Scientific Journal of Impact Factor (SJIF): 5.71
e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 6, Issue 02, February -2019

IPv6-A Literature Review

Lokesh Kumar[1]

[1]Department of Computer Science & Engineering,College of Engineering and Technology, Bhubaneswar

Abstract —*This paper is about the Internet Protocol version 6 (Ipv6) which is the newer version of the protocol being used for communication over the Internet. It has been in existence for over 20 years.But the migration to Ipv6 has been slow because of many security considerations. As the popularity of Ipv6 has risen so has the number of threats.Therfore this paper covers all major aspects of Ipv6 and its security vulnerabilities and in the summarizeswith the countermeasures that can be employed.*

Keywords-*Ipv6, ICMPv6, DHCPv6, IPsec, MIPv6, SEND, SLAAC, IDS, IPS, Security Vulnerabilities*

I. INTRODUCTION

The internet protocol version 6 (IPv6)[1], specified in 1998, is intended to replace IPv4 in the worldwide Internet mainly due to the address exhaustion of IPv4. IPv6 extremely enlarges the address space from 32 bits to 128 bits. 20 years after its release, over 25% of all Internet-connected networks advertise IPv6 connectivity[2]. Most of the world "ran out" of new IPv4 addresses between 2011 and 2018 but still is expected to last till the next decade[3].
IPv6 is an better, improved version of IP that is designed to coexist with IPv4 while providing better internetworking capabilities than IPv4, and resolving unanticipated IPv4 design issues and takes the Internet into the 21st Century [4],[5]. This paper gives an overview of the Ipv6 specifications, features, transition methods, security vulnerabilities, counter-measures and finally a conclusion.
The following changes were introduced with Ipv6:
i. Expanded Addressing capabilities: Increase in IP address size from 32 bits to 128 bits
ii. Header Format Simplification: It was done to limit the bandwidth cost of the Ipv6 header.
iii. Improved Support for Extensions and Options: Changes in the encoding process of IP header options results in more efficient forwarding, lesser strict limits on the length of options, and flexibility for introducing new options in the future
iv. Flow Labeling Capability[6]
v. Authentication and Privacy Capabilities: Extensions to support authentication, data integrity, and (optional) data confidentiality are specified for IPv6.
vi. Stateless auto-configuration: The ability for nodes to determine their own address.
vii. Multicast: Increased use of efficient one-to many communications.
viii. Jumbo grams: The ability to have very large packet payloads for greater efficiency.
ix. Mobility: Simpler handling of mobile or roaming node.

II. SPECIFICATION

Here an overview of the internet protocol IPv6 is given. Its major aspects are explained here such as address space enhancement and the new IPv6 headers and the us of ICMPv6.Also the transition methods from IPv4 to IPv6 is explained.

2.1. Addressing

Each IPv6 address has a length of 128 bits(theoretically, the total numbers of unique IPv6 address is $2^{128} = 3.4 * 10^{38}$, which would be $6.67 * 10^{17}$ addresses per mm^2 surface of the earth. But due to the division of network and interface-IDs, this quantity is not realistic.) which is presented in eight blocks of hexadecimal values. To make these IPv6 addresses more easily to read, two abbreviations exist that are shown in Table 1.1. To have the IPv6 address still unique, the second abbreviation can be used only once.

Table 1. IPv6 address abbreviation

Full IPv6 Address	2001:0db8:0000:0000:cafe:0000:1200:f1b2
Deleting leading zeros in each block	2001:db8:0:0:cafe:0:1200:f1b2
Double colon for consecutive zeroes	2001:db8**::**cafe:0:1200:f1b2

An IPv6 address is splitted into the global routing prefix, the subnet ID and the interface ID (Table 1). The global routing prefix identifies the range of addresses allocated to a site, whereas the subnet ID defines a link within a site which is set by the network administrator. The interface ID identifies an IPv6 interface on a subnet and must be unique within that

subnet. . An IPv6 address is written such as the Classless Inter-Domain Routing (CIDR) notation in IPv4, i.e., the length of the prefix (global routing prefix + subnet ID) is added after a slash to the IPv6 address: ipv6-address/prefix-length. For example, a valid IPv6 prefix is 2001:db8:72ed::/48, whereas a valid IPv6 address be 2001:db8:72ed::417f:8c7f:f12d:96f7/64[7].

For all addresses, the interface ID has to be exactly 64 bits long which makes the differentiation between network & host portion more prominent since the boundary is everytime the same. The interface ID is created with the Modified EUI-64 Format Interface Identifiers, which takes the 48 bit long MAC address of the Ethernet card and expands it to the 64 bits needed for the interface ID[8]. This has the side effect that an interface will always have the same interface ID independent of what site it resides or what prefix it currently uses. This actually makes a node trackable, for example in the case of a mobile phone which accesses the same Internet server from different locations. To thwart this privacy issue, another procedure for creating the interface ID was proposed, namely the privacy extensions, [9]. It generates a complete random interface ID and renews it after a predefined time range. In this way, a unique IPv6 node cannot be tracked anymore in conjunction with its interface ID, even if the computer resides on another network[10]. A host with privacy extensions enabled has at least two global unicast addresses: one with the EUI-64 format and one with the random ID. Temporary addresses are only used by clients, not servers. "An interface that accepts inbound connections and has a DNS name cleary cannot have a private address, but it is still possible to use different addresses for outbound connections",[11].

2.2. Header

Header is a major component of internet protocol as it holds the source and destination addresses and is processed by every router along the path of an IP packet. Therefore, the IPv6 header was constructed in a more direct way than in IPv4, which results in a view changes: the mere IPv6 header has a fixed length of 40 bytes instead of varying from 20 to 60 bytes as in IPv4, [12]. This makes the processing on routers and other network related machines more efficient since they do not have to deal with different header sizes. The IPv6 header has no header checksum field anymore, since checksums are calculated on the upper layers such as Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). This also accelerates the processing of IPv6 packets on a router since no checksums have to be calculated after decrementing the Hop Limit value.

0 3 4 11 12 15 16 23 24 31

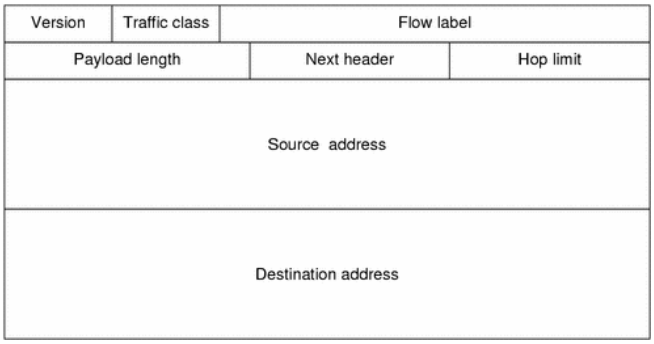

Figure 1. IPv6 header (without extensions)

The source and destination addresses take the biggest part of the header and only a few option fields are present. The Payload Length specifies the length of the data carried after the IP header, inclusive its potentional extension headers. Since this value has a size of 2 byte, it limits the maximum packet payload to 64 KB. The Next Header field describes what kind of packet follows after the initial IPv6 header. This can either be a "normal" protocol such as TCP, UDP, ICMPv6, OSPF, or it can be an extension header, which will be located between the IPv6 header and the TCP or UDP header. In IPv4, this field was called "Protocol Type". The values of the protocols are defined by the IANA, [13]. The last option field in the IPv6 header is the Hop Limit. It holds the number of routers (hops) to be visited before the packet will be discarded. Each router along the path decrements this value by 1. If the packet reaches a Hop Limit value of 0 before it has arrived at its destination, the router discards it. This is mostly the same functionality as the "Time to Live" (TTL) field in IPv4, whereas it is properly named in IPv6, since the TTL field actually holds no time in seconds but rather a counter for hops. Finally, the both address field Source Address and Destination Address contain the originator and the intended recipient of the IPv6 packet. Since an IPv6 address is 128 bits long, these field are both 16 bytes in size.

