IP Tunneling and Stateless DHCPv6 Implementation in an Enterprise Network

Adeyinka A. Adewale[1], Victor O. Matthews[2], Oboyerulu E. Agboje[3], Chinonso Okereke[4], David Ehigbochie[5]
[1,2,3,4,5]Department of Electrical and Information Engineering, Covenant University, Canaanland, Ota, Nigeria.

ABSTRACT

IPv4 has so many limitations such as limited assignable addresses, complex subnetting structure, and inefficient employment of NAT among others. It is because of these shortcomings of IPv4 that IPv6 protocol was introduced. IPv6 increases efficiency in routing and packet processing, promotes a simplified network configuration, supports new services and adds to the improvement QoS by reducing latency during packet transfer. There is therefore a need to move to the IPv6 platform. However, such a process is not automatic but deliberate and requires dealing with the current complexities of the IPv4 network. Tunneling is one of the common ways of transiting from IPv4 to IPv6 and vice versa. In this paper we simulated an IPv6to4 tunnel using cisco packet tracer and GNS software. It was shown that tunneling is a possibility and an effective step to preserving IPv4 infrastructure investments towards migrating from IPv4 to IPv6.

Keywords –IPv4, IPv6, Stateless DHCPv6, Tunneling.

I. INTRODUCTION

IPv4 has been the network layer protocol from the beginning of the internet age which has spanned over 30 years. However it is facing many limitations and challenges such as address exhaustion, routing scalability, broken end to end property, complex subnetting structure, and inefficient address translation slows down the network among others. The IPv4 address space has already run out and the internet scale is still growing fast especially on the user side. One reason for the fast growth of the internet is the use of mobile devices. It is because of these shortcomings of IPv4 that IPv6 protocol was introduced [1]. IPv6 increases efficiency in routing and packet processing, promotes a simplified network configuration, supports new services and improves Quality of Service (QoS) by reducing latency during packet transfer. IPv6 is the latest Internet Protocol (IP) which allows the use of a new and simplified IP header, new and expanded addressing architecture, improves support for IP options, integrated security mechanisms, flow labeling, neighbour discovery and auto configuration. These are features that will support the growing trend of the present internet world even as the number of nodes are increasing compared with IPv4 [2][3].

There is therefore a need to move to the IPv6 platform. Meanwhile, such a process is not automatic or simple but deliberate and requires dealing with the current complexities of the IPv4 network. This is because IPv6 has no inbuilt compatibility for IPv4. There have been different solutions proffered to this transition problem. One of the common solutions is tunneling. Tunneling was defined in [4] as a mechanism that allows IPv6 domains connected via IPv4 networks to communicate with each other or to allow isolated IPv6 hosts not directly connected to an IPv6 router but only to IPv4 machines to reach the wider IPv6 network.

The rest of this paper is organized as follows: Section II makes an overview of some reviewed previous work on IPv4 to IPv6 transition. In Section III, the design of the system to be simulated is explored while the implementation of the simulation is provided in Section IV and Section V is the conclusion.

II. LITERATURE REVIEW

Network address translation (NAT) has been a basic part of the 32-bits IPv4 addressing scheme. Though its deployment delayed the migration to IPv6 but not without its obvious disadvantages of breaking end-to-end characteristics of the Internet. It was said that to establish communication of IPv6 hosts with the hosts of IPv4 should be through translation mechanisms which can be classified into three layers that is network layer, transport and application layers. NAT-PT makes the network layer translation possible while the Transport Relay Translator (TRT) enables exchange of TCP and UDP traffic between IPv6-only hosts and IPv4-only hosts. The translation mechanism at the application layer is socket layer based. Communication requests between different protocols (IPv6 and IPv4 nodes) are translated through the Socks64 gateway. The tunneling approach can be categorized into four which are IPv4 over IPv6 tunnel, IPv6 over IPv4 tunnel, tunnel traversing through NATs and other tunnels. Others in this case refers to IPv4, MPLS tunnels, SSL and SSH at layer 4. In [5] it was mentioned that the transition from IPv4 to IPv6 will be complex because not only infrastructure upgrade will be involved. This is because only few applications are IPv6 ready [6] so there will be upgrade of IP version dependent applications and need for some security considerations.

In IPv6 networks, tunnels are setup between hosts and the servers called tunnel servers which serve as aid for the computer nodes to get connected to neighbouring networks. Thus it implies that hosts on different IPv6 domains may want to communicate with each other via IPv4 domain. Such connections can be achieved by tunneling and it is required that the hosts have a dual IP stack for the purpose of sending and receiving IP datagrams. In [7] and [8] tunnel brokers were introduced as means of updating IPv4 to IPv6 without charges.

