Indian Journal of Science and Technology, *Vol 9(20), DOI: 10.17485/ijst/2016/v9i20/90005, May 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Performance Analysis of IPv4 to IPv6 Transition Methods

C. V. Ravi Kumar*, Kakumanilakshmi Venkatesh, Marri Vinay Sagar and Kala Praveen Bagadi

VIT University, Vellore - 632014, Tamil Nadu, India; ravikumar.cv@vit.ac.in, kakumanilakshmi.2012@vit.ac.in, marrivinay.sagar2012@vit.ac.in, bkpraveen@vit.ac.in

Abstract

It is an arduous and indolent process to switch to IPv6 technology from the existing IPv4. This paper aims at providing a lucid performance analysis of key techniques used in IPv4 to IPv6 transition. Sustainable and real time topologies are built for each of the three robust techniques, namely, dual stack, tunneling, and network address translation. These implementations are done in an open source Network simulator GNS3 (1.3.13), a wide compatible and realistic simulator. All the topologies are analyzed for latency, efficiency and throughput using wire shark packet analyzer. Networks are built using different commercially used cisco 7200, 3600 and 3700 series routers and used serial and fast ethernet cables for connecting the nodes. All topologies are configured as private, to analyze each technique performance at their maximum potential. This analysis can be found useful in employing the right transition technique depending on the network scenario used as it weigh the advantage and limitation for each technique. The analysis depicts the competence of tunneling for its highest latency comparatively. Among the three methods, Dual Stack displays 100% efficiency in communicating within the network. Network address translation show 94% efficiency as it plays an important role when IPv4 only needs to communicate with IPv6 nodes. In most cases, IPv6 show better performance than IPv4, which lucidly explains the potential of IPv6. The analysis can further be extended to hardware implementation by constructing large topologies and with various other sophisticated routers produced by different vendors.

Keywords: GNS3, IPV4, IPv6, Performance Analysis (Throughput; Latency; Efficiency), Transition Techniques (Dual Stack; Tunneling; Translation), Wireshark

1. Introduction

In the burgeoning world of smart devices, people are using copious number of devices. All these devices needed to be connected, for which each device is given with an IP address[1,2]. IPv4 and IPv6 are two well-known and prevailing internet protocols. Most of the existing organizations, businesses are well accustomed to IPv4. Faster growth of digital world left the IPv4 technology into extinction since it is not able to provide sufficient IPs i.e., IPv4 address is only 32 bit long and it can accommodate only 2^{32} i.e., 4.3 billion nodes. With the advent of Internet of things, new and easily usable devices, IPv4 is not able to accommodate the 6 billion potential internet users and their devices.

Not only the end users, all networking infrastructure components such as servers, routers, DNS, ADC, firewalls, switches all requires IP addresses to establish internet network. So there is a great necessity to shift to other technology that solves the problem of addresses. Soon an interesting concept of Network Address Translation (NAT)[3,4] came into existence. It is a way to associate or map an independent network to a single IP address to expand the existence of more nodes on internet. It also brings up the concept of public and private IP addresses. Though it seems to be the promising solution, it brought

*Author for correspondence

many complexities, security issues, and other limitations. So it showed a path for IPv6to come into existence[5,6]. It is the most powerful Internet Protocol ever existed[7]. It eliminates most of the limitations and also provides more sophisticated encryption for best security to the data[8]. Though IPv6 has got some other vulnerabilities[9,10], the important features like header which is made light weight[11] in compared to its previous versions to provide robust[12] and easy data transfer[13].

It is not just as simple as saying to migrate from one version to another. It involves huge money to change the software, hardware components to migrate to IPv6. It is also the matter of time, for the network to transform into IPv6. So there should be some proper transition techniques till IPv6 occupies the entire existing internet space[14]. There are many transition techniques available but Tunneling, Dual Stack, Translation techniques are the major players. This paper gives a candid analysis of all these major translation techniques and provides proper report of advantages, disadvantages and best fit of each technique when different scenarios are taken into consideration.

