Reviewed Study on Solutions for Migrating From IPv4 to IPv6

Manikant Singh[1]* Dr. Sreedhar Mayavan[2]

[1] Sr. Manager IT Security & Operational Excellence Professional

Abstract – 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.

Keywords – Ipv4, Ipv6

---------------------------------x---------------------------------

INTRODUCTION

The Internet has already become a global broadcasting potential for the distribution of information since its emergence in the 1970s, and a medium for information collaboration and interface between diverse users and their systems, separated by large geographical locations. The rate of growth of interconnected devices over the last decade has been on an exponential scale. There are more than 5 billion users using the Internet as of now. According to Cisco, by the year 2015 (Cisco, 2012), the number of interconnected devices will double the world population (about 14 billion devices). The Internet Protocol Version 4 (IPv4), a three-decade-old standard internetworking protocol using 32-bit address space, does not appeal to such a large number of hosts. The Internet Delegated Numbers Authority (IANA), which was assigned the task of assigning IP addresses to the Regional Internet Registry (RIR), completely exhausted the central pool of IPv4 addresses in Feb 2011. (Levin & Schmidt, 2014). As large numbers of devices are connected to the internet, this rapid depletion of IP addresses is inevitable. In the phase of depletion, wasteful usage and remiss preparation of IP address space has also served as a trigger (Shah & Parvez, 2014). Temporary IPv4 patches such as NAT, CIDR and Subnetting etc. are merely minimal short-term alternatives. In addition, IPv4 does not meet the scalability and security characteristics expected by the modern Internet. A step-by-step, phased yet unabridged migration to IPv6 is the protracted solution to these issues. The next version of the IPv6 internet protocol offers 2128 address space, i.e. trillions of addresses that make the space of the IP address theoretically inexhaustible. The adoption of IPv6 thus renders a substitute alternative for IPv4 a paragon. Due to compatibility and interoperability problems related to IPv4, the transition from IPv4 to IPv6 cannot be done instantaneously. Internet Protocol version 6 (IPv6) is not backward compatible with IPv4 due to different header structures.

According to (Govil et al, 2008)

The migration between two heterogeneous protocols which are irreconcilable, i.e. It would be an elongated process from IPv4 to IPv6 and it is very difficult to transpose the entire internet over night to IPv6. IPv6 is not IPv4 backward compatible. IPv4 hosts and routers would also not be able to handle

IPv6 traffic directly and vice versa, either. Since IPv4 and IPv6 can co-exist for a long time, this involves processes of transition and inter-operation.

The immense scale and scope of the internet is overburdening the overwhelming task of migration. Three key transition mechanisms, including Dual Stack, Tunneling, and Translation (Shah & Parvez, 2014) for smooth migration to IPv6, were proposed by the Next Generation Transition Group (NGTrans). These transition mechanisms allow IPv4 to co-exist with IPv6 for a significant amount of time during the migration process. The migration methods, however, do not necessarily break down the problems connected with network migration. In the drafting and ultimate resolution of policies, economic conditions and infrastructural problems also play a major role. Incompatibility between hardware and software, issues with left over legacy IPv4 applications, restricted IPv6 user interface and reluctance to embrace new protocols and confusion regarding business returns on investment are the key roadblocks affecting migration (Waddington & Chang, 2002). The migration and adoption to IPv6 shows a corresponding rise in malicious traffic that is redirected to us Over the years, IPv4 has been checked, although we are all naive about the security implications of the IPv6 Internet protocol of the next decade. The malicious IPv6 traffic detection firewall configurations are also not as well known, configured, and deployed as their IPv4 counterparts. Internet Control Message Protocol version 6 (ICMPv6) opens up new IPv6 vulnerabilities that do not exist in IPv4. In order for IPv6 services to operate properly, firewalls that can be used to exploit DoS attacks on networks must be allowed to transfer ICMPv6 message traffic. As some devices use IPv4-IPv6 tunnelling technologies, if they know which routers are being used to tunnel IPv6 traffic over an IPv4 network, it does not take a great deal of effort for a malicious party to insert malicious traffic. Before the full migration to IPv6 takes place, it is important to protect the Internet migration techniques. These approaches pose a significant threat to networks if left unprotected (Bradner, 2006).