Tunneling is a means of traversing heterogeneous networks and its plane operation is data encapsulation and decapsulation. The tunnel endpoints are deployed at the two ends of the network to be traversed. The entry point is the ingress while the exit point from the network is the egress. This is the scenario when a host in IPv6 domain/network is communicating with another IPv6 host through an IPv4 network and it can also be in the reversed order but whichever case, it has been said by [6] that the transition from IPv4 to IPv6 will take quite some time hence, the need for means of interconnectivity of IPv4 networks to IPv6 networks [8]. Moreover, a strategic approach to migration from IPv4 to IPv6 is provided in [9]. It was said that the tunnel endpoints are the translators at the edges (ingress and egress) and a table of translation matrix for possible scenarios of transition strategies was provided.

III. METHODOLOGY AND DESIGN

This is achieved using by using CISCO Packet Tracer software for test simulation and GNS3 software for the final phase of the simulation [10]. The simulation will include up to date configuration with respect to Network security, Administrative control, Telnet abilities and prevent one point of failure in connections to internetworks and to the Internet Service Provider. To make this happen, an enterprise network was designed and simulated which was conceptualized as in Fig. 1. IPv6 Tunneling was employed to enable hosts on IPv6 network to be routable through the frame relay IPv4 WAN.

The network diagram in Fig. 2 modeled after the conceptual view is comprised of the core layer switches, distribution layer switches as well as the access layer switches based on Cisco's hierarchical model. The core office network is usually modularized into these three [11][12]. The core layer is the layer where high speed switching is implemented which is crucial to corporate communications. The distribution layer is an isolation point between the access layer and core layer and is responsible for the network policy, security filtering and address aggregation/summarization. The access layer provides the endpoint user with access to local segments on the network. The IPv6 networks are purely IPv6 domains and in addition, stateless address configuration, EIGRP, IPv6 tunneling mode and IPv6 routing table were implemented.

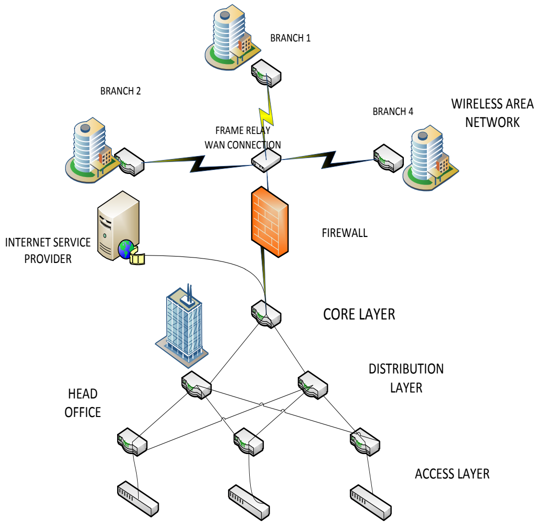

Figure 1: Conceptual Network Design

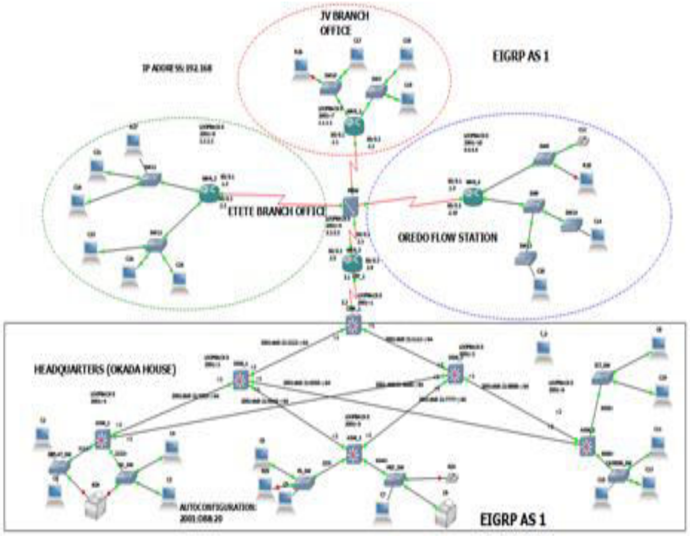

Figure 2: Network Diagram

IV. IMPLEMENTATION AND TESTING

Initial configurations of each router and verification of the configuration was carried out. A multilayer switch was run as a router and IPv6 packets were routed in the network but before that IP addresses were assigned to the links between the core, distribution and access layer switches. Loopback interfaces were created within the multilayer switches ASW_1, ASW_2,ASW_3 DSW_1 and DSW_2 for the purpose of testing and run, EIGRP routing protocol to enable layer three switching. Also, loopback interfaces were created within the multilayer switches of ASW_1, ASW_2, ASW_3 DSW_1 and DSW_2 for the same purpose as mentioned. Table 1 shows the routing table of the core switches successful pings to the directly connected routers between the multilayer switches:

