Proposed Migration Approach to implement IPv6 Network over IPv4

JAWAD HUSSAIN AWAN[*1], RAZA HUSSAIN SHAH[1], SHAHZAD AHMED MEMON[1], MUHAMMAD JURIAL SANGI[2] AND RAHAT ALI KHAN[1]

[1]*Institute of Information and Communication Technology, University of Sindh, Jamshoro*
[2]*Mechanical Department, Mehran University of Engineering & Technology, Jamshoro*
**Corresponding Author's email: Jawad.awan@scholars.usindh.edu.pk*

Abstract

Modern field of edge computing is playing vital role in the development of services of cloud and distributed computing. Therefore, fast and reliable access is necessary for such systems, services and tools. The current study aims to implement Internet Protocol version6 (IPv6) network. It is observed that during upgrading or transforming a network from Internet Protocol version4 (IPv4) to IPv6, the proposed network becomes hybrid due to deployment of IPv4 and IPv6 networks. Further, this research supports and enhances the network compatibility between IPv4 to IPv6. Dual Stack and Tunneling mechanisms are also discussed in this study. Though, Dual stack is one of the most successful mechanism, which works in both networks either it is IPV4 or IPV6 and defines a compatible platform and mechanism to run them in a single mode. It is observed that Tunneling is a reliable and protected mechanism in comparison with different transition methods. Although, it is not appropriate for home users but suitable for Data centres. Moreover, the pools of IPv6 addresses are successfully being deployed at five departments in Campus Area Network (CAN). The author has also discussed a design and specification model, which includes the mechanism of transformation of IPv4 to IPv6 and IPv6 addressing schemes. This paper proposed Dual Stacking Transition Mechanism (DSTM) and 6 to4 Tunneling transition mechanisms for transform of IPv4 to IPv6 transition.

***Keywords**:* IPv4, IPv6, Cisco, Dual Stack, Tunneling, Networking

INTRODUCTION

Internet connectivity is as old as communication [1]. With the passage of time, the communication has widen by providing vigorous, interoperable, and reliable performance. The evolution of technology demands up gradation, advancement and development into communication systems. In this way, IPv6 becomes vital protocol for communication as compared to IPv4. This protocol has various advanced features such as Quality of Service (QoS). However, it has introduced security issues such as inherited attacks of IPv4 and transition threats as discussed in [2]. This digital wireless communication age has evolved in terms of scale and services very rapidly; and now its growth has reached to its limit, as there are no more IPv4 addresses in the world. Therefore, to solve this problem, the IETF (Internet Engineering Task Force) designed the latest extensive version of Internet Protocol with more address space, called as IPv6. It is also called IPng (Internet Protocol Next Generation). IPv6 is an enhanced and successor version of network layer protocol of IPv4 and resolves the problems of IPv4. But, IPv6 faces the backward-compatibility issue with IPv4. These issues led the existing internet (which is based on IPv4) to completely switch to Internet 2 (based on IPv6). Hence, it has become crucial for every organization to implement new generation of Internet Protocol. Since 2010, all public and private networks have started to shift to internet2. Correspondingly, CAN for smart university is experiencing the same global issue of technology-shift, therefore, it needs to hook up with internet2 for implementing IPv6. In this context, this research aims to provide the solutions of IP address exhaustion and global technology-shift problem (IPv4-to-IPv6 change). It also aims to help in better network infrastructure management; with more reliability, and more security. Transformation, up gradation and evolution of technology is complex, because these require higher budget and skilled personnel to maintain, supervise and control, otherwise it requires a training for existing employees. The whole process deploys various techniques, approaches and tools for communication. Further, few mechanisms support co-existence between IPv4 and IPv6 such as DSTM while other like 6 to 4 Point-to-Point Tunneling allows IPv6 packets over existing IPv4 networks. This research covers both transition techniques. The evolution and improvement in technology growth demands better Internet access address solutions. So, it supports the deployment of IPv6 in cyber age. Initial step towards deployment of IPv6 is an advanced version of IPv4 and transforms the transition of internet, which is a huge task for a team to build and maintain across the world. The whole process takes several years [1]. Therefore, co-existence mechanism is proposed as a meaningful choice for internet deployment. The main theme of this research is to achieve the parameters such as deployment of IPv6 on CAN, provision of IPv4 and IPv6 co-existence CAN and provision of IPv6-to-IPv6 communication over IPv4 networks. Although, smart phones also demand better QoS while these devices lack the capability to make changes from voice-centric to multimedia-centric. Software Defined Networking (SDN) is a dynamic and flexible architecture, which tackles and solves routing and handoff problems. The unique nature of SDN has attracted the researcher's attention pertaining to enhance the QoS in mobile computing [3].

