Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 1, January 2015, pg.490 – 496

SURVEY ARTICLE

Next Generation Internet Protocol A Survey on Current Issues and Migration

Junaid Latief Shah

Dept of Computer Science, University of Kashmir, India

***Abstract*— The next-generation Internet Protocol (IPng) also known as IPv6, has been developed by the Internet Engineering Task Force (IETF) to replace the current Internet Protocol version 4.After being in use for almost three decades, the most compelling problem facing the IP Internet today is IP address depletion. The IPv4 extensions such as Sub netting, NAT, CIDR etc were short-term antidote solutions. Motivated by the perceived IP Address shortage crisis and needs of the modern internet, the idea of IPv6 was conceived in 1995 as a panacea to all the problems currently faced by IPv4. IPv6, the next version of the protocol, has provided trillions of addresses which are potentially inexhaustible. The protocol also establishes new features like SLAAC, Neighbor Discovery and improvements in QoS, Security, and Routing. To enable the integration of IPv6 into current operational networks, several transition mechanisms have been proposed by the IETF IPng Transition Working Group which includes Dual Stack, Tunneling, and Translation. The paper focuses to compare and analyze IPv4 and IPv6 networks, study their characteristics and header formats. The paper addresses the issues that are prevalent in IPv4 and explains the reasons for seamless migration to IPv6.The paper also discusses about established migration techniques and highlights their drawbacks from security and performance point of view.**

Keywords - IPv4, IPv6, SLAAC, QoS, IPng, IETF

I. INTRODUCTION

Internet is a network of networks, joining many government, university and private computers together and providing an infrastructure for the use of E-mail, bulletin boards, file archives, hypertext documents, databases and other computational resources. Looking at history, the work on internet began as early as in 1960's with US Department of Defense awarding contracts for packet network systems, including the development of the Advanced Research Projects Agency Network (ARPANET) which would become the first network to use the Internet Protocol [1].ARPANET was used as a means for sharing of resources and was one of the world's first operational packet switching networks; the first network to implement TCP/IP. The TCP/IP protocol was first proposed in 1974 in a research paper by internet pioneer's Vinton G .Cerf and Robert E. Kahn [5].Since the mid-1990s, the Internet has had a revolutionary impact on culture and commerce, including the rise of near-instant communication by electronic mail, instant messaging, voice over Internet Protocol (VoIP) telephone calls, two-way interactive video calls and the World Wide Web with its discussion forums, blogs, social networking, and online shopping sites. The rapid explosion of the internet and existence of high speed wireless and broadband networks have contributed towards depletion of current version of Internet Protocol IPv4.The IPv4 protocol that was introduced more than three decades ago with approximately an address space of 4 billion cannot cater to the needs of modern internet[3]. The address depletion has posed a serious problem on the growth of internetworks. Some temporary solutions were offered, such as NAT (Network Address Translator) or CIDR (Classless Inter Domain Routing), however work began on a new Internet Protocol, namely IPv6. The main reason for a new version of the Internet Protocol was to increase the address space. IPv6 was designed with a 128 bit address scheme, enough to assign every entity on the surface of the earth with a unique address. Furthermore, the only kind of traffic that existed on the internet was emails, file transfers or remote login. This

kind of traffic was very flexible regardless of congestion and the network conditions [11]. On the other hand, real time traffic requires a certain level of guaranteed performance, which if not met; the application does not have the same usefulness. IPv6 was designed for efficiently supporting both conventional and real time traffic. The goals of IPv6 were to support scalability, security, and multimedia transmissions. Firstly, the address space is increased from 32 bits to 128 bits. Unlike IPv4, IPSec support is mandatory in the IPv6 header. QoS handling by routers is supported by the Flow Label and Traffic class field in the IPv6 packet header. Fragmentation is done only by the source hosts. The IPv6 header does not include a checksum and has no options included in the header, but rather introduces extension headers. Finally, IPv6 requires no manual configuration or DHCP (Dynamic Host Configuration Protocol), which will become important as the number of nodes increases. Overall, IPv6 was carefully thought out and was designed with future applications in mind.

