

---

# The Transition To IPv6

David Horton

## Table of Contents

1. Introduction .....	1
2. The Current Standard .....	1
2.1. History of IPv4 .....	1
2.2. Technical Aspects of IPv4 .....	2
3. Limitations of IPv4 .....	2
3.1. Address Constraints .....	2
3.2. Lack of Security .....	3
4. IPv6 .....	3
4.1. History of IPv6 .....	3
4.2. Technical Direction .....	3
5. Fixing IPv4 .....	4
5.1. Addressing Capability Improvements .....	4
5.2. Simplified Header Format .....	5
5.3. Extensions and Options .....	5
6. New Features of IPv6 .....	5
6.1. Flow Labeling .....	5
6.2. Encryption Based Security .....	6
7. Rolling Out IPv6 .....	6
7.1. Building an IPv6 Infrastructure .....	6
7.2. The Transition to IPv6 .....	7
8. Conclusion .....	7
Bibliography .....	7

## 1. Introduction

The Internet Protocol (IP) is the standard method of communication that connects the various host computers into the configuration that we know as The Internet. Today's IP is largely unchanged from its humble beginnings as a Defense Department research project in the late 1970's. However the rise in popularity of The Internet and the ever increasing number of Internet-ready devices is putting a serious strain on the limitations of IPv4. In the late 1990's work was begun on a new Internet Protocol, IP version 6, that would be free of the limitations of IPv4 . This paper will explore some of the improvements of IPv6 and how IPv6 can be transitioned into the existing IPv4 infrastructure.

## 2. The Current Standard

The Internet Protocol in use today is IP version 4. IPv4 has been around for over twenty years and has proved to be remarkably robust during its lifetime.

### 2.1. History of IPv4

The Internet Protocol (IP) was originally designed to facilitate connection of various organizations involved in the defense department's Advanced Research Project Agency (ARPA). [RFC-760] During the time before IP, networks were comprised of proprietary equipment and proprietary protocols. Vendor A's mainframe did not communicate with Vendor B's mini-computer and so on. IP was conceived as a common protocol that would allow these different

computers to talk to each other.

## 2.2. Technical Aspects of IPv4

The Internet Protocol is very simple in its functionality. It is only designed to handle the addressing and fragmentation of datagrams. Any additional functionality such as acknowledgement of received packets and retransmission of corrupted packets is passed off to the higher-level layers such as TCP. [RFC-760]

### 2.2.1. IPv4 Addressing

Each IPv4 packet contains 64-bits of addressing information with 32-bits being reserved for the source address and 32-bits being reserved for the destination address. [RFC-760] The 32-bit address space is frequently represented as dotted quad notation. For example, the 32-bit IP address 0xC0A8012A looks much more familiar when shown as 192.168.1.42.

In order for packets to be routed effectively, these 32-bit address spaces are further divided into subnets which split the address space into network and host sections. [RFC-997] Popular subnets are Class A, B and C with the number of bits reserved for the network portion being 8, 16 and 24, respectively. The remaining bits make up the host portion of the IP address.

### 2.2.2. IPv4 Fragmentation

Because of the nature of communication on packet-switched networks like The Internet, IP datagrams must often be broken into smaller pieces before being transmitted. The pieces of the datagram, called packets are then reassembled back into the original datagram on the receiving end. This process is called fragmentation.

IPv4 reserves 16-bits for information about fragmentation. Three bits are provided as control flags. The remaining thirteen bits are used to sequentially label each fragment so that they may be reassembled in the correct order on the receiving end. [RFC-760] Any datagrams that cannot be reassembled successfully are simply discarded.

## 3. Limitations of IPv4

IPv4 has proved itself to be incredibly robust over the years, but there are some places where IPv4 is beginning to show its age. Primarily IPv4 has been found to be lacking in address space and security.

### 3.1. Address Constraints

The most apparent limitation of IPv4 seen today is the limited address space. 32-bits is simply not large enough to meet the needs of the modern Internet.

#### 3.1.1. Explosive Growth of The Internet

While the actual number of hosts on the Internet is unknown. However, there are over 160 Million registered Internet addresses and that number is increasing at an exponential rate. [Hobbes] One of the reasons for this rapid growth is the popularity of PC's in the home. These days it is relatively easy to get a PC with an always-on connection to the Internet. There are also devices are connecting to the Internet that were not even considered in the days when IPv4 was designed. Popular mobile devices like cell phones and PDA's have Internet capability built in.

#### 3.1.2. Inefficiencies of Subnetting

There is a theoretical upper limit of over four billion ( $2^{32}$ ) hosts in the IPv4 address space. However, this seemingly large number is further reduced because of the inefficiencies of subnetting.

