IPv6 – The Protocol of Future Internet?

Károly Farkas
Computer Engineering and Networks Laboratory (TIK)
Swiss Federal Institute of Technology Zurich (ETH Zurich)
Gloriastrasse 35, CH-8092 Zurich, Switzerland
Email: farkas@tik.ee.ethz.ch

Abstract

The hook that holds the Internet together is the network layer protocol called IP or Internet Protocol. Unlike most other network layer protocols, it was designed from the beginning with internetworking in mind. Its job is to provide a best-effort way to transport datagrams\(^1\) from source to destination in the network. The currently used version of IP is known as IPv4 which is an old\(^2\) and widely deployed protocol in the Internet. However, it seems that IPv4 cannot keep pace with the recent enormously growing number of devices connected to the Internet and the increasing routing complexity even in spite of the continuously introduced add-on solutions to IPv4. This raises the question: What will happen with the Internet when some day IPv4 won’t be able to accomplish its job anymore? The proposed solution is a new and more powerful version of IP, called IPv6, which is supposed to replace IPv4 soon. But is this idea realistic? If yes, when this switch-over will take? We will discuss these issues in this tutorial.

Introduction

The Internet today interconnects a large number of computers and networks worldwide. It grew out from the ARPANET network sponsored by the USA Department of Defense (DoD) starting in the 1960s. The number of networks, machines, and users connected to the ARPANET increased rapidly after TCP/IP (Transmission Control Protocol/Internet Protocol) became the only official protocol on January 1, 1983. This point in time can be considered as the ‘birthday’ of today’s Internet. The technical success of the Internet is due to the large variety of applications, e.g., from e-mail and file transfer to World Wide Web and online gaming, that IP can support and the many different networks that can implement IP. The rapid growth of this network is fueled mainly by these applications which make even spectacular multimedia information available at the click of a mouse. This growth was exponential during the last decade and its pace is still expected to remain the same even during the upcoming years meaning that the number of connected machines doubles approximately every year.

This tremendous success leads at the same time to the main dilemma of the Internet: How long can the actual version of the IP protocol, IPv4 still support this pace of growth and what will happen when IPv4 is not capable to carry out its job anymore? The problems come from the nature and working mode of the Internet. Every machine connected to the network must have a unique identifier which is called IP address. Using this address the nodes are differentiated from each other and the end points of a logical communication connection can be identified exactly. This is important, because the data to be transferred between the sending and receiving computers, such as usually in data networks, are broken into small packets and each of these packets is handled separately by the intermediate nodes on the path between the sender and receiver. Thus, every packet must contain information about the source of the data it belongs to and the destination it is supposed to be delivered to make packet forwarding

---

\(^1\) Data broken into separate packets which are handled individually in the network

\(^2\) The first implementation of IPv4 is dated back in 1981
decisions possible at the intermediate nodes (i.e., to which direction the packet has to be forwarded). This mechanism is called hop-by-hop routing. The intermediate node, or usually called router, investigates the destination IP address of the received packet. This IP address is then compared to the entries of the intermediate node’s so-called routing table. An entry in this table contains an IP address range and the identifier of a neighbor node. If the destination IP address of the received packet matches the IP address range of one of these entries, the packet is forwarded to the neighbor node belonging to the matching entry. Otherwise, the packet is forwarded using the so-called default route. IPv4 uses a 32-bit space to create and assign IP addresses to network nodes, which allows the identification and addressing of ‘only’ \(2^{32} \approx 4.3\) thousand million (\(4.3 \times 10^9\)) nodes as the theoretical maximum\(^3\). By today approximately 70% of this address space has already been reserved or used, the rest (or some 1.3 thousand millions) is yet to be allocated. We could say that this is still a huge number. But in the light of the fact that China alone could use up in one year the entire IPv4 address space left the situation seems to be more critical. This problem is known as IPv4 address space depletion. Besides that some other limitations of IPv4 are the complex protocol header, the difficult mechanisms for introducing extensions and options, the limited number of different services, the continuously growing routing tables in size and complexity at the routers, and poor security and privacy. To overcome these limitations, in 1990, IETF (Internet Engineering Task Force)\(^4\) started work on a new version of IP known today as IPv6. The standardization of the core of IPv6 has already been finished but its worldwide deployment is still ahead.

