ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 1, July 2013

Rush on IPv6 - a brief on its New Features, Security, QOS and Mobility

Md. Amran Hossain, A.K.M. Niaz Morshed, Nahid Imtiaz Chowdhury

Abstract*— At different rates in different parts of the world, the next-generation Internet protocol, IPv6, is inching its way toward adoption. Asian countries are moving fastest, at least partly because their need for IPv6's expanded address space is greatest. Many students, educators, and other professionals are increasingly finding that they need to become familiar with networking protocols. While the technical details are more complex than most professionals need, an understanding of the basic uses, features, terminology, and configurations is essential for any technical decision-maker or computer professional. Because of the Internet's dominance, computer professionals need to be, at least, familiar with its basic functionality. Whether you are an educator, student, technician, or manager, if you need to know network communication, you will need to know Internet Protocol version 6.

***Index Terms*— Internet security, IPv6, Multicast address, Next generation internet etc.**

I. INTRODUCTION

Currently, Internet Protocol version 4, IPv4, is the standard for Internet communications. However, with the tremendous expansion of the Internet, IPv4 is proving to be incapable of handling the coming demand. Internet Protocol version 6, or IPv6, is the next currently proposed standard for Internet communications. While the basic function of IPv6 is similar to IPv4, IPv6 is drastically different in form. Differences fall into the categories of addressing, security, and configuration.

II. /WHAT IS AN IP ADDRESS?

IP address (short for Internet Protocol address) helps devices to communicate (like a phone number that helps a phone to communicate with another phone) with websites, Internet services, and other devices. IP addresses are numbers that are displayed as strings of letters or numbers, such as 192.0.2.1 (for IPv4) and 2001:db8:: 1234:ace:6006:1e (for IPv6).

There are 3 different types of IPv6 addresses:

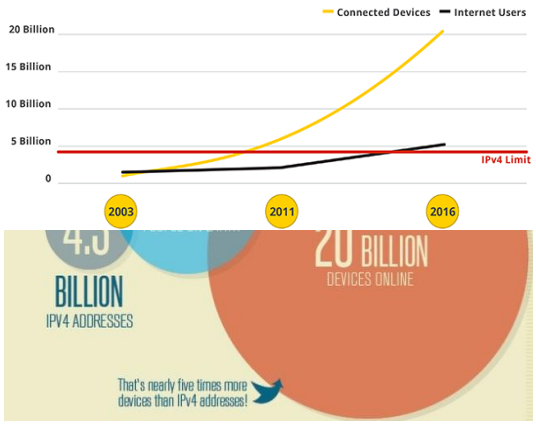
- **Unicast**: identifies a single interface. A packet with an address of this type in the destiny is delivered only to that interface.
- **Multicast**: identifies a set of interfaces. A packet with this address as destiny is delivered to all the interfaces of the set.
- **Any cast**: identifies also a set of interfaces, but in this case, a packet with this kind of address as destiny, is delivered only to one interface of the set. Usually the next interface, according to the routing protocol.

The main differences between IPv4 and IPv6 addresses are the appearance of the IPv6 any cast addresses, and the disappearance of IPv4 broadcast addresses, that are replaced by the IPv6 multicast addresses.

III. WHY IPV6?

- IPv4, only has room for about 4 billion addresses.
- Today, the number of devices connected to the Internet exceeds the number of people alive.
- With IPv6 protocol, will have 340,282,366,920,938,463,463,374,607,413,786,211,456 possible internet addresses. That's 100 for every atom on the face of the earth.
- IPv6 enables more efficient routing, the efficient use of modern hardware and the ability to support modern networking concepts like mobility.

The Internet Engineering Task Force documented IPv4 in 1981 and deployed it two years later in a global switchover from Arpanet's Network Control Protocol. It was supposed to last for a very long time, with an addressing space of 4000 millions of addresses (Certainly not to supply the current world population of 7 Billion), but the enormous growth of the internet and the way the addresses were assigned (classes A, B and C), resulted in a serious lack of addresses.



There are several methods that avoid the total run out of addresses: PPP/DHCP (address sharing), CIDR (classless inter-domain routing) and NAT (network address translation), but do not seem to be enough in a few years, specially having into account the growing number of devices that need a permanent allocation of an IP address (UMTS, DSL, etc), and the applications that are end-to-end, and are not compatible with NAT (IPsec, VoIP, etc.). Another problem is that, because of being designed many years ago, the functionalities involved with security, mobility and quality are handled by

