International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Transition from IPv4 to IPv6 and their Security Challenges

Sridevi

Assistant Professor, Department of Computer Science, Karnatak University, Dharwad, Karnataka, India

Abstract: ***At a time where the available Internet Protocol version 4 (IPv4) address pools are running out, still too many Internet Service Providers (ISPs) and network administrators have yet to acknowledge this new reality and adapt their networks and systems. Although the depletion of addresses has been repeatedly mentioned and commented for the past decade amongst relevant networking circles, 2011 and 2012 showed us a growing and urgent need for Internet Protocol version 6 (IPv6) adoption as Regional Internet Registries (RIRs) are depleting their IPv4 address pools. This research paper studies the IPv6 protocol security challenges and the effects this migration has on network security. To that end, different transition strategies are detailed as well as possible vectors of attack to the IPv6 protocol and dual-stack environments.***

Keywords: IPv4, IPv6, Internet, Transition, security, Network Access Points, IPSec

1. Introduction

The Internet has continually evolved this last decade to become something that our society depends upon. It is used by people across different sectors, computer savvy and otherwise, for all kinds of services and purposes: videogames, social interactions, banking, accounting and globally disperse teams collaborating and communicating remotely are just a few examples. Currently widely deployed, IPv4 is a twenty-year-old internetworking standard protocol at the core of devices communication in packet-switched networks (such as Ethernet) and uses 32-bit unique addresses to identify each host on the network, with no concern or guarantees as to the delivery or integrity of messages. While there are efforts to secure communications both at the application layer as well as the internet layer (notably Secure Sockets Layer (SSL), Internet Protocol Security (IPSEC) and Domain Name System Security Extensions (DNSSEC)), with the amount of trust deposited in the correct operation of the networks, security is essential.

2. Problem Statement

The problem addressed in this paper is twofold. First, the transition to IPv6 is a complex feat that requires skilled effort and investment from ISPs; it is not only a technical challenge with very different and intricate transitional protocols but also a business constraint due to the implications it has on service availability to customers, expected lifetime of a dual-protocol situation and cost of transition (acquisition of compatible hardware, training, etc).

Secondly, IPv6 brings along many security issues with its renewed pool of IP addresses. It's a fundamental paradigm change in the way we think about internetworking, due to its security features and the impact on current industry standard practices.

1. Internet Protocol (IP)

The Internet Protocol enforces two basic operations; addressing and fragmentation. The Internet modules use the addresses carried in the Internet header to transmit datagrams towards their destinations [5]. An IP packet or a datagram has two fundamental components; IP header and payload [6]. Transmission control protocol (TCP) and the Internet protocol (IP) are the basic two protocols started function with IP. The TCP/IP Internet protocol derives from the Network layer in the OSI model.

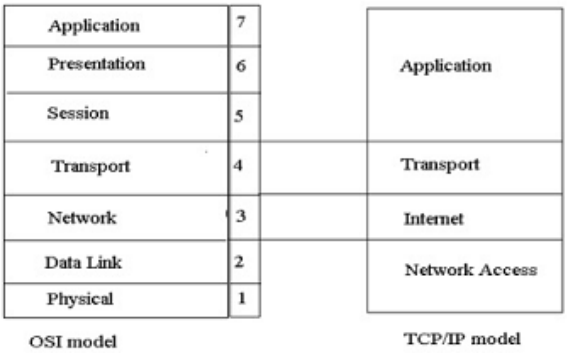

Figure 1: OSI – TCP/IP model

Present Internet has two well-known Internet protocols. Without these protocols present and the future Internet cannot exit. Those are;

- Internet Protocol Version 4 (IPv4)
- Internet Protocol Version 6 (IPv6)

An IPv4 address is a 32 bit numeric address to a node in a network. Internet protocol utilizes IP addresses to make a communication with a particular node in the network. An IPv4 address carries two sort of information such as "Network address" and "Host Address". The network address is used to find location of a network and host address is utilized to reach particular destination within a network. The Internet Engineering Task Force (IETF) designed the IPv6 Address scheme. The IPv6 protocol represents an upgrade of the IPv4 [1]. IPv6 is designed not

only to solve the IP addresses shortage problems, but also improves and enhances prominent features over IPv4.

