IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 9, Issue 12, December 2020

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 12, December 2020 ||

Security Aspect of IPv6 Network

Muskan Tiwari, Prof.Mrs.Rama S.Bansode

P.G. Student, Department of Computer Application, P.E.S. Modern College of Engineering College, Pune, Maharashtra, India

Research Scholar, TMV Pune & Asst. Professor, P.E.S. Modern College of Engineering, Pune, Maharashtra, India

ABSTRACT: This paper is about IPV6 security. The current version followed is Internet Protocol is IPv4 that is used to send data over the Internet. It makes interaction between different services possible. As we know, this protocol has significant limitations, mainly the maximum addressing space and some known security issues. The security problems are in many ways, dependentupon the original development project, which certainly did not consider "security" as a determining factor, and the whole final environment was considered to be friendly. However, over many years, as response to these deficiencies and in consideration of a global network in rapid growth, new technologies such as SSL/TLS and IPSec, have been introduced for remedying these issues.

Despite these enhancements, however, the whole architecture is still missing the level of security and flexibility that was expected. As result of these known limitations, a new project for a new Internet Protocol has been designed by the Internet Engineering Task Force(IETF) in the early 90′, having in mind "ease-of-configuration", performance and security.

In this paper we are going to analyze the security features of the new internet protocols IPv6 its advantages and disadvantages, as well as the possible implications from a security point of view.

I. INTRODUCTION

1.1 What is IPv6?

An Internet Protocol Version 6 (IPv6) address is a 128-bit alphanumeric string to identify an endpoint device in the IPv6 addressing scheme arranged in eight blocks, each of which is 16 bits. Eachblock is expressed as four hexadecimal digits and theseblocks are separated by colons.

