Study of Various Issues of Internet Protocol Version 6

Rajveer Kaur [1], Raman Maini [2]

[1]Research Scholar, University College of Engineering
Punjabi University, Patiala, Punjab, India

[2]Associate Professor, University College of Engineering
Punjabi University, Patiala, Punjab, India

ABSTRACT

The issues of an IPv6 stack within the today's network are the major part of the research. IPv6 is currently being deployed in the world, and will be the Internet Protocol for at least the next fifty years. The objective of the article is to present the main Issues of IPv6 and how we tackle the new mechanisms introduced by IPv6. Finally, this paper provide some major differences between the most known protocol version IPV4 and the latest upcoming version i.e. IPv6 and study the various changes made to the existing protocol.

Keywords: IPv6, IPng, NAT, Multihoming, auto configuration

1. INTRODUCTION

Telecommunication and more generally network communication made huge progress in the past hundred years. We saw the first telephony devices in the late 1800s, while today almost every home is equipped with high speed Internet which links together all computers in the world. This evolution has been possible thanks to the important research effort that has been done. Network communication involves many areas of expertise, such as the media transport, wired and wireless propagation, channel coding, MAC and network protocols, routing mechanism, etc.

Internet Protocol Version 6 (IPv6) is a version of the Internet Protocol that is designed to succeed Internet Protocol version 4 (IPv4), the first publicly used Internet Protocol, which is still in dominant use currently. IPv6 is an Internet Layer protocol for packet-switched internetworks. The main driving force for the redesign of Internet Protocol was the foreseeable IPv4 address exhaustion. IPv6 is specified by the Internet Engineering Task Force (IETF) and described in Internet standard document RFC 2460, which was published in December 1998[6]. IPv6 has a vastly larger address space than IPv4. This results from the use of a 128-bit address, whereas IPv4 uses only 32 bits. The new address space thus supports 2128(about 3.4×1038) addresses. This expansion provides flexibility in allocating addresses and routing traffic and eliminates the primary need for network address translation (NAT). IPv6 also implements new features that simplify aspects of address assignment (stateless address auto configuration) and Network security.

The first publicly used version of the Internet Protocol, Version 4 (IPv4), provides an addressing capability of about 4 billion addresses (232). This was deemed sufficient in the early design stages of the Internet when the explosive growth and worldwide proliferation of networks was not anticipated. During the first decade of operation of the Internet, by the late 1980s, it became apparent that methods had to be developed to conserve address space. In the early 1990s, even after the introduction of classless network redesign, it became clear that this would not suffice to prevent IPv4 address exhaustion and that further changes to the Internet infrastructure were needed. By the beginning of 1992, several proposals appeared and by the end of 1992, the IETF announced a call for white papers [2] and the creation of the IP Next Generation (IPng) area of working groups[3][4].The Internet Engineering Task Force adopted the IPng model on July 25, 1994, with the formation of several IPng working groups. By 1996, a series of RFCs were released defining Internet Protocol version 6 (IPv6), starting with RFC 1883.The IETF assigned version 6 for the new protocol as a successor to version 4, because version 5 had previously been assigned to an experimental flow-oriented streaming protocol (Internet Stream Protocol), similar to IPv4, intended to support video and audio.

2. IPV6 SPECIFICITIES

The protocol used over the Internet for data delivery between hosts is currently the Internet Protocol version 4 (IPv4 [5]). This protocol, even though being nearly thirteen years old, has been quite efficient during the past years. However, the increasing popularity of Internet has raised address shortage and route maintenance issues. The address shortage problem is partially tackled by the massive introduction of NATs (Network Address Translators) which allow associating a single public IP address to multiple hosts in a private network. Although such mechanism is encouraged by most of ISPs (e.g. NATs are largely externalized cost of ISPs), the usage of NAT raises several complications in communication between hosts (especially when considering incoming data packets) and may also have a performance impact. Another solution to resolve these issues and enhance the services offered by IP is to adopt the new version of IP known as IP version 6 (IPv6 [2]). Given the experience acquired with IPv4, IPv6 has been defined to resolve most of the issues observed over the last thirty years in the Internet. First, it extends the address space from 232 to 2128. An IPv6 address is composed of 128 bits: the 64 first bits generally identify the network subnet (also known as subnet prefix) whereas the last 64 bits usually identify a host in this subnet. An IPv6 address is also associated to a scope which specifies the validity of an address: link-local, site-local or global. The validity of link-local addresses is limited to the link (hence the name), i.e. such addresses are only used for communication between direct neighbors. A link-local address is automatically configured on each enabled network interface by combining the FE80::/64 prefix to the IEEE 802 EUI-64 of the interface. For a site which is not connected to the Internet or which remains private, the site-local scope has been introduced.

