Service Provider IPv4 to IPv6 Network Migration Strategies

Babu Ram Dawadi1,2, Shashidhar Ram Joshi2, Ananda Raj Khanal3
1Department of Electronics and Computer Engineering, Tribhuvan University, Central Campus Pulchowk, Nepal
2Department of Engineering, Nepal Telecommunications Authority, Kathmandu, Nepal
3*Department of Engineering, Nepal Telecommunications Authority, Kathmandu, Nepal {baburd, srjoshi}@ioe.edu.np, arghanal@nta.gov.np

ABSTRACT

With the increase of Internet of Things (IoT) smart devices and the trend of world moving to converged network environment into the mode of packet based communication network, internet protocol address becomes the major logical infrastructure for all kinds of voice and data communications, led to the exhaustion of 32 bits IPv4 address space. Several issues like security, quality of service, addressing, routing management along with the depletion of addresses have been sought with the IPv4 addressing infrastructure. This forced the world required to migrate into IPv6 as a new addressing paradigm. Currently, the term 'migration' refers to different research dimensions in the world of science and engineering. The Information and Communication Technology (ICT) service providers are in the rush of not only the migration to IPv6 but also towards the migration into cloud computing and software defined networking, where "migration in togetherness" is coined to enter into the new era of IT based businesses and services. IPv4 and IPv6 are not interoperable. Hence moving into IPv6 operable network is a gradual process. The concerned organizations throughout the world are in different stages of network migration to IPv6. Service Providers and organizations of the developing countries are lacking behind the migration due to the lack of awareness, training, and cost of transition. This paper proposed the network transition steps after highlighting the migration strategies for Service Providers(SP) with different transition technologies.

Keywords: IPv4, IPv6, Service Providers, Transition, Strategies, Migration Approach, Tunneling, Dual Stack, Translation.

1. INTRODUCTION

Different addresses are required for complete communication defined in the computer network[1]. The addresses are generally categorized as physical address (e.g.: MAC address), logical address (IPv4/IPv6 address), Port address (e.g.: SMTP: 25, TELNET:23) and domain address (e.g.: www.ioe.edu.np). The logical address should be scalable due to its WAN scope. Hence, the concept of 128 bits IPv6 address is conceptualized against the limitations of IPv4.

The Internet user growth has rapidly increased throughout the world for almost a decade, and 32-bits IPv4 address space limitations have become severe. IPv4 address space is allocated by IANA, the central registry for RIRs and from RIRs to NIRs or LIRs according to the hierarchical structure of the registry, and then assigned to end users. The exhaustion point is the point in time when the IANA has allocated all the IPv4 address space in the pools it retains, when the RIRs have allocated all the IPv4 address space retained in its pool to the LIRs, when the IPv4 address space in the pool retained by the LIRs is completely assigned to end users[2]. At this stage, all IPv4 address space managed by registries is distributed and the registries can no longer assign new IPv4 address space [2]. There are still in some address spaces in the RIR pools and their exhausted timeline have also been projected[3].

Looking into the exhaustion status in Table 1, Africa is safe for next 2/3 years. Africa has opportunity to define policies and plan for migration to IPv6, however the continent should create global competent environment to be synchronized with the latest network infrastructure under rapid deployment by other continents due to lack of ipv4 address[4]. Several countries worldwide have already developed roadmap, plan and policies for the network migration to IPv6.

Table 1: Projected RIR Address Pool Exhaustion

<table>
<thead>
<tr>
<th>RIR</th>
<th>Projected Exhaustion Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>APNIC</td>
<td>19-Apr-2011</td>
</tr>
<tr>
<td>RIPE NCC</td>
<td>14-Sep-2012</td>
</tr>
<tr>
<td>LACNIC</td>
<td>10-Jun-2014</td>
</tr>
<tr>
<td>ARIN</td>
<td>24-Sep-2015</td>
</tr>
<tr>
<td>AFRINIC</td>
<td>23-Apr-2019</td>
</tr>
</tbody>
</table>

Taking the reference of Nepal as a developing country, the mobile penetration rate has crossed 100% but the internet penetration is not that much expected. However the internet users are also rapidly increasing likely to cross the penetration rate by 50% in the year 2015[5]. Almost developed countries worldwide have developed their national roadmap with projected timeline for network migration to IPv6[6]. It is necessary for all service providers of the developing countries to plan for the timely migration to IPv6 network as well as the infrastructure for cloud computing and the software defined networking.

