THOMSON REUTERS
ENDNOTE

[Ekka, January, 2017]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

IPV6 : A VIEW POINT

Sushila Ekka*

*Lecturer In Goernment Women's Polytechnic Ranchi

ABSTRACT

The Internet Protocol, IPv4, is slowly losing position because of its various limitations such as limited address space, lack of functionality and inadequate security features. In anticipation of the impending demise of IPv4, the Internet Engineering Task Force has come up with a new protocol that defines the next generation IP protocol. This protocol is known as "IPv6". IPv6 addresses all the problems faced in IPv4, and at the same time provides features like Scalability, Security, ease-of-configuration and so on. IPv6 has now been standardized and will carry TCP/IP networks and applications.

KEYWORDS: Introduction, main features, Addressing, comparison with IPV4

INTRODUCTION

The most recent version of the Internet Protocol (IP)is **Internet Protocol version 6** (**IPv6**).It is the communications protocol which provides an identification and location system for computers on networks and directs traffic across the Internet. To deal with the long-anticipated problem of IPv4 address tiredness development of IPv6 was done by the Internet Engineering Task Force (IETF).

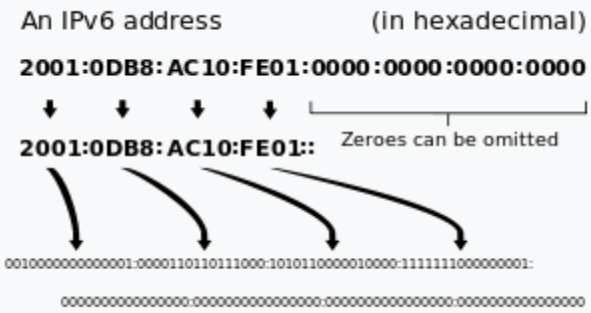
For identification and locating the devices on the Internet a unique IP address is assigned. After commercialization in the 1990s,a rapid growth of the Internet took place and it was necessary that more addresses should provided to connect as limited address space was provided by IPv4. By 1998, the Internet Engineering Task Force (IETF) had formalized the successor protocol. IPv6 uses a 128-bit address, theoretically allowing 2^{128}, or approximately 3.4×10^{38} addresses. The actual number is slightly smaller, as multiple ranges are reserved for special use or completely excluded from use. It uses 32-bit addresses and provides approximately 4.3 billion addresses The total number of possible IPv6 addresses is more than 7.9×10^{28} times as many as IPv4. The two protocols are not designed to be interoperable, complicating the transition to IPv6. However, communication between IPv4 and IPv6 hosts has been permitted by numerous devised IPv6 transition mechanisms.

IPv6 provides other technical benefits in addition to a larger addressing space. In particular, it permits hierarchical address allocation methods that facilitate route aggregation across the Internet, and thus limit the expansion of routing tables. The use of multicast addressing is expanded and simplified, and provides additional optimization for the delivery of services. Device mobility, security, and configuration aspects have been considered in the design of the protocol.

IPv6 addresses are represented as eight groups of four hexadecimal digits with the groups being separated by colons, for example 2001:0db8:0000:0042:0000:8a2e:0370:7334, but methods to abbreviate this full notation exist.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

MAIN FEATURES



Decomposition of the IPv6 address representation into its binary form

IPv6 is an Internet Layer protocol for packet-switched internetworking and provides end-to-end datagram transmission across multiple IP networks, closely adhering to the design principles developed in the previous version of the protocol, Internet Protocol Version 4 (IPv4). IPv6 was first formally described in Internet standard document RFC 2460, published in December 1998.

In addition to offering more addresses, IPv6 also implements features not present in IPv4. It simplifies aspects of address assignment (stateless address autoconfiguration), network renumbering, and router announcements when changing network connectivity providers. It simplifies processing of packets in routers by placing the responsibility for packet fragmentation into the end points. The IPv6 subnet size is standardized by fixing the size of the host identifier portion of an address to 64 bits to facilitate an automatic mechanism for forming the host identifier from link layer addressing information (MAC address). Network security was a design requirement of the IPv6 architecture, and included the original specification of IPsec.

