IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 1, January 2016.

www.ijiset.com

ISSN 2348 – 7968

An analytical study for Security in IPv6

M.A. Hadi[1]

[1] Department of Networks & Communication Systems, Princes Nourah University, Riyadh, KSA,
Email: mohahadi@yahoo.com.

Abstract

The IPv6 protocol has solved some, but not all, of the security problems found in IPv4 networks.so in this paper we will introduce the IPv4 Limitations, the need for IPv6, the security different in IPv6, the benefits of IPv6, security regarding IPv6, the Security Considerations, IPv6 Packet Security and Transition to IPv6 .

Keywords: IPv4; IPv6; IPsec; Security; Transition.

1. Introduction

The Internet Protocol is a set of technical rules that defines how computers communicate over a network. There are currently two versions: IP version 4 (IPv4) and IP version 6 (IPv6).

Internet Protocol (IP) addresses are the unique numbers assigned to every computer or device that is connected to the Internet. Among other important functions, they identify every device connected to the Internet, whether it is a web server, smartphone, mail server, or laptop. After years of rapid Internet expansion, the pool of available unallocated addresses for the original Internet Protocol, known as IPv4, has been fully allocated to Internet Services Providers (ISPs) and users. That's why we need IPv6, the next generation of the Internet protocol that has a massively bigger address space than IPv4. [1]

The major reasons why IPv6 was developed is that the eventual exhaustion of IPv4 addresses because we see every day more and more devices are being connected to the internet, so The Internet Engineering Task Force (IETF) in 1991 decided to create a new version of the Internet Protocol (IP) called Internet Protocol version 6 (IPv6) [1] to replace the old Internet Protocol version 4 (IPv4). [2]

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. The only security feature provided in IPv4 is a security option field that provides a way for hosts to send security and handling restrictions parameters1.

As a result, the Internet Engineering Task Force (IETF) has been working on the IPv6 (Internet Protocol version 6) specifications in order to address these limitations, along with a number of performance, ease-of-configuration, and network management issues [3]. The core IPv6 specifications have been defined by various Request for Comments (RFCs) such as RFC 24602 (IPv6 Protocol)[4] , RFC 48613 (IPv6 Neighbour Discovery)[5] , RFC 48624 (IPv6 Stateless Address Auto-Configuration)[6] , RFC 44435 (Internet Control Message Protocol for IPv6 (ICMPv6))[7], RFC 42916 (IPv6 Addressing Architecture)[8], and RFC 43017 (Security Architecture for IP or IPsec)[9] . IPv6 is also referred as the Next Generation Internet Protocol (IPng) [10].

We will offer a brief introduction and then the understanding of the IPv4 Defined, What Is the IPv4, The advantages and benefits of IPv6, all this will be explained in section II, the security in IPv6, security consideration and packet structure will be explained in section III, . The comparison between IPv4 and IPv6 for Which is more secure will discuss in section IV. In Section V, we explore the transition to IPv6. We will suggest a general recommendation proposed and set of previous suggested solutions in conclusion.

II. IPv6 Vs IPv4

- **What is IPv4?**

In 1991, the IETF decided that the current version of IP, called IPv4, had outlived its design. The new version of IP, called either IPng (Next Generation) or IPv6 (version 6), was the result of a long and tumultuous process which came to a head in 1994, when the IETF gave a clear direction for IPv6. IPv6 is designed to solve the problems of IPv4. [1].It does so by creating a new version of the protocol which serves the function of IPv4, but without the same limitations of IPv4. IPv6 is not totally different from IPv4: what you have learned in IPv4 will be valuable when you deploy IPv6.The differences between IPv6 and IPv4 are in five major areas: addressing and routing, security, network address translation, administrative workload, and support for mobile devices. IPv6 also includes an important feature: a set of possible migration and transition plans from IPv4. Since 1994, over 30 IPv6 RFCs have been published. Changing IP means changing dozens of Internet protocols and conventions, ranging from how IP addresses are stored datagram's are sent and routed over Ethernet, PPP, Token Ring, FDDI, and every other medium, to how programmers call network functions. The IETF, though, is not so insane as to assume that everyone is going to change everything overnight. So there are also standards and protocols and procedures for the coexistence of IPv4 and IPv6: tunneling IPv6 in IPv4, tunneling IPv4 in IPv6, running IPv4 and IPv6 on the same system (dual stack) for an extended period of time, and mixing and matching the two protocols in a variety of environments [11]

- **Limitations**

The problem of the limited IPv4 addresses could be solved in different alternative technologies such as: subnetting, Network Addresses Translation (NAT), or Classless Inter-Domain Routing (CIDR). However, with NAT, the external people see the entire subnet as one computer, and this inherits problems [12]. IP addresses might be solved for a while, but they will no longer be able to handle the fast growth of Internet. Moreover, some more problems are hardly to be solved relating to the current structure of IPv4.