2.2 IPv6 Adoption

The entire IPv4 address pool consists of 4 294 967 296 (2^{32}) addresses, which are currently being consumed at a rate of 5 percent every year. Current estimates place the pool depletion at a date no later than 2015 (Figure 2) at which time most ISPs will need to have either an IPv6 deployment strategy or IPv6 already available for customers and/or internal networks. However, IPv6 adoption is still very slow with IPv6-enabled Autonomous Systems (AS) registered with regional internet registries (RIR) still below 20 percent of the total AS (Figure 3) [4]. The World IPv6 day in 2011 has been a successful step towards global IPv6 adoption: for 24 hours, many online businesses, academic institutions and network enthusiasts enabled IPv6 alongside IPv4 on their networks and systems. This coordinated effort brought together high traffic websites, Content Distribution Networks (CDNs) and others to help test the performance and realistic operating capacity of an IPv6 network in today's Internet, both as an end-user and as a service provider. The Internet Society, responsible for this event, has deemed the results successful and, building on those results, set 2012's World IPv6 Launch day7 to become a global coordinated launch of IPv6 availability – participants enabled IPv6 permanently, providing their services in a dual-stack environment from that day on. In total, more than 3000 websites, including the four more popular ones by the Alexa rank, 65 ISPs and 5 major router vendors participated in the World IPv6 Launch day. An estimated 27% of the Internet is now available via IPv6, meaning that suddenly IPv6 became much more important and many more network links are active, potentially exposing many networks and systems. Even more, many other ISPs are reportedly preparing IPv6 deployment, so this figure is expected to continue growing in the near future.

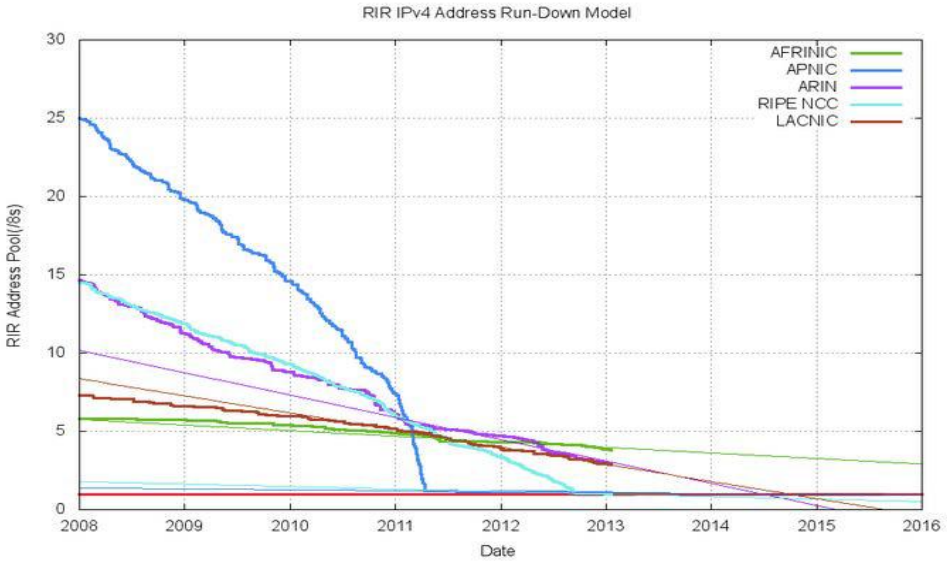

Figure 2: Projection of consumption of remaining RIR IPv4 Pools

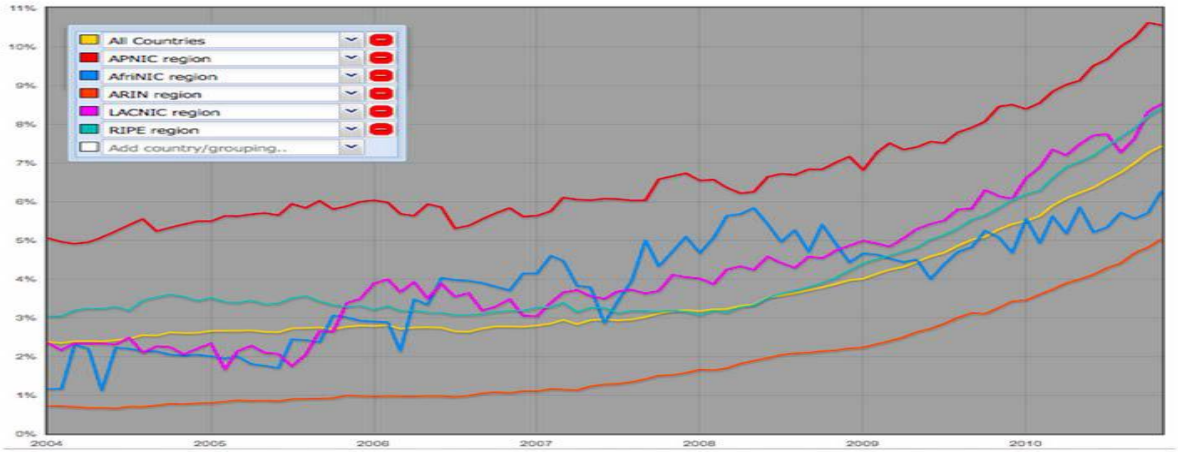

Figure 3: Percentage of IPv6-enabled Autonomous Systems registered in each RIR

With IPv4 shortage rapidly progressing and IPv6 adoption becoming a priority for many ISPs, this growth rate is expected to increase in the following years. The Internet Society has already declared publicly that the Internet has run out of IPv4 addresses. However, due to backwards-compatibility with systems and networks that remain IPv4 only, it is expected that for several years both protocols

will have to co-exist and ISPs will have to adapt with the following two constraints:

1. IPv6 deployment in their internal networks and availability as a service to customers
2. Efficient use of IPv4 addresses, to reduce costs and enable IPv4 connectivity

The path to a IPv6-only Internet is far from complete and there are significant challenges ahead. First, the transition period will bring a mix of partial and full-transitioned networks online to coexist with the current IPv4 networks and provision of online services is expected not to be disrupted. Secondly, IPv6 as a protocol has several security misconceptions and vulnerabilities by design, which adds to the challenge of transitioning the Internet to a new routing protocol in a safe and cost-effective way.

3. Transition Mechanisms

Since there is such a large difference between IPv4 and IPv6, they cannot communicate directly with each other. A system that is capable of handling IPv6 traffic can be made backward compatible, but an already deployed system that handles only IPv4 is not able to handle IPv6 datagrams. This means that a major upgrade process would need to take place, involving hundreds of millions of machines, in order to make a complete transition to IPv6.

3.1 Dual-Stack Technique

The dual-stack technique or also called dual-stack transition mechanism (DSTM) is that all devices interoperate with IPv4 devices using IPv4 packets, and with IPv6 devices using IPv6 packets. In other words, the dual-stack technique is basically using IPv4 and IPv6 addresses in parallel. All connections and devices like routers, end-user devices and other infrastructure devices are dual stacked and they can communicate over both IPv4 and IPv6. The major assumption within DSTM is that DSTM is fully transparent to applications because it can continue to work with IPv4 addresses. Also, it is transparent to the network, which carries only IPv6 packets. The other assumptions in DSTM architecture are listed below:

1. The DSTM domain is within an Intranet and it is not on the Internet.
2. The DSTM server allocates the temporary IPv4 address and different protocols like DHCPv6 can be used to assign the IPv4 address.
3. Except temporarily communication with IPv4 applications, dual stack IPv6/IPv4 nodes do not maintain IPv4 addresses.
4. DSTM uses IPv6 routing and it will keep IPv4 routing tables to a minimum. With DSTM dominant IPv6 network, DSTM will reduce the network management required for IPv4 during transition.
5. Dynamic tunnelling is used to encapsulate the IPv4 packet within the IPv6 packet once IPv6 nodes have obtained IPv4 addresses. After that packet is forwarded to an IPv6 tunnel end point (TEP) DSTM border router, where the packet will be decapsulated and forwarded using IPv4
6. In DSTM, existing nodes and IPv4 applications do not have to be modified [7].

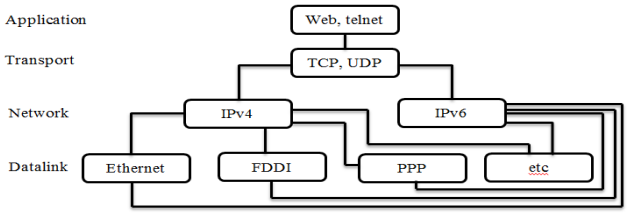

Figure 4: Dual-Stack Technique

Figure 4 shows the basic dual-stack technique. In the dual-stack technique, subsets of both routers and hosts are upgraded for IPv6 support, in addition to IPv4. If the upgraded nodes want to communicate with IPv4-only nodes at that time they always do it by using IPv4. If the upgraded nodes want to communicate with IPv6-only nodes at that time they can do it by using IPv6.

3.2 Tunnelling

Tunnelling basically means that IPv6 packets are placed inside IPv4 packets, which are routed through the IPv4 routers. In other words we can say that IPv6 packet is encapsulated into IPv4 packet and it goes from source to destination where it is decapsulated and retransmitted. This technique has the ability to be used in an existing IPv4 routing infrastructure to carry IPv6 traffic. Different tunnelling methods exist in IPv6 are listed below:

1. Manual IPv6 Tunnels
2. 6 to 4 Tunnels: IPv4 Compatible Tunnels
3. IPv6 rapid deployment
4. Generic Routing Encapsulation (GRE) IPv6 tunnels

3.3 Translation Technique

For translating IPv6 traffic to IPv4 traffic or IPv4 traffic to IPv6 traffic the translation technique is used. In this translation technique, the traffic is converted to the destination type. There is no traffic encapsulation here.

