A Hybrid Transition for IPv4-IPv6 Co-existence in Small Size Organization

B. I. D. Kumar, Vasanth G., SudalaiMuthu T.

Abstract: Internet Protocol version 6 (IPv6) is the current generation Internet protocol developed by the Internet Engineering Task Force (IETF) to handle the shortage of IP addresses in IPV4. The transition from IPv4 to IPv6 is gradually being done not happening as anticipated. It is unavoidable to have both IPv4 and IPv6 networks during the transition period, but unfortunately they are not compatible in nature. It is essential to maintain the IPv4 and IPv6 coexistence. The inter-communication ability of IPv4 and IPv6 is the dire need of network community. Many transition techniques are proposed in the recent years. This paper discussed the key difficulties in IPv4-IPv6 transition, and introduced the hybrid approach for coexistence of IPv4 and IPv6. It hybrid the advantages of weightage and tunneling translation techniques for providing inter-communication ability of IPv4 and IPv6. The proposed algorithm has been simulated and the performance metrics; transmission latency, throughput, jitter and delay have been analyzed from end to end host, through various scenarios includes IPv4 only, IPv6 Only, Dual stack, GRE tunneling. The performance of the proposed algorithm is analyzed and the future scope is discussed.

Keywords: IPv4, IPv6, ISP, Transition techniques.

I. INTRODUCTION

In the early 1990s, it was identified that IPv4 address space would not be sufficient by 2000. The IPv4 had exhausted in the year 2011 in IANA. This exhaustion has demanded more address spaces which implies the any other solution to handle the situation. Several temporary solutions had evolved along with the demand of new address space for the future use of IP in the Internet world. Some temporary solutions were offered to deal with the shortage of address space, such as NAT (Network Address Translator) or CIDR (Classless Inter Domain Routing) besides with the start of development of new enhanced IP protocol work. A new IPv6 has been designed and enhanced in many ways. The number of bits in the address space is increased from 32 to 128. The flow label field of IPv6 supports payload identification to QoS handling. The IPv6 has extension headers instead of option filed as in the IPv4. This extension header can increase the size of the packets. The DHCP (Dynamic Host Configuration Protocol) is used for IPv6 configuration and hence there is no manual configuration is required. The expansion of Internet usage in the recent decades causes the shortage of IPv4 address space. This matter will threaten the continuation of an internet service that working on IPv4. Internet Engineering Task Force (IETF) has begun in 1994, designed and developed an enhanced size of address space namely Internet Protocol version 6 (IPv6). The IPv6 is a new protocol to replace IPv4 over the coming years. The new protocol is designed to support the growing use of the Internet, and the address security problems. IPv6 uses a 128-bit address size and will allow for 3.4x1038 distinguish addresses, which are enough to cover any number of Internet connecting devices.
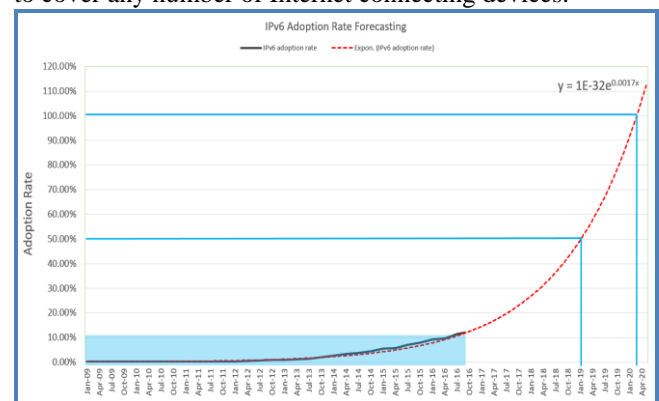

Fig.1 IPv6 Adaption Rate Forecasting

In the recent decades, the IoT demands large number of IP address in the new inter world. As IoT devices are required to connecting to the Internet, each IoT required a IP for their communication with the rest of the world. As the available IPv4 address is very limited, they migrating into IPv6 gradually. But this migration required another decade of time to use IPv6 only networks. The deficiency of IPv4 space headed to deploy IPv6 address space. This deployment may take a decade of time. The Co-existence of IPv4 and IPv6 is unavoidable; hence the transition mechanisms are the dire need of the Internet world. The carried research work provides a solution for the of co-existence of IPv4 and IPv6. The IPv6 yielded the deployment challenges in IPv4-based infrastructures. The replacement of IPv4-based infrastructure with IPv6 is costly and impractical for the small size organizations.