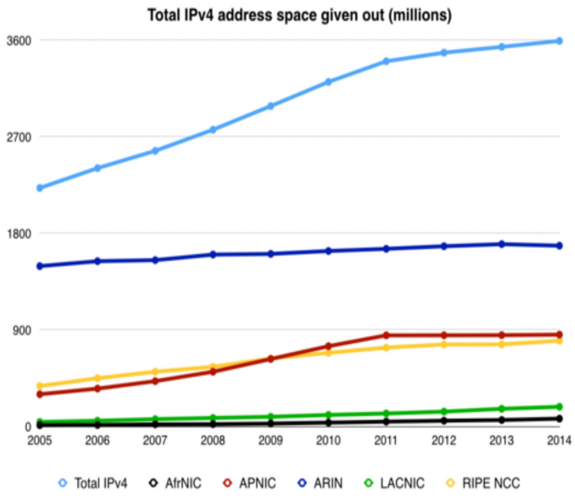


Fig. 1

http://bgpexpert.com/addrspace2014.php

- **What is IPV6?**

Internet Protocol (IPv6 or IPng) is the next generation of IP and it is the successor of IP version 4 which is widely used nowadays. The development of IPv6 started in 1991 and was completed in 1997 by the Internet Engineering Task Force (IETF), and was officially used in 2004 when ICANN added IPv6 addresses to its DNS server [2].

Data transfers between hosts in packets across networks, these packets require addressing schemes. Using IPv4 and IPv6 these packets can identify their sources and also find their destinations. Every device on the Internet needs an IP address to communicate with other devices, and the growth of the Internet led to a need for a new alternative for IPv4, because IPv4 cannot provide the needed number of IP address around the world [13].

The address space in IPv6 is much larger than the address space of IPv4, and it went from 32 bits to 128 bits; in other words, it went from 4 billion addresses to 340 trillion trillion trillion of unique address [2]. IPv6 is designed to provide unique addresses for everyone on earth. This expansion in address space will not just provide more unique address but it will also make routing easier and cleaner because of its hierarchical addressing and simpler IP header [2].

The IPv6 addressing structure is designed to provide compatibility with existing IPv4 networks and allows the existence of both networks. IPv6 does not only solve the problem of shortage that IPv4 is causing, but it is also enhances and improves some of the features that IPv4 has [4].

IPv6 uses 128 bits addressing format that is represented by 16-bit hexadecimal number fields separated by colons ":". Using this format makes IPv6 less messy and error-free. Here is an example of an IPv6 address [2]: 2031:0000:130F:0000:0000:09C0:876A:130B

Additionally, this address can be shortened using some rules like compressing the block of zeros to a single zero like this [2]: 2031:0:130F:0:0:9C0:876A:130B or 0000=0

Also, successive fields of zero can be represented by double colons "::", but it is only allowed once to use a double colon, so the above example will be shortened to this:[2]. 2031:0:130F::9C0:876A:130B

IPv6 (Internet Protocol version 6, also known as IP Next Generation, or IPng) has been developed by the Internet Engineering Task Force (IETF) to overcome the shortcomings in the current IPv4. For instance, IPv6 enables 128-bit address lengths, some four times that of IPv4. It is envisaged that this protocol will satisfy the demand for addresses for a long time. In addition, IPv6 has other features that are intended to provide more reliable services, such as stateless address auto-configuration, a simplified header format to reduce the cost of packet handling and bandwidth, built-in security, and better support for quality of service requirements. The current Internet is mostly based on IPv4, which was defined in 1981 at a time when developers could not imagine the scale of addresses required by the Internet today. IPv6 is a newer numbering system that provides a much larger address pool than IPv4, amongst other features. It was deployed in 1999 and should meet the world's IP addressing needs well into the future.

The great expansion architecture evolve to accommodate the new technologies that support the growing demand for use (by users, application, or services). IPv6 is a newer numbering system that provides a much larger address pool than IPv4. It was deployed in 1999 and should meet the world's IP addressing needs well into the future.[13] of the internet, these days, creates more significant challenges. Not only the addressing of new hosts like computer, tablets, laptop, cell phone but also the technologies. Requires that its overall

