On the Migration of a Large Scale Network from IPv4 to IPv6 Environment

Muhammad Yeasir Arafat[1], Feroz Ahmed[2] and M Abdus Sobhan[3]

Department of Electrical and Electronic Engineering, School of Engineering and Computer Science, Independent University, Bangladesh

ABSTRACT

This work mainly addresses the design a large scale network using dual stack mechanisms. We focused on the most important theoretical concepts of the IPv6 protocol, such as addressing, address allocation, routing with the OSPF and BGP protocols and routing protocols performance in dual stack network using GNS3 and Wireshark simulators. we have a tendency to measure a perfect model and a true large-scale network atmosphere victimization out there end-to-end activity techniques that focuses on a large-scale IPv4 and IPv6 backbone and created performance the IPv4 and IPv6 network. In this paper, we compiled IPv6 address planning in large scale network, performance statistics of each network in terms of TCP throughput, delay jitters, packet loss rate, and round trip time. It is found that, a minor degradation within the throughput of the TCP, delay jitter, a lower packet loss rate, and a rather longer round trip time are occurred in a real large scale dual stack network.

KEYWORDS

IPv6, IPv4, double stack, BGPv4, OSPFv3, ISP, throughput, TCP and RTT

1. INTRODUCTION

Presently, the Internet consists of native IPv4 (IPv4-only), native IPv6, and IPv4/IPv6 dual networks. Unfortunately, IPv4 and IPv6 are incompatible protocols. If both IP versions are accessible and the users of Internet wish to affix afterwards any restrictions, a transition mechanism is required. During the period of migration from IPv4 to IPv6 networks, a number of transition mechanisms accept been proposed by IETF to make sure smooth, stepwise and independent changeover. IPv6 [1] is developed as a network layer protocol, overcoming the problems in IPv4. Its 128-bit address format significantly enlarges the address space and will satisfy the address demands for a reasonably durable. However, IPv6 has no congenital backwards affinity with IPv4, which suggests IPv6 networks cannot acquaint with IPv4 in nature. Essentially IPv6 has created a parallel, independent network that coexists with its counterpart IPv4. IPv6-capable applications and IPv6-accessible capacity are still the minority [2]; the majority of arrangement resources, casework and applications still abide in IPv4.We have a number of transition techniques to maintain the connectivity of both IPv4 and IPv6, to achieve inter connection between IPv4 and IPv6, and to support the adoption process of IPv6. Vendors apprehend to advance on implementing well-developed alteration techniques, so that their articles can accept acceptable adequacy and accompany top profits. As for Internet Service Providers (ISP), they charge to acquisition a way to accommodate the absolute casework for both IPv4 and IPv6 users, and alike their casework with an accountable deployment of transition techniques on the Internet. This paper introduces dual stack network mechanisms is the easy, cost effective solution for ISP to build up IPv4 and IPv6 backbone network.

DOI : 10.5121/ijcnc.2014.6210

2. TRANSITION METHOD

Since there is such a huge difference between IPv4 and IPv6, they cannot communicate directly with one another. A system that is capable of handling IPv6 traffic will be created backward compatible, but an already deployed arrangement that handles alone IPv4 is not able to handle IPv6 datagram. This means that that a significant upgrade method would want to require place, involving hundreds of millions of machines, in adjustment to accomplish a complete translation to IPv6. This method is too costly and time consuming and in any case will not happen immediately. The network world can possibly see a gradual transition to IPv6, wherever IPv6 are going to be integrated into the IPv4 world that exists these days. There are altered kinds of technologies which might be applied such as dual stack, tunnelling, and translation. Over many transition techniques are used and tested for the communications between completely different networks to make sure IPv4 and IPv6 ability. Therefore, to accomplish accommodation on the best ill-fitted alteration methods, it is absolutely important to accept an overview of the accepted IPv4 networks. In addition, enterprises should analyze required functionalities, scalability, and securities in the corporation [3].

2.1. Dual Stack

The Dual Stack Technique is additionally known as native dual stack or Dual IP layer. Both protocols IPv4 and IPv6 run parallel on an equivalent network infrastructure don't need encapsulation of IPv6 inside IPv4 and vice versa. A universal dual-stack migration approach as shown in figure 1 makes a transition from the core to the edge. This contains allow two TCP/IP protocol stacks on the Wide area Network (WAN) core routers. In a very common dual stack network migration first of all the perimeter routers, and firewalls, then the server-farm switches and eventually the desktop access routers. Once the network supports IPv6 and IPv4 protocols, the method can change dual protocol stacks on the servers and then the edge entities. The dual stack method is literally to use two IPv4 and IPv6 stacks for operating simultaneously, which enables devices to run on either protocol, according to available services, network availability, and administrative policies. This can be accomplished in both end systems and arrangement accessories [3]. As an end result, IPv4 enabled programs use IPv4 stack and this goes the equivalent for IPv6.

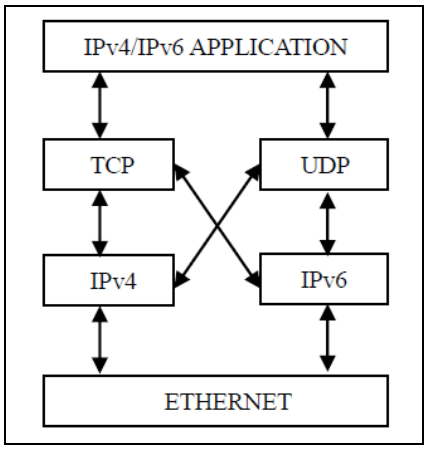

Figure 1: Dual Stack Mechanism [2]

The IP header adaptation field would play an important role in accepting and sending packets. In short words, this type of IPv6 transition is the encapsulation of IPv6 within IPv4. The complete transition will be managed by DNS.

