AN ANALYSIS OF THE RISK EXPOSURE OF ADOPTING IPV6 IN ENTERPRISE NETWORKS

A thesis submitted in partial fulfilment of the
requirements for the degree of

MASTERS IN SCIENCE
of
RHODES UNIVERSITY

by

ISTVAN SANDOR BERKO

December 2014

ABSTRACT

The IPv6 increased address pool presents changes in resource impact to the Enterprise that, if not adequately addressed, can change risks that are locally significant in IPv4 to risks that can impact the Enterprise in its entirety. The expected conclusion is that the IPv6 environment will impose significant changes in the Enterprise environment - which may negatively impact organisational security if the IPv6 nuances are not adequately addressed. This thesis reviews the risks related to the operation of enterprise networks with the introduction of IPv6. The global trends are discussed to provide insight and background to the IPv6 research space. Analysing the current state of readiness in enterprise networks, quantifies the value of developing this thesis.

The base controls that should be deployed in enterprise networks to prevent the abuse of IPv6 through tunnelling and the protection of the enterprise access layer are discussed. A series of case studies are presented which identify and analyse the impact of certain changes in the IPv6 protocol on the enterprise networks. The case studies also identify mitigation techniques to reduce risk.

ACKNOWLEDGEMENTS

I am thankful for the blessing The Almighty God has bestowed upon me with the opportunity to develop this thesis to completion.

This document would not have been possible without the help and consistent support of my supervisor, Prof. Barry Irwin and the departmental manager, Mrs Caro Watkins.

I would also like to thank my wife Naldine, my daughter, Alexa and my family, who have always provided me with the time and space to invest in my studies. I would like to, posthumously, thank my mother Irene, who always believed in me and planted and nurtured the seed for broadening my knowledge. I am also grateful to my father, Sandor, who inspires me daily.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

ALG	Application-Layer Gateway
APNIC	Asia Pacific Network Information Centre
ARP	Address resolution protocol
ASIC	Application Specific Integrated Circuit
CCNA	Cisco Certified Network Associate
CGA	Cryptographically Generated Address
CRC	Cyclic Redundancy Check
DAD	Duplicate address detection
DNS	Domain Name Service
DoS	Denial of Service
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
GDP	Gross Domestic Product
GIG	Global Information Grid
GRE	Generic Routing Encapsulation
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IoT	Internet of Things
MAC	Media Access Control
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NDP	Neighbour Discovery Protocol
NPAT	Network Port Address Translation
NRO	Numbers Resource Organization
OID	Organizationally Unique Identifier
OSI	Open Systems Interconnection
OTV	Overlay Transport Protocol
PACL	Port Access Control Lists
RFC	Request for Comment
RFID	Radio-frequency identification

RIPE NCC	Réseaux IP Européens Network Coordination Centre
RIR	Regional Internet Registries
SATCOM	Satellite communications
SAVI	Source Address Validation Improvement
SCTP	Stream Control Transmission Protocol
SEND	SEcure Neighbour Discovery
SHA	Secure Hashing Algorithm
SLAAC	Stateless Address Autoconfiguration
SQL	Structured Query Language
SSL	Secure Socket Layer
TCAM	Ternary Content-Addressable Memory
TLS	Transport Layer Security
VXLAN	Virtual Extensible LAN
VPLS	Virtual Private LAN Service
VRF	Virtual Routing and Forwarding
VSS	Virtual Switching System

Chapter 1

Introduction

Although the global adoption of IPv6 has been slow in recent years, it is, at present, showing a steady increase as the depletion of the IPv4 address space has become reality in our modern age (Narayan, Tauch & Zealand, 2010). Enterprises have been resistant to the change in the past because of the little perceived economic value in the migration or even adoption of an IPv6 network protocol. The clients of these enterprises and corporations, as well as their global partners, have started the migration process in locations where IPv6 service is provided and preferred and therefore the economic value of IPv6 connectivity is realising (Grossetete, Popoviciu & Wettling, 2008). The Internet is a space where milliseconds can have a dramatic impact on competition between organisations (Lohr, 2012). Owing to the scale and geographical diversity of the network, an ecosystem where the adoption of IPv6 can provide the competitive edge in business, will result in an accelerated drive to go ahead and adopt IPv6 in Enterprise.

The adoption of IPv6 does present a number of challenges. These obstacles form part of the resistance to adopt the protocol, which partially consists of the following:

- People skills and knowledge
- New and legacy technology support
- Service Provider adoption
- Historic IPv6 implementation failure

The lack of suitably skilled people has prevented widespread adoption owing to the perceived complexity and lack of understanding of the protocol mechanism and mean of addressing. In response to this Cisco (and other vendors) have started to use IPv6 as part of their basic network curriculum, and consequently, providing the industry with a pipeline of fresh IPv6 skills. The October 2013 release of the Cisco Certified Network Associate Routing and Switching Certification[1] (CCNA 100-101 and 100-102) now includes IPv6 (Cisco Systems Inc, 2013). As these new students pass through the training and the base knowledge spreads, the adoption will scale up.

In conjunction to the lack of skills, the technology support life cycle has been a major factor in contributing to the lack of IPv6 support in the enterprise. Technology assets have an estimated three to five year lifespan, where after the business may choose to maximize the value of the asset by continuing to use it beyond the expected lifespan (Longbottom, 2012). As a result, some equipment, although deprecated, have continued to be used in the organization with the understanding that the asset will be replaced when it stops functioning or lacks new features that support the business processes. The practice of sweating assets introduces technical debt into the organization, that may cultivate an unfavourable business environment (Longbottom, 2012). As the legacy technology is refreshed by updated hardware and software, the support for IPv6 becomes available. This support has partially been based on the grounds of the Memorandum 05-22 from the US government. It incentivized the adoption of IPv6 in new technologies by vendors interested in winning lucrative government contracts (Evans, 2008). A perceived lack of IPv6 support does still exist, although it must be considered that it may be the result of a lack of information (or documented operational experience) available to network managers (Davies, Krishnan & Savola, 2007, sec.4.1).

Internet Service Providers' adoption are also lacking due to the perceived deficiency of IPv6 requirements in the context of business and its consumers. There has been growth in the industry, especially in the mobile service provider space, where companies like T-Mobile have started deploying new smartphones in an IPv6 only network and enabling IPv4 connectivity using a transition mechanism known as 464XLAT (T-Mobile, 2014). According to Gordon Greeff, Solutions Architect from Internet Solutions and Peter Hart-

[1] Cisco Certified Network Associate is a popular foundational network certification.

Davis from MWeb (two large South African Tier 1 ISPs), their respective backbones are IPv6 enabled, and capable of providing native support to clients (personal communication, August 28, 2014). The factors hampering the adoption of IPv6 in South Africa are therefore not technical, but rather a lack of sales and business drivers from their clients. This has prevented the deployment of IPv6 to the client edge.

The implementation of the IPv6 protocol by vendors has not been without ramifications to existing networks. Poor implementation of the supporting services has caused performance issues in IPv4 only environments. A poor implementation has been published by Yourtchenko and Wing (2012) from Cisco in Request for Comment (RFC) 6555. The work identified a problem whereby hosts that have a functioning IPv4 network and a non-functioning IPv6 stack can experience a significant delay in a connection that, in turn, degrades the user experience. Operating systems such as Microsoft Windows, Linux and Apple OS X have improved their implementation in recent years and presently provide support for the IPv6 protocol.

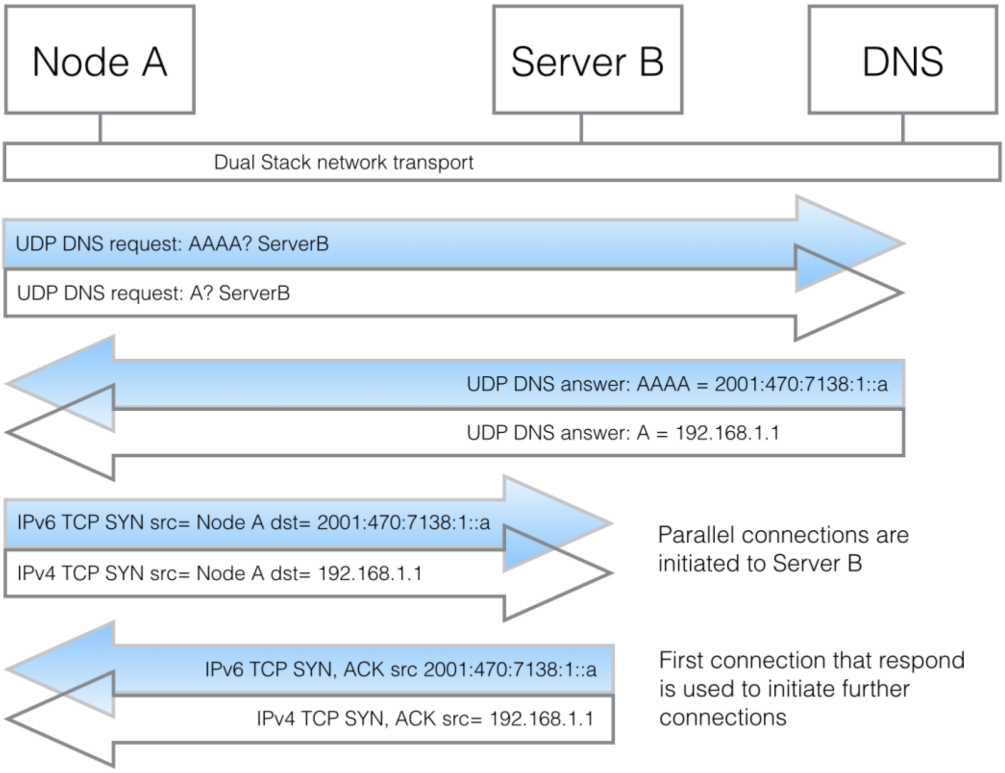

Node A
Server B
DNS
Dual Stack network transport
UDP DNS request: AAAA? ServerB
UDP DNS request: A? ServerB
UDP DNS answer: AAAA = 2001:470:7138:1::a
UDP DNS answer: A = 192.168.1.1
IPv6 TCP SYN src= Node A dst= 2001:470:7138:1::a
IPv4 TCP SYN src= Node A dst= 192.168.1.1
Parallel connections are initiated to Server B
IPv6 TCP SYN, ACK src 2001:470:7138:1::a
IPv4 TCP SYN, ACK src= 192.168.1.1
First connection that respond is used to initiate further connections

Figure 1. Implementation of Happy Eyeballs

The updated IPv6 implementation has improved the user experience and mitigated the reasons for disabling the IPv6 stack in the operating system. RFC 6555 and “Happy Eyeballs” when implemented will alleviate the problems with multi-protocol user experience (Degen, Holtzer, van der Kluit, Schotanus, van der Oije, Bartels, van

Ramesdonk, de Groot, Kollee, Keuper, Stols, Ottow, van der Bij, Mune & Spruyt, 2014) and ensures that a connection will utilise the connectivity that will provide the best network performance (as shown in Figure 1). This has been implemented on operating systems such as Apple Mac OS X Lion (version 10.7) in conjunction with the Safari web browser as well as operating system independent browsers such as Chrome and Firefox[2] (Huston, 2012) since 2012. It is noted that, based on the connectivity and protocol available that provides the best performance to the node, the traffic could follow widely divergent routes to connect to the destination service.

1.1 Introduction to the problem space

The Internet has been growing organically since its inception, with most of the growth occurring from 1994 to the present day (Odlyzko, 2001). The growth that has been induced by social, technical and economic adoption will be discussed in this section. The growth has been organic in nature, as the number of existing networked technologies has grown. As discussed in section 2.1.2, the event of ubiquitous computing and the adoption of new technologies that leverage the network will increase significantly.

As a consequence of the growth in the number of devices and people using the network, the existing address space in IPv4 has become an inhibitor to progress (Grossetete et al., 2008). Once the Internet number registries have exhausted their supply of IPv4 addresses, new requirements for the scarce resource will become costly and increasingly difficult to acquire.

1.2 Specific research questions

This research addresses selected risks associated with the implementation of IPv6 in the Enterprise’s supporting network infrastructure and how the implementation (or lack thereof) can impact Enterprise security. Through the identification and classification of security risks, certain mitigating controls are identified that can be deployed to provide a preventative and detective solution to the problem space.

Although the IPv6 protocol implementation and support has matured since the protocols definition in RFC 2460, the question is: are enterprise organisations ready to deploy and manage this technology securely? In the network environment, IPv4 has had years to

[2] On Firefox the “network.http.fast-fallback-to-IPv4” configuration parameter has to be enabled

mature and the controls that are available to the Enterprise to deploy are well documented and ratified. In contrast, the IPv6 environment is still in its infancy and consequently, there are risks associated to its implementation (Zulkiflee, Azirah, Haniza, Zakiah & Shahrin, 2011). Although the IPv6 protocol provides the network functionality in the same way as IPv4 did historically, the changes in the protocol introduced new ways of managing the local network segments through Neighbour Discovery Protocol (NDP) in contrast to the existing Address Resolution Protocol (ARP).

The risks that affect the deployment and the management of the protocol are identified. These impact the network from layer 1 to layer 7 of the Open Systems Interconnection (OSI) stack.

1.2.1 "Determine whether the average enterprise network access layer device can support and manage IPv6 equipment securely."

An enterprise network consists of numerous devices (as expanded upon in section 4.1) which are used to frame the research scope. This thesis will attempt to determine whether the devices of the average enterprise network access layer can support the IPv6 in a secure and manageable manner. Cisco devices are used to test and perform the case studies in Chapter 5.

Although the IPv6 Memorandum by the United States Government (mentioned in section 2.1.4) ensured that base support for IPv6 is present in vendor products. The question remains whether the selected network products have taken the changes in the IPv6 protocol into consideration.

1.2.2 "Should enterprise organisations adopt IPv6 in the near future?"

In conjunction with the question mentioned earlier, it is asked whether Enterprise should adopt the IPv6 protocol today and what controls and checks are necessary to ensure they take the risks into consideration throughout the process.

1.2.3 "Does current IPv6 implementations introduce an unacceptable risk into the Enterprise?"

Using all the case studies in Chapter 5 and the related research: are there options available to provide a secure network infrastructure to the Enterprise?

1.3 Scope of the research

The scope of this research document will focus on the Enterprise adoption of the IPv6 protocol and the effect that it, and the lack of it, will have on the risk posture of organisations. IPv6 deployment in enterprise organisations is still quite confined to companies such as Google that are pioneering global deployment of IPv6 in their engineering environments (Babiker, Nikolova & Chittimaneni, 2011). It was found that the major challenge was not the network technology stack, but more accurately, the people and vendor relations surrounding the environment, as well as the organisational buy-in that is required to affect the necessary changes.

The research identifies and catalogues the vulnerabilities that will impact an organisation's risk posture through IPv6 deployment. Through a selection process that takes impact and remediation into consideration, we will present four case studies in Chapter 5 that highlights the risks for the enterprise.

1.4 Document structure

Chapter 2 provides a review of the IPv6 protocol in a global setting. By documenting the changes introduced and the impact thereof on the network, the challenges that face IPv6 are brought to the fore. The structure of the protocol is described, followed by an explanation of the way that ICMP in IPv6 has changed from ARP in IPv4. The three deployment methodologies that provide the basis for the case studies are discussed in **Chapter 5**.

Chapter 3 expands upon the discussion in **Chapter 2.** Here security related research done by academics and security researchers in the IPv6 context is presented. The vulnerabilities that are identified are classified by the OSI stack: layers 2 and 3 and layers 5-7 are examined to identify the impact to the Enterprise.

The laboratory that is employed to facilitate the case studies and provide the infrastructure to the test environment is described in **Chapter 4**. Cisco and VMware are used in the laboratory which provides a review of the connected campus, otherwise known as the hierarchical network model.

The IPv6 case studies examined as part of this thesis are documented in **Chapter 5**. Resource attacks that have been prevalent in IPv4, the modifications to the IPv6 protocol, and the impact to resources are examined through the DHCPv6 protocol. We then review the traffic interception attacks in the IPv6 environment and show how IPv6 can be used to tunnel data out of a controlled environment if there is a lack of IPv6 specific controls. Finally, we discuss the distributed monitoring application that provides visibility to the IPv6 network and its function that serves to notify the network administrator of abnormalities by giving him a view of the environment.

The document concludes by reviewing the findings of the thesis and identifying the future work that can build upon this research.

Chapter 2

Literature Review

The IPv6 specification (Deering & Hinden, 1998) and the security that affects the Enterprise will form part of the literature review available on the adoption of IPv6 in enterprise networks. Security in IPv6 has, as a young science, little formal academic writing; therefore industry experts and the research they have produced in industry conferences provide a valuable source of content and information. The Internet Engineering Task Force (IETF) has also formed a major source of information through the informational and Standards Track of their request for comment library.

IPv6 has grown since it was devised in 1998, but still lies on the fringes of the mainstream Internet. This despite the fact that the Global Number Resource Organization's (NRO) IPv4 address space has been depleted since 2011 (Number Resource Organization, 2011). This poses the primary reason for the adoption of the IPv6 protocol in a mature IPv4 network environment. Although the protocols have similar characteristics and provide the same network layer function in the OSI stack, the increased header functionality allows IPv6 to be used in new and creative ways. The large network address space also provides the ability to be deployed and used in creative ways on the network layer which will have the ability to align to devices, appliances and information classifications (Skjesol, Sydskjør, Lillebrygfjeld & Bøe, 2013).

Protocol changes from IPv4 to IPv6 include a number of header fields that have a direct consequence to the way that the protocol is leveraged (discussed in Chapter 5**)** to introduce unexpected networking results. It follows then, that a base understanding of the new fields and the changes in the handling of the packets are documented in section 2.1.

Other than the change in the packet header, there have been significant changes in the way that network controls have been deployed. These include the change from ARP to the Internet Control Message Protocol v6 (ICMPv6) based NDP protocol. ICMP protocol is used to provide control to IPv6 and is used by identifying fragmentation information to allocate and detect an address space in the locally connected network subnets.

The difference in the base transport of the two protocols has further effects. An example is illustrated by the changes required to prevent misuse of the protocols (as described in section 2.5). In IPv4 networks, ICMP was generally dropped in favour of security and therefore a change in the controls that manage the ICMPv6 protocol is required in order to ensure that end-to-end connectivity is available to the required packet flows.

In section 2.6 the address configuration is discussed and the integration with the ICMP protocol is clarified. IPv6 nodes have the potential to configure numerous IPv6 addresses to each interface, providing different functions and allows for local and global connectivity. The different address types are identified and context is provided to their uses as well as the various auto-configuration methodologies.

Although there are many different IPv6 deployment methodologies, we focus on three high level deployment methodologies that provide the Enterprise with the most flexibility and support. Dual stack permits the phased migration of legacy applications and network infrastructure, but increases the management overhead as well as the complexity in the environment. Tunnelling also provides a certain amount of flexibility in the deployment of IPv6 but introduces certain challenges around control and the inspection of traffic on the Enterprise's edge. In certain enterprise networks, a native deployment, as unintuitive as it seems, may be a strong contender if the enterprise application stack supports the IPv6 network layer.

2.1 Introduction to the problem space

In conjunction to the factors mentioned in 1.1 that are driving IPv6 adoption, the US government also released a memorandum in 2005 that spurred the adoption of the IPv6 protocol in technology vendors (Grossetete et al., 2008). This provided a financial incentive for product vendors to implement the protocol and justified the business case for development of IPv6 functionality. The following sections describe the various influences to the networking ecosystem and the factors that are advocating the adoption of IPv6 in the Enterprise.

The Internet is growing and affecting the global economies. Internet adoption statistics show a correlation to the Gross Domestic Product (GDP) of these countries (Kende, 2014). This provides governments with the necessary motivation to provide a decent network infrastructure to their constituents. As a result, we can see an increase in the address requirements in the networking protocol.

2.1.1 The Growth of the Internet

In 1981, the original IPv4 protocol specification was published. The protocol provided end-to-end communications between 4.3 billion (2^{32}) interconnected devices, which at the time, was deemed to be a sufficiently large number by the research team (Postel, 1981). The 33-year growth of this computing network as a global, social, economic, legal and academic enabler led to a phenomenal acceptance and everyday use of the technology which was unforeseen by the original inventors (Grossetete et al., 2008). To put the current challenges in perspective: the global population has ballooned from 4.5 billion, with an adoption of around 213 hosts in 1981, to 7.2 billion people with an estimated adoption of 2.9 billion active Internet users in May 2014 (Kende, 2014). At the current growth the projected, the Internet population will increase to more than three billion users in 2015. This is significant even in the unlikely scenario where each user only has one address. In conjunction to growth in world population and the Internet adoption, the occurance of Smart mobile devices and ubiquitous computing, also known as the Internet of Things (IoT), has changed the dynamics of the Internet and introduced a trend through which users may utilize numerous devices that connect and share information via the Internet (Friedewald & Raabe, 2011).

In anticipation of the exhaustion of the IPv4 address space, the Network Working Group lead by Stephen Deering, designed an updated specification for an IP version 6 protocol which would provided a substantially larger address space that would facilitate addressing of up to 340.3 undecillion (2^{128}) devices (Deering & Hinden, 1998).

The demand for larger address requirements stems from a number of macro trends that are shaping the future of Information and Communication Technologies. These macro trends include the explosion of data management; the reduction of power utilization in computing devices; the miniaturization of computing; and the adoption of microprocessors in common smart objects (which facilitate the autonomous and responsible behaviour of resources) whether it be for commercial or personal purposes (Friess, 2011). Part of the justification for establishing the Internet of Things includes the development of standards as well as the formulation of a common network bus for communication that will allow ease of discovery, access and use of disparate systems. This reinforces the need and value of end-to-end addressable communication (Jara, Varakliotis, Skarmeta & Kirstein, 2013)

2.1.2 The arrival of mobile and ubiquitous computing

With the arrival of modern cellular phones, the interconnected device count has increased significantly, as a 2013 study from Pew Internet found (Smith, 2013). These devices promote the need for perpetual Internet connectivity to enable IP based online services. Uninterrupted, stable connectivity has changed the dynamics of the cellular industry: where phones in the past only required temporary connectivity to facilitate an outbound connection. The arrival of “smart” functionality, now requires perpetual connected networking to enable service and data transfer to the phone (Zheng & Ni, 2006). In 2013 it was found that 91% of Americans[3] own a cellular phone and that 63% of those users use their phones to connect to the Internet. This equates to 57% of the American population that use the Internet through their mobile phones. Furthermore, 21% of these users indicated that the cellular Internet is their primary method of Internet access (Smith, 2013).

Using the data presented by Smith (2013) the following can be deduced. In Africa the percentage of user Internet penetration is approximately 15.6% of the population which is less than the Americas that have 56.1% (All About Market Research, 2014b).

The following provides the number of users that are currently not using the Internet and therefore anticipates the potential growth.

$Potential\ Growth$ = Est. $Population\ of\ Continent$ x (1-$Current\ penetration\ percentage$ / 100)

[3] Americas include North America, South America, Central America and the Caribbean

The African continent has an estimated population of ≈1,125,721,038 (All About Market Research, 2014a); therefore the potential African growth is:

$$P^{(g)} \approx 1{,}125{,}721{,}038 \times (1 - 15.7 \div 100) \approx 948{,}982{,}835$$

Assuming that each connecting user requires a single IP address, the IP requirements for a connected society would be ≈ 948,982,835 additional addresses - a number that excludes the infrastructure network that requires address space to operate the transit and infrastructure service for the providers.

This illustrates the potential demand for IP infrastructure that will be realized through a mature economy in Africa.

This potential growth based on the extremely conservative premise of a single IP per person in Africa, with no adjustment for population growth, will therefor utilise more than a ≈22.095% stake of the entire IPv4 address pool.

$$\frac{948{,}982{,}835}{2^{32}} \times 100 \approx 22.095\%$$

This demonstrates how, in effect, the existing IPv4 protocol is inadequate to facilitate the growth for Africa, let alone the global population and the expected growth in the coming years (Grossetete et al., 2008). The use and implementation of mobile Internet is not only restricted to the cellular communications market but also includes Notebook derivatives, tablet devices, wearable computing devices such as smart watches and even industrial technologies and appliances that all require interconnection and form part of the Internet of Things (Jara, Ladid, Skarmeta, Comsoc & Etc, 2009). The increase of the above - mentioned devices is higher than the traditional computing market, with Android device registrations reaching new heights: more than 1.5 million device activations daily. Google’s Eric Schmidt stated in July 2013 that more than one billion devices were reported as activated globally in September of the same year (Chris, 2013).

The Internet of Things is developing past these standard definitions of mobile devices, forming part of ubiquitous computing – a concept originally conceived by Xerox PARC Chief Scientist Mark Weiser (Weiser, 1991) – which pervades everyday objects, from industrial to commercial reflecting concepts such as “pervasive computing”, “ambient intelligence” and the aforementioned “Internet of Things” (Jara et al., 2009; Friedewald & Raabe, 2011). Ubiquitous computing includes countless small and very small, wireless intercommunicating microprocessors (Friedewald & Raabe, 2011) which include devices such as e-Tags implemented in South African Gauteng Toll systems and Radio-frequency identification (RFID) chips. As the technology expands, the connectivity requirements to support the technology will need to adopt IPv6 to facilitate the interconnected nature of the large number of computing, monitoring and service devices. To facilitate these devices and improve end-to-end communication, concepts and implementation, enterprises will need to review technologies such as legacy network address translation (NAT) and port address translation. Through the assessment of communication mediums and the supported migration paths, IPv6 can be positively leveraged. As the growth of the devices and requirements for IP addressing expands, the world faces the exhaustion of IPv4 address pools.

2.1.3 Exhaustion of IPv4 address pools

The allocation of IP address space has been managed by the Internet Assigned Numbers Authority (IANA) (Bradner & Paxson, 2000) through the regional distribution by the Regional Internet Registries (RIR) (Number Resource Organization, 2014). The RIRs were established to facilitate the distribution of the locally assigned IP address pools to their designated countries globally.

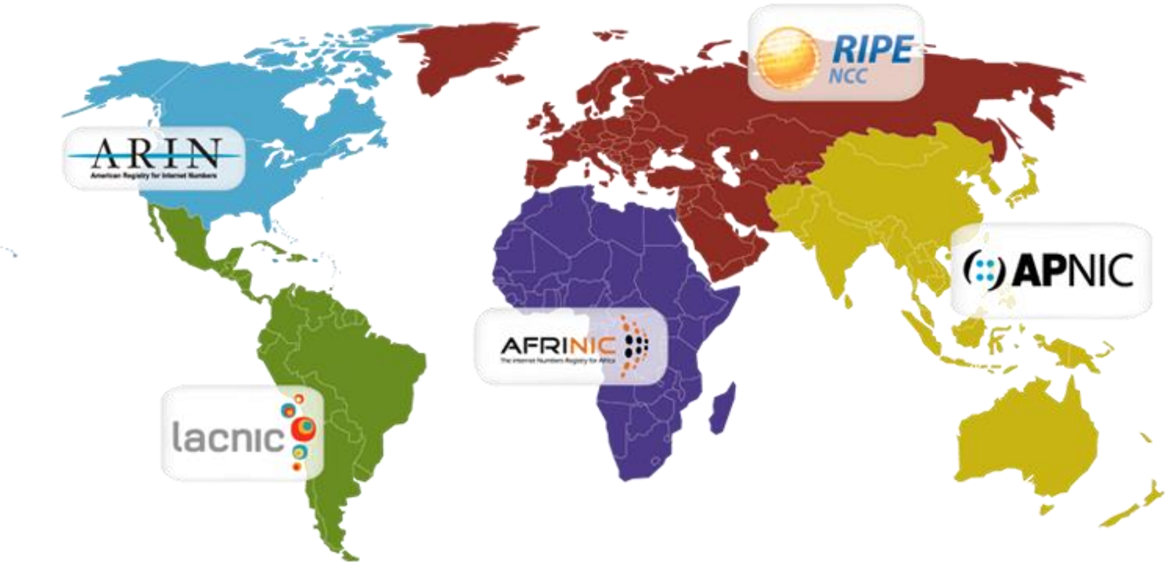

RIPE
NCC
ARIN
American Registry for Internet Numbers
APNIC
AFRINIC
The Internet Numbers Registry for Africa
lacnic

Figure 2. Regional Internet Registries (Number Resource Organization, 2014)

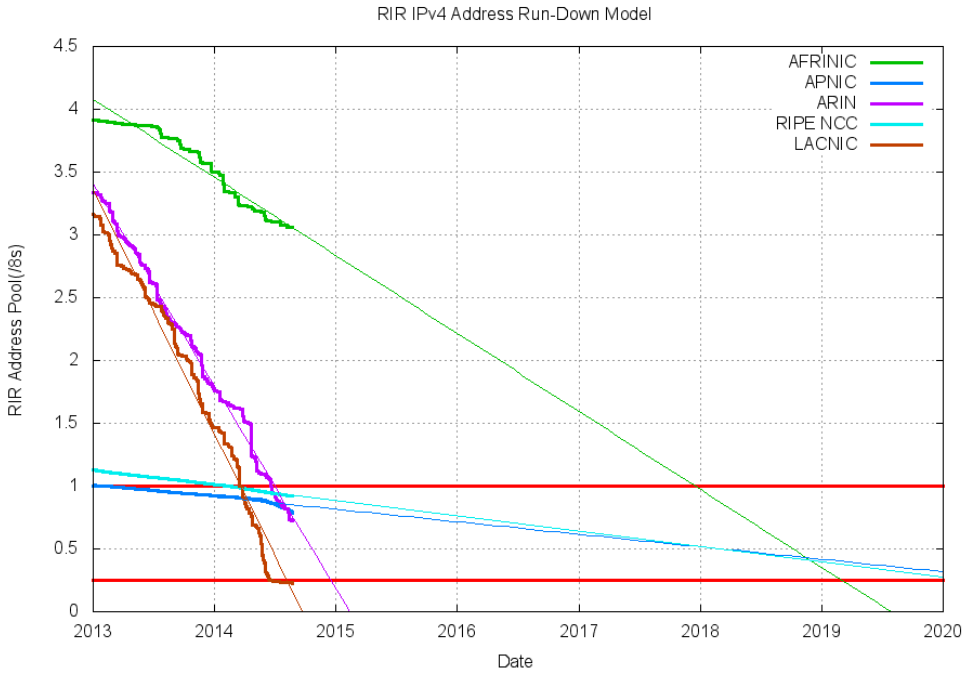
These five RIRs cover the geographically significant territories (as indicated by the map in Figure 2). Table 1 shows the five registries and their related regions and World Wide Web URLs.

As of 31 January 2011, the public IPv4 address space (that was managed by Internet Assigned Numbers Authority) was depleted as reported on 3 February 2011 by the Number Resource Organization (Number Resource Organization, 2011). The last five /8 (legacy Class A) address pools, compromising of 16.7 million unique addresses each, were divided and allocated to the five Regional Internet Registries (RIR).

Table 1: Regional Internet Registries

RIR	Region	URL
AFRINIC	Africa	https://www.afrinic.net
APNIC	Asia Pacific	https://www.apnic.net
ARIN	North American	https://www.arin.net
LACNIC	South American	https://www.lacnic.net
RIPE NCC	European / Russian	https://www.ripe.net

Tracking of IP addresses depletion by the RIR provides valuable predictive value to companies, organisations and the Internet at large.



(Normalized: 1 = 2^8 IP addresses)

Figure 3. RIR IPv4 Address Run-Down Model (Huston, 2014)

To undertake the issue of tracking IP address pools geographically, Geoff Huston developed a tool[4] (Huston, 2014) that graphs the five RIRs IP allocations and dynamically plots a Run-Down model which attempts to forecasts the depletion of the IPv4 public addresses from the respective RIR pools in a composite graph (as shown in Figure 3).

As the RIR's IPv4 address pools near depletion, they will implement mitigation processes to delay complete exhaustion. To preserve addresses, the RIRs typically reduce the prefix and delegation sizes allocated and increase the motivation required as the available pools are reduced (Nobile, 2012; RIPE NCC, 2014). The Asia Pacific Network Information Centre (APNIC) proposal, prop-088 (Bush & Smith, 2010), released in November 2010 and the Réseaux IP Européens (RIPE) proposal, ripe-606 (RIPE, 2014) released in February 2014, formalized their respective processes for handling any IPv4 space once the final Class A (/8) network distribution starts.

2.1.4 The United States Government as a driving force

On 2 August 2005 the United States government released Memorandum 05-22 by the Office of Management and Budget that required the implementation of IPv6 in their governmental network backbone by June 2008 (Evans, 2008). The scope of this memorandum included the bulk of the government networks, such as the OneNet and Global Information Grid (GIG). The memorandum sought to ensured that the IPv6 protocol would be in use by June 2008 in the network backbone of the various government organisations, which, as stated in (Choudhary & Sekelsky, 2010), encompasses the following types of networks:

1. Local area network
2. International partners' networks
3. Wired and wireless networks
4. Satellite communications (SATCOM)
5. Tactical operations networks such as those deployed in a battle- field or an emergency response operation.

Although the implementation of IPv6 was not achieved by 2008, the various product roadmaps were updated to ensure that network-enabled equipment and services require

[4] Geoff Huston's IPv4 Address Report, http://www.potaroo.net/tools/ipv4/

IPv6 support (Grossetete et al., 2008). This ensured the acceleration of IPv6 support and compliance by vendors who endeavoured to provide lucrative equipment and services to the United States government.

2.1.5 Economic driver to ensure Internet growth

The Internet is part of the strategic and economic growth of companies and countries throughout the world. In mature economies, the Internet's industries contribution to their GDP growth has doubled to 21% in the past 5 years (Manyika & Roxburgh, 2011). The IPv4 address depletion will reduce the ability for companies and individuals to procure or loan publically accessible IPv4 addresses. This will have a direct (negative) impact to the future growth throughout the economy. In the context of developing economies this is particularly relevant. The Internet ecosystem's maturity directly correlates to a country's general standard of living as well as the ability to rapidly leap forward economically and facilitate further Internet-related growth (Manyika & Roxburgh, 2011).

2.2 Statement of the research problem

To facilitate this growth and to ensure continued communication with clients, employees and business partners, organisations are on the precipice of deploying the new IP protocol and supporting infrastructure into their environments (Grossetete et al., 2008). The implementation and deployment of new technologies into enterprise environment introduce risks that need to be identified so that their impact on business can be minimized and an equivalent security posture established.

