ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 6 June, 2013 Page No. 2006-2011

COMPARISON ANALYSIS OF VARIOUS TRANSITION MECHANISMS FROM IPV4 TO IPV6

Shivani Savita*, Monalisa

Department of computer science Suresh Gyan Vihar University, Jaipur
savitashivani@gmail.com

monalisa0575@gmail.com

ABSTRACT

IPV4 and IPV6 are incompatible protocol that means one device with IPV4 address cannot directly communicate with the IPV6 address. Many network devices are IPV4-only, they will not communicate in IPV6-only environment and few of those can or will upgrade to IPV6. The purpose of this study is to configure the network with address allocation, router configuration with OSPF routing protocol, implementation of Dual-stack, tunnels namely Manual Tunnel, GRE-IPv4 tunnel, ISATAP and 6to4 tunnel, it allows the communication between the IPv4 and IPv6 network hosts. The entire configuration is implemented using GNS3 simulator.

Keywords: IPv4/IPv6, Dual-stack, Tunneling, Translation, OSPF.

1. INTRODUCTION:

IPV4 is the most dominant internet protocol on the internet but the current exponential growth in internet users and their increasing requirement of IP addresses cannot be fulfilled because of the limited number of IP addresses offered by the IPV4 address space. The biggest motivation of IPV4 to IPV6 transition is that IANA, IANA is the internet organisation that allocates IPV4 and IPV6 addresses to everyone. The last batch of IPV4 addresses allocated on February 3, 2011 by IANA [1].

Internet engineering task force was warned in 1992 about the shortage of IPV4 addresses because of the drastic increase in the number of internet devices, some temporary solution were developed to overcome this problem, such as network address translation (NAT) [2], dynamic host configuration protocol (DHCP), class-less inter domain routing (CIDR) [3] etc. But even after these solutions increased demand of IP addresses required more number of IP addresses and then in 1992 Internet Engineering Task Force (IETF) developed the IPV6 protocol to solve the problem of address exhaustion with the IPV4, which is the next generation of network layer protocol [4]. The most obvious difference among IPV4 and IPV6 is its address size. IPV4 has 32 bit address length which means 2^{32} addresses that gives 4.2 billion IP addresses, and comparative to this IPV6 has 128 bit address length which means 2^{128} addresses that is 3.4* 10^{38} addresses, almost unlimited. Thus, the problem of IPV4 address exhaustion is solved by the IPV6 and it is the best available solution [8].

A seamless migration from IPV4 to IPV6 is hard to achieve; therefore a mechanism is required which ensures smooth, stepwise and independent change to IPV6, not only the transition, integration of IPV6 is required into the existing networks. The solutions (or mechanisms) can be categorised into three categories: dual stack, tunnelling and translation [5]. A number of

solutions from dual-stack, tunneling categories will be reviewed subsequently.

2. TRANSITION MECHANISMS

Different techniques will be needed to allow communication from IPv4 hosts to IPv6 hosts. Transferring traffic from IPv6 nodes to an IPv4 network is simple, IPv6 has sufficient addresses to refer to all IPv4 addresses and lots of addresses are still left for other uses. The other way, from IPv4 to IPv6, is not trivial and various solutions have been suggested. But here mentioned strategies are dual stack, 4 types of tunnelling strategies because only these strategies are supported by GNS3 hence included in this research.

2.1 Dual stack:

In dual stack, network nodes are equipped with IPV4 and IPV6 protocol stacks, one for IPV4 and one for IPV6 depending on the application or protocol they are using they just use one protocol stack with the other. Most of the operating systems support this [9]. This is the most widely used IPV4 to IPV6 transition mechanism because it does not require any tunnelling or translation.

Generally it is achievable to configure the dual stack to use only one of the protocols among IPV4 and IPV6 while disabling the other. Dual stack is capable of working with both the network nodes (workstations or servers) and the routers [6].

In a network, dual stack (IPV4/IPV6) has to be implemented in all the routers to work effectively. This solution can only work if these two addressing schemes are running in parallel because there is no communication between the IPv4 network nodes and the IPv6 network nodes; applications must be capable of supporting both modes. The dual stack mechanism is used frequently today, but requires that all network nodes must have an adequate amount of processing power and memory to maintain two different Internet Protocol stacks and dual management is also essential.