2. Transition Stratagies

2.1 Dual Stack/Dual IP Configuration

The easiest way for IPv6 nodes to co-exist with IPv4-only nodes is by directly providing the IPv4 implementation. IPv6nodes which provide both IPv4 and IPv6 implementations are called "IPv6/IPv4 nodes". These nodes have the capacity to exchange both IPv4 and IPv6 data-packets. They can simultaneously send IPv4 packets to IPv4-only nodes and Ipv6 packets to IPv6-only nodes. So, there exist two stacks, one for IPv4 and the other for IPv6 in a single router. Since the nodes support both IP v4 and v6 protocols, these are configured with both IP addresses[15].

Though every Dual-Stack node is equipped with both IPv4 and IPv6 stacks, one of these stacks can be made disabled when required since both the stacks can exist independently. These use DHCP or other IPv4 mechanisms to get their v4 address and SLAAC (Stateless Address Auto Configuration) or DHCPv6 to acquire their v6 address.

DNS resolver has capability of handling AAAA records (IPv6 compatible) and A records (IPv4 compatible). And on request to DNS and based on the preferences set, DNS sends either IPv4/v6 address or both to the client.

2.2 Tunneling

IPv6 infrastructure will be deployed some parts at a time. In many pragmatic situations, the functional IPv4 infrastructure exists in between functional IPv6 infrastructure. It is really difficult to establish communication between two IPv6 only networks over other IP versions. Similarly we find, IPv6-only network in between IPv4 networks and creates a predicament at times. So tunneling provides a solution through which one version data packets can be sent or tunneled through the other versions' functional infrastructure[16]. For example tunneling can provide a method to make use of existing IPv4 infrastructure to carry IPv6 data packets. Here IPv6 packets are encapsulated within the information part of IPv4 packet[17].

Tunneling is used and implemented in myriad of ways i.e. in between router and router, host and router, host and host, router to host. Some of the important tunneling mechanisms are: 1. Entrance node of the tunnel create an IPv4 header and send the encapsulated IPv6 packet and at the exit of the tunnel[18], the header is removed and packet is decapsulated to retain its original form of IPv6. Tunnel can be either manually or dynamically configured[19].

2.3 Translation

This translation concept is very prominent because of the NAT (Network Address Translation), as an extension of the IPv4 network. The basic theory of NAT and the other address translation techniques used for IPv4 and IPv6 transitions are very much similar. This is an innovative approach to establish communication between IPv4-only nodes to communicate with IPv6-only nodes. Though the basic concept remains the same for NAT in IPv4 and IPv4/v6 transition, v4/v6 transition technique involves little more complexity and integration of different concepts. There are different methods through which the translation occurs. In this paper we discuss about NAT-PT and NAT-64 only.

NAT-PT (Network Address Translation-Protocol Translation) has great potential to translate protocol services such as DNS (Domain Name Service), FTP (File Transfer Protocol), ICMP (Internet Control Messaging Protocol)[20], etc. along with address translation capability. The ALG (Application Layer Gateway) is the key component used for the above mentioned translation services. Though, stupendous NAT-PT provided vast services, ALG introduced a large number of issues[21].

So, a new methodology NAT64 and DNS64 came into existence that uncoupled the application layer translation and address translation functionalities of NAT-PT.

NAT64 uses NAT64 gateway, which translates IPv6 address to IPv4 or vice-versa. An IPv6 node fixes IPv4 address with which it wants to communicate using host part of IPv6 and forwards the packet to resulting address. Generally, a mapping is made between Ipv4 and Ipv6 addresses using NAT64 gateway. It is done either manually or automatically. DNS64 resembles a DNS server which can synthesizes AAAA records (IPv6 resource records) from A records (IPv4 resource records). This is implemented by encoding the retrieved IPv4 address to IPv6 format.

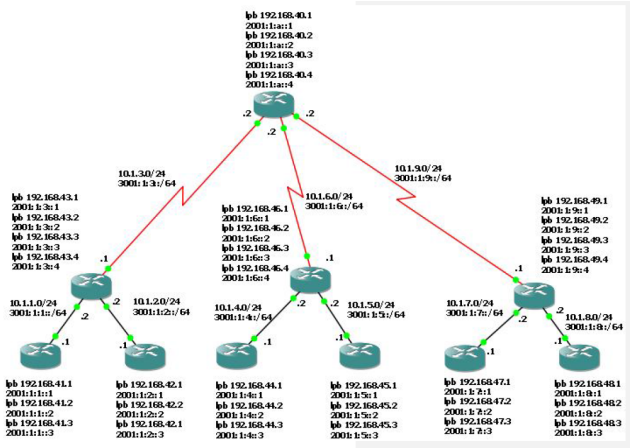


Figure 1. Dual stack topology.

