Abstract

There has been specific research conducted into technical IPv6 security risks, but not that much on putting it all together and also taking risk for IT management into account. In this research the following question is answered: what impact has IPv6 on the security and management of IT infrastructures, and which mitigating controls are to be implemented? Research on the latests Internet standards, books, papers, articles and presentations has been conducted, showing that security risks are present for both technology and IT management. Security risks which can be exploited using publicly available tools. Technical solutions for security risks exists and IT management can train IT personnel and improve policies, processes and guidelines.
5 Recommendations & mitigating controls

5.1 Technical security risks

5.1.1 Man-in-The-Middle (MiTM) & Denial-of-Service (DoS)

5.1.2 IPv6 address privacy

5.1.3 Dual stack hosts

5.1.4 Extension Headers

5.1.5 IPv6 tunnels

5.2 IT management risks

5.2.1 Implementation maturity

5.2.2 Lack on IPv6 knowledge

5.2.3 Address notation

5.2.4 Public IT infrastructure security

5.3 Conclusion
1 Introduction

IPv6 is the successor of IPv4 and was developed in the nineties to solve the problem on the lack of IPv4 addresses (figure 1). The address field in IPv4 is 32 bits long and has therefore support for a total of \(2^{32} (4 \times 2^{96})\) possible addresses. IPv6 uses 128-bit addresses, for an address space of \(2^{128}\) (approximately \(3.4 \times 10^{38}\)) addresses. In addition, many other changes were introduced in the IPv6 protocol\[1\] due to lessons learned from IPv4. For example, the header of an IPv6 packet always has the same length (40 bytes) to increase performance of routing packets over the Internet.

Besides changes in the protocol itself, IPv6 is also the driving force for the development of new and/or modified protocols. For example, protocols to tunnel IPv6 traffic over IPv4 IT infrastructures, new version of ICMP with more features (ICMPv6), Neighbor Discovery Protocol (NDP) replaces Address Resolution Protocol (ARP) as used in IPv4, etc. All of these changes may introduce new security risks.

Up till now IPv6 is hardly used and many argue that the transition from IPv4 to IPv6 will not happen soon\[2\]. Other argue that IPv6 is already widely supported in both hardware and software, and therefore should be taken serious regarding security\[3\].

![Figure 1: XKDC Nanobots (nr. 865)](image)

1.1 Research question

The main question for this research is:

- What impact has IPv6 on the security and management of IT infrastructures, and which mitigating controls are to be implemented?

This main question is divided into the following three sub questions:

- Which changes in technology are introduced with IPv6?
- What are the implications of the identified security risks of IPv6 regarding technology and IT management?
- What are the recommendations and/or mitigating controls of the identified security risks?
1.2 Research limitations

This research has the following limitations:

- Only the available Internet standards, books, research papers, articles and presentations available until 1 April 2013 have been taken into account for this research.
- Only a subset of identified security risks will be tested in a lab environment.
- Tested security risks will only cover the hardware and software as available in the lab environment.
- Research and development of mitigating controls for identified security risks will not be part of this research.

1.3 Research approach

The research has been divided into three parts, which will be answered in the following chapters:

IPv6 theory - Chapter 2
In order to answer the main research question we will first answer the first sub research question, by conducting literature research. This will include the latests Internet standards, books, research papers, articles and presentation on IPv6 given at IT security conferences.

IPv6 security risks in theory and practice - Chapters 3 and 4
Based on the results of the literature research, the security risks of IPv6 will be discussed for technology and IT management in chapter 3. A selection of technological security risks will be tested in a dedicated lab environment using existing tools in chapter 4.

Recommendations & mitigating controls - Chapters 5
For answering the main research and last sub research question, the results of both first two sub research questions will be analysed and documented.
2 IPv6 theory

In this chapter we will discuss the theory of IPv6, which will be important throughout the whole research into IPv6 security risks. We will start with a short introduction of the Internet Protocol (IP) in chapter 2.1 and an introduction to IPv6 in chapter 2.2. In chapter 2.3 the changes introduced with IPv6 will be discussed, and hence answering the first sub research question:

- Which changes in technology are introduced with IPv6?

2.1 Introduction to the Internet Protocol version 4 (IPv4)

The Internet Protocol (IP) was standardised as IPv4 in 1981 and is a fundamental part of the Internet, without IP the Internet would not operate. IP is being used by hosts (e.g. smartphone, tabled, server, etc) to communicate with other hosts. For example, when visiting a news website or when playing an online game with friends. The communication data is encapsulated within IP packets. Just like old fashion mail, IP packets contain a unique source (return address) and destination address, which are assigned to IP packets before being send across the Internet. A global network of routers, similar to a mail delivery company, use the address information to send (route) the IP packets to its correct destination.

The address field of an IP packet is 32 bits long, theoretically limiting the number of hosts that can be connected to the Internet to a total of $2^{32}$ (4 294 967 296). Currently we are running out of available IP addresses and therefore restricting new hosts that can be connected. This puts a hold on the growth of the Internet.

The Internet Protocol is part of the TCP/IP stack, which is an networking and protocol model used by hosts to communicate over the Internet. Figure 2 shows where the IP protocol is situated (layer 3) in relation to other protocols of the TCP/IP stack.

2.2 Introduction to the Internet Protocol version 6 (IPv6)

Already in the early 1990s, the IETF\(^1\) realized that a new version of IP would be needed to solve the problem on the lack of IPv4 addresses in the future. A Task Force was started drafting the new protocol’s requirements. IP Next Generation (IPng) was created, which then became IPv6 (RFC 1883). The IPv6 protocol was fully standardized at the end of 1998 in RFC\(^2\) 2460[1].

As already discussed in the previous chapter, the lack on IPv4 addresses will limit the number of hosts that can be connected to the Internet. Which has been partly resolved by the introduction of technical solution NAT\(^3\). A sustainable solution is introduced with IPv6, with support for a much larger IP address space. IPv6 uses 128 bit instead of 32 bit addresses, for an address space of $2^{128}$

\(^1\)The IETF develops and promotes Internet standards, in particular with standards of the Internet protocol suite (TCP/IP stack). It is an open standards organization, with no formal membership or membership requirements.

\(^2\)A Request for Comments (RFC) is a publication of the IETF.

\(^3\)Network Address Translation (NAT) allows the Internet to actually have far more hosts connected than its address space would normally support. With NAT multiple devices can share the the same IP address (or a pool of addresses) to access the Internet.
TCP/IP stack

<table>
<thead>
<tr>
<th>Layer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Type of communication. For example: e-mail (SMTP), web browsing (HTTP), file transfer (FTP)</td>
</tr>
<tr>
<td>Transport</td>
<td>Ensures delivery of entire file or message. (e.g. TCP, UDP)</td>
</tr>
<tr>
<td>Network</td>
<td>Routes packets to different networks, based on the IP address. (e.g. IPv4, IPv6, ICMP)</td>
</tr>
<tr>
<td>Data Link</td>
<td>Transmits packets from node to node (on the same network), based on Data Link Layer address. (e.g. Ethernet, PPP)</td>
</tr>
<tr>
<td>Physical</td>
<td>Electrical signals and cabling. (e.g. UTP, Wi-Fi)</td>
</tr>
</tbody>
</table>

Figure 2: Overview of the TCP/IP stack.

(approximately $3.4 \times 10^{38}$) addresses. S. Leibson [4] explains why this is more than enough:

So we could assign an IPv6 address to every atom on the surface of the earth, and still have enough addresses left to do another 100+ earths. It is not remotely likely that we will run out of IPv6 addresses at any time in the future.

