Journal Homepage: -www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
ISSN NO. 2320-5407
Article DOI:10.21474/IJAR01/6953
DOI URL: http://dx.doi.org/10.21474/IJAR01/6953

RESEARCH ARTICLE

A COMPARATIVE STUDY ON IPV4 AND IPV6.

Ahmed A. Radif Al-khafaji[1] and Hasan H. Balik[1,2]
1. Department of Computer Engineering Yildiz Technical University Istanbul, Turkey.
2. Air Force Academy, National Defense University, Istanbul, Turkey.

……………………………………………………………………………………………………....

Manuscript Info

……………………..
Manuscript History

Received: 15 February 2018
Final Accepted: 17 March 2018
Published: April 2018

Abstract

……………………………………………………………….
The addresses of Internet protocol (IP) are avital resource for the Internet. In the network, IP address is assigned to every interface which connects to the Internet. The addresses are still assigned by using Internet Protocol version 4 (IPv4). IPv4 has demonstrated robust, compatibility with vast range of protocols, applications and easy implementation. IPv4 had been supposed to cover all the network interfaces, however with huge increase of the number of devices (computer, mobile, tablet, routers, server, etc) the reserve of assigned addresses is exhausted. IPv6 has been deployed for providing new services and for supporting the internet growth. This study compares the key specifications of IPv4 and IPv6, contrasts IPv4 and IPv6 header's fields, the structure of headers, explains advantages of IPv6 and disadvantages of IPv4, and why.

……………………………………………………………………………………………………....

Introduction:-

The internet technology has been recognised as the global system of interconnected computer networks that make use of standard internet protocol suite (TCP/IP). This protocol suite plays an inevitable role in connecting billions of computing devices, across the globe. In short, internet technology has commendably contributed in the evolution and tremendous growth of the digital devices and their application in approximately all aspects of life. It has been established from the analysis of the study of Shah (2013) that since its advent the operations of the internet became dependent on IPv4 (Internet Protocol Version 4). IPv4 is the fourth version of IP that is famous for efficiently routing traffic on the internet. IPv4 is nothing more than the connectionless protocol that works on packet-switched networks. IPv4 had served the internet world for the period of fifty years and it is also the fact that the internet, based on IPv4 has made considerable success during the period of last twenty years. However, because of the insufficiency of the unallocated IPv4 addresses, this protocol was not able to fulfil the changing needs of the ever expanding internet. In other words, it can be affirmed that the exponential growth in the number of technological systems and devices had resulted in the exhaustion of IPv4. Some of the researchers have claimed that the scale of IPv4 internet has become far bigger than it was expected at the time of its designing. The situation had resulted in causing series of issues to IPv4 that include broken end-to-end property, scalability of routing, and address exhaustion (Aluko, Olusanya, Oloyede, and Ebisin, 2014; Shah, 2013; Wu et al, 2013).

It has been documented in the study of Wu et al (2013) that in the year 2011, *Internet Assigned Numbers Authority* (IANA) had started facing the issue of IPv4 address pool exhaustion. At that time, it was predicted that in next threeyearsall 'Regional Internet Registries'

Corresponding Author:- Ahmed A. Radif Al-khafaji.
Address:- Department of Computer engineering Yildiz Technical University Istanbul, Turkey.

RIRs) will completely utilise their address space (specifically the one that belong to IPv4). In the year 2011, February ICANN (Internet Corporation for Assigned Names and Numbers) had given out the last block of the IPv4 address. In short, it is expected the address space of IPv4 will be completely depleted. Though, SPs (service providers) have resorted to a number of mechanisms, for instance, multi-layers of NAT (*Network Address Translation*). The main objective of such initiatives is to reuse and save the address blocks from exhaustion. However, the more appropriate approach to handle this issue was to move from IPv4 to IPv6.

According to Sharma and Singla (2016), IPv6 which is also referred as IPng is the most viable solution to the depletion of IPv4 address space. In other words, IPv6 has been designed and presented as the next-generation network layer protocol that would efficiently overcome the issues in IPv4. IPv6 possess the address space of 128 bit and authorises around 340 undecillion addresses (Sharma and Singla, 2016). It shows that IPv6 would definitely fulfil address needs of continually increasing network devices. Besides that, the address length of IPv6 also plays a significant role in making the prefix aggregation fairly flexible; thereby, successively achieving global routing and addressing in a hierarchical pattern. Thereby, it can be asserted that IPv6 is the feasible, mature, and the most viable solution for the next-generation internet that is demanding increasing IP addresses (Wu et al, 2013).

Problem Statement:-

IPv6 with its enhanced features, in terms of new addressing schemes and improved IP packet headers, had gained considerable recognition in

the networking and technology-driven organisations. Regardless of these benefits, the adoption of IPv6 is still in its infancy and the majority of the organisations prefer to continue on IPv4. According to Doshi, Chaoua, Kumar, and Mallya (2012), the adoption of IPv6 is slowed down because of facing numerous obstacles. First of all, there is not any financial driver for the organisations that could motivate them to move towards IPv6. Moreover, it is also observed that IPv4 address space exhaustion has been advertised for several years that have resulted in leading the industry towards developing such technologies that could help them in extending the use of IPv4 address. In this regard, one of the most popular technologies includes NAT (Network Address Translation).

Wu et al (2013) has established that IPv6 does not have backward compatibility with IPv4. This feature ultimately limits the communication amid IPv6 and IPv4 networks. In particular, an independent and parallel network has been developed by IPv6 that exist with IPv4. In such circumstances, if the IPv4 network supports the communication activities of IPv6 then it will have to ensure dedicated routing and addressing for IPv6 while upgrading its network devices. Interestingly, the IPv6-accessible contents and IPv6-driven application are still in minimum number and the majority of the network applications, services, and resources are compatible to IPv4. This scenario shows that IPv4 networks are expected to last for the longer periods of time and it would take several years to completely move towards IPv6 from IPv4.