TABLE 1: EIGRP Verification for each Router

```
CSW_1#show ipv6 route
IPv6 Routing Table - 33 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
LC  2001::1/128 [0/0]
     via ::, Loopback0
D   2001::2/128 [90/409600]
     via FE80::C00D:AFF:FE38:0, FastEthernet0/0
D   2001::3/128 [90/409600]
     via FE80::C00F:AFF:FE38:0, FastEthernet0/1
D   2001::4/128 [90/435200]
     via FE80::C00F:AFF:FE38:0, FastEthernet0/1
     via FE80::C00D:AFF:FE38:0, FastEthernet0/0
D   2001::5/128 [90/412160]
     via FE80::C00F:AFF:FE38:0, FastEthernet0/1
D   2001::6/128 [90/412160]
     via FE80::C00D:AFF:FE38:0, FastEthernet0/0
D   2001:DB8:20:1111::/64 [90/309760]
     via FE80::C00F:AFF:FE38:0, FastEthernet0/1
     via FE80::C00D:AFF:FE38:0, FastEthernet0/0
D   2001:DB8:20:2222::/64 [90/309760]
     via FE80::C00F:AFF:FE38:0, FastEthernet0/1
     via FE80::C00D:AFF:FE38:0, FastEthernet0/0
D   2001:DB8:20:3333::/64 [90/309760]
     via FE80::C00F:AFF:FE38:0, FastEthernet0/1
D   2001:DB8:20:4444::/64 [90/309760]
     via FE80::C00F:AFF:FE38:0, FastEthernet0/1
D   2001:DB8:20:5555::/64 [90/309760]
     via FE80::C00D:AFF:FE38:0, FastEthernet0/0
D   2001:DB8:20:6666::/64 [90/309760]
     via FE80::C00D:AFF:FE38:0, FastEthernet0/0
C   2001:DB8:21:1111::/64 [0/0]
     via ::, FastEthernet0/1
L   2001:DB8:21:1111::1/128 [0/0]
     via ::, FastEthernet0/1
C   2001:DB8:21:2222::/64 [0/0]
     via ::, FastEthernet0/0
L   2001:DB8:21:2222::1/128 [0/0]
     via ::, FastEthernet0/0
D   2001:DB8:21:3333::/64 [90/307200]
     via FE80::C00D:AFF:FE38:0, FastEthernet0/0
D   2001:DB8:21:5555::/64 [90/284160]
     via FE80::C00D:AFF:FE38:0, FastEthernet0/0
D   2001:DB8:21:6666::/64 [90/307200]
     via FE80::C00F:AFF:FE38:0, FastEthernet0/1
D   2001:DB8:21:7777::/64 [90/284160]
     via FE80::C00F:AFF:FE38:0, FastEthernet0/1
```

```
CSW_1#ping 2001::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
CSW_1#ping 2001::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/28/68 ms
CSW_1#ping 2001::3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/20/48 ms
CSW_1#ping 2001::4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/34/60 ms
CSW_1#ping 2001::5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/39/72 ms
CSW_1#ping 2001::6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::6, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
8/39/52 ms
```

Frame relay is an internet protocol used to connect WANs across a network and to accomplish this, loopback interface were assigned to each WAN router (WAN_1- 4) test were carried out by pinging other WANs from WAN_3, Table 2 shows the routing table after frame relay full mesh network was applied to WAN_3.

Table 2: Frame-Relay Verifications for each WAN

```
WAN_3#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
D       1.1.1.1 [90/30757632] via 192.168.2.2, 00:29:41, Serial0/0.1
     2.0.0.0/32 is subnetted, 1 subnets
D       2.2.2.2 [90/30757632] via 192.168.2.6, 00:29:41, Serial0/0.2
     3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3 is directly connected, Loopback0
     4.0.0.0/32 is subnetted, 1 subnets
```

```
D      4.4.4.4 [90/30757632] via 192.168.2.10, 00:29:40, Serial0/0.3
D    192.168.1.0/24 [90/31141632] via 192.168.2.10, 00:29:41, Serial0/0.3
               [90/31141632] via 192.168.2.6, 00:29:42, Serial0/0.2
               [90/31141632] via 192.168.2.2, 00:29:42, Serial0/0.1
     192.168.2.0/30 is subnetted, 3 subnets
C      192.168.2.8 is directly connected, Serial0/0.3
C      192.168.2.0 is directly connected, Serial0/0.1
C      192.168.2.4 is directly connected, Serial0/0.2
     192.168.3.0/29 is subnetted, 1 subnets
C      192.168.3.0 is directly connected, Serial0/1
WAN_3#ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/55/104 ms
WAN_3#ping 2.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/39/84 ms
WAN_3#ping 3.3.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
WAN_3#ping 4.4.4.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/32/64 ms
```

