Challenges Security Aspects and Solutions for Migrating From IPv4 TO IPv6

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

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

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 Sub netting 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.

Keywords – Security, Solutions, IPv6

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

INTRODUCTION

The Internet has advanced to be one of humanity's biggest designing structures. The hidden protocols which comprise the Internet network have needed to scale to the elements of the current network, and the variety of uses and actual layers. The way that the Internet really works, regardless of the fast development and change, is a colossal accolade for the Internet Protocol (IP). The expanding requests of uses are making inspiration to reevaluate the central mechanisms of the Internet. The Internet will keep on developing, both in size, limit and requests of uses.

Internet Protocol Version 6 (IPv6) is another adaptation of the internetworking protocol intended to address the adaptability and administrations deficiencies of the current norm, IPv4 (Marc et al (1998), Afifi and Toutain 1999). It is an Internet layer protocol for parcel exchanged internet works. It is assigned as the replacement of IPv4, the current adaptation of the Internet Protocol, for general use in the Internet.

Sadly, IPv4 and IPv6 are not straightforwardly viable; henceforth projects and frameworks intended to one standard can't speak with those intended to the next. Anyway IPv4 frameworks are pervasive and are not going to disappear "overnight" as the IPv6 frameworks move in. Thus, it is important to create smooth transition mechanisms that empower applications to keep working while the network is being overhauled.

The primary change brought by IPv6 is a lot bigger location space that permits more prominent adaptability in allocating addresses. The all-encompassing location length (Nakajima and Kobayashi 2004) disposes of the need to utilize network address interpretation to keep away from address weariness, and furthermore streamlines the parts of address task and renumbering while evolving suppliers.

It is entirely expected to see models that endeavor to show that the IPv6 address space is very huge. For instance, IPv6 underpins 2128 (about 3.4×1038) addresses Microsoft Corporation, (2006). IPv6 address space should be overseen to benefit the internet network. The huge number of addresses permits a various leveled allotment of addresses that may make steering and renumbering less difficult. With IPv4, complex CIDR techniques were created to make the most ideal utilization of a limited location space. Renumbering, while evolving suppliers, can be a significant exertion with IPv4, as examined in (Ferguson and Berkowitz 1997).

FEATURES AND DIFFERENCES FROM

IPv4 generally, IPv6 is a moderate expansion of IPv4. Most vehicle and application layer protocols need practically zero change to work over IPv6; exemptions are applications protocols that install network-layer addresses, (for example, FTP or NTPv3). Applications, notwithstanding, normally need little changes and a recompile to run over IPv6.

- **Larger address space**

The fundamental element of IPv6 that is driving appropriation today is the bigger location space: addresses in IPv6 are 128 pieces in length versus 32 pieces in IPv4, (Deering and Hinden 1998) The bigger location space makes organization of medium and enormous networks more straightforward, by staying away from the requirement for complex subnetting plans. Subnetting will, preferably, return to its motivation of consistent division of an IP network for ideal steering and access, (Atkinson 1995)

- **Stateless Address Auto Configuration (SLAAC)**

IPv6 hosts can be arranged naturally when associated with a steered IPv6 network utilizing ICMPv6 switch disclosure messages, (Thomson et al 1996). At the point when originally associated with a network, a host sends a connection neighborhood multicast switch sales demand for its design boundaries; whenever arranged appropriately, switches react to such a solicitation with a switch notice bundle that contains network-layer setup boundaries. On the off chance that IPv6 auto design isn't reasonable, a host can utilize stateful setup (DHCPv6) or be arranged physically. Stateless auto setup is just appropriate for has switches should be arranged physically or by different methods.

- **Multicast**

Multicast is important for the base particulars in IPv6, in contrast to IPv4, where it was presented later.IPv6 doesn't have a connection nearby transmission office; a similar impact can be accomplished by multicasting to the all-has gathering (FF02::1).

Most conditions, notwithstanding, don't as of now have their network frameworks arranged to course multicast; multicast on single subnet will work, however worldwide multicast may not.