Dividing addresses into Class A, Class B and Class C address ranges gives 128, 16,384 and 2,097,152 possible net-

works, respectively with the remaining bits are used to indicate the host portion of the address. [RFC-997] This gives a total of 2,098,914 available networks.

Because of subnetting, each organization desiring Internet connectivity registers for one of these networks rather than registering their individual hosts. This causes the number of available IP addresses to be consumed much more quickly. For example, an organization holding a Class A network address has taken over 16 million ( $2^{24}$ ) hosts out of the pool of available addresses. Whether or not all of these host addresses are used does not matter as they are reserved for the network address holder and no longer available to be assigned elsewhere.

### 3.1.3. Impossibility of End-to-End Communication

Because of the limited number of IP addresses available, most organizations will hide their networks behind a firewall and use one of the reserved address ranges as defined by RFC-1597 for internal addressing. The firewall can then perform Network Address Translation (NAT) to let the internal hosts see the outside Internet. [RFC-1631]

Using NAT allows an organization to have only a small number of registered IP addresses while maintaining a large number of internal hosts. The good side of NAT is that each of the internal hosts can initiate communication with the Internet without having a registered IP. The bad side of NAT is that hosts cannot accept incoming communication from the Internet. Until recently this was not a problem, because the information intended for public consumption was centralized on an organization's web servers, mail servers and FTP servers. These few servers are given actual, registered IP addresses and the rest of the hosts were hidden using NAT.

As the Internet becomes increasingly decentralized and the functionality once handled by servers moves into individual homes, cars and portable devices, NAT falls short of being the perfect solution. In an ideal situation each host on the Internet should be able to initiate communication with any other host on the Internet.

Drawing an example from the telephone industry, NAT would be similar to an organization that has a few main numbers and all of the other phones are given extensions. People can call out, but it is impossible to contact someone inside the organization without going through an operator or automated attendant. Ideally, every telephone in an organization should have a valid number so that calls can bypass the switchboard and come in directly.

## 3.2. Lack of Security

The IPv4 header provides flags to indicate security, but these are little more than suggestion. The packet payload is transmitted in clear text and can easily be intercepted and read using a network sniffer. IPSec was introduced in the late 1990's, but is not often used. Outside of VPN tunnels, most of the traffic on the Internet is not secured.

## 4. IPv6

In the early 1990's it was noticed that the existing IPv4 protocol could not survive the demands of the modern Internet much longer. [RFC-1597] Soon after work was begun on IPv6. IPv6 was designed to alleviate the limitations with IPv4 as well as to provide feature enhancements.

### 4.1. History of IPv6

Around the same time that NAT was being standardized as a solution for the IPv4 address space problem, work was begun on IPv6. RFC-1883 first documented the Internet Protocol Version 6 standard in 1995. Previous to this document IPv6 was referred to as IP Next Generation or IPng.

### 4.2. Technical Direction

RFC-1883 defines five broad categories of goals for the IPv6 design. These are defined as follows:

1. Expanded Addressing Capabilities

2. Header Format Simplification
3. Improved Support for Extensions and Options
4. Flow Labeling Capability
5. Authentication and Privacy Capabilities

Drawing a parallel to the computer software industry can help to further simplify these goals. Computer software upgrades are often broken down into two categories, bug fixes and feature releases. Bug fixes correct problems found in the previous version whereas feature releases enhance the software by adding new functionality. By thinking in these terms it is possible to group the first three goals of IPv6 under the category of bug fixes and the last two goals can be classified as feature enhancements.

## 5. Fixing IPv4

The designers of IPv6 wanted to design a protocol free from the limitations of IPv4.

### 5.1. Addressing Capability Improvements

Addressing limitations are a major shortfall of IPv4. Consequently, significant effort was put into IPv6's addressing capabilities to ensure that IPv6 would meet the needs of the IT community for many years.

#### 5.1.1. Expanded Address Space

One of the most significant improvements of IPv6 is the size of its address space. Where IPv4 used 32-bit addresses, IPv6 uses 128-bit addresses. These additional ninety-six bits allow IPv6 to address  $3.40 \times 10^{38}$  individual devices. IPv6 uses a standardized subnetting scheme that splits the address into 64-bits for the network prefix and 64-bits for the host identifier.