2.3 IPv6 technology primer

The IPv6 specification was released by the IETF in December 1995 in RFC 1883 (Deering & Hinden, 1995). It highlighted the main differences from the existing IPv4 protocol to the new IPv6 protocol as expanded addressing capabilities; header format simplification; improved support for extensions and options; flow labelling capability; and authentication and privacy capabilities. The IPv6 specification was updated in RFC 2460 (Deering & Hinden, 1998) to the current standard in 1998.

2.3.1 Header format

In comparison to IPv6, the IPv4 packet header (as shown Figure 2) is a single header that can contain various amounts of data and protocol options, specified by the header length and added after the initial 20 bytes of the header.

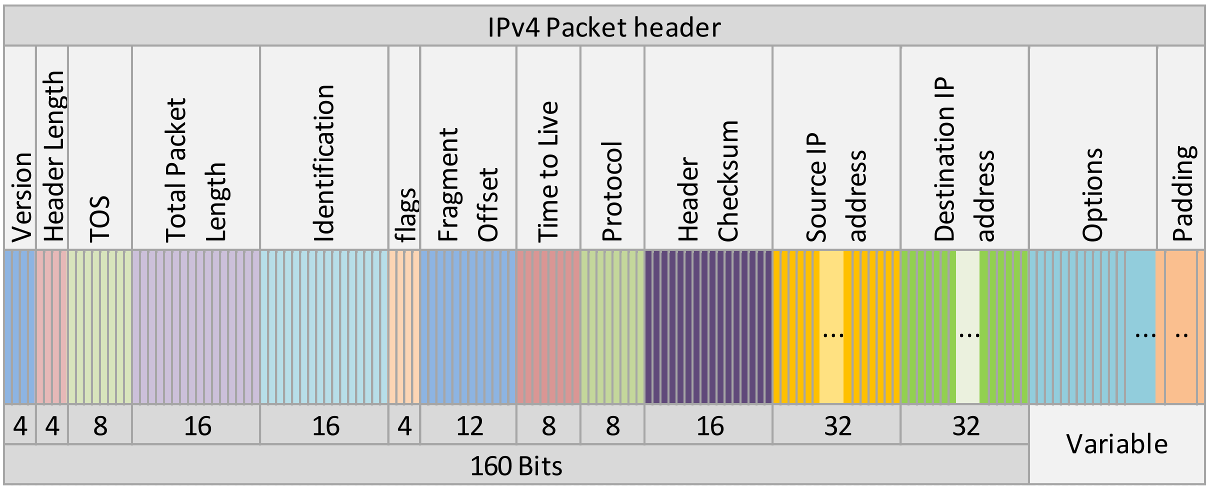


Figure 4. IPv4 header layout per RFC 791 (Postel, 1981)

In the IPv6 protocol the packet header complexity has been reduced and certain fields have been removed that are not specifically required in the base packet header of the protocol. To simplify the IPv6 header (shown in Figure 4) fields such as “Fragmentation offset” have not been included and the fragmentation information and functionality have been implemented through the use of a fragmentation extension header. The header length field and checksum fields have been removed as a result of the new fixed header length and to reduce the processing overhead of the header checksum update on each hop. The checksum for the packet data is implemented in the higher protocol layers, such as the Transmission Control Protocol (TCP).

These changes in the IPv6 header facilitate improved handling of the packet by routing devices as well as reducing the bandwidth overhead of the IPv6 header. The header architecture reduces the necessity to inspect and process all extension header along the network path by routing devices (Deering & Hinden, 1998; Blokzijl, 2009). The exception is the Hop-by-Hop Options header - which is required to be processed by each node along a packet's delivery path (Deering & Hinden, 1998).

The functionality of the IPv4 “time to live” field has been implemented by the “Hop limit” field, and remains functionally equivalent whereby the value contained in the field is decremented by each node that forwards the packet until it reaches zero and is then discarded (Encapsulated data is not modified during transit, so multiple hops could be seen as a single hop in a tunnel). In the situation where the packet is dropped, an alert to the source is initiated by means of an ICMPv6 Hop Limit exceeded message (Deering & Hinden, 1998). The “Protocol” field present in IPv4 has been replaced by the “Next header type" field that facilitates the implementation of extension headers (Durdağı & Buldu, 2010). All these changes simplify the IPv6 packet header structure, but increases the complexity in terms of the use of the various extension headers (Klein, 2012; Sheila, Graveman & Rooks, 2010).

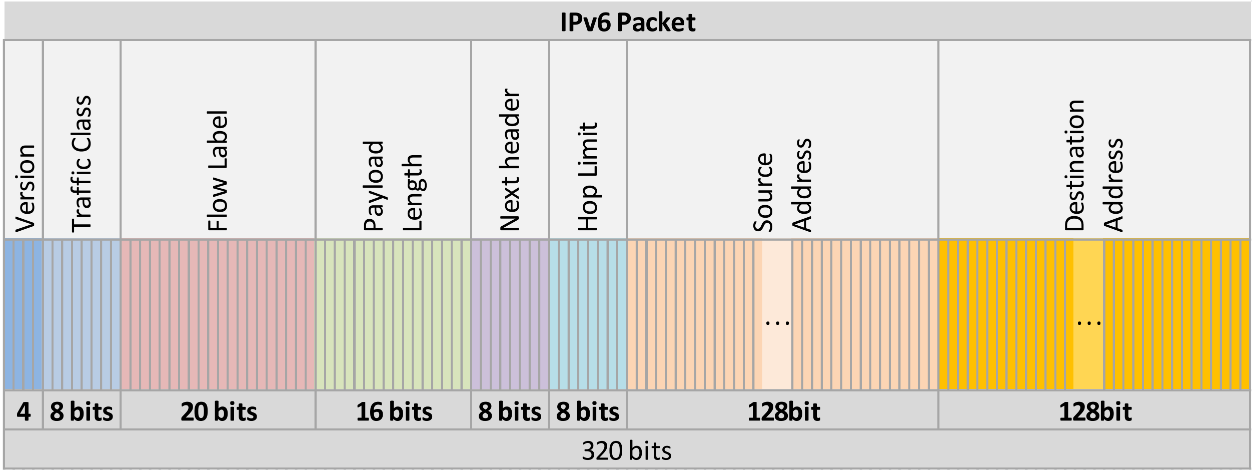


Figure 5. IPv6 header layout per RFC 2460 (Deering & Hinden, 1998)

There are various extension headers that are not usually processed by intermediary nodes in the network traffic flow, with the exception of the hop-by-hop options header. Some devices such as firewalls, load-balancers, intelligent routers and optimisation devices may need to process the various headers to allow for the ability to filter, balance or optimise the various complex traffic types. These intelligent devices will need to process the various subsequent headers in the IPv6 packet, which could be ordered and processed in different ways with difference potential conditions. The ability to change the header order or to chain the large numbers of header extensions may introduce issues in the standard operation of the protocol (Podermanski, 2011). Cisco, as part of a mandate by the United States federal civilian agencies[5], produced a report on their routing devices to document the latency and throughput of key Cisco Routing platforms. This IPv4 protocol performed better on the small packet sizes, although this was limited to the smaller software based switches (such as the Cisco 1841 ISR). The larger hardware platforms based on Application Specific Integrated Circuit (ASIC) technology did not show any throughput variance (Cisco Systems Inc, 2007).

[5] This included the Social Security Administration and the Department of Education, and the Joint Chiefs of Staff (Cisco Systems Inc, 2007).

The extension headers that was released with the full implementation of IPv6 in RFC2460 (Deering & Hinden, 1998) compromises the following:

- Hop-by-Hop Options
- Routing (Type 0)
- Fragment
- Destination Options
- Authentication
- Encapsulating Security Payload (ESP)

Figure 6 presents the order of extension headers that are suggested in RFC2460 section 4.1; however although suggested, the specification does not enforced the order in the protocol (Deering & Hinden, 1998).

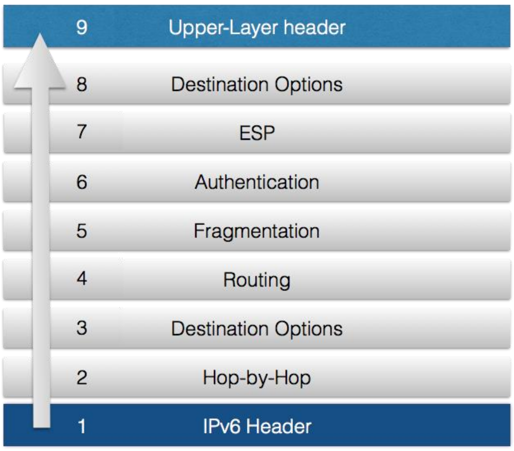


Figure 6. Suggested Extension header order - RFC2460

The IPv6 protocol specification does however state that nodes receiving the extension headers need to attempt to process the included header extensions regardless of their order.

Extension headers can be stacked in numerous ways, and even multiple times (as shown in Figure 6) the destination options header occurs more than once (but according to the RFC, at most twice).

The ambiguity in the use of extension headers introduces a lack of header control and has exposed the IPv6 protocol to new attack vectors that include new forms of fragmentation attacks (Atlasis, 2012; Atlasis, 2013; Gont, 2013).

2.3.2 Addressing

As discussed in section 2.1.1, the growth of the Internet was a prominent reason for the development of IPv6. To allow for the necessary growth, the IPv6 protocol's address space has been increased to 2^{128} individual addresses in comparison to the IPv4 standard that provided 2^{32} addresses (Deering & Hinden, 1998). This has increased the size of the networking environment and has changed the way that the address space is managed and assigned to the devices that are connected.

In IPv6, addressing has been divided into three types of addresses as shown in Table 2.

Table 2: IPv6 Address types from RFC4291

Address type	Description
Unicast	An identifier for a single interface. A packet sent to a unicast address is delivered to the interface identified by that address.
Anycast	An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the "nearest" one, according to the routing protocols' measure of distance).
Multicast	An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to a multicast address is delivered to all interfaces identified by that address.

Taken from (Hinden & Deering, 2006, sec.2)

There is no definition for broadcast addressing, as the address type has been removed to improve the efficiencies in the addressing mechanism (Hogg & Vyncke, 2009) and the functionality has been superseded by multicast addresses. Table 3 shows the common multicast addresses defined in RFC 3513.

Table 3: Commonly used Multicast addresses

Scope	Address	Description
Node Local Scope	FF01:0:0:0:0:0:0:1	All Nodes Address
Node Local Scope	FF01:0:0:0:0:0:0:2	All Routers Address
Link Local Scope	FF02:0:0:0:0:0:0:1	All Nodes Address
Link Local Scope	FF02:0:0:0:0:0:0:2	All Routers Address
Link Local Scope	FF02:0:0:0:0:1:FFXX:§X	Solicited-Node Address
Site Local Scope	FF05:0:0:0:0:0:0:2	All Routers Address

Taken from (Hinden & Deering, 2003, sec.2.7.1)

The length of the IPv6 address has been identified as a difficulty for humans to grasp, and therefore there are a number of ways that the address can be represented as shown in Table 4. Request for Comment 4291, section 2.2 describes the text representations of an IPv6 address.

Table 4: IPv6 address representation examples

IPv6 Address	Description
20010db8000000000000df80102263aa	Full IPv6 address
2001:db8:0:0:0:df80:1022:63aa	IPv6 Grouped notation
2001:db8::df80:1022:63aa	Consolidate consecutive 0s
0:0:0:0:0:0:192.168.0.1 or ::192.168.0.1	Mixed Mode

The hexadecimal address would present as follows if no separators where used to group sections.

```
20010db8000000000000df80102263aa
```

Grouping the address into groups of four hexadecimal numbers (16 bit groups) improves the readability of the address and we have the benefit of being able to remove leading 0s in the groups. This presents us with the following:

```
2001:db8:0:0:0:df80:1022:63aa
```

To further improve the presentation the groups of 0s can be compressed by the : ":" (colon) notation which can appear once within the address.

```
2001:db8::df80:1022:63aa
```

Mixed mode is also allowed whereby the IPv6 decimal notation is used for the low order 8-bit pieces of the address. The following is an example where 192.168.0.1 is used as the low order bits:

```
0:0:0:0:0:0:192.168.0.1 or ::192.168.0.1
```

In IPv6, the addresses space has been allocated into a number of subnets that represent the intended functionality. In Table 5, we have listed the IPv6 addresses that have been allocated from the 128-bit address space, and as shown, some of the address space has been deprecated.

The fec0::/10 site local address allocation has been deprecated in RFC 3879 (Huitema & Carpenter, 2004) as well as the 0000::/96 IPv4-Compatible allocation in RFC 4291 (Hinden & Deering, 2006, sec.4). Although the 0400::/7 address has numerous references to being allocated for the IPX transition, the author could not find any reference to the RFC that provided a basis for this allocation.

Table 5: Special purpose allocated IPv6 address

Prefix	Notes
0000::/3	Non interface based addresses
0000::/8	Reserved
0000::0/128	node local: unspecified address
0000::1/128	node local: localhost
0000::0000:0000:0000/96	obsolete: IPv4 compatible
0000::ffff:0000:0000/96	IPv4 mapped
0200::/7	NSAP
0400::/7	obsolete : IPX
2000::/3	aggregatable global
fc00::/8	unique local reserved
fd00::/8	unique local random /48 subnets
fe80:0000::/10	link local
fec0:0000::/10	obsolete: site local

2.4 Changes in ICMP and packet fragmentation

In IPv6 the use of the Internet Control Message Protocol (ICMP) has become a critical component of the protocol control. It performs neighbour discovery; stateless address autoconfiguration (Thomson & Narten, 1998); and Path Maximum Transmission Unit (MTU) Discovery (among others).

It was defined in RFC 2827 (Ferguson & Senie, 2000) that in IPv4, the control traffic represented by ICMP traffic was often dropped on the perimeter as best practice. The use not only limited flow control, but resulted in error-reporting, path MTU discovery and default gateway redirection (that was optional) and therefore introduced a negligible impact to the protocol's functionality. The IPv4 protocol provided routing devices with the ability to fragment IPv4 packets on the node level along the path of the traffic with the result that oversized packets could be repackaged and fragmented to fit the local MTU with no functional impact to the end-to-end communication. In IPv4, even though Path MTU Discovery functionality was implemented with RFC 1191 (Deering & Mogul, 1990), the lack of ICMP would not prevent the connectivity of IPv4 devices.

In IPv6, packet fragmentation has been delegated to the source node or device, and is no longer performed by the routers along the network path (Deering & Hinden, 1998, p.18). To facilitate Path MTU Discovery (PMTUD) that the source nodes will use to determine the maximum transmission unit, IPv6 requires end-to-end ICMP traffic to facilitate the Type 2, "Packet Too Big" message that a router may send back in the scenario where the packet is too large for the local MTU (Carter, 2011). This forms part of the re-iterative Path MTU Discovery process that continues until the packet is less than or equal to the actual PMTU and can therefore traverse the entire path.

The requirement for ICMPv6 throughout the network includes connections from untrusted external (Internet/3rd Party) networks. This requirement alters a fundamental best practice: to deny all untrusted network connectivity that is not specifically required for a service. The change in access to allow untrusted ICMP will introduce risk to one's network. Potentially, there could be DoS attacks based on ICMP flooding as well as spoofed "Packet Too Big" reactions which will impact the Path MTU Discovery negatively. The ICMPv6 message types that are required to facilitate IPv6 traffic to be passed from an external network to the internal network include the following as represented in the table below (Davies & Mohacsi, 2007; Hogg & Vyncke, 2009).

Table 6: ICMPv6 messages required through the perimeter

Description	ICMPv4 types	ICMPv6 types
Destination Unreachable	Not required	1
Packet Too Big – Path maximum transmission unit discovery		2
Time Exceeded		3
Parameter Problem		4
Echo Request and Echo Reply		128 and 129

According to Choudhary and Sekelsky, an attacker can burden the routers by flooding the device with maliciously crafted packets with the hop-by-hop option header, causing a flood of 'Parameter Problem' ICMPv6 error messages packets. This may potentially cause a denied or deteriorated service state to the sender (Choudhary & Sekelsky, 2010). ICMP crafted by attackers may also be sent to multicast addresses which offer an attacker the option to execute packet amplification attacks by spoofing an address and generating high packet count of return traffic which could result in a DoS (Hogg & Vyncke, 2009).

In lieu of the ICMPv6 functionality and dependency in IPv6 protocol, careful consideration is necessary to ensure that there is security on the perimeter and the internal network. Some of the techniques include discarding ICMPv6 packets with message types that are not required, as well as packets that are not valid in production network implementations as indicated in the following table (Hogg & Vyncke, 2009).

To reduce the impact of unnecessary and potentially malicious ICMP packets, the ICMP types in Table 7 should be filtered and not passed on the production network. In RFC4890 the ICMPv6 filtering policies have been defined (Davies & Mohacsi, 2007) and has been categorised into the following functional groups:

- Returning Error messages
- Connection Checking
- Discovery functions
- Reconfiguration Functions
- Mobile IPv6 Support
- Experimental Extensions

Table 7: Current IPv4 and IPv6 invalid ICMP message types

Description	ICMPv4 types	ICMPv6 types
Unallocated error messages	1-2, 7, 42-252	5–99; 102–126
Unallocated informational messages	N/A	155–199; 202–254
Experimental messages	20-29,41,253-254	100,101,200,201
Extension type numbers	N/A	127, 255
Depreciated	4, 15-18,39-39	

With the restriction of above functional groups, the impact and attack surface is significantly reduced and with logging. This can be leveraged to collect, identify and alert on indicators of compromise from maliciously crafted ICMP packets.

The increased attack surface, configuration complexity and requirement to define one's network requirements have made matters more complicated in contrast to version IPv4. The required functionality that is tied to these selected functional ICMPv6 messages will need to form part of the troubleshooting. Furthermore, the network device baseline access control will need to adapt to accommodate the functionality in the IPv6 stack.

An example of the use case for such ICMPv6 messages is Mobile IPv6. It requires ICMPv6 type 144-147 access for Home agent address discovery and a mobile prefix advertisement. This access is specified in Section 4.4 of RFC6275 (Perkins, Johnson & Arkko, 2011) and is required from networks that roaming mobile IPv6 users will be expected to connect. A deliberate access policy will need to be followed which dictates where Mobile access such as this will be permitted.

Although ICMP attacks does not impact integrity and confidentially directly, an attack to the availability of a platform can be modelled on the attack against the Estonian country and government which occurred in April 2007 (Geers, 2008).

2.5 Neighbour and router discovery

In IPv6 the ARP protocol is no longer used to facilitate Media Access Control (MAC) (layer 2) to network (layer 3) address resolution - that functionality is now provided by ICMPv6 and the IPv6 Neighbour Discovery Protocol (NDP) using the link-local addressing which has been implemented to facilitate layer 2 communication (Narten, Nordmark & Simpson, 1998).

The IPv6 NDP was first defined in RFC 2461 (Narten et al., 1998) and it listed security considerations that identified the Denial of Service (DoS) and potential for traffic interception by malicious nodes. The solution proposed by RFC 2461 was tightly linked to the mandatory IPsec implementation that was defined in RFC 1883 (Deering & Hinden, 1995) as part of the initial IPv6 specification. The proposal was to utilise the authentication header to validate the node. It would identify, authenticate and discard invalid NDP packets. The lack of adoption of the IP security (IPSec) and the realization that not all devices can support or require IPsec has changed the mandatory implementation to an option in RFC 6434. For this reason the solution is no longer valid.

The NDP RFC defines five ICMPv6 packet types that include Router Solicitation (133); Router Advertising (134); Neighbour Solicitation (135); Neigbour Advertisement (136); and Redirect (137). NDP includes two aspects to the protocol: firstly, the Router advertisement and solicitations that are used for the host configuration of the local networks and secondly, the related routers. The Node advertisement and solicitation as well as Duplicate Address Detection (DAD) is also used to confirm a link-local address and the other IPv6 addresses configured on the interface. Concurrently it performs a process to validate the IP address and to confirm that the address generated is not already in use.

Information can be passed to the routers and hosts on the locally connected network. It is used to provide configuration information such as MAC address information, Domain Name Service (DNS) information and address prefixes. In conjunction to the aforementioned, the protocol also provides for router redirection on a locally connected subnet (Narten et al., 1998).

2.6 Address configuration

The IPv6 address numbering consists of the following potential addresses that may all be present on a device interface:

- Link-local address (LLA) – RFC4291 (Hinden & Deering, 2006)
- Unique-local address (ULA) - RFC4193 (Hinden & Haberman, 2005)
- Global Unicast address (GUA) – RFC4291 (Hinden & Deering, 2006)
- Cryptographically Generated addresses (CGA) RFC3972 (Aura, 2005)

The various IPv6 address types are implemented for specific functionality, for example the Link-local address which facilitates the Neighbour discovery that replaced the ARP functionality and the Unique Local addressing that is used for much the same purpose as the RFC1918 (Rekhter, Moskowitz, Karrenberg, de Groot & Lear, 1996) private address ranges. The LLA is only significant locally in a layer 2 network domain and does not facilitate connectivity between multiple layer 3 domains. Broadcast traffic on the network has been replaced by link-local scope multicast, thereby reducing the amount of broadcast flooding (Biondi, 2007).

Owing to the changes from IPv4 to IPv6 DHCP, the IPv6 address pool management strategy will need to take a new direction. Currently in DHCPv6 there is no provision for a default gateway configuration field. This means that the network gateway configuration is still locally managed by the router advertisement on the layer 2 segment (Jinmei, 2007).

An IPv6 address auto-configuration mechanism has been developed in order to provide either *stateful* or *stateless* configuration methodologies or processes. The latter, *stateless* auto-configuration, allows the host device to generate its own IPv6 address based on a combination of locally available information advertised by the router and a locally significant interface identifier such as the device MAC address for Modified EUI-64 (Jinmei, 2007). In contrast, *stateful* configuration with DHCPv6 provides managed configuration with a host of configuration options that may include an address and other information, which may be carried by DHCP option values as described in RFC3315 (Droms, Bounds, Volz, Lemon, Perkins & Carney, 2003).

Unlike IPv4, where devices under normal situations only configure a single address, IPv6 configures a number of interface addresses based on the auto - configuration methods provided by the Router advertisement. Interfaces which have IPv6 enabled will always have a Link-Local address configured, which by combining the fe80::/64 prefix with a locally derived machine identifier.

Table 8: IPv6 autoconfiguration options

Address Autoconfiguration Method	ICMPv6 RA (Type 134) Flags		ICMPv6 RA (Type 134) ICMPv6 Option Prefix Info		Prefix Derived from	Interface ID Derived from	Other configuration options DNS, time, tftp, etc	Number of IPv6 Addresses on interface
	M Flag	O Flag	A Flag	L Flag				
Link-Local (always configured)	N/A	N/A	N/A	N/A	Internal (fe80::/64)	M-EUI-64 or Privacy	Manual	1
Manual assigned	Off	Off	Off	Off	Manual	Manual	Manual	2 (LL, manual)
SLAAC	Off	Off	On	On	RA	M-EUI-64 or Privacy	Manual	3 (LL, IPv6, IPv6 temp)
Stateful (DHCPv6)	On	N/R	Off	On	DHCPv6	DHCPv6	DHCPv6	2 (LL, DHCPv6)
Stateless DHCPv6	Off	On	On	On	RA	M-EUI-64 or Privacy	DHCPv6	3 (LL, IPv6, IPv6 temp)
Combination Stateless & DHCPv6	On	N/R	On	On	RA and DHCPv6	M-EUI-64 or Privacy and DHCPv6	DHCPv6	4 (LL, IPv6, IPv6 temp, DHCPv6)

Taken from (Carrell, 2013)

The randomised temporary address is defined in RFC4941 (Narten, Draves & Krishnan, 2007). It provided the node with a temporary privacy preserving addressing that could not be tracked. The temporary address does introduce management complexity in enterprise deployment: the privacy provided to the node, reduces the ability of administrators to bind physical assets to their respective IP addresses.

In Table 8 Carrell (2013) documents the various IP address configurations in an IPv6 environment. The configuration options are identified in the ICMPv6 Router advertisement flags.

DHCPv6 provides managed address configuration and supplementary information to the router auto-configuration. The protocol is based on ICMPv6 and is able to supply additional information such as DNS, domain name, download servers and NTP servers to the client devices - as specified in RFC 3315 (Droms et al., 2003).

2.6.1 Link-local address

The node generates the Link-local address when an interface that has IPv6 capabilities is enabled. As described in RFC 4862 (Jinmei, 2007) in section 5.3, the interface address is formed by combining the FE80::0/10 Link-local prefix which is defined by Hinden and Deering (2006) and a modified IEEE EUI-64 identifier which has the inverted "u" bit. The EUI-64 process is well defined in Appendix A of RFC 4291 (Hinden & Deering, 2006, Appendix A) and illustrates how the MAC is used to populate 48bits of the identifier and the shim of hexadecimal numbers 0xFF and 0xFE are inserted before the 25th bit.

2.6.2 Unique-local address

The Unique-local address is best compared to the RFC1918 private addresses in IPv4 which are used in private environments and behind NAT perimeter devices. The address prefix fc00::/7 has been allocated to the address type and is not routed on the global IPv6 Internet.

This address space has been defined in RFC 4193 (Hinden & Haberman, 2005) for use in private sites and can span multiple sites where the traffic is privately routed, or tunnelled and does not travers the public boundary. The use case for NAT may still exist in certain enterprises, and for this reason, this address space can be used in conjunction with ratified frameworks for IPv4/IPv6 translation such as RFC 6411 (Baker, Li, Bao & Yin, 2011) and contentious[6] RFC 6296 (Wasserman & Baker, 2011) .

2.6.3 Global unicast address

The Global unicast address is the IPv6 space that is routed for normal use on the IPv6 Internet which consists of the 2001::/3 network. This is defined in RFC 4291 (Hinden & Deering, 2006) which rendered RFC 3513 obsolete.

2.6.4 Temporary/Privacy address

The Stateless Address Autoconfiguration (SLAAC) method of assigning addresses using a unique interface identifier i.e. the device's unique MAC address which is used in the Modified EUI-64 format, has been presented as a potential leak for personally identifiable information. According to Nour El-Kadri and Sowmyan Jegatheesan, privacy issues will complicate the use of IPv6 owing to the inclusion of a globally significant fixed identifier

[6] As described by Tom Hollingsworth in the Networking Nerd blog (Hollingsworth, 2011)

(Individually identifiable information) that can form a part of a node’s global IP address. By using the Identifiable information, Internet services will be able to track a device and therefore its user across various disparate networks, regardless of the network Prefix (Oliphant, 2011; El-kadri & Jegatheesan, 2013).

To prevent Individually identifiable information from being linked to the IPv6 address, RFC 4941 (Narten et al., 2007) was proposed in order to provide a temporary address that could be used from which to initiate connections. The temporary address is generated generated using a pseudo-random address suffix that is used in the SLAAC process to configure the interface. Although the pseudo-random address provides an abstracted address, it is important to refresh the interface and deprecated the previous address, which removes the value of tracking the address. As the addresses are refreshed, the open connections should still continue, and the newly generated address should be used for any new connections from the device.

2.6.5 Cryptographically generated address

The lack of attribution and repudiation in network traffic formed the base requirement for CGA as standardised in RFC 3972 (Aura, 2005). The address is generated as part of the SEcure Neighbour Discovery (SEND) protocol, described in RFC 3971 (Arkko, Kempf, Zill & Nikander, 2005).

Using the Secure Hashing Algorithm (SHA-1) one-way hash in conjunction with a public key (and other auxiliary information) the address is cryptographically generated. The SEND protocol has not been widely adopted as it requires a trusted central certificate authority, such as Microsoft CA and can be used in layer 2 attacks. This element will be discussed in section 3.1.

2.7 Network Address Translation

The inevitable depletion of the unique public IP address space has been facing the Internet since 1994, when Kjeld Egevang and Paul Francis released the first RFC (Egevang & Francis, 1994). It proposed the concept of network address translation to deal with the address depletion and to alleviate problems such as the scaling of the routing table on a global scale because of the limitations of technology. IP network address translation (NAT) was implemented as a short term solution, reducing the required IP addressed for provider stub networks and thereby reducing the growing routing table (Egevang &

Francis, 1994). There have been benefits and disadvantages associated to NAT implementations. The improved privacy it provided to interconnected networks that were obfuscated behind a NAT gateway was an advantage. The disadvantages of NAT are also a result of this obfuscation: the end-to-end significance of IP addresses were lost. In addition to the obfuscation, the network address translation added additional processing requirements to the perimeter and boundary network devices which performed the NAT. This required the additional management of the session, as well as the packet modification of the packets traversing the gateway or firewall (Hunt, 1997).

Some complex application protocols such as active File Transfer Protocol (FTP) requires that an independent return data connection be established; another example is the Streaming Control Transmission Protocol (SCTP) which includes host address information in the network packet data. Both FTP and SCTP requires an Application-layer Gateways (ALG) to assist in facilitating the modification of the network data payload to support the relevant applications. This limitation and complexity introduced in NAT is described in Section 8 of RFC2663 (Srisuresh & Holdrege, 1999). Once the packet is updated with the recalculated values, the NAT device needs to update the 32-bit Cyclic Redundancy Check (CRC32[7]) checksum in the packet header to ensure compliance with the protocol. In addition to the complexity in translation and state management, any multipath routing requires that the sessions and NAT states are kept in sync and are shared between the cooperating NAT devices, so that the manipulation of the IP packet header and payload will be similar between the devices. (Srisuresh & Egevang, 2001; Randall & Tüxen, 2007)

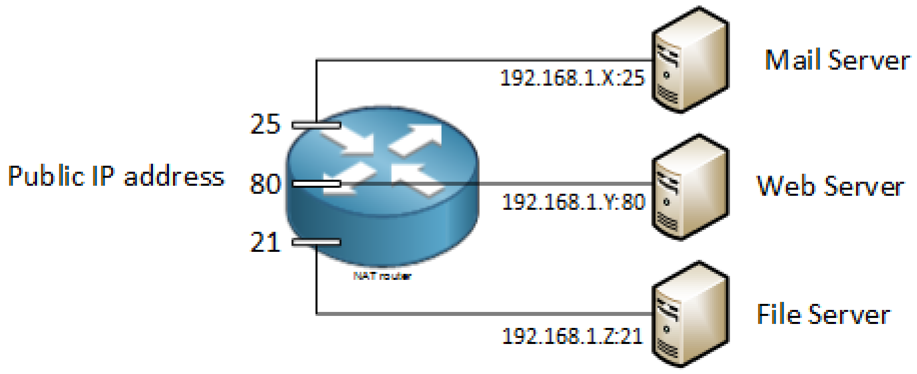


Figure 7. Example network Port Address Translations

[7] CRC32 is a lightweight 32-bit checksum that provides integrity validation of the header (Postel, 1981)

As IPv4 addresses became a scarce resource, a consolidation of hosting services were implemented by utilizing network Port Address Translation (NPAT) and service reflection to allow multiple applications and services through minimum consolidated IP addresses. This translation method (as shown in Figure 7) has the benefit of permitting numerous services through a limited IP address space, but as a result it also reduces the complexity and work effort that attackers need to expend to enumerate the services for an organization where a single Internet IP is known. Various services are presented and distributed from a single NPAT enabled IP address to the various service systems on a private network.

The private IP address space that is not routed on the public Internet was ratified by RFC 1918 (Rekhter et al., 1996) and it defines a number of subnets that can be used locally.

With IPv6 end-to-end connectivity restored, the application and protocol complexity in gateway devices will be reduced. That said, with the reduced privacy one needs to ensure that access control is strictly enforced in order to reduce the increased potential access provided by this form of connectivity. *Stateful* connectivity should be implemented in an IPv6 environment so one can ensure that inbound packets are only allowed when specifically permitted and that the return traffic from established sessions are passed.

2.8 Dual Stack deployment

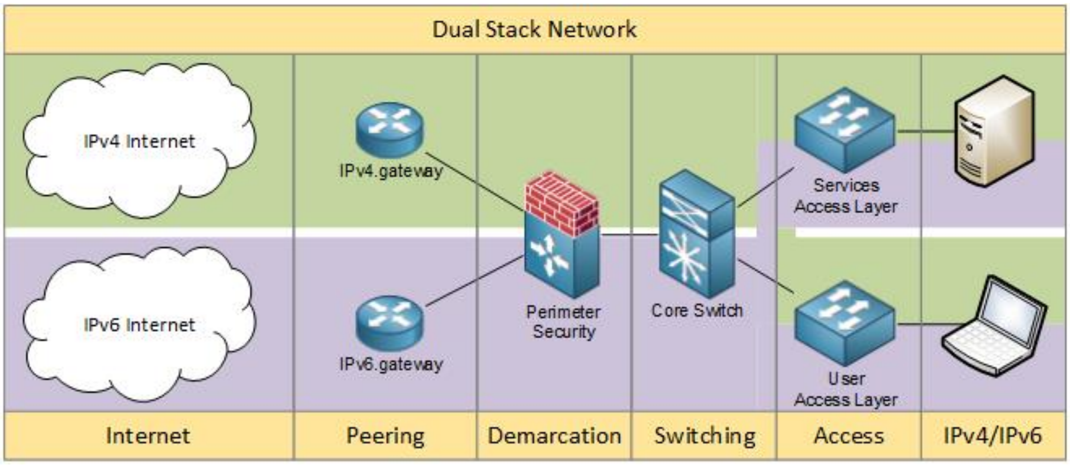


Figure 8. Dual Stack network

The IPv6 protocol can co-exist with other protocols on the same network platform, and as a result it provides a flexible deployment strategy for enterprise networks. This reduces the potential impact of a direct IPv4 to IPv6 migration strategy on business.

As shown in

Figure 8, dual stack facilitates a parallel IPv6 deployment throughout the existing IPv4 network - which can include the whole campus network, from perimeter to access layer. Many large enterprises such as Google have chosen dual stack as their IPv6 deployment strategy (Babiker et al., 2011). This decision has allowed them to provide IPv6 connectivity in a phased approach.

Facilitating connectivity through multiple network stacks is not a new phenomenon and has, in the past, facilitated the change in networking methodologies from protocols such as Internetwork Packet eXchange (IPX) to IPv4. Loshin (2004) notes the mechanisms whereby the IPX protocol was phased out by the Internet Protocol and how the multiprotocol architecture of the network permitted users on the network to browse the web and use email clients while still utilizing Netware IPX. This provided protocol flexibility to users even though the Novell delayed deployment of a native TCP/IP stack on their NetWare network operating system. The IP protocol functionality was available to users of the Netware products and it allowed Novell to add native support in 1998. This has proved that TCP/IP can integrate and co-exist with other network protocols in production environments (Loshin, 2004, sec.4.2.2). The multi-protocol architecture distinction is identified in the data link layer of the OSI model. The link layer header contains an ethertype value which specifies the protocol type and identifies the stack to which it should be passed (Loshin, 2004, sec.5.3). In the same way, the IPv6, which has an ethertype of 0x86DD, can co-exist with the IPv4, ethertype 0x0800, stack with little functional limitations (as shown in Figure 9).