- **Link-local areas**

IPv6 interfaces have connect local areas expansion to the worldwide tends to that applications typically use. These connection residential locations consistently present and never show signs of change, which rearranges the plan of setup and steering protocols.

- **Jumbo grams**

In IPv4, bundles are restricted to 64 KB of payload. At the point when utilized between competent correspondence accomplices and on correspondence joins with a most extreme transmission unit (MTU) bigger than 65,576 octets (65536 + 40 for the header), IPv6 has discretionary help for bundles over this limit, alluded to as kind sized grams which can be as extensive as 4 GB (Borman et al 1999). The utilization of kind sized grams may improve execution over high-MTU networks.

- **Network-layer security**

IPSec, the protocol for IP network-layer encryption and verification (Kent and Atkinson 1998), is an indispensable piece of the base protocol suite in IPv6 dissimilar to IPv4, where it is discretionary (however generally executed). IPSec, in any case, isn't broadly utilized at present aside from making sure about traffic between IPv6 Border Gateway Protocol switches.

Less difficult preparing by switches IPv4 has a checksum field that covers the whole parcel header. Since specific fields, for example, the TTL field change during sending, the checksum should be recomputed by each switch (Ferguson and Berkowitz 1997). IPv6 has no blunder checking at the network layer yet rather depends on connection layer and transport protocols to perform mistake checking, which should make sending quicker.

IPV4/IPV6 TRANSITION ANALYSIS

The transition between the IPv4 Internet today and the IPv6 Internet of things to come will be a long cycle during the two protocols exists together. Fig-1.1 shows the different IPv4/IPv6 transition stages. A mechanism for guaranteeing smooth, stepwise Exordium 11 and autonomous change over to IPv6 administrations is required. Such a mechanism should help the consistent conjunction of IPv4 and IPv6 hubs during the transition time frame. The IETF has made the Ngtrans Group to encourage the smooth transition from IPv4 to IPv6 administrations. The different transition methodologies can be comprehensively partitioned into three classes, for example, Dual stack, Tunneling and Header interpretation mechanisms.

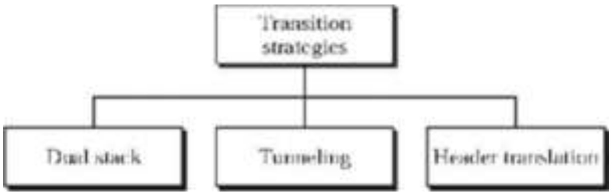

Fig.1: Schematic representation of IPv4/IPv6 transition

IPV4/IPV6 DUAL STACK TRANSITION MECHANISM (DSTM)

As the word implies, dual- stack mechanisms incorporate two protocol stacks that work in resemble and permit network hubs to convey either by means of IPv4 or IPv6 . They can be actualized in both end framework and network hub. In end framework, they empower both IPv4 and IPv6 applications to work simultaneously. The dual stack abilities of network hubs uphold the vehicle of both IPv4 and IPv6 bundles. In the double stack mechanism, determined in IETF RFC2893, a network hub incorporates both IPv4 and IPv6 protocol stacks in equal. IPv4 applications utilize the IPv4 stack, and IPv6 applications utilize the IPv6 stack. Stream choices depend on the form field of IP header for getting, and on the objective location type for sending. The kinds of addresses are generally gotten from DNS queries, the suitable stack is chosen because of the sorts of DNS records returned. Numerous off-the-rack business working frameworks as of now have double IP protocol stacks. Thus, the dual stack mechanism is the most broadly utilized transition arrangement. Nonetheless, dual stack mechanisms empower just comparative network hubs to speak with each other(IPv6-IPv6 and IPv4-IPv4). Considerably more works are needed to make a total arrangement that upholds IPv6-IPv4 and IPv4-IPv6 interchanges.