The available IPv4 address will eventually be depleted, which will push the wider use of IPv6. Despite the fact, we are almost out of IPv4 addresses[5], most of the IPv6 use is still experimental. However, all modern devices present in today’s IT infrastructures already support IPv6 out of the box, and have it mostly enabled by default. IPv6 and its security risks (chapter 3 Security risks of IPv6) are thus already present in today’s IPv4 IT infrastructures.
2.3 IPv4 versus IPv6

In this chapter we will discuss the changes introduced with IPv6 in relation to IPv4. Changes in the IP protocol itself and the introduction of new protocols that are necessary for the operations of IPv6.

We will start of with an overview of differences and similarities between IPv4 and IPv6 in table 1. In the upcoming sections we will be explaining these differences in more detail.

<table>
<thead>
<tr>
<th></th>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address size</strong></td>
<td>32 bits long</td>
<td>128 bits long</td>
</tr>
<tr>
<td><strong>Address notation</strong></td>
<td>Dotted decimal notation: 192.0.2.20</td>
<td>Hexadecimal notation: FDF8:F200:0234:AB00:0123:4567:8901:ABCD</td>
</tr>
<tr>
<td><strong>Packet header</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Version field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP header Length</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Length</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type of Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not present</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flags</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fragment Offset</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time To Live (TTL)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Checksum</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Options</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Padding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dst. address (32 bits)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Src. address (32 bits)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broadcast</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Multicast</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Packet fragmentation</td>
<td>Routers and sending hosts</td>
<td>Sending hosts only</td>
</tr>
<tr>
<td>ICMP</td>
<td>ICMPv4</td>
<td>ICMPv6</td>
</tr>
<tr>
<td>Address configuration</td>
<td>Manual or via DHCP</td>
<td>Manual, Stateless Address Autoconfiguration (SLAAC) or DHCPv6</td>
</tr>
<tr>
<td>Address resolution</td>
<td>Broadcast ARP</td>
<td>Multicast NDP</td>
</tr>
<tr>
<td>Multicast management</td>
<td>IGMP</td>
<td>MLD</td>
</tr>
</tbody>
</table>

Table 1: Differences and similarities between IPv4 and IPv6
2.3.1 Address size

As already discussed in chapter 2.2 the address space of IPv6 has been increased significantly to a total of $2^{128}$ (approximately $3.4 \times 10^{38}$) addresses. The problem on the lack of IPv4 addresses has been partly resolved with the introduction of NAT. With IPv6 we have no technical need any more to have NAT in front of systems that require Internet activity.

2.3.2 Address notation

The 128 bits IPv6 addresses are having a different notation then 32 bit IPv4 addresses. Instead of using a decimal notation for the address, a hexadecimal notation is being used. An IPv6 address is grouped into 8 blocks of each 4 hexadecimal digits (or 16 bits). For example: \texttt{FDF8::1234:0000:0000:0000:0000:0000:0000:0000:0001} would be a valid IPv6 address. For ease of use, addresses can be shortened by omitting leading zeros. The use of `::` indicates one or more groups of 4 hexadecimal digits of zeros, which can only appear once in an address. Therefore, the previous IPv6 address example would become: \texttt{FDF8:1234::1}.

Table 2 contains another few examples of IPv6 addresses and there shorter notation:

\begin{center}
\begin{tabular}{|l|l|}
\hline
\texttt{FDF8:1234:0000:0000:0000:0000:AB12:0001} & \texttt{FDF8:1234::AB12:1} \\
\texttt{FDF8:2000:0123:0000:0000:0000:0002} & \texttt{FDF8:2000:123::2} \\
\texttt{FDF8:0012:000A:000A:000A:0000:5080:0002} & \texttt{FDF8:12:A:A::5080:2} \\
\texttt{FDF8:0006:0000:0000:0000:2000:1000:0001} & \texttt{FDF8::2000:1000:1} \\
\hline
\end{tabular}
\end{center}

\textbf{Table 2: Examples of IPv6 addresses}

2.3.3 Packet header

The packet header for IPv6 has changed a significantly if compared to IPv4 (figure 3), it is actually much simpler as it contains less header fields. The differences and similarities between the IPv4 and IPv6 header are discussed below.

\textbf{Header fields kept from IPv4 to IPv6}

The following header fields have not been changed from IPv4 to IPv6:

- **Version field** Hosts receiving an IP packet need to know if it needs to be processed as an IPv4 or IPv6 packet. The IP packet contains a version field for this, as expected it has the value 4 for IPv4 and 6 for IPv6.

- **Src. Address** The source address is now 128 bits instead of 32 bits.

- **Dst. Address** The destination address is now 128 bits instead of 32 bits.
Figure 3: IPv4 vs IPv6 header

**Header fields not kept in IPv6**

The following header fields have been removed from IPv6:

- **Options & Padding** Due to the removal of options in the standard IPv6 header, the Options and Padding header field are no longer necessary.

- **IP Header Length** Due to the removal of the option headers the IPv6 packet now has an fixed size header of 40 bytes, and the IP header length field is therefore no longer required.

- **Identification, Flags & Fragment Offset** All of these header fields have been removed, as support for packet fragmentation is no longer part of the standard IPv6 header. Support for packet fragmentation has been replaced with Extension Headers (chapter 2.3.4).

- **Checksum** With IPv4 routers must verify the IP checksum of any packet that is received, and discard packets containing invalid checksums. With IPv6 it was viewed as redundant with higher-layer error-checking (i.e. the TCP checksum) and therefore no longer necessary to be part of IPv6. In addition, it saves processing power at routers, as it is no longer required to perform any checksum validation on IP packets.

**Name and position changed in IPv6**

The following header fields have their position and name changed:

- **Payload Length** The Total Length field has been renamed to Payload Length. It describe the total length of the packet, this

---

<table>
<thead>
<tr>
<th>IPv4 Header</th>
<th>IPv6 Header</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Traffic Class</td>
</tr>
<tr>
<td>IHL</td>
<td></td>
</tr>
<tr>
<td>Type of Service</td>
<td>Flags</td>
</tr>
<tr>
<td>Total Length</td>
<td>Fragment Offset</td>
</tr>
<tr>
<td>Identification</td>
<td></td>
</tr>
<tr>
<td>Time to Live</td>
<td>Protocol</td>
</tr>
<tr>
<td>Source Address</td>
<td>Next Header</td>
</tr>
<tr>
<td>Destination Address</td>
<td></td>
</tr>
<tr>
<td>Options</td>
<td>Padding</td>
</tr>
</tbody>
</table>

Legend
- *Field names kept from IPv4 to IPv6*
- *Fields not kept in IPv6*
- *Name & position changed in IPv6*
- *New field in IPv6*
includes the IPv6 header, any Extension Headers and the payload (e.g. TCP). The Payload Length field is used by hosts to process the IP packet.

**Traffic Class** The Type of Server header field has been renamed to Traffic Class. It is being used to classify and prioritize traffic (Quality-of-Service), to support applications that require some degree of consistent throughput, delay, or jitter (e.g. VOIP calls).

**Hop Limit** The Time To Live (TTL) header field has been renamed to Hop Limit. The Hop Limit sets a limit on the number of hops (i.e. routers) an IP packet can pass before it is discarded. Without a Hop Limit, IP packets that are not reaching their destination may loop for infinity on the Internet (or internal network), resulting in network congestion.

**Next Header** The protocol header field has been renamed to Next Header. The Next Header describes what type of packet is encapsulated within the IPv6 packet. Most often this would be a TCP segment or UDP datagram.

**New header field in IPv6**
The following header field is new for IPv6:

**Flow label** The Flow Label header field is still experimental and subject to change as the requirements for flow support in the Internet become clearer.