2.2. Tunnelling

Tunnelling, from the perspective of transitioning, enables incompatible networks to be bridged, and is usually applied in a point-to-point or sequential manner. Three mechanisms of tunnelling are presented: IPv6 over IPv4, IPv6 to IPv4 automatic tunnelling, and Tunnel Broker [4].Tunnelling IPv6 traffic over an IPv4 network is another possibility. This approach permits the IPv6 traffic to be encapsulated in an IPv4 packet and forwarded, creating an IPv6 tunnel over the IPv4 infrastructure. A tunnel may be created as a solution for transporting IPv6 traffic, from IPv6 node to the destination IPv6 node, over the IPv4-only network. A "virtual link" is formed and, from the outlook of the two establishing IPv6 nodes, this appears as a point-to-point link. The various forms of tunnelling techniques can be considered into two types: manually configured and automatic tunnelling. A point-to-point link must be manually organized, because the name suggests. For automatic tunnelling, an IPv6 node will dynamically tunnel packets by using a 6 to 4 address. This is used to transfer data between well-suited networking nodes over unsuited networks. There are two regular scenarios to apply tunnelling: the allowance of end systems to apply off link transition devices in a distributed network and the act of enabling edge devices in networks to inter-connect over incompatible networks. The current infrastructure is what the developers of applications adapt to since ISPs have not deployed IPv6. Fortunately, 6to4 is a technique that meets (most of) the IPv6 user's requirements, while meeting the ISP's requirements in terms of costs and administration.

2.3. Translations

The meaning of translation is to convert directly protocols from IPv4 to IPv6 or vice versa, which might result in transforming those two protocol headers and payload. This mechanism can be established at layers in protocol stack, consisting of network, transport, and application layers. The translation method has many mechanisms, which can be either stateless or stateful. While stateless means that the translator can perform every conversion separately with no reference to previous packets, stateful is the vice versa, which maintains some form of state in regard to previous packets. The translation process can be conducted in either end systems or network devices. The fundamental part of translation mechanism in transition process is the conversion of IP and ICMP packets. All translation methods, which are used to establish communication between IPv6-only and IPv4-only hosts, for instance, NAT-PT or BIS, apply an algorithm known as Stateless IP/ICMP Translator (SIIT) [5].

3. DESIGN A LARGE SCALE NETWORK IN DUAL STACK

In this paper, a large scale network design by dual stack network. We have design a dual stack network for a National Wide ISP. Design considerations are given below.

3.1. Topology Design

In this paper our designed ISP has 4 main operating area or region. Each region has 2 small POP. Each region will have one data centre to host content. Regional network are inter-connected with multiple link.

3.1.1. Regional Network

Each regional network will have Point of Present (POP). In every POP there will be three routers. There are one core and two edge routers per. Every POP have a router to terminate customer network i.e. Edge Router. POP will be used for an aggregation point of ISP customer.

3.1.2. Design Consideration

Each regional network should have address summarization capability for customer block and CS link WAN. To increase the network in future, prefix planning should have scalability option for next couple of years for both customer block and infrastructure. No Summarization require for infrastructure WAN and loopback address. All WAN links should be ICMP reachable for link monitoring purpose (At least from designated host). Conservation can get high preference for IPv4 address coming up with and aggregation can get high preference for IPv6 address planning. OSPF is running in ISP network to hold infrastructure IP prefix. Each region is a separate OSPF area. Transport core is in OSPF area 0. Customer will connect on either static or eBGP (Not OSPF). iBGP will carry external prefix within ISP core IP network**.**

3.1.3. IPv6 address plan consideration

Big IPv6 address space will cause terribly massive routing table size. Most transit service provider apply IPv6 aggregation prefix filter (i.e. anything other than /48 & <=/32 prefix size. Prefix advertisement charge to forward to Internet should be either /32 or /48 bit boundary IPv6 address plan consideration (RFC3177). WAN link can be used on a /64 bit network block. End user/Customer sub allocation can be made between /48~/64 bit boundary. APNIC Utilization/HD ratio will be calculated based on /56 end site assignment/sub-allocation

3.1.4. Addressing Plans – ISP Infrastructure

- Point-to-Point links: Protocol design prospect is that a /64 bit network block is used (where a /127 network block now recommended/standardized (rfc6164)). (Reserve /64 block network for the link, but address it as a /127)
- Other options: A /126s are being used (mirrors IPv4 /30). A /112s are being used. For node ID we have leaves free final 16 bits. There are some discussion about /80s, /96s and /120s.
- ISPs should receive /32 from their RIR: Address block for router loop-back interfaces generally a number all loopbacks out of one /48. We used a network block which allocated /128 IP address per loopback. The address block for infrastructure /48 network permits 65k subnets. A /48 network address per region, this is for the largest international networks. A /48 network address for whole backbone. Customers get one /48 network block. Unless customers have more than 65k subnets in which case they get a second /48 network address. In typical deployments today several ISPs give small customers a /56 network block or single LAN end-sites a /64 network block address, e.g.: /64 if end-site will only ever be a LAN. A /56 network address for medium end-sites (e.g. small business) and a /48 for large end-sites. Registries can typically assign ensuing the next block to be contiguous with the first allocation, where minimum allocation is /32. Terribly possible that subsequent allocation will make this up to a /31
- IPv6 Allocation Form registry is: 2406:6400::/32
- IPv4 Allocation From registry is: 172.16.0.0/19

3.2. Address plan for IPv6

For the address planning we followed RFC 3849, which is IPv6 address prefix reserved for documentation [6]. Details IP address plan for IPv6 is given below (Table 1 to 6):

Table 1. Top Label Distribution Infrastructure and Customer

Block	Prefix	Description
1	2406:6400::/32	Parent Block
2	2406:6400:0000:0000::/36	Infrastructure
	2406:6400:1000:0000::/36	
	2406:6400:2000:0000::/36	
	2406:6400:3000:0000::/36	
	2406:6400:4000:0000::/36	
	2406:6400:5000:0000::/36	
	2406:6400:6000:0000::/36	
	2406:6400:7000:0000::/36	
3	2406:6400:8000:0000::/36	Customer network Region 1
	2406:6400:9000:0000::/36	
4	2406:6400:a000:0000::/36	Customer network Region 2
	2406:6400:b000:0000::/36	
5	2406:6400:c000:0000::/36	Customer network Region 3
	2406:6400:d000:0000::/36	
6	2406:6400:e000:0000::/36	Customer network Region 4
	2406:6400:f000:0000::/36	

Table 2. Loopback address

Block	Prefix	Description
20	2406:6400:0000:0000::/48	Loopback
43	2406:6400:0000:0000::1/128	R1 loopback 0
44	2406:6400:0000:0000::2/128	R2 loopback 0
45	2406:6400:0000:0000::3/128	R3 loopback 0
46	2406:6400:0000:0000::4/128	R4 loopback 0
47	2406:6400:0000:0000::5/128	R5 loopback 0
48	2406:6400:0000:0000::6/128	R6 loopback 0
49	2406:6400:0000:0000::7/128	R7 loopback 0
50	2406:6400:0000:0000::8/128	R8 loopback 0
51	2406:6400:0000:0000::9/128	R9 loopback 0
52	2406:6400:0000:0000::10/128	R10 loopback 0
53	2406:6400:0000:0000::11/128	R11 loopback 0
54	2406:6400:0000:0000::12/128	R12 loopback 0

