Ipv6 Change Threats Behavior

Firas Najjar
National Advanced IPv6 Center (Nav6)
Universiti Sains Malaysia
Penange, Malaysia

Homam El-Taj
Computer Science
Tabuk Univesity
Tabuk, Saudi Arabia

***Abstract*—IPv4 address pool is already exhausted; therefore, the change to use IPv6 is eventually necessary to give us a massive address pool. Although IPv6 was built with security in mind, extensive research must be done before deploying IPv6 to ensure the protection of security and privacy. This paper firstly presents the differences between the old and new IP versions (IPv4 and IPv6), and how these differences will affect the attacks, then the paper will show how the attacks on IPv4 and IPv6 will remain mostly the same; furthermore, the use of IPv6 will give rise to new types of attacks and change other types' behavior.**

Keywords—Computer Attacks; IPv4; IPv6; Security

I. INTRODUCTION

Internet Protocol (IP) is a set of technical rules that define how computers communicate through networks [1], IP address is just like a home address or telephone number. In computer network; all devices in the same network must have a unique IP address to exchange data between them, without a well configured IP address, the communication with other devices in the network will be broken.

Nowadays most commercial and governmental information systems are connected through the Internet, using new technology like IPv6 at the time being might seem risky because it isn't be fully tested, which make it possible to attack. These systems must be protected from unauthorized access that may expose critical information, this can be done by detecting any suspicious anomalies in the network traffic patterns due to Distributed Denial of Service (DDoS) attacks, worm propagation [2] [3], viruses, Trojans and other kinds of malicious programs that introduce more panic into network society. Based on these attack types, securing such networks infrastructure has become a priority for most researchers.

The first IP address system widely deployed is Internet Protocol Version 4 (IPv4); IPv4 has proven to be robust, easily implemented, and interoperable. It has stood up to the test of scaling an internetwork to a global utility, the size of today's Internet, this is a tribute to its initial design[1], but the huge growth of using internet leads to the exhaustion of the IPv4 address pool [4], as a result, public IPv4 addresses have become relatively scarce, forcing many users and some organizations to use a Network Address Translation (NAT) [5]; to map a small number of public IPv4 addresses to multiple private IPv4 addresses. Although NATs promote the reuse of the private address space, they violate the fundamental design principle of the original Internet that all nodes have a unique, globally reachable address; additionally the growth of using the internet insures the reduction of IPv4 public addresses.

In 2011, Internet Assigned Number Authority (IANA), which is the main authority for IP address allocation announced the exhaustion of its free pool of IPv4 addresses [6], in addition, on 14th of September 2012 the Europens Network Coordination Centre (RIPE NCC) which is responsible of addresses in Europe and in the middle east began to allocate IPv4 address space from the last /8 address pool of IPv4 address space it holds. Table I and Figure 1 show the exhaustion dates of IPv4 pool addresses.

TABLE I. PROJECTED RIR ADDRESS POOL EXHAUSTION DATES [6]

RIP	Exhaustion Date	RIP Pool/8
APNIC	19-Apr-11	0.8180
RIPE NCC	14-Sep-2012	0.8535
LACNIC	19-Jan-2015	1.4427
ARIN	12-Feb-2015	1.5558
AFRINIC	24-May-2022	3.4479

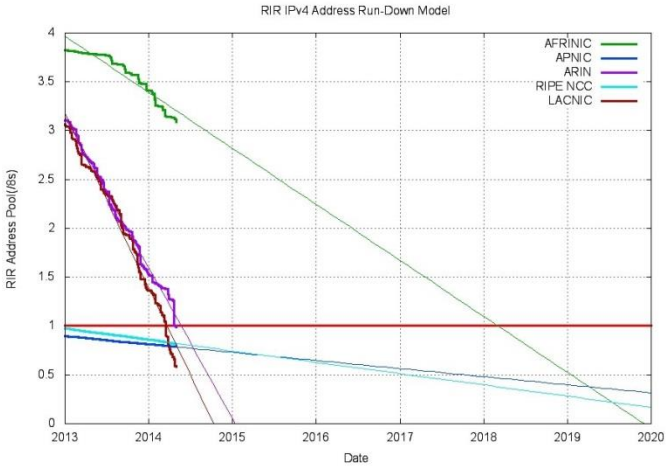

Fig. 1. Projection of consumption of Remaining RIR Address Pools [6]

Internet Protocol Version 6 (IPv6) [7] was deployed to overcome IPv4 address exhaustion limitation. IPv6 intended to replace IPv4 that still carries the vast majority of Internet traffic 2013. In December 2013, the percentage of users reaching Google services over IPv6 surpassed 2.7% [8], for that we must prepare ourselves to the next generation of addressing system IPv6.

