Impact of IPv4, IPv6 and Dual Stack Interface over Wireless Networks

Varsha Jain
Student M.Tech, BIST, Bhopal
E-mail: its.varsha16@gmail.com

Damodar Tiwari
Assistant Professor, BIST, Bhopal
E-mail: damodarptiwari21@gmail.com

Shailendra Singh
Professor & Head, NITTTR, Bhopal
E-mail: ssingh@nitttrbpl.ac.in

Sanjeev Sharma
Professor & Head, SOIT, RGPV, Bhopal
E-mail: sanjeev@rgtu.net

Abstract—The entire networking society is tremendously moving towards the IPv6 addressing architecture leaving behind the IPv4 address space. This happens due to the tremendous growth of Internet usage over the networking. The government has mandated that all the devices would be IPv6 compatible as the delay in the deployment of IPv6 would result in the negative impact of future growth and global connectivity of the internet. In this paper we are dealing with the impact of different interfaces like IPv4 only, IPv6 only and Dual stack mechanism over wireless networks with varying PHY and MAC layer interface of 802.11 a/g and 802.11 b standards. The results are simulated over Qualnet 5.1 simulator with various parameters like throughput, delay, jitter and packet delivery ratio is been calculated.

Index Terms—Dual Stack, Interface, IPv4, IPv6, nodes.

I. INTRODUCTION

Internet protocol version 4 (IPv4) is the most widely used addressing protocol defined in the world's standard and is in the final stage of exhaustion of its unallocated address space. IPv4 is the 32 bit protocol which uniquely and universally defines the connection of a device to the Internet. With its 32 bits it can address up to 2^{32} devices i.e. more than 4.3 billion addresses[1]. IPv4 was developed in 1982, at that time traffic was very elastic and internet was only used for mail and file transfer purpose. To handle this kind of traffic is very flexible, on the other hand the tremendous growth of internet have resulted for the use of multimedia and different kinds of inelastic traffic which requires a certain level of performance which cannot be met using IPv4. IPv6 was designed to meet with the requirements of future applications in mind and to solve the address exhaustion problem faced by IPv4.

IPv6 is the next generation internet protocol uses 128 bits, i.e. it can be used to address 2^{128} devices over the internet which is 2^{96} times more than IPv4[2]. IPv6 additionally offers sundry advantages over the legacy IPv4 like larger address space, Scalability, Fixed Header, Quality of Service, Security, Plug and play and many more. The usage of IPv6 will led the organizations to take the numerous opportunities presented by Internet of Things (IOT) to Internet of Everything (IOE). This adoption will provide various technological enhancements which could be beyond our imagination. The migration towards IPv6 is not an option it's a necessity as a very few IPv4 addresses are remaining. There will be estimated 50 billion connected devices by 2020, which is not possible with the usage of IPv4 address [3, 14]. So in future to amend the network connectivity and operations the organizations public and private, regime sectors will require to transition towards IPv6.

IPv6 will gradually supersede IPv4 and it will still take a lot of time to migrate towards IPv6. Till then we have to deal with networks in which IPv4, IPv6 and both the networks will coexist. The biggest problem with the two protocols is that IPv6 is not a superset of functionality that is backward compatible with IPv4 and IPv4 hosts and routers do not support IPv6. Different migration techniques have been suggested from the past to enable the smooth transition between the two protocols like dual stack, tunneling and header translation [4]. Dual stack [5]

enables to operate both the protocol stack on all the components of the network system. Tunneling deals with encapsulating one packet inside another and carrying the packets across the networks. Header translation deals with header and address translation through between the two protocols, by translating through CG NAT (Carrier Gateway Network Address Translator) device. Fig 1 depicts the transition scenario how IPv6 would gradually replace IPv6.
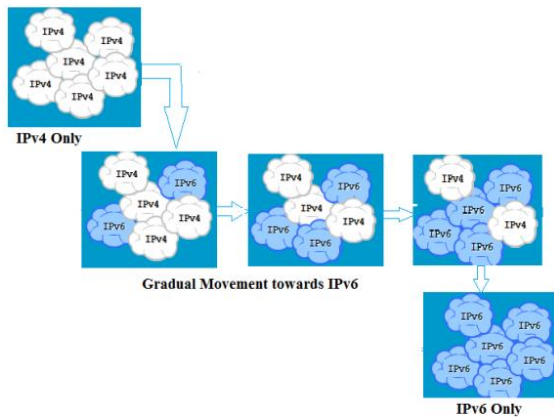