IPv6 addresses are so large that a new notation needs to be used to represent them. Rather than attempting to put addresses in the familiar dotted quad notation (eg. 192.168.1.42) IPv6 uses hexadecimal numbers separated every four digits by colons. A sample IPv6 address could be expressed as ABC0:0123:0:0:0:4567:1040:A001. [RFC-1884]

Since IPv6 addresses can be rather long and awkward to deal with, there is a shortened format where multiple, consecutive groups of zeros can be removed. Looking at the example address ABC0:0123:0:0:0:4567:1040:A001, the three consecutive groups of zeros following ABC0:0123: can be removed. This leaves ABC0:0123::4567:1040:A001 as the shortened address. [RFC-1884]

#### 5.1.2. Address Auto-configuration

Another feature of IPv6 addressing is improved auto-configuration capability. IPv6 can be configured in three different ways.

- Manual configuration

This involves configuring the host with a static IPv6 address. There is little deviation from the IPv4 static IP method of configuration.

- Stateful auto-configuration

The stateful method uses a IPv6 aware DHCP server (DHCPv6) to obtain an IPv6 address and any additional configuration information held in the DHCPv6 server database. This is much like IPv4 DHCP.

- Stateless auto-configuration

The stateless auto-configuration method has no direct parallel in IPv4. With stateless auto-configuration IPv6 hosts can intelligently select their own IP address using their own MAC address and prefix information advertised by IPv6 aware routers on the local network segment. Stateless auto-configuration can even work on segments without routers with the obvious constraint that traffic will be isolated to the local segment. [RFC-2462]

## 5.2. Simplified Header Format

The IPv6 header consists of 320 bits of information. At first glance it might seem that the header is becoming bloated when compared to 192-bit header of IPv4. In actuality the information contained in the IPv6 header is much more streamlined than the IPv4 header.

Much of the IPv6 header size can be attributed to the increased address space. Larger addresses use more bits. The 256 bits used to represent source and destination addresses in IPv6 consumes 192 bits more than the addresses used in IPv4. This is the price for increasing the address space. But looking beyond the large number of bits used for addresses it can be seen that the additional header information in IPv6 has actually been cut in half.

One of the ways the IPv6 header was simplified was to allow headers to be chained together. Instead of trying to allocate space for every conceivable option, the designers of IPv6 decided to include only the most commonly used information in the standard header. An 8-bit *Next Header* field can be used as a pointer to additional information if it is needed. This flexible design allows the majority of packets to consume less bandwidth by using a simple, streamlined header. There is still the option of using a large, complex header, but in IPv6 it is the exception rather than the rule.

## 5.3. Extensions and Options

A number of extensions are defined in order to add flexibility to the simplified IPv6 header. [RFC-1883] These are briefly described below.

- Jumbo Payload Option

This option contains additional information about packet length that allows payloads of over 65,535 octets (64k bytes) to be delivered in a single packet.

- Routing Information

This information is similar to the *source route* information defined in IPv4 and lets the sender of a packet define the path that should taken in order to reach the destination address.

- Fragmentation Information

The fragmentation information defines how the source host has fragmented a packet that is too big for the MTU size and how that packet should be reassembled at the destination.

These are just a few of the possible header extensions. Additional extensions and options are defined in RFC-1826 and RFC-1827.

## 6. New Features of IPv6

Besides just fixing IPv4, IP version 6 also added some new features.

### 6.1. Flow Labeling

The demand for real-time processing capability is increasing as technologies like streaming video and IP-telephony come into the forefront. Real-time is an area where traditional IPv4 does not fare well, because IPv4 gives no guarantees. One IPv4 packet is treated like any other regardless of whether it contains latency sensitive, real-time information like streaming video or low priority traffic like the latest email chain-letter.

Typically, organizations implementing real-time technologies like streaming video turned to ATM because of its guaranteed quality of service capability. However, IPv6 flow labels and priority flags allow some packets to receive higher priority service than others. Typically routing information and real-time interactive traffic receives highest priority and bulk transfers like email and usenet news are relegated to the lowest ranks.

## 6.2. Encryption Based Security

Information security has become a major concern in recent times as more and more computers are being moved out of isolated workgroup environments and connected to the global Internet. With so much data flowing over public networks the risk of sensitive information falling into the wrong hands has increased exponentially.

IPSec is one of the protocols currently being used with IPv4 to mitigate these risks. IPSec provides a method of using public key encryption for IP packets. When packets are encrypted with strong keys (128-bit or better) there is a much better chance that the information will remain secure. [RFC-2401]

With IPv6, the use of IPSec is required for all packets. [RFC-1883] This has the advantage of providing a standard network-layer encryption scheme for all packets with no special handling required for sensitive information. Requiring encryption on all packets also makes the potential system cracker's job much harder since he would not be able to differentiate between the packets that contain important information and the ones that contain spam email.