B. I. D. Kumar*, Associate Professor, Department of Computer Science and Engineering, Amruta Institute of Engineering and Management Sciences, Bangalore (Karnataka) India.

Vasanth G., Professor, Department of Computer Science and Engineering, Government Engineering College, K. R. Pet (Karanataka) India.

SudalaiMuthu T., Associate Professor, Department of Computer Science and Engineering, Hindustan Institute of Technology and Science, Chennai (Tamil Nadu) India.

Retrieval Number: B4511129219/2019©BEIESP
DOI: 10.35940/ijeat.B4511.129219
Journal Website: www.ijeat.org

3416

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The IETF IPng Transition Working Group has proposed many transition strategies to deploy IPv6 into existing networks successfully. The encapsulation strategy is employed in transition mechanisms as the IPv6 encapsulate into IPv4 packets. The transition strategy is an idea of using IPv6 over the IPv4. The objective of the research work is to propose a new transition mechanism and evaluate it with the other transition mechanisms in the state of the art.

II. LITERATURE REVIEW

Priya Bali (2015) has concluded that native Dual-Stack is suitable for IPv6-IPv4 Co-existence. They have illustrated the performance of IPv4/IPv6 co-existence transition strategies. They have used Dual Stack, Tunneling and Transition mechanisms for comparison. They have reviewed IPv4-to-IPv6 transition coexistence strategies in detail. They also have compared their performances. The authors reported that the impact of network behavior on the performance of the transition strategies. They have used Dual stack, Tunneling and Translation methods for comparison. The authors have reviewed Automatic IPv6 Transition and Manual Transition. They have concluded that Dual stack was the optimum method for IPv6 deployment. The authors also reported that the next optimum method was NAT64 IPv4/IPv6 transition deployment in the company. They author also quoted that the companies are planned to use NAT64 for a while and move to Native IPv6 mechanisms when they IPv6 set up would ready. The companies also planned to use Rapid Deployment strategy while implementing IPv6 deployment. The author has also found that NAT444 used as a intermediator in the transition period. It can be used to use IPv4 services eve after IPV4 address space was exhausted.

Dipti Chauhan (2015) has reported a mechanism that compress IPv6 header to increase the efficiency of the IPv4-IPv6 tunneling. The IPv6 header has been compressed from 40 bytes to 6 bytes. An additional parameter was used to extract back to 40 bytes' information at the sender side. The value '0' is set to additional parameter implies normal tunneling is to be used. The value '1' is set to additional parameter implies compressed header methods is to be used. They have simulated the compressed header approach and found that this approach yielded better throughput and Jitter. The authors were used small network simulation setup with the minimum number of nodes and routers. The compressed methods were improved the Packet delivery ratio, throughput and Jitter. This strategy was tested in the small networks and hence the performance in the large network is yet to be tested. Parra, J. (2014) had reported that study on co-existence of IPv4/IPv6. The author also discussed the common transition technologies for co-existence of IPv4/IPv6. The author also experimented the different migrating scenarios for co-exist tense of IPv4/IPv6. He explored the performance of the migrating scenarios under Dual stack, Tunneling and Translation. He found that Native Dual stack performed better than other simulated scenarios. He also suggested to use the native dual stack for small size organizations for IPv4/IPv6 deployment.

Tach pat Terawatt and et.al. (2014) has created a mechanism in GNS3 with predefined transferring route of data. They have compared the performance of their mechanism with the

Dual Stack and Tunneling mechanisms. They have used both TCP and UDP file stream with the variable file size for their experiments. They also have used different rate of streaming in their experiments for comparison their techniques in IPv6 transition. They reported that dual stack provided more throughputs and minimum jitter in the defined network. It yielded the shortest time to download TCP file downloading. The authors also presented a comparative study of migration techniques and their performance in various scenarios. However, they have not experimented in the RIPng and OSPFv3 environment.

