International Journal of Advanced Engineering and Nano Technology (IJAENT)
ISSN: 2347-6389 (Online), Volume-9 Issue-2, February 2022

Investigating Security Issues and Preventive Mechanisms in IPv6 Deployment

J. Sebastian Nixon, Megersa Amenu

Abstract*: *Internet Protocols are utilized to empower the communication between the computing devices in the computer networks. IPv6 offers additional address space and more noteworthy security than IPv4. The progress from IPv4 to IPv6 has been finished through three primary change systems: dual-stack, tunneling, and translation. The IPv6 progress relies upon the similarity with the enormous introduced base of IPv4 nodes and routers just as keeping up with the security of the network from possible threats and vulnerabilities of both Internet protocols. This research identifies potential security issues in the transition mechanisms and proposing prevention mechanisms to the problems identified. Dual-Stack & Tunneling mechanisms were completely implemented in this research work and the security test was based on dual-stack network. A simulation has been designed by using GNS3 and the penetration test by the THC-IPv6 toolkit. After the implementation of simulation, IPv6 in the dual-stack mechanism was identified as vulnerable to DoS via RA flooding and IPv6 fragmentation attacks that shown the IPv6 security problems. Therefore, IPv6 ACLs and RA guards were proposed in order to protect from flooding attacks and VFR should be configured to prevent IPv6 fragmentation.

Keywords: *IPv4, IPv6, Fragmentation, Ra Flooding, Security.*

I. INTRODUCTION

Internet Protocol variant 6 (IPv6) is the cutting edge internet protocol. It is created by the Internet Engineering Task Force (IETF) to give better execution and furthermore new administrations in correlation with Internet Protocol variant 4 (IPv4) [1]. The IPv6 was developed to eradicate the weaknesses of IPv4 [2]. The IPv6 address administration work was formally appointed to the internet assigned numbers authority (IANA) in December 1995 [RFC1881]. The registration strategy was affirmed with the IETF. IPv6 address has 128 bits or 16 bytes. It is separated into eight hexadecimal blocks isolated by colons ":"; E.g. *2001:0db8:3c4d:0004:0213:72ff:fe7b:3cde.* The internet users and devices that need more IP addresses to be assigned to them are rapidly increasing. Web associated items are turning out to be progressively well known, and keeping in mind that IPv4 address couldn't satisfy the need for internet of things (IoT) items, IPv6 gives IoT items a stage to work on for seemingly forever. It will depend on IPv6 and the new threats they both bring to the party. The IoT requires more IP addresses than IPv4 can offer. To solve this problem, IPv6 was developed to expand the availability of address spaces [3]. The IPv6 protocol suite has been configured to meet the present and future growth of the Internet by providing a much larger address space than that of its IPv4 counterpart and is expected to be the successor of the primary IPv4 protocol suites. The imminent exhaustion of the IPv4 address space has already led to the deployment of IPv6 in numerous production environments, with many other internet service providers (ISP) planning to deploy IPv6 in the near term [4]. The IETF has been working on the IPv6 requirement to overcome these address limitations in IPv4.

IPv6 gives a much bigger address space of 340 undecillion addresses to meet this request [8]. IPv6 is to address these issues, in the age of the Internet today, the existing Internet Protocol, IPv4, is faced with issues of scalability and space limitation of IP addresses as well as security [6]. It is intended to settle a few of the issues of IPv4, along with auto-design, portability, and generally extensibility.

IPv6 spreads out the address space on the Internet and supports a number of devices which will be straightforwardly associated with the Internet [7]. Exhaustion of the address space and security weakness was the main aim of the deployment of IPv6.

Several unexpected vulnerabilities are likely to further emerging with large-scale deployment of the new internet protocol Because of the weariness of accessible IPv4 addresses by the IANA on February 03, 2011, the need for utilizing IPv6 turns out to be increasingly self-evident [8]. IPv6 solves the long exhaustion of IPv4 addresses, IPv6 also brings other advantages such as; simplified routing aggregation, simplified address format, eliminating NAT, auto-configuration, support Internet Control Message Protocol Version 6 (ICMPv6) for neighbor discovery, integrated encryption, and mobility benefit absents in IPv4 [9].

Around the world, clients of Google are an accurate representation of Web clients; Google estimates that current IPv6 selection rates are around more than 30% of the internet. Google gathers statistics about IPv6 adoption on the Web on progressing premise. We trust that distributing this data will offer assistance to internet providers, site proprietors, and policy-makers as the industry rolls out IPv6. Google gathers measurements about IPv6 reception on the Internet on a continuous premise. They consistently were estimating the accessibility of IPv6 network among Google clients. The following chart shows the level of clients that entrance Google over IPv6 [10].

Manuscript received on January 13, 2022.
Revised Manuscript received on February 01, 2022.
Manuscript published on February 28, 2022.
* Correspondence Author
J. Sebastian Nixon*, School of Informatics, Wolaita Sodo University, Ethiopia. Email: dr.nixon14@gmail.com
Megersa Amenu, School of Informatics, Wolaita Sodo University, Ethiopia. Email: mgersaamenu7@gmail.com

Figure 1: Percentage of users who access Google over IPv6

The protocol seeks to achieve these goals by eliminating IPv4 artifacts like ARP, NAT, ICMP, and DHCP and instead implementing SLAAC, ICMPv6, DHCPv6, IPsec, extension headers, and more [11]. To guarantee reasonable and convenient deployment of IPv6, the security aspects ought to be considered. Unused and additional characteristics in IPv6 request unused deployments to secure another era of the internet. Until the time total movement to IPv6 takes place, the internet migration methods ought to secure. If cleared out unprotected, distinctive strategies pose a series of risks to systems. As the organization of IPv6 continues, security issues show up at the same time. That is, existing security assaults against IPv4 changed to assault IPv6 networks and clients, while new IPv6-just dangers emerge from the new protocol determination[8]. Two problems make IPv6, particularly vulnerable. One is the immature network infrastructure and the second is misconfigured gateways that link to IPv4 & IPv6 networks [1].

II. REVIEW OF LITERATURE

A. Internet Protocols: an overview

1) Comparisons of IPv4 and IPv6

IP is the network layer protocol and is a vital communication protocol of the internet. Its quick extension is driven to a deficiency of IPv4 addresses and activated the current change handle to the changed from IPv6 with an address extend of 2^{128}. Even though the new version was updated multiple times, the fundamental security and protection configuration was made in 1998. The IANA dispersed its last IPv4 address to the Regional Internet Registries and some of them have effectively run out of addresses [18]. IPv6 was designed to provide sufficient numbers of globally unique IP addresses to enable true peer-to-peer communication between nodes on interconnected networks. Table 1 below can provide some of the differences between both IP protocols.

Table 1: Comparison among IPv4 and IPv6

IPv4	IPv6
It has a 32-bit address length	It has a 128-bit address length
IPsec support is only optional	It has inbuilt IPsec support
ARP	Neighbor Discovery of ICMPv6
No packet flow identification	Packet flow detection is there within the IPv6 header utilizing the Flow Label field
Broadcast messages are available	multicast IPv6 address (FF02::1) is used
Manual configuration of IPv4 addresses	Auto-configuration address is available
Address per interface: Almost One	Unlimited + Link-Local Address

The IPv6 header is 40 bytes long and contains eight fields, whereas IPv4 headers may be as short as 20 bytes or as long as 60 bytes and contain at least 12 different fields [19].

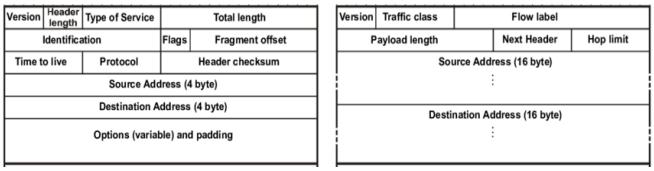


Figure 2: IPv4 & IPv6 header comparison

IPv6 headers have Fixed Header and Extension Headers (EH). Fixed Header contains all the necessary information that is essential for a router. The EH comprises optional information, which assists routers to understand how to handle a packet. The functions of each header described in the following list.

- ✓ Version: the 4-bit Version number of IPv 6
- ✓ Traffic Class: 8-bits, used for routers to manage the traffic depend on the priority of the packet
- ✓ Flow Label: 20-bit field used by the source to label the packets belonging to the same flow to request distinctive handling by intermediate IPv6 routers.
- ✓ Payload Length: 16-bit unsigned number, which is the remainder of the packet that follows the IPv6 header, in octets .
- ✓ Next Header: 8-bit distinguishes the kind of header that quickly follows the IPv6 header
- ✓ Hop Limit: 8-bit unsigned number. Decremented by one by isolated hub that advances the packet.. The packet is rejected if Hop Limit is reduced to zero
- ✓ Source Address: 128 bit the address of the source of the packet
- ✓ Destination Address: 128 bit the address of the intended receiver of the packet

IPv6 consists of an improved optional over IPv4. IPv6 options are located in individual extension headers that are available among the IPv6 header and the transport-layer header. The EH is described in the following table 2.

Table 2: the IPv6 extension headers [20]

Extension Header	Next Header Value	Description
Hop-by-Hop Options header	0	read by all devices in transit network
Routing header	43	contains methods to support making routing decision
Fragment header	44	contains parameters of datagram fragmentation
Destination Options header	60	read by destination devices
Authentication header	51	information regarding authenticity
Encapsulating Security Payload header	50	encryption information

2) IPv6 Features

Extension Headers are a header found in packets that are sent over the IPv6 network. These headers can be bound together to permit one header to point. Spoofing packets in these ways may lead to a DoS and causes issues for all nodes on the network. Inside extension headers, an assailant can send a packet that stays undetected if the go-between firewalls don't completely look at the alternatives of these headers [21]. *Auto-Configuration:* Auto-configuration could be a strategy for creating the address for end-devices.

Retrieval Number: 100.1/ijaent.B0466019222
DOI:10.35940/ijaent.B0466.029222
Journal Website: www.ijaent.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication

It permits the network to run without the DHCP server. IPv6 end-devices can configure themselves through either stateless or stateful setup. The SLAAC will create an address based on the network prefix. It does have a lot of network vulnerabilities and security concerns. *Multiple Addresses:* Multicasting implies sending a packet to the address of nodes inside a multicast group. It reduces network transfer speed using since the sender as it were makes a single packet, which is sent to numerous beneficiaries. It makes duplicates of the packet and transmits them to the significant ports. As it had within the multicast gather that requires the packet to get a duplicate of it [22]. Utilizing certain multicast messages, an attack can exceptionally quick do a reconnaissance attack on a LAN [21].

Table 2: Most known link-local scope multicast addresses

Address	Multicast in	Address	Multicast in
ff02::1	All Nodes	ff02::6	OSPFv3 DR Routers
ff02::2	All Routers	ff02::9	RIPng
ff02::5	OSPFv3 Routers	ff02::A	EIGRP

B. Overview of Transition Mechanism

The migration of IPv4 into IPv6 is not going to happen overnight. It includes many changes in network configurations with the help of IP addresses. The implementation of IPv6 never said to be easy and simple, even for experienced administrators. One factor hindering the implementation of IPv6 is that it is not interoperable with IPv4 meaning IPv6 and IPv4 are not compatible with the same network and as a result led to the adoption of various transition mechanisms [9]. Since there is a huge distinction somewhere in the range of IPv4 and IPv6, both don't communicate straightforwardly with one another. A technique that is equipped for taking care of IPv6 traffic can be finished in reverse viable, yet a generally sent framework that handles just IPv4 can't deal with IPv6 datagrams [23]. Transition mechanisms permit the current IPv4 systems to coexist and interoperate with IPv6 systems, frameworks, and administrations. Organizations ought to arrange their sending and account for the total life cycle of gear from starting to transfer [19]. During the transition phase, both IPv4 & IPv6 will exist together; due to the technical differences, both are not compatible [24]. Nahom Gizachew proposed a framework for EthioTelecom IPv6 deployment based on a dual-stack mechanism. The reason why Dual-stack has been chosen is the nature of it, Dual-stack has no effect on the current application running and its ability to be deployed with a minimum effect on the network. Also, dual-stack supports both versions of protocols and allows flexibility while and after deploying it [25]. The IETF has created various protocols, tools, and mechanisms to help network administrators migrate their networks to IPv6. These techniques can be classified into 3 categories: dual-stack, tunneling, translation [26] [27].