Although this strategy adds complexity to the network, we can use the lessons learned through the protocol migration from IPX and apply it to the phased migration and co-existence from IPv4 to IPv6.

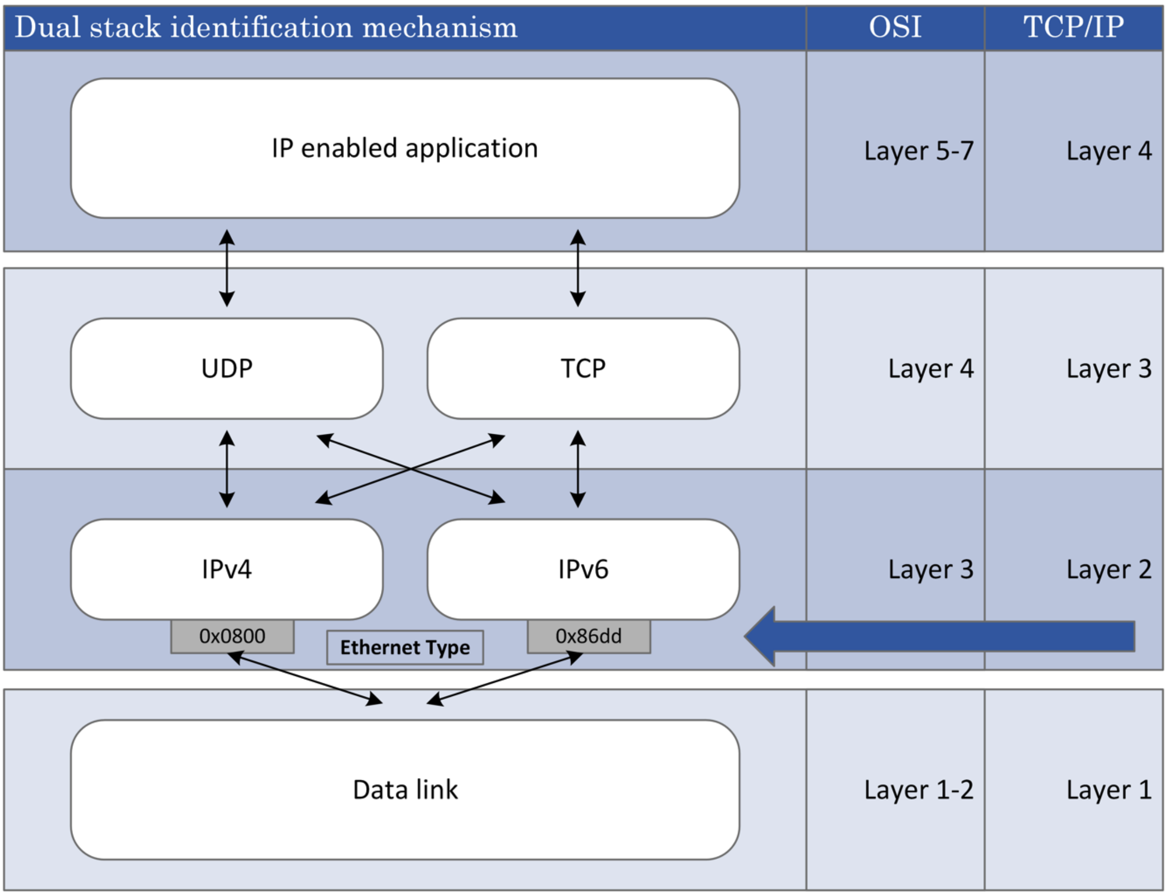


Figure 9. Dual stack identification mechanism

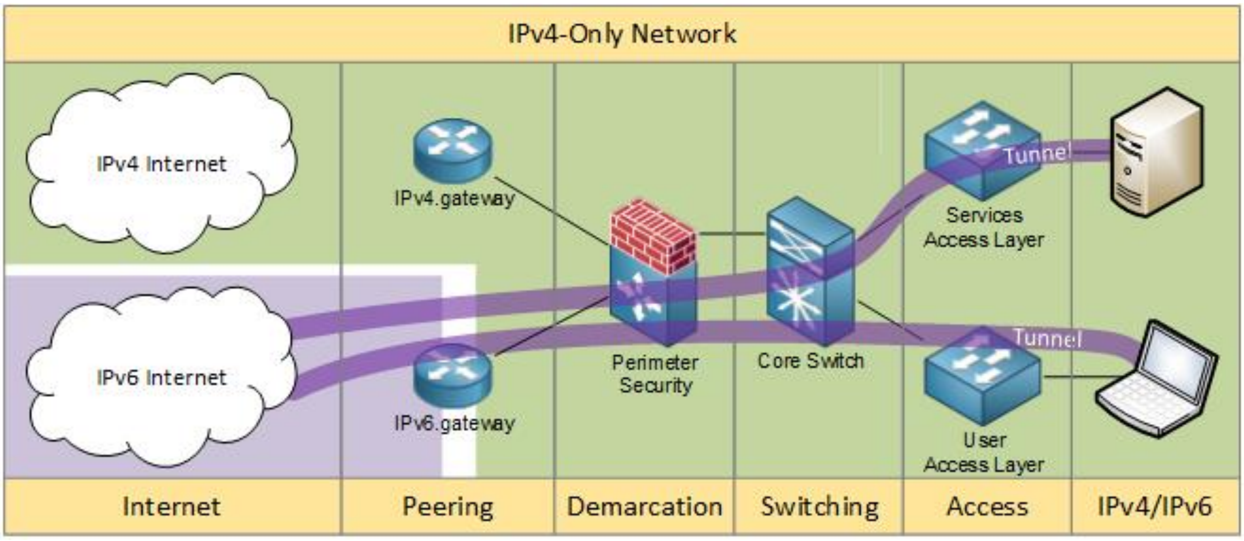


Figure 10. IPv6 Tunnel access

2.9 Tunneling

As an alternative to a native dual stack, network tunnelling can be used as an enabler for the dual stack LAN or Endpoint. Tunnelling is the mechanism whereby one network protocol is encapsulated in another network protocol (or application communication layer) to facilitate transparent transport. The tunnelled protocol is unaware of the tunnel transport and will therefore not increment the hop counter while in tunnel transit (Sheila et al., 2010). IPv6 tunnelling over IPv4 networks solves the problem when the existing infrastructure is not capable to support IPv6 dual stack and can be used as a phase of an IPv4/IPv6 transition strategy.

There are more than 16 standardised methods of encapsulating and tunnelling IPv6 traffic over an IPv4 network that partially consists of the standards in Table 9 (Tesar, 2012).

Some methods directly encapsulated the IPv6 header in a IPv4 packet and then use protocol number 41 to identify it as implemented in 6in4 tunnelling (Convery, 2004). Microsoft Windows operating systems can use a wide variety of dynamic tunnelling methods automatically i.e. Intra-Site Automatic Tunnel Addressing Protocol (ISATAP); Teredo; 6over4; and 6to4.

Table 9: Traffic encapsulation protocols and supporting standards

Associated RFC	Description	Reference
RFC 1933 **RFC 2893** **RFC 4213**	Configured and Automated tunnels	(Gilligan & Nordmark, 1996) (Gilligan & Nordmark, 2000) (Gilligan & Nordmark, 2005)
RFC 2401	IPsec tunnel	(Kent & Atkinson, 1998b)
RFC 2473	IPv6 generic packet tunnel	(Conta & Deering, 1998)
RFC 2529	6over4 tunnel	(Carpenter, 1999)
RFC 3056	6to4 tunnel	(Carpenter & Moore, 2001)
RFC 4214 **RFC 5214**	ISATAP	(Templin, Gleeson, Talwar & Thaler, 2005) (Templin, Gleeson & Thaler, 2008)
RFC 4380	Teredo	(Huitema, 2006)

Statically configured protocol encapsulation such as Generic Routing Encapsulation

(GRE), Secure Socket Layer (SSL) / Transport Layer Security (TLS), IPSec ESP or 6to4 is also used in the transport of IPv6 over an IPv4 network but does require manual configuration of the tunnel endpoint and the routing over the tunnel. The manual implementation of infrastructure tunnels enables IPv6 in environments in a controlled manner, providing a traffic control point that may be configured to align with the enterprise security policy.

The security controls (and the location of these controls) should be considered if protocol tunnels are permitted in the Enterprise. Traffic that is encapsulated in tunnels may pass unrestricted through IPv4 infrastructure controls at the perimeter as well as between segregated zones implemented between nodes in an organization. SSL/TLS and IPSec are examples of encrypted protocols that are problematic by design (Loshin, 2004, sec.6.3; Kent & Seo, 2005; Kent & Atkinson, 1998a), as no inspection capability currently exists to identify and control the tunnelled traffic during transit. Deep packet inspection and SSL/TLS inspection can potentially assist in the identification, but the certificate used to decrypt the traffic would need to be trusted by the tunnel members (Hogg & Vyncke, 2009).

2.10 Native IPv6 environment

In the current environment, the potential to run commercially viable IPv6 only environments are limited owing to the lack of consumers and services available natively. There are alternative methods to close the service gap between the IPv6 and IPv4, which would include: services such as applications proxies, which would facilitate application brokering for requests between the two disparate networks. Examples of such application proxies are Web proxy services and Socks64 application services, which enable the connection brokering between IPv4 or IPv6 and the other network stacks.

Web application proxy services allow connection from either IPv4 or IPv6 and will facilitate the connection to the web page regardless of the protocol - allowing an IPv6 client to request a resource from a website that may be on the IPv4 network. The connection from the client is manually directed at the proxy or may also be intercepted using transparent technologies. Once the proxy receives the request from the client, it will then act on behalf of the client and request the resource from the target server (Saini, 2011). Configuration of manual traffic redirection would include settings in the browser that would incorporate the configuration of an explicit proxy in the system and browser settings on the client. Alternatively, technologies like gateway traffic redirection on the network level are possible with firewalls and supported routers or with services such as the "Web Cache Control Protocol" (WCCP) in the network configuration. WCCP is also known as the "Web Cache Coordination Protocol" and the acronym, WCCP, is frequently used to avoid confusion (Cooper, Tomlinson & Melve, 2001). Google attempted to use WCCP technology in 2011 as a part of their transition process, but found that the software revision of their Cisco iOS devices available at the time did not permit IPv6 WCCP interception (Babiker et al., 2011). WCCP allows one to leverage the proxy benefits with little configuration impact to the client device.

SOCKS IPv4/IPv4 Gateway, which is based on the SOCKS standard, has been defined in RFC1928 (Leech, 1996) and provides a transport relay that is encapsulated in a standard IP packet, providing proxy services which allow "socksified" applications to transmit their connections through the socks service . In RFC3089 (Kitamura, 2001) the application of SOCKS as a IPv6/IPv4 gateway is described to enable a smooth heterogeneous communications between IPv6 and IPv4 nodes (though it may be implemented at the costs of a simplified environment). Even though this transport is enabled without the development or introduction of a new protocol, using only the existing SOCKS mechanism, as explained in Wang, Yeo & Ananda 2001, the implementation still breaks the end-to-end principle of the Internet and therefore is not a favoured solution. One can infer that the implementation of an encapsulated application layer transport such as this will inherit the same security issues that exist in tunnelled traffic.

2.11 Summary

The IPv6 protocol has introduced a change to the network stack that has been inert since the introduction of IPv4. Although the packet, the addressing and the semantics around the protocol management have changed, the TCP and UDP transport layer protocols are still available from an application perspective. This, in turn, will facilitate the use of the protocol in the same way in future: not specifically impacting the security of the organisation adopting the technology.

Vendors and their products are still, in many instances, immature based on their experience and the lack of client adoption in large networks. Consequently they will still experience some of the same challenges that IPv4 experienced. It can be stated that based on the growth of the Internet, organisations will need to adopt the protocol, and as a matter of course, the deployment methodologies will need to accommodate their risk and security requirements.

Chapter 3

Related IPv6 security research

The attack landscape of IPv6 is similar to other protocols such as IPv4 which consist of vectors that include Denial of Service (DoS); Evasion; Eavesdropping; and exploitation. The use of the IPv6 protocol on layer 2 and layer 3 has changed with the implementation of NDP over ARP on layer 2 and the way that routers and nodes handle layer 3 changes i.e. extension headers.

In Table 15, on p.66, a list of the twelve vulnerabilities that can be used to introduce unexpected behaviour on an IPv6 network are noted. The vulnerabilities were selected owing to the pervasive nature of the attack vectors posed by the common access layer to Enterprise.

The related research that is discussed in this chapter, frames the basis of the selection and the research that has formed the basis of the case studies in Chapter 5.

3.1 IPv6 Security on the Ethernet layer

The IPv6 protocol has fundamentally altered the way that the Link-layer is discovered (discussed in section 2.5). In IPv4, the ARP protocol used has been deprecated and replaced by ICMPv6 NDP, shown in Figure 12 (Narten et al., 1998). The IPv6 layer 2 attack surface has been documented, since the definition of the Neighbour Discovery for IPv6 in 1998 by RFC 2461. RFC 2461 states that there are attacks to the protocol that may cause IP packets to flow unexpectedly as well as attacks that may cause unexpected failure in the node configuration which may introduce a DoS state. This was updated by RFC 4861 in 2007 and the attack surface was reaffirmed through threat analysis and expanded to form three vulnerability categories (Simpson, 2007, sec.11.1):

- Denial-of-Service (DoS) attacks
- Address spoofing attacks
- Router spoofing attacks

The fact that certain operational changes have occurred may have an impact on enterprise security: for example the switch from ARP to NDP. This does change the attack implementation of man in the middle attacks on the same layer 2 network (van Heerden, Bester & Burke, 2013).

The protocol facilitated the discovery of host MAC addresses without broadcast traffic and changes this to a combination of multicast and limited scope multicast. The NDP is defined in RFC 2461 and defines the following message formats.

- Router Solicitation Message Format
- Router Advertisement Message Format
- Neighbour Solicitation Message Format
- Neighbour Advertisement Message Format
- Redirect Message Format

These messages are used in a number of processes that perform device address configuration. NDP facilitates processes such as address resolution, prefix discovery, Duplicate Address Detection, next-hop discovery, router discovery, configuration parameter discovery, and neighbour unreachable detection.

By removing the mandatory IPsec implementation in the IPv6 stack, IPv6 has effectively been left no more or less secure from a layer 2 perspective than IPv4 (Threat & Miller, 2004). The risk identified is expanded upon as part of the four case studies completed in Chapter 5. Chapter 5 will also identify the compensating controls in order to reduce the enterprise risk.

An additional security control implementation for the access layer is the SEcure Neighbour Discovery (SEND) which was proposed in RFC 3971 (Arkko et al., 2005): to implement an authorisation and delegation process and provide a process whereby a node can provide proof of address ownership. The SEND process' SHA-1 hash functions have been identified as a potential attack vector that reduces trust in the process (Kukec, Krishnan & Jiang, 2011). In IPv6 Security (Hogg & Vyncke, 2009, p.199) it is identified that the cryptographic process is susceptible to a DoS attack to the control plane due to the workload required to generate and process certificates.

As discussed by Jeremy Duncan (2012), the challenges that have presented itself in SEND is mainly the low rate of adoption. This is because Microsoft Windows and Apple Mac OS X do not offer default support for the SEND mechanism. The SEND mechanism is patented (US 2008/0307516 A1) which may introduce additional hesitation from vendors to adopt the technology.

Without SEND, or the underlying IPsec authorisation, this layer 2 attack vector is implemented in various open toolkits such as the THC-IPV6[8] and Evil-FOCA[9] which allow one to test and verify one's network and confirm the network susceptibility to an attack.

These attacks use the default high transport priority of IPv6 to redirect traffic through an IPv6 NAT64 gateway with a DNS64 implementation which facilitates the conversion of the requested DNS names (Hauser, 2005; Alonso, 2013). As shown by Hauser, even though IPv6 and IPv4 have numerous changes in the protocol, the security inherent is similar and that the basic methodologies employed to leverage vulnerabilities remain relatively the same. Similar methods of attack were possible in IPv4 when DHCP was used in environments through the exploitation of DHCP spoof responses. Using the SLAAC auto - configuration that we discuss in section 2.5, in an enterprise network environment additional ways of intercepting local traffic are possible without modifying the node's inherent IPv4 connectivity. We elaborate upon this research in section 5.3 where we explore three redirection methods which enable the interception and modification of normal traffic.

[8] The hacker choice IPv6 toolkit - https://www.thc.org/thc-ipv6/

[9] Evil-FOCA IPv4 and IPv6 penetration testing and auditing tool - http://www.informatica64.com/evilfoca/

As end point devices are currently still dealing with the relatively new implementation of the stack, numerous DoS states can be introduced with a few defensive controls available outside vendor specific implementations.

These attacks are also important to consider in production enterprise environments where an IPv6 implementation has been planned and the default nature of the stack has not been disabled. Without the implementation and control of IPv6 in one's environment, the network is susceptible to this form of attack owing to the high prevalence of nodes configured with default IPv6 stacks which automatically attempt IPv6 connectivity.

The following images depict the process where node F can influence and impact the operation of the NDP.

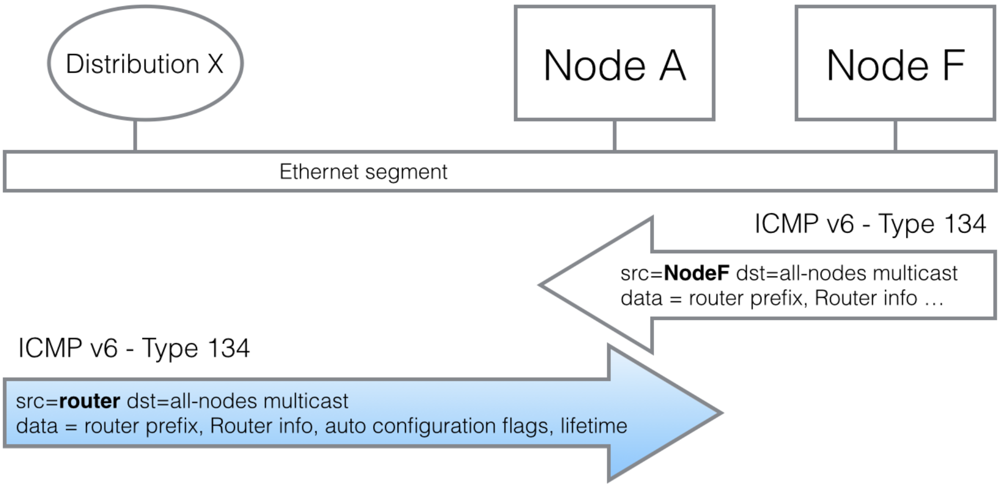

Distribution X
Node A
Node F
Ethernet segment
ICMP v6 - Type 134
src=**NodeF** dst=all-nodes multicast
data = router prefix, Router info …
ICMP v6 - Type 134
src=**router** dst=all-nodes multicast
data = router prefix, Router info, auto configuration flags, lifetime

Figure 11. Router advertisement

In Figure 11, Node A and Distribution X establish the routing information that Node A will use to connect to the provided networks, which may include a default gateway.

In this example Node F can advertise local routes and provide numerous routes to Node A. This has, in the past, caused a DoS states in Windows, Linux and other major operating systems because the number of routes that the host would learn from the advertisement would deplete the network resources.

Modern patches and operating systems have prevented this occurrence by limiting the number of routes that can be learnt from the router advertisements. This does not prevent a DoS that may be introduced by filling that route table, but it does protect the stability of the Operating System and prevent its failure.

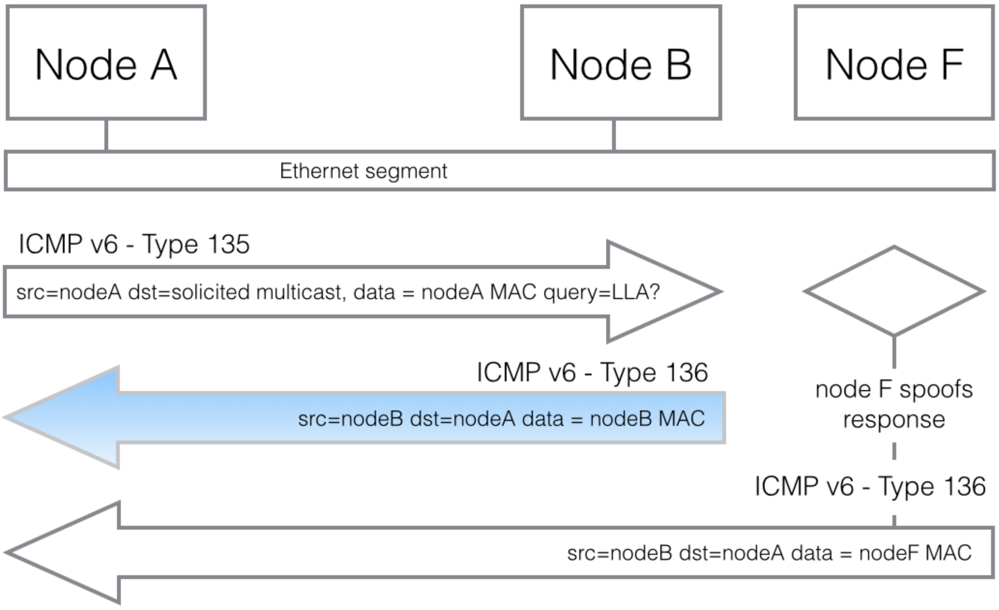

Node A
Node B
Node F
Ethernet segment
ICMP v6 - Type 135
src=nodeA dst=solicited multicast, data = nodeA MAC query=LLA?
ICMP v6 - Type 136
src=nodeB dst=nodeA data = nodeB MAC
node F spoofs response
ICMP v6 - Type 136
src=nodeB dst=nodeA data = nodeF MAC

Figure 12. NDP Link Layer Detection

In Figure 12 the Address Resolution Protocol (ARP) replacement is indicated (explained previously in section 2.5). This is the process whereby hosts use ICMPv6 and multicast to request other locally connected host MAC addresses. The figure also depicts how the process can be used by Node F to provide Node A with a spoofed ICMPv6 reply that injects an incorrect physical address (MAC).

This can be used by Node F to intercept traffic in the way that we describe in section 5.3 and it provides the node with an unavailable MAC address that will cause the host not to be able to connect to the destination node.

In Figure 13 the DAD process is illustrated. It provides nodes with the ability to confirm that there are no duplicate IPv6 devices on the local network which could prevent normal operations. In the example, Node A requests whether there are any other devices connected to the network with an IPv6 address it has generated. Node F then responds that is has the address, even though this is not the case. Node A recalculates the IP address to a new value and attempts the process again. In the case where Node F continues to respond to Node A’s requests, it will deny Node A network access and Node A will not be able to configure a usable IPv6 address.

The attacks described were also possible in IPv4 through ARP poisoning attacks (Harper, Harris, Ness, Eagle, Lenkey & Williams, 2011). It must be stated that, although the attacks were possible, the controls to prevent the exploitation of the ARP features were well defined and implemented in standard enterprise switching fabrics i.e. the Catalyst 2960.

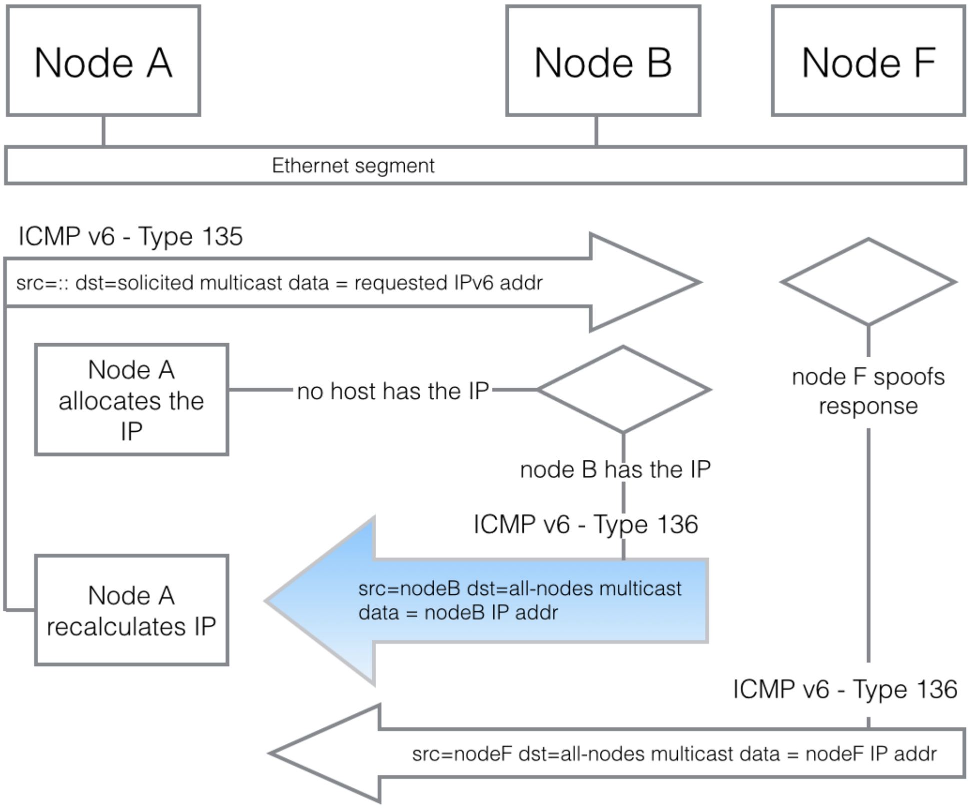


Figure 13. Node Duplicate address Detection (DAD)

They present through feature sets like `ip arp inspection` and `ip dhcp snooping` which provide dynamic ARP inspection (Cisco Systems Inc, 2010a) and association to the DHCP service. In IPv4, switches only needed to inspect ARP protocol requests and prevent that protocol from misbehaving, whereas the advent of the NDP (as part of the IPv6 ICMP protocol) increased the complexity in the inspection and prevention of attacks (Alonso, 2013; Ullrich, Krombholz, Hobel, Dabrowski & Weippl, 2014).

3.1.1 Mitigating risks in layer 2

Various network equipment vendors have developed mitigating and filtering controls. These are intended to prevent the malicious and unexpected use of the NDP in IPv6. These neighbor discovery protections on the Cisco IOS include Router advertisement guard and DHCPv6 guard and Security Bindings which attempts to prevent devices from introducing unmanaged routes and causing DoS states by the use of NDP.

Table 10: Cisco access layer IPv6 PACL support

IOS	Platform Name	Platform type
15.2	CAT2960C405	Catalyst
15.2	CAT2960C405EX	Catalyst
15.2	CAT2960S	Catalyst
15.2	CAT3560C405	Catalyst
15.2	CAT3560C405EX	Catalyst
15.2	CAT3560X	Catalyst
15.2	CAT3750X	Catalyst
15.2	CAT4500E-SUP6L-E	Catalyst Chassis
15.2	CAT4948-E-F	Catalyst Chassis
15.2	CAT4948E	Catalyst Chassis
15.2	CAT4900M	Catalyst Chassis
15.2	CAT4500E-SUP6E	Catalyst Chassis

The RA guard can be enabled to prevent the injection of rogue routes (to be discussed in section 5.3.1). The Cisco platform provided two methods: Router Guard and Port based access control which can be used to implement this as James Small (2013) demonstrated. The Router Guard functionality on the Cisco 3560 switch was found to prevent legitimate router advertisements and was therefore able to prevent a misconfigured router from flooding the network from a standard interface (Hogg & Vyncke, 2009). The RA guard functionality is however easily bypassed with packet manipulation (as discussed in section 4.4.3).

The alternative method of preventing the injection of unexpected neighbour advertisements is by applying ingress port filters. This is a more effective protection mechanism, but the support for this functionality is limited to the higher end devices as shown in Table 10. These protections are not always available for the access layer.

3.2 IPsec transport security in IPv6

The state of AH and ESP header affects the protocol security and has established an erroneous statement of inherent security in IPv6. The implementation of the IPsec protocol is very similar in IPv4 and IPv6, thought the position in the packet differs (this will be discussed further in this section). The authentication header facilitates integrity in the protocol with the ability to authenticate users and facilitates non-repudiation in the communications (Friedl, 2005). The AH functionality has previously been implemented in the payload of the IPv4 packet (Friedl, 2005), whereas the IPv6 protocol has included a header to implement the functionality. This includes the ability to prevent manipulation and tampering and also facilitates detection of such attempts. The AH header protocol can optionally include protection from replay attacks by using its sequence number field as a part of a sliding scale (Sotillo, 2006). The IPv6 protocol has mutable header fields that change during transit throughout the network. Therefore the authentication header protocol only implements integrity checking for immutable packet fields that do not change in transit. These mutable fields include the following header fields and are zeroed prior to the Integrity Check Value (ICV) calculation (Deering & Hinden, 1998):

- DSCP (6 bits, see RFC2474 (Nichols, Blake, Baker & Black, 1998))
- ECN (2 bits, see RFC3168 (Ramakrishnan, Floyd & Black, 2001))
- Flow Label
- Hop Limit

In Figure 14 the structure of the IPv6 Authentication header is shown to have a fixed header size and the sequence number field. This facilitates the optional mitigation of replay-attacks.

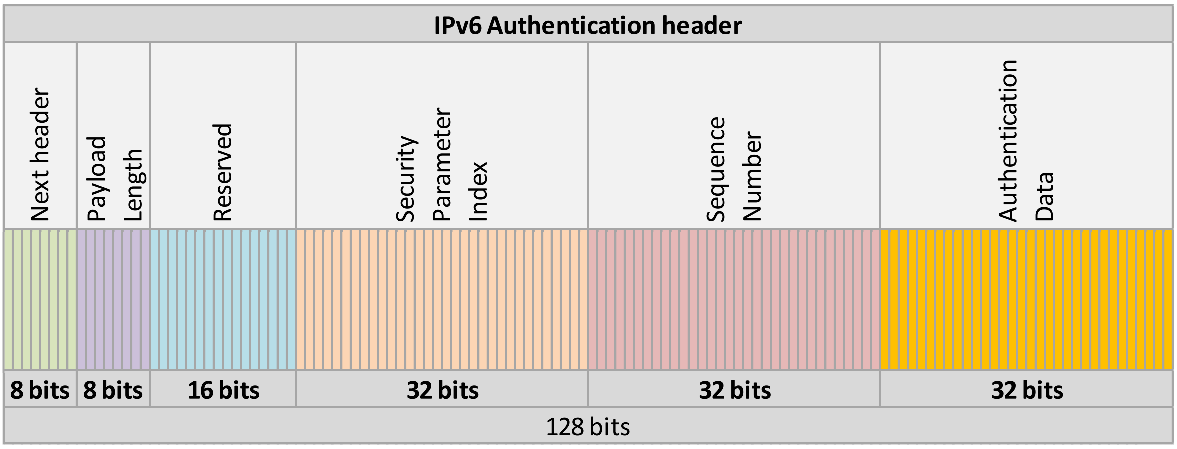


Figure 14. AH header specification

The ESP functionality can provide various security and integrity services to IP traffic, regardless whether it is IPv4 or IPv6. As stated in the standards document, RFC 4303 (Kent, 2005), “ESP can be used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and (limited) traffic flow confidentiality.” The usage and selection of the various options in ESP are chosen during the establishment phase of the security associations (SA) as well as the way that the device is connected to the network and the selected traffic flows.

Kent documented in the introduction of RFC 4302 (Kent, 2005, sec.1) that ESP can be used in isolation from AH, but this will only protect the encapsulated traffic flow from passive attacks as active attacks will be able to compromise the security of the ESP traffic through the use of identity enumeration techniques in the native exposed IPv6 header. Ken and Seo do however indicate in RFC4301 that although IPsec utilises both the AH and ESP headers to facilitate a secure connection, the use of AH is not mandated and that the functionality of ESP leaves a few contexts where ESP is not able to provide the requisite security services. ESP can be used to provide integrity without the confidentiality aspects which facilitate the same functionality as AH (Kent & Seo, 2005).

Figure 15 shows the layout of the ESP header. In IPv4 the ESP header was added between the IP protocol and the transport layer, but with the IPv6 implementation, the header is an extension of the IPv6 protocol.

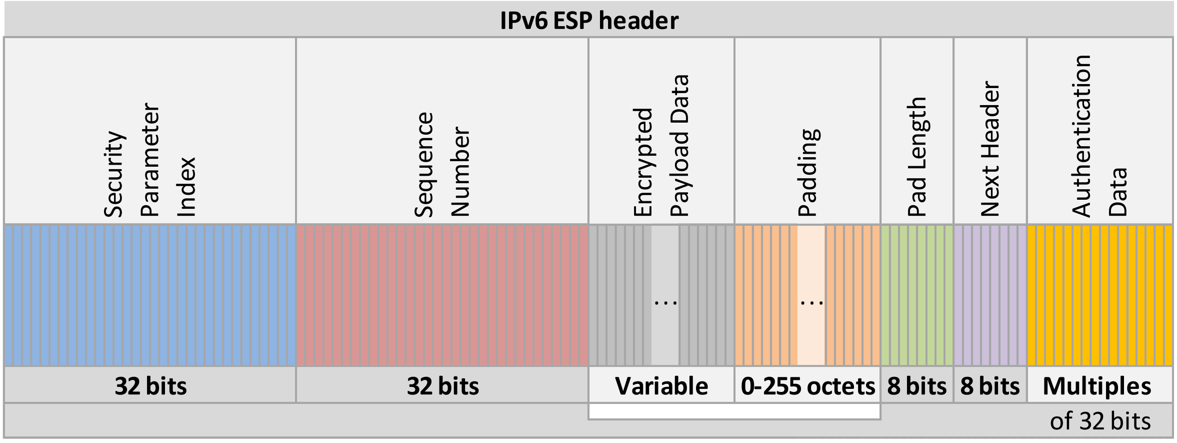


Figure 15. IPv6 ESP extension header

The assumption exists that IPv6 is more secure through the implementation of the mandatory native IPsec in the protocol stack. The mandatory implementation of IPsec may have been the original intention, but the implementation was downgraded by RFC 6434 (Jankiewicz, Loughney & Narten, 2011) in December 2011, changing the recommended support in RFC 4301 from MUST to SHOULD. The change in the recommended support was as a result of the recognition and the existence of a range of IPv6 capable devices which may use an alternative security approach to enable security or are simply too low powered to support a full IPsec stack.

