2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)

IPv4 to IPv6 Migration and Performance Analysis using GNS3 and Wireshark

Ravi Kumar CV
School of Electronics Engineering (SENSE)
Vellore Institute of Technology
Vellore, India
ravikumar.cv@vit.ac.in

Hrithik Goyal
School of Electronics Engineering (SENSE)
Vellore Institute of Technology
Vellore, India
ravikumar.cv@vit.ac.in

***Abstract*—The internet is a system of various interconnected networks accessible worldwide. IPv4, a layer 3 protocol enables two or more computers to share the data among them. At the beginning of 2011, all the IPv4 address space was exhausted and now we are going for IPv6. Migration techniques have been proposed in this project, to migrate to the IPv6 network. Dual stack transition and manual tunneling transition techniques have been proposed in this paper to transmit an IPv6 packet through an IPv4 network. These transition techniques have been simulated using Graphical Network Simulator (GNS3). The transfer of packets has been analyzed in both static and dynamic routing scenarios. Wireshark has been used to capture a live packet on the wire and to analyze the packet header. We investigate migration techniques performance in terms of success rate and the minimum, average and maximum round – trip time and latency and throughput.**

Keywords—IPv6, GNS3, Wireshark, Routers, Hosts, IPv4/IPv6 Transition, Static Routing, Dynamic Routing

I. INTRODUCTION

Internet Protocol (IP) is the best-known Layer 3 or Network layer protocol. Presently two versions of IP are assigned by Internet Assigned Number Authority (IANA) [1]–[3]. The designers of IPv4 did not envision the explosive growth of its use. 4.3 billion addresses seemed more than enough [4]. The IPv4 protocol is not particularly efficient in its use of the available space, with many addresses being wasted. The internet authorities started to predict address exhaustion in the late 1980s and IPv6 was developed in the 1990s as the long-term solution.

There is not a seamless migration from IPv4 to IPv6 due to IPv6 being incompatible with IPv4. The demand for transition techniques will go on until and unless a complete transition from IPv4 to IPv6 is completed. The transition to IPv6 from IPv4 can be divided into 3 phases as follows: Phase I, IPv6 network is an island in an IPv4 ocean, where IPv4 continues to dominate on global networking. Phase II, after a few years, IPv4 will become an island while IPv6 will be an ocean. At this stage, IPv6 is much bigger than IPv4. Phase III, the final phase, in this phase most of the networks are in IPv6 native [5].

As of February 2019, the percentage of IPv6 traffic according to Google statistics is 23 percent which is an increase of 20 percent over the past 5 years. Moreover, it is expected that in the coming 4 to 5 years, the IPv6 traffic will see an increase to between 30 and 40 percent. Therefore, we need to implement the solutions for transitions. These transition techniques will keep IPv4 networks running on the IPv6 networks in which IPv4 will be a small portion of the interconnected networks across the globe. IPv6 was delivered with migration techniques to cover every conceivable IPv4 upgrade case, with many being rejected by the networking community. In this paper, we investigate two popular IPv6 transition techniques Dual-Stack and Tunnelling discussed in [6], [7], [8]. We will simulate the topologies using GNS3 and then present the simulations result of these transition techniques in terms of success rate and the minimum, average and maximum round – trip time and latency and throughput. These performances considered will affect their scalability and quality of service (QoS).

This paper is organized as follows: In section II, the theory will be given. In section III system architecture will be given. In section IV, Simulation Results will be provided. In section V, the performance of both the migration techniques will be analyzed. We conclude the paper in the last section.

II. THEORY

A. IPv4 and IPv4 Addressing

The Network Layer, Layer 3 of the Open Systems Interconnection model (OSI model) is responsible for routing packets to their destinations and for Quality of service. Internet Protocol (IP) is the best-known layer 3 protocol IPv4 is a connectionless protocol with no acknowledgments at Layer 3. IP addressing is a logical addressing scheme implemented at layer 3. The network designers use IP addressing to partition the overall network into smaller subnets. An IPv4 address is 32 bits long. It is written as 4 ‘octets’ in dotted decimal format. Each octet is 8 bits long.