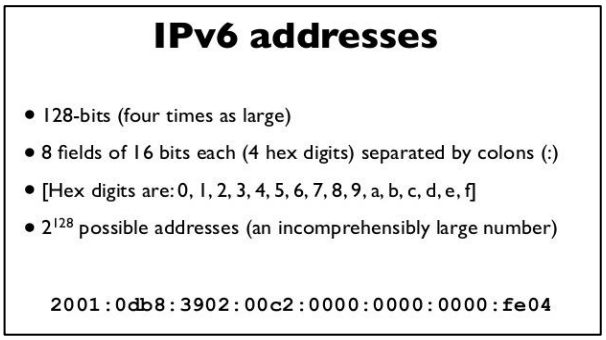


Fig. 1.1 IPV6 Address

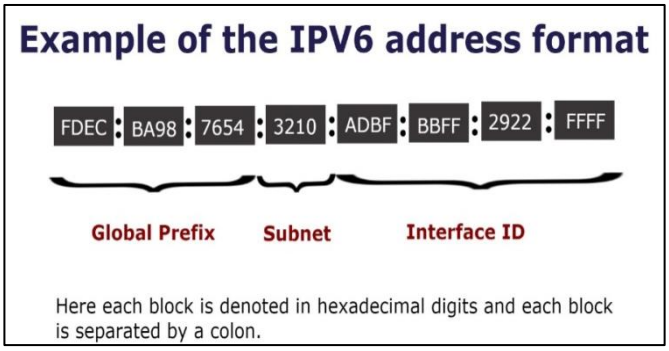


Fig.1.2 IPV6 Example

1.2 History:

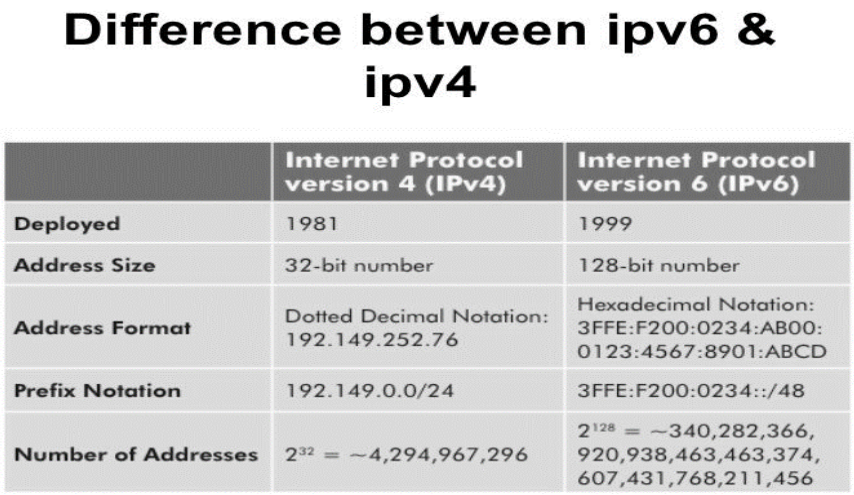
- IPv6 is the latest version of the Internet Protocol used to identify devices across the internet in order to locate them. Every device over the internet is identified through its own IP address in order for internet communication to work. In that respect, it's just similar to the street addresses and zip codes we need to know in order to mail a letter.
- The previous version that is IPv4, uses a 32-bit addressing scheme and supports over 4 billion devices, which was initially thought to be enough. However, the growth of the internet, personal computers, smartphones and various other devices and now Internet of Things devices proves that the world needed more addresses.
- Fortunately, the Internet Engineering Task Force (IETF) recognized this about20 years ago. In 1998 it created IPv6, which instead of 32-bit uses 128-bit addressing to support approximately 340 undecillions. Instead of the

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 12, December 2020 ||

IPv4 address method of four sets of one- to three-digit numbers, IPv6 uses eight groups of four hexadecimal digits, separated by colons known as hextets.

1.3 IPv4 vs IPv6:



	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Deployed	1981	1999
Address Size	32-bit number	128-bit number
Address Format	Dotted Decimal Notation: 192.149.252.76	Hexadecimal Notation: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD
Prefix Notation	192.149.0.0/24	3FFE:F200:0234::/48
Number of Addresses	2^{32} = ~4,294,967,296	2^{128} = ~340,282,366, 920,938,463,463,374, 607,431,768,211,456

Fig. 1.2 IPv4 vs IPv6

To overcome IPv4 security issues, new technologies, like SSL/TLS and IPSec, have been introduced to remedy these issues.

SSL (Secure Sockets Layer) is the technology that keeps an internet connection safe and secure carrying sensitive data being sent between two systems and preventing attackers from reading or modifying any information transferred, that includes potential personal details. It makes use of encryption algorithms that scrambles the data in transit, preventing hackers from reading it as it is sent over the connection. This information could be anything sensitive or personal which can include credit card numbers and other financial or transaction information, names and addresses.

Transport Layer Security (TLS) is an advance,updated and more secure version of SSL.

Despite these enhancements, however, the whole architecture is still missing the security and flexibility level expected. As result of these certain known limitations, by the IETF, a new project for a new Internet Protocol has been developed in the early 90′, having in mind “ease-of-configuration”, performance and security.

II. IP ADDRESSES SECURITY

2.1 IPv4 Security Issues

The following are the security issues of IPv4 some of which are common in both IPv4 and IPv6 address protocols:

1) Reconnaissance Attacks:

This kind of attack takes place because of the relatively small size of IPv4 addressing, because a whole network can be scanned to find openor unpatched services. It is pretty easy to perform a reconnaissance scan of a class C network in a few minutes. We can add methods such as“Ping Sweep” “Port Scan” and “Application Vulnerability Scan” in this category.

2) Denial of Service Attacks:

In this kind of attack, a service is rendered unavailable through a flood of large amounts of illegitimate requests. We can to mention thesmurf attack this category.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 12, December 2020 ||

3) Man-in-the-middle Attacks:

The lack of its own authentication mechanism in communications lets hackers to intercept data in transit.

4) ARP poisoning Attacks:

In IPv4, ARP (Address Resolution Protocol) is the one responsible for mapping a host's IP address with its physical MAC address. This information is stored locallyin (ARP Table) by each host which is part of the communication. The **ARP Poisoning** attack includes sending malicious ARP packets to some default gateway on a network in order to change the pairings in its IP to MAC address table.

