6.5^{1023} IP addresses.

However more exactly the meaning of IPv6 addressing scheme is that longer address length makes it possible to be able to present modern multi-layered internetworking.

The IPv6 addressing scheme is similar in general concept to IPv4 addressing, but has been completely overhauled to create an addressing system capable of supporting Internet expansion and new applications for the foreseeable future.

3.2 Security

In IPv6 security features are standardized and mandated, all implementations must offer them. IPv6 enforces the implementation of IPSec to provide authentication, data integrity and encryption, and also resistance of replay attack.

The embedded security scheme of IPv6 is realized by Authentication Header (AH) and Encapsulation Security Payload (ESP) of IPSec. AH can realize data integrity, data source authentication and resistance of replay attack. ESP based on the security functions of AH, supports data encryption.

As one important application of IPSec, IPv6 integrated VPN functions, which makes it able to more easily realize safer VPN networks.

The security scheme operates at the IP layer and is invisible to applications. The basic mechanisms for data transporting stay mostly unchanged, and upper-layer protocols are also largely unchanged. It therefore protects all upper layer protocols, and protects both end-to-end router-to-router "secure gateway".

4. Counter Arguments

Even with the advantages and enhancements presented by IPv6, and great efforts endeavored by many countries and companies, it's clear that for the

past decade the progress of deploying IPv6 was quite slow. Even today most of the progress is still done in labs and research institutions. To the contrary, techniques over IPv4 to ameliorate IPv4 issues still are deemed as good options for short to medium run of Internet.

4.1 NATs

The original notions for transition from IPv4 to IPv6 or even higher generations of IP protocols were motivated by IP address exhaustion, low address allocation efficiency and the needs for Internet security, data transmission quality services etc. Among all these issues, addressing space and security are two of the most important issues. NAT technique is created to solve the addressing problem and security issue is still unsolved in the proposed new generation of IP protocol – IPv6.

4.1.1 IPv4 NATs Today

Network Address Translation (NAT) mechanism enables a local-area network to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box located where the LAN meets the Internet makes all necessary IP address translations. Hence, addresses allocated are locally unique but not globally unique.

With this scheme many large companies and organizations just need a relatively small amount of addresses from the globally unique IP address space. The Internet can benefit by successful conservation of addressing space which will in turn effectively lengthen the lifetime of the IPv4 protocol. The companies and organizations also can benefit from the increased flexibility provided by a relatively large internal private addressing space.

So most of today's applications deployed in the Internet have factored in NAT behavior, and they are able to traverse single-NAT-layer, otherwise they are considered practically undeployable.

4.1.2 End-To-End in NATs

NATs provide a solution to IP address shortage of enterprises, however it compromises the "end-to-end" coherence of the network, or cause the problem known as "NAT traversal". Because from outside of a router it's not possible to get the internal clients' IP addresses, direct end-to-end communication between external and internal of a router cannot be conducted when home or company private IP addresses are used behind wideband routers. (But to some extent this can also be utilized as a security policy)

However, this end-to-end communication is still possible via certain application software. People have found solutions from application software and router configurations. For example, service providers can set up servers, which act as the agent to realize end-to-end communications. When a certain port is visited, routers are configured to forward the data packets to a specific internal client end. Currently, service providers usually have to set up servers according to the needs of different application software to realize the communications between PC clients. However for non-PC clients, for example home network devices, such as fridge and microwave, other than personal PCs, the communications are limited by the clients their own CPU processing ability and memory space etc.

Researches in this area have been carried out for a long time, and progress has already been achieved. Actually, via server relay all end-to-end communications is possible. When client send messages to server, a virtual tunnel is formed between client and server. This is like the normal web visit, connection can be done successfully even address conversion is needed. When the connection to server is made, an ELIP address is allocated, which is a class A private IP address with the prefix of 10. End clients could use this ELIP addresses to communicate. By using client-server public communication on the Internet, via the virtual communication network, all IP communications including ICMP, Multicast etc can be achieved.

