

# REPORT ON THE SECURITY IMPLICATIONS OF IMPLEMENTING IPv6

**INTECO-CERT**

## ACKNOWLEDGEMENTS

The National Institute of Communication Technologies (INTECO) would like to acknowledge and thank the following people and companies for their invaluable help and contribution in the preparation of this report: Joao Damas from *Bondis*, Jesús Rodríguez from *Voztele*, Juan Cerezo from *BT* and Jordi Palet, Cesar Olvera and Álvaro Vives from *Consulintel*.

The copyright of this document belongs to the National Institute of Communication Technologies (INTECO) and is licensed under the Creative Commons Attribution-NonCommercial 3.0 Spain license; therefore, you are free to copy, distribute and transmit this work under the following conditions:

- Attribution: Third parties are free to reproduce all or part of the content of this report, quoting the source and including express reference both to INTECO and its website: [www.inteco.es](http://www.inteco.es). This attribution shall in no case mean that INTECO provides support to that third party or support the use made by it of this document.
- Noncommercial use: The original material or its derivative works may be distributed, copied or displayed as long as they are not used for commercial purposes.

For any reuse or distribution you must make clear to others the license terms of this work. Some of these terms may not be applied if INTECO gives you permission to act as copyright holder. No part of this license damages or diminishes the moral rights of INTECO. <http://creativecommons.org/licenses/by-nc-sa/3.0/es/>

This document meets the PDF format accessibility requirements. It is a tagged and structured document, with alternatives to every non-textual element, language marking and appropriate reading order.

For further information on the production of accessible PDF documents consult the guide available in the section Accessibility > Training > Manuals and Guides of our website <http://www.inteco.es>

## CONTENTS

---

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>MOTIVATION AND OBJECTIVES</b>   | <b>4</b>  |
| <b>2</b> | <b>INTRODUCTION TO THE IP PROTOCOL</b>   | <b>5</b>  |
| 2.1      | The need for the IPv6 protocol   | 5         |
| <b>3</b> | <b>IPv6 SECURITY IMPROVEMENTS</b>  | <b>7</b>  |
| 3.1      | IPsec deployment   | 7         |
| 3.2      | Greater robustness of the network  | 9         |
| 3.3      | Other improvements   | 9         |
| <b>4</b> | <b>IPv6 SECURITY CONSIDERATIONS</b>  | <b>11</b> |
| 4.1      | Technical aspects  | 11        |
| 4.1.1    | Security devices that do not analyse the IPv6 protocol                                   | 11        |
| 4.1.2    | Presence of devices which are not known to be capable of using IPv6, and of IPv6 tunnels | 11        |
| 4.1.3    | Stopping using NAT   | 12        |
| 4.1.4    | Need for multicast and ICMP  | 12        |
| 4.1.5    | Change in network monitoring   | 13        |
| 4.1.6    | IPv6/IPv4 dual-stack systems   | 13        |
| 4.1.7    | Upgrade of protocols and devices to IPv6   | 13        |
| 4.2      | Management issues  | 13        |
| 4.2.1    | Learning curve   | 13        |
| 4.2.2    | Implementation of dual-stack systems   | 13        |
| 4.3      | Specific structure or features of IPv6   | 14        |
| 4.3.1    | Identity theft in the IP address auto-configuration process                              | 14        |
| 4.3.2    | Privacy  | 14        |
| <b>5</b> | <b>RECOMMENDATIONS FOR ACTION</b>  | <b>16</b> |
| 5.1      | General recommendations  | 16        |
| 5.2      | Recommendations for the use of IPv6  | 16        |
| <b>6</b> | <b>CONCLUSIONS</b>   | <b>18</b> |
| <b>7</b> | <b>INFORMATION SOURCES</b>   | <b>19</b> |

## 1 MOTIVATION AND OBJECTIVES

---

In order for the Internet to keep growing and evolving, one of its key elements needed to be reviewed: the IP protocol. Its new version, IPv6<sup>1</sup>, is designed as the successor to IPv4 in the Internet, providing solution to many of its faults. The IPv6 protocol, among other advantages, solves the IP address exhaustion problem, includes security capabilities for the encryption and authentication in end-to-end communications and enables the creation of new services.

