IPv6-only Network for Today's Internet: Prospects and Problems

Shashidhar Ram Joshi[#1], Babu Ram Dawadi [#2]

[#]*Department of Electronics and Computer Engineering, Tribhuvan University*
Institute of Engineering, Central Campus Pulchowk, Nepal

{[1]srjoshi, [2]baburd}@ioe.edu.np

ABSTRACT

The internet has been using its protocol, IPv4, for more than a quarter of a century. The internet saw its deployment found the tipping point in early 1990s with the popularity of World Wide Web. This fast pace development, however, creates problems for IPv4 like address space exhaustion, NAT proliferation, security etc. A new version of the Internet Protocol, IPv6, has been developed and is likely to replace IPv4. IPv6 has been developed to solve the problems regarding to IPv4 and also new features are designed to supposedly enhance network traffic. It is the time to have a transition from IPv4 to IPv6. The current Internet age is running in its transition phase to the new generation internet addressing. In this perspective, this research paper tries to analyze the IPv6 RFCs for its implementation as well as explore about migrating the current network into IPv6 only operation properly by performing a test with NAT-PT implementation under translation mechanism and analyzing different transition mechanisms which led us to conclude to better approach for the successful migration.

Keywords: IPv6, IPv4, Protocol, NAT, Proxy, TOTD, DNS, DNS-ALG, NAT-PT, Tunneling, Subnet, PREFIX.

1. INTRODUCTION

These days, we are experiencing rapid growth in internet users with large IP address consumers. The growth with its anticipated future requirement for more addresses is a key factor driving the new version of the internet protocol. Devices like PDAs, pagers, refrigerators, telephones and many other new inventions will have computing power and less expensive than a PC may require internet address for the connectivity on network. Methods such as NAT have been implemented to make better use of the IPv4 addresses, but these methods are said to destroy some of the original features about the Internet Protocol, e.g. loss of transparency and loss of unique addresses. The initial design of IPv4 did not anticipate the following:

- The recent exponential growth of the Internet and the impending exhaustion of the IPv4 address space.
- The growth of the Internet and the ability of Internet backbone routers to maintain large routing tables.
- The need for simpler configuration.
- The requirement for security at the IP level.
- The need for better support for real-time delivery of data—also called quality of service (QoS).

To address these and other concerns, the Internet Engineering Task Force (IETF) has developed a suite of protocols and standards known as IP version 6 (IPv6). As the work progressed it was agreed upon that several features about IPv4 in addition to the address space needed an upgrading. The essential areas are:

- Support for real-time services.
- Security support.
- Auto-configuration.
- Enhanced routing functionality.

IPv6 is now in a deployment phase. Several pieces of network equipments that support IPv6 have been shipped, and some network providers have started IPv6 commercial services. However, more analysis, implementations and experiments are still necessary. IPv6 deployment faces a number of challenges, including:

- The IPv6 costs and risks,
- The fact that NAT is required to incrementally deploy IPv6 yet appears to eliminate the need for IPv6, and
- The inability to really use the IPv6 features effectively during incremental deployment.

2. THE INTERNET GROWTH

During this past decade, the internet users and internet technology rapidly increased. The Internet has grown so large that an updating of the Internet protocol seems necessary. And more important, the growth will not stop. This is the major challenge for the next generation Internet protocol, and perhaps the most important thing to learn from IPv4; it must be able to manage a severe growth. To predict the future growth it is important to understand the growth up till now.

The main goal is to connect together the computers in government, business, universities, and schools. The growth of the computer market has been exponential. The future growth of the computer market is not expected to be exponential; instead other markets are expected to represent the largest growth of the Internet. Device control is also predicted to grow, and will be in the need of an Internet protocol. This market consists of devices such as lighting equipment, heating and cooling equipment and other types of equipment which are currently controlled via analogue

switches and in aggregate consume considerable amounts of electrical power. The solutions for this market must be robust and simple. The current internet growth shows that the IPv4 address will run out till 2010 [4].

3. PROBLEMS WITH IPv4

The current IPv4 internet infrastructure has lost a lot of functionalities because of the address conservation [3].