The rest of this paper will be organized as following: Section 2 will cover an overview on network system to produce basic knowledge about network concepts, Section 3 shows how the differences between IPv4 and IPv6 will affect

the security of networks, furthermore how these differences affect the types of the attacks, and does IPv6 reduce the attacks?

II. NETWORK OVERVIEW

Networks are simply two or more computers connected to each other through medium to exchange data between them. In order to exchange data there must be some protocol or model that organizes the transmission between computers, for that International Organization for Standard (ISO) produced a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers called Open Systems Interconnection (OSI) model [9].

Each layer of OSI model serves the layer above it, and served by the layer below it, Table II shows the OSI model layers with main function and example protocol from real world.

TABLE II. OSI MODEL LAYERS WITH MAIN FUNCTIONS AND PROTOCOLS

NO.	Layer Name	Function	Protocols
7	Application	Provide service protocol to applications	FTP, HTTP
6	Presentation	Data representation, encryption and decryption	SSL,TLS
5	Session	Control Conversations/ sessions between application	PPTP,RTP
4	Transport	Reliable delivery of packets between points on a network	TCP, UPD
3	Network	End to end Delivery	IP, ICMP
2	Data Link	Reliable direct point-to-point data connection.	PPP
1	Physical	Media Interface Transmission Method	

A. Internet Protocol Suite

Internet protocol suite is a suite of protocols, which were first designed for the Defence Advanced Research Project Agency (DARPA) network, which was called the (ARPAnet) during the early 1970s [10].

In the early 1980s, it was included as an integral part of Berkeley's UNIX version 4.2. Today, it is the protocol used by ARPAnet, MILnet and many other networks. The Internet Protocol suite is also commonly called TCP/IP protocol suite, because the most two important protocols in it: the transmission control protocol (TCP) and the Internet protocol (IP), these were also the first two protocols in the suite to be developed. If we compare Internet Protocol suite with OSI model, Internet Protocol suite contains four layers:

a) The Internet application layer includes OSI Model application layer, presentation layer, and most of the session layer.

b) Transport Layer includes the graceful close function of the OSI session layer as well as the OSI transport layer.

c) Internet layer is a subset of the OSI network layer.

d) Link layer includes the OSI data link and physical layers, as well as parts of OSI's network layer.

1) IPv4

IPv4 [1] is the fourth version of the Internet Protocol (IP) used to address the devices on the network to identify them, Internet Protocol is one of the major protocols in Internet Protocols suite, this protocol works at Network layer of OSI model and at Internet layer of Internet Protocol model. IPv4 is the first version of internet protocol widely used [11], IPv4 packet header consists of 14 fields, of which 13 are required, and the 14th field is optional.

IP protocol is responsible for the identification of hosts based upon their logical addresses and to route data between them over the underlying network, additionally IP provides uniquely identification mechanism to host by IP addressing scheme. IP does not guarantee the delivery of packets to destined host, but it will do its best to reach the destination.

IPv4 uses 32-bit addresses, which limits the address space to 4294967296 addresses, and because the exhaustion of these addresses, Internet Engineering Task Force developed, a new version called Internet Protocol Version 6 (IPv6), that uses 128-bit addresses, which is a very huge number of addresses.

2) IPv6

IPv6 is the latest version of the Internet Protocol (IP). IPv6 developed by the Internet Engineering Task Force (IETF) to overcome IPv4 address exhaustion. IPv6 is an Internet Layer protocol for packet-switched internetworking and provides end-to-end datagram transmission across multiple IP networks. Compare IPv6 to IPv4, IPv6 uses simplified header format in seven fields instead of 13 fields in IPv4, with fixed length header of 40 bytes only even that the IPv6 header contains two 128 bit addresses (source and destination IP address).

Figure 2. shows the differences between header formats for both protocols.IPv6 packet header contains fields that facilitate the support for true Quality of Service (QoS) for both differentiated and integrated services, to provide better support for real-time traffic like Voice over IP. IPv6 also includes labeled flows in its specifications to recognize the end-to-end packet flow through routers [12]. Due to the large address space, IPv6 uses stateless address auto configuration to auto configure addresses to hosts. IPv6 is not that different from IPv4, they use the same routing protocol, layer 4 unchanged, and Layer 2 also remain unchanged.