Internet Protocol Version 6 (IPv6)

Version 6 (IPv6) of the Internet Protocol is the next version of the Internet Protocol designed to replace the existing IPv4 version. IPv6, also known as IP Next Generation IPng, was developed by IETF to take an evolutionary step forward after discovering that there was no new IP address space. IPv6 comes with a 128-bit address system and an address space of 2128 addresses (approximately 3.4 ⁇ 1038), enough to cover almost every wired computer on earth with a specific global address space (Dunn, 2002). Such a wide address space makes access to the internet for any computer and user in the world. It also removes the IPv6 use of NAT and increases network communication, stability and flexibility. IPv6's design goals were to accommodate broader address space, protocol protection and real-time multimedia transmission. IPSec support, unlike in IPv4 where it was optional, has become a mandatory requirement in IPv6. The payload identification (used in QoS) field in the IPv6 packet has been replaced with the Flow Mark field. It has eliminated the notion of fragmentation. Extension headers in IPv6 have substituted the checksum and the options. In addition, IPv6 does not need manual configuration or DHCP because the device is involved in automatic "stateless" configuration, one of IPv6's design objectives. Finally, the size of the packet header was also increased from 20 bytes in IPv4 to 40 bytes in IPv6 (Shah & Parvez,2014).

Technical Issues

It is a daunting process to migrate to IPv6 from IPv4 deployments. Network infrastructure, protection and data centers must be built and operated in such a way that both IPv4 and IPv6 are supported concurrently for the forward and upward transition to IPv6 (Shah & Parvez,2014). It is important to deal with a variety of difficulties and security concerns. For instance, if the configuration is not right, the network's security features are at risk. The configuration process must be carried out with extra caution. Also in IPv6, if there are routing loops or if the routing tables are not properly maintained because IPv6 routing protocols have not been checked as extensively as IPv4 routing protocols, it cannot be predicted how fast convergence can occur. Due to several IPv4 and IPv6 paths, the routers and backbone links are placed with additional burden due to which transactions may take longer to complete. It can become congested with the routers doing the conversion.

Due to multicast transfer, security problems including Distributed Denial of Service (DDoS) attacks are also possible in the transition process. The basic internet migration strategies as suggested by the IETF include the Dual Stack, Tunneling and Header Translation (Gilligan & Nordmark, 2000) Dual Stack Strategy for integration between IPv4 and IPv6, although it offers a migration workaround, but it also requires a large amount of memory to maintain two protocol stacks and two routing tables. The introduction of two protocol stacks also entails the use of high computing capacity in nodes, resulting in high infrastructure costs.

Tunneling suffers from the disadvantage of encapsulation and decapsulation of packet headers that can cause potential overhead processing. Since IPv6 is designed for faster processing, these migration step bottlenecks are unbearable. The technique of header translation is less stable and has possible defects. This technique is not favoured due to loss of information during translation. Thus, all the above-mentioned migration strategies have their own merits and demerits. You will find the comparative study of these approaches in (Govil et al, 2008). Protection has been the primary problem in the implementation of IPv6 (Dunmore, 2005).

Since IPSec and other built security protocols are supported for IPv4 and IPv6, these mechanisms are not enforced by all current IPv4 systems. In large scale deployment environments such as IPv4, the redesign or remodelling of these security architectures may be expensive. In the long term, the decision to deploy a new IPv6 architecture (where IPSec is mandatory) seems to be more strategic and efficient than integrating these capabilities into the IPv4 infrastructure (Parvez & Peer, 2012). Network administrators can, however, be unaware to malicious IPv6 traffic that has tunneled into their networks, because IPv6 implementation is brimming. Only external sections of tunneled datagram's are analyzed by the implemented security algorithms, which may be within allowed tolerance, but ignoring the data content within. If this traffic succeeds in encapsulating itself successfully at the other end of the tunnel inside the protected network, then it is likely to be very important because the safety security mechanism within a network itself is comparably poor (Dunmore, 2005). The deployment of IPSec in conjunction with IP translation mechanisms such as NATPT and TRT, including packet alteration, would make packets inaccurate (Waddington & Chang, 2002). It also interrupts the end-to-end security architecture of IPSec.

IPv6 DNS has been modified (Saurabh & Shilpa, 2011) and the new address format must be supported by a redesign of the TCP/IP protocol set. In RFC 2874, the IETF introduced a DNS specification for IPv6 named AAAA and A6 records. In addition to mapping IPv6 address prefixes to partial domain names, A6 records map 128 bit IPv6 addresses to domain names. The DNS server must therefore obtain an unabridged string of A6 records for resolving IPv6 addresses or addresses from domain names (Waddington & Chang, 2002). IPv6 has also modified routing protocols. Direct extensions of IPv4 routing protocols are most interior and exterior routing protocols.