Theses addresses are equivalent to private IPv4 addresses (e.g. 192.168.0.0). However, such addresses have been deprecated due to routing and site delimitation issues. They have been replaced by Unique Local Address [4]. At last, global IPv6 addresses are routable over the entire IPv6 Internet and therefore are used for communications between any two remote IPv6 hosts.

Note that all popular operating systems now support IPv6.However; IPv6 is not backward compatible with IPv4. As the network migration from IPv4 to IPv6 is progressive, transitional mechanisms have been defined such as dual stack nodes which support both IPv4 and IPv6.

In most regards, IPv6 is a conservative extension of IPv4. Most transport and application-layer protocols need little or no change to operate over IPv6; exceptions are application protocols that embed internet-layer addresses, such as FTP . IPv6 specifies a new packet format, designed to minimize packet header processing. Since the headers of IPv4 packets and IPv6 packets are significantly different, the two protocols are not interoperable.

2.1 Larger address space

The most important feature of IPv6 is a much larger address space than that of IPv4: addresses in IPv6 are 128 bits long, compared to 32-bit addresses in IPv4 [1]. The very large IPv6 address space supports a total of 2128 (about 3.4×1038) addresses—or approximately 5×1028 (roughly 295) addresses for each of the roughly 6.8 billion (6.8×109) people alive in 2010.[12]

The size of a subnet in IPv6 is always 264 addresses (64-bit subnet mask), the square of the size of the entire IPv4 address space. Thus, actual address space utilization rates will likely be small in IPv6, but network management and routing will be more efficient because of the inherent design decisions of large subnet space and hierarchical route aggregation.

2.2 Stateless address auto configuration

IPv6 hosts can configure themselves automatically when connected to a routed IPv6 network using Internet Control Message Protocol version 6 (ICMPv6) router discovery messages. When first connected to a network, a host sends a link local router solicitation multicast request for its configuration parameters; if configured suitably, routers respond to such a request with a router advertisement packet that contains network-layer configuration parameters[9].

If IPv6 stateless address auto configuration is unsuitable for an application, a network may use stateful configuration with the Dynamic Host Configuration Protocol version 6 (DHCPv6) or hosts may be configured statically.

2.3 Multicast

Multicast, the transmission of a packet to multiple destinations in a single send operation, is part of the base specification in IPv6. In IPv4 this is an optional although commonly implemented feature [6]. IPv6 does not implement traditional IP broadcast, i.e. the transmission of a packet to all hosts on the attached link using a special broadcast address, and therefore does not define broadcast addresses In IPv6, the same result can be achieved by sending a packet to the link-local all nodes multicast group at address ff02::1, which is analogous to IPv4 multicast to address 224.0.0.1.IPv6 multicast addressing shares common features and protocols with IPv4 multicast, but also provides changes and improvements by eliminating the need for certain protocols. Unicast address assignments by a local Internet registry for IPv6 have at least a 64-bit routing prefix, yielding the smallest subnet size available in IPv6 (also 64 bits). With such an assignments it is possible to embed the unicast address prefix into the IPv6 multicast address format, while still providing a 32-bit block, the least significant bits of the address, or approximately 4.2 billion multicast group identifiers. Thus each user of an IPv6 subnet automatically has available a set of globally routable source-specific multicast groups for multicast applications (RFC 3306).In IPv4 it was very difficult for an organization to get even one globally routable multicast group assignment and implementation of inter-domain solutions was very arcane.[7]IPv6 also supports new multicast solutions, including embedding Rendezvous Point addresses in an IPv6 multicast group address which simplifies the deployment of inter-domain solutions.

