International Journal of Digital Communication and Networks (IJDCN)
Volume 2, Issue 1, January 2015

Design of IPV6 Enterprise Network with Stateless Address Auto configuration

J.Sajimi Nisha[1] and Dr.S.Anila[2]

Abstract-Internet Protocol Version 6 (IPv6) is a new routing protocol and it is the most mature protocol for future internet. It is the advanced version of Internet Protocol Version 4 (IPv4). Internet protocol is used for address configuration. The IPv4 network does not support more number of users since the available address space is 32 bits only. The present IPv4 address exhaustion problem is being solved through Network Address Translation (NAT) and the transition to next generation internet. The advantages offered by the next generation internet are larger address space, mobility, security, Quality of Service (QoS). In IPv6, the stateless address autoconfiguration allow the host to configure the address itself without any help from other devices. In proposed system IPv6 network is designed and stateless address autoconfiguration is enabled. Addresses are configured initially and OSPF (Open Shortest Path First) algorithm is used in multi area where virtual link is established for configuration.

Keywords: IPv6, IPv4, SLAAC, NAT, OSPF

1 INTRODUCTION

IPv6 is the next generation protocol for the internet. It is designed to provide several advantages over current IPv4 [3]. IPv6 define network layer protocol i.e., how data is sent from one computer to another computer over packet switched networks such as the internet. IPv6 is designed to allow the internet to grow steadily, both in terms of the number of hosts connected and the total amount of data traffic transmitted, it will have a 128 bit address looking like 1234:5678:90AB:CDEF:FFFF:FFFF:FFFF:FFFF, and it will support up to 340,282,366,920,938,463,463,374,607,431,768,211,456 (3.4x1038) unique addresses.

1.1 NETWORK ADDRESS TRANSLATION (NAT) ISSUES IN IPV4

Internet Protocol version (IPv4) addresses can be from an officially assigned public range or from internal intranet private (but not globally unique) blocks. In the internal intranet private address case, a NAT function is employed to map the internal addresses to an external public address when the private to public network boundary is crossed. IPv4 theoretically allow up to 2^{32} addresses, based on a four octet address space. In IPv4 it is a 32 bit (4 byte) binary address used to identify the device. It is represented by the classification A, B, C, D, E and the range is from 0 to 255. Public globally unique addresses are assigned by the Internet Assigned Numbers Authority (IANA). NAT mechanism consists of using only a small set of public IPv4 addresses for an entire network to access to internet. A number of protocols cannot easily travel through a NAT device, and hence the use of NAT implies that many applications cannot be used effectively in all instances [7]. As a consequence, these applications can only be used in intranets. Examples include

- Multimedia applications such as videoconferencing, Voice over Internet Protocol (VoIP), or video on demand do not work smoothly through NAT devices.
- IPSec (IP Security) is used extensively for data authentication, integrity, and confidentiality. Network Address Translation does not support IPSec.

The need for obligatory use of NAT disappears with IPv6. IPv4 network is more disadvantages such as address space is less, less security, not economical, need manual configuration. Hence, IPv6 is used for enhancing security and to provide autoconfiguration.

1.2 IPV6 SPECIFICATIONS

IPv6 has a very large address space and consists of 128 bits as compared to 32 bits in IPv4[3]. Thus the decision was made to consider the 16 octets of an IPv6 address as 8 unsigned integers and writing each number with 4 hexadecimal digits separated with colons. For example: 1080:0000:0000:0000:0008:0800:200C:417A. In the example shown above, the address representation may be compressed by eliminating leading zeros within each octet and eliminating series of octets containing zeros (although this can only be applied once to an address). So, the previous IPv6 address now becomes: 1080::8:800:200C:417A. As mentioned before, an IPv6 prefix identifies how many bits of the address are assigned to the subnet work. It is represented by the notation: IPv6

1. J.Sajimi Nisha, PG scholar, Department of Electronics and Communication Engineering, Sri Ramakrishna Institute of Technology, Coimbatore, Tamil Nadu, India
(E-mail: sajiminisha@gmail.com).
2. Dr.S.Anila, Associate Professor, Department of Electronics and Communication Engineering, Sri Ramakrishna Institute of Technology, Coimbatore, Tamil Nadu, India (E-mail: anilasatish@gmail.com).

address/prefix length. For example: 1080:0:0:0:8::/80 display a subnet with an 80-bit prefix.