3.3 IPv6 packet manipulation

Similar to IPv4, the IPv6 protocol is also susceptible to attacks to the transport of the packet beyond the layer 2 fabric. The complexity that has been introduced through the optional headers and the way that IPv6 is implemented has resulted in various vulnerabilities and an increased attack surface in the protocol. In 2008 more than forty-seven IPv6 vulnerabilities were identified. Many of them being silently remediated (Podermanski, 2011).

An example of the vulnerabilities introduced in IPv6 through the updated implementation of packet fragmentation has been discussed by Antonios Atlasis in subsequent years (Atlasis, 2012; Atlasis, 2013). It has been established that most hosts do not implement the packet fragmentation correctly and allow packets that are undersized (smaller than 1280 octets) and therefore in contradiction to RFC 2460 (Deering & Hinden, 1998). This opens up the protocol to be used in unexpected ways.

Packets that pass through IPv6 to IPv4 translation may receive return ICMP responses which indicate that the MTU is lower than 1280 octets. In that instance the node would include a Fragmentation Header for the IPv4 to IPv6 translating router which would obtain an identification value (Atlasis, 2013, p.38). According to RFC 6946 (Gont, 2013) the host that received a packet with a Fragmentation header that has a “Fragmentation offset” of 0 and the “m” flag’s value of 0, should process this packet in isolation of any other packets. Conforming to RFC 6946 the impact that a malicious packet can have on the host (and the flow of packets with which it is associated) is isolated.

In addition to the fragmentation attack, IPv6 has introduced the Hop-by-hop header that as per RFC 2460 (Deering & Hinden, 1998) needs to be processed by each node in the path of the packets’ flow. According to the standard, the hop-by-hop packet is placed first in the optional header order to improve the performance by which the devices can inspect the header.

The hop-by-hop extension header can also provide a covert channel which applications can use to transfer data outside the data area of the IP packet. This can be reproduced in the laboratory (defined in section 3.2) from Node A to the Service Node F through the use of

Scapy[10]. Scapy provides an interactive and programmatically flexible toolkit that provides the ability to build customized packets (forge packets) and decode received packets. This example is documented in example 2.1 by Hogg and Vyncke in *IPv6 Security* (2009, p.31). The IPv6 header needs to be processed by the control plane CPU and therefore does not benefit from the performance that ASIC technology provides in a new routing and switching platform. As a result, this can create a DoS state owing to resource consumption attack (van Heerden et al., 2013, sec.2.6.4).

3.4 IPv6 impact to applications and services

IPv6 protocol has the potential to impact the Application security of the networked environment and in the same way (as identified in section 3.1) the protocol does not provide improved security over IPv4. In the majority of attacks similar to the Structured Query Language (SQL) injection, IPv6 does not provide increased security which is as expected because the network security is bypassed by the application attacks (Cho & Pan, 2013).

A major benefit of the IPv6 address space is that it provides the increased deployment capacity. On the flip side, this may very well be the reason for the unexpected attacks on resources and infrastructure (Droms et al., 2003; Convery, 2004). DHCPv6 is an example of such a service which provides automatic configuration information to hosts, and is subsequently required to keep track of device to IP address mappings.

In IPv4 the address pool was restricted and the address space was recommended (under normal circumstances) to use less than 1024 addresses per broadcast domain. This recommendation was designed to limit the amount of broadcast traffic that would produce excessive network noise and prevent optimal device operations on the Ethernet broadcast domain. By reducing the number of hosts on the shared Ethernet domain, the reliability of the network was improved by reducing the size of broadcast domains (Spirgeon & Joann, 2014). In the IPv4 segments, resource exhaustion was restricted to the locally connected segment and did not negatively affect other segments interconnected through layer 3 on the network.

[10] Scapy was developed by Philippe Biondi and is available at http://www.secdev.org/projects/scapy/

By using Multicast to displace broadcast traffic, IPv6 has the ability to host more devices with less chatter, and the address space has been expanded to facilitate this. The LAN address space is large enough to provide SLAAC compatibility by providing a /64 network per segment.

In theory, this permits nearly 18,446,744,073,709,552,000 addresses in each segment, and it provides a different resource exhaustion attack vector. An example of this would be the way it permits a malicious host to generate DHCPv6 requests and generate a large number of DHCP mapping in the DHCP server. This can complicate the administration of the network and introduce a high signal to noise ratio that introduces complexity in confirming valid and invalid host mappings (described in section 5.1). Under certain conditions this can negatively impact the DHCPv6 service and will result in denial or degradation levels of service for the entire organization (Droms et al., 2003).

3.5 IPv6 NDP resource exhaustion

Resource exhaustion vulnerabilities may also exist on the network platform and not only on application services. It was found by Wheeler (2011) that in many data centre switching hardware that utilizes Application Specific Integrated Controlled (ASIC) assisted switch planes the IPv6 neighbour discovery memory capacity is a limited ternary content-addressable memory (TCAM) space. This potentially exposes the switching ASIC to memory exhaustion attacks through the spoofing of a large number of IPv6 addresses

This attack is called neighbour cache exhaustion. It has been tested and found that the implementation is not as easy as stated in the presentation by Wheeler. On the Insinuator Blog, Rey (2013a) has tested the NDP exhaustion and found that Wheeler's assumption was incorrect that the incomplete NDP expiration time is "long" (Wheeler, 2011). RFC 4861 documents the default behaviour of the NDP protocol, and if the node adheres to these the retransmit timer (RETRANS_TIMER) will be 1,000 milliseconds and the number of solicitations (MAX_RTR_SOLICITATIONS) are configured to delete any INCOMPLETE state in 3 attempts.

In section 5.2, the assumptions are tested in the test laboratory and the conclusion that Rey found is confirmed.

3.6 Attack classification and prioritization

The paper release at the USENIX 2014 entitled *IPv6 Security: Attacks and Countermeasures in a Nutshell* includes a detailed attack matrix as shown in Table 11. It evaluates the countermeasures available for IPv6 attacks as well as the vectors employed by the attacks (Ullrich et al., 2014).

The paper presents a table which provides classification of the security vulnerabilities that include 36 named vulnerabilities. The table indicates the prevalence of attacks in the Neighbour and Route advertisements and motivates the identification of the access layer as a vulnerable attack surface, with enterprise impact.

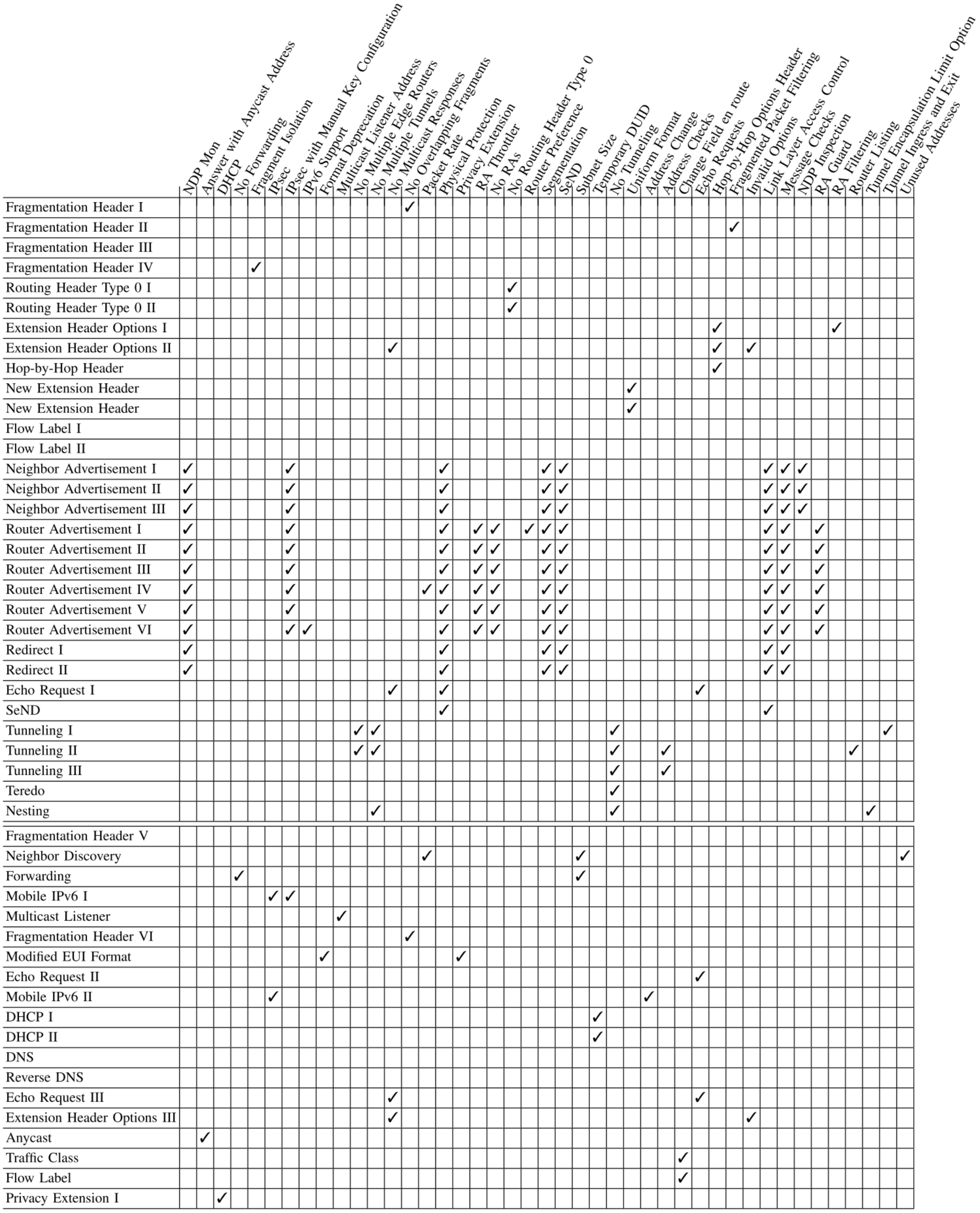
3.7 Summary

Although the various vulnerabilities and manipulation methods exist for IPv6, it is found that the protocol has similar characteristics to the legacy IPv4 protocol. The new functionality and application that appears in IPv6 does serve to provide an additional attack landscape (highlighted in Table 11) and requires controls that expand into packet inspection and network monitoring.

Some identified risks which have been presented by network researchers have also been found to be impractical and theoretical of nature i.e. the NDP resource exhaustion attacks discussed in section 3.5 and tested in section 5.2. The identified resource may still be exhausted by combining distributed methodologies to the attack, or by the addition of an additional attack vector.

There has been a consistent flow of research by various academics and industry specialists since the early implementation of IPv6. The adoption of the IPv6 protocol into Enterprise as well as the expanding deployment on the Internet will continue to increase the value of the research.

Table 11: Evaluation of Countermeasures



	NDP Mon	Answer with Anycast Address	DHCP	No Forwarding	Fragment Isolation	IPsec	IPsec with Manual Key Configuration	IPv6 Support	Format Deprecation	Multicast Listener Address	No Multiple Edge Routers	No Multiple Tunnels	No Multicast Responses	No Overlapping Fragments	Packet Rate	Physical Protection	Privacy Extension	RA Throttler	No RAs	No Routing Header Type 0	Router Preference	Segmentation	SeND	Subnet Size	Temporary DUID	No Tunneling	Uniform Format	Address Change	Address Checks	Change Field en route	Echo Requests	Hop-by-Hop Options Header	Fragmented Packet Filtering	Invalid Options	Link Layer Access Control	Message Checks	NDP Inspection	RA Guard	RA Filtering	Router Listing	Tunnel Encapsulation Limit Option	Tunnel Ingress and Exit	Unused Addresses
Fragmentation Header I														✓																													
Fragmentation Header II																																	✓										
Fragmentation Header III																																											
Fragmentation Header IV					✓																																						
Routing Header Type 0 I																				✓																							
Routing Header Type 0 II																				✓																							
Extension Header Options I																																✓							✓				
Extension Header Options II													✓																			✓		✓									
Hop-by-Hop Header																																✓											
New Extension Header																											✓																
New Extension Header																											✓																
Flow Label I																																											
Flow Label II																																											
Neighbor Advertisement I	✓						✓									✓						✓	✓												✓	✓	✓						
Neighbor Advertisement II	✓						✓									✓						✓	✓												✓	✓	✓						
Neighbor Advertisement III	✓						✓									✓						✓	✓												✓	✓	✓						
Router Advertisement I	✓						✓									✓		✓	✓		✓	✓	✓												✓	✓		✓					
Router Advertisement II	✓						✓									✓		✓	✓			✓	✓												✓	✓		✓					
Router Advertisement III	✓						✓									✓		✓	✓			✓	✓												✓	✓		✓					
Router Advertisement IV	✓						✓								✓	✓		✓	✓			✓	✓												✓	✓		✓					
Router Advertisement V	✓						✓									✓		✓	✓			✓	✓												✓	✓		✓					
Router Advertisement VI	✓						✓	✓								✓		✓	✓			✓	✓												✓	✓		✓					
Redirect I	✓															✓						✓	✓												✓	✓							
Redirect II	✓															✓						✓	✓												✓	✓							
Echo Request I													✓			✓															✓												
SeND																✓																			✓								
Tunneling I											✓	✓														✓																✓	
Tunneling II											✓	✓														✓			✓											✓			
Tunneling III																										✓			✓														
Teredo																										✓																	
Nesting												✓														✓															✓		
Fragmentation Header V																																											
Neighbor Discovery															✓									✓																			✓
Forwarding				✓																				✓																			
Mobile IPv6 I						✓	✓																																				
Multicast Listener										✓																																	
Fragmentation Header VI														✓																													
Modified EUI Format									✓								✓																										
Echo Request II																															✓												
Mobile IPv6 II						✓																						✓															
DHCP I																									✓																		
DHCP II																									✓																		
DNS																																											
Reverse DNS																																											
Echo Request III													✓																		✓												
Extension Header Options III													✓																					✓									
Anycast		✓																																									
Traffic Class																														✓													
Flow Label																														✓													
Privacy Extension I			✓																																								

Taken from (Ullrich et al., 2014 Table V)

Chapter 4

Research Methodology

This chapter identifies and documents the environment that will form part of the scope of the research in the Enterprise. The same environments are utilised in the scenarios in Chapter 5. In section 4.1 the network and security architecture of the common enterprise as defined by industry vendors such as Cisco (2008), Huawei (2011), Juniper (2008) and Brocade (2014) will be discussed. This chapter will examine the architecture that is commonly known as Spine and Leaf. It will also explain how the network has evolved from a hierarchical structure to a meta-structure that enables a flat network to span across the infrastructure in conjunction with pointing out the benefits of hierarchical architecture. The Spine and Leaf architecture has become a best practice for enterprise networks in that it provides consistency and scalability deployment in a local or distributed network.

The flat layer 2 that can be virtually spanned throughout the environments (described in section 4.1.5) exposes the entire network to threats in the access layer that may expand beyond the limited broadcast domain. By passing the access layer traffic over virtually spanned broadcast domains, it introduces heightened risks to the network.

In section 4.2 the Test Laboratory is described as it relates to the Enterprise Architecture in section 4.1. This virtual laboratory has been used as the simulated environment in that it provides the necessary service and network structure used to research the findings in this document.

The research takes into consideration the IPv6 deployment from a systems and environmental management perspective. This is complicated by the growth in addressable space. Providing information around the IPv6 network environment will become complex, when taking into consideration the large number of addresses that may be deployed in an environment not forgetting the meta-data that will associated with each address.

4.1 Network and security architecture

The network architecture and the transport layers that provide traffic segregation and the flow of data in an enterprise are designed to enable businesses' requirements for connectivity in a highly redundant manner. Network architectures can be deployed in various manners that dictate the way that the network responds to devices and how the scope of traffic flow is determined, whether it is local, segregated or globally significant. This aspect is important to consider during the evaluation of threats that have historically introduced risk which were locally significant. These threats are now facilitated through the new transport technology (discussed in section 4.1.5) and have the potential to impact a far more significant part of the enterprise network environment.

4.1.1 Evolution of Traditional the campus network

The campus network (or otherwise known as the Hierarchical internetworking model) has formed part of the enterprise network and security model for the past twenty years and has evolved based on the advancements in technology and the shifting requirements of business (Cisco, 2008; Huawei, 2011; Brocade, 2014).

One of the primary principles of the hierarchical network design has been to compartmentalise services and functionality to their respective building blocks, thereby allowing for agile and scalable deployment (Huawei, 2011). This was implemented through a routed distribution layer that interacted with the core layer and provided services to the localized access layer. The allows an enterprise network architect to align the business requirements to the functions available in the various building blocks and thereby use a modular approach to constructing the necessary network infrastructure.

The traditional campus network as show in Figure 16 provides three layers in the network stack. The core network provides high capacity network switching and routing transport between the attached distribution layer. The distribution or aggregation layer is a combination of routing and switching devices which provides connectivity, services and control to the third layer called the Access layer. This has included the network services that have been discussed in section 2.5 and section 2.5 It provides access nodes with the auto-configuration and routing configuration information.

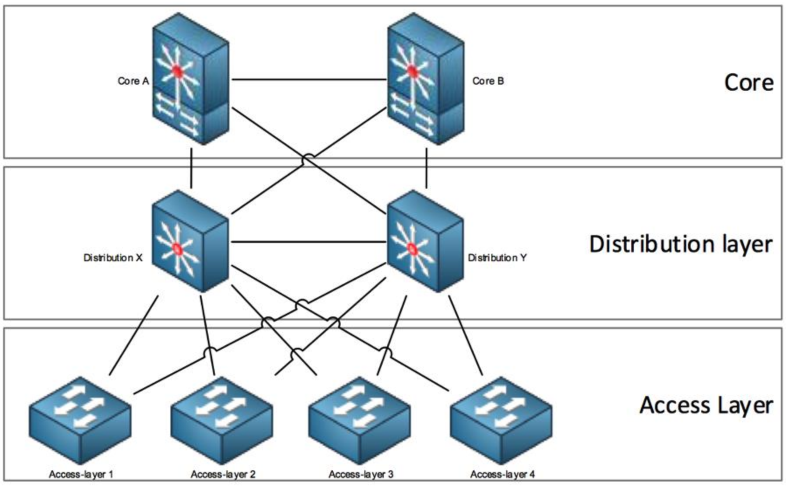


Figure 16. Traditional Campus architecture

The final layer, which is the access layer, has traditionally provided high port density that facilitates the connectivity of layers 1 and 2 to the end points in the network. The access switch is impacted through the deployment of IPv6 (or lack thereof) which then introduces the risk of unexpected behaviour in the network (shown in section 5.3).

The industry is attempting to move the boundaries of layer 3 down from the distribution layer to the access layer. The drivers for the change are the promotion of scalability and resiliency, as the layer 3 routed infrastructure provides improved convergence performance (Cisco, 2007).

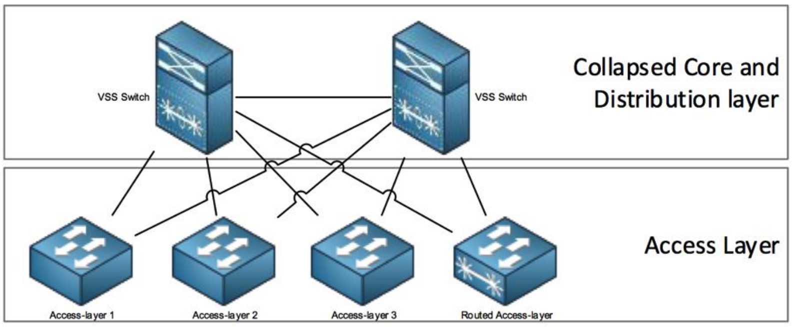


Figure 17. Converged core architecture

Simplifying the environment has become possible by collapsing aspects of the core, distribution and access layers into a consolidated platform. The collapsed distribution and core provides the same services that the individual layers provided in the three-tiered architecture, still with sufficiently high port density to provide access to the access layer and the server environment in two tiers. Although the collapsed core architecture does not provide the scalability possible with the three tier model, it does provide the required connectivity to an average enterprise network (Cisco, 2008). The bandwidth requirement between the distributed cores would also need to be considered on the inter switch links and as the environment grows, a core switch may provide the best point to aggregate the links (Mcfarland, Sambi, Sharma & Hooda, 2011).

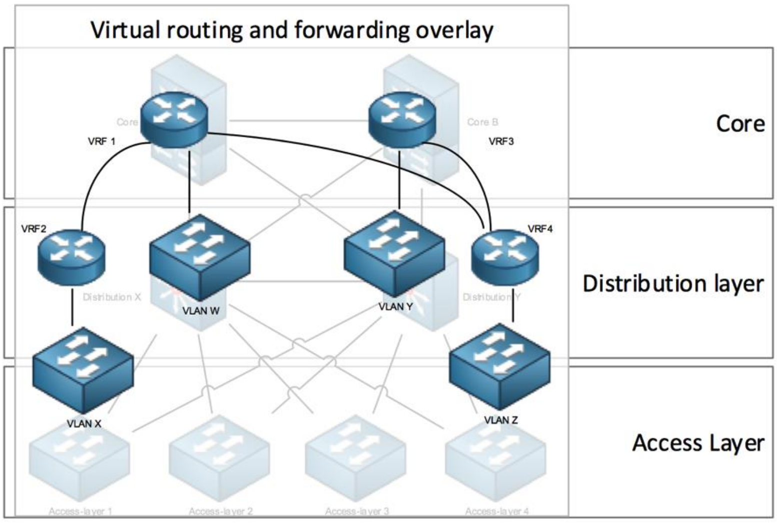


Figure 18. Virtual routing and forwarding overlay

Virtualisation in the routing and switching infrastructure facilitates the logical segregation of traffic flow and routing instances .This enables the creation of logical building blocks as shown by the overlay in Figure 18. The segregation can promote security, improve resiliency and provide improved flexibility in the campus architecture (Cisco, 2008; Mcfarland et al., 2011) Virtual routing technology forms a part of the requirement of new enterprise networks, providing the ability to segregate the network virtually.

The virtual network, that now provide an extended layer 2 broadcast domain that can span multiple geographical locations, impact the risk that Ethernet vulnerabilities represent. In the past the Ethernet vulnerabilities were isolated to individual switches and will now be able to impact the entire hierarchical model, negatively impacting all three layers.

4.1.2 Access layer

The enterprise access layer is the edge of the network and also forms the demarcation between the end-user devices and the network. This is provided by the connectivity to the network infrastructure in layers 2 and 3 and facilitated high port density to extend into the physical building infrastructure to provide connectivity throughout the building.

The access layer is the fabric where MAC addresses are bound to the higher layer network protocols. These include IPv4 and IPv6. In IPv6 this layer has significantly changed with the deprecation of the ARP protocol which was utilised to map IPv4 addresses to MAC addresses. IPv6 provides internal functionality through ICMPv6 and Neighbour Discovery as defined in RFC 2461 (Narten et al., 1998) in that it also includes the ICMP redirect functionality and ICMP router discover functionality.

The introduction of the NDP has the benefit of using Multicast over Broadcast and will in future reduce the amount of broadcast noise on the access layer.

4.1.3 Distribution layer

The distribution layer acts as an aggregation point for the access layer and provides a control boundary to the core network. The distribution layer has historically provided intelligent services which consisted of quality of service, routing and filtering. Many of these intelligent functions have started to migrate to the access layer and respond to classes of attacks similar to the attacks discussed in Chapter 5.

IPv6 introduced the ICMPv6 Router Advertisement as part of the NDP RFC 2461 (Narten et al., 1998) which enabled the local router to advertise a local segment and facilitate the auto-configuration of clients. Historically, this function has existed in the distribution layer and largely still provides workstation and client access to the network. Using Router Advertisements in conjunction with DHCPv6 (Droms et al., 2003) one is able to automatically configure the clients. The relay function is primarily facilitated through the distribution layer and permits expansion through options such as Relay Agent Remote-ID defined in RFC 4649 (Volz, 2006).

4.1.4 Core layer

The core layer is a high-speed network which provides an interconnection between the distribution layer's devices. The core network device needs to provide enough network performance to facilitate a high throughput between numerous distribution layer devices that potentially use various protocols. In the past, the core network device has provided little intelligence and services, mainly owing to its limitations on a functional processing capacity (Cisco, 2008). As the new generation of routing and switching equipment is developed and released, the processing capacity is improved and therefore facilitates functional capabilities that were not possible in the past. This is one of the factors driving the consolidation of the core and distribution layers into the collapsed core model.

With the arrival of IPv6 and the support of the aforementioned Memorandum in section 2.1.4, core layer network devices have been designed to run a virtualised, encapsulated IPv4 environment on an IPv6 campus backbone.

4.1.5 Distributed networking

With advent of Multi-protocol label switching (MPLS) for the layer 3 extension and LAN extension technologies such as Virtual Extensible LAN (VXLAN) (Mahalingam, Hutt, Duda, Agarwal, Kreeger, Sridhar, Bursell & Wright, 2014) and Virtual Private LAN Service (VPLS) (Kompella & Rekhter, 2007) distributed networks are possible which also provide a remote data centre and wide area network infrastructure that can share layer 2 and layer 3 networks.

An example in Figure 19 shows how VLAN X is extended over a layer 3 inter-network between Site V and Site T. This also illustrates how VLAN Z is locally significant in Site T and that only selected layer 2 networks are extended.

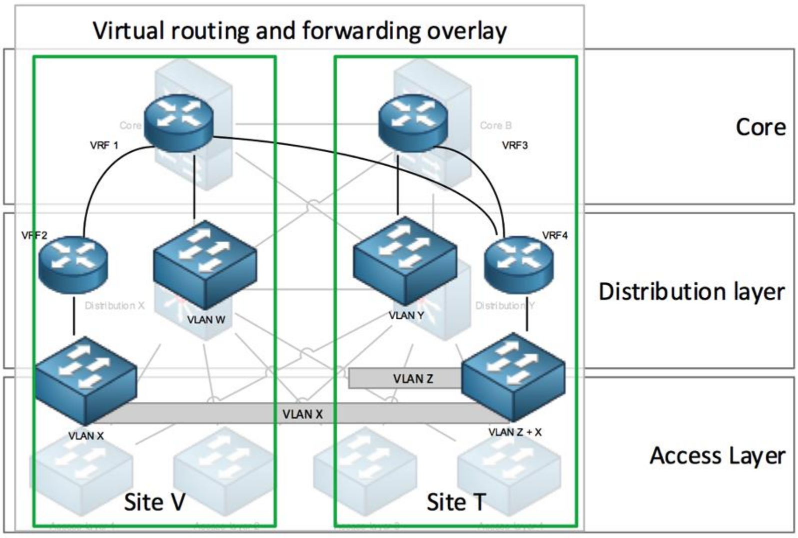


Figure 19. Multi Site layer 2 and layer 3 extension

As discussed in section 2.8.5, the localisation of the layer 2 Ethernet network provided a limited scope domain that would isolate the first hop attack impact on the connected switches. This extension and transport of the Ethernet broadcast domain exaggerates the impact that access layer IPv6 vulnerabilities may have on the operation of the enterprise layer 3 network.

The layer 3 network only has visibility of the encapsulated Ethernet Frames and therefore the controls to restrict the impact of a distributed attack on an Ethernet segment does not exist in the transport layer. Cisco also has proprietary transport virtualisation i.e. Overlay Transport Protocol (OTV) which provides additional functionality and control (Cisco Systems Inc, 2010b).

4.1.6 Perimeter

The perimeter provided the network infrastructure that interconnects an enterprise network to third party networks or the Internet. This has been the demarcation point where corporations have placed their Firewall devices to protect the Local LAN from the foreign networks and attackers. As NAT has depreciated and end to end addressing becomes a reality in IPv6, it will be fundamentally important to implement *stateful* firewall controls that will provide protection from uninitiated external connectivity into the local LAN to reduce the attack exposure to the internal nodes (Convery, 2004).

This said, the mobility of end user devices is changing the perimeter model (Hogg, 2007) and therefore network perimeter security should only be part of a larger holistic security architecture. Trends such as the “Bring your own device” movement is bringing insecure consumer equipment into the enterprise network and therefore internal networks may need to be classified as perimeters to organisation’s information network.

4.2 Test laboratory

In Figure 20 the enterprise network stack is reproduced in a virtual environment to align to the Hierarchical/Spine and Leaf Campus design and the best practices discussed in section 4.1.

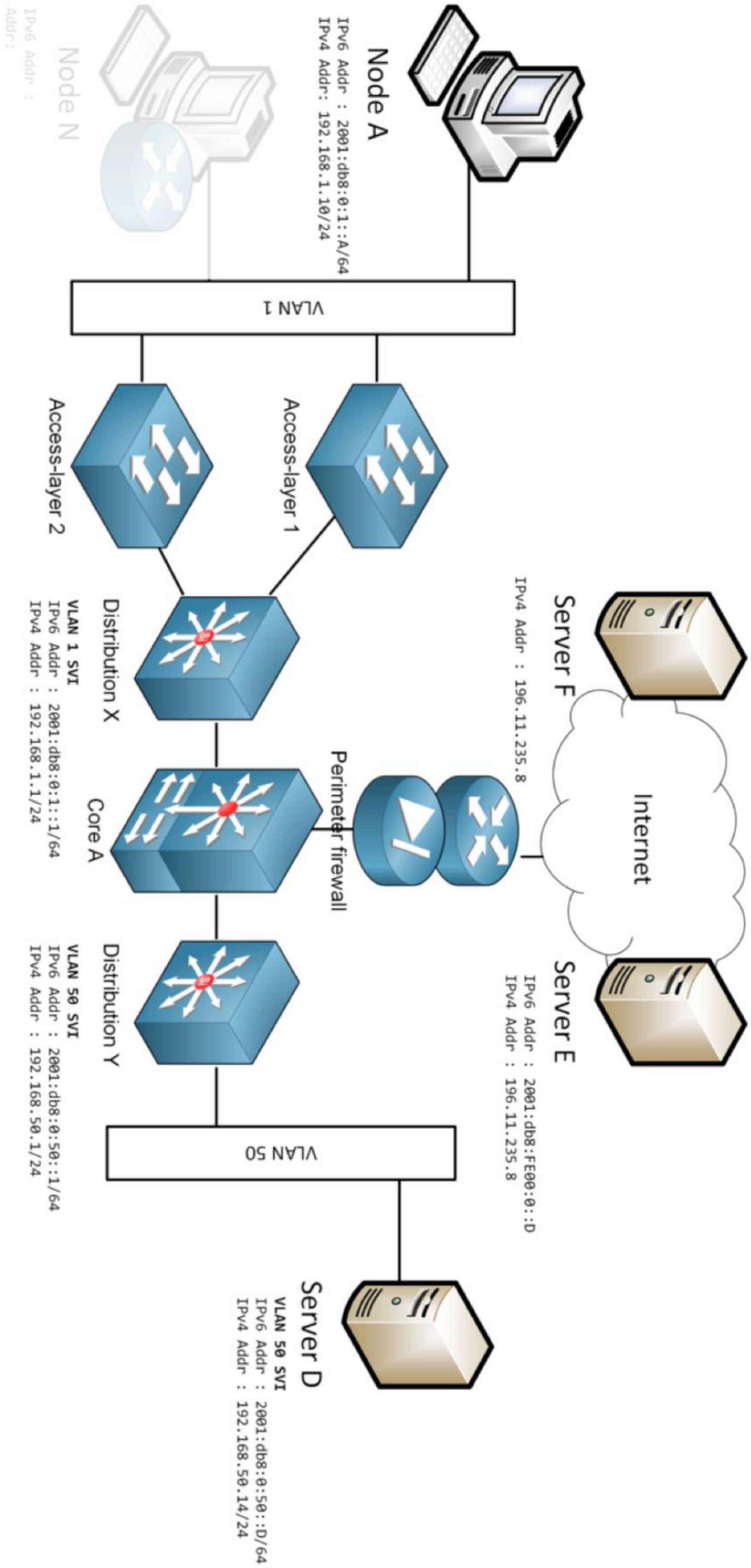

Node A
IPv6 Addr : 2001:db8:0:1::A/64
IPv4 Addr: 192.168.1.10/24
Node N
IPv6 Addr :
Addr :
VLAN 1
Access-layer 1
Access-layer 2
Server F
IPv4 Addr : 196.11.235.8
Internet
Distribution X
VLAN 1 SVI
IPv6 Addr : 2001:db8:0:1::1/64
IPv4 Addr : 192.168.1.1/24
Perimeter firewall
Core A
Server E
IPv6 Addr : 2001:db8:FE00:0::D
IPv4 Addr : 196.11.235.8
Distribution Y
VLAN 50 SVI
IPv6 Addr : 2001:db8:0:50::1/64
IPv4 Addr : 192.168.50.1/24
VLAN 50
Server D
VLAN 50 SVI
IPv6 Addr : 2001:db8:0:50::D/64
IPv4 Addr : 192.168.50.14/24

Figure 20. Virtualised test laboratory

The VLAN access layer segmentation is virtualised through VMNet networks which are configured on the VMWare Workstation. The VMNet virtualization provides the broadcast domain segmentation, but does not provide the necessary port based configurations and features that are tested in Chapter 5. The scenarios which require physical switching ASICs have been implemented by spanning two VMNet networks to two different physical network interfaces on the VMware host. The traffic flow between the one network interface through a physical switching device and back to the other interface which is associated to another spanned VMNet.