2. IPv4 AND IPv6 COMPARISON

The exhaustion of IPv4 address had already been predicted in 1990s to be depleted within next 20 years when the World Wide Web became popular around the globe. However the IPv4 network infrastructure is well stable in its service, it has several issues which are briefly highlighted with the improvement in IPv6 in this section.

IPv4 provides approximately 4.3 billion addresses, which is already depleted as announced by IANA. This is the main cause of birth of IPv6 having 128 bits address length. It has $2^{128} = 3.4X10^{38}$ addresses where 80 bits is already astronomical. It is expected that there will be living beings on other planets as well in the future and they shall be able to communicate as an inter planet communication due to the sufficiency of IPv6 addresses.
NAT (Network Address Translation) is the technology which maps one public IPv4 address to many private addresses in the hidden zone. But unfortunately, NAT is not suitable to several applications which require end to end communication like FTP, NFS and group conferencing[7]. NAT is not require in IPv6 due to the sufficiency of addresses in which every device shall have more than one IPv6 addresses. Address assignment is an another issue in IPv4 network. Either Static (i.e. the network administrator manually set IPv4 address on every machine, which is a headache to set address for hundreds of machine in the LAN) or provide address dynamically via DHCP server, which raise machine renumbering problem making difficulties for network administrator to take control over the devices remotely. IPv6 has additionally unique approach called SLAAC (Stateless Address Auto-Configuration)[8] in which every machine in the LAN calculates its interface identification number by using the technique like EUI-64 (SUFFIX) and receive always unique PREFIX via router advertisement.

The main task of router is optimal path finding to route the packet to proper destination. But sometimes IPv4 router is overloaded due to fragmentation of oversized packets by itself. Hence IPv4 has special header fields (identification, flag & fragmentation offset) to handle fragmented packets. But IPv6 router never fragments the packet. Instead it generates the ICMPv6[9] packet too big message to the source so that source itself is liable to fragment the packets below MTU size[10]. The packet size in IPv4 is variable changing form 20-60 bytes where the 8 bytes (source and destination address) are not required by the router to be processed. Every time the router requires to view the header size due to variability nature of IPv4 packet header length. The packet header is efficiently modified in IPv6 and it is fixed 40 bytes in which 32 bytes (source and destination address) are not required for the router to be processed. IPv6 header has special header field called flow level in addition with modified header field ‘traffic class’ to handle the traffic which requires special handling for better quality of service. IPv6 header with its extension headers are managed into daisy chained fashions that ensure extensibility features of IPv6. The built in ESP (Encapsulating Security Payload) and AH (Authentication) extension headers and protocols defined under IPSec framework ensures better security in IPv6 capable Networks[11]. IPv4 has unicast, multicast and broadcast addressing types where anycast is experimental. The concept of broadcast is easily incorporated into multicast address in IPv6. Hence IPv6 has unicast, multicast and anycast address format[12].

3. CAUSE OF MIGRATION TO IPv6 NETWORK

Moving into IPv6 is not an individual or organization’s interest. It is becoming compulsion due to the fact that there is no more IPv4 address available. Comparative studies have already shown that IPv6 is far improved from different perspectives. From technical perspectives, IPv6 helps to avoid address inadequacy, enhance security in the network and support for better quality of service, improve efficiency and optimization of the network, create better environment to move into converged network and the next generation networking infrastructure.

From business and economic perspectives, the latest network infrastructure with IPv6 helps to develop perfect e-Commerce implementation, secure online transactions, reliable and quality email-internet service to the customers, gain or increase customers by the service providers, catch growth opportunities, encouraged for the network and service expansion, prevent increased cost and disruption of service. Businesses that do not commit to IPv6 transition, and do not start to take the proper steps to initiate this process, will risk accessibility problems of their websites and other internet-connected locations and services.

Similarly, from government and authority point of view, it is require to move to IPv6 to have better policy for country wide digital infrastructure, better public service delivery, efficient regulation over converged licensing framework, develop international trends and standards, create global competitive and regulatory environment.

