ABSTRACT
IPv6 is the successor of IPv4 and will replace it in the long run as the main protocol of the network layer. IPv6 is aimed at providing end-to-end communication between network interfaces even when the number of Internet participants and corresponding demand for address space keep on growing massively, for example caused by the growing demand for Internet-enabled mobile devices. There are a number of differences between IPv6 and IPv4 protocols, but security is not related to these inherent characteristics alone. The conversion process might also generate new questions for security experts. Is IPv6 more secure than its ancestor protocol IPv4? Although the answer may depend on the perspective, it would be fair to say it doesn’t make a lot of dissimilarity for now. Besides, IPv6 had also brought some security risks as well according to the current status of IPv6 transition.

Keywords
IPsec; Security; Threats; Protocols

1. INTRODUCTION
The internet, in very broad terms, is a connected network of networks which consist of billions of devices, including personal computers, mobile phones, switches, routers and many other end user or intermediary nodes. The growing number of internet-enabled appliances has reached a scale at which the current network infrastructure and its original protocols, such as IPv4, were never expected to work when they were designed.

The prevailing Internet Protocol standard is IPv4 (Internet Protocol version 4), which dates back to the 1970s. There are well-known limitations of IPv4, including the limited IP address space and lack of security. IPv4 specifies a 32-bit IP address field, and available address spaces are rapidly running out.

IPv6 is the successor of IPv4 and will replace it in the long run as the main protocol of the network layer. IPv6 is aimed at providing end-to-end communication between network interfaces even when the number of Internet participants and corresponding demand for address space keep on increasing massively, for example caused by the growing demand for Internet-enabled mobile devices IPv6 is not downward compatible, therefore a simple switch of protocols is not possible. This is also due to various old network devices that are optimized for the use with IPv4 and hence do not support new version. The development of the next generation Internet protocol began in 1993 when people realized that the address space would not suffice forever.

2. Comparison of IPv6 and IPv4
IPv4 uses a 32-bit address space which can be used to assign 4,294,967,296 unique addresses. There are technical solutions such as Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT) which enable users to share public IP addresses in order to connect to the internet from an inner domain and thus get out of the problem. On the other hand, IPv4 routing is getting more complex every day. IPv6 uses a 128-bit address space which can contain up to 34x10^37 IP addresses. Thus, it is realistic to say that the IPv6 address space is more than enough for now and for the foreseeable future.

In order to describe the difference between protocol header layouts, an overview of IPv4 and IPv6 packet headers can be seen below (Figure 1). Related Request for Comments (RFC) can be found in the internet Engineering Task Force’s web site.
In addition to packet headers, there is also a difference in IPv6 where the smallest permissible value for the Maximum Transmission Unit (MTU) is larger, so all network links transporting IPv6 must be able to deliver packets of at least 1280 bytes. In IPv4, the smallest permissible MTU is 576 bytes.

Looking at the header fields in the figure above, IPv6 addresses are significantly bigger than IPv4 addresses. The reason behind the vast capacity of IPv6 addressing possibilities is related to 128 bit addressing mechanism.

A sample IPv6 is shown below (Figure 2).

```
2001:0db8:0f61:a2b4:0000:baba:dede:0020
```

Figure 1. IPv4 and IPv6 Header Fields

Figure 2. IPv6 Address Example
The following table lists the important differences between IPv4 and IPv6.[12]

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 addresses are 32 bit length.</td>
<td>IPv6 addresses are 128 bit length.</td>
</tr>
<tr>
<td>IPv4 addresses are binary numbers represented in decimals.</td>
<td>IPv6 addresses are binary numbers represented in hexadecimals.</td>
</tr>
<tr>
<td>IPSec support is only optional.</td>
<td>Inbuilt IPSec support.</td>
</tr>
<tr>
<td>Fragmentation is done by sender and forwarding routers.</td>
<td>Fragmentation is done only by sender.</td>
</tr>
<tr>
<td>No packet flow identification.</td>
<td>Packet flow identification is available within the IPv6 header using the Flow Label field.</td>
</tr>
<tr>
<td>Checksum field is available in IPv4 header</td>
<td>No checksum field in IPv6 header.</td>
</tr>
<tr>
<td>Options fields are available in IPv4 header</td>
<td>No option fields, but IPv6 Extension headers are available.</td>
</tr>
<tr>
<td>Address Resolution Protocol (ARP) is available to map IPv4 addresses to MAC addresses.</td>
<td>Address Resolution Protocol (ARP) is replaced with a function of Neighbor Discovery Protocol (NDP).</td>
</tr>
<tr>
<td>Internet Group Management Protocol (IGMP) is used to manage multicast group membership.</td>
<td>IGMP is replaced with Multicast Listener Discovery (MLD) messages.</td>
</tr>
<tr>
<td>Broadcast messages are available.</td>
<td>Broadcast messages are not available. Instead a link-local scope “All nodes” multicast IPv6 address (FF02::1) is used for broadcast similar functionality.</td>
</tr>
<tr>
<td>Manual configuration (Static) of IPv4 addresses or DHCP (Dynamic configuration) is required to configure IPv4 addresses.</td>
<td>Auto-configuration of addresses is available.</td>
</tr>
</tbody>
</table>