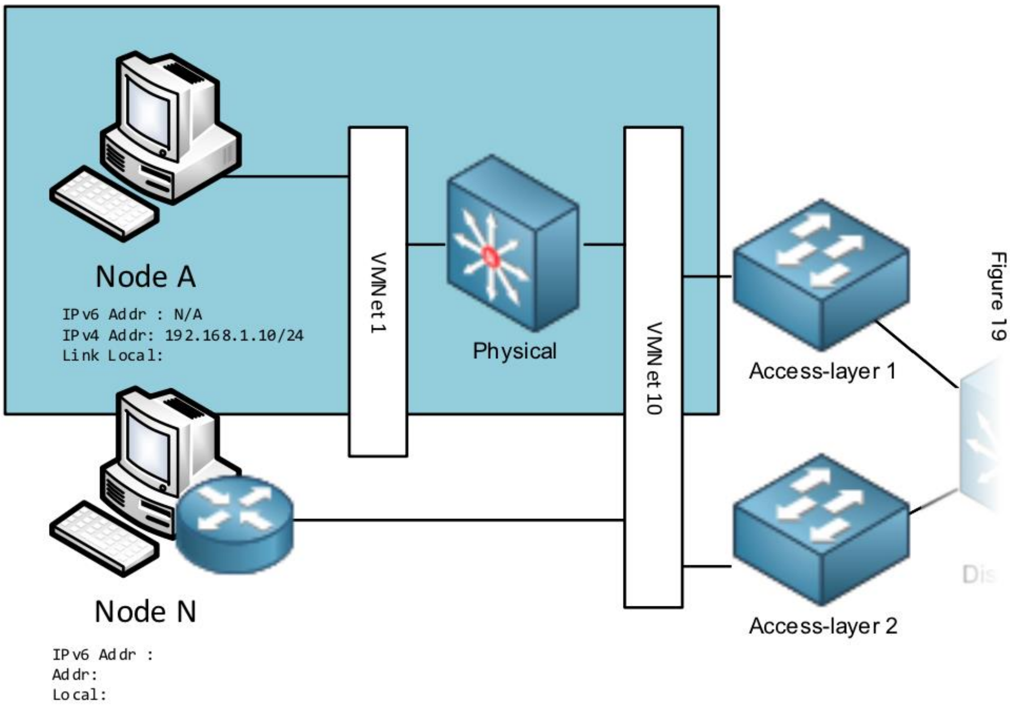


Figure 21. Physical integration to Virtual test Laboratory

In Figure 21 the logically segregated VMNet 1 and VMNet 10 network segments are “bridged” by using a physical switch. The VMware host has the two physical ports configured to enable the flow of traffic from one network to another.

The distribution layer is provided by a FreeBSD based pfSense[11] firewall (version 2.1.4-RELEASE) which provides the intersegment routing through the Core. The firewall policy

[11] http://www.pfsense.com

of the distribution layer pfSense nodes were configured to permit all traffic between the various networks so that it would mimic a standard enterprise layer 3 Switch.

The distribution devices that are listed in Table 12 provide the services required for auto - configuration and routing by the access layer. These services include Dynamic Host Configuration Protocol (DHCP) server as well as a relay to forward the requests to a dedicated DHCP server. A DNS caching server is available to resolve DNS requests from the hosts. These services are provided on IPv4 and IPv6 (as required by the specific scenario).

These distribution devices provide the default gateway to the connected layer 2 domain, and Distribution W through Z can provide IPv6 Router Advertisements to facilitate local SLAAC and DHCP information requests if necessary in the scenario.

Table 12: Network switching and routing nodes

Node Name	Description	Interface configuration
Distribution W	*Hostname: lab_distrX_pfSense* Services Distribution layer	VMnet10 / VLAN 10 VMnet11 / VLAN 11
Distribution X	*Hostname: lab_distrX_pfSense* IPv4 Distribution layer	VMnet10 / VLAN 10 VMnet11 / VLAN 11
Distribution Y	*Hostname: lab_distrX_pfSense* IPv4 / IPv6 Distribution layer	VMnet12 / VLAN 12 VMnet13 / VLAN 13
Distribution Z	*Hostname: lab_distrX_pfSense* IPv6 Distribution layer	VMnet10 / VLAN 10 VMnet11 / VLAN 11
Core A	*Hostname: lab_CoreA_pfSense* Core Interconnect	

Three access layer networks are provided for an IPv4, IPv6 and dual stack environment. The interfaces are configured to provide IPv6 and IPv4 connectivity and facilitate relaying of DHCP queries to Server A.

To provide the necessary the infrastructure and hosts to facilitate the various configurations in the case studies, the hosts in **Table 13** were prepared with default system auto-configuration. The various operating systems would interact with the network in the same way as a vanilla host would, and therefore would be part of our baseline configuration. The VMware environment did permit the use of cloned hosts and consequently, multiple revisions of these hosts were available to deploy in line with the case studies requirements.

Table 13: Access layer Lab nodes

Node Name	Description	Interface configuration
Node A	*lab_[VmnetID]_win7_v[46]* Windows 7 host	IPv6 and IPv4 auto configured
Node F	*lab_[VmnetID]_win8_v[46]* Windows 8.1 host	IPv6 and IPv4 auto configured
Node C	*lab_[VmnetID]_ubuntu1404_v[46]* Ubuntu 14.04 Desktop host	IPv6 and IPv4 auto configured
Node D	*lab_[VmnetID]_freebsd10_v[46]* FreeBSD 10 host	IPv6 and IPv4 auto configured – No DHCPv6 support
Node F	*Lab_[VmnetID]_kali107* Kali Linux 1.07 penetration testing host	Adaptive configuration based on the scenario

VMWare tools have been installed on all hosts that support it.

4.3 Summary

The landscape of enterprise network is changing and the borders that have prevented a far reaching negative impact on the network are being flattened with the arrival of the virtually extended layer 2 zones. By associating the attack landscape to the enterprise environment, the access layer has been identified as a potential attack vector that will be discussed in Chapter 5. The ability to introduce network route and poisoned link local addresses are similar to the challenges faced in IPv4 and are understood, although the new vectors take into account the attributes of IPv6 that impact the effectiveness of the compensating controls.

The combination of the access layer and the enormous SLAAC required network ranges also provide a malicious attacker with ample address space to introduce a new DHCP resource attack. The focus on the address pool has shifted to the server CPU and memory resources. This situation provides another scenario worth considering and will be described in section 5.1. Here the IPv4 environment was locally affected by address depletion attacks, and the new attack could impact the entire organisation.

Chapter 5

IPv6 threat mitigation case studies

In this chapter we use Cisco technology in conjunction with a VMWare environment to demonstrate the implementation of technical mitigations in the enterprise environment. The Cisco environment consists of equipment from the Cisco Validated design as presented in section 4.1. Cisco is one of the most pervasive network technologies in the enterprise network segment. Although the network segment is changing, the current landscape in South Africa, and specifically in the Western Cape, indicates that Cisco will still be a leader in the next three to five years.

By using the test laboratory defined in section 4.2, the cases in this chapter were deployed and tested to verify the impact. Table 15, consists of the vulnerabilities that are used to identify and quantify the impact to the Enterprise. The following cases tested in this chapter will provide the feedback to complete the final matrix and provides supports to the research questions as provided in **Table 14**.

Tests have been conducted multiple times during preparation and the capture process, however no numerous runs were not completed to prove statistical significance, as we were not quantifying the information. All the case studies in this chapter have been completed in the duplicate environments based on the Research Methodology lab in Chapter 4.

Table 14: Research questions in support of the case studies

Research Question	NDP resource exhaustion	DHCPv6 resource exhaustion attack	Traffic interception attacks	IPv6 management challenges and recommendations		
				Network Solicitation	Router Advertisement attacks	Network Router Advertisement
Determine whether the average enterprise network access layer device can support and manage IPv6 equipment securely.	X	X		X	X	X
Should enterprise organisations adopt IPv6 in the near future?			X	X	X	X
Does current IPv6 implementations introduce an unacceptable risk into the Enterprise?”	X	X		X	X	

The DHCP resource exhaustion attack occurred in the IPv4 environment and morphed from address exhaustion to a system resource exhaustion attack. This is an example where the increase in the address space could hold challenges for the network management and resourcing of the network services. The NDP resource exhaustion is also assessed to verify the impact that the attack vector could have on the enterprise environment.

Next, the various methods of traffic interception are reviewed and tested, showing the way that standard IPv6 deployment will counter the attack vector. In conjunction to the traffic interception, information gathering methods are identified whereby misconfigured hosts that are attempting to tunnel in the enterprise can be detected.

Table 15: Identified Protocol vulnerabilities

Associated protocol	Description
IPv6 Protocol	Optional Header attack - Hop by Hop Amend a Hop by Hop header to bypass prevention mechanisms
IPv6 Protocol	Optional Header attack - Atomic Fragmentation header Amend a Fragmentation header to bypass prevention mechanisms
IPv6 Protocol	Optional Header attack - Destination header Amend a DOH to bypass prevention mechanisms
IPv6 Protocol	Fragmentation overlapping and timing attack Fragment headers into multiple packets to bypass detection and filtering
NDP (RA 134)	Fake route advertisement Intercept traffic, own IP as default router
NDP (RA 134)	Fake route advertisement Generate Random RA with numerous prefixes
NDP (RA 134)	Fake route advertisement - 0 lifetime spoof
NDP (NA136)	Address resolution spoofing Spoof requested link-layer NA packet
NDP (NA136)	Address resolution spoofing Prevent address resolution, respond to all DAD requests
DHCPv6	DHCP DUID IAID spoofing Spoof the DUID and IAID of a host machine to target a static IP address, or IP with access
DHCPv6	DHCP response spoofing Provide target with address and a malicious gateway to MITM
DHCPv6	Client DHCP spoofing Generate random Client DHCP requests. DoS the DHCP service

Control configurations (presented in section 5.3.4) identify tunnelled traffic and prevent the tunnelling through access control lists. Owing to the nature of the change in IPv6 over the IPv4, the controls are not sufficient to stop the potential attacks, and therefore the last control is detective in nature and monitors the network for abnormal traffic and device patterns. In section 5.4, management of the IPv6 environment and the deployment of sensors which provide visibility into the environment are discussed.

5.1 DHCPv6 resource exhaustion attack

Dynamic Host Configuration Protocol has been vulnerable to resource exhaustion attacks in IPv4 and also in IPv6, but the exhaustion methods have changed significantly (Ferguson & Senie, 2000; Hauser, 2005). The IPv4 network address pool allocated to a network which segmented in an enterprise network was up to 1024 addresses of which 1022 hosts were facilltated on the segment with the broadcast and network address (Spirgeon & Joann, 2014). In IPv4 networks, the resource targeted by DHCP attacks were focussed on the limited address pool, which was easily depleted by spoofing DHCP requests. This attack, although effective, only impacted the local network segment and created a limited DoS state on that segment.

The significantly larger address spaces allocated to the IPv6 local segments presents a risk to the whole enterprise. The increased size of a standard /64 network used in LAN segments presents the local devices 18,446,744,073,709,551,614 IP addresses.

By expanding the address pool, the resource limitation has move from the address pool to resources such as memory, CPU and network performance. The administrative overhead of identifying misconfigured or malicious hosts on the network is complicated by the size of the address pool. On Node F (as shown in Figure 28), the flood_dhcpc6 can be used to simulate a DHCP client attack on Server D's DHCP server as follow.

First we need to start the parasite6 application that will answer all Neighbour Solicitation requests. The parasite6 application is part of the THC IPv6 Attack Toolkit developed by van Hauser as part of The Hacker's Choice IPV6 toolkit[12] and provides the same functionality as an ARP spoofing on an IPv4 network segment. The THC-IPv6 toolkit was presented in the talk "Attacking the IPv6 Protocol Suite" by van Hauser at PacSec Applied Security Conference in 2005 (Hauser, 2005).

```
# parasite6 eth0 &
```

This provides Node F with the ability to generate random MAC addresses so that the origin cannot be easily detected.

[12] The Hacker's Choice, https://www.thc.org/thc-ipv6/

The flood_dhcpc application is then started which initiates multiple requests for addressing from the DHCP server.

```
# flood_dhcpc eth0
```

It is possible to use a single MAC address and Link Local address, which with to increase the performance of the attack and it does not impact the other devices on the local segment with the parasite6 application.

```
# flood_dhcpc -N eth0
```

On the Server D the impact of Node F is evident as the system load immediately rises by approximately 70% as shown in Figure 22.

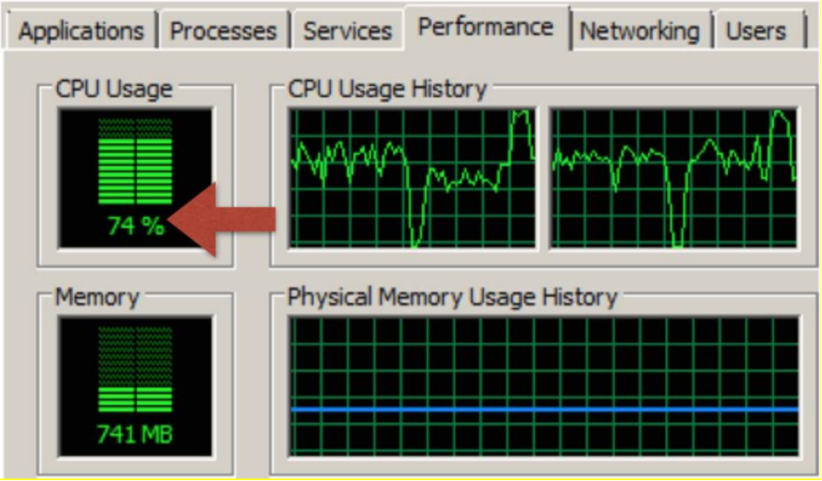
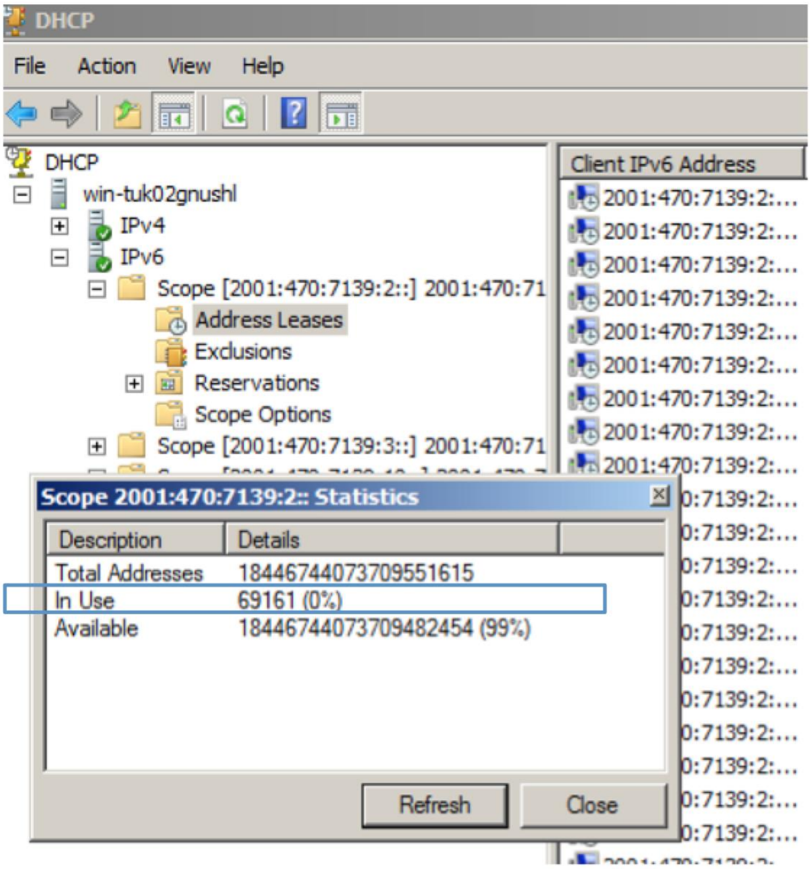


Figure 22. DHCP flood server impact

Although this does not impact the availability of IPv6 addresses, during this test the empty IPv6 DHCP scope is populated by 69,161 IPv6 leases in less than three minutes as shown in Figure 23.

This attack therefor has the potential to impact the compute resources of the DHCP server, which would include the CPU and memory on the server. The impact that this attack would present in small business environments (where various services are consolidated on single servers) may include a DoS to application beyond the DHCP service.

As a mitigating measure, the pool of the DHCP scope can be reduced to a more manageable number of IP addresses without introducing any impact on business. This can be implemented in the scope definition or one can set up scope exclusion in the DHCP server. This will allow an attacker to impact the local LAN segment, but will reduce the impact to the DHCP server and the wider enterprise environment.



Description	Details
Total Addresses	18446744073709551615
In Use	69161 (0%)
Available	18446744073709482454 (99%)

Figure 23. DHCP flood scope statistics (sample of 3 minute attack)

5.2 NDP resource exhaustion

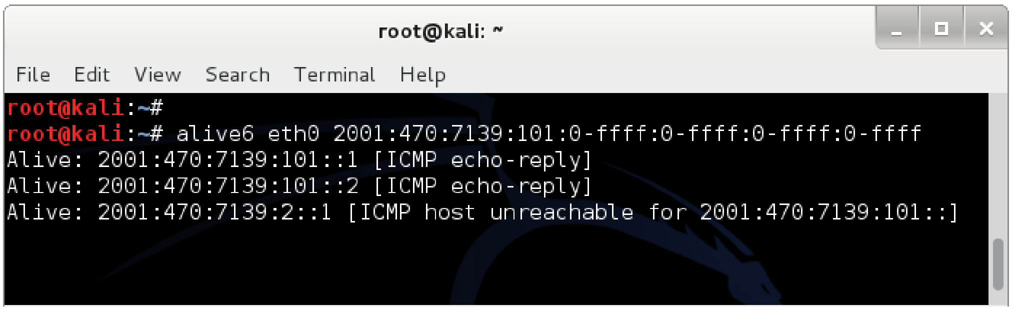
As described in section 3.5, there have been attacks described to affect the standard operation of switching platforms through the exhaustion of the NDP neighbour cache.

The tests used in this case study will use Node F to generate a high number of connection attempts to a layer 3 connected network on various IPv6 addresses. The address consists of the fixed address portion of the destination address and a configurable variable portion. In Figure 24 the “2001:470:7139:101” is the fixed network portion and the “0-ffff” indicates a variable portion for each of the last four 4-digit hexadecimal groups.

The alive6 application from the THC IPv6 toolkit is used to generate scanning traffic destined to the selected network. The purpose of this application is to scan and enumerate live IPv6 devices in the selected address network. This process generates a flood of packets in quick succession, which are processed by Distribution X and destined to the uplink network. We use the uplink network segment as the destination to emulate the environment whereby distribution can occur.

```
NodeF# alive6 eth0 2001:470:7139:101:0-ffff:0-ffff:0-ffff:0-ffff
```

The output of the command is shown in Figure 24.



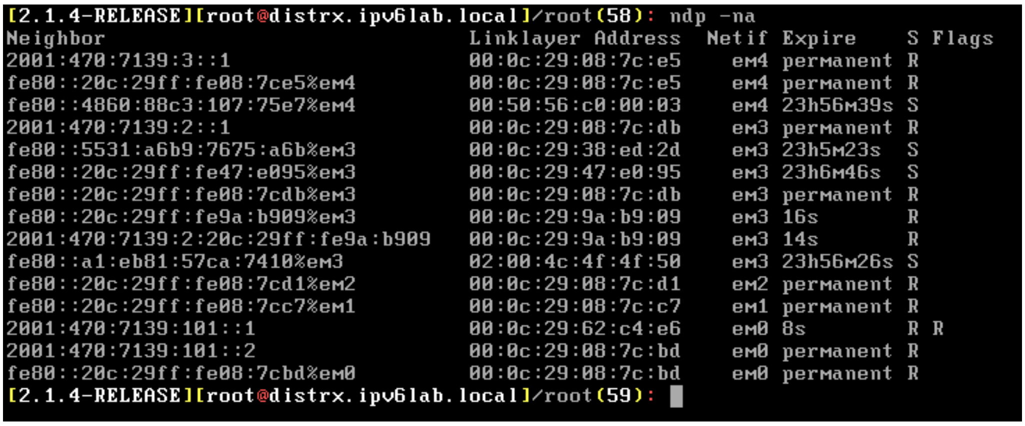
```
root@kali:~#
root@kali:~# alive6 eth0 2001:470:7139:101:0-ffff:0-ffff:0-ffff:0-ffff
Alive: 2001:470:7139:101::1 [ICMP echo-reply]
Alive: 2001:470:7139:101::2 [ICMP echo-reply]
Alive: 2001:470:7139:2::1 [ICMP host unreachable for 2001:470:7139:101::]
```

Figure 24. NDP exhaustion: alive6 execution

At the same time that the alive6 attack is generating the flood of packets, we can view the NDP states on the pfSense distribution X device using the ndp command as follows:

```
NodeF# ndp -na
```

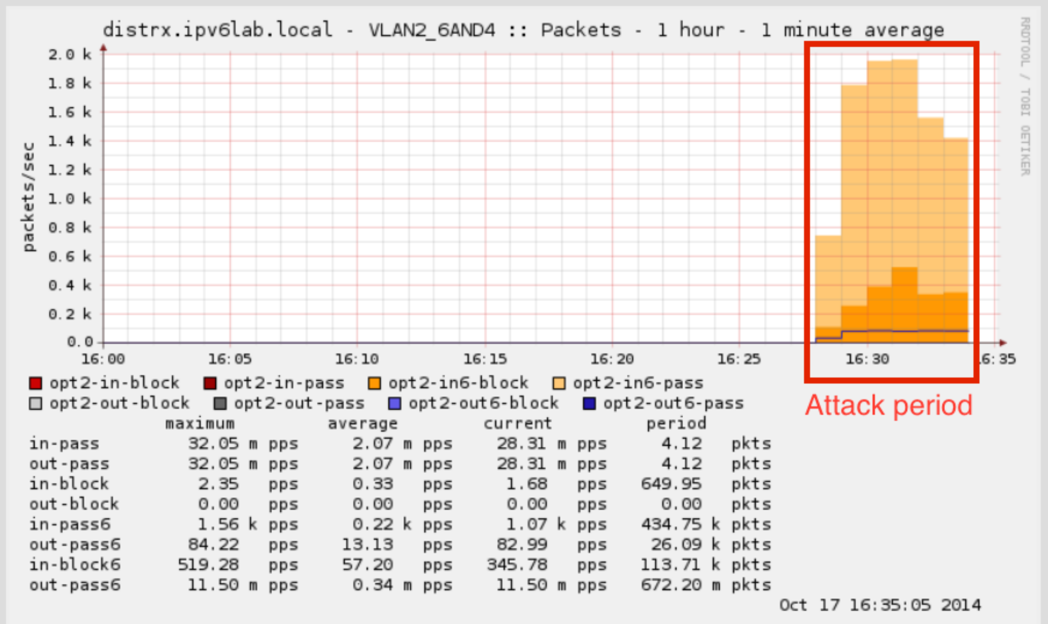
The output is shown in Figure 25.



```
[2.1.4-RELEASE][root@distrx.ipv6lab.local]/root(58): ndp -na
Neighbor                             Linklayer Address  Netif Expire    S Flags
2001:470:7139:3::1                   00:0c:29:08:7c:e5    em4 permanent R
fe80::20c:29ff:fe08:7ce5%em4         00:0c:29:08:7c:e5    em4 permanent R
fe80::4860:88c3:107:75e7%em4         00:50:56:c0:00:03    em4 23h56m39s S
2001:470:7139:2::1                   00:0c:29:08:7c:db    em3 permanent R
fe80::5531:a6b9:7675:a6b%em3         00:0c:29:38:ed:2d    em3 23h5m23s  S
fe80::20c:29ff:fe47:e095%em3         00:0c:29:47:e0:95    em3 23h6m46s  S
fe80::20c:29ff:fe08:7cdb%em3         00:0c:29:08:7c:db    em3 permanent R
fe80::20c:29ff:fe9a:b909%em3         00:0c:29:9a:b9:09    em3 16s       R
2001:470:7139:2:20c:29ff:fe9a:b909   00:0c:29:9a:b9:09    em3 14s       R
fe80::a1:eb81:57ca:7410%em3          02:00:4c:4f:4f:50    em3 23h56m26s S
fe80::20c:29ff:fe08:7cd1%em2         00:0c:29:08:7c:d1    em2 permanent R
fe80::20c:29ff:fe08:7cc7%em1         00:0c:29:08:7c:c7    em1 permanent R
2001:470:7139:101::1                 00:0c:29:62:c4:e6    em0 8s        R R
2001:470:7139:101::2                 00:0c:29:08:7c:bd    em0 permanent R
fe80::20c:29ff:fe08:7cbd%em0         00:0c:29:08:7c:bd    em0 permanent R
[2.1.4-RELEASE][root@distrx.ipv6lab.local]/root(59):
```

Figure 25. NDP exhaustion: ndp state output

On the pfSense platform this attack does not reflect as none of the MAC addresses have been associated to the requested IPs. During this simulated attack, the maximum rate of the packets processed by the distribution device is close to ≈1,950 packets per second (shown in Figure 26) and despite the packet flood, the average system is not significantly affected (shown in Figure 27).



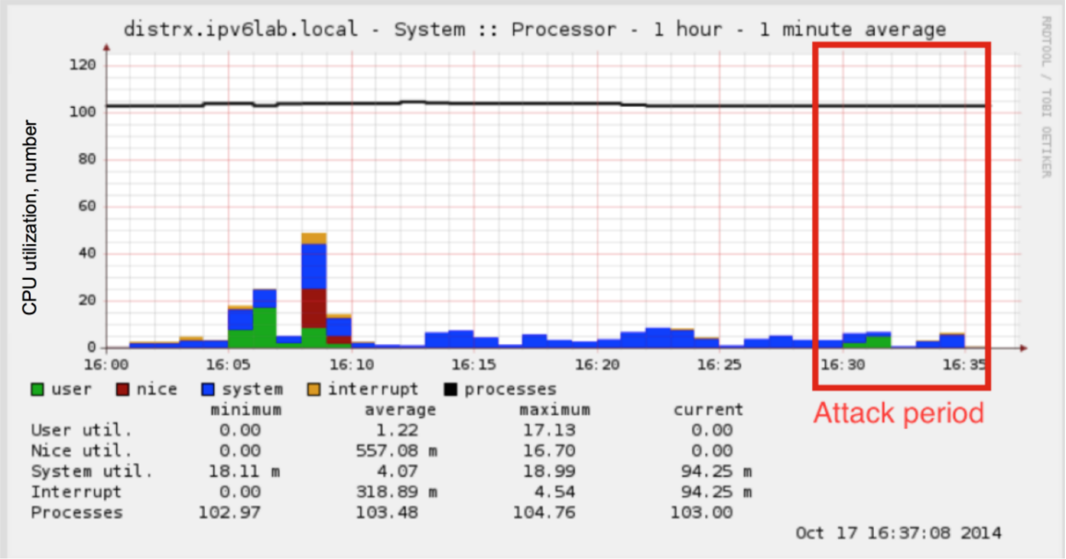
```
■ opt2-in-block   ■ opt2-in-pass   ■ opt2-in6-block   □ opt2-in6-pass
□ opt2-out-block  ■ opt2-out-pass  ■ opt2-out6-block  ■ opt2-out6-pass
             maximum         average        current         period
in-pass      32.05 m pps     2.07 m pps     28.31 m pps     4.12   pkts
out-pass     32.05 m pps     2.07 m pps     28.31 m pps     4.12   pkts
in-block      2.35   pps     0.33   pps      1.68   pps   649.95   pkts
out-block     0.00   pps     0.00   pps      0.00   pps     0.00   pkts
in-pass6      1.56 k pps     0.22 k pps      1.07 k pps   434.75 k pkts
out-pass6    84.22   pps    13.13   pps     82.99   pps    26.09 k pkts
in-block6   519.28   pps    57.20   pps    345.78   pps   113.71 k pkts
out-pass6    11.50 m pps     0.34 m pps     11.50 m pps   672.20 m pkts
                                                      Oct 17 16:35:05 2014
```

Figure 26. NDP exhaustion: packet generation rate

The test conducted in the test laboratory (described in 4.2) indicated that even low powered software routing platforms are not susceptible to NDP solicitation exhaustion as the unconfirmed address state does not persist for a sufficient amount of time to invoke a state of exhaustion using a single device.

Throughout the simulated attack, the system memory and CPU load did not incur any noticeable deviation from load under normal packet forwarding conditions.

To prevent the attack, one can deploy the network environments with DHCP and smaller network subnets, which will reduce the potential targets addressable in the broadcast domain. One can still allocate the /64 subnet, but reduce the network in use to a /118, with the rest of the /64 black hole routed. In this case one can then expand the IP scope in the broadcast domain if necessary. One caveat is that SLAAC will not work with these allocations as the /64 is required (Jinmei, 2007).



	minimum	average	maximum	current
User util.	0.00	1.22	17.13	0.00
Nice util.	0.00	557.08 m	16.70	0.00
System util.	18.11 m	4.07	18.99	94.25 m
Interrupt	0.00	318.89 m	4.54	94.25 m
Processes	102.97	103.48	104.76	103.00

Oct 17 16:37:08 2014

Figure 27. NDP exhaustion: Gateway CPU processing load

5.3 Traffic interception attacks

There are various methods whereby one can execute Man-in-the-Middle attacks on an enterprise environment. The attacks can be executed on local network using the stateless auto-configuration with DHCP (described in section 5.3.1). The same process has been available in IPv4 and is possible through the manipulation of the Address resolution protocol (ARP). Gratuitous ARP was used to direct traffic to a Man-in-the-Middle node that would be able to intercept the traffic and potentially pass it on and modify it. The difference between the ARP situation (in IPv4) is the way that IPv6 performs Link Layer Detection (LLD) with ICMPv6 in the protocol implementation.

Tunnelling can be used as an initiation process which directs the flow of traffic through an intermediary node (Node F) without the knowledge of Node A. These attacks make use of the DNS hijacking and poisoning to inject a node into the path of traffic. The ISATAP and Teredo tunnel interception methods are also possible remotely if the trusted DNS can be remotely poised to redirect the tunnel to a false target. This aspect will be discussed in more detail in section 4.4.2.

The IPv6 SLAAC attacks are similar in many respects to the Man-in-the-Middle attacks which are in IPv4, but with the higher priority of the IPv6 protocol in many operating systems, this presents a way to tunnel traffic over a covert channel with little impact to the node’s standard operations.

The network in Figure 28 is a logical representation of the enterprise access layer (defined in section 4.2) that utilises IPv4 stacks. Connectivity from the access layer to the enterprise is facilitated through automated configuration by a relayed DHCP service and standard IPv4 networking. There is no NAT implemented in this environment, and the perimeter NAT that may be part of the external Internet connectivity from this network, does not extend to this scope.

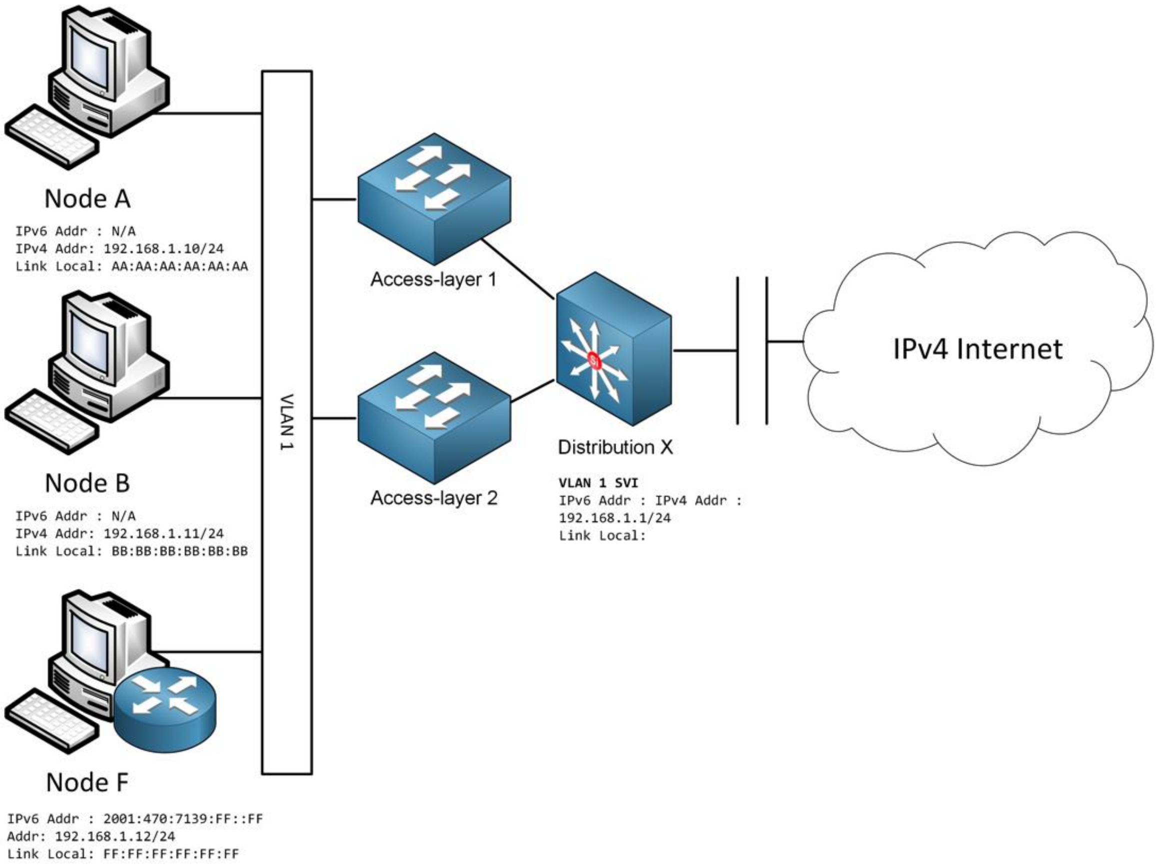


Figure 28. Logical enterprise access layer

The aforementioned network will be used to show how SLAAC and tunnelling can be used to intercept and forward the client traffic. We will also describe the ways that we can implement mitigating controls to prevent such attacks in section 5.3.2.

5.3.1 Hybrid IPv6 traffic redirection attacks

The SLAAC and DHCP method of changing the traffic flow of a device can be initiated from any device that is connected to the same layer 2 network. This is based on the fact that multicast is used to facilitate the Neighbour discovery, and that the relevant multicast address is link-local as defined in RFC 4861 (Jinmei, 2007, sec.2.3). Therefore the local gateway router should never forward it.

Existing protections exist, but are not at the protocol layer, and technologies such as Network Access Control (NAC) or manual network port access control are optional controls which can protect the physical layer (Hogg, 2007). This does not remove the attack surface completely, but it does reduce the attack scope to include only hosts that have pre-existing physical access to the network. Subsequently, the interception vector would change to leverage the connected hosts.

Figure 29 illustrates the process whereby traffic originating from Node A and Node B is directed through Node F by using IPv6 Router Advertisements and SLAAC.