2.2.1. Extension Headers. IPv6 uses extension headers [1] to indicate the transport layer information of the packet (TCP or UDP) or to extend the functionality of the protocol. Extension headers are identified with the Next Header (NH) field within the IPv6 header. Within an IPv6 header, bits 48–55 (8 bits) form the next header field, which identifies the header following the IPv6 header. These optional headers indicate what type of information follows the IPv6 header in the formation of the packet. Extension headers are defined for a variety of functions that augment the IPv6 network layer. IPv6 header is followed by extension headers and are a sequential list of optional headers.

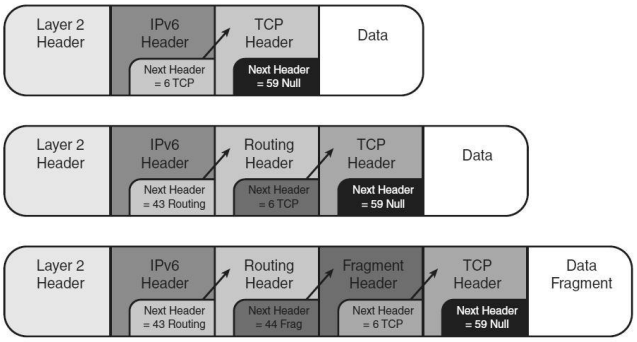

Figure 2. Example of the extension headers

A uniform format for extension headers has also been proposed.[14].Here the Next Header field has a 8-bit selector which identifies the type of header immediately after the extension header.Hdr Ext Len field has a 8-bit unsigned integer which indicates the length of the extension header in 8-octet units not including the first 8 octets and the Header Specific Data field is of variable length.

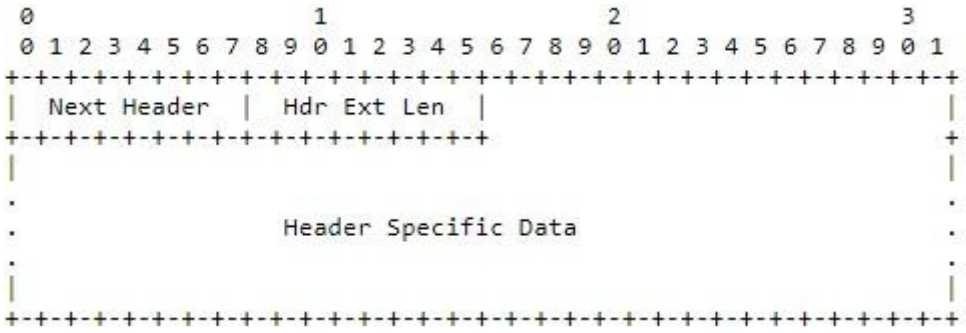

Figure 3. Uniform format of extension header

Some of the Extension Headers are as follows-

i. Hop-by-Hop Options Header: The Hop-by-Hop Options Header carries optional information that must be processed by every node along the path of the packet. It has a next header value of 0 and is used in conjunction with other features such as the router alert for the Multicast Listener Discovery (MLD).

ii. Routing Header: A Routing Header stores a list of intermediate nodes that should be visited through the packets flow to their final destination. It is specified by a next header value of 43. There are two types of routing headers specified: Routing Type 0 (RH0), which can be used for normal IPv6 packets and Routing Type 2 (RH2), which works in conjunction with the Mobile IPv6 approach.

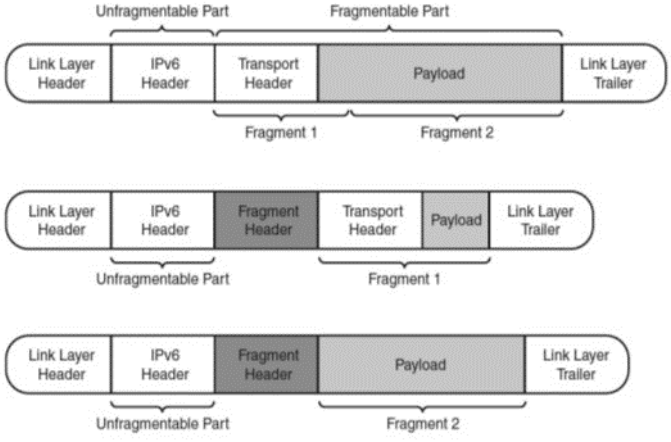

Figure 4. Packet fragmentation

iii. Fragment Header: Fragmentation is the process in which a node splits one packet into smaller packets in order to travel through a connection which has a smaller maximum transmission unit (MTU) than the actual packet size. The destination node will then resassemble these smaller packets to the entire packet.In IPv6 only the source node is able to fragment packets which is different than IPv4 where every router in the path could fragment packets. It first runs the Path MTU Discovery procedure to recognize the Path MTU. If fragmentation is needed, the node inserts a Fragment header, which contains among other things the Fragment Offset and an Identification. With these information, the destination node can reassamble the fragments.

iv. Destination Options Header: The destination options header carries additional information that are only examined by the destination node. It has a next header value of 60 and is, for example, used with Mobile IPv6.

2.3. Internet Control Message Protocol Version 6 (ICMPv6)

The Internet Control Message Protocol Version 6 (ICMPv6) is the successor of ICMPv4 and is mandatory for the IPv6 network to operate at all. IPv6 nodes uses ICMPv6 to report errors encountered in processing packets, and to perform other internet-layer functions, such as diagnostics ICMPv6 "ping"[15]. ICMPv6 is an essential part of IPv6, and the base protocol (all the messages and behavior required by this specification) MUST be fully implemented by every IPv6 node.Therefore, it replaces not only ICMPv4 along with other network related protocols such as the Address Resolution Protocol (ARP) for the resolving of link-layer addresses or the Internet Group Management Protocol (IGMP) which is used for establishing of multicast group memberships. ICMPv6 messages have a next header value of 58. They contain a Type value for specifying the ICMPv6 message, which ranges from 1-127 for error messages and from 128-255 for informational messages. The echo-request message which is used to ping a destination has the message number 128, while the echo-reply message has the number 129.

2.3.1. Error messages. There are four types of ICMP error messages[15]:

i.Type 1-The Destination Unreachable message is sent if a IP packet cannot be delivered. It uses the Code field of the ICMPv6 header to specify the reason, such as "No route to destination" or "Address unreachable" and is sent to the source address of the invoking packet.

ii. Type 2-Packet Too Big mesage is sent backward to the souce if the router cannot deliver the IP packet due to smaller maximum transmission unit (MTU) values on the forwarding link.So it stores the MTU of the next hop link to inform the originating node to fragment its future packets with this size. This feature is used by the "Path MTU Discovery" [16] which identifies the smallest MTU along the path from the source to the destination node by sending IP packets to the destination node until a direct reply instead of a Message Too Big error message comes back.

iii. Type 3-Time Exceeded message is sent back to the originating node if the Hop Limit value in the IPv6 header reaches its limit of 0. This could either indicate a routing loop or a Hop Limit value that was set too low from the source node.

iv. Type 4-Parameter Problem is sent if an IPv6 node is unable to process an IPv6 packet due to an error in its header or any of the extension headers.

All ICMPv6 error messages contain the original IPv6 header and as much data from the original IPv6 packet as possible, until the ICMPv6 message size is fulfilled. These information reveals which connection they belong to and are used by stateful firewalls for their security decisions.

