CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

IPv6 Transition and Security Threat Report

Emin Çalışkan

Tallinn 2014

www.ccdcoe.org
publications@ccdcoe.org

Internet Protocol version 6 (IPv6) is the next version of Internet Protocol which is currently in the transition phase from its predecessor, Internet Protocol version 4 (IPv4). Putting aside the debates about the necessity of the IPv4 to IPv6 shift which arose from exhaustion of IPv4 public addresses, the focal point of this article is about the peculiarities of IPv6 from a security perspective and its differences in that regard compared to IPv4. The current state of IPv6 usage, IPv4 to IPv6 transition issues and the managerial perspective of this new protocol will be discussed, along with the common misunderstandings and misperceptions about why IPv6, although an important development from the security perspective, is not a 'game changer'.

Introduction

The internet, in very broad terms, is a connected network of networks which comprises 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 underlying protocols, such as IPv4, were never expected to work when they were designed. Today even some household devices are able to connect to the internet and have something in common with all other high-tech devices such as PCs and smart phones; they require an Internet Protocol (IP) address to operate and get connected to the internet.

1. Necessity

One of the main reasons behind creation of IPv6 is related to IPv4's scarce IP space. IPv4 uses a 32-bit address space which can be used to assign 4,294,967,296 unique addresses. Today, 2.7 billion people are connected to the internet and there are more than 10 billion internet-enabled devices in the world. This clearly shows why IPv4 addresses have run out. 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 circumvent the problem. Nevertheless, IPv4 routing is getting more complex every day. IPv6 uses a 128-bit address space which can accommodate up to $34\text{x}10^{37}$ IP addresses. Thus, it is reasonable to say that the IPv6 address space is more than enough for now and for the foreseeable future. This is one of main drivers behind the IPv6 shift and it can be summarized as 'scalability related improvements'.

2. Technical Background

IPv6 not only brings vast number of IP addresses which would enable numerous devices to have their own unique identifiers, it also has different peculiarities in terms of packet layout and underlying transmission techniques. In order to depict 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.[1,2]

[1] Postel, J., Internet Protocol, STD 5, *RFC 791*, September 1981.
[2] Deering, S. and R. Hinden, Internet Protocol, Version 6 (IPv6) Specification, *RFC 2460*, December 1998.