- Deficiency of address space - various devices connected to the Internet grows exponentially. The size of address space 2 32 is quickly exhausted.
- Loss of transparency - due to the use of mechanisms such as NAT (Network Address Translator).
- Loss of robustness - because of the implemented topology that has little room for redundancy.
- Loss of stable addresses - i.e. the address of a node changes each time it is connected to the Internet.
- Weak expansibility of the protocol - the insufficient size of heading IPv4 doesn't allow placing demanded quantity of additional parameters in it.
- Problem of safety of communications - it is not stipulated any means for differentiation of access to the information placed in a network.
- Absence of support of quality of service (QoS) - accommodation of the information about throughput, the delays and demanded for normal work of some network appendices is not supported.
- Absence of the auto-configuration - IP addresses mechanism and Machine renumbering problem.
- Loss of application independence - An example is that many systems are developed with functionality to avoid problems created by NAT.

The major point that is necessary to come to new IP version is the exhaustion of address space with current version. Not only this but also other features about the Internet Protocol is taken into consideration and found necessary to change or upgrade.

- Proliferation of NAT
- Lack of IPv4 Address Space
- Routing Table Explosion
- Limited Security
- Lack of Better QoS

There is a lot of skepticism towards NAT as it may be appropriate to some businesses that do not need full connectivity to the outside world, but for others, who require constant and robust contact with the Internet, NAT will not fulfill the requirements. It creates a bottleneck between the business and the Internet; it does not support end-to-end security and breaks the peer-to-peer model.

Following figure was created to show potential IPv4 address space exhaustion dates based on steady-state allocations and the past 4 year growth rates of IPv4 address space and the continued growth. By applying different assumptions, the IPv4 address exhaustion could occur as early as 2008/2009 and as late as 2012[8].

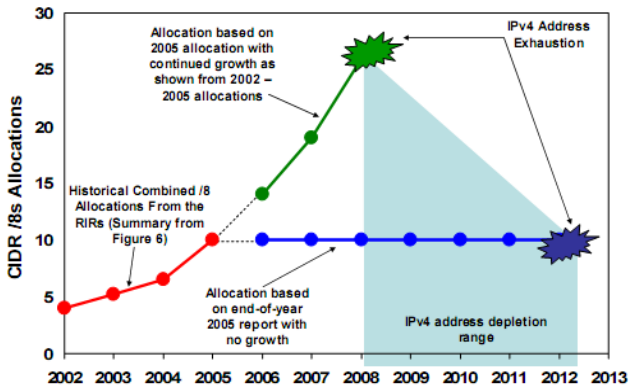

Figure 1 IPv4 address exhaustion Timeline [8]

IPv4 address allocation scheme does not allow effective routing information aggregation at the core of the internet. Currently, the number of prefixes in the internet routing table has more than 130 thousand prefixes before aggregation and more than 95 thousand entries after aggregation [7]. Routing table explosion burdens core routers, and may create instability problems and routing accidents.

Security in IPv4 is limited. There is no authentication or encryption mechanism at IP level and dependent on higher level protocol, hence vulnerable to denial-of-service and address deception or "spoofing" attacks. Packets sent at IP-level needs encryption to protect the private data from being viewed or modified. Also the QoS depends on the TOS field in the header. Though the QoS is defined, but not generally used consistently.

4. INTERNET PROTOCOL VERSION 6 (IPV6)

IPv6 is the "next generation" protocol designed by the IETF to replace the current version Internet Protocol, IP Version 4 ("IPv4"). Most of today's internet uses IPv4, however, because of its growing shortage of IPv4 addresses, the addresses will run out in about year 2008 +/- 3, according to calculations by IETF in 1994. In order to fix the problem, IPv6 - a new version of protocol was proposed by numerous internet groups such as "CNAT", "Nimrod", etc in 1993.

IPv6 working group started its WIDE project for the deployment of the IPv6 environment in 1995. So, the WIDE project started KAME (a joint effort of six companies in Japan to provide a free IPv6 and IPSec stack for BSD variants to the world) as a subproject for the purpose of combining the power of implementation. Although the members of IPv6 Working Group and KAME overlap, while IPv6 WG does technical and innovative researches. Mainly, KAME is in charge of implementation. AI3 & SOI-ASIA project under WIDE has started its IPv6 operation from Nov. 16 2005. Until January 2007, all SOI-ASIA applications are upgraded to IPv6 and after conducting operator's workshop on July/August 2007 for IPv6 only operation, the AI3/SOI-ASIA network is fully operable in IPv6 only network [7].