4. SERVICE PROVIDER NETWORK MIGRATION STRATEGIES

Service providers throughout the world are in different stages of migrating to IPv6 network. Exhaustion of IPv4 address increased pressure to service providers to follow effective and smooth migration despite the risk of service interruption in their businesses. To successfully migrate to IPv6, service providers must be able to design and manage data centers, network infrastructure, and security systems that simultaneously support both IPv4 and IPv6[13]. Several strategic approaches have been proposed with integrated solution commercially available like BIG-IP[14] for IPv4 and IPv6 network inter-communication, applications and network security and traffic load balancing. Service providers shall follow the different strategies mentioned by Smith[25] have been reviewed in this paper below for the business interest and service provisioning.

4.1 Do Nothing

Migration to IPv6 network is inevitable. However no activities and position of don’t care condition for service providers ultimately push their business into dead end. This strategy is a short term business plan for the service providers who just want to sustain with their existing infrastructure until they have customer in their business. But definitely they will be unable to retain their valued customers in the long run and can't compete with the market due to hurdle in network expansion.

4.2 Extend life of IPv4

Doing something is better than nothing. Service providers shall use Network Address Translation (NAT) so called Large Scale NAT (LSN)/NAT444 in their networks to expand service with IPv4 until all the outside
interconnecting network become IPv6 operable. However this is not a long term solution. Alternatively, the IPv4 address trading business shall help to acquire limited public IPv4 addresses. ISPs may force customers to use NAT by moving to either RFC6598 and/or RFC1918 address space whichever is feasible. Ultimately service providers should have to follow some alternate transition approaches like tunneling, dual stack or protocol translation[15][16] after its customers have demand on IPv6 based services.

4.3 Deploy IPv6

There are several deployment techniques available where service providers can strategically apply based on the status of their current network infrastructure and customer demands. Deploying IPv6 means to follow progressive steps towards native IPv6 services. However gradual migration process should be followed. The most popular approaches in the migration process are broadly categorized as Tunneling, Dual Stack and Translation then finally to native IPv6 services.

If the intermediate network or public network in between the communicating points does not understand the corresponding IP packet, then the tunneling approach is used to encapsulate one packet into another packet which is understandable and routable in the network. The intermediate network shall be IPv4 only or IPv6 only. IPv6 over IP4 or IPv4 over IPv6 tunneling shall be applied. Broadly the tunneling is divided into automatic and configured tunneling. Automatic tunneling dynamically tunnel the packets and send to the tunnel end points by using IPv4 compatible IPv6 address. Tunneling is applied based on the communication between the tunnel end points like Host-to-Host, Router-to-Router, Host-to-Router or vice versa.

**Figure 1 Router to Router Tunneling**

Different tunneling approaches[17] like 6to4, 6RD, Teredo, ISATAP, tunnel broker services are available to establish the communication between corresponding IPv4 and IPv6 end networks.

Those networking devices which can process both IPv4 and IPv6 packets independently at a time are called Dual Stack [18] devices. We can enable one stack like IPv4 or IPv6 only stack at a time or both stacks. It helps to smooth transition to IPv6 only network because if the network is fully IPv6 ready then just disable the IPv4 stack in the dual stack network.

A method of translation is required if your hosts within the IPv6 only network wants to communicate with IPv4 only hosts in the another network. We need a translator router in the boarder. The main task of translator router performs the network address and protocol translation from IPv6 to IPv4 and vice versa.

**Figure 2 Translation Mechanism[19]**

The boarder router is a dual stack router contains pool of IPv4 addresses and map with the corresponding IPv6 address of the host machine in IPv6 network. DNS-ALG [20] generates the destination IPv6 address (fake IPv6 address) for the source IPv6 host. Hence all the IP and ICMP packets will be translated at the boarder router. The concept of NAT-PT[21] is deprecated due to the cause mentioned in [22] and likely replaced by NAT64[23], an address family translation. It is also recognized as Career Grade-NAT (CGNAT) or network operator version of subscriber NAT, which performs translation of large volume traffic at a time from IPv6 clients to IPv4 servers and vice versa.