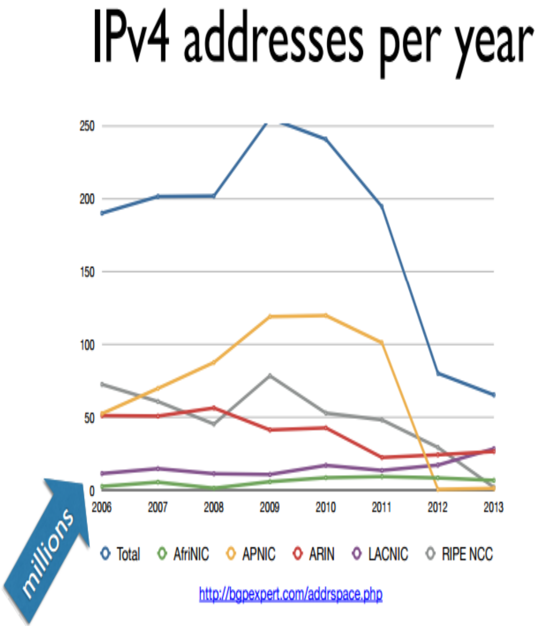


Fig. 2

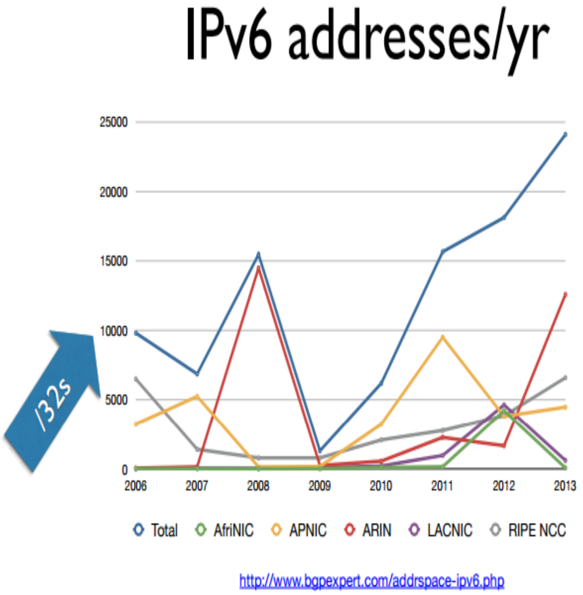


Fig. 3

- **IPv6 Header**

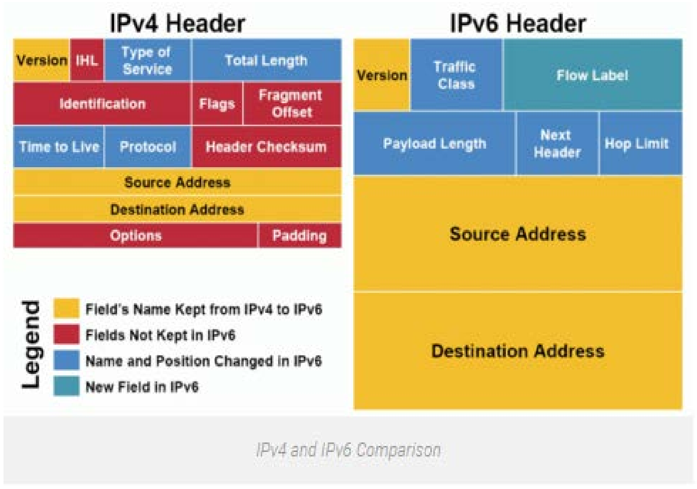
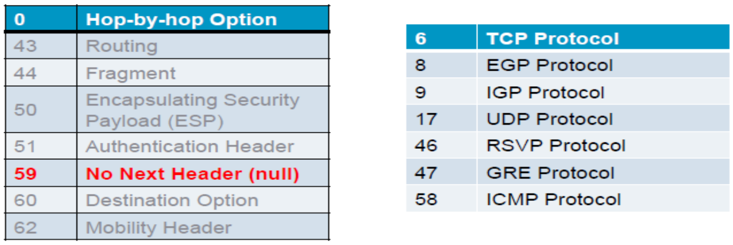


Fig. 4

- **Extension Headers & Fragmentation**



0	Hop-by-hop Option
43	Routing
44	Fragment
50	Encapsulating Security Payload (ESP)
51	Authentication Header
59	No Next Header (null)
60	Destination Option
62	Mobility Header

6	TCP Protocol
8	EGP Protocol
9	IGP Protocol
17	UDP Protocol
46	RSVP Protocol
47	GRE Protocol
58	ICMP Protocol

Fig. 5

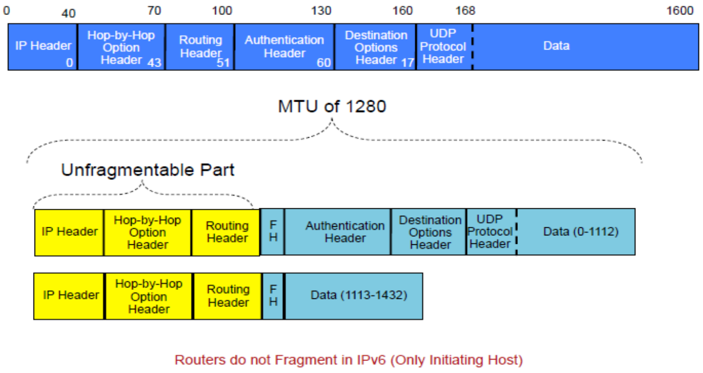


Fig. 6

- **The Benefits of IPv6**

Six Benefits Of IPv6 [14]

