RESEARCH ARTICLE OPEN ACCESS

A Comprehensive Study on Next Generation Internet Protocol (Ipv6) and Security Vulnerabilities

M. Buvaneswari [1], Dr. N. Rajendran [2]
Research Scholar [1]
Bharathiar University, Coimbatore
Principal [2]
Vivekanandha Arts and Science College for Women, Sankari
Tamil Nadu – India

ABSTRACT

Internet Protocol version 6 (IPv6) is the newest version of the protocol that is used for communications on the Internet. This version has been in existence for many years. But, currently many organizations have slowed their migration to IPv6 because they realize that the security considerations and products for IPv6 might be insufficient, despite the fact that the network infrastructure is ready to support IPv6 transport. They realize that they cannot deploy IPv6 without considering the security of this protocol at first. IPv6 security vulnerabilities currently exist, and as the popularity of the IPv6 increases, so do the number of threats. This paper covers and reviews some of the fundamental vulnerabilities topics of IPv6 security, considerations, issues and threats. At the end, it summarizes some of the most common security concerns the new suite of protocols creates.

Keywords: - IPv6, IPsec, Network Security, Security Vulnerabilities

I. INTRODUCTION

IP Next Generation (IPng) was created, which then became IPv6 (RFC1883) [1]. IPv6 offers several new functions and is considered a step forward in the evolution of the Internet Protocol. These improvements came in the form of an increase of the address space, extensible headers, a streamlined header format, and the ability to preserve the integrity and confidentiality of communications. In the end of 1998 the protocol was fully standardized in RFC 2460[2]. IPv6 offers the potential of achieving increased scalability, reach ability, end-to-end interworking, Quality of Service (QoS), and commercial-grade robustness for data communication, mobile connectivity, and for Voice over IP (VoIP). The current version of the Internet Protocol, IPv4, has been in use successfully for almost 30 years and exhibits some challenges in supporting emerging demands for address space cardinality, high density mobility, multimedia, and strong security[3][4].

II. OVERVIEW OF IPv6

IPv6 is the successor of IPv4 and will replace it in the long run as the main protocol of the network layer. IPv6 is aimed at providing end-to-end communication between network interfaces even when the number of Internet participants and corresponding demand for address space keep on increasing massively, for example caused by the growing demand for Internet-enabled mobile devices. Security, Quality of Service (QoS), and reduced load for routers are further goals of IPv6 [5]. IPv6 is not downward compatible; therefore a simple switch of protocols is not possible. This is also due to various old network devices that are optimized for the use with IPv4 and hence do not support new version. IPv6 quadruples the address length of IPv4 to 128 bit. This extension leads to an exponentially growth of the address-space size to $2^{128} = 340$ un decillion. This would in theory correspond to 6.65×10^{23} addresses per square meter of the earth. Such a tremendous amount of addresses makes it possible to give a unique address to every device connected to the Internet for a practically indefinite amount of time and enables a true end-to-end communication among them.

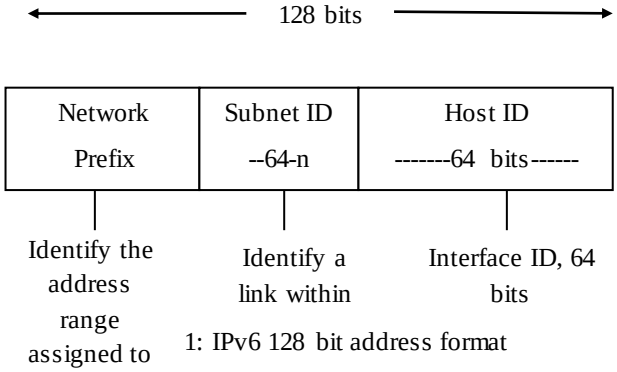
The effectively available address space is certainly smaller than theoretically possible, since large blocks are reserved for special purposes such as multicast, or for purposes yet unknown. The smallest allocation possible is furthermore a/64 prefix.

This leaves 64 bit to be assigned to network devices. While this will also lead to a lot of waste of addresses, this decision was made to improve manageability and routability of networks [6]. Moreover, there are also further standards published around IPv6 that, for example, define interoperability with other protocols or compatibility with IPv4. Basically, IPv6 serves the same purpose as IPv4 does, namely the packet-oriented connection of host systems. The following are the main features introduced with IPv6: Extended Address Space, Auto Configuration, IP Header Structure, Extension Headers, IP Security Extensions (IPsec), and Mobility, Quality of service, Route aggregation and efficient transmission [7].

a) Extended Network Address

Each IPv4 address is typically 32 bits long and written as four decimal numbers, each representing 8-bit octets and separated by decimal points or periods (e.g. 192.168.1.1). EachIPv6 address is 128 bits long (as defined in RFC 4291) and written as eight 16-bits fields in colon delimited hexadecimal notation. (e.g. fe80:43e3:9095:02e5:0216:cbff:feb2:7474).This new 128-bit address space provides a significant number of unique addresses, 2128 (or3.4x1038) addresses, compared with IPv4's 232 (or 4.3x109) addresses.

That is enough for many trillions of addresses to be assigned to every human being on the planet. Moreover, these address bits are divided between the network prefix and the host identifier portions of the address. The network prefix designates the network upon which the host bearing the address resides. The host identifier identifies the node or interface within the network upon which it resides. The network prefix may change while the host identifier remains static. The static host identifier allows a device to maintain a consistent identity despite its location in network. This enormous number of addresses allows for end-to-end communication between devices with globally unique IP addresses.