2.3.2. Neighbor Discovery. Neighbor Discovery is a family of various functions with are related to other IPv6 nodes on the same link such as finding routers and other nodes, maintaing reachability information about active neighbours (Neighbor Unreachability Detection-NUD) or configuring their own unique IPv6 addresses via Auto configuration (Duplicate Address Detection-DAD).Five ICMPv6 messages specified are [17]-

i. Router Solicitation message-It is ICMPv6 informational message type 133, and is sent by a node in order discover any routers on the link. So, its sent to all routers multicast address ff02::2.

ii. Router Advertisement message-If a router is present on the link, it responds quickly with this Router Advertisement message which is type 134 message which contains the following information[18]:The "managed address configuration" (M) flag informs the node whether stateful configuration is to be used (M flag set = DHCPv6) or it should use stateless configuration. The "other configuration" (O) flag tells the node to use stateless configuration but with the inclusion of other non-address related information such as DNS servers will be accessbile via DHCPv6.The "Home Agent" (H) flag is used with mobile IPv6. At last, the Options field can hold several information such as the source link-layer address of the router, the MTU for that link, the prefix information in order to allow the nodes to auto configure themselves, or IPv6 addresses of recursive DNS servers [19].

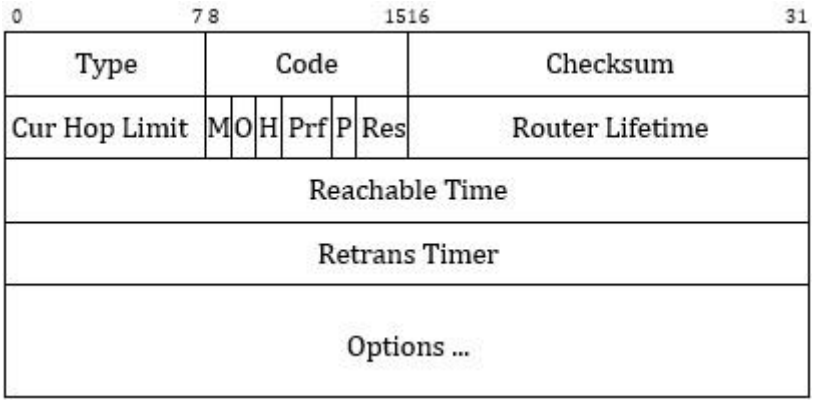

Figure 5. ICMPv6 router advertisement message

iii. Neighbor Solicitation and Neighbor Advertisement-They are type 135 and 136 messages.They together have two functions:link layer address resolution(done by ARP in IPv6), and Neighbor Unreachability Detection (DAD) mechanism.Suppose, a node A wants to resolve the link layer address corresponding to the IPv6 address of node B,then node A sends a Neighbor Solicitation message to the solicitated-node multicast address of node B which is derived from its IPv6 address.Afterwards, node B responds with a Neighbor Advertisement message in which it transports its link-layer address.The NA holds flags such as Router (R) flag which indicates whether the node is a router, the Solicited (S) flag which is set if the advertisement is sent in response to a solicitation, and the Override (O) flag which indicates that the node should overwrite its neighbor cache entry with the just gathered information. Each node maintains a Neighbor Cache in which all IPv6 and link-layer addresses of its neighbors are listed. This is equivalent to the ARP cache in IPv4. It has five states (INCOMPLETE, REACHABLE, STALE, DELAY, and PROBE)[17] and is automatically updated after each communication with a neighbor or after receiving a Neighbor Advertisement. After a period of time, the entries are outdated and deleted.
4-Redirect Message-Its a type 137 message. It is sent from a router to a node so as to indicate a more appropriate first-hop node along the path to the destination network. This can either be another different router on the same link or a directly connected neighbor node in the case that the originating node did not expect it on the same link because of other used IPv6 prefixes. A redirect message contains two addresses, the Target Address which is the best next hop and the Destination Address which is the address of the location of the original IPv6 packet.

2.3.3. SEcure Neighbor Discovery (SEND). SEND was developed so as to protect the messages as neighbor discovery can be used for a number of attacks.It should be used in situations where physical security is not ensured[20]. With a public/private key pair, an IPv6 node generates its interface ID based on the IPv6 prefix, its public key and a third option called Modifier/Nonce. All parameters are hashed with SHA1 and the least significant 64 bits are taken as the interface ID. This IPv6 address is called a Cryptographically Generated Address (CGA)[21]. In addition, there are a few new Neighbor Discovery Protocol options such as the CGA option or the RSA signature options.For all ND messages, especially the NA answer during a link-layer resolving, the source node can sign its message and adds this signature and its own public key in the appropriate option to the NA message. With these parameters, the receiving node can verify the signature and is assured that the sender of the NA, hence the proposed link-layer address, is correct. SEND can also use certification paths to certify the authority of routers. This requires certificates issued by a trusted certification authority (CA), which adds even more complexity for the network administrators, but is able to differ between legitimate routers and those which are spoofed by an attacker.SEND only assures that the binding of an IPv6 address and the appropriatie link-layer address is correct,i.e., that no attacker can spoof the correct IPv6 address, but does not indicate whether the IPv6 node is trustworthy on the network.

2.4. Address Configuration
A huge new feature with IPv6 is the possibilty that a node can autoconfigure its IPv6 addresses. There is no need of any manual configuration on a host and no DHCPv6 server is required. Only the routers on each link must be configured with their addresses and Router Advertisement (RA) messages. The address autoconfiguration [22] is a major new feature compared to IPv4.

2.4.1. Stateless Address Autoconfiguration (SLAAC).SLAAC provides the ability to address a host based on a network prefix that is advertised from a local network router via RA. SLAAC is implemented on the IPv6 client by listening for these local RA's and then taking the prefix that is advertised to form a unique address that can be used on the network. For this to work, the prefix that is advertised must advertise a prefix length of 64 bits (i.e., /64); SLAAC will then dynamically form a host identifier that is 64 bits long and will be suffixed to the end of the advertised prefix to form an IPv6 address. Originally, the host identifier was formed using the EUI-64 rules (the same that are used to form link local addresses) and many devices still use this method. However, some Microsoft operating systems by default do not use this original method. Instead, they take advantage of some additional privacy extensions[9].
One problem ocuurs with the use of autoconfiguration: the IPv6 node has not yet learned the IP addresses of DNS servers which are mandatory for an IP node to work properly. In IPv4, this information comes with the use of DHCP or is configured manually. To solve this problem, there are three different approaches being used: An administrator can set up an DHCPv6 server in stateless mode, which means that the DHCPv6 server does not allocate IPv6 addresses but does assign other information such as DNS servers or the domain search list, [23]. This works in conjunction with the "other configuration" (O) flag set in the Router Advertisement. The node parses the O flag in the RA and sends an information request message to the DHCPv6 server with the option request option "DNS recursive name server", [24]. The DHCPv6 server returns with an information reply message which contains the IPv6 addresses of the DNS name servers.
Another method to distribute DNS servers is the recursive DNS server (RDNSS) option in the Router Advertisement messages which embeds the IPv6 addresses of the RDNSS directly in the RA, [19]. This avoids using a DHCPv6 server and therefore satisfies the autoconfiguration feature without the need of any other procotols. The third technique is to hard-code multicast DNS server addresses in the soft-/hardwares directly, e.g. ff02::fb or ff05::fb for Multicast DNS mDNSv6[25].

2.4.2. Dynamic Host Configuration Protocol Version 6 (DHCPv6).DHCPv6 is a client/server protocol that provides managed configuration of devices.The mode in which the DHCPv6 server assigns IPv6 addresses to node is called Stateful DHCPv6, since the DHCPv6 server must store a state of every assigned IPv6 addresses. DHCP is the "stateful address autoconfiguration protocol" and the"stateful autoconfiguration protocol"[26].