II. BACKGROUND

For a node to be globally and uniquely identifiable, it requires an IP address [1]. Depletion of address space and security vulnerabilities was the main motivation behind the deployment of IPv6. The Internet Protocol version 4 (IPv4) is the delivery mechanism used by the TCP/IP protocols. It is an unreliable, best-effort, and connectionless packet delivery protocol. Best-effort means that datagram's may be lost, arrive out of order, and even be duplicated [8]. IP assumes that higher layer protocols (e.g., TCP) will address these anomalies. There are two prevalent notations to represent an IPv4 address-the binary notation and dotted decimal notation. IP addresses are represented by a 32-bit unsigned binary value, which is usually expressed in a dotted decimal format (e.g., 193.205.80.1) because the numeric form (e.g., 193205801) is hard to read. An easier way to remember IP addresses is by assigning to them a name (e.g., www.google.com), which is resolved through the Domain Name System (DNS).IPv4 uses 32 bit numbers which means that the address space is composed of 2^{32} or 4,294,967,296(more than 4 billion) addresses. This means theoretically if there were no restrictions more than 4 billion devices would connect to the internet [3]. However all of these addresses have been exhausted as of now with no more address space left now. The main reasons for such a large demand for addresses have been due to:

- Growth of large scale Mobile devices.
- Always-on connections like gateway devices (routers, broadband modems) which are rarely turned off.
- Growth of Users: In 1990, only a small fraction of households around the world had Internet connectivity. Just 15 years later, almost half of them had persistent broadband connections and it's still growing.
- Inefficient address use: Organizations that obtained IP addresses in the 1980s were often allocated far more addresses than they actually required, because the initial class full network allocation method was inadequate to reflect reasonable usage. For example, large companies or universities were assigned class A address blocks with over 16 million IPv4 addresses each, because the next smaller allocation unit, a class B block with 65536 addresses, was too small for their intended deployments.

The main difference in the packet layout between IPv4 and IPv6 is that IPv4 has a 20 byte header while IPv6 has a 40 byte header [3]. Although the address space in IPv6 is four times the size of its counterpart, IPv6 has reduced the number of required fields and made them optional as extension headers. Since the Ethernet MTU size is 1514 bytes, the additional 20 bytes of header information only incur an additional 1.3% overhead; an additional 20 bytes of header information when an IPv6 packet is encapsulated in an IPv4 packet raises the overall overhead to 2.6%. In theory, this performance overhead between these two protocols is minimal.IPv4 Datagram as shown in figure 1 is basically composed of two parts-header and data. Header contains information essential to routing of packet where as data part contains the actual payload.

The various fields in the header are as follows:

1. ***Version :*** 4 bit field defines the version of IP protocol(whether 4 or 6)
2. ***Header Length:*** 4 bit field defines the length of total header in 4 byte words. Header length is variable between 20-60 bytes. When there are no options, the header length is 20 bytes and its value is 5.When the options are present, the max value in this field is 15.
3. ***Service***: 8 bit field indicating type of service required by datagram (whether to prioritize throughput, reliability, lower cost and delay).