1: IPv6 128 bit address format

b) Auto Configuration

IPv6 enables plug-and-play networking, or **auto configuration**, which allows devices to configure themselves independently using a stateless protocol and to configure their IP addresses and other parameters without the need for a server. Also, the time and effort required to renumber a network by replacing an old prefix with a new prefix are reduced. Auto configuration is described in RFC4862. An IPv6 host can get an IPv6 address automatically using two types of auto configuration mechanism, stateful address auto-configuration that uses Dynamic Host Configuration Protocol version 6 (DHCPv6) to generate IPv6 address for host and stateless address auto-configuration that includes generating a link local address and generating global addresses. Whereas IPv4, hosts were originally configured manually or with host configuration protocols like DHCP, IPv6 auto configuration goes a step further by defining a method for devices to configure their IP address and other parameters automatically without the need of a server. IPv6 defines both Stateful and Stateless address auto configuration. SLAAC requires no manual configuration of hosts, minimal (if any) configuration of routers and no additional servers.

This allows a host to generate its own addresses using a combination of locally available information and information advertised by the routers. Locally available information is delivered to a host when routers advertise prefixes that identify the subnets associated with a link. In turn, a host generates an

interface identifier (IID) (see figure 1) that uniquely identifies an interface on a subnet. If a router is not available to advertise subnet prefixes, a host can only generate link-local addresses, which are sufficient for allowing communication among nodes attacked to the same link; in the presence of a router, a host will generate its link-local address in addition to other addresses.

Stateful auto configuration for IPv6 is known as DHCPv6. DHCPv6 is a client-server protocol that provides IPV6 addresses with address assignments and other configuration information.DHCPv6 is not described in the IPv6 standards as an essential component, but as more enterprises start to use IPv6, demand for DHCPv6 is growing. DHCPv6 servers assign IPv6addresses to network interfaces on a lease basis. The client may use the assigned IPv6 address for an administratively pre-determined amount of time before the lease expires. This means that IPv6 addresses assignments made by DHCPv6 servers are not permanent, and over time, more than one node may use a given IP address, but no more than one node can use an address at one time [7][8][9].

c) Simpler Header Structure

In comparison with IPv4, the IPv6 header is much simpler and has a fixed length of 40 bytes (as defined in RFC 2460). An IPv6 datagram has a structure that always includes a 40-byte base header and, optionally, one or more extension headers. This base header is similar to the header of an IPv4 datagram, though having a different format. Five IPv4 header fields have been removed: IP header length, identification, flags, fragment offset and header checksum. The IPv6header fields are as follows: Version (IP version 6); Traffic Class (replacing IPv4's type of service field); Flow Label (a new field for Quality of Service (QoS) management); Payload length (length of data following the fixed part of the IPv6 header), which can be up to 64KB in size in standard mode, or larger with a jumbo payload option; Next Header (replacing IPv4's protocol field); Hop Limit (number of hops); and Source and Destination addresses [10]. Figure 2 shows the IPv6 header format.

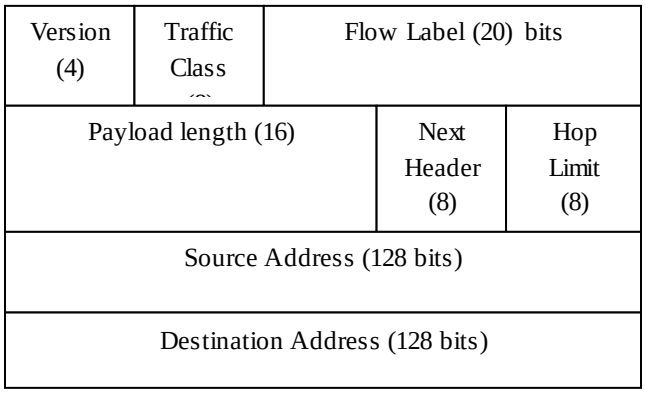


Figure 2: The IPv6 Packet Header Format

d) Extension Headers

Extension headers are defined in RFC 2460 to indicate the transport layer information of the packet (TCP or UDP) or extend the functionality of the protocol. Extension headers are identified with the Next Header field within the IPv6 header, which identifies the header following the IPv6header. These optional headers indicate what type of information follows the IPv6 header in the formation of the packet. Extension headers are a sequential list of optional headers, which can be combined. Several appear in a single packet, but only a few are used in combination. The following rules applying to extension headers: Each extension header should not appear more than once, with the exception of the destination header; The Hop-by-Hop options header should appear once and should be the first header in the list because it is examined by every node along the path; the destination option header should appear at most twice (before a routing header and before a upper-layer header), and should be the last header used in the list, if it is used at all; the fragmentation should not appear more than once and should not be combined with Jumbo Payload Hop-by-Hop option[10].

Extension headers must be processed in the order that they appear in the packet. The following order should be used: 1) IPv6 header; 2) Hop-by-Hop Options header; 3) Destination Options Header; 4) Routing Header; 5) Fragment Header; 6) Authentication Header; 7) Encapsulation Security Payload header; 8) Destination Options Header; 9) Upper-layer header. Each extension header has a unique number to be

used in the preceding header's Next Header value, which identifies the type of header that will follow so that the receiver knows how parse the header to follow. Next-header number's are defined by IANA and are sync with the protocol numbers or Pv4. Figure 3 shows the structure of an extension header and describes how they form a linked list of headers before the packet payload

