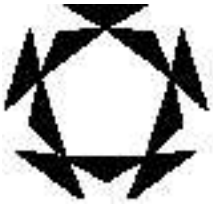


LONDON
SOUTH BANK
UNIVERSITY

Network and Broadband Systems
IPv6 What's new?

Andreas Hofmeier

Contents

Chapter 1

IPv6, What's New?

Andreas Hofmeier

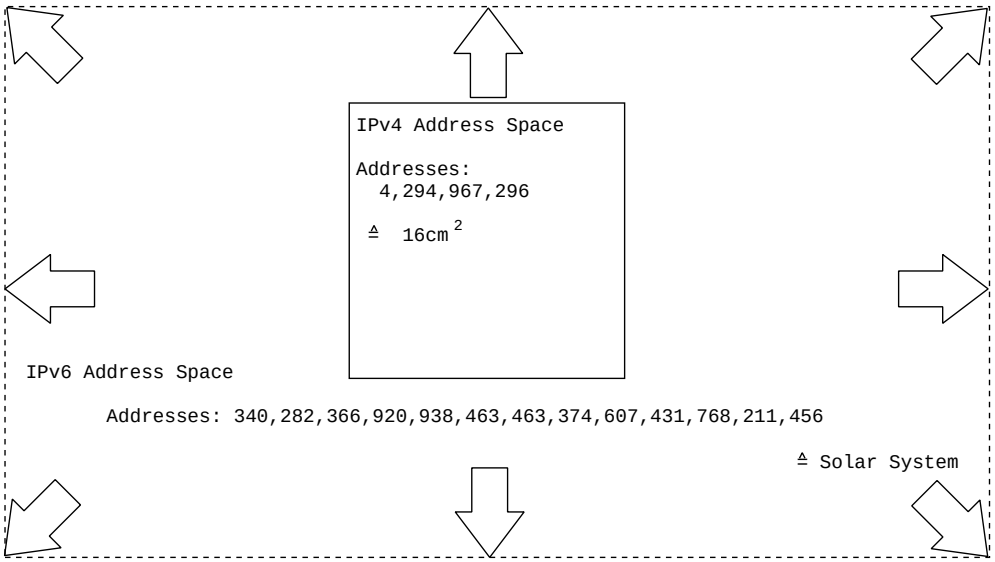
1.1 Introduction

This part of the report will give an overview about the new Internet Protocol version 6 (IPv6). In particular the improvements and changes will be discussed. At first an introduction to the new addresses will be given. After that the influences and advantages of the bigger address space will be discussed. Auto-configuration and the mobile usage of IPv6 are mentioned. The last things that are mentioned are header structure and security in IPv6.

1.2 Address Space

The most important improvement in IPv6 is the much bigger address space. IPv4 uses 4 bytes (32 bit) addresses, this is equivalent to 4,294,967,296 ($4.3 * 10^9$) addresses. IPv6 increases the address-size to 16 bytes (128 bit). With this address size 340,282,366,920,938,463,463,374,607,431,
768,211,456 ($3.4 * 10^{38}$) different addresses can be distinguished (Sæther, 2004).

It is difficult to find a suitable analogy because the IPv6 address space is so much larger than the IPv4 one. Kozierok (2004) found a good analogy:



Analogy IPv4 to IPv6 Address Space compared with $16cm^2$ to area of solar system

"To make this diagram to scale, imagine the IPv4 address space is the 1.6-inch square above. In that case, the IPv6 address space would be represented by a square the size of the solar system." (Kozierok, 2004) $1.6inch \approx 4cm \Rightarrow 16cm^2$.

1.3 Address Notation

An IPv4-address is displayed as four decimal numbers separated by dots:

`134.102.199.160`

Every number must be in the range between 0 and 255 because it is an 8 bit (1 byte) value. This notation is impractical with IPv6 because of the long address. An IPv6 address is written as eight groups of 4 hexadecimal digits each (en.wikipedia.org, 2004; de.wikipedia.org, 2004; Forouzan, 2001; Hinden, Deering, 1998; Bieringer, 2004). Every of this group is a 16 bit (2 bytes) value and can vary between 0000H and FFFFH. This is equal to 0 and 65535.