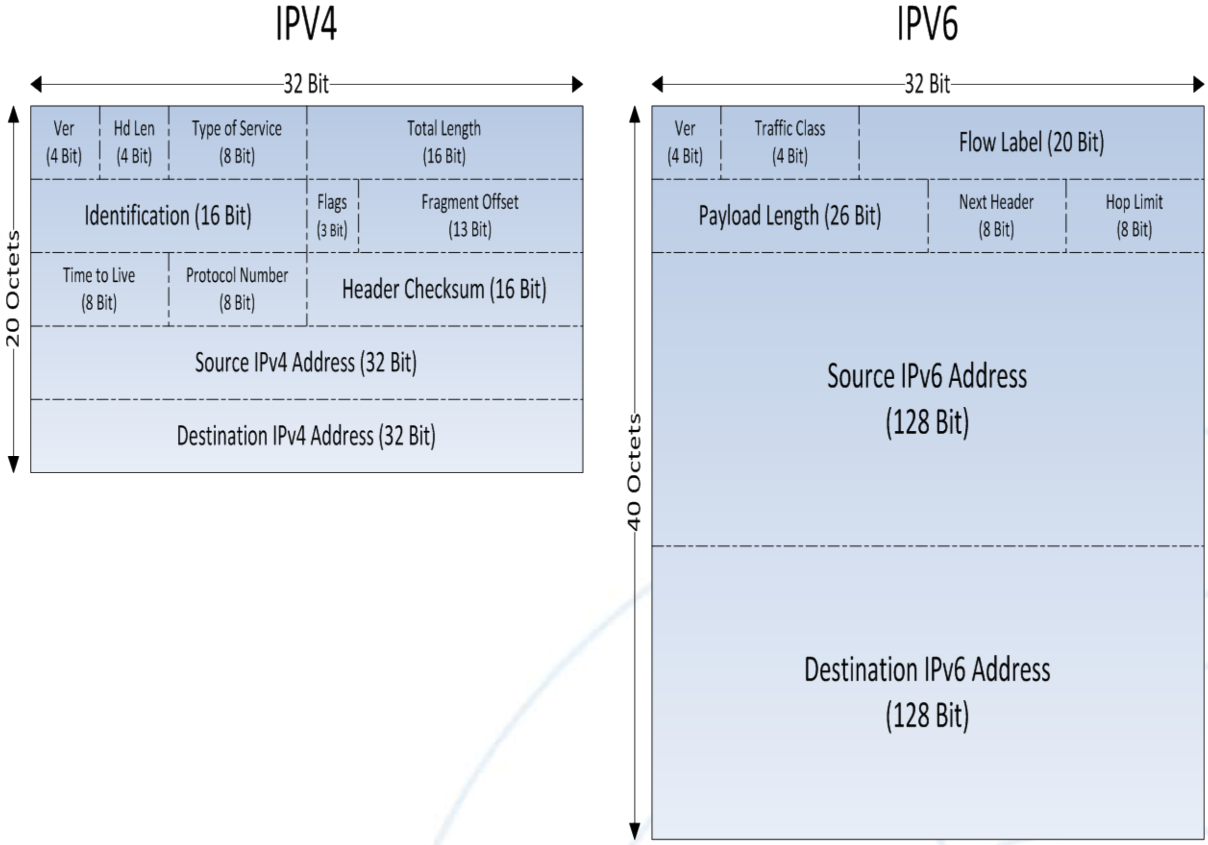


Figure 1. IPv4 and IPv6 Header Fields

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).

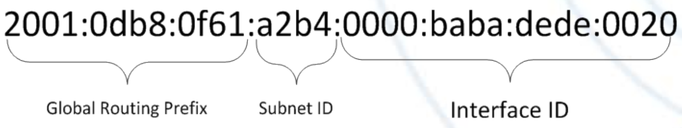


Figure 2. IPv6 Address Example

IPv6 addresses are written in hexadecimal digits and divided into eight pairs of two byte blocks. The global routing prefix is a value which is assigned to a site and can be a cluster of subnets or links; the subnet ID is an identifier of a link within the site; and the Interface ID is being used to identify interfaces on a link.[3] In terms of the text representation of IPv6 addresses, there is a new compression methodology available. Since IPv6 addresses may contain all '0' bits in one or more of those eight blocks, a colon or just one zero digit can be used

[3] Hinden, R. and S. Deering, IP Version 6 Addressing Architecture, *RFC 4291*, February 2006.

instead of four zero bits for convenience. Note that if a colon is used without any zero digits, this compression can only be used once in an address. See Figure 3.

2001:0DB8:0000:0000:0008:0800:200C:417A

2001:DB8:0000:0000:8:800:200C:417A

2001:DB8:0:0:8:800:200C:417A

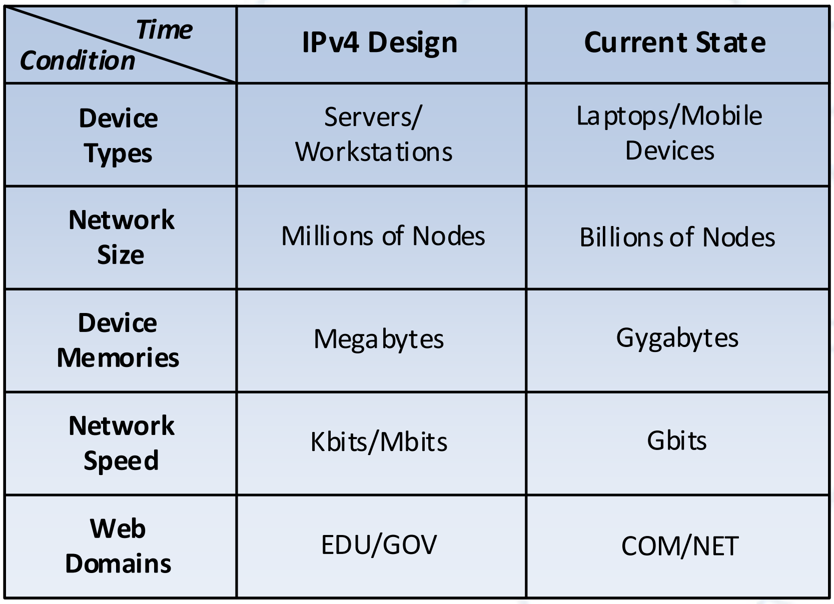
2001:DB8::8:800:200C:417A

Figure 3. Different IPv6 Representations of the Same IP Address

These addresses are pointing to the same IPv6 addresses, but using notations. From the security perspective, these notations may bring some difficulties for IDS and IPS, firewall or similar mechanisms since these IPv6 addresses require different parsing implementations.