### 2.3.4 Extension Headers

As discussed in chapter 2.3.3 *Header fields not kept in IPv6*, options are no longer part of the standard IPv6 header. With IPv6 Extension Header have been introduced to replace the options. Currently the following Extension Headers have been defined as follows in RFC 2460[1]:

**Fragment Header** The Fragment header is used by an IPv6 source to send a packet larger than would fit in the path MTU\(^4\) to its destination.

**Hop-by-Hop Options Header** The Hop-by-Hop Options header is used to carry optional information that must be examined by every node along a packet’s delivery path.

**Routing Header** The Routing header is used by an IPv6 source to list one or more intermediate nodes (i.e. routers) to be “visited” on the way to a packet’s destination. This function is very similar to IPv4’s Loose Source Routing.

Please note, that the use of the Routing Header has been depreciated. The Routing Header can be exploited in order to achieve traffic amplification over a remote path for the purposes of generating Denial-of-Service traffic [6].

\(^4\)Maximum Transmission Unit (MTU) defines the maximum size (in bytes) of data that the layer (i.e. router) can pass onwards.
**Destination Options Header** The Destination Options header is used to carry optional information that need be examined only by a packet’s destination node(s).

### 2.3.5 Broadcast

With IPv4 we have a broadcast address (255.255.255.255). Packets that have its destination set to this address are delivered to every node on the local network segment, figure 4. With IPv6 we no longer have a broadcast address.

![Figure 4: Broadcast.](image)

However, just like IPv4, some IPv6 services have the need to send a packet to all nodes on the local network. Therefore, a IPv6 multicast address exists the can be used to send a packet to all nodes on the local network segment. The IPv6 multicast address FF02::1 basically offers the same functionality as the IPv4 broadcast address.

### 2.3.6 Multicast

IPv4 does not make that much use of multicast addresses, IPv6 does. The following are a few examples of well known IPv6 multicast addresses:

- **FF02::1** - All nodes on the local network segment
- **FF02::2** - All routers on the local network segment
- **FF02::1:FF00:0/104** - Solicited-Node multicast address

Every node on the network is a member of the all nodes multicast group (FF02::1) and only routers are a member of the all routers multicast group (FF02::2). The Solicited-Node multicast addresses are used in the Neighbour Discovery Protocol (chapter 2.3.10) for obtaining the MAC address of other hosts on the local network segment.

---

5A multicast address allows a host to send IP packets to multiple hosts/destinations at once.

6Media Access Control address (MAC address) is a unique identifier assigned to network interfaces for communications on the local network segment.
2.3.7 ICMPv6

ICMPv6 plays a much bigger role for IPv6 as ICMPv4 did for IPv4. ICMPv6 is essential for the operations of IPv6 and provides all message types for the basic functionality of IPv6:

- Error Messages
- Informational Messages
- Address Resolution (chapter 2.3.10)
- Address Configuration (chapter 2.3.9)
- Multicast Management (chapter 2.3.11)

ICMPv6 defines the following type of Error Messages:

**Destination Unreachable** This kind of ICMPv6 messages is generated by the host or inbound gateway (i.e. router) to inform the recipient of the IP packet, that the destination is for some reason unreachable.

**Packet Too Big** If a packet received at a router exceeds the MTU of the outgoing link, an ICMPv6 Packet To Big messages is send. This message is send to the source of the packet.

**Time Exceeded** This type of ICMPv6 messages is generated when the following occurs:

0 If a router receives a packet with a Hop Limit of zero, or a router decrements a packet’s Hop Limit to zero, it must discard the packet and send an Time Exceeded message with code 0 to the source of the packet.

1 If reassembling a fragmented packet exceeds the time limit, a host may send a Time Exceed message with code 1.

**Parameter Problem** This type of ICMPv6 message is send by a host when receiving an IPv6 packet containing errors in the IPv6 header or Extension Headers, such that the host cannot complete processing the packet.
ICMPv6 defines the following type of Informational Messages:

**Echo Request & Replay** This type of ICMPv6 messages are being used by the famous network utility **ping** to test reachability of a host and for calculating the round-trip-time.\(^7\)

**Node Information Query & Response** This is an experimental ICMPv6 messages that can be used to request the hostname and configured IPv4 and IPv6 addresses of a node.

### 2.3.8 Packet fragmentation

With IPv4 both routers and hosts were fragmenting packets that were too big (exceeding the MTU) to send any further along the path to its destination. Fragmentation of packets take up resources (CPU cycles and memory) and therefore pose a large cost on the performance of routers. With IPv6 the decision was made to no longer support fragmentation of packets at routers but only at hosts. Routers will still inform hosts when receiving a packet that is too big, by sending back an **ICMPv6 Packet Too Big Error Message**.

By removing support for fragmentation at routers, no fragmentation options are by default present in the IPv6 packet header. Instead Extension Header were introduced to support fragmentation of packets at hosts using the Fragment Extension Header (chapter 2.3.4 **Extension Headers**).

### 2.3.9 Address configuration

The IP address of a IPv4 connected hosts can be manually configured or automatically using DHCP. With IPv6 we can still have DHCP, namely DHCPv6 which offers much of the same functionality as DHCPv4. However, by default addresses for IPv6 are automatically configured using a process called Stateless Address Auto Configuration (SLAAC).

Before explaining how SLAAC works, we will first discuss the IPv6 address format, the default IPv6 address and Duplicate Address Detection (DAD).

**IPv6 address format** IPv6 address are consisting of a 64 bits network and 64 bits host part (table 3). The network part is also often called the prefix, for example **FDF8:1111:2222:3333/64** would be a valid 64 bit length prefix. The network part is assigned to the host an cannot be chosen, the host part can. Freely by the hosts itself if SLAAC or manual configuration is being used, and assigned to the host in the case of DHCPv6.

The host part is by default based on the MAC address of the interface, and a mechanism has been developed to generate a host part that can be completely random.\(^7\)

\(^7\)The round-trip-time is the length of time it takes for a signal (e.g. IP packet) to be sent plus the length of time it takes for an acknowledgment of that signal to be received.
Default IPv6 address  With IPv6 it is normal to have multiple IPv6 addresses per network interface. For IPv4 this is quite unique. In addition to the IP address a host may get assigned through SLAAC, every host has by default at least one link-local address configured. The link-local address is only valid within the current local network segment and consists of the following network prefix: FE80::/64. For example: FE80::A288:B4FF:FE17:F8B0/64 would be a valid link-local IPv6 address.

Duplicate address Detection (DAD)  Because the host part of the IPv6 address can be selected freely, their is always a slight chance that the selected address is already in use. Therefore, hosts first need to verify if the selected IPv6 address it not already in use by another host. This verification process is called Duplicate Address Detection (DAD), and makes use of the Neighbour Discovery Protocol (chapter 2.3.10 Address Resolution). If DAD indicates that the IPv6 address is already in use, the host needs to select another IPv6 address, and again perform DAD, until a free IPv6 address is found.

Stateless Address Configuration (SLAAC)  SLAAC allows hosts to automatically configure an IPv6 address, based on the network prefix advertised by the router on the local network. Hosts could just simply wait for the router to send the periodic Router Advertisement (RA) message containing the prefix information, or forcing the router to send a Router Advertisement by sending a Router Solicitation (RS) message. The latter is the default when a system start up.

How it works can be best explained by the example from figure 6:

- 1. Host Alice sends a Router Solicitation to the all router multicast address (FF02::2) with the IPv6 unspecified address as source (::). Bob (the router) will receive this message.

- 2. Bob sends back a Router Advertisement to the all node multicast address (FF02::1) containing (among other information) the network prefix.