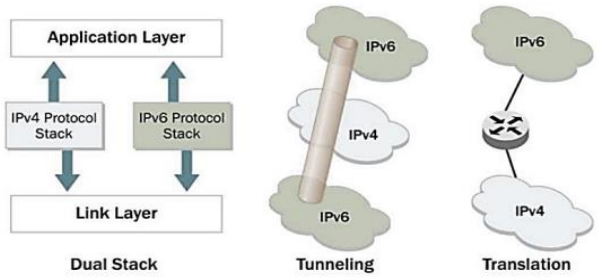


Figure 3: The Three Transition Mechanisms [27]

Dual-Stack Mechanism

Dual-stack includes two protocols stacks, IPv4, and IPv6. Both IP adaptations can coexist on the same network, as well as network devices, run IPv4 & IPv6 protocol stacks. The most disadvantage of dual-stack is that most working frameworks utilize IPv6 by default and IPv6 security deployments are not controlled [28]. In a double stack transition system (DSTM) is that all gadgets interoperate with IPv4 gadgets utilizing IPv4 packets, and with IPv6 gadgets utilizing IPv6 packets. All connections and devices like router, end-user devices, and other framework devices are dual-stacked and they can communicate over both IPv4 & IPv6 [23]. Dual-stack is a preferred, most versatile way to deploy IPv6 in existing IPv4 environments. IPv6 can be engaged any spot IPv4 is enabled close by the connected parts expected to make IPv6 routable, profoundly accessible, and secure. Now and again, IPv6 isn't empowered on a particular interface on account of the presence of inheritance applications or nodes for which IPv6 isn't upheld [26]. The interface of the device configured as dual-stack can have IPv6-only or IPv4-only or both addresses. The router contains two routing tables, one for IPv4 addresses and one for IPv6 addresses [29]. Since both IPv4 & IPv6 would be empowered in a host, IPv4 may not be protected appropriately, such as by utilizing individual firewalls and another preventive mechanism. If an attacker sends RA tests to that node, this would trigger the host to begin utilizing IPv6 quietly. This attack constitutes a basic but effective technique to exploit dual-stack enabled nodes [31]. When a dual-stack environment is set up, it must be guaranteed that the devices, which are on the network, have satisfactory security to moderate the hazard of attacks in both IPv4 & IPv6 situations. Nodes will therefore control firewalls, VPN clients, and IDS/IPS frameworks and these must be able to examine the activity from IPv4 & IPv6 and portion any unauthorized activity freely of each other. The network administrator inside an environment ought to consider executing IPv6 as it were firewalls that can secure the network the same way it would be secured within the IPv4 network [29].

Tunneling Mechanism

Tunneling implies that IPv6 packets are set interior IPv4 packets, which are directed through the IPv4 routers. It has numerous vulnerabilities that have to be examined, in specific,

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication

the 6to4 tunnel which has vulnerabilities to sniffing, spoofing, and DoS attacks [29]. Tunneling can be either manual or automatic. An automatic tunnel does not require pre-configuration; it is created based on information contained in the IPv6 packet [34].

Configured Tunnels

Configured Tunnels inside the tunneling situations, the IPv6 area that is sent from the beginning device are encapsulated inside an IPv4. Within the conclusion, the packets are decapsulated into IPv6 activity. The setup data, which is put away on the endpoint of the tunnel, will decide the addresses. It can put inside a router-to-router, host-to-router/router-to-host, or host-to-host situations. The accompanying tunneling setups are characterized by RFC 2893 considers the tunneling of IPv6 traffic between the hubs across an IPv4 only infrastructure [29]. **Router-to-Router**: The tunnel, which interfaces IPv6 nodes by way of IPv4 with the utilizing of the consistent connection between the source and destination routers, communications are probable as in Figure 4

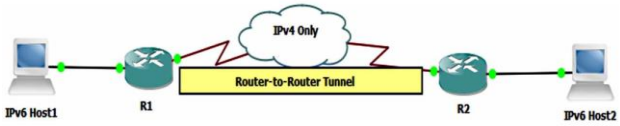


Figure 4: Router-to-router tunnel [29]

Host-to-Router or Router-to-Host: The IPv6 nodes, which are found inside an IPv4 network, will make the IPv6 over IPv4 tunnel to get a handle on the IPv6/IPv4 router. The tunnel starts at the host and finishes up at the router as in Figure 5.

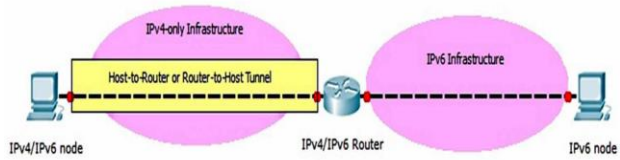


Figure 5: Host-to-router or router-to-host tunnel [29]

Host-to-Host: The IPv6/IPv4 node that is residing inside the IPv4 set-up will make the IPv6 over the IPv4 tunnel. The tunnel expands from the source to the destination nodes as in Figure 6.

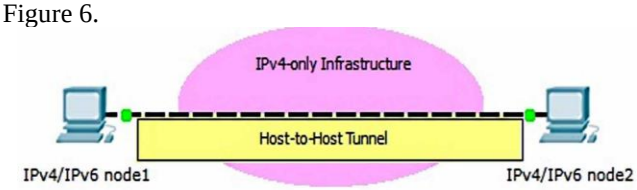


Figure 6: Host-to-host tunnel [29]

Automatic Tunnels

Automatic tunnels are not as secure as physically arranged tunnels. It is simply affected by fake packet and DoS attacks. The network design must provide mechanisms, which can protect against IPv4 & IPv6 vulnerabilities [31]. **6to4:** The 6to4 strategy permits association to existing between two IPv6 domains where an IPv4 network is found in between them. The IPv4 addresses are a portion of the IPv6 addressing construction whereas the packets are being exchanged, as IPv4 is the connect. The 6to4 strategy features a one of a kind prefix: 2002: IPv4 address:: /48. This strategy works inside the router-to-router arrangement. As defined in RFC 3964, 6to4 is susceptible to the ND messages, spoofing; reflecting, IPv4 broadcast attack [31]. **6over4:** Where a network comprises of IPv6 able has and routers, but the networks works inside IPv4, 6over4 will treat the IPv4 network as a virtual Ethernet for IPv6 communications. IPv4 multicast is utilized to tunnel the IPv6 packets. **ISATAP:** it utilized inside the unicast IPv6 network, where the IPv6 and IPv4 nodes present inside an IPv4 intranet. It is not able to support multicasts because it employments a Non-Broadcast Multi-Access (NBMA) communication show. Much like 6to4, ISATAP utilizes headers to send data from one convention adaptation to another, and thus it is vulnerable to the same sorts of dangers, which have been examined in 6to4. **Tunnel Broker:** The tunnel broker acts as a tunnel creation instrument between two nodes inside the network. This as it were requires there to be a web server and client-side confirmation to assemble details elements such as IP address, working framework, and IPv6 compatibility.

Teredo: it relies upon the endpoints of the tunnel to epitomize and decapsulate packets, hence any host, which to any nodes beside the firewall, can encapsulate and decapsulate packets. It is hard to secure all endpoints and thus a single firewall would be required to secure the network. Since the packets are encapsulated, the firewall cannot protect the data inside the packets. Hence, packet spoofing is still a concern [31]. Tunneling mechanisms have no built-in security at all, no authentication, no integrity check, and no confidentiality. It could easily give advantages for attackers to conduct tunnel sniffing, tunnel injection, or unauthorized use of tunnel service attacks. If proper prevention mechanisms are not in places, such as checking the IPv4 source address, using anti-spoofing techniques, using ACLs and IPsec, these threats could even bypass corporate firewalls [30].

Translation Mechanism

In the translation method, the IPv6 packet is not encapsulated in an IPv4 header like tunneling. An IPv4 header replaces the IPv6 header of the packet. Hence, the IPv6 packet is transformed into an IPv4 packet. NAT64/DNS64 may be a technique that creates it possible for IPv6-only clients to exchange IPv4 devices. RFC 1918, as NAT is a familiar method in IPv4, is commonly used to translate between private addresses and public IPv4 address space. The NAT64 transparently provides access among IPv6-only and IPv4-only networks [26] [27].

C. Overview of IPv6 Security Issues

Security Threats in IPv4 & IPv6 Networks

A few sorts of attacks have not been on a very basic level changed by the appearance of the IPv6 protocol. Indeed even though security enhancements actualized within the unused IPv6 protocol, IPv6 systems are still uncovered to diverse sorts of attacks. Therefore, different attack types could potentially harm IPv6 networks. Some types of attacks can affect both IPv4 & IPv6 networks [31]. The types of attacks acknowledged in the IPv4 network did not a general sense alter with the appearance

of the unused IPv6 protocols are the sniffing attacks, flooding attacks, Rogue devices, and Man-in-the-middle attacks [26]. *Denial of Service Attack* This attack aims to prevent the nodes from normally running the functions provided by the NDP. For instance, when a client executes the DAD, an assailant can eavesdropper the NS messages sent from this strategy and send back forged NA saying, "I have involved this address.". Hence, the victim can't complete the DAD to get an IPv6 address for the accompanying communication. Essentially, an assailant can send forged RA and NA messages to make DoS assaults on router discovery and NUD methodology [16]. The attacker's activities to block authorized clients get to a specific benefit. A broadcast flooding attack known as Smurf attack is a case of a DoS attack. A DoS attack on an IPv6 network can be forced by misusing vulnerabilities within the Multicast, Expansion Headers, ICMP messages, and DAD protocol [27]. DoS and DDoS are flooding attacks used often to leave a network. The difference between these attacks merely relates to their number of attacks. DoS is conducted by one computer, while the DDoS, a large-scale DoS is by hundreds of computers that may attack a network [32]. A report from the National Vulnerability Database (NVD) showed that the majority of attacks against IPv6 are DoS attacks [3].

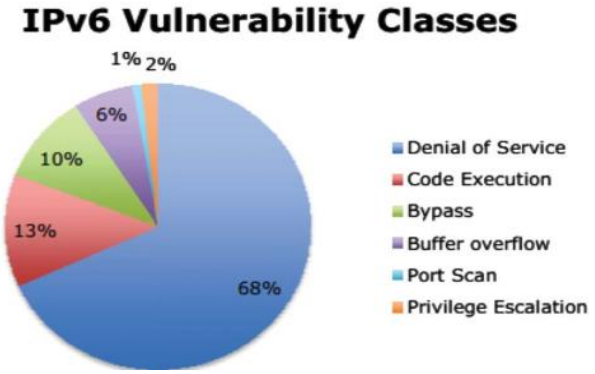


Figure 7: IPv6 vulnerability classes as NVD [62]

Man-In-The-Middle Attack

In this attack, an assaulter enters in between two nodes that are communicating. The attacker ensures that all traffic between the nodes goes through him and can see the whole traffic. Because of the absence of legitimate authentication mechanism in IPv4, these assaults can be effortlessly accomplished.

This attack has been done by acting as the intermediary between the device and the destination in communication. This attack is conducting further attacks, such as sniffing and session hijacking [33]. MITM attack hijacks the communication between two nodes. When PC1 sends an NS message to resolve the MAC address of PC2, the attacker can pretend to answer this NS with spoofed NA. Then, the attacker will receive the subsequent packets from PC1 and forward them to PC2 using spoofed packets. This way, both PC1, and PC2 seem to be normally communicating with each other, the attacker has taken over all the traffic flows between them without being perceived [16]. MITM assaults, as its name recommends, is an assault where a message is intercepted or replicated and resent to its final destination. In this assault, neither the sender nor the recipient knows about the attacker capturing all messages in their communication [34]. Lacking strong authentication, any attacks using MITM will have the same possibility in IPv6 as in IPv4.

Spoofing Attack

A spoofing assault is a malevolent party imitates another device t or clients/users on a network to take personal information, spread malware, and/or bypass gets to controls. This assault is performed by utilizing a forged address and may cause a bogus section in a client's neighbor cache. Mocking is regularly used to use different assaults, for example, MITM assaults, DoS assaults, and divert assaults [16].

In the event that an assailant sends spoofed RA inside a subnet, all IPv6 clients will quickly change their routing tables and store the attackers as one of the default routers. This leads to a condition in which the attacker can completely modify all outgoing traffic from the IPv6 nodes to the Internet, which makes the MITM attack [35].

Flooding Attack

Flooding attacks happen when a network gets to be so hold down with packets starting insufficient association demands that it can now not handle. By flooding an end-device with systems that cannot be completed, the flood attack, in the long run, fills the host's memory buffer. IPv6 flooding attacks are like IPv4.A flooding assault can be nearby or a distributed DoS when the designated network device is being overflowed by network traffic from many clients simultaneously. This sort of assault can likewise influence the IPv6 networks in light of the fact that the fundamental standards of the flooding assault continue as before. New sorts of augmentation headers in IPv6, new kinds of ICMPv6 messages, and relying upon multicast addresses in IPv6 might give better approaches for abuse in flooding assaults [31].

Sniffing Attack

A representative attack that affects both IPv4 & IPv6 networks is a sniffing attack. The sniffing attack comprises the capture of the information being transmitted through the network. In the event that that classified information is sent in a plaintext convention, an attacker running a sniffing assault can undoubtedly compromise them..

A sniffing assault type can be kept away from by legitimate utilization of the IPsec security architecture, which is utilized in IPv4 as a choice and in IPv6 as a commitment [31]. Sniffing assault includes catching information and data through network connects to be abused, particularly when sent in plain message format [13]. IPv6 is as same vulnerable to sniffing as IPv4.

Reconnaissance Attack

Reconnaissance attack is the type of attack with the help of discovering any week ports by using application software like port scanning. The attacker picks up basic information relating to the victim network by reconnaissance attacks. Hop-by-hop causes execution suffering for a router that gets a huge number of the packet with the router that receives a large hop-by-hop alternative.

Scanning is a procedure utilized for this reason, which uncovers open ports and other network data. Since the IPv4 address space is little, it is simpler to scan the whole address space. Reconnaissance attack is possible in IPv6 due to its Multicast feature and response from ICMPv6 messages [27]. An interloper utilizes ping tests to figure out which IP addresses are being used in the victim network. In the wake of having tracked down an available framework, an assailant plays out the port sweep methodology. IPv6 is much more resistant to reconnaissance assaults than IPv4 networks [31].

D. IPv6 Security Improvements

Large Address Space

Port filtering is one of the known surveillance strategies being used today. It allows intruders to listen to specific ports that could be related to well-known vulnerabilities. In IPv4 networks, port scanning is very simple. IPv6 subnets use 64 bits for allocating host addresses. Scanning such a huge address space is mostly an impossible operation. Nevertheless, it is not impossible [31].