## 7. Rolling Out IPv6

The global Internet is so large that it would be impossible to replace or upgrade all IPv4 devices all at once. Instead a phased approach must be taken.

### 7.1. Building an IPv6 Infrastructure

Many of the necessary pieces of the IPv6 infrastructure are already available. Vendors are working with the Internet Engineering Task Force (IETF) to build products with native IPv6 support as well as a means to connect them.

#### 7.1.1. Device Support

There are several operating systems vendors who have already incorporated IPv6 protocol support into their products. A few of these vendors and their products are listed below. [sun-ipv6]

Operating Systems

- Apple OSX
- IBM AIX 4.3
- Linux kernel version 2.2.x
- Microsoft Windows 2002 (XP) products
- Novell Netware 6.1
- Sun Microsystems Solaris 8

## Router Support

- 3Com Netbuilder and Pathbuilder version 11.0
- Cisco IOS 12.2
- Nortel Networks BayRS version 12.0

### 7.1.2. Backbone Support

IPv6 devices need a way to communicate with each other outside of isolated LAN environments. 6bone is a collaborative effort aimed at replacing IPv4 networks with IPv6 native protocols. In the beginning 6bone was completely virtual with IPv6 packets encapsulated in IPv4 and tunneled over existing IPv4 networks. But more and more links are being converted to native IPv6 as the project progresses. [About-6bone]

## 7.2. The Transition to IPv6

Early adopters of IPv6 must take into account the large base of installed IPv4 devices. Consider the scenario of an organization that has two offices, one on the west coast and one on the east coast. Even though the organization has converted to native IPv6 in both facilities, the telecom company supplying the WAN connection still employs ipv4 devices. How then can the two offices communicate?

The solution to this problem can be handled in a few different ways using a mechanism called 6to4 translation. [RFC-2893]

- Dual protocol stacks

This method involves using a border relay with knowledge of both IPv6 and IPv4 packets. The relay chooses the appropriate protocol stack to use depending on the capabilities of the device it is communicating with.

- Tunneling

Tunneling IPv6 over IPv4 involves using a relay to add an IPv4 header to the IPv6 packet and then send the encapsulated information over the IPv4 link. A relay on the other end is responsible for stripping away the IPv4 header and sending the original packet on its way through the IPv6 network.

- Automatic tunneling of IPv6 over IPv4

Automatic tunneling is a special case of tunneling using IPv4-compatible IPv6 addresses. An IPv4-compatible address is any IPv6 address that begins with 96 zero bits. The remaining 32 bits of the 128-bit IPv6 address are then mapped onto the IPv4 address space. Automatic tunneling does not work with the IPv4 private address space, but for organizations with registered IPv4 addresses it provides an easy encapsulation method.

## 8. Conclusion

IPv6 is a very capable protocol replacement for IPv4. IPv6 does not suffer the address space limitations that plague IPv4 today. IPv6 also adds many feature enhancements such as auto-address configuration, priority handling for real-time information and built-in encryption-based security. The design of IPv6 lends itself to a straightforward, phased transition from IPv4 and work is already underway on a global IPv6 backbone. IPv6 should provide robust connectivity for many years to come.

# Bibliography

- [Hobbes] Robert Hobbes. *Hobbes' Internet Timeline*. <http://www.zakon.org/robert/internet/timeline>. 2003.
- [RFC-760] John Postel. *RFC-760 Internet Protocol*. January 1980.
- [RFC-997] J. Reynolds. *RFC-997 Internet Numbers*. January 1987.
- [RFC-1631] K. Egevang. *RFC-1631 Internet Numbers*. January 1987.
- [RFC-1883] S. Deering. *RFC-1883 Internet Protocol, Version 6 (IPv6) Specification*. December 1995.
- [RFC-1884] R. Hinden. *RFC-1884 IP Version 6 Addressing Architecture*. December 1995.
- [RFC-2401] S. Kent. *RFC-2401 Security Architecture for the Internet Protocol*. November 1998.
- [RFC-2462] S. Thomson. *RFC-2462 IPv6 Stateless Address Auto-configuration*. December 1998.
- [About-6bone] *What is the 6bone?*. [http://www.6bone.net/about\\_6bone.html](http://www.6bone.net/about_6bone.html). January 2000.
- [RFC-2283] T. Bates. *RFC-2283 Multiprotocol Extensions for BGP-4*. December 1998.
- [sun-ipv6] Sun Microsystems. <http://playground.sun.com/ipv6/ipng-implementations.html>.