The Benefits and Characteristics of IPv6

Abhay Aggrawal
Dept. of CSE
PES University, EC Campus
Banglore,Karnataka,India
abhayagarwal383@gmail.com

Isha Arora
Dept. of CSE
PES University, EC Campus
Banglor,Karnataka,India
aroraisha99@gmail.com

Aditya Abhishek
Dept. of CSE
PES University, EC Campus
Banglore,Karnataka,India
adityaabhishek31@gmail.com

***Abstract*— Internet has developed exponentially over years and has become an identity. To define a system using internet unique there are addresses provided known as IP address. Rapid expansion of the Internet has created a "success disaster" in terms of IP addresses. The used technology to address systems uniquely was IPv4 but with the time, address provided by IPv4 is soaking. Here IPv6 comes into picture. IPv6 can provide more address as compared to IPv4. Existing studies have discussed the notation that IPv6-centric next generation network are widely developed and applied. In order to gain a good understanding of IPv6, this paper revisits several benefits and characteristics of using IPv6. The characteristics of IPv6 have been seen to meet the future demands providing new benefits over orthodox IPv4.**

Keywords—internet, address, IPv4, IPv6, characteristics, benefits

I. INTRODUCTION

Web Protocol variation six (IPv6) is another amount tradition of the basic *internet* tradition. Web Protocol (IP) may be a typical non-standard speech of the web, every appliance related to the web should bolster it. The present version of IPv4 (IP frame 4) includes a few insufficiencies that area unit inescapable and confound such drained address area, security problems, non-availability of auto-setup and currently demonstrate an obstruction to, the further improvement of the Internet. Currently IPv4 is the main form of Internet set of rules with a more than 4 billion network addresses. Even with such a large number, it is insufficient to keep going forever.

IoT industry is growing at an enormous rate. To be exact, it is progressing at a rate of 28.5% per year, which is unmatched by any other industry in the world. Due to this growth, an enormous increase in the amount of device connecting to the internet has been seen. As all devices connected to the internet requires a unique address so that they can be recognized and can follow internet protocols and terms of use. As the number of devices increase, the number of address we need increases as well. This makes IPv6 so important. IPv6 provides larger range of addresses as compared to IPv4. After the addresses provided by the IPv4 will be used up, IPv6 will become a necessity and shift towards IPv6 will be necessary.

To adapt the technology in its pure form, we need to understand what IPv6 actually is, its benefits, characteristics, security and risks. While the IPv6 system is not backward compatible with IPv4, both protocols are able to work in parallel without significant disruption.

IPv6 is the latest version of the Internet Protocol, which identifies devices across the internet so that they can be located. Every device that is identified through the internet has its own IP address in order for internet communication to work. The current industry norm is the IPv4 but is slowly being replaced with IPv6. IPv6, due to its more complex nature and immense amount of address spaces is used for the IOT industry.

In this paper, we will be talking about different characteristics, benefits and risks of using IPv6 in IoT devices. We will also talk about different security options, applications and enhancements.

II. IPV6 ADDRESS DESIGN

x:x:x:x:x:x:x:x – where x is a 16 bits hexadecimal field and x speaks to four hexadecimal digits.
A case of IPv6: 2020:0000:1234:0000:0000:C17E:CBDA:6034
There are:

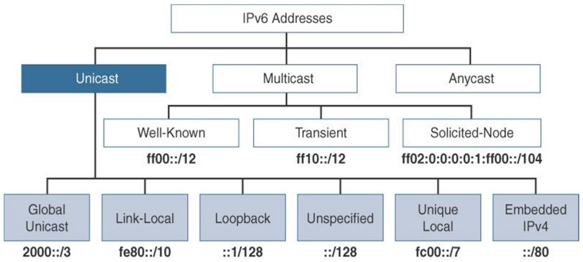
- 8 gatherings of 4 hexadecimal digits.
- Each gathering speaks to 16 bits (4 hexa digits * 4 bit)
- Separator is ":"
- Hex digits are not case delicate, so "DBCA" is same as "dbca" or "DBca"…

III. EASE OF USE

A. Expanded addresses space

IPv6 uses 128 bits to deal with a address allocation on the internet it's eight 16-bit segments, separated by colons. This abundant of additional bits will give around 3.4×1038 totally different combos of addresses. This address will accumulate the aggressive demand of address allotment for nearly everything during this world this offers an unfathomable range of supported devices 340 undecillions to be precise.

From an estimate, 1564 addresses may be allotted to each area unit of this earth. The notation of the address may be reduced by omitting leading 0s and by victimization the double colon to interchange contiguous hextets of 0s. This dilated address house conjointly helps to interrupt the NAT (Network Address Translation) barrier..