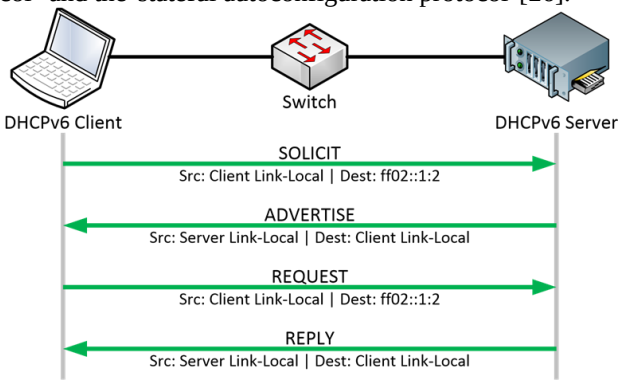

Figure 6. DHCPv6 message exchange

Compared to DHCPv4, a few more messages types are introduced while some other types are renamed. A straightforward DHCPv6 message exchange contains the following four messages, as depicted in Figure 6: the client sends a SOLICIT to the all-dhcp-agents multicast address in order to discover the DHCPv6 servers, which will reply with an ADVERTISE message to the link-local IPv6 address of the client. This message already contains an IPv6 address among the other information. The client then sends a REQUEST message to the selected DHCPv6 server, which replies with a final REPLY message.

2.5. Further Aspects

2.5.1. IPSEC. IPsec is a set of protocols that secure IP communications. It implements numerous security principles such as authentication, integrity, or confidentiality and is well-known for its use with Virtual Private Networks (VPNs). IPsec works with both internet procotols, i.e., IPv4 and IPv6, but with the difference that it is placed directly in the standards of IPv6 whereas it was retrofitted for IPv4. Since IPv6 works with an end-to-end communication model without the usage of NAT, IPsec can be used in more modes of operation and has lower administrative complexity than with IPv4. However, IPsec with IPv6 is not better secured than with IPv4. IPsec is not the cure for all security concerns with IPv6. It provides specific functionality such as cryptographic transforms to mitigate threats and vulnerabilities from the network layer up through the application layer. It does not replace other security functionality dealing with malware, spam, access controls, intrusion detection, and so forth", [11].

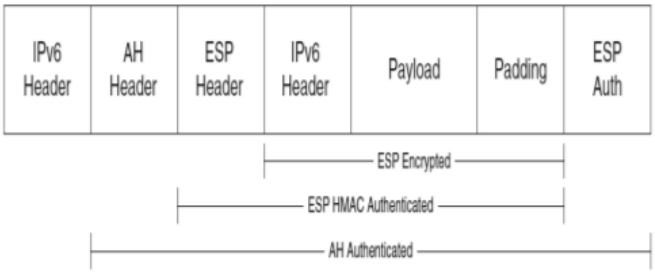

Figure 7. IPv6 ipsec packet

2.5.2. Mobile IPv6 (MIPv6). In the last few years the popularity for mobile devices such as smartphones etc has grown exponentially. These devices are able to access the Internet and they are expected to hold their connections as they are moved around just like cellphones retain the phone calls when they are moved. . Since most Internet connections are based on TCP which is defined by the pairs of source & destination IP addresses and ports, they will be disrupted if the mobile device changes its IP address. Therefore, the approach of Mobile IPv6 (MIPv6) specifies a way for mobile devices to keep their IPv6 address, i.e., their connections, even when they move to a different network (roaming)[27]. Here a mobile device, when at home, registers itself by a home agent. When the mobile device accesses a new network it gets a new IPv6 address, called the care-of-address, communicates with its home agent, and establishes a bidirectional tunnel with it. In that way it can further communicate with its former IP address, since the home agent forwards all IP packets through the tunnel to the care-of-address of the mobile device.

2.6. Transition Methods

Since it was not applicable to do a worldwide change from IPv4 to IPv6 side by side, IPv6 was designed to coexist with IPv4 in order to have an easy and continuous transition over a long duration which might take several years[10]. The basic transition methods are described as follows [28].

2.6.1. Dual-Stack. The most direct transition method is to have both IP stacks activated concurrently. This technique acts as an IPv4-only node when communicating with other IPv4 nodes and similarly behaves as an IPv6-only node when communicating with other IPv6 nodes. Both internet protocol versions can coexist on the data link layer because they are identified by different Ethertype values. In all modern operating systems, IPv6 is always preferred over IPv4 if there exist a native IPv6 connectivity. If a network runs with dual-stacked nodes, all intermediary devices must either be dual-stacked, too, or two devices with each serving one protocol must exist. For example, all routers/firewalls must either have a dual-stack implementation or there exists one IPv4-only firewall and one IPv6-only firewall. The same applies to the services such as the routing protocols running on the routers, and the security policies enforcement on the firewalls, etc. One disadvantage of the dual-stack transition method is the excessive consumption of memory on all devices because of two routing tables, two routing processes, etc., i.e., one for each protocol.

2.6.2. Tunnels. If a native IPv6 connectivity is not available by the ISP a tunnel can be used to forward IPv6 traffic over an existing IPv4 infrastructure. It encapsulates an IPv6 packet as the payload of an IPv4 packet. At both ends of a tunnel, a dual-stack node sends/receives the IPv4 packet and does the en/decapsulation of the inner IPv6 packet. "For instance, if your provider still has an IPv4-only infrastructure, tunneling allows you to have a corporate IPv6 network and tunnel through your ISP's IPv4 network to reach other IPv6 hosts or networks. Or you can deploy IPv6 islands in your corporate network while the backbone is still IPv4", [29]. This tunneling process operates with 41 IP protocol number. A tunnel can be a Site-to-Site tunnel which operates between two IPv6 networks, or a Remote Access tunnel in which a single host connects to an IPv6 network. In the first case, a dual-stack router can offer an IPv6 prefix and all hosts in that network can access the IPv6 network. The second case offers IPv6 to only one single machine. There exists a few different variants of IPv6 tunnels:
i. Configured Tunnel, also called 6in4 tunnel, encapsulates a complete IPv6 packet in an IPv4 packet. This Site-to-Site tunnel can easily be configured on routers as only the tunnel endpoint addresses (IPv4) and the routed IPv6 networks must be known. 6in4 tunnels cannot traverse NAT/NAPT devices (since they rely not on TCP or UDP) and they have no built-in security mechanisms. Furthermore, they must be configured manually.
ii. Dynamic 6to4 tunnel which does not need any specific configuration on the tunnel endpoint (automatic tunneling). Its IPv6 prefix is derived from the currently used IPv4 address. Therefore, the IPv6 address space 2002::/16 is reserved for that tunnel method. If two IPv6 islands behind 6to4 routers want to communicate with each other, they can extract the IPv4 address of the tunnel endpoint directly from the destination IPv6 address. In order to communicate with a native IPv6 node, a 6to4 relay router is needed, i.e., a dual-stack node that receives the encapsulated IPv6 packet via its IPv4 node and delivers the IPv6 packet via its local IPv6 node. Such 6to4 relay routers can be accessed via the IPv4 anycast address 192.88.99.1. A 6to4 tunnel can either be set up on a single IPv4 host which has a global routable IPv4 address, or on a IPv4 router that could then offer the IPv6 prefix to the complete inside network (which could house many dual-stacked hosts).

2.6.3. Protocol Translation. This protocol translation adds the possibility for IPv4-only nodes to communicate with IPv6-only nodes and vice versa. It dynamically maps IPv4 addresses to IPv6 addresses. Since the address spaces of both internet protocols differ in its size, this mapping cannot be a a one-to-one mapping. Furthermore, specific algorithms must be used to change the complete internet protocol header. This is more complicated than simply changing the IP address as done with standard NAT for IPv4 networks. It must be dealt with modifying ICMPv6 error messages or UDP checksums that have to be calculated differently in both IP versions. Via an application layer gateway (ALG), DNS queries and replies are rewritten/modified to let the clients connect to the right IP addresses. Not all IPv6 extension headers can be used and multicast traffic cannot be forwarded. Since the protocol translation breaks the end-to-end communication, IPsec cannot be used, and "because the DNS ALG translates DNS requests, the mechanisms of DNSSEC will not work either", [29]. Summarized, protocol translation should only be deployed if no other translation method is applicable, [29].