3. Security Improvements over IPv4

3.1. Massive Size of the IP Address Space

Attackers usually employ port scanning as a reconnaissance technique to gather as much information as possible about a victim's network. It is expected that the entire IPv4 based Internet can be scanned in about 10 hours with enough bandwidth, given that IPv4 addresses are only 32 bits wide. IPv6 dramatically increases this limit by expanding the number of bits in address fields to 128 bits. By itself, such a massive address space creates a significant barrier for attackers wanting to conduct comprehensive port scanning.

However, it should be noted that the port scanning reconnaissance technique used in IPv6 is basically the same as in IPv4, apart from the larger IP address space. Therefore, current best practices used with IPv4, such as filtering internal-use IPv6 addresses in border routers, and filtering un-used services at the firewall, should be continued in IPv6 networks.

Cryptographically Generated Address (CGA)

In IPv6, it is possible to attach a public signature key to an IPv6 address. The resulting IPv6 address is called a Cryptographically Generated Address (CGA). This provides additional security protection for the IPv6 neighborhood router discovery mechanism, and allows the user to provide a “proof of ownership” for a particular IPv6 address. This is a key differentiator from IPv4, as it is uneconomical to retrofit this functionality to IPv4 with the current 32-bit address space constraint. CGA offers three main advantages:

1. It makes spoofing attacks against, and stealing of, IPv6 addresses much harder.
2. It allows for messages signed with the owner's private key.
3. It does not require any upgrade or modification to overall network infrastructure.

3.1.2. IP Security (IPsec)

IP Security provides interoperable, high quality and cryptographically based security services for traffic at the IP layer. It is optional in IPv4 but has been made compulsory in the IPv6 protocol. IPsec enhances the original IP protocol by providing authenticity, integrity, confidentiality and access control to each IP packet through the use of two protocols: AH (authentication header) and ESP (Encapsulating Security Payload).

**Authentication Header (AH)** The heart of the Authentication Header is the integrity check value (ICV) field. The ICV is computed by the source and computed again by the destination for verification. This procedure provides both...
connectionless integrity and data origin authentication. Connectionless integrity detects modifications to the payload. Data origin authentication verifies the identity of the source of the data. The AH also contains a sequence number field that can be used to detect packet replay attacks, which tie up receiving system resources. By examining the sequence numbers, we can spot the arrival of duplicate IP packets.

- **Encrypted Security Payload (ESP) Header** IPv6 can provide confidentiality by encrypting the payload. The IPv6 ESP header contains a security parameter index (SPI) field that refers to a security association telling the destination how the payload is encrypted. ESP headers may be used end-to-end or for tunneling. When tunneling, the original IPv6 header and payload are both encrypted and jacketed by outer IPv6 and ESP headers. Near the destination, a security gateway strips away the outer headers and decrypts the original header and payload. This encapsulation provides limited traffic flow confidentiality because a traffic analyzer may see.

### 3.1.3. Replacing ARP by Neighbor Discovery (ND) Protocol

In the IPv4 protocol, a layer two (L2) address is not statically bound to a layer three (L3) IP address. Therefore, it can run on top of any L2 media without making significant change to the protocol. Connection between L2 and L3 addresses is established with a protocol named Address Resolution Protocol (ARP), which dynamically establishes mapping between L2 and L3 addresses on the local network segment. ARP has its own security vulnerabilities (such as ARP Spoofing). In the IPv6 protocol, there is no need for ARP because the interface identifier (ID) portion of an L3 IPv6 address is directly derived from a device-specific L2 address (MAC Address). The L3 IPv6 address, together with its locally derived interface ID portion, is then used at the global level across the whole IPv6 network. As a result, the security issues related to ARP no longer apply to IPv6. A new protocol called Neighbor Discovery (ND) Protocol for IPv6 is defined in RFC 4861[3] as a replacement to ARP.