When the adoption of IPv6 was assessed in the global context, it was observed that Belgium has been ranked as the global leader in the adoption of IPv6 with 46.4% connections. However, some of the countries have considerably low adoption rate of IPv6, including Singapore (3.5 per cent), Israel (2.9 per cent), Austria (3.0 per cent), South Korea (2.2 per cent), Oman (0.1 per cent), Bosnia / Herzegovina (2.9 per cent), Denmark (1.2 per cent), China (0.3 per cent), Tanzania (0.2 per cent), Zambia (0.1 per cent), and Iraq (0.0 per cent) (Akamai, 2017017.).

The biggest issue that is hindering the complete transition from IPv4 to IPv4 is the limited knowledge of the executive and technical experts regarding IPv6 and its associated functions. It is a fact that the security solutions that are currently being used for the mitigation of the IPv4 security issues are not sufficient for the threats that are posed to IPv6. However, hackers have developed such malicious codes and techniques that have IPv6 specific features. It is established that the malicious codes and security vulnerabilities can be easily identified during the phases of penetrating testing; however, security experts usually avoid carrying out these activities as they are time-consuming (Çalışkan, 2014). It is also found that the limited awareness, lack of comprehensive penetration testing practices, and the unwillingness of the organisations to invest in employee training and infrastructure, lack of compatibility amid IPv4 and IPv6, etc. are the core factors that are hindering the transition to IPv4 to IPv6.

Aim and Objectives:-

The aim of the present paper is to examine the reasons that are involved in the existence of IPv4, despite the development of IPv6. In order to successfully accomplish this research aim, following objectives have been formulated.

-To examine the functions and characteristics of IPv4;
-To analysis the functions and characteristics of IPv6;
-To understand the need of transition from IPv4 to IPv6;
-To recognise the security threats that are posed to IPv4 and IPv6;
-To assess the factors that are hindering the adoption or assimilation of IPv6;
-To make recommendations to the IT experts of Iraq to ensure a smooth transition from IPv4 to IPv6.

Internet Protocols and its Functions:-

Oki, Rojas-Cessa, and Vogt (2012) have demonstrated internet protocol (IP) as the one that is present in the network layer. The main function that is carried out by this protocol is to transmit data from the source host to the destination host. It is important to note that a unique number is assigned to each host that eradicates the risk of duplication or any other related issue. In short, the IP is nothing more than the network-layered protocol that incorporates source control information as well as the addressing information that ultimately leads the packets to be routed. Aluko, Olusanya, Oloyede, and Ebisin (2014) had stated that internet has played an inevitable role in making the entire world, a global village, specifically by connecting billions of devices. It is important to note that the correct, secured, and meaningful connection between these devices is established through distinctive IPs. Therefore, it can be affirmed that the overall performance and functions of the internet are based on IP. For this reason, internet protocols have become the most famous non-proprietary (open system) protocol suite. Abdullahi and Mahadevan (2010) had stated that IP is the protocol that facilitates communication activities, across the internet. The primary task of the protocol is to deliver datagrams, belonging from different protocols to the specific destination. These operations are based on the packet encapsulation, security techniques, specific addressing formats and other related capabilities of the internet protocol. According to Kozierok (2005), IP is nothing more than the collection of protocols that are solely aimed at facilitating communication amid the networks.

Aluko, Olusanya, Oloyede, and Ebisin (2014) had highlighted some of the functions of internet protocols that include addressing, indirect delivery/routing, fragmentation and reassembly, and data encapsulation and formatting/packaging. The main function of IP is associated with the host addressing that enable the datagrams to be delivered to the correct device, regardless of the presence of the arbitrarily large networks. While describing the data encapsulation and formatting/packaging function of IP, Aluko, Olusanya, Oloyede, and Ebisin (2014) had suggested that it receives data from transport layer protocols TCP and UDP. Afterward, this data is encapsulated into the IP datagram before the commencement of formal transmission. Another function that is carried out by IP is the reassembly and fragmentation. In this account, the IP datagrams are transferred to the data link layer so as to pass the information towards the local network. However, when the IP datagram has to be delivered to the destination which is on the similar local network, it is usually done by the help of network's underlying WAN/WLAN/LAN protocol. This practice is usually termed as direct delivery. Aluko, Olusanya, Oloyede, and Ebisin (2014) had stated that this activity is usually carried out with the help of some other protocols that mainly include the TCP/IP routing/gateway protocols and ICMP, such as BGP and RIP.

Internet Protocol Version 4:-

Bons and Weigand (2011) had referred to the definition of RFC 791 and regarded IPv4 as the first protocol version that was deployed on ARPANET. After some time, ARPANET had become the internet. This internet protocol version had 32 bits address space that means it offered the space of 4, 294, 967, 296 addresses. Abdullahi and Mahadevan (2010) had stated that the main objective of developing IPv4 was to ensure network interconnectivity. The operations of IPv4 are based on two-level hierarchy that mainly includes host part and network part. As far as the function of both of these parts is concerned, it is found that host is responsible for carrying out the data packets to the final destination. On the other hand, network part has the responsibility of finding network's location, specifically where the host is connected. In this way, the functions of data transmission are performed on IPv4.