1.3 STATELESS ADDRESS AUTOCONFIGURATION (SLAAC)

IPv6 includes a Plug and play mechanism that facilitates the connection of equipment to the network [8]. The unicast IPv6 addressing architecture uses one half of the address (64 bits) to insert IEEE EUI-64 (Extended Unique Identifier-64) in each interface address. The use of globally unique EUI-64 on every interface allows systems to derive globally unique IPv6 addresses automatically from simple statement from neighboring systems [5].

2 PROPOSED SYSTEM

In the proposed system, IPv6 network is designed and stateless address autoconfiguration is enabled. The design of IPv6 network is carried out using routing protocol such as Open Shortest Path First (OSPF) and RIP. The stateless address autoconfiguration contains information messages such as Router Advertisement (RA) and Router Solicitation (RS), Neighbor Advertisement (NA) and Neighbor Solicitation (NS). The Proposed System is shown in Figure 2.1.

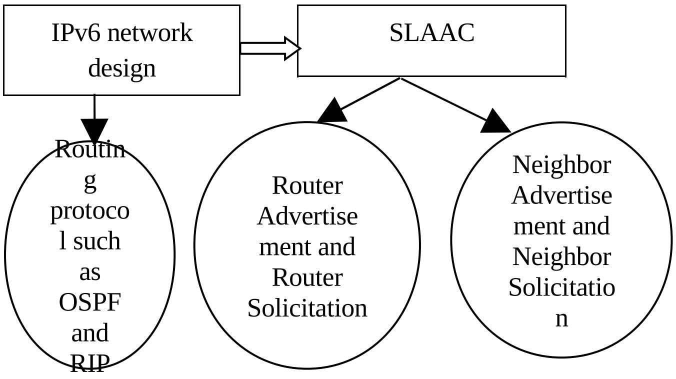

IPv6 network design
SLAAC
Routing protocol such as OSPF and RIP
Router Advertisement and Router Solicitation
Neighbor Advertisement and Neighbor Solicitation

Figure 2.1 Proposed System

2.1 OPEN SHORTEST PATH FIRST (OSPF)

Internet protocol traffic follows rules established by routing protocols, such as Open Shortest Path First (OSPF). Each router computes shortest paths using weights assigned by the network operator, and creates destination tables used to direct each IP packet to the next router on the path to its final destination. OSPF is an adaptive routing protocol for IP networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single Autonomous System (AS). OSPF is perhaps the most widely used IGP in large enterprise networks. IS-IS, another link state dynamic routing protocol, is more common in large service provider networks. The most widely used exterior gateway protocol is the BGP, the principal routing protocol between AS on the Internet [10], [6].

2.2 MULTI AREA OPEN SHORTEST PATH FIRST (MAOSPF)

As OSPF supports ‘n’ nodes, more routing information is available and processing delay will increase. So a single area could be divided into several areas. This is known as multi area concept. The area can be identified by using area id. Area 0 must be compulsorily available. Multi area concept reduces latency and hence increases network performance. OSPF routers there are 4 types such as Backbone Router (BR), Internal Router (IR), Area Border Router (ABR) and Autonomous System Boundary Router (ASBR).

Backbone Router (BR)

Backbone Router have one or more interfaces in Area 0(the backbone area).

Internal Router (IR)

An internal router is a router that has OSPF neighbor relationships with interfaces in the same area. An internal router has all its interfaces in a single area.

Area Border Router (ABR)

An Area Border Router (ABR) is a router that connects one or more areas to the main backbone network. If OSPF virtual link area used an ABR also be used to connect to the area using the virtual link to another non backbone area.

Autonomous System Boundary Router (ASBR)

An Autonomous System Boundary Router (ASBR) is a router that is connected to more than one routing protocol and that interact routing information with routers in other protocols.

2.3 RIP (ROUTING INFORMATION PROTOCOL)

The RIP is a distance vector routing protocol, which employs the hop count as a routing metric. It sends the complete routing table out to all active interfaces every 30 seconds [6]. RIP prevent routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for in this protocol. This hop limit, however, also limits the size of networks that RIP can support.

2.4 IPV6 STATELESS AUTOCONFIGURATION

Stateless Autoconfiguration exploits several new features in IPv6, including link local addresses, multicasting and NDP, and the ability to generate the interface identifier of an address from the underlying data layer address. The stateless mechanism enables a host to generate its own addresses [9]. This mechanism uses local information that is advertised by routers to generate the addresses. Routers advertise prefixes that identify the subnet or subnets that are associated with a link. Hosts generate an interface identifier that uniquely identifies an interface on a subnet. An address is formed by combining the prefix and the interface identifier. In the absence of routers, a host can generate only link local addresses. However, link local addresses are only sufficient for allowing communication among nodes that are attached to the same link [1].