Fig.1. Transition Scenarios

In this paper we are dealing with the dual stack mode of transition. In dual-stack architecture, all the components of the network system should support both the protocols IPv4 and IPv6. Applications must choose either IPv4 or IPv6, by selecting the correct address based on the type of IP traffic and particular requirements of the communication. Currently dual-stack is the most preferred deployment strategy for the network with a mixture of IPv4 and IPv6 applications that require both the protocols. But it includes many problems like all the network infrastructures i.e. router, bridges devices etc must be upgraded to IPv6 and it also requires the dual management of IPv4 and IPv6 routing tables. Simplicity of routing is supposed to be a strength of IPv6, if this sort of transition mechanism were used it would become a weakness. In this paper we are analyzing the impact of IPv4 interface, IPv6 interface and Dual stack interface over wireless networks with varying PHY and MAC layer interface of 802.11 a/g and 802.11 b standards. 802.11a/g PHY is an extension to IEEE 802.11 PHY that applies to wireless LANs and provides up to 54 Mbps in the 5 GHz band. 802.11a PHY uses an orthogonal frequency division multiplexing encoding scheme[6]. 802.11b PHY is an extension to IEEE 802.11 PHY that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b PHY uses only Direct-Sequence Spread-Spectrum (DSSS) modulation [7].

Here we have considered different scenarios to assist the migration towards IPv6. It is not possible to convert the entire network to IPv6 in one shot so dual stack and tunneling mode will be used. The different scenarios have been considered for the work to do are.

1. Backbone becomes Dual Stack: In this case, the core

backbone is converted to dual stack (IPv4 and IPv6) and the servers and tributaries remain at IPv4. This approach could be the starting point for migrating towards IPv6. Here No applications needs to be converted as this is very difficult and time consuming task. Fewer pieces of equipment need to be converted. In this approach, only the backbone or core routers need to be converted.

2. Backbone remains IPv4; only edge/boundary becomes IPv6: In this case, the core remains at IPv4. Here an application at a remote server must be accessed via IPv6. A tunnel or translation gateway must be provided. The options include: static tunnels, 6to4 dynamic tunnels, GRE tunnels or IPv6 proxies. The remote routers will perform conversion of packets from IPv6 to IPv4. The IPv4 packet will go across the network and be converted to IPv6 at the receiving end.

Rest of the paper is structured as follows: Section II describes about the deployment status of IPv6 across the internet. Section III discuss about the different types of nodes available during the transition process. Section IV describes the Simulation scenario & Algorithm. Results are discussed in section V. Section VI concludes the paper.

II. DEPLOYMENT STATUS OF IPv6 ACROSS THE INTERNET

Today, Internet of Things is very much a part of our everyday lives and it would be impossible to keep us away from this development. Internet design is inspired by types of communication in that time, such as mail, telephone and telegram. The popularity and wide acceptance in the world of internet, causing rapid and unexpected growth in this network, so that we have seen popularity among billions of users [8]. As per Gartner's prediction, by 2020 there will be 20.4 billion connected devices in 2017, up 31% from 2016 and market value 2.1 trillion dollars by 2020[9]. This would be possible with the adoption of next generation internet protocol IPv6. The next generation internet protocol IPv6 is in the various stages of deployment across the internet. Despite of numerous advantages that IPv6 offers over IPv4, the adoption rate of IPv6 by the end users is very slow. To adopt IPv6 is the only way to sort out the address depletion problem which was the major issue faced by IPv4. As per the recent Google's statistics as on 14 May 2017, shows the availability of approximately 18% IPv6 addresses availability to its user[10]. The availability of IPv6 connectivity among Google users is shown in fig 2.