To summarize the changes between IPv4 and IPv6, there only three major changes:

- Fixed Header Length.
- Larger IP Address space.
- Address Resolution Protocol (ARP)[13]replaced with Neighbor DiscoveryProtocol (ND)[14].

The following list summarizes the features of the IPv6 protocol:

- New header format.
- Large address space.
- Stateless and stateful address configuration.

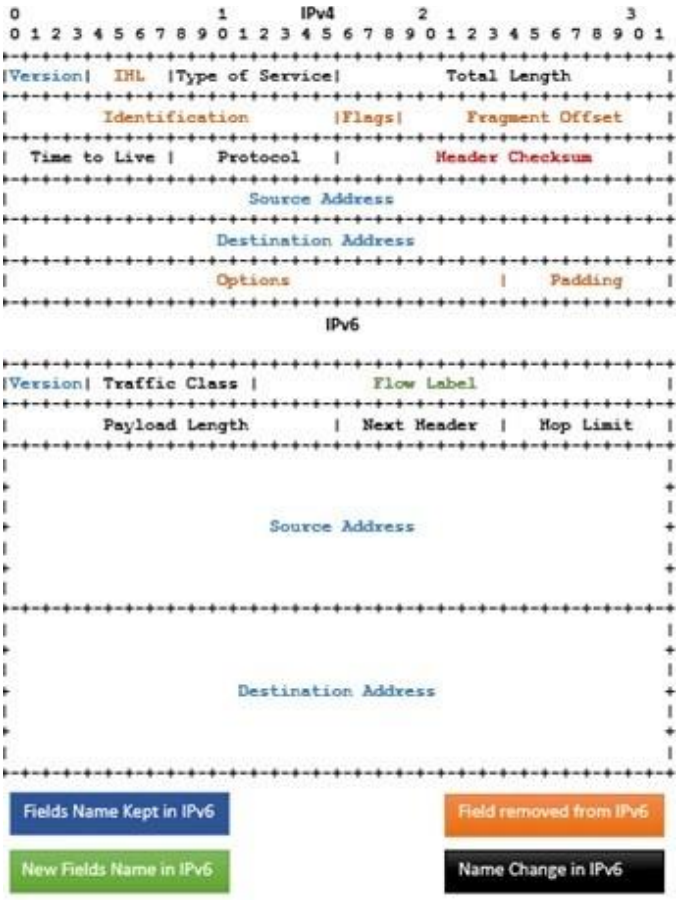

Fig. 2. Comparing IPv4 and IPv6

Internet Engineering Task Force (IETF) standards for IPv6 protocol stack functionality, includes the following:

- IP security (IPsec)[15] header support required. Better support for prioritized delivery.
- New protocol for neighboring node interaction.
- The IPv6 header [16].
- Unicast, multicast, and anycast addressing [17].
- The Internet Control Message Protocol for IPv6 (ICMPv6) [18].
- Neighbor Discovery Protocol (NDP) [19].
- Multicast Listener Discovery (MLD) [20] and MLD version 2 (MLD v2) [21].
- Stateless address auto-configuration [22].

Until IPv6 completely supplants IPv4, many mechanisms produced to make communication between IPv4 and IPv6 networks, by translating complete headers between IPv4 and IPv6 headers or by tunneling IPv4 packets in IPv6 packets [45]. These mechanisms are beyond the scope of this paper.

III. IPv4 and IPv6 Differences and Attacks

IPv4 and IPv6 differences change the types of attacks; IPv6 substantially changes how IP interacts with the link layer, in particular host. NDP will replace ARP, which is ICMPv6 based, and the use of protocols such as SEcure Neighbor Discovery (SEND) [23] is a must to secure NDP or we will fall prey to the same class of attacks we faced in IPv4 over networks[44].

This Section outlines the common known attacks against IPv4 and then compares how these attacks might affect an IPv6 network, new types of attacks will rise and other will change their technique.

A. Reconnaissance

Reconnaissance attacks used to gather information as much as possible about the victim network when the adversary has no specific target. These attacks include port scanning and IP scanning using methods to establish a range of IP addresses which map to live hosts called PING SWAP tools.