Because of the huge address space a lot of addresses will be unused, many zeros will occur. One zeros-sequence can be condensed with the `::`-operator. This operator can be used only once. First zeros in a column can be left out. (en.wikipedia.org, 2004; de.wikipedia.org, 2004; Forouzan, 2001, Hinden, Deer-

ing, 1998)

```
2001:0DB8:0000:0000:0000:0000:1428:57ab
2001:0DB8:0000:0000:0000::1428:57ab
2001:0DB8:0:0:0:0:1428:57ab
2001:0DB8:0::0:1428:57ab
2001:DB8::1428:57ab       (adapted form en.wikipedia.org, 2004)
```

An alternative is the mixed notation which is helpful by dealing with IPv4 in IPv6 addresses. Because of the large address space it is no problem to map the old IPv4 addresses in the new IPv6 address space. In this special notation the last four bytes of an IPv6 address are written in dot-decimal (Hinden, Deering, 1998; Kozierok, 2004). For example:

```
0:0:0:0:0:0:8666:A6A0
0:0:0:0:0:0:134.102.166.160
::134.102.199.160
```

1.4 Sharing of IP Addresses is no Longer Necessary

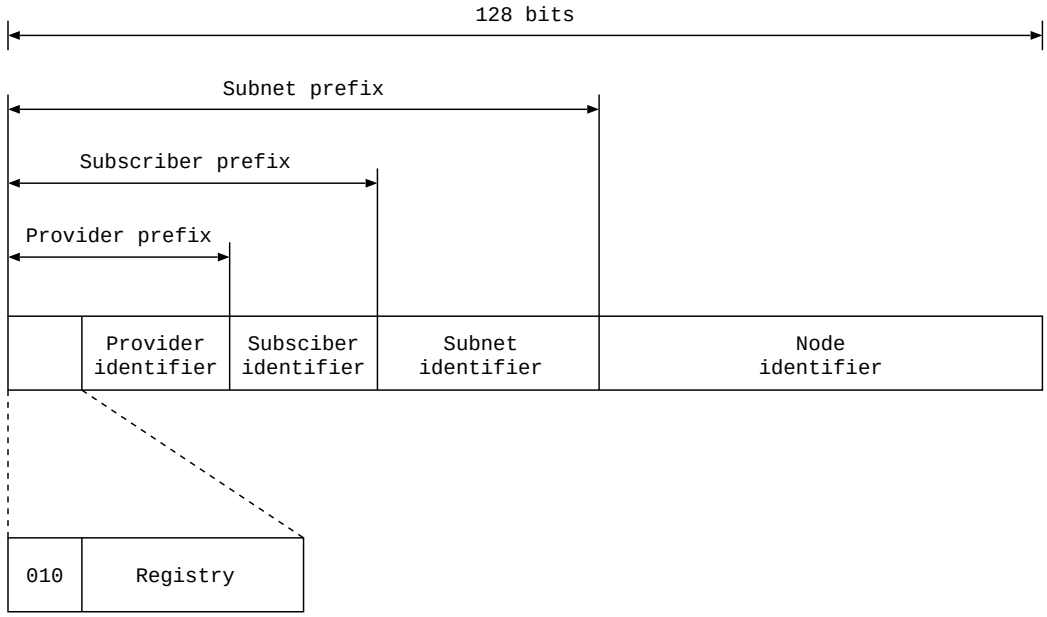
Because of the strong limited address space of IPv4 it is necessary for users to share IP addresses (Cocquet, 2004). One possibility is a time sharing in which the IP addresses are dynamical assigned during establishing the connection to the Internet Service Provider (ISP). Not every terminal can be online at the same time but the new technologies like DSL make it possible and affordable to be always on. For some applications like tele- and video-conferencing it makes sense to be online 24 hours a day. These kind of applications are becoming more and more important. The time-sharing confines the usage of such applications.

Another possibility to share IP addresses is to do a Network Address Translation (NAT). NAT masquerades many private (internal, not public) IP addresses behind few public addresses. One of the most important disadvantages of NAT is that the terminals behind a NAT are not accessible from outside/public. This is no problem in a server-client-structure but the trend goes to Peer-to-Peer applications such as Voice over IP. These applications cannot be fully used through a NAT (Cocquet, 2004).