With IPv6, everything from appliances to automobiles can be interconnected. But an increased number of IT addresses isn't the only advantage of IPv6 over IPv4. In honor of World IPv6 Day, here are six more good reasons to make sure your hardware, software, and services support IPv6. With IPv6, everything from appliances to automobiles can be interconnected. But an increased number of IT addresses aren't the only advantage of IPv6 over IPv4. In honor of World IPv6 Day, here are six more good reasons to make sure your hardware, software, and services support IPv6.

- **More Efficient Routing**

IPv6 reduces the size of routing tables and makes routing more efficient and hierarchical. IPv6 allows ISPs to aggregate the prefixes of their customers' networks into a single prefix and announce this one prefix to the IPv6 Internet. In addition, in IPv6 networks, fragmentation is handled by the source device, rather than the router, using a protocol for discovery of the path's maximum transmission unit (MTU).

- **More Efficient Packet Processing**

IPv6's simplified packet header makes packet processing more efficient. Compared with IPv4, IPv6 contains no IP-level checksum, so the checksum does not need to be recalculated at every router hop. Getting rid of the IP-level checksum was possible because most link-layer technologies already contain checksum and error-control capabilities. In addition, most transport layers, which handle end-to-end connectivity, have a checksum that enables error detection.

- **Directed Data Flows**

IPv6 supports multicast rather than broadcast. Multicast allows bandwidth-intensive packet flows (like multimedia streams) to be sent to multiple destinations simultaneously, saving network bandwidth. Disinterested hosts no longer must process broadcast packets. In addition, the IPv6 header has a new field, named Flow Label that can identify packets belonging to the same flow.

- **Simplified Network Configuration**

Address auto-configuration (address assignment) is built in to IPv6. A router will send the prefix of the local link in its router advertisements. A host can generate its own IP address by appending its link-layer (MAC) address, converted into Extended Universal Identifier (EUI) 64-bit format, to the 64 bits of the local link prefix.

- **Support for New Services**

by eliminating Network Address Translation (NAT), true end-to-end connectivity at the IP layer is restored, enabling new and valuable services. Peer-to-peer networks are easier to create and maintain, and services such as VoIP and Quality of Service (QoS) become more robust.

- **Security**

IPSec, which provides confidentiality, authentication and data integrity, is baked into in IPv6. Because of their potential to carry malware, IPv4 ICMP packets are often blocked by corporate firewalls, but ICMPv6, the implementation of the Internet Control Message Protocol for IPv6, may be permitted because IPSec can be applied to the ICMPv6 packets.

- **The following are the features of the IPv6 protocol:**

□ Header simplification and new header format
□ Large addressing capability
□ Efficient and hierarchical addressing and routing infrastructure
□ Better support for prioritized delivery
□ Extensions for authentication and privacy

Ipv6 came as need of a big growth of the internet. It is the continuation of many opportunities to make meet the needs for the future. The features of IPv6 are:

□ Large address space
□ New header format
□ Efficient addressing and routing infrastructure
□ Built-in security
□ Better support for QoS (Quality of Service)

These enhancements in IPv6 provide better security in certain areas, but some of these areas are still open to exploitation by attackers.

III. The Security in IPv6

In IPv4 the IP Security Protocol is used which is not different in principle to IPv6 but is very complex and difficult to use. IPv6-enabled nodes must support the IP Security Protocol; therefore IPv6 nodes are more secure. It also includes security features, such as payload encryption, authentication of the communication and data integrity safeguards, in its specifications. Another advantage of IPv6 over IPv4 is IP spoofing, which is known to be one of the most common forms of denial-of-service-attack. With IPv4 is impossible for a server to determine whether packets are being received from a legitimate end node, while an IPv6 server is able to.

A) Security Considerations [15]

1. Massive Size of the IP Address Space

- Makes Port Scanning Harder

When they start, attackers usually employ port scanning as a reconnaissance technique to gather as much information as possible about a victim’s network. It is estimated that the entire IPv4 based Internet can be scanned in about 10 hours with enough bandwidth8, 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 bind 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 neighbourhood 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 impossible to retrofit this functionality to IPv4 with the current 32-bit address space constraint. CGA offers three main advantages:

a. It makes spoofing attacks against, and stealing of, IPv6 addresses much harder.

b. It allows for messages signed with the owner's private key.

c. It does not require any upgrade or modification to overall network infrastructure.