The adversary uses PING SWEEP (also known as an ICMP sweep) to determine which of a range of IP addresses map to live hosts like computers or servers, whereas a single PING will tell you whether one specified host exists on the network or not.

PING SWEEP tools consists of Internet Control Message Protocol (ICMP) ECHO requests sent to multiple hosts, if a given address were live, it would return an ICMP ECHO reply. Ping sweeps are among the older and slower methods used to scan a network. After identifying reachable hosts, the adversary can systematically probe these hosts on any number of Layer 4 ports scanning to find services both active and reachable, by discovering hosts with active services, the adversary can then move to the next phase of attacks, this is why these attacks called passive attacks.

1) IPV4 Reconnaissance Attack

In IPv4, it is feasible to scan host address space of a specific network. If we have network address space of 16 bits (class B network) which represents 65536 hosts, the adversary can scan the whole network within less than two hours if the scan uses 10 addresses per second. This makes scanning usable mean for reconnaissance in IPv4 networks.

2) IPV6 Reconnaissance Attack

In IPv6, the situation is more complicated, the usual subnet size is 64 bits and with the same speed of scanning IPv4 subnet, it would take 60 billion years to scan all addresses, this makes scanning techniques impossible unless an adversary uses different approaches. As T. Chown [24] mentioned, some techniques will reduce the subset size, as if the adversary knows the Ethernet vendor prefix, the search space will reduce to 48 bit, and furthermore, if the adversary knows the Ethernet vendor, the search space may be reduced to 24 bits. Network Mapper (NMAP)[25] which is a tool that can perform all these scan types at the same time, produces new techniques to find all the hosts who use IPv6 on a target network:

- Targets-ipv6-multicast-echo sends an ICMPv6 echo request packet to the all-nodes link-local multicast address (ff02::1), collect the IPv6 addresses that come from and mark those hosts as potential scan targets

- Targets-ipv6-multicast-invalid-dst sends an ICMPv6 packet with an invalid extension header to the all-nodes link-local multicast address. Any hosts replying with an ICMPv6 parameter problem packet can be marked as up and available for potential scanning.
- Targets-ipv6-multicast-mld attempts to discover available IPv6 hosts on the LAN by sending an MLD (multicast listener discovery) query to the link-local multicast address (ff02::1) and listening to any responses.
- Targets-ipv6-multicast-slaac sends an ICMPv6 router acknowledgment packet with a random address prefix, causing hosts to begin stateless address auto-configuration (SLAAC) and send a solicitation for their newly configured address.

These new techniques will help the adversary to identify a reachable host in victim's network to make the next step without spending much time like brute force scan, after identifying reachable systems; the adversary tries to find active ports and services that used for its next step of the attack.

B. ARP and DHCP Attacks

ARP Spoofing is a type of attack in which adversary tries to link a legitimate Media Access Control (MAC) host to adversary IP address. Once the adversary MAC address is connected to an authentic IP address, the adversary will begin receiving any data that is intended for that IP address.

Furthermore, the adversary can simulate network servers like Dynamic Host Configuration Protocol (DHCP) server, with this action the adversary will be able to reply to DHCP request before the real DHCP server; because it is closer to the client host. It will configure the Client host with IP address of that subnet, but it will also give a false Default Gateway address to host and maybe even false DNS server address.

1) IPV4 ARP AND DHCP ATTACKS

ARP spoofing can enable adversary parties to intercept, modify, or even stop data in-transit. ARP spoofing attacks can only occur on local area networks that utilize the Address Resolution Protocol. Cisco implemented a new technique called snooping [26] to overcome DHCP identity thief, by allowing certain ports to send DHCP server messages.

2) IPV6 ARP AND DHCP ATTACKS

The situation significantly changes in IPv6; ARP protocol replaced by Neighbor Discovery Protocol (ND), similar attack is still possible through Neighbor Solicitation/Advertisement Spoofing [27]. To verify sender ownership of claimed IP address, SEcure Neighbor Discovery (SEND) is used, which is a security mechanism used to secure ND from attacks, based on Cryptographically Generated Addresses (CGA) [28] and asymmetric cryptography. SEND uses cryptographically generated addresses to verify the sender's ownership of a claimed address. CGAs are IPv6 addresses in which part of the address is generated by applying a cryptographic one-way hash function based on a nodes public key and auxiliary parameters. The hash value can then be used to verify the binding between the public key and a nodes address. By default, a SEND-enabled node should use only CGAs for its own addresses. The basic purpose of CGAs is to prevent the stealing or spoofing of existing IPv6 addresses. While SEND is a robust mechanism for verifying sender ownership, it is difficult to implement because it's based on Public Key Infrastructure (PKI), and most popular hot operating systems do not support SEND [29] [30].