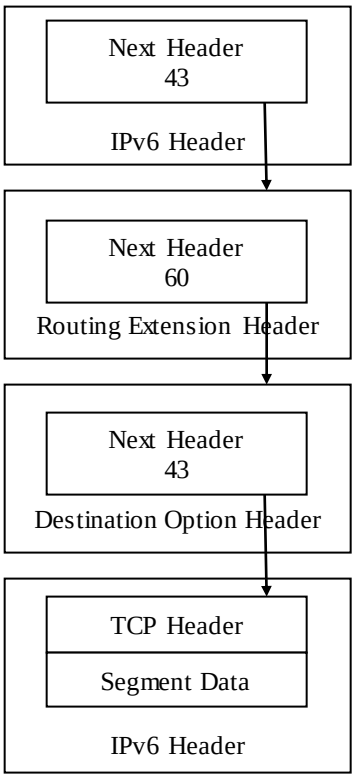


Figure 3: IPv6 datagram format including extension header

e) IP Security

IP Security, or IPsec for short, provides interoperable, high quality and cryptographically based security services for traffic at the IP layer. IPsec is a framework for securing Internet Protocol (IP) communications by authenticating the sender and thus provides integrity protection plus optionally confidentiality for transmitted data. This is accomplished by using two extension headers: the Encapsulating Security Payload (ESP) and the Authentication Header (AH). The negotiation and management ofIPsec security protections and the associated secret keys is handled by the Internet Key Exchange (IKE) protocol. IPsec is a mandatory part of an IPv6 implementation; however, its use is not required. IPsec is also specified for securing particular IPv6 protocols, such as Mobile IPv6and Open Shortest Path First version 3 (OSPFv3) [11][12].

It basically uses the cryptographic security services for protection or authentication and encrypts each IP packet of a communication session. These can be either between a pair of nodes, or between a pair of security gateways or between a security gateway and a node. It is an open standard and makes use of the following 3 basic protocols:

Authentication Header: AH provides connectionless integrity and data origin authentication for IP datagram and provides protection against replay attacks. That is it can be used by the nodes to authenticate the neighbor advertisement and the router advertisement messages.

Encapsulating Security Payloads: ESP provides confidentiality, data origin authentication, connectionless integrity, an anti-replay service and limited traffic flow confidentiality.

Security Associations: SA provides number of algorithms and data that provide the parameters necessary to operate the AH and/or ESP operations. It is used to make sure that the nodes in a network are trustworthy. It depends upon the addresses generated by the neighbor discovery, security keys etc. This SA needs to be set up between all the communicating nodes in advance. It can either use the manual mechanism or can be done automatically. As the networks are growing and there are more and more nodes less than one network the number of SAs in a single network also increases

f) Mobile IPv6

Mobile IPv6 (MIPv6) is an enhanced protocol supporting roaming for a mobile node, so that it can move from one network to another without losing IP-layer connectivity. In IPv4 already had mobility support, but with various limitations, such as, limited address space, dependence on ARP, and challenges

with handover when a device moves from one access point to another[13][14]. MIPv6 uses IPv6's vast address space and Neighbor Discovery (RFC4861) to solve the handover problem at the network layer maintaining connections to applications and services when a device changes its temporary address. Mobile IPv6 also introduces new security concerns such as route optimization (RFC4449) which secures data flow between the home agent and the mobile node [15][16].

g) Quality of Service (QoS)

IP treats all packets alike, as they are forwarded with the best effort treatment and no guarantee for delivery through the network. TCP adds delivery confirmations but has no options control parameters, such as bandwidth allocation or delay. Enhanced policy-based networking options to prioritize the delivery information are now offered to achieve QoS. Within the IPv6 header two fields can be used for QoS, the Traffic Class and Flow Label fields (see figure 2). The new Flow Label field and an enlarged Traffic Class field in the main header allow for more efficient and finer grained differentiation of the various types of traffic. The flow Label field can contain a label identifying or prioritizing a certain packet Flow such as voice over IP (VoIP), or videoconferencing, both of which are sensitive to timely delivery [10].

III. IPV6 PROTOCOL SECURITY VULNERABILITIES

a) Extension Headers Vulnerabilities

IPv6 header itself does not represent any security vulnerabilities. Rather it is how these packets are created and processed that can lead to security issues. An example of this is extension headers which could potentially cause problems inside networks if used maliciously by a user. An attacker can perform header manipulation on the extension headers to create several attacks. An IPv6 packet that meets the specification protocol could be created with an unlimited number of extension headers linked together in a considerable list, so a packet like this can cause a DoS of intermediary systems along the transmission path or at the destination. Such crafted packet might also pass through the network without causing any problems or even been detected by Firewalls and Intrusion Prevention Systems (IPS) [17].

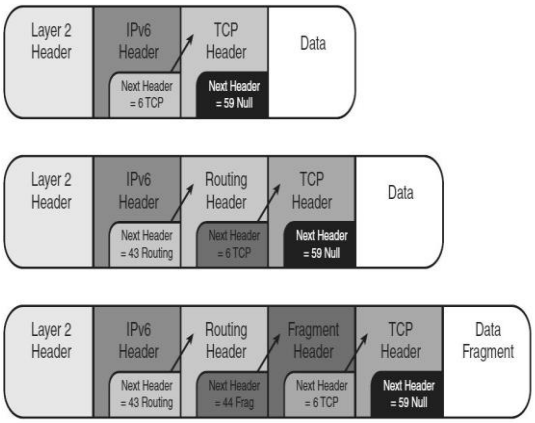


Figure 4: Example of the Extension Headers.

Figure 4 shows the structure of an extension header and describes how they form a linked list of headers before the packet payload. There are many more types of extension headers available for use in IPv6 packets, but this figure shows how they are arranged in the packet. A packet with a large chain of extension headers could fragment the payload into a second fragmented packet that eventually would not be detected by a firewall that usually is only looking at the initial fragment. Solutions to these types of attacks involve filtering of the extension headers or having specialized products that have specific rules for handling only the extension headers allowed.

b) Hop-by-Hop and Destination Options Header

Hop by hop option header is the only extension header that will be processed by routers along the packet journey to destination. This extension header is placed in the first order of IPv6 extension header chain. It may contain more options and each option could appear multiple times with various sizes as shown in Figure 5. This could be exploited by an attacker to make DoS attack by manipulating inconsistent options. The DoS attack could be launched by forming IPv6 packets with large number of options. As every router has to look at each option carried by the header, it will be difficult to control. In addition, if all routers along the path get affected by

this attack, packet transmission will be in problem. Potential security issue is present within the option field, where one of the options is the Router Alert option. Misuse of this option could degrade the CPU performance of router [18][19].