B. IPv6 and IPv6 Addressing

Internet Protocol version 6 (IPv6) also known as IP next generation (IPng). The Internet Engineering Task Force (IETF) as a solution for the exhausted IPv4 address space developed IPv6 in the 1990s. In addition to the larger address space, IPv6 was designed to support built-in security and host mobility. IPv6 uses a 128-bit address compared to IPv4’s 32-bit address [3]. The address is written as Y:Y:Y:Y:Y:Y:Y:Y, where each ‘Y’ is a 16-bit hexadecimal field (Hex values are 0 to 9, A to F). Each segment is 16 bits and is sometimes called hextets.

C. Need for IPv6

IPv6 provides more than $7.9*10^{28}$ times as many addresses as IPv4. In addition to the larger address space, IPv6 also needed to overcome the limitations that existed

978-1-5386-9353-7/19/$31.00 ©2019 IEEE

with IPv4, more latency, less address space, and less security.

D. Graphical Network Simulator (GNS3)

GNS3 is a network software emulator used to simulate complex networks by allowing the combination of virtual and real devices. We use GNS3 to make topologies for both Dual-Stack and Tunneling Transition techniques.

E. Wireshark

Wireshark is a packet-sniffing open source software used to analyze and troubleshoots a network. We use Wireshark to capture the packet during the tunneling transition and analyze its header [9].

F. Routing Protocols

If a router receives traffic for a network, which is not directly connected to, it needs to know to get there in order to forward the traffic. An administrator can manually add a static route to the destination, or the router can learn it via a routing protocol.

1) Static Routing: In this type of routing, the routing entries remain unchanged. The routes are added manually by entering the desired commands in command line interface (CLI). Routes can be viewed in the routing table using 'show ip route' command in 'privileged exec mode'. Routes configured using static routing need to be manually configured if any change occurs in the network topology.

2) Dynamic Routing: Routing protocols, which allow routers to advertise their best paths to known networks to each other. Routers use this information to find out their own best path to the known destinations. Routing protocols are more scalable than administrator defined static routes. If a subnet is added or removed, the routers will automatically discover that and update their routing tables. If the best path to a subnet goes down routers automatically discover that and will find a new best path if one is available.

3) OSPF: We have used the Open Shortest Path First (OSPF) protocol to design our topologies for dynamic routing. OSPF is an open standard protocol and thereby supported on all vendors equipment. OSPF is a link state routing protocol and is a part of interior gateway routing protocols (IGPs). It has a very fast convergence time and supports large networks. In link-state routing protocols, each router describes itself and its interface to its directly connected neighbors.

G. Performance Metrics

First Using Dual-stack protocol we find the latency and throughput for various cases namely, Static Ipv4, Static IPv6, Dynamic IPv4, and Dynamic IPv6. We find out which of the above dual stack techniques gives us better performance. Secondly, we use the performance metrics for tunneling techniques. At last, deduce which protocol (Dual-stack or Tunnelling) provides better performance and QoS (Quality of Service).

1) Latency: The delay before a transfer of data begins following instruction for its transfer from the client.

$$Latency = (Average\ Round\ trip\ time\ for\ Packet\ /\ 2)\ \text{ms} \quad (1)$$

2) Throughput: Also referred to as network throughput, it is the rate of successful packet delivery over a communication channel.

$$Throughput = (Packet\ Size\ /\ Latency)\ \text{Mbps} \quad (2)$$

III. System Architecture

We have used real IOS (Internetwork operating system) images to make the topologies on the GNS3. The virtual tools used is the simulation are routers, Ethernet switches and VPCs (Virtual PC's) as shown in Fig.1.

Fig. 1. Devices used in GNS3

A. Dual-Stack Transition Technique

IPv4 and IPv6 do not have to be an 'either or' decision. In a dual stack implementation, a network interface can have both an IPv4 and IPv6 address at the same time. It can communicate using either of the protocol available.

B. Design and Configuration of the Dual-Stack Transition Technique

Dual stack is designed to support both the IPv4 and IPv6 addresses on the same network interface, thereby allowing the data to transfer from IPv4 network to IPv6 network using both static and dynamic routing. The network consists of five routers, two Ethernet switches, and four end hosts. All router interfaces, as well as the hosts, have been configured with an IPv4 address as well as with an IPv6 address. The network can then communicate using either protocol.