3. Implementation and Analysis

There are myriad of software network simulators available in the market. Cisco VIRL, OPNET, Riverbed, Cisco Packet Tracer, GNS3, etc are some famous simulator softwares. Each has its own advantages. In this paper we implemented the various network topologies using GNS3 (3.0.1) network simulator which is one of the most accurate, agile, vendor-agnostic software and it has also got copious networking components. Moreover, it provides a great GUI with which any complex topologies can be implemented easily. All the analysis of the topologies has been carried out using Wireshark packet analyzer.

Wireshark is an open source, free and user-friendly packet analyzer software which is generally used for troubleshooting, protocol development, and analysis of data.

Similar topologies are built for each transition technique i.e., Dual stack, tunneling and translation. A combination of cisco 3640, cisco 3725, cisco 7200 routers are used for routers and set of Qemu hosts as end Linux PCs and end servers are used in the implementations.

3.1 Dual-Stack Implmentation

A ten router Dual Stack topology has been implemented with three virtual hosts as shown in the Figure 1. All the routers are connected using Fast Ethernet cables and serial cables. All routers are configured with IPv4 and IPv6 addresses i.e., all routers used in this network are dual stack /dual IP configured routers. Routers R10 is c7200 routers which are more robust and can handle traffic effectively. R3, R6, R9 are c 3725, whereas the end

```
R1#traceroute 192.168.48.1

Type escape sequence to abort.
Tracing the route to 192.168.48.1

  1 10.1.1.2 472 msec 160 msec 92 msec
  2 10.1.3.2 644 msec 900 msec 624 msec
  3 10.1.9.1 728 msec 1076 msec 1500 msec
  4 10.1.8.1 1824 msec 1932 msec 2080 msec
R1#traceroute 2001:1:8::1

Type escape sequence to abort.
Tracing the route to 2001:1:8::1

  1 FE80::C005:3FF:FEF0:0 312 msec 120 msec 252 msec
  2 3001:1:3::1 448 msec 380 msec 608 msec
  3 3001:1:9::1 612 msec 616 msec 580 msec
  4 2001:1:8::1 812 msec 896 msec 1180 msec
R1#
```

Figure 2. Trace route of IPv4 ping and IPv6 ping from R1 to R8 lpb.

routers are c3640. All the routers are configured with their respective loopback networks to represent the real time scenario.

The Trace Route helps to find the different routes the data-packet takes to reach the destination. It also finds the RTT(Round–trip time) of a data-packet to hit all intermediate routers. RTT is the time taken for the packet to be sent from the source to that particular host and get acknowledgement from that host to source. The upper portion of the Figure 2 gives the details about the ICMPv4[11] sent from R1 to R8.TraceRoute command sends three datagrams at a time and so in the Figure, three different times are seen. Each time period represents the time taken by that particular datagram to reach that particular host. In most cases, RTT is treated as latency. So, the latency of IPv4 packet to reach R8 from

R1 is 1945msec (avg.). Whereas, the lower part of the Figure 2 displays the trace route details of R1 to R8. It is clearly evident that IPv6 is having less latency and it is about 962msec (avg.), which is nearly half of that of IPv4's time. One inference that can be drawn from the above results is that with the distance increased, the performance of IPv6 is better in terms of latency in this scenario. Another important parameters to analyze are throughput and efficiency of the data.

As mentioned in the beginning of the section, all the analysis is carried in wireshark packet analyzer. For the analysis in this topology, we captured the data passing through the interface f0/0 of R10. 3001:1:3:2/64 or 10.1.3.0/24 link. Considerable traffic is generated across that link for the analysis. For better understanding, only ICMP v4 and v6 are individually filtered and analyzed on the parameters throughput and efficiency.

In networking, throughput is defined as the amount of data transferred from one node to another in a given time interval. Whereas, the efficiency is coined as the number of packets successfully reached the destination. It is observed from the Figure 3(a) that the throughput of the ICMPv4 packets is 0.003Mbits/s with 100% efficiency in this network scenario. Results of ICMPv6 in Figure 3(b), shows that throughput is almost similar to that of ICMPv4 traffic. Figure 3(c) provides the comparative analysis of ICMPv4 and ICMPv6 packets' throughput in log scale over time.