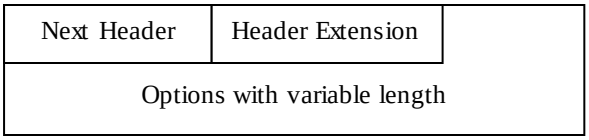


Figure 5: Format of Hop by Hop Option Header

The joint analysis of these two headers is due to the fact that Hop-by-Hop Options Header and Destination Option Header present the same structure, which consists of an option header, with an 8-bit next header field, an 8-bit header length field, and option length field and the rest of the option data, they are used for different purposes. Hop-by-Hop Options Header is used to carry optional information that must be examined by every node along a packet's delivery path and is identified by a Next Header value of 0 in the IPv6 header [20]. On the other hand, the Destination Options header is used to carry optional information that need be examined only by a packet's destination node(s). The Destination Options header is identified by a Next Header value of 60 in the immediately preceding header. Currently, only a few Hop-by-Hop/Destinations options are defined:

- Pad1 option: The Pad1 option is used to insert one octet of padding into the Options are a of a header. If more than one octet of padding is required, the Pad N option, described next, should be used, rather than multiple Pad1 options.
- Pad N option: The Pad N option is used to insert two or more octets of padding into the Options area of a header. For N octets of padding, the Opt Data Len field contains the value N-2, and the Option Data consists of N-2 zero-valued octets.
- Tunnel Encapsulation Header Option: Encapsulates other packets within IPv6 packets.
- Router Alert option: All routers along the path must process this option header.
- Jumbo payload option header: Indicates a jumbo packet.
- Home Address option: Mobile IPv6 packet containing home address of mobile node.

Hop-by-Hop headers should appear only once within an IPv6 packet, but there are no limits to the number of options that the packet can contain. The options can also appear in any order; they could also be optimized, but options within the header could be skipped by nodes along the path because they would not know how to parse them. Alternatively unknown options can cause some problems for nodes with IPv6 implementations that cannot parse a packet like this. Pad1 and Pad N options can also appear multiple times and have variable sizes. In Hop-by-Hop Options header or Destination Options Header, using padding only ensures that an IPv6 packet ends on an octet boundary. Padding typically is not needed because the header and option header are already aligned on an 8-octet boundary. These padding options could be used to contain information as part of a covert channel. A covert channel is a communication path that allows transferring information in a way that violates a system security policy. Because of their concealed nature, detecting and preventing covert channels are obligatory security practices. Covert channels can be created by embedding one protocol within another protocol, and it is possible to use IPv6 protocol itself as a covert channel. IPv6 addresses, flow label, error messages, control messages, and other fields could be used to hide communications. The bits in these fields can be used to send data between two hosts over the course of many packets. This could also cause other problems, such as firewall resource consumption if they are used incorrectly. It is recommended for firewalls to check that Pad N options contain no payload and that the data within the padding is not part of some potential attack. To observe how this covert channel works, we will generate an IPv6 packet that has a large Pad N Hop-by-Hop Options header.

c) Routing Header – Type 0 (RH0)

The Routing header is used by an IPv6 source to list one or more intermediate nodes to be visited on the way to a packet's destination. The IPv6 type 0

routing header packet is delivered to the destination address as specified in the IPv6 packet header. However the IPv6 destination node should now inspect the routing header of the packet, and if the type 0 routing header is present and if the Segments Left counter in the routing header is non-zero then the destination node is responsible for swapping the destination address with the next address in the routing header (as pointed to by the Segments Left counter), decrementing the Segments Left counter ,and forwarding the packet onward to this next destination which is now in the IPv6 destination address of the IPv6 packet header[21][22].

If the packet filtering does not have capability to process routing header, attacker could access the filtering system to gather secret information. The information may be used to generate malicious packet with routing header to perform attacks on the IPv6 network. If an IPv6 packet has single RH0 that contain more intermediate nodes addresses, same address may appear more than once. This is also a vulnerability that allows attacker to construct such packet that will be processed many times between two RH0 inside the packet. Attacker may also launch a packet to be amplified along the path between two remote routers. This will lead to network congestion. Thus, a legitimate packet is difficult to be transmitted in this way [23].

d) Fragmentation Header

In IPv6, all links must handle a datagram size up at least 1280 bytes. Therefore, very small fragments are suspicious. Attacks that use a large number of very small fragments are very disruptive and should be prevented. In IPv6 networks, there is no reason to have a fragment smaller than 1280 bytes unless the packet is the final fragment and the more fragments bit is set to zero. In IPv6 networks, attackers can easily leverage the use of fragmentation to circumvent security measures. Fragmentation is usually used to obfuscate the data and force the firewall to pass the information, even though the firewall is not able to decipher the content of the packet after it is fragmented. This is also known as an IDS/IPS evasion technique3.

In addition, the usage of fragmentation header in IPv6 also introduces security vulnerability that does not appear in IPv4. The first security hole is when the fragments overlap that is not specified in RFC 2460. It could be used by attackers to bypass the filtering system in the receiver. Attackers can form the following fragment by changing the TCP header such as, change the ACK = 0. By doing this, the receiver will think that the packet received in a connection is a request instead of response. RFC 5722 stated that this security hole is more dangerous in IPv6 than in IPv4. This is because a fragment in IPv6 may contain source and destination port that are exploitable by attackers [24]. To avoid the negative impact of fragment overlapping, it is important to consider the packet fragmentation. If the fragmentation is required by sender, it must not create overlapping. When the packets reach the destination that needs to reassemble, the receiver has to discard the datagram with fragment overlapping indication.