2. IP Security (IPsec)

IP Security, or IPsec for short, provides interoperable, high quality and cryptographically based security services for traffic at the IP layer. It is optional in IPv4 but has been made mandatory 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).

3. Replacing ARP by Neighbour 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 Neighbour Discovery (ND) Protocol for IPv6 is defined in RFC 486111 as a replacement to ARP.

B) Concerns, Potential Threats and Measures

1. IP Addressing Structure

The IP addressing structure defines the architecture of a network. A well-planned addressing structure will reduce potential risks associated with new features provided by IPv6. The following areas should be considered when designing an IPv6 network.

Numbering plan and hierarchical addressing

The numbering plan describes how the organization segregates its IPv6 allocation, for example, if an organization is granted with a 16 subnet bits (/48) address block, this will allow supporting 65,000 subnets. A good numbering plan can simplify access control lists and firewall rules in security operations, and identify ownership of sites, links and interfaces easily. Organizations should carefully plan and create a site hierarchy by consider subnet methods as follows:

□Sequentially numbering subnets
□VLAN number
□IPv4 subnet number
□Physical location of network
□Functional unit of an organization (Accounts, Operation, etc.)

2. Unauthorized IPv6 Clients

IPv6 support is available for most modern operating systems or equipment; it can be easy and sometime unnoticeable to user where the IPv6 protocol is enabled. Due to the extended capabilities of IPv6, as well as the possibility of an IPv6 host having a number of global IPv6 addresses, it potentially provides an environment that make network level access easier for attacker if the access controls are not properly deployed.

To reduce the risk, the following measures could be considered:

□Locate and disable any IPv6 enabled equipment

□Detect and block IPv6 or IPv6 tunnel traffic at network perimeter

□Include IPv6 usage policies in the organization's security plan

3. Neighbour Discovery and Stateless Address Auto-configuration

Neighbour discovery (ND) is a replacement for ARP, and stateless address auto-configuration—which allows an IPv6 host to be configured automatically when connected to an IPv6 network—is a lightweight DHCP-like function provided in ICMPv6. They are both powerful and flexible options in the IPv6 protocol. However, ND may be still subject to attacks that could cause IP packets to flow to unexpected places. Denial of service may be one of the results. Also, such attacks could be used to allow nodes to intercept and optionally modify packets destined for other nodes. While this may be protected with an IPsec AH, RFC 375613 (IPv6 ND Trust Models and Threats) also defines the type of networks in which the secure IPv6 ND mechanisms are expected to work. The three different trust models can roughly corresponding to secured corporate intranets, public wireless access networks, and pure ad hoc networks. Moreover, the SEcure Neighbor Discovery (SEND) protocol is developed to provide an alternate mechanism for securing neighbor discovery with a cryptographic method.

Neighbour discovery, as well as router solicitation in the IP network (v4 or v6) uses ICMP. While ICMPv4 is a separate protocol on the outside of IPv4, ICMPv6 is an integral protocol running directly on the top of the IPv6 protocol, which again could lead to security problems.

Exchanging ICMPv6 messages on the top of the IPv6 protocol for vital "network health" messages and environment solicitations are crucial for IPv6 communication. However, this could be abused by sending fake, carefully crafted response messages for denial of service, traffic re-routing or other malicious purposes. For security reasons, the IPv6 protocol recommends that all ICMP messages use an IPsec AH, which is able to offer integrity, authentication and anti-relay functions.

It may be better to specify critical systems as static Neighbour entries to their default router, instead of using ND, this would avoid many typical Neighbour-discovery attacks. However, certain administrative efforts would be required.

4. Dual Operations

Organizations cannot change all their networks to IPv6 overnight, IPv6 will be gradually deployed while IPv4 will be supported for legacy clients and services. A dual protocol environment increases the complexity for operations and also security. Nevertheless, existing measures on IPv4 should be maintained while the same level of coverage should be applied to IPv6. Organizations need to implement a consistent security policy for both IPv4 and IPv6 (including firewalls and packet filters). During operations, administrators should be aware of relevant threats and vulnerabilities in both protocols and apply appropriate measures to mitigate the risks.

c) Common Attacks In Both IPv4 and IPv6

IPv6 cannot solve all security problems. Basically it cannot prevent attacks on layers above the network layer in the network protocol stack. Possible attacks that IPv6 cannot address include:

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 is 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.

D) IPv6 Packet Security [16]

Unlike IPv4, IPsec security is mandated in the IPv6 protocol specification, allowing IPv6 packet authentication and/or payload encryption via the Extension Headers. However, IPsec is not automatically implemented; it must be configured and used with a security key exchange.

1) IPv6 Packet Structure

The IPv6 header is not variable, as in IPv4, but has a simple, efficient fixed 40-byte length. Minimum packet size is 1280 bytes, from 40 bytes of header plus 1240 bytes of payload.