III. TRANSITION MECHANISMS

The IPv6 is deployed gradually with the existing IPv4 networks. As IPv6 is not backward compatible, it is could not send packets to IPv4 networks, hence there is need of co-existence IPv4 and IPv6 infrastructure. The transition mechanism plays a compatible role in between the IPv4 networks and IPv6 networks. The transition mechanism enables the transition in the co-existence of IPv4 and IPv6. The "Internet Engineering Task Force" (IETF) has provided three major mechanisms for IPV4/IPv6 coexistence.
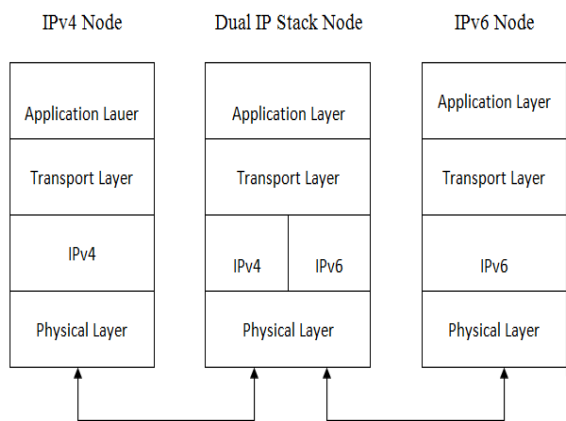
- Dual Stack
- Translation
- Tunneling

A. Dual Stack Transition Mechanism (DSTM)

The Dual-stack transition mechanism consists of both IP stacks (IPv4 and IPv6) in a single node. Both protocols run in parallel to provide the end to end service for the user as shown in figure 2. The common shared transport layer protocol is used by IPv4 and IPv6. TCP/IP model for dual stack node is shown in figure 2. The Dual stack mechanism supports to maintain IPv4 / IPv6 coexistence as each node in the network can act dual role. The dual stack node use IPv4 address while communicating to IPv4 address nodes and it use IPv6 address while communicating with IPv6 address node. The network application can choose the version of the IP based on the requirements of further communication.

As each communication takes place directly based on the requirements of the version of IP, this method is very simple and easy to implement. However, the deployment dual stack on each node is yielding additional overhead cost in the network which is refrain the organization to deploy dual stack to handle the IPv4/IPv6 coexistence. Since each dual stack node is able to communicate directly, the DNS should handle the situations appropriately. The DNS server should able to handle the "AAAA" records of the node to version of the IP is to be considered for communication. A dual-stack implementation can be deployed by three ways: (1). IPv4 stack enabled, (2). IPv6 stack enabled and (3). Both IPV4/IPv6 stacks enabled.

1. The IPv4 stack enabled
2. The IPv6 stack enabled
3. Both IPV4/IPv6 stacks enabled

Dual stack requires a huge investment, but yields better throughputs and RTTs when compared to tunneling mechanisms.

Fig.2 Dual stack TCP/IP model

The challenge in the Dual stack approach is that it required IPv4 and IPv6 are to be deployed in the same infrastructure. The node should be able to understand the version of the IP and process it accordingly. The routing protocol decides that which IP protocol is to be used based on the requirements soughed.

B. Translation Mechanisms

The translations mechanism converts the IP protocols from IPV4 to IPv6 and vice versa directly. It works in the principles of transformation of header and payload of the IPV4 and IPv6 protocols. The Translation mechanisms uses translators that can translate given IPv4 address to corresponding IPv6 address as in Figure 3. As the translation mechanism is requiring a break in end to end network, it would not be a good choice. Some of the translation mechanisms are SIIT, BIS, BIA, NAT-PT, TRT.

Dual stack mechanisms require a huge investment to update current equipment and invest in new ones. On the other hand, tunneling mechanisms connect IPv6 islands but are unable to allow the connection between the IPv4 realm and IPv6 realm. So translation is needed to allow resource migration and coexistence between both protocols while the migration occurs. The usage of translation mechanisms is unavoidable while the services that are available through IPv4 may not be available in IPv6. The translations mechanism converts the IP protocols from IPV4 to IPv6 and vice versa directly. It works in the principles of transformation of header and payload of the IPV4 and IPv6 protocols.
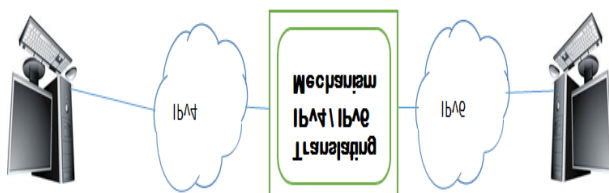
Fig.3 Translation Mechanism Infrastructure

The Translation mechanisms uses translators that can translate given IPv4 address to corresponding IPv6 address as in figure 3. As the name states, translation enables direct communication between IPv4 and IPv6 hosts. As this mechanism makes a break in end to end network; this would not be a good choice. Examples of translation mechanisms are: DNS64, NAT64, Stateless IP/ICMP Translation (SIIT) and IVI, BIS, BIA, NAT-PT, TRT.