B. IPv6 Header

The header of IPv6 is forty bytes long and contains precisely eight fields. IPv6's header has been disentangled by moving all pointless knowledge and selections (which square measure obtainable in IPv4 header) to the end of the IPv6 header. The verification field in IPv6 is born and every one verification computation in IPv6 should be administered by upper-layer protocols like transmission control protocol and UDP. IPv6 routers are not allowed to fragment packets they forward; solely the initial sender of Associate in Nursing IPv6 packet is permissible to interrupt the packets in fragments, thus fragment field is born from IPv6.

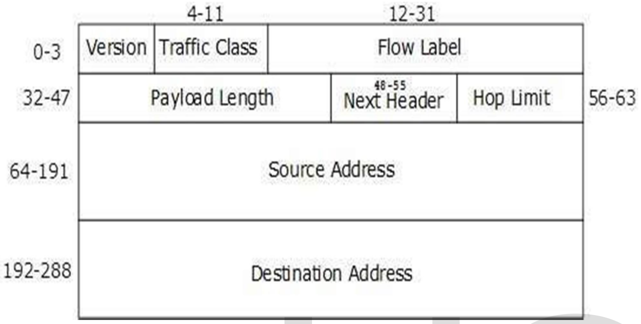


Figure: IPv6 Fixed Header

C. Enhance Qos Support

A key advantage of the larger packet header is that the ability to implement Quality of Service (QoS) technologies. The IPv6 packet header contains fields that facilitate the support for QoS for each differentiated and integrated services..

D. Auto Configuration

IPv6 supports each stateful and homeless motorcar configuration mode of its host devices. This way, absence of a DHCP server doesn't place a halt on buries section communication. Address motorcar configuration mechanism square measure designed to permit plug-and-play of network devices - merely enter the host machine and it'll mechanically put together information processing address, network prefix, and mechanically realize all accessible routers. This feature can scale back the management and operation overhead.

E. End-to-end Connectivity

Every system currently has distinctive information processing address and may traverse through the web while not mistreatment NAT or alternative translating elements. once IPv6 is totally enforced, each host will directly reach alternative hosts on the web, with some limitations concerned like Firewall, organization policies, etc. once IPv6 is totally dead, every host will foursquare deliver the goods completely different has on the web, with a number of constraints enclosed like Firewall, association ways, and so on.

F. Mobility

IPv6 was designed keeping the mobility in mind. This component empowers hosts and enables hosts to roam around in different geographical area and remain connected with the same IP address. This feature exploits and takes advantage of IPv6's auto IP arrangements feature and Extension headers feature. It enables a user/host to stay free from the pain of taking care of the IP of their device and can remain connected to the network.

G. Enhanced Priority Support

In IPv6, Traffic category and Flow label square measure wont to tell the underlying routers a way to expeditiously method the packet and route it.

H. Routing

IPv6 reduces the size of the routing tables and make it more hierarchical and efficient. The fragmentation is handled by the source device and not by router. The device uses a protocol for finding the path's maximum transmission unit.

I. Packet Processing

IPv6 does not contain IP level checksum. So the recalculation of checksum does not happen at every router hop.

J. Multicast / NO broadcast

IPv6 supports multicast rather than broadcast. Multicast permits bandwidth-intensive packet flows to be sent to multiple destinations at the same time, saving network information measures. IPv6 doesn't have any communication bolster to any extent further. It utilizes multicast to talk with numerous hosts.

K. Tiny Operating Systems and Network Stacks

IPv6 application to the net of Things has been researched for several years. The analysis community has developed many operational systems like TinyOS and Contiki that are comparatively tiny and support the higher than protocol suites and environments. whereas the most IPv6 is extremely made in attainable options, these reduced environments have usually restricted fastidiously the options offered to satisfy IoT wants whereas reducing the dimensions of the underlying system and effort extra space for applications. as an example, a basic Contiki system takes but 20KByte, and even one supporting a full IPv6 stack and also the different high-level protocols together with DTLS will most likely work into seventy Kbyte[].

L. Increased Hardware Support

It is attainable to map several options of the physical IoT devices onto IPv6 addresses. this will ease large-scale deployments – though at the price of unveiling to anyone interested field of study options of the IoT devices thanks to the transparency of the name Service entries.

In distinction, IPv6 provides for privacy by mechanically randomizing the suffix of the IPv6 address to cover the MAC address or any serial range used as a symbol once connecting to the web.

This feature is created accessible on all in operation systems mechanically.

