Abstract

Internet Protocol (IP) is the ubiquitous internetworking protocol that drives the internet and world business communication channel today. The protocol permits millions of users to communicate and share information over the World Wide Web. Originally conceived in 1974 by Vinton G Cerf and Robert E Kahn, Internet Protocol Version 4 (IPv4) which was developed almost three decades ago is the mostly pervasive protocol version in use today. However, with the expeditious and exponential growth of internet and increase in number of connected devices, we are facing a scenario where IPv4 addresses are potentially exhausted. The IPv4 extensions such as NAT, CIDR and Subnetting etc are merely limited short-term solutions. Moreover the scalability and security features that are required by the modern Internet can't be fulfilled by IPv4. The long term solution to these problems is a step-by-step, phased but complete migration to IPv6. While IPv4 address space can hold billions of addresses, IPv6, which is the next version of the protocol, has provided trillions of addresses which are potentially inexhaustible. Thus evolution of new version of protocol i.e. IPv6 seems to be a flawless replacement choice for IPv4.

However migration to IPv6 cannot be overnight due to prodigious installed network infrastructure base of IPv4.There needs to be seamless integration and co-existence between the two protocols for quite some time till migration process completes.IPv6 transition is not a transparent process for the layers above IP. Changing the protocol requires remodeling the existing data structures that have embedded IP addresses. Also API's supporting IPv4 need to be altered. In general legacy protocols like NAT, DHCP, ICMP and PPP which were written keeping IPv4 in mind will also undergo change. This change will harbor security vulnerabilities also. Thus to support IPv6, the existing protocols should either be modified or re-oriented. These changes are significant to internet because not only the software (operating systems, application programs) but also hardware needs to be enhanced at TCP/IP layers. Also, the migration techniques will introduce performance bottlenecks which are significant in the transfer of data packets and will slow down the network performance. In the near future, internet will transform into a large cluster of non-homogeneous protocols operating in a dual IPv6/IPv4 environment for a long period of time.

In this thesis, an attempt has been made analytically as well as empirically to analyze and address the above IPv4/IPv6 migration issues and carry out an in-depth investigation of the deployment and security issues of the next generation internet protocol IPv6.

In the first chapter, an attempt has been made to throw light on introduction to IPv6 and Migration Techniques with the motivation for taking the topic. The chapter outlines the objectives of the research and also reports the contribution made by the author during the course of study.

In the initial part of this research work, we examine the reasons for migrating to IPv6.The migration involves challenges (both technical and non technical) which need to be addressed. We also establish guidelines or benchmarks for IP migration.

For seamless integration and co-existence between the two non-homogeneous protocols, the migration techniques need to be optimized and correctly deployed so that internet downtime doesn't occur which may lead to performance and QoS degradation. In this research work, we have empirically carried out implementation of existing migration techniques using OPNET Modeller Simulation. Based on the calculated parameters, an approach has been made towards finding better technique among the existing migration techniques. The experiment helps us in solving the problem of choosing best IPv6 migration technique.

Talking about the migration from IPv4 to IPv6, one thing that automatically comes to our mind is the security aspects of the internet migration. The security of the previous version of IP i.e. IPv4 has been tested over the years, but in case of IPv6, we are still naive about the security vulnerabilities. The migration to next version of IP will certainly introduce security leaks and will have impact on performance. In this thesis, we also carry out in-depth analysis of the security aspects of IPv6 and Internet migration. We empirically evaluate the Internet Protocol Security (IPSec) protocol which was introduced later in IPv4 as a security measure and as an extension option in IPv6.The main purpose is to study its impact on performance in IP and migration networks.

Since IPSec is incompatible with NAT and also has bootstrap problems (i.e. IKE entails for a working IP stack) in IPv6 Neighbor Discovery Protocol (NDP); Secure Neighbor Discovery Protocol (SEND) was introduced to secure IPv6 link layer operations. Despite its innumerable tangible benefits, SEND faces major challenges including intense computation, vast implementation, deployment and security issues. Cryptographically generated address (CGA)

which is an important innate component of SEND protocol find their application in proving address ownership and prevents spoofing or theft of IPv6 addresses by binding senders public key with the generated address. Though CGA is a promising technique and offers substantial amount of security, it does possess some limitations and performance bottlenecks. CGA is computationally intensive determined by the security parameter ‘sec’ and bandwidth gobbling due to use of RSA keys. For a higher value of sec, there is no guarantee on termination of brute force search for modifier. This thesis evaluates the performance and discusses certain techniques that can be used in optimizing the use of IPv6 CGA. These techniques are implemented in proposed model and then compared with the standard CGA Results show that by incorporating certain changes, optimization of standard CGA is possible.

Although CGA provides for message integrity, authentication and mitigating address impersonation, the process harbors DoS attacks in IPv6 Stateless Address Auto Configuration (SLAAC) and some privacy limitations. In the last part of the thesis, we have proposed a novel technique for address generation having a minimal computation cost as compared to CGA. The technique generates a highly randomized Interface Identifier that helps maintain nodes privacy and allows the nodes to ascertain the uniqueness on the link. It also provides robust security against Denial of Service (DoS) attacks during the Duplicate Address Detection (DAD) process of SLAAC.