This report aims to support security managers, system administrators and security technicians when considering the transition to this new version of the IP protocol which is so important to the organisations' information systems. The main purpose of this report is to inform on the following aspects:

- To describe its capabilities.
- To detail the security issues that must be taken into account.
- To provide a good practice code or recommendations for action.

---

<sup>1</sup> <http://tools.ietf.org/html/rfc2460>

## 2 INTRODUCTION TO THE IP PROTOCOL

---

The IP protocol is the protocol most used by computer systems to intercommunicate. The majority of higher-level applications or protocols (HTTP, SMTP, P2P, etc.) are based on this protocol for their functioning.

Computers and devices using the IP protocol are assigned a unique identifier called IP address to route the message through the different communication network nodes from source to destination. This identifier is a 32-bit integer number which is usually represented as four numbers, from 0 to 255, each separated by a dot, for its greater ease of handling.

### 2.1 THE NEED FOR THE IPv6 PROTOCOL

Since the IP address consists of 32 bits, it is possible to have some 4,300 millions of different addresses. Nevertheless, mainly due to the huge number of devices or computers using the IP protocol which consequently need an IP address, the number of available addresses is exhausting. Although an attempt to alleviate this with solutions such as NAT<sup>2</sup> or CIDR<sup>3</sup> has been made, these are not able to settle the basic problem and, additionally, bring limitations such as the loss of end-to-end connectivity.

A new protocol version known as IPv6 has been created to resolve this problem, which uses a 128-bit integer as IP address, so that IPv6 has  $2^{96}$  times more addresses than IPv4. In reality, however, considering that the smallest IPv6 subnet is 64 bits long, it is more appropriate in IPv6 to talk about a total space of 2 raised to the power of 64 subnets with 2 raised to the power of 64 possible addresses in each one. Moreover, by reviewing the protocol, further improvements and capabilities have been included:

- Automatic IP address auto-configuration and reconfiguration without needing servers (stateless).
- Native and improved support for multicast addressing and creation of the anycast addressing.
- Required IPsec deployment.
- More efficient routing.
- Optimized IP mobility support.
- Implementation of flow labels for QoS.
- Implementation of Jumbograms.

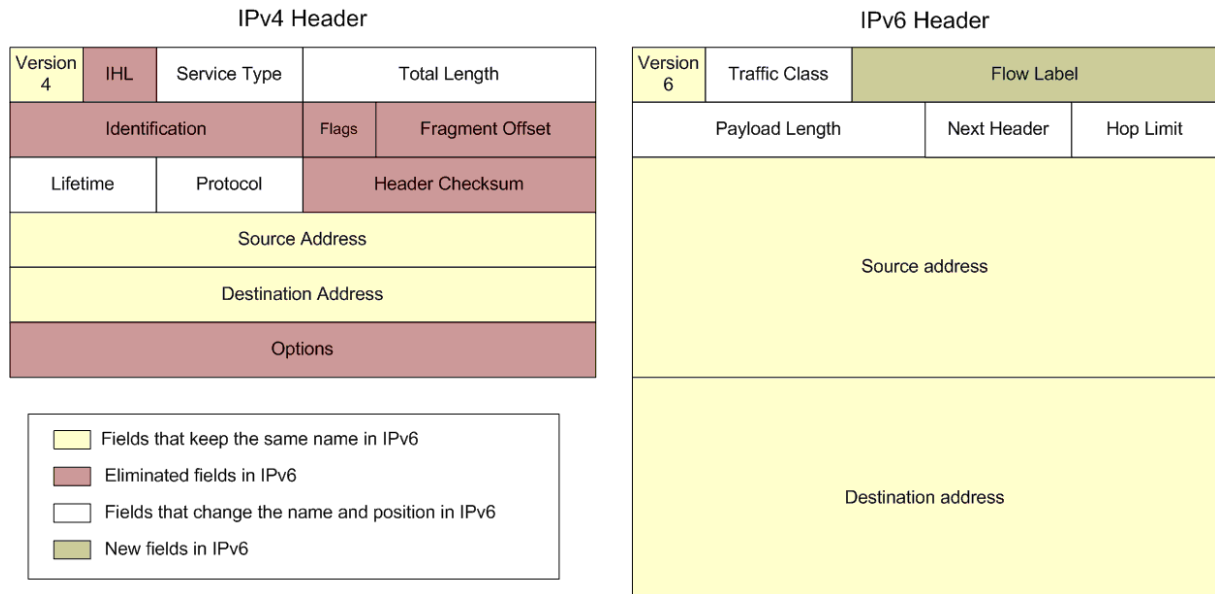
---

<sup>2</sup> Network Address Translation: [http://es.wikipedia.org/wiki/Network\\_Address\\_Translation](http://es.wikipedia.org/wiki/Network_Address_Translation)