The altered protocols include RIPv6, OSPFv6, IDRP, BGP4, DHCPv6, etc. Another problem impeding the adoption of IPv6 is interoperability between hardware and software. Windows 2003 and XP were in use during the early years of computing, which did not support IPv6 and thus prevented its deployment. To function with the latest IP protocol, these legacy operating systems require adaptations and modifications. Applications must also be ported in order to run over IPv6. If the application strictly segregates the application layer from the communication layer, this can be achieved easily. However, if complex middleware and customised application programming interfaces (APIs) are used by the application, it will be very difficult to port. Upgrading the programme can include recompiling it with various APIs. The problems of compatibility that may occur may be addressed later. In total, it can be claimed that only a small range of IPv6 protection resources, policies and skills are available in the current scenario. The rate of adoption is significantly influenced by the fact that a large percentage of network professionals may refuse to accept the new technology because of the phobia of disrupting existing services.

REVIEW OF LITERATURE

Ang Li, Maoke Chen, Yong Cui (2006) have Introduced another answer for steering IPv4 in IPv6 spine without express. The subtleties of the plan and potential arrangements are Illustrated in 3 states from the most straightforward to the muddled: A Basic plan for an Intra area climate, An Access network transition conspire and an Inter-space arrangement. They had likewise proposed another strategy of sending IPv4 traffic in IPv6-just spine is created.

Bilski.T.(2011) has introduced a study of tradeoffs identified with the basic transition time frame. Furthermore, there is a tradeoff between various essential security angles: privacy and accessibility. Expanding classification level may cause decline in accessibility level. The issues ought to be deliberately dissected, particularly in the dangerous period of juvenile, Dual-stack design trademark for IPv4/IPv6 transition period.

Marcelo Bagnulo, Alberto Garcia-Mertinez and Arturo Azcorra(2007) have depicted engineering for IPv6 portable host multi homing that empowers transport layer survivability through different disappointment modes. The proposed approach depends on the collaboration between the MIPv6 and the SHIM6 protocols. They have likewise introduced engineering for the arrangement of multi homing help to 4G portable hubs. Such design empowers the safeguarding of set up correspondence through blackouts. While these suspicions may remain constant for single-homed cell phones, it isn't the situation for multi homed portable hosts.

Altaher A., Ramadass S., Ali. A. (2011) have proposed a Dual Stack IPv4/IPv6 network proving ground for managing the assignment and usage of an Intelligent methodology for malware discovery in IPv6 networks. All the Equipments, Tools and Network are arranged and dependent on the genuine Implementation of a double stack IPv4/IPv6 network. With completely practical activity for taking care of fundamental transition between IPv6 customers over IPv4 networks, the double stack IPv4/IPv6 proving ground is reasonable for examining the malware recognition in genuine IPv6 networks. The trial results from the testing stage shows the proficiency and the usefulness of the double stack IPv4/IPv6 Test bed.

Nathan Robinson, Cesar Ramos P.E., and Jose Luis Jara (2005) have talked about a portion of the transition systems created to encourage migration from the almost omnipresent IPv4/IPv6. The particular points of interest and the challenges of the significant systems were introduced close by of a clarification of the fundamentals of each transition plot. The significant awards of IPv6 will be found in usage, for example, 1. Cost decreases from expanded proficiency and diminished unpredictability. I. Estimation of far off access and progressively cell phones or potentially benefits. ii. Development in correspondences, applications and online items and additionally benefits. iii. Cost decreases coming about because of improved security, start to finish and shared correspondences.

Romanyasinovskyy, Alexander L., Wijesinha R, Amesh Karn (2010) have directed a Research work to assess VoIP execution with IPSec in IPv4, IPv6 and 6 to 4 networks, and furthermore utilizing Teredo for NAT crossing in a test LAN. The analyses have utilized delicate telephones to settle on decisions and generated back ground traffic to make clog on the connections and switches. The outcomes exhibited the plausibility of utilizing a solitary Linux box to deal with IPSec, 6 to 4 and NAT handling.

D. Shalini Punithavathani, K. Sankaranarayana (2009) have tended to the presentation of the different Tunneling transition systems utilized in various networks. The impact of these components on the exhibition of start to finish applications is investigated utilizing measurements, for example, Transmission Latency, Throughput, CPU usage and Packet misfortune rate. They likewise estimated distinctive execution measurements, for example, Latency and Throughput of the IPv6/IPv4 system. These are superior to those of the Configured Tunnel constantly intermediary instruments and the IPv6/IPv4 system that should work much harder(greater overhead) for every bundle sent and it should in this manner run at a higher CPU Utilization of the edge switch. The Larger bundles had kept up higher parcel misfortune rates, for all the Three Tunneling Mechanisms.