The new Internet Protocol version 6 eliminates these disadvantages. Dirty tricks to share IP addresses are no longer necessary because of the huge address space. Every terminal gets its own public and unique IP address. Anyway, the old techniques like NAT and firewalling can be also applied on IPv6. Sometimes this makes sense for security reasons (Cocquet, 2004).

1.5 Address Structure

A IPv6 address is built up with two main parts: the address (subnet) prefix and the node identifier. The second part of the IP address is generated from the layer two MAC address. For privacy reasons there is a random component in it, so it is not possible to observe a particular terminal, because it changes its IP address every time it connects to the network. A more detailed hierarchy was adapted from Forouzan (2001). The width of all parts of the hierarchy (excluding the first one) can vary.



The hierarchy of an IPv6 address in its fragments

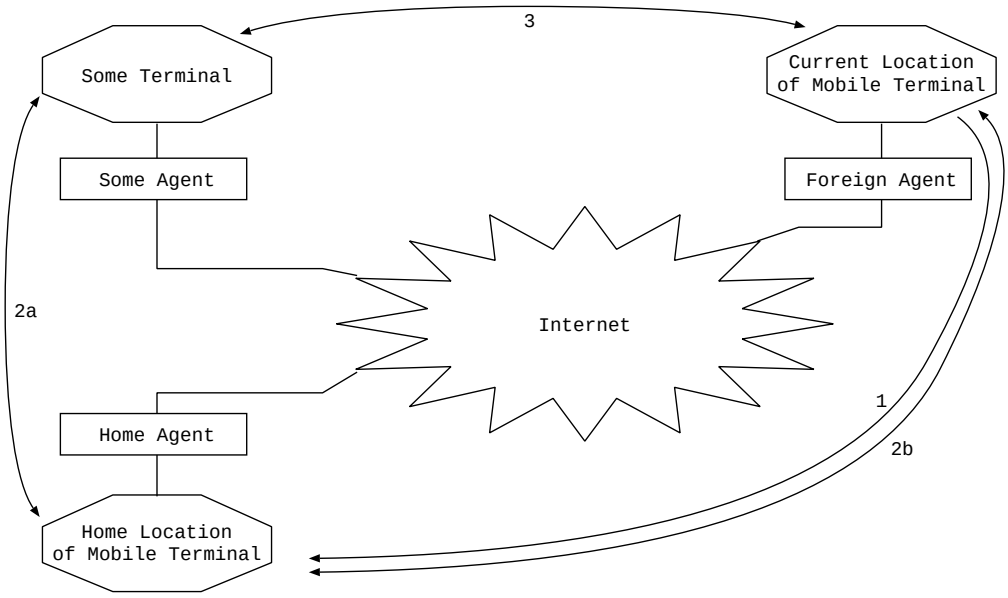
1.6 Auto Configuration

In IPv6 the configuration is much easier because of the new auto-configure feasibility. The terminal gets its address fully automatically, no manual configuration is needed. On the other hand, it is still possible to set the IP address manual.

After the terminal is switched on, the node identifier is generated. The address prefix is set to an special value which indicates that this first address is a local address. This address enables the terminal to access the local network. After it has been checked that the calculated node identifier is unique, the terminal connects the local router and ask for an auto-configuration. There are two ways of configuring the IP address: the first possibility is that the router gives an address prefix to the terminal. With this new prefix the IP address of the terminal is complete and access to the Internet is possible. In the second scenario the router gives the IP address of an local DHCP server to the terminal. The terminal gets its IP than from the DHCP server. This design makes it possible to keep it simple (way one) or to do IP address management with a DHCP server. This is a very important benefit in the mobile environment because it makes it possible to move through different networks without knowledge of them. (Kozierok, 2004)