5) Address Spoofing Attacks:

The current communication protocols have one of the keys to complete cyber-attacks is the ability to modify the source address of a packet. IPv4 allows this possibility since it does not provide any kind of source-to-end authentication mechanism. These types of attacks are used to spread spam, malware and also to perform DoS/DDoS attacks. IP spoofing also allows masking the true and exact origin of the malicious packets, making the tracking operations more complex.

6) Malware Attacks:

Malware, remains one of the biggest security-related problems today. When it comes to IPv4, malware cannot just damage the host affected, but saturate (or use part of) the network resources in place as well. It's necessary to mention that, with the advent of IPv6, there was no way to eradicate these threats and issues, and the conception of the potential damage by malware infection will essentially remain the same. It's possible to assume that, however, due to the broader spectrum of addressing, its spread could be slower and time consuming.

2.2 What's New in IPv6?

IPv6, along with the basic features of an IP address protocol, it is a totally new suite of protocols. This means that the differences between the two are marked:

1) Address Space:

IPv4 provides as many as 2^32 addresses. It provides as many as 2^128 addresses.

2) Hierarchical Addressing:

In IPv6 there are 3 major types of addresses: Unicast, Multicast and Anycast.

3) QoS (Quality-of-Service) and Performances:

The IPv6 packet header provides fields that facilitate the support for QoS. In addition, the new standard is way forward in terms of performance.

4) Security:

The use of IPSec in IPv6 is not optional, but it is mandatory.

5) Extensibility:

In spite the new features and the considerable increase of addressing space, the IPv6 header is only slightly bigger than that of IPv4. The IPv6 header does not include checksum and any optional fields. Here are explanatory images of an IPv4 header and an IPv6 header for ease of comparison:

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 12, December 2020 ||

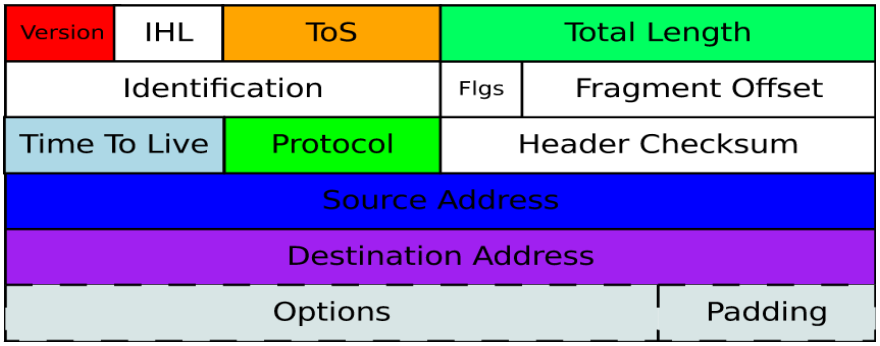
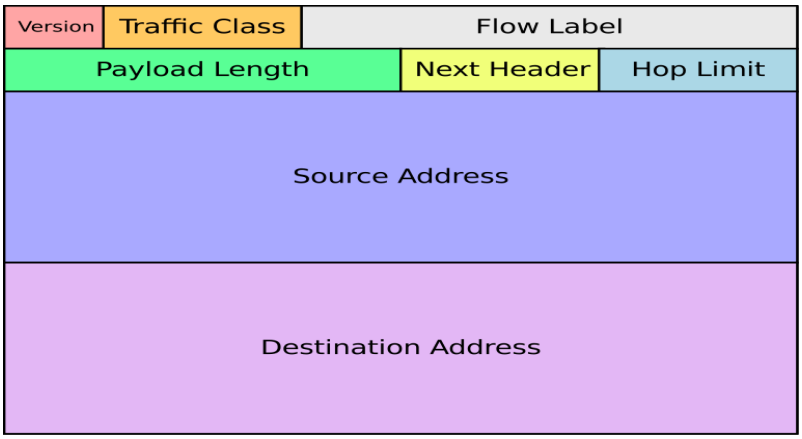


Fig.2.1 IPv4 Header Format

In IPv4, the IPv4 header is followed by data of transport protocol (TCP, UDP), also called "payload."



The IPv6 header has "Extensions Header" and thenfollowed by data of transport protocol.

