An Experimental of IPv6 Address Assignment for Global Unicast Address Using NS-3

Dr. P. Sumathi
Assistant Professor, PG & Research Department of Computer Science, Government Arts College, Coimbatore
Dr. Saroj Patel
Associate Professor, Department of Mathematics, Jodhpur National University, Jodhpur, Rajasthan
Prabhakaran
Ph.d Scholar, Department of Computer Application, Jodhpur National University, Jodhpur, Rajasthan

---ABSTRACT---

Internet Protocol Version 6 (IPv6) is the next generation protocol and in the near future, routers are going to become more faster and new technologies are going to reduce the Internet delay. IPv6 global unicast address is similar to IPv4 public address and globally routable. This Global unicast address assignment process provides new function called Stateless Address Auto Configuration (SLAAC) is a significant feature for host itself generating and configuring own addresses to enable communication. In this paper aims to describe experimental about IPv6 address assignment for global unicast address and evaluation of a host using various parameters such as Default router IP address, Throughput, Average End to End Delay and Domain Name Server (DNS) IP address. The study was carried out using an open source Network Simulator (NS-3) to study and analyses the behavior of IPv6 address assignment.

Keywords - **IPv6 Address, Packet Delivery ratio. SLAAC, Unicast Address.**

Date of Submission: Aug 29, 2015 Date of Acceptance: Oct 30, 2015

1. INTRODUCTION

IPv6 is the replacement protocol for Internet Protocol version 4 (IPv4). IPv6 provides the ultimate solution for the problem of shortage of existing IPv4 addresses in the global internet by using a 128-bit address, approximately $4*10^9$ total addresses in IPv4 [2]. IPv6 is Internet Layer protocols for packet switched inter networking and provides end-to-end datagram transmission across multiple numbers of networks. IPv6 was formally described in Internet standard document Request for Comment (RFC 2460). The idea of IPv6 deployment proposed by RFC 5211 [1]. During the first decade of the 21st century, the Internet has grown further to billions of addressable devices with the majority of people having some form of Internet access with that pervasive access came a wide range of applications and uses including voice, video, collaboration and social networking with a generation that has grown up with this easily accessed global network [2]. The migration to IPv6 will likely be driven by the need for plenty of network layer address; practically every mobile phone supports Internet traffic requiring the use of an Internet Protocol address. Most new cars have the capability to acquire and use an internet address, along with wireless communications, expected that the Internet would be fully migrated to IPv6 in these days. Internet Assigned Numbers Authority (IANA) declared IPv4 address pool is already depleted more than 10% Autonomous Systems (AS) announces IPv6 prefix in global Border Gateway Protocol (BGP) table [3] and most of operating systems support IPv6. However, IPv6 prefixes can be difficult to memorize. IPv6 general prefixes are a convenient tool that allows an administrator to define and reference prefixes by human-friendly names with possible host addresses. IPv6 abandons the drawbacks of IPv4, at the same time inherits many of its advantages, So IPv6 shows a more technical advantages. IPv6 address management advantages embody three aspects, such as enlargement of address space, automatic address assignment configuration and mobility support [5]. Improvements of IPv6 header mainly embody two aspects. First, simplifying the basic header, eliminating some fields such as identifier, flag, checksum and offset in the IPv4 header, this simplifies the processing of the header second, extending header, which can follow basic header with optional way and maximum flexibility. A built-in security mechanism of IPv6 comprises Internet Protocol Security (IPsec), Authentication Header (AH) and Encapsulated Security Payload (ESP). The IP4 take a best effort transmission, Quality of Service (QoS) is difficult to guarantee. IPv6 provides a good support for QoS, especially the transmission of Voice over Internet Protocol (VoIP) and other real time data stream by setting priority, label of the data flow and resource reservation.

2. GLOBAL UNICASTADDRESS

IPv6 unicast global addresses are similar to IPv4 public addresses also known as aggregatable global unicast addresses and global addresses are globally routable [4]. Table 1 shows the IPv6 unicast global address structure and corresponding fields. A modified version of the addressing hierarchy the first Top Level Aggregation (TLA) prefix (TLA 0x0001) has been divided into further blocks called "sub-TLAs" with a 13-bit sub-TLA identifier part of the reserved space and the Next Level Aggregation (NLA) space. The "slow start" of a sub-TLA, the first allocation to a TLA Registry will be a /35 block (representing 13 bits of NLA space).