BACKGROUND

IP Protocol is an essential communication protocol, which is used to connect different nodes in a system. IPv6 is a widespread solution for internet access, and deploys ever-expanding schema of supplementary users, devices and traffic services [4]. More than 200 million modern Internet services are offered every year and those services are used by 7.6 billion internet users approximately. All of these services are covered by IP protocol [5,6].

IPV4 ADDRESS EXHAUSTION

In 2011, IANA (Internet Assigned Numbers Authority) transferred the rights of last address blocks to the RIRs (Regional Internet Registry). Since then, there is no more IP address for any RIR. The unallocated pool of IPv4 addresses has become utterly emptied. This task was carried out on 3rd Feb 2011, which is a critical point in the domain of Internet. It reached to the allocation of the left over IPv4 addresses from a fundamental pool of IANA. After that task, IANA was unable to provide new addresses to any of five RIRs. The APNIC

(Asia-Pacific Network Information Centre) fatigued its broad use of IPv4 address pool in 2011. To overcome this IP address exhaustion, IETF planned to restructure the IPv4 addresses, and designed new addressing style termed as Variable Length Subnet Mask (VLSM).

VARIABLE LENGTH SUBNET MASK (VLSM)

VLSMs is an additional subnet mask network, which is assigned to a network by IP, and considers it VLSM embedded network due to the extensive network statistics having different lengths at every subnet making level. As VLSM solved the issue of IP address exhaustion, on the other side it has created another issue that is: it leads the overflow in the global routing tables of core routers at backbone networks caused by increased number of subnets created with VLSM as a solution to address exhaustion. Again, to solve this issue another technique was created that is Classless Inter-Domain Routing (CIDR).

CLASSLESS INTER-DOMAIN ROUTING (CIDR)

CIDR is also called supernetting. It is an effective mechanism to overcome the problems of IPv4 exhaustion as well as it supports to route table overflow. The main advantage of CIDR is to permit route aggregation or route summarization of multiple subnet masks by supernetting the subnets. This approach significantly decreases the routing information at the fundamental level of backbone. CIDR is an efficient technique to impede the IP address allocation flood and routing table overflow [7]. The internet systems which were developed in 1994 and 1995 lacks CIDR.

NETWORK ADDRESS TRANSLATION (NAT)

NAT is an efficient and fundamental routing function and its function is to translate network addresses from one network to another. Port Address Translation (PAT) has importance over NAT technology, because PAT can translate various IP addresses into another one. NAT Breaks IP’s End-to-End Model, Applications Problems with NAT, Security Problems with NAT and Address Space Collision are emerging challenges to NAT [8]. Renumbering or twice the NAT approach is a solution of above-mentioned issues. However, these approaches are expensive and increase the complexness of NAT.

Problem Statement

The present international share of IPv6 is low in the development and implementation phases during promotion. The research community has urged the requirements to understand the reasons regarding slowness of transition in adaptation of IPv6. In addition, it is also unknown that which factors may be used to migrate from IPv4 to IPv6. To overcome these issues, the author proposed a design and specification model, which includes the mechanism of transformation of IPv4 to IPv6, IPv6 addressing schemes, Dual Stacking Transition Mechanism (DSTM) and 6 to 4 Tunneling transition mechanisms.

Proposed Approach to Migrate from IPv4 to IPv6

We proposed the designing approach to adopt IPv6 instead of IPv4 to improve the communication traffic among networks. In addition, this section includes tools & techniques, specification & design and IPv6 addressing schemes.

Tools and Techniques

This section comprises of tools, Cisco IOS, and IPv4 to IPv6 transition techniques. It also contains sub sections to develop a IPv6 based network to solve IPv4 related issues.

Tools

University of Sindh Campus Network is providing Dynamic Host Addressing, Domain Name Service, Web Server and some other services. These network services are used as supporting tool for this research.