While highlighting the operational significance of IPv4, Ali (2012) had stated that it is a fourth internet version and is among the first protocol's version that has widely been deployed in advanced TCP/IP. The protocol is supporting million and billion of networking devices because of having strong capability of delivering datagrams to the correct destination networks, without harming the integrity of the information. On the basis of this mechanism, the internet based on this protocol version (i.e., version 4) had made commendable success during the period of last twenty years. Bi, Wu, and Leng (2007) had highlighted that because of the unavailability of empty address spaces, this protocol cannot fulfil the needs of continually expanding devices that are driven by the internet. Hanumanthappa (2009) had also presented the same idea by claiming that the unexpected explosion of internet-based devices has played a major role in the exhaustion of IPv4 address space that was based on only 32 bits. According to Ali (2012), the exhaustion of IPv4 address space is apparent since the 1980s. Though a number of measures like CIDR addressing, etc. have been made to control the situation but the consumption of IPv4 addresses has reached to the alarming situation. Primarily, it is found that the increased utilisation of the cable modems, ADSL modems, increased usage of internet, increasing mobile devices, and growing internet users have significantly contributed to the depletion of IPv4 address spaces.

Security Threats posed to IPv4:-

It has already been discussed that IPv4 does not contain any built-in security mechanism. This feature ultimately exposes this protocol version to malicious security attacks. Durdağı and Buldu (2010) have claimed that sniffing attacks are the most common attacks that are encountered by IPv4. In sniffing attacks, the hackers steal the confidential information of the users that are being transmitted over the network. In this situation, if the confidential and private information is transferred in the form of a plaintext protocol, it results in devastatingly impacting the integrity of the information due to sniffing attacks. Some of the other security attacks that are introduced to IPv4 networks are flooding attacks, application layer attacks, man-in-the-middle attacks, etc. (Durdağı and Buldu, 2010).

However, Wieringa, De Laat, and Visser (2012) had stated that worms, Trojans, and viruses are the prominent attacks that devastatingly affect the security of IPv4. According to Minoli and Kouns (2016), worms, Trojans, and viruses, once entered into a network, have the capability of spreading themselves across different hosts. Viruses and worms are usually transferred from one host to another or from one computer to another in the form of a file. However, Trojans is quite different from both of these types of attacks and seems to be like useful software, but damages the entire system. Luntovskyy and Spillner (2017) had stated that reconnaissance and port scanning are other security threats that are posed to IPv4. In this security attack, the attacker scans the host for getting an access to the available UDP and TCP. In this way, open ports are accessed to introduce a security attack to the specific host. Wieringa, De Laat, and Visser (2012) had regarded

DoS (denial of service) attacks, fragmentation attacks, and MITM (Man-in-the-middle) attacks as the most malicious and dangerous security threats to IPv4. It shows that due to the absence of any built-in security framework, IPv4 is vulnerable to malicious security attacks.

Limitations of IPv4:-

According to Hanumanthappa and Manjaiah (2008), there were some serious problems that resulted in the development of next-generation internet protocol, i.e., IPv6. In particular, the biggest issue is associated with the unavailability of unique addresses to be allocated on to the devices. Some of the other issues of IPv4 that have been demonstrated by Hanumanthappa and Manjaiah (2008) include increasing the size of the routing tables, inefficient packet sizes, and inflexibility of the fixed length headers for new functions. Aluko, Olusanya, Oloyede, and Ebisin (2014) had also highlighted some limitations of IPv4 that are mainly related to addressing configuration and service quality, security, and scarcity of

addresses. However, Shah (2013) had claimed that the exhaustion of IP address is the prominent issue in IPv4. Though, the structure of IPv4 is based on 32-bit address spaces, which has the capacity of offering approximately 4.3 billion unique addresses. Nonetheless, the rapid technological advancements and increased adoption of networking devices had resulted in an unexpected situation. In particular, the dramatic increase in internet users had caused scarcity of unique IP addresses and it is expected that in the upcoming years it would result in the complete exhaustion of address space. Besides the dramatic increase in networking devices, it is also found that *Internet Assigned Numbers Authority* (IANA) has registered a large number of IP addresses for special or local uses. This feature has also resulted in the exhaustion of address spaces in IPv4.

Another limitation of IPv4, as highlighted by Hanumanthappa and Manjaiah (2008); Aluko, Olusanya, Oloyede, and Ebisin (2014); Shah (2013) is related to large-sized routing tables. Since each network needs to have separate and unique routing table entry so if any network includes more hosts than the specific class it results in the need of moving up to the subsequent class or having two IP addresses of the similar class. It is important to note that besides the growing routing tables and inefficient allocation of addresses, the process of routing is also complex in IPv4. Shah (2013) had stated that another prominent aspect that could be considered as the biggest limitation of IPv4 is security. In the contemporary era, organisations have become cautious about the security of their confidential information. However, in IPv4, security is optional, which is regarded as the biggest limitation of this protocol version. Momtaz and Swanson (2015) had affirmed that during the development of IPv4 the only motive of the inventors was to develop such protocol that could facilitate communication. The security feature (i.e., IPSec, authentication) was added into this protocol, after a long time of its development. It shows that security is not built-in on the IPv4 infrastructure. Apart from it, QoS (Quality of Service) is another prominent factor that is deployed and considered as a type of service field that is usually present in its header. Shah (2013) has suggested that besides security, large sized routing tables, and exhaustion of address spaces, there are some other features that are required in IPv4. These include the accommodation of plug and play or auto-configuration capabilities as well as the improved capabilities of multicasting.

Tavakoli Momtaz and Swanson (2015) had stated that configuration of the address is impossible to be managed in IPv4. There are mainly two methods that are often used for the allocation of IP addresses. These include the utilisation of DHCP server, which needs additional cost. On the other hand, the second method is to allocate unique IP to each user and ask them to specifically use those addresses to their devices. This procedure is found to be tough for the users. Momtaz and Swanson (2015) have stated that mobility-related issues are also associated with IPv4. In particular, IPv4 requires the nodes to make use of different addresses for different networks. Such practices result in affecting the network performance because of sudden connection drops that are due to frequent switching of networks.