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 1, July 2013

additional protocols, because they are not integrated in the protocol itself. The lack of security and authentication in IPv6 is IP does not encrypt packets. You cannot digitally sign a transmission. It is relatively easy to monitor TCP connections, even hijack them and make them yours. Hackers all over the world routinely use such tools to break into systems. Yet another problem is the lack of quality of service. If you stream an audio or video over the Web, there is no guarantee that you will have enough network bandwidth consistently to deliver the goods. In addition, the Internet today doesn't have a structure that reflects IP address allocation, thus requiring huge routing tables to be maintained by routers. Network congestion abounds. So a new working group of the Internet Engineering Task Force (IETF) was created with the name: "IP next generation" (IPng). And some time later, the name was changed to IPv6. The IETF documented IPv6 (http://www.ietf.org/rfc/rfc2460.txt?number=2460) in 1998. But, the Internet community grew exponentially in the 15 years between 1983 and 1998. It became truly global as well as commercial, which made the switchover from IPv4 to IPv6 a significantly more complex problem. The main characteristics of this protocol had to be the following:

- Larger addressing space, structured addresses and no addresses classes.
- Automatic configuration.
- Simplified routing.
- Better structuring options for the networks.
- Improved security features.
- Support for real-time and multimedia services.

IV. IPV6 HEADER AND EXTENSIONS

The IPv6 protocol defines a set of headers, including the basic IPv6 header and the IPv6 extension headers.

A. Header Format

The following figure shows the elements that appear in the IPv6 header and the order in which the elements appear.

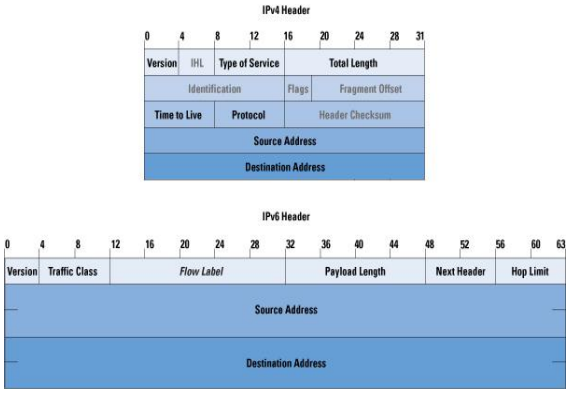


Fig 2: IPv6 and IPv6 Header Format

The following list describes the function of each header field.

- **Version** – 4-bit Version number of Internet Protocol = 6.
- **Traffic Class** – 8-bit traffic class field.
- **Flow Label** – 20-bit field.
- **Payload Length** – 16-bit unsigned integer, which is the rest of the packet that follows the IPv6 header, in octets.
- **Next Header** – 8-bit selector. Identifies the type of header that immediately follows the IPv6 header. Uses the same values as the IPv4 protocol field.
- **Hop Limit** – 8-bit unsigned integer. Decremented by one by each node that forwards the packet. The packet is discarded if Hop Limit is decremented to zero.
- **Source Address** – 128 bits. The address of the initial sender of the packet.
- **Destination Address** – 128 bits. The address of the intended recipient of the packet. The intended recipient is not necessarily the recipient if an optional Routing Header is present.

B. Extension Headers

IPv6 includes an improved option mechanism over IPv4. IPv6 options are placed in separate extension headers that are located between the IPv6 header and the transport-layer header in a packet. Most IPv6 extension headers are not examined or processed by any router along a packet's delivery path until the packet arrives at its final destination. This feature is a major improvement in router performance for packets that contain options. In IPv4, the presence of any options requires the router to examine all options. Unlike IPv4 options, IPv6 extension headers can be of arbitrary length. Also, the number of options that a packet carries are not limited to 40 bytes. This feature, plus the manner in which IPv6 options are processed, permits IPv6 options to be used for functions that are not practical in IPv4. A good example of IPv6 options is the IPv6 authentication and security encapsulation options.

To improve performance when handling subsequent option headers, and the transport protocol that follows, IPv6 options are always an integer multiple of eight octets long. The integer multiple of eight octets retains the alignment of subsequent headers.

The following IPv6 extension headers are currently defined.

- **Routing** – Extended routing, like IPv4 loose source route
- **Fragmentation** – Fragmentation and reassembly
- **Authentication** – Integrity and authentication, security
- **Encapsulation** – Confidentiality
- **Hop-by-Hop Option** – Special options that require hop-by-hop processing
- **Destination Options** – Optional information to be examined by the destination node

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 1, July 2013

V. QUALITY OF SERVICE (QOS) IN IPV6

The goals to achieve by the quality of service mechanisms are:

- Real time applications.
- Less latence and "jitter".
- More tolerance to packet losses.
- Retransmissions are less important.
- More importance of the temporal relationships.

