Volume 4, Issue 1, January 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Migration from IPv4 to IPv6: Security Issues and Deployment Challenges

Junaid Latief Shah, Javed Parvez

Department of Computer Science
University of Kashmir
Srinagar, India

Abstract*—IP protocol was first proposed in 1974 in a research paper by Vinton G .Cerf and Robert E. Kahn. Internet Protocol Version 4 (IPv4) which was developed almost three decades ago is the mostly prevalent protocol version in use today. However, with the rapid and ubiquitous growth of internet and increase in number of connected devices, we are facing a scenario where IPv4 addresses are essentially exhausted. The IPv4 extensions such as NAT, CIDR etc are merely limited short-term solutions. Moreover the scalability and security features that are required by the modern Internet can't be fully provided by IPv4. The long term solution to these problems is a step-by-step, phased but complete migration to IPv6. While IPv4 address space can hold billions of addresses, IPv6, which is the next version of the protocol, has provided trillions of addresses which are potentially inexhaustible. The primary focus of this paper is to compare and analyze IPv4 and IPv6 networks, study their characteristics and header formats. The paper also attempts to outline the key deployment issues and security-related challenges which are being faced and dealt with during the migration process.

***Keywords*—NAT, CIDR, ARPANET, IPv4, IPv6, Extension Headers, Authentication.**

I. Introduction

The rapid explosion of the internet and existence of high speed wireless and broadband networks have contributed towards depletion of IPv4.The IPv4 protocol created more than three decades ago with approximately an address space of 4 billion cannot cater to the needs of modern internet. The IANA (Internet Assigned Numbers Authority) allocated the last chunk of IPv4 addresses on Feb 3, 2011 to the Regional Internet Registries announcing end of IPv4 addresses [1]. The address depletion has posed a serious problem on the growth of internetworks. The short term solutions like PPP/DHCP (address sharing), CIDR (classless inter-domain routing) and NAT (network address translation) do not seem to help considering the number of devices that are getting connected to the internet daily. Also as the protocol was developed long time back, the features related to mobility, security and QoS (Quality of Service) are handled by additional protocols which cannot be integrated within the protocol. For example Internet Protocol Security (IPSec) is a protocol suit which provides network security by encrypting and protecting the data being sent. Internet Protocol Security (IPSec) provides security for IPv4 packets, but Internet Protocol Security (IPSec) is not built-in and use of IPSec in IPv4 has compatibility issues with NAT. Looking at IPv4, standards do exist for real time data delivery, known as QoS (Quality of Service) but the traffic load relies on just 8 bit TOS (type of service) field and identification of the payload data. The TOS in IPv4 has limited domain and with the passage of time has been redefined with different interpretations. Also payload identification is not possible when IPv4 packet is encrypted using a TCP or UDP port.

II. Brief Background

The Internet Engineering Task Force (IETF) in 1991 came to the conclusion that IPv4 was on the verge of exhaustion. The address scarcity and needs of the modern internet led to the development of IPv6, a new version of IP which was a result of a long term research that came into being in 1994.The IPv6 protocol was proposed to solve the long term problems of IPv4.[3]

The architecture and header structure of IPv6 is different from IPv4.The differences are in six major areas:

- Larger addressing space (128 bits)
- Stateless Automatic configuration.
- Simplified Packet Routing.
- Simplified Header.
- Improved security features (IPSec Support)
- Real-time support and multimedia services.

To Implement IPv6 network, over 30 RFC's have been published since 1994. Adopting the protocol requires changes to dozens of network protocols like DNS, PPP, NAT, DHCP etc associated with IPv4 because those protocols were developed keeping IPv4 in mind which uses 32 bit addresses.

Since IPv6 uses 128 bit addresses, the incompatibility problem for protocols naturally exists. IETF therefore suggested that IPv4 and IPv6 protocols need to co-exist for a substantial amount of time until complete migration takes place.

III. INTERNET PROTOCOL VERSION 6

Internet Protocol version 6 also known as IPng (IP next generation) is the latest version of the IP for the Internet. IPv6 comes with a 128 bit address scheme, enough to cover nearly every connected device on earth with a global unique address [4].IPv6 uses 128 bit addresses with an address space of 2^{128} (approximately 3.4×10^{38}) addresses. Such a large address space allows for every device and user in the world to connect to the internet. It also eliminates the use of NAT in IPv6 and improves connectivity, reliability and flexibility in the network. The design objectives of IPv6 were to support larger address space, security in the protocol and real time multimedia transmission. IPSec support has become a mandatory requirement in IPv6 unlike in IPv4 where it was optional. Payload identification (used in QoS) has been replaced by Flow Label field in IPv6 packet. The concept of fragmentation has been removed. The checksum and options has been replaced by extension headers in IPv6.Also IPv6 does not require manual configuration or DHCP because the system participates in "stateless" auto configuration which is one of the design goals of IPv6.Finally the packet header size has also been changed from 20 byte in IPv4 to 40 byte in IPv6[5].