From the fig it is clear that the IPv6 adoption rate by the users is still very low. This is due to the fact of incompatibility of two protocols. IPv4 will remain in the market for the long time unless the entire network will be switched to IPv6. In this duration both the protocols need to coexist for a long time.
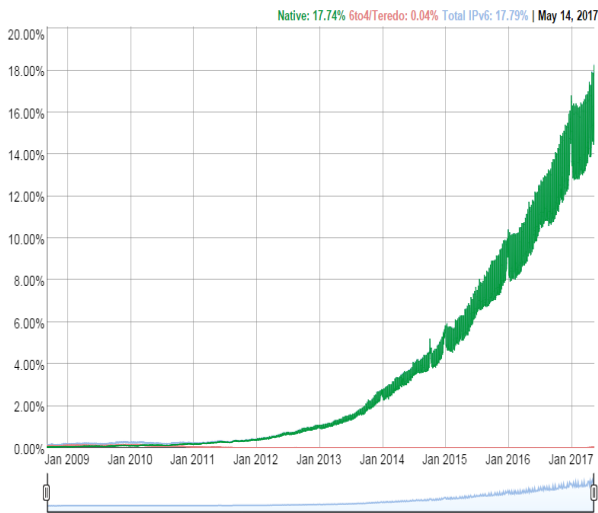
Fig.2. Percentage of users that access Google over IPv6

III. TYPES OF NODES

Successful transition from IPv4 to IPv6 is a crucial task as only a very small part of the world's population is using IPv6. The main issue arises with the compatibility of the two protocols is that both the protocols are not compatible with each other [11]. The differences arise in their headers and the way the routers and intermediate devices handles the packets. An IPv6 packet cannot be handled by an IPv4 device and vice versa. To enable the smooth transition process the devices must be compatible to deal with both the protocol stacks. The IPv6 specification requires 100 per cent compatibility for the existing protocols and existing applications during the transition. The different types of devices available in the network are and their compatibility is shown in table-1:

1. IPv4 only node – This type of host or router implements only IPv4 and it does not understand IPv6. It discards IPv6 packets. The devices that exist before the transition begins are IPv4 only nodes.
2. IPv6 only node – This type of host or router implements only IPv6 and it does not understand IPv4. It discards IPv4 packets. These devices will exist once the entire network will be moved towards IPv6.
3. IPv6 node – This type of host or router implements IPv6. But it also understands IPv4
4. IPv6/IPv4 and IPv6-only nodes are both IPv6 nodes.
5. IPv4 node – Any host or router that implements IPv4. IPv6/IPv4 and IPv4-only nodes are both IPv4 nodes.
6. IPv6/IPv4 node – A host or router that implements both IPv4 and IPv6, which is also known as dual-stack.
7. IPv6-only node – A host or router that implements IPv6, and does not implement IPv4.

The following section III describes about the simulation of all the cases discussed in table 1.

Table 1. Compatibility for Types of Nodes

Type of Node	IPv4 only node	IPv4 node	IPv6 only node	IPv6 node
IPv4 only node	√	√	X	√
IPv4 node	√	√	X	√
IPv6 only node	X	X	√	√
IPv6 node	X	√	√	√

IV. SIMULATION SCENARIO & ALGORITHM

Simulation is done to provide a suitable environment for specifying the network conditions like channel properties, terrain details, networking devices and the specifications of entire protocol stack. Different Simulators have been used from the past to test the network protocols over different networks due to the fact that it is difficult to test the performance of network over a large scale live network. To acquire all the necessary details a scenario has been designed in Qualnet 5.1 to simulate our desired characteristics. Qualnet 5.1 Simulator which is a comprehensive suite of tools for modeling large wired and wireless networks. It uses simulation to predict the behavior and performance of networks to improve their design, operation and management. We have tested the impact of IPv4, IPv6 and Dual stack protocols over wireless networks with hundred nodes. Fig 3 shows the scenario of wireless networks.
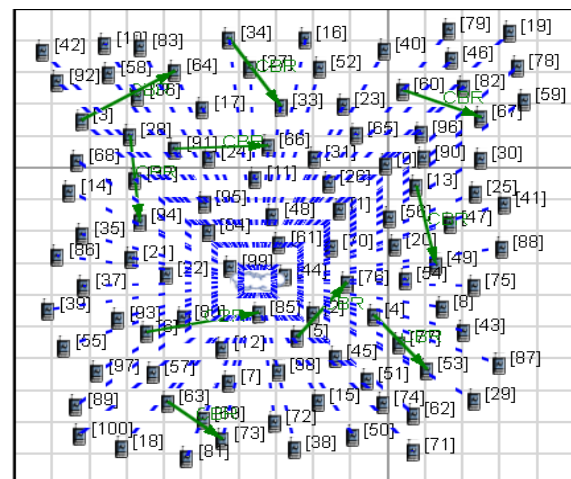

Fig.3. Scenario Wireless Network

A Field configuration of 1500m x 1500m is used for simulation on Qualnet 5.1 simulator. In this scenario we have taken wireless network 802.11 a/g and 802.11 b with 100 nodes. Each node in the network acts as router which routes packet to its intended destination. To generate the application layer traffic 10 Constant Bit Rate (CBR) application are used for transmitting packets of a fixed size at a fixed rate [12]. The sending rate is 100 packets per second. MAC protocol 802.11 for wireless network is used. Here we have considered five different cases based on the interfaces and types of nodes.