In this tutorial, we shortly overview the main properties and features of IPv6 and discuss the most important arguments what are for and against the total replacement of IPv4 by the new version and when we can expect this replacement if it takes place at all.

**IPv6**

Up to the mid 1990s, the Internet has been used only by universities, high-tech industry, and the governmental offices. With the explosion of interest, it has been used by a much larger group and number of people now, especially by industry and businesses and even by individuals mainly from the younger generations. The main driving factors today are electronic and mobile commerce and multimedia entertainment. Under these circumstances, it became apparent that IP had to evolve and become more flexible [2].

Envision the above mentioned problems of IPv4 on the horizon, in 1990, IETF started work on a new version of IP, one which would never run out of addresses, would solve a variety of other problems, and be more flexible and efficient as well. The major goals of the new IP version were to

- Support thousands of millions of hosts, even with inefficient address space allocation
- Reduce the size of the routing tables
- Simplify the protocol, to allow routers to process packets faster
- Provide better security (authentication and privacy) than IPv4
- Make it possible for a host to roam without changing its address
- Allow the protocol to evolve in the future

---

\(^3\) In practice, this limit is even smaller since not every number of this range is allowed to be used as a node address

\(^4\) IETF is an international organization being responsible for the standardization of technologies used in respect to the Internet
Permit the old and new protocols to coexist for years

After long discussions and debates, IETF selected one from the several proposals for being the next version of IP and gave the designation IPv6 to it (IPv5 was already reserved and in use for some experimental research purposes). IPv6 meets the mentioned goals well. It maintains the good features of IP, discards or deemphasizes the bad ones, and adds new ones where needed. However, an important fact to mention is that IPv6 is not compatible with IPv4.

**Improvements Introduced by IPv6**

The main and most important improvement is that IPv6 has longer and thus larger addresses than IPv4. They are 128 bits long, which solves the problem of IPv4 address space depletion and provides an effectively unlimited supply of Internet addresses. Doing a little computation we can see that with 128 bits \(2^{128}\) nodes can be addressed in the network, which is approximately \(3 \times 10^{38}\). This is quite a large number. If the entire earth, land and water, were covered with computers, IPv6 would allow \(7 \times 10^{23}\) IP addresses per square meter. However, using long addresses has an inherent practical problem: How can they be efficiently represented and handled by, for example, system administrators? To overcome this problem the following notation has been devised for these addresses: They are written down as eight groups of four hexadecimal digits with colons between the groups, like this: ‘0000:0000:0000:0000:1234:5678:9ABC:DEFF’. Since many addresses will contain many zeros, three optimizations have been authorized in the notation. First, the leading zeros within a group can be omitted, so 0345 can be written as 345. Second, one or more groups of 16 zeros can be replaced by a pair of colons. Thus, the previous example address in a shorter form is: ‘::1234:5678:9ABC:DEFF’. And finally, IPv4 addresses can be written as a pair of colons and a dotted decimal number: ‘::129.132.66.157’.

Another major improvement of IPv6 is the simplification of the protocol header. As mentioned earlier, every data packet has to contain some information which can be used by
the intermediate routers to make routing decisions. This information is located in the IP header of the packet. IPv6 contains only 8 header fields versus 14 in IPv4. This change allows routers to process packets faster and thus increase the amount of data traveling through a given router. Figure 1 depicts the IPv4 and IPv6 headers, and shows the mapping of the IPv4 fields which were more or less kept by IPv6. An interesting feature here is using the Next Header field. This is the reason why the IPv6 header could be simplified, i.e., if it’s necessary the header can be extended by additional (optional) fields. The Next Header field tells which of the (currently) six extension headers, if any, follows the actual one. If the header is the last extension header used in case of a given packet, the Next Header field tells which transport protocol handler (e.g., TCP – Transmission Control Protocol) to pass the packet to. Figure 2 shows how this mechanism works and gives some examples about the use of chained extension headers.