Level 1				**Level 2**	**Level 3**
Public Topology				Site Topology	Interface of a node on a specific subnet
001	TLA ID	Res	NLA ID	SLA ID	Interface ID
3 bits	13 bits	8 bits	24 bits	16 bits	64 bits

Table 1. Structure of Unicast Global Address

The Regional Internet Registry (IR) making the allocation will reserve an additional six bits for the allocated sub-TLA. When the TLA Registry has fully used the first /35 block, the Regional IR will use the reserved space to make subsequent allocations. All router interfaces are required to have at least one link-local unicast address. It is recommended that link-local addresses be used for all point-to-point links, loopback addresses, and so forth. As these are not required to be visible outside the site's network, they do not require public address space. Any global unicast address space assigned must not be used for link-local purposes as there is address space reserved for these purposes. Table 2, shows detailed description about fields in unicast global address.

Field	**Description**
001	Identifies the address as an IPv6 unicast global address.
Top Level Aggregation Identifier (TLA ID)	Identifies the highest level in the routing hierarchy. TLA IDs are administered by IANA, which allocates them to local Internet registries, which then allocate a given TLA ID to a global ISP
Res	Reserved for future use (to expand either the TLA ID or the NLA ID).
Next Level Aggregation Identifier (NLA ID)	Identifies a specific customer site.
Site Level Aggregation Identifier (SLA ID)	Enables as many as 65,536 (216) subnets within an individual organization's site. The SLA ID is assigned within the site; an ISP cannot change this part of the address.
Interface ID	Identifies the interface of a node on a specific subnet

Table 2. Fields in a Unicast Global Address

3. ASSIGNING GLOBAL UNICAST ADDRESS

Neighbor Discovery Protocol (NDP) is one of the main protocols in the IPv6 suite. It is heavily used for several critical functions, such as discovering other existing nodes on the same link, determining others link layer addresses, detecting duplicate addresses, finding routers and maintaining reachability information about paths to active neighbors. The hosts to multicast a message that finds all routers on the link to announce by using two different type of information, this process uses ICMP messages called a Router Solicitation (RS) and a Router Advertisement (RA). Table 3 shows five different options for IPv6 global address assignment. Each method can use dynamic processes or static configuration, and each method can differ in terms of how a node or router gathers the other parameters such as DNS IP addresses.

Method	**Dynamic or Static**	**Prefix and Length learned from**	**Address Identification**
Stateful DHCP	Dynamic	DHCP Server	DHCP Server
Stateless DHCP	Dynamic	DHCP Server	DHCP Server
Stateless Auto configuration	Dynamic	Router, using NDP	Derived from MAC
Static configuration	Static	Local	Local configuration
Static EUI-64	Static	Local	Derived from MAC

Table 3. Types of IPv6 Address Assignment for Global Unicast Addresses

3.1 Stateful DHCP

Clients and servers exchange DHCP messages using User Datagram Protocol (UDP). The client uses a link-local address or addresses determined through other mechanisms for transmitting and receiving DHCP messages. DHCP servers receive messages from clients using a reserved, link-scoped multicast address. A DHCP client transmits most messages to this reserved multicast address, so that the client need not be configured with the address or addresses of DHCP servers. Once the client has determined the address of a server, it may under some circumstances send messages directly to the server using unicast. When a DHCP client does not need to have a DHCP server assign it IP addresses, the client can obtain configuration information such as a list of available DNS servers or NTP servers through a single message and reply exchanged with a DHCP server. To obtain configuration information the client first sends an Information-Request message to the Servers multicast address. Servers respond with a Reply message containing the configuration information for the client

[10]. This message exchange assumes that the client requires only configuration information and does not require the assignment of any IPv6 addresses. When a server has IPv6 addresses and other configuration information committed to a client. IPv6 node can use stateful DHCP to learn and lease an IP address and corresponding prefix, the IP address of the default router, and the DNS IP address. The idea works basically like DHCPv4; the node sends a multicast packet searching for the DHCP server. When a server replies, the DHCP client sends a message asking for a lease of an IP address, and the server replies, listing an IPv6 address, prefix length, and DNS IP addresses. The Stateful DHCPv6 does not supply the default router information, instead relying on Neighbor Discovery Protocol between the client and local routers [2].

