INTERNATIONAL JOURNAL ON ORANGE TECHNOLOGY

https://journals.researchparks.org/index.php/IJOT e-ISSN: 2615-8140 | p-ISSN: 2615-7071

Volume: 03 Issue: 7 |Jul 2021

Transition from IPv4 to IPv6 Network in IoT Security Based Upon Transition Methods

Ms. Shilpa B. Sarvaiya[1], Dr. D. N. Satange[2]

[1]Department of Computer Science, Vidyabharati Mahavidyalaya, Amravati, Maharashtra, India

[2]Director, Student Development, S. G. B. A. University, Amravati, Maharashtra, India

----------***----------

Abstract: While deployments of IPv6 networks have increased over recent years, especially in IoT Paradigm. Today there are two types of internet protocol versions that are currently working in the global internet to transfer data from one electronic device to another.IPv4 which consists of 32 bits long addresses and IPv6 which consists of 128bits long addresses which is more effective as it can handle billions of devices and can assign each device different IP address. This paper will present an overview of the main migration technologies that can be used to transition from an IPv4 network to an IPv6 network, this paper will also research on finding and comparing the effects of IPv6 transition methods such as Dual Stack, Tunneling and Network Address Translation-Protocol Translation will be compared on variant parameters to find the best performing transition method in IoT Network in terms of security.

Keywords: IoT (Internet of Things), IPv4 (Internet Protocol Version 4), IPv6 (Internet Protocol Version 6), Transition Methods, Dual Stack, Tunneling, NAT-PT.

1. Introduction:

In the modern area there are two types of internet protocol versions that are currently working in the global internet to transfer data from one electronic device to another. IP address are assigned to every device and every device has its unique address generated through binary values consists of 0 and 1. Today these two versions of Internet protocol are widely used to connect different networks to each other. IPv4 is the earlier version of IPv6. IPv4 consists of 32 bits long addresses and each unique address is assigned to each device so data can be transmitted to that specific address [1].

The new version of Internet Protocol was published in 1996 called IPv6 which consists of 128 long bits addresses. Due to large number of growths in electronic devices, an IPv4 address was not enough to cover all the devices. To resolve the issue IPv6 introduced which can handled billions of devices and more than that and assign each device different unique address that is IP address. IPv6 found out much better and efficient in addressing of devices, routing of networks, security of information and data, translation of network address also in support of configuration of protocol. Assign a unique IP address IoT devices establish a secure communication channel, their connection should be bootstrapped through the so-called device binding process and visualize sensor data, users can easily understand the physical environment and operate the devices [2].

A variety of transition methods are available to facilitate the migration to IPv6.These methods have been observed and compared with each other and the effects of these transition methods on IPv6 in IoT security. These transition strategies are observed and compared that are Dual-Stack, Tunneling and NAT-PT Each method or technique has its own pros and cons and each method performs its own strategy [3].

1.1. Importance of IPV6 Network in IoT Security:

The internet communications have evolved rapidly after the creation of IPv6 Internet Protocol version 6. The major difference of IPv6 is that it allows more unique addresses to create. There are five major reasons why IPv6 is more important and better option for the IoT network paradigm than IPv4 Internet Protocol version 4.

First and most important one is the security: Security is the most important feature used to secure the communication between the IoT devices from threats, virus, attacks, etc. IPv6 uses end-to-end encryption technology which can encrypt the data so it can be secured and cannot be hacked. IPv6 also supports more secure and safe name resolution than IPv4.

INTERNATIONAL JOURNAL ON ORANGE TECHNOLOGY
https://journals.researchparks.org/index.php/IJOT e-ISSN: 2615-8140 | p-ISSN: 2615-7071
Volume: 03 Issue: 7 |Jul 2021

Second is the scalability: Ipv6 protocol provides the connections of devices in more scalable form. It provides large area of devices so they can connect together on a large scale communicating over a long distance as well [4].

Third is the connect ability: which means connecting billions of devices to each other and allow a networking protocol so they can transfer data to each other.IPv6 allows much more addresses than IPv4 so billions of devices can connect to each other.

Fourth is Internet Protocol version 6 uses multicasting: To transmit data packets from one destination to another means IPv6 supports multicasting of packets at one time in different destinations.

Fifth is IP Protocol version 6 providing Authentication: IP version 4 does not provide authentication whereas IP version 6 provides Authentication as well as Confidentiality, Integration, and Access control of each data packet [5].