A. IPv6 Header Structure

Figure 1 shows the difference between IPv6 and IPv4 headers.

- The length of header has been changed from 20 to 40 bytes
- IPv4 has 4 bytes for address (i.e. 32 bits) while as IPv6 has16 bytes (128 bits).
- The fields in the header has been reduced from 12(IPv4) to 8(IPv6).
- There is no options field in IPv6 header, however it uses "extension headers" that support greater functionalities

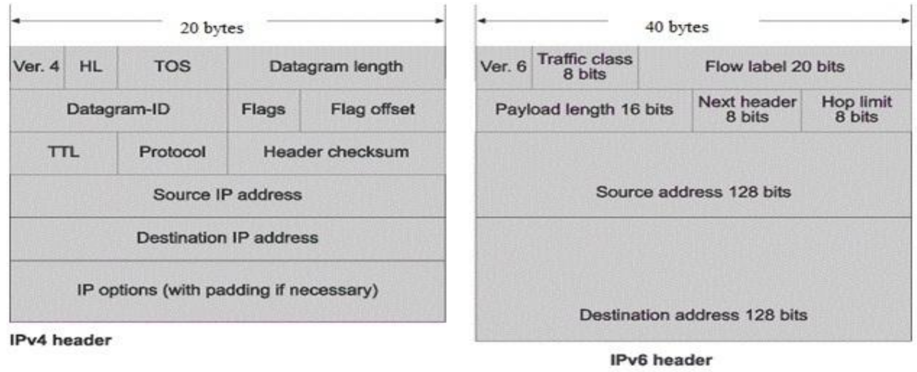
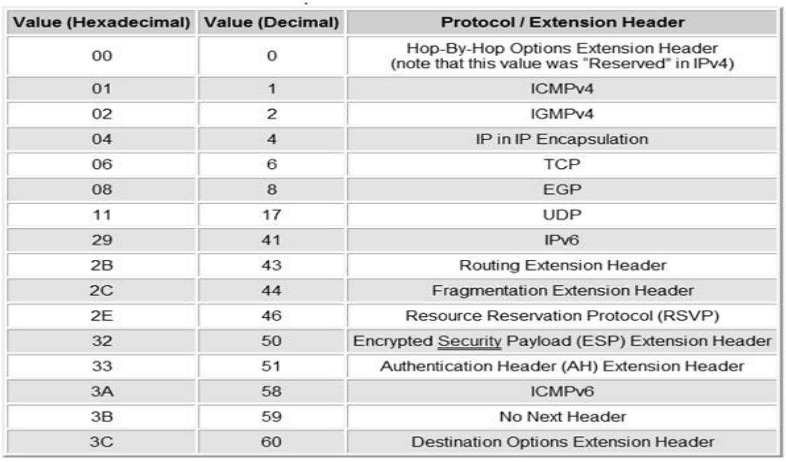


Figure 1-IPv4 and IPv6 Header comparison [6]

The header fields are described below:

1) *Version:* Version field describes the current version of the IP protocol. Its value is 6.
2) *Traffic class:* Previously in IPv4, defined as the type-of-service (ToS), the traffic class field defines the class-of-service priority of the packet. Its length is 8 bits. Priority ranges from 0 (lowest) to 7 (highest)
3) *Flow Label:* Flow Label is used by the source to label all packets belonging to a particular flow. The flow is a unique combination of the source address and the value of a non zero flow label. Multiple flows may exist between destination and source nodes. The routers treat packets belonging to a particular flow in a similar way .Its length is 20 bits.
4) *Payload Length:* **T**he payload length field specifies the length of the IPv6 payload. Its Length is 16 bits.
5) *Next Header:* Next Header field shows the next extension header to examine. Its Length is 8 bits.
6) *Hop Limit:* Also known as TTL in IPv4, the value in this field gets decremented each time packet passes through a router. When the value approaches zero without making up to its intended destination, the packet gets discarded. The maximum allowed value in IPv6 is 255 hops. The length of this field is 8 bits.
7) *Source and Destination Address:* This field specifies the 128 bit source and destination IP addresses.