Table 3. Summarization customer block Region 1

Block	Prefix	Description
	2406:6400:8000:0000::/35	Customer block region 1 [R2]
	2406:6400:8000:0000::/37	Customer block POP1 [R1]
	2406:6400:8800:0000::/37	Customer block future use/POP

	2406:6400:9000:0000::/37	Customer block future use/POP
	2406:6400:9800:0000::/37	Customer block POP2 [R3]

Table 4. Summarization customer block Region 2

Block	Prefix	Description
	2406:6400:A000:0000::/35	Customer block region 2 [R5]
	2406:6400:A000:0000::/37	Customer block POP1 [R4]
	2406:6400:A800:0000::/37	Customer block future use/POP
	2406:6400:B000:0000::/37	Customer block future use/POP
	2406:6400:B800:0000::/37	Customer block POP2 [R6]

Table 5. Summarization customer block Region 3

Block	Prefix	Description
	2406:6400:c000:0000::/35	Customer block region 3 [R8]
	2406:6400:C000:0000::/37	Customer block POP1 [R7]
	2406:6400:C800:0000::/37	Customer block future use/POP
	2406:6400:C000:0000::/37	Customer block future use/POP
	2406:6400:C800:0000::/37	Customer block POP2 [R9]

Table 6. Summarization customer block Region 4

Block	Prefix	Description
	2406:6400:e000:0000::/35	Customer block region 4 [R11]
	2406:6400:E000:0000::/37	Customer block POP1 [R10]
	2406:6400:E800:0000::/37	Customer block future use/POP
	2406:6400:E000:0000::/37	Customer block future use/POP
	2406:6400:E800:0000::/37	Customer block POP2 [R12]

3.3. Address plan for IPv4

IP address Plan for IPv4 is given below (Table 7 to 9):

Table 7. Parent Block IPv4

Block	Prefix	Size	Description
1	172.16.0.0	/19	Parent Block
2	172.16.0.0	/20	Infrastructure
3	172.16.16.0	/20	Customer Network

Table 8. Details infrastructure WAN block IPv4

Block	Prefix	Size	Description
12	172.16.10.0	/24	WAN Prefix
13	172.16.10.0	/30	Router 2-1 WAN
14	172.16.10.4	/30	Router 2-3 WAN
15	172.16.10.8	/30	Router 1-3 WAN
16	172.16.10.24	/30	Router 5-4 WAN
17	172.16.10.28	/30	Router 5-6 WAN

18	172.16.10.32	/30	Router 4-6 WAN
19	172.16.10.48	/30	Router 8-7 WAN
20	172.16.10.52	/30	Router 8-9 WAN
21	172.16.10.56	/30	Router 7-9 WAN
22	172.16.10.72	/30	Router 11-10 WAN
23	172.16.10.76	/30	Router 11-12 WAN
24	172.16.10.80	/30	Router 10-12 WAN

Table 9. Details customer IPv4 block

Block	**Prefix**	**Size**	**Description**
28	172.16.6.0	/20	Customer network
29	172.16.16.0	/22	Router 2 summary net
30	172.16.16.0	/23	Router 1 CS network
31	172.16.18.0	/23	Router 3 CS network
32	172.16.20.0	/22	Router 5 summary net
33	172.16.20.0	/23	Router 4 CS network
34	172.16.22.0	/23	Router 6 CS network
35	172.16.24.0	/22	Router 8 summary net
36	172.16.24.0	/23	Router 7 CS network
37	172.16.26.0	/23	Router 9 CS network
38	172.16.28.0	/22	Router 11 summary net
39	172.16.28.0	/23	Router 10 CS network
40	172.16.30.0	/23	Router 12 CS network

4. SIMULATIONS AND ANALYSIS

Simulations are performed using GNS3. For the simulation we used Cisco 7200 series router. In the test bed dual stack network, an ISP has 4 main operating area or region. Each region has 2 small POP. Each and Every POP will use a router to terminate client's network. GNS 3 topology is given in figure 2.

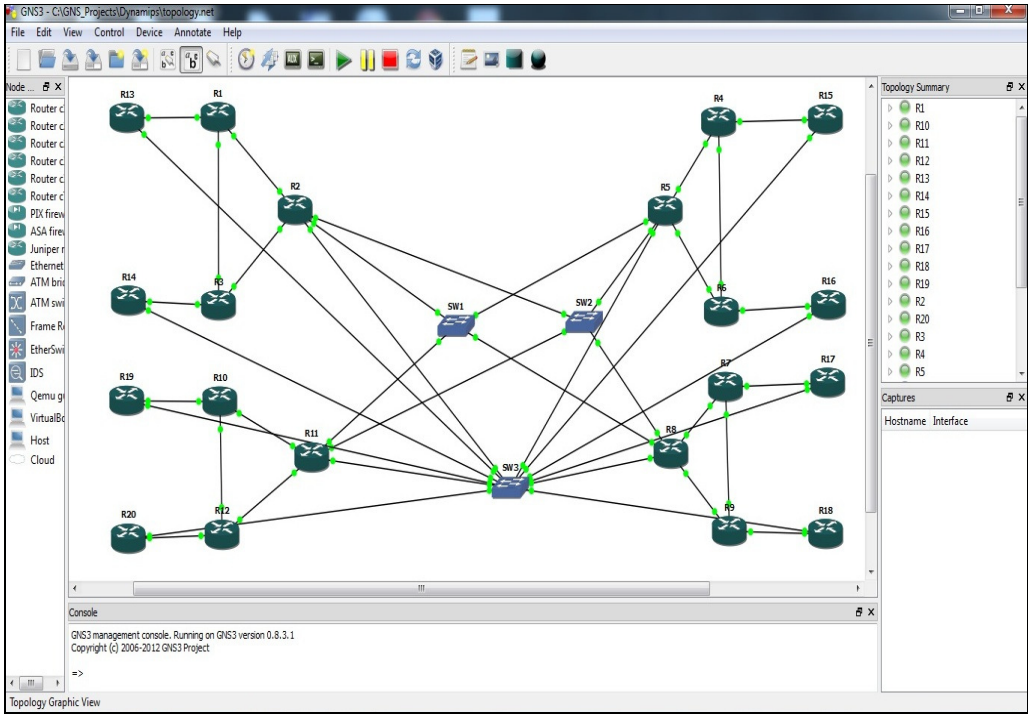

Figure 2: Simulation Network in GNS 3

4.1. Network Connection Pattern

Before enabling OSPF3 on an Interface, the following steps must be done on a Router. Enable IPv6 unicast routing and Enable IPv6 CEF. In region 1 router R1, R2, R3 have iBGP peering with other networks figure 3.