IPv6 does not specify interoperability features with IPv4, but essentially creates a parallel, independent network. Exchanging traffic between the two networks requires translator gateways employing one of several transition mechanisms, such as NAT64, or a tunneling protocol like 6to4, 6in4, or Teredo.

ADDRESSING

IPv6 addresses have 128 bits. The address space of the IPv6 is designed with different philosophy in comparison with IPv4, which used subnetting to improve the efficiency of utilization of the small address space. In IPv6, the address space is deemed large enough for the expected future, and 64 bits is utilized by local area subnet for the host portion of the address, selected as the interface identifier, while the most-significant 64 bits are used as the routing prefix.

The identifier is only unique within the subnet to which a host is connected. IPv6 has a mechanism for automatic address detection, so that address auto configuration always produces unique assignments.

Address representation

IPv6 address of 128 bits are represented in 8 groups of 16 bits each. Each group is written as four hexadecimal digits and the groups are separated by colons (:). An example of this representation is 2001:0db8:0000:0000:0000:ff00:0042:8329.

For convenience, an IPv6 address may be shortened to abbreviator notations by application of the following rules.

- One or more leading zeroes from any groups of hexadecimal digits are removed; this is usually done to either all or none of the leading zeroes. For example, the group 0042 is converted to 42.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

- A double colon (::) replace repeated sections of zeroes. The double colon may only be used once in an address, as multiple use would render the address undefined. RFC 5952 recommends that a double colon must not be used to denote an omitted single section of zeroes.

An example of application of these rules:

Initial address: 2001:0db8:0000:0000:0000:ff00:0042:8329

After removal of all leading zeroes in each group: 2001:db8:0:0:0:ff00:42:8329

After omitting repeated sections of zeroes: 2001:db8::ff00:42:8329

The loopback address, 0000:0000:0000:0000:0000:0000:0000:0001, may be abbreviated to ::1 by using both rules.

As an IPv6 address may have more than one representation, the IETF has issued a proposed standard for representing them in text.

Address uniqueness

The individuality of addresses assigned by sending a neighbor solicitation message asking for the Link Layer address of the IP address is been verified by the Hosts. If any other host is using that address, it responds. However, each network card minimizes chances of duplication due to uniquely designed MAC addresses.

Whether the network is connected to any router or not is firstly determines by the host, because if not, then by using the link-local address which is already assigned to the host all nodes are reachable. A Router Solicitation message is send by host to all-routers multicast group with its link local address as source. If there is no answer an assumed is made that no routers are connected, the host after its preset number of attempts. There will be network information inside the response of a router which is needed to create a globally unique address. Whether the host should use DHCP to get further information and addresses or not are concluded by two flag bits:

- The Manage bit, that indicates whether or not the host should use DHCP to obtain additional addresses
- The Other bit, that indicates whether other information should obtain through DHCP or not by the host. The other information consists of one or more prefix information options for the subnets that the host is attached to, a lifetime for the prefix, and two flags:
- On-link: If this flag is set, the host will treat all addresses on the specific subnet as being on-link, and send packets directly to them instead of sending them to a router for the duration of the given lifetime.
- Address: This is the flag that tells the host to actually create a global address.

Link local address

A link-local address is required by all interfaces of IPv6 hosts. A link-local address is derived from the MAC address of the interface and the prefix fe80::/10. The process involves filling the address space with prefix bits left-justified to the most-significant bit, and filling the MAC address in EUI-64 format into the least-significant bits. bits are set to zero only if it remain to be filled between the two parts. The Duplicate Address Detection (DAD) method checks The uniqueness of the address on the subnet.

Global addressing

The global addresses assignments procedure is parallel to local address construction. The router advertisements are supplied to prefix on the network. multiple addresses is to be configured Multiple prefix announcements.

As defined in RFC 4291 Stateless address auto configuration (SLAAC) requires a /64 address block. Local Internet registries are assigned at least /32 blocks, which they divide among subordinate networks. The initial recommendation stated assignment of a /48 subnet to end-consumer sites (RFC 3177). This was replaced by

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

RFC 6177, which "recommends giving home sites significantly more than a single /64, but does not recommend that every home site be given a /48 either". /56s are specifically considered. It remains to be seen if ISPs will honor this recommendation. For example, during initial trials, Comcast customers were given a single /64 network.