III. SECURITY VULNERABILITIES

3.1. Tracking The Identity Of The User

Traditional interface identifiers for network adapters has a 48-bit address called an IEEE 802 address. It contains a 24-bit company ID (also called the manufacturer ID), and a 24-bit extension ID (also called the board ID). The combination of the company ID, which is unique in nature and assigned to each manufacturer of network adapters, and the board ID, which is uniquely assigned to each network adapter at assembly time, produces a globally unique 48-bit address. This 48-bit address is also called the Media Access Control (MAC) address. In IPv4-based Internet, a general Internet user connects to an Internet Service Provider (ISP) and obtains an IPv4 address using the Point-to-Point Protocol (PPP) and the Internet Protocol Control Protocol (IPCP). Each time the user connects, a different IPv4 address might be obtained. Because of this process, the identity of users on the Internet is often unknown. So, it is difficult to track a dial-up user's traffic on the Internet on the basis of IP address [30]. And this has created an environment where attackers can easily operate, without their targets knowing much about the source of the messages. Also, the usage of Network Address

Translation (NAT) is often misunderstood as a security protection measure because it hides the internal addresses and thus secures the internal network topology. NAT breaks the use of the full end-toend communication model that IP Security (IPsec) needs to be fully effective. For a IPv6-based dial-up connections, the user is assigned a 64-bit prefix after the connection is made through router discovery and stateless address auto-configuration. If the interface identifier is always based on the EUI-64 address (as derived from the static IEEE 802 address) as shown in figure 8, it is possible to identify the traffic of a specific node regardless of the prefix, making it easy to track a specific user and their use of the Internet.

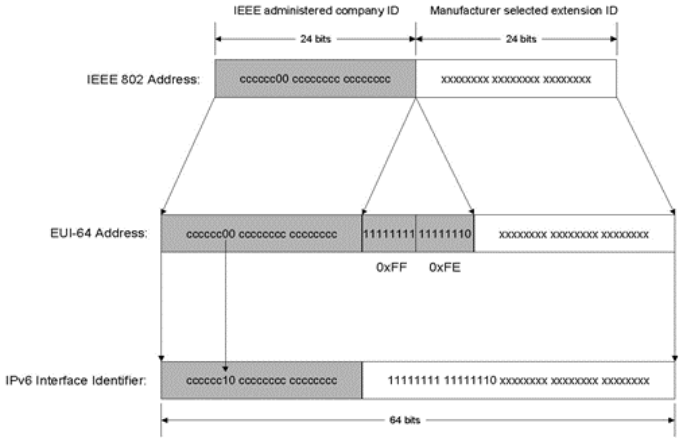

Figure 8. The conversion of a universally administered, unicast IEEE 802 address to an IPv6 interface identifier.

3.2. Attacks against IPv6 protocol

3.2.1. Multicast Security Vulnerability. Multicast Vulnerability is considered one of the deficiencies of the Ipv6 specification. IPv6 has no broadcast method of packet forwarding and instead relies on multicast for all one to-many communications. IPv6 uses multicast for neighbor discovery, Dynamic Host Configuration Protocol (**DHCP**), and traditional multimedia applications. If an attacker could send traffic to these multicast groups and all the systems that are part of these groups respond, that would give the attacker information that could be used for further attacks [23]. The attacker would have information about all the routers within the IPv6 network and all the DHCPv6 hosts. These are critically important nodes for aiding an attacker in determining what other computers are contained within the network, either through neighbor caches, binding updates, or DHCPv6 logs.Its arguable that this phase known as reconnaissance phase is no longer required with IPv6.To launch a blind attack (no return traffic) against all DHCPv6 servers, the attacker simply has to send his packet to FF05::1:3.[31]. The Reconnaissance phase uses multicast messages to reveal potential targets on the network but does not actually attack them.

For an attacker the full potential of the multicast is in sending spoofed messages in order to attack all host at once or at least to use all hosts on a network to attack a single host. The former could be used to run a denial of service attack (DoS) against the whole network while the latter one is a kind of a distributed denial of service attack (DDoS) in which many hosts try to interrupt a single host. These types of attacks are called “amplification attacks" because they multiply the quantity of packets, i.e., the payload on the network.

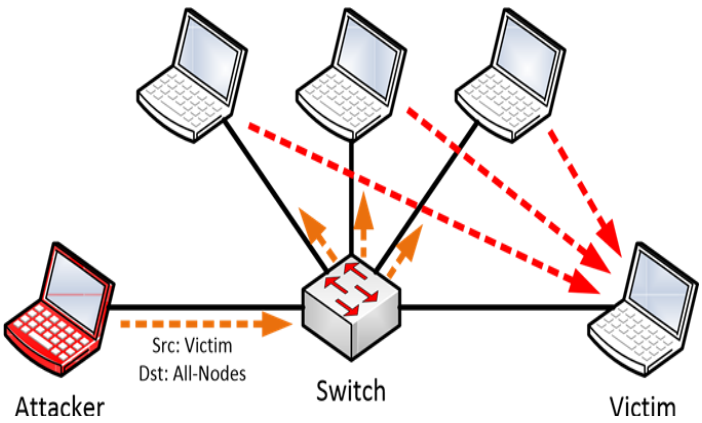

Figure 9. The attacker sends a single spoofed packet which is amplified by all IPv6 nodes on the link and directed to the victim.

A spoofed source address in a packet destined to a multicast address could result in amplification of the return traffic toward the target spoofed source address, which is called a Smurf attack, shown in figure 9 .In reverse smurf attack, the

source address is all-nodes multicast and the destination address is victims unicast.Whereas total flood ocurrs when source and destination addresses are all-nodes multicast.
IPv6 has a few advantages such as eliminating broadcast packets which reduces network congestion, but it has also a few disadvantages such as the possibility for attackers to send spoofed multicast packets which will be delivered to any node participating in the appropriate multicast group. Since multicast packets are mandatory for a correct functioning of IPv6 nodes, it cannot be disabled entirely. Fortunately, these attacks are not that critical because they reveal only basic information about the IPv6 nodes such as their addresses, or they try to run DoS attacks. Since few more powerful and dangerous DoS tools and even attacks that can gather confidential information via man-in-the-middle attacks exists, their is no reason for excessive dread about the concept of multicast.

3.2.2. Extension Header. The Ipv6 protocol specifications have not limited the usage of extension headers as shown in figure 2, they could potentially cause problems if used maliciously [31].The strucure of Ipv6 headers makes it difficult to inspect packets. While routers have a simple job since they only need to examine the IPv6 destination address and the Hop-by-Hop Options header, its the firewalls that have to enforce the security policy and must identify and parse through all existing extension headers since the upper-layer protocol information reside in the last header. An attacker can create an Ipv6 packet that meets the Ipv6 protocol specifications and chain unlimited of extension headers in a big list in order to pass firewall and intrusion detections and prevention systems. He can also cause a denial of service attack if an intermediary device or a host is not capable of processing lots of chained extension headers and might fail. A Hop-by-Hop options header carries optional information and has a typical structure of 8-byte(1-byte) next header field, an 8-bit(1-byte) header length field, and a variable length options field and its inspected by every node in packet's path. Hop-by-Hop Options headers should appear only once within any IPv6 packet, but there are no limits to the number of options that the packet can contain. Within a single Hop-by-Hop header, there could potentially be many options, and the options can appear in any order.There could also be customized, yet unknown, options within the header that would be skipped by nodes along the path because they would not know how to parse them. Alternatively, the unknown options can cause problems for nodes with IPv6 implementations that cannot parse a packet like this. Pad1(Inserts 1 octet of padding into the options of the header) and PadN(inserts variable amount of padding into the options of the header)options can also appear multiple times and have variable sizes.In a Hop-by-Hop Options header, the use of padding ensures that an IPv6 packet ends on an octet boundary. Padding typically is not needed because the header and option headers are already aligned on an 8-octet boundary. PadN options are required to have a 0-byte payload, so if these fields contain any information, it is an error or something deliberate. These padding options could be used to contain information as part of a covert channel. These padding options could also cause other problems, such as firewall resource consumption, if they are used incorrectly. Therefore, it is a good idea for firewalls to check that PadN options contain no payload and that the data within the padding is not part of some type of attack.