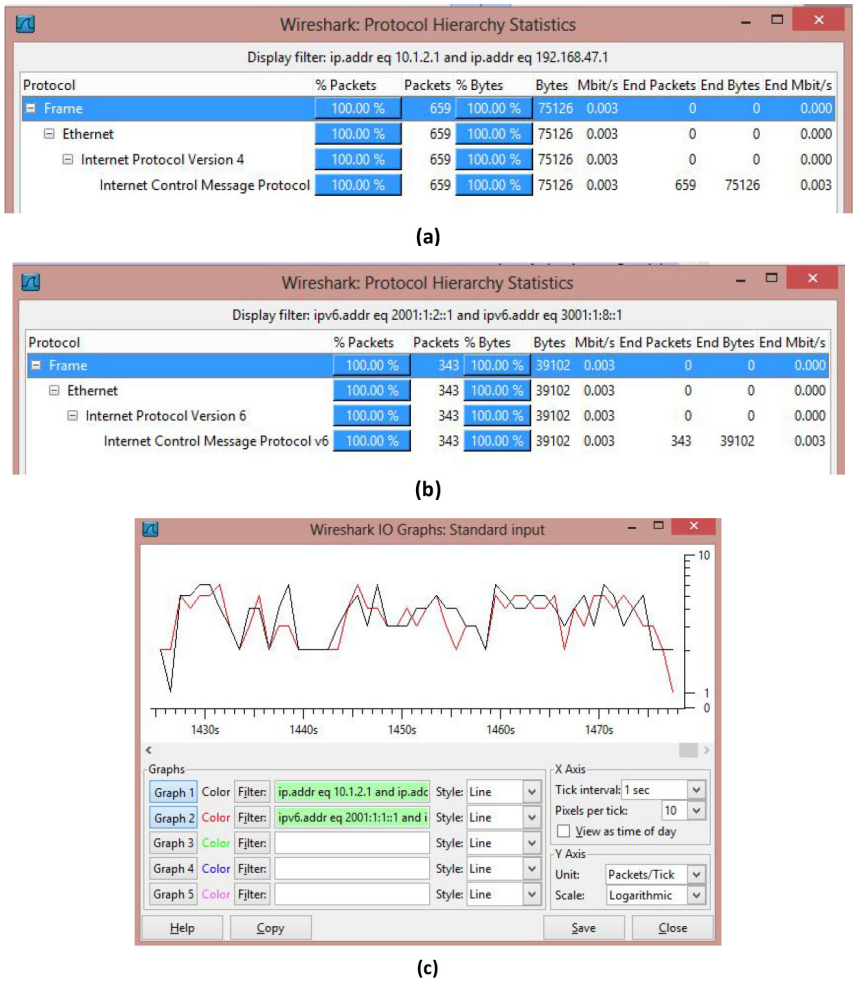


Figure 3. (**a**) IPv4 ICMP packet throughput. (**b**) IPv6 ICMP packet throughput. (**c**) IPv6 and IPv4 ICMP packet throughput comparative analysis.

3.2 Tunneling Implmentation

The Figure 4 shows the tunneling topology with ten routers similar to that of the dual stack topology. Here R1, R4, R7 are IPv4 configured and have IPv4 loopbacks configured to it. R2, R5, R8 areIPv6 configured and they are assigned with their respective loopbacks. R3, R6, R9, R10 are tunnel initiators and each of these have IPv4 loopbacks. This topology contains two IPv6 tunnels for allowing v6 traffic over v4 network and one IPv4 tunnel for allowing v4 traffic over v6 traffic. First IPv6 tunnel is present between R3 and R10, second in between R9 and R10. The IPv4 tunnel is located between the R6 and R10. The traffic is generated throughout the network and the data is captured for interfaces s0/0 and s0/1 of R10 in order to get the analysis of both v4 and v6 tunnels.

In the Figure 5 the third hop in the list i.e., 10.1.6.1 is v4 over v6 tunnel. The total latency of the IPv4 packet over v6 network is 575 msec (avg). The second hop in the Figure 6, i.e., 3001:1:A::2 represents the IPv6 tunnel over v4 network. The latency of the v6 packet over v4 network is being 648 msec (avg) which is nearly same as that of v4 packet latency.