The second security hole is the predictable value of fragment identification field. The usage of a global counter for setting the fragment identification field may generate predictable values. If this happens, it may potentially result in information leakage that can be exploited by a malicious node [25]. This can be done by determining the packet rate at which a given system is transmitting information. It also can be used to perform a DoS attack by sending *packet too big* report from a third party. The victim then replies a packet with fragmentation header to the third party. Identification value inside the packet can be used to forge IPv6 packets resulting in sending malicious fragment from attacker. Identification field on fragmented packets is very important. Thus, the value has to be unpredictable. This can be done by performing destination cache entry look up before sending an IPv6 packet. In the cache if the last fragment identification value exists, the next value should be incremented.

e) Unknown Option Headers

Routers and Firewalls should drop packets which contain unknown extension headers. As they do not understand them, they cannot process them, so they waste precious resources by forwarding them.

Besides, these unknown extension headers might be part of a crafted packet, so it is safer to drop them.

f) Reconnaissance on IPv6 Networks

Reconnaissance of the target is the first phase of any attack. Computer hackers first assess the target and try to evaluate the easiest way to penetrate the defenses and the best way to exploit vulnerabilities. Attackers typically start their attacks by first finding a victim by using ping sweeps [26] on the target's position. Another way to perform reconnaissance is by checking registries (e.g whois), checking DNS (e.g. nslookup), checking trace route discovery, and using popular search engines to discovery information about the IP address that some organization owns. By performing these steps, an illegitimate user would identify computers that could be further investigated.

Due to larger addresses, IPv6 relies on DNS. DNS is therefore likely to be a target for attackers. The aim of an attacker is to gather as much information as possible about the information stored from DNS servers, in order to increase the probability of success of subsequent attacks. Another technique that could be used by attackers is simply a DNS scan, trying for examplea.foo.com, then b.foo.com then c.foo.com and so on [27]. Most attacks could not succeed without reconnaissance. Even though the act of scanning is not considered an attack, we need to limit them as a part of good-defense approach to securing networks.

g) Layer 2 and Layer 3 Spoofing

With IPv4 networks an illegitimate user can create packets that do not have a legitimate source address. In this type of network, it is also common for network administrators to disable source routing of packets which would allow an attacker to receive the return traffic. Due to the hierarchical addressing structure of IPv6 this kind of attacks would be limited to perform. Typically IPv6 address blocks are allocated to companies by Internet Service Providers (ISP), so those addresses should be the only ones used when that company generates Internet traffic. Therefore, if packets being sent by a company have source addresses different from their allocated address block, these packets should be dropped.

h) ICMPv6

The IPv6 specifications redefine the Internet Control Message Protocol (ICMP) of IPv4 with a number of additions and changes. The resulting protocol is documented in RFC 4443[28] and called ICMPv6. ICMPv6 is an integral aspect of the IPv6 specification. It reports errors if packets cannot be processed properly and sends informational messages about the status of the network. An ICMPv6 error message provides useful information back to the source of the IPv6communications about any errors that might have occurred in the connection. Error messages use types 0 through 127, whereas informational messages use types 128 to 255 [28]. The IANA maintains a list of ICMPv6 type numbers5.

Typically, ICMPv6 messages are sent when an IPv6 packet cannot reach the destination. Are encapsulated and sent as the payload of IPv6 packets. Because they are carried in IPv6 packets, they are unreliable. Figure 6 shows the relationship of the ICMPv6 message and the IPv6packet.

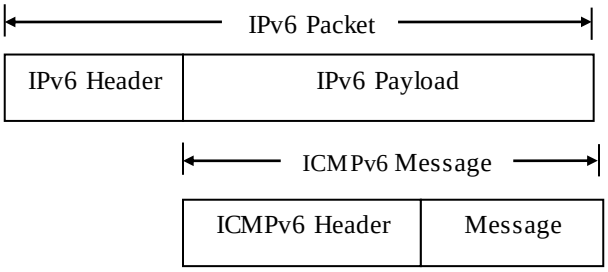


Figure 6: Relationship of the ICMPv6 Message and the IPv6 packet

An operational IPv6 network depends upon proper implementation and functionality of ICMPv6.To achieve secure IPv6 operations, it is crucial that network administrators and managers understand the design of ICMPv6 and how it functions. Managers of IPv4-only networks should consider adding the capability of detecting ICMPv6 traffic to enhance security on their networks. ICMPv6 provides IPv6

with administrative and network diagnostic functions. ICMPv6 provides familiar capabilities like ping and destination unreachable. In IPv6, as in IPv4, ping can be used by network administrators as a diagnostic tool to confirm that a node's address is properly configured and responsive to specific ICMPv6 requests, called echo requests.

IV. IPV6 PROTOCOL SECURITY VULNERABILITIES IN WIDE AREA NETWORK

The success of IPv6 will be evaluated over the next years for its ability to mitigate the threats that exist now on the current IPv4 Internet. These threats have the potential do deny service to critical services and spread malware. Because illegitimate users can forge packets, so filtering based on IP address is a requirement. When connected to the Internet one of the main security measures is indeed to perform these policies of ingress and egress.