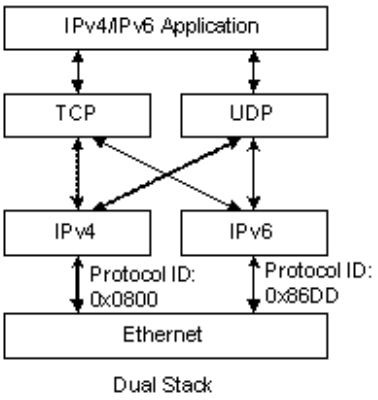

Figure 1: Dual stack

2.2 Tunneling:

The term tunneling means when one network protocol encapsulates another protocol. By using tunnels we can carry a packet over an incompatible destination network. Here as an IPv6 migration strategy the purpose of tunneling is to interconnect IPv6 network hosts via IPv4 backbone using IPv6 tunnels [7]. Overlay tunnels are the techniques that may be used to establish the connection between isolated IPv6 networks. Though, the use of tunneling strategies must not be considered as a concluding IPv6 network architecture, to a certain extent, it is a temporary solution until Dual stack and Native IPv6 can be completely implemented. Main reasons for using tunneling strategies lie into the below mentioned categories:

- Tunneling strategies provide an inexpensive means for connecting IPv6 networks. Only the endpoints i.e. border routers need to be upgraded to support both IPv4 and IPv6 protocols.
- Tunneling strategies allow communication establishment between IPv6 networks over a network that is IPv4 only or still not ready to deploy IPv6.

The IPv6 tunnel is shown in Figure 2. There are 4 types of tunnels supported by GNS3 which are discussed subsequently.

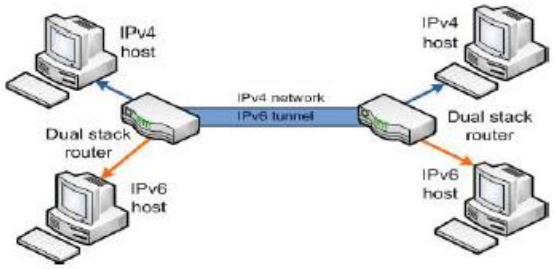

Figure 2: IPv6 tunnel

2.2.1 Manual tunnel:

It constructs a permanent virtual connection, connecting two IPv6 networks that are associated over an IPv4 backbone. Manual tunnel is a point-to-point static tunnel. The source and destination of the tunnel has IPv4 addresses and they are dual-stacked, and tunnel interface is configured with an IPv6 address. IPv6 packets travel over the IPv4 environment [10].

Because the manual tunnel needs to be manually configured, it is not scalable and has high maintenance if a network change is required. Therefore, the more tunnel endpoints required, the greater the management overhead

2.2.2 GRE tunnel:

GRE (Generic Routing Encapsulation) tunnel is a different type of Manual tunnel with tunnel source and tunnel destination both are configured for GRE manually shown in Figure 3. The source and destination of the tunnel has IPv4 addresses and they are dual-stacked, and tunnel interface is configured with an IPv6 address.

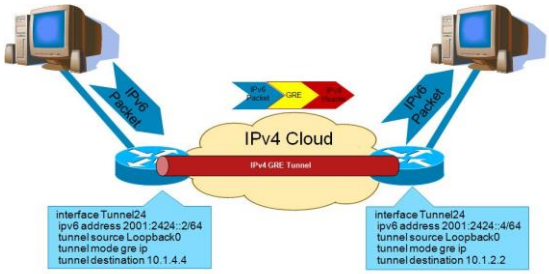

Figure 3: GRE-IPv4 tunnel

The GRE tunnel have an IPv6 packet embedded inside the GRE header and then inside the IPv4 header. GRE tunnel is also a point to point tunnel [10]. It has the same drawback of less scalability and greater management overhead as manual tunnel since it is also a type of manual tunnel.

2.2.3 ISATAP tunnel:

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) provides means of host-to-host, router-to-host and host-to-router automatic tunneling. ISATAP tunneling take place without the requirement of direct access to an IPv6 router on the site border, and it furthermore allows IPv6 nodes to access an IPv6 Internet network through a border router. It offers basic IPv6 unicast addressing connectivity between the IPv6 hosts across an IPv4 intranet hence the term Intra-site is used. ISATAP host don't require any manual configuration, it is automatic by the protocol stack to create ISATAP addresses using standard address configuration mechanisms. ISATAP tunnel is shown in Figure 4. By means of this approach, ISATAP gives a new way of IPv6 addressing format. With proper formatting, Dual-stack host's IPV4 address is implanted in the interface identifier segment of its IPV6 address. The prefix of an IPV6 address can be any prefix that is suitable according to the IPv6 addressing rule. Though, it is held in reserve for ISATAP use within the site. An instance of an ISATAP address encoding format is PF::0200:5EFE:IPv4.