6) Auto-Configuration:

IPv6 provides both stateful and stateless auto-configuration of IP addresses. Stateful auto-configuration utilizes DHCP whereas Stateless auto-configuration occurs without the use of DHCP.

2.3 Security Enhancements

It is fair to consider that IPv6 is not necessarily more secure than IPv4 for a correct point of view. The approach to security put in place, even though considerably implemented, is still marginal and not totally new. However, there are some considerations that, without doubt, it has increased the level of IPng reliability.

1) Mandatory use of IPSec:

IPv4 also offers IPSec support. But, support for IPSec in IPv4 is optional. The RFC4301 instead makes it mandatory for IPv6 to use IPSec. IPSec consists of a set of cryptographic protocols made to provide security in data communications. IPSec has AH (Authentication Header) and ESP (Encapsulating Security Payload) in its suite. The first provides for authentication and data integrity, the second, in addition to these, also provides for confidentiality.

A fundamental concept of IPSec is"Security Association". SA is uniquely identified by some parameters like SPI (Security Parameters Index) which is a field in the AH/ESP header, the security protocol and the destination IP address. The SA defines the security services type for a connection and usually contains the key for data encryption as well as

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

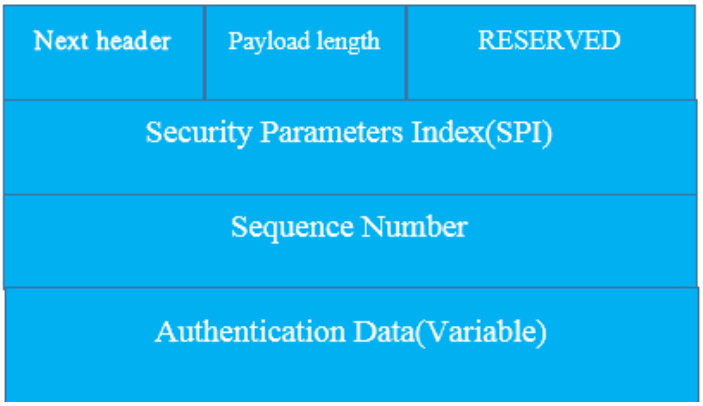
|| Volume 9, Issue 12, December 2020 ||

the encryption algorithms to be used. The Internet Key Exchange (IKE) is the process that is used for negotiating parameters needed to establish a new SA. Following are details about the AH and ESP:

AH (Authentication Header):

AH provides for authentication along with the data integrity for the entire IPv6 packet. The meaning of "Authentication" is that if an endpoint receives a packet with a particular source address, it assures that the IP packet did indeed come from that IP address.

Assuring that if any endpoint receives data, the original content of that data has not been modified in the path from the source to the destination is called "Integrity". The format for AH is shown below:



Next Header is a field which is used to identify the type of transport, such as UDP. **Payload Length** helps identifying the length of Authentication Header. The SPI field provides for identifying the security parameter index which will be used to identifying the SA. The "Sequence Number Field" is a counter that is incremented by 1 when a sender or a receiver receives or transmits some data. By SNF, an anti-replay protection is provided, because when the receiver receives a packet with a duplicate Sequence Number Field, this is discarded

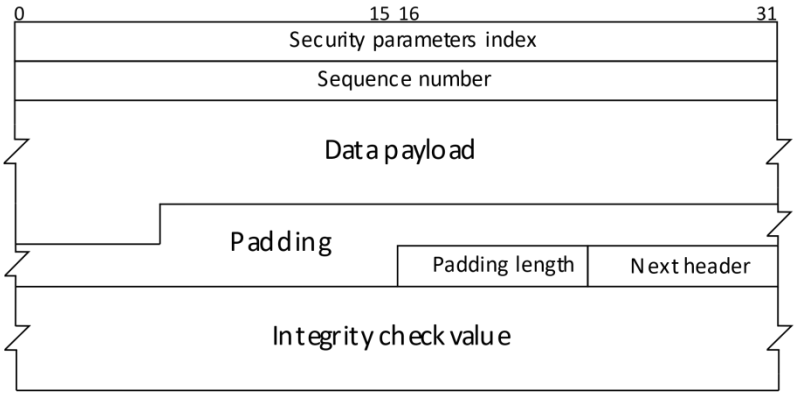
The Authentication Data contains the Integrity Check Value (ICV) which provides for data integrity and authentication. The ICV is calculated by using the IP header, the IP packet payload and AH header. What happens actually is that when the receiver receives the packet, it calculates the ICV with some algorithm and the specified key in SA. As per the details mentioned and the technology that is used, AH can prevent "IP Spoofing Attack".