C. Tunneling Mechanisms

Tunneling provides the ability to deal with IPv6 traffic in IPv4 infrastructure. The IPv6 packet is encapsulated in IPv4 traffic in order to provide a tunnel for IPv6 packets to carry through IPv4 infrastructure. Tunneling is used in the where the networks infrastructure is not capable of dealing with the IPv6. The deployment of tunneling is simple and no additional management is required. Tunneling is required to be configured at the end point only. On the other hand, the Tunneling takes more CPU time and it has a single point of failure. Many tunneling techniques are employed which are includes Static Tunneling, Intrusive Automatic Tunnel.

Another technique is the use of tunnels. The tunnels are used to create a customized communication for IPv6 communication from IPv4 nodes. The nodes are creating a point-to-point dedicative tunnel for their IPv6 communications. The IPv6 packet is encapsulated into IPv4 packet in-order to get transmitted from IPv4 infrastructure. The destination node is reassembling or de capsulating the IPv4 packet back into IPv6 packet. The encapsulation and de capsulation process is to be carried out for each IPv6 packet which is required for transmission through IPv4 infrastructure. Tunnels can be created manually at end-points or automatically. Automatic tunneling includes 6to4, Tore do, ISATAP, Tunnel Brokers and 6rd mechanisms.

IV. WEIGHT BASED TRANSITION ALGORITHM

The proposed weight based Transition algorithm is designed using the weight values of the determined factors. The Weight vector "w" is computed empirically using the past history of the transmission. The Weight Vector "w" represents the priority of the transmission by considering the importance factors of the IPv4 to IPv6 conversion. The Weight vector "w" is determined for particular interval of time "T" based on the recent past transmission history. The packets are encapsulated with its weight value $w[i]$ at the IPV4/IPv6 source and used at the IPv4/IPv6 destination. The packets are encapsulated with its weight value $w[i]$ at the IPV4/IPv6 source and used at the IPv4/IPv6 destination. The encapsulation is carried out at edge router of the originating host and de-capsulation is carried out at the edge router of the destination host. The tunnel is established between the two edge routers with the ability to analyze the weight vector "w". It emphasis the importance of the conversion and those packets will be treated as specified to reduce the conversion overheads. The weight Vector has been obtained as $W = (0.5, 0.3, 0.2)$ on Throughput, RTT, Packet Loss empirically by doing the trail experiments initially. The Throughput, RTT and Packet Loss were considered with respect to the nature of the packets pattern. The packets are queued in the waiting queue for transition conversion; a packet is selected for conversion based on the weight value of the packet.

Retrieval Number: B4511129219/2019©BEIESP
DOI: 10.35940/ijeat.B4511.129219
Journal Website: www.ijeat.org

3418

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The packet with greatest weight is selected for conversion in order to improve the performance of the conversion and hence RTT latency and loss rate were improved.
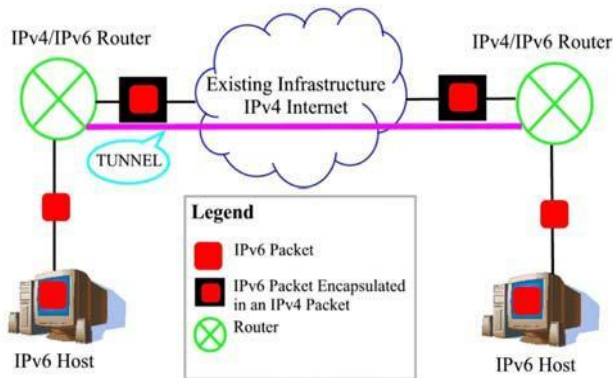
Fig.4 Weight Based Router – Router Tunneling