IP Security (IPsec)

IPsec is a important element of IPv6. OSPF routing provides IPsec for IPv6 authentication security, to protect IPv6 unicast and multicast traffic and IPv6 IPsec tunnel mode encapsulation is used [36]. IPv6 Authentication Header (AH) and IPv6 Encapsulating Security Payload (ESP) are features of the new IPsec. An extension header that is called the IPv6 AH and ESP, provides authentication and integrity, without confidentiality, to IPv6 datagrams [37]. In IPv6 network, both the AH and the ESP header are characterized as expansion headers. IPsec accommodates a third set-up of protocol for protocol negotiation and key exchange management known as the Internet Key Exchange (IKE). This protocol suite gives the underlying functionality expected to set up and arranging security boundaries between endpoints. Moreover, it monitors this data to ensure that communication keeps on being secure up to the end [31].

E. IPv6 Specific Vulnerability Areas and Threats

IPv6 security is progressed relate to IPv4, but IPv6 still has numerous security vulnerabilities that are the same as IPv4 or more up to date. Network administrators must get security vulnerabilities [39]. IPv6, incorporate the need for the development of the implementation that in this manner are exceedingly likely to still contain much newer vulnerability [40]. The problem of NDP in IPv6 is the identification of assaults that utilization the genuine IPv6 address, for example, flooding, DoS assaults on address resolution and the likely weaknesses of this component likewise should be investigated [16]. The security vulnerabilities that too ended up issues in IPv6 deployment are reconnaissance, misuse of routing headers, fragmentation related attack, auto-configuration and ND, abuse of ICMPv6, and multicast as well as well-known threats like unauthorized get to, impersonate, and DoS attacks [41]. IPv6 design's functions are wide-open to security threats like the DAD process, which is vulnerable to DoS attack. Such a danger keeps the host from configuring its IP address by reacting to each Neighbor Solicitation through the fake Neighbor Advertisement [38]. All the security aspects and implications, which exist, must be looked at before any migration to avoid network disruption. Due to the new environment of the IPv6 network, these risks are higher than ever. The security issues need to be looked into to consist of IPv6 protocol issues, transition mechanisms, and the IPv6 deployment issues [29].

Security Threats Related to IPv6 Routing Headers

All IPv6 nodes must be capable of preparing, directing headers. Unfortunately, routing headers can be utilized to maintain a strategic distance from getting to controls based on goal addresses. Such behavior can deliver a few security issues. There is a chance that an aggressor sends a packet to in open address with a routing header containing a address on the victim network. The freely open host will forward the packet to an destination expressed in the routing header, even though recipient address is filtered.

By parodying packet source address an assaulter can easily perform DoS assault by utilizing any openly available host for diverting attack packets [31].

Fragmentation Related Security Threats

An IPv6 source client utilizes the fragment header to send a packet bigger than would fit in the way MTU to its destination. . The source node initially performs the path MTU discovery procedure to discover the PMTU value. The procedure is an IPv6's best effort attempt to avoid fragmentation. The original unfragmented packet consists of two parts: the unfragmentable part and the fragmentable path [39]. The minimal recommended MTU size for IPv6 networks is 1280 octets. For security issues, it is energetically prescribed to dispose of all fragments with under 1280 octets unless the packet will be the last in the flow. An assaulters can cause an over-burden of recreation buffers on the target framework possibly inferring a framework to crash, which is a kind of DoS assault. To keep away from such issues it is a prescribed security practice to restrict the all out number of fragments and their permitted arrival rate [31]. IPv6 of course doesn't forbid the reassembly of covering sections despite the fact that this is a notable security danger, which can be utilized to stay away from firewalls.

Only source nodes perform fragmentation in IPv6, not by routers along a packet's delivery path as allowed in IPv4 [19]. Fragments can be used to bypass IDS/IPS systems as well as firewalls. The techniques for hiding attack patterns or evading security systems are [40].

- ✓ Evasion: embedding a part which isn't prepared by IDS/IPS but let through due to its straightforwardness
- ✓ Insertion: inserting a part which is acknowledged by IDS/IPS but disposed of by a target host
- ✓ Overlapping fragments: overlapping fragments could cause DoS during reassembly or misinterpretation of the data thus hiding attack pattern
- ✓ Tiny fragmentation: attempt to hide attack pattern; a huge amount of tiny fragments is a sign of a coming attack
- ✓ The disordered arrival of fragments: disordered fragments of several packets arriving at once is a technique trying to avoid deep packet inspection,

- ✓ Fragment flooding: another strategy designated to avoid deep packet inspection

Security Threats Related to ICMPv6 and Multicast

ICMPv6 plays a key role in the proper usage of IPv6. Especially the ND messages such as RAs and NS/NA are needed for the straightforward usage of the new Internet Protocol [41]. ICMPv6 messages should be permitted in view of appropriate network activity, for instance packet too huge' message is needed for the technique of way most extreme transmission unit revelation, a message is important if an unnoticed alternative happens in the IPv6 packet header. ICMPv6 detail additionally permits a error notice reaction to be shipped off multicast addresses. An assaulter can abuse that reality by sending an appropriate packet to a multicast address and can cause various reactions focused on at the victim [31]. ICMPv6 is vulnerable to DoS and DDoS attacks using different techniques due to the shortcomings of its current defense mechanisms. Some of the existing mechanisms can be the reason for DoS or DDoS attacks themselves, such as the SeND approach [13]. ICMPv6 is vulnerable to a set of attacks that contributes to preventing IPv6 from being trusted for full implementations on today's networks. One of these attacks is the RA flooding attack by sending huge traffic toward a victim to consume its resources and stop its services [5]. Router ACLs, firewalls, and other security components must be carefully managed to retain ICMPv6 functionality [19].

Neighbor Discovery Protocol Related to Attack

The NDP is among the new features introduced in IPv6 and NDP security is an important part of IPv6 security. NDP suffers from various attacks, such as DoS, DDoS attacks, last-hop router attack, MIMT, ARP spoofing, and fake redirect packet. Many researchers have proposed suggestions and novel mechanisms to improve NDP security and mitigate threats against the NDP. However, the NDP is still incomplete with practical use and there are no best practices to ensure the security of NDP [42]. Router discovery in IPv6 is vulnerable to rogue RAs, wherein unintended and possibly incorrect RAs make their way into the network. Flooding with RAs is an easy technique resulting in a denial-of-service attack [43]. DAD is a portion of IPv6's Network Discovery Protocol that is weak to security threats like Spoofing, and DoS [44]. It is a procedure that is part of the address auto-configuration that is utilized to check whether the addresses generated has already been configured or not. Nevertheless, the design of the DAD process is vulnerable to the DoS attack, leaving nodes un-configured [45]. ND plays an important role in addressing because it provides address resolution and address auto-configuration. These are accomplished through the different processes in the ND protocol, which consists of five different ICMP packet types [19]:

- ✓ *RS:* When an interface gets to be empowered, has may send Router Solicitation that asks the router to create RAs instantly instead of at another planned time.
- ✓ *RA:* Routers publicize their nearness at the side of different links and internet parameters either occasionally or in response to RS message. RAs contain prefixes utilized for on-link assurance and address configuration, a proposed hop-limit value, the Maximum Transmission Unit (MTU) for the link, etc.
- ✓ *NS:* Nodes send NSs to decide the link-layer address of a next node or to confirm that the next node is still reachable through a cached link-layer address. NSs are too utilized for duplicate address detection (DAD).
- ✓ *NA:* may too send spontaneous NAs to report a link-layer address alters.
- ✓ *Redirect Message:* Used by routers to inform nodes of a better first-hop for a destination.

F. Security problems Related to Transition Mechanisms

To confirm a well transition to a updated version of the protocol various transition techniques are developed. The highly important transition techniques are dual-stack and tunneling configurations. These transition techniques can lead some new, earlier unknown security vulnerable. Thus, network engineers need to understand the security implications of transition mechanisms to apply proper security mechanisms, such as firewalls and intrusion detection mechanisms [31].

Other Attacks

Replay: The attackers can get the multicast packets then resend them in the network to confuse the computing devices with fake information. All ND packets are vulnerable to replay attacks [16].

Rogue Router: In this technique, an attacker system can act like router and send false RA messages. If a device selects it as the default router, it can draw off the traffic of this device may act as MITM [16]. An assaulter can also place his DHCPv6 server inside a network and distribute falsified values [21].

Smurf Attack: The efficiency of multicasting can be preyed upon by using it to launch a Smurf attack. It is a kind of DDoS attack that is introduced by an attacker via a spoofed source address of a target node to send echo-requests to a whole multicast group. To overwhelm the spoofed source address with a huge amount of traffic due to the amplified amount of response messages sent back from the multicast group to the victim node [46]. In an IPv6 network, a Smurf attack happens when an attacker sends spoofed ICMP resound ask packets to a multicast group (FF02::1) with the target machine as the source. The problems primarily consider for IPv6 deployment. The primary problem is the finding of a assaults that utilize the real IPv6 address, such as DoS attacks on address resolution. The Secondary problem is the potential weakness of this mechanism also needs to be researched [16]. An attacker can force a router in the way to a destination host to assess a fragmented packet that evaluates a fragmented packet that is a dense load on a router by allowing a hop-by-hop option in a fragmented packet. How can a router be protected contrary to it [1]. Previously RA Guard was tested for flood_router6 older version [61]. However, this thesis experimented with a new version, which is the Flood_router26 attack tool. Therefore, RA Guard can protect from the RA flooding attack of both versions of the flood router attack.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication

G. Prevention Mechanisms Review

IPv6 and IPv4 are both network-layer protocols, many of the network layer vulnerabilities are similar. Security is needed to every nodes in network [47].

Internet Protocol Security (IPsec)

The IPsec is a suite of protocol between end-to-end communication over the IP network that contributes to information authentication, integrity, and privacy. It characterizes the encrypted, decrypted, and uthenticated packets. IPv6 includes the option of using the IPsec security model, which provides transparency, integrity, and confidentiality for end-to-end communications [48]. IPsec is available with IPv6. IPv6 Administrators rely on the IPsec protocol suite for security. The similar security risks for MITM attacks in IKE in IPv4 are existing in IPv6 [47]. Sniffing and spoofing attacks can be resolved by using IPsec, in both IPv4 & IPv6 by default [49]. The main protocols that utilize IPsec standardizes are AH, ESP, and Web Security association and Key Administration protocol. IPsec permits clients numerous choices within the kind of administrations they execute for assignments such as end-to-end encryption or tunneling. The original NDP design called to use IPsec to secure NDP messages, ambiguity about how to use it stills an issue. IETF is then developed SeND to overcome these weaknesses [50]. IPsec still leaves some existing security issues unsolved. New security problems still continuing due to constant changes of its packet header which makes the security framework more complex, thereby leading it weakness to various sorts of attacks [9]. So far the major attacks that can be launched against an IPv6 network by exploiting the packet header vulnerabilities are Reconnaissance, MITM, DoS attack [46]. IPsec was later standardized to fill the gap; its use has not been broadly implemented. It is not a solution to all the security problems of the current Internet. Therefore, security in IPv6, which mandates the attachment of IPsec should be seen as no different from that of IPv4 [39]. IPsec could be considered a solution to block the DoS issues on the IPv6 network, but IPsec relies on a PKI that has not yet been fully standardized [1].

Firewall

Firewalls are widely installed in most organizations connected to the Internet. In light of a bunch of rules or security policy, firewalls act as a guard to the network, which determines the particular packet of packets can pass through them. The common firewall implementation is setting it as an edge firewall because it is believed that intruders always come from outside while in reality, the greater effect of a security harmful attack is mostly coming from the insiders [51]. Firewalls planned for use in IPv6 networks more likely than not implicit help for the IPv6 protocol. Since sifting rules should be characterized independently for IPv4 & IPv6 traffic. The IPv6 protocol presents another packet header design that should be appropriately perceived and prepared by the IPv6 firewall. In the experimental IPv6 network, different tests of firewalls have been performed both on the MS Windows and on the Linux platform [52]. A firewall does not filter fragmented packets that are sent by the attacker. In IPv6, the primary fragment header estimate does not avoid the attack since the different expansion headers can exist between the IP and upper-layer header [39]. RFC 4942 Firewalls ought to drop all packets with overlapped fragments: certain executions in both firewalls and other nodes have now dropped such packets.

Attacks that use multiple extension headers can easily bypass firewalls. To prevent such attacks, firewalls need to perform deep packet inspection. It may not be effective against flooding based DoS attacks [53].

Access control list (ACL)

ACL is the most popular mitigation technique against IPv6 attacks. ACLs can be configured on a router &/ switch to drop incoming malicious Router Advertisements on ports to which end-user computers are connected since only router ports need to transmit Router Advertisements. ACL configuration can contain certain keywords to block unusual attack packets. For example, the Cisco IOS software supports the ACL 'undetermined-transport' keyword [40]. ACLs are used to control traffic filtering. It allows trusted traffic and blocks all other traffic on a device interface based on source and destination MAC or IP addresses. IPv6 ACLs are set by utilizing the *IPv6 access-list list-name* instructions to deny or allow keywords in global configuration mode [54].

Secure Neighbor Discovery (SeND)

This protocol offers security for NDP messages such as RA. It utilizes Cryptographically Generated Addresses (CGAs) for encryption of NDP messages and verification of senders' addresses. CGAs can prevent address spoofing and DoS attacks. SeND packets usually contain more information than normal NDP packets, such as CGA. For this reason, they are quite large and need to be fragmented. Thus, SeND is vulnerable to fragmentation-based attacks. While SeND is supposed to prevent DoS attacks, the protocol itself is prone to some of them [53].