The overall graph of the adoption of IPv6 by Internet users since late 2015 to 2025 is shown in figure 1.

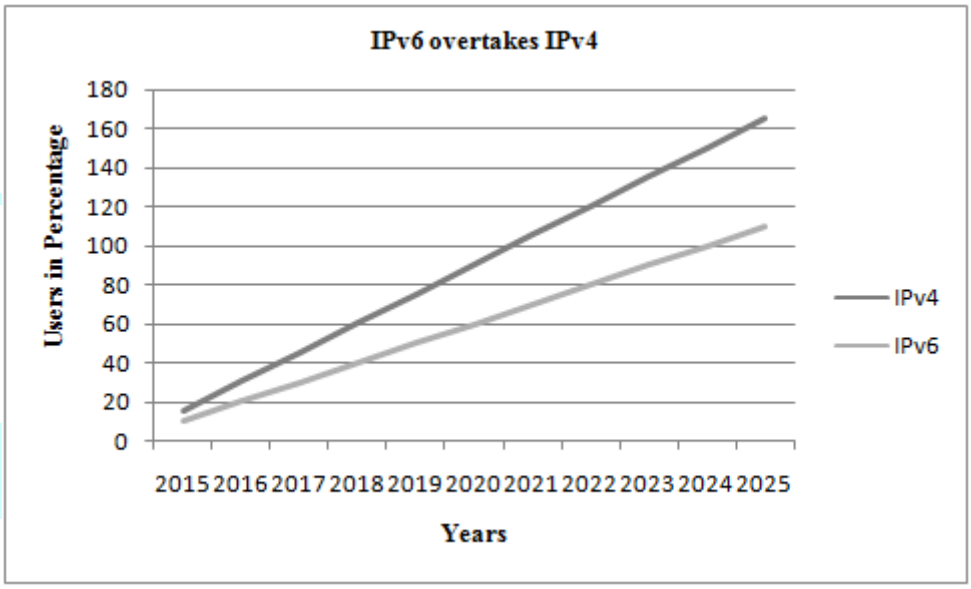

Figure 1: Growth from IPv6 to IPv4 Network

2. History:

In late 1960's there was a great need and demand of research centres and universities to develop a protocol or networking system to exchange data. To overcome this need ARPA (Advanced Research Project Agency) developed a net called ARPANET from 1972 it renamed DARPA from ARPANET [6].

In 1981 the ARPANET developed a transfer control protocol called IPv4 which was a huge success [7].

After 1990's IPv4 address space was getting full and at that time there was not enough addresses left to assign the new devices [8].

The new version of Internet Protocol was published in 1996 called IPv6 which consists of 128 long bits addresses. IPv6 found out much valuable and impressive as compared to IPv4 and it found out much better and efficient in addressing of devices, routing of networks, security of information and data, translation of network address and in support of configuration of protocol [9].

Still now these two versions are using. Both internet protocols have different configurations and are used in different environment. A census of the Internet's connected devices would readily number in the tens of billions of devices. If they all needed a globally unique permanent IP address, IPv6 would have been an imperative over a decade ago [10].

INTERNATIONAL JOURNAL ON ORANGE TECHNOLOGY
https://journals.researchparks.org/index.php/IJOT e-ISSN: 2615-8140 | p-ISSN: 2615-7071
Volume: 03 Issue: 7 |Jul 2021

3. Transition from IPV4 to IPV6 Network in IoT Security:

There is not complete transition from IPv4 to IPv6 because IPv6 is not backward compatible. However; there are three methods, which can convert IPv4 to IPv6.The methods that can convert IPv4 to IPv6 are described as below.

3.1. Transition Methods:

One of the most important parts of implementing IPv6 is being able to gracefully transition from IPv4.The methods discussed in this paper can each be used as option when beginning an IPv6 deployment and should each be looked over for applicability depending on the specific requirements of an organization. There are three main methods that can be used when transitioning a network from IPv4 to IPv6 in IoT environment. These methods are 1) Dual-Stack, 2) Tunneling and 3) NAT-PT is explained in this section.