2.4 Mandatory support for network layer security

Internet Protocol Security (IPSec), the protocol for IP encryption and authentication, forms an integral part of the base protocol suite in IPv6 [6] .IPSec support is mandatory in IPv6; this is unlike IPv4, where it is optional.

2.5 Simplified processing by routers

In IPv6, the packet header and the process of packet forwarding have been simplified to make packet processing by routers more efficient, and thereby extending the end-to-end principle of Internet design. Specifically:

- The packet header in IPv6 is simpler than that used in IPv4, with many rarely used fields moved to separate options; as a result, although the addresses in IPv6 are four times as large, the option-less IPv6 header is only twice the size of the option-less IPv4 header.

- IPv6 routers do not perform fragmentation. IPv6 hosts are required to either perform PMTU discovery, perform end-to-end fragmentation, or to send packets no larger than the IPv6 default minimum MTU size of 1280 octets.
- The IPv6 header is not protected by a checksum; integrity protection is assumed to be assured by both link layer and higher layer (TCP, UDP, etc.) error detection. Therefore, IPv6 routers do not need to recompute a checksum when header fields (such as the time to live (TTL) or hop count) change.
- The *TTL* field of IPv4 has been renamed to *Hop Limit*, reflecting the fact that routers are no longer expected to compute the time a packet has spent in a queue.

2.6 Mobility

Unlike mobile IPv4, mobile IPv6 avoids triangular routing and is therefore as efficient as native IPv6. IPv6 routers may also support network mobility which allows entire subnets to move to a new router connection point without renumbering. [8]

2.7 Options extensibility

The IPv4 protocol header has a fixed size (40 octets) for option parameters. In IPv6, options are implemented as additional extension headers after the IPv6 header, which limits their size only by the size of an entire packet. The extension header mechanism provides extensibility to support future services for quality of service, security, mobility, and others, without redesign of the basic protocol.[6]

2.8 Jumbograms

IPv4 limits packets to 65535 (216 - 1) octets of payload. IPv6 has optional support for packets over this limit, referred to as jumbograms, which can be as large as 4294967295 (232 - 1) octets. The use of jumbograms may improve performance. The use of jumbograms is indicated by the Jumbo Payload Option header.

2.9Neighbor Discovery

IPv6 includes a new protocol known as Neighbor Discovery [6] which achieves various tasks such as router discovery; address resolution (mapping IPv6 addresses with link-layer addresses), address auto configuration, neighbor unreachability detection, next-hop determination and host redirection. All messages introduced by Neighbor Discovery are Internet Control Message Protocol for the Internet Protocol Version 6 (ICMPv6 [6]) messages. Neighbor Discovery introduces a new address configuration procedure known as stateless address auto configuration mechanism [12]. A host may automatically configure a valid global IPv6 address upon receiving a Router Advertisement message that a local access router periodically broadcasts over an IPv6 link. A Router Advertisement generally provides the link prefix (es) for global address configuration in addition to the link-layer address of the local access router. Note that the IPv6 link-local address of the router is retrieved from the IPv6 header of the Router Advertisements no additional packet exchange is needed to forward IPv6 packets to this router. Upon receiving a Router Advertisements, a host configures a global IPv6 address for each prefix listed in the message by combining these prefixes with the IEEE 802 EUI-64 of the interface that received the message. Also, the host adds the relevant routes in its routing table (default route, route for on-link destination, etc.) and registers in the neighbor cache (equivalent to the ARP cache in IPv4) the mapping between the IPv6 and the link-layer addresses of the router. Furthermore, the access router provides a lifetime for each prefix announced in order to help hosts to know when an address is deprecated and should not be used to initiate new communication. Note that IPv6 also enables a stateful address auto configuration through Dynamic Host Configuration Protocol version 6 (DHCPv6 [3])or manual address configuration. Before assigning a unicast IPv6 address to an interface (regardless the scope and how the address has been obtained), a host must ensure that this address is unique by performing a Duplicate Address Detection (DAD) [12]. This procedure consists in multicasting a Neighbor Solicitation message to request a potential neighbor host which already uses the target address to reply with a Neighbor Advertisement. After a certain amount of time without reception of such a message, the address is determined to be unique and therefore is assigned to the interface by the originator of the DAD procedure. When the DAD fails (i.e. the target address is already in use by a neighbor), the address must not be assigned to the interface.