<sup>3</sup> Classless Inter-Domain Routing: [http://es.wikipedia.org/wiki/Classless\\_Inter-Domain\\_Routing](http://es.wikipedia.org/wiki/Classless_Inter-Domain_Routing)

IPv4 devices are expected to coexist with IPv6 devices for a long time (this is hard to predict, but possibly for 10 to 20 years) thanks to transition and co-existence mechanisms, implementing both protocols simultaneously or through tunnels over IPv4.

This huge increase in the number of available IP addresses will allow the interconnection of a virtually unlimited number of elements such as electrical household appliances, cars, sensors, etc. with the aim of providing new services.



*Figure 1 - IPv4 and IPv6 headers*

## 3 IPv6 SECURITY IMPROVEMENTS

---

### 3.1 IPSEC DEPLOYMENT

IPv6 explicitly includes the option of using the IPsec (Internet Protocol Security) security model, which **provides transparency, integrity and confidentiality for end-to-end communications**.

IPsec is a set of open protocols aimed at providing security for communications of the OSI network layer (to which the IPv6 protocol belongs) and, consequently, for all upper-layer protocols.

The deployment of IPsec in IPv4 is defined in a specification different from the IPv4 protocol itself, so the inclusion of the protocol is performed through mechanisms defined outside it, whereas in IPv6 the very “extensible” architecture of the protocol allows implementing IPsec in a natural way. It is also important to highlight that IPv6 enables the use of IPsec, but not the specific encryption and authentication mechanisms of IPsec.

IPsec offers two functioning modes, each providing distinct security levels:

- Transport mode: the IP payload is encrypted and/or authenticated, but the headers are not considered. It has the advantage that it can be used end-to-end but, on the other hand, the header data, such as the source and destination IP addresses, are readable.
- Tunnel mode: a platform, or gateway, encapsulates the original packet in another packet. Through this, the entire original packet is encrypted and/or authenticated, but a gateway is required for the tunneling.

In addition to this, IPsec offers two transference models or protocols which may, in turn, work in tunnel or transport mode:

- AH (Authentication Header): provides authentication, integrity and (optional) anti-replay protection.
- ESP (Encapsulating Security Payload): apart from the above mentioned advantages, it also provides confidentiality.