- 3. Alice can now configure her interface with a valid IPv6 address (FDF8:2000::A)
Alice configures the address: FDF8:2000::A

2.3.10 Address Resolution

Besides DAD, one of the most important services provided by the Neighbour Discovery Protocol (NDP) would be Neighbour Solicitation (NS) and Advertisement (NA) messages, which replaces ARP from IPv4. Just like ARP, NDP is used to resolve the link-layer address (i.e., MAC address) of a host’s IP address.

How it works can be best explained by the example from figure 7.

- Before hosts Alice and Bob can exchange any data, the need to know each other link-layer address (MAC address).
- 1. Alice will send a Neighbour Solicitation message to Bob’s Solicited-Node multicast address asking for his link-layer address.
- 2. Bob will answer this question by sending his link-layer address to Alice using a Neighbour Advertisement message.
- Alice and Bob can now exchange data.

2.3.11 Multicast Management

In IPv4 management of multicast groups (joining and leaving multicast groups, inform routers of group membership) is done through Internet Group Management Protocol (IGMP). With IPv6 this has been replaced with the Multicast Listener Discovery (MLD) protocol, which uses ICMPv6 messages.
Alice
FDF8:2000::1111:A

Bob
FDF8:2000::1111:B

1. Neighbor Solicitation
Src: FDF8:2000::1111:A
Dst: FF02::1:FF11:B
Data: link-layer address of Alice
Query: what is your link-layer address?

2. Neighbor Advertisement
Src: FDF8:2000::1111:B
Dst: FDF8:2000::1111:A
Data: link-layer address of Bob

Alice and Bob can now exchange data

Figure 7: IP to link-layer address resolution.

2.3.12 IPv6 transition/co-existence technologies

IPv6 is not backward compatible with IPv4. The original transition plan was to deploy IPv6 before we ran out of IPv4 address space, and eventually turn off IPv4 when no longer needed. Unfortunately this did not happen. Currently there are 3 different types of transition/co-existence plans:

- Dual stack
- Tunnels
- Translation

Dual stack
The host part can be chosen. With dual stack each host supports both IPv4 and IPv6 and therefore communicates with other hosts using IPv4 or IPv6 as needed. Domain names of dual stack hosts will include both an A (for IPv4) and AAAA (quad A for IPv6) DNS record. For example, www.google.com is dual stack and has therefore both an A and AAAA domain name record (table 4).

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>173.194.78.147</td>
</tr>
<tr>
<td>AAAA</td>
<td>2a00:1450:400c:c00::93</td>
</tr>
</tbody>
</table>

Table 4: Domain name record for www.google.com

Virtually all popular operating systems have IPv6 support enabled by default, and because IPv4 is still the standard, most hosts are already dual stack.

16
Most operating systems will also prefer IPv6 over IPv4 for communication. For example, hosts that have a working IPv6 connection to the Internet will prefer to communicate with www.google.com over IPv6.

**Tunnels**

Tunnels are used to transport IPv6 packets from and to IPv6 hosts over an IPv4 infrastructure. This allows hosts to communicate over IPv6 despite the underlying IT infrastructure only supports IPv4. Figure 8 shows an example of a typical IPv6 tunnel setup.

For example, when host Alice at IPv6 network A wants to communicate over IPv6 with host Bob at IPv6 network B, Alice sends its IPv6 packets to Router A. Router A (which has an IPv6 tunnel configured) receives the IPv6 packets from Alice and encapsulates the IPv6 packets within IPv4 packets. The IPv4 packets are send across the IPv4 network to the tunnel end-point, which would be Router B. On receiving the encapsulated IPv6 packets, Router B will decapsulate the IPv6 packets (i.e. removing the IPv4 header) and forward the IPv6 packet to the destination host Bob.

![IPv6 tunnel setup](image-url)

**Figure 8: Typical IPv6 tunnel setup**

**Translation**

All previous transition/co-existence technologies require both IPv4 and IPv6 addresses. If there are no IPv4 addresses left, some other mechanisms have been developed to continue the growth of the Internet. For example:

- **NAT64**
  Allows IPv6-only hosts to communicate with IPv4-only hosts.

- **DNS64**
  DNS64 provides an IPv6 DNS record (AAAA) for a hosts that only have a IPv4 DNS record (A). It is commonly used in conjunction with NAT64.

- **Carrier-Grade NAT (CGN)**
  Used by Internet Service Providers (ISPs) to dynamically share IPv4 addresses by a large number of customers (e.g. 320 customers could be sharing one single public IPv4 address [8]).

17
As IPv4 address space becomes more scarce every day, ISPs can use this technique to provide IPv4 Internet access despite it has no public IPv4 addresses left for customers.

2.4 Conclusion

IPv6 has introduced some significant changes. The IP address size has been increased to 128 bits, which also comes with a new and complex address notation format. The standard IP header has been simplified with the removal of some features. Some of these features are still available with the introduction of the IPv6 Extension Headers. New protocols have been designed to support services such as IP address configuration and IP address resolution for IPv6. Services which make extensive use of multicast that is hardly used for IPv4. And to support the transition from IPv4 to IPv6 and the co-existence of the two IP versions, several new tunnelling and translation protocols have been designed.
3 Security risks of IPv6

In this chapter we will discuss the security risks of IPv6. Starting with technical security risks in chapter 3.1 and IT management risks in chapter 3.2. Hence answering the following sub research question:

- **What are the implications of the identified security risks of IPv6 regarding technology and IT management?**

Technical security risks have to do with the technology behind IPv6, and IT management risks relate to changes introduced with IPv6 and its influence on people and processes.

3.1 Technical security risks

Table 5 shows an overview of the technical security risks of IPv6. Security risks which are caused by the technical changes introduced with IPv6 as described in the previous chapter and discussed in several research papers, articles and presentation on IPv6 given at IT security conferences. Please note that the security risks Man-in-The-Middle and Denial-of-Service are actually attacks.

<table>
<thead>
<tr>
<th>Security risk IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Man-in-The-Middle (MiTM)</td>
</tr>
<tr>
<td>Denial-of-Service (DoS)</td>
</tr>
<tr>
<td>IPv6 address privacy</td>
</tr>
<tr>
<td>Dual stack hosts</td>
</tr>
<tr>
<td>Extension Headers</td>
</tr>
<tr>
<td>IPv6 tunnels</td>
</tr>
</tbody>
</table>

Table 5: Technical security risks of IPv6

3.1.1 Man-in-The-Middle

**ATTACK** With IPv6 we have more possibilities to perform a Man-in-The-Middle attack (MiTM) compared to IPv4. Before going into these possibilities, we will first explain the basic concept of an MiTM attack (see figure 9):

- Alice and Bob are communicating with each other on the local network over the *original connection*.
- Mallory is the evil attacker and interested in the data exchanged between Alice and Bob. The communication data could contain valuable information, such as a username and password.
- Mallory performs an MiTM attack by letting Alice think he is Bob, and Bob think he is Alice.
- When the attack is successful, all communication between Alice and Bob will now first pass through Mallory’s *MiTM connection* before being send to its actual destination.
Below we list the specific IPv6 techniques that can be used to perform a MiTM attack. It is important to note that all of the MiTM attacks listed below are only effective on the local network segment:

**Neighbour Advertisement spoofing**  As discussed earlier, Neighbour Advertisements replaced ARP as used with IPv4. By spoofing Neighbour Advertisement packets we are performing an attack that is similar to ARP spoofing. The same type of technical principles are used for this attack as illustrated at figure 9.

**ICMPv6 redirect spoofing**  With ICMPv6 redirect messages we can perform a similar MiTM attack as can be done with ICMPv4 redirect messages. With this attack we spoof a redirect message to the host we want to intercept traffic from, the victim. The redirect message will tell the victim that it needs to send its IP traffic to a different router for a particular destination IP address. When the attack is successful, the attacker is able to intercept all traffic that is send to this particular destination from the victim.