3. Comparison of IPv4 and IPv6

There is a considerable number of technical differences between IPv4 and IPv6 protocols, but there is another reality to consider which drives all those updates and improvements: the current capabilities of information technology (IT) devices and the rapid growth of internet speed. The following comparison could be useful to depict the main differences between today's reality and the conditions when IPv4 protocol was designed (Figure 4).



Time *Condition*	**IPv4 Design**	**Current State**
Device Types	Servers/ Workstations	La ptops/Mobile Devices
Network Size	Millions of Nodes	Billions of Nodes
Device Memories	Mega bytes	Gygabytes
Network Speed	Kbits/Mbits	Gbits
Web Domains	EDU/GOV	COM/NET

Figure 4. IPv4 Design and Current State

Starting from the first row, device types are quite different nowadays. Portable mobile devices which can connect to the internet are prevalent compared to the legacy servers and workstations of a few years ago. This has expanded network size significantly; currently there are billions of nodes which are connected to the internet. Also, the size of IT devices is getting smaller, but paradoxically their capacities in terms of memory and storage grow almost exponentially. Network speed is much faster and capabilities to transmit gigabytes of data in a short time have now expanded users' internet landscape significantly.

Some of these conditions are the results of technological advancements and arose by themselves; others were invented on purpose. No matter how these conditions occurred, the change is evident.

Current State and Transition to IPv6

Before elaborating on security issues related to IPv6 and comparing its characteristics with IPv4, we will take a closer look at the current state of IPv6 readiness in the world. Usage statistics and connectivity methods, along with the internal features of IPv6, will be discussed in this section.

1. Methods of IPv6 Connectivity

Native IPv6 can be used and there are workaround solutions to use IPv6, such as ISATAP, Teredo and 6to4. These are tunneling solutions which enable IPv4 hosts to connect IPv6 networks where there is not a native IPv6 support.

Native IPv6

Native IPv6 refers to a state where all devices, end points, routing infrastructure and network services such as DHCP and DNS completely support and use IPv6 in a network. It is pure IPv6 implementation and it is predicted that not all networks will quit using IPv4 and use native IPv6 because of the connectivity concerns about networks which do not support IPv6.

6to4

In 6to4 tunnels, a router with a 6to4 tunnel is used to generate a link from an inside IPv6 network to the rest of the IPv6 world over the IPv4 Internet. These *6to4 routers* take the IPv4 address and compute the IPv6 network prefix by combining the 6to4 2002::/16 prefix with the 32-bit IPv4 address of the internet-facing interface to form a /48 prefix for the IPv6 network.[4] This technique basically generates IPv6 addresses using IPv4 addresses, and connects IPv6 networks over 6to4 routers which enable this operation.

ISATAP

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) is a tunneling technique for dual stack hosts for which the details are specified in RFC 4124.[5] ISATAP exhibits a remote-access use case for IPv4 hosts, where IPv6 packets are encapsulated in IPv4 packets and transmitted over IPv4 networks.

Teredo

Teredo is another transition technology which enables IPv6 capable hosts which do not have native IPv6 connectivity. The prominent feature of Teredo tunnels compared to other techniques is their ability to perform tunneling even behind NAT environments. Teredo is described in RFC 4380.[6] Microsoft, which is behind the invention of this tunneling system, is planning to shut down this solution since native IPv6 support is becoming more and more widespread every day.[7]

2. IPv4 and IPv6 Usage Statistics

There are different sources which monitor the latest IPv6 usage statistics across the world. According to Google, 2.2% of its users access Google's services via IPv6.[8] From the providers' perspective, 3.4% of all the web sites support IPv6 connectivity.