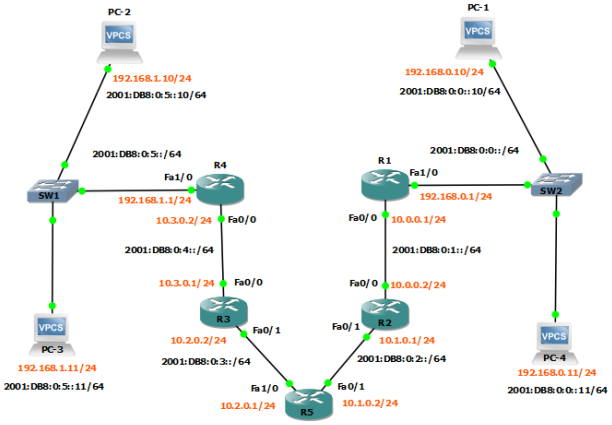

Fig. 2. Dual-Stack Topology

Fig.2 shows router R1 and router R4 are connected to end hosts using Ethernet switch. To differentiate the internal host network from the router-to-router network, the internal host network has been designed using 192.168.0.0/16 IPv4 address space. Router to router connections has been designed using 10.0.0.0/8 IPv4 address space. The IPv6 (IPng) address space used for the entire topology is 2001:db8:0::/48.

```
R4#show run | begin interface
interface FastEthernet0/0
 ip address 10.3.0.2 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2001:DB8:0:4::2/64
 ipv6 address FE80::4 link-local
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2001:DB8:0:5::1/64
 ipv6 address FE80::4 link-local
!
```

Fig. 3. Router R4 address configuration

Fig.3 shows IPv4 and IPv6 addresses assigned to the fast-Ethernet (fa) interface fa0/0 and fa1/0 on router R4. Fig.4 shows static routes for both IPv4 and IPv6 network configured on router R4, therefore R4 has reachability over the entire network. Fig.5 shows the routing table of router R4. 'S' indicates Static routes have been configured for routing within the network. The figure shows the routes for both the IPv4 and IPv6 network. 'C' indicates the connected network to the router.

```
R4#show run | begin ip route
ip route 10.0.0.0 255.255.255.0 10.3.0.1
ip route 10.1.0.0 255.255.255.0 10.3.0.1
ip route 10.2.0.0 255.255.255.0 10.3.0.1
ip route 192.168.0.0 255.255.255.0 10.3.0.1
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
ipv6 route 2001:DB8::/64 2001:DB8:0:4::1
ipv6 route 2001:DB8:0:1::/64 2001:DB8:0:4::1
ipv6 route 2001:DB8:0:2::/64 2001:DB8:0:4::1
ipv6 route 2001:DB8:0:3::/64 2001:DB8:0:4::1
```

Fig. 4. Dual-Stack Static Routing Configuration-I

```
     10.0.0.0/24 is subnetted, 4 subnets
S       10.2.0.0 [1/0] via 10.3.0.1
C       10.3.0.0 is directly connected, FastEthernet0/0
S       10.0.0.0 [1/0] via 10.3.0.1
S       10.1.0.0 [1/0] via 10.3.0.1
S    192.168.0.0/24 [1/0] via 10.3.0.1
C    192.168.1.0/24 is directly connected, FastEthernet1/0
R4#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       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
S   2001:DB8::/64 [1/0]
     via 2001:DB8:0:4::1
S   2001:DB8:0:1::/64 [1/0]
     via 2001:DB8:0:4::1
S   2001:DB8:0:2::/64 [1/0]
     via 2001:DB8:0:4::1
S   2001:DB8:0:3::/64 [1/0]
     via 2001:DB8:0:4::1
C   2001:DB8:0:4::/64 [0/0]
     via ::, FastEthernet0/0
```

Fig. 5. Routing Table of Router R4

```
R4#show run | begin ospf 2
router ospf 2
 log-adjacency-changes
 network 10.0.0.0 0.255.255.255 area 0
 network 192.168.0.0 0.0.255.255 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
ipv6 router ospf 1
 log-adjacency-changes
```

Fig. 6. Dual-Stack dynamic routing configuration-I

Fig.6 shows OSPF protocol has been configured on router R4 enabling dual stack transition using dynamic protocols. Enabling OSPF requires a different configuration for both the IPv4 network and the IPv6 network. OSPFv2 is used for IPv4, whereas OSPFv3 is used for IPv6. To enable OSPF for IPv4 network command need to be entered in 'Global configuration mode', whereas to configure OSPF for IPv6 network command needs to be entered in both global configuration mode and interface global configuration mode.

```
R4#show run | begin interface
interface FastEthernet0/0
 ip address 10.3.0.2 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2001:DB8:0:4::2/64
 ipv6 address FE80::4 link-local
 ipv6 ospf 1 area 0
```