Securing a service provider's network is also an important area that requires special attention. The way a service provider secures its network directly impacts the security of the Internet as a whole. Service Providers use BGP extensively, so securing this routing protocol require special care. Providing secure Internet access is also a challenge for service providers. Also, many customers have critical services running on their networks, so they are usually connected to multiple service providers for adding some reliability to their networks. This chapter covers all these aspects with an emphasis on the mechanisms used to secure a network when connected to the global IPv6 Internet. As the Internet is evolving from IPv4 to IPv6, so are the threats. Packet-flooding is possible using both IP versions in a similar fashion. However, Internet worms operate differently in IPv6networks. Distributed Denial of Service (DDoS) attacks are also possible in IPv6, but there are new ways to track them, which involves the use of tracing back an attack toward its source to stop the attack and finding out the identity of the attacker. In this section we focus our attention in packet flooding, issues related to multicast addresses, worms, DDoS and Botnets.

a) Packet Flooding: IPv6 does not use broadcasts as a form of communication. One could hence assume that the impact of packet flooding is limited, but this is not true. IPv6 relies on multicast, and these multicast addresses might be used for traffic amplification. For example, an attacker on a subnet can try to send traffic to the link local all nodes multicast address (FF02::1) and the link routers multicast address (FF02::2).

b) Multicast Address Vulnerabilities: IPv6 relies on multicast for many functions that were performed with broadcasts in IPv4. In fact, IPv6 has no broadcast method of packet forwarding and instead uses multicast for all one too many communications. IPv6 uses multicast for Neighbor Discovery, Dynamic Host Configuration Protocol (DHCP) and for traditional multimedia applications. Because IPv6 relies heavily on multicast, there will be issues with attackers sending traffic to multicast addresses. Multicast groups such as FF05::2 (All IPv6 routers) and FF05:1::3 (All DHCP servers) may be the targets.

c) Internet Worms: A Worm is a type of malware particularly destructive because it spreads automatically through the network by exploiting known or unknown vulnerabilities. Given IPv6 large address space, the activity of worms in the Internet and its spreading ability may be affected. IPv6worms must have more advanced techniques to surpass the problem of scanning IPv6 addresses to spread. As these worms need to be more sophisticated, more code is required, and the size of the worm will increase which will make it more difficult for the worm to spread.

d) Ingress and Egress Filters: One of the important aspects of perimeter security is filtering at the organization's borders. If we are an ISP, our network borders are other service providers and our customers. If we are an enterprise, our borders are ISPs and other business partner organizations. BCP84/RFC3704 covers the best practice for IPv4 networks which can be easily adopted by IPv6 networks. Points where ISPs network, interconnect customers and other ISP networks are locations where filtering should occur. Regarding to filtering allocated addresses service providers needs to be careful about the address space that they are using and assign to their customers [29].

e) Prefix Delegation Issues: Prefix delegation is used to assign a network address prefix to a user site, configuring the user's router with the prefix to be used for each LAN. This is one of the methods for delegating IPv6address prefixes to an IPv6 subscriber's network, which is described by RFC3769.Broadband customers could be allocated a /48, /56 or /64 network prefix depending on service provider's policies and their CPE would allow the customer's hosts to perform Stateless Address Auto-

Configuration (SLAAC). This technique could be used to uniquely allocate the addresses, and the Neighbor Discovery Protocol (NDP) and Duplicated Address Detection (DAD) can be used to avoid addressing conflicts. Before allowing the customer on the network, services providers might want some type of authentication. With the aim to have more control over the subscriber, service providers can use DHCPv6 rather than SLAAC. DHCPv6 is used for the automatic configuration of IPv6 nodes [30].

V. IPV6 PROTOCOL SECURITY VULNERABILITIES IN LOCAL AREA NETWORK

This section will give emphasis to attacks performed at Layer 2 of the Open Systems Interconnection (OSI) model, focusing only on IPv6 security. Layer 2 ensures the reliability of the physical layer (Layer 1), where standards define how data frames are recognized and provide the necessary flow control and error handling at the frame level. If Layer 2 is compromised, an attacker can perform attacks on upper-layer protocols using techniques such as Man-in-the-middle (MitM). By this an attacker is able to intercept any traffic that allows him to insert himself in clear text communication, such as Telnet or HTTP or even encrypted traffic such as SSL or SSH. To perform Layer 2 attacks, an attacker should be physically near the target.

a) Layer 2 Vulnerabilities: Although IPv6 is a Layer 3 protocol, we need to give special attention to the messages that adjacent IPv6 routers use to communicate, which is performed over a Layer 2 link. IPv6 routers need to discover each other's with the help of the Neighbor Discovery Protocol (NDP) which runs over ICMPv6 and not directly over Ethernet like Address Resolution Protocol in IPv4networks. Due to the fact ICMPv6 cannot be completely filtered by firewalls or by router access lists, the importance of ICMPv6 in IPv6 networks makes it desirable for attackers.

b) Stateless Address Auto configuration Issues: IPv6 provides a mechanism for an easier configuration of IPv6 hosts named Stateless Address Auto configuration (SLAAC). It is stateless because unlike DHCP in IPv4 environment, SLAAC does not keep state, which is the actual leased IPv6 address. With SLAAC routers exchange periodically multicast router advertisements (RA) messages which are transported over ICMPv6as type 134. Typically routers also transmit RAs in response to Router Solicitation (RS) messages, also over ICMPv6 but now as type 133. SLAAC does not provide any authentication mechanism so a malicious user can send rogue RA messages and pretend to be the default router. This can be accomplished by an attacker which injects false information into the routing table of all other hosts. As a result all nodes send their packets leaving the subnet to the malicious host. Besides capturing the traffic, adversary can cause a Denial of Service by drop all packets sent by adjacent nodes to a new default route advertised in the RA message, which could or not exist.

c) Privacy Extension Address Issues: One of the benefits of the IPv6 over IPv4 is its capability for automatic interface addressing. By implementing the IEEE's 64-bit Extended Unique Identifier (EUI-64) format, a host can automatically assign itself a unique 64-bit IPv6 interface identifier without the need for manual configuration or DHCPv6. This could be accomplished on Ethernet interfaces by referencing the unique 48-bit MAC address, and reformatting that value to match the EUI-64 specification. RFC2373 describes the conversion process which is performed in two steps. The first step is to convert the 48-bit MAC address to a 64-bit value. To do this, the MAC address is break into two 24-bit halves: the Organizationally Unique Identifier (OUI) and the NIC specific part. The 16-bit hex value 0xFFFE is then inserted between these two halves to form a 64-bit address [31].