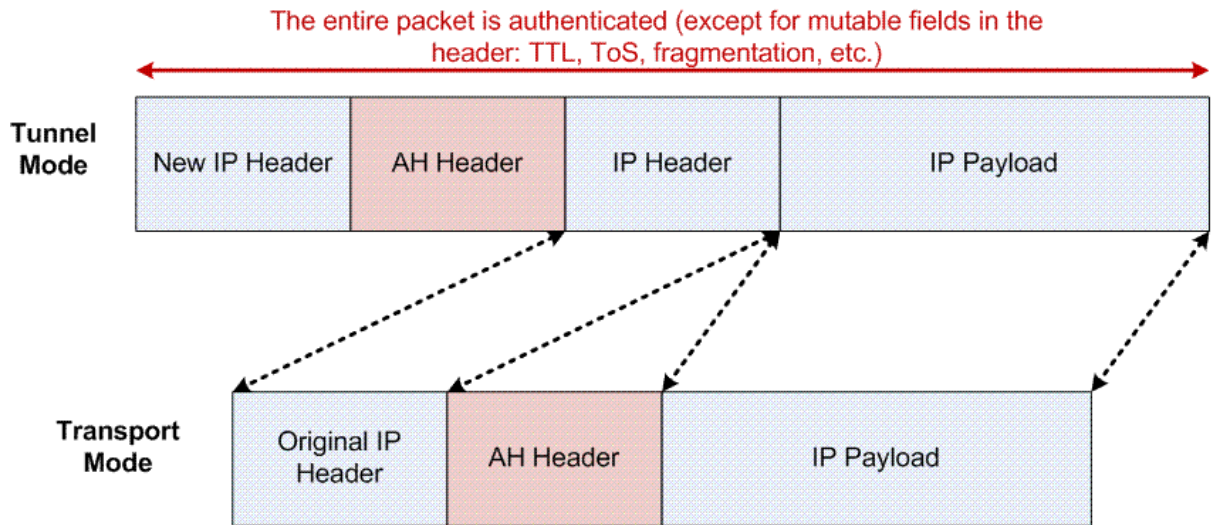


Figure 2 – AH implementation in tunnel and transport mode

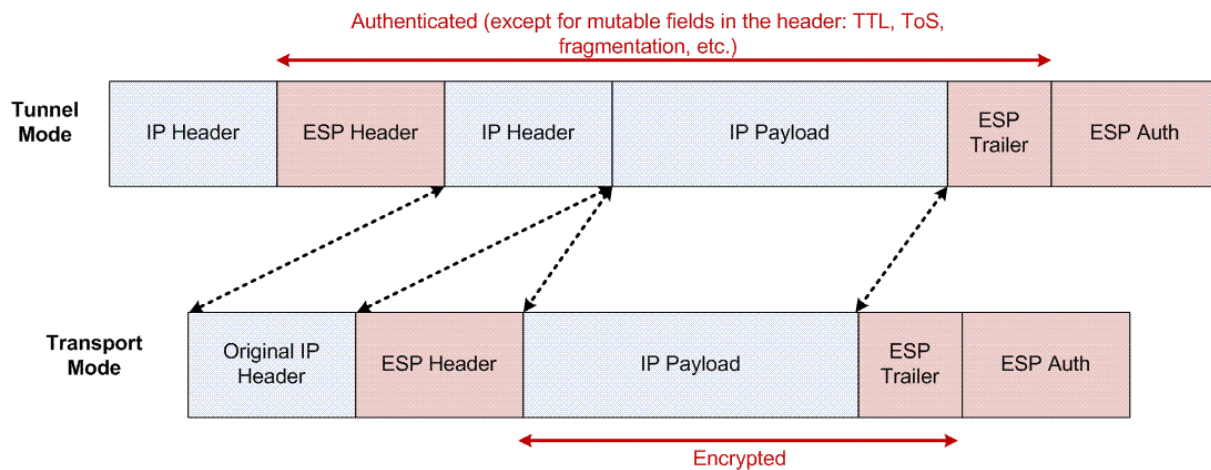


Figure 3 - ESP implementation in tunnel and transport mode

In practice, the use of IPsec is limited, especially due to the lack of a widespread and global key exchange mechanism. Therefore, the use of IPsec in IPv6 is for the moment similar to that in IPv4 for pre-configured connections such as, for example, those used in VPNs.

The future solution to the above mentioned problem may lie in external mechanisms, such as certificates transported through DNSSEC<sup>4</sup>-secured DNS.

<sup>4</sup> Domain Name System Security Extensions: <http://www.icann.org/es/announcements/dnssec-qa-09oct08-es.htm>

## 3.2 GREATER ROBUSTNESS OF THE NETWORK

The new version of the protocol includes some new features that improve the efficiency of the IP packet routing process. This will allow the network elements to be capable of managing a greater number of transmissions more rapidly. The changes are as follows:

- Simplified and fixed-size headers.
- No fragmentation of IP packets by intermediate elements. The size of the packets will be determined by the communication endpoints. Nevertheless, although this should favour the data flow in the long term, as it greatly differs from what is done in IPv6 and is based on ICMP, this feature is causing problems in the implementation of IPv6, leading to connectivity errors that are making IPv6 appear not to be working entirely correctly in practice.
- It facilitates the address aggregation in the routing tables thanks to the strict use of CIDR for all address types and to a better organization of their assignments. On the other hand, this improvement is indispensable because of the huge increase in the number of IP addresses.
- Required and improved implementation of multicast addressing and creation of the anycast addressing, where a set of hosts that provide the same service share a common address, so that the host selected to provide such service will be determined by the efficiency of access, even though it is difficult to implement this addressing in practice and it is mostly only used by routers.
- Use of labels for QoS (Quality of Service) within communications: this protocol includes the possibility of labeling communication classes and flows in order for routers to give priority to some transmissions over others.