Fig. 7. OSPF Configuration at Interface level for IPv6

Fig.7 shows the entire configuration done on fa0/0 for dual-stack dynamic routing. It can be seen that OSPFv3 has been enabled at the interface. ('ipv6 ospf 1 area 0'). Fig.8 shows the routing table of router R4. 'O' indicates OSPF routes meaning that OSPF routing protocol is responsible for routing within the network. The figure shows the routes for both the IPv4 and IPv6 network.

```
     10.0.0.0/24 is subnetted, 4 subnets
O       10.2.0.0 [110/20] via 10.3.0.1, 00:05:32, FastEthernet0/0
C       10.3.0.0 is directly connected, FastEthernet0/0
O       10.0.0.0 [110/40] via 10.3.0.1, 00:05:32, FastEthernet0/0
O       10.1.0.0 [110/30] via 10.3.0.1, 00:05:32, FastEthernet0/0
O    192.168.0.0/24 [110/41] via 10.3.0.1, 00:05:32, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet1/0
R4#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       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
O   2001:DB8::/64 [110/41]
     via FE80::C603:18FF:FEF8:0, FastEthernet0/0
O   2001:DB8:0:1::/64 [110/40]
     via FE80::C603:18FF:FEF8:0, FastEthernet0/0
O   2001:DB8:0:2::/64 [110/30]
     via FE80::C603:18FF:FEF8:0, FastEthernet0/0
O   2001:DB8:0:3::/64 [110/20]
     via FE80::C603:18FF:FEF8:0, FastEthernet0/0
C   2001:DB8:0:4::/64 [0/0]
```

Fig. 8. Routing Table of Router R4

C. *Tunneling Transition Technique*

Tunneling transition is used for the secure transmission of data. Tunneling allows private network data packets to be transmitted across a public network through the encapsulation process. Tunneling provides a secure path for data transmission through an open or untrusted network. In this paper, we have configured manual tunneling. A virtual tunnel is created between two routers and packets are sent through the tunnel. Manual tunneling provides a stable connection between two routers, for providing connections to remote IPv6 networks over the IPv4 network.

D. *Design and Configuration of the Tunneling Transition Technique*

Fig.9 shows the topology for manual tunneling created using GNS3. The clouds represent end users or hosts sitting in the IPv6 network.

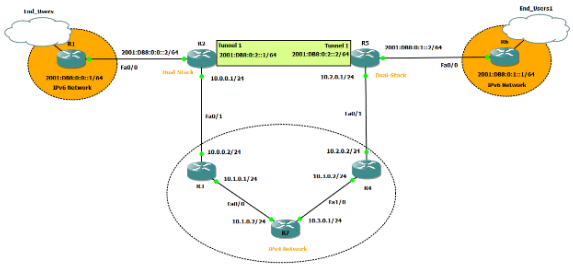

Fig. 9. Tunneling Topology

Designing of tunneling transition technique is done to transfer the data packets from an IPv6 network on router R1 to another IPv6 network on router R6 through Routers R3, R4, and R7 that make up the IPv4 network. The designing of this manual tunneling is done using the OSPF protocol. Routers R2 and R5 are the edge routers having one of their interface connected to an IPv6 network and the other interface to IPv4 network. These routers R2 and R5 are called dual-stack routers. When the data is sent to R1 from R6 (or vice-versa) as it reaches the dual stack router R5, the router attaches an IPv4 header with the IPv6 packet, thereby allowing the packet to tunnel across the IPv4 network and arriving at the other dual stack router R2 where the IPv4 header is removed from the IPv6 packet and the packet is forwarded to the IPv6 network.