d) Neighbor Discovery Protocol Issues: The Neighbor Discovery Protocol is a protocol in the Internet Protocol Suite used in IPv6, is sent to an Ethernet multicast address. It operates Layer 2 and is responsible for address auto configuration of nodes, determining the Link Layer addresses of the nodes, discovery of the other nodes on the link, duplicate address detection, finding available routers and Domain Name System (DNS) servers, address prefix discovery, and maintaining reach ability information about the paths to other active neighbor nodes (RFC 4861). The protocol defines five different ICMPv6 messages types to perform functions for IPv6 similar to those ARP and ICMP performed in IPv4. NDP essentially follows the ARP mechanism. An IPv6 multicast Neighbor Solicitation (NS) message is sent to all nodes in the Layer 2 network using ICMPv6 message type 135. The ICMPv6payload contains the destination IPv6 address. When received, the

destination router answers with a Neighbor Advertisement (NA) message, using ICMPv6 type 136, which contain its MAC address in the ICMPv6 payload.

e) Redirection Issues: ICMPv6 provides a mechanism named Redirection. Routers send redirect packets to inform a host of a better first-hop node on the path to a destination. Hosts can be redirected to a better first-hop router but can also be informed by a redirect that the destination is in fact a neighbor. The latter is accomplished by setting the ICMP target address equal to the ICMP destination address.

f) Duplicated Address Detection Issues: To prevent duplicated addresses, IPv6 provides a mechanism called Duplicated Address Detection. This must be used before using any IPv6 address, including link-local addresses. This procedure occurs always when a host changes its own IPv6 address or reboot. For that a host sends a Neighbor Solicitation message asking for the resolution of its own address, and it should never get a response, otherwise it means that another host was using the same IPv6 address.

VI. IPV6'S TRANSITION MECHANISMS

Transition from IPv4 to IPv6 will not be achieved overnight, and for a certain period of time both will coexist. The Internet Engineering Task Force (IETF) has therefore developed several transition mechanisms, such as tunneling and dual-stack configurations (supporting both IPv4 and IPv6) [32]. It is crucial for network designers and administrators to understand the security implications of the transition mechanisms in order to apply proper security mechanisms, such as Intrusion Detection mechanisms and Firewalls.

Dual-Stack: A mechanism to provide complete support for both IPv4 and IPv6 in hosts and routers [33]. The basic way for IPv6 nodes to remain compatible with IPv4 nodes is by providing a complete IPv4 implementation. These nodes are called "IPv6/IPv4 nodes" or "Dual-Stack nodes". The nodes have two protocol stacks (IPv4 and IPv6) enabled and use IPv6 to contactIPv6 nodes and IPv4 to contact IPv4 nodes. Figure 7 shows the relationship between the dual stack and single stack IPv4.

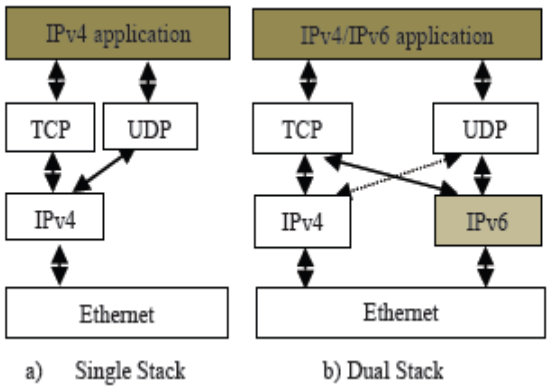


Figure 7: IPv4/IPv6 dual stack in relation to the IPv4 stack

Tunnels: Hosts or routers send and receive IPv6 packets using an overlay network of tunnels established over an IPv4 network or over an MPLS network. This mechanism allows IPv6networks to connect each other using IPv4 network. The five main tunneling techniques are used:

- IPv6 manually Configured Tunnel;
- IPv6 over IPv4 Generic Routing Encapsulation (GRE);
- Intrasite Automatic Tunnel Addressing Protocol ISATAP;
- Automatic IPv4-compatible tunnel;
- Automatic 6to4 tunnel;

Protocol Translation: A protocol translator that acts as a proxy between the IPv4 and the IPv6 Networks.

VII. CONCLUSIONS

IPv6 security is a major challenge nowadays as the migration to IPv6 is a short-term reality. In this paper start by addressing the understanding IPv6 protocol overview and features. Next brief study about IPv6 security vulnerabilities, with a focus on those that are related to extension headers, Hop-by-Hop, Destination and Routing headers. Despite the new IPv6 features introduced by IPv6, fragmentation and reconnaissance attacks are still possible, so we also analyzed countermeasures to mitigate these attacks. IPv6 only provides a single control protocol, ICMPv6. We show that IPsec can be used to secure routing protocols (e.g. OSPFv3), remote access to organizations, and transition mechanisms. Tunneling mechanisms can facilitate an intruder to avoiding ress/egress filters checks, so special attention was paid to automatic tunneling mechanisms. In

conclusion, we can say that the major vulnerabilities that IPv6 faces in local and wide area networks.

REFERENCES

[1] S. Deering, R. Hinden. RFC1883, "Internet Protocol, Version 6 (IPv6) Specification". [Online] 1995. http://www.ietf.org/rfc/rfc1883.txt.

[2] Deering, S and R. Hiden. RFC2460, "Internet Protocol, Version 6 (IPv6) Specification". s.l. : http://www.ietf.org/rfc/rfc2460.txt, 1998.

[3] Khaldoun, B. Khaled, B. Amer, A. 2011. The need for IPv6. International Journal of Academic Research, Vol. 3. No. 3. II Part. PP.431-448, Azerbaijan. http://www.ijar.lit.az

[4] Minoli, D. Kouns, J. 2009. Security in an IPv6Environment. CRC Press, USA.