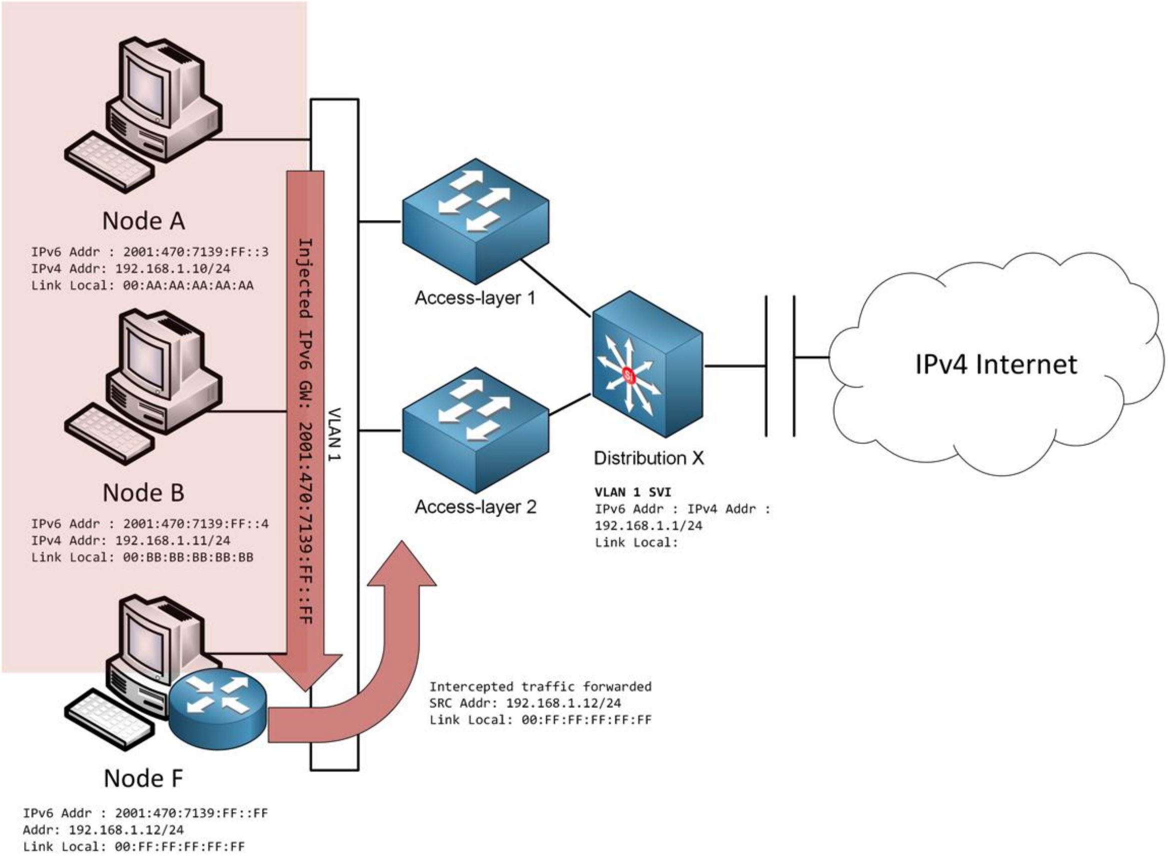

Node A
IPv6 Addr : 2001:470:7139:FF::3
IPv4 Addr: 192.168.1.10/24
Link Local: 00:AA:AA:AA:AA:AA
Node B
IPv6 Addr : 2001:470:7139:FF::4
IPv4 Addr: 192.168.1.11/24
Link Local: 00:BB:BB:BB:BB:BB
Node F
IPv6 Addr : 2001:470:7139:FF::FF
Addr: 192.168.1.12/24
Link Local: 00:FF:FF:FF:FF:FF
Injected IPv6 GW: 2001:470:7139:FF::FF
VLAN 1
Access-layer 1
Access-layer 2
Distribution X
VLAN 1 SVI
IPv6 Addr : IPv4 Addr :
192.168.1.1/24
Link Local:
IPv4 Internet
Intercepted traffic forwarded
SRC Addr: 192.168.1.12/24
Link Local: 00:FF:FF:FF:FF:FF

Figure 29. Traffic redirected to Node F

The Node F will then use NDP and generated ICMPv6 packets to present an IPv6 gateway to the locally connected hosts. As shown in Figure 29, Host A's network configuration will be altered by Node F's Router Advertisement and the specified route will be added to Host A's IPv6 routing table.

Figure 30 shows the process whereby fake Router Advertisements are used by the Node F to impact Node A and Node B network configuration. Once the client has accepted the fake advertisement, traffic will start to flow to Node F, altering the normal flow of traffic. The address range that has been added to Host A's routing table will effectively now be directed to Node F. This redirection of the traffic has placed Node F in a Man-in-the-Middle position and will permit the node to inspect and manipulate the traffic traversing Node F.

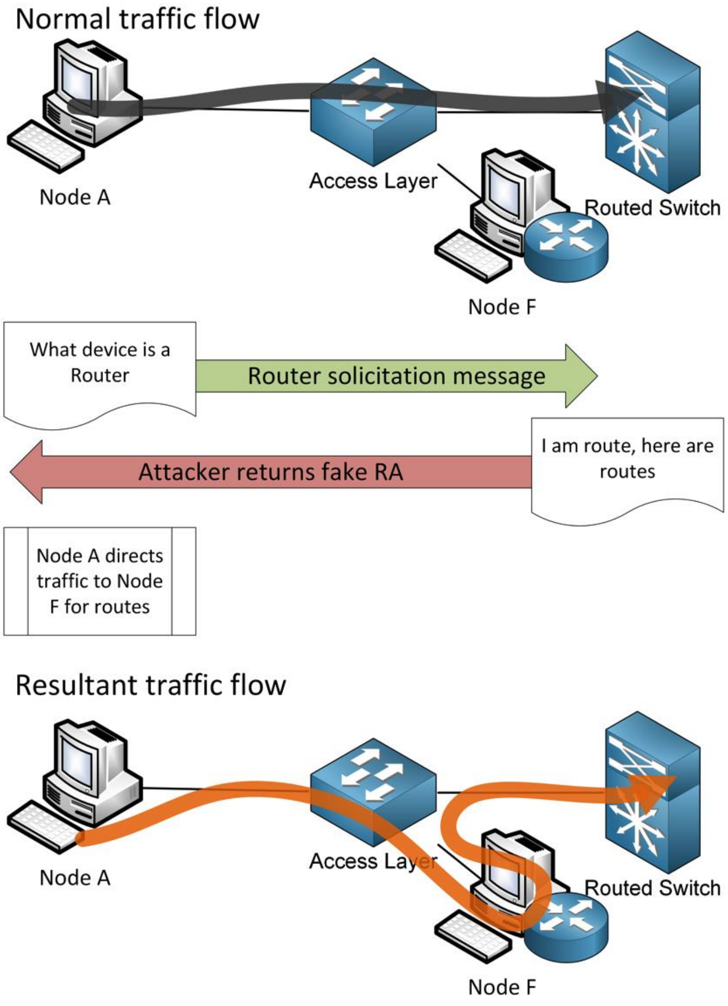
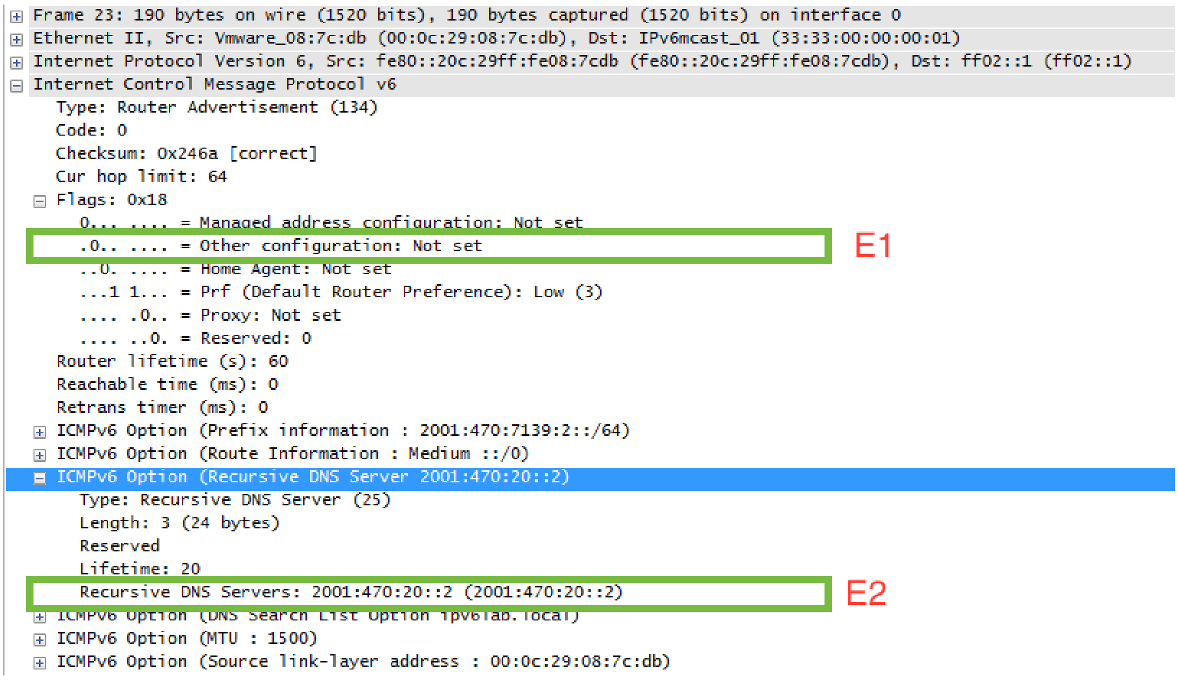


Figure 30. Fake Router Advertisement

The next step is to manipulate Node A to use the IPv6 addresses instead of the IPv4 addresses provided by the DNS service on Server D. This is a process that translates the domain name queries from IPv4 to IPv6. There are two methods that we are able to introduce Node F's modified DNS service to Node A through the standard network autoconfiguration.

The first option would be to use a DHCPv6 server which can be configured to update the host with additional DNS servers that are hosted by the attacker. This DHCP configuration method would be used in conjunction to the Router Advertisement “O” flag during the SLAAC process and would be an INFORMATION-REQUEST from the client. An example IPv6 Router advertisement packet with an unset “O” flag is shown in Figure 31, marked by E1.



```
⊞ Frame 23: 190 bytes on wire (1520 bits), 190 bytes captured (1520 bits) on interface 0
⊞ Ethernet II, Src: Vmware_08:7c:db (00:0c:29:08:7c:db), Dst: IPv6mcast_01 (33:33:00:00:00:01)
⊞ Internet Protocol Version 6, Src: fe80::20c:29ff:fe08:7cdb (fe80::20c:29ff:fe08:7cdb), Dst: ff02::1 (ff02::1)
⊟ Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0x246a [correct]
    Cur hop limit: 64
  ⊟ Flags: 0x18
      0... .... = Managed address configuration: Not set
      .0.. .... = Other configuration: Not set
      ..0. .... = Home Agent: Not set
      ...1 1... = Prf (Default Router Preference): Low (3)
      .... .0.. = Proxy: Not set
      .... ..0. = Reserved: 0
    Router lifetime (s): 60
    Reachable time (ms): 0
    Retrans timer (ms): 0
  ⊞ ICMPv6 Option (Prefix information : 2001:470:7139:2::/64)
  ⊞ ICMPv6 Option (Route Information : Medium ::/0)
  ⊟ ICMPv6 Option (Recursive DNS Server 2001:470:20::2)
      Type: Recursive DNS Server (25)
      Length: 3 (24 bytes)
      Reserved
      Lifetime: 20
      Recursive DNS Servers: 2001:470:20::2 (2001:470:20::2)
  ⊞ ICMPv6 Option (DNS Search List Option ipv6lab.local)
  ⊞ ICMPv6 Option (MTU : 1500)
  ⊞ ICMPv6 Option (Source link-layer address : 00:0c:29:08:7c:db)
```

Figure 31. Example IPv6 Router Advertisement

The second option (which is less likely to work) makes use of the DNS configuration option in the Router advertisement as shown by E2 in Figure 31. Although this attack may work on certain devices, Windows 7 and Windows 8/8.1 were tested and were found not to support the router advertisement of a recursive DNS services.

The Interception of the DNS requests, and the translation of the answers to redirect the traffic from the IPv4 address to the IPv6 address, requires a translating DNS, known as DNS64 service. The DNS64 service is located on Node F and responds to the DNS queries for Server F from Node A and returns the translated IPv6 AAAA addresses for the queries generated. As shown in Figure 32, the IPv6 address that is returned to Node A is formed by a combination of a known IPv6 prefix (such as 2001:db8:100:ffff::/96, which would correspond to the route included in Node A’s routing table) and the resolved IPv4 destination address of Server F as the suffix.

The traffic that is now directed to the malicious host will contain the intercepted domain requests in the targeted traffic flow. The packets will need to be processed and translated back to IPv4 so that the malicious host can serve the content expected by the client. Deploying a NAT-PT or NAT64 gateway will facilitate the IPv6 translation and invoke an ALG which will enable complex protocols such as FTP and SIP. The NAT-PT protocol has been depreciated, but it is still functional to deploy for this attack.

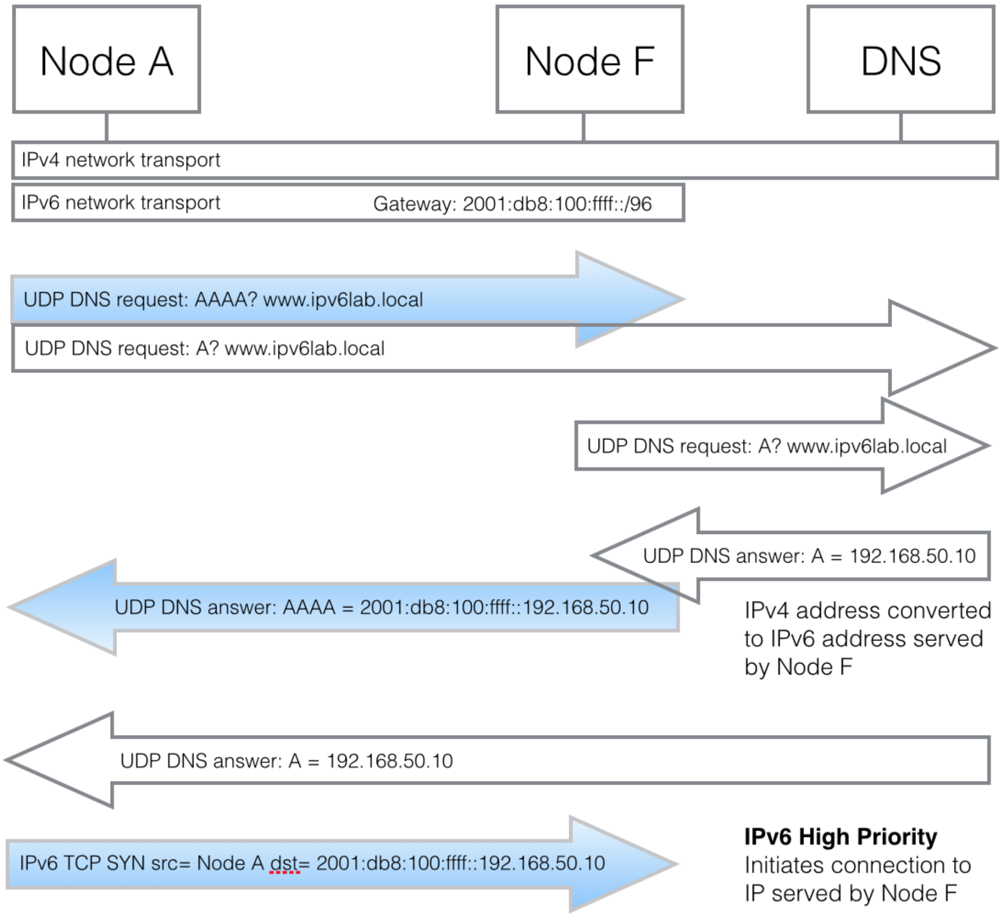

Node A
Node F
DNS
IPv4 network transport
IPv6 network transport
Gateway: 2001:db8:100:ffff::/96
UDP DNS request: AAAA? www.ipv6lab.local
UDP DNS request: A? www.ipv6lab.local
UDP DNS request: A? www.ipv6lab.local
UDP DNS answer: A = 192.168.50.10
UDP DNS answer: AAAA = 2001:db8:100:ffff::192.168.50.10
IPv4 address converted to IPv6 address served by Node F
UDP DNS answer: A = 192.168.50.10
IPv6 TCP SYN src= Node A dst= 2001:db8:100:ffff::192.168.50.10
IPv6 High Priority
Initiates connection to IP served by Node F

Figure 32. DNS translation from IPv4 to IPv6

5.3.2 Mitigation of IPv6 first hop attacks

Deploying an implementation of IPv6 in the enterprise network will reduce the ability of an attacker to leverage attack methods which prioritize traffic over the IPv4 protocol. By deploying an IPv6 network, the native IPv6 network available to the node will take preference over any of the tunnelled networks, reducing the chance that the traffic will be forwarded to the attacking node.

As identified in RFC 6555 (Yourtchenko & Wing, 2012, sec.3.2), an common alternative strategy is to disable IPv6 in environments where IPv6 is not deployed and may in certain operating systems improve the user experience. The protocol deployment can be aligned to the enterprise IPv6 deployment. This is described and documented by Atik Pilihanto, where he recommends disabling the IPv6 stack of devices and servers that do not require IPv6 (Pilihanto, 2011).

Disabling IPv6 on the operating system does however not prevent the Operating systems from running an IPv6 stack and therefore, tunnelling may still be possible from devices that only have IPv4 enabled on their interfaces.

Certain precautions are necessary to reduce the risk of spoofed Router advertisements in an enterprise where an IPv6 network is deployed. On Cisco switching hardware the following configuration can be enabled on the access layer's port configurations. Implementation of the RA guard feature is simple, and applied to the standard interface from which that RA is not expected .

```
Device# configure terminal
Device(config)# interface [INT]
Device(config-if)# switchport mode access
Device(config-if)# ipv6 nd raguard
```

This will implement the IPv6 RA-Guard feature as defined in RFC6105 (Levy-Abegnoli, Van de Velde, Popoviciu & Mohacsi, 2011). Although it is easily bypassed by a determined attacker, it provides a necessary first layer of defence as part of a holistic approach to First Hop Security (Gont, 2011).

The following policy would then be applied to all network switching ports on the access layer that do not provide connectivity to the routing infrastructure in the environment.

```
Device(config-ra-guard)# device-role host
```

Once the network port has been configured as a host role, it will disregard all router advertisements and redirect messages.

As documented by Fernando Gont (2011): in order to bypass the RA guard feature, one has to simply use fragmentation headers to prevent the router from classifying the router advertisement. To prevent Router Advertisements that are obfuscated by the use of fragmented packets, one would need to prevent ICMPv6 packets that are classified without a determined transport layer. This requires port based access control lists that can match and validate packets received from the interface. An ENDPOINT_NODE access list is created that would deny the packets not expected from the end point, which includes any ICMP type 134 router advertisements (discussed in section 2.5) as well as any packets that the switch cannot determine the transport type associated to them.

```
switch(config)# ipv6 access-list ENDPOINT_NODE
switch(config-ipv6-acl)# 101 deny icmp any any router-advertisement
switch(config-ipv6-acl)# 102 deny ipv6 any any undetermined-transport
switch(config-ipv6-acl)# 200 permit ipv6 any any
switch(config-ipv6-acl)# interface g0/1
switch(config-if)# ipv6 traffic-filter ENDPOINT_NODE in
```

The ENDPOINT_NODE access-list is then applied to ingress traffic on end-point switch ports and applied to all packets from the end point. It was found that the implementation on the Cisco devices are still inconsistent, as some switches will return errors when this is configured, but will continue to function correctly (Rey, 2013b).

In the same way that Router Advertisements are susceptible to spoofing attacks, Dynamic Host Configuration Protocol in IPv6 can also be spoofed to introduce inconsistent configuration. Using the ENPOINT_NODE access list unauthorized and erroneous DHCPv6 server responses to other hosts on the network segment are prevented. This is matched by filtering source UDP traffic that originate from port 547 and is destined to port 546.

```
switch(config)# ipv6 access-list ENDPOINT_NODE
switch(config-ipv6-acl)# 103 deny udp any eq 547 any eq 546
```

Using the Port based ACLs will provide improved First Hop protection to the network and is the implementation which is recommended as part of the switch baseline configuration.

The draft document, “SAVI Solutions for DHCP” being developed by the Internet Engineering Task Force discusses Source Address Validation Improvement (SAVI) and describes a procedure whereby a SAVI device will listen to the DHCP binding in the network layer, in conjunction with suitable binding anchors (Bi, Wu, Yao & Baker, 2014). This binding is then used to validate traffic and prevent spoofing and interception of addresses on the network. This SAVI procedure has only been developed to focus on the *stateful* DHCPv6 while stateless DHCPv6 remains out of the scope of the standard.

Unlike the IPv4 and ARP protection that is available on the Cisco platform, the IPv6 protection feature set does not currently permit one to log or deactivate the offending port. If an offending device is attempting to bypass the controls on the first hop protection, there will be no log or alert that will signal the presence of an attack.

The low end switches such as the Cisco Catalyst 2960 Plus Series SI and the SME market switches do not support any IPv6 first hop defence configuration, and are widely deployed by enterprises to the workstation access layer. This prevents the deployment of the security mitigations such as RA guard until the device update cycle is completed.

5.3.3 Tunneling interception attacks

There are a number of IPv6 transitional tunnelling and translation protocols that are available to provide automated IPv6 connectivity i.e. 6to4, NAT-PT (decremented), Teredo and Intra-site Automatic Tunnel Addressing Protocol (ISATAP) in an IPv4 only environment. Teredo, as defined in RFC 4380 (Huitema, 2006), is one of the examples of tunnelling protocol that we will present in a case study of how the IPv6 tunnels can be used to create a cover network in an enterprise.

The rationale for selecting the IPv6 and Teredo tunnelling service stems from the wide adoption by Microsoft as default functionality on Windows Vista, 7 and 8/8.1 hosts (Palmer, 2013). In Linux, Apple Mac OS X and FreeBSD the Teredo support is provided by optional software in the form of tools such as Miredo[13]. For this reason, the tunnelling services are not implemented by default. If malware infection or other abilities to manipulate Node A are taken into account, deployments of Terendo software to compromised nodes are possible.

Dr James Hoagland from Symantec has completed research into the security aspects of the Teredo service in more detail. He states that it takes into account the implications of the access provided by the IPv6 access (Hoagland, 2007). The focus of this case is on the server spoofing aspects as highlighted in the section *Teredo Service for a Man-in-the-Middle Attack* in RFC 4380 (Huitema, 2006, sec.7.2). Further it takes into consideration the ability to impact a large number of homogenous enterprise PCs though a predictable manner. Dr Hoagland briefly discussed this form of attack, but indicated that the gain

[13] Miredo: Teredo IPv6 tunneling for Linux and BSD - http://www.remlab.net/miredo/

would not be worth the effort. It is argued that as the work-effort of attacks increase in conjunction with the reduction of attack surface in the enterprise, these attacks could become feasible.

The Miredo platform is a functional Teredo client, relay and server package that has been developed by Rémi Denis-Courmont and works on Linux and FreeBSD with a port to Apple Mac OS X.

By combining the process of DNS spoofing and the Teredo server, one can redirect the Teredo service to an unintended destination. This can be achieved by using the DNS spoof tool that is part of the Dsniff toolkit.

```
root@kali:~# dnsspoof -f /etc/dnsspoof.hosts
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.1.20]
192.168.1.10.58505 > 192.168.1.1.53:  26718+ A? teredo.ipv6.microsoft.com
192.168.1.10.63494 > 192.168.1.1.53:  17817+ A? teredo.ipv6.microsoft.com
```

This redirects the Teredo clients' connection to a Teredo server of your choosing. The installation and configuration of a Teredo server that can be used to which connect is included in Appendix A. The Teredo server requires two consecutive globally unicast IP addresses and will provide the gateway to IPv6.

ISATAP provides another tunnel transport that can be used to facilitate traffic redirection in the same way that the Teredo protocol enables it. The DNS of Node A can be poisoned to redirect or impersonate the isatap.clientdomain.local hostname to Node F.

To facilitate the tunnel connection from the ISATAP client Node F will configure an ISATAP tunnel service on the host by creating the necessary interfaces and enable the Router advertisement daemon.

The first step is to create the ISATAP interface on the host using the local IPv4 address (V4ADDR)

```
# ip tunnel add isatap0 mode isatap local [V4ADDR] ttl 64
```

ISATAP generates an IP address for the client by prefixing an IPv6 network [PREFIX] and 0x5efe to Node A's IPv4 address as well as a Link-local with fe80::5efe:[V4ADDR]. In a mixed notation the IPv6 address would look like this: 2001:db8:100:fffe::5efe:192.168.1.1

if the PREFIX was 2001:db8:100:fffe:: and the V4ADDR was 192.168.1.1. We now configure the address on the isatap0 interface and enable it:

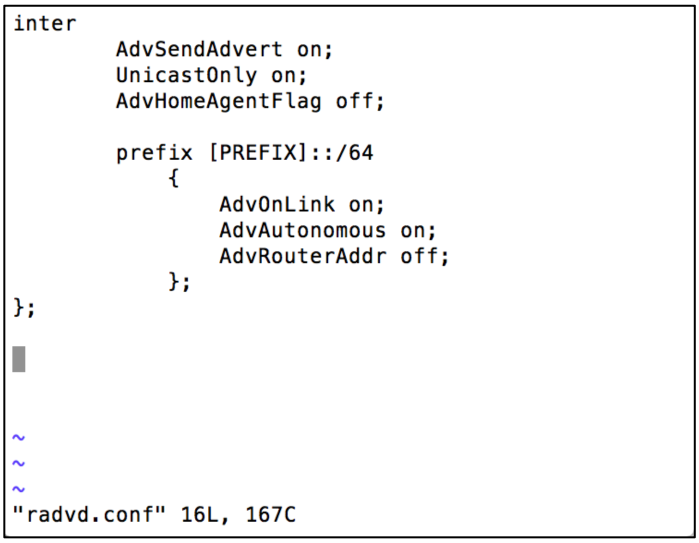
```
# ip addr add [PREFIX]::5efe:[V4ADDR]/64 dev isatap0
# ip link set isatap0 up
```

This will generate a tunnel interface named isatap0 which can be verified with the following command:

```
# ifconfig isatap0
isatap0   Link encap:IPv6-in-IPv4
          inet6 addr: [PREFIX]:5efe::[V4ADDR]/64 Scope:Global
          inet6 addr: fe80::5efe:[V4ADDR]/64 Scope:Link
          UP RUNNING NOARP  MTU:1480  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

The next step would be to install the radvd daemon on Node F. The radvd service provides the Router Advertisements to the network and facilitates the addressing of Node A’s ISATAP interface. The radvd daemon was developed by Reuben Hawkins in 1996 to provide an open sourced Routing advertisement daemon as specified in RFC 2461 (Narten et al., 1998). The download and compilation of the radvd is available in Appendix A.

The `radvd.conf` configuration file in Figure 33 will enable the ISATAP interface functionality and may be configured with additional nuances in the environment.



```
inter
        AdvSendAdvert on;
        UnicastOnly on;
        AdvHomeAgentFlag off;

        prefix [PREFIX]::/64
            {
                AdvOnLink on;
                AdvAutonomous on;
                AdvRouterAddr off;
            };
};

~
~
~
"radvd.conf" 16L, 167C
```

Figure 33. radvd configuration file

With the Teredo and ISATAP tunnel initiation methods, Node F will potentially be able to hijack the traffic of a client using a method similar to the one mentioned in section 5.3.1 whereby NAT64 and DNS64 is used to translate, capture or modify the traffic from the victim to the IPv4 Internet (Hogg & Vyncke, 2009).

5.3.4 Mitigating unmanaged IPv6 tunneling.

Mitigation can be implemented on the client devices as well as the network in order to contain devices that do not conform to enterprise policies.

In an enterprise environment, where IPv6 tunnelling is not required by business, the following mitigating configurations can be implemented to the client nodes that will disable the automatic establishment of tunnels.

Disable Teredo client on Windows XP:

```
C:\Windows> netsh interface ipv6 set teredo disabled
```

Disable Teredo client on Windows 7 (Administrative user):

```
C:\Windows\system32> netsh interface teredo set state type=disabled
```

Disable ISATAP on Windows 7 (Administrative user):

```
C:\Windows\system32> netsh interface isatap set state disabled
```

Disable 6to4 tunnelling on Windows 7 (Administrative user)

```
netsh int ipv6 6to4 set state disabled
```

DNS monitoring can assist in detecting hosts that are not configured to disable the tunnelling protocols as part of monitoring the enterprise environment.

In Windows 2003 or 2008 one can use the Domain Name System Microsoft Management Console to enable the logging of the DNS requests to the server.

Select the DNS option in the Administrative tools and select the properties of the configured DNS server as shown in Figure 34 on Server D.

In the Properties window, select the “Debug Logging” tab that contains the configuration for the DNS activity logging. Select the “Log packet for debugging” and select the options shown in Figure 35, taking note of the file name selected for the logging.

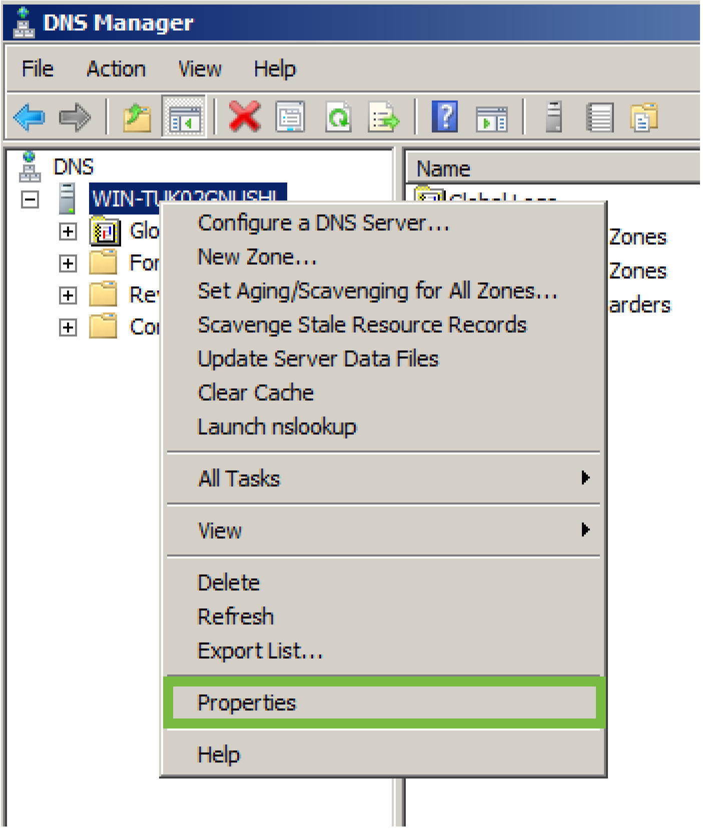
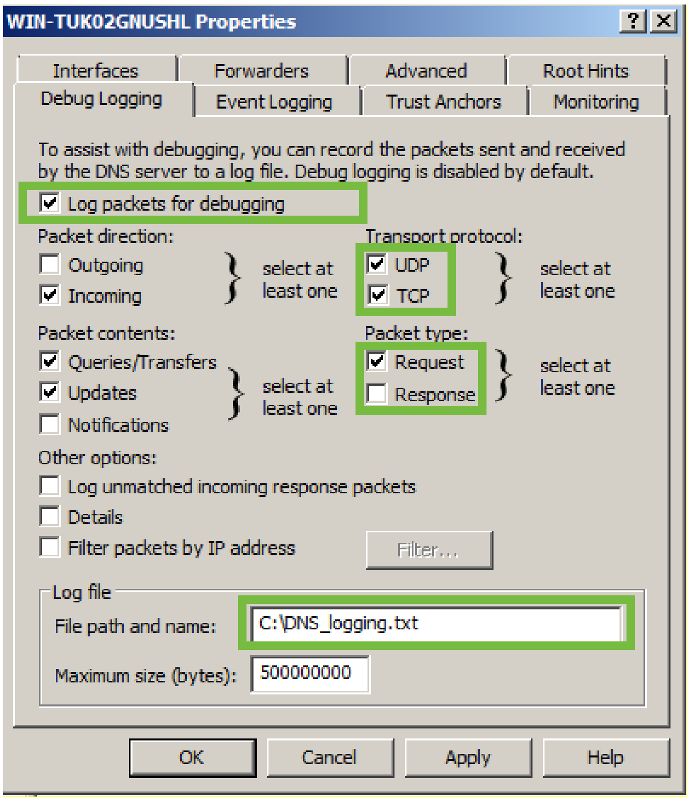


Figure 34. Windows Server DNS management console



To assist with debugging, you can record the packets sent and received by the DNS server to a log file. Debug logging is disabled by default.

☑ Log packets for debugging

Packet direction:
☐ Outgoing
☑ Incoming
} select at least one

Transport protocol:
☑ UDP
☑ TCP
} select at least one

Packet contents:
☑ Queries/Transfers
☑ Updates
☐ Notifications
} select at least one

Packet type:
☑ Request
☐ Response
} select at least one

Other options:
☐ Log unmatched incoming response packets
☐ Details
☐ Filter packets by IP address

Log file
File path and name: C:\DNS_logging.txt
Maximum size (bytes): 500000000

Figure 35. Windows DNS Server - Debug Logging

Once the configuration is complete one can open a command line and execute the following commands to identify potential attempts by Windows clients to contact tunnelling services.