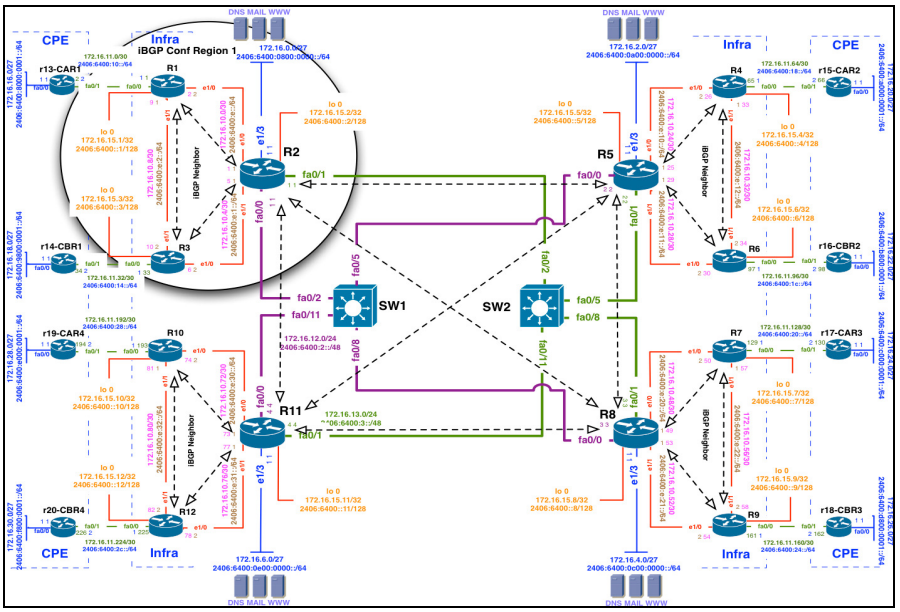

Figure 3: iBGP peering For Region 1

In the same way R5, R4, R6 have iBGP peering with others in Region 2. R8, R7, R9 have iBGP peering with others in Region 3. R11, R10, R12 have iBGP peering with others in Region 4.

4.2. Simulation Output and Analysis

For analysis routing protocols we used Wireshark. Packets are captured from the routers interface. We have discussed some measurement from the topology with necessary figures.

4.2.1. OSPFv3 packet Analysis

Open Shortest Path First (OSPF) is a commonly used intra domain routing protocol based on Dijkstra's least-cost path algorithm for calculating the best paths to subnets. When routing information changes, or upon initialization, the router generates a link-state advertisement representing all link-states of the router. The Hello packet has no address information at all. It includes an Interface ID that the originating router has assigned to uniquely identify its interface to the link. This Interface ID will be used as the network-LSA's Link State ID if the router becomes the Designated Router on the link. The neighbour organizations perform the same function in both IPv6 and IPv4. Explicitly, it collects all information required to form an adjacency between two routers when such an adjacency becomes necessary. Each neighbour structure is bound to a single OSPF interface.

The Interface ID that the neighbour advertises in its Hello packets must be recorded in the neighbour structure. The router will include the neighbour's Interface ID in the router's router-LSA when either a) advertising a point-to-point or point-to-multipoint link to the neighbour or b) advertising a link to a network where the neighbour has become the Designated Router. *In* IPv6 OSPF sprints directly over IPv6's network layer. When, it is encapsulated in one or more IPv6 headers with the Next Header field of the immediately encapsulating IPv6 header set to the value 89 [7]. In figure 4 we have shown OSPF v3 hello packet which source OSPF route from 172.16.10.53. This designated route from 172.16.10.54 and destination IP 224.0.0.5. In figure we also see the backup designated router to 172.16.10.53 and active neighbour 172.16.15.9.

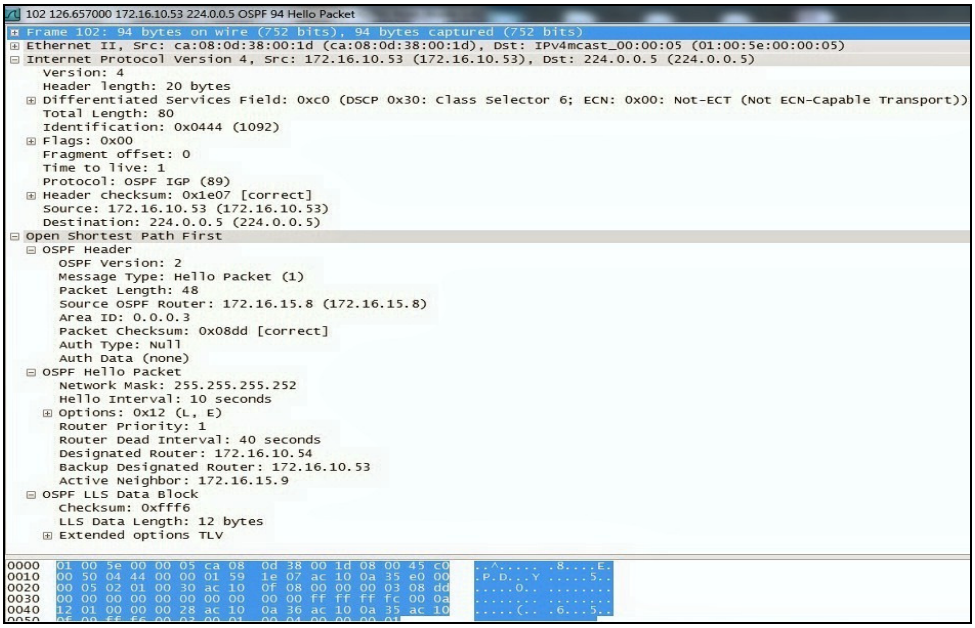

Figure 4: OSPF Packet Analysis

4.2.2. BGP Packet Analysis

BGP is the path-vector protocol that is work on exchanging external AS routing information and operates level of address blocks or AS prefixes [8]. BGP routers exchange routing information using open, update, notification and keepalive message.