4.1 Features of IPv6

The feature which IPv6 protocol brings to plate are described in several RFCs and internet drafts could be summarized as follows.

- New header format
- Large address space
- Efficient & Hierarchical addressing and routing infrastructure
- Stateless and stateful address configuration
- Security
- Better Quality of Service Support
- New protocol for neighboring node interaction
- Extensibility

The IPv6 header has a new format that is designed to have a header overhead. The IPv6 header is only twice the size of IPv4 header, even though the number of bits in IPv6 address is four times larger than IPv4 addresses. This is achieved by moving both nonessential and optional fields to extension headers that are placed under the IPv6 header.

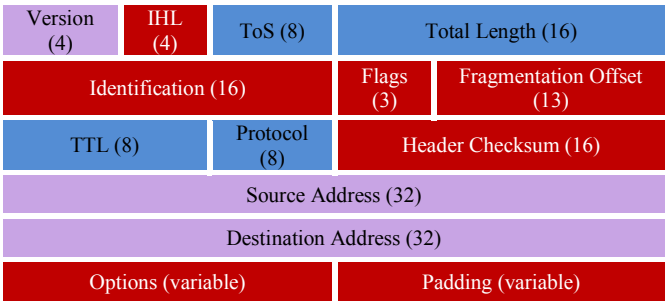

Figure2 IPv4 Header format

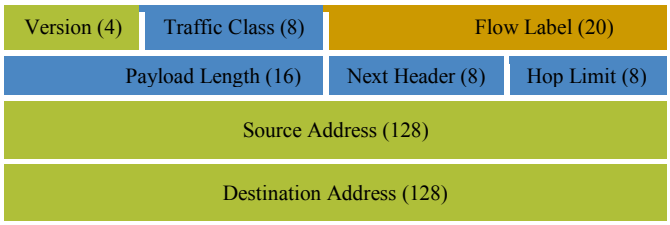

Figure 3 IPv6 Header Format

In the table 4.1a, the fields with red colors are removed in IPv6. Other fields of IPv4 header are also available in IPv6 but modified and one new field is added on IPv6 which is Flow Level.

4.2 IPv6 Address Distribution

An address allocation is defined by allocation size and location. Allocation size specifies how large of the address block or prefix is assigned. Allocation location is where in the address pool this block is allocated to [9]. The IP address allocation hierarchy is shown in figure below. At the top of the hierarchy, the whole address pool is controlled by the Internet Assigned Number Authority (IANA). IANA allocates large address blocks to each of the Regional Internet Registries (RIR) serving North America (ARIN), Europe (RIPE), Asia Pacific (APNIC), Africa (AfriNIC) and Latin America & Caribbean (LACNIC). The regional registries divide up these large address blocks into medium blocks to allocate to Local Internet Registries (LIRs), consisting mainly of internet service providers (ISPs). The ISPs further assign smaller address blocks to their users including companies, universities and smaller ISPs etc. The policies on IP allocation size vary from different registries at different levels. Different RIRs adapt their own policies for allocation to LIR/ISPs with unit size varying from /10 to /20. The size assign to end users by each ISP also vary accordingly. Due to historical allocation schemes, fragmentation is a common problem in IPv4; one ISP is often left with multiple prefixes.

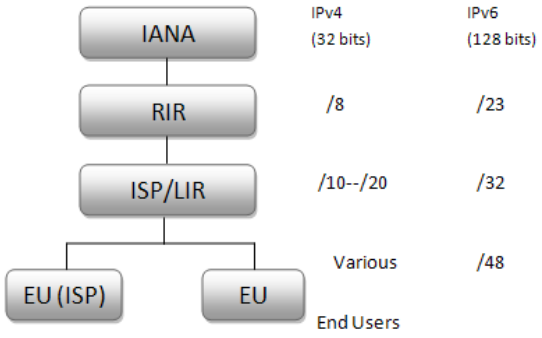

Figure 4 Address allocation hierarchy

IPv6 address allocation only considers the top 64 bits. Assigning appropriate address size at different level has been under extensive discussion.