C. Smurf attack

Smurf attacks were one of the first network-based denial-of-service attacks. The name Smurf came from the name of the source code (Smurf.c). The Computer Emergency Response Team (CERT) first issued Smurf attacks in January 1998.

1) IPV4 Smurf attack

In Smurf attacks, the adversary sends an echo-request message (ping) with a destination address of a subnet broadcast and a spoofed source address using the host IP address of the victim; this causes all the devices on the subnet to respond to the spoofed source IP address and flood the victim with echo-reply messages.

A ping allows remote systems to quickly determine whether another system is live on the network. If system X wants to"ping" system Y, it sends an ICMP echo request packet with a source address of X and a destination address of Y. When Y receives the echo request, it reads the source address (in this case, X) and sends an ICMP echo reply message back to the originating host. These replies quickly add up and, when repeated, can overwhelm the victim system, causing a denial of service.

Many Broadcast Amplification attacks are easy to disable by simply disabling directed broadcast forwarding [31].

2) IPV6 Smurf attack

In IPv6 the concept of an IP broadcast is removed, there is no implementation of traditional IP broadcasting in IPv6; there are only multicast, unicast and any-cast.

To mitigate these attacks in IPv6; A.Conta and S.Deering [32] states that: an ICMPv6 message should not be generated as a response to a packet with an IPv6 multicast destination address, a link-layer multicast address, or a link-layer broadcast address. On the other hand, even nodes are compliant to RFC 2463, the smurf attack can use the generated "Parameter problem ICMPv6 message" error messages in response to a packet destined to a multicast group [33], and it may use the packets, which were used in multicast video stream, because multicast video stream required allowing path maximum transmission unit (MTU) discovery. E. Vyncke, S. Hogg [33] stated: this opens the door to an amplification attack in the same shot. In addition, to mitigate this problem they advise to apply rate limiting to those ICMP messages: They should be rare in every network so that a rate limit (10 messages/sec) can permit the correct use of those messages (path MTU discovery) while blocking the amplification attack.

D. Flooding attack

Flooding is a type of Denial of Service (DoS) attack, which attempts to cause a failure in network communication by sending many requests to a network hosts, too many requests cause the attacked host to collapse.

Flooding attack is one of the most frequent attack types present in IPv4 networks, this type of attack can also affect the IPv6 networks by sending Router Advertisement packets and forcing operating systems to create IPv6 addresses in response to every packet it receives. By flooding the network with enough RAs, the host machines will consume more CPU time as the Stateless Auto Configuration process tries to configure the addresses [35].

E. Application Layer Attack

An application-layer attack targets application and operating systems causing a fault in applications and operating systems. This results in the adversary gaining the ability to bypass normal access controls and takes advantage of this situation to gain control of the application, operating system, or network. Some known types of these attacks are: buffer overflow, web application attacks, viruses and worms.

Most of these attacks are not affected by moving to use IPv6, because it is difficult if not impossible to recognize these attacks on Network layer, especially when using IPsec, because IPsec would make it impossible to read encrypted data. However, the advantage of IPsec implementation would make it easier to trace back to the adversary, because of mandatory authentication. Without IPsec, the source address can be spoofed.

The only change in Application-Layer attack is the propagation of worms. Traditionally worms make local and wild scanning to find victim hosts, which make it unlikely to succeed in IPv6 environment, but as we discussed earlier; taking advantage of local knowledge and patterns in address-space assignment, the attack program can cut the search space considerably.

There is a number of strategies worms could use in an IPv6-based Internet to find new targets:

- Routing Tables, many organization run routing protocol internally such routing protocol (RIPng) [36] worm would be able to consult the host routing table [37].
- Multicast, is a fundamental part for IPv6 which can be abused for target discovery by worm.
- Server Logs, servers must log incoming mail server, website, DNS server; these logs are valued information for the worms to spread out.
- Server Addresses, IPv6 addresses are very hard to remember, most administrators tend to select easily memorized IP, which can be exploited by worms.
- Search Engine, for worms that target Web server, search engine is the best source of information; A.kamra [38] shows that DNS worm in IPv6 could spread as fast as an IPv4 address scanning worm.