Internet Protocol Version 6:-

Momtaz and Swanson (2015) have established that after observing the limitations of IPv4, IPv6 was developed. IPv6 is an acronym of internet protocol version 6 as is recognised as a next generation internet protocol. According to Ali (2012), IP next generation (Ipng) is the expected to serve the networking needs of the virtual world. Similar to IPv4, this internet protocol also offers end-to-end transmission of datagrams, across numerous IP networks. One of the characteristics of IPv6 is that it is based on 126-bit address space that would remarkably contribute in fulfilling the increasing need of address space. In other words, it can be affirmed that IPv6 would allow a number of users and devices on the internet to use the unique address. It would also increase flexibility in the allocation of addresses while increasing the routing efficiencies. Most importantly, it would completely eradicate the need of NAT (Network Address Translation) that was used for alleviating the exhaustion of IPv4 address space.

According to Abdullahi and Mahadevan (2010), it is anticipated that IPv6 would take over the current position of IPv4, after its complete exhaustion. It is due to the fact that it posses a number of exclusive features including higher scalability of the network, improved flexibility, etc. IPv6 also facilitates the process of end-to-end communication without having the need of utilising other features, like NAT, etc. Shah (2013) had also established that IPv6 is specifically developed for the resolution of IPv4 issues. Some additional features have been added in the pre-existing architecture to retain the advantageous elements of IPv4; thereby, achieving higher operational efficiencies. It is established that the applications, based on IPv6 posses the capability of providing improved performance and higher efficiency, in terms of latency and bandwidth (Bi, Wu, and Leng, 2007).

Johansson (2016) had presented the same idea by claiming that IPv6 is an improved version of IPv4 and this enhancement is beyond the address spaces. IPv6 makes use of multicast and unicast addresses, similar to IPv4; however, it also utilises any-cast address. This can be considered as one of the greatest features that guarantee timely availability of the network. This feature ultimately eradicates the need of using extra protocols for the management of virtual addresses. Besides that, Johansson (2016) had also highlighted that as compared to IPv4 the next generation internet protocol version is less complex and offers efficient and more improved routing capabilities to the network. While demonstrating the objective of developing IPv6, Aluko, Olusanya, Oloyede, and Ebisin (2014) had contended that the dramatic internet growth and increased networking devices have played a substantial role in creating the need for expanding address spaces on IPs. IPv6 utilises 128-bit addresses that would provide address space of approximately 3.4x1038 addresses; thereby, it is expected that it would adequately satisfy the networking needs of the internet-driven world.

Bons and Weigand (2011) had claimed that IPv6 has not just resolved the issue of address space, but it has also played a remarkable role in restoring end-to-end internet transparency. The greatest feature that IPv6 is expected to offer to the companies is the enforcement of regional and geographic addressing. This feature would help the companies in having common prefixes on the basis of their geographical locations as well as their network providers. In short, IPv6 would resolve the current issues of the organisations by ensuring terminal mobility, automatic router and terminal configuration, end-to-end and highly protected accessibility for P2P applications, and unlimited addressing space. Abdullahi and Mahadevan (2010) had also stated that strong security and mobility mechanisms are the prominent features of IPv6. IPv6 has built-in IPsec facilities, unlike IPv4, that protects the network from unintended security risks and vulnerabilities. According to Aluko, Olusanya, Oloyede, and Ebisin (2014), IPv6 has integrated IPsec that is based on cryptographic security techniques. These techniques robustly secure the integrity, authenticity, and confidentiality of the network. Besides that, Abdullahi and Mahadevan (2010) had underlined another feature that makes IPv6 better than IPv4, i.e., the simplicity of the header. This feature plays an imperative role in improving the flow of traffic, i.e., no checksums and broadcasting are needed for determining traffic flows; thereby, resulting in better forwarding and performance of the network, at scalable rates.

Security Threats posed to IPv6:-

Despite having built-in security mechanism (i.e., IPSec) IPv6 is vulnerable to the security threats. According to Durdağı and Buldu (2010) reconnaissance attacks severely threatens the security of IPv6. In this attack, the hacker collects important information from the network of the victim and uses it for performing malicious activities. It is found that reconnaissance attack is performed by using different active methods, like passive data mining techniques and scanning techniques. However, Sotillo (2006) had contended that IPv6 is also prone to encounter dual-stack related issues. IPv6-IPv4 dual stacks would surely result in increasing the risks and vulnerabilities related to the security of the network, mainly due to the similar infrastructures of IPv4 and IPv6. As per the specification of IPv6 protocol, all related nodes should have the ability to process the routing headers. However, routing headers can also be utilised to avert access control initiatives on the basis of destination addresses. It is found that such behaviour usually results in the occurrence of security-related incidents. It is possible that the intruder tries to transmit packets of data to the publically accessible addressing along with the forbidden address, contained in a routing header.

Such practices result in leading the host (that is publically accessible) to transfer the data packet to the destination; thereby, result in DoS attacks or spoofing attacks. Shah and Parvez (2015) had supported the idea by presenting the elaboration of the security attacks that are often encountered by IPv6. The issues that were explained by theresearcher included firewall evasion by fragmentation, header manipulation, smurf attack (broadcast amplification attack), host initialisation attack, and reconnaissance attack. The prevalence of these attacks in IPv6 was also acknowledged by a number of researchers including Ullrich et al (2014); Durdağı and Buldu (2010); Choudhary (2009); Sabir, Fahiem, and Mian (2009); Dawood (2012); Caicedo, Joshi, and Tuladhar (2009).