## 3.3 OTHER IMPROVEMENTS

- Impossibility to scan networks through “brute force”. Before the appearance of this protocol, hackers or malicious software, such as worms, could find targets in a network by checking all possible addresses. However, due to the exponential growth in the total number of addresses, this scan is now, a priori, unfeasible.
- The necessity of using NAT disappears. Although this technology has been highly useful, it has the disadvantage that it generates a false sense of security and that the possibility of establishing secure end-to-end connections is lost, thus increasing the complexity and cost of developing applications.

- To carry out a broadcast- or smurf<sup>5</sup>-type DDOS attack is not possible anymore, since this addressing method is removed and certain security measures are implemented for multicast.

---

<sup>5</sup> <http://www.cert.org/advisories/CA-1998-01.html>

## 4 IPv6 SECURITY CONSIDERATIONS

---

For the time being, the number of security problems and attacks on IPv6 is small, since this protocol is not deployed at large scale yet. This trend is, however, expected to change as operators and content providers start to implement it in their networks and services.

The following section provides an overview of the main security-related aspects of this protocol, which must be considered from three different perspectives:

- Technical aspects
- Management issues
- Specific structure or features of IPv6

### 4.1 TECHNICAL ASPECTS

#### 4.1.1 Security devices that do not analyse the IPv6 protocol

Security devices, such as firewalls or IDSs, or network management tools may not be capable or configured to analyse IPv6 data flow. If this was the case then malicious communications could be established from and to network computers supporting IPv6.

#### 4.1.2 Presence of devices which are not known to be capable of using IPv6, and of IPv6 tunnels

The IPv6 protocol is enabled by default in many Operating Systems, namely the majority of modern Windows systems, Mac OS X, Linux and Solaris.

There may also be IPv6 tunnels. A tunnel is a point-to-point connection, where the IPv6 packets are encapsulated in IPv4 packets so as to transmit IPv6 through an IPv4 infrastructure. The original IPv6 packet is then unencapsulated (or extracted) in the tunnel endpoint.

Perimeter security devices may not be prepared or configured to analyse these data flows, which can be used for unauthorised communications such as, for instance, botnet or P2P C&C (Command and Control) backdoors.

The option of creating IPv6 tunnels is supported by all operating systems, such as Windows Vista and Windows 7, in which the Teredo<sup>6</sup> technology is enabled by default, although this is disabled if it detects through its local network that the computer belongs to an IPv6 domain or

---

<sup>6</sup> <http://msdn.microsoft.com/es-es/library/aa965905%28v=VS.85%29.aspx>

supports IPv6. Other tunnel implementation methods that may be used are 6to4<sup>7</sup> and ISATAP<sup>8</sup>.