It is more flexible and supports plug and play operation. Unicast addresses were used to a node [5]. Every address had two lifetimes associated with it, the valid lifetime defines the period of time duration which the address can be used and the preferred lifetime indicated the period during which the addresses can safely be used for all communication. The preferred lifetime must be shorter than the valid lifetime [8]. Neighbor Discovery (ND) is implemented within the Internet Control Message Protocol (ICMP) making all services including address resolution independent of link technologies.

2.5 ICMPV6 MESSAGES

ICMPv6 (Internet Control Message Protocol Version 6) is the implementation of the ICMP for IPv6. ICMPv6 is an integral part of IPv6 and performs error reporting and diagnostic functions and has a framework for extensions to implement future changes. ICMPv6 information messages such as Router Advertisement (RA) and Router Solicitation (RS), Neighbor Advertisement (NA) and Neighbor Solicitation (NS) and Redirect [2].

RA and RS

The RS and RA message are used to find and achieve information from router. RA uses these messages to inform other nodes existing on all links to which they are connected, of their presence. The process occurs periodically or in response to a RS message. These messages also provide other link related information. Through RA, a host can build its default router list automatically, and thus overcome the limitation of the manual configuration of the default router in IPv4. Router Solicitation upon the enabling of an interface of a node, these messages can be used to request all routers on the same local link to send Router Advertisements immediately, rather than waiting until the next periodically scheduled advertisement.

NS and NA

These messages have three main purposes. The first is to discover the link layer address of a neighbour as part of the address resolution process. This process replaces the use of ARP (Addresses Resolution Protocol) requests and replies in IPv4. The second purpose is to determine the reachability of a neighbour. The last is to detect the presence of duplicate IPv6 addresses during the address autoconfiguration process. In Neighbour Advertisement (NA) these messages are either in response to Neighbour Solicitations, or those sent by a neighbour to announce a change in its link layer address. Upon receipt of a NA, a node will update its neighbour cache which contains mappings between IPv6 and link layer addresses of neighbours.

Redirect

These messages are used by routers to inform hosts that a better link router exists for a given destination address.

3 RESULTS AND DISCUSSION

Cisco equipments and window devices are used in the proposed system. The IPv6 has been configured mainly on Cisco router 7200.

3.1 DESIGN OF IPV6 NETWORK WITH STATELESS ADDRESS AUTOCONFIGURATION

Figure 3.1 shows the designed IPv6 network with stateless address autoconfiguration. Autoconfiguration is shown in the left hand side of the network. The transmission path uses multi area OSPFv3 & RIP Protocols (RIP is by the right hand side). There are five routers linked to the switches, switch 1 and switch 2. Two hosts, C1 and C2 are connected to switch 1 and another two hosts C3 and C4 are connected to switch 2.

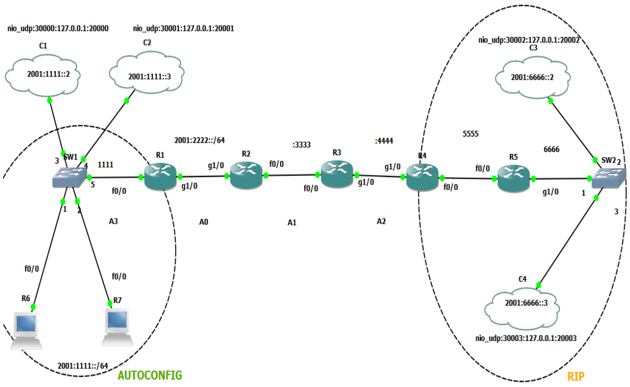
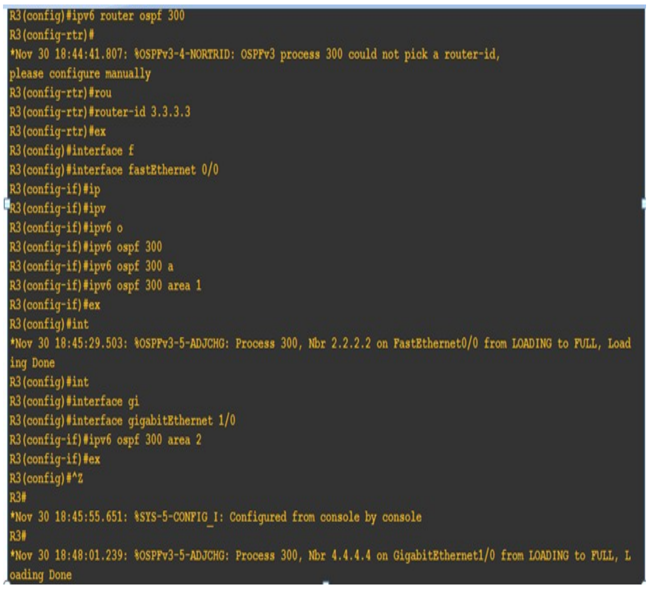