Benefits of IPv6 over IPv4:-

According to Ali (2012), along with considerably huge address space, internet service providers will be able to easily allocate the addresses to the users. It is a fact that NAT is helping the service providers in coping with the issues, related to address space exhaustion, but it is not effective for several internet applications like DNS, NFS, group conferencing, etc. IPv6 removes the need of NAT while providing improved services to the internet users in terms of higher flexibility, reliability, and strong connectivity. Yadav, Abad, Shah, and Kaul (2012) had also categorised the benefits of IPv6 into three types, i.e., no need for broadcasting features, strong security, and increased mobility. AbuAli, Shayeb, Batiha, and Aliudos (2010) have stated that IPv6 is one of the greatest initiatives towards re-establishing end-to-end traffic and transparency across the internet.

Ali (2012) had presented an idea that IPv6 plays an indispensable role in minimising the total time that is required for the management and configuration of the systems. The exclusive features of IPv6 support auto-configuration that result in the creation of unique and secured IP addresses, specifically through the combination of provided prefix and LAN MAC address; thereby, reducing the need of DHCP.

Babatunde and Al-Debagy (2014) had outlined some of the benefits of IPv6 including improved support for mobile computing and networking devices, expansion of multicast addresses, providing plug-and-play features, auto-configuration, strong security that is based on IPSec, reduced dependency over NAT (network address translation), hierarchical architecture of the network, and huge address space.

Comparing Internet Protocol Version 4 with Internet Protocol Version 6:-

According to Hanumanthappa and Manjaiah (2008), IPv4 and IPv6 possess similar basic framework; however, they are different in several perspectives. In the context of addressing, Momtaz and Swanson (2015) had established that the most prominent difference that is present in IPv4 and IPv6 is associated with their addresses. The address of IPv4 is based on 32 bits; on the other hand, IPv6 possess 128 bits. It is also important to note that in IPv6, the total number of bits is equally divided among the host address and network address. It means that 64 bits are allocated for host address and 64 bits are allocated for the network address. Contrary to IPv4, IPv6 offers clear routing and addressing another difference amid IPv4 and IPv6, which is related to hierarchical addressing. According to the researcher, IPv4 makes use of three addresses, i.e., multi cast, broad case, and unicast addresses. In contrast, IPv6 also uses three types of addresses, but are different from IPv4, i.e., multicast, unicast, and any-cast address. It shows that the only difference amid both of this protocol version is the introduction of any-cast address, which facilitates multiple nodes to be assigned the similar any-cast address. The application of the any-cast address is found in the creation of mirror websites that could be accessed at any geographical location, by using the similar any-cast address.

According to Ahmed (2006), in IPv4 the fragmentation is carried out by both the sending host as well as by the routers. Contrarily, in IPv6 it is only performed by the sending host and not by the routers. Apart from that, in the context of security, Ahmed (2006) had outlined that in IPv4 IPSec is optional. On the other hand, in the case of IPv6, it is mandatorily required for the protection of the network from security-related incidents. The brief yet insightful comparison of IPv4 and IPv6 is provided in the below-provided table 1.

Table 1:- IPv4 and IPv6 Comparison (Ahmed, 2006; Momtaz and Swanson, 2015)

Internet Protocol	**Internet Protocol**
Version 4	**Version 6**
Destination and source	Destination and source
addresses are 4 bytes	addresses are 16 bytes
(32 bits) in length.	(128 bits) in length.
Mandatory to be	No requirement od DHCP
configured through	or manual configuration.
DHCP or manually.	
Options are included in	IPv6 extension headers
the header.	are there to receive
	optional data.
The checksum is	No checksum is included
included in the header.	in the header.
IPSec (security) is not	IPSec (security) is not
mandatory.	optional.
Broadcast addresses are	IPv6 does not include any
utilised for the sake of	broadcast address.
transferring traffic to	
the nodes that are	
present on a subnet.	
The local subnet group	The replacement of IGMP
membership is used for	is performed with MLD
the management of	(multicast listener
IGMP (internet group	discovery) messages.
management protocol).	

Factors Hindering the Transition from IPv4 to IPv6:-

Babatunde and Al-Debagy (2014) had established that the migration or transition from IPv4 to IPv6 has been initiated, but the adoption rate is found to be too slow. A number of factors are involved in the slow adoption of IPv6 that mainly include infrastructure issues, financial issues, tunnelling issues, and security issues. Babatunde and Al-Debagy (2014) had stated that IPv6 adoption is greatly hindered due to the infrastructure issues. A number of technologies and protocols are needed to be redesigned for the sake of supporting IPv6. These include TCP/IP, ARP, BGP, RIP, OSPF, and DHCP. On the other hand, Dey and Shilpa (2011) had identified tunnelling issues are the ones that are hindering IPv6 adoption. The researcher has stated that without any transformation in applications, the next generation internet protocol can be utilised in a pre-existing network, by using tunnelling techniques. It would act as a medium between IPv6 and IPv4. However, tunnelling is a time-consuming process and it has extremely minimal throughput. Babatunde and Al-Debagy (2014) had recognised the need of additional financial resources as the limiting factor of IPv6 adoption. According to the researcher, the transition from IPv4 to IPv6 needs the companies and enterprises to invest their capital cost in the account of routers, switches, employee training etc. that restricts them to switch from IPv4 to IPv6. The vague and unclear security mechanism of IPv6, due to limited testing, is also restricting the companies to move from IPv4.