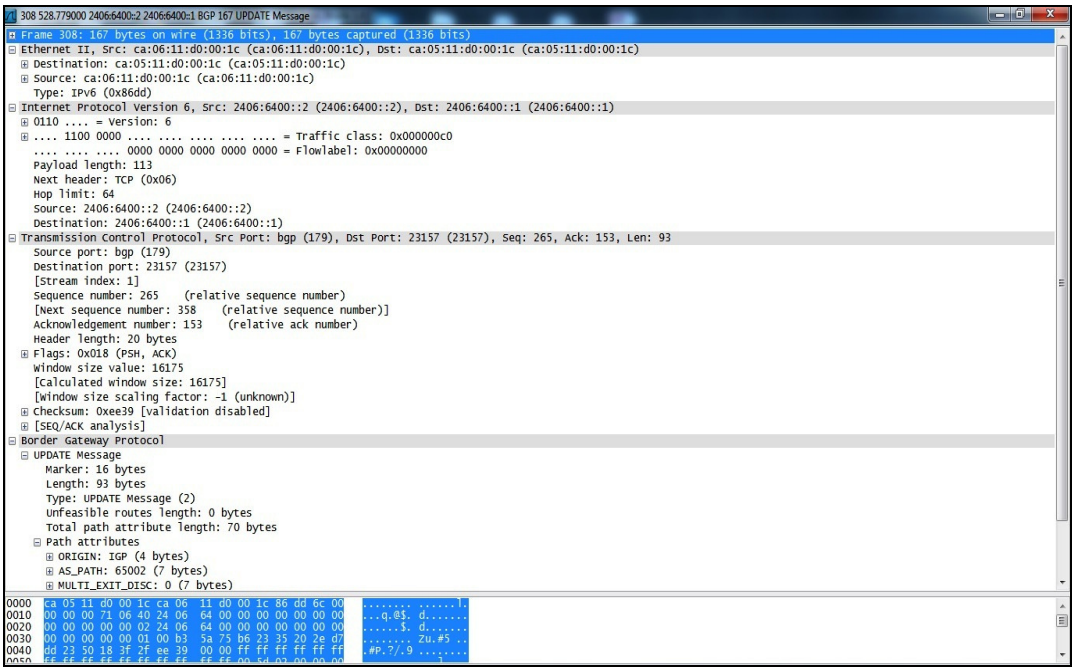

Figure 5: BGP Packet Analysis

A snippet of captured date showing update and keepalive message is shown in figure 5. Captured BGP traffic is from the TCP port 179. Figure 5 illustrates frame number 138 and the number of bytes captured on this frame. As messages originate from multiple protocols, the frame shows Ethernet protocol source and destination address, the source and destination addresses of IP, source and destinations port numbers for TCP, and details of BGP. As messages originate from multiple protocols, the frame shows Ethernet protocol source and destination address, the source and destination addresses of IP, source and destinations port numbers for TCP, and details of BGP. There are four types of message like type 1 indicates open message, Type 2 indicates that this message is an update message, type 3 indicates notification message, and type 4 indicates keepalive message.

4.2.3. TCP Operations

ACK is used to to point whether or not the acknowledgment field is valid. PSH is about once the sender needs the remote application to push this information to the remote application. RST is used for reset the connection. SYN (for synchronize) is used within the connection start up phase, and FIN (for finish) is used to close the connection in an arranged method. The TCP checksum verification is applied to a synthesized header that has the supply and destination addresses from the outer IP datagram. The first segment of a TCP session is establishment of the connection. This requires a three-way handshake, ensuring that both sides of the connection have an explicit understanding of the sequence number space of the remote side for this session.