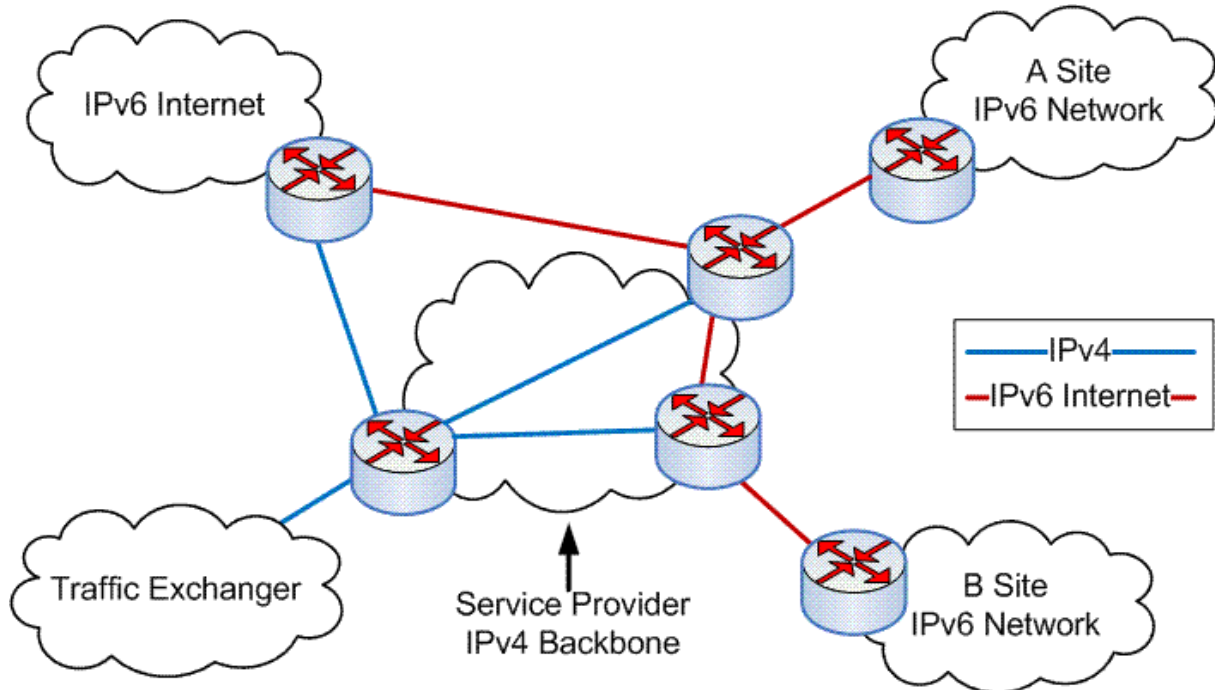


Figure 4- IPv6 tunnel in IPv4

### 4.1.3 Stopping using NAT

A direct implication of using NAT is that it is used as firewall to protect internal computers from outside connections. Nevertheless, as IPv6 eliminates the need for using NAT, the firewall settings will have to be changed, according to the security policy, in order for the firewall to filter or not to filter the direct communications with the computers in the private network.

### 4.1.4 Need for multicast and ICMP

A great number of firewalls block these protocols, even though certain parts may be vital, e.g. the use of ICMP for PMTU. These features are essential for the functioning of IPv6 and, therefore, the security policies will have to be modified to allow specific multicast and ICMP communications.

<sup>7</sup> Intra-Site Automatic Tunnel Addressing Protocol: <http://es.wikipedia.org/wiki/ISATAP>

#### 4.1.5 Change in network monitoring

Owing to the huge number of available addresses, scanning the network through “brute force” will not be feasible and, consequently, computers would find another way, such as, for example, through a DNS server.

Nevertheless, it is possible that other methods to scan the network will appear: there are specific multicast addresses to find services (e.g. FF05::2 All routers, FF05::1:3 All DHCP Servers) and link-local addresses which permit communication in the network segment to which the user is connected. A hacker may use these addresses to make contact with computers or services. In practice, however, this method is not likely to be successful, since most operating systems are configured not to reply to these requests.

#### 4.1.6 IPv6/IPv4 dual-stack systems

Dual-stack systems supporting both protocol versions and IPv6 transition mechanisms will co-exist for years, which will lead to a greater risk of the appearance of vulnerabilities.

On the other hand, a system can be attacked using IPv4, IPv6 or a combination of both, e.g. using IPv4 to detect the computer and using IPv6 as hidden communication channel.

#### 4.1.7 Upgrade of protocols and devices to IPv6

The great majority of protocols have been adapted to be capable of using IPv4 and IPv6 addresses, such as BGP or DNS. Implementing IPv6 will involve the installation and/or configuration of these protocols.

There is the problem that some applications working with IPv6 are not updated very often. There is also currently lack of support by some manufacturers of routers, switches and firewalls, although a further boost is expected as wider adoption of the protocol takes place.

### 4.2 MANAGEMENT ISSUES

#### 4.2.1 Learning curve

Just like with any adoption of a new technology, organisations will need time and resources to acquire the necessary knowledge to securely implement and manage the IPv6 protocol.

#### 4.2.2 Implementation of dual-stack systems

The implementation of IPv6 will involve a significant change in communication systems, since these will have to support both protocols and their interoperability. The design, implementation and configuration of these dual-stack systems, which implement both IPv4 and IPv6, will be a complex process in which all possible security requirements will need to be assessed.