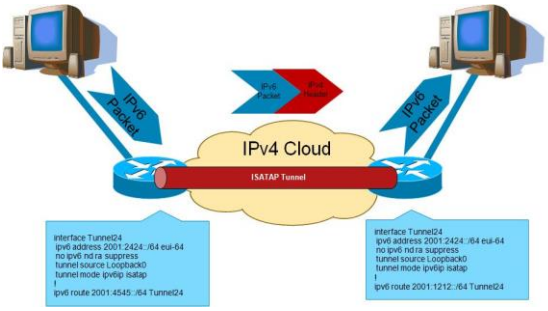

Figure 4: ISATAP tunnel

Host creates link local IPv6 addresses from configured IPv4 addresses. So as the graphic below depicts that IPv4 address is actually embedded making the 32 bits of the IPv6 address. So when IPv4 address is configured on the host it automatically derive IPv6 address from that. It uses next significant 32 bits with values 0000:5EFE and 64 bits for global/local unicast prefix.

64 bits	32 bits	32 bits
Global/Local unicast prefix	0000:5EFE	IPv4 address

2.2.4 6to4 tunnel:

6to4 Tunnel is a global IPv4 internet solution for automatic tunneling; it is a router-to-router tunneling strategy illustrated in Figure 5. It provides unicast IPv6 connectivity between IPv6 sites and hosts across the global IPv4 internet. The 6to4 mechanism uses a specific IPv6 address

format: the initial 16 bits of 128 bits in the IP address always starts with prefix hex "2002"[11]. After that 32 bits are IPV4 address of host followed by arbitrary subnet address. The last 64 bits are the host part of the address. Format to represent the IPv6 address is:

2002:<IPv4 address>:<subnet>::/64

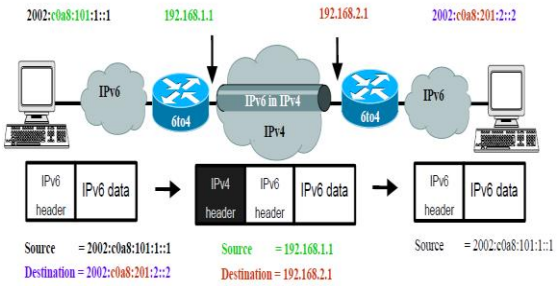

Figure 5: 6to4 Tunnel

To communicate between network nodes and networks using 6to4 mechanism relay routers are required. IPv4 and IPv6 network both must be connected to relay router. When a relay router receives a packet from an IPv4 host it removes the IPV6 address and forward the datagram to an IPv6 network at the same point of time when a relay router receives a datagram with initial 16 bits as '2002' from an IPv6 host the datagram is encapsulated and transferred to the IPv4 network. To communicate with a 6to4 network and an IPv6 network relay routers are needed. On the other hand a 6to4 border router (or just say 6to4 router) is required to connect to the 6to4 node. This design will lead to asymmetric routing with a relay router. The asymmetric routing results because of any cast method to place the adjacent relay [12].

3. PROPOSED WORK

In this research a network test-bed is implemented with 4 Cisco routers of 3640 series as IPv4 backbone and at each end an IPv6 host is connected for each IPv6 transition strategy using GNS3 network simulator. The network supports IPv6 addressing protocol, all the routers and network hosts were configured, routing protocol OSPF was implemented and the network is tested for each transition strategy so that IPv6 hosts in the test network can communicate via IPv4 network.

The network topology designed and simulated in GNS3 is illustrated in Figure 6 which is same for all transition strategies so that the parameters chosen for comparison should not vary because of the network design.

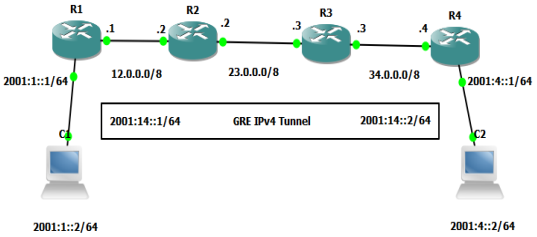

Figure 6: Designed network topology in GNS3

In Dual-stack network topology all the routers are configured with both IPv4 and IPv6 addresses. Where as in tunneling, tunnel is configured on the boarder routers as here router-to-router tunneling is chosen as experiment and it requires that tunnel end-points supports both IPv4 and IPv6 protocols; and middle routers are IPv4-only routers.

