FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

FEUP

IPv4 to IPv6 transition: security challenges

Tomé Araújo Duarte

Master in Informatics and Computing Engineering

Supervisor: J. Magalhães Cruz (PhD)

2^{nd} February, 2013

IPv4 to IPv6 transition: security challenges

Tomé Araújo Duarte

Master in Informatics and Computing Engineering

Approved in oral examination by the committee:

Chair: João Cardoso (Prof., PhD)
External Examiner: Jorge Mamede (Prof., PhD)
Supervisor: João Magalhães Cruz (Prof., PhD)

6^{th} February, 2013

Abstract

At a time where the available Internet Protocol version 4 (IPv4) address pools are running out, still too many Internet Service Providers (ISPs) and network administrators have yet to acknowledge this new reality and adapt their networks and systems. Although the depletion of addresses has been repeatedly mentioned and commented for the past decade amongst relevant networking circles, 2011 and 2012 showed us a growing and urgent need for Internet Protocol version 6 (IPv6) adoption as Regional Internet Registries (RIRs) are depleting their IPv4 address pools.

Technology evolved throughout the years and became increasingly available, becoming ubiquitous in first world countries both for personal users and businesses. As Internet access became available, reliable and comparable to local network speed, computer software explored new avenues for information processing and sharing through network connectivity. From multi-player network video games, to online storage and backups and web-based accounting software, the Internet-available services and software quickly became dominant, creating a great dependence upon Internet connectivity.
Vital tasks for our daily lives and our modern society are now dependant upon Internet connectivity (banking and stock markets being examples of such), which leaves the end users implicitly trusting networks and by consequence network operations teams with a huge responsability.

Availability and security are key in the correct operation of networks and the Internet. This new protocol means new security attacks, a new paradigm and a difficult path ahead to switch the Internet's core communication medium. The transition from IPv4 to IPv6 embarks great challenges migrating users and services in a reliable and cost-effective way. Even if the transition between IPv4 and IPv6 is smooth, the issue of providing (at least) the same level of security as we have today on such a different new protocol lies ahead, waiting to be addressed.

This thesis studies the IPv6 protocol security challenges and the effects this migration has on network security. To that end, different transition strategies are detailed as well as possible vectors of attack to the IPv6 protocol and dual-stack environments.

Keywords:

- IPv6
- Protocol transition
- Security

Resumo

Ainda que estejamos já a esgotar as últimas reservas de endereços IPv4, muitos ISPs e administradores de rede ainda não se consciencializaram da nova realidade a que têm de adaptar as suas redes e sistemas. A escassez de endereços IPv4 é comentada há já vários anos nos círculos relevantes, tendo ainda assim sido demonstrada nos anos de 2011 e 2012 uma necessidade cada vez mais urgente de adopção de IPv6 à medida que os RIRs esgotam as suas reservas de endereços IPv4.

Ao longo dos anos a tecnologia evoluiu, estando omnipresente nos países de primeiro mundo para fins pessoais e profissionais. Com acesso à Internet a velocidades e qualidade de serviço quase equiparável às redes locais, o *software* desenvolveu novas formas para processamento e partilha de informação. Desde vídeo-jogos em rede, soluções de armazenamento e cópias de segurança online até software de facturação web, os serviços e *software* disponibilizados online preencheram o mercado e criaram uma grande dependência no acesso à Internet.
Tarefas vitais no nosso dia-a-dia e para a sociedade moderna estão actualmente dependentes da comunicação através da Internet (as indústrias da banca e da bolsa de mercados são exemplos disso), formalizando de forma implícita uma confiança absoluta nas redes sobre as quais operam, forçando também uma enorme responsabilidade nas equipas de gestão de operações de redes.

Os factores chave da gestão de redes (e também na Internet) são a disponibilidade de serviço e a segurança do mesmo. Com este novo protocolo surgem também novos ataques de segurança, um novo paradigma de redes e inicia-se a troca do principal meio de comunicação da Internet - a mudança de IPv4 para IPv6 levanta desafios na transição dos serviços e utilizadores de forma segura e economicamente sustentável. Mesmo conseguindo uma transição suave, aguarda-nos ainda o desafio de garantir (pelo menos) o mesmo nível de segurança informática existente hoje nas nossas redes com um conjunto tão diferente de protocolos.

Esta tese estuda os desafios de segurança inerentes ao protocolo IPv6 e os efeitos que esta migração de procolos tem na segurança de redes. Nesse sentido, são analisados diferentes possibilidades como estratégias de transição e os possíveis ataques ao protocolo IPv6 e a ambientes com as duas versões do protocolo IP disponíveis em paralelo.