[5] Hagen, S. IPv6: Grundlagen, Funktionalität, Integration; Sunny Connection AG: Maur, Switzerland, 2009.

[6] Deering, S.; Hinden, R. Internet Protocol, Version 6 (IPv6) Specification; RFC 2460; IETF: Fremont, CA, USA, 1998

[7] Thomson, S.; Narten, T.; Jinmei, T. IPv6 Stateless Address Autoconfiguration; RFC 4862; IETF: Fremont, CA, USA, 2007.

[8] Request for Comments 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6), in 2003, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc3315.txt.

[9] Request for Comments 4862, IPv6 Stateless Address Auto configuration, in 2007, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc4862.txt.

[10] Deering, S and R. Hiden. RFC2460, "Internet Protocol, Version 6 (IPv6) Specification". s.l. : http://www.ietf.org/rfc/rfc2460.txt, 1998.

[11] RFC4301 (http://tools.ietf.org/html/rfc4301)

[12] Kent, S.; Seo, K., "Security Architecture for the Internet Protocol," *RFC 4301*, Dec. 2005, http://tools.ietf.org/html/4301.

[13] Johnson, D., Perkins, C. and Arkko, J. RFC 3775 "Mobility Support in IPv6". [Online] June 2004. http://www.ietf.org/rfc/rfc3775.txt.

[14] C. Perkins, Ed. RFC3344 "IP Mobility Support for IPv4". [Online] August 2002. http://www.ietf.org/rfc/rfc3344.txt.

[15] Narten, T., et al. RFC4861 "Neighbor Discovery for IP version 6 (IPv6)". [Online] September 2007. http://tools.ietf.org/html/rfc4861.

[16] Perkins, C. RFC4449 "Securing Mobile IPv6 Route Optimization Using a Static Shared Key". [Online] June 2006. http://tools.ietf.org/html/rfc4449.

[17] Hogg, S. Vyncke, E. 2009. *IPv6 Security*, Cisco Press, USA.

[18] Choudhary, A.R. and A. Sekelsky. *Securing IPv6 network infrastructure: A new security model.* 2010 IEEE International Conference on Technologies for Homeland Security (HST). 2010.

[19] Krishnan, S., The case against Hop-by-Hop options, Internet Draft 2010 work in progress. Internet Engineering Task Force. http://tools.ietf.org/html/draft-krishnan-ipv6-hopbyhop-05

[20] IPv6 Extension Headers Review and Considerations. [Online] 10 2006. [Cited:24, 2011] http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd80 54d37d.pdf.

[21] Jeong-Wook, K., et al. Experiments and Countermeasures of Security Vulnerabilities on Next Generation Network. Future Generation Communication and Networking (FGCN 2007). 2007.

[22] Wadhwa, M. and M. Khari, Vulnerability Of IPv6 Type 0 Routing Header And It's Prevention Algorithm. International Journal of Advanced Engineering Sciences and Technologies 2011. Vol.5(No. 1): p. 056 - 061.

[23] Biondi, P. and A. Ebalard, IPv6 Routing Header Security, in CanSecWest 2007: Canada. Available from: www.secdev.org/conf/IPv6_RH_security-csw07.pdf

[24] Request for Comment 5722, Handling of Overlapping IPv6 Fragments, in, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc5722.txt.

[25] Gont, F., Security Implications of Predictable Fragment Identification Values, Internet Draft work in progress 2011, Internet Engineering Task Force. http://tools.ietf.org/id/draft-gont-6manpredictable- fragment-id-00.txt

[26] Sousa, Miguel Pupo Correia e Paulo Jorge. Segurança no Software. s.l. : FCA Editores, September 2010.

[27] Cisco Systems, Inc. "Cisco IPS 4200 Series Sensors". [Online] 2011. http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/ps9157/product_data_sheet09186a008014873c.pdf.

[28] Conta, A., Deering, S. and M. Gupta, Ed. RFC4443 "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification". [Online] March 2006. http://tools.ietf.org/html/rfc4443.

[29] Weider, C. and Wright, R. RFC1491, "A Survey of Advanced Usages of X.500". [Online] July 1993. http://tools.ietf.org/html/rfc1491.

[30] Miyakawa, S. RFC 3769, "Requirements for IPv6 Prefix Delegation". [Online] June 2004. http://www.ietf.org/rfc/rfc3769.txt.

[31] IEEE Standards Association. Guidelines for 64-bit Global Identifier (EUI-64™) Registration Authority. [Online] http://standards.ieee.org/develop/regauth/tut/eui64.pdf.

[32] Gilligan, R. and Nordmark, E. RFC 2893, "Transition Mechanisms for IPv6 Hosts and Routers". [Online] August 2000. http://www.ietf.org/rfc/rfc2893.txt.

[33] Nordmark, E. and Gilligan, R. RFC4213, "Basic Transition Mechanisms for IPv6 Hosts and Routers". [Online] October 2005. http://tools.ietf.org/html/rfc4213.

AUTHORS PROFILE

M.Buvaneswari received her M.Phil(C.S) Degree from Bharathiar University,Coimbatore in the year 2006. She has received her M.Sc.,(CS) Degree from Periyar University, Salem in the year 2004. She is working as Assistant Professor, Department of Computer Science, Vivekanandha College for Women, Namakkal, Tamilnadu, India. Her areas of interest include Data Communication and Network, Network Security and Wireless Networks.

Dr.N.Rajendran received his Ph.D Degree from Periyar University, Salem in the year 2011. He has received his M.Phil, Degree from Bharathiar University, Coimbatore in the year 2000. He has received his M.C.A Degree from Madras University, Chennai in the year 1990. He is working as Principal of Vivekanandha Arts and Science College for Women, Sankari, Salem , Tamilnadu, . He has 24 years of experience in academic field. He has published 15 International Journal papers and 13 papers in National and International Conferences. His areas of interest include Digital Image Processing and Networking.