H. IPv6 security Test and Analysis Tools

Wireshark: is an IP-based network protocol analyzer. It reads packets from the network with the help of PCAP, TCPDUMP, etc. Moreover, details them in an easily understandable way. It is an open-source network analyzer founded in 1998 [1]. It is used to analyze the security issues of IPv6 to outline the most common vulnerabilities and security issues during the transition [29]. **Graphical Network Simulator-3 (GNS3)** is a network software emulator first released in 2008. It allows the combination of virtual and real devices, used to simulate complex networks. It uses Dynamics emulation software to simulate Cisco IOS [55].

The Hacker Choice (THC-IPv6) is an open-source toolkit maintained by "van Hauser". THC permits the penetration test on the IPv6 protocol to challenge the shortcomings of the node.

It is an open-source community that creates the security weakness of IP based systems. They extend points to uncover the security breaches of items. THC was established in 1995 and it has been distributed scientific researches and releases security penetration tools [1].

III. RESEARCH METHODOLOGY

A. Introduction

This chapter explains the research methodologies used. The research methodologies used for this research are Design science and Qualitative research. Under these designs, different methods that explain the way the methodology is applied as well as why the specific methodology has been chosen to carry out the research are presented.

Research Design

This research employed design science research that investigates the security issues of IPv6 deployment in the simulation platform. The study mainly focused on experimenting, analyzing, and interpreting that exist in security issues in the transition mechanism. Design science researchers are available in many areas, especially Computer Science and Engineering and there are an assortment of approaches, strategies, and procedures utilized in deign science research [56]. The research was conducted in steps that will let it have the most and best results. First, a broad literature review of related work was done to select transition mechanisms for the IPv6 deployment. Next, the research has been chosen the transition method would be tested using the tools based on the generated network traffic on how it will react to each attack. Finally, it was completed by a series of findings and recommendations.

Methodology

The most technique utilized in the research is Design Science. Design Science investigate could be a set of manufactured and expository procedures and points of view for performing investigate in an information system. It includes two essential exercises to make strides and get it the behavior of perspectives of information system: one is the creation of unused information through the design of novel or inventive artifacts and moment is the investigation of the artifacts utilize and/or execution with reflection and reflection [53]. Design science is an outcome-based IT research methodology, which offers specific guidelines for evaluation and iteration within research projects. This strategy centers on the development and performance of artifacts with the unequivocal aim of improving performance of the artifact. Design science research typically applies to categories of artifacts, including algorithms, human/computer interfaces, design methodologies, and languages [57]. Design science-centered inquire about to think about that attempted to examine potential security issues that will best suit the ways in transitioning from IPv4 to IPv6 whereas still keeping IPv4 for systems that might not however back IPv6. The study tested the potential security problems related to IPv6. This methodology was preferred because it takes into account the activity problem that contains a real situation and includes the difficulties that would come across in the workplace.

Problem Identification and Motivation

These days, the sending of IPv6 systems has ended up required as well as a need. Nevertheless, there are a few challenges like obstacles in transition mechanism, security issues, and a few common misconceptions, which make a genuine issue within the sending of IPv6. The most inspiration for doing this investigation was that IPv6 security ought to deeply administer innovation.

The way the world is going on the communication journey shows that they have to be a move to IPv6 is predictable. Since numerous devices have recognized the vulnerability of the IPv6 network, its assurance component should be examined. As the security of the IPv6 network, have numerous mechanism to identify the vulnerability. Still, packets of ISP utilize IP is defenseless to the nearby network as well as wide zone network risk. It is critical to consider how IPv6 network vulnerability happens and what compelling countermeasure can anticipate the network risk. In this manner, these issues motivated the researcher to consider security solutions related to the IPv6 network.

Demonstration

The simulation of the experimental device was used to further prove the IPv6 vulnerability areas. GNS3 was selected as a simulation tool for this study because of its ability to simulate a real device router and to run the image of a device. It gave a better simulation to get a result close to the actual device. The configured network tested how the security can easily be identified using both Wireshark GUI and command-line. The Wireshark packet capturing software was used to analyze data, which was sent between the IPv6 networks. The penetration testing was done using the THC-IPv6 toolkit to implement, replicate, simulate, and test the threats and vulnerabilities of IPv6. THC-Toolkit was installed on Kali Linux 2019.3 to generate abnormal behavior, while Wireshark Version 3.2.3 was used to capture, filter, and save packets in a different format. Table 4 below lists the tools that were used to implement the IPv4 to IPv6 transition method and to test the vulnerabilities of the IPv6 network environment in this research.

Table 3: The types of tools used for simulation

S/N	Type	Name & Specification
1	Network software emulator	GNS3 2.8
2	Virtual machine	GNS3 VM 2.8
		VMware workstation 15 Pro version 15.5.5
3	Cisco router IOS	Cisco 7200
4	Victims	Windows 10
5	Attacker	Kali Linux 2019.3
6	Connector	Serial and Ethernet cable
7	Packet analyzer	Wireshark Version 3.2.3
8	Internet access	NAT1
9	Switch	Cisco Ethernet switches

Data Analysis Method

The security issues were analyzed using experimentation of comes about gotten from a simulation of the Wireshark tool displayed figures that were acquired from the GNS3 test system and using tables. Qualitatively, after the simulation experiment, the results obtained were narrated and summarized. This includes the examination of the outcomes that may well be shown on the packet analyzer.

B. Implementations Of Ipv4/Ipv6 Network

IPv6 Routing protocol

The determination of a way for transmitting datagrams is called routing. The critical assignment of a router in a network is to decide the best way during the packet sending process.

The routing prepare needs a router to utilize the routing table and the routing table contains entry data in diverse ways through the routing protocols. The IPv6 uses a similar kind of routing protocol with IPv4, but with some modifications. However, IPv6 is aupdated version of the protocol and different from IPv4. The routing table is also managed separately from the IPv4 routing table when both protocols were enabled on a router [58]. Routing of IPv6 can be applied through static routes and dynamic routing protocols. Static routes are manually defined by the administrator. In dynamic routing protocols, IPv6 uses updated versions of the same routing protocols available for IPv4; Among the most important ones are: Routing Information Protocol next generation (RIPng), Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6, a link-state routing protocol (IS-IS) for IPv6, the multiprotocol border gateway protocol (MP-BGP4) and Shortest Path First routing protocol (OSPFv3) for IPv6.

RIPng is the steering protocol utilized to execute the availability tests with IPv6 and is the new age of RIP for IPv6. It is a distance-vector directing protocol that utilizes bounce count as a routing steering metric, with 15 as maximum, its multicast updates are issued every 30 seconds. RIPng utilizes IPv6 to move, incorporates the IPv6 prefix, and the following hop IPv6 address utilizes the multicast bunch FF02::9 as the destination address for RIP refreshes and sends refreshes for the UDP port 521 [58].The comparison between three different routing protocols RIP, EIGRP, OSPF showed EIGRP is relatively faster but in some respect and small connection could lead to RIP faster [59].

Transition Mechanism Implementation

Dual-Stack Implementation

This mechanism implements both protocols on each router and other nodes within the network; IPv4 and IPv6; each node with dual-stack within the network will have two addresses, one for IPv4 and the other for IPv6. A test network was implemented using GNS3, the network supported IPv6 as addressing protocol with implemented using RIPng and RIPv2 routing for IPv6 and IPv4 respectively.

Method

In the experiment, the network was joined using two routers through a serial connector on which both IPv4 & IPv6 were configured. Figure 8 shows the Dual-Stack implemented in the WAN network to test the attack of one LAN in another LAN area. Both routers on the bottom side of interface GigabitEthernet1/0 of R1 and R2 were configured with IPv6-only. As displayed below side network (including Windows 10 and Kali Linux) was configured IPv6 only. However, the upside Gigabit Ethernet (g0/0) is configured with both protocols.

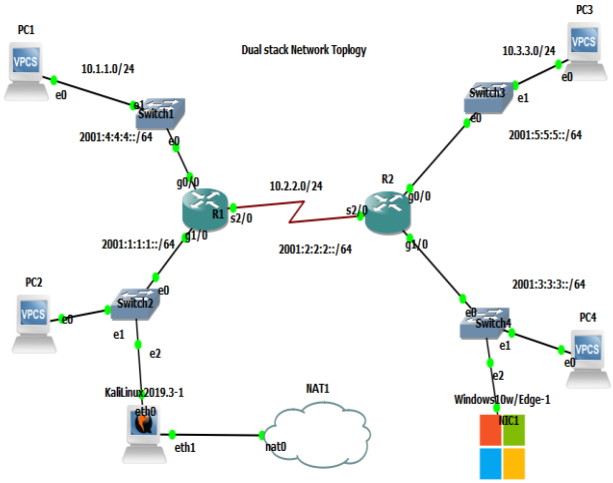


Figure 8: Dual-stack Network Topology

All configurations of dual-stack, and network addresses can be found in **Error! Reference source not found.**1.

Table 5: LAN1 & LAN 2 Configuration

LAN 1	LAN 2
R1#enable *Config t* *IPv6 unicast-routing* *IPv6 router rip DSTM* *Int serial2/0* *IPv6 enable* *IP add 10.2.2.1 255.255.255.0* *IPv6 add 2001:2:2:2:: 1/64* *IPv6 rip DSTM enable* *No shutdown* *Interface g1/0*	*No IP add* *IPv6 enable* *IPv6 add 2001:1:1:1::1/64* *IPv6 rip DSTM enable* *No shutdown* *Interface g0/0* *IP add 10.1.1.1 255.255.255.0* *IPv6 enable* *IPv6 add 2001:4:4:4::1/64* *IPv6 rip DSTM enable* *No shutdown*

Results

Figure 9 below, based on dual-stack network the Frame 5 and Frame 12 indicates the Wireshark capture built in the serial link between the Routers of IPv4 & IPv6 with Routing protocol RIP version 2 and RIPng.

Figure 9: Wireshark Captures for RIPv2 IPv4 and RIPng of IPv6

Figure 10 below shows the ping communications of Windows 10 is running IPv6 addresses 2001:3:3:3::3 which was configured manually on the IPv6 network and with Kali Linux 2019.3 with address 2001:1:1:1:dea7:f29b:2f3a:2ccc running on the IPv6 only.

```
PS C:\Users\IEUser> ping 2001:1:1:1:dea7:f29b:2f3a:2ccc

Pinging 2001:1:1:1:dea7:f29b:2f3a:2ccc with 32 bytes of data:
Reply from 2001:1:1:1:dea7:f29b:2f3a:2ccc: time=1563ms
Reply from 2001:1:1:1:dea7:f29b:2f3a:2ccc: time=68ms
Reply from 2001:1:1:1:dea7:f29b:2f3a:2ccc: time=81ms
Reply from 2001:1:1:1:dea7:f29b:2f3a:2ccc: time=60ms

Ping statistics for 2001:1:1:1:dea7:f29b:2f3a:2ccc:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 60ms, Maximum = 1563ms, Average = 443ms
PS C:\Users\IEUser>
```

Figure 10: Windows 10 Ping to Communicate with Kali Linux 2019.3

Figure 11 below shows a screenshot of the Wireshark output after the "ping" command was done. The source's IP address is a PC1 IPv6 address and the destination's IP address is a PC3 IPv6 address. It could be seen that the IP datagram within this packet has a protocol number for ICMPv6. This indicates that the payload of the IP datagram is an ICMPv6 packet.

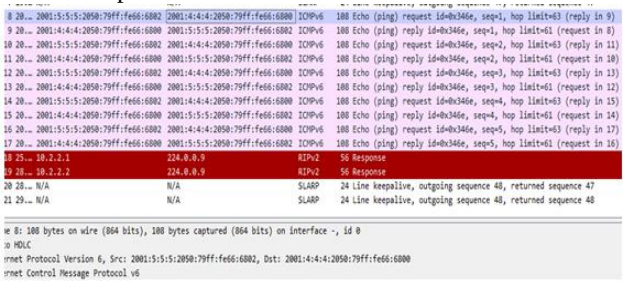
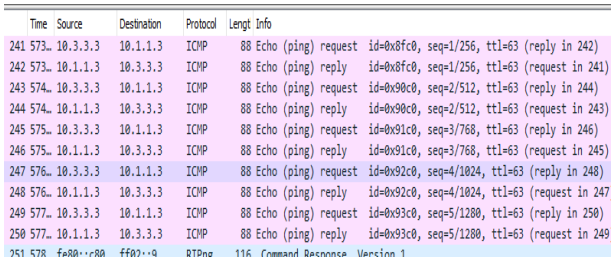


Figure 11: ICMPv6 Ping Communication Packet Capture between PC1 and PC3

In Figure 12 below, it could be seen that the IP datagram within this packet has a protocol number, which is the protocol number to ICMP. This indicates that the payload of the IP datagram is an ICMP packet



Time	Source	Destination	Protocol	Lengt	Info
241 573…	10.3.3.3	10.1.1.3	ICMP	88	Echo (ping) request id=0x8fc0, seq=1/256, ttl=63 (reply in 242)
242 573…	10.1.1.3	10.3.3.3	ICMP	88	Echo (ping) reply id=0x8fc0, seq=1/256, ttl=63 (request in 241)
243 574…	10.3.3.3	10.1.1.3	ICMP	88	Echo (ping) request id=0x90c0, seq=2/512, ttl=63 (reply in 244)
244 574…	10.1.1.3	10.3.3.3	ICMP	88	Echo (ping) reply id=0x90c0, seq=2/512, ttl=63 (request in 243)
245 575…	10.3.3.3	10.1.1.3	ICMP	88	Echo (ping) request id=0x91c0, seq=3/768, ttl=63 (reply in 246)
246 575…	10.1.1.3	10.3.3.3	ICMP	88	Echo (ping) reply id=0x91c0, seq=3/768, ttl=63 (request in 245)
247 576…	10.3.3.3	10.1.1.3	ICMP	88	Echo (ping) request id=0x92c0, seq=4/1024, ttl=63 (reply in 248)
248 576…	10.1.1.3	10.3.3.3	ICMP	88	Echo (ping) reply id=0x92c0, seq=4/1024, ttl=63 (request in 247
249 577…	10.3.3.3	10.1.1.3	ICMP	88	Echo (ping) request id=0x93c0, seq=5/1280, ttl=63 (reply in 250)
250 577…	10.1.1.3	10.3.3.3	ICMP	88	Echo (ping) reply id=0x93c0, seq=5/1280, ttl=63 (request in 249

Figure 12: IPV4 ICMP Ping Communication between PC1 and PC3

As the experiment conducted above shows, it can be concluded that concerning the router dual-stack, only the same protocol, which was working with the nodes can communicate with each other. IPv6 nodes can connect with each other and both IPv4 nodes communicate with each other. However, the IPv6 host is cannot able to communicate with another IPv4 host.