The Figure 7(a) lucidly depicts the v6 traffic is carried as v4 traffic as the v6 tunnel is present there and data is carried with 100% efficiency and with 0.003 Mbits/sec. Similar to that, Figure 7(b) gives a insight on the v4 tunnel where the v4 traffic is carried in v6 packets. Data throughput and efficiency are same as that of the above.

```
R1#traceroute 192.168.44.1

Type escape sequence to abort.
Tracing the route to 192.168.44.1

  1 10.1.1.2 192 msec 88 msec 232 msec
  2 10.1.4.2 168 msec 1112 msec 252 msec
  3 10.1.6.1 680 msec 452 msec 476 msec
  4 10.1.2.1 548 msec 560 msec 620 msec
```

Figure 5. Trace Route between R1 and R4 lpb.

```
R2#traceroute 2001:1:5::1

Type escape sequence to abort.
Tracing the route to 2001:1:5::1

  1 3001:1:1::2 156 msec 144 msec 188 msec
  2 3001:1:A::2 328 msec 368 msec 400 msec
  3 3001:1:4::1 300 msec 336 msec 408 msec
  4 2001:1:5::1 604 msec 788 msec 600 msec
```

Figure 6. Trace Route between R2 and R5 lpb.

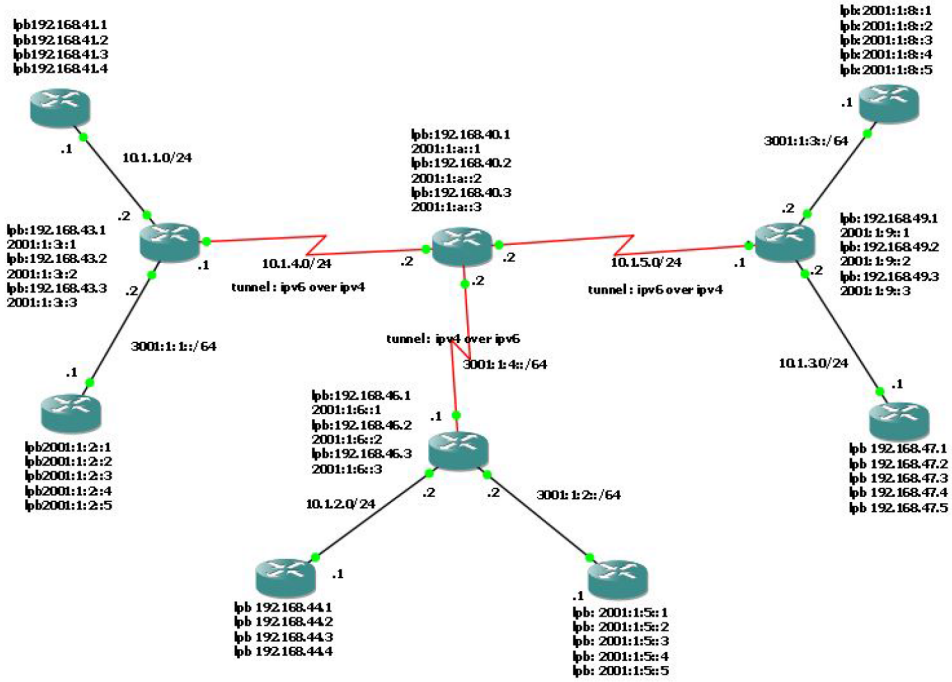
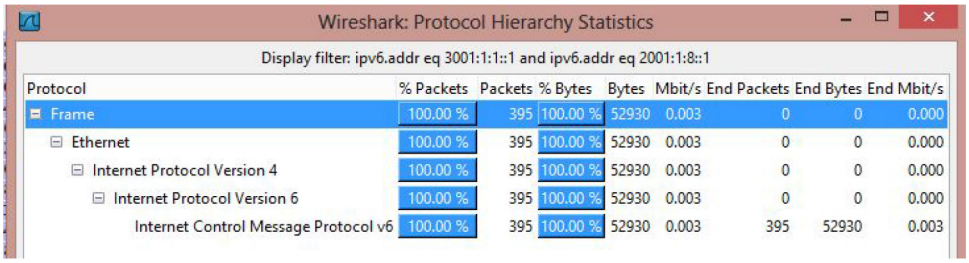
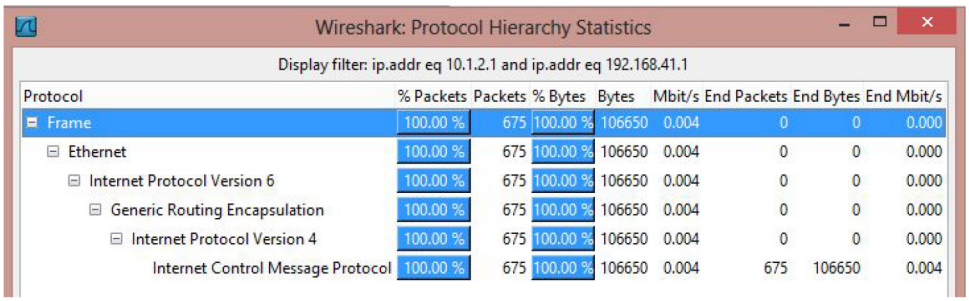