5. SERVICE PROVIDER NETWORK MIGRATION APPROACHES

The most important part that any service provider should take care while the network transitioning to IPv6 is to assess the readiness of its network resources whether the existing software, hardware (routers, switches) and operating systems are capable to operate IPv6 or not. Service providers worldwide are in different stages of migration. Looking into the Nepalese service providers, the survey shows that they have not planned yet for the transitioning however the core networks of major service providers are almost dual stack capable. Steps for smooth transition with different scenarios are being discussed in this paper for those service providers who are at the different stages of their network migration.

5.1 First Scenario

If the service provider network is IPv4 only and immediate replacement of Customer Premise Equipment (CPE) for IPv6 operability is not possible and there is customer demand for IPv6 services, service provider may provide Tunnel Broker service (Figure 3) where direct tunneling of IPv6 over IPv4 shall be possible from customer end device to the tunnel broker/server. Detail of tunnel broker and server is mentioned in [24]. This is just a very short term solution which does not encourage for migration. Tunneling the traffic increase the additional load for encapsulation and decapsulation of traffic at the
end points, where the tunnel server load balancing is required.

5.2 Second Scenario

Even if the service provider network is IPv4 only, service providers shall replace the customer premise devices with dual stack capable and follow 6 Rapid Deployment (6RD) approach which tunnel the customer IPv6 traffic from CPE to edge router to connect to IPv6 internet.

5.3 Third Scenario

Next step for service provider is to enable its network infrastructure into dual stack mode by either migrating the software or replacing the hardware equipments. The drawback of dual stack network is that every dual stack device processes v4 and v6 packet separately, consumes big resources and also the separate firewalls for v4 and v6 should be maintained. However this approach in the transition runs longer period because service provider may not take risk of immediate migration to IPv6 with the fear of service interruption to their customers. It also provides the chances to verify the operability of hardware, software, OS and network stability with IPv6 during the dual stack operation.

Based on the IPv4 and IPv6 traffic volume status incoming and outgoing from the network, service provider shall decide to move from dual stack to dual stack lite approach. With the increased demand on IPv6 network interconnection, transit services and increasing volume of IPv6 incoming traffic as well as decreasing IPv4 traffic at the network access point (NAP), switching to Dual Stack Lite approach is preferable.

5.4 Fourth Scenario

During the moment when all the networks are IPv6 operable and there still exists some IPv4 servers which are required to be connected from the IPv6 only network, the concept of Address Family Translation (NAT64) can be used to translate the IPv6 header to IPv4 and vice versa. DNS64 server is required for domain name resolution together with NAT64 for large family of address translation. DNS64 server provides the answer of native IPv6 DNS queries while it forwards the query to the IPv4 DNS outside of its network to extract IPv4 address of the domain.

5.5 Fifth Scenario

If the limited IPv4 (private) consumers want to access public IPv4 resources which are limitedly available across the IPv6 network, then the IPv4 traffic has to pass across the public IPv6 network. We need translator at two edges
of the IPv6 network: customer end (core) and public IPv4 internet end (edge). Hence a combination of stateless protocol translation at the core and stateful protocol translation at the edge so far known as 464XLAT is proposed by RFC6877[27]. It is a simple and scalable technique which combines the NAT46 (stateless IP/ICMP translation) and NAT64 across the IPv6 network.

![Figure 7 464XLAT](image)

This approach is commercially available in the market and fairly easy as well as less expensive to deploy[14]. However translation at the both ends, requires massive processing. Looking into the different scenarios of transition strategies, the transition matrix is summarized in Table 2.

<table>
<thead>
<tr>
<th>Home Network</th>
<th>Service Network</th>
<th>Destination Network</th>
<th>Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>IPv4</td>
<td>IPv4/4 internet</td>
<td>LSN/NAT444</td>
</tr>
<tr>
<td>IPv6</td>
<td>IPv4</td>
<td>IPv6/6 Internet</td>
<td>Tunnel Broker, 6RD</td>
</tr>
<tr>
<td>IPv4/v6</td>
<td>IPv4/6</td>
<td>IPv4/6 Internet</td>
<td>Dual Stack</td>
</tr>
<tr>
<td>IPv4</td>
<td>IPv6</td>
<td>IPv4 Internet</td>
<td>Dual Stack Lite</td>
</tr>
<tr>
<td>IPv6</td>
<td>IPv6</td>
<td>IPv4 Internet</td>
<td>NAT64 (AFT)</td>
</tr>
<tr>
<td>Private IPv4</td>
<td>IPv6</td>
<td>IPv4 Internet</td>
<td>464XLAT</td>
</tr>
<tr>
<td>IPv6</td>
<td>IPv6</td>
<td>IPv6 Internet</td>
<td>Native IPv6</td>
</tr>
</tbody>
</table>

Service Providers have to plan from the beginning so as for smooth migration and continue their business without interruption of the services. The overall guideline for service provider is proposed by the flowchart Figure 8.