Finally as a result statistical analysis is carried out for comparison among the performance metrics of these strategies to estimate any statistically-significant variations among them. The main purpose of this study is to rank the abovementioned IPv6 transition strategies and categorize the better strategy that offers lowest delay, lowest jitter, and highest throughput.

4.RESULTS AND CONCLUSION

After successful configuration of all the networks, connectivity tests were performed between IPv6 hosts and it was observed that all the IPv4 and IPv6 devices are successfully communicating with each other.

Once connectivity test is done then statistical analysis is carried out for comparison among the performance metrics of these strategies to estimate any statistically-significant variations among them. Performance metrics included in this study are Round-trip-time, Jitter and throughput.

Different transition strategies or tunneling mechanisms adds to delays particularly in the connection establishment since there is more signalling performed before the actual connection can be opened for user data. The values of delay differ to a great extent between the transition

strategies depending on amount of signalling done.

Delay variation (Jitter) and Round Trip Time (RTT) is measured using the Ping program. Ping command forwards an ICMPv6 echo request message to the remote host and the remote host act in response to it with an ICMPv6 echo reply message. Time for sending the echo message and receiving the reply is measured to get the value of RTT. RTT value is measured in groups on 10 echo request and reply messages using ping program.

To measure the value of Jitter and RTT IPv4 and IPv6 packets are sent using Ping and tested one by one, both for ten times. Including both internet protocols there were 200 requests sent in total. During the measurement no packet loss or any other network faults are noticed, all packets are delivered successfully. After every pair of 10 echo request and reply messages ping program was ended and it provided a summary of the test. The summary consists of following information: minimum RTT, average RTT, and maximum RTT.

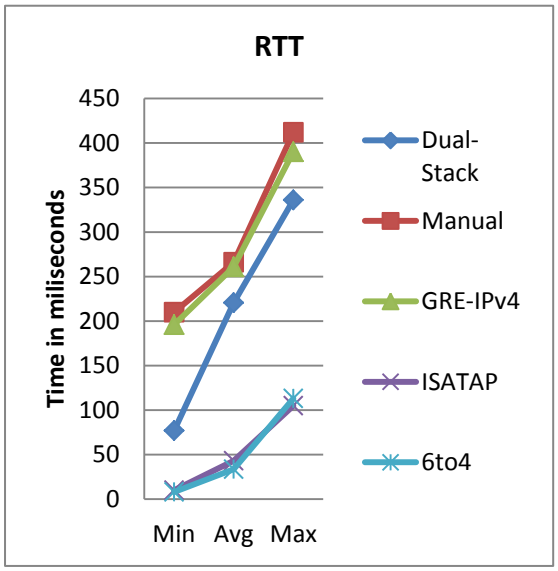

Figure 7: Round Trip Time results

Automatic tunnels 6to4 and ISATAP have the lowest values of RTT, so the applications which are delay sensitive must use automatic tunnels for IPv6 transition. RTT value of Dual stack is moderate and manual tunnels have the highest value of RTT.

Typically the size of Maximum Transmission Unit (MTU) is 1500 bytes used in Internet Protocols which is a maximum value set by the Ethernet protocol. The header of the higher layers takes the a number of bytes from these 1500 bytes, which means complete 1500 bytes of MTU cannot be real payload size holding the user data. The smallest value of the IPv4 and IPv6 header size is 20 bytes and 40 bytes respectively. TCP, UDP, ICMP or few other higher layer headers are going to get a number of bytes from the packet payload that user observes in addition to IP headers.

After assuming that network hosts are capable of handling few Ethernet packets of maximum size, it is feasible to calculate a theoretical throughput value of the network using equation:

Throughput = MTU size / RTT X 10^{-6}

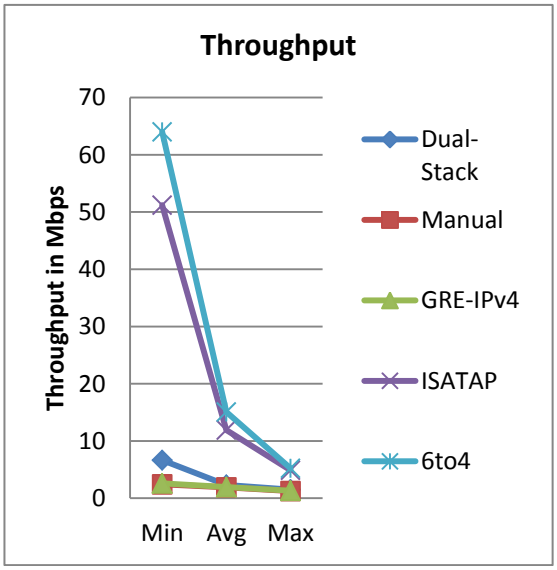

Figure 8: Throughput results

6to4 tunnel has the highest value of throughput, then ISATAP tunnel and after that dual-stack and manually configured tunnels i.e. Manual and GRE tunnel. So the throughput sensitive application must use the automatic tunnels.

