Performance Comparison of Internet Protocol v4 with Internet Protocol v6

Mrs. Sheetal Mali
Department of Electronics and Telecommunication
Parvatibai Genba Sopanrao Moze College of Engineering
Wagholi, Pune-412102, M.S India

Dr. D.B. Salunke
Department of Electronics and Telecommunication
Parvatibai Genba Sopanrao Moze College of Engineering
Wagholi, Pune-412102, M.S India

***Abstract*— this paper deals with the performance check of the Internet Protocol v4 and Internet Protocol v6 in terms of connectivity and Round Trip Time (RTT). This is done in a environment where migration of Internet Protocol v4 to Internet Protocol v6 is done using Dual-Stack technique for a small independent Local Area Network (LAN). Implementation of a dual stack network involves creation of a small testbed of private network which consists of Domain Name System (DNS) and Dynamic Host Control Protocol (DHCP) server, a web server, a physical machine having configured with a software router and a virtual client. All three computers are connected through a layer 2 physical switch forming a network. The performance of the network is analyzed using the PING connectivity and Round Trip Time (RTT) of IPv4/IPv6 networks.**

Keywords- IPv4, IPv6, dual-stack technique, Graphical Network Simulator (GNS3), (Round Trip Time) RTT

I. INTRODUCTION

Internet Protocol version 4 (IPv4) is being used on Internet all over the world today. As the size of the Internet and number of end devices such as PCs, routers, or switches etc, are increasing IPv4 address exhaustion is taking place, IPv4 network suffers more and more problems, such as the lack of address space etc. IPv6 is developed by the Internet Engineering Task Force (IETF) to deal with IPv4 address exhaustion. IANA's pool of IPv4 addresses has been exhausted in February 2011, and it is estimated that Regional Internet Registry's (RIR) pool would be depleted in 2011 [1]. So migration from IPv4 to IPv6 is a need of time.

There are three ways of migration namely, Dual stack, Translation and Tunneling. Dual-stack method supports the simultaneous existence of IPv4 and IPv6 resulting in reduction of network device up gradation cost, hence Dual-stack technique is the optimum solution. In tunneling technique tunnel encapsulate the IPv6 packets in IPv4 packets are carried out to the network parts that are not IPv6 enabled. Translation methods are basically used when an IPv4 only device wants to communicate with an IPv6 only device, or vice versa. As the IPv6 has large address size it is the best solution for today's Internet network. The IPv6 has larger address space because the IP address of 128 bits where as it is 32 bits in IPv4, hence transition mechanism from IPv4 to IPv6 is studied widely and this paper mainly focuses on dual stack mechanism.

II. IPv6 ADDRESSING SCHEMES

IPv6, 128 bit address is represented in eight groups of four hexadecimal digits. A typical IPv6 address uses first 64 bits to represent the network and last 64 bits to represent the interface identifier or host, example shows the network identifier of an IPv6 and also indicating /64 prefix bits.
Address: 2001:0db8:85a3:0042:1000:8a2e:0370:7334/64
Network portion: 2001:0db8:85a3:0042
Host portion: 1000:8a2e:0370:7334

Address prefixes are usually written in the form prefix::/length. Prefix defines the value of bits in the address beginning and length contains the number of important bits from the start. Because the rest of the prefix is not important, zeroes are used in this part of the address, and the "::" abbreviation is deployed. So for example prefix dedicated to the 6to4 transition mechanism is 2000::/16 [4]. The Classless Inter-Domain Routing (CIDR) prefix representation is used to represent the IPv6 address. An example of this notation is 2001:DB8:130F:: 870:0:140B/64. The /64 indicates that the first 64 bits are being used to represent the network and the last 64 bits are being used to represent the interface identifier. Three types of IPv6 addresses are defined in IPv6 address architecture: Unicast, Multicast and Anycast [5].

ISSN: 2278 – 7798

A. Unicast Address

A unicast address is defined as an identifier for a single interface. These addresses are typically used when a specific end system needs to communicate with another specific end system, IPv6 unicast addresses also have a scope defined for them: global, unique local and link local [6].