```
type c:\DNS_logging.txt | findstr /R /C:”teredo”
type c:\DNS_logging.txt | findstr /R /C:”6to4”
type c:\DNS_logging.txt | findstr /R /C:”isatap”
```

Not all clients are managed in the environment and therefore additional controls should be implemented to detect tunnelling redirection in the network environment. The following controls can be deployed that will inspect and deny traffic that is associated to tunnelling protocols and provide the hosts attempting the connections.

Tunnelling, as discussed in section 2.9, can present tunnelling indicators such as protocol 41 that is also known as Simple Internet Translation (Warfield, 2003). It can be used by a number of the tunnelling protocols which include the 6over4, ISATAP and 6to4. The tunnelling protocols require configured tunnel peers which translate the encapsulated IPv6 traffic to native IPv6 and may be configured manually or managed dynamically by tunnelling brokers. Monitoring and alerting on this protocol allows one to detect unauthorized tunnelling in the environment and block the use on the perimeter firewall and distribution layer switches.

Blocking protocol 41 on the boundary of the network reduces the potential for unauthorized tunnels to be established into one’s network. This does not prevent all tunnelling protocols, as some such as Teredo uses UDP traffic on port 3544 and can be customized to change port on a manual basis (Sheila et al., 2010; Babiker et al., 2011, p.131). As described in RFC 3068, the IPv4 IP address range 192.88.99.0/24 is associated with the 6to4 relay routers and enables easy deployment into an organisation. This may provide an additional method to initiate a tunnel with the user knowledge.

An access port that will prevent the standard tunnelling would include the following access control statements. This equivalent access list can be deployed to the network perimeter on the client edge router or the firewall. The following configurations occur in the terminal configuration mode of the devices.

The client edge router ACL configuration is applied to Gig0/1, which is the interface that is restricted from tunnel use.

```
Router# ip access-list extended DenyIPv6tun
Router# deny 41 any any log
Router# deny udp any any eq 3544
Router# deny ip 192.88.99.0 0.0.0.255 any
Router# deny ip any 192.88.99.0 0.0.0.255
Router# interface Gig0/1
Router# ip access-group DenyIPv6tun in
```

On the Cisco ASA perimeter firewall, the following access-list is created and applied to the “inside” interface.

```
asafw# access-list extended DenyIPv6tun deny 41 any any
asafw# access-list extended DenyIPv6tun deny udp any any eq 3544
asafw# access-list extended DenyIPv6tun deny ip 192.88.99.0 255.255.255.0
any
asafw# access-list extended DenyIPv6tun deny ip any 192.88.99.0
255.255.255.0
asafw# access-group DetectIPv6 in interface inside
```

By utilising an Intrusion Detection and Prevention device that has the ability inspect the traffic and provide protocol aware signature matching, prevention of certain tunnelling protocols (that are not using standard configuration methods) are possible.

Using the Cisco IPS device, one can prevent detected IPv6 tunnels on the perimeter. The following Cisco IPS signatures identify and detect tunnelling IPv6 traffic.

Table 16. IPv6 IPS tunnel detection signatures

Signature	Traffic detected
1007	**This signature detects tunnelled IPv6 packet** ISATAP 6to4 (RFC 3056) Manually configured tunnels (RFC 4213) IPv6 over GRE Teredo (IPv6) inside UDP MPLS (unencrypted) IPv6 over IPv6
1410	**This signature detects a IPv6 Over MPLS Tunnel**
1405 – 1408	These signatures detects Teredo traffic attributes

The IPS device is able to prevent, log and issue an alert of the traffic attempting to traverse the perimeter. The enterprise should ensure that the tunnelling is only permitted to valid tunnels and that the signatures are configured to deny the traffic by default.

5.4 IPv6 management challenges and recommendations

The technical facets of IPv6 have numerous challenges that infiltrate into the operational management of the Enterprise. By providing the extended addressing space to the local network segments, the following operational challenges are introduced:

1) Network access management;
2) Rogue device detection;
3) Network address attribution management; and
4) Troubleshooting the IPv6 stack.

The research (in this section) is focused on device inventory management in order to create an inventory system that keeps track of the device MAC and the attributes that show the attribute mapping to an IPv6 address.

Using NDP to provide the input to the sensor, a network-monitoring tool has been created that provides a distributed method to monitor the health of the enterprise IPv6 network. The application catalogues the local network devices and performs an alert when there are specific local first hop attacks, and simultaneously it records the IPv6 to MAC bindings received by the neighbor discovery packets.

The following attacks that are currently detected and alerted upon include.

1. Neighbour Advertisement flooding;
2. Neighbour Solicitation flooding;
3. Router advertisement flooding;
4. Inconsistent router injection; and
5. Unexpected vendor connections[14].

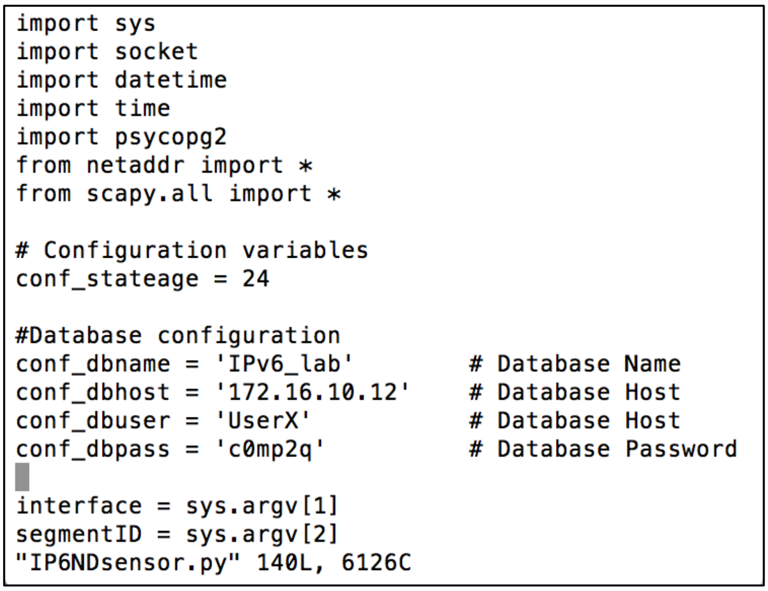
The application is developed using the Scapy packet manipulation library in Python. It provides rapid application development that facilitates packet generation and packet

[14] Identification of a vendor Organizationally Unique Identifier (OUI) that is part of the MAC address, not expected in the environment.

interception. The Psycopg2 database library is used to centralise the results and provide a single store for the monitoring tool.

The IP6NDsensor application works by creating a listener on a specified network segment, and by associating a segmentID to the daemon. The application configuration is currently stored in the header of the application and contains the next configuration variables:

The application creates a database connection to a PostgreSQL, an object-relational database system. The application defines the connection details in the variables conf_dbname, conf_dbhost, conf_dbuser and conf_dbpass. The conf_dbname represents the database name, the conf_dbhost provides the database hostname, the conf_dbuser stores the database username and the conf_dbpass contains the password associated to the username. This will provide the central storage database which will provide distributed access and deployment of the sensors.



```
import sys
import socket
import datetime
import time
import psycopg2
from netaddr import *
from scapy.all import *

# Configuration variables
conf_stateage = 24

#Database configuration
conf_dbname = 'IPv6_lab'        # Database Name
conf_dbhost = '172.16.10.12'    # Database Host
conf_dbuser = 'UserX'           # Database Host
conf_dbpass = 'c0mp2q'          # Database Password

interface = sys.argv[1]
segmentID = sys.argv[2]
"IP6NDsensor.py" 140L, 6126C
```

Figure 36. IP6ND configuration variables

The following command line shows how the application can be executed to monitor the interface and how that interface will be identified and categorised as a segmentID.

```
root@ip6sensor# IP6NDsensor [interface] [segmentID]
```

The application initialises by attempting to import the past twenty-four hours of associations detected so that it does not duplicate currently existing states. The states are stored in the central PostgreSQL database.

5.4.1 Network Solicitation and Router Advertisement attacks

Identification of spoofed and flooding of the Neighbour discovery process is difficult without support by the access layer switching platforms (described in section 5.3.2). By introducing the monitoring of the various layer 2 segments, it will provide us with the ability to identify and classify access requests to the Ethernet layer.

The IP6NDsensor identifies the Neighbour Advertisements and Solicitations by the packet header identification in Scapy. The two header types that are analysed are ICMPv6ND_NS and ICMPv6ND_NA. The standard manner to identify mappings include the source MAC address to source IP address - though we have expanded this to include the Target IP header field which assists in recording association requests.

The database structure that is used to store the data includes the following fields that can be correlated to identify attacks and track devices associations.

```
type            varchar(5)   # Type of request
segmentID       integer      # Segment Identification (eg. VLAN)
macaddr         macaddr      # The associated MAC address
ip6addr         inet         # The associated IPv6 address
update          timestamp    # Timestamp of last update
```

The IP6NDsensor inspects and returns the metadata inspected on the network segment to the central database. The data can then be used to identify devices connected to the associated segment and track the movement of devices from segment to segment.

The type field consists of the following options:

D – NDP RS/RA request with destination mapping

R – NDP RS request for an IP address (reports the tgt field as IP)

S – NDP RA request with source mapping

The sensor also evaluated the packets received to verify whether they include routing information: Routing Prefixes or Routing Information. This is our next topic of discussion.

5.4.2 Network Router Advertisement

The IP6sensor, in conjunction with recording MAC to IPv6 bindings, also analyses and reports on the ICMPv6 routing messages in the network. By inspecting the packets for the

ICMPv6NDOptPrefixInfo and ICMPv6NDOptRouteInfo header information the routing information can be recorded.

This provides us with detailed information of the routing state within an IPv6 network segment and it is stored in the database using the following data fields:

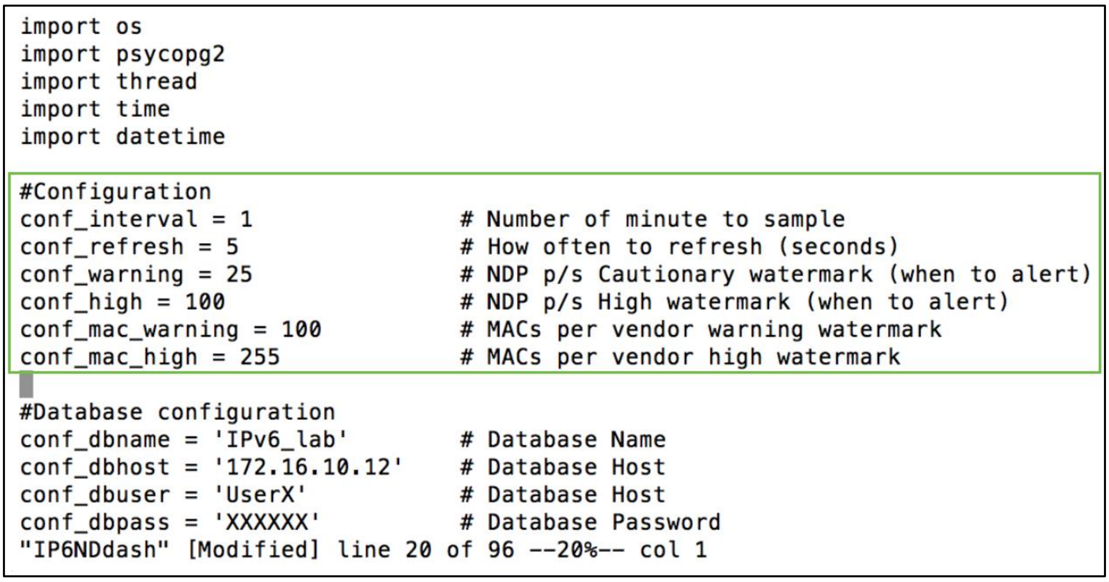
```
type            varchar(5)    # Type of request
segmentID       integer       # Segment Identification (eg. VLAN)
macaddr         macaddr       # The associated MAC address
macOption       macaddr       # The MAC address option presented
ip6addr         inet          # The associated IPv6 address
prefix          cidr          # The route Prefix advertised
update          timestamp     # Timestamp of last update
```

By entering all of the potential routes detected and comparing them to routes that are expected in the production network, one can identify rogue routes that attempt to intercept traffic.

5.4.3 Centralised monitoring

To keep track of the distributed IP6NDsensor sensors in the network, the IP6NDdash application connects to the PostgreSQL database and retrieves and interprets the state of the environment.

The IP6NDdash application is configured with user variables which can be tailored to the environment and the activity in the environment as shown in Figure 37. This will set warning and high watermarks that can be used to initiate a visual or audio alert.



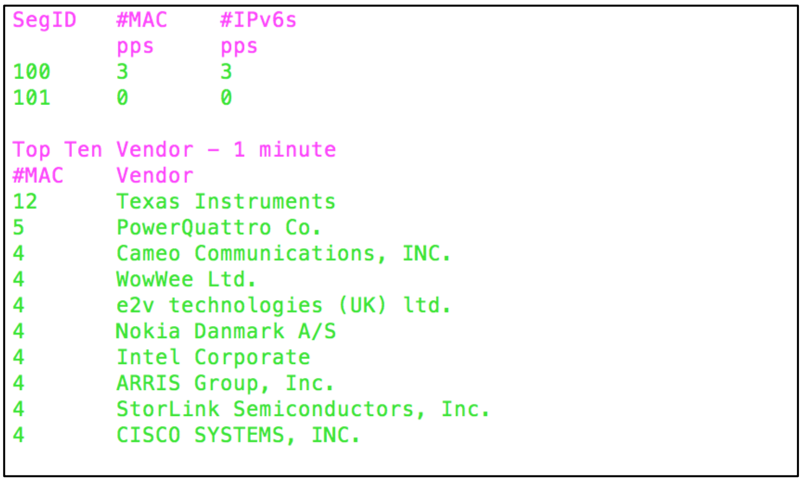
```
import os
import psycopg2
import thread
import time
import datetime

#Configuration
conf_interval = 1               # Number of minute to sample
conf_refresh = 5                # How often to refresh (seconds)
conf_warning = 25               # NDP p/s Cautionary watermark (when to alert)
conf_high = 100                 # NDP p/s High watermark (when to alert)
conf_mac_warning = 100          # MACs per vendor warning watermark
conf_mac_high = 255             # MACs per vendor high watermark

#Database configuration
conf_dbname = 'IPv6_lab'        # Database Name
conf_dbhost = '172.16.10.12'    # Database Host
conf_dbuser = 'UserX'           # Database Host
conf_dbpass = 'XXXXXX'          # Database Password
"IP6NDdash" [Modified] line 20 of 96 --20%-- col 1
```

Figure 37. IP6NDdash configuration variables

The application measures the NDP activity over the sampled interval time, and determines a packet per second indicator that can be used to identify average Neighbour traffic utilization.



```
SegID   #MAC    #IPv6s
        pps     pps
100     3       3
101     0       0

Top Ten Vendor - 1 minute
#MAC    Vendor
12      Texas Instruments
5       PowerQuattro Co.
4       Cameo Communications, INC.
4       WowWee Ltd.
4       e2v technologies (UK) ltd.
4       Nokia Danmark A/S
4       Intel Corporate
4       ARRIS Group, Inc.
4       StorLink Semiconductors, Inc.
4       CISCO SYSTEMS, INC.
```

Figure 38. IP6NDdash example output

The interface of the application is simple and designed to be a functional monitor as shown in Figure 38. This shows a summary of the MAC and IPv6 activity on the monitored segments as well as a review of the devices identified in the network.

The indicators that show that a network attack is when the IPv6 increase over the MAC devices and the ration is not in the region of 1 MAC to 3 IPv6 addresses. Attacks that use spoofed MAC addresses randomize the MAC and therefore the vendor list is also a valuable indicator when an attack is under way.

5.5 Summary

By analysing and testing the case studies identified in this chapter a table of the outcomes are represented in Table 17. Table 15 which was originally proposed has subsequently been updated with the outcomes of the research, and has been amended with the additional controls and attacks that have been identified in the process.

The management of the resource exhaustion attacks have been documented and the impact of these attacks ascertained. By using the recommendations noted, the environment is less likely to be negatively affected by the attacks. It is also found that some of the attacks that have been identified are not as prevalent in the enterprise (we refer here to the NDP cache attack in section 5.2).

The traffic interception attacks that have been part of the case studies are included and the two attack methods have been added to the table. As found with the deployment of First-hop protection on the access layer in section 5.3.2, this attack vector is significantly reduced though malware, and other systems that are on the device may still be able to leverage this traffic exfiltration methods.

Table 17: Research outcomes

Associated protocol	Description	Prevent	Detect
IPv6 Protocol	Optional Header attack - Hop by Hop	Yes	
IPv6 Protocol	Optional Header attack - Atomic	Yes	
IPv6 Protocol	Optional Header attack - Destination header	Yes	
IPv6 Protocol	Fragmentation overlapping and timing attack	Yes	
IPv6 Protocol	Traffic interception – Tunnelling	Yes	
IPv6 Protocol	Traffic interception – NDP	Yes	
NDP (RA 134)	Fake route advertisement – 1	Yes	Yes
NDP (RA 134)	Fake route advertisement – 2	Yes	Yes
NDP (RA 134)	Fake route advertisement – 3	Yes	Yes
NDP (NA136)	Address resolution spoofing – 1		Yes
NDP (NA136)	Address resolution spoofing – 2		Yes
NDP (NA136)	Resource exhaustion	Yes	
DHCPv6	DHCP DUID IAID spoofing	Yes	Yes
DHCPv6	DHCP response spoofing	Yes	Yes
DHCPv6	Client DHCP spoofing		

As the research identified a lack in support on the network technology stack (especially the lower end devices) a monitoring system was developed to provide visibility to the NDP traffic on the network and provide pro-active alerting during a potential attack scenario. The deployment also provided the ability to record asset information between the physical devices and configure the IP addresses. The MAC addresses that are detected on the network are resolved to the vendor, which also gives the administrator the ability to verify the validity of the equipment connected.

The collected information was centrally stored and that provides a dashboard of the segments that the sensors are deployed to. This provides organisations that are in the middle of a technology life cycle or that cannot afford high-end IPv6 supported equipment with a means to monitor and react to IPv6 attacks or malfunctions.

Chapter 6

Conclusion

IPv6 will form part of most enterprise networks in the next few years and therefore the implementation and deployment will become a functional requirement. Whether it will be a social or a business requirement that will drive the adoption forward, network and security practitioners will be forced to provide compatibility for their infrastructure and applications to IPv6 (described in Section 2.1). The attacks that have been identified through the related IPv6 research in Chapter 3 determines how vulnerabilities IPv6 protocol have been identified as well as the work that is being done to reduce the impact to organisations.

In addition to the business and social drivers, the hardware vendors have started providing support for basic network and first hop IPv6 security, but this is yet to be tested under the load of a world wide deployment. In Chapter 3 the protections that are available at the high-end range of network equipment are described, but it is stated that the existing and lower spec devices still lack basic protections.

By deploying IPv6, the enterprise will also reduce the risk of IPv4 tunnel redirection threats which can be exploited (discussed in section 5.3). Deploying the First Hop protections in the supported Cisco platform will provide preventative controls that will reduce the misuse of the NDP and will provide protection to the access layer.

6.1 Brief review of the document

Chapter 2 provides the foundation of research that this Thesis was based upon. A detailed view of the problems exposed by the lack of address space and functionality in the IPv4 network is provided. In conjunction to the growth of existing environment and network expansion, disrupting technologies such as the Internet of Things is presenting unprecedented growth in network and security infrastructure.

In conjunction to describing the problems, **Chapter 2** provides the technical introduction to the IPv6 technology, illustrating the addressing and functional operational changes, including NDP. The various IPv6 deployment methodologies are expanded upon and the benefits and disadvantages are identified.

Chapter 3 identifies some of the existing research in the IPv6 environment. The impact of IPv6 functionality is described on the Ethernet layer as well as the network layer that may impact the network. The changes in the IPv6 protocol also introduces altered attack vectors such as resource exhaustion attacks that have changed from IPv4 limited attributes, to system and infrastructure compute resources.

The research laboratory environment is described in Error! Reference source not found. that relates to the scenarios tested in **Chapter 5**. By using the research in **Chapter 3** some case studies are tested to validate impact and potential tunneling attacks that may provide cover channels to an IPv4 network are discussed. A lack of controls in lower range network equipment is identified, and a solution that provides centralized NDP monitoring and alerting to Ethernet segments.

6.2 Research outcomes

By reviewing the original research questions we evaluate what the outcome of the associate research was for each of the goals stated in **Chapter 1**. The outcomes are tied to the research conducted in this document through the case studies presented.

6.2.1 Determine whether the average enterprise network access layer device can support and manage IPv6 equipment securely

As part of this research the Cisco access layer equipment was evaluated (section 5.3.1) as a means of first hop attack mitigation. It was found that although the vendors have technical mitigations available on the majority of their SME and enterprise equipment, the controls are not implemented by default and are trivial to bypass by using publically available IPv6 attack toolkits. The lack of the sufficiently robust protection which is required by the implementation of additional controls in the form of port access control lists (PACL) provides stronger protection. Unfortunately the PACL functionality is only available in the higher end enterprise equipment and therefore additional research was undertaken to determine how monitoring would be able to provide visibility to the access layer.

Implementation of network routing devices that can provide protection to IPv6 tunnelling over IPv4 was discussed in section 5.3.3. This utilised standard IPv4 access lists as the transport is still on the IPv4 protocol and therefore the controls are well established. Although prevention for tunnelling with indicators such as protocol 41 is easily implemented, encrypted and obfuscated tunnelling protocols are available which, in turn, complicates the detection and prevention. Intrusion prevention technology provides an additional method to prevent encapsulated traffic through deeper packet inspection and packet signature matching.

Vendor technology which provides required IPv6 safeguards is available and should be part of the criteria in the selection of technology in the network and security life cycle.

6.2.2 Should enterprise organisations adopt IPv6 in the near future?

The benefits of deploying IPv6 into the enterprise will include technical aspects, as discussed in Chapter 2, but soon the benefits will shift into the business space. This will provide enterprises with a strategic advantage in network connectivity which (as discussed in section 2.1.5) will increase the potential value to a business. The Internet connectivity to the IPv4 exhausted regions will soon also require IPv6 to provide end-to-end connectivity based on the currently dwindling IPv4 address space (section 2.1.3).

The introduction of IPv6 is inevitable if we take into consideration the ecosystem growth described in section 2.1.1 not overlooking the flood of new devices that require persistent connectivity. Although the implementation of IPv6 will come with unknown complications, the time is right to start wide spread enterprise adoption. This will allow continued growth and innovation in the network and enterprise business. By using any one of the phased deployment approaches for IPv6 described in sections 2.8, 2.9 and 2.10, one can provide a low impact introduction to the protocol.

6.2.3 Does current IPv6 implementations introduce unacceptable risk into the Enterprise?

Although not all enterprise environments have equipment that provides the IPv6 protection necessary to safeguard the organisation, there are compensating systems such as the IP6NDsensor (section 5.4.3). The IP6NDsensor and IP6NDdash can provide a compensating monitoring solution (described in section 5.4) which provides visibility into the Ethernet (layer 2) environment. Monitoring does not provide protection but rather a detection of issues; visibility into the NDP operations; and insight into the health of the environment. Utilising the tool will also provide network administrators with a central repository of IPv6 to MAC bindings with visibility into the environments vendors and the movement of the devices in the network.

As IPv6 is introduced into the enterprise further hardware, protocol and implementation vulnerabilities will be identified and these will need to be remediated in a manner equivalent to the growth path that IPv4 followed. Further research is required to expand the monitoring and trend alerting on interfaces in the network in a lightweight manner. This will, in conjunction to the increased support for IPv6 on hardware, provide visibility, alerting and protection of the environment. System and device IPv6 protections should be enabled by default and the configuration parameters should be identified.

Enterprise organisations will have to identify the benefits and restrictions to deploying IPv6 in their own environment in conjunction to the state of their technology life cycle. The current protocol support available in enterprise equipment in conjunction to the ability to deploy compensating solutions in environments that lack the full support indicates that IPv6 deployments now pose a manageable risk to organisations.

6.2.4 Closing

The problem statement, shown in section 2.1, can be inferred as a statement of advantage for the adoption of the IPv6 protocol. The problems that face organisations with the introduction of IPv6 will transform in future to form part of the benefits for adoption by providing improved network capacity in conjunction with the additional network devices and services that will be facilitated by it. Secure deployment is now possible as we introduce the protocol, and it will provide us with the platform to apply research to the use of the expanded address space and integration to software defined networking.

6.3 Future Work

Future work that can build upon this research would include an analysis of the impact that IPv6 first hop attacks would present to the new encapsulated transport mediums that distribute layer 2 segments over large geographic spaces. As these transports become more dynamic and aligned in nature to the data centre orchestration layer, the impact that IPv6 will have on existing Software Defined Networking implementations will need to be explored.

Implementation of the lab environment was facilitated with the use of virtualization technology and therefor performance based testing was lacking. To provide improved insight into the physical platforms and performance additional testing can be conducted on physical devices in a non-shared environment.

The expansion of the IP6ND tools, discussed in section 5.4, can be developed to use next generation ‘nosql’ databases[15], which will enable the application to scale to every segment of a production enterprise network. The Kibana analysis engine available from Elasticsearch will be able to enable powerful analytics and visualisation.

[15] Such as Elasticsearch, Distributed restful search and analytics - http://www.elasticsearch.org

REFERENCES

All About Market Research, 2014a. Internet Users in Africa @ www.internetworldstats.com. Available at: http://www.internetworldstats.com/stats1.htm [Accessed October 15, 2014].

All About Market Research, 2014b. Internet World Stats @ www.internetworldstats.com. Available at: http://www.internetworldstats.com/ [Accessed February 22, 2013].

Alonso, C., 2013. Fear the Evil FOCA - Attacking Internet Connections with IPv6. In *DefCon 21*. Available at: https://www.defcon.org/images/defcon-21/dc-21-presentations/Alonso/DEFCON-21-Alonso-Fear-the-Evil-FOCA-Updated.pdf [Accessed February 14, 2014].

Arkko, J., Kempf, J., Zill, B. & Nikander, P., 2005. SEcure Neighbor Discovery (SEND). IETF. RFC 3971. Available at: http://tools.ietf.org/html/rfc3971.

Atlasis, A., 2012. Attacking IPv6 implementation using fragmentation. In *Black Hat Europe*. Available at: https://media.blackhat.com/bh-eu-12/Atlasis/bh-eu-12-Atlasis-Attacking_IPv6-Slides.pdf [Accessed July 20, 2013].

Atlasis, A., 2013. Fragmentation Overlapping Attacks against IPv6. In *Troopers 2013*. Available at: https://www.troopers.de/wp-content/uploads/2013/01/TROOPERS13-Fragmentation_Overlapping_Attacks_Against_IPv6_One_Year_Later-Antonios_Atlasis.pdf [Accessed July 20, 2014].

Aura, T., 2005. Cryptographically Generated Addresses (CGA). IETF. RFC 3972. Available at: http://tools.ietf.org/html/rfc3972.

Babiker, H., Nikolova, I. & Chittimaneni, K.K., 2011. Deploying IPv6 in the Google Enterprise Network . Lessons learned . In *Large Install System Administrator Conference*. Usenix. Available at: https://www.usenix.org/legacy/event/lisa11/tech/full_papers/Babiker.pdf [Accessed June 28, 2014].

Baker, F., Li, X., Bao, C. & Yin, K., 2011. Framework for IPv4/IPv6 Translation. IETF. RFC 6411. Available at: http://tools.ietf.org/pdf/rfc6144.pdf.

Bi, J., Wu, J., Yao, G. & Baker, F., 2014. draft-ietf-savi-dhcp-29 - SAVI Solution for DHCP. Available at: https://tools.ietf.org/html/draft-ietf-savi-dhcp-29.

Biondi, P., 2007. IPv6 Routing Header Security. In *CanSecWest*. Vancouver. Available at: http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf [Accessed February 10, 2014].

Blokzijl, R., 2009. IPv4 Header vs IPv6 Header. *RIPE NCC Roundtable Meeting*. Available at: http://www.ripe.net/ripe/meetings/roundtable/february-2009/RobBlokzijlroundtable2009Rob2.pdf [Accessed September 14, 2013].

Bradner, S. & Paxson, V., 2000. IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers. IETF. RFC 2780. Available at: http://tools.ietf.org/html/rfc2780.

Brocade, 2014. The Effortless Network : HyperEdge Architecture for the Campus Network. Available at: http://www.brocade.com/downloads/documents/white_papers/brocade-effortless-network-wp.pdf [Accessed October 17, 2014].

Bush, R. & Smith, P., 2010. prop-088-v001 @ www.apnic.net. Available at: https://www.apnic.net/policy/proposals/prop-088/prop-088-v001.txt [Accessed March 5, 2014].

Carpenter, B.E., 1999. Transmission of IPv6 over IPv4 Domain without Explicit Tunnels. IETF. RFC 2529. Available at: http://tools.ietf.org/html/rfc2529.

Carpenter, B.E. & Moore, K., 2001. Connection of IPv6 Domains via IPv4 Clouds. IETF. RFC 3056. Available at: http://tools.ietf.org/html/rfc3056.

Carrell, J.L., 2013. IPv6 Security Assessment Tools and Infrastructure mitigation. In *Sharkfest*. Available at: http://sharkfest.wireshark.org/sharkfest.13/presentations/SEC-03_IPv6-Security-Assessment-Tools-and-Infrastructure-Mitigation_Jeff-Carrell.pdf [Accessed June 6, 2014].

Carter, E., 2011. ICMP and Security in IPv6. *Cisco Blog > Security*. Available at: http://blogs.cisco.com/security/icmp-and-security-in-ipv6/ [Accessed February 8, 2014].

Cho, Y.-C. & Pan, J.-Y., 2013. Vulnerability assessment of IPv6 websites to SQL injection and other application level attacks. *TheScientificWorldJournal*, 2013.

Choudhary, A.R. & Sekelsky, A., 2010. Securing IPv6 network infrastructure: A new security model. In *2010 IEEE International Conference on Technologies for Homeland Security (HST)*. IEEE. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5654971 [Accessed November 25, 2014].

Chris, V., 2013. Google Announces 1B Total Android Activations, Names Next Version "KitKat" @ techcrunch.com. Available at: http://techcrunch.com/2013/09/03/google-announces-1b-total-android-activations-names-next-version-kitkat/ [Accessed February 22, 2014].

Cisco, 2008. Enterprise Campus 3.0 Architecture : Overview and Framework. Available at: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/campover.html [Accessed June 10, 2013].

Cisco, 2007. High Availability Campus Network Design — Routed Access Layer using EIGRP or OSPF. Available at: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/routed-ex.html [Accessed July 14, 2014].

Cisco Systems Inc, 2013. 640-822 ICND1 @ www.cisco.com. Available at: http://www.cisco.com/web/learning/exams/list/icnd1.html [Accessed August 29, 2014].

Cisco Systems Inc, 2010a. Catalyst 2960 and 2960-S Switch Software Configuration Guide. Available at: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960.pdf [Accessed September 14, 2014].

Cisco Systems Inc, 2010b. Overlay Transport Virtualization for Geographically Dispersed Virtual Data Centers : Improve Application Availability and Portability. Available at: http://www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-series-switches/solution_overview_c22-574939.pdf [Accessed October 19, 2014].

Cisco Systems Inc, 2007. *Performance-Comparison Testing of IPv4 and IPv6 Throughput and Latency on Key Cisco Router Platforms*, Available at: http://www.cisco.com/web/strategy/docs/gov/IPv6perf_wp1f.pdf [Accessed October 8, 2014].

Conta, A. & Deering, S.E., 1998. Generic Packet Tunneling in IPv6 Specification. IETF. RFC 2473. Available at: http://tools.ietf.org/html/rfc2473.

Convery, S., 2004. IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation. Available at: http://www.seanconvery.com/v6-v4-threats.pdf [Accessed March 22, 2013].

Cooper, I., Tomlinson, G. & Melve, I., 2001. Internet Web Replication and Caching Taxonomy. IETF. RFC 3040. Available at: http://tools.ietf.org/html/rfc3040.

Davies, E.B., Krishnan, S. & Savola, P., 2007. IPv6 Transition/Coexistence Security Considerations. IETF. RFC 4942. Available at: http://tools.ietf.org/html/rfc4942.

Davies, E.B. & Mohacsi, J., 2007. Recommendations for Filtering ICMPv6 Messages in Firewalls. IETF. RFC 4890. Available at: http://tools.ietf.org/html/rfc4890.

Deering, S.E. & Hinden, R.M., 1995. Internet Protocol, Version 6 (IPv6) Specification. IETF. RFC 1883. Available at: http://tools.ietf.org/html/rfc1883.

Deering, S.E. & Hinden, R.M., 1998. Internet Protocol, Version 6 specification. IETF. RFC 2460. Available at: http://www.ietf.org/rfc/rfc2460.txt.

Deering, S.E. & Mogul, J., 1990. Path MTU Discovery. IETF. RFC 1191. Available at: http://tools.ietf.org/html/rfc1191.

Degen, S., Holtzer, A., van der Kluit, B., Schotanus, H., van der Oije, H.S., Bartels, D.-J., van Ramesdonk, M., de Groot, G.J., Kollee, F., Keuper, D., Stols, T., Ottow, C., van der Bij, G., Mune, C. & Spruyt, A., 2014. Testing the security of IPv6 implementations. In Nederland: Dutch Ministry of Economic Affairs. Available at: https://www.tno.nl/downloads/testing_the_security_of_IPv6_implementations.pdf [Accessed May 20, 2014].

Droms, R., Bounds, J., Volz, B., Lemon, T., Perkins, C.E. & Carney, M., 2003. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). IETF. RFC 3315. Available at: https://tools.ietf.org/html/rfc3315.

Duncan, J., 2012. IPv6 Secure Neighbor Discovery (SeND) and CGA. In *Rocky Mountain IPv6 Task Force*. Denver Colorado. Available at: http://www.rmv6tf.org/wp-content/uploads/2012/11/IPv6_SeND_PPT1.pdf [Accessed April 19, 2013].

Durdağı, E. & Buldu, A., 2010. IPV4 / IPV6 security and threat comparisons. *Procedia Social and Behavioral Sciences*, 2.

Egevang, K.B. & Francis, P., 1994. The IP Network Address Translator (NAT). IETF. RFC 1631. , (January 1993). Available at: http://tools.ietf.org/html/rfc1631.

El-kadri, N. & Jegatheesan, S., 2013. Privacy and Security in IPv6. Available at: http://arxiv.org/pdf/1305.3212.pdf [Accessed October 22, 2014].

Evans, K.S., 2008. Memorandum for the Chief Information Officers. Available at: http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-22.pdf [Accessed March 14, 2014].

Ferguson, P. & Senie, D., 2000. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. IETF. RFC 2827. Available at: http://tools.ietf.org/html/rfc2827.

Friedewald, M. & Raabe, O., 2011. Ubiquitous computing: An overview of technology impacts. *Telematics and Informatics*, 28(2). Available at: http://linkinghub.elsevier.com/retrieve/pii/S0736585310000547 [Accessed February 22, 2014].

Friedl, S., 2005. An Illustrated Guide to IPsec. *Steve Friedl's Unixwiz.net Tech Tips*. Available at: http://www.unixwiz.net/techtips/iguide-ipsec.html [Accessed February 16, 2014].

Friess, O.V.& P., 2011. *Internet of Things - Global Technological and Societal Trends From Smart Environments and Spaces to Green ICT*, River Publishers.

Geers, K., 2008. Cyberspace and the Changing Nature of Warfare. In *Black Hat Japan*. Japan: Blackhat. Available at: http://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Geers/BlackHat-Japan-08-Geers-Cyber-Warfare-Whitepaper.pdf.

Gilligan, R.E. & Nordmark, E., 2005. Basic Transition Mechanisms for IPv6 Hosts and Routers. IETF. RFC 4213. Available at: http://tools.ietf.org/html/rfc4213.

Gilligan, R.E. & Nordmark, E., 1996. Transition Mechanisms for IPv6 Hosts and Routers. IETF. RFC 1933. Available at: http://tools.ietf.org/html/rfc1933.

Gilligan, R.E. & Nordmark, E., 2000. Transition Mechanisms for IPv6 Hosts and Routers. IETF. RFC 2893. Available at: http://tools.ietf.org/html/rfc2893.

Gont, F., 2011. draft-gont-v6ops-ra-guard-evasion-01 - IPv6 Router Advertisement Guard (RA-Guard) Evasion. Available at: https://tools.ietf.org/html/draft-gont-v6ops-ra-guard-evasion-01 [Accessed October 10, 2014].

Gont, F., 2013. Processing of IPv6 “Atomic” Fragments. IETF. RFC 6946. Available at: http://tools.ietf.org/html/rfc6946.

Grossetete, P., Popoviciu, C. & Wettling, F., 2008. *Global IPv6 Strategies: From business analysis to operational planning* 1st ed. P. Kanouse, ed., Cisco Press.

Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G. & Williams, T., 2011. *Gray Hat Hacking* 3rd ed. M. Baucom, ed., New York: McGraw-Hill Education.

Hauser, V., 2005. Attacking the IPv6 Protocol Suite. In *PacSec Applied Security conference*. Tokyo: The Hacker’s Choice. Available at: https://www.thc.org/papers/vh_thc-ipv6_attack.pdf [Accessed November 6, 2012].

Van Heerden, R.P., Bester, I.M. & Burke, I.D., 2013. A review of IPv6 security concerns. In *IWSP 2013*. Pretoria. Available at: http://www.iwsp.ukzn.ac.za/index.php?option=com_content&view=article&id=86&Itemid=77 [Accessed March 19, 2013].

Hinden, R.M. & Deering, S.E., 2003. Internet Protocol Version 6 (IPv6) Addressing Architecture. IETF. RFC 3513. Available at: http://tools.ietf.org/html/rfc3513.

Hinden, R.M. & Deering, S.E., 2006. IP Version 6 Addressing Architecture. IETF. RFC 4291. , 6. Available at: http://tools.ietf.org/html/rfc4291.

Hinden, R.M. & Haberman, B., 2005. Unique Local IPv6 Unicast Addresses. IETF. RFC 4193. Available at: http://tools.ietf.org/html/rfc4193.

Hoagland, J., 2007. *The Teredo Protocol : Tunneling Past Network Security and Other Security Implications*, Cupertino, CA. Available at: http://www.symantec.com/avcenter/reference/Teredo_Security.pdf [Accessed February 5, 2014].

Hogg, S., 2007. IPv6 Security. In *Rocky Mountain Information Security Conference*. Denver, Colorado: Global Technology Resources Inc.

Hogg, S. & Vyncke, E., 2009. *IPv6 Security* J. Karpenko & D. Miller, eds., Indianapolis: Cisco Press.

Hollingsworth, T., 2011. What’s The Point of NAT66? @ networkingnerd.net. *The Networkin Nerd*. Available at: http://networkingnerd.net/2011/12/01/whats-the-point-of-nat66/ [Accessed September 8, 2014].

Huawei, 2011. Huawei One Net Campus Network Solution. Available at: http://www.telephorum.org/teledocs/w/images/b/b1/Huawei_One_Net_Campus_Network_Solution.pdf [Accessed October 5, 2014].

Huitema, C., 2006. Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs). IETF. RFC 4380. Available at: http://tools.ietf.org/html/rfc4380.

Huitema, C. & Carpenter, B., 2004. Deprecating Site Local Addresses. IETF. RFC 3879. Available at: http://tools.ietf.org/html/rfc3879.

Hunt, C., 1997. *TCP/IP Network Administration* 2nd ed. M. Loukides & G. Estabrook, eds., Sebastopol, CA: O'Reilly Media, Inc.

Huston, G., 2012. Bemused Eyeballs: Tailoring Dual Stack Applications for a CGN Environment @ www.potaroo.net. *The ISP Column*. Available at: http://www.potaroo.net/ispcol/2012-05/notquite.html [Accessed August 15, 2014].

Huston, G., 2014. IPv4 Address Report @ www.potaroo.net. Available at: http://www.potaroo.net/tools/ipv4/index.html [Accessed February 21, 2014].

Jankiewicz, E., Loughney, J. & Narten, T., 2011. IPv6 Node Requirements. IETF. RFC 6434. , 1721. Available at: http://tools.ietf.org/html/rfc6434.

Jara, A.J., Ladid, L., Skarmeta, A., Comsoc, I. & Etc, I., 2009. The Internet of Everything through IPv6 : An Analysis of Challenges , Solutions and Opportunities. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications,* 4(3).

Jara, A.J., Varakliotis, S., Skarmeta, A.F. & Kirstein, P., 2013. Extending the Internet of Things to the Future Internet through IPv6 support. *Mobile Information Systems,* 10(1).

Jinmei, T., 2007. IPv6 Stateless Address Autoconfiguration. IETF. RFC 4862. Available at: http://tools.ietf.org/html/rfc4862.

Juniper Networks, 2008. Enterprise Data Center Network Reference Architecture. Available at: http://www.valleytalk.org/wp-content/uploads/2013/03/enterprise-reference-design.pdf [Accessed October 5, 2014].

Kende, M., 2014. *Internet Society Global Internet Report 2014,* Available at: http://www.internetsociety.org/doc/global-internet-report [Accessed February 6, 2014].

Kent, S., 2005. IP Encapsulating Security Payload (ESP). IETF. RFC 4303. Available at: http://tools.ietf.org/html/rfc4303.

Kent, S. & Atkinson, R., 1998a. IP Encapsulating Security Payload (ESP) Status. IETF. RFC 2406. Available at: http://tools.ietf.org/html/rfc2406.

Kent, S. & Atkinson, R., 1998b. Security Architecture for the Internet Protocol Status. IETF. RFC 2401. Available at: http://tools.ietf.org/html/rfc2401.

Kent, S. & Seo, K., 2005. Security Architecture for the Internet Protocol. IETF. RFC 4301. Available at: http://tools.ietf.org/html/rfc4301.

Kitamura, H., 2001. A SOCKS-based IPv6/IPv4 Gateway Mechnism. IETF. RFC 3089. Available at: http://tools.ietf.org/html/rfc3089.

Klein, J., 2012. The Shifting Security Paradigm Scope of the CyberSecurity problem - What is the cost of Cybercrime ? - Number of records compromised ? - Number of Systems / Networks / Applications Compromised ? In *gogoNET LIVE! 3 IPv6 Conference*. Available at: http://gogonetlive.com/pdf/3/joe_klein.pdf.

Kompella, K. & Rekhter, Y., 2007. Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling. IETF. RFC 4761. Available at: http://tools.ietf.org/html/rfc4761.

Kukec, A., Krishnan, S. & Jiang, S., 2011. The Secure Neighbor Discovery (SEND) Hash Threat Analysis. IETF. RFC 6273. Available at: http://tools.ietf.org/html/rfc6273.

Leech, M., 1996. SOCKS Protocol Version 5. IETF. RFC 1928. Available at: http://tools.ietf.org/html/rfc1928.

Levy-Abegnoli, E., Van de Velde, G., Popoviciu, C. & Mohacsi, J., 2011. IPv6 Router Advertisement Guard. IETF. RFC 6105. Available at: http://tools.ietf.org/html/rfc6105.

Lohr, S., 2012. For Impatient Web Users, an Eye Blink Is Just Too Long to Wait @ www.nytimes.com. Available at: http://www.nytimes.com/2012/03/01/technology/impatient-web-users-flee-slow-loading-sites.html [Accessed February 10, 2013].

Longbottom, C., 2012. *Don't sweat assets, liberate them!*, Available at: https://www.t-systems.com/umn/uti/838010_2/blobBinary/Quocirca-April-2012_Maintaining-business-focus.pdf.

Loshin, P., 2004. *IPv6: Theory, Protocol, and Practice* 2nd ed. R. Adams, T. Lilly, & K. Johnson, eds., Morgan Kaufmann Publishers.

Mahalingam, M., Hutt, D.G., Duda, K., Agarwal, P., Kreeger, L., Sridhar, T., Bursell, M. & Wright, C., 2014. VXLAN: A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks. , (October). Available at: http://tools.ietf.org/pdf/draft-mahalingam-dutt-dcops-vxlan-09.pdf.

Manyika, J. & Roxburgh, C., 2011. The great transformer : The impact of the Internet on economic growth and prosperity.

Mcfarland, S., Sambi, M., Sharma, N. & Hooda, S., 2011. *IPv6 for Enterprise Networks,* Cisco Press.

Narayan, S., Tauch, S. & Zealand, N., 2010. IPv4-v6 Transition Mechanisms Network Performance Evaluation on Operating Systems.

Narten, T., Draves, R. & Krishnan, S., 2007. Privacy Extensions for Stateless Address Autoconfiguration in IPv6. IETF. RFC 4941. Available at: http://tools.ietf.org/pdf/rfc3041.pdf.

Narten, T., Nordmark, E. & Simpson, W.A., 1998. Neighbor Discovery for IP Version 6. IETF. RFC 2461. Available at: http://tools.ietf.org/html/rfc2461.

Nichols, K., Blake, S., Baker, F. & Black, D.L., 1998. Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers - rfc2474. Available at: http://tools.ietf.org/html/rfc2474.

Nobile, L., 2012. IPv4 Countdown Plan. In *ARIN XXIX*. Vancouver, BC. Available at: https://www.arin.net/resources/request/ipv4_countdown.html [Accessed November 23, 2013].

Number Resource Organization, 2011. Free Pool of IPv4 Address Space Depleted @ www.nro.net. Available at: http://www.nro.net/news/ipv4-free-pool-depleted [Accessed January 28, 2014].

Number Resource Organization, 2014. Regional Internet Registries @ www.nro.net. Available at: http://www.nro.net/about-the-nro/regional-internet-registries [Accessed February 21, 2014].

Odlyzko, A., 2001. Internet growth: Myth and reality, use and abuse. *Journal of Computer Resource Management*. Available at: http://lambda.csail.mit.edu/~chet/papers/others/o/odlyzko/internet.growth.myth.pdf.

Oliphant, T., 2011. IPv6 Complicates Privacy @ blog.polk.com. *The IHS Automotive Blog*. Available at: http://blog.polk.com/blog/blog-posts-by-therran-oliphant/ipv6-complicates-privacy [Accessed September 7, 2014].

Palmer, C., 2013. Teredo @ Microsoft Present and Future. In *IETF 88*. Redmond, WA: IETF. Available at: http://www.ietf.org/proceedings/88/slides/slides-88-v6ops-0.pdf [Accessed November 20, 2013].

Perkins, C.E., Johnson, D.B. & Arkko, J., 2011. Mobility Support in IPv6. IETF. RFC 6275. Available at: http://tools.ietf.org/html/rfc6275.

Pilihanto, A., 2011. A Complete Guide on IPv6 Attack and Defense. Available at: http://www.sans.org/reading-room/whitepapers/detection/complete-guide-ipv6-attack-defense-33904 [Accessed July 23, 2014].

Podermanski, T., 2011. Security concerns and solutions with IPv6. In *GN3 IPv6 Workshop - Networking without IPv4?* Espoo, Finland: Youtube. Available at: http://www.youtube.com/watch?v=mOuPmaQCYWY [Accessed December 12, 2014].

Postel, J., 1981. Internet Protocol. IETF. RFC 791. Available at: http://tools.ietf.org/html/rfc791.

Ramakrishnan, K.K., Floyd, S. & Black, D.L., 2001. The Addition of Explicit Congestion Notification (ECN) to IP. IETF. RFC 3168. Available at: http://tools.ietf.org/html/rfc3168.

Randall, S. & Tüxen, M., 2007. NAT and SCTP. *Seventieth Internet Engineering Task Force*. Available at: http://www.ietf.org/proceedings/70/slides/behave-5.pdf [Accessed November 1, 2014].

Rekhter, Y., Moskowitz, R.G., Karrenberg, D., de Groot, G.J. & Lear, E., 1996. Address Allocation for Private Internets. IETF. RFC 1918. Available at: http://tools.ietf.org/html/rfc1918.

Rey, E., 2013a. IPv6 Neighbor Cache Exhaustion Attacks – Risk Assessment & Mitigation Strategies, Part 1 @ www.insinuator.net. *Insinuator*. Available at: http://www.insinuator.net/2013/03/ipv6-neighbor-cache-exhaustion-attacks-risk-assessment-mitigation-strategies-part-1/ [Accessed August 6, 2014].

Rey, E., 2013b. Some more Notes on RA Guard Evasion and "undetermined-transport" @ www.insinuator.net. Available at: http://www.insinuator.net/2013/04/some-more-notes-on-ra-guard-evasion-and-undetermined-transport/ [Accessed September 16, 2014].

RIPE, 2014. ripe-606 - IPv4 Address Allocation and Assignment Policies for the RIPE NCC Service Region. Available at: http://www.ripe.net/ripe/docs/ripe-606 [Accessed February 24, 2014].

RIPE NCC, 2014. Policy Proposal, Abandoning the Minimum Allocation Size for IPv4 @ www.ripe.net. Available at: http://www.ripe.net/ripe/policies/proposals/2014-01 [Accessed March 28, 2014].

Saini, K., 2011. *Squid Proxy Server 3.1, Beginners's Guide* S. Cullington et al., eds., Packt Publishing Ltd.

Sheila, F., Graveman, R. & Rooks, M., 2010. Guidelines for the Secure Deployment of IPv6. *NIST Special Publication*, (800-119).

Simpson, W., 2007. Neighbor Discovery for IP version 6 (IPv6). IETF. RFC 4861. Available at: http://tools.ietf.org/html/rfc4861.

Skjesol, T., Sydskjør, R., Lillebrygfjeld, E. & Bøe, G., 2013. *Recommendations for IPv6 addressing plan for the HE sector*, Norway. Available at: http://services.geant.net/cbp/Knowledge_Base/Campus_Networking/Documents/gn3-na3-t4-ufs_137.pdf [Accessed August 20, 2014].

Small, J., 2013. IPv6 Attacks and Countermeasures. In *Rocky Mountain IPv6 Task Force*. Denver, Colorado: CDW Advanced Technology Services. Available at: http://www.rmv6tf.org/wp-content/uploads/2013/04/5-IPv6-Attacks-and-Countermeasures-v1.2.pdf [Accessed April 28, 2014].

Smith, A., 2013. *Cell Internet Use 2013*, Washington, D.C. Available at: www.pewresearch.org [Accessed September 8, 2013].

Sotillo, S., 2006. *IPv6 Security Issues*, Greenville, NC. Available at: http://www.researchgate.net/publication/228869792_IPv6_Security_Issues/file/3deec5166e61ed0f33.pdf [Accessed August 12, 2013].

Spirgeon, C.E. & Joann, Z., 2014. *Ethernet: The Definitive Guide* 2nd ed., Sebastopol, CA: O'Reilly.

Srisuresh, P. & Egevang, K.B., 2001. Traditional IP Network Address Translator (Traditional NAT). IETF. RFC 3022. Available at: http://tools.ietf.org/html/rfc3022.

Srisuresh, P. & Holdrege, M., 1999. IP Network Address Translator (NAT) Terminology and Considerations. IETF. RFC 2663. Available at: http://tools.ietf.org/pdf/rfc2663.pdf.

Templin, F.L., Gleeson, T., Talwar, M. & Thaler, D., 2005. RFE 4214 - Intra-Site Automatic Tunnel Addressing Protocol (ISATAP). Available at: http://tools.ietf.org/html/rfc4214.

Templin, F.L., Gleeson, T. & Thaler, D., 2008. Intra-Site Automatic Tunnel Addressing Protocol (ISATAP). IETF. RFC 5214. Available at: http://tools.ietf.org/html/rfc5214.

Tesar, J., 2012. Intrusion Prevention System. In *Cisco Club 2012*. Cisco Systems Inc. Available at: http://ftp.cisco.cz/Seminare/2011-ExpoClub/2012-03-29-IPS-jitesar/IPS_jitesar.pdf.

Thomson, S. & Narten, T., 1998. RFC 2462 - IPv6 Stateless Address Autoconfiguration. Available at: http://www.ietf.org/rfc/rfc2462.txt.

Threat, I.-I. & Miller, D., 2004. IPv6- IPv4 Threat Comparison v1.0. In *NANO 31*. Available at: https://www.nanog.org/meetings/nanog31/presentations/miller.pdf.

T-Mobile, 2014. T-Mobile IPv6 is Here and Now. Available at: https://sites.google.com/site/tmoipv6/lg-mytouch [Accessed August 28, 2014].

Ullrich, J., Krombholz, K., Hobel, H., Dabrowski, A. & Weippl, E., 2014. IPv6 Security : Attacks and Countermeasures in a Nutshell. In *USENIX*. Available at: https://www.usenix.org/system/files/.../woot14-ullrich.pdf [Accessed September 20, 2001].

Volz, B., 2006. Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option. IETF. RFC 4649. Available at: http://tools.ietf.org/html/rfc4649.

Wang, K., Yeo, A. & Ananda, A.L., 2001. DTTS : A Transparent and Scalable Solution for IPv4 to IPv6 Transition. In *Tenth International Conference on Computer Communications and Networks*. Scottsdale, AZ: Institute of Electrical and Electronics Engineers.

Warfield, M., 2003. Security implications of IPv6. In *Black Hat*. Las Vegas, NV: Internet Security Systems. Available at: http://www.blackhat.com/presentations/bh-federal-03/bh-federal-03-warfield/bh-fed-03-warfield.pdf [Accessed August 12, 2013].

Wasserman, M. & Baker, F., 2011. IPv6-to-IPv6 Network Prefix Translation. IETF. RFC 6296. Available at: http://tools.ietf.org/html/rfc6296.

Weiser, M., 1991. The computer for the 21st Century. *Pervasive Computing, IEEE*, 1(1).

Wheeler, J.S., 2011. IPv6 NDP Table Exhaustion Attack. Available at: http://inconcepts.biz/˜jsw/.

Yourtchenko, A. & Wing, D., 2012. Happy Eyeballs: Success with Dual-Stack Hosts. IETF. RFC 6555. Available at: http://tools.ietf.org/html/rfc6555.

Zheng, P. & Ni, L.M., 2006. Spotlight: the rise of the smart phone. *IEEE Distributed Systems Online*, 7.

Zulkiflee, M., Azirah, S. a., Haniza, N., Zakiah, a. & Shahrin, S., 2011. Behavioral analysis on IPv4 malware on different platforms in IPv6 network environment. *2011 IEEE Conference on Open Systems*. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6079278.

Appendix A

Technical artifacts

A-1. System application configurations

The appendix provides the technical information required to implement the IP6ND tools and the supporting services, which include the PostgreSQL database instance. The source code of the dashboard and the sensor is included that provides a functional instance of the tool.

A-1.1 APT package manager update

Update and configuration of the apt package manager