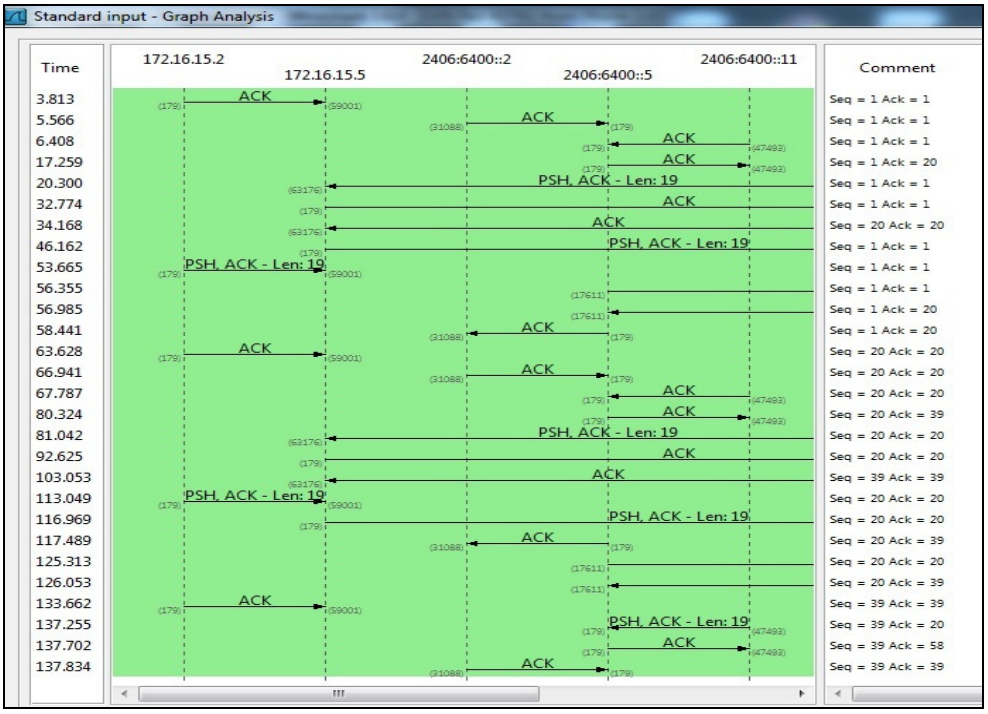

Figure 6: TCP Connection handshake

The performance reference of this protocol exchange is that it takes one and a half round-trip times (RTTs) for the two systems to synchronize status before any data can be sent. When the connection has been established, the TCP protocol handles the reliable exchange of data between the two systems. The traffic service reply time is defined as the time between a request and the corresponding reply. The flow graph of the captured IPv4 and IPv6 traffic is shown in Figure 6. It includes the source address, destination address, TCP port number, TCP message (ACK). The flow graph shows the IPv4 and IPv6 peers participating in the traffic exchange. At time 3.813 s, an ACK message is sent from source address 172.16.15.2 to the destination address 172.16.15.5 and the destination sends an acknowledgement back to the source implying that it is ready for traffic exchange. An exchange of data happens between only two BGP peers at a time. At time 5.566 s, an ACK message is sent from source address 2406.6400::2 to the destination address 2406.6400::5 and the destination sends an acknowledgement back to the source implying that it is ready for traffic exchange. An exchange of data happens between only two BGP peers at a time. At 6.408 s, the destination address 2406.6400::11 sends a ACK message to source address 2406.6400::5 to confirm that the link between the two is operating. When the destination address receives the acknowledgement, it knows that the link is active and it resumes the data exchange again.

4.2.4. Time Sequence Graph:

A graph of TCP sequence numbers versus time. While an ACK is obtained, it includes the sequence number connecting to the following byte to be received. The protocol analyser tools Wireshark convert all sequence numbers into relative numbers to facilitate comprehension and tracking of the packs involved in a TCP session. This means that the sequence number matching to the first packet in a TCP connection always begins with 0 and not from a random value 0 to (2^32)-1) created by the TCP/IP stack of the operating system [9]. Under ideal conditions, the representation of connection will show a line growing over time showing the efficient

performance of TCP connection. A time sequence graph is shown in figure 7. However, due to occasion's gaps and jumps that interrupts the continuity of the line. In general this happened due to a resend of data as an effect of lost segments, ACK duplications, expired timeouts, etc. This graph gives a very valuable source of information to detect anomalies in the behaviour of certain connections.

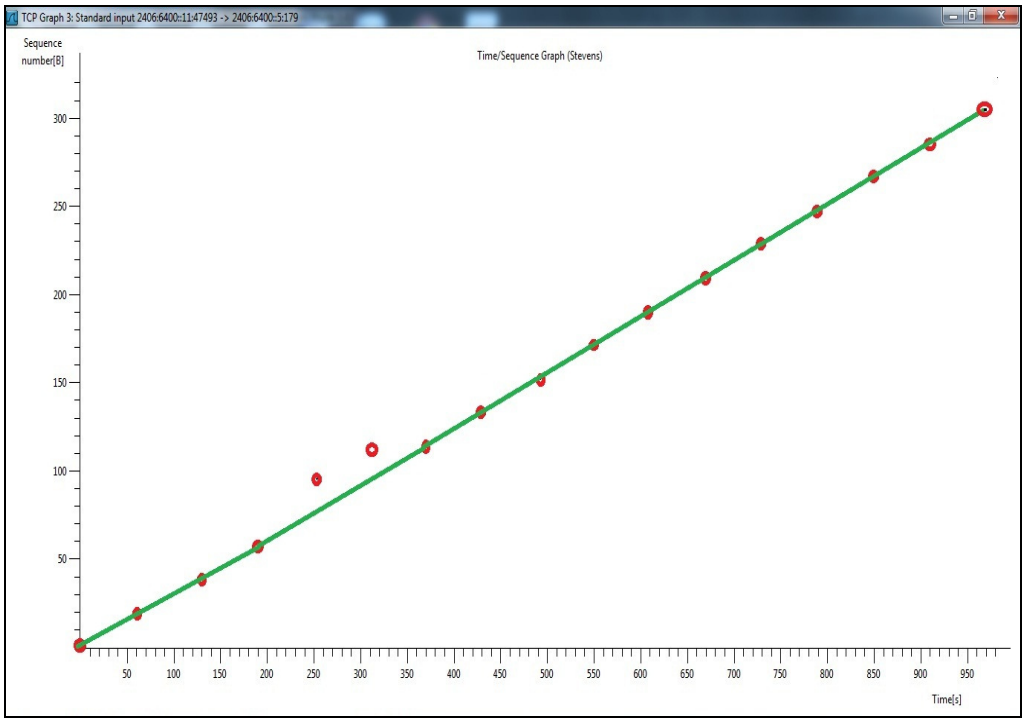

Figure 7: Time sequence graph

4.2.5. RTT Measurements

Round-trip time (RTT) is the duration of time it takes for a signal to be sent plus the length of durations it takes for an acknowledgment of that signal to be received. This time delay consequently comprises of the transmission time span between the two points of a signal. In the context of computer networks, the signal is generally a data packet, and the RTT is also known as the ping time. The RTT was originally estimated in TCP which can be found reference number: RTT = (α · Old RTT) + ((1 − α) · New round trip sample), Where α is constant weighting factor ($0 \leq \alpha < 1$). Select a value α close to 1 makes the weighted average opposed to to changes that last a short time. Choosing a value for α close to 0 makes the weighted average respond to changes in delay very quickly. In a network, particularly a wide-area network or the Internet, RTT is one of several factors affecting latency, which is the time between a request for data and the complete return or display of that data. RTT estimation is one of the most important performance parameters in a TCP exchange, especially in the case of a large file transfer. All TCP implementations eventually drop packets and retransmit them, no matter how good the quality of the link. If the RTT estimate is too low, packets are retransmitted unnecessarily; if it is too high, the connection may sit idle while the host waits for a timeout. One simple way to find the RTT for such a flow is to find the time between the syn-ack and the data packet. The response flows take a little different information. When a host transmits a TCP packet to its peer, it must to wait a certain time for an acknowledgment.