4.1.3 More NATs

If the major issue of NAT technique, end-to-end communication, can be solved as discussed above, a possible short to medium term response to urgent IPv4 address exhaustion is to increase the density of NAT deployment, and the associated deployment of multi-party application architectures that perform more complex operations in order to set up the application.

There are already examples that successfully utilized this approach. For example in the SIP-related work, protocols such as Simple Traversal of User Datagram Protocol through Network Address Translators NATs (STUN) and Traversal Using Relay NAT (TURN) are designed to perform dynamic discovery and negotiation of NATs.

STUN protocol allows applications operating through a NAT to discover the presence and specific type of NAT, and obtain the mapped (public) IP address (NAT address) and port number that the NAT has allocated for the application's User Datagram Protocol (UDP) connections to remote hosts. The protocol requires assistance from a 3rd-party network server (STUN server) located on the opposing public site of the NAT, usually the public Internet.

TURN protocol is designed to allow an element behind a NAT or firewall to receive incoming data over TCP or UDP connections.

Probably there is still a long way before we reach the practical limits of NAT deployment, and from the service provider's perspective, as long as the costs of this option don't directly fall on them, then this looks like a very attractive option.

4.2 Address Markets

One of the major reasons that causes the IPv4 address exhaustion is the low efficiency in allocating the IP addresses. There are lots of IP addresses allocated to institutions or enterprises that are not used and idle, especially the class A addresses. Therefore there will be enterprises that want more IPv4 addresses and presumably there will be other enterprises that have more IPv4 addresses than they really need. Under such situations markets usually emerge to meet the need. Hence it's reasonable to look forward the happening of redistribution of IPv4 addresses within some form of market-based regime in the short to medium term. As a short to medium term response to the exhaustion of the IPv4 address pool, there is some merit in frostering such a market.

4.3 IPv6 Transition Drawbacks

The option of IPv6 transition requires industry actually undertakes a comprehensive deployment of IPv6, supporting IPv6 in the network in servers, in infrastructure such as the DNS, and in all other places where we use IPv4 today, running in parallel to the current IPv4 network. Of course part of the reason why this has not already happened is that such a deployment is neither costless nor completely simple.

In addition to IPv4, IPv6 is a second protocol, requiring another new set of routing table in the network switching components, additional network management domain etc. None of these reduces the current workload of IPv4, hence actually the deployment of IPv6 will increase the management and maintenance cost of service providers.

However even if the service providers take the cost and responsibility to make the IPv6 transition and switch from an IPv4 service to full dual-stack IPv4/IPv6 support, it's hard for the end users to notice the benefits gained from the transition. For example, for the end users, they still see the same internet, the same web services. So from this side, service providers cannot gain more retail profits. The expectation is that the costs of transition to a dual stack service network are not accompanied by incremental revenue from customer base. From this aspect to observe the failure of IPv6 deployment is not because the industry is short-sighted and ignorant of the advantages of the new generation of IP protocol, we can only say that IPv6 as a business model cannot succeed. In that it lacks the typical drivers for investment in new infrastructure.

4.4 Other Technology Side Considerations

Just turning on IPv6 won't increase or decrease your security, but it does make things more complicated because a "dual-stack" network should be maintained in a long time. Few security issues are related to attacks on the IP layer, most of which are on application level. Therefore although IPv6 make implementation of IPSec, no revolutionary improvement on Internet security can be achieved.

4.5 Cost to Migrate

America is still the lead of technology, including the Internet. So it reasonable to make estimation based on the observation of the attitude and action of America towards IPv6.

Since except government projects and several testing projects conducted in a small amount of companies, there are not too many institutions in America utilize this new protocol whose existence is more than 10 years. This makes it difficult to quantify the cost of this IPv4 to IPv6 Migration.

RTI International conducted cost estimation projects for the government since 2004, and rough estimations were published in recent years. According to their report, in the cost generated by IPv6 transition, within the hardware and software replacement cost, network monitoring/management software and ERP software will be very high expenses; within the labor cost, IT personal training, installation and hardware deployment and testing will be very high expenses; except for these, security related cost is also very high.