**Router Advertisement spoofing**  The Router Advertisement messages used for SLAAC (chapter 2.3.9 *Address configuration*) can be spoofed to perform a type MiTM attack not present in IPv4. There are several techniques that can be used in different scenarios to perform a MiTM attack with spoofed Router Advertisement messages.

**IMPACT**  The IPv6 MiTM attacks enables a malicious user or attacker to intercept and modify traffic sent over an internal network infrastructure, with the result of loosing data confidentially and integrity for data sent by a specific host or hosts.

---

8With spoofing, we deliberately send forged data packets to perform various attacks. For example, we could send an IP packet with a source IP address that is not of our own, to mislead other hosts on the network.
3.1.2 Denial-of-Service

**ATTACK**  With a Denial-of-Service attack (figure 10) we disrupt the network connectivity of a host or whole network segment. Disruption can lead to partly or completely loosing network connectivity for the host or network segment. There is broad range of techniques that can be used with IPv6 to perform a Denial-of-Service (DoS) attack. Techniques involve spoofing and flooding various types of IPv6 packets. In this chapter we will list the types of IPv6 packets that can be used to perform DoS attacks. In chapter 4 *IPv6 security risks in practice* we will show a common technique.

**Spoofing** The following IPv6 packets can be spoofed to perform a DoS attack:
- Router Advertisement (RA)
- Duplicate Address Detection (DAD)
- IPv6 multicast packets (Smurf attack)

**Flooding** The following IPv6 packets can be flooded to perform a DoS attack:
- Router Advertisement (RA)
- Neighbour Solicitation (NS)
- Neighbour Advertisement (NA)
- IPv6 packet with router alert option set

---

**Figure 10: Denial-of-Service attack**

---

9With flooding we send dozens of packets that may cause a node (e.g. computer, router, switch) to partly or completely loose network connectivity.
The IPv6 DoS attacks enables a malicious user or attacker to disrupt the network connectivity (both via the Internet and internal network) of hosts or even a whole network, with the result of loosing availability of hosts and networks.

3.1.3 IPv6 address privacy

In chapter 2.3.9 Address configuration we explained that the host part of the IPv6 address is based on the MAC address or it can be completely random. If a device (e.g. smartphone, laptop) is configured to use an IPv6 address based on its MAC address for communication on the Internet. It will use the exact same host part (e.g. a288:b4ff:fe20:b1c5) on every network it joins. This allows the device to be tracked by its IPv6 address host part across different networks around the globe.

With IPv4 this was not possible, because the majority of people connected to the Internet are sharing one single IPv4 address with others using NAT. NAT hides their real IP address from the Internet.

IPv6 addresses based on the MAC address can be used by companies like Facebook or Google to track people around the globe without the use of cookies or other tracking technologies. Users may not be aware of this, and unwillingly allow websites or other services to track them and violate their privacy.

3.1.4 Dual stack hosts

As explained in chapter 2.3.12 Dual stack, dual stack hosts support both IPv4 and IPv6 connectivity, by default the IPv6 stack is enabled on the operating system and IPv6 is preferred over IPv4 for communication. Furthermore, every IPv6 enabled hosts has by default one IPv6 address configured (chapter 2.3.9 Address configuration).

If the security policy of a companies IT infrastructure only takes IPv4 into account (which is for today’s IT infrastructures most properly true), then the above characteristics are a risk for IT security. An attacker could for example perform the following two attacks:

- **Bypass network filtering** Network filtering rules on hosts will most properly only take IPv4 into account. For example, the host could be configured to only allow access to management interfaces (e.g. Windows Remote Desktop, SSH) from a specific set of IPv4 address, but unfiltered access from any IPv6 address. An attacker could exploit the insufficient network filtering to perform attacks on additional network services, that are not accessible from IPv4 but are accessible from IPv6 (figure 11).

- **Man-in-The-Middle attack** An attacker could send a Router Advertisements on the local network while providing native IPv6 connectivity to the Internet. Almost immediately all hosts on the network will configure a valid global IPv6 address and will use their IPv6 connectivity with a higher preference over IPv4.

When combined by the attacker with NAT64 and DNS64, nearly all network traffic send by hosts to other networks can now be intercepted.
IMPACT Having dual stack hosts may lead to bypassing internal or external network filtering policies. Policies which prevents accessing specific systems or network services. In addition, dual stack hosts may be vulnerable for a local MiTM attack with result of loosing communication data confidentially and integrity for that host.

3.1.5 Extension Headers

RISK The IPv6 specification[1] allows the creation of IP packets with an arbitrary size of successive Extension Headers contained within a single IPv6 packet, with IPv4 this is not possible. We call this Header Chains. Header Chains can further be combined with fragmented packets to create IP traffic causing various security problems[9]. Monitoring and packet filtering systems are having trouble in processing this kind of traffic[10, 11], and can become ineffective.

IMPACT An attacker could exploit Header Chains on both internal and external networks to bypass or crash for example firewall- & intrusion detections systems.

3.1.6 IPv6 tunnels

RISK Various IPv6 tunnel mechanisms have been developed to transport IPv6 traffic from and to IPv6 hosts over an IPv4 infrastructure (chapter 2.3.12 IPv6 transition/co-existence technologies). The use of tunnels creates security risks, which can be divided in one of the following two categories[12]:

![Diagram showing access to network service filtered by IPv4 firewall with IPv6 traffic unfiltered.](image-url)
Network security bypass  Network-based security devices (e.g. firewall, IDS) are often not aware of tunnelled traffic, because they are not configured for this or do not support the inspection of tunnelled traffic. As a result it is very likely that tunnelled traffic does not receive the intended level of security inspection by network-based security devices.

IP Ingress and egress filtering bypass  IP addresses inside tunnels are not subject to ingress and egress network filtering at the perimeter of a company’s IT infrastructure, unless extraordinary measures are taken. Ingress network filtering is done to mitigate attacks originating from the Internet, targeted at internal hosts. Egress network filtering is done to prevent internal host from sending insecure or malicious traffic to the Internet.

IMPACT  If internal network security controls, ingress or egress network filtering can be bypassed, controls that are supposed to provide an additional layer of defence against external attacks are lost.

3.2 IT management risks

Table 5 shows an overview of the IT management risks of IPv6. IT management risks that are caused by the changes introduced with IPv6 (chapter 2) and immaturity of IPv6 in technical solutions and products (e.g. firewall, monitoring). Based on these factors we identified the IT management risks as listed in table 5.

<table>
<thead>
<tr>
<th>Security risks IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementation maturity</td>
</tr>
<tr>
<td>Lack on IPv6 knowledge</td>
</tr>
<tr>
<td>Address notation</td>
</tr>
<tr>
<td>Public IT infrastructure security</td>
</tr>
</tbody>
</table>

Table 6: IT management risks of IPv6

3.2.1 Implementation maturity

RISK  Although IPv6 is a relative old standard (created in 1998), it still 18 years younger than IPv4 and usage is still experimental, hence many IPv6 implementations are not that mature. Implementations that not confirm with the standard, bugs in the implementations itself and lack of support for IPv6. We call this implementation maturity risk. Some examples of implementation security risk are:

Security product immaturity  Security products such as firewalls, IDSs\(^\text{10}\), security monitoring products (e.g. SIEM\(^\text{11}\)) always have supported IPv4, but lack on the support for IPv6 and therefore less effective. For example, IPv6 firewalls are less affective in filtering IPv6 traffic:

\(^\text{10}\)An Intrusion Detection System (IDS) is a device that monitors network traffic to detect malicious activities that could harm the IT infrastructure.