A Weight-Based IPv4/IPv6 Transition Algorithm

For each requested packet,

1. If the requested packet is IPv4 packet, then transmit as IPv4 packet

2. Else if the packet is IPv6, then the IPv4/IPv6 router encapsulate the packet as follows

(i) The Weight Vector $W_0 = (0.5, 0.3, 0.2)$ on Throughput, RTT, Packet Loss is used to determine the "Importance value", $I_v(R)$ as

$$I_V(R) = d(R_0, R_I) = \sqrt{W(R_0 - R_I, R_0 - R_I)} = \sqrt{\sum (R_{0i} - R_{Ii,})}$$

Where R_0 is a ideal value vector for a packet $(1,1,1)$, R_I is a requested IPv6 packet and $W_0 = \{0.5, 0.3, 0.2\}$. The W_0 is a initial weight computed by a empirical analysis. The "W", weight vector is re-determined for every interval of time T.

3. The "Importance Value", Iv is appended in the Option filed of IPv6 packet and encapsulated into the IPV4 packet.

4. The edge router of the source transmits the encapsulated IPv4 packet into the network using IPV6 protocols.

5. The edge router of the destination receives the encapsulated IPv4 packet and decodes the packet to get the importance value of the packet.

6. The decoded packet is processed based on the priority of the importance value of the packet, which is resulted the impact on Throughput, RTT, Packet Loss.

V. EXPERIMENTAL SETUP

The experiments were conducted in a lab environment using Graphical Network Simulator (GNS3). GNS3 allows the same type of emulation using Cisco Inter-Network Operating Systems. It allowed to run a Cisco IOS in a virtual environment. GNS3 also supports other emulation programs, namely Qemu, Pemu and Virtual Box. The traffic in the network was simulated traffic generated by jperf. The jperf tool was used to generate the multicast traffic and to measure the network latency of the generated traffic. Multicast traffic was generated using jperf tool for analysis purpose. The defined network was simulated and Graphical Network Simulator-3(GNS3) was used as emulator. Our testbed consisted of two dual stacks, two identical workstations configured as separate networks with the 100Mb/s link. The experiments were executed for a sufficiently long period of time, 5 minutes to 180 minutes and results are taken for 32B

packet to 1,024B packet sizes. The experiments carried out for the Auto-configure Tunneling, 6to4 Tunneling and Weight Based Transition mechanism independently. Each value is an average of 100 independent experiments. The outline values have been ignored for computing average of the set of values.

The proposed Weight Based Transition mechanism was experimented in three different scenarios:
1. The IPv4 only networks (A most present scenario)
2. The IPv6 only networks (Anticipated future scenario)
3. The interim transitional phase (IPv4 and IPv6 co-exist) using tunneling.
- Dual Stack
- GRE Tunneling

VI. RESULTS AND DISCUSSION

The Weight Based Hybrid Transition algorithm was simulated under various scenarios includes IPv4 Only network, IPv6 Only Networks, Dual stack and GRE Tunneling. The GNS3 and "jperf" tools. The test period was 10 minutes. Each result shown was the average taken from 100 simulation runs. The Throughput, Jitter are taken for analysis purpose, as each simulation ran was independent of other, the distribution of mean job times approximated to a normal distribution.

Throughput: The IPv4 Only, IPv6 Only, Dual Stack, GRE Tunneling and Weight Based Transition were simulated independently. The throughput values were recorded for the duration of 10 minutes' test period as tabulated in Table 1.

Table.1 Throughput of the various algorithms

Size of the packet (bytes)	Throughput in %, Test Period=10 minutes.				
	IPv4 Only	IPv6 Only	Dual Stack	GRE Tunnelling	Weight Based Transition
32	100	100	94.841	100	100
64	100	100	94.844	100	100
128	100	100	94.846	100	100
256	100	100	94.856	100	100
512	100	100	94.872	100	100
1024	100	100	94.897	100	100

