Chapter 1

Introduction

1.1 Introduction

The Internet since its genesis in 1970's has already become a global broadcasting potential for information dissemination, and a channel for information collaboration and interface between disparate users and their systems separated by large geographical locations. The rate of growth of interconnected devices has been on exponential scale from the last decade. As of now, more than 5 billion devices are accessing the Internet. According to Cisco, the number of interconnected devices will double the world population (approximately 14 billion devices) by the year 2015 (Cisco,2012).The Internet Protocol Version 4 (IPv4) which is a three decade old standard internetworking protocol using 32 bit address space fails to cater such a large number of hosts. In Feb 2011, Internet Assigned Numbers Authority (IANA) which has been assigned the task of allocating IP addresses to Regional Internet Registries (RIR) exhausted the central pool of IPv4 addresses completely (Levin & Schmidt, 2014). This rapid depletion of IP addresses was inevitable as large number of devices are getting connected to internet. Also inefficient utilization and remiss planning of IP address space acted as catalyst in the process of depletion (Shah & Parvez, 2014).The temporary IPv4 patches 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 protracted solution to these problems is a step-by-step, phased but unabridged migration to IPv6. The next version of the internet protocol IPv6 provides an address space of 2^{128} i.e. trillions of addresses making the IP address space potentially inexhaustible. Thus adopting IPv6 makes a paragon choice of replacement for IPv4.

The transitioning from IPv4 to IPv6 cannot be achieved instantaneously due to compatibility and interoperability issues relating to IPv4.The Internet Protocol version 6 (IPv6) is not backward compatible with IPv4 due to different header structure.

According to (Govil et al, 2008)

> *The migration between two irreconcilable heterogeneous protocols i.e. IPv4 to IPv6 will be an elongated process and it is rather impossible to transpose the entire internet over to IPv6 over night. IPv6 is not backward compatible with IPv4.Also IPv4 hosts and*

routers will not be able to directly handle IPv6 traffic and vice-versa. As IPv4 and IPv6 will co-exist for a long time, this requires the transition and inter-operation mechanisms.

The daunting task of migration is overburdened by the enormous size and complexity of the internet. The Next Generation Transition Group (NGTrans) proposed three main transition mechanisms that included Dual stack, Tunneling, and Translation (Shah & Parvez, 2014) for seamless migration to IPv6.These transitions mechanisms allow the IPv4 to co-exist with IPv6 for a substantial amount of time during the migration process. However the migration techniques actually do not break down the issues that are related with network migration. The economic considerations and infrastructural issues also play a major role in drafting policies and overall resolution. The major roadblocks impacting migration include incompatibility between hardware and software, issues with left over legacy IPv4 applications, limited user experience with IPv6 and hesitation to accept new protocol and uncertainty about business returns on investment (Waddington & Chang,2002).The migration and adoption to IPv6 instantiates corresponding rise in malicious traffic that is routed using IPv6.The reason being that previous version i.e. IPv4 has been tested over the years whereas we are still naive about the security aspects of the next generation internet protocol IPv6. Also the firewall configurations detecting malicious IPv6 traffic are not as well documented, configured, and deployed as their IPv4 counterparts. The Internet Control Message Protocol version 6 (ICMPv6) opens up new vulnerabilities in IPv6 that do not exist in IPv4.For IPv6 services to function properly,ICMPv6 message traffic must be allowed to pass firewalls which can be used to leverage DoS attacks on networks. Since some systems use IPv4-IPv6 tunneling technologies, it does not take a great deal of effort for a malicious entity to inject malicious traffic if they know which routers are being used to tunnel IPv6 traffic over an IPv4 network. Until the time complete migration to IPv6 takes place, the internet migration techniques need to be secured. If left unprotected, these techniques pose a serious threat to networks (Bradner, 2006).

1.2 Motivation

The adoption of next generation internet protocol IPv6 is mushrooming and has been on exponential scale since the last decade (Google, 2015).The transition mechanisms are only seen as short term interim measures for interoperability between IPv4 and IPv6.However till

migration phase completes, networks need to be optimized and secured. The users cannot tolerate internet downtime and reliability of the network. The operation of transition mechanism will act as bridge between two heterogeneous protocols but at the same time will introduce performance bottlenecks. For example; tunneling mechanism suffers from encapsulation and decapsulation delays, dual stacks require higher computational and processing power among the nodes. Also it's anticipated that the next generation internet protocol (IPng) will introduce vulnerabilities in addition to those inherent in IPv4. While the existing security infrastructure like IPSec, SSL, PKI, and DNSSec might be sufficient for IPv4, the protocol security associated with IPv6 and migration networks needs to be assessed and analyzed (Ford,2005). Thus more studies and investigation needs to be carried out for studying the behavior of IPv6 and Migration networks.