Value (Hexadecimal)	Value (Decimal)	Protocol / Extension Header
00	0	Hop-By-Hop Options Extension Header (note that this value was "Reserved" in IPv4)
01	1	ICMPv4
02	2	IGMPv4
04	4	IP in IP Encapsulation
06	6	TCP
08	8	EGP
11	17	UDP
29	41	IPv6
2B	43	Routing Extension Header
2C	44	Fragmentation Extension Header
2E	46	Resource Reservation Protocol (RSVP)
32	50	Encrypted Security Payload (ESP) Extension Header
33	51	Authentication Header (AH) Extension Header
3A	58	ICMPv6
3B	59	No Next Header
3C	60	Destination Options Extension Header

Figure 2: Next Header Values [7]

B. IPv6 Extension Headers

The Extension header fields are listed below:

1) *Hop by Hop Option:* This option is used when the source passes the information to all the routers visited by a datagram. Only 3 options are currently defined so far: Pad-1, Pad-n, Jumbo payload.Pad-1 option having length 1 byte is designed for alignment purposes.Pad-n option is similar to pad-1 except it's used when 2 or more bytes are used for alignment purposes. Jumbo payload refers to a payload length more than 65,535 bytes.
2) *Source Routing:* It involves the concept of strict source route and loose source route as in IPv4.Strict source route is used by the source for predetermined route for the datagram as it travels through the internet. The sender can make a choice about route with a specific type of service such as minimum delay or max throughput. It may also choose a route that is more safer and more reliable for the sender's purpose. If a datagram chooses a strict source route, all the defined routers in the option are to be visited by the datagram.Loose source route is similar to the strict source route but a bit flexible. Along with each router in the list that must be visited, the datagram can visit other routers as well which are not in the list.
3) *Fragmentation:* Its same concept as in IPv4 however with a little difference. In IPv4, the source or a router fragments the datagram if the size of the datagram is larger than the supported MTU of the network over which the datagram has to travel. In IPv6, the original source can only fragment. A source then finds the smallest value of MTU supported by any network on the path by using a technique for path MTU discovery. Using this gained knowledge, the source then re-fragments the datagram..
4) *Authentication:* This header carries out the validation of the message sender and ensures that the integrity of data is maintained.
5) *Encrypted Security Protocol:*This header provides confidentiality and guards against eavesdropping
6) *Destination Option:* It's used when the source passes the information to the intended destination only. The routers in-between are not permitted to access to this information.

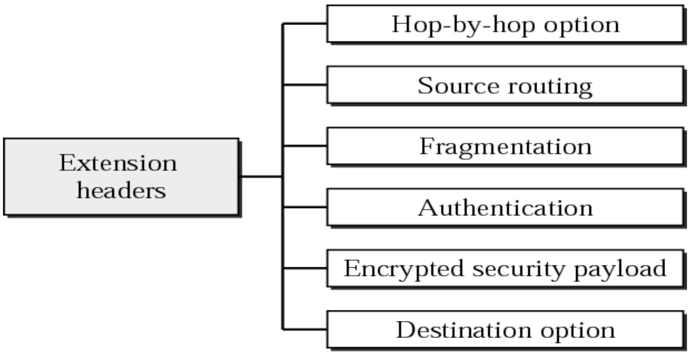


Figure 3: IPv6 Extension Headers

IV. MIGRATION FROM IPV4 TO IPV6

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. A technique and set of protocols for ensuring smooth forward, stepwise and independent changeover to IPv6 services is required. The Ngtrans Group created by IETF is assigned the job to facilitate the smooth transition from IPv4 to IPv6 services [8]. The various transition strategies can be broadly divided into two categories, including dual stack and tunneling mechanisms.

A. Dual Stack

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[11].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.