Figure 4. Tunneling topology.



(a)



(b)

Figure 7. (**a**) ICMP packet throughput analysis over v6 tunnel. (**b**) ICMP packet throughput analysis over v4 tunnel.

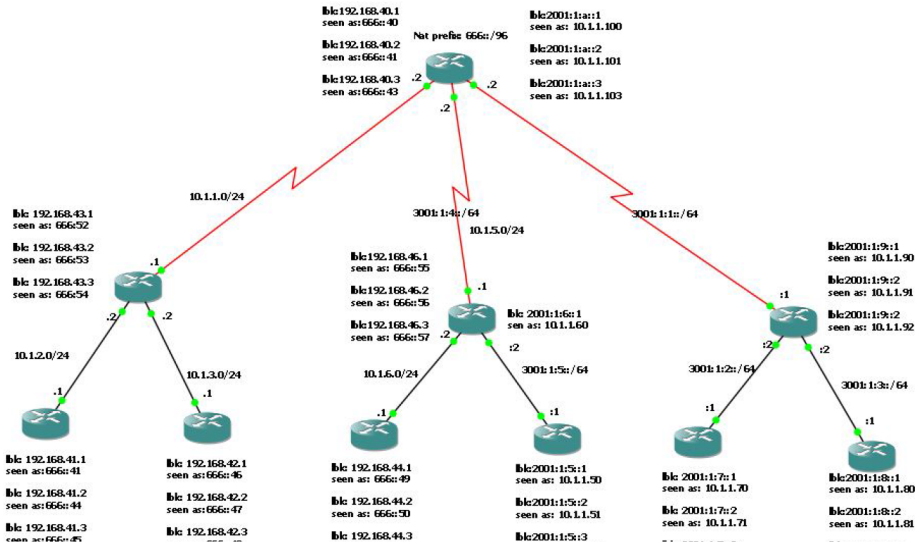


Figure 8. Translation topology.

3.3 Translation Implmentation

A similar configuration to that of above techniques is chosen to compare and topology which is shown in Figure 8. Only router R10 is configured manually for NAT-PT translation. So, the address translation from v4 to v6 or vice-versa happens only at R10 and the data transfer continues. Translation table looks like as shown in Figure 9. The translation table consists of IP addresses and their corresponding conjugate addresses. Every time when v4/v6 packet comes to the router, then the address of the packet is changed to respective v6/v4 address as in the translation table. These translations can be either automatically configured or done manually.

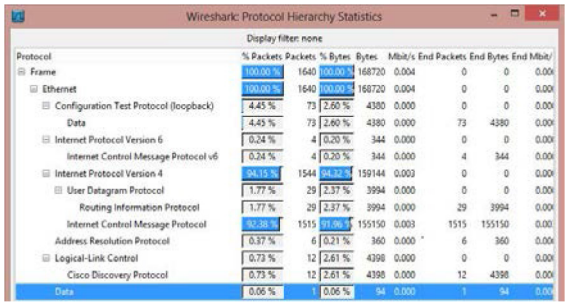
The Figure 10 shows 97% efficiency in their pings when 9809 packets are sent from R1 to R8. It shows better performance i.e., 99% efficiency when less number of packets are sent. However, the RTT is remained same in

both cases which nearly 1050 msec(avg). In this case Trace Route is able to show only the intermediate nodes till NAT server because of the address translation. In the above scenario IPv6 to IPv4 address translation took place at router R10. So, an IPv4 configured R1 is able to ping IPv6 configured R8. Similarly any version IP address can ping any version IP address with the help of NAT-64 and NAT-PT.