M. Fully Internet compliant Gateways

It is possible to build a proprietary network of smart things or to interconnect one's own smart things with rest of the world via a gateway that is fully compliant with IP requirements towards the internet.

IV. Security Benefits

A. End-to-End Encryption

IPv6 will run end-to-end-encryption. This technology was retrofitted into IPv4, it wasn't universally used and was unbroken as an optional additional. The cryptography and integrity-checking utilized in current VPNs may be a normal element in IPv6, offered for all connections and supported by all compatible devices and systems. Victimization of this system, it's harder for man-in-middle attacks and keeps the info a lot of safe and personal.

B. Secure Neighbor Discovery Protocol(SEND)

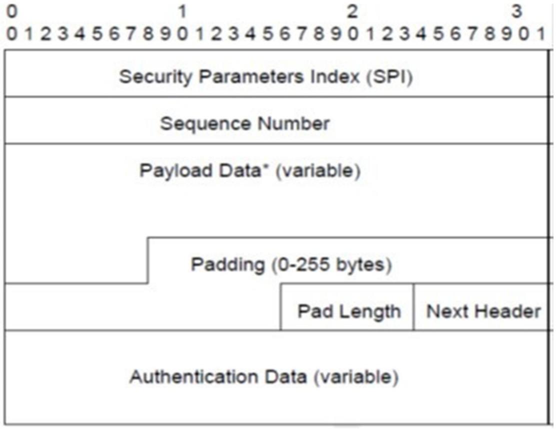
This protocol renders Address Resolution Protocol (ARP) poisoning and alternative naming-based attacks harder. And whereas not a replacement for application or service-layer verification, it still offers an improved level of trust in connections.

It is laborious to direct a network between 2 legitimate hosts and manipulate the speech communication or a minimum of observing it. IPv6 supports a more-secure name resolution that is capable of enabling science confirmation that a host claims to be at connection time.

C. ESP (Encapsulating Security Payload)

The E.S.P. provides confidentiality, authentication, and knowledge integrity. With the terms "confidentiality", we have a tendency to mean that nobody else, even the meant receiver, will scan the content of communication in transit.

E.S.P. provides anti-replay protection. The image below shows the format of an E.S.P. packet:



V. Security Threats

Even after the advancement in protocol, some attacks are not changed fundamentally for IPv6. Various improvements had been in new IPv6 protocol but still IPv6 network are still exposed to different types of attack. There is various attacks that makes IPv6 vulnerable.

Attacks such as the sniffing attacks, application layer attacks, flooding attacks, rogue devices and man-in-the-middle attacks are common between IPv4 and IPv6 protocols. There are many types of attacks and security threats only specific to IPv6.

VI. IPv6 Specific Attacks

A. Application Layer Attacks

This attack include belong buffer overflow attacks, web application attacks, different types of viruses and worms. These are the most popular attacks these days. The transition from IPv4 to IPv6 protocol will not prevent electronic devices and network from such attacks. This will also not alleviate the consequences as both the protocols are application layer protocol. . These attacks are performed at the application layer of the ISO.OSI network model.

B. Reconnaissance attacks in IPv6 networks[5]

The first phase of the larger attack is usually a reconnaissance attack. An intruder uses reconnaissance attacks to gather some essential data about the victim network that can be misused later in further attacks. For the reconnaissance attack an intruder can use active methods, such as different scanning techniques, or passive data mining.

- First, an intruder uses ping probes in order to determine which IP addresses are in use in the victim network.
- After having found an accessible system, an intruder performs the port scan technique. The subnet size in the IPv6 networks is much larger than in the IPv4 networks (the default subnet size in IPv6 networks is 64 bits).
- To perform a scan of the whole subnet an intruder should make 264 probes – so that makes it impossible.

Owing to this fact, IPv6 networks are much more resistant to reconnaissance attacks than IPv4 networks. Unfortunately, there are some types of multicast addresses used in IPv6 networks that can help an intruder to identify and attack some resources in the targeted network.

D. Security threats related to IPv6 routing headers

Routing headers can be used to avoid access controls based on addresses of destinations. Such behavior can produce some security problems. There is a possibility that an intruder sends a packet to publicly accessible address with a header including address on the victim network. By spoofing packet source addresses an intruder can easily initiate a denial of service attack by using any publicly accessible host for redirecting attack packets.

E. Security threats related to ICMPv6 and multicast

The common IPv4 practice for blocking ICMP packets as a supposed security measure should not occur, as IPv6 functioning depends on ICMPv6 for error messages, path MTU discovery, multicast group management and Neighbor Discovery.