4.3 IPv4/IPv6 Transition Mechanisms

For the future implementation of IPv6 only operation we need transitions from IPv4 to IPv6 currently. To make IPv4 and IPv6 coexist, transition mechanisms have been designed. The mechanisms can be divided into three groups:

- Tunneling techniques, used when IPv6 packets traverse over the IPv4 infrastructure.
- Dual-stack techniques, allowing IPv4 and IPv6 to coexist in the same devices and networks
- Translation techniques, making IPv6-only nodes able to communicate with IPv4-only nodes.

The tunneling and Dual-stack techniques exists until there will be IPv4 internet infrastructure as dominant but translation technique is the one which helps to migrate to IPv6 only network. This translation technique is utilized to communicate between IPv6 islands and also between IPv4 and IPv6 Islands. We may have IPv6 only networks and to communicate with IPv4 Island, there exists end node on IPv6 only network which perform IPv6/IPv4 translation and make the network communicable.

IPv6 tunneling enables IPv6 hosts and routers to connect with other IPv6 hosts and routers over the existing IPv4 Internet. IPv6 tunneling encapsulates IPv6 datagrams within IPv4 packets. The encapsulated packets travel across an IPv4 Internet until they reach their destination host or router.

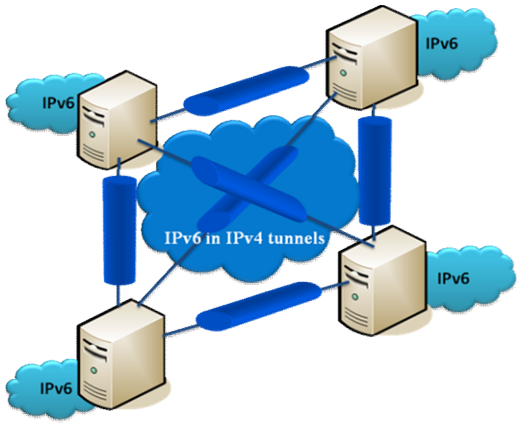

Figure 5 Tunneling IPv6 over IPv4

Tunneling can be categorized as configured and automatic. In configured tunneling the tunnel endpoint address is determined from configuration information in the encapsulating node. For each tunnel, the encapsulating node must store the tunnel endpoint address. In automatic tunneling, the tunnel end point address is determined by the IPv4-compatible destination address of the IPv6 packet being tunneled. Automatic tunneling allows IPv6/IPv4 nodes to communicate over IPv4 routing infrastructures without pre-configuring tunnels.

Table 1: IPv4 Compatible IPv6 Address Format

96-bits	32-bits
0:0:0:0:0:0	IPv4 Address

Dual stack node has support for both protocol versions. To communicate with IPv6 only node, that node acts like IPv6 only node and with IPv4 only node, it acts like IPv4 only node. Hence dual stack node has three stacks: IPv4 stack, IPv6 stack and dual stack.

4.4 Translation Mechanisms

Translation mechanism enables IPv6-only node to communicate with IPv4-only nodes and vice versa. The nodes need a mechanism for address translation, in order to make the connection. The major translation methods are:

- Stateless IP/ICMP Translation (SIIT) &
- Network Address Translator – Protocol Translator (NAT-PT)

SIIT is a mechanism which translates IPv6 packets in to IPv4 packets and vice versa. Basically SIIT describes a method by which a router interprets an IPv4 header and creates a parallel IPv6 header with equivalent information and the inverse equivalent operation of converting an IPv6 header into an IPv4 header. The actual means of converting an IPv4 address to an IPv6 address or vice-versa may vary, and the means by which the routing occurs is unspecified [RFC 2765].

IP and ICMP headers for IPv4 and IPv6 have some differences. So NAT-PT requires translating all IP/ICMP headers from V4 to V6 and vice-versa for end-to-end IPv4/IPv6 communication.

Translating IPv4 headers to IPv6 headers

The header translation is almost explained in RFC 2765 within SIIT apart from the following fields:

- **Source address:** The low-order 32 bits is the IPv4 source address. The high-order 96 bits is the designated PREFIX for all v4 communications. Addresses using this PREFIX will be routed to the NAT-PT gateway PREFIX::/96).
- **Destination address:** NAT-PT retains a mapping between the IPv4 destination address and the IPv6 address of the destination node. The IPv4 destination address is replaced by the IPv6 address retained in that mapping.