Implementations of the 6to4 Tunneling Mechanism

An automated 6to4 tunnel enables isolated IPv6 domains to be joined over an IPv4 network to virtual IPv6 networks. It very well may be designed on a border router in a disconnected IPv6 network and makes a tunnel on a per-packet basis to a boundary router in another IPv6 network over an IPv4 framework. Therefore, the routers that execute IPv4 & IPv6 simultaneously encapsulate IPv6 traffic inside IPv4 packets.

Method

As a simulation experiment of 6to4 tunneling Figure 13 below shows a tunnel is created between R1 and R3 for the two IPv6 networks to communicate through the existing IPv4 network. The two IPv6 networks were connected via Gigabit Ethernet ports (g0/0) on routers R1 and R3, which assigned IPv6 addresses. The IPv4 & IPv6 were configured with routing protocols OSPF and RIPng respectively

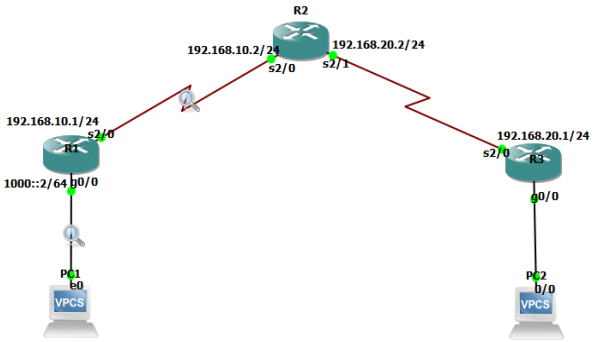


Figure 13: 6to4 Tunneling Network Topology

To configure 6to4 tunnels, it needs to set the tunnel mode *ipv6ip* 6to4 identify the tunnel source, and configure the 6to4 IPv6 address for that tunnel. It will not require a tunnel destination because IPv4-compatible with IPv6 tunnels; the tunnel destination will be derived from the IPv4 rooted in the destination IPv6 address. Therefore, 6to4 is a point-to-multipoint tunnel type, which treats the underlying IPv4 infrastructure as a Non-Broadcast Multi-Access (NBMA) network. The following is the sample configuration commands.

All configurations of 6to4 tunneling, network addresses, and routing tables can be found in Appendix 2: 6to4 tunneling all routers configuration source code

R1# IPv6 unicast-routing
Interface tunnel 0
IPv6 address2002::1/64
IPv6 rip 6bone enable
Tunnel source s2/0
Tunnel destination 192.168.20.1
Tunnel mode IPv6ip
No shut
Exit
Interface s2/0
IP add 192.168.10.1 255.255.255.0
No shut
Exit
Interface g0/0
IPv6 enable
IPv6 add 1000:: 2/64
IPv6 rip 6bone enable
No shut

R1 and R3 have the same configuration way except for address number (the IPv6 assigned on interface tunnel 0 is add 2002: 2/64, interface serial 2/0 is 192.168.20.1/24, interface Gigabit Ethernet 0/0 is 3000::2/64).

C. Simulation Experiment Result

Figure 14 below explains a packet within the tunnel shows that IPv6 data can move through the IPv4 network, which proves that the IPv6 packet is encapsulated within the IPv4 tunnel as an IPv4 packet.

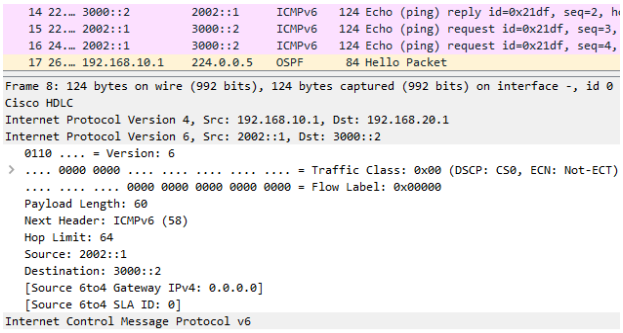


Figure 14: ICMPv6 message OSPF Hello Packet and IPv6 RIPng

Figure 15 below shows PC1 from the IPv6 network can communicate with PC2 of another IPv6 network by tunneling through the IPv4 network.

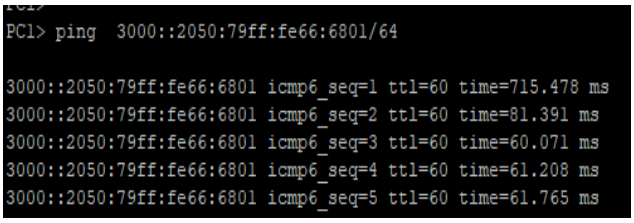


Figure 15: Ping Communication between PC1 and PC2

The analysis of a packet within the tunnel shows both IPv4 & IPv6 exist within the same ICMP, which verifies the IPv6 packet, was encapsulated within the IPv4 tunnel. However, the source and destination only refer to the start and ends of the tunnel.

IV. RESULT AND DISCUSSION

Analysis of Transition Mechanisms

The simulation experiment implemented confirmed how dual-stack and 6to4 tunneling works. The Dual-stack network is well appropriate to move between devices with dissimilar protocols on a network. However, a 6to4 tunnel is suitable to carry over a diverse protocol network. The dual-stacked device can interoperate in the same way with IPv4 devices, IPv6 infrastructure, and other dual-stacked end-devices. Tunnels can be made where there are IPv6 isolated by an IPv4. A tunnel indicates to encapsulate IPv6 in IPv4 so the packets can be sent over a backbone that does not back the encapsulated IP form. The security chance related to automated tunneling lets nodes set up tunnels that bypass a site's security spot check such as firewalls. In tunneling unencrypted IPv6 datagrams in IPv4, network security concerns impact information security.

In translators, a device or router is capable of interpreting from IPv4 to IPv6 or vice versa. This component is expecting to dispose of the requirement for dual-stack network operation by translating messages from IPv4-only devices to function inside an IPv6 framework. The comparisons of the three IPv6 transition techniques are analyzed in Table 6 below.

Table 4: Transition Mechanism Analysis

Transition	Strength	Weakness	Security
Dual-stack	✓ available on the most platforms ✓ simple to deploy ✓ Greatest flexibility ✓ Support all OS/ device	✓ Extra Memory and CPU required ✓ Security requirements became more challenging ✓ Two routing table required	✓ subject to attack on both IPv4 and IPv6 ✓ Two firewalls &/ IDIPS sets and policies
Tunneling	✓ Allows the IPv6 transported over an IPv4 network ✓ No additional management	✓ Additional CPU load to perform the encapsulation or decapsulation ✓ Harder to network management	✓ Automatic tunneling is less secure ✓ susceptible to packet forgery and DoS attacks
Translation	✓ support private address space ✓ Solve network interoperability problems	✓ Complicated to be administered ✓ Some security risks especially with NAT ✓ Harder to control on a larger scale	✓ IPsec can't be used end-to-end ✓ DNSsec can't be used with DNS64

Dual-stack achieves every requirement for transition mechanism, however, tunneling and translation mechanism not allow the use of IPv4 & IPv6 together and afford a seamless transition from IPv4 to IPv6. Nowadays, most of the hardware and software already keep up with both protocols. Therefore, dual-stack was preferred as the transition mechanism for the testbed, which was illuminated in the next sections.

IPv6 Dual-stack Vulnerability Test and Results

Kali Linux 2019.3 was used to simulate as the attacker on the network. The THC-IPv6 of tools was loaded on the machine and the next attack tools were executed. The tools used to carry out this thesis simulation experiment were *flood_router26, DoS-new-ip6, exploit6 of THC-IPv6.* It was not possible to simulate attacks for all the tools due to the many attacks, which exist. Those three attack tools were selected purposely to demonstrate that IPv6 is vulnerable to DoS as many literature shows. However, this shows the possibility of many attacks that can be carried out. The remaining THC-IPv6 attack tools are listed in Appendix 4: THC-IPv6 toolkit tools and their description

Flood_router26: THC-IPv6 toolkit that can flood the LAN with router advertisements.

The flood of packets attack inhibits computers from joining the IPv6 network that has already joined the network using automatically configured IPv6 addresses to lose their network connections. When a RA flood attack was launched, the attack packets were sent to all nodes within the network using the all-nodes multicast address, ff02::1. The command prompt terminal of Kali Linux 2019.3 was opened by making both attacker and victim system into the same LAN1 and then the command 'atk6-flood_router26 eth0' was typed. It started flooding the network with router advertisements on eth0, and then dots were printed for every 1000 packets, as shown in Figure 16 below.

Figure 16: The updated Version of the Flooding Router Tool

A flood attack in which the attacker attempts to overwhelm a targeted device with ICMPv6 echo request packets, causing the target network or node to become inaccessible to normal traffic.

The Experiment Result of RA Flooding

Figure 17 below is the Wireshark result while flood_router26 attack running shows the attacker Kali Linux 2019.3 sends unlimited RA flooding to the Local Network. The Router Advertisement (134) with code 0 indicates that the network was sending RA flooding

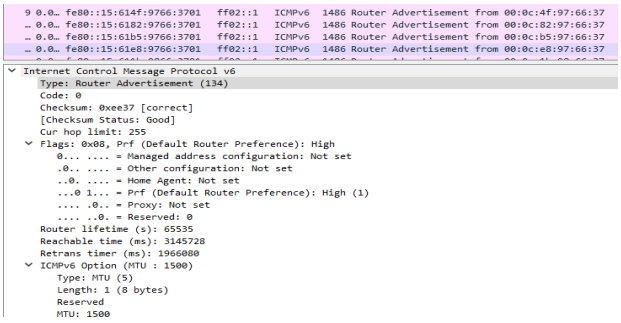


Figure 17: Router Advertisement flooding from the attacker

All RA's message was sent to FF02::1 multicast group so that all nodes on the same link would be received the announced fake prefixes. These nodes will configure their default gateway based on **the** fake announced prefixes. The different levels of preference are high (specify a high preference for a device), low (low preference for a device), and medium (specify a medium preference for a device this is the default preference). The default router sends out RAs with "Medium" preference, but the fake RAs set the preference flag to "high," pushing nodes to use it as their default gateway. If it is labeled with high preference, this could avail to make fake Router Advertisements that are transmitted. Figure 18 below Windows 10 was completely unresponsive and hard to access when the '*ipconfig*' command is running on windows PowerShell; it needed a reboot to restore its initial state. The computer would be flooded with the router advertisements, make the computer overhang to a point where it is unusable. Therefore, the attack made the automatically configured windows 10 to lose its network connection.

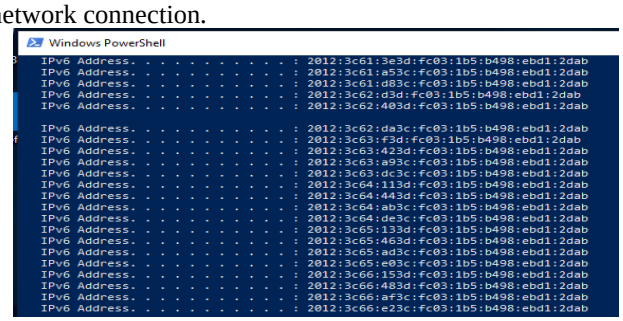


Figure 18: during Flood, Windows 10 unable to get IPv6 Address

Once attack against the network, the Windows 10 possessed and lead to all IPv6 routes advertised by the RA, which leads R1 to high CPU usage as figure 19 below. Packets diffused for the **period** of flooding attacks can exhaust the CPU, which can lead to the degradation of entire network performance.