Xiaoming Zhou, Martin Jacobs child et. al. (2007) dissected in excess of 600 start to finish IPv6 ways between 26 test boxes of RIPE Network coordination focus more than two years and look at the deferral and misfortune execution after some time with their IPv4 partners. They have introduced and examined the estimation approachs and show that IPv6 ways have a higher postponement and misfortune than their IPv4 partner passages to deliver an extra overhead in the parcel size and handling the time on entryway.

WanmingLuo, Baoping Yan, Xiaodong Li and Wei Mao (2008) have introduced insightful models to research the adaptation to internal failure issue of their different methodologies. Their Research work gave rules and experiences into plan, execution and design of the IPv4/IPv6 interpreter. IPv6 is another variant convention for cutting edge Internet, which has the upsides of supporting versatility, portability and security better than current IPv4 Internet. The challenges of this work lie in three regions: I. Viable utilization of network processor assets. ii. Plan and usage of a high level control plane on a commodity OS, iii. Adaptation to non-critical failure to improve dependability of the entire framework.

CONCLUSION

IPv6 and Internet Migration is today's dynamic, complicated problem that needs time and large-scale resource commitment. The IPv4 exhaustion solution has yet to be conceived by companies as a difficult issue, placing themselves at risk of inadequate time and economic capital. Infrastructural migration costs (software up gradation, hardware costs, staff preparation and network testing), ambivalent network efficiency of the new protocol and possible security problems that may occur during implementation are the key bottlenecks preventing the adoption of IPv6. Given the severity of the problems in the current network scenario, the only feasible solution in the long run might be the IP migration process. IPv6 also offers significant features and characteristics needed by the stable internet of today.

While it is expected that migration or transfer between the two protocols would take a significant amount of time, the mechanisms of transition are in place to provide interoperability between the two protocols. While a number of transition strategies have been developed and standardized, the development of an optimal one is still a hot research field and no best possible transition plan solution has emerged to date. As is evident from chapter 3, these transition techniques significantly attenuate the efficiency of the network; where we made an empirical evaluation of four transition mechanisms most commonly used, namely Dual Stack, Automatic 6to4 Tunneling, Manual 6in4 Tunneling and NAT-PT, and compared performance metrics with the native IPv6 environment. As a result of this review, it was concluded that transformation strategies can only be seen as feasible during the migration phase and may not be sufficient for the long-term implementation of internet applications. Full implementation of IPv6 is the only feasible option for bandwidth efficacy and higher throughput.

REFERENCE

[1] F. Gont and T. Chown (2012). Network Reconnaissance in IPv6 Networks - draft-gont-opsec-ipv6-host-scanning02. http://tools.ietf.org/ html/draft-gont-opsec-ipv6- host-scanning-02

[2] Y. Cui, J. Wu, P. Wu, Q. Sun, C. Xie, C. Zhou, Y. Lee, and T. Zhou (2011). “Lightweight 4over6 in access network,” IETF draft.

[3] O. Troan and W. Dec and X. Li and C. Bao and Y. Zhai and S. Matsushima and T. Murakami (2012) “Mapping of Address and Port (MAP),” IETF draft.

[4] R. Despres and R. Penno and Y. Lee and G. Chen and S. Jiang (2012). “IPv4 Residual Deployment via IPv6 - a unified Stateless Solution (4rd),” IETF draft.

[5] M. Mawatari and M. Kawashima and C. Byrne (2012). “464XLAT: Combination of Stateful and Stateless Translation,” IETF draft.

[6] E. Rosen, D. Tappan, G. Fedorkow, Y. Rekhter, D. Farinacci, T. Li, and A. Conta (2012). “MPLS Label Stack Encoding,” IETF RFC 3032.

[7] S. Kent and R. Atkinson (1998) “Security Architecture for the Internet Protocol,” 1998, IETF RFC 2401. Y. Cui, J. Dong, P. Wu, J. Wu, C. Metz, Y. Lee, and A. Durand, “Tunnel based IPv6 Transition,” IEEE Internet Computing(accepted).

[8] Y. Cui, J. Wu, X. Li, M. Xu, and C. Metz (2006). “The Transition to IPv6, Part II: The Softwire Mesh Framework Solution,” IEEE Internet Computing, vol. 10, pp. 76 – 80.

[9] J. Wu, Y. Cui, C. Metz, and E. Rosen (2009) “Software Mesh Framework,” IETF RFC 5565.

[10] J. Wu, Y. Cui, X. Li, and C. Metz (2006). “The Transition to IPv6, Part I: 4over6 for the China Education and Research Network,” IEEE Internet Computing, vol. 10, pp. 80 – 85.

Corresponding Author

Manikant Singh*

Sr. Manager IT Security & Operational Excellence Professional