CISCO IOS

Cisco Internetwork Operating System (IOS) is a network support program, which is used in Cisco Systems, network routers and network switches [9]. IOS is a complete package that includes routing, switching, and internetworking functions. These all functions are integrated in a real time operating system.

The specification for the proposed research requires CISCO Systems Vendor, IOS Software, 12.3 major release with 12.3(26) release number, 2501-2525 platform, IP plus as feature set and c25000-is-l.123.26.bin as image name. 16 MB Dynamic Random Access Memory (DRAM) and Flash are minimum requirements while the proposed research includes Authentication, Authorization, and Accounting (AAA), Access Control List (ACL), Address Resolution Protocol (ARP), Asynchronous Transfer Mode (ATM), Border Gateway Protocol (BGP), Cisco Discovery Protocol (CDP), Dynamic Host Configuration Protocol (DHCP), Domain Name Servers (DNS), Enhanced Interior Gateway Routing Protocol (EIGRP), Frame Relay, File Transfer Protocol (FTP), Hyper Text Transfer Protocol (HTTP) Web Server, HTTP Security, Internet Protocol Service Level Agreements (IP SLAs), Internet Protocol Security (IPSec), Internet Protocol Version 6 (IPv6), Integrated Services Digital Network (ISDN), Layer 2 Forwarding-Fast Switching, Quality of Service (QoS), Network Time Protocol (NTP), Next Hop Resolution Protocol (NHRP), Open Shortest Path First (OSPF), Password Authentication Protocol (PAP), Protocol-Independent Multicast (PIM) Version 1, PIM Version 2, Policy-Based Routing (PBR), Point to Point Protocol (PPP), RADIUS, Response Time Reporter (RTR), Routing Information Protocol (RIP), Resource Reservation Protocol (RSVP), Real-Time Transport Protocol (RTP), Simple Network Management Protocol (SNMP), Spanning Tree Protocol (STP), Virtual Private Dial-up Network (VPDN) and X.25 [10].

IPv4-TO-IPv6 TRANSITION TECHNIQUES

IPv6 is an advanced or successive version of IPv4. Thus, IPv6 is not "backward-compatible". Moreover, Back-ward compatibility allows gradually transition, that's why IPv6 is regarded as an abundant functional alternative for IPv4. So, the recent devices and networking tools deploy IPv6 in communication networks. IPv4 and IPv6 both are divergent and dissimilar communication protocols.

The inference of this compatibility and failure to work as automated translator, this practice maintains inclusive any-to-any connectivity in the transition process, each device is deployed to perform a transition with IPv4 and IPv6 protocol stacks. This approach allows the device to be "bilingual," and intermediate between IPv4 and IPv6 to provide effective communication. The whole transition process is termed as dual-stack transition. In this research, following two transitions are proposed to transform the IPv4-IPv6 transition:

- DSTM
- 6 to 4 Tunneling

DSTM

DSTM is a basic and fundamental technique of migration strategy. This approach allows both IPv4 or IPv6 tools and equipment to communicate in both modes. Dual stacking upgrades the system or network devices and programs on the network once. Thus, it becomes easy for use and deployment. Moreover, all connected or associated hosts and devices require to be upgraded [11]. Normally, all communication prefers successive version, and improves their internet access. The implementation of DSTM is as shown in Figure 1 and Figure 2.

6 to 4 Tunneling

6 to 4 tunneling are also interesting and supportive mechanism to carry IPv6 data over an existing or IPv4 compatible network. It is relatively achievable to have IPv6 subnets, and allows all networks to communicate with each other. It is not complicated but require a Wide Area Network (WAN) for this mechanism [12]. In this approach, the host or node devices are connected in IPv6 network with connected router. When it is connected to another router for communication it requires tunneling the IPv6 into IPv4 as shown in figure 1 where Physics and Chemistry departments are taken as an example to illustrate the implementation while complete architecture is illustrated in Figure 2.