\(^\text{11}\)Security Information and Event Management (SIEM) solutions used to analyse large amounts of logging events to detect abnormalities that may indicate malicious actions.
There’s an insanely large amount of work to be done in the area of IPv6 firewalling F. Gont[13].

TCP/IP stack The IPv6 TCP/IP stack contains more unresolved software bugs than its IPv4 counterpart[3], which can lead to security vulnerabilities. For example, a vulnerability exists that can be used to crash devices by flooding it with Router Advertisements[14].

New security bugs in existing software Added IPv6 support in existing application introduce new functionality. New functionality (i.e. new programming code) is likely to contain software bugs, and hence security vulnerabilities. For example, the personnel firewall Kaspersky Internet Security 2013 contained an IPv6 vulnerability that could be exploited to crash the system[15].

IMPACT IPv6 implementation maturity has a negative impact on the effectiveness of security product’s capability to filter and monitor traffic. In addition, it could lead to additional security vulnerabilities from IPv6 implementations and existing software. Security vulnerabilities which can be exploited to perform attacks on systems.

3.2.2 Lack on IPv6 knowledge

RISK IT personnel is very familiar with IPv4, but good knowledge on IPv6 is lacking. P. Bedwell Fortinet vice president of product marketing says the following[16]:

There is not the institutional knowledge around IPv6 the way there is around IPv4. IPv4 has been around for decades. The extensive knowledge base is huge. It is not there yet for IPv6 yet. There is a potential for knowledge gaps or misconfigurations.

IMPACT Lack on good IPv6 knowledge could lead to security risks due to misconfigurations, insecure configuration, network design flaws and other gaffes.

3.2.3 Address notation

RISK In chapter 2.3.2 Address notation we explained how IPv6’s address notation differs from that of IPv4. The more complex notation of IPv6 can lead to mistakes made by IT personnel. Such as typing mistakes due to the longer IP address, and errors made in shortened IPv6 address notations.

IMPACT Mistakes and errors may result in faulty network filtering rules and other security risks. For example, a server containing sensitive customer data, becomes accessible to the Internet due to a typing mistake. Or documentation on the IT infrastructure may contain incorrect information on IPv6 addresses.
3.2.4 Public IT infrastructure security

**RISK**  IT security consulting companies may be requested to identify security vulnerabilities on a client’s public reachable IT infrastructure (e.g. websites, VPN endpoints, mail servers). The client provides the IT security company with their IP address ranges, which will be used as input for vulnerability testing activities. With IPv6 we can no longer use the same exact approach.

The smallest possible IPv6 IP range is 4.294.967.296 times bigger then the size of the whole Internet, too large to use as direct input for a vulnerability test. Their are some solutions to this problem (see chapter 5.2.4 Public IT infrastructure security), but those solutions still have the risk of not identifying all hosts within a IPv6 address.

**IMPACT**  Due to the large size of the IPv6 address space, there will always be the risk that a vulnerability test on an IPv6 IT infrastructure fails to identify a possible vulnerability.

3.3 Conclusion

Changes in technology as described in the previous chapter have caused some similar security risks as already present with IPv4, but mostly many new security risk in both technology and IT management.

Technical security risks that allow performing Man-in-The-Middle or Denial-of-Service attacks, with the result of loosing communication data confidentially, integrity or availability of hosts and networks. Privacy of user may be at risk, as IPv6 addresses can be used to track people around the globe without the use of cookies and other tracking technologies. And duals stack hosts, exploitation of Extension Headers and IPv6 tunnels could result in the circumvention of network-based security controls, such as bypassing firewalls and monitoring solutions (e.g. IDS).

IT management risks may cause additional exposure of the IT infrastructure to attacks, due to immature IPv6 implementations and lack on IPv6 knowledge from IT personnel. The complex IPv6 address notation may result in faulty network filtering rules and other security risks. For example, a system containing accessible customer data becomes accessible from the Internet due to a typing mistake. And security vulnerabilities on the public reachable IT infrastructure may not be identified due to the large IPv6 address space.
4 IPv6 security risks in practice

In this chapter we will show three practical examples of technical security risks described in the previous chapter. We have chosen those three, because they are common to occur in real life or are easy to perform. The security risks will be tested in the lab environment shown in figure 12 using the publicly available toolkit THC-IPV6 from M. Heuse[17]. Please note that the real IP addresses (both for IPv4 and IPv6) of the test result have been anonymised for security and privacy reasons.

![Lab environment diagram](image URL)

Figure 12: Lab environment
4.1 MiTM - Neighbour Advertisement spoofing

In this test we will be showing how we can use the THC-IPV6 toolkit to perform a Man-in-The-Middle attack on the lab environment by spoofing Neighbour Advertisement messages. As explained in chapter 2.3.10 Address Resolution, Neighbour Advertisement messages are used by hosts on an internal network segment to respond to a Neighbour Advertisement by telling which MAC address (layer 2 addressing) belongs to an IP address (layer 3 addressing).

For this test we have put a file with the name "test" on Bob’s web server with the content "secret information...". Alice will download this secret information from Bob using wget. The goal is to let Mallory intercept this secret information by capturing the traffic with tcpdump.

Let’s first show what information Mallory can see when capturing traffic without performing the MiTM attack. Alice downloads the file from Bob using wget:

```
Connecting to 2001:8d0:1102:1800:a00:27ff:febb:bbbb:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 22 [text/plain]
Saving to: test
100%[=======================================>] 22 --.-K/s in 0s
2013-08-09 10:01:36 (2,23 MB/s) - test saved [22/22]
```

Mallory’s output of tcpdump only shows the Neighbour Solicitation message from Alice, asking for Bob’s MAC address. The secret file is not there:

```
ICMP6, neighbor solicitation, who has 2001:8d0:1102:1800:a00:27ff:febb:bbbb
```

We will now do the same, but this time Mallory will perform a MiTM attack using the tool fake_advertise6, by letting Alice think he is Bob and vice versa:

```
Starting advertisement of 2001:8d0:1102:1800:a00:27ff:feaa:aaaa ...
...
Starting advertisement of 2001:8d0:1102:1800:a00:27ff:febb:bbbb ...
```

This time the output of tcpdump does show the secret file. Our MiTM attack is successful:

```
HTTP/1.1 200 OK
Date: Fri, 09 Aug 2013 10:04:23 GMT
Server: Apache/2.2.16 (Debian)
Last-Modified: Fri, 09 Aug 2013 07:59:03 GMT
ETag: "66305-16-4e37f25e59fc0"
Accept-Ranges: bytes
Content-Length: 22
```

12wget is a Linux command line utility to download files from web servers.
13tcpdump is a Linux command line utility to capture traffic on a network interface.
4.2 DoS - Router Advertisement flooding

In this test we will try to make host Alice and Bob unresponsive by letting Mal- lory flood them with Router Advertisements messages using \texttt{flood\_router26} from the THC-IPV6 toolkit. As explained in chapter 2.3.9 Address configura- tion, Router Advertisements are sent by routers to inform hosts on the internal network segment which IPv6 prefix to use for configuring an IPv6 address.