- Next Header Field

The Next Header field defines the type of header immediately following the current one. It is usually the payload, but sometimes Extension Headers provide valuable functions. Encryption capabilities are defined by the Authentication and Encapsulated Security headers.

- Extension Headers

Protocol numbers in required order of use
000 Hop-by-hop – must be examined by every node on path to destination 043 Routing header – list of nodes that should be visited on path
060 Destination options – processed by routers along path
044 Fragment header – packet was fragmented at source if too large for path
051 Authentication header – part of IPsec
050 Encapsulated security payload – IPsec
060 Destination options – processed at destination

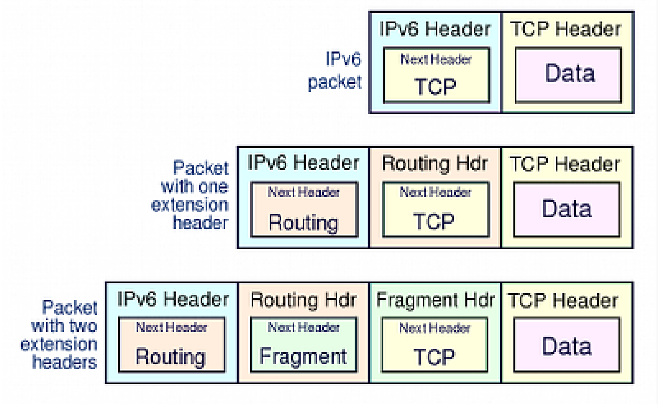


Fig. 7

Right: A simple IPv6 packet (top row) with a TCP header and data payload. The second row shows the packet with an additional Routing header, third row has Routing and Fragment headers.

2) IPv6 Packet Encryption [16]

IPsec defines cryptography-based security for both IPv4 and IPv6 in RFC 4301. IPsec support is an optional add-on in IPv4, but is a mandatory part of IPv6. It provides two security headers which can be used separately or together: Authentication Header (AH) and Encapsulating Security Payload (ESP), used in conjunction with security key exchange.

- Authentication Header

AH provides connectionless integrity, data-origin authentication and protection against replay attacks. It authenticates with an Integrity Check Value (ICV) calculated over the payload, the header, and unchanging fields of the IPv6 header and options. AH does not provide privacy and confidentiality of packet contents. See RFC 2402.

- Encapsulating Security Payload

ESP also provides connectionless integrity, data-origin authentication, protection against replay attacks, limited traffic flow confidentiality, but also provides privacy and confidentiality through encryption of the payload. See RFC 2406.

- IPsec Modes

IPSec operates in two different modes: Transport mode (host-to-host) and Tunnel mode (gateway-to-gateway or gateway-to-host).
Transport mode: the IPv6 header of the original packet is used, followed by the AH or ESP header, then the payload.
Tunnel mode: a new IPv6 header encapsulates the AH or ESP header and the original IP header and payload.
Extension headers (Hop-by-Hop, Routing, and Fragmentation) immediately follow their IP headers, except for Destination Options, which can appear before or after AH or ESP.

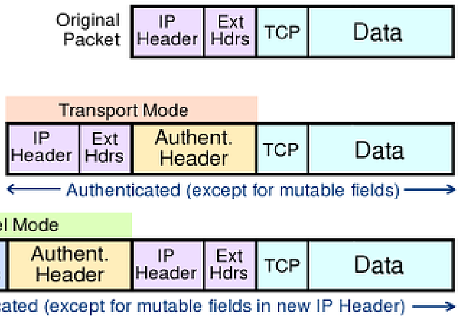


Fig. 8

- AH in Transport & Tunnel Mode

AH authenticates the packet and the outermost IPv6 addresses (except for mutable fields), but does not encrypt payloads. AH cannot be used to traverse NATs, as it calculates the integrity check value (ICV) over source and destination addresses: NATs translate addresses, so would invalidate ICVs.

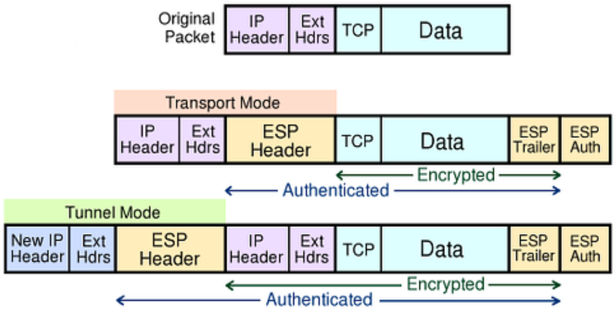


Fig. 9

- ESP in Transport & Tunnel Modes

ESP authentication does not include the outermost IPv6 headers, but in Tunnel mode it protects the original headers. ESP is used to build virtual private network tunnels between sites. It permits NAT traversal, as it does not use the outermost address values in the ICV calculation. If AH and ESP are used together, ESP is applied first, and then AH authenticates the entire new packet.