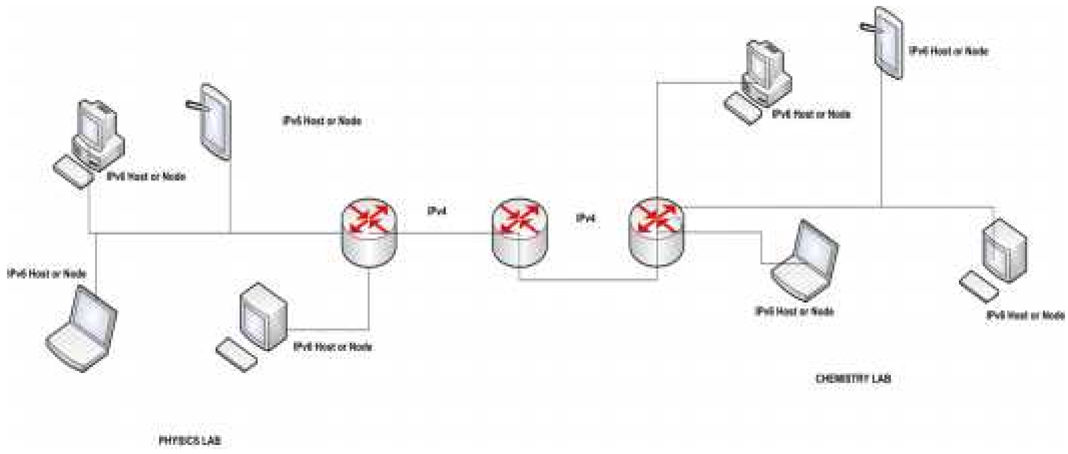

Figure 1 IPv6 to IPv4 Tunneling

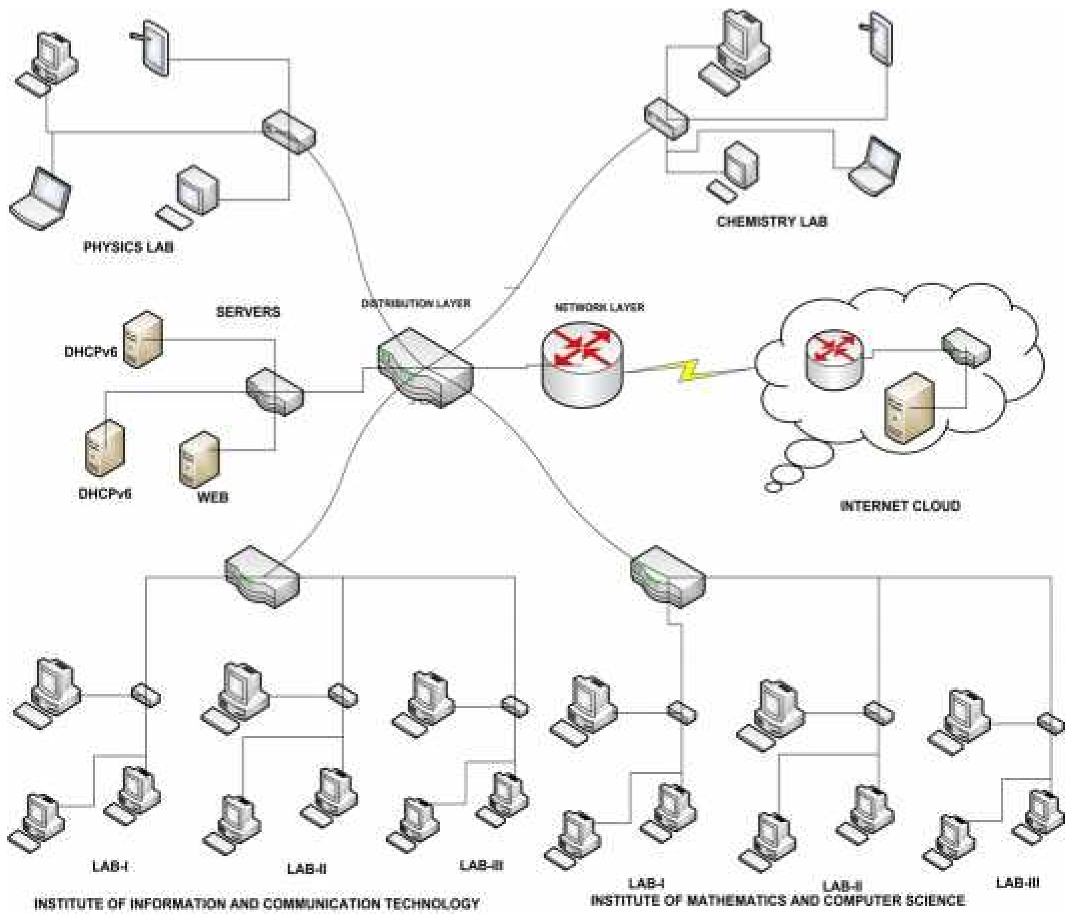

Figure 2: Overall Network Map of CAN

SPECIFICATION & DESIGN

This section includes CISCO three layer network model, core layer, distribution layer as explained below:

The CISCO Three-Layer Network Model

CISCO is a Network Company which defined three layered network model. This model is mostly preferred by network professionals for designing, implementation, and maintenance of a scalable, consistent, inexpensive network model. Core layer, distribution layer and access layer are main three layers of above mentioned model as shown in Figure 2. [13]. Above mentioned layers are logical instead of physical and each layer performs specific functionality. Physical implementations of this network requires devices to perform function either in a single or double layer. “Keep local traffic local” becomes a famous concept and phrase of networking principle due to the merit of the concept in discussion.

The Core Layer

The Core layer is central part and soul of the network. This layer is responsible to transport the hefty amounts of traffic data in an efficient and quickest manner. The main purpose of this layer is to toggle the traffic rapidly, while distribution layer process the user data and forwards the requests to the core if requested. Unfortunately, fault tolerance is a challenge for this layer. Following are the specifications of core layer.

- Design high reliability core.
- Routing information of Virtual Local Area Networks (VLANs), access lists, and filtration of packets take place.
- Usage of lower convergence protocols.

The Distribution Layer

The Distribution layer is the middleware and most important point between access layer and core layer. The key role of distribution layer is to provide the network information such as routing, filtering, and WAN/CAN access. Moreover, it determines the movement or exchange of packets from networks and can access the core, if desired. The implementation of the policies may take place in this layer for the network.

The Distribution layer includes following mechanism or procedures to achieve reliable and requested results.

- Implementation of tools like access lists, filtration of packets, and creating queues.
- Adoption of some security and network policies such as firewall, and address translation.
- Redistribution of routing between static and dynamic routing protocols.
- Routing of data between VLANs.

The Access Layer

This layer monitors the network resources, access controls of user and workgroup. It is also referred as the desktop layer. The network resources are defined and provided at local level as users get access of them easily. Some functions are defined as under:

- Data flow starts from distribution layer to get access control and enforce policies.
- Segmentation takes place to create separate collision domains.
- Connecting workgroup with distribution layer.

IPV6 ADDRESSING SCHEME

In this section, multiple scenarios of CAN are taken and the results of University of Sindh are used as sample. Every department is allocated a separate pool of IPv6 addresses and one pool for Network Operation Centre (NOC). The below mentioned address schemes are allocated to different departments on testing purpose. Therefore, there is not any fixed limit for start and end schemes while tested addressing schemes are discussed in the following Table 1. For practical use IPv6 chart is available for usage [14].

Table 1: Address Allocation Details of different IPv6 Pools

Location	IPv6 Pools no.	Network	Prefix Length	Starting IPv6	Ending IPv6
IICT	11	**2001:DB8:0:11::**	64	2001:DB8:0:11::	2001:DB8:0:11:FFFF:FFFF:FFFF:FFFF
IMCS	22	**2001:DB8:0:22::**	64	2001:DB8:0:22::	2001:DB8:0:22:FFFF:FFFF:FFFF:FFFF
Chemistry	33	**2001:DB8:0:33::**	64	2001:DB8:0:33::	2001:DB8:0:33:FFFF:FFFF:FFFF:FFFF
Physics	44	**2001:DB8:0:44::**	64	2001:DB8:0:44::	2001:DB8:0:44:FFFF:FFFF:FFFF:FFFF
NOC	100	**2001:DB8:0:100::**	64	2001:DB8:0:100::	2001:DB8:0:100:FFFF:FFFF:FFFF:FFFF