3.2 Stateless DHCP

Stateless Dynamic Host Configuration Protocol service for IPv6 (DHCPv6) is used by nodes to obtain configuration information, such as the addresses of DNS recursive name servers, that does not require the maintenance of any dynamic state for individual clients. A node that uses stateless DHCP must have obtained its IPv6 addresses through some other mechanism, typically stateless address auto configuration [8]. To obtain configuration parameters through stateless DHCP, a node uses the DHCP information request message. DHCP servers respond to the nodes message with a reply message that carries configuration parameters for the node. The Reply message from the server can carry configuration information, such as a list of DNS recursive name servers. The client indicates that it is requesting configuration information by sending an Information-request message that includes an Option Request option specifying the options that it wishes to receive from the DHCP server.

3.3 IPv6 Stateless Auto configuration

Auto configuration is performed only on multicast capable links and begins when a multicast capable interface is enabled during system startup. Nodes begin the auto configuration process by generating a link-local address for the interface. A link-local address is formed by appending an identifier of the interface to the well-known link-local prefix. All interfaces on IPv6 nodes must have a link-local address, which is usually automatically configured from the identifier for an interface and the link-local prefix FE80::/10. A link-local address enables a node to communicate with other nodes on the link and can be used to further configure the node. Nodes can connect to a network and automatically generate global IPv6 addresses without the need for manual configuration or help of a server, such as a Dynamic Host Configuration Protocol server. With IPv6, A device on the link advertises any global prefixes in Router Advertisement (RA) messages, as well as its willingness to function as a default device for the link. RA messages are sent periodically and in response to device solicitation messages, which are sent by hosts at system startup. A node on the link can automatically configure global IPv6 addresses by appending its interface identifier (64 bits) to the prefixes (64 bits) included in the RA messages. The resulting 128-bit IPv6 addresses configured by the node are then subjected to duplicate address detection to ensure their uniqueness on the link. If the prefixes advertised in the RA messages are globally unique, then the IPv6 addresses configured by the node are also guaranteed to be globally unique. Device solicitation messages, which have a value of 133 in the Type field of the ICMP packet header, are sent by hosts at system startup so that the host can immediately auto configure without needing to wait for the next scheduled RA message.

3.4 Static configuration

Host addresses can only be static if subnet prefixes are also static. Static prefixes are such a long established practice in enterprise networks that it is hard to discern the reason for them, before DHCP became available, there was simply no alternative. Thus it became accepted practice to assign subnet prefixes manually and build them into static router configurations [9]. Static configuration is type in the entire 128-bit IPv6 address for the network node to knowing its full address and prefix length. The node does not need to statically configure default router and DNS IP addresses. The node can use the usual NDP process to discover any default routers and stateless DHCP to discover any default routers and stateless DHCP to discover the DNS IPv6 addresses.

3.5 Static configuration with EUI-64

Static configuration with EUI-64 is configuring the 64-bit prefix and performs the device to use and EUI-64 calculation for the interface ID portion of the addresses. RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture requires that the interface identifier portion of all unicast IPv6 addresses, except those that start with binary value 000, be 64 bits long and be constructed in Modified EUI-64 format. The security appliance can enforce this requirement for hosts attached to the local link [7]. The Main IPv6 benefits over IPv4 are capability for automatic interface address configuration. By implementing the IEEE 64-bit Extended Unique Identifier (EUI-64) format the node can automatically acquire itself a unique 64-bit IPv6 interface identifier without the need for manual or dynamic configuration. This is accomplished on Ethernet interfaces by referencing the already unique 48-bit Layer 2 address and reformatting that value to match the EUI-64 specification. RFC 2373 explain the conversion process. Convert the 48-bit MAC address to a 64-bit value, separate the MAC address into two portion of each 24-bit. The 16-bit hex value 0xFFFE is then inserted between these two values to form a 64-bit address. Invert the universal/local (U/L) flag bit 7 in the

OUI portion of the address. Globally unique addresses assigned by the IEEE originally have this bit set to zero, indicating global uniqueness. Likewise, locally created addresses, such as those used for virtual interfaces or a MAC address manually configured by an administrator, will have this bit set to one. The U/L bit is inverted when using an EUI-64 address as an IPv6 interface ID.