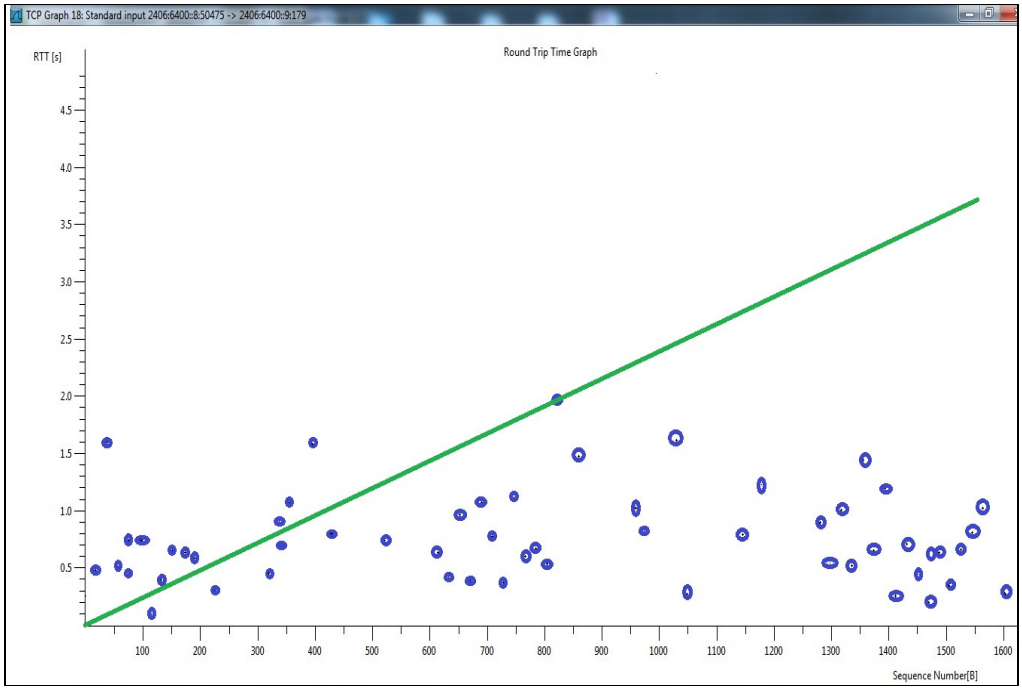

Figure 8: RTT graph

If the reply does not arrive within the expected period, the packet is assumed to have been lost and the data are retransmitted. If the traffic flows over the wide-area Internet, a second or two seconds are reasonable during peak utilization times. Network traffic for Transmission Control Protocol RTT is shown in Figure 8. If the RTT guess is too low, packets are retransmitted gratuitously; if it is too high, the connection may sit inactive while the host waits for a timeout. From the figure 8 average RTT for IPv6 address 2406:6400::8 to 2406:6400::9 are average 0.5-0.8s. Sometimes we got higher RTT when router working process becomes high. In our experiment the differences in round trip time on IPv4 and IPv6connection do not show significant difference.

4.2.6. Throughput

Throughput is valuable in understanding end-to-end performance. In figure 9 shows the TCP throughput results of an ideal model and a real IPv6 backbone for different packet sizes.

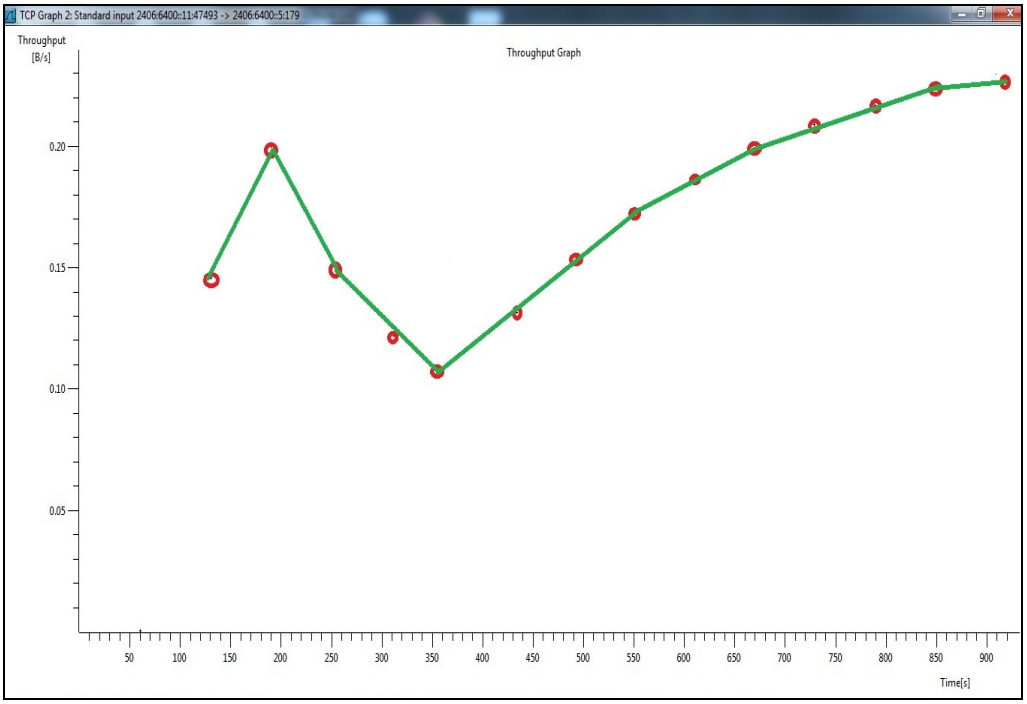

Figure 9: Throughput graph

.

From the TCP throughput results in we observed that there are very close throughputs for both IPv4 and IPv6 networks in terms of small message sizes. From the TCP throughput results, we also found that throughputs for both IPv4 and IPv6 networks in any message size are very similar. In a real large-scale network, the throughputs of the IPv6 network increase quickly in small message sizes of 256 bytes. Then the throughput becomes smoother until the 768-byte message size range. However, the throughputs decreased a little bit up to the 1408-byte message size range. In a real large-scale network, we obtained a minor degradation for IPv6 compared to IPv4 networks because the overhead of the IPv6 address size is more significant. TCP considers two most important factors: TCP window size and the round trip latency to transfer data. If the TCP window size and the round trip latency are identified, the maximum possible throughput of a data transfer between two hosts may be calculated regardless of the bandwidth using the expression: TCP-Window-Size-in-bits / Latency-in-seconds = Bits-per-second throughput. Instantaneous throughput is the rate (bps) at which a host receives the packets. If the packets consist of F bits and the transfer takes T seconds for the host to receive all F bits, then the average throughput of the packets transfer is F/T bps.