In another report release from RTI International in 2006, The proposed conversion from the current version of the Internet Protocol (IPv4) to a newer version, IPv6, will cost an estimated $25 billion over 25 years. Based on information from those interviewed for the study, including representatives from more than 30 stakeholder organizations, researchers observed considerable disagreement about whether, to what extent, and at what pace such demand for addresses will develop.

Although this cost estimation is relatively small to the overall expected expenditure in hardware and software, under the current global economy circumstances, it's pessimistic that governments and enterprises are willing to keep investing in this migrant project, which still has many uncertainties, at the cost of cutting off more employees.

4.6 Non-traditional Concerns

Current IPv4 supported Internet has addressing space of about 4 billion IP addresses, and about more than 70 percent of them have already been allocated. America was the lead of IPv4 Internet, and grabbed

67 percent of the IP addresses, which means 9 IP addresses for each American. To the contrary, the countries followed the lead got a pity portion of the IP addresses, especially Asian countries. Asia has 56 percent of the whole world population but only got 9 percent of the addresses. For example, if divide the IP address number by the population, in China it's 0.06 address per person, and in India it's even 0.006 address per person. Also Japan's well developed mobile communication pinches its IP address resource.

Therefore in Asia, research and propagation on IPv6 were backed by government from the very beginning. Japan's research, development and deployment plan on IPv6 started from 1992, and now only Japan's device manufacturers provide IPv6 hardware support. There are more 10 ISPs provide IPv6 services, and IPv6 backbone routers had been released. China focused on IPv6 later than Japan, but in recent decade China's National Natural Sciences Fund, National Education Department, Chinese Academy of Sciences and "863" Plan performed intensive research on IPv6. In 2006 China already deployed a IPv6 network and connected with most of the large ISPs. And IPv6 was used in 2008 Beijing Olympic Games.

Although China, Japan, South Korean, and other Asian countries have many different reasons to greatly invest in IPv6, the next generation of Internet protocol, there is one common motivation from them. They expect IPv6 could be finally deployed, so they can gain relative higher competence against America in the new generation of Internet, and break America's long time dominant status in technology.

The plan was well designed, but whether it can be finally carried out as expected depends on many factors. First in the sections before we have already discussed the apparent advantages of IPv6 over IPv4, but other short to medium run options are also available. IPv6 is a good option but it's not the only good option. And there are so many obstacles let enterprises and manufacturers hesitate to run into the age of IPv6 Internet. Second since the purposes of Asian countries on investing IPv6 are very clear, America won't let go its dominant status easily. This might also be one of the reasons we cannot see much zeal for IPv6 in America. Before guaranteeing its status in the new generation of Internet and locking its benefits, its not clear of the coming of IPv6.

5. Conclusion

IPv4 has so many deficiencies as the development of Internet. So many new techniques emerged to solve them. By comparison, IPv6 is by all means better than IPv4, and can serve all the current and near future needs. However, IPv6 is still not the ultimate solution for Internet due to its own limitations. And for the already commercialized Internet, the factors and powers propel the transition to IPv6 are from the economy and business side. And the technology leading countries don't want to run into the new generation of Internet in haste and share even status with the countries in inferior position in technology before. Therefore there are adequate techniques supporting IPv4 to survive for at least beyond 2011, and there are not sufficient reasons from business side and technology competence side to end the IPv4 age.

6. REFERENCES

[1] Lixia Zhang, A Retrospective View of NAT, IETF Journal Volume 3 Issue 2.

[2] Michael Gallaher Colleen McCue,Converting to New Internet Protocol Will Cost $25 Billion, RTI International - News Release - 2.2.2006

[3] Geoff Huston. IPv4 Unallocated Address Space Exhaustion, APNIC 24, September 2007 *(CHI '00)* (The Hague, The Netherlands, April 1-6, 2000). ACM Press, New York, NY, 2000, 526-531.