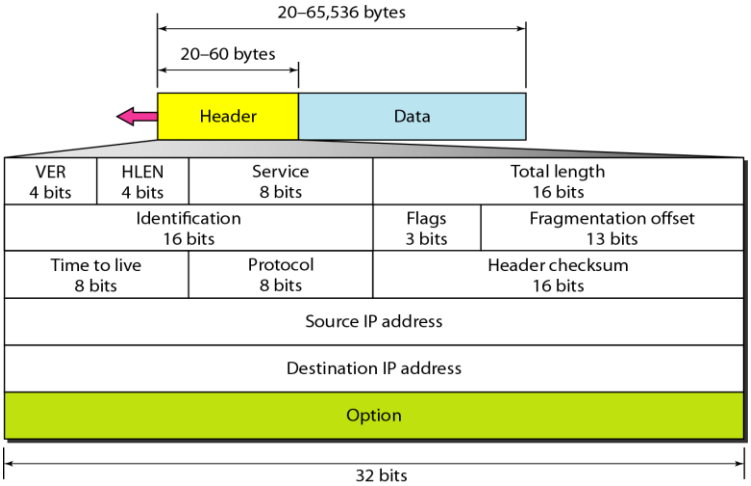

Fig 1 IPv4 Header

4. ***Total Length*** *:* 16 bit field indicating the total length(header+data)
5. ***Identification****:* 16 bits: used in fragmentation (It identifies to which datagram, the newly arrived fragment belongs. All fragments have the same identification value as the original datagram)
6. ***Flags****:* 3 bit-used in fragmentation (First bit is reserved. Second bit is called do not fragment bit. If the value is 1, the machine must not fragment the datagram. If its zero the datagram can be fragmented as necessary. Third bit is called more fragment bit. If its value is 1.It means that datagram is not the last fragment, there are more fragments after this one. If its value is zero, this is the last or only fragment)
7. ***Fragmentation Offset*** *:* 13 bits used in fragmentation(shows relative position of this packet w.r.t whole datagram)
8. ***Time to live***: 8 Bits: Maximum lifetime of packet. Its value is decremented at every hop the packet visits. When it hits zero, the packet is discarded.
9. ***Protocol***: 8 Bits: Indicating higher level protocol that uses the services of IPv4.An IPv4 datagram can encapsulate data from several higher level protocols such as TCP, UDP and other higher layer protocols. The field specifies the final destination protocol to which the data gram is submitted.
10. ***Header Checksum***:16 bits: The value of header checksum
11. ***Source IP*** : 32 bits
12. ***Destination IP*** : 32 bits

To address the problem of address depletion, the researchers proposed the following solutions.

- ***Sub netting***

A sub network, or subnet, is a logical, visible subdivision of an IP network. The practice of dividing a network into two or more networks is called sub netting. Computers that belong to a subnet are addressed with a common and identical most-significant bit-group in their IP address. Sub netting provides a means of allocating a part of the host address space to network addresses, which lets you have more networks. The part of the host address space allocated to new network addresses is known as the subnet number.

- ***CIDR***

CIDR or Classless Inter Domain Routing provides the flexibility of borrowing bits of Host part of the IP address and using them in network part known as Subnet Id. By using sub netting, one single Class A IP address can be used to have smaller sub-networks which provides better network management capabilities.

- ***NAT***

Network Address Translation (NAT) is the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. Network Address Translation (NAT) is a way to map an entire network (or networks) to a single IP address. NAT is necessary when the number of IP addresses assigned to you by your Internet Service Provider is less than the total number of computers that you wish to provide Internet access for.

III. INTERNET PROTOCOL NEXT GENERATION IPV6

IPv6 is the next generation Internet Protocol.IPv6 address is composed of 128 bits which is four times larger than an address in IPv4.i.e. $2^{128} \approx$ 340 trillion trillion trillion addresses are possible. Each IPv6 packet is composed of a mandatory base header followed by the payload. The payload consists of two parts: optional

extension headers and data from an upper layer. The base header occupies 40 bytes, whereas the extension headers and data from the upper layer contain up to 65,535 bytes of information. The figure 2 below shows the IPv6 header.