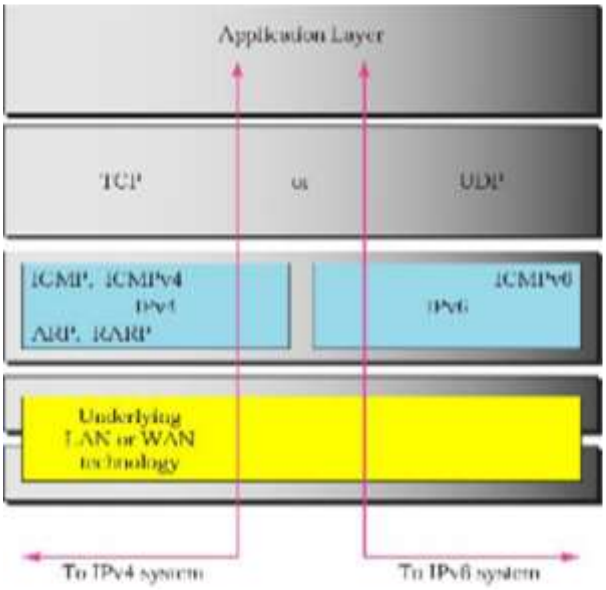

Fig.2: Dual Stack Transition Mechanism (DSTM) in IPv4/IPv6 transition

IPv4/IPv6 Tunneling Mechanisms

Tunneling from the viewpoint of transitioning, empowers contrary networks to be crossed over and is generally applied in a highlight point or consecutive way. Three instruments of tunneling are introduced: 6over4, 6to4 programmed tunneling and tunnel Broker.

Execution Evaluation of IPv4/IPv6 Transition

Presently a day's, network figuring has gotten increasingly more prevailing in the PC applications on PC stages. The exhibition of the networking applications relies upon the accompanying number of elements.

i. Physical qualities of the processor (CPU speed , Memory size and Disk store size and so forth)

ii. Bandwidth of the Network association.

iii. Efficiency of the application program.

iv. Efficiency of the network convention stack that is utilized for correspondence by the application.

The exhibition of the protocol stack along with the conduct of a working framework enormously influences the effectiveness of network applications based on top of it. The Investigation of network protocol execution, just as the assessment approach is a vital advance of enhancing the exhibition of the protocol.

OBJECTIVES OF THE STUDY

An endeavor will be made to audit and study the Next Generation Internet Protocol IPv6. We will examine about the need to move to IPv6 and investigation of challenges (specialized/non-specialized) to migration will likewise be introduced. We will introduce a few rules that should be dealt with while migration and will have a review of generally deployment of IPv6 on the planet. The correlation and the differentiation somewhere in the range of IPv4 and IPv6 protocols.

RESEARCH METHODOLOGY

The methodology continued in this research work is as per the following. A broad writing study was conveyed to get comfortable with the ideas and phrasing utilized in the convention. At that point the convention configuration was made express by indicating a portrayal of the convention viable. While cautiously recording each helpful detail of every convention, models of every convention were built and this was spoken to by mapping outline. In the underlying piece of this research work, we inspect the purposes behind relocating to IPv6.The movement includes challenges (both specialized and non-specialized) which should be tended to.

We likewise set up rules or benchmarks for IP movement. For consistent coordination and conjunction between the two non-homogeneous protocols, the movement techniques should be upgraded and accurately conveyed so internet personal time doesn't happen which may prompt execution and QoS corruption. In this research work, we have exactly done usage of existing movement techniques utilizing OPNET Modeler Simulation. In view of the determined boundaries, a methodology has been made towards finding better procedure among the current movement techniques. The investigation causes us in tackling the issue of picking best IPv6 movement method.

The primary intention is to examine its effect on execution in IP and movement networks. Since IPSec is inconsistent with NAT and furthermore has bootstrap issues (for example IKE involves for a working IP stack) in IPv6 Neighbor Discovery Protocol (NDP); Secure Neighbor Discovery Protocol (SEND) was acquainted with secure IPv6 interface layer tasks. Regardless of its countless substantial advantages, SEND faces significant challenges including extreme calculation, tremendous usage, deployment and security issues. Cryptographically generated address (CGA) vii which is a significant natural part of SEND convention discover their application in demonstrating address possession and forestalls ridiculing or burglary of IPv6 addresses by restricting senders public key with the created address. In spite of the fact that CGA is a promising method and offers significant measure of security, it has a few constraints and execution bottlenecks.