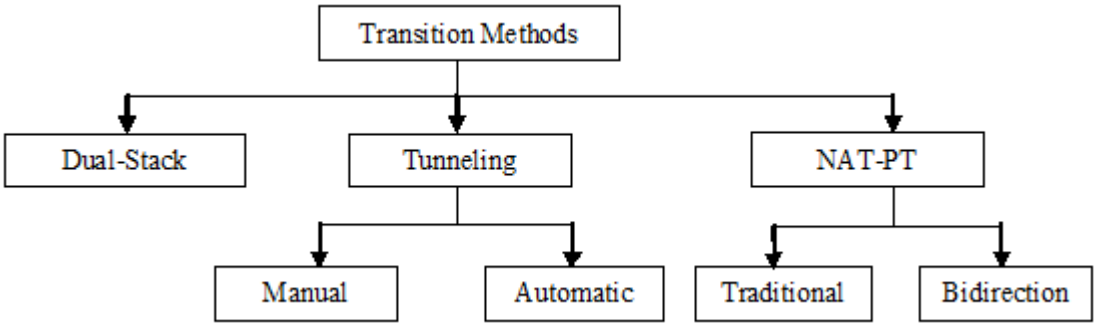

Figure 2: Types of Transition Methods

3.1.1. Dual-Stack Method

Dual Stack can process both IPv4 and IPv6 traffic simultaneously. The increase of devices day by day, it seems we are running out of IP address in IPv4 for each format which seems a big issue. IPv6 is the solution which is a new IP address format. The ISPs (Internet Service Provider) task is to provide net connections to their customers which are IPv4-to-IPv4 or IPv6-to-IPv6 but because of Dual Stack, every network is configured on both IPv4 and IPv6 and data can follow or both protocols simultaneously. Dual Stack equipped with both of the stacks, it can disable any of the stack when required either IPv4 or IPv6 and also can run both at same time [11].

Dual Stack is a simple transition method or solution that supports both internet protocols. Dual Stack devices like PC, a router or a server and other IoT (internet of things) can support both IPv4 and IPv6. This transition method is effective because IPv4 is not compatible sometimes on IPv6 devices and vice versa. Dual Stack includes both protocols working parallel which can be applied on both end system to establish connection and flow [12].

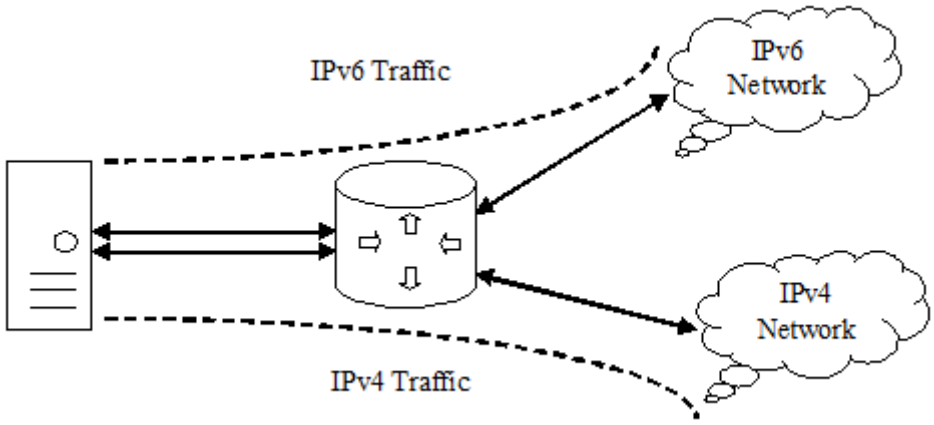

Figure 3: Dual Stack Router Connectivity

https://journals.researchparks.org/index.php/IJOT e-ISSN: 2615-8140 | p-ISSN: 2615-7071
Volume: 03 Issue: 7 |Jul 2021

In the above figure 3, a server having IPv4 as well as IPv6 address configured for it can now speak with all the hosts on both the IPv4 as well as the IPv6 networks with the help of a Dual Stack Router. The dual Stack Router can communicate with both the networks. It provides a medium for the hosts to access a server without changing their respective IP versions.

3.1.2. Tunneling Method

For minimizing the transitions, all the routers on the way between the two IPv6 nodes do need to support IPv6.This method of transition is called Tunneling. Primarily IPv6 packets are placed inside IPv4 packets then the packets are routed through the IPv4 routers.

Tunneling is another transition method that provides a way or a tunnel to use IPv4 infrastructure to carry traffic of IPv6. This method uses routing infrastructure of one internet protocol to carry internet protocol traffic via channel also called tunnelling. Tunneling can be used as Router-to-Router or Host-to-Router or Host-Host or Router-to-Host. Most of the internet traffic is carried from one router or host to another via tunnels to migrate from IPv4 to IPv6 as the different devices uses different versions. IPv4 which is a 32-bit address can support around 4.3 billion devices where as IPv6 uses 128-bit address and support much more devices i.e. 2 times to 128 power [12].