![IPv6 Header](image1) TCP Header and Data

![IPv6 Header](image2) Routing Header TCP Header and Data

IPv6 introduces essential improvement also in regard with security. Security is a built-in (feature) of the IPv6 protocol in contrast to the add-on solutions in IPv4. Security takes the form of both authentication and encryption at the IP level. Authentication provides the ability for a recipient of a packet to be sure that the source address is authentic, and that the packet has not been altered during transmission. Encryption ensures that only the intended recipient can read the content of the packet. IPv6 does not, however, have procedures for authorization, i.e., to find out whether the user, once identified, is permitted to access the resources. That is still in the domain of application-level programs. To successfully deliver the security benefits, a key system is employed in IPv6, whereby senders and receivers agree on the key value to be used for authentication and encryption. In addition, senders and receivers must generate a set of agreements that constitute a security association. This association consists of the key, the authentication or encryption algorithm and other parameters, such as the lifetime of the key. With a security association in place, receivers will only decode a packet if the packet can be linked with a particular security association. In practical terms, authentication is delivered in the IPv6 world via one of the generic header extensions discussed above, the Authentication Header. The authentication data is generated by performing a mathematical operation on the source address, plus some fields of the IP header, then sending this value along with the original packet contents. The used algorithm (keyed MD5 – Message Digest 5) is extremely
difficult to reverse engineer and ensures that the source address has not been tampered with and the packet originates from the expected source. The Authentication Header does not, however, encrypt the data part of the packet. This means the packets are still readable by those not intended as the recipient. To avoid this, the Encrypted Security Payload extension header is used. This extension header must be the first header after the default IPv6 header, since it encrypts both the authentication and the data part. The default method of encryption is based on the Data Encryption Standard (DES), known as Cipher Block Chaining.

Moreover, Quality of Service (QoS) issues got more attention in the design of IPv6 than in the past with IPv4. The Traffic Class field (cf. Figure 1) of the IPv6 header is used to distinguish between packets whose sources can be flow controlled and those that cannot. Values 0 through 7 are for transmissions that are capable of slowing down in the event of congestion (such as web traffic). Values 8 through 15 are for real-time traffic whose sending rate is constant, even if all the packets are being lost. Audio and video fall into this latter category. This distinction allows routers to deal with packets better in the event of congestion. The Flow Label field (cf. Figure 1) is still experimental but will be used to allow a source and destination to set up a logical connection with particular properties and requirements. The flow can be set up in advance and given an identifier. When a packet with a nonzero Flow Label shows up, all the routers can look it up in their internal tables to see what kind of special treatment it requires. Each flow is designated by the source address, destination address, and flow number, thus many flows may be active at the same time between a given pair of IP addresses. However, flow level QoS service provisioning has well-known scalability limitations in big networks, which can cause problems in IPv6 flow handling.

And the final improvement, we discuss here, is the inherent features within the IPv6 infrastructure to support mobility (i.e., moving nodes that want to remain connected to the Internet). IPv6 provides support for address autoconfiguration via both stateful and stateless manners. The stateful autoconfiguration is based on using DHCP (Dynamic Host Configuration Protocol), like in IPv4, which requires the existence and maintenance of some DHCP servers in the network. The stateless address autoconfiguration eliminates this need. With stateless address autoconfiguration, a host is expected to build its IPv6 address by concatenating its MAC address (Medium Access Control address, which is usually the unique identifier of the host’s network interface) with the subnet prefix (which is the identifier of the network segment the host is connected to) that the host learns by using neighbor discovery from the routers that are on the same network segment as the host. The neighbor discovery procedures are also improved in IPv6. All the mechanisms related to the interaction among hosts and routers on a single network segment are consolidated into a single protocol, the Neighbor Discovery Protocol (ND). It replaces the Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP) Router Discovery and ICMP redirect functions used in IPv4, as well as providing some enhancements. These features facilitate the use of Mobile IP, a protocol standard to make mobility handling available in the Internet, in the IPv6 environment.

Is IPv6 the Solution?

Now that we have seen the main benefits of IPv6 over IPv4, we can raise the question: Why hasn’t IPv6 been deployed already worldwide when it has a lot of improvements over IPv4?
Even the standardization of its main parts has already been finished and the IPv6 Forum\(^5\) [3] has been promoting and fostering the operational use of IPv6 for many years.

It is not easy to answer this question. For this we have to take a closer look whether the improvements offered by IPv6 are really valid improvements [4, 5].