Palavras-chave:

- IPv6
- Transição de protocolos
- Segurança

Acknowledgements

College was a real journey for me. I learned how valuable bonding with others can be, how to work with other people and even how to lead others into doing magnificent teams - not because of my leadership, but for being crazy enough to believe we had it in us.

I drove most everyone around me mad about my schedule, priorities and overall seemingly delusional attitude. I started businesses, got into more things that I should, played and learned through everything I could take in from FEUP and the people in it.

I would like to thank my family, my girlfriend for being there for me all these years and everyone whoever asked me how something could be done - it's the challenge in learning that makes us move forward.

Last but not least, I would like to thank my supervisor for being supportive of my time constraints and hectic schedule. I wouldn't be able to do it any other way.

Tomé Duarte

"Better to fail spectacularly than do something mediocre."

Randy Pausch
in Last Lecture

Contents

List of Figures

LIST OF FIGURES

List of Tables

Abbreviations

ACL	Access Control List
ARP	Address Resolution Protocol
AUP	Acceptable Use Policy
APNIC	Asia-Pacific Network Information Centre
ARPANET	Advanced Research Projects Agency Network
AS	Autonomous System
BGP	Border Gateway Protocol
BIND	Berkeley Internet Name Domain
CDN	Content Distribution Network
CGA	Cryptographically Generated Addresses
CGN	Carrier-Grade Network
CPE	Customer Premise Equipment
CSO	Chief Security Officer
CSRF	Cross Site Request Forgery
DARPANET	Defense Advanced Research Projects Agency Network
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoS	Denial of Service
DS-Lite	Dual-Stack Lite
DUID	DHCP Unique Identifier
FCCN	Foundation for National Scientific Computing
FTP	File Transfer Protocol
I-D	Internet Draft
IAID	Identity Association Identifier
ICANN	Internet Corporation for Assigned Names and Networks
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPSEC	Internet Protocol Security

IPTV	Internet Protocol Television
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IRC	Internet Relay Chat
ISP	Internet Service Provider
LACNIC	Latin American and Caribbean Network Information Centre
LAN	Local Area Network
MITM	Man In The Middle
MTU	Maximum Transmission Unit
NA	Neighbor Advertisement message
NAP	Network Access Point
NAT	Network Address Translation
NSFNET	National Science Foundation Network
NS	Neighbor Solicitation message
NDP	Neighbor Discovery Protocol
NOC	Network Operations Center
P2P	Peer to peer
PDF	Portable Document Format
POP	Post Office Protocol
OSI	Open Systems Interconnection
QoS	Quality of Service
RA	Router Advertisement message
RFC	Request for Comments
RH	Routing Header
RIR	Regional Internet Registry
RS	Router Solicitation message
SCADA	Supervisory Control And Data Acquisition
SeND	Secure Neighbor Discovery
SLAAC	StateLess Address Auto Configuration
SMB	Small Medium Business
SMTP	Simple Mail Transfer Protocol
SPAM	Unsolicited bulk email
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP/IP	Internet Protocol Suite - TCP and IP combined
TLD	Top Level Domain
TTL	Time-to-live
UDP	User Datagram Protocol
UNIX	UNiplexed Information and Computing System
UPnP	Universal Plug and Play
WWW	World Wide Web
XSS	Cross-site Scripting

Chapter 1

Introduction

1.1 Overview

The Internet has continually evolved this last decade to become something that our society depends upon. It is used by people across different sectors, computer savvy and otherwise, for all kinds of services and purposes: videogames, social interactions, banking, accounting and globally disperse teams collaborating and communicating remotely are just a few examples.
Computer networks (Internet enabled or not) have propagated to enable communication and collaboration in offices and ludic purposes in our households. It is the required medium upon which important industries such as banks and stock markets all over the world depend on. Everywhere, users increasingly rely on computer networks as their first option for all kinds of activities in their daily lifes, whether on a personal computer, a tablet or a smartphone as the frontend.
The Internet has greatly potentiated this usage and reliance on computer networks, being used for such diverse things as television - now being delivered by Internet Protocol television (IPTV) - or businesses' customer relations, where email has taken its place as a key communication channel with both suppliers and customers for many businesses. Governments are also taking part in this growth, relying access to services such as social security and tax reports to web-enabled platforms, essentially turning Internet access into an important resource in the daily life of many.