Figure 5 is taken from Google's IPv6 statistics page. It clearly shows the fast growth of IPv6-enabled users beginning in 2011, yet the total number of IPv6 connections is still around 2% overall. This situation may also be related to debates around the necessity of IPv6 and the time until the transformation is expected to finish.

[4] S. Hogg, E. Vyncke, Securing the Transition Mechanism, *IPv6 Security*, Indianapolis, IN: Cisco Press, 2009, pp. 423-428.
[5] Templin, F., Gleeson, T., and D. Thaler, Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), *RFC 5214*, March 2008.
[6] Huitema, C., Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs), *RFC 4380*, February 2006.
[7] Microsoft's Teredo connectivity web page (http://teredo.ipv6.microsoft.com) has not been responding for a while. This may be part of a forecasting effort to measure the impact of the service being turned off.
[8] Google's IPv6 statistics can be found at http://www.google.com/ipv6/statistics.html.

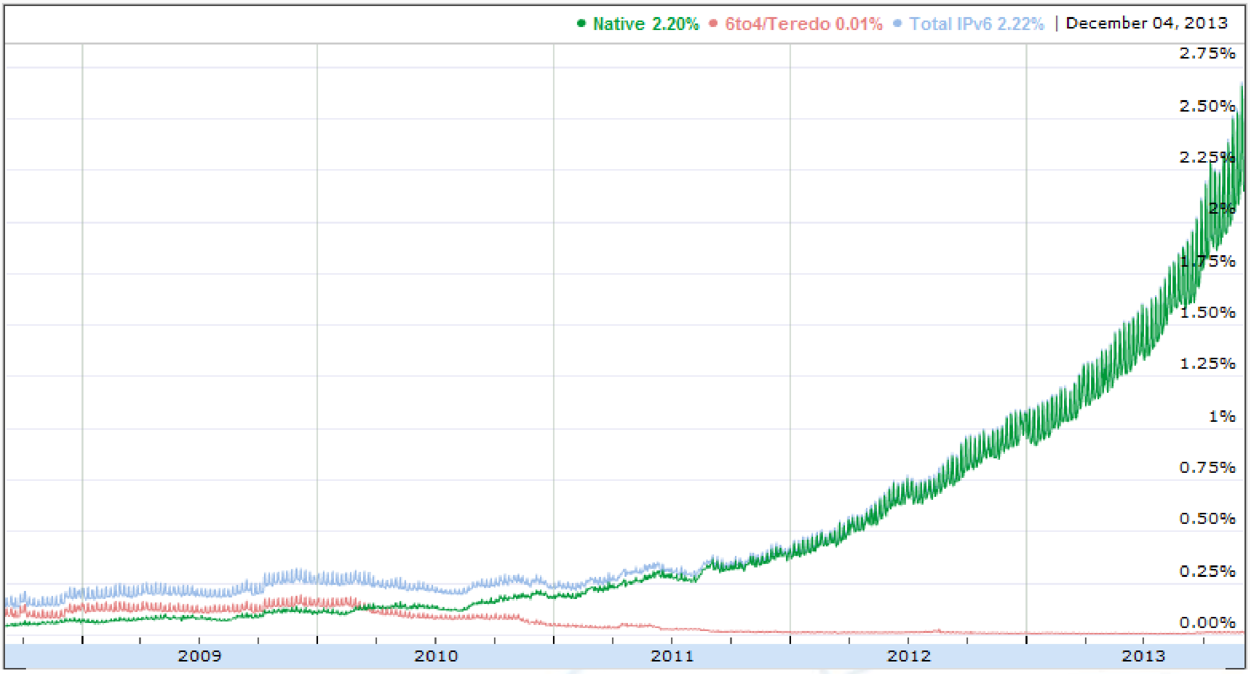


Figure 5. IPv6 connectivity of Google Users

There are other valuable resources on this subject as well. The 'World IPv6 Launch' initiative, which is hosted at http://www.worldipv6launch.org, could be considered for IPv6 development discussions and usage statistics. There are a number of IPv6 usage measurement activities listed on the website.[9]

3. Discussions

Before the technical, transitional and managerial discussions around the security of IPv6, we will briefly discuss why IPv6 implementation efforts are going slowly and IPv6 deployment deadlines are continuously postponed for most organizations.