CONCLUSION

IPv6 is an extended and successive version of Internet Protocol. It became evident due to rapid growth of the Internet technology that supplementary addresses would be required to connect devices as compared to IPv4 address space. This advancement introduced modern features and functionalities in the network technology to overcome the limitations of IPv4. The grouping arrangement of CIDR and NAT support the network as the collapse time of IPv4 address may lessen. Although, the NAT mechanism splits the end nodes of Internet Protocol model, that’s why it has limitations for protocols. In migration stage of technology, transition mechanism is one of the best solution which provides compatible platform to run a network of IPv6 with same infrastructure of IPv4 networks. Moreover, other mechanism and approaches have been developed and designed as per request in organizations. This paper has discussed two mechanisms: Dual Stack and 6 to 4

Tunneling. These mechanisms have distinct features in their defined Infrastructure. Dual Stack transition is most preferable mechanism in networking and communication. It is also appropriate for Internet Service Providers (ISPs), home users and enterprise network users. Tunneling is a reliable and protected mechanism in comparison with different transition methods. Similarly, it is not appropriate for home users but suitable for Data centres. At last, it is concluded that the transition methods accomplish and resolve the issues of potential network development and require selection as per infrastructure requirement. With the evolution of technology, the communication has widened and has come across interoperable, and reliable performance issues. Thus, IPv6 is used to cover these issues instead of IPv4. This persistent research can attract the attention of researcher and academicians to provide QoS, security and flexible network.

ACKNOWLEDGMENT

We are thankful to the Director, Institute of Information & Communication Technology, University of Sindh, Jamshoro, Pakistan for providing Information Technology laboratory and digital library access facility to accomplish this research work.

REFERENCES

[1] Huston, G., "A Rough Guide to Address Exhaustion," The Internet Protocol Journal, vol. 14, no. 1, pp. 2-11, Indiana, USA, 2011 [Online]. Available: https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-51/141-address.html

[2] Internet World Statistics, "Top 20 countries with the highest number of internet users," Miniwatts Marketing Group, Sayre, Africa, 2017.

[3] Amoss, J.J., and Minoli, D., Handbook of IPv4 to IPv6 Transition, Methodologies for Institutional and Corporate Networks, New York: Auerbach, 2007.

[4] Bruno, A., and Ciesielczyk, J. M., "Method and system for gateway selection in inter-region communication on IP networks". US Patent US20070011351A1, Jan 11, 2007.

[5] Barayuga, V. J. D. , and Yu, W. E. S., "Packet Level TCP Performance of NAT44, NAT64 and IPv6 Using Iperf in the Context of IPv6 Migration," in *5th Int. Conf. IT Convergence and Security (ICITCS),* Kuala Lumpur, Malaysia, 2015.

[6] Desmeules, R., Cisco Self-Study: Implementing Cisco IPv6 Networks (IPv6), Cisco Press, Indiana, USA, 2003.

[7] Fairhurst, G., and Jones, T., "Transport Features of the User Datagram Protocol (UDP)," Internet Society and The Internet Engineering, University of Aberdeen, Aberdeen, UK, 2018.

[8] Tahir, H.M *et al.*, "Implementation of IPv4 Over IPv6 using Dual Stack Transition Mechanism (DSTM) on 6iNet," in *2nd Int. Conf. Information Communication Technologies*, Damascus, Syria, 2006.

[9] Al-Azzawy, D. S. and Neamah, M. R., "Comparative Analysis Study on Network Performance of VoIP and Data Traffic Pattern using Queuing Algorithms in Wired Network Environment: An Implementation using OMNeT++ Simulator," *Ind. J. Sci. Technol.*, vol. 10, no. 36, September 2017.

[10] McMillan, T., *Cisco Networking Essentials*, Wiley, Canada, August, 2015.

[11] RIPE Network Coordination Centre, "IPv6 chart," RIPE NCC, Amsterdam, 2015.

[12] Tsetsi, E., and Rains, S. A., "Smartphone Internet access and use: Extending the digital divide and usage gap," *Mobile Media Commun.*, vol. 5, no. 3, pp. 239 - 255, London, UK, 2017.

[13] Shiranzaei, A., and Khan, R. Z., "IPv6 Security Issues—A Systematic Review," in *Advances in Intelligent Systems and Computing*, D. Lobiyal *et al.*, Eds. vol. 638, pp. 41-49, Springer, Singapore, 2018.

[14] Yap, K. L., and Chong, Y. W., "Software-Defined Networking Techniques to Improve Mobile Network Connectivity: Technical Review," IETE Technical Review, pp. 1-13, London, UK 2017.