4. SIMULATION AND RESULT ANALYSIS

The Network Simulation 3 (NS 3.22) has been used for the running the simulation of analysis global unicast addressing. The simulation scenario in this research analysis uses the internetwork shown in Figure 1. The figure shows a diagram might see in an implementation plan, with the four IPv6 subnet numbers shown over the five links connect to nodes. The configuration process on router, which uses EUI-64 on four interfaces, and a complete IPv6 address on another. Also, the configuration includes the IPv6 unicast routing, which enables the router to route IPv6 traffic. The IPv6 address commands both enable IPv6 on the associated interfaces and define either the prefix with the EUI-64 option or the entire address. After the configuration confirm the IPv6 addresses.

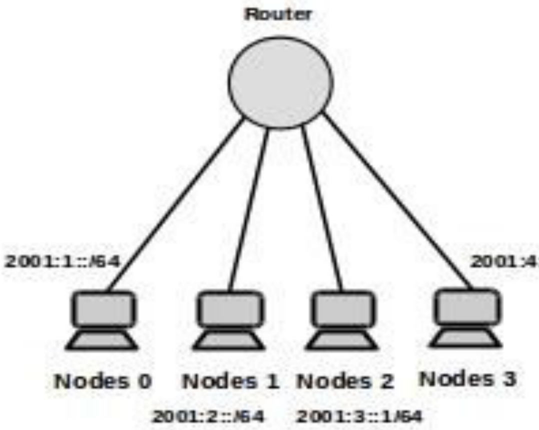

Figure 1. IP address and Device Identification

All the four interfaces now have link local addresses that begin FE80. The nodes have the configured prefixes 2001:1: /64, 2001:2:: /64, 2001:3::1 /64 and 2001:4:: /64 respectively, but with EUI-64 derived interface-IDs. MAC address shown in the table 4. Multicast Groups Joined by IPv6 Router Interfaces, the first multicast, FF02::1, represents all IPv6 devices, so router interfaces must listen for packets sent to this address. FF02::2 represents all IPv6 routers so again router must listen for packets sent to this address. Finally, the FF02::1:FF beginning value is the range for an address solicited node multicast address, used by several functions, including the duplicate address detection (DAD) and neighbor discovery (ND). The interface ID of each interface is shown in table 4.

ID	MAC Address	Unicast Address	Link - Local	Methods
0	0000:00 00:0001	2001:1::2 00:ff:fe00 :1	FE80::200: ff:fe00:1	Stateful DHCP
1	0000:00 00:0002	2001:2::2 00:ff:fe00 :4	FE80::200: ff:fe00:4	Stateless autoconfiguration
2	0000:00 00:0003	2001:3::1	FE80::200: ff:fe00:5	Static
3	0000:00 00:0004	2001:4::2 00:ff:fe00 :7	FE80::200: ff:fe00:7	Static EUI-64

Table 4. IP address and Device Identification

After running the simulation events were generated in the trace file. The trace files were analyzed using the result analysis. In this study Flow Monitor and PCAP (Packet Capture) were used for analysis. The parameters such as the following are used for the analysis

1. Default router IP address
2. Throughput and Average End to End Delay
3. DNS IP address

4.1 Default router IP address

Figure 1, shows a subset of the internetwork seen in table 4, with the same IPv6 addresses and subnets used. Routers interface has already been configured with an IPv6 address. Node 0, using stateless auto configuration to sends the RS message as an IPv6 multicast message destined to all IPv6 routers on the local link. The RS send query to all routers to respond to the questions and request of prefix and subnet. The router response with router response (RS) message, listing the prefix and with routers own IPv6 address as a potential default router IP address. Routers interface 2001:5::1/64 has been assigned as default router IP address.