Kaur (2015) had claimed that the lack of required experiences and skills are limiting the organisations to assimilate and adopt IPv6. Grossetete, Popoviciu, and Wettling (2004) have presented an idea that there is a limited availability of IPV6 SME (subject matter experts). Hovav and Schuff (2005) had also supported the idea by claiming that the lack of IPv6 skilled employees may restrict the organisation towards fully assimilating and adopting IPv6. Moreover, the study of Dell (2010) has presented an idea that the wrong perception of the organisations towards IPv6 is also delayed IPv6 adoption. Some of the organisations perceive that IPv6 is immature and instable. Bons and Weigand (2011) have also stated in this regard that perceived immaturity of IPv6 is the biggest hurdle in its adoption as most of the organisations consider this technology as the biggest risk to their security. Dell, Kwong, and Liu (2008) have mentioned that the prominent barrier in IPv6 adoption is the reluctance of the organisations towards becoming an early adopter. Organisations usually find it better to learn from the experience of other organisations so as to save them from potential risks.

Hovav and Popoviciu (2009) have stated that cost is the biggest barrier to the assimilation and adoption of IPv6. Organisations tend to avoid the cost that is required for bringing additional hardware, employee training, etc. Grossetete, Popoviciu, and Wettling (2004) have claimed that any investment that is related to IPv6 is considered as cost and organisations prefer to avoid this cost. Another factor that is responsible for the limited adoption of IPv6 has been presented by Hovav and Popoviciu (2009) i.e., underestimating the power of IPv6. In other words, some companies do not consider IPv6 as the strong and resilient business champion, as compared to other tools and systems. Such perceptions ultimately result in slow-paced adoption of IPv6 and leading the businesses to continue their operations on IPv4. Kaur (2015) has affirmed that cultural differences also act a barrier to digital infrastructure adoption. Organisations, belonging from specific cultures or countries tend to delay or avoid the adoption of IPv6 because of having the low inclination and knowledge about digital technologies.

Bons and Weigand (2011) have presented an idea that complexity of IPv6 and size of the organisation act as a barrier in IPv6 assimilation. It is found that large-sized companies usually avoid adopting IPv6, as they have to replace a greater number of equipment and applications during the adoption process. On the other hand, small sized organisations usually avoid its adoption because of having minimal financial resources. Gallaher and Rowe (2006) had also emphasized that the size of the organisation act as a barrier in the decision of an organisation to assimilate IPv6. On the other hand, Kaur (2015) had identified that lack of support from senior level management and decision makers also limit IPv6 adoption in organisations. White, Shah, and Cook (2005) had indicated that the over reliance of organisations on workaround technologies is the biggest factors that are hindering IPv6 adoption. These technologies were initially developed for the sake of handling the scarcity of IPv4 addresses; however, despite the development of IPv6, organisations are still relying on it. Some of the prominent technologies include CIDP (classless inter-domain routing), DHCP (dynamic host configuration protocol), and NAT. The analysis of all of these evidences has revealed that IPv6 transition must be carried out gradually so as to cause minimal disturbance to the existing networks. Moreover, organisations also need to be vigilant and cautious during the planning phase, as it requires huge investment and efforts (Mason and Mahindra, 2011; Che and Lewis, 2010).

Security Advantages of IPv6 over IPv4:-

Security advantage of IPv6 over IPv4 can be discussed with the fact that IPsec was not installed primarily in the design, but was developed as an additional feature. In IPv6 networks, IPsec protocol is embedded and is also made mandatory. IPv6 networks maintain simplicity and provide greater security assurance than IPv4 networks (Sharma, 2014, p. 19). IP security is implemented on layer 3 present in the OSI model, and with open standard protocols to provide security for datagram transmission. This method provides encryption and authentication to the packets during data communication, while providing data confidentiality and data integrity (Sharma, 2014, p. 31). The main purpose of introducing IPv6, apart from the increase in a number of addresses was the lack of data protection provided in IPv4.

However, apart from a few changes in IPv6, it is still very familiar to IPv4 with respect to basic transmission mechanisms and above-layer protocols mostly unchanged (Sameeha, 2012, p. 34). In IPv4, the infiltrator has many ways to collect information, since the reconnaissance mechanism of IPv4 is vulnerable. The infiltrator can do ping sweeps by determining the addresses of the organisation, because the number of addresses in IPv4 configuration is limited. Furthermore, the hacker can execute the scanning of the ports to identify reachable or active systems and then use these active ports to determine the versions of operating systems and various applications running on the host and manipulate them. However, in IPv6 the number of addresses is much more than IPv4, which creates a type of barrier to identify the active ports (Sameeha, 2012, p. 34).

The most common issue of IPv4 networks were the spoofing attacks of layer 3 and layer 4, which occurred on a daily basis. Ipv4 networks had difficulties to track denial of service attacks, spams, and worms, due to the sheer bulk of their occurrences. Layer 3 spoofing is difficult for the infiltrator because of the complications in guessing what the return traffic holds, therefore it is not used in interactive attacks. However, layer 4 spoofing is used interactively to change the destination of where the traffic actually came from. Some filtering mechanisms are discussed in various researches, but they are not generally implemented because they require extensive usage (Sameeha, 2012, p. 35). However, IPv6 networks are allocated in a way that filters can be applied on different points in the network. This allows internet service providers to guarantee that at least their own customers are not spoofing externally. address in IPv4 is 32-bit, it is increased to 128-bit in IPv6. Mobility is another drawback of IPv4, if a mobile node changes its location, it will lose the current IP address and it should be established again. In contrast of IPv4, IPv6 enhances mobility. IPv6 allows mobile nodes to change their location without dropping the IP address. The security field (IPsec) in IPv4 is optional and all the responsibility of security belongs to the end nodes which is not safe. IPv6 header contains IPsec field, and it is required. This field is implemented by using AH, ESP and IKE. In IPv4, the configuration of IP is done by either manually or DHCP but IPv6 made configuration easy by using auto configuration. According to the previous considerations, IPv6 protocol will be better as compared to the IPv4 protocol. It has arrived as the next generation Internet Protocol and provides several functionalities to eliminate the limitations of IPv4.