F. SnifferAttack

A sniffer attack is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunneled) packets can be broken open and read unless they are encrypted and the attacker does not have access to the key.

IPv6 provides fundamental technology preventing sniffing attacks with IPsec and Internet Key Exchange Protocol Version 2 (IKEv2) [39].

G. Rogue Devices

Rogue device is an unauthorized node on the network; rogue device can be a router, switch, or simply a laptop, which acts as DHCP or any server type. When a client enters the network, both legal and rogue servers will offer services for the client. For example, DHCP servers will offer IP addresses, default gateways and other services, if the client accepts services from rogue DHCP, it may lead to sniff all client data or the client cannot access the network resources which lead to denial of services.

Rogue DHCP servers can be toppled by means of intrusion detection systems [40] with appropriate signatures, as well as by some multilayer switches, which can be configured to drop the packets. In addition, we can use 802.1X as a way of preventing entry and IPsec as a way of preventing access; it becomes evident that in order to attempt to solve the rogue machine problems in different ways we have to analyze our threats, consider our risk stance, and choose the appropriate way to protect our system[41].

IV. CONCLUSION

IPv6 is the future for sure; the main reason for migrating to use IPv6 is the exhaustion of IPv4 address pool, not any security issues. The security concerns between IPv4 and IPv6 are largely the same, packet transporting techniques are almost unchanged, and the upper-layer protocols: the application layer and transport layer are not affected, therefore, most of the attacks on IPv4 can be applied on IPv6, the concept of the attacks remain the same, but types and attacks' behavior are changed.

IPsec is mandatory in IPv6, which make it more secure, on the other hand, network administrator will be blind, because all the data are encrypted, and network administrators cannot apply network policies between any two IPv6 nodes.

Many organizations got IPv6 running on their networks and they do not even realize it; because many computer operating systems by default enable both IPv4 and IPv6, which could cause security vulnerabilities if one of them is less secure than the other . IPv6 security vulnerabilities currently exist, as the popularity of the IPv6 protocol increases, the number of threats increases too, Table III. proves that most tools used in IPv4 attacks have new versions that work on IPv6, which mean; IPv6 didn't eliminate the attacks, it just change the behavior and techniques for the attacks.

TABLE III. IPV6 ATTACK TOOLS [42][43]

Attack	IPv6 Attack Tool
Reconnaissance	NMAP6, Dnsdict6, Alive6,Thcping6
Flooding	6tunneldos, Flood-router6, Flood-advertize6
Smurf	Smurf6 ,rsmurf6
Rogue Device	Fak-router6
Man In The Middle	Redir6, Parasite6, Toobig6

REFERENCES

[1] J Postel, Internet Protocol, DARPA Internet Program Protocol Specification (September1981), RFC 791.

[2] Christos Douligeris, Aikaterini Mitrokotsa, DDoS attacks and defence mechanisms : classification and state-of-the-art ,Computer Networks: The International Journal of Computer and Telecommunications Networking, Vol. 44, Issue 5 , pp: 643 - 666, 2004.

[3] Z. Chen, L. Gao, K. Kwiat, Modeling the spread of active worms,Twentyv, Second AnnualJoint Conference of the IEEE Computer and Communications Societies (INFOCOM), Vol. 3, pp. 1890 1900, 2003.

[4] R. L. Mitchell. The grill: John Curran. Computer-World, Apr. 2010.

[5] K. Egevang, P. Francis, The IP Network Address Translator (NAT), RFC 1631, May 1994.

[6] G.Huston, GeoHuston http://www.potaroo.net/tools/ipv4/index.html, DEC. 2013.

[7] S Deering, R Hinden, Internet Protocol, Version 6 (IPv6) Specification,RFC 2460 ,December 1998.

[8] Google Statistics, www.google.com/intl/en/ipv6/statistic.html,2012.

[9] International Organization for standerd ISO/IEC 7498-1

[10] V.Cerf, The Internet Activities Board, RFC 1160, May 1990.

[11] BGP Analysis Reports Retrieved, Jan 2014.

[12] J. Rajahalme, A. Conta, B. Carpenter, S. Deering, IPv6 Flow Label Specification,, RFC3697 March 2004.

[13] David C. Plummer, An Ethernet Address Resolution Protocol, RFC 826, NOV 1982.