```
#    echo "deb http://kali.org/kali kali main non-free contrib" >
     /etc/apt/sources.list
#    echo "deb http://security.org/kali kali/updates main non-free
     contrib" >> /etc/apt/sources.list
#    echo "deb-src http://kali.org/kali kali main non-free contrib"
     >> /etc/apt/sources.list
#    echo "deb-src http://security.org/kali kali/updates main non-
     free contrib" >> /etc/apt/sources.list
#    apt-get update
```

This should update the repositories for the Kali distribution and permit additional package installations with apt-get.

A-1.2 Router Advertising Daemon installation on Kali Linux 1.07

Preparation:

Install the check package, this is required by the build process of radvd.

```
#    apt-get install cache
```

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  check
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 118 kB of archives.
After this operation, 286 kB of additional disk space will be
   used.
WARNING: The following packages cannot be authenticated!
  check
Install these packages without verification [y/N]? y
Get:1 http://http.kali.org/kali/ kali/main check amd64 0.9.8-2
   [118 kB]
Fetched 118 kB in 3s (30.3 kB/s)
Selecting previously unselected package check.
(Reading database ... 342664 files and directories currently
   installed.)
Unpacking check (from .../check_0.9.8-2_amd64.deb) ...
Processing triggers for install-info ...
Setting up check (0.9.8-2) ...
```

Download radvd-2.5.tar.gz from http://www.litech.org/radvd/

Extract the content of the file:

```
#    tar zxvf radvd-2.5.tar.gz
```

This will extract the content of the file to the radvd-2.5 folder. Complete the compilation of the source and the installation with the following commands:

```
#    cd radvd-2.5/
#    ./configure
#    make
#    make install
```

A-1.3 Installation of Miredo Relay/Server

Preparation:

Download miredo-1.2.4.tar.bz2 from http://www.remlab.net/files/miredo/

Extract the content of the file:

```
#    tar xjvf miredo-1.2.4.tar.bz2
```

This will extract the content of the file to the miredo-1.2.4 folder. Complete the compilation of the source and the installation with the following commands:

```
#    cd miredo-1.2.4
#    ./configure
#    make
#    make install
```

A-2. Source Code

The source code for IP6NDdash and IP6NDsensor, developed as part of section 5.4 of the case studies.

A-2.1 IP6NDdash

```
#!/usr/bin/python2.4
#
# Small script to show central reporting from PostgreSQL
#

import sys
import os
import psycopg2
import thread
import time
import datetime

#Configuration
conf_interval = 1           # Number of minute to sample
conf_refresh = 5            # How often to refresh (seconds)
conf_warning = 25           # NDP p/s Cautionary watermark (when to
alert)
conf_high = 100                    # NDP p/s High watermark (when to
alert)
conf_mac_warning = 100             # MACs per vendor warning
watermark
conf_mac_high = 255         # MACs per vendor high watermark

#Database configuration
conf_dbname = 'IPv6_lab'    # Database Name
conf_dbhost = '172.16.10.12'# Database Host
conf_dbuser = 'UserX'       # Database Host
conf_dbpass = 'c0mp2q'             # Database Password

#Connect to the database
try:
    conn = psycopg2.connect("dbname='" + conf_name + "' user='" +
conf_dbuser + "' host='" + conf_dbhost + "' password='" +
conf_dbpass +"'")
```

```
conn.set_isolation_level(psycopg2.extensions.ISOLATION_LEVEL_AUTOCOM
MIT)
except:
    print "I am unable to connect to the database"

# Color class
class bcolors:
    HEADER = '\033[95m'
    OKBLUE = '\033[94m'
    OKGREEN = '\033[92m'
    WARNING = '\033[93m'
    FAIL = '\033[91m'
    ENDC = '\033[0m'



# measureNDP()
#Measure the amount of NDP events in the environment
#Print different colors based on the conf_high and conf_warning
water marks and sound audible alarm.
#
def measureNDP():
 cur.execute ("""select segmentID, count(macaddr)/60,
count(ip6addr)/60 from ip6mac_bindings where update > now() -
interval '%s minutes' group by segmentID""", (conf_interval,))
        rows = cur.fetchall()
 print bcolors.HEADER + "SegID" + "\t" + "#MAC" + "\t" + "#IPv6s" +
bcolors.ENDC
 print bcolors.HEADER + "     " + "\t" + "pps" + "\t" + "pps" +
bcolors.ENDC

        for row in rows:
        if ( row[1] > conf_high ) :
           print bcolors.FAIL + str(row[0]) + "\t" + str(row[1]) +
"\t" + str(row[2]) + bcolors.ENDC + "\a\a\a";
                elif ( row[1] > conf_warning ):
           print bcolors.WARNING + str(row[0]) + "\t" + str(row[1])
+ "\t" + str(row[2]) + bcolors.ENDC;
        else:
           print bcolors.OKGREEN + str(row[0]) + "\t" + str(row[1])
+ "\t" + str(row[2]) + bcolors.ENDC;
 cur.execute ("""select segmentID, count(macaddr)/60,
count(ip6addr)/60 from ip6mac_bindings where update > now() -
interval '%s minutes' group by segmentID""", (conf_interval,))
```

```
# listTopVendors()
# List the top Device Vendors based on MAC addresses.
# This is used to see whether there is MAC spoofing happening that
is not using local hardward prefixes.
# Print different colors based on the high and warning water marks
and sound audible alarm.
#
def listTopVendors():
  cur.execute ("""select vendor, maccount from topvendor LIMIT 10""")
  rows = cur.fetchall()
  print ""
  print bcolors.HEADER + "Top Ten Vendor - 1 minute" + bcolors.ENDC
  print bcolors.HEADER + "#MAC" + "\t" + "Vendor" + bcolors.ENDC

  for row in rows:
        if ( row[1] > conf_mac_high ) :
               print bcolors.FAIL + str(row[1]) + "\t" + str(row[0])
+ bcolors.ENDC + "\a\a\a";
        elif ( row[1] > conf_mac_warning ):
               print bcolors.WARNING + str(row[1]) + "\t" +
str(row[0]) + bcolors.ENDC;
        else:
               print bcolors.OKGREEN + str(row[1]) + "\t" +
str(row[0]) + bcolors.ENDC;

try:
    while True:
  cur = conn.cursor()

  os.system('clear')
  measureNDP()
  listTopVendors()
        time.sleep(conf_refresh)
  cur.close()
except KeyboardInterrupt:
    pass

print 'Thanks...'
```

A-2.2 IP6NDsensor

```
#!/usr/bin/python2.4
#
# Distributed monitoring agent
#

import sys
import socket
import datetime
import time
import psycopg2
from netaddr import *
from scapy.all import *
# Configuration variables
conf_stateage = 24
#Database configuration
conf_dbname = 'IPv6_lab'        # Database Name
conf_dbhost = '172.16.10.12'    # Database Host
conf_dbuser = 'UserX'           # Database Host
conf_dbpass = 'c0mp2q'          # Database Password
interface = sys.argv[1]
segmentID = sys.argv[2]
associations = []
associationd = []
associationr = []
unique = []
class mac_custom(mac_unix): pass
mac_custom.word_fmt = '%.2X'
#Connect to the database
try:
    conn = psycopg2.connect("dbname='" + conf_name + "' user='" +
conf_dbuser + "' host='" + conf_dbhost + "' password='" +
conf_dbpass +"'")
except:
    print "Unable to connect to the specified Database"
cur=conn.cursor()
# define the state age from now()
dt = datetime.datetime.now() -
datetime.timedelta(0,(conf_stateage*24))
#  importStates()
# Import the existing matches from the Database to prevent numerous
duplication on sensor restart
#
```

```
def importStates():
 print "Importing Database state: " + str(conf_stateage) + " hours - 
from " + str(dt)
 cur.execute ("""select type,segmentID, macaddr, ip6addr, type
                        from ip6mac_bindings where update > %s and 
segmentID = %s""", (dt,segmentID))
 rows = cur.fetchall()
 count = 0
 for row in rows:
        associations = str(row[0]) +";"+ str(row[1]) +";"+ 
str(row[2]) +";"+ str(row[3])
        unique.append(associations)
        count += 1
 print str(count) + " associations loaded, monitoring starting"
def sniffMAC(p):
# Initiate time variable
 ts = time.time()
 st = datetime.datetime.fromtimestamp(ts).strftime('%Y-%m-%d 
%H:%M:%S')
# If the packet is Ethernet
 if p.haslayer(Ether):
        macSrc = p.sprintf("%Ether.src%")
        macDst = p.sprintf("%Ether.dst%")
        # Define the IPv6 Source and Destination variables
        if p.haslayer(IPv6):
               IPv6src = p.sprintf("%IPv6.src%")
               IPv6dst = p.sprintf("%IPv6.dst%")
        # If the OptSrcLLAddr is set then use that as source. 
Assists in detecing flooding
        if p.haslayer(ICMPv6NDOptSrcLLAddr):
               macOption = p.sprintf("%ICMPv6NDOptSrcLLAddr.lladdr%")
        else:
               macOption = "00:00:00:00:00:00"
        if p.haslayer(ICMPv6ND_NS):
               # Create association variable to keep track of unique 
objects
               associations = p.sprintf("D;%Ether.src%;%IPv6.src%")
               SRtgt = p.sprintf("%ICMPv6ND_NS.tgt%")
               typeA = 'D'
               # If this is a Request for an IP, and the Source is :: 
use the requested IP as source and Identify as Request
               if IPv6src == '::':
                      associations = 
p.sprintf("R;%Ether.src%;%ICMPv6ND_NS.tgt%")
                      IPv6src = SRtgt
                      typeA = 'R'
               # Only report on unique IP/MAC mappings
               if unique.count(associations) == 0:
                      unique.append(associations)
                      cur.execute("""INSERT into
ip6mac_bindings(type, segmentID, macaddr, ip6addr, update) VALUES
(%(typeA)s, %(segmentID)s, %(mac)s, %(ip6)s, now())""", {'typeA':
typeA, 'segmentID': segmentID, 'mac': macSrc, 'ip6':IPv6src})
        #If the ICMPv6 packet has a Neighbour Advertisement of
Neighbour solicitation
        if p.haslayer(ICMPv6ND_NA) and not p.haslayer(ICMPv6ND_NS):
               associations = p.sprintf("D;%Ether.dst%;%IPv6.dst%")
               associationd = p.sprintf("S;%Ether.src%;%IPv6.src%")
               if unique.count(associations) == 0:
                      unique.append(associations)
                      typeA = 'D'
                      cur.execute("""INSERT into
ip6mac_bindings(type, segmentID, macaddr, ip6addr, update) VALUES
(%(typeA)s, %(segmentID)s, %(mac)s, %(ip6)s, now())""", {'typeA':
typeA, 'segmentID': segmentID, 'mac': macDst, 'ip6':IPv6dst})
               if unique.count(associationd) == 0:
                      unique.append(associationd)
                      typeA = 'S'
                      cur.execute("""INSERT into
ip6mac_bindings(type, segmentID, macaddr, ip6addr, update) VALUES
(%(typeA)s, %(segmentID)s, %(mac)s, %(ip6)s, now())""", {'typeA':
typeA, 'segmentID': segmentID, 'mac': macSrc, 'ip6':IPv6src})
        #If the ICMPv6 packet has a ND Optional Prefix (local
prefixes)
                if p.haslayer(ICMPv6NDOptPrefixInfo):
                        counter = 1
                        PrefixInfo =
p.sprintf("%ICMPv6NDOptPrefixInfo:"+str(counter)+".prefix%")
                        while PrefixInfo != "??":
                      length =
p.sprintf("%ICMPv6NDOptPrefixInfo:"+str(counter)+".prefixlen%")
                      PrefixInfoC = PrefixInfo + "/" + length
                                typeA = "PI"
                      associationr =
p.sprintf("D;%Ether.src%;%IPv6.src%;") + PrefixInfoC
                      if unique.count(associationr) == 0:
                             cur.execute("""INSERT into
ip6router_advertisements (type, segmentID, macaddr, macOption,
ip6addr, prefix, update) VALUES (%(typeA)s, %(segmentID)s, %(mac)s,
%(macOption)s, %(ip6)s, %(prefix)s, now())""", {'typeA': typeA,
'segmentID': segmentID, 'mac': macSrc, 'macOption': macOption,
'ip6': IPv6src, 'prefix': PrefixInfoC})
                            unique.append(associationr)
                                counter += 1
                                PrefixInfo =
p.sprintf("%ICMPv6NDOptPrefixInfo:"+str(counter)+".prefix%")
        #If the ICMPv6 packet has a ND Optional Route Prefix
(Network Routes)
                if p.haslayer(ICMPv6NDOptRouteInfo):
                        counter = 1
                        RouteInfo =
p.sprintf("%ICMPv6NDOptRouteInfo:"+str(counter)+".prefix%")
                        while RouteInfo != "??":
                      length =
p.sprintf("%ICMPv6NDOptRouteInfo:"+str(counter)+".plen%")
                      RouteInfoC = RouteInfo + "/" + length
                                typeA = "RI"
                      associationr =
p.sprintf("D;%Ether.src%;%IPv6.src%;") + RouteInfoC
                      if unique.count(associationr) == 0:
                            cur.execute("""INSERT into
ip6router_advertisements (type, segmentID, macaddr, macOption,
ip6addr, prefix, update) VALUES (%(typeA)s, %(segmentID)s, %(mac)s,
%(macOption)s, %(ip6)s, %(prefix)s, now())""", {'typeA': typeA,
'segmentID': segmentID, 'mac': macSrc, 'macOption': macOption,
'ip6': IPv6src, 'prefix': RouteInfoC})
                            unique.append(associationr)
                                counter += 1
                                RouteInfo =
p.sprintf("%ICMPv6NDOptRouteInfo:"+str(counter)+".prefix%")
 conn.commit()
importStates()
sniff(filter='icmp6',iface=interface,prn=sniffMAC)
```

A-2.3 Database preparation

The following SQL is used to prepare the PostgreSQL table structure. It should be executed in a existing database that provides network connectivity for IP6NDsensor.

```
DROP TABLE ip6mac_bindings;

CREATE TABLE ip6mac_bindings (
        type            varchar(5),
        segmentID integer,
    macaddr             macaddr,
    ip6addr             inet,
    update        timestamp
);

CREATE INDEX ip6mac_idx ON ip6mac_bindings (macaddr);
CREATE INDEX ip6adr_idx ON ip6mac_bindings (ip6addr);

DROP TABLE ip6router_advertisements;

CREATE TABLE ip6router_advertisements (
    type          varchar(5),
    segmentID     integer,
    macaddr             macaddr,
    macOption     macaddr,
        ip6addr         inet,
    prefix        cidr,
    update        timestamp
);

CREATE INDEX ip6rmac_idx ON ip6router_advertisements (macaddr);
CREATE INDEX ip6raddr_idx ON ip6router_advertisements (ip6addr);
```