## 4.3 SPECIFIC STRUCTURE OR FEATURES OF IPV6

The use of IPv4 has evolved over time, the problems arising being solved thanks to its widespread use for many years. Technologies such as NAT, CIDR or IPsec have been therefore created.

The IPv6 protocol may go through a similar process, although mitigated by the experience gained of Ipv4. An example of the protocol evolution process is the decision of rejecting packets that use the RH0<sup>8</sup> header, which is used to determine the packets' route, because it could be used to carry out a DoS attack<sup>9</sup>.

There are already available solutions to the issues described below, although there are some operating systems which do not implement them yet.

### 4.3.1 Identity theft in the IP address auto-configuration process

One of the new features of the IPv6 protocol is the capability of an interface to generate its IP address from its MAC address. During this process the device asks the rest of the network devices whether some are using that address. Likewise, if the device is connected to a network where there is a router, this will receive from it the remaining configuration settings, such as the network prefix.

During this process, any device would be able to generate a false response in a continuous way, informing that the address is being used, and cause the device requesting an address to fail to connect to the network. It could also pretend to be a router in order to carry out a man-in-the-middle attack.

The SEND<sup>10</sup> protocol solves this problem, although it has not been implemented yet in most operating systems. SEND is an extension that improves the security of the NDP<sup>11</sup> protocol, which is responsible for detecting other nodes within the local network, routers, etc. In order to perform its functions, SEND uses asymmetric encryption and electronic signature. SEND represents a clear improvement compared to IPv4, where there is nothing similar.

### 4.3.2 Privacy

If a computer generates an IP address from its MAC address, an IP can be univocally associated with a computer and, likewise, a PC can be associated with an individual.

When using the Internet, the user leaves traces of their IP address in the different servers or networks with which communication is established. Through this IP address, it would be possible to know which web servers or services the user visited.

---

<sup>8</sup> Routing Header type 0: <http://tools.ietf.org/html/rfc5095>

<sup>9</sup> <http://www.securityfocus.com/news/11463>

<sup>10</sup> Secure Neighbor Discovery: <http://tools.ietf.org/html/rfc3971>

<sup>11</sup> Neighbor Discovery Protocol: <http://tools.ietf.org/html/rfc4861>

A solution to this problem is the random generation of part of the IP address, what is known as privacy extensions<sup>12</sup>. Most operating systems support privacy extensions and these are even enabled by default in some of them (Windows XP, Vista and 7). Another possible solution is to temporarily assign addresses through DHCPv6.

---

12 Privacy Extensions for Stateless Address Auto-configuration in IPv6: <http://tools.ietf.org/html/rfc4941>

## 5 RECOMMENDATIONS FOR ACTION

---

### 5.1 GENERAL RECOMMENDATIONS

1. To create security policies which take into account the IPv6 protocol.
2. To acquire knowledge on the management of IPv6 systems, since, although all IPv6 traffic can be currently blocked or the user can have IPv4 addresses, this protocol will be increasingly necessary, as the providers will integrate their services with IPv6. The best way to do this is gradually, starting with a few highly controlled services. It is advisable to begin as soon as possible, since in June 2010 the overall available space for IPv6 addresses has been reduced to less than 6%.
3. To have security devices and network management tools which are capable of analysing and, if necessary, blocking the IPv6 data flow and the IPv6 tunnels or transition mechanisms. To follow an IPv6 security policy similar or identical to the one used for IPv4, e.g. not to allow the transmission of a certain type of traffic in IPv6 if this is not permitted either in IPv4. When allowing IPv6 traffic flow is required, it is advisable, if possible, to define a subset of differentiated security policies and rules for IPv6 traffic; and specifically for ICMPv6: as previously pointed out, the filtering of ICMPv6 traffic may have a much more direct impact on the permitted traffic and on the computers' IPv6 connectivity.
4. To prepare an inventory of existing devices supporting the IPv6 capability or capable of creating IPv6 tunnels and disable this option if not needed.