IPv4 Only, IPv6 Only, GRE Tunneling and Weight Based Transition were yielded 100 % throughput over the packet size from 32 to 1024 Bytes. The Dual Stack yielded throughput as an average of 94.85% over the packet size 32 to 1024 Bytes.
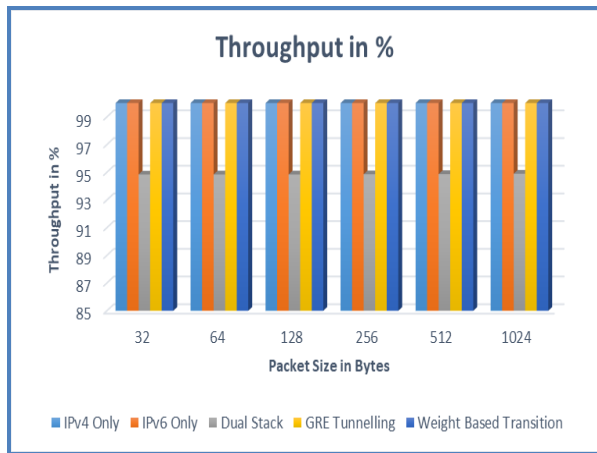
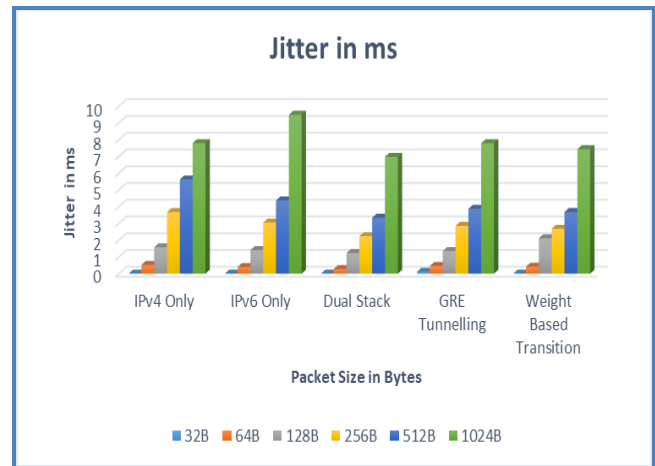**Fig.5 Throughput of various transition algorithms**

It was found that the Dual stack produced low throughput as it was required a complex computation to deal IPv4 and IPv6 coexistence conversion. The developed Weight Based Transition algorithm yielded 100% throughput as IPv4 Only, IPv6 Only and GRE Tunneling as the design principle was same as them. The 100% throughput performance was obtained for the range of data size from 32Bytes to 1024 Bytes. The throughput performance beyond this range of packet size was not the scope of the experiments. Hence, the performance of the throughput was not predictable beyond the range of the packet size i.e less than 32Bytes and greater than 1024Bytes of packet size.

Jitter: The IPv4 Only, IPv6 Only, Dual Stack, GRE Tunneling and Weight Based Transition were simulated independently. The throughput values were recorded for the duration of 10 minutes to an Hour as tabulated in Table 2.

**Table.2 Jitter of the various algorithms**

Size of the packet (bytes)	Jitter in ms, Test Period=10 – 60 minutes.				
	IPv4 Only	IPv6 Only	Dual Stack	GRE Tunnelling	Weight Based Transition
32	0	0	0	0.112	0
64	0.522	0.395	0.275	0.461	0.421
128	1.576	1.406	1.234	1.350	2.113
256	3.682	3.049	2.241	2.857	2.681
512	5.623	4.371	3.341	3.873	3.681
1024	7.792	9.487	6.972	7.787	7.432

IPv4 Only, IPv6 Only, Dual Stack, GRE Tunneling and Weight Based Transition were yielded Average Jitter as 3.839 ms, 3.741 ms, 2.812 ms, 3.265 ms and 3.265 ms over the packet size from 32, 64, 128, 256, 512 and 1024 respectively.

Fig.6 Jitter of various transition algorithms

The IPv6 only network was produced more jitter time at the packet size of 1024 Bytes while comparing with others. But surprisingly it was produced less Jitter time at 512Bytes when compared with IPv4 only network strategy as shown in Figure 7.1.2. It was because of packet handling mechanism in IPv6 network only strategy.
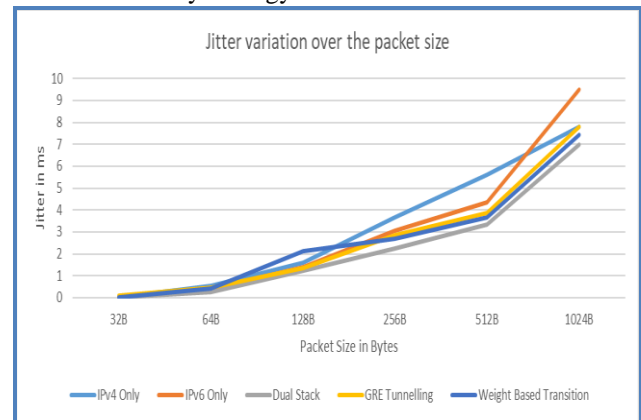
Fig.7 Jitter variation over the packet size

The presented Weight Based Transition algorithm had produced better Average Jitter time performance as 3.265 ms, than IPV4 and IPv6 only strategy. The jitter performance was as like as GRE Tunneling. However, it was under performed than Dual stack in Jitter time performance.