Tunneling encapsulates IPv6 packets routed over IPv4 network which is not possible normally. Table 3 shows the routing table filtering out tunneling routes only after tunneling has being applied and successful routing of IPv6 packets over an IPv4 network verified by successful pings to IPv6 loopback interfaces at WAN_1-4.

Table 3: Tunnel Configurations and Verification

```
CSW_1#show ipv6 route
IPv6 Routing Table - 33 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B -
BGP
      U - Per-user Static route, M - MIPv6
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS
summary
      O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1,
OE2 - OSPF ext 2
      ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
      D - EIGRP, EX - EIGRP external
S   2001::7/128 [1/0]
     via ::, Tunnel15
S   2001::8/128 [1/0]
     via ::, Tunnel25
S   2001::9/128 [1/0]
     via ::, Tunnel35
S   2001::10/128 [1/0]
     via ::, Tunnel45C   2003:15::/64 [0/0]
     via ::, Tunnel15
L   2003:15::2/128 [0/0]
     via ::, Tunnel15
C   2003:25::/64 [0/0]
     via ::, Tunnel25
L   2003:25::2/128 [0/0]
     via ::, Tunnel25
C   2003:35::/64 [0/0]
     via ::, Tunnel35
L   2003:35::2/128 [0/0]

CSW_1#ping 2001::7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::7, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
8/39/68 ms
CSW_1#ping 2001::8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::8, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
36/59/88 ms
CSW_1#ping 2001::9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::9, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
4/16/40 ms
CSW_1#ping 2001::10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::10, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
12/34/52 ms
```

The tunnels can be nullified by typing 'no' before the tunnel commands in global configuration mode, the result is shown in Table 4:

Table 4: Tunneling Configurations and Verifications

```
CSW_1#ping 2001::7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::7, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
CSW_1#ping 2001::8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::8, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
CSW_1#ping 2001::9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::9, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
CSW_1#ping 2001::10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::10, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
CSW_1#ping 1.1.1.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/41/76 ms
CSW_1#ping 2.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/36/68 ms
CSW_1#ping 3.3.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/19/36 ms
CSW_1#ping 4.4.4.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/41/72 ms
CSW_1#ping 5.5.5.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
CSW_1#
```

From the table above it can be noticed that pings to the IPv4 loopbacks went through, while those to the IPv6 loopbacks did not go through because the 6-to-4 tunnel has being removed and normally IPv4 networks cannot route IPv6 packets. Also, authentication interfaces were set up on all devices on the network for telnet purpose to prevent an unauthorized person from gaining access to the device command line interface (CLI).

The stateless mechanism allows a host to generate its own addresses using a combination of locally available information and information advertised by routers. The stateless approach is used when a site is not particularly concerned with the exact hosts addresses use, so long as they are unique and properly routable [13]. Stateless address auto-configuration is used to configure both link-local addresses and additional non-link-local addresses by exchanging router solicitation and router advertisement messages with neighboring routers.

This demonstration shows how the stateless auto-configuration can be setup, as well as a nifty stateless DHCPv6 implementation that can assist with the other configuration information. The stateless DHCPv6 was applied to the access interfaces of ASW_2 and Table 4 shows what happen before and after auto-configuration was applied to the clients' (T_S) system (cisco user).

Table 5: Stateless DHCPv6 Verification

```
T_S>enable
T_S#sh ipv6 interface brief
FastEthernet0/0          [administratively down/down]
T_S#show ipv6 dhcp int fa0/0
T_S#!no address(es) yet
T_S#let us see what happens after I apply auto config to the interface
fastethernet0/0
T_S#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
T_S(config)#int f0/0
T_S(config-if)#no shutdown
T_S(config-if)#ipv6 add autoconfig
T_S(config-if)#end
T_S#
*Mar  1 00:00:58.423: %SYS-5-CONFIG_I: Configured from console by
console
*Mar  1 00:00:59.027: %LINK-3-UPDOWN: Interface FastEthernet0/0,
changed state to up
*Mar  1 00:01:00.027: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/0, changed state to up    T_S#sh ipv6 interface
brief
FastEthernet0/0          [up/up]
    FE80::CE00:16FF:FE74:0
    2001:DB8:20:4444:CE00:16FF:FE74:0
T_S#show ipv6 dhcp int fa0/0
FastEthernet0/0 is in client mode
  State is IDLE
  List of known servers:
    Reachable via address: FE80::C00B:14FF:FE7C:1
    DUID: 00030001C20B147C0000
    Preference: 0
    Configuration parameters:
      DNS server: 2001::1
      Domain name: ine.com
  Rapid-Commit: disabled
T_S#
```