1.7 Mobile IP

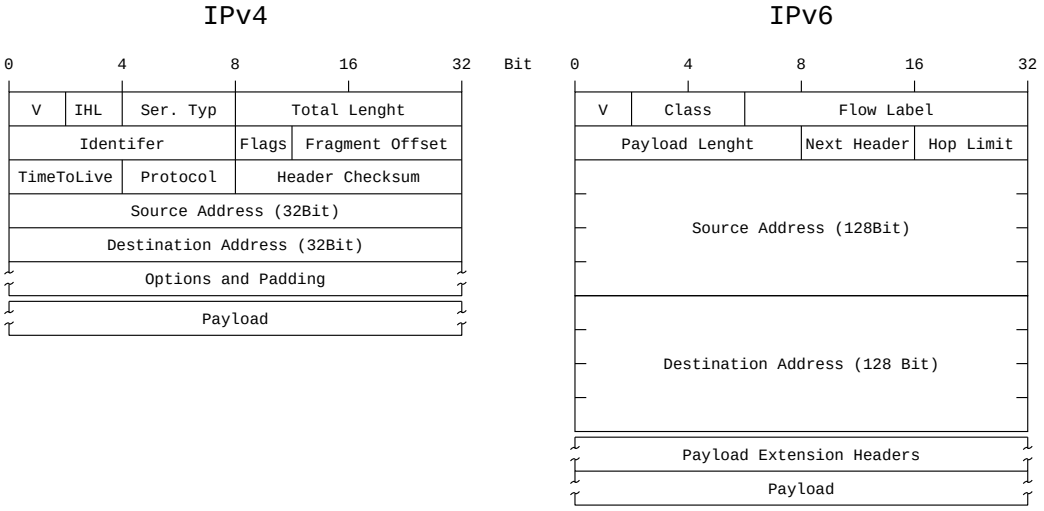
Mobile IPv6 provides the possibility to connect a terminal anywhere in the Internet. When the terminal uses the home-network/provider to get access to the Internet there is no problem connecting it. This becomes difficult if the terminal has moved from the home subnet to another subnet. By changing the subnet, the IP address changing as well. In this case the home agent has to know where the mobile terminal can be found. In step 1 the mobile terminal tells the home agent its new address (current location). If some terminal wants to connect the mobile terminal it tries to connect the home location of the mobile terminal (2a). The home agent knows that the mobile terminal is not at home and hands the connection over a tunnel to the current location of the mobile terminal (2b). This way of communication is not efficient because all transmissions have to transmit through the home agent. For this reason it is possible to give the current location of the mobile terminal to the 'some terminal'. After this the a direct connection can be established (3). Adapted from Strand (2004) and Palet (2004).



The way of data if the mobile terminal is not at home. Routing over the home agent or direct.

1.8 New Header Structure

The following picture faces the protocol headers of IPv4 and IPv6. Adapted from Impress (2003) and Forouzan (2001).



The header structure of IPv4 faced against IPv6's ones.

The header structure in IPv6 was reviewed and optimised. It can be faster processed by routers and other devices. The most important change is the increase of the address fields form 32 bit to 128 bit. The `Time to Live` (TTL) field from IPv4 is now called `Hop Limit`, it is still an 8 bit field. It contains the number of still allowed hops. Within every hop this value is decreased by one. The 8 bit field `Next Header` is a pointer which point to a payload extension header. Additional information such as header from an upper layer (TCP, UDP or ICMPv6), fragmentation, encryption or authentication details can be stored in the payload extension header. The overall size of the payload is stored as a 16 bit value in the `Payload Length` field. The `Flow Label` field provides the possibility of special handling of particular data-flows. It is 24 bit long. Traffic control with `Priority` if realized with a 4-bit-field. The `V`-field (Version) does not change its meaning, position or size. It still contains the version number of IP. In IPv4 a binary 4, and in IPv6 a binary 6. (Impress, 2003; Palet, 2004)

The IPv4 header has not a fixed size. The smallest header is 20 bytes long and grows if some additional information, such as encryption details, are stored in the option field. In contrast, IPv6 has a fixed header size of 40 bytes. Additional information is not longer stored in the header of the packet. This information is stored in the `Payload Extension Headers` which are a part of the Payload. Because of the fixed header size and the fact that all important information (for routing, for example payload length) stored in the beginning of each packet, it is possible to process an IPv6 packet much faster as an old IPv4 one. The unnecessary checking of the header information was disestablished, because this will be done in the previous layer. This speeds up the processing of an IPv6 packet again, because the checksum does not need to be recalculated in every hop. (Palet, 2004; Forouzan, 2001)