Figure 10. Covert channel inside the padding of an extension header

Usage of RH0 has several security issues such as dos can occur between two nodes if RH0 contains the Ipv6 addresses of two nodes and if the payload is huge.Also an Ipv6 packet with appropriate routing header may bypass certain firewall configurations as show in figure 11.

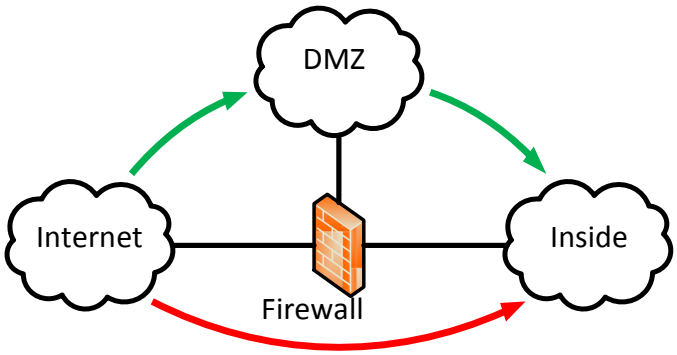

Figure 11: Firewall bypassing with RH0: the firewall would block a direct connection from the internet to the inside network, but allows it through the DMZ.

Firewall Evasion can be done by using Fragment Header. Each packet fragment is given a unique identifier (fragment ID) to distinguish it from all the other fragments. Each packet fragment is also given an offset value of the number of bytes the fragment is away from the initial fragmentable part of the original packet. The receiving host reassembles the

fragments by putting all the fragments back together in order and then passing the resulting complete IP packet up the protocol stack. This is a normal process on networks, but it can also lead to security issues. As the end hosts are allowed to create and reassemble fragments,an attacker could try to bypass a firewall or IDS/IPS inspection by either fragmenting his packets to many small fragments or by chaining a few extension headers before his payload in order to place the upper-layer information in a rearmost packet. Attackers can also create fragments in such a way as to exploit weaknesses in the method an end host uses to reassemble the fragments. Examples of this would be overlapping fragments, where there is an overlap in the offset and out-of-order fragments where the fragments IDs do not match correctly with the data. Another type of fragment attack involves an attacker sending an incomplete set of fragments to force the receiving node to wait for the final fragment in the set. Fragmentation attacks can also involve nested fragments or fragments within fragments, where the IPv6 packet has mult iple fragmentation headers. Fragmentation attacks are typically used by hackers with tools such as Whisker, Fragrouter, Teardrop, and Bonk [31].

3.3. Attacks Against ICMPv6

3.3.1. Router Advertisement Spoofing. A router sends Router Advertisement ICMPv6 messages (Figure 5)in order to inform all nodes on the link about its presence and its routes. In many small networks, there might be only one default router available. A layer 2 attacker can send its own Router Advertisements in order to falsify the routing tables of all hosts that are listening to RA messages. This results at least in a denial of service attack. In the worst case, all hosts will send their tra_c to the IPv6 address of the attackers router which brings the attacker in a situation in which he can see all IPv6 packets of all hosts (man-in-the-middle attack, MITM). If the attacker forwards all packets to a correct next hop router so that all connections reach their destination, the hosts will not register this attack until they dive deep into the information of their IPv6 stack. Since Router Advertisements are sent to the all-nodes multicast address, all IPv6 nodes on the link receive them. However, only hosts and not other routers must generate IPv6 addresses (via SLAAC) or change its routing tables upon
evaluating Router Advertisements.
New Default Router Man-in-the-Middle- Until now, the falsifying of the victim's routing table only lead to a denial of service attack because all IPv6 traffic is sent to the attackers machine and is then discarded. Another situation arises when the attacker forwards all received packets to the real default router so that the victims do not register any change in their workow, i.e., the attack is complete transparent for the victims. This is a kind of a man-in-the-middle attack since the attacker then resides between the victim and the default router. Another name for this attack is redirect attack[32]. In fact, this RA attack is not a complete man-in-the-middle attack because the answering packets from the Internet will go straight ahead to the victims computer. The default router knows that it has to forward any packets to an IPv6 address that sits on the same subnet as one of its interfaces. Since the router does not process the falsified RA packets from the attacker, it sends all packets directly to the victim.

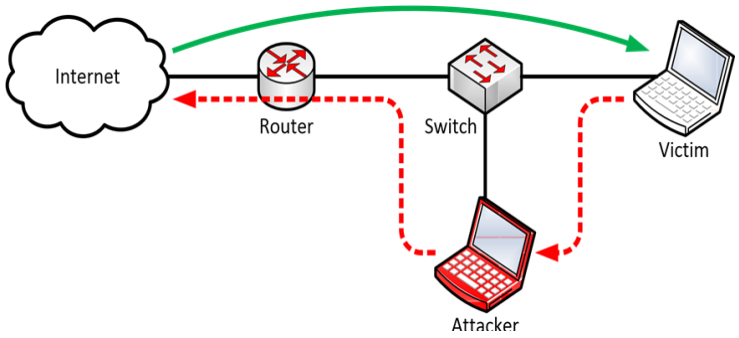

Figure 12. Router advertisement "half" man-in-the-middle attack: all initiated packets from the victim are routed via the attackers computer while the returning traffic remains untouched since the attacker only spoofs the router

Figure 12 shows this situation in which all IPv6 connections traverse through this asymmetric routing. Even though the attacker cannot intercept the whole communication from the victims, he is able to capture all packets that are sent from the victims to the Internet. With a snffer such as Wireshark [33] or tcpdump [34], this traffic can be analyzed and saved. All IPv6 addresses are visible and all plaintext communications and passwords can be read out directly. For example, all URLs that are accessed via HTTP, and all passwords that are sent with unencrypted protocols such as FTP, Telnet, POP3, and so on.

3.3.2. Neighbor Discovery Spoofing. An IPv6 node sends Neighbor Discovery messages for four different purposes:Stateless Address Autoconfiguration(SLAAC),Duplicate Address Detection(DAD), resolving of link-layer addresses, and Neighbor Unreachability Detection.This deals with the wrong insertion of neighbor cache entries in a victim's neighbor cache.
Neighbor Advertisement Spoofing during Link-Layer Resolving-An attacker can disturb the link-layer address resolving if he answers to a Neighbor Solicitation (NS) with a falsified Neighbor Advertisement (NA) which contains the link-

layer address of himself. If the victim accepts this packet, its IPv6 node will send all data link frames to the MAC address of the attacker. If the attacker then spoofs the destination node with falsified Neighbor Ad-vertisements,he performs a man-in-the-middle attack i.e he redirects the complete conversation between two parties and can read all the data as shown in figure 13.