The link-local scope identifies all hosts within a single layer 2 domain. The unicast addresses used within this scope are called link-local addresses. Link local address is identified by the initial 10 bits which are set o 1111 1110 10 and next 54 bits set to 0, which are used by the nodes communicating with neighboring nodes on the same link. Prefix for link-local addresses is always set to FE80::/64.

The unique-local scope identifies all devices reachable within an administrative site or domain that typically contains multiple distinct links. The unicast addresses used within this scope are called unique-local addresses (ULAs). Unique local addresses are not allowed to be routable across the Internet. Unique link-local addresses are all from FC00::/7 address block.

The global scope identifies all devices reachable across the Internet. The unicast addresses used within this scope are called global unicast addresses (GUAs). Global unicast addresses are identified by high level three bits set to 001 (2000::/3).

B. Multicast Address

A multicast address is defined as an identifier for a set of interfaces that typically belong to different nodes. Multicast addresses are normally used to identify groups of interfaces that are interested in receiving similar content (e.g., video). Multicast addresses are all assigned out of the FF00::/8 block.

C. Anycast Address

An IPv6 anycast address is an address that is assigned to more than one interface (typically belonging to different nodes), with the property that a packet sent to an anycast address is routed to the nearest interface having that address. Anycast addresses must not be used as a sender address in the IP datagram [7].

III. TRANSITION MECHANISMS

A. Dual stack mechanism

Dual stack mechanism is one of the simplest methods of introducing IPv6 to a network and is also the best way for IPv4 to IPv6 to coexist in the same time before the complete transformation to IPv6 only network in the future. In dual stack, all hosts/routers maintained both protocol IPv4 and IPv6 stacks this becomes the advantage of a transition technique. Dual stack hosts/routers are able to communicate with not only IPv6 system but also IPv4 system. The dual stack hosts use IPv6 address while communicating with IPv6 host and use IPv4 address while communicating with IPv4 hosts [8], [9]. This technology requires all routers and access devices to be upgraded so that they can have both IPv4 and IPv6 protocol.

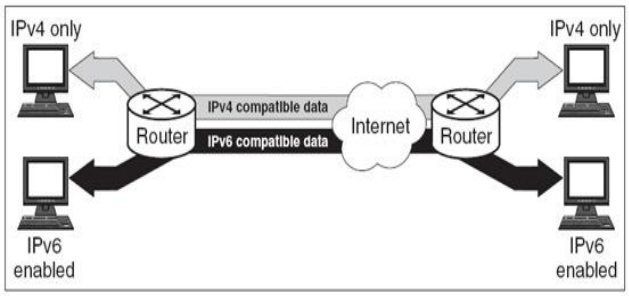

Fig. 1: Dual stack technique

B. Tunnel Mechanism

In the transition technique, IPv6 datagram is encapsulated into IPv4 by dual stack protocol routers while IPv6 datagram entering IPv4 network, and to make the IPv6 packet become part of IPv4 packet. There are generally three steps involved in the tunneling process such as encapsulation, decapsulation and tunnel management. The tunneling technique is used when the network is not at all or partly offering native IPv6 functionality [8], [10].

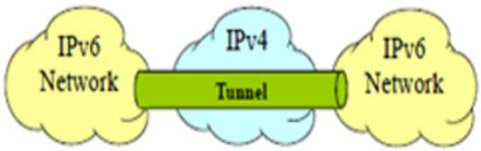

Fig. 2: Tunneling technique

C. Translation Mechanism

Translation methods are basically used when an IPv4 only device wants to communicate with an IPv6 only device or vice versa. IPv6 translation schemes implement some form of packet header translation between the IPv6 and IPv4 addresses. The goal is to translate packets with IPv6 addresses to those with IPv4 addresses, so that IPv6 only hosts can talk to the IPv4 only Internet [5], [8].