Translating IPv6 headers to IPv4 headers

- **Source address:** The NAT-PT retains a mapping between the IPv6 source address and an IPv4 address from the pool of IPv4 addresses available. The IPv6 source address is replaced by the IPv4 address retained in that mapping.
- **Destination address:** IPv6 packets that are translated have a destination address of the form PREFIX::IPv4/96. Thus the low-order 32 bits of the IPv6 destination address is copied to the IPv4 destination address.

4.4.1 Network Address Translator – Protocol Translator (NAT-PT)

NAT-PT is used as a migration tool to help customers transition their IPv4 network to IPv6 networks. Using a protocol translator between IPv6 and IPv4 allows direct communication between hosts speaking a different network protocol. This approach, in comparison to SIIT also allows IPv6 only hosts to talk to IPv4 only hosts and vice-versa. It uses a dedicated server and requires at least one IPv4 address per site [RFC 2766]. One of the benefits of NAT-PT is that no changes are required to existing hosts because all the NAT-PT configurations are performed at the NAT-PT router. Customers with existing stable IPv4 networks can introduce an IPv6 network and use NAT-PT to allow communication without disturbing the existing network. For example the IPv6 Node wants to communicate with the IPv4 Node. IPv6 Node creates a packet with: Source Address, for example SA=FBDC:AB57::1234:3210 and Destination Address, DA = prefix::202.70.91.6. The packet is routed via the NAT-PT gateway, where it is translated to IPv4, using the same method as in SIIT. If the outgoing packet is not a session initialization packet, the NAT-PT should already have stored some state about the related session, including assigned IPv4 address and other parameters for the translation. If this state does not exist, the packet should be silently discarded. If the packet is a session initialization packet, the NAT-PT locally allocates an address (eg: 202.249.24.215) from its pool of addresses and the packet is translated to IPv4.

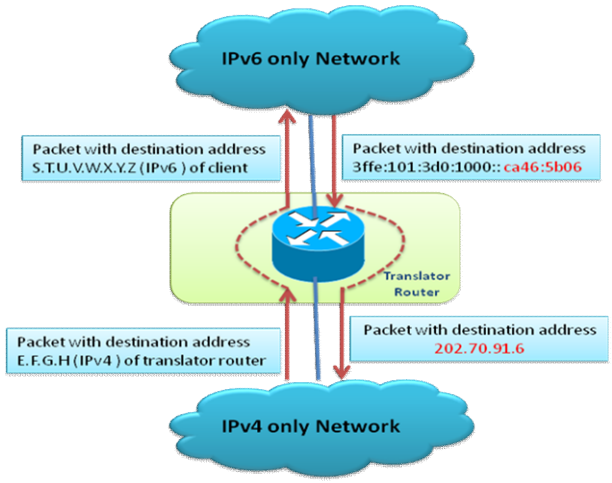

Figure 6 IPv4/IPv6 Translation Mechanism

4.4.2 DNS-ALG for NAT-PT: Trick or Treat Daemon (TOTD)

TOTD is a small DNS proxy name server which supports IPv6 and enable IPv6 only sites to access IPv4 sites by using some translation mechanism such as NAT-PT, KAME faith etc. it is a IPv6 DNS proxy which receive DNS queries from clients and forward it to a normal DNS server. If the reachable normal DNS server is IPv4 only, TOTD must be configured with dual stack mechanism otherwise for IPv6 reachable DNS server, it can be configured for IPv6 only server.

- **Request an AAAA/A6 records**: when a client request an AAAA/A6 record, the TOTD server simply forward the request to the client only if the requested record exists otherwise an A record is requested to normal DNS server and TOTD will receive an answer in IPv4 which will be translated into IPv6 address by adding certain PREFIX to the IPv4 address and forwards it to the client.
- **PTR lookup**: when a client tries a PTR lookup, TOTD simply proxies the look up only if the PTR lookup is using normal global IPv6 address. Otherwise if the PTR lookup is using converted IPv6 address, TOTD will convert the address back to IPv4 and the PTR lookup result will be forwarded to the requested client.
- **Other request**: other queries will be always ignored and the reply is simply forwarded to the client without modification.