The Tunneling method is also divided into two types of methods one is Manual Tunneling and another one is Automatic Tunneling are listed below.

Manual Tunneling: Tunnels which uses peer to peer topology and need manual configuration called manual IPv6 tunnel.

Automatic Tunneling: Tunneling uses the embedded address information of IPv4 in IPv6 packet then this type of tunnelling known as Automatic Tunneling.

In a scenario where different IP versions exist on intermediate path or transit networks, tunneling provides a better solution where user's data can pass through a non-supported IP version.

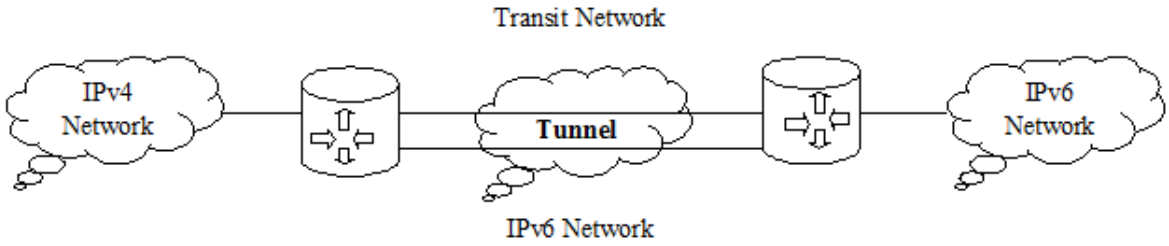

Figure 4: Tunneling Between Ipv6 over IPv4 Network

The above figure 4 depicts how remote IPv4 networks can communicate via a Tunnel, where the transit network was on IPv6.Vice versa is also possible where the transit network is on IPv6 and the remote sites that intend to communicate are on IPv4.

3.1.3. Network Address Translation-Protocol Translation (NAT-PT)

This is another important method of transition to IPv6 by means of a Network Address Translation-Protocol Translation (NAT-PT) enabled device. With the help of a NAT-PT device, actual can take happens between IPv4 and IPv6 packets and vice versa.

Network Address Translation (NAT) method facilitates communication between IPv4-only and IPv6-only network by translating two different IP address families. This method translates IPv6 from IPv4 and gives consistent Internet experience to the users by accessing contents over the Internet, which have Ipv4 services. NAT-PT is similar to the NAT system utilized in IPv4 that is frequently used for converting private (RFC 1918) IPv4 address to public IPv4 address and vice versa. It is used to convert IPv4 address to IPv6 address and vice versa. This method should be used only when there are no other techniques to allow IPv6-only devices to communicate with IPv4-only devices [13].

INTERNATIONAL JOURNAL ON ORANGE TECHNOLOGY
https://journals.researchparks.org/index.php/IJOT e-ISSN: 2615-8140 | p-ISSN: 2615-7071
Volume: 03 Issue: 7 |Jul 2021

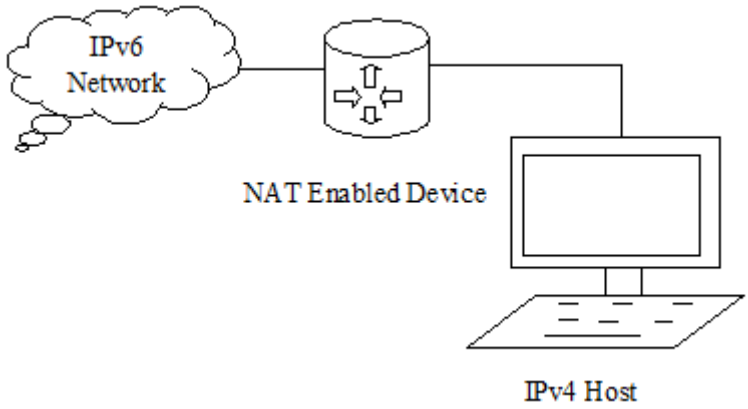

Figure 5: NAT-Protocol Translation Basic Operation

In the above figure 5, a host with IPv4 address sends a request to an IPv6 enabled server on Internet that does not understand IPv4 address. In this scenario, the NAT-PT device can help them communicate. When the IPv4 host sends a request packet to the IPv6 server, the NAT-PT device/router strips down the IPv4 packet, removes IPv4 header, and adds IPv6 header and passes it through the Internet. When a response from the IPv6 server comes for the IPv4 host, the router does vice versa.