V. CONCLUSION

It was mentioned that IPv4 is almost get exhausted with the last set of its IP addresses being already assigned and that the inexhaustible IPv6 protocol is being introduced as a most successful replacement for networking devices [14]. However, no matter how urgent this protocol migration is required, it has to be gradual because there are still applications and network domains that are not IPv6 compatible and the investments in place cannot be jeopardized. Therefore, the need for IPv6to4 tunneling as a means of IP protocol translation. A brief overview of the impact of IPv6 in an enterprise network as it provides a better Quality of Service (QoS) than IPv4 was given. In this implementation, the successful pings show that there in network connectivity over the frame-relay network. The show run command displays IPv6 running configurations as desired for an IPv6 network. Virtual local area network was incorporated into the network to help logically separate the different arms of the enterprise and give priorities to whom it is due to. This research has come up with design that is very secure (IPsec), which provides confidentiality, authentication and data integrity. IPv6 simplified packet header has made packet processing more efficient compared with IPv4 because IPv6 contains no IP-level checksum, so, the checksum does not need to be recalculated at every router hop. Likewise, compatibility issue has been resolved by eliminating NAT and true end-to-end connectivity at the IP layer is restored, enabling new and valuable services. Peer-to-peer networks are easier to create and maintain, and QoS has become more robust [15][16]. It has been shown in this that tunneling is a possibility and an effective step towards migrating from IPv4 to IPv6.

REFERENCES

[1] M. Levy, Six Benefits of IPv6. www.networkcomputing.com/IPv6/six-benefits-of IPv6. Retrieved February 26, 2016.

[2] A.S. Narayanan, M.K. Mohideen & M.C. Raja, IPv6 Tunneling Over IPv4, *International Journal of Computer Science Issues*, 9(2), 2012, 599–604.

[3] J. Bi, J. Wu, & X. Leng, IPv4/IPv6 Transition Technologies and Univer6 Architecture, *International Journal of Computer Science and Network Security*, 7(1), 2007, 232-243.

[4] P. Wu, Y. Cui, J. Wu, J. Liu, C. Metz, Transition from IPv4 to IPv6: A State-of-the-Art Survey, *IEEE Communications Surveys & Tutorials*, 2012 IEEE, 1553-877X. DOI:10.1109/SURV.2012.110112.00200.

[5] A. Albkerat & B. Issac, Analysis of IPv6 Transition Technologies, *International Journal of Computer Networks & Communications,* 6(5), 2014. DOI: 10.5121/ijcnc.2014.6502

[6] B.R. Dawadi, S.R. Joshi & A.R. Khanal, Service Provider IPv4 to IPv6 Network Migration Strategies, *Journal of Emerging Trends in Computing and Information Sciences*, 6(10), 2015, 565-572.

[7] Starting up with GNS: http://www.gns3.net. Retrieved: March 27, 2016.

[8]_A.S. Tanenbaum, "*Computer Networks"*, Pearson Education, 2006.

[9] Tom Sheldon, "Enterprise Network", www.linktionary.com/new/enterprise.html.

[10] Understanding of address configuration in automatic mode and installation of DHCPv6 Server, blog.technet.com/b/teamdhcp. Retrieved March 25, 2016.

[11] Walt Howe, A Brief History of the Internet, www.walthowe.com. Retrieved April 13, 2016.

[12] Fujitsu, Ethernet - Ethernet Prerequisite.pdf, Pg. 3, Retrieved April 11, 2016.

[13] Telcordia GR-253-Core, Synchronous Optical Networks (SONET) Transport Systems: Common Generic Criteria, 2009. Issue 5 http://telecom-info.telecordia.coom/site-cgi/ido/doc./cgi?ID=SEARCH.

[14] G. Huston, OPINION: The Mythology of IP version 6, *the Internet Protocol Journal,* 6(2). http://www.cisco/web/about/ac123/ac147/achivedissues/ipj_6_2/myth_of_IPv6.html.

[15] D. O. Awduche, The Benefits of IPv6 for Enterprises, http://www.verizon.com. Retrieved, February 27, 2016.

[16] Implementing EIGRP for IPv6 by Cisco, www.cisco.com. Retrieved March 25, 2016.