1.9 Fragmentation

Another simplification is made in the fragmentation process. In IPv6 only the sender of a packet does fragmentation (Kozierok, 2004). If a router receives an IPv6 packet which is too large, an error message is sent back to the sender. The sender has to send smaller packets. An IPv4 packet will be fragmented by the router if it is too big. In this case the other side has to be able to do the reserve process, the defragmentation. Therefore information about the fragmentation process has to be stored in the packet header. This makes the processing of an IPv4 packet much slower and more complicated. All information about fragmentation in IPv6 are stored in a payload extension header. The payload extension headers are within the payload and have no influence on the

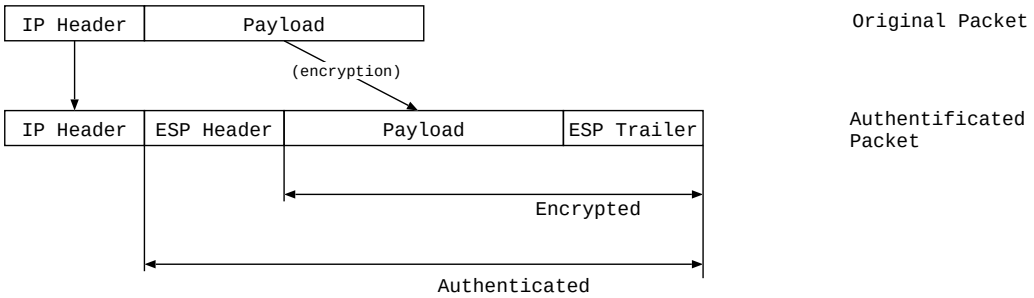
transport (the routers do not take it into account). The payload headers are used for the end-to-end communication only. (Palet (2004) mentioned the exception of the routing header)

1.10 IPsec

IPsec was developed for IPv6, it is native implemented in IPv6. Because of the fact that the majority of the computers still use IPv4, IPsec was adapted to IPv4 as well. The basic idea of IPsec is the encapsulation of data to establish a virtual private networks (VPNs). This is a end-to-end process because it is undesirable that any terminal between the sender and the receiver can access or modify the data. There are two categories of these VPSs: encryption/authentication and tunnelling. If authentication is used, an authentication header (AH) is added to the packet. This extra header contains information which is used to make sure that the sender is the right one.

IPsec: The transformation of an packet to an authenticated one.

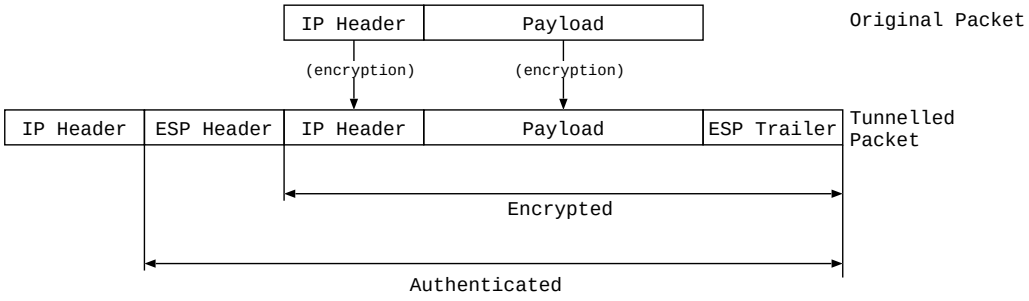
In case of an encryption the payload of a packet will be encrypted. An ESP (encapsulation security payload) header and trailer is added to maintain encryption and authentication.



IPsec: The transformation of an packet to an encrypted one.