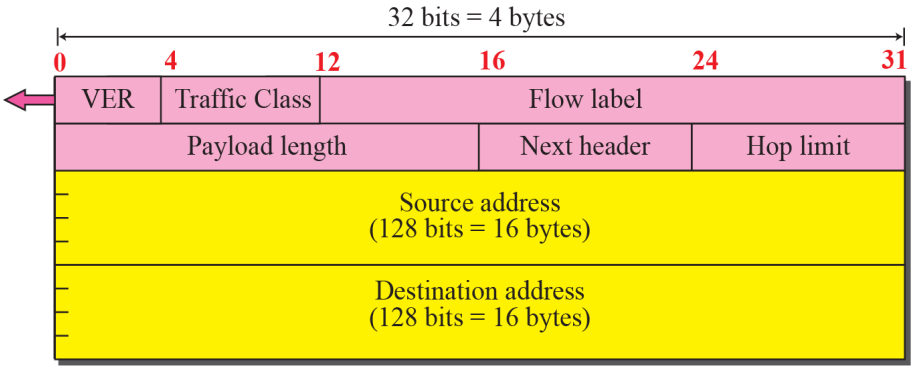

Fig 2 IPv6 Header

1. ***Version****:* 4 bits are used to indicate the version of IP and is set to 6
2. ***Traffic Class*** – Indicates the class or priority of the IPv6 packet. The size of this field is 8 bits. The Traffic Class field provides similar functionality to the IPv4 Type of Service field.
3. ***Flow Label*** – Indicates that this packet belongs to a specific sequence of packets between a source and destination, requiring special handling by intermediate IPv6 routers. The size of this field is 20 bits. The Flow Label is used for non-default quality of service connections, such as those needed by real-time data (voice and video). For default router handling, the Flow Label is set to 0. There can be multiple flows between a source and destination, as distinguished by separate non-zero Flow Labels.
4. ***Payload Length*** – Indicates the length of the IPv6 payload. The size of this field is 16 bits. With 16 bits, an IPv6 payload of up to 65,535 bytes can be indicated.
5. ***Next Header*** – Indicates either the first extension header (if present) or the protocol in the upper layer PDU (such as TCP, UDP, or ICMPv6). The size of this field is 8 bits.
6. ***Hop Limit*** – Indicates the maximum number of links over which the IPv6 packet can travel before being discarded. The size of this field is 8 bits. The Hop Limit is similar to the IPv4 TTL field
7. ***Source Address*** –Stores the IPv6 address of the originating host. The size of this field is 128 bits.
8. ***Destination Address*** – Stores the IPv6 address of the current destination host. The size of this field is 128 bits. In most cases the Destination Address is set to the final destination address. However, if a Routing extension header is present, the Destination Address might be set to the next router interface in the source route list.

❖ IPv6 Advantages

The following list provides a summary of the most important advantages between IPv4 and IPv6 [7], showing some of the ways that the IPv6 team met the design goals for the new protocol.

- ***Address space***

Since IPv6 address is composed of 128 bits which is four times larger than an address in IPv4,around 2^{128} addresses are possible i.e. about 340 trillion trillion trillion addresses are possible overcoming the address depletion problem.

- ***End-to-End Connectivity***

Since IPv4 utilizes NAT and NAT interferes with QoS and IPSec, this concept has been removed from IPv6 ensuring end to end connectivity.

- ***Ease of configuration***

Provision for Plug and Play support for network devices (through IPv6 SLAAC) removing the need for manual configuration or DHCP

- ***Security concerns***

Inbuilt support for IPSec in the form of extension headers.

- ***QoS***

IPv6 header has Flow Label and Traffic class Field. Allows for all packets of a certain 'flow' to be handled the same way. Flow: A sequence of packets sent from a particular source to a particular (Unicast or multicast) destination for which the source desires special handling by the intervening routers.

❖ Comparison between IPv4/IPv6

The following points list the comparison between the two protocols IPv4 and IPv6.

1. The Header length is eliminated from IPv6 because the length of the header is fixed in this version. i.e.40 bytes
2. The Type of Service is eliminated from IPv6.The traffic class and flow label fields together take over the function of Type of service field in IPv4.
3. The total length field is eliminated in IPv6 and replaced by the payload length field.
4. The identification, flag, and offset fields are eliminated from the base header in IPv6.They are included in the fragmentation extension header.
5. The TTL field is called hop limit in IPv6.
6. The protocol field is replaced by the next header field.
7. The header checksum is eliminated because the checksum is provided by the upper layer protocols: it is therefore not needed at this level.
8. The options fields in IPv4 are implemented as extension headers in IPv6.

IV. MIGRATION FROM IPV4 TO IPV6

The Transition from IPv4 to IPv6 is inevitable because of lack of IPv4 address space and motivation for new protocol i.e. IPv6 [2]. Because of the huge number of systems on the Internet, the transition from IPv4 to IPv6 cannot happen suddenly. It takes a considerable amount of time before every system in the Internet can move from IPv4 to IPv6. The transition must be smooth to prevent any problems between IPv4 and IPv6 systems. Transition strategies may be dissected into three categories.