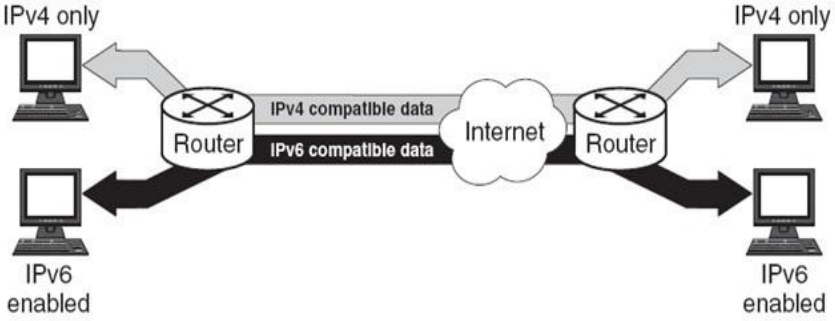


Figure 3-Dual Stack Router Implementation [10]

B. IPv6-IPv4 Tunneling

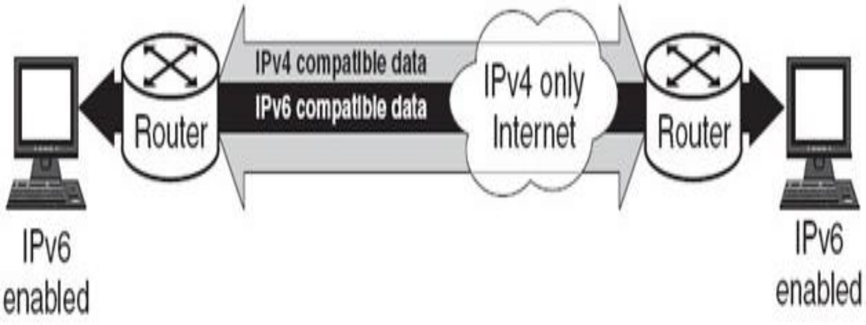


Figure 4- IPv4 Tunneling [10]

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 the connect. The most common are Host to Host, Router to Router, Router to Host, Host to Router Tunnels.

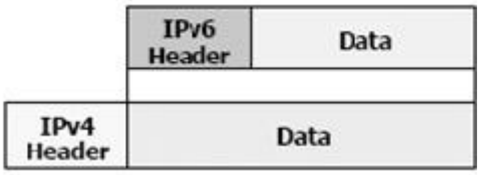


Figure 5 IPv6-IPv4 Encapsulation

V. CONCLUSIONS

Migration Process from IPv4 to IPv6 is been often compared to the Y2K problem, demanding time and investment of resources. Companies are yet to recognize IPv4 number exhaustion as an alarming problem, and are not ready to put off the investment required into the future. In the future there may be risk of insufficient time and cost [10]. The cost of migration to IPv6 could be a problem. Costs involved include renumbering networks and running two protocol stacks (IPv4 and IPv6) at the same time, upgrade to relevant software and hardware, training the manpower, and testing network implementations. However IPv6 does provide considerable benefits and features required by the modern secure internet. Given the number of problems in the current internetwork, migration process may be the only solution viable in the long run.

REFERENCES

[1] http://inetcore.com/project/ipv4ec/index_en.html.
[2] http://www.omnisecu.com/tcpip/ipv6/differences-between-ipv4-and- ipv6.php.
[3] "IPv6 Headers", Online: http://www.cu.ipv6tf.org/literatura/chap3.pdf, chapter 3, pp. 40-55, Des 12 1997.
[4] T. Dunn, "The IPv6 Transition," IEEE Internet Computing, Vol.6, No.3, May/June 2002, pp.11-13
[5] IPv6 users' site: http://www.ipv6.org.
[6] http://www.juniper.net/techpubs/en_US/junose14.2/information-products/topic-collections/swconfig-ip ipv6/index.html? topic-64529.html.
[7] http://ipv6security.wikia.com/wiki/Ipv6_header
[8] IETF IPv6 Transition Working Group, http://www.6bone.net/ngtrans.
[9] http://en.wikipedia.org.
[10] http://www.cybertelecom.org/dns/ipv6_transition.htm.
[11] RFC 4213, Basic Transition Mechanisms for IPv6 Hosts and Routers.
[12] http://www.gao.gov/new.items/d05471.pdf.
[13] RFC 3513: Internet Protocol Version 6 (IPv6) Addressing Architecture .
[14] RFC 2893: Transition Mechanisms for IPv6 Hosts and Routers.
[15] RFC 3596: DNS Extensions to Support IP Version 6 .
[16] www.linecity.de/INFOTECH_ACS_SS04/acs4_top_4.pdf.
[17] Ali, AmerNizar Abu. "Comparison study between IPV4 & IPV6." (2012).
[18] Dutta, Chiranjit, and Ranjeet Singh. "Sustainable IPv4 to IPv6 Transition."*International Journal* 2.10 (2012).
[19] Doshi, Jinesh, et al. "A Comparative Study of IPv4/IPv6 Co-existence Technologies."