TOTD generates the fake IPv6 address by appending IPv4 address with IPv6/64 prefix. The prefix is configured with TOTD configuration and constant for all generated addresses. For example if 202.70.91.6 is the IPv4 address then for the selected /64 prefix (2001:B30:101:555::/64), the figure 7. The DNS server most listens on other port than TOTD if both installed on the same machine.

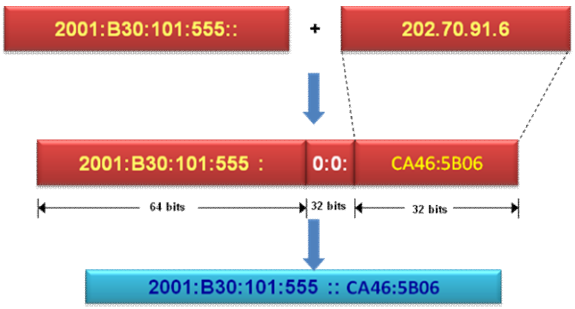

Figure 7 Fake IPv6 Address Generation

TOTD forwards the DNS query to normal DNS server to the specified port. The TOTD configuration is:

#cat /etc/totd.conf
forwarder ::1 port Linsten_port
forwarder IPv6-DNS_address port 53
forwarder IPv6-DNS_address port 53
prefix PREFIX::

First line shows that the TOTD server forwards its DNS queries to BIND DNS server at port 5353. Other two lines are the DNS server at other machines. Last line is the prefix set to be prepended with the client's IPv4 address.

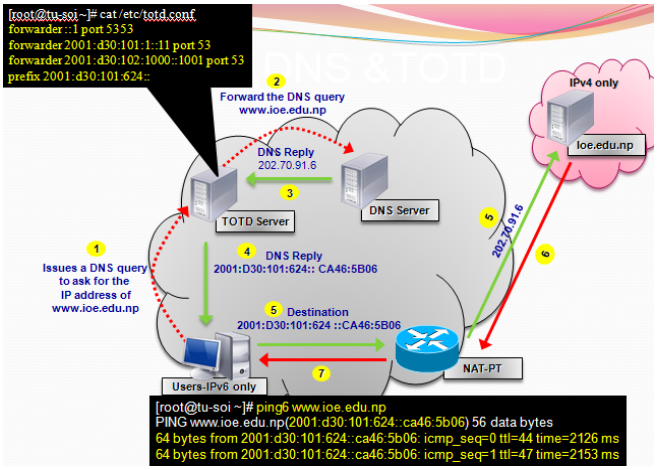

Figure 8 Ping Reply to IPv6 only Machine from IPv4 Host

The web server for www.ioe.edu.np has only IPv4 address (202.70.91.6) but TOTD generated the fake IPv6 address like *PREFIX::IPv4_Addr* (2001:d30:101:624:: ca46:5b06). The NAT-PT device translates that IPv6 address to IPv4 and forwards the packet to the destination.

For the current IPv4 dominant network, NAT-PT consumes many CPU resources with increasing internet traffic. Scalability may be the one important issue needs to be studied such that how many end-hosts a NAT-PT router can support. One simple solution to reduce the load of NAT-PT is to use the proxy server. Hence we can use proxy server for all the application that support proxy settings. Applications that do not support proxy setting will make a connection to internet using NAT-PT. A new patch was developed by Dr. Husni (squid-v6-2.6.STABLE9-31.soifc6) that solved the problem of the CONNECT for use with a

proxy that can dynamically switch to being a tunnel. The configuration is the figure below:

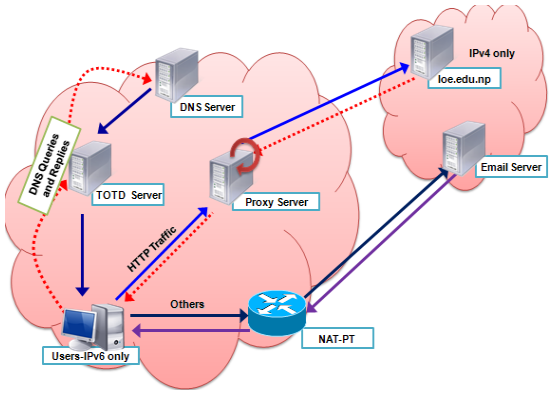

Figure 9 NAT-PT, TOTD, DNS & SQUID Test

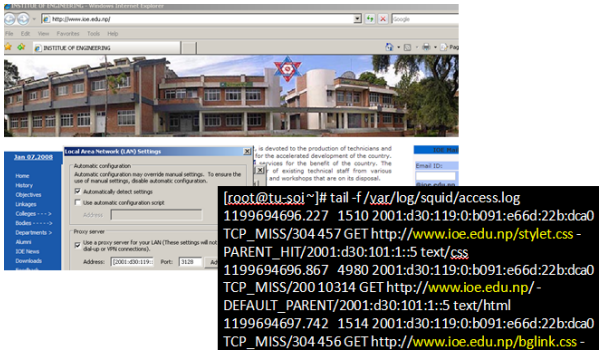

Figure 10 IPv4 web access via IPv6 proxy

4.5 Comparison: Tunneling, Dual Stack & Translation

Tunneling:

- Can communicate with remote IPv6 network without supporting IPv6 in ISP network
- Loads on the router (consumes time & CPU power for encapsulation and dcapsulation)
- MTU size issue and fragmentation problems

Dual-Stack:

- Easy to use and can communicate with both hosts
- Two separate protocols running over single machine consumes CPU power and memory
- Firewall protection for both protocols (burden)
- Don't solve the problem of IPv4 address exhaustion

Translation:

- Does not support Advanced IPv6 feature
- Easy to implement, single border router acting as NAT-PT
- IPv6 hosts can directly communicate with IPv4 hosts
- Independent of Hosts
- Encourage for transition to IPv6 network

5. IPV6 DEPLOYMENT: CHALLENGES AND RISKS

Deployment of IPv6 still has some challenges like:

- IPv6 costs and risks
- NATing yet appears to eliminate the need for IPv6
- Inability to use IPv6 features effectively during its deployment

Deploying IPv6 first in the enterprise level with some portion of corporate network requires NAT between the IPv6 portion and the legacy IPv4 portion. This route would eliminate the risk of disrupting the end hosts, router, and switches to upgrade to IPv6 however IPv6 support is still largely experimental that seems difficult to get IPv6 deployed initially in an enterprise network.

Some country such as China will so desperately need addresses that it would deploy IPv6. However, this scenario raises a number of issues. To communicate with the rest of the existing Internet, China would require sufficient (global) IPv4 addresses in any case for NAT-based communication from its internal IPv6 to these IPv4 addresses. However, if it has these addresses, it would be far easier to run the whole country behind a NAT boundary using IPv4 addresses, given that would allow the use of existing routers, switches and host software. It seems inadvisable for a country with limited Internet expertise and industry to commit to the least proven technology and possibly be forced to largely develop its own products, especially with uncertain prospects of other markets for these products. IPv6 introduces a privacy risk because it encodes information in the addresses, making this information externally visible. For instance, with IPv6, one can determine a company's ISP based on the addresses used by its hosts. IPv6 also makes every host that uses multiple ISPs effectively multi-homed. IPv6 addresses can also encode MAC addresses that can reveal the manufacturers of the Ethernet interfaces in the hosts. These issues have already caught the attention of privacy groups. IPv6 disallows fragmentation at intermediate hops, making it even more difficult to use multicast efficiently in a highly diverse environment. Some networks impose fragmentation on large packets to provide delay guarantees for latency-sensitive traffic. This fragmentation may only come into play when such applications are running. It seems inappropriate to force a small MTU on a distant multicast source, for all receivers, just because a local low bandwidth link is carrying voice, for instance.

6. AI3/SOI-ASIA NETWORK: AN IPV6-ONLY INFRASTRUCTURE

AI3/SOI-ASIA project under WIDE University has 27 partner universities among 13 Asian countries. The project was lunched aiming to contribute to higher education (online) with satellite based internet infrastructure. For autonomous operation of the project, each operator should be capable of maintaining the SOI-Asia environment in each partner site. Until the year 2007, all the applications that requires for online live classes are IPv6 enabled. Hence an IPv6-only network has been setup and lunched successfully after the operator's workshop in august.