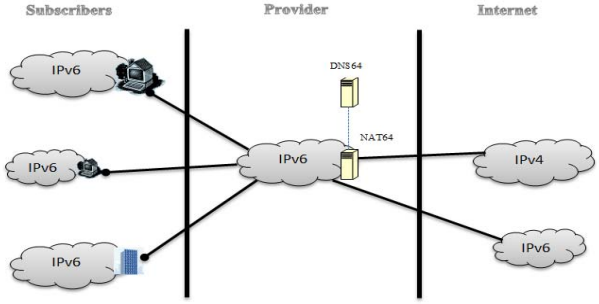

Figure 5: Translation Technique

Figure 5 shows the basic translation technique. There are two methods that are typically used with translated IPv6 networks which are listed below:

1. NAT-PT (Protocol Translation
2. NAT64

2. IPv6 Security

Designing an Internet Protocol is a daunting task, which few dare to attempt. Even though several people typically collaborate to produce a document and there is sufficient peer review, some errors happen to slip by. When they do so in such important RFCs, they are bound to be discovered and updated in later specifications [8]. Since the first IPv6 protocol RFC, several other RFCs and drafts have appeared to correct specific vulnerabilities or to enhance operation issues. While this is good to formalize improvements of the protocol, it brings along a major problem when the updates are specific to protocol implementation: it means every implementation of IPv6 (or any other protocol, for that matter) ever made needs to be updated accordingly [1]. The design of IPv6, at the time of its proposal, contemplates network operations and security with the mindset of 1995. It contemplates the following changes regarding IPv4 [2].

- Expanded Addressing
- Header Format
- Improved Support
- Flow Labelling
- Authentication and Privacy

At the time, the IPv6 protocol RFC (2460) was compliant with the "Security Architecture for the Internet Protocol" RFC (2401), which does not support multicast in a standard way and left room for further definition in later documents. The IPv6 Protocol relies on multicast communication for local-link operations and also states IPSEC as mandatory. Since IPSEC a multicast operation was not clearly defined at the time, this leaves a huge gap in the specification [9]. Further development of multicast support for IPSEC continued but was only resolved definitively a decade later, with RFCs 4301 (2005) and 5374 (2008).

Private Addresses

Private addresses are now defined through Unique Local Addresses, for use in context of:

- Addressing for isolated networks (e.g. IPv4 private networks)
- Persistent local-context addresses (e.g. IPv4 DHCP fixed leases)
- Interconnection of local network contexts

Stateless Address Auto-configuration

Stateless Address Automatic Configuration is one of the major new features of IPv6. It moves address allocation to the core of network protocols instead of an upper layer alternative (i.e. DHCP in IPv4)[3].

DNS Configuration

The first major problem of SLAAC is DNS configuration. DNS information is not provided by SLAAC's first draft, leaving two options for hosts:

1. Use locally-configured DNS servers in every network or reach hosts through their IPv6 addresses

- Using ipv6 addresses instead of DNS records is not acceptable for most users
- Using the same public DNS servers everywhere creates a great dependency upon them
- Setups in which network operator maintain a private set of DNS records for their domains (for internal hosts) can't work unless network nodes use local DNS servers1

2. Obtain an address through DHCPv6 or similar protocol

- Will automatically revert the address allocation being part of the Internet layer.
- Complicates ubiquitous connectivity since hosts need to be configured or somehow discover what sort of address allocation method is in-place when connecting to a network.

4. Conclusions

To expose the current state of transition, what can be expected to follow as the IPv6 transition continues and highlights possible research paths taking the current state of the industry into account.

The IPv6 protocol is not secure by default and care must be taken to implement appropriate security measures for address and router configuration. Secure deployment of IPv6, both in dual-stack and IPv6-only networks, is a difficult task prone to error and it's easy to misconfigure some host or device. This new protocol stack is being actively developed upon to improve functionality and remove liabilities, with many IETF working groups and individuals contributing drafts improving recommendations, implementation requirements and proposing new protocols or protocol enhancements.

References

[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. IPv6 Stateless Address Auto configuration, http://tools.ietf.org/html/rfc4862, 2007
[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-bound-dstm-exp-03
[8] R. Housley. Guidelines to Authors of Internet-Drafts. http://www.ietf.org/ietf-ftp/1id- guidelines.txt, 2010
[9] R. Hinden and S. Deering. IP Version 6 Addressing Architecture. http://tools.ietf. org/ html/ rfc2373, 1998
[10] R. Hinden and S. Deering. Internet Protocol Version 6 (IPv6) Addressing Architecture. http://tools.ietf.org/html/rfc3513, 2003
[11] F. Gont and T. Chown. Network Reconnaissance in IPv6 Networks - draft-gont-opsec-ipv6-host-scanning-02. http://tools.ietf.org/ html/draft-gont-opsec-ipv6-host-scanning-02, 2012