1.3 Objectives

The main objective of this research is to analytically as well as empirically analyze and address the IPv4/IPv6 migration issues and carry out an in-depth investigation of the deployment and security issues of the next generation internet protocol IPv6. The objectives of this research work are as under:

1. An attempt will be made to review and study the Next Generation Internet Protocol IPv6. We will discuss about the need to migrate to IPv6 and study of challenges (technical/non technical) to migration will also be presented. We will present some guidelines that need to be taken care of while migration and will have an overview of overall deployment of IPv6 in the world.
2. An attempt will be made to Review and provide Comparative Analysis of IPv4 to IPv6 Migration Techniques. Also, we will carry out implementation of existing migration techniques using OPNET Modeller simulation and calculate the performance parameters. Based on the calculated parameters, an approach towards finding better among the Migration techniques will be presented.
3. We will carry an extensive study of security issues related to Migration and will evaluate security of next generation Internet Protocol (IPv6). Using simulation; we will carry out

an empirical investigation of the parameters that are affected by implementation of IPSec in IPv6 and Migration Networks.

4. We will survey the Link Layer Security of IPv6. Analysis of SEND protocol will be carried out and an attempt will be made to optimize and enhance the IPv6 Cryptographically Generated Address in Secure Neighbor Discovery Protocol.
5. Lastly, we will explicate discussion over the IPv6 Stateless Address Auto configuration Mechanism and explain the problems associated with it. An attempt to study the various attacks like DoS on IPv6 DAD, Man-in-the-Middle etc on SLAAC in IPv6 Neighbor Discovery Protocol and to find out alternate ways and techniques to mitigate the attacks will be presented.

1.4 Contributions

The contributions that we have made during this research work are as under:

1. An attempt has been made to review and study the Next Generation Internet Protocol IPv6. We have discussed about the need to migrate to IPv6 and studied various challenges (technical/non technical) to migration .We have also presented some guidelines that need to be taken care of while migration. Also we have given an overview of overall deployment of IPv6 in the world.
2. We have Reviewed and provided Comparative Analysis of IPv4 to IPv6 Migration Techniques. Also, we have carried out implementation of existing migration techniques using OPNET Modeller simulation and calculated the performance parameters. Based on the calculated parameters, an approach has been made towards finding better among all the Migration techniques.
3. An extensive study of security issues and attacks related to IPv6 and IP Migration are presented. Using simulation; we have carried out an empirical investigation of the parameters that are affected by implementation of IPSec in IPv6 and Migration Networks.
4. An investigation of the IPv6 Link Layer security and SEND protocol has been carried out. An attempt has been made to optimize and enhance the IPv6 Cryptographically Generated Address in Secure Neighbor Discovery Protocol.

5. Lastly, we have explicated discussion over the IPv6 Stateless Address Auto configuration Mechanism and explained the problems associated with it. We have studied the various attacks like DoS on IPv6 DAD, Man-in-the-Middle etc on SLAAC in IPv6 Neighbor Discovery Protocol. We have proposed a new address generation technique that has a minimum computational cost and time complexity as compared to CGA. The technique maintains nodes privacy and is also secure against DoS attack during the Duplicate Address Detection phase. In particular, the technique is effective in mitigating duplicate addresses in local subnet.

1.5 Outline

Chapter two reviews and provides an insight into the Next Generation Internet Protocol IPv6. It also discusses about the need to migrate to IPv6 and presents various challenges (technical/non technical) to migration. The chapter also gives an overview of overall deployment of IPv6 in the world and provides guidelines to migration.

Chapter three reviews and provides Comparative Analysis of IPv4 to IPv6 Migration Techniques. It also empirically carries 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.

Chapter four carries out in-depth analysis of the security aspects of IPv6 and internet migration. The chapter empirically evaluates the IPSec protocol which was introduced later in IPv4 as a security measure and as an extension option in IPv6.The main purpose is to evaluate its impact on performance in IP and migration networks.

Chapter five carries an investigation of the IPv6 Link Layer security and SEND protocol. An attempt has been made to optimize and enhance the IPv6 Cryptographically Generated Address in Secure Neighbor Discovery Protocol. For comparative analysis, proposed model is then implemented and compared with the standard CGA.

Chapter six presents a novel technique for IPv6 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 DoS attacks during the DAD process of IPv6 SLAAC