Conclusion:-

In this paper we compared IPv4 and IPv6 in history, address structure, header’s structure, the fields of headers, security, routing protocols, IP address configuration, function of different protocols, etc. IPv4 is the first version of IP which has been used globally. When IPv4 was designed, it was estimated to be used for a long time, but the number of devices which are able to connect network is increasing, so that IPv4 faced some problems. In this study we found the main drawbacks of IPv4 and the major features of IPv6 that eliminates the drawbacks of IPv4. Address shortage is one of the important problems of IP, people use multiple devices like PC, laptop, PDA and phones thus the request for IP addresses is raising thus the number of IPv4 addresses is being a problem in future. IPv6 provides larger address space, the length of

References:-

1. Abdullahi, G. A. and Mahadevan, V. 2010. Why is IPv4 still in Existence?. School of Information Science, Computer and Electrical Engineering
2. Halmstad University, retrieved from, http://www.diva-portal.se/smash/get/diva2:380776/FULLTEXT0 pdf
3. AbuAli, A.N., Shayeb, I.G., Batiha, K. and Aliudos, H.Y., 2010. The Benefits of Using Internet Protocol Version 6(IPV 6). International Review on Computers and Software, 5(6), pp.583-587.
4. Ahmed, M.M., 2006. A Comperative Study on the Performance of IPv4 and IPv6. Independent University, Bangladesh.Akamai. 2017. IPv6 Adoption Visualisation. Akamai. retrieved from, https://www.akamai.com/uk/en/about/our-thinking/state-of-the-internet-report/state-of-the-internet-ipv6-adoption-visualization.jsp
5. Ali, A.N.A., 2012. Comparison study between IPV4 & IPV6. International Journal of Computer Science Issues, 9(3), pp.314-317.
6. Aluko, T.S., Olusanya, O.J., Oloyede, O.E. and Ebisin, A.F., 2014. Comparative Analysis between Internet Protocol Version 4 & 6 (IPv4 and IPv6). International Journal of Scientific & Engineering Research. 5(8).

7. Aluko, T.S., Olusanya, O.J., Oloyede, O.E. and Ebisin, A.F., 2014. Comparative Analysis between Internet Protocol Version 4 & 6 (IPv4 and IPv6). International Journal of Scientific & Engineering Research, Volume 5, Issue 8.
8. Babatunde, O. and Al-Debagy, O., 2014. A comparative review of internet protocol version 4 (ipv4) and internet protocol version 6 (ipv6). arXiv preprint arXiv:1407.2717.
9. Bernard, H.R. and Bernard, H.R., 2012. Social research methods: Qualitative and quantitative approaches. Sage.
10. Bi, J., Wu, J. and Leng, X., 2007. IPv4/IPv6 transition technologies and univer6 architecture. International Journal of Computer Science and Network Security, 7(1), pp.232-243.
11. Bilski, T., 2011. From IPv4 to IPv6–data security in the transition phase. In Proc. 7th Int. Conf. Netw. Serv. ICNS 2011 (pp. 66-72).
12. Bons, E. and Weigand, H., 2011. IPv6: Drivers and Barriers for Adopting. Department of Information Management, Tilburg University.
13. Caicedo, C.E., Joshi, J.B. and Tuladhar, S.R., 2009. IPv6 security challenges. Computer, 42(2), pp.36-42.
14. Çalışkan, E., 2014. IPv6 transition and security threat report. NATO CCD COE, Tallinn.
15. Che, X. and Lewis, D., 2010. Ipv6: current deployment and migration status. International Journal of Research and Reviews in Computer Science (IJRRCS), 1(2), pp.22-29.
16. Choudhary, A.R., 2009, November. In-depth analysis of IPv6 security posture. In Collaborative Computing: Networking, Applications and Worksharing, 2009. CollaborateCom 2009. 5th International Conference on (pp. 1-7). IEEE.
17. Dawood, H., 2012. IPv6 security vulnerabilities. International Journal of Information Security Science, 1(4), pp.100-105.
18. Dell, P., 2010. Two economic perspectives on the IPv6 transition. info, 12(4), pp.3-14.
19. Dell, P., Kwong, C. and Liu, Y., 2008. Some reflections on IPv6 adoption in Australia. info, 10(3), pp.3-9.
20. Dey, S. and Shilpa, N. 2011. Issues in IPv4 to IPv6 Migration. International Journal of Computer Applications in Engineering Sciences (IJCAES). 1 (1).
21. Doshi, J., Chaoua, R., Kumar, S. and Mallya, S., 2012. A Comparative Study of IPv4/IPv6 Co-existence Technologies. University of Colorado, Boulder.
22. Durdağı, E. and Buldu, A., 2010. IPV4/IPV6 security and threat comparisons. Procedia-Social and Behavioral Sciences, 2(2), pp.5285-5291.
23. Gallaher, M.P. and Rowe, B.R., 2006. The costs and benefits of transferring technology
24. infrastructures underlying complex standards: the case of IPv6. The Journal of Technology Transfer, 31(5), pp.519-544.
25. Grossetete, P., Popoviciu, C.P. and Wettling, F., 2004. Global IPv6 strategies: from business analysis to operational planning. Cisco Press.
26. Hanumanthappa, J. and Manjaiah, D.H., 2008. A Study on Comparison and Contrast between IPv6 and IPv4 Feature Sets.
27. Hanumanthappa, J., 2009. IPv6 and IPv4 Threat reviews with Automatic Tunneling and Configuration Tunneling Considerations Transitional Model: A Case Study for University of Mysore Network. arXiv preprint arXiv:0908.0548.
28. Hovav, A. and Popoviciu, C., 2009. Adoption leadership and early planners: Comcast's IP upgrade strategy. Communications of the ACM, 52(7), pp.143-146.
29. Hovav, A. and Schuff, D., 2005. Global Diffusion of the Internet V-The Changing Dynamic of the Internet: Early and Late Adopters of the IPv6 Standard. Communications of the Association for Information Systems, 15(1), p.14.
30. IPv6-test. 2017. IPv6 in Iraq. Ipv6-test.com, retrievde from, http://ipv6-test.com/stats/country/IQ Johansson, E., 2016. Evaluation of prerequisites for an IPv4 to IPv6 transition.
31. Kaur, A., 2015. How is digital infrastructure adopted and assimilated? The IPv6 story (Doctoral dissertation, Auckland University of Technology).
32. Khudhair, H. E. and Mohammed, J. I. 2017. A Prototype and Roadmap for Transition to IPv6 with Performance Evaluation. Research Journal of Applied Sciences, Engineering and Technology. 14(8): 299-309.
33. Kozierok, C.M., 2005. The TCP/IP guide: a comprehensive, illustrated Internet protocols reference. No Starch Press.
34. Luntovskyy, A. and Spillner, J., 2017. Security in Distributed Systems.In Architectural
35. Transformations in Network Services and Distributed Systems (pp. 247-308). Springer Fachmedien Wiesbaden.
36. Mason, A. and Mahindra, T., 2011. Report for IDA: IPv6 Adoption Guide for Singapore.