4.2 Throughput and Average End to End Delay

The Throughput is one of the performance metrics to evaluate the performance. Generally it is defined as the amount of data processed in a specified amount of time. From the trace file generated by running the simulation the throughput values were captured and plotted graph with the values of Throughput of receiving bits Variation with Simulation Time as shown in Figure 2. Each packet generated by a source is routed to the destination via a sequence of intermediate nodes. Throughput is calculated packet flow for node 0 and node 1 and sending TCP packets node 0 as source and node 1 as destination.

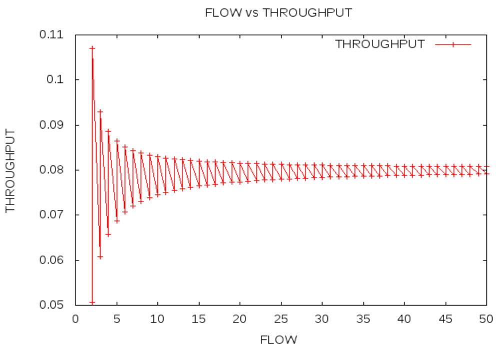

Figure 2. Flow vs. Throughput

The End-to-End delay is the sum of the delays experienced at each hop on the way to the destination of each packet. If this value is lesser, then the packets will be delivered faster from source to destination. The average End-to-End delay is computed as below.

$$\text{Average End to End Delay} = \frac{\text{Sum of End to End Delay of All packets}}{\text{Total No. Of Received Packets}}$$

4.3 DNS IP address

The stateless DHCP server supplies the DNS server IPv6 address to nodes. All hosts typically use the same small number of DNS servers, the stateless DHCP server does not need to keep track of any state information. user simply configures the stateless DHCP server to know the IPv6 addresses of the DNS servers, and the servers inform any host or other device that send request packet to keep no record of the process. Nodes that use stateless configuration also use stateless DHCP to learn the DNS server IPv6 addresses.

5. CONCLUSION

The NS-3 is an useful educational tool for simulation of IPv6 by writing relatively simple simulation scripts and evaluate the standard protocols also modify existing protocols or replace them with own solutions. From the results analysis of IPv6 address assignment shows very much improved performance and more flexible to modify the exits modules and perform the analysis. The goal is to study these protocols and analyze their performance for Global Unicast address based on performance metrics like Default router IP address, Throughput, End to End Delay and DNS IP address.

REFERENCES

[1] J. Curran, "An Internet Transition Plan", RFC 5211, IETF, Internet Engineering Task Force, July 2008; http://tools.ietf.org/html/rfc5211

[2] Wendell Odom, CCNP ROUTE 642-902, Pearson Education, Inc., Publishing as Cisco Press, 2010.p.529

[3] BGP Routing Table Analysis Reports, [online], URL:http://bgp. potaroo.net, 2015

[4] "IPv6 Address Types", [online], URL: https://technet.microsoft.com/en-us/library/cc757359%28v= ws.10%29.aspx

[5] R. Hinden et al. RFC 2373. "IP Version 6 Addressing Architecture," July 1998.

[6] "Preparing An Ipv6 Address Plan", Surf Net, http://www.ipv6forum.com/dl/presentations/Ipv6 addressing-plan-howto.pdf , ver 2, September 2013

[7] "Cisco Security Appliance Command Line Configuration Guide", http://www.cisco.com/c/en/us/td/docs/ security/asa/asa72 /configuration/guide/conf_gd/ipv6.pdf

[8] R. Droms, "Stateless Dynamic Host Configuration Protocol (DHCP) Service for Ipv6" , RFC 3736, IETF, Internet Engineering Task Force, April 2004, http://www.ietf.org/rfc/rfc3736.txt

[9] B. Carpenter, S. Jiang, "Problem Statement for Renumbering IPv6 Hosts with Static Addresses", RFC 6866, IETF, July 30, 2012

[10] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, "Dynamic Host Configuration Protocol for IPv6", RFC 3315, IETF, July 2003