IPv6 addresses are classified by three types of networking methodologies:

- unicast addresses: identify each network interface
- any cast addresses: identify a group of interfaces, usually at different locations of which the nearest one is automatically selected
- multicast addresses: are used to deliver one packet to many interfaces. The broadcast method is not implemented in IPv6. Each IPv6 address has a scope, which specifies in which part of the network it is valid and unique. on the local (sub-) network Some addresses are unique. Others are globally unique.

Some IPv6 addresses are reserved for special purposes, like6to4 tunneling, loopback and Teredo tunneling, as outlined in RFC 5156. As described in RFC 4193, Unique Local addresses (ULA), link-local addresses use on the local link, solicited-node multicast addresses used in the Neighbor Discovery Protocol and many other uses has made these address range special

COMPARISON WITH IPV4

On the Internet, data is transmitted in the form of network packets. IPv6 specifies a new packet format, designed to minimize packet header processing by routers. Because the headers of IPv4 packets and IPv6 packets are significantly different, the two protocols are not interoperable. However, in most respects, IPv6 is an 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 File Transfer Protocol (FTP) and Network Time Protocol (NTP), where the new address format may cause conflicts with existing protocol syntax.

Larger address space

The main advantage of IPv6 over IPv4 is its larger address space. The length of an IPv6 address is 128 bits, and that of IPv4 is 32 bits. The address space therefore has 2^{128} or approximately 3.4×10^{38} addresses.

In addition, the IPv4 address space is poorly allocated; approximately 14% of all accessible addresses were utilized in 2011. While these numbers are large, it was not the intent of the designers of the IPv6 address space to assure geographical saturation with usable addresses. Rather, the longer addresses simplify allocation of addresses, enable efficient route aggregation, and allow implementation of special addressing features. In IPv4, complex Classless Inter-Domain Routing (CIDR) methods were developed to make the best use of the small address space. The standard size of a subnet in IPv6 is 2^{64} addresses, the square of the size of the entire IPv4 address space. Thus, IPv6 actual address space utilization rates will be small, but routing efficiency and network management are enhanced by the large subnet space and hierarchical route aggregation.

IPv4 major exertion is renumbering an existing network for a new connectivity provider with different routing prefixes. However, changing the prefix announced by a few routers can in principle renumber an entire network in IPv6, since the host identifiers (the least-significant 64 bits of an address) can be independently self-configured by a host.

Multicasting

The transmission of a packet to multiple destinations in a single send operation is known as Multicasting. In IPv6 it is one of the basic conditions but in IPv4 this is an optional although commonly implemented feature. A common features and protocols is shared between IPv6 and IPv4 multicast by multicast address, by eliminating the need for certain protocols it also provides changes and improvements. 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 multicasting to address 224.0.0.1. IPv6 also provides for new multicast implementations, including simplifying the deployment of inter-domain solutions through embedding rendezvous point addresses in an IPv6 multicast group address.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

In IPv4 it is very difficult for an organization to get even one globally routable multicast group assignment, and the implementation of inter-domain solutions is arcane. 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 assignment 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.

Stateless address auto configuration (SLAAC)
Using the Neighbor Discovery Protocol via Internet Control Message Protocol version 6(ICMPv6) router discovery messages IPv6 hosts can arrange themselves automatically when connected to an IPv6 network. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet Layer configuration parameters.

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 manually using static methods.

Routers present a special case of requirements for address configuration, as they often are sources of auto configuration information, such as router and prefix advertisements. Stateless configuration of routers can be achieved with a special router renumbering protocol.

Network-layer security
Internet Protocol Security (IPsec) was originally developed for IPv6, but found widespread deployment first in IPv4, for which it was re-engineered. IPsec was a mandatory specification of the base IPv6 protocol suite, but has since been made optional.

Simplified processing by routers
In IPv6, simplifies the packet header and the process of packet forwarding. Although IPv6 packet headers are at least twice the size of IPv4 packet headers, packet processing by routers is generally more efficient because less processing is required in routers. This furthers the end-to-end principle of Internet design, which envisioned that most processing in the network occurs in the leaf nodes.