Fig.10 shows a virtual tunnel interface, Tunnel-1 created on router R2 and in working state (up/up state). The up/up state depicts that both the physical cable and layer 2 protocol are functioning properly. A similar configuration is done on router R5. OSPF protocol is used for routing the network information over the entire network. Fig.11 shows the configuration for the tunnel1 interface on router R2. 'Tunnel mode ipv6ip' command performs IPv6 over IP encapsulation. Fig.12 shows the routing table of router R4. 'O' indicates OSPF routes meaning that OSPF routing protocol is responsible for routing within the network and the tunnel. The figure shows the routes for both the IPv4 and IPv6 network.

```
R2#show ipv6 int b
FastEthernet0/0            [up/up]
    FE80::C602:20FF:FE14:0
    2001:DB8::2
FastEthernet0/1            [up/up]
FastEthernet1/0            [administratively down/down]
FastEthernet2/0            [administratively down/down]
FastEthernet3/0            [administratively down/down]
Tunnel1                    [up/up]
    FE80::A00:1
    2001:DB8:0:2::1
```

Fig. 10. Router R2 configuration for Manual Tunneling

```
R2#show run | begin interface
interface Tunnel1
 no ip address
 ipv6 address 2001:DB8:0:2::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 tunnel source 10.0.0.1
 tunnel destination 10.2.0.1
 tunnel mode ipv6ip
```

Fig. 11. Tunnel-1 configuration on Router R2

```
O       10.2.0.0 [110/31] via 10.0.0.2, 00:19:52, FastEthernet0/1
O       10.3.0.0 [110/21] via 10.0.0.2, 00:19:52, FastEthernet0/1
C       10.0.0.0 is directly connected, FastEthernet0/1
O       10.1.0.0 [110/20] via 10.0.0.2, 00:19:52, FastEthernet0/1
R2#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       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
C   2001:DB8::/64 [0/0]
     via ::, FastEthernet0/0
L   2001:DB8::2/128 [0/0]
     via ::, FastEthernet0/0
O   2001:DB8:0:1::/64 [110/11121]
     via FE80::A02:1, Tunnel1
C   2001:DB8:0:2::/64 [0/0]
     via ::, Tunnel1
L   2001:DB8:0:2::1/128 [0/0]
     via ::, Tunnel1
```

Fig. 12.Routing Table of Router R2

IV. Simulation Results

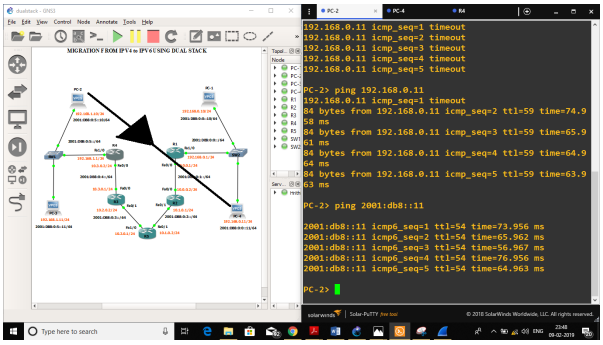

Fig. 13. Dual-Stack Static Routing Round Trip status

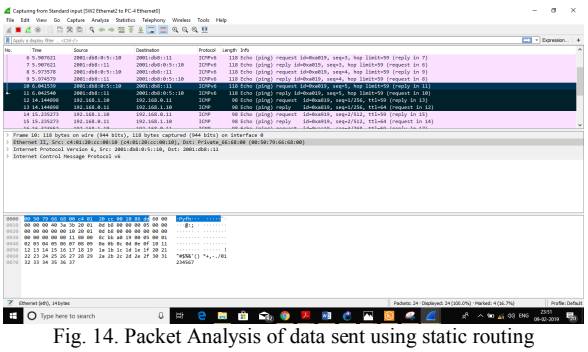

Fig. 14. Packet Analysis of data sent using static routing

Fig.13 shows PC2 on the top left side of dual-stack topology is able to successfully establish a connection and communicate with PC4 on the bottom right with either of the IPv4 or IPv6 network using static routing. Fig.14 shows the packet captured during the transmission between PC2 and PC4. We use the 'ping' command to test the connection between two separate hosts.

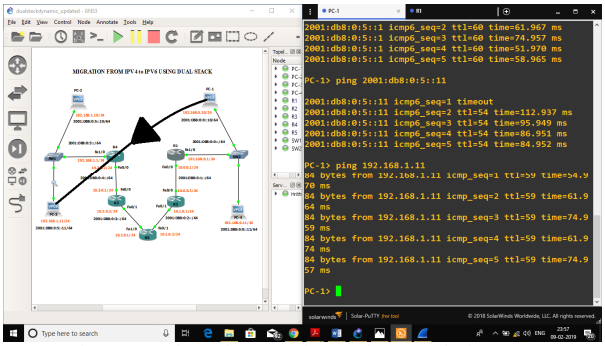

Fig. 15. Dual-Stack Dynamic Routing round trip status

Fig.15 shows PC1 on the top right side of the topology is able to communicate with PC3 on the bottom left with either of the IPv4 or IPv6 networks using dynamic routing protocol OSPF.