Network inventory maintains the list of network equipments including both hardware and software which are required to be migrated for IPv6 operation. Planning is the most important for any critical project. Migration is a project which include phase wise activities. The development of strategic planning[28] shall cover identification of customer requirements, IPv6 address reservation, human resource development, IPv6 only test-bed network for pilot test, hardware/software upgrade/replacement, budgeting for the migration, risk management, network and server security audit over IPv6 network, interconnection with other service provider network and choice of transition approaches. The strategic plan drives the smooth migration to IPv6 only network as a business continuity plan. Hence service providers should be well clever throughout the migration to understand the other networks and international migration scenarios so that they can review their migration plan as per the requirements.

![Figure 8 Transition Steps](image)
5. CONCLUSION

With an increasing demand on smart devices, the growth of internet users is rapid and global ICT market is highly competitive. From different perspectives, IPv6 infrastructure is comparatively better than IPv4. However it still has several challenges in the implementation due to interoperability problem between IPv4 and IPv6. So both the networks co-exists for longer period of time as a transition period. This paper has mostly reviewed the different transition technologies and discuss the migration strategies from IPv4 to IPv6 network. A strategic plan for migration to next generation Internet Protocol version 6 for service providers is recommended. It elaborates the business continuity plan with smooth transitioning approach to IPv6 operable network by giving broad idea to those voice and data service providers who are in the beginning stage of their network migration to IPv6. Basically service providers of the developing countries are at the early stage of migration. Hence timely migration of the network is inevitable to continue and expand the business for better sustainability.

ACKNOWLEDGEMENT

This research study was partially funded by Nepal Telecommunications Authority under the research grant "IPv6 Network Migration Roadmap of Nepal" carried out from February to August 2015.

REFERENCES


[27] Mawatari M., Kawasima M., Byrne C., (2013). 464XLAT: Combination of Stateful and Stateless Translation. RFC6877


AUTHOR PROFILES

**Babu Ram Dawadi** Received His B.Sc. in Computer Engineering and M.Sc. in Information System Engineering in 2008 from Tribhuvan University, central campus Pulchowk, Nepal. He worked as system/network engineer and lecturer at Pulchowk Campus, TU for 5 years, Assistant Director for 3 years at Nepal Telecommunications Authority. Currently, he is working as an Asst. Professor at department of electronics and computer engineering, IOE Pulchowk Campus. His area of interest is Networking, Distributed Computing and Data Mining.

**Shashidhar Ram Joshi** completed his Bachelor of Electrical Engineering from Sardar Ball abvhai Regional College of Engineering, South Gujarat University, Surat, India in 1984 and passed with first class first with distinction. He passed his Master’s of Science in Electrical Engineering from University of Calgary, Canada in 1992. He did his Ph. D. from Tribhuvan University in 2007. He was research fellow in Osaka Sangyo University, Japan for one year from 1997 to 1998 and published four papers in the peer reviewed international journals. He has joined Institute of Engineering in 1985 and presently he is a full professor in the Department of Electronics and Computer Engineering, Institute of Engineering, Central Campus Pulchowk, Nepal. His area of research is Image Processing, Networking and Artificial Intelligence.

**Ananda Raj Khanal** has Bachelor of Engineering degree in Electronics and Communications and Master of Science in Communication Engineering. He is a gold medalist in Bachelor of Law ( LLB). He is currently Director at Nepal Telecommunications Authority (NTA). Before joining NTA in April 2006, he was with the Kathmandu University in Nepal in the capacity of Assistant Professor. He continues to be a visiting faculty at different universities in Nepal. His area of interest is Telecommunications and ICT.