Figure 3.1 design of IPv6 network with stateless address autoconfiguration

3.2 OSPF IN MULTI AREA

OSPF supports ‘n’ nodes. In OSPF, a single area can be divided into multiple areas. This is known as multi area concept. It can have a maximum of up to 65,535 areas. The area can be identified by using area id. Area 0 must be compulsorily available. In multi area concept, different protocols can be redistributed across the network and convergence can be achieved. Multi area concept reduces latency and hence increases network performance and is shown in Figure 3.2.

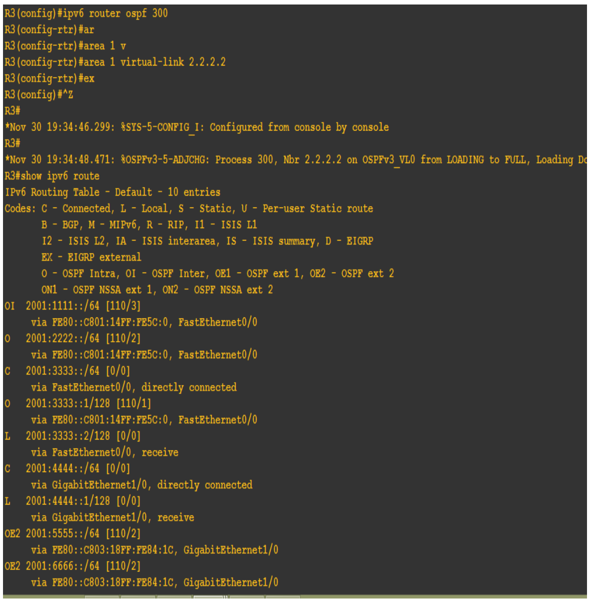


```
R3(config)#ipv6 router ospf 300
R3(config-rtr)#
*Nov 30 18:44:41.807: %OSPFv3-4-NORTRID: OSPFv3 process 300 could not pick a router-id,
please configure manually
R3(config-rtr)#rou
R3(config-rtr)#router-id 3.3.3.3
R3(config-rtr)#ex
R3(config)#interface f
R3(config)#interface fastEthernet 0/0
R3(config-if)#ip
R3(config-if)#ipv
R3(config-if)#ipv6 o
R3(config-if)#ipv6 ospf 300
R3(config-if)#ipv6 ospf 300 a
R3(config-if)#ipv6 ospf 300 area 1
R3(config-if)#ex
R3(config)#int
*Nov 30 18:45:29.503: %OSPFv3-5-ADJCHG: Process 300, Nbr 2.2.2.2 on FastEthernet0/0 from LOADING to FULL, Load
ing Done
R3(config)#int
R3(config)#interface gi
R3(config)#interface gigabitEthernet 1/0
R3(config-if)#ipv6 ospf 300 area 2
R3(config-if)#ex
R3(config)#^Z
R3#
*Nov 30 18:45:55.651: %SYS-5-CONFIG_I: Configured from console by console
R3#
*Nov 30 18:48:01.239: %OSPFv3-5-ADJCHG: Process 300, Nbr 4.4.4.4 on GigabitEthernet1/0 from LOADING to FULL, L
oading Done
```

Figure 3.2 OSPF in Multi Area

3.3 OSPF VIRTUAL LINK CONNECTION

OSPF can be used in point to multipoint because of virtual link and hence more routing information is available. Communication is accomplished via a distinct type of one-to-many connection, providing multiple paths from a single location to multiple locations using virtual link connection between router 2 and router 3. OSPF Virtual Link Connection is shown in Figure 3.3.