In IPv6, there are two types of NAT-PT

Traditional: Traditional NAT-PT where sessions from IPv6 network are unidirectional. In this type, it allows hosts that are in IPv6 network to access the hosts that are in IPv4 network.

Bidirectional: In Bidirectional NAT-PT, sessions from both networks can be initiated i.e. from hosts in the IPv6 network as well as in the IPv4 network.

NAT-PT transition method main task is to migrate from IPv4 to IPv6 and also to provide connection bidirectional between IPv6 and IPv4.

4. Comparison between Transition Methods of IPv6 over IPv4:

All three transition methods are observed, compared and the effect of transition methods in IoT security. All transition methods are useful in some way and all of them has pros and cons according to the system.Comparision has been observed and studied that is presented below [14, 15].

Table1: Comparative Analysis of Three Transition Methods

Parameters/Transition Methods	Dual-Stack	Tunneling	NAT-PT
Latency	Medium	Low	High
Throughput	Moderate	Highest	Lowest
Packet Loss	High	Low	High
Traffic	High	Low	Medium
Packet Delivery	Fast	Fast	Slow
Delay	Minimum	Minimum	Maximum
Security	Higher	Lowest	Average
Connectivity	Bidirectional	Bidirectional	Bidirectional
Transition Approach	Simplest	Complex	More Complex
Flexibility	Greatest	Moderate	Lowest
Cost	Low	High	Medium
Advantages	Easy to implement. Already supported in all Operating System and Devices.	Simple Deployment. No Additional Management.	Solve Network Issues. The Router is used as a Translation Communicator.

https://journals.researchparks.org/index.php/IJOT e-ISSN: 2615-8140 | p-ISSN: 2615-7071
Volume: 03 Issue: 7 |Jul 2021

Drawbacks	Required additional Memory and CPU Power. Two Routing Tables.	Harder to troubleshooting and Network Management Vulnerable to security attacks	Complexity increases in IP addresses. Reduction in the overall value and utility of the network.
Limitations	Two firewalls sets of policies.	Have single points of failure.	Harder to control on a larger scale
Performance Analysis	Dual-Stack transition method shows better performance in the network compared to Tunneling in terms of Latency and Delay.	Better deliverables are produced in terms of Packet Delivery and Delay.	Rapid Deployment mechanism is convenient and easy to manage. However it has low flexibility.

5. Problems and Discussion:

It is most important that the transition from IPv4 to IPv6 is stable and Non-Interruptive to exiting services. The effect of IPv6 over IPv4 transition methods in IoT security includes the problems in the following majors' areas: Address Architecture, Connectivity, 3) High Availability, 4) Applications and 5) Network Management [16, 17].

1. **Address Architecture Problems:** IPv6 has much larger address space in comparison with IPv4. Due to the large IPv6 address space, special attention is needed when designing the IPv6 network since it differs from the fragmented and smaller IPv4 address design.
2. **Connectivity Problems:** While shifting the transition from IPv6 to IPv4 network to provide continuity of services to the users. The Dual-Stack is the natural approach but due to the depletion of IPv4 address, cost and up-gradation of the network to IPv6-only.
3. **High Availability**: High Availability is the major requirement for every service and network service. An application running on IPv6 may need to failover to IPv4 network due to network failure during transitioning.
4. **Applications Problems:** During the transition process, IPv4 and IPv6 applications will co-exist in the network. Regardless of what technology providers choose to use, services should be provided to the customers. Users should find out the best for the transition without affecting the services they provide.
5. **Network Management:** New technologies and methods may be introduced during the transition process. These new technologies and techniques require new operation models.

6. Conclusion:

In this paper, the three transition methods of the IPv4 to IPv6 transition have been discussed, deployed and compare. It has been found that these three methods have distinct advantages, drawback and features. The appropriate transition mechanism will be chosen for the network based on various parameters like the size of the network, the availability of the latest devices, the cost, and the security concern. If Latency, Throughput and Packet Loss are considered then Tunneling method is the best choice as compare to the Dual-Stack and NAT-PT. But the Tunneling method has vulnerable to security attacks, solved these security issues by IPSec (IP Security).So, our recommendation is to use Tunneling mode with IPSec for the transition purpose. The Dual-Stack remains more popular and practical with low cost in implementation and supported by wide range of devices. Transition Methods, like Tunneling and NAT-PT, are not optimally supported for the networks during a transition from IPv4 to IPv6.Thus; Dual-Stack seems the preferable method to begin adopting IPv6 with upgradable devices in order to securely manage the exiting IPv4 infrastructure. The deployment of IPv6 over IPv4 network is the best way for the growth of IoT's devices as well as also improvement in terms of their security.