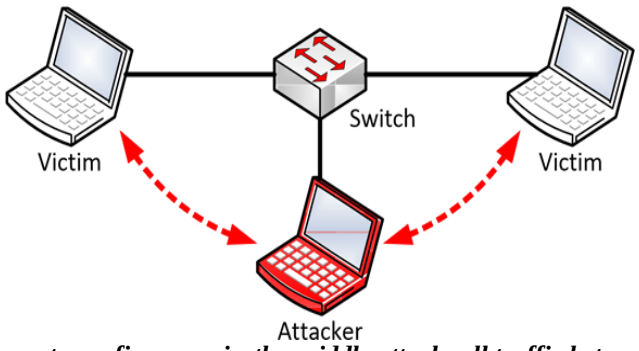

Figure 13. Neighbor advertisement spoofing man-in-the-middle attack: all traffic between two ipv6 nodes on the same layer 2 link traverses through the attackers machine

This Neighbor Discovery spoofing attack is very similar to an ARP spoofing attack in IPv4 networks, in which the attacker spoofs ARP packets with falsified MAC addresses. The primary goal for both attacks is the same: the attacker wants to be able to sniff the packets even in an switched network[35]. As the IPv6 subnet size is /64, trillions of addresses can be used but a huge number of them remain nassigned. So as Network Discovery attempts to do address resolution for large number of unassigned addresses it can be vulnerable to DoS attacks[36].This attacks can be from a malicious attacker or can result from operational tools that scan the networks for inventory and such purposes[17].

3.4. Attacks against DHCPv6

DHCPv6 is used in either stateless mode to only distribute some additional information to IPv6 clients such as DNS servers, or in stateful mode to fully allocate IPv6 addresses to IPv6 nodes. Even though the protocol changed from DHCPv4 to DHCPv6, the same attacks as in IPv4 networks are possible, i.e., DHCPv6 scope exhaustion in which a rogue client requests lots of addresses, or the installation of a rogue DHCPv6 server which allocates IPv6 addresses to IPv6 nodes and distributes falsified DNS server entries.

3.4.1. Address Space Exhaustion. Here an attacker tries to seize the complete range of available IPv6 adresses from a stateful DHCPv6 server. Unlike the address scopes in IPv4 networks which could only be a few thousand IPv4 addresses in size,DHCPv6 scopes may have a complete /64 prefix and will therefore only be exhausted after requesting $2^{\wedge 64}$= 18,446,744,073,709,551,616 different addresses, which is incapable for any attacker. Hence, the DHCPv6 starvation attack is only successful if the network administrator has configured a small IPv6 address range, e.g., a few thousand addresses. However, since the stateful DHCPv6 server must store a few bytes of information for each allocated IPv6 address, i.e., the state, an attacker can still try to ood the DHCPv6 server until its memory is fully loaded. This would end in a DoS attack against the DHCPv6 server. For DHCPv6, a single node, i.e., single MAC address can request many IPv6 addresses. Hence, port security cannot prevent any of the specific flooding attacks.

3.4.2. Rogue DHCPv6 Server. Here the attacker places an additional rogue DHCPv6 server in the network which allocates IPv6 addresses and provides falsified DNS server information. Afterwards, the attacker is able to run MITM attacks if he also provides an IPv6 router uplink to the Internet, or if he spoofes DNS replies at the rogue DNS server which is under his control which actually results in a vast security risk. With a rogue DNS server, an attacker can redirect the IPv6 node to his own servers (called “pharming") and can execute several attacks such as the spread of malware or man-in-the-middle attacks, [37,38,39]

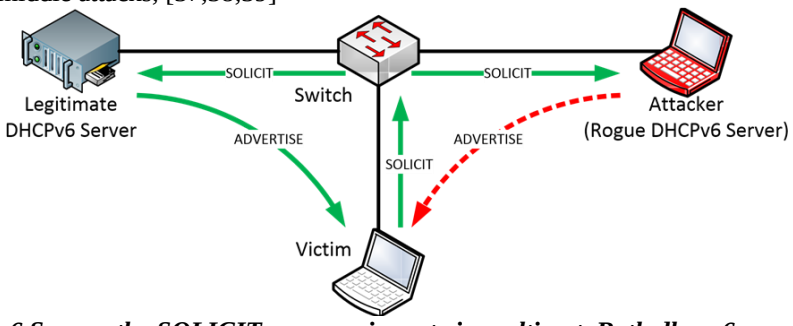

Figure 14. Rogue dhcpv6 Server: the SOLICIT message is sent via multicast. Both dhcpv6 server respond with an unicast ADVERTISE message.

Figure 14 shows a simple attack installation with the legitimate and the rogue DHCPv6 server. Since the client sends its messages via multicast, both DHCPv6 servers receive them. The THCIPv6 attacking toolkit [40] provides a DHCPv6 server spoofing tool can be used here.The 4 message exchange which occurs is the normal DHCpv6 protocol process, i.e, SOLICITATE, ADVERTISE, REQUEST, and REPLY.As a result of this attack the victim accepts the falsifies DNS server IPv6 address from the attacker and sends its future DNS queries to the proposed IPv6 addrsess.

IV. COUNTERMEASURES

1- A straightforward countermeasure for IPv6 nodes here in multicast vulnerability is to block any echo-request messages, i.e., not answering with echo-replies, or at least not answering if the requested IPv6 address is a multicast address. But since the more profound reconnaissance tools such as the Nmap SLAAC script use other techniques than echo-requests, IPv6 nodes do not have a chance to stay undetected on a local network if they communicate with each other. Also simply blocking all echo-request messages might not be the best choice for a network administrator since legitimate tasks could not use these features anymore, too. For example, to monitor intermediary devices like switches, routers or WLAN access points, a network management utility needs to ping these devices.
One countermeasure which does not allow any node to reply to each message at a very fast rate is to implement rate limiting for 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”, [31].]. It should be noted that these types of amplification attacks only work if the attacker already resides on the local subnet. In addition, he can also attack the local subnet.Hence, port statistics of the network infrastructure can reveal the attacking host quickly.Its difficult to address concerns regarding extension headers as its a balance between usability and security.For example, even if its unusual to recieve lots of small fragments which could constitute an attack, RFCs have not specified to block them.Therefore, a securty administrator must decide whether to implement strict rules or to have the Ipv6 stack work without any hassles.
Following steps can be taken in the firewall-
i.Use of IDS and IPS
ii.Blocking all unused or unknown extension headers and to review the list on a regular basis.
iii. All IPv6 packets with routing header type 0 should be blocked.
Iv. A firewall should be able to reassemble fragmented packets in order to investigate the upperlayer information of the initial IPv6 packet. It should then enforce its security policy.

2- SEcure Neighbor Discovery (SEND) is proposed to secure the appropriate messages[20]. If a host has a configured trust anchor, it will only accept routers with correct certifications. That is, an attacker could not trigger Router Advertisement spoofing attacks anymore. With Cryptographically Generated Addresses (CGA) and their corresponding public key cryptography and signatures, Neighbor Solicitations and Neighbor Advertisements could be signed and authenticated.
Limting the number of IPv6 addresses a host manages can counter a DoS attack by an attacker if he floods Router Advertisements.Also network based intrusion detection/prevention systems should be placed on switches so it can detect duplicate NA messages used in Neighbor Advertisement spoofing attack and block them or report them.
A method to allow only authenticated machines to participate on the network is Network Access Control (NAC), e.g., IEEE 802.1X. This is an IP independent security approach and requires further services such as a Supplicant, Authenticator, and Authentication Server, [35]. Once NAC is implemented, it does not thwart the mentioned IPv6 attacks, but it only allows trusted machines to enter the network. If the attacker is able to gain access to an authenticated machine, he can run these attacks as always.
Following steps can be taken in the firewall-
i. Mechanisms are to implemented in layer 2 devices to prevent layer 2 attacks such as network switches or specific IDS/IPS.
ii. IDS can alert network administrator if some unknown or spoofed RAs arrive.
iii. IPS can help detect duplicate Neighbor Advertisements as the attacker will send them in order to spoof the NA of a victim and it is abnormal that a NS is answered with two NA with two different MAC addresses

3- Dynamic Host Configuration Protocol for IPv6 (DHCPv6)[41] propses an authentication mechanism for DHCPv6 messages. It is based on the authentication design for DHCPv4, [42] and it uses the DHCPv6 authentication option to reliably identify the source of a DHCP message and confirms that the contents of the DHCP message have not been tampered with. A new IPv6 node must be authenticated and authorized before it can receive information from the DHCPv6 server. For the communication between relay agents and the DHCPv6 server, IPsec should be used. The use of manual configuration and installation of static keys are acceptable in this instance because relay agents and the server will belong to the same administrative domain and the relay agents will require other specific configuration (for example, configuration of the DHCP server address) as well as the IPSec configuration"[41]. DHCPv6 snooping can stop both Layer 7 and 2 attacks.It can be activated on switches and it provides the following-

i.Limits rate of DHCPv6 packets received by a switch port.If the threshold is exceeded, the switch gets switched off.This prevents DoS attacks.
ii. Forward DHCPv6 server replies only if they arrive from trusted ports.
An IDS can be used as it actively probes for rogue DHCPv6 servers by sending a SOLICIT message and investigates the answers. If not only legitimate DHCPv6 servers answer but other ADVERTISE messages arrive at the IPv6 node, the network is possible under attack or at least a misconfigured DHCPv6 server resides on the network.