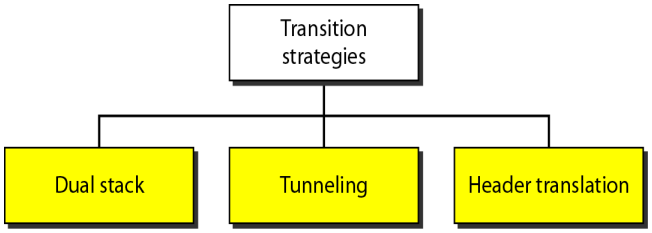

Fig 3 Migration Techniques

A. Dual Stack

In dual stacking, a device runs both protocol stacks: IPv4 and IPv6. Of all the transition methods, this is the most common one. Dual-stack (or *native dual-stack*) refers to simultaneous implementation of IPv4 and IPv6. In this case, all the routers are able to process both protocols. Dual-stack is mentioned in RFC 4213.Although, dual stack is the most preferred implementation because it avoids various complexities and roadblocks associated with tunneling (such as increased security, increased latency and overall management overhead),it's not always possible due to the presence of outdated network infrastructure which may not support IPv6.

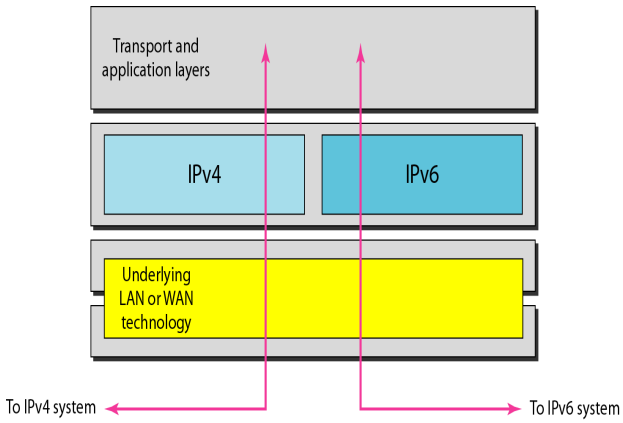

Fig 4 Dual Stack

B. Tunneling

Tunneling is the other mechanism used by IPv4 to communicate with IPv6 networks because all networks do not support dual stack. The IPv6 packets are encapsulated within IPv4 payload and are then transported through IPv4 infrastructure, thus using IPv4 as a transport medium for IPv6.The tunnels are of different categories depending upon the type of system they connect. The most common are Host to Host, Router to Router, Router to Host, Host to Router Tunnels.

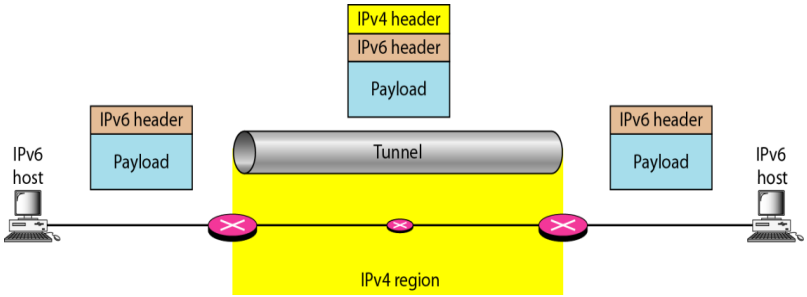

Fig 5 Tunneling

C. Translation

A translator device converting IPv4 to IPv6 headers and vice versa is installed, and communications between IPv4 and IPv6 nodes are enabled via this translator, so to speak, it serves as an "interpreter" between IPv4 and IPv6. It just translates IPv4 packets to IPv6 Packets and vice versa**.**

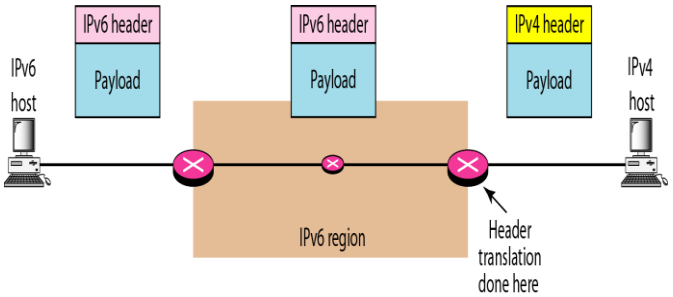

Fig 6 Translation

V. ISSUES WITH MIGRATION

Migrating from IPv4 to IPv6 is a daunting task because the users cannot tolerate downtime of the internet for the purpose of migration and then restart the systems again. Since IPv4 and IPv6 are incompatible, both the protocols need to co-exist for some period of time, till whole migration process takes place. The migration period itself will not be secure and there are performance issues [11] in the migration which are listed below.