IPv6 also relies upon multicast availability, which will have impact on firewalls, intrusion detection/search and access control rules. ICMPv6 specifications also allow an error notification response to be sent to multicast addresses. This fact can be misused by an attacker.

F. Security issues related to transition mechanism

The transition from IPv4 to IPv6 protocol will not be rapid because of already existing enormous web of IPv4 network. Both protocols need to exist in parallel as the transition will be gradual. To ensure a good and smooth transition from one protocol to other i.e. form IPv4 to IPv6 different transition mechanism are developed.

Most widely used transition mechanisms are tunneling and dual-stack configuration, a configuration that supports both IPv4 and IPv6. These mechanisms introduce some new and previously unknown threats. This makes very important for developers and deplorer to understand security implication of transition mechanisms in order to apply proper security mechanisms, such as firewalls and intrusion detection mechanisms.

VII. SIMILARITIES BETWEEN IPV6 AND IPV4

After being a new approach and new design, IPv6 is not much different from IPv4.

- Layer 2 unchanged.
- Layer 4 (TCP, UDP..) and above unchanged
- Same routing protocols : BGP, OSPF, RIP
- Same security issues: DDoS, sniffet attacks.

VIII. MAJOR DIFFERENCE BETWEEN IPV4 AND IPV6

Key	IPv4	IPv6
Deployment started in	1981	1999
Address Size	32-bit number	128-bit number
Address Format	Dotted Decimal Notation: 192.149.252.76	Hexadecimal Notation: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD
Prefix Notation	192.149.0.0/24	3FFE:F200:0234::/48
Number of Addresses	232 = ~4,294,967,296	2128 = ~340,282,366, 920,938,463,463,374, 607,431,768,211,456

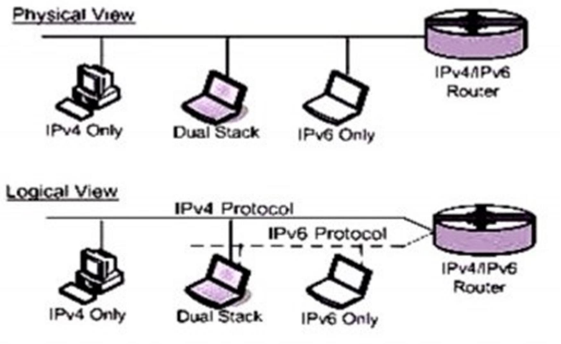
IX. TECHNOLOGIES FOR TRANSITION TO IPV6

As the need for the transition to IPv6 is growing rapidly, there are numerous applications developed and talked about for the transition:

- Double Stack
- Burrowing
- Interpretation

A. Dual Stack Approach

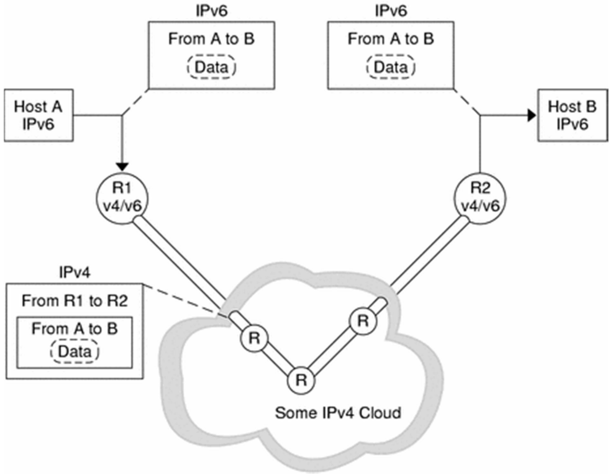
A common dual-stack migration strategy is to make the transition starting from the core to the edge. This requires enabling two TCP/IP protocol stacks on the WAN core routers, then perimeter routers and firewalls, then the server-farm routers and finally the desktop access routers. After the network supports IPv6 and IPv4 protocols, the process will start dual protocol stacks on the servers and then the edge computer systems. It comprise of running of both IPv4 and IPv6 convention stack on the gadgets that required access to both system layer advances and client gadgets. For instance, IPV6 address is auto-designed, while IPV4 address is acquire by DHCPV4.

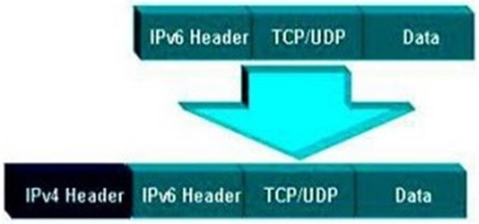


B. Tunneling

To minimize all dependencies during the transition, the routers in the path between two IPv6 nodes do not need to support IPv6. This mechanism is called **tunneling**. Basically, IPv6 packets are placed within IPv4 packets, which are then routed through the IPv4 routers.