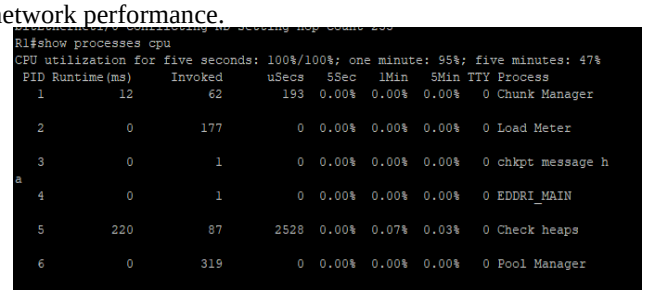


Figure 19: R1 CPU status, after Attacked by Flood Router

On R1 before the attack started, the CPU usage was almost 1%. After the attack CPU usage for five seconds is 100%. This is the CPU usage on the router for the last 5 seconds. During an interfere with, the CPU should deal with the capacities for the interaction rather than an interface. 95% is the CPU usage of the **router** in the course of the last one minute. During five minutes, the CPU utilization is 47%, which is over the last 5 minutes. Figure 20 below shows that the windows 10 CPU utilization was 8% before being attacked and it became 100% after the attack

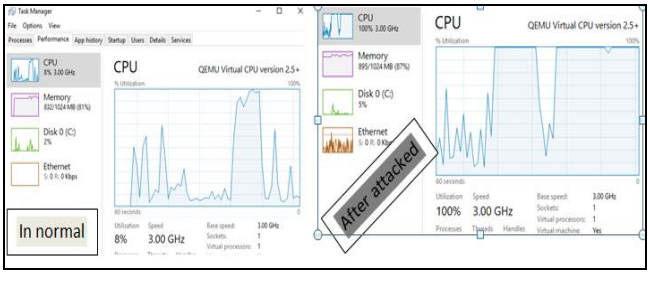


Figure 20: Windows 10 CPU Utilization before and after the Attack

DoS-new-ip6: This tool avoids new IPv6 interfaces to come up to the network, by sending answers to duplicate IPv6 checks DAD.

An attempt of DoS on DAD attack during address auto-configuration in IPv6 link-local communication has been examined. This tool can be considered as a couple of *detect-new-ip6*. It sneaks around for ICMPv6 DAD packets on the network, however in the event that it sees one, it will send a reaction that this IPv6 address as of now exists, this way we can come to that no host will actually want to interface with the network. The "*atk6-DoS-new-ip6 eth0*" command tool was run on the Kali Linux 2019.3 to test the IPv6 network. ICMPv6 started to send a spoofed packet shown in figure 21

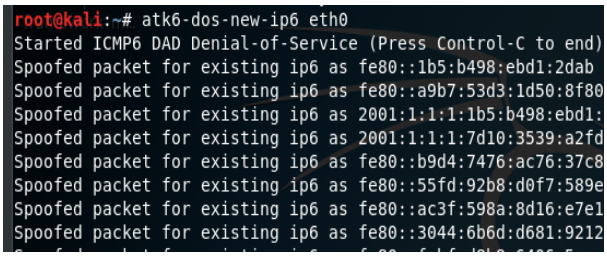


Figure 21: DoS Attack through Kali Linux 2019.3

Result

After the network was attacked, Windows 10 cannot communicate using IPv6. In the IPv6-only network, the host is disconnected from its neighbor and is not able to communicate. During the attack, if the Local Ethernet is disabled and then enabled, it has been noticed that Windows 10 nodes are unable to configure Global and Temporally IPv6 addresses after the attack command was running as displayed in Figure 21.

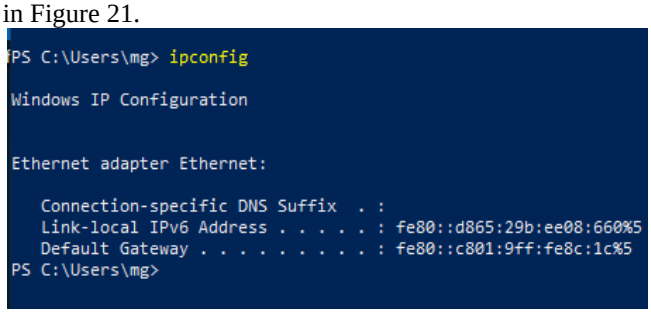


Figure 22: Windows 10 unable to get Global link address

Exploit6:- Performs exploits of various CVE known IPv6 vulnerabilities on the destination. Exploit6 implements various CVE and non-CVE techniques to compromise a victim host. The following figure 23 shows the exploit attack against Windows 10 with IPv6 address from the Kali Linux 2019.3

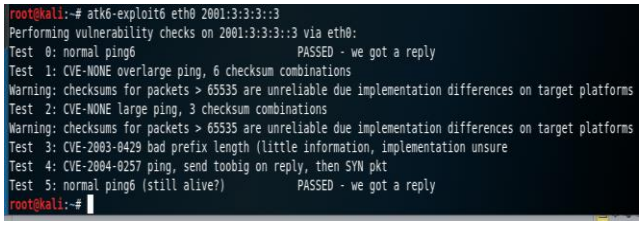


Figure 23: CVE and Warning while Exploiting Attack run on Kali Linux 2019.3

Common Vulnerabilities and Exposures (CVE): CVE database maintains a list of all kinds of discovered security issues within commonly used products, both hardware, and software. **Vulnerability** is a fault in software that makes available an attacker with direct admittance to a framework or network. An exposure is demarcated as a misstep in software or configuration that furnishes an assailant with indirect admittance to a framework or network.

Table 5: Vulnerability Types and Their Properties

Vulnerability detail	Confidentiality Impact	Integrity Impact	Availability Impact	Access Complexity	authentication	Vulnerability type(s)
2004-0257	None	None	Partial	Low	Not required	DoS
2003-0429	Partial	Partial	Partial	Low	Not required	DoS

CVE-2004-0257 lets remote attackers cause DoS by transferring an IPv6 packet with a less MTU to a snooping port and then allowing a TCP connection to that port. CVE-2003-0429 is earlier permits, remote attackers, to cause a DoS and conceivably execute self-assertive code by means of invalid IPv4 or IPv6 prefix lengths, perhaps setting off a support flood

Wire shark Result of Exploit6 Attack

RFC 6948, if the reassembled packets were less than 1280 bytes then the devices are supposed to drop them since any data link layer conveying IPv6 data must be capable of delivering an IP packet containing 1280 bytes or less without the need to invoke end-to-end fragmentation at the IP layer. When an attacker sends a spoofed packet huge message to the target device, it may unnecessarily divide the packet into fragments and send each fragment to an end node.

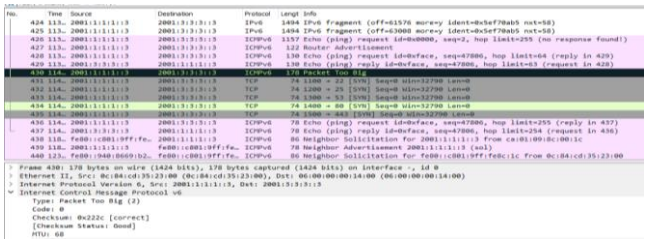


Figure 24: ICMPv6 Packet huge message sent after Attacked

A packet of fewer than 1280 bytes of MTU is regarded as illegal [60]. If the MTU size is less than the packet length, it drops the packet and sends an ICMPv6 Packet Too Big (PTB) message to the source node [61].

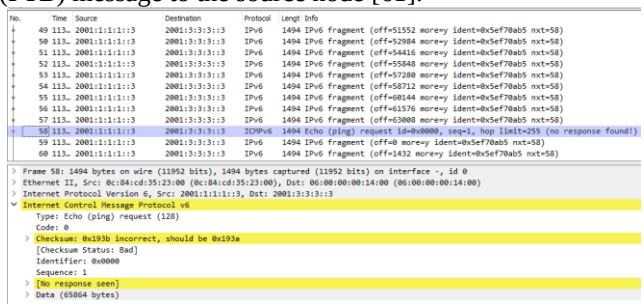


Figure 25: many IPv6 Fragments Result from no Response to the destination Host

The Next Header for IPv6 (44) indicates the IPv6 fragmentation Extension header. IPv6 fragmentation could consume CPU, which leading to a Denial of Service. It could indicate that the network is mix up these types of extension headers,

which create a more complex packet to get into the node. The RFC 2460 defines the extension headers as shown in Appendix 3, ICMPv6 error message, codes, and extension header. When a sender sends a packet to the end device, the routers on the path compare the packet size with their MTU. The lesser MTU sizes are found by accepting PTB messages. If the goal is multicast, there are numerous paths and packets may travel, and each way can have a diverse path MTU. PTB messages will be produced fairly as with a unicast goal, and the packet size utilized by the sender is the smallest path MTU of the destination.

Proposing Preventive Mechanism Preventive Mechanism for Flood_Router26 Attack

The prevention mechanism purposes to break an attack before it occurs to a local or a wide network. According to IETF, types of solutions have been introduced to protect NDP, which is IPsec and SeND. Router ACLs, firewalls, and other security mechanisms need to be carefully managed to hold ICMPv6 functionality [19]. firewalls are not as obtainable for the IPv6 protocol compared to IPv4 [21].

Table 6: ICMPv6-based DoS and DDoS preventive mechanism [62]

Preventive method	Description	Drawbacks
IPsec	ICMPv6 DoS attacks can be prevented using IPsec based on attacks are performed using spoofed source addresses	It cannot solve security problems Because IPsec depends on IKE which needs a valid IPv6 address,
SeND	It added CGA to the NDP, an option to prevent address spoofing based on the public-private key to be generated by all nodes.	CGA cannot verify the real identity of users and is also insufficient to ensure the CGA address that belongs to a particular node
SAVI	SAVI prevents address spoofing by binding each switch's physical port with an IPv6 source address.	it cannot handle flooding DoS or DDoS attack when it is launched by the real identity of the attacker
RA Guard	RA Guard prevents DoS assaults that are based on RA messages only.	Cannot be used on trunk ports, it cannot protection Wi-Fi, some switches do not support
Disable IPv6	Completely deactivate the IPv6 protocol from the system	The system cannot get IPv6 service

RA Guard: IPv6 RA Guard care for the network to block unwanted RA messages that derive from the network. It inspects these RAs and filters out RAs that are sent by illegal devices.

Method

The following RA Guard has configured on layer 2 switches interface with running on GNS3, the number of processor 2, amount of memory 512MB, and type Telnet.

Switch2#conf termin
Enter configuration commands, one per line. End with CNTL/Z.
Switch2 (config)#ipv6 nd ra-guard enable // Enable the IPv6 RA guard
Switch2 (config)#IPv6 nd raguard policy Host //create policy
Switch2 (config-nd-raguard)#device-role host
Switch2 (config)#IPv6 nd raguard policy ROUTER //create policy
Switch2 (config-nd-raguard)#device-role router
Switch2 (config-nd-raguard)#interface g1/0
Switch2 (config-nd-raguard)#vlan configuration 1
Switch2 (config-nd-raguard)#router-preference maximum medium
Switch2 (config-vlan-config)#IPv6 nd raguard attach-policy HOST //define the role of the device attached to the port
Switch2 (config-vlan-config)#IPv6 nd raguard attach-policy ROUTER
//define the role of the device attached to the router
Switch2 (config-vlan-config)#end
Configured from console by console
Switch2#show ipv6 nd raguard policy Host
Policy Host configuration:
router-preference maximum medium
Policy Host is applied on the following targets:
Target Type Policy Feature Target range
Gi1/0 PORT Host RA guard vlan all
vlan 1 VLAN HOST RA guard vlan all
Switch2#debug device-tra
Switch2#debug device-tracking raguard //IPv6 device tracking offers IPv6 host liveness tracking, updated when an IPv6 host disables
Switch2#undebug all
IPv6 snooping - RA guard debugging is on

Result

After the switch was configured and the RA flooding attacked windows 10 through Kali Linux, the ping communication, accessibility, and CPU utilization was normal. The effect was displayed in figure 26 below by putting both screenshots together

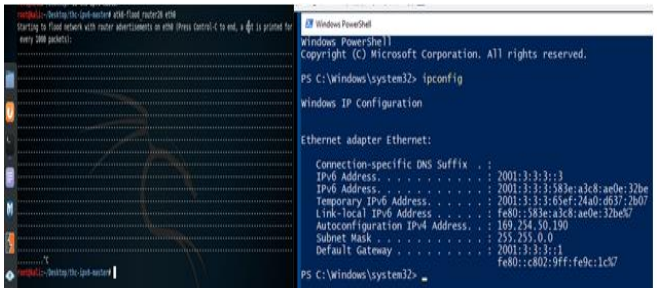


Figure 26: flooding attack and ipconfig response after RA Guard configured

Preventive Mechanism against Exploit6 Attack

Fragmentation is a normal process that occurs when a large packet is received. Fragmentation disassembles the IP packet into smaller packets before transmission to the destination host.

However, due to the attack, there are irregular IPv6 packet fragmentations that cause no response or crash system (Table 9).

Table 7: IPv6 fragmentation type with proposed solutions

Fragmentation Type	Description	Solutions
Overlapping Fragment	The attacker can overwrite the fragment offset in the non-initial IP fragment packets.	RFC5722 disallowing in IPv6 fragments to stop this attack
Atomic Fragments	packets are typically sent by nodes that have received an ICMPv6 "Packet Too Big" error message that advertises a Next-Hop MTU smaller than 1280 bytes [63]	eliminating this attack vector [62]
Tiny Fragment	An IPv6 Tiny Fragment is defined as a non-last fragment that has a payload length of fewer than 1200 octets [64].	A Tiny Fragment should be treated to have malicious intent and SHOULD be silently dropped [64].

The Cisco IOS includes a Virtual Reassembly, which checks divided packets. It reassembles divided packets, analyzes any out of fragments. Virtual Fragment Reassembly (VFR) empowers the Cisco IOS XE Firewall to make conceivable dynamics ACLs to secure the network from different fragmentation attacks. It gives the capacity to gather the fragments and give Layer 4 data for all fragments for IPsec and NAT64 highlights [65].