7. References:

1. Farhan Anwar Ghumman, "Effects of IPv4/IPv6 Transition Methods in IoT (Internet of Things): A survey" SSRN-ID: 3402664, PP. 01-06, 19 June 2019.
2. Abubakar Isa and Idris Abdulmumine, "Design and Comparison Migration between IPv4 and IPv6 Transition Techniques", Proceedings of the

https://journals.researchparks.org/index.php/IJOT e-ISSN: 2615-8140 | p-ISSN: 2615-7071
Volume: 03 Issue: 7 |Jul 2021

3rd Yusuf Maitama Sule University, Kano, PP. 179-189, November 2017.

3. Steffen Hermann and Benjamin Fabian, "A Comparison of Internet Protocol (IPv6) Security Guidelines", Future Internet 2015, ISSN: 1999-5903, PP. 01-61, 24 May 2015.
4. C. V. Ravi Kumar et al, "Performance Analysis of IPv4 to IPv6 Transition Methods", Indian Journal of Science and Technology, ISSN: 0974-6846, Vol. 9, PP. 01-08, May 2016.
5. Aparna Sivaprakash and S. Kayalvizhi, "A Survey on Optimal IPv4 to IPv6 Transition Techniques" International Journal of Research Granthaalayah, ISSN: 2350-0530, Vol. 4, Issue 4; PP. 90-96 April 2016.
6. Iman Akour, "Between Transition from IPv4 and IPv6 Adaption: The Case of Jordanian Government", International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 7, No. 9, PP. 248-252, 2016.
7. Md. Asif Hossain et al, "Performance Analysis of Three Transition Mechanisms between IPv6 Network and IPv4 Network: Dual Stack, Tunneling and Translation", International Journal of Computer (IJC), ISSN: 2307-4523, Vol. 20, No. 1, PP. 217-228, 2015.
8. Daniel Enache et al, " A Study of the Technology Transition From IPv4 to IPv6 For An ISP", Review of the Air Force Academy, Vol. 1, PP. 117-121, 2016.
9. I Kullayamma et al, "Scenarios in Migration of Networks from IPv4 to IPv6", International Journal of Lates Trends in Engineering and Technology-ISSN: 2278-621XVol. 8, Issue 1, PP. 097-105, 2015.
10. Edwin S. Cordeiro, "Comparison between IPv4 to IPv6 Transition Techniques", arXiv, PP. 01-11, 1 Dec 2016.
11. Peng Wu et al, "Transition from IPv4 to IPv6 a State-of-the-Art Survey", In IEEE Communications Surveys and Tutorials, Accepted for Publication, 2015.
12. Pyung Soo Kim, "Analysis and Comparison of Tunneling based IPv6 Transition Mechanisms", International Journal of Applied Engineering Research, ISSN: 0973-4562, Vol. 12, No. 6, PP. 894-897, 2017.
13. Nellore Karthikeyan and K. Chandra Mouli, "Corporate Migration from IPv4 to IPv6 using Different Transition Mechanisms", International Journal of Engineering Science and Research Technology, ISSN: 2277-9655, Vol. 5, PP. 802-808 October 2016.
14. B. I. D. Kumar et al, "A Hybrid Transition for IPv4-IPv6 Co-existence in Small Size Organization" International Journal of Engineering and Advanced Technology(IJEAT), ISSN: 2249-8958, Vol. 9 Issue 2, PP. 3416-3421, Decenber 2019.
15. Fuiang Li et al, "A Case Study of IPv6 Network Performance: Packet Delay, Loss, and Reordering", Hindawi Mathematical Problems in Engineering, Article ID: 3056475, Vol. 2017 PP. 01-11, 2017.
16. Dr. Jitendranath Mungara et al, "Survey on IPv4 and IPv6 Using Dual Stack, Tunneling and Translation", International Journal of Advanced Research in Computer and Communication Engineering, ISSN: 2278-1021, vol. 7, Issue 2PP. 187-189, February 2018.
17. Julianne S. et al, "IPv4 to IPv6 Transition Strategies for Enterprise Networks in Developing Countries", Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, PP. 94-104, 2015