Underneath the application layer, where previously mentioned services are exposed to the end-user, the network consists of many routers, servers and other network-enabled devices which communicate with each other using a standard set of protocols. These protocols were designed to enable address allocation and routing of messages from one endpoint to another, among many other features. Most, however, did not contemplate at the time of their design mechanisms to enable confidentiality and integrity of the information transmitted across the network, allowing for tampering and interception with ease

for a skilled attacker.[DK06]
Currently widely deployed, IPv4 is a twenty-year-old internetworking standard protocol at the core of devices communication in packet-switched networks (such as Ethernet) and uses 32-bit unique addresses to identify each host on the network, with no concern or guarantees as to the delivery or integrity of messages. While there are efforts to secure communications both at the application layer as well as the internet layer (notably Secure Sockets Layer (SSL), Internet Protocol Security (IPSEC) and Domain Name System Security Extensions (DNSSEC)), with the amount of trust deposited in the correct operation of the networks, security is essential. A myriad of people build, maintain and secure the networks ranging from network administrators to penetration testers and the information security industry has developed tools and methodologies to help secure networks and protect its users and information.[Har97, IET]
With the coming end of IPv4 availability, IPv6 has been selected to substitute it and provide a growth path for ISPs. This protocol features enhanced security capabilities - see the following chapter - that can help operate more secure networks in the future. While network security knowledge and practices have evolved alongside the size and usage of computer networks these past decades, this migration of protocols is the perfect opportunity to architect computer networks with security in mind from the start, instead of an afterthought.[Jor07, Hus11b]

This thesis aims to provide a clear analysis on the current state of IPv6 security, network transitioning between the two protocols and what challenges hinder a simple and safe migration from IPv4 to IPv6 on today's networks and the Internet. While most professionals still understand IPv6 only as a bigger address space, a safe adoption of the IPv6 protocol in corporate networks pertains not only to the correct implementation of routing and address allocation strategies but also to the availability, coverage and adequacy of security policies, access control lists (ACLs) and related security mechanisms.

1.2 Context

1.2.1 Device communication on the Internet

The Internet, as we know it today, is, at its core, a network of computer networks. Network traffic[1] originates at one given network node (e.g. a computer, a smartphone or a router) and traverses the network until it reaches its destination or is unable to find it after a given amount of hops.[ALM+05]

[1]Network traffic consists of network packets, with an identified source, destination and payload data when appropriate. The standardization of packet structure and content is up to the Internet Engineering Task Force (IETF), which publishes Request For Comments (RFC) documents pertaining future protocols and developments of the Internet, some of which become industry standards for new network protocols.

The transit of data packets in the Internet is possible due to the existence of routers and switches. These devices have a processing unit and multiple network ports, bridge different network links and forward relevant network traffic between them. Each link can belong to a totally diferent network[2] or simply another node on the local network[3].[ALM+05, MBD04]

A few decades ago, vendor lock-in[4] was common place and vendors actually made an effort to hamper customers' efforts to mix their hardware or software with other vendors' material, to maximize their profit. This practice created a need to provide abstraction of the physical infrastructure and networks configuration for protocols and services, solved by different approaches and models, more notably so through the Open Systems Interconnection (OSI) model. A more simplified and pratical model was developed by the IETF, called TCP/IP - the Internet Protocol suite - and uses encapsulation to provide an abstraction of the information being communicated with network packets. Simply put, we can think of and characterize traffic according to the relevant layer for the discussion thus providing a common language for the analysis, discussion and development of network protocols, data and traffic. Figure 1.1 depicts both the OSI and TCP/IP model, as well as their approximate correspondences.[Neta]

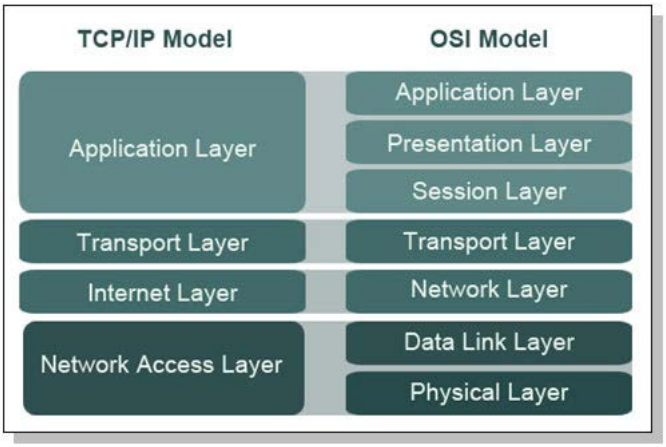

Figure 1.1: The Internet Protocol suite and the Open Systems Interconnection model. The former is commonly referred to as the TCP/IP model.

1.2.2 IPv6 adoption

The entire IPv4 address pool consists of 4 294 967 296 (2^{32}) addresses, which are currently being consumed at a rate of 5 percent every year. Current estimates place the

[2]Each public network has unique addresses assigned by the Internet Corporation for Assigned Names and Numbers (ICANN), a local RIR or an ISP, depending on the size of the network and its uses.

[3]There are specific network addresses reserved for "local network" uses; that is to say, those addresses cannot be reached from the Internet nor from nodes in any different network directly.