Fig. 3: Translation technique

ISSN: 2278 – 7798

IV. IMPLEMENTATION OF DUAL STACK TECHNIQUE

As in most of the organizations data centre and network devices are not compatible with IPv6, in such a case dual stack IPv6 implementation is the suitable mechanism. Incompatibility is because in organizations there are many old PCs and old version OS which do not support IPv6 and it is not feasible to change the hundreds of PCs and devices, hence the dual stack approach is chosen as it supports both IPv4 and IPv6.

V. SOFTWARE SIMULATION OF NETWORK

Packet Tracer version 6.0.1 is software used for testing the real scenarios before implementing actually in the network. We can create small logical network and can observe how to modify physical workplace by creating new objects, removing existing objects and moving from one location to another location in physical workplace. Various end devices used in the software are switches, routers, PCs, hub etc. Using the software a small network is simulated and tested for both IPv4 and IPv6 connectivity for the end devices used in the network. In the following network few PC's are connected to the software of the network and software is connected to the router of the same network, this complete forms the one separate network. This network is connected to the router of the Internet network which further is connected to the web server of the Internet network. Fig.4 indicates the logical network created on the simulation environment.

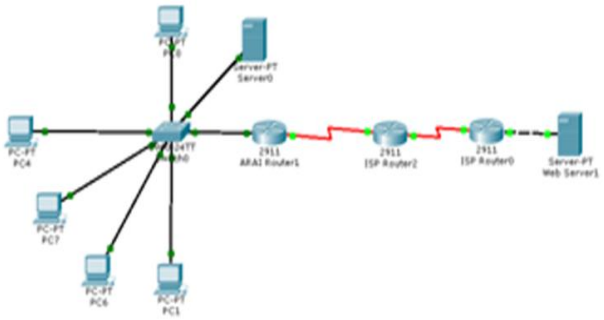

Fig.4: Network diagram

In Fig.5, PING command output window shows the connectivity between two PC's in the network. Connectivity between two PC's is checked using a command ping <IP address> or ping <Hostname>, and ping output is generated on command prompt window.

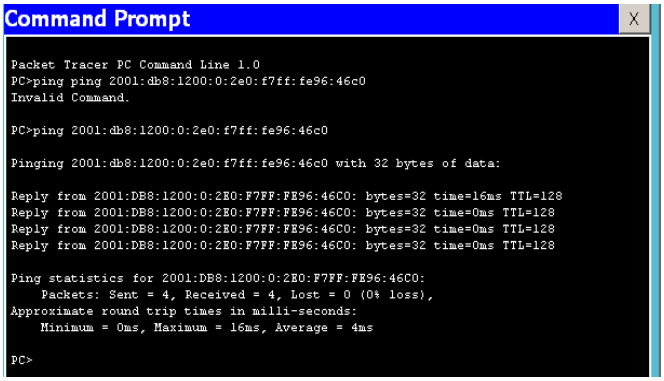

Fig. 5: ping command output

VI. ANALYSIS RESULTS OF SIMULATED NETWORK

In the test design network devices are IPv4/IPv6 enabled. Using Packet Tracer a scenario is created where end devices have IPv4 and IPv6 address both. When a IPv4 based URL request is sent through the browser, in the response IPv4 based web page is seen. But when IPv6 based URL request is sent, protocol not supported message is displayed.

Fig 6 shows the IPv4 based website accessed from the client machine

Fig. 6: web page for IPv4 based URL request

However in Fig.7 the IPv6 based output window the URL request response seen is protocol not supported because of unavailability of IPv6 based web page at the server.

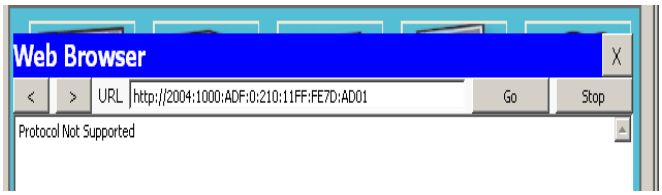

Fig. 7: IPv6 based web page

The simulation software Packet Tracer gives us the clear idea regarding dual stack based network and its connectivity for both IPv4/IPv6 address. From Fig. 6 and Fig. 7 it is clear that in Dual-stack transition platform IPv4 based websites can be accessed and web page is displayed, however, IPv6 based webpage also can be displayed unless the webpage is available at the server side.