5. CONCLUSIONS

In this paper we focused on IPv4 to IPv6 migration in a large scale network. It is proposed that dual stack is the better technique to migrate in IPv6 network in compare to tunnelling and NAT techniques. In near future we have to fully migrate on IPv6 no more IPv4 address in the world. Dual stack give this facility to migrate gradually to IPv6. In Dual stack network we can easily run both IPv4 and IPv6 parallel. It permits hosts to at the same time reach IPv4 and IPv6 content agreeable authoritative it an adjustable coexistence strategy. In the tunnelling concept we cannot move fully in IPv6. There are also other problems like TCP migration IPv4 to IPv6 increase protocol overhead that increase latency and packet delay, each and every router need to configure tunnel for IPv6, which gives more overhead. It is also difficult to maintain the network as a

Service Provider. There is no NAT concept in IPv6. In IPv4 we used NAT due to lack of IP address but in IPv6 no more restriction on IP address. In this paper, we conducted IPv6 address planning, an end-to-end performance evaluation on a real large-scale network backbone. The following shows our investigative findings: For TCP throughputs, the IPv6 network does as well as the IPv4 network in terms of end-to-end performance. In a real large-scale environment, the throughput of the IPv6 network increased quickly in small message sizes of 256 bytes, after which, it levelled out until the 768-byte message size range.

ACKNOWLEDGEMENTS

The authors would like to thanks Department of Electrical and Electronic Engineering, School of Engineering and Computer Science, Independent University, Bangladesh.

REFERENCES

[1] Tahir Abdullah, Shahbaz Nazeer, Afzaal Hussain, "NETWORK MIGRATION AND PERFORMANCE ANALYSIS OF IPv4 AND IPv6", European *Scientific Journal,* vol. 8, No.5, 2013

[2] Lefty Valle-Rosado, Lizzie Narváez-Díaz, Cinhtia González-Segura and Victor Chi-Pech, "Design and Simulation of an IPv6 Network Using Two Transition Mechanisms", *IJCSI International Journal of Computer Science Issues*, Vol.9, No.6, pp: 60-65, Nov. 2012.

[3] Internet Engineering Task Force (IETF) RFC 6052, 3513, 4291, 6104, *http://tools.ietf.org/html/*

[4] Febby Nur Fatah, Adang Suhendra , M Akbar Marwan , Henki Firdaus Henki Firdaus , "Performance Measurements Analysis of Dual Stack IPv4-IPv6", *Proc. of the Second Intl. Conference on Advances in Information Technology — AIT*, 2013..

[5] Y. Wang, S. Ye, and X. Li, "Understanding Current IPv6 Performance: A Measurement Study", *10th IEEE Symposium on Computer Communications*, June 2005.

[6] Cebrail CIFLIKLI, Ali GEZER and Abdullah Tuncay OZSAHIN, "Packet traffic features of IPv6 and IPv4 protocol traffic, Turk", *J Elec Eng & Comp Science*, Vol.20, No5, pp: 727-749, 2012

[7] Alex Hinds, Anthony Atojoko, and Shao Ying Zhu, "Evaluation of OSPF and EIGRP Routing Protocols for IPv6", *International Journal of Future Computer and Communication (IJFCC)*, Vol.2, No.4, pp: 287-291, Aug. 2013.

[8] T. Bates, R. Chandra, D. Katz, and Y. Rekhter, "Multiprotocol Extensions for BGP-4," *Internet Request for Comments*, vol. RFC 4760, Jan. 2007.

[9] Ing. Luis Marrone, Lic. Andr´es Barbieri and Mg. Mat 'as Robles, "TCP Performance - CUBIC, Vegas & Reno", *JCS&T*, Vol.13, No.1, pp:1-8, April 2013

[10] Kevin R. Fall and W. Richard Stevens, "TCP/IP Illustrated", volume 1, published by *Addison-wisely professional computer series, Pearson Education*, 2012

Authors

Muhammad Yeasir Arafat received the B.Sc. degree in Electronic and Telecommunications engineering from Independent University, Bangladesh, in 2012, the M.Sc. degree in Computer Network and Communications engineering from Independent University, Bangladesh, in 2014. He worked as a System Engineer at Dhakacom Limited. His research interests include Computer networks, Network architecture, Network planning, design and Network security, communication protocols: SIP, H.323, Linux and UNIX, Open source VoIP system, Asterisk, VoIP development, integration, VoIP Security, Quality of Service and Universal radio peripheral (USRP) Software. He has published over 4 papers in different peer reviewed international journals and 3 papers on national and international conferences. Mr. Yeasir is a member of the Institute of Electrical and Electronic Engineers (IEEE).

Feroz Ahmed received the B.Sc. degree in electrical and electronic engineering from Rajshahi University of Engineering and Technology, Bangladesh, in 1995, the M.Sc. degree in electrical engineering from University Technology Malaysia, Malaysia, in 1998, and the Ph.D. degree in communication engineering from the University of Electro-Communications, Tokyo, Japan in 2002. From 2002 to 2005, he worked as a postdoctoral research fellow at Gunma University, Gunma, and the University of Electro- Communication, Tokyo, Japan. In 2005, he was appointed as an Assistant Professor in the school of engineering and computer science at the Independent University, Bangladesh and became an Associate Professor in 2011. His research interests include optical fiber communications, wireless communications, and network security. He has published over 50 papers in different peer reviewed international journals and conferences. Dr. Ahmed is a member of the Institute of Electrical and Electronic Engineers (IEEE).

M Abdus Sobhan was born in 1948 in Kushtia district of Bangladesh. He obtained first class B.Sc. Honors and M.Sc. degrees in Physics in '69 and App Phys & Electronics in '70 respectively from Rajshahi University (RU). He got the PhD degree from the Electronics & Electrical Com Engg. Dept of IIT Kharagpur in 1989.He did the Post-Doctoral research in the Physics Dept of CTH, Gothenburg. He was a Professor of the Dept of App Phys & Electronic Engg Dept of RU until 2005. Prof. Sobhan is the founder Chairman of CSE Dept of RU. He is also the founder Vice Chancellor of Prime University, Dhaka, Bangladesh. He served the Bangladesh Computer Council, Ministry of Science & ICT, GoB as its Executive Director for five years. Currently, he is a Professor of the department of Electrical and Electronic Engineering, School of Engineering and Computer Science of Independent University, Bangladesh (IUB), Dhaka. He is the Life fellow of IEB and BCS and a member of the IEEE. He supervised and supervising big number of M.Sc. and PhD Theses. He has published more than 180 technical papers in referred conferences and journals.