Case-1: V4 only- In this case nodes as well as interface on the network is based of version 4 of internet protocol.

Case-2: V4 nodes Dual interface- In this case node on the network is V4 and the interface is dual stack. In this case the communication is done through V4 mode.

Case-3: V6 Only - In this case nodes as well as interface on the network is based of version 6 of internet protocol.

Case-4: V6 nodes Dual interface - In this case node on the network is V6 and the interface is dual stack. In this case the communication is done through V6 mode.

Case-5: Dual Stack- In this case both nodes and interfaces are operating upon dual stack environment.

On the basis of these five cases following parameters have been taken into consideration [13]-

Throughput: Throughput is defined as the average rate of successful packet delivery on the communication channel. This is important metric because it reflects the overall performance of the network, and its effect is also shown on other network parameters. Generally it is measured in bits / second. The formula for throughput is given as:

$$Throughput\ (T) = 8 \times \frac{(Total\ No.\ of\ bytes\ received)}{(Time\ last\ packet\ sent - time\ first\ packet\ sent)}$$

Average End-to-End Delay: It is time to send a packet to the source until it is received by the destination. This includes various delays such as queuing delay, processing delay, propagation delay etc. This is very important factor for any network because it affects the quality of the service. This is usually measured in seconds. The formula for calculation of delay is given as follows:

$$Average\ end-to-end\ delay = \frac{(Total\ transmission\ delays\ of\ all\ received\ packets)}{Number\ of\ packets\ received}$$

Where

$$Transmission\ delay\ of\ a\ packet = (Time\ packet\ received\ at\ server - Time\ packet\ transmitted\ at\ client)$$

Average Jitter: It is time difference in the interval between two consecutive packets. For example, if the packet reaches T1 and packet2 at the time, then it reaches the time 2, compared to Jitter = (T1-T2). Jitter is inversely proportional to the quality of application. Jitter can be calculated only when at least two packets have been received. The formula for calculation of jitter has been given as follows:

$$Average\ jitter = \frac{Total\ packet\ jitter\ for\ all\ received\ packets}{(number\ of\ packets\ received - 1)}$$

Where

$$Packet\ Jitter = (Transmission\ delay\ of\ current\ packet - transmission\ delay\ of\ previous\ packet)$$

Packet Delivery Ratio: Packet Delivery ratio is the ratio of total number of packets received at the destination to the total number of packets sent by the source. The formula for packet delivery ratio (PDR) is given as:

$$Packet\ Delivery\ Ratio = \frac{(Total\ number\ of\ packets\ received)}{(Total\ number\ of\ packets\ sent} \times 100$$

Algorithm:

Step 1: Configure the wireless network with 100 nodes.

Step 2: Select the nodes and add them to the wireless device so that they can be configured under a single wireless domain.

Step 3: Configure the interfaces using Command line interface (CLI) from the GUI and consider the following cases:

Case-1: **V4 only**- In this case nodes as well as interface on the network is based of version 4 of internet protocol. For this case all the nodes are capable of running IPv4 only protocol stack. At the physical Interface we have configured v4 interface. All the devices are IPv4 only devices and are capable of executing v4 interface. They cannot handle v6 traffic.

Case-2: **V4 nodes Dual interface**- In this case node on the network is V4 and the interface is dual stack. For this case all the nodes are capable of running IPv4 only protocol stack. At the physical Interface we have configured dual stack interface. All the devices are IPv4 only devices and are capable of executing dual stack interface. In this case the communication is done through V4 mode.

Case-3: **V6 Only** - In this case nodes as well as interface on the network is based of version 6 of internet protocol. For this case all the nodes are capable of running IPv6 only protocol stack. At the physical Interface we have configured v6 interface. All the devices are IPv6 only devices and are capable of executing v6 interface. They cannot handle v4 traffic. Here network is capable of handling IPv6 applications but cannot support IPv4 applications. This scenario is the scenario of native IPv6.