ISSN: 2278 – 7798

VII. RESULTS AND ANALYSIS OF PHYSICAL IMPLEMENTATION OF IPv4/IPv6 NETWORK

Implementation of a dual stack network involves creation of a small test bed of private network which consists of DNS and DHCP server, a web server, a physical machine having configured with a software router and a virtual client. All three computers are connected through a layer 2 physical switch forming a network. The test bed is checked for Ipv4/Ipv6 connectivity and its performance in terms of Round Trip Time (RTT) and HTTP latency. HTTP response time is observed for both IPv4 and IPv6 HTTP request by increasing the number of users using software named J-meter. The fig. no.8 is a block diagram of physical test bed.

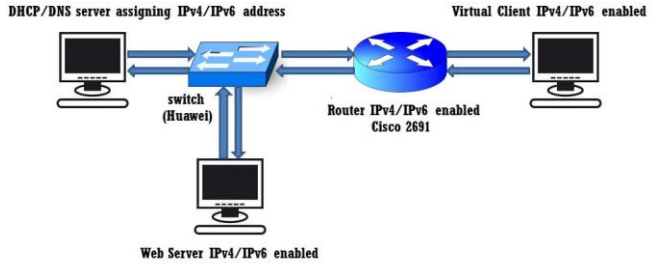

Fig. no.8 block diagram of Dual-stack network

A CONFIGURATION OF DNS/DHCP

A DNS/DHCP server is configured inside a physical machine using server OS named windows 2012 enterprise edition. While installing the OS, DNS and DHCP roles are selected. Dynamic Host Control Protocol (DHCP) dynamically assigns the IPv4 and IPv6 address to machines present in the network. DHCP provides both the IP protocol services to the clients in the network. Domain Name System (DNS) maintains the host entries of both A and AAAA type resource record in its database against each client. Thus DHCP assigns IPv4/IPv6 address dynamically to the Web server physical and client machine.

B CONFIGURATION OF WEB SERVER

A web server is created on one of the physical machine using windows server 2008 r2 and IIS role is installed on the web server, two static websites are published, one IPv4 address based and other IPv6 address based.

C CONFIGURATION OF ROUTER AND VIRTUAL CLIENT

A software router is configured on a physical machine using software named Graphical Network Simulator (GNS3). The image of the router selected is of Cisco 2691 having two ports. The router is both IPv4/IPv6 enabled hence two interfaces of the router are assigned with IPv4 and IPv6 address. One of the interface of the router is connected to client machine, which is installed on the same physical machine as a virtual client through on VM workstation having windows 2007 OS. And the interface of the router is connected to rest of the network through switch. The Fig. no.34 represents the logical topology of the network.

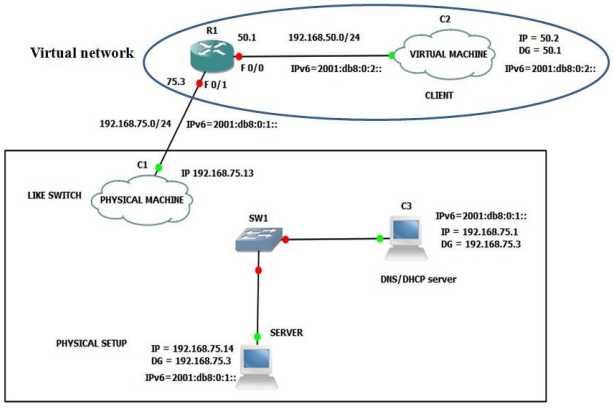

Fig. no.9 logical topology of Dual-stack network

The virtual network represents the physical machine having virtual router and a virtual client. The interface f0/0 of a router connected to a client is from 192.168.50.0/24 network and for IPv6 it is from 2001:db8:0:2::/64 network. And the other interface f0/1 of the router is on the different network of 192.168.75.0/24 for IPv4 and 2001:db8:0:1::/64 for IPv6, the IP addresses of these networks are assigned through DHCP. Fig. no. 10 shows the snapshot of physical topology.