VII. CONCLUSION AND FUTURE WORK

The large address space of IPv6 is able to provide the demand of larger address space globally. But the network environment is to be upgraded from the existing facilities to use IPv6. The organizations are to be prepared for these changes in terms of technical, hardware/software support and economical terms. It may take another decade(s) with respect to their ability. This transition time urged to have a transition mechanism to the co-existence of IPv4 and IPv6.

A weight based hybrid transition mechanism has been developed to the co-existence of IPv4 and IPv6. The developed algorithm has been executed in the defined simulation bed and the results have been analyzed with the comparison of existing mechanisms.

It was found that the developed Weight Based Transition algorithm yielded the better performance in RTT latency as 42%, 42%, 40%, 38%, 36%, 37% reduction in RTT for 32, 64, 128, 256, 512, 1024 KB packet size respectively while comparing with the Tunneling mechanism. It is also observed that the performance on RTT decreases gradually as the size of the packet increases when comparing with the Tunneling mechanism.

The developed algorithm has been experimented in the defined simulation bed. The various transition strategies; include IPv4 only, IPv6 only, Dual stack, GRE Tunneling; Router-to-Router and Host-to-Host were used as simulation scenarios. The results have been analyzed with the comparison of existing mechanisms.

The proved algorithm can be used in small size organization to reduce cost of IPv6 deployment. The proved algorithm will give the better performance under Tunneling, Dual stack scenarios. However, it is not suitable in 6 to 4 mechanisms. The proposed algorithm can be used in the organization to minimize the RTT latency. The proposed algorithm can also be used in defense to minimize the IPv6 infrastructure overheads and increase the throughput in adhoc military networks. Particularly, it can be used in the nuclear ships for IP communication and management. The defense industry can use the proved algorithm for IP communication analysis with the limited amount of additional infrastructure and optimized bandwidth.

The future research direction of Weight Based Hybrid mechanism for IPV4/IPv6 transition algorithms can focus on the nature of 6 to 4 mechanism and prediction function for designing optimized algorithm for IPv4/IPv6 transition in the network. The various parameters and its impact on network performance will be considered for designing the multi-dimensional weight vectors for IPv4/IPv6 transition. The future algorithms will use the multi-dimensional weight vector for quantifying the importance of the packet for IPV4/IPv6 transition.