The following VFR code was configured on the R1 to drop ICMPv6 PTB error messages, which makes CPU overload and directed to the host that advertises IPv6 fragments and MTU smaller than 1,280 bytes.

```
R2#conf terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
R1(config)#inter
R1(config)#interface g1/0
R1(config-if)#IPv6 virtual-re
R1(config-if)#IPv6 virtual-reassembly max-re
R1(config-if)#IPv6 virtual-reassembly max-reassemblies 32
max-fra
R1(config-if)#$l-reassembly max-reassemblies 32
max-fragments 4 time
R1(config-if)#$ly max-reassemblies 32 max-fragments 4
timeout 7 drop-fra
R1(config-if)#$ssemblies 32 max-fragments 4 timeout 7
drop-fragments
R1(config-if)#exit
R1(config)#end
R1#
*Oct  6 14:42:09.343: %SYS-5-CONFIG_I: Configured
from console by console
R1#show IPv6 virtual-reassembly
 All enabled IPv6 interfaces...
%Interface GigabitEthernet1/0
  IPv6 configured concurrent reassemblies
(max-reassemblies): 32
  IPv6 configured fragments per reassembly
(max-fragments): 4
  IPv6 configured reassembly timeout (timeout): 7 seconds
  IPv6 configured drop fragments: ON
IPv6 current reassembly count:0
 IPv6 current fragment count:0
 IPv6 total reassembly count:0
 IPv6 total reassembly timeout count:0
```

Where,

Max-reassemblies: - Maximum number of IPv6 datagrams that can be reassembled at any given time. If the maximum value, all fragments within the fragment set will be dropped. Default value: 16.

Max-fragment: - Maximum number of fragments that are allowed per IPv6 datagram (fragment set). In case an IPv6 datagram that is being reassembled gets more than extreme permitted parts, the IPv6 datagram will be dropped. Default value: 32

Timeout: - Timeout value, in seconds, for an IPv6 datagram that is being reassembled. On the off chance that an IPv6 datagram does not get all of the fragments inside the desired time, the IPv6 datagram will be dropped. Default value: 3 seconds.

Result

The above experiment shows the IPv6 VFR feature configured on the entrance interface name GigabitEthernet1/0 of R1. Therefore, during the attack, Windows 10 drops fragments. As a result, IPv6 fragment flooding and PTB errors were not sent. The attack from the Kali Linux and the result on the Wireshark analyzer was displayed in figure 27 below.

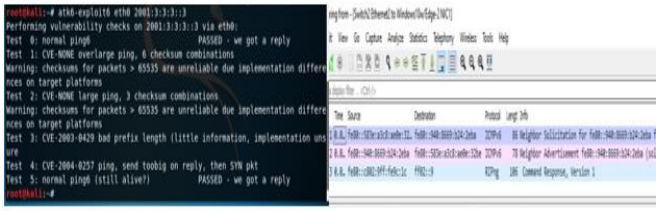


Figure 27: Screenshot after VFR configured

In other words, the screenshot of Wireshark above shows that there is no ICMPv6 PTB error message and IPv6 fragment flooding delivered to the source and destination address from the router.

V. DISCUSSION

After this research experiment was implemented, the dual-stack mechanism was selected because of its prominence, availability on many platforms, and simplicity to deploy to the existed network by implementing a security system for both IPv4 & IPv6 simultaneously. The IPv6 security vulnerability was tested by using attack tools like Flood_router26, DoS-new-ip6, and exploit6 of THC-IPv6 toolkits.

A Flood_router and DoS-new-ip6 of THC-IPv6 attack are to disturb network made to take down the targeted network, host, or PCs with fake traffic and block new devices from the network. The purpose of such an attack is to make it inaccessible to the network.

RA flooding attack affects performance issues by overwhelming computer resources such as CPU and crashes the network completely. The other attack was tested by exploit6 of the THC-IPv6 tool. This type of attack made IPv6 fragmentation. The attacker splits the packet into many small fragmented packets less than the IPv6 standard (1280 bytes). IPv6 nodes might receive ICMPv6 PTB packets because of the Exploit6 attack. However, the recommended MTU for IPv6 is 1500 bytes. When attacks are flooded with many IPv6 fragment packets, the data do not arrive at the destination; the router sends back the ICMPv6 message 'no response' and makes the systems busy. RA Guard was configured to layer-2 switch to protect from the RA flooding in this thesis and the result was effective to prevent such attack. The other DoS vulnerability was IPv6 fragmentation. This type of attack could be protected by configuring VFR. VFR drops the atomic IPv6 fragmentation, so the entire network, particularly the CPU of the destination device was free from being overloaded because of large fragmentation.

VI. CONCLUSION

In this thesis that set out to resolve a practical problem with design science research, to achieve the general objective of 'investigating the security problems related to IPv6 and proposing the preventive mechanism' specific objectives were set. Different kinds of literature related to the research were reviewed. The researcher has understood IPv4 addresses were almost entirely depleted. Therefore, the research focused on transitioning to IPv6 which would be necessary to deploy within a short time. Through a simulation experiment, the implementation of transition mechanisms (dual-stack and tunneling) and the security vulnerabilities of dual-stack were recognized in this paper. According to the experiments on security vulnerabilities, an attacker can cause DoS, because the IPv6 fragmented PTB caused many atomic fragment packets and RA flooding attack that makes devices inaccessible to the network. Therefore, intermediary devices must be configured very well to protect from RA flooding and IPv6 fragmentations, IPv6 ACLs and RA guards were proposed in order to protect from flooding attacks and VFR should be configured to prevent IPv6 fragmentation.

REFERENCES

1. M. Nazari and L. Galla, "Denial of Service attack in IPv6 networks and counter measurements," 2016.
2. J. L. Shah, "A novel approach for securing IPv6 link local communication," *Inf. Secur. J.*, vol. 25, no. 1–3, pp. 136–150, 2016.
3. A. Alsadhan *et al.*, "Locally weighted classifiers for detection of neighbor discovery protocol distributed denial-of-service and replayed attacks," *Trans. Emerg. Telecommun. Technol.*, no. March, pp. 1–15, 2019.
4. J. Beeharry and B. Nowbutsing, "Forecasting IPv4 exhaustion and IPv6 migration," *2016 IEEE Int. Conf. Emerg. Technol. Innov. Bus. Pract. Transform. Soc. EmergiTech 2016*, pp. 336–340, 2016.
5. O. E. Elejla, B. Belaton, M. Anbar, and I. M. Smadi, "A New Set of Features for Detecting Router Advertisement Flooding Attacks," *Proc. - 2017 Palest. Int. Conf. Inf. Commun. Technol. PICICT 2017*, pp. 1–5, 2017.
6. A. S. Ahmed, R. Hassan, and N. E. Othman, "Denial of service attack over secure neighbor discovery (SeND)," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 5, pp. 1897–1904, 2018.
7. R. Alnakhalny, S. Ramadass, and S. Manickam, "A Study on Detecting ICMPv6 Flooding Attack based on IDS," *Australian Journal of Basic and Applied Sciences*, 2013. .
8. J. Weber, "Master Thesis IPv6 Security Test Laboratory," 2013.
9. M. F. Suleiman and J. Cordry, "Analysis of organizations IPv6 deployment strategies in Nigeria and evaluating suitable transition mechanisms," *Proc. 2017 IEEE 2nd Adv. Inf. Technol. Electron. Autom. Control Conf. IAEAC 2017*, pp. 695–704, 2017.
10. Google, "Google IPv6." https://www.google.com/intl/en/ipv6/statistics.html.
11. J. Gin, "Evaluation of Open-Source Intrusion Detection Systems for IPv6 Vulnerabilities in Realistic Test Network," pp. 177–192, 2010, [Online]. Available: https://repositories.lib.utexas.edu/bitstream/handle/2152/62661/GIN-MASTERSREPORT-2017.pdf?sequence=1&isAllowed=y.
12. G. K. D. K. S. Kahlon, "Study and Comparison of Network Security in IPv4 and IPv6," *Int. J. Sci. Res.*, vol. 6, no. 4, pp. 2434–2436, 2017, [Online]. Available: https://www.ijsr.net/archive/v6i4/ART20172958.pdf.
13. O. E. Elejla, M. Anbar, and B. Belaton, "ICMPv6-Based DoS and DDoS Attacks and Defense Mechanisms: Review," *IETE Tech. Rev. (Institution Electron. Telecommun. Eng. India)*, vol. 34, no. 4, pp. 390–407, 2017.
14. W. N. A. W. Ali, A. H. M. Taib, N. M. Hussin, R. Budiarto, and J. Othman, "Distributed security policy for IPv6 deployment," *3rd ISESEE 2011 - Int. Symp. Exhib. Sustain. Energy Environ.*, no. June, pp. 120–124, 2011.
15. S. Praptodiyono, R. K. Murugesan, I. H. Hasbullah, C. Y. Wey, M. M. Kadhum, and A. Osman, "Security mechanism for IPv6 stateless address autoconfiguration," *Proc. 2015 Int. Conf. Autom. Cogn. Sci. Opt. Micro Electro-Mechanical Syst. Inf. Technol. ICACOMIT 2015*, pp. 31–36, 2016.
16. Y. Lu, M. Wang, and P. Huang, "An SDN-based authentication mechanism for securing neighbor discovery protocol in IPv6," *Secur. Commun. Networks*, vol. 2017, 2017.
17. N. C. Arjuman and S. Manickam, "A review on ICMPv6 vulnerabilities and its mitigation techniques: Classification and art," *I4CT 2015 - 2015 2nd Int. Conf. Comput. Commun. Control Technol. Art Proceeding*, no. August, pp. 323–327, 2015.
18. J. Ullrich, K. Krombholz, H. Hobel, A. Dabrowski, and E. Weippl, "IPv6 Security : Attacks and Countermeasures in a Nutshell," *Usenix*, no. 4, 2014, [Online]. Available: https://www.usenix.org/system/files/.../woot14-ullrich.pdf.
19. S. Frankel, R. Graveman, J. Pearce, and M. Rooks, "Guidelines for the Secure Deployment of IPv6 Recommendations of the National Institute of Standards and Technology," *NIST Spec. Publ. 800-119*, p. 188, 2010.
20. Tutorials Point India Limited, "IPv6 Headers." https://www.tutorialspoint.com/ipv6/ipv6_headers.htm.
21. H. Sharma, S. Saad, and S. A. Khan, "IPv6 Exploits."
22. K. Mudaliar, "Performance Evaluation of Defence Mechanisms against ICMPv6 Router Advertisement Flood Attacks By," 2015.
23. "Transition from IPv4 to IPv6 and their Security Challenges," *Int. J. Sci. Res.*, vol. 4, no. 12, pp. 1837–1841, 2015.
24. A. Chandra and K. Lalitha, "IPv4 to IPv6 Network Migration and Coexistence," pp. 1005–1009, 2015.
25. G. Nahom, "IPV6 Migration Framework for IPV6 Migration Framework for EthioTelecom .," no. March, 2019.
26. D. Programme and I. N. Information, "IMPLEMENTATION OF IPv6," no. September, p. 73, 2014.
27. U. States, E. Union, C. Code, and P. Capita, "Migration from IPV4 to IPV6 in India," pp. 4–7.
28. A. Shiranzaei, "IPv6 Security Issues — A Systematic Review," pp. 41–49.
29. W. Alzaid and B. Issac, "Analysis of IPv6 through implementation of transition technologies and security attacks," *Int. J. Bus. Data Commun. Netw.*, vol. 12, no. 1, pp. 36–62, 2016.
30. E. Çalışkan, "IPv6 Transition and Security Threat Report," *Ccdcoe*, pp. 1–11, 2014.
31. E. Durdağı and A. Buldu, "IPV4/IPV6 security and threat comparisons," *Procedia - Soc. Behav. Sci.*, vol. 2, no. 2, pp. 5285–5291, 2010.
32. G. B. Satrya, R. L. Chandra, and F. A. Yulianto, "The detection of DDOS flooding attack using hybrid analysis in IPv6 networks," *2015 3rd Int. Conf. Inf. Commun. Technol. ICoICT 2015*, pp. 240–244, 2015.
33. A. Epishkina, M. Finoshin, and K. Kogos, "Information Science and Applications (ICISA) 2016," *Lect. Notes Electr. Eng.*, vol. 376, pp. 641–650, 2016.