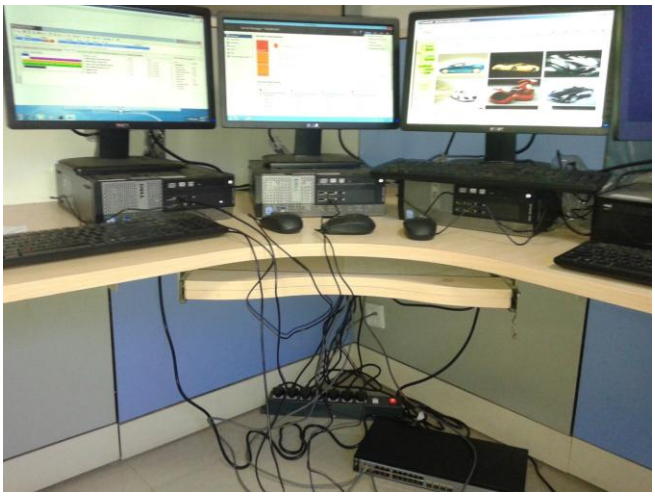

Fig. no.10 snapshot of physical network

D Round Trip Time (RTT) Latency for IPv4 and IPv6

The network in fig. no.11 is checked for client and web server connectivity, router and web server connectivity for both IPv4 and IPv6. The connectivity between two network devices is checked using PING command. The following result shows the PING connectivity between client and web server for the IPv4/IPv6 address.

ISSN: 2278 – 7798

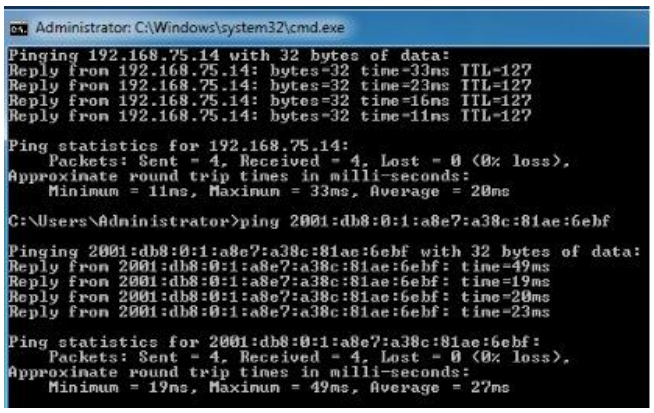

Fig. no.11 IPv4/IPv6 PING connectivity from client to web server

Now to check the IPv4/IPv6 performance in terms of RTT it is performed by varying the packet size in ascending order. The different packet sizes vary from 512 byte to 4026 byte. It observed that minimum RTT for 512 byte IPv4 packet is 12 ms and average RTT is 17 ms, for 1028 IPv4 packet minimum RTT is 14 ms and average RTT is 20 ms which is slightly greater than 512 byte packet. Similarly it is observed that minimum RTT for 2048 byte packet is 32ms and average RTT is 38 ms, for 4026 byte packet minimum RTT is 50 ms and average RTT is 57 ms, again it is greater than all other packet sizes. Similarly for IPv6 RTT is observed for various packet sizes and its RTT is compared to the IPv4 RTT. It is observed that minimum RTT and average RTT increases as size of the packet increases. The RTT for IPV6 is compared with IPv4 RTT. The table shows the RTT comparison between the two as the size of the IP packet is increased.