7. CONCLUSION

By this paper, the prospects and problems of implementing IPv6 have been investigated. The issues of what IPv6 will contribute to the network, what is required for an upgrade and when this has to be done according to the complexity of IPv6 have been addressed. Information regarding problems of IPv4 and issues in IPv6 implementation has been analyzed almost depending on the internet and related RFCs of IETF. A study over different transition mechanisms have been performed by which it can be seen that tunneling/dual-stack mechanisms seems better approach for current IPv4 dominant network but NAT-PT will play dominant role when there will be IPv6 ocean. Gglobally, the upgrading process is at very different stages. Asia is the leading area, already offering commercial IPv6. SOI-ASIA project under WIDE university is the one successful to implement IPv6 only operation by its online education. World's almost all research agencies and ISPs are under rush to implement IPv6 but there are still difficulties for ISPs regarding the implementation due to the lack of end user motivation and application/hardware compatibilities. From IPv4 address exhaustion report and current status of IPv6 shows that the world must have IPv6 only network beyond 2030 which is depicted in figure below.

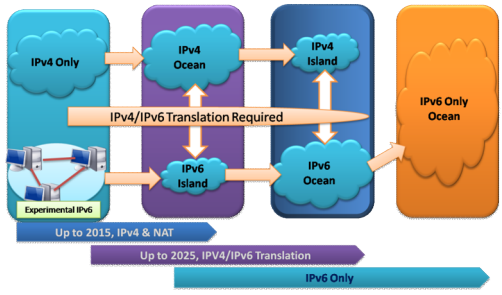

Figure 11 Projected IPv6-only Network Beyond 2030

ACKNOWLEDGEMENT

We would like to express our sincere thanks to AI3/SOI-ASIA project team for their full support to establish IPv6-only network in Center for Information Technology as a TU-RO Site. Our thanks goes to Nripa Dhoj Khadka, Purushottam Sigdel and CIT team for providing study over IPv6-only Network.

REFERENCES

[1] www.microsoft.com,"*Introduction to IPv6",* 2003, http://www.microsoft.com/windowsserver2003/technologies/ipv6/introipv6.mspx

[2] Sun Microsystems, *"IPv6 and the Future of the internet"*, a technical white paper, 1999

[3] S. Deering, *"Next steps for IPv6 standards",* Global IPv6 summit in Korea 2002, presentation I-1 http://www.ipv6.or.kr/summit/presentation/I-1.pdf

[4] Katsuyasu Toyama, *"SIGCOMM2007:IPv6 in Japan and future Deployment"*, IPv6 Panel Discussion, August 2007

[7] Achmad Husni Tamrin, SOI-ASIA global e-workshop, *"Internetworking with IPv6",* August 2006. http://www.soi.wide.ad.jp/soi-asia/ow/2006-summer/wstextbook/index.html

[8] Dale Geesey, *"Understanding IPv4 Address Exhaustion"* http://www.usipv6.com/6sense/2006/mar/pdf/UnderstandingIPv4AddressExhaustion.pdf

[9] Mae Wang, *"Tackling IPv6 Address Scalability from the Root",* SIGCOMM-2007 conference in Japan.

[10] Documentation by Visoottiviseth, "*TOTD operation & setup*" http://mucc.mahidol.ac.th/~ccvvs/totd-setup.html

[11] E. Nordmark, *"Stateless IP/ICMP Translation Algorithm (SIIT)"*, RFC2765, February 2000, (Proposed Standard)

[12] G. Tsirtsis, P. Srisuresh, *"Network Address Translation - Protocol Translation (NAT-PT)"*, RFC 2766, February 2000, (Proposed Standard)

AUTHOR'S PROFILE

Shashidhar Ram Joshi completed his Bachelor of Electrical Engineering from Sardar Ball avbhai 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, Pulchowk Campus, Nepal. His areas of research are Image Processing, Networking and Artificial Intelligence.

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. Currently, he is working as a System/Network Administrator at Center for Information Technology (CIT), IOE Pulchowk Campus. His area of interest is Networking, Distributed Computing and Data Mining.