ESP (Encapsulating Security Payload):
The ESP gives confidentiality, authentication and data integrity. Confidentiality means that nobody else, even the intended receiver, can read the content of communication in transit. ESP provides an anti-replay protection also. The

format of an ESP packet:

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 12, December 2020 ||



ESP also has an SPI field that identifies the SA. The Sequence Number field, like in the AH, provides an anti-replay protection facility. **Next Header** field, which describes the data type contained in the **Payload Data** field (the entire packet if ESP is used in Tunnel Mode or only payload if is used in Transport Mode). The **Authentication Data** field contains the ICV (if auth service is specified by SA associated with SPI), which provides authentication and data integrity. The authentication algorithm used to calculate the ICV is also specified by the SA.

2) Large Addressing Space:

As mentioned before that in IPv4, reconnaissance attacks and port scanning are simple tasks relatively. The most common network segments in the current Internet Protocol (IP) are that of class C, with 8 bits allocated for addressing. Performing this type of attacks on these network segments does not take more than a few minutes. Allocating 64 bits for addressing,as expected in an IPv6 subnet means performing a net scan of 2^64 that is equal to 18446744073709551616 hosts is practically impossible.

3) Neighbour Discovery:

Neighbour Discovery (ND) is the mechanism that is used for router and prefix discovery. It is a network layer protocol, like IPv4 equivalents ARP and RARP. ND works too closely with address auto-configuration, that is the mechanism used by IPv6 nodes to acquire configuration info. ND and address auto-configuration both contribute to make IPv6 more secure than its predecessor.

III. IPv6 SECURITY

3.1 Advantages provided by IPv6

The main advantage of IPv6 is that it provides a lot more address space. IPv6, being a more recent protocol,surely, does have a few design improvements over IPv4, particularly in the areas of auto-configuration, mobility and extensibility. But increased address space is the main benefit of IPv6.

3.2What are the key security concerns?

There are a lot many factors which make the IPv6 protocol suite challenging from a security point.

• IPv6 implementations are less mature than that of their IPv4 counterparts making it to have a number of vulnerabilities to be discovered and mitigated before their robustness matches that of the existing IPv4 implementations.

• Security products like firewalls and Network Intrusion Detection Systems have less support for the IPv6 protocols than for their IPv4 counterparts.

• A number of transition or co-existence technologies have been developed to aid in the deployment of IPv6 and the co-existence of IPv6 with the IPv4 protocol. These technologies will increase complexity of the network which may introduce new attack vectors in existing networks.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 12, December 2020 ||

• Technical personnel have lesser confidence with the IPv6 protocols as compared to their IPv4 counterparts. This creates a likelihood that security implications are overlooked when the protocols are deployed.

IV. SECURITY IMPLICATIONS

4.1 What should be done?

Risk assessment can be completed on how IPv6 and related technologies (such as transition or co-existence technologies) may affect the security of existing IPv4 networks. Develop a plan for transition; IPv6 affects every network and there is no 'do nothing' option. Ensuring that relevant staff, such as network engineers and security administrators, are confident with IPv6 and related technologies before they are required to deploy and operate IPv6 in production networks. Working with equipment and application suppliers to improve the robustness of its implementation, such that the robustness of IPv6 implementations roughly matches that of typical IPv4 implementations can be done.