For tunnelling it is necessary to create a complete new packet which contains a new IP header, (an encrypted version of) the original packet, ESP header and

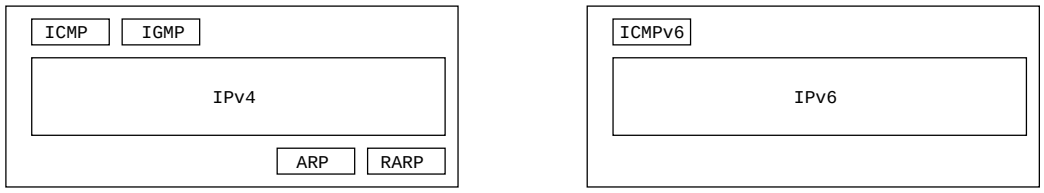
trailer. Adapted from Forouzan (2001).



IPsec: The transformation of an packet to an tunnelled one.

1.11 Network Layer

The following graph shows the difference between the two (IPv4 and IPv6) network layers. Adapted from Forouzan (2001).



The difference between the network layers in IPv4 and IPv6.

IP works within or is a part of the network layer. The IPv4 network layer contains additionally to the IPv4 the Internet Control Message Protocol (ICMP), the Internet Group Management Protocol (IGMP), the Address Resolution Protocol (ARP), and the Reverse Address Resolution Protocol (RARP). IGMP provides the feasibility to doing multi-casting (Baccala, 1997). The ICMP announces network errors, network congestion, and timeouts. In addition it can be used to assist troubleshooting (Baccala, 1997). The ARP is necessary to figure out the right corresponding (to the Network or IP address) physical address. The RARP does this the other way around. Forouzan (2001) says that IGMP, ICMP, and ARP centralised to the ICMPv6 within the IPv6. RARP is not longer supported because it is rarely used.

1.12 Conclusion

The experience of the strengths and weaknesses in IPv4 was used to develop the new Internet Protocol. That is the reason why this Internet Protocol in version 6 solves all the major problems of today's (and hopefully the future's) Internet.

1.13 Bibliography

Saint Baccala, B (1997) *Connected: An Internet Encyclopedia*
[Online] Available at http://www.freesoft.org/CIE/
(accessed 29 November 2004)

Bieringer, P. (2004) *Linux IPv6 HOWTO*
[Online] Available at http://www.tldp.org/HOWTO/Linux+IPv6-HOWTO/
(accessed 20 November 2004)

Cocquet, P. (2004) *IPv6 on DSL: The Best Way to Develop Always-On Services*, Proceedings of the IEEE 92 (9) September 2004 pp 1400-1408
[Online] Available at http://ieeexplore.ieee.org/iel5/5/29301/01323288.pdf
(accessed 2 October 2004)

de.wikipedia.org (2004) *IPv6*
[Online] Available at http://de.wikipedia.org/wiki/Ipv6
(accessed 27 November 2004)

en.wikipedia.org (2004) *IPv6*
[Online] Available at http://en.wikipedia.org/wiki/Ipv6
(accessed 27 November 2004)

Forouzan, B. A. (2001) *Data Communication and Networking, 2nd edition.* McGraw-Hill, New York

Hinden, R.; Deering, S. (1998) *RFC 2373 - IP Version 6 Addressing Architecture*
[Online] Available at http://www.faqs.org/rfcs/rfc2373.html
(accessed 5 December 2004)

Impress, NTT Communications (2003) *IPv6style: Learning the IPv6 header*
[Online] Available at http://www.ipv6style.jp/en/tech/20030331/index.shtml
(accessed 29 November 2004)

Kozierok, C. M. (2004) *The TCP/IP Guide*
[Online] Available at http://www.tcpipguide.com/free/index.htm
(accessed 1 December 2004)

Palet, J (2004) *What are the technical benefits of implementing IPv6*
[Online] Available at http://www.cu.ipv6tf.org/pdf/006.pdf
(accessed 05 Decemder 2004)

Sæther, Ø (2004) *Why you want IPv6*
[Online] Available at http://linuxreviews.org/features/ipv6/
(accessed 12 November 2004)

Strand, L (2004) *Linux Mobile IPv6 HOWTO*
[Online] Available at http://www.tldp.org/HOWTO/Mobile-IPv6-HOWTO/index.html
(accessed 5 December 2004)