Mallory sent 3 ICMPv6 ping requests to Alice, and observes that her connec- tivity is OK:

```
ping6 -c 3 2001:8d0:1102:1800:a00:27ff:feaa:aaaa
PING 2001:8d0:1102:1800:a00:27ff:feaa:aaaa 56 data bytes
64 bytes from 2001:8d0:1102:1800:a00:27ff:feaa:aaaa: icmp_seq=1 ttl=64 time=8.42 ms
64 bytes from 2001:8d0:1102:1800:a00:27ff:feaa:aaaa: icmp_seq=2 ttl=64 time=2.55 ms
64 bytes from 2001:8d0:1102:1800:a00:27ff:feaa:aaaa: icmp_seq=3 ttl=64 time=2.86 ms
```

--- 2001:8d0:1102:1800:a00:27ff:feaa:aaaa ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2015ms
rtt min/avg/max/mdev = 2.552/4.613/8.420/2.695 ms

Now we start flooding her (and Bob) with Router Advertisement messages:

```
flood\_router26 eth0
```

Starting to flood network with router advertisements on eth0
(Press Control-C to end, a dot is printed for every 100 packet):
```
........................................................................
........................................................................
........................................................................
```

When flooding, Alice immediately becomes unresponsive (both on IPv4 and IPv6):

```
ping6 -c 3 2001:8d0:1102:1800:a00:27ff:feaa:aaaa
PING 2001:8d0:1102:1800:a00:27ff:feaa:aaaa 56 data bytes
From 2001:8d0:1102:1800:b21a:93a2:1258: icmp_seq=1 Destination unreachable: Address unreachable
From 2001:8d0:1102:1800:b21a:93a2:1258: icmp_seq=2 Destination unreachable: Address unreachable
From 2001:8d0:1102:1800:b21a:93a2:1258: icmp_seq=3 Destination unreachable: Address unreachable
```

--- 2001:8d0:1102:1800:a00:27ff:feaa:aaaa ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2015ms

When we started flooding Alice and Bob with Router Advertisements. Both hosts started configuring a new IPv6 address for every Router Advertisement received, which took up all the resources at the host and made it unresponsive.
4.3 Dual stack host

For this test we will be using a real life example from a native IPv6 Internet connection provided by an ISP. The router from the ISP is the same device for IPv4 and IPv6, but its filtering policy for IPv6 is lacking. With IPv4 the router’s Telnet management interface is not accessible, but over IPv6 it is\textsuperscript{14}. Let’s have a look at the test results, which have been performed from a company’s Linux server.

First we run the command "\texttt{route -n}" in order to find out that the router’s IPv4 address is 125.90.211.33:

\begin{verbatim}
route -n
Kernel IP routing table
Destination Gateway   Genmask      ...   125.90.211.32 0.0.0.0 255.255.255.240 ...
      0.0.0.0 125.90.211.33 0.0.0.0  ...
\end{verbatim}

Next we perform a Nmap\textsuperscript{15} scan on the router IPv4’s address and discover that the router is up, but has no available network services:

\begin{verbatim}
nmap -n 125.90.211.33
Starting Nmap 6.25 ( http://nmap.org ) at 2013-08-07 11:30 CEST
Nmap scan report for 125.90.211.33
Host is up (0.0020s latency).
All 1000 scanned ports on 125.90.211.33 are closed
MAC Address: 00:07:7D:AC:B4:41 (Cisco Systems)
Nmap done: 1 IP address (1 host up) scanned in 3.88 seconds
\end{verbatim}

Now we run the command "\texttt{ip -6 route show}" in order to find out that the router’s IPv6 address is 2001:e76:1210::1:

\begin{verbatim}
ip -6 route show
2001:e76:1210::/64 dev eth0 proto kernel metric 256 ...
fe80::/64 dev eth0 proto kernel metric 256 ...
default via 2001:e76:1210::1 dev eth0 metric 1 ...
default via fe80::fa66:f2ff:fe92:eb7b dev eth0 proto kernel metric 1024 ...
default via fe80::207:7ff:feac:b441 dev eth0 proto kernel metric 1024 ...
\end{verbatim}

When we perform the same Nmap scan on the router’s IPv6 address, we discover that the network service Telnet is available. Some tests from locations other than the company’s Linux server, were also showing the available Telnet service.

\begin{verbatim}
nmap -6 2001:e76:1210::1
Starting Nmap 6.25 ( http://nmap.org ) at 2013-08-07 11:31 CEST
Nmap scan report for 2001:e76:1210::1
Host is up (0.00074s latency).
Not shown: 999 closed ports
PORT  STATE SERVICE
14 The ISP has been informed on this security risk and resolved the issue.
15 Nmap is a network scanner to discover hosts and services on a computer network.

\end{verbatim}
23/tcp open telnet
MAC Address: 00:07:7D:AC:B4:41 (Cisco Systems)

Nmap done: 1 IP address (1 host up) scanned in 3.88 seconds

4.4 Conclusion

Public available tools and real life examples are available to put security risks described in chapter 3 Security risks of IPv6 into practise. The described security risks are not only theoretical examples but a real threat.
5 Recommendations & mitigating controls

In this chapter we will discuss the recommendations and mitigation controls for the identified security risk as discussed chapter 3. Starting with the technical security risks in chapter 5.1 and IT management risks in chapter 5.2. The last and main sub research questions will be answered in chapter 5.3 Conclusion.

5.1 Technical security risks

5.1.1 Man-in-The-Middle (MiTM) & Denial-of-Service (DoS)

Many MiTM and DoS attacks can be stopped when having Secure Neighbour Discovery\[18\] (SEND) running at hosts. SEND is a protocol designed to secure the Neighbour Discovery Protocol (NDP) using a cryptographic method. If implemented correctly\[11\], it can be used to mitigate almost all MiTM and DOS attacks that make use of NDP messages. However, a number of factors, such as the high administrative burden of managing the cryptographic infrastructure for SEND, and the unavailability of SEND implementations make SEND hard to deploy\[19\].

A more lightweight approach would be filtering malicious traffic at network devices and not at hosts. For example, RA-guard\[20\] is a mechanism, if implemented correctly\[10\], that can be used at network switches for filtering unauthorised Router Advertisement messages, mitigating many MiTM and DOS attacks based on these messages. If port security would be enabled on all network switches, many attacks will be blocked immediately since they send packets from spoofed source MAC addresses. Furthermore, other filtering and monitoring mechanism exists or could be developed to mitigate or inform network administrators on attacks.

In addition to filtering and monitoring for malicious IPv6 traffic, configuration and implementation changes could be made to further secure IPv6. For example, changing the configuration at host to disable support for ICMPv6 redirect messages to mitigate MiTM redirect attacks\[16\]. To prevent attacks based on flooding various IPv6 packets (e.g. Router Advertisements), implementation could be improved to set limits. Limits on the maximum of configured IPv6 addresses, limits on the size of the IPv6 neighbour cache, rate limits for the Hop-by-Hop Extension Header, limits on the number of requests per second for responding to Neighbour Solicitation messages, etc.

5.1.2 IPv6 address privacy

To mitigate the risk of having IPv6 addresses based on the MAC address that can be tracked, privacy extension has been developed to generate random IPv6 addresses\[7\]. However, privacy addresses have the habit to change a lot, which is a big drawback for using them within a company’s IT infrastructure. For example, network monitoring is much more effective when having IP addresses which are a stable as possible. Managing network filtering rules based on IP addresses becomes impossible when hosts are changing their IP address every so often.

\[16\] ICMPv6 redirects are not really necessary for the operations of an IT infrastructure. With IPv4 it is already good security practice to disable support for ICMP redirects.
F. Gont has proposed the use of stable privacy addresses in an Internet-Draft document[21]. These privacy addresses are stable within each subnet and change only when hosts move from one network to another. They are recommended to be used within a company’s IT infrastructure. It is not recommended using the stable privacy addresses at home, they still provide some possibility for tracking.

5.1.3 Dual stack hosts
Systems (e.g. hosts, network devices, printers, etc) that have no requirement to communicate over IPv6 should have support for IPv6 disabled. This way systems are protected from attack based on IPv6. We recommend security baselines have this included as a requirement.

If IPv6 communication is required, the network security policy for IPv6 should have the same rules and enforcement strength as for the IPv4 network.