2.9 Multihoming

Multihoming refers to a situation where a host is reachable through multiple paths, either because this host has several network interfaces connected to various access networks, or because the subnet in which the host is located is multihomed itself. Whereas a host could only have one address per interface in IPv4, IPv6 allows a host to assign several IPv6 addresses (regardless the scopes are) to a single interface. A practical scenario which illustrates such configuration is a link provided with two access routers advertising one unique prefix each. A host would configure at least 3 addresses on the interface connected to this link: one link-local address and two global addresses (referred to as IP1 and IP2 in the following), each corresponding to a prefix. Thus, this host could either communicate with IP1 or IP2 only, or both IP1 and IP2 simultaneously.

3. IMPLEMENTATION

Difference between IPv4 and IPv6

IPv4

- Source and destination addresses are 32 bits (4 bytes) in length.
- IPSec support is optional.
- IPv4 header does not identify packet flow for QoS handling by routers.

- Both routers and the sending host fragment packets.
- Header includes a checksum.
- Header includes options.
- Address Resolution Protocol (ARP) uses broadcast ARP Request frames to resolve an IP address to a link-layer address.
- Internet Group Management Protocol (IGMP) manages membership in local subnet groups.
- ICMP Router Discovery is used to determine the IPv4 address of the best default gateway, and it is optional.
- Broadcast addresses are used to send traffic to all nodes on a subnet.
- Must be configured either manually or through DHCP.
- Uses host address (A) resource records in Domain Name System (DNS) to map host names to IPv4 addresses.
- Uses pointer (PTR) resource records in the IN-ADDR.ARPA DNS domain to map IPv4 addresses to host names.
- Must support a 576-byte packet size (possibly fragmented).

IPv6

- Source and destination addresses are 128 bits (16 bytes) in length.
- IPSec support is required.
- IPv6 header contains Flow Label field, which identifies packet flow for QoS handling by router.
- Only the sending host fragments packets; routers do not.
- Header does not include a checksum.
- All optional data is moved to IPv6 extension headers.
- Multicast Neighbor Solicitation messages resolve IP addresses to link-layer addresses.
- Multicast Listener Discovery (MLD) messages manage membership in local subnet groups.
- ICMPv6 Router Solicitation and Router Advertisement messages are used to determine the IP address of the best default gateway, and they are required.
- IPv6 uses a link-local scope all-nodes multicast address.
- Does not require manual configuration or DHCP.
- Uses host address (AAAA) resource records in DNS to map host names to IPv6 addresses.
- Uses pointer (PTR) resource records in the IP6.ARPA DNS domain to map IPv6 addresses to host names.
- Must support a 1280-byte packet size (without fragmentation).

IPv6 Header

Fig 1- IPv6 Header Format

<table>
<tr><td>Version
(4 bit)</td><td>Traffic class
(4 bit)</td><td colspan="3">Flow Label
(24 bit)</td></tr>
<tr><td colspan="3">Payload Length
(16 bit)</td><td>Next Header
(8 bit)</td><td>Hop Limit
(8 bit)</td></tr>
<tr><td colspan="5">Source Address(128 bit)</td></tr>
<tr><td colspan="5">Destination Address(128 bit)</td></tr>
</table>

IPv6 header contains the following things:

- **Version** - This field contains the version of the IP used in the packet. It is of 4-bit in IP version 6.
- **Traffic class** - This is an 8-bits field determining the packet priority. Priority values subdivide into ranges: traffic where the source provides congestion control and non-congestion control traffic.
- **Flow label** - These 20 bits specifies the QoS management. Originally created for giving real-time applications special service, but currently unused.
- **Payload length** - These 16 bits determines the payload length in bytes. When cleared to zero, the option is a "Jumbo payload" (hop-by-hop).
- **Next header** - This 8-bits field specifies the next encapsulated protocol. The values are compatible with those specified for the IPv4 protocol field.
- **Hop limit** - This is an 8-bits field newly introduced in IPv6. It replaces the time to live field of IPv4.
- **Source Address** - This 128 bits field determines the logical address of the host that is sending the packet.
- **Destination Address** - This 128 bits field determines the logical address of the host that is receiving the packet.