1. Encapsulation/Decapsulation Delays in Tunneling

Using tunneling, the networks suffer encapsulation and decapsulation delays for data packets. These delays are significant and introduce performance bottlenecks in the transmission of data packets. This will result in slow network performance.

2. Computational Power In Dual Stack and Cost

The cost of introducing dual stack enabled devices in the network is very high. These devices require high end processors and significant computation power which may not be feasible for some ISP's.Dual Stack hosts need to process two protocol stacks demanding rapid fast processing power.

3. Loss of Information in Translation/Security Leak

During the translation of packet headers, a lot of information is dropped and gets lost. This information may also be vital for the data packet. This introduces security leaks in the data packet.

VI. CONCLUSIONS

As summarized in this paper, IPv6 has both advantages as well as drawbacks as compared to IPv4 from the performance and security point of view. The paper carried out an extensive survey over IPv4 and IPv6 header structure and brought forward the issues and motivation for embracing the next version of the Internet Protocol IPv6. The paper also discussed about current migration techniques and tried to highlight their weaknesses. These techniques demand optimization in hardware and software like enhancing router software, operating systems etc. The similarities in two protocols help in implementing strong security policies to secure IPv6 and migration networks. It is expected that IPv4 and IPv6 hosts will need to coexist for a substantial time during the steady migration from IPv4 to IPv6, and the development of transition strategies, tools, and mechanisms has been part of the basic IPv6 design from the start.

REFERENCES

[1] Wikipedia contributors. "Internet." *Wikipedia, The Free Encyclopedia*. Wikipedia, the Free Encyclopedia, 27 Jan. 2015. Web

[2] Shah, J. L., & Parvez, J. (2014, July). An examination of next generation IP migration techniques: Constraints and evaluation. In *Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on* (pp. 776-781). IEEE.

[3] Shah, Junaid Latief and Javed Parvez. "Migration from IPv4 to IPv6: Security Issues and Deployment Challenges." *International Journal of Advanced Research in Computer Science and Software Engineering* 4.1 (2014):373-76.

[4] Shah, J. L., & Parvez, J. (2014, July). Performance evaluation of applications in manual 6in4 tunneling and native IPv6/IPv4 environments. In *Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on* (pp. 782-786). IEEE.

[5] Cerf, Vinton G., and Robert E. Icahn. "A protocol for packet network intercommunication." *ACM SIGCOMM Computer Communication Review* 35.2 (2005): 71-82.

[6] Shah, J. L., & Parvez, J. (2014, September). Evaluation of queuing algorithms on QoS sensitive applications in IPv6 network. In *Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on*(pp. 106-111). IEEE.

[7] Sasanus, Saowaphak, and Kamol Kaemarungsi. "Differences in bandwidth requirements of various applications due to IPv6 migration." *Information Networking (ICOIN), 2012 International Conference on*. IEEE, 2012.

[8] Parvez, J. (2012). Security Aspects & Performance Analysis of Mobile & IP Networks. Ph.D Thesis. University of Kashmir.

[9] Waddington, Daniel G., and Fangzhe Chang. "Realizing the transition to IPv6."*Communications Magazine, IEEE* 40.6 (2002): 138-147

[10] Govil, Jivika, et al. "An examination of IPv4 and IPv6 networks: Constraints and various transition mechanisms." *Southeastcon, 2008. IEEE*. IEEE, 2008.

[11] Pezaros, Dimitrios P., et al. "Service quality measurements for IPv6 inter-networks." *Quality of Service, 2004. IWQOS 2004. Twelfth IEEE International Workshop on*. IEEE, 2004.

[12] Bilski, T. "Network performance issues in IP transition phase." Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference on. IEEE, 2010.