Quality of Service (QOS) is an important term and an emerging feature of modern networks. IPV6 brings quality of service that is required for several new applications such as IP telephony, video/audio, interactive games or ecommerce. Whereas IPv4 is a best effort service, IPv6 ensures QoS, a set of service requirements to deliver performance guarantee while transporting traffic over the network. For networking traffic, the quality refers to data loss, latency (jitter) or bandwidth. In order to implement QOS marking, IPv6 provides a traffic-class field (8 bits) in the IPv6 header. It also has a 20-bit flow label. Several features are added to IPv6 specification in addition to 128-bits addressing as the IPv6 specification made its way through the IETF committee process. This includes, Levels of assured service, enhance security, and improved reliability. IPv4 networks typically give each and every packet a "best level of effort" service, even if the content of every packet isn't really important or time-sensitive data. An IPv4-based system has no way to differentiate between data payloads that are time sensitive, such as streaming video or audio, and those that aren't time-sensitive, such as status reports and file transfer. Streaming audio and video application are very sensitive to delay of a few packets - lips move without sound or picture break up - but IPv4 has no way to prevent those problems. If a packet is lost in transit, TCP recognizes the loss and requests a retransmission, but only after an inevitable delay. The single delayed TCP packet is probably part of a much larger packet of audio or video data, so the entire big packet is delayed and probably thrown out because the smallest part didn't arrive on time. IPv6 provides a way for applications to request handling without delay throughout the WAN. The term often used to describe this is low latency. Streaming audio and video requires low latency through high priority. To prevent a break down in the scheme, the various applications can share connection via priority level.

- Level 0 - No specify priority
- Level 1 - Background traffic (news)
- Level 2 - Unattended data transfer (email)
- Level 3 - Reserved
- Level 4 - Attended bulk transfer (FTP)
- Level 5 - Reserved
- Level 6 - Interactive traffic (Telnet, Windowing)
- Level 7 - Control traffic (routing, network management)

VI. MOBILE IPV6

Changes in IPv6 for Mobile IPv6

- A set of mobility options to include in mobility messages
- A new Home Address option for the Destination Options header
- A new Type 2 Routing header
- New Internet Control Message Protocol for IPv6 (ICMPv6) messages to discover the set of home agents and to obtain the prefix of the home link
- Changes to router discovery messages and options and additional Neighbor Discovery options
- Foreign Agents are no longer needed

The major differences between Mobile IPv4 and Mobile IPv6:

- There is no need to deploy special routers as "foreign agents", as in Mobile IPv4. Mobile IPv6 operates in any location without any special support required from the local router.
- Support for route optimization is a fundamental part of the protocol, rather than a nonstandard set of extensions.
- Mobile IPv6 route optimization can operate securely even without pre-arranged security associations. It is expected that route optimization can be deployed on a global scale between all mobile nodes and correspondent nodes.
- Support is also integrated into Mobile IPv6 for allowing route optimization to coexist efficiently with routers that perform "ingress filtering" .
- The IPv6 Neighbor Unreachability Detection assures symmetric reach ability between the mobile node and its default router in the current location.
- Most packets sent to a mobile node while away from home in Mobile IPv6 are sent using an IPv6 routing header rather than IP encapsulation, reducing the amount of resulting overhead compared to Mobile IPv4.
- Mobile IPv6 is decoupled from any particular link layer, as it uses IPv6 Neighbor Discovery instead of ARP. This also improves the robustness of the protocol.
- The use of IPv6 encapsulation (and the routing header) removes the need in Mobile IPv6 to manage "tunnel soft state".
- The dynamic home agent address discovery mechanism in Mobile IPv6 returns a single reply to the mobile node. The directed broadcast approach used in IPv4 returns separate replies from each home agent.

Wireless e-commerce is one application area that will benefit from IPv6 deployment, according to Cisco's Baker. When your mobile device has a globally recognized IPv6 address, network services can pick up your presence directly, along with personal information you've chosen to associate with that address. For example, if you're running an errand and want directions to your destination, an available network-based service can immediately tell you where to go next as you join different networks along the way.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 1, July 2013

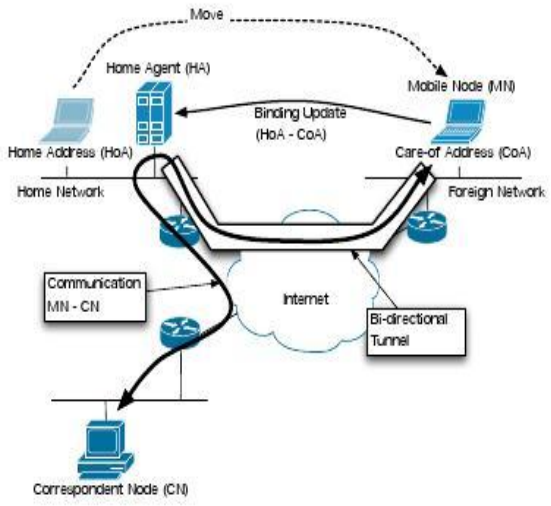


Fig 3 : Basic operation of Mobile IPv6

Secure mobile communication is essential for the pervasive accessibility of critical information infrastructure. Connecting control systems with the business enterprise, wireless telemetry and mobile user interaction with critical infrastructure systems are examples of services that motivate the need for secure mobile communication. Mobile IPv6 is being touted to provide communication support for such services. The security of Mobile IPv6 poses key challenges impeding its wide-scale adoption. Several security mechanisms have been proposed in the literature. There are a number of important security features that are either already implemented in IPv6, or that are on the drawing board for the near future:

- IPSec (encrypted VPNs) are now a mandatory component. IPSec still needs to be configured properly, but at least it is now universally available.
- A plethora of addresses will allow for logic and functional address assignment. We no longer need to design subnet sizes around "what's available" but we can now design networks that make sense.
- Addresses with different scopes allow for the proper isolation of hosts.
- Simplified rules for fragmentation make it easier to defend diverse networks with different network technologies.
- If desired, end to end connectivity with reliance on "NAT" (Network Address Translation) will allow for a simpler configuration of end-to-end encrypted networks
- Address will no longer be shared among different devices, allowing for an easier attribution of network traffic and simpler asset control.
- Using a so far not widely implemented extension, it will be possible to create addresses cryptographically and validate them on the local network.

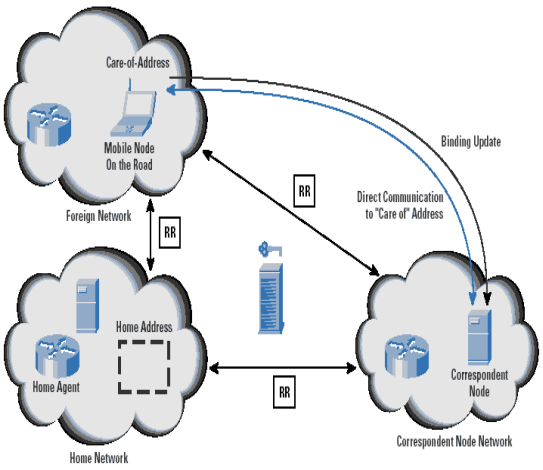


Fig 4: Route Optimization with Built-In Security

VII. SUMMARY OF BENEFITS IN A NUTSHELL

1. Increased address space
2. More efficient routing
3. Reduced management requirement
4. Improved methods to change ISP
5. Better mobility support
6. Multi-homing
7. Security
8. Scoped address: link-local, site-local and global-address space.

REFERENCES

[1] IPv6 - The Next Generation Internet - by Kaushik Das.

[2] http://www.census.gov/main/www/popclock.html.

[3] http://blogs.cisco.com/news/the-internet-of-things-infographic/

[4] http://ipv6.com/articles/research/Secure-Neighbor-Discovery.htm

[5] http://www.worldipv6launch.org

[6] http://www.ipv6forum.com/

[7] Comparison of IPv4 and IPv6 Networks Including Concepts for Deployment and Interworking, Jesús Ibáñez Parra

[8] In Brief: IPv6 and Distributed Applications, David Geer

[9] http://docs.oracle.com/cd/E19683-01/817-0573/chapter1-fig-8/index.html

[10] http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-3/ipv6_internals.html

[11] http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-3/ipv6_behind_the_wall.html.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 1, July 2013

AUTHOR BIOGRAPHY

Md. Amran Hossain was born on 1985 in Chittagong, Bangladesh. Currently he is studying Masters in Computer Science in Jahangirnagar University. He is working at Sonali Bank Limited, which is the leading and largest public bank in Bangladesh. His research interests include wireless communication, Network security, open-source computing, open source computing platform, ICT development in rural area etc. He is also a member of Bangladesh Computer Society. E-mail: amranmailbox@yahoo.com

A.K.M. Niaz Morshed was born on 1987 in Sirajgonj, Bangladesh. He has completed B.Sc. in Electrical and Electronic Engineering from the Ahsanullah University of Science & Technology (AUST) Bangladesh in 2009. He has previously worked at ZTE Corporation as Transmission Engineer, which is one of the International Telecommunication Vendor. Besides, he has various research interests including Microwave Engineering, VLSI, HCI, Distributed Computing, Network Security, Wireless communication etc. Currently he is pursuing MSc under JU. He is also a member of IEB. E-mail: akm_niaz@yahoo.com

Nahid Imtiaz Chowdhury received his B.Sc (Engg.) degree in Computer Science and Engineering from Mawlana Bhashani Science and Technology University, Santosh, Tangail-1902, Bangladesh, in 2010. He previously worked as Asst .Lecturer in Department of Computer Science and Engieering at Gono University, Savar, Dhaka, Bangladesh. Now he is working as a software Engineer in Grameen phone IT which is the join bencher of two giant Multinational companies, Accenture and Telenor Group. Besides, He has various research Interests including VLSI, Cloud computing , Distributed computing , Network security etc.E-Mail:nahid.mbstu.cse@gmail.com