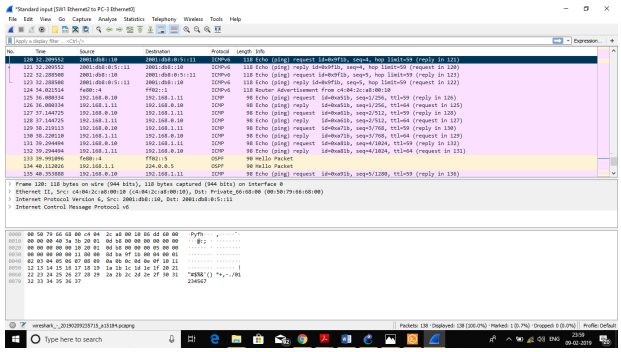

Fig. 16. Packet Analysis of data sent using OSPF

Fig.16 shows the packet captured during the transmission between PC1 and PC3. The figure at the bottom also shows the exchange of the OSPF hello packets, which depicts that dynamic routing is enabled and running on the network.

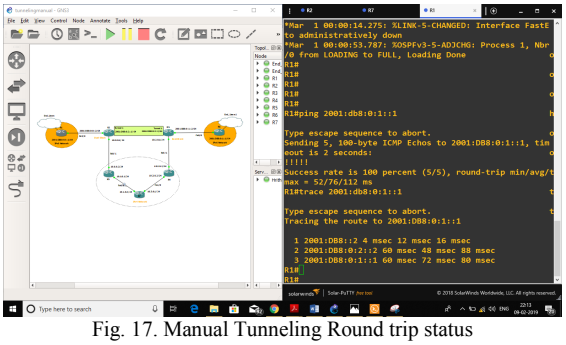

Fig. 17. Manual Tunneling Round trip status

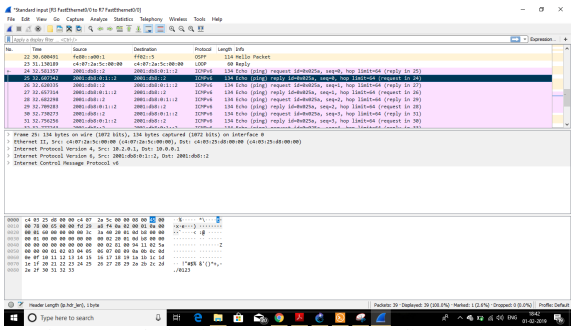

Fig. 18. Analysis of data sent using a tunneling mechanism

Fig.17 shows the connection between two separate IPv6 networks separated by an entire pool of IPv4 networks between them. The figure also shows that the route taken by IPv6 packet over the IPv4 network is through the virtual tunnel. Fig.18 shows the IPv6 packet captured during the transmission between two IPv6 hosts sitting on different networks and separated by an IPv4 network lying between the two. The header of IPv6 packet captured shows that dual-stack router attached an IPv4 header to the packet.

V. PERFORMANCE ANALYSIS

Fig.19 plotted from the values taken from Table 1 shows that the routes learned through dynamic routing have less latency as compared to the routes learned using static routing. As the number of packets, increases static IPv6 protocol and dynamic IPv4 protocol tend to have the same latency. Fig.20 plotted from the values taken from Table 1 shows that the routes configured using static routing provide less throughput as compared to the routes configured using dynamic routing. Dynamic IPv6 protocol provides the best throughput.

Table 1.Performance comparison of Static and Dynamic Dual-Stack

Dual Stack Techniques	Number of Packets	Success Rate(%)	Round Trip Time (ms)			Latency (ms)	Throughput (Mbits/sec)
			Minimum	Average	Maximum		
Static IPv4	5	100	40	56	72	28	3.57
Static IPv6	5	100	40	54	68	27	3.70
Dynamic IPv4	5	100	36	48	84	24	4.17
Dynamic IPv6	5	100	24	46	76	23	4.35
Static IPv4	10	100	20	56	124	28	3.57
Static IPv6	10	100	40	54	64	27	3.70
Dynamic IPv4	10	100	20	50	76	25	4.00
Dynamic IPv6	10	100	20	46	76	23	4.35
Static IPv4	20	100	24	56	144	28	3.57
Static IPv6	20	100	36	50	72	25	4.00
Dynamic IPv4	20	100	24	50	76	25	4.00
Dynamic IPv6	20	100	24	47	88	23.5	4.26
Static IPv4	50	100	20	54	84	27	3.70
Static IPv6	50	100	36	51	72	25.5	3.92
Dynamic IPv4	50	100	20	50	88	25	4.00
Dynamic IPv6	50	100	16	45	76	22.5	4.44