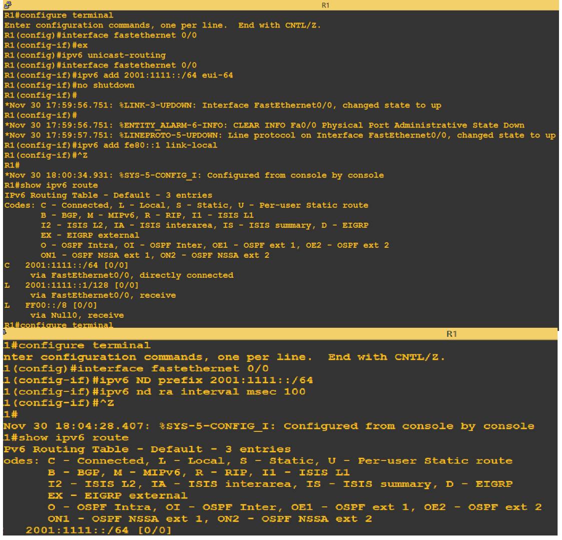


```
R3(config)#ipv6 router ospf 300
R3(config-rtr)#ar
R3(config-rtr)#area 1 v
R3(config-rtr)#area 1 virtual-link 2.2.2.2
R3(config-rtr)#ex
R3(config)#^Z
R3#
*Nov 30 19:34:46.299: %SYS-5-CONFIG_I: Configured from console by console
R3#
*Nov 30 19:34:48.471: %OSPFv3-5-ADJCHG: Process 300, Nbr 2.2.2.2 on OSPFv3_VL0 from LOADING to FULL, Loading D
R3#show ipv6 route
IPv6 Routing Table - Default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OI  2001:1111::/64 [110/3]
     via FE80::C801:14FF:FE5C:0, FastEthernet0/0
O   2001:2222::/64 [110/2]
     via FE80::C801:14FF:FE5C:0, FastEthernet0/0
C   2001:3333::/64 [0/0]
     via FastEthernet0/0, directly connected
O   2001:3333::1/128 [110/1]
     via FE80::C801:14FF:FE5C:0, FastEthernet0/0
L   2001:3333::2/128 [0/0]
     via FastEthernet0/0, receive
C   2001:4444::/64 [0/0]
     via GigabitEthernet1/0, directly connected
L   2001:4444::1/128 [0/0]
     via GigabitEthernet1/0, receive
OE2 2001:5555::/64 [110/2]
     via FE80::C803:18FF:FE84:1C, GigabitEthernet1/0
OE2 2001:6666::/64 [110/2]
     via FE80::C803:18FF:FE84:1C, GigabitEthernet1/0
```

Figure 3.3 OSPF Virtual Link Connection

3.4 STATELESS ADDRESS AUTOCONFIGURATION

In IPv6 SLAAC, the node creates the rightmost 64 bits IID, which identifies an individual node within a local network. The IID is often configured from the EUI-64 that is generated based on the interface hardware identifier, usually the MAC address of the network. Autoconfigurations of router 1 and 7 is shown in Figure 3.4.



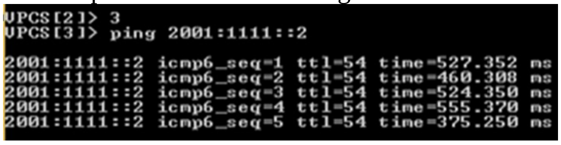
```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface fastethernet 0/0
R1(config-if)#ex
R1(config)#ipv6 unicast-routing
R1(config)#interface fastethernet 0/0
R1(config-if)#ipv6 add 2001:1111::/64 eui-64
R1(config-if)#no shutdown
R1(config-if)#
*Nov 30 17:59:56.751: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
R1(config-if)#
*Nov 30 17:59:56.751: %ENTITY_ALARM-6-INFO: CLEAR INFO Fa0/0 Physical Port Administrative State Down
*Nov 30 17:59:57.751: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config-if)#ipv6 add fe80::1 link-local
R1(config-if)#^Z
R1#
*Nov 30 18:00:34.931: %SYS-5-CONFIG_I: Configured from console by console
R1#show ipv6 route
IPv6 Routing Table - Default - 3 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2001:1111::/64 [0/0]
     via FastEthernet0/0, directly connected
L   2001:1111::1/128 [0/0]
     via FastEthernet0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#configure terminal
```

```
1#configure terminal
nter configuration commands, one per line.  End with CNTL/Z.
1(config)#interface fastethernet 0/0
1(config-if)#ipv6 ND prefix 2001:1111::/64
1(config-if)#ipv6 nd ra interval msec 100
1(config-if)#^Z
1#
Nov 30 18:04:28.407: %SYS-5-CONFIG_I: Configured from console by console
1#show ipv6 route
Pv6 Routing Table - Default - 3 entries
odes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
    2001:1111::/64 [0/0]
```