34. J. Bejar and C. Caicedo, “IPv6 Security Analysis,” no. June, 2014, [Online]. Available: https://www.researchgate.net/publication/263444409_IPv6_Security_Analysis.
35. J. Weber, “IPv6 Security - An Overview,” 2013. https://labs.ripe.net/Members/johannes_weber/ipv6-security-an-overview#:~:text=If an attacker sends spoofed,one of the default routers.&text=This leads to a situation,IPv6 nodes to the Internet.
36. I. Cisco Systems, “Implementing IPsec in IPv6 Security.” .
37. Oracle Corporation and/or its affiliates, “IPv6 Security Improvements,” 2010. https://docs.oracle.com/cd/E19683-01/817-0573/chapter1-29/index.html.
38. A. K. Al-Ani, M. Anbar, S. Manickam, and A. Al-Ani, “DAD-match; Security technique to prevent denial of service attack on duplicate address detection process in IPv6 link-local network,” *PLoS One*, vol. 14, no. 4, pp. 1–20, 2019.
39. M. Teku, “a study on the nature of ipv6 intrusions and the road map towards their detection & prevention,” 2011.
40. “Department of Computer Science and Master Thesis Vulnerabilities and Threats in IPv6 Environment,” 2013.
41. A. T. Zamani, “Deploying IPv6 : Security and Future,” vol. 3, no. 4, pp. 34–42, 2014.
42. T. Zhang and Z. Wang, “Research on IPv6 Neighbor Discovery Protocol (NDP) security,” *2016 2nd IEEE Int. Conf. Comput. Commun. ICCC 2016 - Proc.*, pp. 2032–2035, 2017, doi: 10.1109/CompComm.2016.7925057.
43. C. Ouseph and B. R. Chandavarkar, “Prevention of MITM attack caused by rogue router advertisements in IPv6,” *2016 IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. RTEICT 2016 - Proc.*, pp. 952–956, 2017.
44. S. U. Rehman and S. Manickam, “Significance of duplicate address detection mechanism in IPv6 and its security issues: A survey,” *Indian J. Sci. Technol.*, vol. 8, no. 30, pp. 1–8, 2015.
45. S. U. Rehman and S. Manickam, “Novel mechanism to prevent Denial of Service (DoS) attacks in IPv6 duplicate address detection process,” *Int. J. Secur. its Appl.*, vol. 10, no. 4, pp. 143–154, 2016.
46. A. Zubair, A. Jwaid, and A. Salih, “Analysing denial of service attack traffic signature in IPv6 local network using correlation inspection,” *FTC 2016 - Proc. Futur. Technol. Conf.*, no. December, pp. 1008–1013, 2017.
47. H. A. Dawood, “IPv6 Security Vulnerabilities,” vol. 1, no. 4, pp. 100–105.
48. INTECO-CERT, “REPORT ON THE SECURITY IMPLICATIONS OF IMPLEMENTING IPv6,” no. June, 2010.
49. J. W. Kim, H. H. Cho, G. J. Mun, J. H. Seo, B. N. Noh, and Y. M. Kim, “Experiments and countermeasures of security vulnerabilities on next generation network,” *Proc. Futur. Gener. Commun. Networking, FGCN 2007*, vol. 2, pp. 559–564, 2007.
50. A. S. Ahmed, R. Hassan, and N. E. Othman, “Improving security for IPv6 neighbor discovery,” *Proc. - 5th Int. Conf. Electr. Eng. Informatics Bridg. Knowl. between Acad. Ind. Community, ICEEI 2015*, pp. 271–274, 2015.
51. A. Hj, M. Taib, and R. Budiarto, “Security Mechanisms for the IPv4 to IPv6 Transition,” no. May 2014, 2008.
52. G. Drago, “Security aspects in IPv6 networks – implementation and testing,” vol. 33, pp. 425–437, 2007, doi: 10.1016/j.compeleceng.2007.05.008.
53. Z. Ashraf and M. Yousaf, “Secure Inter-VLAN IPv6 Routing : Implementation & Evaluation SECURE INTER-VLAN IPv6 ROUTING : IMPLEMENTATION & EVALUATION,” no. January, 2019.
54. P. P. Jeremy Grossmann, Dominik Ziajka, “Graphical Network Simulator-3.” .
55. K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, “A Design Science Research Methodology for Information Systems Research A Design Science Research Methodology for Information Systems Research,” vol. 1222, 2014.
56. S. T. March and G. F. Smith, “Design and natural science research on information technology,” *Decis. Support Syst.*, vol. 15, no. 4, pp. 251–266, 1995.
57. A. I. Conference, “Yusuf Maitama Sule University , Kano Faculty of Science,” no. November, pp. 16–20, 2017.
58. G. Sharma and B. Sharma, “Comparison of Routing Protocols in-terms of Packet Transfer Having IPV6 Address Using Packet Tracer,” vol. 2, no. 4, pp. 4–8, 2018.
59. K. Yun and L. Yan, “Distributed intrusion detection and research of fragment attack based-on IPv6,” *Adv. Mater. Res.*, vol. 268–270, pp. 1797–1801, 2011.
60. Juniper Networks, “Understanding Path MTU Messages for IPv6 Packets,” 2020. https://www.juniper.net/us/en/company/.
61. M. A. &Bahari B. Omar E. Elejla, “ICMPv6-Based DoS and DDoS Attacks and Defense Mechanisms: Review,” 2016.
62. F.Gont, "Processing of IPv6 atomic fragments" internet engineering task force: Request For Comment, 2013
63. S.Krisman Ericsson, "Handling of overlapping IPv6 fragments", network working group, December 2009
64. C. I. O. S. Firewall--specifically, “Restrictions for Virtual Fragmentation Reassembly,” pp. 1–6.

APPENDICES

Appendix 1: Dual-stack R1 and R2 both IP and routing configuration on GNS3

Table 1: Router R1 & R2 Configuration

R1	R2
R1#enable	R2#enable
Config t	Configure t
IPv6 unicast-routing	IPv6 unicast-routing
IPv6 router rip DSTM	IPv6 router rip DSTM
Int serial2/0	Int serial2/0
IPv6 enable	IPv6 enable
Ip add 10.2.2.1 255.255.255.0	Ip add 10.2.2.2
IPv6 add 2001:2:2:2::1/64	255.255.255.0
IPv6 rip DSTM enable	IPv6 add 2001:2:2:2::2/64
No shutdown	IPv6 rip DSTM enable
Interface g1/0	No shutdown
No ip add	Interface g1/0
IPv6 enable	No ip add
IPv6 add 2001:1:1:1::1/64	IPv6 enable
IPv6 rip DSTM enable	IPv6 add 2001:3:3:3::1/64
No shutdown	IPv6 rip DSTM enable
Interface g0/0	No shutdown
Ip add 10.1.1.1 255.255.255.0	Interface g0/0
IPv6 enable	Ip add 10.3.3.3
IPv6 add 2001:4:4:4::1/64	255.255.255.0
IPv6 rip DSTM enable	IPv6 enable
No shutdown	IPv6 add 2001:5:5:5::1/64
	IPv6 rip DSTM enable
	No shutdown

Table 2: Dual stack network addresses

Appliance name	Local-link scope	Global scope	Router link layer	MAC
Pc1	fe80::250:79ff:fe66:6800/64	2001:4:4:4:2050:79ff:fe66:6800/64	ca:01:09:8c:00:08	00:50:79:66:68:00
	10.1.1.3/24			
Pc2	fe80::250:79ff:fe66:6801/64	2001:1:1:1::2/64	ca:01:09:8c:00:1c	00:50:79:66:68:01
Pc3	fe80::250:79ff:fe66:6802/64	2001:5:5:5:2050:79ff:fe66:6802/64	ca:02:09:9c:00:08	00:50:79:66:68:02
	10.3.3.3/24			
Pc4	fe80::250:79ff:fe66:6803/64	2001:3:3:3::2/64	ca:02:09:9c:00:1c	00:50:79:66:68:03
Kali linux	Fe80::940:8669:b24:2eba/64	2001:1:1:1::3/64 2001:1:1:1:dea7:f29b:2f3a:2ccc/64	0c:84:cd:35:23:00	
Window 10	Fe80:addf:f8b9:666e:7a9e/64	2001:3:3:3::3/64 2001:3:3:3:addf:f8b9:666e:7a9e/64		

Appendix 2: 6to4 tunneling all routers configuration source code

Table 1: 6to4 tunneling all routers configuration source code

R1	R2	R3
R1# IPv6 unicast-routing Interface tunnel 0 IPv6 address2002::1/64 IPv6 rip 6bone enable Tunnel source s2/0 Tunnel destination 192.168.20.1 Tunnel mode IPv6ip No shut Exit Interface s2/0 Ip add 192.168.10.1 255.255.255.0	R2# conf t Inter s2/0 Ip add 192.168.10.2 255.255.255.0 No shut Exit Inter s2/1 Ip add 192.168.20.2 255.255.255.0 No shut Exit Router ospf 1 Network 192.168.10.0 0.0.0.255 area 0	R3# conf IPv6 unicast-routing Interface tunnel 0 IPv6 add 2002::2/64 IPv6 rip 6bone enable Tunnel source s2/0 Tunnel destination 192.168.10.1 Tunnel mode IPv6ip No shut Exit Inter s2/0 Ip add 192.168.20.1
No shut Exit Interface g0/0 IPv6 enable IPv6 add 1000::2/64 IPv6 rip 6bone enable No shut Exit Router ospf 1 Network 192.168.10.0 0.0.0.255 area 0 Exit exit	Network 192.168.20.0 0.0.0.255 area 0 Exit	255.255.255.0 No shut Exit Interface g0/0 IPv6 enable IPv6 address 3000::2/64 IPv6 rip 6bone enable No shut Exit Router ospf 1 Network 192.168.20.0 0.0.0.255 area 0 Exit

Table 1: 6to4 tunneling network addresses

Name	Link-local scope	Global scope	Router link layer	MAC
Pc1	fe80::250:79ff:fe66:6800/64	1000::2050:79ff:fe66:6800/64	ca:01:08:f9:00:08	00:50:79:66:68:00
Pc2	fe80::250:79ff:fe66:6801/64	3000::2050:79ff:fe66:6801/64	ca:03:09:18:00:08	00:50:79:66:68:01

Here you will found the routing table in configuration 6to4 that was used to simulate the network used.

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.10.0/24 is directly connected, Serial2/0
O    192.168.20.0/24 [110/128] via 192.168.10.2, 00:09:14, Serial2/0
R1#show ipv6 route
IPv6 Routing Table - Default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   1000::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   1000::2/128 [0/0]
     via GigabitEthernet0/0, receive
C   2002::/64 [0/0]
     via Tunnel0, directly connected
L   2002::1/128 [0/0]
     via Tunnel0, receive
R   3000::/64 [120/2]
     via FE80::C0A8:1401, Tunnel0
L   FF00::/8 [0/0]
     via Null0, receive
```

Figure 1: R1 IPv4 and IPv6 Routing Table

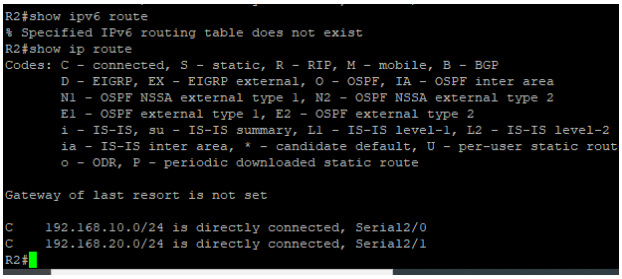


Figure 2: R2 IPv4 routing table

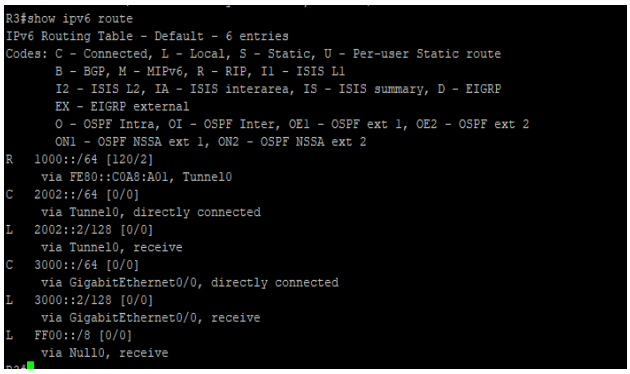


Figure 3: R3 IPv6 routing table

Appendix 3: ICMPv6 error messages and extension headers Here are some information of related ICMPv6 error messages and extension headers with their codes.

Table 1: ICMPv6 Error messages

Type Value	Message Name	Summary Description of Message Type
1	Destination Unreachable	Indicates that a datagram could not be delivered to its destination. *Code* value provides more information on the nature of the error.
2	Packet Too Big	Sent when a datagram cannot be forwarded because it is too big for the MTU of the next hop in the route. This message is needed in IPv6 and not IPv4 because in IPv4, routers can fragment oversized messages, while in IPv6 they cannot.
3	Time Exceeded	Sent when a datagram has been discarded prior to delivery due to the *Hop Limit* field being reduced to zero.
4	Parameter Problem	Indicates a miscellaneous problem (specified by the *Code* value) in delivering a datagram.

Table 2: IPv6 Extension Headers and their Recommended Order in a Packet

Header Type	Next Header Code
Hop-by-Hop Options	0
Destination Options (with Routing Options)	60
Routing Header	43
Fragment Header	44
Authentication Header	51
Encapsulation Security Payload Header	50
Destination Options	60
Mobility Header	135
No next header	59
TCP	6
UDP	17
ICMPv6	58

Appendix 4: THC-IPv6 toolkit tools and their description

Table 1: THC-IPv6 toolkit tools and their description

Tools	Descriptions
alive6	alive scanning, which will detect all systems listening to this address
denial6	a collection of denial-of-service tests against a target
detect-new-ip6	detect new IPv6 devices which join the network
DoS-new-ip6	Detect new IPv6 devices and tell them that their chosen IP collides on the network
exploit6	known IPv6 vulnerabilities to test against a target
fake_advertiser6	announce yourself on the network
fake_mIPv6	steal a mobile IP to yours if IPSEC is not needed for authentication
fake_mld6	announce yourself in a multicast group of your choice on the net
fake_router6	announce yourself as a router on the network, with the highest priority
flood_advertise6	flood a target with random neighbor advertisements
flood_router6	flood a target with random router advertisements
fuzz_ip6	fuzzer for IPv6
implementation6	performs various implementation checks on IPv6
parasite6	ICMPv6 NS/NA spoofer, puts you as man-in-the-middle, same as ARP MitM
redir6	redirect traffic to man-in-the-middle with a clever ICMPv6 redirect spoofer
sendpees6	Which generates a NS requests with many CGAs (crypto) to keep the CPU busy
smurf6/ rsmurf6	Local/remote smurfer, known to work only against Linux targets at the moment
toobig6	mtu decreaser with the same intelligence as redir6
trace6	very fast traceroute6 with supports ICMP6 echo request and TCP-SYN

AUTHORS PROFILE

J. Sebastian Nixon is a Ph.D. holder; he has published more than 20 international journals and a book in the area of Ad hoc networks. His research area interested is networking, ML and data science.

Megersa Amenu, has completed his Master's in Information Technology. He is having 12 years of teaching experience. His research area interested is networking & AI.