37. Minoli, D. and Kouns, J., 2016. Security in an IPv6 environment. CRC Press.
38. Oki, E., Rojas-Cessa, R. and Vogt, C., 2012. Advanced internet protocols, services, and applications. John Wiley & Sons.
39. Sabir, M.R., Fahiem, M.A. and Mian, M.S., 2009, January. An overview of IPv4 to IPv6
40. transition and security issues. In Communications and Mobile Computing, 2009. CMC'09. WRI International Conference on (Vol. 3, pp. 636-639). IEEE.
41. Shah, H., 2013. Comparing TCP-IPv4/TCP-IPv6
42. Network Performance. University of Missouri- Columbia.
43. Shah, J. and Parvez, J., 2015. Security Issues in Next Generation IP and Migration Networks. IOSR Journal of Computer Engineering, 17(1), pp.13-18.
44. Sharma, P. and Singla, R. M. 2016. A Detail Comparative Review on IPv4/IPv6 Dual Stack Co-existence Techniques. International Journal of Innovative Research in Computer and Communication Engineering. 4(4).
45. Sotillo, S., 2006. Ipv6 security issues. Scanning.
46. Tavakoli Momtaz, M. and Swanson, M., 2015. IPv4 to IPv6 Transition and Security.
47. Ullrich, J., Krombholz, K., Hobel, H., Dabrowski, A. and Weippl, E.R., 2014, August. IPv6 Security: Attacks and Countermeasures in a Nutshell. In WOOT.
48. White, G.L., Shah, J.R. and Cook, J.R., 2005. Internet Technology in 2010: The Issue of IPv6 Adoption in the USA. Journal of International Technology and Information Management, 14(3), p.5.
49. Wieringa, F., de Laat, C. and Visser, M.R., 2012. IPV6 risks and vulnerabilities Project Report.
50. Wu, P., Cui, Y., Wu, J., Liu, J. and Metz, C., 2013. Transition from IPv4 to IPv6: A state-of-the-art survey. IEEE Communications Surveys & Tutorials, 15(3), pp.1407-1424.
51. Yadav, A., Abad, P., Shah, H. and Kaul, A., 2012. IPv6 protocol adoption in the US: Why is it so slow?. Capstone paper, University of Colorado, May, 4.
52. Bäckström, I., 2009. Performance measurement of IP networks using the two-way active measurement protocol. Skolan för datavetenskap och kommunikation, Kungliga Tekniska högskolan.
53. Clark, A. and Claise, B., 2011. Guidelines for Considering New Performance Metric Development
54. Dawood, H., 2012. IPv6 security vulnerabilities. International Journal of Information Security Science, 1(4), pp.100-105.
55. Dhall, H., Dhall, D., Batra, S. and Rani, P., 2012, January. Implementation of IPSec protocol. In Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on (pp. 176-178). IEEE.
56. Gilad, Y. and Herzberg, A., 2013, September. Plug-and-play IP security. In European Symposium on Research in Computer Security (p. 257). Springer, Berlin, Heidelberg.
57. IBM. 2012. IPv6 Introduction and Configuration. International Technical Support Organization, pp. 15-17
58. Kocak, C. and Zaim, K., 2017, May. Performance measurement of IP networks using Two-Way Active Measurement Protocol. In Information Technology (ICIT), 2017 8th International Conference on p. 249. IEEE.
59. Malik, R. and Syal, R., 2010. Performance analysis of IP security VPN. International Journal of Computer Applications, 8(4), p.6
60. Sameeha, M.A.A., 2012. Look at IPV6 Security advantages over IPV4. Network and Complex Systems, ISSN, pp. 34-35
61. Sharma, G., 2014. Implementation of IPv6. Rovaniemi University Of Applied Sciences School Of Technology. pp. 19, 31-32
62. Sotillo, S., 2006. Ipv6 security issues. Scanning, p.4
63. Soumyalatha, N., Ambhati, R.K. and Kounte, M.R., 2013, August. Performance evaluation of ip wireless networks using two-way active measurement protocol. In Advances in Computing, Communications and Informatics (ICACCI), 2013 International Conference on p. 1896 IEEE.
64. Stallings, W., 2011. Cryptography and network security: principles and practices. Pearson Education India.