5.1.4 Extension Headers
F. Gont has proposed a fix[9] to the current IPv6 standard[1] to solve some of the security problems with Extension Headers. His proposed fix makes network-based security devices no longer ineffective in inspecting malicious traffic contained within Header Chains.

In addition to this fix, we recommend to putting a limit on successive Extension Headers, and thus restricting the maximum size of Header Chains. It is good for performance and prevents malicious traffic from taking up all resources at network-based security devices, which may cause traffic not to be inspected.

5.1.5 IPv6 tunnels
The network security policy should include additional controls to protect the IT infrastructure from attacks through tunnels. Controls to prevent to use of tunnels and controls for legitimate use of tunnels.

If the use of tunnels is not required, network-based security devices should filter the use of tunnelling protocols at all network perimeters. In addition, it is good security practice to have security baselines include requirements to have support for tunnelling protocols disabled at hosts. For example, Windows (Vista and newer) has by default support for the automatic IPv6 tunnelling protocol Teredo enabled.

If the use of tunnels is required, network-based security devices should only allow the use of authorised tunnelling protocols, and filter all other. Support for filtering and monitoring tunneled IPv6 traffic should be possible. Therefore, it is important to make sure that the network-based security devices support the authorised tunnelling protocols.
5.2 IT management risks

5.2.1 Implementation maturity

An organisation is almost never in power to fix implementation security bugs or increasing the maturity level of implementations. This makes the mitigation of IPv6 implementation maturity risks very hard. It is important for IT management to be aware of this problem when IPv6 is being used, and take appropriate mitigating controls within their IT department.

Some implementation security risk can be mitigated with having a good software update policy and process. Although is should be noted that a good update process can only fix known issues with implementation maturity. The update policy should not only be focusing on security patches, but certainly also on features updates. Feature updates could increase the maturity level of implementations when providing new functionality. For example, functionality that increases the possibility for monitoring IPv6 traffic for suspicious traffic.

It is recommended that implementation maturity has an important role when in the process of purchasing a new network-based security device that has to have support for IPv6. Certainty on implementation maturity should be acquired as much as possible before making the final selection. Acquiring Certainty is not easy. IT management should try asking manufactures and vendors to provide security assessment reports on their products. Or hire an IT security specialist to perform a thorough security assessment on a selection of devices.

5.2.2 Lack on IPv6 knowledge

IT management should make training on IPv6 possible for IT personnel to lower the risk of misconfigurations, insecure configuration, network design flaws and other gaffes. Because IPv6 is also a risk for current IPv4 IT infrastructures, IT management should encourage IT personnel to attend this training. Training in which IPv6 security plays a important role is recommended.

5.2.3 Address notation

Risks of the more complex address notation, can be partly resolved by good IPv6 training. Mistakes in the shortened IPv6 address notation are properly less likely to happen when IT personnel is well trained on IPv6. In addition to training, IT management could create a policy stating that direct use of IP addresses by IT personnel should be avoided whenever possible. Instead IT personnel should make extensive use of Domain Names\(^\text{17}\) in configurations and documentation. Domain Names have the advantage of being centrally managed and the IP-address of a system has only be typed in once, lowering the risk on typing errors and mistakes.

5.2.4 Public IT infrastructure security

The risk of a vulnerability test that fails to identify possible vulnerabilities at a public reachable IT infrastructure, can be partly mitigated by IT management and the IT security consulting company performing the vulnerability test.

\(^{17}\)A Domain Name is an identification string that identifies one or more IP addresses (e.g. www.google.com).
IT management should make sure that there is a strict policy and process in place to ensure that the IT department has good knowledge on every host that is reachable from the Internet. This information should actually already be available for IPv4, but with IPv6 it becomes much more important. Information should be documented in for example a CMDB\textsuperscript{18}, and among with the company’s IPv6 ranges provided to the security consulting company performing the vulnerability test. The more accurate the information is, the higher the quality of the vulnerability test.

IT security companies should take a new approach for performing vulnerability test on public reachable IPv6 IT infrastructure. In addition to the information proved by the client, some new techniques should be adopted for discovering publicly reachable hosts. Employees should be provided training for this. Training which could be based on own research, techniques discussed by M. Heuse’s presentation at Hack in The Box\textsuperscript{3} and techniques discussed in an Internet-Draft published by F. Gont and T. Chown\textsuperscript{22}.

5.3 Conclusion

Before we will answer the main research question we will first answer the last sub research question:

- What are the recommendations and/or mitigating controls of the identified security risks?

The following technical recommendations and mitigating controls apply to resolving the technical security risks. It is very important to note that all of the below categories are requiring the appropriate policies, processes and guidelines to be successful:

More strict filtering and monitoring
Implementation of new (or developed) and more strict network-based security filtering and monitoring to mitigate MiTM and DoS attacks. In addition it resolves risks related to IPv6 tunnels.

Improving standards
Adoption of proposed and approved improvements to current Internet standards to mitigate the risks IPv6 address privacy and Extension Headers.

Disable IPv6 and/or features
Disabling IPv6 support at systems and IPv6 features (e.g. Teredo), if not necessary for the operations of the system. This could mitigate risks related dual stack hosts and IPv6 tunnels. In addition it resolves some of the MiTM and DoS attacks.

Setting limits
IPv6 implementations can be improved by setting limits to counter some MiTM and DOS attacks, and risks related to Extension Headers. Limits on the maximum of configured IPv6 addresses, limits on the size of the

\textsuperscript{18}A Configuration Management Database (CMDB) is a repository of information related to all the components of an IT infrastructure.
IPv6 neighbour cache, rate limits for the Hop-by-Hop Extension Header, limits on the number of requests per second for responding to Neighbour Solicitation messages, etc.

The following recommendations apply to resolving the IT management risks:

**Training**

It is recommended for IT management to provide training on IPv6 and its security aspects. IT management should encourage IT personal to attend this training to resolve risks related to lack on IPv6 knowledge, address notation and public IT infrastructure security.

**Processes**

It is recommended for IT management to make improvements to current policies, processes and guidelines to resolve risks related to implementation maturity, address notation and public IT infrastructure security:

- IPv6 implementation maturity should be an important criteria when in the process of purchasing a new network-based security device that has to have support for IPv6.
- Creating a policy stating that direct use of IP addresses should be avoided whenever possible by making extensive use of DNS.
- Having a strict policy and process in place to ensure that the IT department has good knowledge on every IPv6 hosts that is reachable from the Internet.

A large portion of the main research question, namely mitigating controls (and recommendations), are already answered in the last sub research question. Only the impact of IPv6 on security and management of IT infrastructures remains to be answered:

- What impact has IPv6 on the security and management of IT infrastructures, and which mitigating controls are to be implemented?

The impact of IPv6 on IT infrastructures has effect on all ITIL\[23\] principles people, processes and technology (figure 13). Technical security risks that allows performing Man-in-The-Middle or Denial-of-Service attacks, with the result of losing communication data confidentially, integrity or availability of hosts and networks. Privacy of user may be at risk, as IPv6 addresses can be used by companies like Facebook and Google to track people around the globe, without the use of cookies or other tracking technologies. And duals stack hosts, exploitation of Extension Headers and IPv6 tunnels could result in the circumvention of network-based security controls, such as bypassing firewalls and monitoring solutions (e.g. IDS).

IT management risks may cause additional exposure of the IT infrastructure to attacks, due to immature IPv6 implementations and lack on IPv6 knowledge from IT personnel. The complex IPv6 address notation may result in faulty network filtering rules and other security risks. For example, a system containing accessible customer data becomes accessible from the Internet due to a typing mistake. And security vulnerabilities on the public reachable IT infrastructure may not be identified due to the large IPv6 address space.
Figure 13: Shows for every identified security risk where the main focus on resolving the issue should be.
References