Table 2. Performance Comparison of IPv4 and IPv6 protocols in Tunneling Transition

Protocol	Number of Packets	Success Rate (%)	Round Trip Time (ms)		
			Minimum	Average	Maximum
IPv4	5	100	40	55	76
	5	100	28	53	72
	10	100	36	51	80
	10	100	32	60	84
	20	100	28	54	76
	20	100	24	50	88
	50	100	16	52	76
	50	100	28	52	92
IPv6	5	100	36	53	68
	5	100	24	48	76
	10	100	40	52	64
	10	100	28	48	80
	20	100	24	48	80
	20	100	48	55	72
	50	100	24	48	76
	50	100	16	50	76

Table 3. Performance comparison for Latency and Throughput between IPv6 and IPv4 in Tunneling Technique

Number of Packets	IPv6		IPv4	
	Latency (ms)	Throughput (M bits/s)	Latency (ms)	Throughput (M bits/s)
5	26.5	3.77	27.5	3.64
5	24	4.17	26.5	3.77
10	26	3.85	25.5	3.92
10	24	4.17	30	3.33
20	24	4.17	27	3.70
20	27.5	3.64	25	4.00
50	24	4.17	26	3.85
50	25	4.00	26	3.85

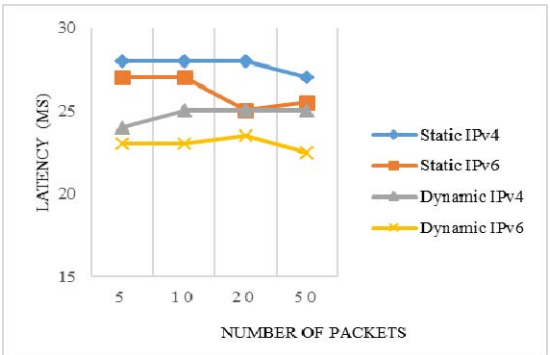

Fig. 19. Dual-Stack Latency comparison

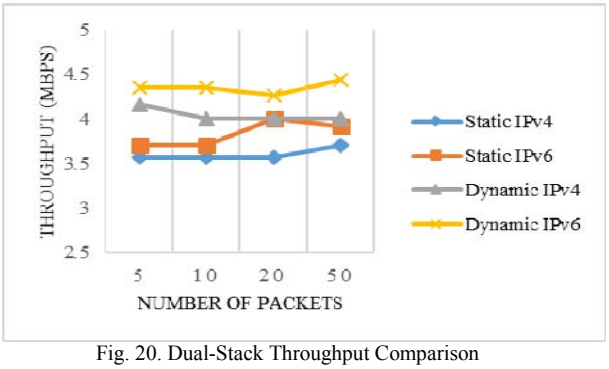

Fig. 20. Dual-Stack Throughput Comparison

Fig.21 plotted from the values taken from Table 3 shows that the IPv6 protocol has less latency as compared to the IPv4 protocol for the Tunneling transition technique. Fig.22 plotted from the values taken from Table 3 show that the IPv6 protocol provides better throughput for transmission of the packet over the cable as compared to the IPv4 protocol. Even as the number of the packets transmitted increases, the IPv6 protocol provides better throughput than the IPv4 protocol.Fig.23 shows a comparison between the Dual-stack and Tunneling transition technique in terms of throughput. Dual-stack transition technique provides a better throughput as compared to the Tunneling transition technique.