### 5.2 RECOMMENDATIONS FOR THE USE OF IPV6

1. Depending on the degree of control you want to have over each network, different address configuration mechanisms must be used. From lower to higher control and traceability we can find the following options:
  - Stateless auto-configuration. There are two options:
    - Interface identifier through random numbers (privacy extensions). This option is not recommended if, for legal reasons, having a record of use of the network by each user is required. Neither is it advisable when static addresses are needed, for example, for Peer-to-Peer applications, which generally involves recording DNS addresses.
    - Interface identifier through the MAC address.
  - Stateful auto-configuration – DHCPv6
  - Manually configured addressing

2. Not to use deducible or predictable addresses, with the aim of making it difficult to find attackable nodes in a network in the case of manually configured addresses.
3. As a general rule, it is advisable to filter traffic coming from prefixes which are not assigned by IANA or RIRs<sup>13</sup>. The ULA-type (Unique Local Address) addresses must not reach the Internet or enter the network, since these addresses are for internal use only. The addresses relative to the old 6Bone test network and to the documentation IP addresses, the prefix of which is 2001:0DB8::/32, must also be filtered.

---

<sup>13</sup> <http://www.iana.org/numbers/>

## 6 CONCLUSIONS

---

In addition to alleviating the shortage of IP addresses, the IPv6 protocol has been created from the start with the aim of achieving security and efficiency; measures such as the implementation of IPsec, the new design of the IPv6 packet or the IP address assignment methods are all evidence of that purpose.

Nevertheless, to replace a protocol as widespread and important as IPv4 involves a management and technical challenge with implications for the security of information systems.

Since most operating systems include the possibility of using IPv6, it is necessary to plan a security policy which provides for this aspect and take the appropriate measures to meet its requirements.

Due to the exhaustion of IPv4 addresses and the increasing emergence of IPv6 services and other new services which take advantage of the explosion of available IP addresses, it is also required to begin to gain knowledge and experience on the implementation and management of this protocol and its interoperability mechanisms with IPv4. The best way to do this is to gradually enable it in some services in a highly controlled manner.

## 7 INFORMATION SOURCES

---

European Commission: [http://ec.europa.eu/information\\_society/policy/ipv6/index\\_en.htm](http://ec.europa.eu/information_society/policy/ipv6/index_en.htm)

ENISA: <http://www.enisa.europa.eu/act/res/files/resilience-features-of-ipv6-dnssec-and-mpls/?searchterm=ipv6>

SecurityFocus: <http://www.securityfocus.com/news/11463>

IETF: <http://www.ietf.org/rfc/rfc3971.txt>

Microsoft: <http://technet.microsoft.com/en-us/network/bb530961.aspx>

Consulintel: [http://www.mundointernet.es/IMG/pdf/ponencia162\\_1.pdf](http://www.mundointernet.es/IMG/pdf/ponencia162_1.pdf)

NetworkWorld: <http://www.networkworld.com/news/2009/071309-ipv6-network-threat.html>

Portal IPv6: <http://www.ipv6tf.org>

IPv6-To-Standard: <http://www.ipv6-to-standard.org>

[[RFC3756](#)] Nikander, P., Kempf, J., and Nordmark, E., "IPv6 Neighbor Discovery (ND) Trust Models and Threats", May 2004, IETF Request For Comment

[[RFC3971](#)] Arkko, J., Kempf, J., Zill, B., and Nikander, P., "Secure Neighbor Discovery (SEND)", March 2005, IETF Request For Comment

[[RFC4193](#)] Hinden, and R., Haberman, B., "Unique Local IPv6 Unicast Addresses", October 2005, IETF Request For Comment

[[RFC4861](#)] Narten, T., Nordmark, E., Simpson, W., and Soliman, H., "Neighbor Discovery for IP version 6 (IPv6)", September 2007, IETF Request For Comment

[[RFC4941](#)] Narten, T., and Draves, R., "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", January 2001, IETF Request For Comment

[[RFC5095](#)] Abley, J., Savola, P., and Neville-Neil, G., "Deprecation of Type 0 Routing Headers in IPv6", December 2007, IETF Request For Comment

[[RFC5157](#)] T., Chown, "IPv6 Implications for Network Scanning", March 2008, IETF Request For Comment

Scott Hogg, Eric Vyncke, "IPv6 Security", Cisco Press, 2008

Daniel Minoli, Jake Kouns "Security in an IPv6 Environment", Auerbach Publications, 2008