- The Security Association

Security Association is a record of the authentication algorithm, encryption algorithm, keys, mode (transport or tunnel), and sequence number, overflow flag, expiry of the SA, and anti-replay window. The SA is held in a database at each endpoint, indexed by outer destination address, IPsec protocol (AH or ESP), and Security Parameter Index value.

Selection of SA can be manually (pre-shared keys) but preferably is automated with Internet Key Exchange (IKE, IKEv2). IKE uses Diffie-Hellman techniques to create a shared secret encryption key used to negotiate SA data. For key exchange, IKE depends on a Public Key Infrastructure (PKI), which is not yet widespread. The framework and syntax for key exchange is ISAKMP (Internet Security Association and Key Management Protocol). See RFC 2408.

I. Which is more secure IPv6 or IPv4

Which is more secure?

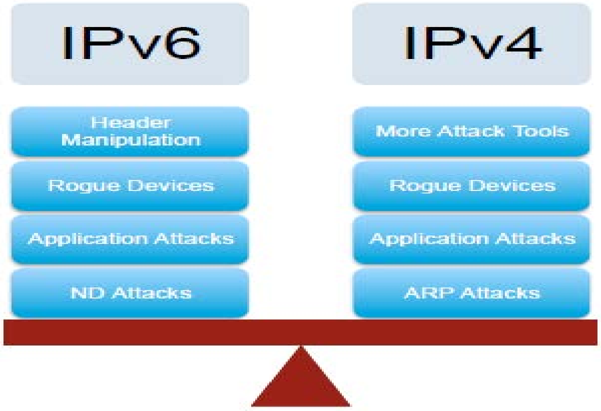


Fig. 10

Debates concerning IPv4 versus IPv6 security often focus on different aspects of network deployment. It has been said that IPv6 supports improved security because the specifications mandate the inclusion of the IP Security (IPsec) suite of protocols in products. In IPv4, including IPsec is optional, but it is commonly available. Because the IPsec protocol suite is designed to be indifferent to IP versions, the technology works generally the same way in both IPv4 and IPv6. In this way, the benefits of using IPsec are similar in either environment.

The increased address space provided by IPv6 does eliminate the need to use NAT devices, which are pervasive in many IPv4 networks. Broadly speaking, security is harder to deploy and troubleshoot when NATs are present in a network as they disrupt IP layer traceability and therefore security audit trails. In addition, the address rewriting that NAT performs is considered by some security protocols to be a security violation. Thus, with the increased address space eliminating the need to use NATs, IPv6 potentially facilitates deployment of end-to-end security.

Many of the IPv6 security issues reported today have to do with vulnerabilities in individual products, not the IPv6 protocol. IPv4 is widely deployed and individual IPv4 products have gone through the recurring cycle of discovering and fixing security vulnerabilities and other bugs. Because IPv6 products are comparatively new, they have not benefited from similar experience. Consequently, security vulnerabilities in IPv6 products will need to be discovered and repaired, just like for other products.

Also, the operational practices built up over many years for IPv4 networks will have to be adapted for IPv6. New practices will need to be developed for the dual stack IPv4 and IPv6 environment. This will be accelerated as more network operators deploy IPv6 and continue to exchange information about experience and best practices through established operators groups, the IETF Operations area, and other forums.

Overall, maintaining network security will continue to be a challenging undertaking in both IPv4 and IPv6 contexts. Neither protocol provides a simple solution to the complexities associated with securing networks. Like with IPv4, network operators should become educated on IPv6 security practices and keep up-to-date with developments as they plan for and deploy IPv6.

- IPv6 Prevents Man-In-The-Middle Attacks [17]

Since IPv6 doesn't use Address Resolution Protocol (ARP), it's assumed that it prevents man-in-the-middle-attacks. In fact, IPv6 uses ICMPv6 to implement the Neighbor Discovery Protocol, which replaces ARP for local address resolution. The Neighbor Discovery Protocol, notes

Moore, is just as vulnerable to man-in-the-middle attacks as ARP--if not more so.

- IPv6 With Mandatory IPSec Is More Secure Than IPv4 [17]

A widely assumed benefit of IPv6 is IPSec support, but the reality is more nuanced. While IPv6 supports IPSec for transport encryption, notes Moore, actually using IPSec is not mandatory and it is not configured by default.