Case-4: **V6 nodes Dual interface** - In this case node on the network is V6 and the interface is dual stack.

In this case the communication is done through V6 mode. For this case all the nodes are capable of running IPv6 only protocol stack. At the physical Interface we have configured dual stack interface. All the devices are IPv6 only devices and are capable of executing dual stack interface. In this case the communication is done through V6 mode.

Case-5: Dual Stack- In this case both nodes and interfaces are operating upon dual stack environment. For this case all the nodes are capable of running IPv4 and IPv6 protocol stack. At the physical Interface we have configured dual stack interface. In this case the communication is done through both the stacks depending upon the application. Here network is capable of handling both the applications but preference is given to IPv6 over IPv4.

Based on the above cases different configuration files and settings have been done.

Step 4: Once the case is decided and necessary configuration files have been changed the scenario is compiled.
Step 5: After successful compilation, results have been obtained and on the basis of the performance we have calculated different parameters.
Step 6: End Algorithm.

V. RESULT & DISCUSSION

On the basis of simulation results we have developed our results for different parameters. We have tested it over 802.11 a/g and 802.11 b standards. The metric based analysis for different interfaces and nodes types based on five cases are shown in table 2-5 and fig- 4-7.

Throughput: Fig 4 shows the comparison of throughput for all the five cases. In the comparison of performance for throughput of different cases, we have obtained the best throughput for 802.11 a/g standard is obtained in the case of v6 nodes dual stack. This is the case when nodes are v6 only and the interface used for communication is v6 from the dual stack mode. This is due to the fact when the nodes are v6 only they are using better mechanism for communication and the packet loss is less in this case. Where as in v4 nodes dual stack mode and purely dual stack modes the results are same. For 802.11 b standard better results are obtained in the case of v4 nodes dual stack mode and purely dual stack modes. This is due to the case that in both the standards the communication is done using v4 protocol stack. Results are high in 802.11a/g standard due to high bandwidth as compared to 802.11b.
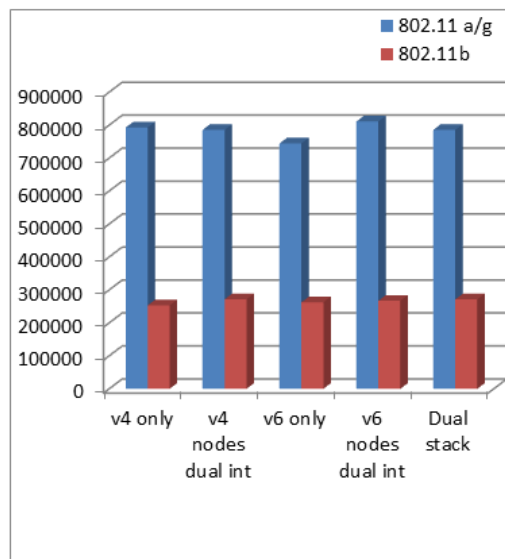

Fig.4. Throughput

Table 2. Throughput (bits/s)

Node Types	802.11 a/g	802.11b
v4 only	792558	252974
v4 nodes dual int	785483	271234
v6 only	744347	262457
v6 nodes dual int	810843	267034
Dual stack	785483	271234

Average End-to-End Delay (s): Fig 5 shows the comparison of Average end-to-end delay for all the five cases. In the comparison of performance for Average End-to-End Delay of different cases the minimum delay for 802.11 a/g and 802.11 b standard is obtained in the case of v4 only nodes. This is the case when the entire network is v4 only including the backbone network. Due to small packet size and high throughput the delay is reduced however in other cases delay is less but it is highest in v6 only case for 802.11a/g because due to more number of bits transmitted in this case.
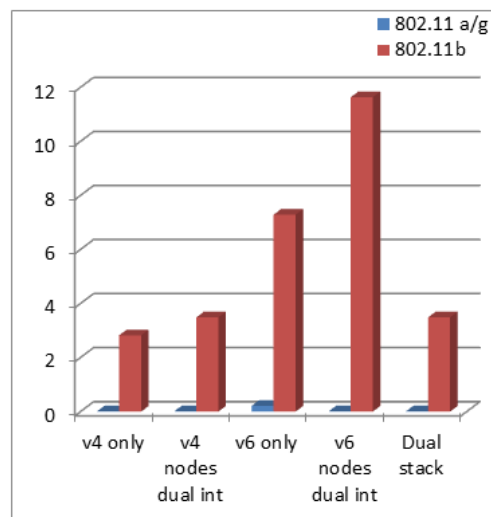