The packet header in IPv6 is simpler than the IPv4 header. Many rarely used fields have been moved to optional header extensions.

IPv6 routers do not perform IP fragmentation. IPv6 hosts are required to either perform path MTU discovery, perform end-to-end fragmentation, or to send packets no larger than the default Maximum transmission unit (MTU), which is 1280 octets.

The IPv6 header is not protected by a checksum. Integrity protection is assumed to be assured by both the link layer or error detection and correction methods in higher-layer protocols, such as TCP and UDP. In IPv4, UDP may actually have a checksum of 0, indicating no checksum; IPv6 requires a checksum in UDP. Therefore, IPv6 routers do not need to recompute a checksum when header fields change, such as the time to live (TTL) or hop count.

The *TTL* field of IPv4 has been renamed to *Hop Limit* in IPv6, reflecting the fact that routers are no longer expected to compute the time a packet has spent in a queue.

Mobility
Unlike mobile IPv4, mobile IPv6 avoids triangular routing and is therefore as efficient as native IPv6. Entire subnets can move to a new router connection point by the permit of IPv6 routers without renumbering.

Options extensibility
The IPv6 packet header has a minimum size of 40 octets. Options are implemented as extensions. Without affecting core packet, the extend in protocol for the future structure can be done. However, a widespread dropping of IPv6 packets containing extension headers were indicated in study of 2015.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Jumbograms

IPv4 limits packets to 65,535 ($2^{16}-1$) octets of payload. An IPv6 node can optionally handle packets over this limit, referred to as jumbograms, which can be as large as 4,294,967,295 ($2^{32}-1$) octets. The use of jumbograms may advance performance over high-MTU links. The Jumbo Payload Option header indicates the use of jumbograms.

Privacy

Activities of each device can potentially be tracked by IPv6 like IPv4, as it supports globally unique IP addresses. The design of IPv6 intended to re-emphasize the end-to-end principle of network design that was originally conceived during the establishment of the early Internet. In this approach each device on the network has a unique address globally reachable directly from any other location on the Internet.

Network prefix tracking is less of a concern if the user's ISP assigns a dynamic network prefix via DHCP. Privacy extensions do little to protect the user from tracking if the ISP assigns a static network prefix. In this scenario, the network prefix is the unique identifier for tracking and the interface identifier is secondary.

In IPv4 the effort to conserve address space with network address translation (NAT) obfuscates network address spaces, hosts, and topologies. In IPv6 when using address auto-configuration, the Interface Identifier (MAC address) of an interface port is used to make its public IP address unique, exposing the type of hardware used and providing a unique handle for a user's online activity.

It is not a requirement for IPv6 hosts to use address auto-configuration, however. Yet, even when an address is not based on the MAC address, the interface's address is globally unique, in contrast to NAT-masqueraded private networks. Privacy extensions for IPv6 have been defined to address these privacy concerns, although Silvia Hagen describes these as being largely due to "misunderstanding". When privacy extensions are enabled, the operating system generates random host identifiers to combine with the assigned network prefix. These ephemeral addresses are used to communicate with remote hosts making it more difficult to track a single device.

Privacy extensions are enabled by default in Windows (since XP SP1), OS X (since 10.7), and iOS (since version 4.3). Some Linux distributions have enabled privacy extensions as well.

In addition to the temporary address assignments, interfaces also receive a stable address. Interface Identifiers are generated such that they are stable for each subnet, but change as a host moves from one network to another. In this way it is difficult to track a host as it moves from network to network, but within a particular network it will always have the same address (unless the state used in generating the address is reset and the algorithm is run again) so that network access controls and auditing can be potentially be configured.

The traditional method of generating interface identifiers in use for unique address assignments was based on MAC addressing. In favor of better privacy protection, this method has been deprecated in some operating systems with newly established methods of RFC 7217.