Although IPv6 has some superior features compared to IPv4, including being a native supporter of IPsec by design, being more mobile-friendly, being more efficient and being scalable, the main motivation behind IPv6 transition is related to the IP address space. IPv4 provides around 4.3 billion addresses, whereas currently there almost 10 billion devices which are connected to the internet. Obviously, there are techniques to share IP addresses between devices which prevent internet users encountering connectivity problems.

The technologies behind this IP sharing are Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT). They enable internet access for different devices in a network segment via using shared IP addresses. As an example, an ISP can assign one IP address to multiple homes in a neighborhood, or similarly, an organization can use just one IP address for its entire facility to provide internet access for users.

These techniques mitigate the IPv4 scarce address issue, which is therefore not the devastating and imminent threat that some people believe. IPv6 might bring some extra features and benefits to the Internet Protocol, but it also has some constraints and drawbacks, especially related to security concerns.

[9] Measurement activities of IPv6 deployment on the global Internet can be found at: http://www.worldipv6launch.org/measurements/.

Security Issues

IPv6, with all its improvements about IP packet headers and new addressing scheme, is mainly a technical topic, but there is more. Especially during the transition period where IPv4 and IPv6 will be used together, there might be additional security issues which arise. Besides all this, IPv6 is still in its infancy in terms of prevalence. This brings managerial discussion topics to the table, since defining *how* and *when* to move IPv6 is an executive decision.

This section is divided into three subsections; technical issues, issues related to transition and management issues. Each subsection will contain main topics about the security discussions related to IPv6.

1. Technical Issues

Although there may be lots of technical topics to discuss from the security perspective, we will mention three main subjects in that regard: Network Address Translation (NAT), Internet Protocol Security and Layer 2 Security.

Network Address Translation

In IPv6, the limited number of available public IP address constraints is no longer the problem it was with IPv4. In IPv4, NAT technology is a solution to tackle this issue and it has another benefit to users in terms of security concerns: it brings obscurity. Users connecting to the internet behind a NAT router are somewhat hidden behind their perimeters since their IP address is not directly open to the internet. This is why some people support using NAT in IPv6 as well. There are other solutions to sustain this advantage in IPv6. One of them is Unique Local Addressing (ULA) which is defined in RFC 4139.[10] The use of private addresses, defined in RFC 4941,[11] can also help users to protect their IP addresses. As a result, along with other technical reasons, NAT is not required and is even discouraged in IPv6 networks.

Internet Protocol Security (IPsec)

One of the main motivations behind IPv4 to IPv6 transition is about advanced security capabilities. IP Security (IPsec) might be the root cause of this. IPsec is a protocol suite in which IP packets are encrypted and authenticated during transmission. It is a framework rather than a single protocol. IPsec can be used in protecting data flows between a pair of hosts (*host-to-host*), between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*).[12] IPsec details are defined in RFC 2401.[13]

In terms of relations between IPsec and IPv4-IPv6 protocols, IPv6 natively supports IPsec whereas IPv4 doesn't. IPsec was developed in conjunction with IPv6 and it was originally required in all standards and compliant implementations of IPv6, until RFC 6434[14] made it only a recommendation.[15] It is advised that IPsec should be used with IPv6, but according to this updated RFC 6434, it was downgraded to 'should' from 'must'. The reason may be related to the computing requirements of encryption process in IPsec, since not every device would have sufficient capabilities, such as smartphones, printers, or household devices. IPsec and IPv6 might have a close relationship, but IPsec can also be used in IPv4 as well. More than that, it can be assumed that IPv4 IPsec implementations are more ubiquitous than IPv6 today. However, the usage of IPsec in IPv4 is not a native approach for this secure transmission technology and it brings additional overheads to these IPv4 connections.

[10] Papadimitriou, D., Drake, J., Ash, J., Farrel, A., and Ong L., Requirements for Generalized MPLS (GMPLS) Signaling Usage and Extensions for Automatically Switched Optical Network (ASON), *RFC 4139*, July 2005.

[11] Narten, T., Draves, R., and S. Krishnan, Privacy Extensions for Stateless Address Autoconfiguration in IPv6, *RFC 4941*, September 2007.