REFERENCES

1. Chen, C.-H., Lin, Y.-A., Wu, W.-T., Huang, Y.-T., Chu, C.-C., Design and Implementation of IPv4 and IPv6 Provisioning Technologies for VPC Architecture, 2019 20th Asia-Pacific Network Operations and Management Symposium: Management in a Cyber-Physical World, APNOMS 2019, 2019.
2. Abdullah, S.A., SEUI-64, bits an IPv6 addressing strategy to mitigate reconnaissance attacks, Engineering Science and Technology, an International Journal, Vol: 22,Issue: 2, 2019.
3. Augustus Devarajan, A., Sudalaimuthu, T., A cloud storage monitoring system using deduplication and file access pattern, International Journal of Recent Technology and Engineering, Vol: 8,Issue: 3, 2019.
4. Augustus Devarajan, A., Sudalaimuthu, T., Cloud storage monitoring system analyzing through file access pattern, ICCIDS 2019 - 2nd International Conference on Computational Intelligence in Data Science, Proceedings, 2019.
5. Bdair, A.H., Abdullah, R., Manickam, S., Al-Ani, A.K., Brief of Intrusion Detection Systems in Detecting ICMPv6 Attacks, Lecture Notes in Electrical Engineering, Vol: 603,Issue: , 2020.
6. Chen, C.-H., Lin, Y.-A., Wu, W.-T., Huang, Y.-T., Chu, C.-C., Design and Implementation of IPv4 and IPv6 Provisioning Technologies for VPC Architecture, 2019 20th Asia-Pacific Network Operations and Management Symposium: Management in a Cyber-Physical World, APNOMS 2019, 2019 .
7. Dawadi, B.R., Rawat, D.B., Joshi, S.R., Evolutionary Dynamics of Service Provider Legacy Network Migration to Software Defined IPv6 Network, Advances in Intelligent Systems and Computing, Vol: 936,Issue: , 2020.
8. Jeevitha, R., Bhuvaneswari, N.S., Solutions to overcome ipv4/ipv6 compatibility issues in vehicular adhoc networks, International Journal of Innovative Technology and Exploring Engineering, Vol: 9,Issue: 1, 2019.
9. Jia, S., Luckie, M., Huffaker, B., Elmokashfi, A., Aben, E., Claffy, K., Dhamdhere, A., Tracking the deployment of IPv6: Topology, routing and performance, Computer Networks, 2019.
10. Lin, J.-J., Wang, K.-C., Cheng, S.-M., Liu, Y.-C., On exploiting SDN to facilitate IPv4/IPv6 coexistence and transition, 2017 IEEE Conference on Dependable and Secure Computing, 2017.
11. Muthu, T.S., Kumar, K.R., Hybrid predictive approach for replica replacement in data grid, 2017 4th International Conference on Advanced Computing and Communication Systems, ICACCS 2017, 2017.
12. Pandiaraj, S., Sudalai Muthu, T., Prioritization of replica for replica replacement in data grid, International Journal of Recent Technology and Engineering, Vol: 7,Issue: 5, 2019.
13. Rohini, A., Sudalai Muthu, T., A weight based scheme for improving the accuracy of relationship in social network, International Journal of Innovative Technology and Exploring Engineering, Vol: 8,Issue: 11, 2019.
14. Rohini, A., Sudalai Muthu, T., Weight based approach for improving the accuracy of relationship in social network, Journal of Advanced Research in Dynamical and Control Systems, Vol: 11,Issue: 8, 2019.
15. Su, C., Liu, R., Li, X., A study on the distribution of active IPv6 addresses used by websites, Proceedings of 2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference, ITAIC 2019, 2019.
16. Sudalai Muthu, T., Rohini, A., A correlative scrutiny for improving the career guidance links in social network, International Journal of Engineering and Advanced Technology, Vol: 9,Issue: 1, 2019.
17. Sudalaimuthu, T., Rameshkumar, K., Sarukesi, K., A weight based replica replacement algorithm in data grid, Journal of Advanced Research in Dynamical and Control Systems, Vol: 9,Issue: Special Issue 6, 2017.
18. Zhang, Q.-L., Jiang, C.-P., Wang, J.-L., Li, X., A Survey on IPv6 Address Structure Standardization Researches [IPv6] Jisuanji Xuebao/Chinese Journal of Computers, Vol: 42,Issue: 6, 2019.

AUTHORS PROFILE

Dr. B. I. D. Kumar is working as an Associate Professor in the Department of Computer Science and Engineering, Amruta Institute of Engineering and Management Sciences, Bangalore, India. He received his Ph.D degree from VTU University, Karnataka. He has more than ten publications in the reputed International Conferences and Indexed Journals. His research areas are Computer Networks, Network Forensics. He is an active member of CSI, ISTE and IEEE.

Dr. G. Vasanth, is working as a Professor in the Department of Computer Science and Engineering, Government Engineering College, Visvesvaraya Technological University K.R.Pet, Karanataka, India. He received his Ph.D degree from Magadh University, Bodh Gaya, Bihar, India. He has more than 50 publications in the reputed International Conferences and Indexed Journals. He also chaired and delivered 20+ keynote speech in the reputed International Conferences. His research areas are Computer Networks, Network Security, He is a life time member of CSI, ISTE, he is a member of ACM and IEEE.

Dr. Sudalaimuthu T, is working as an Associate Professor in the Department of Computer Science and Engineering, Hindustan Institute of Technology and Science, Chennai. Tamilnadu, India. He received his Ph.D degree from Hindustan University, Chennai. India. He is a ETH Certified Ethical Hacker. He has has more than 30 publications in the reputed International Conferences and Indexed Journals. He delivered more than 30 key note speeches in International Conferences, Seminars, and Workshops. He is received many awards and accolades in his career includes Best Teacher Award, Best innovator Award. His research areas are Network Security, Advanced Computing. He is a life time member of CSI, ISTE, he is a member of ACM and IEEE.