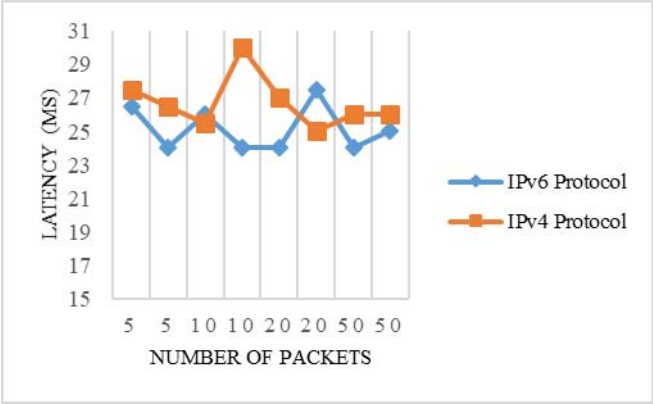

Fig. 21. Tunneling: IPv6 vs IPv4 latency comparison

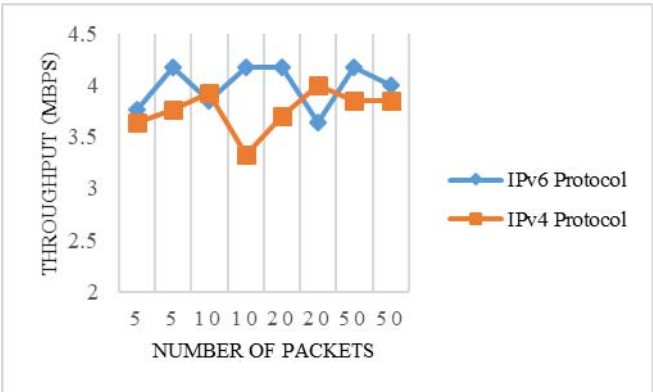

Fig. 22. Tunneling: IPv6 vs IPv4 throughput comparison

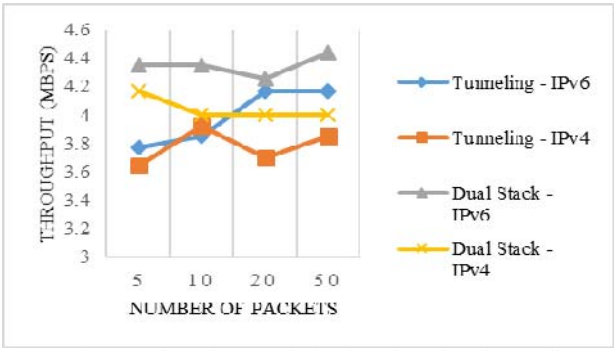

Fig. 23. Throughput Analysis of Dual-Stack and Tunneling Techniques

VI. CONCLUSION

The application of Dual-Stack transition technique and Tunneling transition technique for migration to the IPv6 network from the IPv4 network has been studied. The transfer of a different number of packets across the network using both static and dynamic routing has been studied. Round trip time has been analyzed in both the transition techniques and by using these value latency and throughput has been calculated. We conclude that IPv6 protocol along with providing much wider address space also provides less latency and better throughput than the IPv4 protocol.

REFERENCES

[1] L. H. Sahasrabuddhe and B. Mukherjee, “Multicast Routing Algorithms and Protocols” pp. 90–102, 2000.

[2] R. Rastogi, Y. Breitbart, M. Garofalakis, A. Member, and A. Kumar, “Optimal Configuration of OSPF Aggregates,” vol. 11, no. 2, pp. 181–194, 2003.

[3] L. Colitti, S. Member, G. Di Battista, and M. Patrignani, “IPv6-in-IPv4 tunnel discovery : methods and experimental results,” vol. 1, no. 1, pp. 1–10, 2004.

[4] Y. Sookun and V. Bassoo, “Performance Analysis of IPv4 / IPv6 Transition Techniques,” 2016.

[5] N. Chuangchunsong, “Performance Evaluation of IPv4 / IPv6 Transition Mechanisms : IPv4-in-IPv6 Tunneling Techniques,” pp. 238–243, 2014.

[6] S. Aravind and G. Padmavathi, “Migration to Ipv6 From IPV4 by Dual Stack and Tunneling Techniques,” no. May, pp. 107–111, 2015.

[7] S. Savita, “Comparison analysis of various transition mechanisms from ipv4 to ipv6,” vol. 2, no. 6, pp. 2006–2011, 2013.

[8] M. Alexandru and U. T. Brasov, “A STUDY OF THE TECHNOLOGY TRANSITION FROM IPv4 TO IPv6 FOR AN ISP,” no. May 2016, 2018.

[9] S. Wang, “Analysis and Application of Wireshark in TCP/IP Protocol Teaching,” 2010.