[12] Kent, S. and R. Atkinson, IP Encapsulating Security Payload (ESP), *RFC 2406*, November 1998.

[13] Kent, S. and R. Atkinson, Security Architecture for the internet Protocol, *RFC 2401*, November 1998.

[14] Jankiewicz, E., Loughney, J., and T. Narten, IPv6 Node Requirements, *RFC 6434*, December 2011.

[15] IPSec, http://en.wikipedia.org/wiki/IPsec.

One last point to underline the relationship of IPv6 and IPsec is that IPv6 is considered to be more secure than IPv4 just because of *by design* IPsec support. This may not be true. Not all IPv6 communications would have IPsec because of the scalability issues and other operational expenses. IPv4 can also use IPsec features despite the fact that it wouldn't be a native implementation. As a result, switching to IPv6 and using IPsec would be a viable solution, but this will not prevent unencrypted packet transmissions in the foreseeable future.

Layer 2 Security

Layer 2 security plays an important role for IPv6 because it differs from IPv4 about the operations happening in that layer. Layer 2 (Local Links) processes deal with First Hop Security (FHS) which encompass different issues such as default gateway discovery, local network configuration, and address initialization resolution.[16]

Taking into account 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.[17]

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 couple 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 NDPMon, which is a public domain utility. This checks all RA messages and compares them with a XML configuration file.[18] 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.[19]

Another Layer 2 security concern for IPv6 networks is based on Neighbor Discovery, which is similar to Router Discovery, but between hosts.[20] 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. During address resolution, hosts forward packets to endpoints in order to gather MAC address information. After the NS and NA exchange, the node which forwards the data packet learns the MAC address of the end node and creates a cache entry. If proper protection mechanisms are not employed, an attacker in between these nodes can execute MITM attacks and monitor the traffic.

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. In this duplicate address detection mechanism, hosts probe other nodes in the environment to check whether anyone has the requested IP address. If no one responds with a NA message to the requestor,

[16] IPv6 First-Hop Security Concerns, http://www.cisco.com/web/about/security/intelligence/ipv6_first_hop.html.
[17] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, Neighbor Discovery for IP version 6 (IPv6), *RFC 4861*, September 2007.
[18] S. Hogg, E. Vyncke, Local Network Security, in *IPv6 Security*, Indianapolis, IN: Cisco Press, 2009, pp. 199-201.
[19] Rafixd tool can be downloaded from https://github.com/gws/rafixd.
[20] Nikander, P., Ed., Kempf, J., and E. Nordmark, IPv6 Neighbor Discovery (ND) Trust Models and Threats, *RFC 3756*, May 2004.

the host can start using the IP address it intended to have. If a node in the network sends a NA which claims it has the requested IP address, the host will not take that IP address and try another one. If attacker replies to every message coming from that node, it will prevent that node getting an IP address and will turn into a DDoS attack.

In order to alleviate these neighbor discovery attacks, the IETF published Secure Neighbor Discovery (SEND)[21] and Cryptographically Generated Addresses (CGA)[22] 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.[23]

There are different attack vectors in IPv6 which may cause MITM and DDoS conditions in local networks. Although there are solution mechanisms as well, this situation shows that security aspects continue to be important, as they are in IPv4. From the security point of view, IPv6 has issues to contend with. Also, considering the fact that most attacks come from the application level, changing the protocol which networks operate would help but not solve these upper layer issues.

2. Transition Issues

There are a number of differences between IPv6 and IPv4 protocols, but security is not related to these inherent characteristics alone. The transition process might also generate new questions for security practitioners.

IPv6 transition seems to be taking more time than was estimated; most companies and governmental organizations are continuously postponing the transition and others are reluctant to switch to IPv6 at all. This situation forces organizations to consider using both versions at the same time.

There is a technical approach to deal with networks using IPv4 and IPv6 at the same time: dual stack. In dual stack operations, IPv6 is used to communicate with other IPv6 hosts when required. Otherwise, IPv4 is used. This would turn into a host based threat rather than network related malicious activities; since both IPv4 and IPv6 would be enabled in a host, IPv4 may not be protected appropriately, such as by using personal firewalls and other prevention mechanisms. Even when the network does not run IPv6, the default assumption 'I have no security problems with IPv6' might not be valid. 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.[24] 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 antispoofing techniques, using Access Control Lists (ACLs) and IPsec, these threats could even bypass corporate firewalls.