4.2 Security implications of IPv6 A brief comparison of IPv4 security and IPv6 security

The security implications of the basic IPv6 protocol are very similar to those of IPv4. Similar vulnerabilities are present in both protocols, with the differences lying in the specific attack vectors provided by each of protocol. However, IPv6 protocol suite has a number of supporting protocols that are more complex in general than their IPv4 counterparts (or that were not even present in the IPv4 protocol suite). For example, for the host configuration, IPv6 provides not only DHCPv6 (the equivalent of DHCP for IPv4), but also a mechanism for Stateless Address Auto-Configuration (SLAAC) that introduces a lot of attack vectors which were not present in IPv4. Regardless of the similarities and differences between IPv4 and IPv6, there is a key aspect in the resulting level of security of IPv6 networks is the level of IPv6 support in security devices. It is generally the case that there are better security features in IPv4 products compared with IPv6 products, either in terms of performance, the variety of products, the variety of features. This will probably make it difficult to enforce exactly the same policies in IPv6 networks like how they are enforced in IPv4 networks, at least for a period of time. As a result, this situation could be exploited by attackers who may leverage IPv6 for bypassing network security controls.

Transition planning

There are a variety of transition mechanisms and a variety of network scenarios in which the IPv6 protocols can be deployed that might be employed in each of those scenarios for the purpose of deploying IPv6. It is important that the appropriate scenario and mechanisms are identified at the outset before resources are expended or weaknesses are exposed. As the least, the transition plan should include:

• A requirements analysis for identifying scope;
• A sequencing plan for the implementation process;
• Development of IPv6 policies as well as mechanisms;
• Development of training for key team members;
• Development of a test plan for interoperability and compatibility;
• Maintenance along with the monitoring programmes;
• An ongoing and continuous update plan for critical architecture;
• Plan for the phased withdrawal from service of IPv4 services and equipment.

Security implications of a dual-stack approach

IPv6 is not backwards compatible with IPv4. This usually means that at least during the transition period IPv6 will need to operate in parallel with IPv4. This has a plenty of security and operational implications. Running a dual-stack which means running IPv4 and IPv6 simultaneously, increases the complexity of a network. Dual-stack nodes need to implement two different protocols, network administrators need to configure two different set of protocols, security administrators need to enforce security policies for two different sets of protocols, and so on. At core routers, support of both IPv4 and IPv6 protocols generally means that two instances of routing protocols and routing tables must be supported, that increases the complexity in the network and may increase the hardware requirements, and increases the available attack surface. In some of the cases, legacy devices might not provide the necessary IPv6 functionalities to match that currently provided for IPv4, and this may result in asymmetric functionality or enforced policies for IPv4

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 12, December 2020 ||

and IPv6. "CORE, 2007" is about an advisory of IPv6 vulnerability found in a highly secure operating system. This, probably is a good example that running two protocol stacks comes with a cost. Transition technologies may also add to this burden, as in usual they not only result in increased complexity, but also prevent existing security devices from enforcing the same type of policies that they can apply to native IPv4 or native IPv6 traffic.

Security implications of NAT-free network architectures

Network Address Translators (NAT) provides many benefits in a network like reduced host exposure, host privacy/ masquerading and topology hiding. The recent internet architecture has incorporated the use of NATs originally as a stop-gap mechanism for the imminent exhaustion of the IPv4 address space. As we know, IPv6 allows the assignment of at least one 'public' address to each device connected to the internet, it is usually claimed or assumed that IPv6 network architectures will not accommodate NAT devices. This would change the architecture of most current networks drastically, in which NATs isolate the internal nodes from the public internet until and unless communication has been initiated from the internal realm of the NAT. That is, the exposure of nodes to the public internet would tend to increase. But it should be noted that the deployment of IPv6 does not necessarily imply a return to end-to-end connectivity, nor does it preclude similar network architecture to that achieved today through the use of NATs. For e.g., it is very likely that IPv6 will be deployed in enterprises along with a perimeter firewall that only allows packets to traverse the firewall from the external realm (policy domain) to the internal realm if communication was initiated from the internal realm. A number of other technologies might be employed to achieve a similar level of host privacy or masquerading and network topology hiding to that currently achieved in IPv4 with NATs and other technologies.