Delay variation i.e. jitter is shown in figure 9.

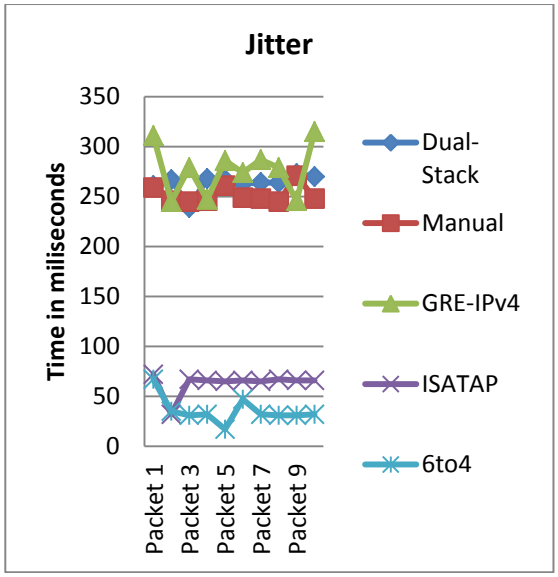

Figure 9: Jitter results

Minimum value of jitter is for automatic tunnels so applications which are jitter sensitive must use automatic tunnels.

Dual stack is easy to implement but network devices must support both the protocols (IPv4/IPv6) and it can only be used to send packets between IPv4 networks or IPv6 networks, an IPv4 device cannot communicate to the IPv6 device and vice versa. Because of the inclusion of both protocols in dual stack devices, the size of the routing table increased considerably resulting in longer processing time and delays of the packet. In contrast, tunneling transition strategy is a better choice in case of the devices which do not support IPv6 protocol. The drawback of tunneling is that packet size increases 20 bytes in the header field of each IPv4 packet resulting in complicated troubleshooting.

5. FUTURE WORK:

This research included only a number of transition strategies whereas there are various other transition strategies such as Teredo, 6RD, tunnel broker and translation techniques. This can also be included as the next step in this research.

The performed test was made in GNS3 which can be made in a real laboratory environment to test and verify the network topologies in physical way for testing of the routing protocols and transition mechanisms.

6. REFRENCES:

[1] L. Beijnum, (2011). "River of IPv4 Address Officially Runs Dry," Arstechnica, http://arstechnica.com/tech-policy/2011/02/river-of-ipv4-addresses-officially-runsdry/

[2] P. Srisuresh, M. Holdrege (August 1999), "IP Network Address Translator (NAT) Terminology and Considerations," Request for Comments 2663, Internet Engineering Task Force.

[3] A. S. Tanenbaum, Computer Networks, Third Edition, Prentice Hall Inc., 1996, pp. 686, 413-436, 437-449

[4] S. Bradner and A. Mankin (1995), "The recommendation for the IP next generation protocol" (Internet RFC 1752).

[5] S. Hagen (July 2006), "IPv6 Essentials", O'Reilly.

[6] E. Nordmark and R. Gilligan. (2005). "Basic Transition Mechanisms for IPv6 Hosts and Routers". RFC 4213.

[7] B and K. Moore. (2001). "Connection of IPv6 Domains via IPv4 Clouds". RFC . Carpenter 3056.

[8] An IEEE-USA White Paper, (2009). "Next Generation Internet: IPv4 Address Exhaustion, Mitigation Strategies and Implications for the U.S".

[9] E. Park, J. Lee AND b. Choe (June 2004), "An IPv4-to-IPv6 dual stack transition mechanism supporting transparent connections between IPv6 hosts and IPv4 hosts in integrated IPv6/IPv4 network", Proceeding of the IEEE International Conference on communications, vol. 2, pp. 1024-1027.

[10] Parisa Grayeli (Jan 2013), "Performance modelling and analysis of IPv6 Transition Mechanisms over MPLs".

[11] C. Huitema. (2001). "An Anycast Prefix for 6to4 Relay Routers". RFC 3068.

[12] B and K. Moore. (2001). "Connection of IPv6 Domains via IPv4 Clouds". RFC Carpenter 3056.