V. CONCLUSION

In this paper, the IPv6 protocol was explained along with its security vulnerabilities. Different scopes of the security issues were also potrayed and categorized into attacks against the IPv6 protocol itself,ICMPv6 attacks and DHCPv6 attacks.
As IPv6 and IPv4 are both network layer protocols, the vulnerabilities are also similar.So network administrators and and security specialists have to gain in-depth knowlodge regarding IPv6 security vulnerabilities, to test the new security equipment and to update all running softwares on the machines if vendors provide firmware updates.New security vulnerabilities and attacks will keep rising so its better to stay informed about current security issues by using libraries such as Common Vulnerabilites and Exposure.

REFERENCES

[1] S. Deering, R. Hinden,"Internet Protocol, Version 6 (IPv6) Specification", IETF, RFC 2460, 1998
[2] "State of IPv6 DeploymenT" , ISOC, 2018
[3] "IPv4 Address Report", https://ipv4.potaroo.net/ , 2019
[4] Khaldoun, B. Khaled, B. Amer, A. "THE NEED FOR IPv6." International Journal of Academic Research, Vol. 3. No. 3. II Part. PP.431-448, Azerbaijan., 2011
[5] Minoli, D. Kouns, J. "Security in an IPv6 Environment.", CRC Press, USA, 2009
[6] S. Amante, B. Carpenter, S. Jiang, J. Rajhalme, " IPv6 Flow Label Specification", Internet Engineering Task Force :RFC 6437, 2011
[7] J. Rosenberg, J. Weinberger, C. Huitema, R. Mahy, "STUN - Simple Traversal of User Datagram Protocol (UDP)Through Network Address Translators (NATs)", Internet Engineering Task Force: RFC 3849, 2003
[8] R. Hinden, S. Deering, "IP Version 6 Addressing Architecture", Internet Engineering Task Force: RFC 4291, 2006
[9] T. Narten, R. Draves, S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", Internet Engineering Task Force: RFC 4941, 2007
[10] E. Davies, S. Krishnan, P. Savola, "IPv6 Transition/Coexistence Security Considerations", Internet Engineering Task Force : RFC 4942, 2007
[11] Sheila E. Frankel, Richard Graveman, John Pearce, and Mark Rooks,"Guidelines for the Secure Deployment of IPv6", NIST, SP 800-119, 2010.
[12] Information Sciences Institute, University of Southern California" INTERNET PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION", IETF, RFC 791, 1981
[13] Internet Assigned Numbers Authority (IANA) "Protocol Numbers", 2012
[14] S. Krishnan, J. Woodyatt, E. Kline, J. Hoagland, M. Bhatia, "A Uniform Format for IPv6 Extension Headers", Internet Engineering Task Force : RFC 6564, 2012
[15] A. Conta, S. Deering, M.Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", Internet Engineering Task Force: RFC 4443, 2006
[16] J. McCann, S. Deering, J. Mogul, "Path MTU Discovery for IP version 6", Internet Engineering Task Force: RFC 1981, 1996
[17] T. Narten, E. Nordmark, W. Simpson, H. Soliman, "Neighbor Discovery for IP version 6(IPv6)", Internet Engineering Task Force: RFC 4861,2007
[18] B. Haberman, R. Hinden, "IPv6 Router Flags Option", Internet Engineering Task Force: RFC 5175, 2008
[19] J. Jeong, S. Park, L. Beloeil, S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", Internet Engineering Task Force: RFC 6106, 2010
[20] J. Arkko, J. Kempf, B. Zill, P. Nikander, "SEcure Neighbor Discovery (SEND)", Internet Engineering Task Force: RFC 3971, 2005
[21] T. Aura, "Cryptographically Generated Addresses (CGA)", Internet Engineering Task Force: RFC 3972, 2005
[22] S. Thomson, T. Narten, T. Jinmei, "IPv6 Stateless Address, Autoconfiguration", Internet Engineering Task Force: RFC 4862, 2007
[23] R. Droms, "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", Internet Engineering Task Force: RFC 3736,2004
[24] R. Droms, "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", Internet Engineering Task Force: RFC 3646, 2003
[25] S. Chesire, M. Krochmal, "Multicast DNS", Internet Engineering Task Force: RFC 6762, 2013

[26] S. Thomson, T. Narten," IPv6 Stateless Address Autoconfiguration", Internet Engineering Task Force: RFC 2462, 1998
[27] C. Perkins, D. Johnson, J, Arkko, "Mobility Support in IPv6", Internet Engineering Task Force: RFC 6275, 2011
[28] E. Nordmark, R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", Internet Engineering Task Force: RFC 4213, 2005
[29] Silvia Hagen, "IPv6 Essentials, Second Edition", O'Reilly Media, Inc., 2006
[30] Microsoft Corporation , "Introduction to IP Version 6", White Paper, Microsoft Windows Server 2008, , USA,2008
[31] Scott Hogg,Eric Vyncke, '*IPv6 Security'*, Cisco Press, USA, 2009
[32] P. Nikander, J. Kempf, E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", Internet Engineering Task Force: RFC 3756, 2004
[33] Gerald Combs, "Wireshark - the world's foremost network protocol analyzer", http://www. wireshark.org/, 2012
[34] Van Jacobson, Craig Leres, and Steven McCanne, "tcpdump - command-line packet analyzer", http://www.tcpdump.org/, 2012
[35] Eric Vyncke and Christopher Paggen, "LAN Switch Security", Cisco Press, 2008
[36] Gelogo, Y. E. Caytiles, R. D. Park, B, "Threats and Security Analysis for Enhanced Secure Neighbor Discovery Protocol (SEND) of IPv6 NDP Security", International Journal of Control and Automation Vol. 4, No. 4. pp:179-184, 2011
[37] Sid Stamm, Zul_kar Ramzan, and Markus Jakobssonl,"Drive-By Pharming",In Proceedings of the 9th international conference on Information and communications security, ICICS'07,pp-495-506, 2007
[38] Chris Karlof, Umesh Shankar, J. D. Tygar, and David Wagnero, "Dynamic Pharming Attacks and Locked Same-origin Policies for Web Browsers",In Proceedings of the 14th ACM conference on Computer and communications security, CCS , pp-58-71, 2007
[39] Saeed Abu-Nimeh and Suku Nairk,"Bypassing Security Toolbars and Phishing Filters via DNSPoisoning", In Proceedings of the Global Communications Conference, GLOBECOM 2008,pp-2001-2006, 2008.
[40] Marc "van Hauser" Heusee, "THC IPv6 Attack Toolkit" ,http://www.thc.org/thc-ipv6/, 2012
[41] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carneys, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", Internet Engineering Task Force: RFC 3315, 2003
[42] R. Droms, W. Arbaughh, "Authentication for DHCP Messages", Internet Engineering Task Force: RFC 3118, 2001