Table. No.1 comparison between IPv4 and IPv6 RTT for different packet sizes

Packet size	IPv4 Min. time	IPv4 Avg time	IPv6 Min. time	IPv6 Avg time
512 bytes	12 msec	17 msec	12 msec	19 msec
1024 bytes	14 msec	20msec	19 msec	27 msec
2048 bytes	31 msec	38 msec	34 msec	38 msec
4026 bytes	50 msec	57 msec	52 msec	56 msec

This table no.1 shows the RTT latency for IPv4 and IPv6 Packet for variable packet size. As seen there is not much difference between the two, for direct v4-v4 connection and v6-v6 connection this difference is hardly seen for networks consisting of less hops. But as the no of hops increases noticeable difference is seen, in IPv6 network comparative to IPv4 network RTT is greater than IPv4. But this contradicts the hop count value which is 1 here which is same for both In general, less hop counts results to lower RTT for a path. However, due to the fact that the number of IPv6 nodes and its concentration are lower and less dense compared to IPv4 nodes. The direct link connectivity of the IPv6 networks is less compared to IPv4 networks, so IPv6 packets need to travel a longer distance between successive hops compared to IPv4 packets, thus IPv6 paths become significantly longer compared to that of IPv4 paths. The longer propagation delay experienced by IPv6 packets translates to higher IPv6 RTTs compared to IPv4 RTTs leading to better performance than IPv4. The graph plotted corresponding to the above comparison table gives the clear idea of how performance of the IPv6 increases with the increase in the packet size.

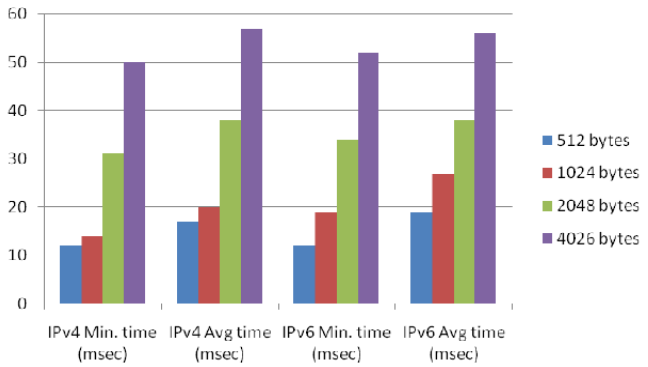

Fig. no.13 Graph for different packet sizes of IPv4 and IPv6

The graph plotted corresponding to the above comparison table gives the clear idea of how performance of the IPv6 increases with the increase in the packet size.

CONCLUSION

Among various transition techniques Dual-Stack is the most preferred one because in this a device or network has two protocol stacks enabled at the same time and operates in Dual stack mode separately. And also the simulation software Packet Tracer gives us the clear idea regarding dual stack based network and its connectivity for both IPv4/IPv6 address. Round Trip Time (RTT) is a parameter to indicate the Quality of Service (QoS) of a network. From the results it is observed that RTT for IPv6 packet is greater than IPv4 because as IPv6 header is 40 bytes and IPv4 header is 20 bytes and hence performance of IPv6 is better than IPv4.

REFERENCES

[1] Deering, S. and R. Hinden, "Internet Protocol, Version (IPv6) Specification", RFC 2460, December 1998.
[2] Hinden, R., Deering, S., and E. Nordmark, "IPv6 Global Unicast Address Format", RFC 3587, August 2003.
[3] Hinden, R. and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, April 2005.
[4] Johnson, D. and S. Deering, "Reserved IPv6 Subnet Anycast Addresses", RFC 2526, March 1999.
[5] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005.
[6] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.
[7] G. Van de Velde and C. Popoviciu, "IPv6 Unicast Address Assignment Considerations", RFC 5375, December 2008.

ISSN: 2278 – 7798

[8] S. Deering, Xerox PARC and R. Hinden," Internet Protocol, Version 6 (IPv6) Specification", RFC 1883, December 1995.
[9] APNIC, ARIN, RIPE NCC, "IPv6 Address Allocation and Assignment Policy", ripe- 421, November 2007, http://www.ripe.net/ripe/docs/ipv6policy.html
[10] Popoviciu Levy and Abegnoli Grossetete, "Deploying IPv6 Networks", Cisco System, Chapter no-2.
[11] "Internet Protocol," Jon Postel, RFC 791, 1981.

ISSN: 2278 – 7798