### 4. Security Threats

The address space of IPv6, local link communications between routers and end-nodes are different in IPv6. Unlike IPv4, ICMPv6 has features which are required for IPv6 local link communication. There is a new Router Discovery (RD) mechanism which uses ICMPv6 messages to discover routers in IPv6. Routers respond to end nodes’ Router Solicitation (RS) messages with Router Advertisement (RA) replies, and these messages are saved in the end nodes’ routing tables for some time. Details of this operation are specified in RFC 4861.[4] This Router Discovery operation could be used to deploy Man in the Middle (MITM) attacks in the Layer 2 communication. If an attacker can position himself in an IPv6 local network, he could send fake RA messages to a victim and act as a router for that victim. After this stage, he could see all the network traffic originating from or passing to that victim.

In order to tackle such rogue RA messages in an IPv6 network, there are couples of solutions which can be applied. One of them uses customized IDS signatures which check the MAC and IP address of the sender. Another solution is using NDP Mon, which is a public domain utility. This checks all RA messages and compares them with a XML configuration file.[5] Another solution to mitigate local network attacks in IPv6 is using a handy tool called ‘rafixd’. The idea behind this tool is to detect all rogue RA messages and clear this rogue information from network.[6]

Another Layer 2 security concern for IPv6 networks is based on Neighbor Discovery, which is similar to Router Discovery, but between hosts.[7] Instead of Router Advertisement and Router Solicitation as it was between routers, there are Neighbor Advertisement (NA) and Neighbor Solicitation (NS) operations between IPv6 hosts. One type of attack can occur during the address resolution process between hosts. Instead of Address Resolution Protocol (ARP) as it is in IPv4, ICMPv6 is used for address resolution in IPv6. One last example of link local security threats which we will mention here is about performing DDoS attacks using Duplicate Address Detection (DAD) technique. DAD is a mechanism which prevents hosts using duplicate addresses. In essence, this type of DDoS attack could block a host from getting an IP address in IPv6 networks by abusing DAD.

If an attacker sends Router Advertisement probes to that host, this would trigger the host to start using IPv6 silently. This attack constitutes a basic but effective technique to exploit dual stack enabled hosts. Another type of threat arises from IPv6 tunnels, because tunneling mechanisms have no built-in security at all; no authentication, no integrity check, and no confidentiality.[9] This situation could easily create opportunities for attackers to conduct tunnel sniffing (MITM), tunnel injection or unauthorized use of a tunnel service attacks. If proper prevention mechanisms are not in place, such as checking the IPv4 source address, using ant spoofing techniques, using Access Control Lists (ACLs) and IPsec, these threats could even bypass corporate firewalls.

### 5. Conclusion

In order to alleviate these neighbor discovery attacks, the IETF published Secure Neighbor Discovery (SEND) and Cryptographically Generated Addresses (CGA)[11] protection mechanisms. For the CGA and another mitigation method called Address Based Keys (ABK), Microsoft has published a research article which might be useful to deploy in IPv6 networks.[8]

Host security controls should deal with both IPv4 and IPv6 attacks in order to tackle with these transition period specific issues, but this approach is based solely on a technical point of view. The real cause of transition period problems is related to awareness of IPv6 security issues and effective management.

Possible attacks that IPv6 cannot address:
1. Application layer attacks: Attacks performed at the application layer (OSI Layer 7) such as buffer overflow, viruses and malicious codes, web application attacks, and so on.

2. Brute-force attacks and password guessing attacks on authentication modules.

3. Rogue devices: Devices introduced into the network that are not authorized. A device may be a single PC, but it could be a switch, router, DNS server, DHCP server or even a wireless access point.

4. Denial of Service: The problem of denial of service attacks is still present with IPv6.

5. Attacks using social networking techniques such as email spamming, phishing, etc.

In this paper, we looked into the by no means complete list of discussion topics related to IPv6 and its main differences from IPv4, especially in terms of security. After elaborating current prevalence status of IPv6 in today’s networks, we have briefly discussed some technical, transitional, and management related issues. IPv6 is the next network protocol and brings some new features. Some of them are quite exciting, such as the availability of a vast number of IP addresses. It also has lots of similarities with IPv4: both operate in the connectionless network layer, both run below TCP and UDP, and both are prone to configuration mistakes which might result in serious security incidents. After all, according to latest research, most vulnerabilities are at the application layer.[10] As a result, the network layer and IPv6 have little or no impact on tackling today’s attacking vectors. Lots of security considerations would stay the same as they are in IPv4.

REFERENCES