Fig.5. Average End-to-end Delay

Table 3. Average End-to-End Delay (s)

Node Types	802.11 a/g	802.11b
v4 only	0.00979836	2.82147
v4 nodes dual int	0.0105683	3.48642
v6 only	0.209504	7.28305
v6 nodes dual int	0.0110946	11.633
Dual stack	0.0105683	3.48642

Average Jitter: Fig 6 shows the comparison of Average Jitter for all the five cases. In the comparison of performance for Average end to end delay of different cases the delay is negligible for 802.11 a/g. It is high in case of 802.11 b standard due to low bandwidth and is extremely high in the case of v6 only node due to large packet size of IPv6. This is the case when the entire network is v6 only and including the backbone network.
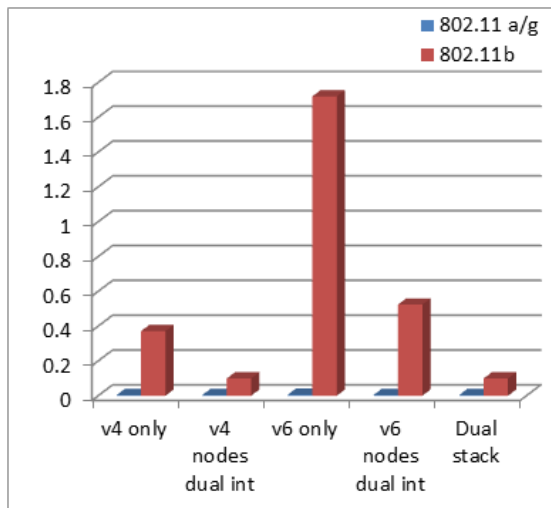

Fig.6. Average Jitter

Table 4. Average Jitter (s)

Node Types	802.11 a/g	802.11b
v4 only	0.00365297	0.371044
v4 nodes dual int	0.00373039	0.098949
v6 only	0.00637955	1.71995
v6 nodes dual int	0.0036351	0.523556
Dual stack	0.00373039	0.098949

Packet Delivery Ratio: Fig 7 shows the comparison of Packet Delivery Ratio for all the five cases. In the comparison of performance for packet delivery ratio of different cases the PDR is highest for v6 nodes dual interface for 802.11 a/g. It is also high in case of 802.11 b for the case Dual stack and the v4 nodes dual int. This can be seen with the performance of throughput also.
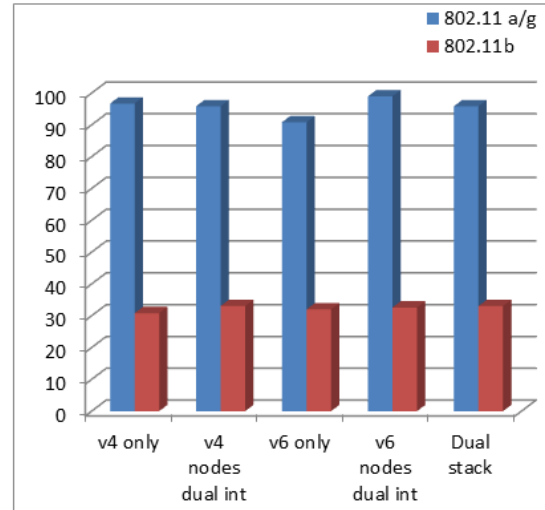

Fig.7. Packet Delivery Ratio

Table 5. Packet Delivery Ratio

Node Types	802.11 a/g	802.11b
v4 only	96.71333333	30.81333
v4 nodes dual int	95.84933333	33.03467
v6 only	90.84133333	31.99067
v6 nodes dual int	98.97466667	32.588
Dual stack	95.84933333	33.03467

VI. CONCLUSION

IPv6 is the next generation Internet protocol which will eventually replace IPv4, but until this happens these two protocols need to coexist for a long time. IPv6 offers several benefits over IPv4, still the adoption rate is very low over worldwide. In this paper we have show the deployment status of IPv6 across the Internet which is very low. IPv6 is necessity and not the choice so it needs to be adopted. In this paper we have deployed the scenario of wireless network over different PHY and MAC layer interface of 802.11 a/g and 802.11 b standards. Five cases have been considered and results have been obtained on Qualnet 5.1 simulator for various parameters like throughput, delay, jitter and packet delivery ratio. Results shows that the out of all the cases best result is obtained for v6 nodes dual int case when a node on the network is V6 and the interface is dual stack. In this case the communication is done through V4 mode. This study would be useful for the deployment of IPv6 protocol across the Internet.