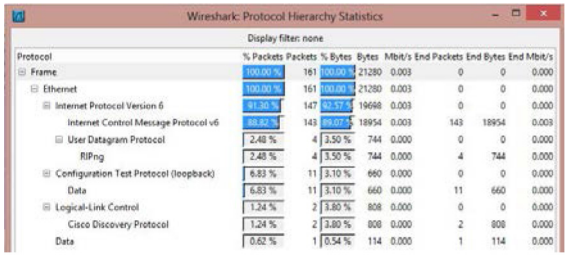
The Figures 11(a) and 11(b), shows the analysis of data captured at interfaces s0/1 and s0/0 of R10 router. Figure 11(a) shows the traffic when data from IPv4 R1 is sent to IPv6 R8. 94.7% of the v4 traffic is converted to IPv6 and sent with the throughput of 0.03 Mbits/sec and similarly there is only 92% efficiency found in the conversion of v6 traffic to IPv4 with throughput of 0.03 Mbits/sec. Another drawback found during translation is IPv4 configured R4 was not able to ping IPv6 configured R5 since both the routers are connected to the same interface of NAT configured R10, which translates and redirects the traffic only to other interfaces.

```
R10#show ipv6 nat translations
Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
---   ---                      ---
      10.1.1.1                 666::11

---   ---                      ---
      10.1.1.2                 666::12

---   ---                      ---
      10.1.2.1                 666::21

---   ---                      ---
      10.1.3.1                 666::31

---   ---                      ---
      192.168.40.1             666::40
```

Figure 9. NAT translation table at R10.



(a)



(b)

Figure 11. (**a**) Throughput and efficiency analysis at int s0/1of R10. (**b**) Throughput and efficiency analysis at int s0/0of R10.

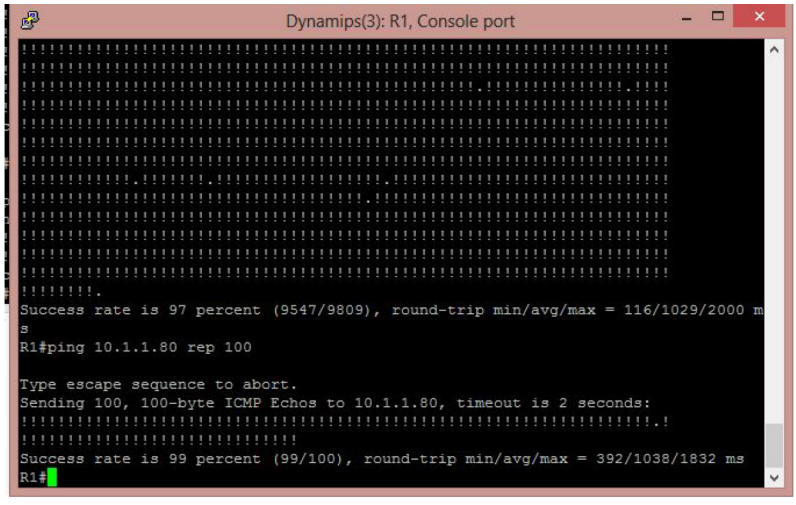


Figure 10. Ping and traceroute from R1 to R8.

4. Conclusion

In the past, IPv4 has proven its ability in terms of reliability, security and quick data transfer. Since the IPs are limited to 4.3 billion with IPv4, new techniques like NAT and IPv6 came into existence to solve the problem of IPs and to provide much more sophisticated experience. However, transition from IPv4 to IPv6 takes time. So, there is utmost necessity for transition techniques to play their role to establish smooth communication between the both IP versions. The Dual Stack, tunneling, translation are three well-renowned transition techniques available today. When all three techniques are compared, Dual Stack and tunneling provided 100% efficiency in data transfer when tested in a small network of 10 routers, each router with its respective loopbacks or private network. But in Dual Stack, the RTT or latency is found high when compared to that of tunneling and Translation because of the complexity involved in the router. Comparing within Dual stack, performance of IPv6 is better than Ipv4 packets. Though Dual stack is versatile and highly efficient, better results can be observed when dual stack routers are used in limited numbers. It can ace and best fit in small topologies. Tunneling is best technique when the network is vast and data needs to be transferred between the same IP version networks over other IP network. The throughput is observed the highest for tunneling because of the simplicity involved in data transfer. Translation technique which works similar to that of NAT, is propitious when IPv4 only node wants to communicate with Ipv6 only node or vice-versa. Since the efficiency of this technique is low, more number of NAT64 or NAT-PT routers can be employed for best results.