III. Transition to IPv6

Most of the existing systems that we use today already support IPv6. If you're using a laptop, odds are, It supports IPv6 and has done so for quite some time. IPv6 is not dramatically different on the network from IPv4, and the machines we used 30 years ago were capable of running IPv6. This means that if the kind of computers operating thirty years ago could run IPv6, then pretty much any cell phone (or even pocket calculator) could run IPv6 today, if you really wanted it to. [18]

There are three basic aspects involved in the deployment of IPv6: the protocol, the products, and the operational practices.

- The IPv6 Protocol

IPv6 has benefited from over 10 years of development within the Internet Engineering Task Force (IETF). The core standards have been stable for many years and deployed in both research and operational contexts. In addition to the core specifications, IPv6 includes a large number of individual standards that have a more limited applicability and are only needed in specialised environments. Additional development work will continue in these areas as new issues are discovered in response to deployment-specific scenarios. Like the continuing evolution of IPv4, there will always be updates and additions to IPv6 in response to deployment experience. Thus, even though the core IPv6 specifications are stable, there will continue to be ongoing work on IPv6-related specifications.

- IPv6 Products

The core IPv6 specifications are becoming increasingly available as a standard part of products and service offerings. However, not all products are fully IPv6 capable at this time and some significant upgrade gaps remain, especially in low-end consumer equipment. Similarly, while many software applications and operating systems (especially in open source code) have already been updated for IPv6, not all products (including some from major vendors) are fully IPv6 ready. It is best to check with specific vendors on the IPv6 readiness of their individual products and services. In addition, in-house application software or custom code that interfaces with the network will likely need updating for IPv6.

- IPv6 Operational Practices

Operational practices built up over many years for IPv4 networks will have to be adapted for IPv6. There is growing experience in the deployment of IPv6 in research networks and R&D projects, while some production networks (primarily in Japan and Korea) have been running IPv6 for a number of years. IPv6 traffic today, however, remains small in comparison to IPv4. As more network operators deploy IPv6 and continue to exchange information about experience and best practices through established operators groups, the IETF, and other forums, the community knowledge level will grow. In summary, IPv6 is ready for deployment, but additional effort is needed to make its use pervasive. The IETF, equipment vendors, application developers, network operators and end users all have roles to play in ensuring the successful wide-spread deployment of IPv6.[18].

Conclusions

There is an immediate need to adopt IPv6 protocol as early as possible, so as to avoid future impediments in the Internet network. IPV6 is the new version of the internet protocol will replace the IPV4 protocol. Due to prevailing security problems occur in IPV4 day by day the acceptance of the IPV6 on the internet is grown at the very fastest rate in the present scenario. The new version of the internet protocol provides numerous features over IPV4 which directly or indirectly improve security for devices that are connected to the internet. Beside these improvements some of the security issues are still exists and needs thorough attention. IPsec protocol in IPV6 is mandates which enhanced the security in IPV6 but cannot solve all the security problems exist in IPV6. Even though IPV6 is accepted protocol but if we provide some more ways and means to solve the existing issues in

However, acceptance and usage of IPv6 has been slow, because change is hard and expensive. The good news is that all operating systems support IPv6, so when you are ready to make the change, your computer will need little effort to convert to the new scheme.

References

[1] IP Version 6 Addressing Architecture, RFC 2373, R. Hinden, S. Deering, July 1998

[2] Amer Nizar Abu Ali, “Comparison study between IPV4 & IPV6”, International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1,May 2012.

[3] http://www.ietf.org/rfc/rfc0791.txt

[4] http://tools.ietf.org/html/rfc2460

[5] http://tools.ietf.org/html/rfc4861

[6] http://tools.ietf.org/html/rfc4862

[7] http://tools.ietf.org/html/rfc4443

[8] http://tools.ietf.org/html/rfc4291

[9] http://tools.ietf.org/html/rfc4301

[10] http://www.opte.org/history/

[11] Ashis Saklani, S. C. Dimri, “Technical Comparison between IPv4 & IPv6 and Migration from IPv4 to IPv6 “,International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064.

[12] Holly Hubbard Preston, Network World: Edge Routers For IPv6 Migration, http://www.itworld.
com/Net/4057/NWW010423tech/. [Retrieved: 16/12/03].

[13] Ghaida Yagoub, and others, “ Comparison Between Ipv4 And Ipv6 Using Opnet Simulator“,IOSR Journal of Engineering (IOSRJEN), Vol. 04, Issue 08 (August. 2014), ||V4|| PP 44-50, www.iosrjen.org

[14] http://www.networkcomputing.com/networking/six-benefits-of-ipv6/d/d-id/1232791?

[15] http://cisco.com

[16] http://www.ipv6now.com.au/primers/IPv6SecurityIssues.php

[17] http://www.networkcomputing.com/networking/4-ipv6-security-fallacies/d/d-id/1234351?

[18] https://www.isoc.org/internet/issues/ipv6_faq.shtml