Privacy extensions do not protect the user from other forms of tracking at other layers, e.g. Application Layer: tracking cookies or browser fingerprinting and Link Layer: IMSI-catcher or IBeacon

CONCLUSIONS

Introduction of new features and functionality in IPv6 had made the job of the network administrator easier and overcome many of the limitations of IPv4. Where IPv6 is significantly different from IPv4, the changes are meant to improve the administration experience. Where the similarities to IPv4 remain, the IPv6 protocol feels "familiar". In the overcoming of IPv4's weaknesses, IPv6 has made great strides. The most obvious is that IPv6 has an address space of 128 bits (versus 32 bits in IPv4), which allows many more machines to be connected to a network. In addition, IPv6 improves router performance issues through the use of more succinct network datagram headers, multicast membership maintenance, reduced network broadcasts, and packet fragmentation delegation.

Major challenges to implementers are due to new technology. However, underlying architecture and principles of network design have not changed which has made the challenges superficial. Thus many changes in IPv6 are superficial. For instance, IPv6 no longer uses "private addresses [RFC 1918]" but instead uses two types of network addresses called "link-local" and "site-local" addresses. Neighbor Discovery Protocol has replaced the

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

"Address Resolution Protocol" and "Router Discovery Protocol". DHCP (Dynamic Host Configuration Protocol) is not necessary. Finally, the textbook implementation techniques that are used for many IPv4 networks are very similar for IPv6 networks. This allows IPv6 implementers to influence their existing expertise in the deployment of next generation networks using the IPv6 framework

REFERENCES

[1] *RFC 2460, Internet Protocol, Version 6 (IPv6) Specification, S. Deering, R. Hinden (December 1998)*
[2] *Google IPv6 Conference 2008: What will the IPv6 Internet look like?. Event occurs at 13:35.*
[3] *Bradner, S.; Mankin, A. (January 1995). "The Recommendation for the IP Next Generation Protocol". RFC 1752.*
[4] *Rashid, Fahmida. "IPv4 Address Exhaustion Not Instant Cause for Concern with IPv6 in Wings". eWeek. Retrieved 23 June 2012.*
[5] *Ward, Mark. "Europe hits old internet address limits". BBC. Retrieved 15 September2012.*
[6] *Huston, Geoff. "IPV4 Address Report".*
[7] *Bradner, S.; Mankin, A. (December 1993). "IP: Next Generation (IPng) White Paper Solicitation". RFC 1550.*
[8] *"Moving to IPv6: Now for the hard part (FAQ)". Deep Tech. CNET News. Retrieved3 February 2011.*
[9] *Ferguson, P.; Berkowitz, H. (January 1997). "Network Renumbering Overview: Why would I want it and what is it anyway?". RFC 2071.*
[10] *Berkowitz, H. (January 1997). "Router Renumbering Guide". RFC 2072.*
[11] *RFC 1112, Host extensions for IP multicasting, S. Deering (August 1989)*
[12] *RFC 3956, Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address, P. Savola, B. Haberman (November 2004)*
[13] *RFC 2908, The Internet Multicast Address Allocation Architecture, D. Thaler, M. Handley, D. Estrin (September 2000)*
[14] *RFC 3306, Unicast-Prefix-based IPv6 Multicast Addresses, B. Haberman, D. Thaler (August 2002)*
[15] *RFC 2675, IPv6 Jumbograms, D. Borman, S. Deering, R. Hinden (August 1999)*
[16] *Statement on IPv6 Address Privacy, Steve Deering & Bob Hinden, Co-Chairs of the IETF's IP Next Generation Working Group, 6 November 1999.*
[17] *"Neues Internet-Protokoll erschwert anonymes Surfen". Spiegel.de. Retrieved19 February 2012.*
[18] *Marten, T; Draves, R (January 2001). Privacy Extensions for Stateless Address Autoconfiguration in IPv6.*
[19] *IPv6 Essentials by Silvia Hagen, p. 28, chapter 3.5.*
[20] *Privacy Extensions (IPv6), Elektronik Kompendium.*
[21] *Overview of the Advanced Networking Pack for Windows XP, Revision: 8.14*
[22] *IPv6: Privacy Extensions einschalten, Reiko Kaps, 13 April 2011*
[23] *"Comment #61 : Bug #176125 : Bugs: "procps" package: Ubuntu". Bugs.launchpad.net. Retrieved 19 February 2012.*
[24] *Gont, F (April 2014). A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC). RFC 7217.*
[25] *Fernando Gont (September 2016). "Recommendation on Stable IPv6 Interface Identifiers".*