The research can be further carried out on the stands of implementing these techniques in larger topologies in real time and analyzing these on different scenarios.

5. References

1. RFC 791: I. S. I. at University of Southern California. Internet Protocol, DARPA Internet Program, Protocol Specification; 1981
2. Postel J. Extensible field addressing. Internet RFC 730; 1977 May.
3. Turanyi Z, Valk A. IPv4+4, 10th IEEE International Conference on Network Protocols, ICNP'02; 2002. p. 1–10.
4. Srisuresh P, Holdrege M. IP Network Address Translator (NAT) terminology and considerations. Internet RFC 2663; 1999 Aug. p. 1–30.
5. Wu P. Cui Y. Wu J, Liu J. Transition from IPv4 to IPv6: A state-of-the-art survey. IEEE Communications Surveys and Tutorials. 2012 Dec; 15(3).
6. IEEE-USA white paper, next generation internet: IPv4 address exhaustion. Mitigation Strategies and Implications for the U.S; 2009.
7. Zeadally S, Raicu I. Impact of IPv6 on end-user applications. 10th International Conference on Telecommunications, ICT 2003; 2003 Feb 23-Mar 1. p. 973–80.
8. Deering S, Hiden R. Internet Protocol, Version 6(IPv6). IETF RFC 2460. Available from: https://tools.ietf.org/html/rfc2460
9. Saad RMA, Almomani A, Altaher A, Gupta BB, Manickam S. ICMPv6 flood attack detection using DENFIS Algorithms.. Indian Journal of Science and Technology. 2014 Feb; 7(2):168–73.
10. Ul Rehman S, Manickam S. Significance of duplicate address detection mechanism in Ipv6 and its security issues: A survey. Indian Journal of Science and Technology. 2015; 8(30):1–8.
11. Mokhtar RA, Ismail AF, Hasan MK, Hashim W, Abbas H, Saeed RA, Islam S. Lightweight Handover Control Function (L-HCF) for mobile internet protocol version six (IPv6). Indian Journal of Science and Technology, 2015 Jun; 8(12). DOI: 10.17485/ijst/2015/v8i12/70656.
12. Raicu I. An empirical analysis of Internet Protocol version 6 (IPv6); 2002.
13. Huitema C. IPV6; The new Internet Protocol. Prentice Hall; 1996.
14. Nordmark E, Gilligan R. Basic transition mechanisms for IPv6 hosts and routers. IETF RFC 2893; 2005 Oct. Available from: https://tools.ietf.org/html/rfc4213z
15. Tahir HM, Taa A, Nasir NBM. Implementation of IPv4 over IPv6 using Dual Stack Transition Mechanism (DSTM) on 6iNet. 2nd Information and Communication Technologies, ICTTA '06; 2006.
16. Deering S, Conta A. Generic packet tunneling in IPv6. IETF RFC 2473. Available from: https://tools.ietf.org/html/rfc2473
17. Raicu I, Zeadally S. Evaluating IPv4 to IPv6 transition mechanisms. Telecommunications, ICT; 2003
18. Cui Y, Dong J, Wu P, Wu J, Metz C, Lee YL, Durand A. Tunnel-based IPv6 transition. IEEE Internet Computing. 2013 Mar; 17(2):62–8. Available from: http://doi.ieeecomputersociety.org/10.1109/MIC.2012
19. Toutain L, Afifi H. Dynamic tunneling: A new method for the IPv4-lPv6 Transition.
20. Postel J. Internet control message protocol. Internet RFC792; 1981 Sep.
21. Tsirtsis G, Srisuresh P. Network Address Translation – Protocol Translation (NAT-PT). IETF RFC2766. Available from: https://www.ietf.org/rfc/rfc2766.txt