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 of this period.

[21] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, SEcure Neighbor Discovery (SEND), *RFC 3971*, March 2005.
[22] Aura, T., Cryptographically Generated Addresses (CGA), *RFC 3972*, March 2005.
[23] Securing IPv6 Neighbor and Router Discovery, http://research.microsoft.com/pubs/69145/wise02.pdf.
[24] Hogg, E. Vyncke, Securing the Transition Mechanism, in *IPv6 Security*, Indianapolis, IN: Cisco Press, 2009, pp. 444-459.

3. Management and Awareness Issues

IPv6 security discussions generally comprise technical details and comparisons between IPv4 and IPv6. As with most other debates related to security, there is a lot more to discuss in terms of management and awareness. Decision makers play a huge role in this, even if they are not aware of the effect or they haven't been informed.

The transition period to IPv6 involves lots of double work. Dual stack management efforts, tunneling operations between IPv4 and IPv6, AAAA DNS records handling which maps IPv6 addresses[25] are some, but not all, of them. Managing both protocols in a secure manner should be also considered seriously in order to support the security posture of an organization. More work requires more investment in terms of manpower and direct costs, especially if experience of working with the additional field is lacking. This is one of the first questions which decision makers will face. Training employees, hiring additional ones, creating transition plans and implementing them all bring additional expenses. If the IPv6 security threats are not visible to executives, reluctance to invest in this technology update would be very likely. This creates a gap between the required skillset to implement adequate preventative mechanisms on IPv6 and the people who are responsible for taking actions.

Another issue related to IPv6 security is the awareness problem for both technical experts and executives. Existing security solutions may not contain the adequate prevention mechanisms for the latest threats. Worse than that, more and more hacking tools nowadays have IPv6 specific features. It is not very common to use IPv6 attacks during penetration tests because it takes more time for security experts who conduct those assessments to feel competent in those attacks. They might need more expertise to use such techniques, but real hackers do not have such constraints; time and resource may not be a big problem for them. All of these reasons may produce an environment where administrators are not totally aware of the situation and do not receive comprehensive penetration testing reports, vendors may not support advanced protection features, and executives are not willing to invest more in a not-so-imminent threat. It is obvious that the winner in this picture would be the malicious hacker.

Whether it has decided to start the transition to IPv6 or not, ignoring the risks associated with IPv6, not having qualified people in place, and not properly managing the current networks which already have IPv6-enabled hosts could expand the attacking vectors targeting such organizations.

Conclusion

IPv6 has brought lots of debates to the IT industry, as well as to security communities, and the discussions do not seem likely to come to an end soon. Some people think all organizations should complete their transition to IPv6 as soon as possible, while others think it is not very urgent to accomplish the task. Looking at the fact that IANA made the final delivery of IPv4 addresses almost three years ago in February 2011,[26] and so far there has not been a catastrophe related to the IPv4 addresses, the urgency of the transition is a contentious topic. Nevertheless, complex routing problems and other scalability issues are also known issues related to IPv4, and they push industry to start transition along with other advancements of IPv6. From the security point of view, the discussions are quite similar. Is IPv6 more secure than its predecessor protocol IPv4? Although the answer may depend on the perspective, it would be fair to say it doesn't make a lot of difference for now. Besides, IPv6 had also brought some security risks as well (Figure 6) according to the current status of IPv6 transition.

[25] Thomson, S., Huitema, C., Ksinant, V., and M. Souissi, DNS Extensions to Support IP Version 6, *RFC 3596*, October 2003.

[26] IANA IPv4 Address Space Registry, http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml.

Top IPv6 Security Risks
Lack of awareness
Lack of training
Complicated log analysis and SIEM operations
Lack of sufficient support at some ISPs and vendors
Ineffective rate limiting and reputation-based protections yet

Figure 6. Current IPv6 Security Risks

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.[27] 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.

[27] Microsoft, Industrywide operating system, browser, and application vulnerabilities, *Microsoft Security Intelligence Report*, Volume 15-January through June, 2013, 2H10–1H13.