Figure 3.4 Router Autoconfiguration

3.5 OUTPUT OF IPV6 NETWORK AND SLAAC

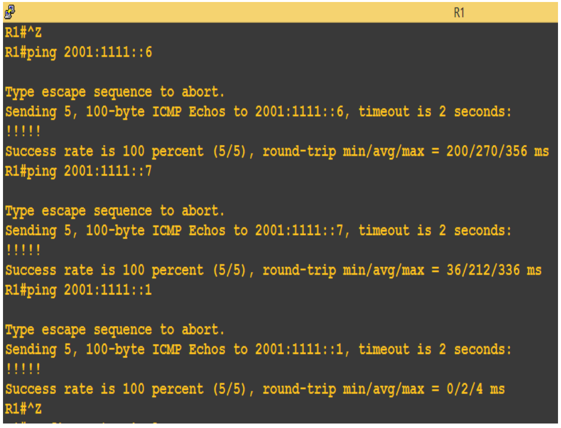
Outputs of IPv6 Network and SLAAC along with the sent packets are shown in Figures 3.5 and 3.6.



```
UPCS[2]> 3
UPCS[3]> ping 2001:1111::2

2001:1111::2  icmp6_seq=1  ttl=54  time=527.352 ms
2001:1111::2  icmp6_seq=2  ttl=54  time=460.308 ms
2001:1111::2  icmp6_seq=3  ttl=54  time=524.350 ms
2001:1111::2  icmp6_seq=4  ttl=54  time=555.370 ms
2001:1111::2  icmp6_seq=5  ttl=54  time=375.250 ms
```

Figure 3.5 Output of IPv6 Network



```
R1#^Z
R1#ping 2001:1111::6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1111::6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 200/270/356 ms
R1#ping 2001:1111::7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1111::7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/212/336 ms
R1#ping 2001:1111::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1111::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/4 ms
R1#^Z
```

Figure 3.6 Output of SLAAC

4 CONCLUSION

The data transmission in IPv6 configured network and package for the enhancing reliability for transmitting packets in IPV6 network has been developed using GNS3 software. The Simulator is an extremely useful tool for the network valuable to redirect and balance various other routers. The OSPF protocol is used in various networks like, point to point, point to multipoint and multi area. Hence fast convergence is achieved, thereby increasing the network performance. The Stateless autoconfiguration is automatically configured and has possession of address in a protected manner.

REFERENCES

[1] Ahmad AlSa'deh, Hosnieh Rafiee, and Christoph Meinel, “IPv6 Stateless Address Autoconguration Balancing Between Security, Privacy and Usability,” 5th International Symposium on Foundations & Practice of Security (FPS), October 2012.

[2] A. Conta and S. Deering, “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) specification,” RFC 2463, The Internet Society, December 1998 [Online] Available: http://www.faqs.org/rfcs/rfc2463.html.

[3] S. Deering and S. Hinden, “Internet Protocol Version 6 (IPv6) Specification,” RFC 2460 (Draft Standard), IETF, December 1998. [Online] Available: http://www.faqs.org/rfcs/rfc2460.html.

[4] R. Hinden and B. Haberman “Unique Local IPv6 Unicast Addresses,” Internet DRAFT, January 2005.

[5] JoAnn W. Klinedinst “IPv6 Features and Benefits,” the Healthcare Information and Management Systems Society (HIMSS), 2008.

[6] P. Ramya N. Gowtham, N. Sri Guruprassad , S. Suresh Kumar , K. Vinoth , Vishnu Vinod, ‘IMPLEMENTING OSPF PROTOCOL IN CISCO 2800 SERIES ROUTER’, International Journal of Innovations in Engineering and Technology (IJIET) Vol. 1 ISSN: 2319-1058, December 2012.

[7] Shiang Ming Hunag and Quincy Wu “A Survey of NAT Behaviour Discovery in VoIP Applications,” Journal of Internet Technology Volume 12 No.2, pp 199-210, 2011.

[8] Thomas Narten, “Neighbor discovery and stateless autoconfiguration in IPv6”, IEEE Internet computing, August 1999.

[9] S. Thomson, T. Narten and T. Jinmei, “IPv6 Stateless Address Autoconfiguration,” RFC 4862 (Draft Standard), IETF, September 2007.

[10] V. Vetriselvan, Pravin R.Patil and M. Mahendran, “Survey on the RIP, OSPF, EIGRP Routing Protocols,” (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2), pp 1058-1065, 2014.