The payload can have a size of up to 64KB in standard mode, or larger with a "jumbo payload" option.

4. CONCLUSION AND FUTURE WORK

In this paper, we presented the various issues related to an IPv6 stack. The new version of IP, namelyIPv6, is currently being deployed in the Internet, and will definitely be the next IP protocol used for the next fifty years. IPv6 offers lot of advantages over IPv4 as it benefits from the experience of more than thirty years of the Internet usage. One of them is certainly the Neighbor Discovery protocol. Inspired from the ARP protocol for IPv4, it enables router discovery, host auto configuration, neighbor discovery, address resolution, and next hop determination. Moreover, IPv6 proposes a simplified header system which eases the development of extensions. IPv6 also offers several protocols for multihoming and mobility support. This support allows optimizing communications of mobile devices such as PDA or Personal Area Network connected to the Internet.

Therefore, it is important to provide the overview of IPv6 as we propose in this paper. However, IPV6 is not implemented in real life till date, so general overview to IPV6 to all is necessary, as it will become the most important protocol for internet in few years. The issues presented in this paper do not pretend to be complete and is still an ongoing work. However, we believe that the main components of an IPv6 have been discussed, and can serve for further development. Our future work is to propose an implementation of other IPv6 protocols, such as Mobile IPv6 [9] or SHIM6 [11]. Currently we are focusing on a complete supports provided by IPv6.

5. ACKNOWLEDGEMENT

The author would like to thank Dr Amardeep Singh from UCoE and the Department of Engineering of Punjabi University for their great help throughout the implementation process. The achievement of this work would not be possible without their invaluable assistance.

6. REFERENCES

[1] David C. Plummer. An Ethernet Address Resolution Protocol. IETF, RFC 826, November 1982.

[2] Internet Protocol: DARPA Internet Program Protocol Specification, University of Southern California Information Sciences Institute. IETF, RFC 791, September 1981.

[3] IP Version 6 Addressing Architecture, R. Hinden, S. Deering (February 2006)

[4] Paper9250-Implementation of an IPv6 Stack for NS-3

[5] RFC 2460, Internet Protocol, Version 6 (IPv6) Specification, S. Deering, R. Hinden (December 1998

[6] RFC 1550, IP: Next Generation (IPng) White Paper Solicitation, S. Bradner, A. Mankin (December 1993)

[7] RFC 1752 the Recommendation for the IP Next Generation Protocol, S. Bradner, A. Mankin, January 1995.

[8] RFC 4862, IPv6 Stateless Address Autoconfiguration, S. Thomson, T. Narten, T. Jinmei (September 2007

[9] RFC 1112, Host extensions for IP multicasting, S. Deering (August 1989

[10] RFC 2908, the Internet Multicast Address Allocation Architecture, D. Thaler, M. Handley, D. Estrin (September 2000)

[11] RFC 3963, Network Mobility (NEMO) Basic Protocol Support, V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert (January 2005)

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

[13] RFC 1886 — DNS Extensions to Support IP Version 6, S. Thomson, Bell core, C. Huitema, INRIA, December 1995.

[14] RFC 1933 — Transition Mechanisms for IPv6 Hosts and Routers, R. Gilligan. Nordmark, Sun Microsystems, April 1996

[15] RFC 2460 — Internet Protocol, Version 6 (IPv6) Specification, S. Deering, Cisco. R.Hinden, Nokia, December 1998

[16] S. Thomson, T. Narten and T. Jinmei. IPv6 Stateless Address Autoconfiguration, Internet Engineering Task Force Request for Comments (RFC) 4862, September 2007