Security implications of IPv6 within IPv4 networks

A number of transition technologies have been developed for the deployment of IPv6 and the co-existence of IPv6 with IPv4 deployments. Some of such technologies aid in the deployment of IPv6 by enabling communication between islands of one network protocol (e.g. IPv6) across networks that employ some other type of network protocol like, IPv4. This is achieved by the 'tunnelling' paradigm, in which one network protocol, for e.g., IPv6, is encapsulated within another network protocol, for e.g., IPv4. While these technologies provide a valuable functionality, this comes with some cost like cost of increased complexity, with the consequent security implications. Say, for example, tunnels may introduce Denial-of-Service (DoS) attack vectors, and may prevent network security devices from enforcing the same security controls that they can readily enforce on non-tunnelled traffic. Furthermore, some transition technologies require very little or no management, and are enabled by default in some of the popular operating systems which may result in a node or site making an unintended use of IPv6 transition or co-existence technologies which could increase the exposure to attack, and/or be leveraged by attackers to bypass network security controls. As a result, IPv6 transition or co-existence technologies should be a concern not only to network engineers and security administrators operating or managing IPv6 networks, but also to network engineers and security administrators operating or managing IPv4 networks, whose security policies may be by-passed by leveraging these technologies.

IPv6 support in network devices

It is a concern when planning to deploy IPv6 should be the level of IPv6 support (if any) in each of the different network devices.
It is usually the case that there is more support for security features in IPv4 products than in IPv6 products, either in terms of variety of products, variety of features, or performance. This will probably make it difficult to enforce exactly the same policies with IPv6 as that are enforced with IPv4, at least for some period of time. Consequently, such situation could be exploited by attackers who would probably leverage IPv6 to bypass network security controls, etc. With both protocols, specific security issues are more probable to be found at the practical level than in the specifications. The practical issues include, for e.g., bugs or available security mechanisms on a given product. When deploying IPv6, it is an important aspect to ensure that the necessary security capabilities exist on the network components specifically when dealing with IPv6 traffic. For e.g., firewall capabilities have often been a challenge in IPv6 deployments.

IPv6 support in applications

Many applications currently do not support IPv6, or have only recently been updated to have support for IPv6. This means that their maturity is less as compared to their IPv4-only counterparts, and it is very likely that a number of vulnerabilities will be discovered in them before their maturity matches that of IPv4 applications.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 12, December 2020 ||

The application security is not likely to be affected by IPv6 itself, but as a result of a lack of secure software development practices (as it is still the case in IPv4).

IPv6 training

In addition to any potential shortcomings of the IPv6 protocols, it is very likely that the 'human factor' will play an important role when it comes to the resulting network security. While IPv6 provides a similar functionality to those that are provided by IPv4, there are substantial differences in how such functionality is achieved. As a simple example, compare how address resolution is performed in IPv6 and in IPv4 (i.e., Neighbour Discovery vs. Address Resolution Protocol). Many organisations are mostly going to end up deploying the IPv6 protocols without proper training, laboratory experimentation, etc., resulting in the deployment of IPv6 in production networks without the same level of confidence and comfort with which the IPv4 protocols have been deployed and are currently operated. Even if the organisations have no concrete plans to deploy IPv6 in any near term, it is highly likely that the network will be affected by IPv6 issues beyond its immediate control, that's why it is recommended that network and security staff be trained on the IPv6 protocol suite. It would also be sensible to conduct experimentation in network labs, so that required expertise is gained before network and security teams are urged to deploy the IPv6 protocols in production networks.

V.CONCLUSION

There is not much difference in IPv4 and IPv6 security aspects. However, it is slower and little more difficult to attack networking dealing with IPv6 Protocol as IPv6 has larger address space, spoofing etc gets complicated.
By being more aware of the security implications of IPv6,businesses can make a secure and safer transition and continue to enjoy the new possibilities offered by IP communications and they can do so securely.

REFERENCES

1. https://resources.infosecinstitute.com/topic/ipv6-security-overview-a-small-view-of-the-future/
2. www.cpni.uk - CPNI VIEWPOINT SECURITY IMPLICATIONS OF IPv6
3. https://www.networkworld.com/article/3254575/what-is-ipv6-and-why-aren-t-we-there-yet.html
4. https://www.geeksforgeeks.org/ - IPV6

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details