REFERENCES

[1] M. D. Rey. California 90291. Internet Protocol, Darpa Internet Program, Protocol Specification. RFC 791. [Online]. Available: http://tools.ietf.org/html/rfc791

[2] W. Lehr, T. Vest, and E. Lear, "Running on empty: The challenge of managing Internet addresses," Internet Assigned Numbers Authority File Version: Internet Address TPRC 10_21_08.doc.

[3] Hurlburt, George F., Jeffrey Voas, and Keith W. Miller. "The Internet of Things: a reality check." IT Professional 14.3 (2012): 56-59.

[4] Chauhan, Dipti, and Sanjay Sharma. "A survey on next generation Internet Protocol: IPv6." Int. J. Electron. Ind. Eng. (IJEEE), ISSN 2.2 (2014): 125-128.

[5] Tsuchiya, Kazuaki, Hidemitsu Higuchi, and Yoshifumi Atarashi. Dual stack hosts using the" bump-in-the-stack" technique (BIS). No. RFC 2767. 2000.

[6] IEEE Std 802.11a–1999, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHz Band." September 16, 1999.

[7] IEEE Std 802.11b-1999, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band." September 16, 1999.

[8] Rezaei, Hadis, and Asad Vakili. "Named Data Networking: Investigate of New Infrastructure for Future of Internet." International Journal of Computer Network and Information Security 9.1 (2017): 40.

[9] Mazhelis, Oleksiy, et al. "Internet-of-things market, value networks, and business models: State of the art report." University of Jyvaskyla, Department of Computer Science and Information systems, Technical Reports TR-39 (2013).

[10] https://www.google.com/intl/en/ipv6/statistics.html#tab=i pv6-adoption&tab=ipv6-adoption.

[11] Bohlin, Erik, and Sven Lindmark. "Incentives to innovate with next generation networks." Communications and Strategies 48.4 (2002): 97-117.

[12] Chauhan, Dipti, Jay Kumar Jain, and Sanjay Sharma. "An end-to-end header compression for multihop IPv6 tunnels with varying bandwidth." Eco-friendly Computing and Communication Systems (ICECCS), 2016 Fifth International Conference on. IEEE, 2016.

[13] Chauhan, Dipti, and Sanjay Sharma. "Addressing the Bandwidth issue in End-to-End Header Compression over IPv6 tunneling Mechanism." International Journal of Computer Network and Information Security 7.9 (2015): 39.

[14] Jain, Jay Kumar, and Dipti Chauhan. "Recent Research Work on Ad-Hoc Networks: A Literature Survey."

Authors' Profiles

Varsha Jain: She completed her B.E. from Truba Institute of Engineering & Information Technology, Bhopal in 2014. She is pursuing M.tech. from Bansal Institute of Science & Technology, Bhopal. Her research interests include next generation networks and IPv6.

Damodar Tiwari: Has been working at the Bansal Institute of Science and Technology, Bhopal since 2006. He holds B. E. and M.Tech in Computer Science. His area of research is cloud computing, parallel computing. Email:damodarptiwari21@gmail.com

Dr. Shailendra Singh: He is a professor and head of the department in CSE deptt at the NITTTR, Bhopal. He holds M.Tech and PhD in Computer Science. His are of research is Support Vector Machine, Machine Learning, Software Engineering, Network Security & Image Processing, cloud computing, parallel computing. Email: ssingh@nitttrbpl.ac.in

Dr. Sanjeev Sharma: He is a professor and head of SOIT- RGPV, Bhopal. He holds M.Tech and PhD in Computer Science. His are of research is Soft Computing, Machine Learning, Network Security & Image Processing, cloud computing, parallel computing. Email: Sanjeev@rgtu.net