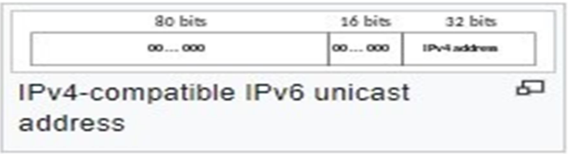
Burrowing of IPV6 bundles by an IPV4 arrange incorporate prefixing each IPV6 parcels with IPV4 headers. Because of this, burrowed bundle course over IPV4 directing framework. Epitome is performed by switch and passage hub of passage.



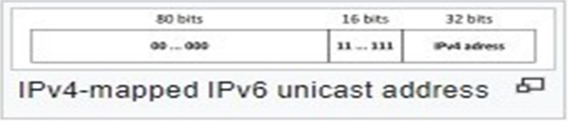


C. *IPv4 mapped IPv6 ddresses*

Hybrid dual-stack IPv6/IPv4 implementations acknowledge a special category of addresses, the IPv4-mapped IPv6 addresses. These addresses are usually written with a 96- bit prefix within the commonplace IPv6 format, and therefore the remaining thirty-two bits written within the customary dot-decimal notation of IPv4.



IPv4-compatible IPv6 unicast address



IPv4-mapped IPv6 unicast address

X. Risk Of Deployment of IPv6

Exclusive of various security threats, there can be various vulnerabilities for the IPv6 deployment. They can be:

- The attackers might have better knowledge or expertise with IPv6 than the organizations in early stage of deployment and testing.
- There can be difficulty in detecting and managing unknown or unauthorized IPv6 assets on existing IPv4 production networks.
- There can be implications of using dual-stack application and systems.
- The rapid multiplication of IPv6 and IPv4 tunnels can complicate defenses.

XI. Operator Case Studies

- Reliance Jio in India started deploying IPv6 after its local registry ran out of IPv4 address space. Reliance reported in 2017 that about 90% of its customers are using IPv6, which makes their 80% of traffic.
- Facebook is in process of removing IPv4 from their servers and data-centers. This change will bring operational improvement and innovation in their software.
- Microsoft, Akamai, Google and many more companies are gradually shifting from old IPv4 protocol to IPv6 protocols. They have the intention to remove IPv4 completely and work on a single protocol instead of dual stack approach.
- Universities throughout world have also started implementing IPv6 in their local servers and devices. They have been early deployment test locations and early adopters as a matter of research and to train for IPv6.

XII. Conclusion

IPv6 despite being not very unique as compared to IPv4 has shown many improvements in already existing network. IPv6 also houses various new features that have a upper hand in using internet connection and devices.

IPv6 is the new technology and provides great advantages over currently existing IPv4 i.e. large address space, support for real time audio and video streaming as well as quality of service (QoS), greater security, extension headers etc. Despite of these advantages the challenging issue is that it will still take time for completely migrate from IPv4 to IPv6, the reason for this is that the devices are not compatible i.e. the devices at layer 2 can work with no or a bit modification, but the devices at layer 3 are needed to be upgraded and it is also difficult to replace already existing 4 billion IPv4 quickly.

IPv6 has proven to be a revolution for the internet protocols because of different security features as well. Since the rapid growth of Internet in last few decades the need of IPv6 is must because IPv6 solves internet scaling challenges, provides flexible transition mechanisms for the current internet, and meets the needs of such new markets as mobile, personal computing devices, network entertainment and device control.

Companies and organizations have already started to migrate to IPv6 with the help of different movement techniques.

Security and Scalability are the major concerns with today's Internet, Thus we must implement IPv6 as early as possible.

XIII. Reference

1. M. D. Rey. California 90291. Internet Protocol, Darpa Internet Program, Protocol Specification. RFC 791. [Online]. Available: http://tools.ietf.org/html/rfc791

2. Dr. Sandeep Taya1 , Dr. Nipin Gupta , Deepak Goyal , Dr. Pankaj Gupta , Monika Goyal: A Review paper on Implementation Issues in IPv6 Network Technology

3. Fuliang Li, Xingwei Wang, Tian Pan and Jiahai Yang: "A case study of IPv6 Network Performance"

4. IPv6-Features: Tutorials point

5. Zagar, & Grgic, 2006; Zagar, Grgic & Snjezana, 2007

6. IPv6 – Wikipedia

7. "Deploying IPv6 Networks" -Popoviciu C., Levy-Avegnoli E., Grossetete, P. -Cisco Press.

8. "When moving to IPv6, beware the risks" – William Jackson