CGA is computationally concentrated controlled by the security boundary 'sec' and transfer speed eating because of utilization of RSA keys. For a higher estimation of sec, there is no assurance on end of beast power look for modifier. This proposition assesses the exhibition and examines certain techniques that can be utilized in upgrading the utilization of IPv6 CGA. These techniques are executed in proposed model and afterward contrasted and the standard CGA Results show that by fusing certain changes, improvement of standard CGA is conceivable. Important outcomes were recorded and reasonable ends or potentially proposals dependent on the above examination were recommended.

A COMPARATIVE ANALYSIS

This section provides a comparative review of the above discussed IPv4/IPv6 migration techniques. Although Dual Stack can be deployed on hosts, routers and on the same interface as IPv4, however it potentially requires 2 routing tables and processes. This comes in addition to the CPU and memory capacity of nodes. On the other hand, Tunnels are easy to deploy and are available on most platforms. But tunnels too have some issues. The tunnels must be manually configured in order to ensure security of the network. Tunnels also have issues with delay and latency through the tunnel in addition to being susceptible to single point of failure. The translation techniques although being cost effective require a significant amount of configuration from the administrative side. For network co-existence, translation techniques are not recommended by IETF.

CONCLUSION

In our research we contemplated IPv4, IPV6, Transition techniques and challenges security aspects and solutions .The IPv6 convention isn't secure naturally and care should be taken to actualize fitting security measures for address and switch design. Secure deployment of IPv6, both in double stack and IPv6-just networks, is a troublesome errand inclined to mistake and it's anything but difficult to misconfigure some host or gadget. The answer for IPv4 fatigue is yet to be brought about by corporates as a difficult issue consequently putting themselves in danger of inadequate time and financial assets. The significant bottlenecks blocking the embracement of IPv6 is the infrastructural relocation cost (software up-degree, hardware costs, labor preparing and network testing), undecided network execution of the new convention and forthcoming security issues that may emerge while deployment. Given the seriousness of issues in the current network situation, IP relocation cycle might be the solitary arrangement feasible over the long haul. Likewise IPv6 gives generous credits and qualities needed by the cutting edge secure internet. Despite the fact that relocation or transition between the two protocols is required to take impressive measure of time, the transition systems become an integral factor for giving interoperability between the two protocols. Despite the fact that, various transition techniques have been contrived and normalized, building up an ideal one is as yet a hot research territory and till date, no best attainable answer for transition plan has developed.

REFERENCE

[1] J. Arkko and S. Bradner. IANA Allocation Guidelines for the IPv6 Routing Header

[2] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) - Specification

[3] S. Thomson, T. Narten, and T. Jinmei (2007). IPv6 Stateless Address Auto configuration, http://tools.ietf.org/html/rfc4862.

[4] Geoff (APNIC) Huston. Transitional Myths. Internet Protocol Journal, 14(1), 2011

[5] Internet protocol version 4 source: http://www.faqs.org/rfcs/rfc791.html by Wilson Defense Advanced Research Projects Agency, Virginia. And Information Sciences Institute University of Southern California, California.

[6] Cisco Self-Study: Implementing Cisco IPv6 Networks (IPv6), Edited by: Regis Desmeules

[7] Bound J. (2005). "Experimental RFC Proposal Internet Draft, Dual Stack IPv6 Dominant Transition Mechanism", https://tools.ietf.org/html/draft-bounddstm-exp-03

[8] R. Housley (2010). Guidelines to Authors of Internet-Drafts. http://www.ietf.org/ietf-ftp/1id-guidelines.txt.

[9] R. Hinden and S. Deering (1998). IP Version 6 Addressing Architecture. http://tools.ietf. org/ html/ rfc2373.

[10] R. Hinden and S. Deering (2003). Internet Protocol Version 6 (IPv6) Addressing Architecture. http://tools.ietf.org/html/rfc3513.

Corresponding Author

Manikant Singh*

Sr. Manager IT Security & Operational Excellence Professional