It’s clear that the practically unlimited address space of IPv6 is a substantial step forward. But is it really necessary in the Internet already today or in the near future? It seems not because the actually used address saving add-on techniques to IPv4, such as Network Address Translation (NAT), and with careful address allocation policies the IPv4 address space may be enough for some further years, yet.

For example, using a NAT router on the boundary of the public Internet and a private network, as depicted on Figure 3, requires only a small number of public IP addresses (often just one) instead of assigning a separate public IP address to every host in the private network. This router translates (exchanges) the source IP address of every packet leaving the private network to one of the public IP addresses it can use. Moreover, it translates back the destination IP address of every reply packet entering the private network to the private IP address used by the given host in the private network. With this technique several different private networks can use the same private IP address range inside increasing the number of assignable IP addresses, since these addresses are not visible from outside and don’t cause conflicts.

However, there are some limitations of using NATs. For instance, the only forms of applications that can traverse a NAT router are those that are initiated on the ‘inside’ of the NAT boundary. The ‘exterior’ cannot initiate a transaction with an ‘interior’ end point simply because there is not an easy way to address this remote device (it is aware only of the NAT router but nothing else behind it). Moreover, a coherent end-to-end packet delivery and end-to-end security cannot be assured by NATs, unless using tunneling, because the end points of a logical connection communicate with the NAT router and not directly with each other.

Concerning the pace of IPv4 address space depletion, we can observe the following: Prior to 1994 some 36% of the available IPv4 address space had been allocated. Since that time, and this includes the entire Internet boom period, a further 20% of the available address space has been allocated [4]. With the continuation of current policies it appears that IPv4 address space will be still available for many years.

---

5 IPv6 Forum is a world-wide non-profit consortium of leading Internet vendors and Research & Education Networks with a clear mission to promote IPv6
It’s also clear, that paying attention to secure communication is getting more important today. Security is a built-in feature of IPv6, since it’s just an add-on solution in case of IPv4 (e.g., using IPsec, a collection of protocols to support secure packet exchange). But how important to have security implemented by the network? A serious application which requires security implements it as part of the application and doesn’t trust the underlying infrastructure, at least today.

In regard to QoS support, still overprovisioning is the simplest and cheapest solution in the Internet. This means that if we need some more capacity somewhere in the network, adding a new cable or increasing the number of optical fibers can solve the problem quickly instead of applying complex QoS policies and techniques. Moreover, due to the above mentioned scalability limitations the flow level QoS supporting approach coming with IPv6 can reserve some further problems.

And finally, with the increasing number of mobile devices connected to the Internet mobility support solutions are getting more attention. The stateless autoconfiguration and improved neighbor discovery techniques of IPv6 can give essential help to mobility support. However, IPv6 per se doesn’t solve the problem. The use of some other protocols, such as Mobile IP, is required but Mobile IP works together with IPv4, too.

Moving Towards IPv6?

After this short analysis it seems that the main motivating factor remained to deploy and use IPv6 worldwide is the vision, when almost every equipment from the fridge to the microwave oven and all of our mobile devices will be connected to the Internet, hence requiring unique IP addresses. But it’s a hard task to estimate when this will take place. Certainly, it won’t happen from one day to another because of the huge transition overhead (time, effort, money, etc.), the lack of operational experience and the risk to replace a familiar working system by an unexperienced one.

However, there are some pilot or even commercial IPv6 networks working in the world. Asia (especially Japan and South Korea) is leading the way. Europe is following with a massive investment in IPv6-related research projects. In Switzerland, SWITCH, the Swiss Education and Research Network [6], has been providing IPv6 connectivity since November 1996. Since June 2004, the SWITCHlambda backbone, the fiber-optical backbone of SWITCH, has been supporting IPv4 and IPv6 in parallel over the same links and using the same routers. Swisscom Innovations, the central innovation unit of Swisscom, has been running IPv6 test networks for quite a while, and currently its operational Intranet is IPv6-enabled [7]. Recently, the USA has started to seriously consider IPv6. The Department of Defense established the goal in 2003 of fully transitioning the entire enterprise IP network to IPv6 by 2008 [8].

Regarding the actual trends, maybe IPv6 will be widely deployed by 2008-2010. But, maybe not…

Acknowledgments

The author would like to express his thankfulness to Lukas Ruf for his valuable comments and feedback.
Selected References