[14] P. Nikander, J. Kempf, E. Nordmark, IPv6 Neighbor Discovery (ND) Trust Models andThreats, RFC 3756, May 2004.

[15] S. Kent, K. Seo,Security Architecture for the Internet Protocol, RFC4301, December2005.

[16] S Deerind, R. Hinden, Internet Protocol, Version 6 (IPv6) Specification, RFC 2460,December 1998.

[17] S Deerind, R. Hinden, IP Version 6 Addressing Architecture, Feb 2006, RFC 4291.

[18] A. Conta, S.Deering, M. Gupta, Internet Control Message Protocol (ICMPv6) for theInternet Protocol Version 6 (IPv6) Specification, RFC 4443, March 2006.

[19] T. Narten, E. Nordmark, W. Simpson, H. Sliman, Neighbor Discovery for IP version 6 (IPv6), RFC 4861, September 2007.

[20] S. Deering, W. fenner, B. Haberman, Multicast Listener Discovery (MLD) for IPv6,RFC 2710, October 1999.

[21] R. Vida, L. Costa, Multicast Listener Discovery Version 2 (MLDv2) for IPv6, RFC3810, June 2004.

[22] S. Thomson, T. Narten, T.Jinmei, IPv6 Stateless Address Autoconfiguration, RFC 4862,September 2007.

[23] J. Arkko, J. Kempf, B. Zill, P. Nikander, Secure Neighbor Discovery (SEND), RFC3971, March 2005.

[24] T. Chown, IPv6 Implications for Network Scanning, RFC 5157, March 2008.

[25] NMAP.Org, NMAP IPv6 Tool, Retrieved 2013.

[26] Cisco, Understanding and configuration DHCP snooping, December 2012.

[27] P. Nikander, J. Kempf, E. Nordmark, IPv6 Neighbor Discovery (ND) Trust Models andThreats, RFC 3756, May 2004.

[28] CISCO, IPv6 Breif, White Paper, Oct 2011.

[29] T. Chown, S. Venaas, Rogue IPv6 Router Advertisement Problem Statement, RFC6104, Feb. 2011.

[30] T. Aura, Cryptographically Generated Addresses, RFC 3972, March 2005.

[31] E. Guttman, L. Leong, G. Malkin, Users Security Handbook, RFC 2504, February 1999.

[32] A. Conta, S. Deering, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, RFC 2463, December 1999.

[33] E. Vyncke, S. Hogg, IPv6 Internet Security for Network, Cisco Press, JUN 2009.

[34] C. Kaufman, P. Hoffman, P. Eronen, Internet key Exchange Protocol Version 2 (IKEv2),RFC 5996, SEPTEMBER 2010.

[35] T. Chown, S. Venaas, Rogue IPv6 Router Advertisement Problem Statement, RFC6104, Feb 2011.

[36] G. Malkin, R. Minnear, RIPng for IPv6, RFC 2080, January 1997.

[37] A. Kamra, H. Feng, V. Misra, A. Keromytis, The Effect of DNS Delays on WormPropagation in an IPv6 Internet, IEEE INFOCOM, March 2005.

[38] C. Zou, D. Towsley, W. Gong, S. Cai, Routing Worm: A Fast Selective Attack WormBased on IP Address, Workshop on principles of Advance and Distributed Simulation, June 2005.

[39] C. Kaufman, Y. Nir, P. Eronen, Internet Key Exchange Protocol Version 2 (IKEv2),RFC 5996, Sep. 2010.

[40] H. Eltaj, F. Najjar, H. Alsenawi, M. Najjar, Intrusion Detection and Prevention Response based on Signature-Based and Anamoly-Based: Investigation Study, International Journal of Computer Science and Information Security, June 2013 .

[41] I. Halil, Detecting and Preventing Rogue Devices on the Network, SANS Institute, Aug2007.

[42] NMAP.org, Network Mapper, May 2012.

[43] Thc.org, thc-ipv6, Dec 2013.

[44] Supriyanto, Iznan Husainy Hasbullah, Raja Kumar Murugesan and Sureswaran Ramadass, "Survey of Internet Protocol Version 6 Link Local Communication Security Vulnerability and Mitigation Methods", Vol 30, no 1, pp 64-71, Jan-Feb 2013.

[45] Ala Hamarsheh, "Assuring Interoperability between Heterogeneous (IPv4/IPv6) Networks without using Protocol Translation", Vol 29, no 2, pp.114-32, Mar-Apr 2012.