[4]Vendor lock-in is a term used to describe configurations where all hardware and/or software in a given network is from the same set of vendors and difficult to integrate with other hardware/software.

pool depletion at a date no later than 2015 (Figure 1.2) at which time most ISPs will need to have either an IPv6 deployment strategy or IPv6 already available for customers and/or internal networks. However, IPv6 adoption is still very slow with IPv6-enabled Autonomous Systems[5] (AS) registered with regional internet registries (RIR) still below 20 percent of the total AS (Figure 1.3).[Hus11a, Husc, RIP]

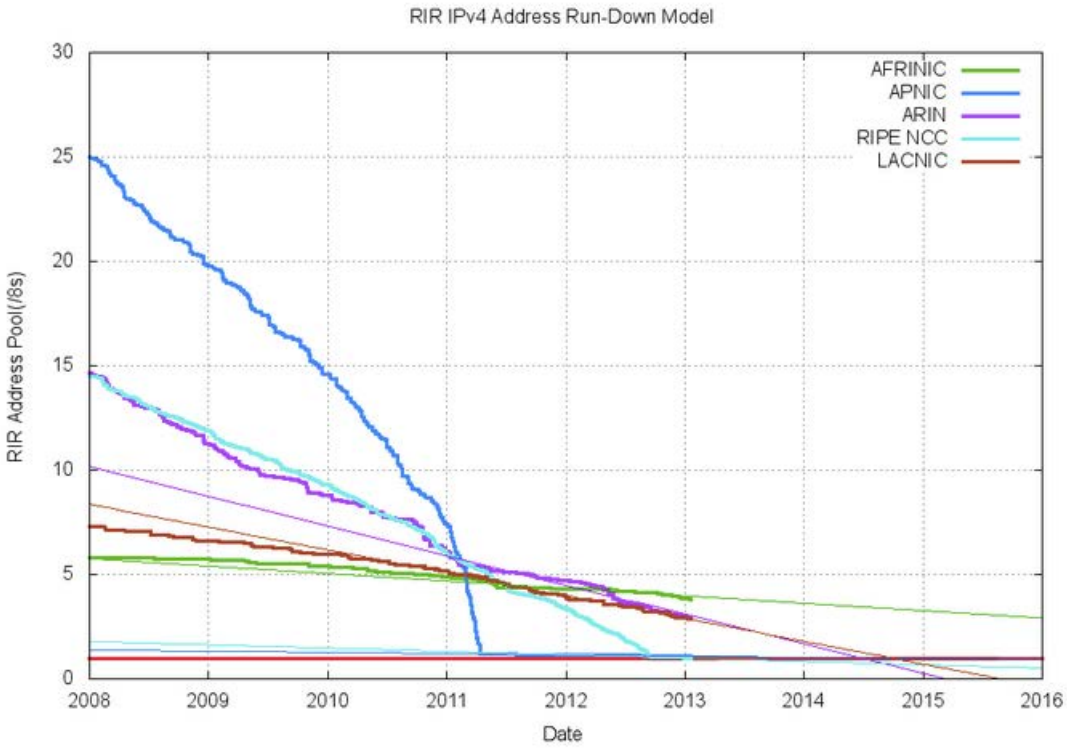

Figure 1.2: Projection of consumption of remaining RIR IPv4 Pools.

The World IPv6 day in 2011[6] has been a successful step towards global IPv6 adoption: for 24 hours, many online businesses, academic institutions and network enthusiasts enabled IPv6 alongside IPv4 on their networks and systems. This coordinated effort brought together high traffic websites, Content Distribution Networks (CDNs) and others to help test the performance and realistic operating capacity of an IPv6 network in today's Internet, both as an end-user and as a service provider. The Internet Society, responsible for this event, has deemed the results successful and, building on those results, set 2012's World IPv6 Launch day[7] to become a global coordinated launch of IPv6 availability - participants enabled IPv6 permanently, providing their services in a dual-stack environment[8] from that day on.

In total, more than 3000 websites, including the four more popular ones by the Alexa

[5] A collection of connected IP routing prefixes with a shared and clearly defined routing policy to the Internet.

[6] In 2011, World IPv6 day happened in the 8th of June; in 2012, the 6th of June marked the World IPv6 Launch day.

[7] A list of participants and more information about this can be found on the official website, located at `http://www.worldipv6launch.org/participants/`

[8] In this environment network-enabled devices make their services available in both IPv4 and IPv6 networks.

rank, 65 ISPs and 5 major router vendors participated in the World IPv6 Launch day. An estimated 27% of the Internet is now available via IPv6, meaning that suddendly IPv6 became much more important and many more network links are active, potentialy exposing many networks and systems. Even more, many other ISPs are reportedly preparing IPv6 deployment, so this figure is expected to continue growing in the near future.[Socb, Fio]

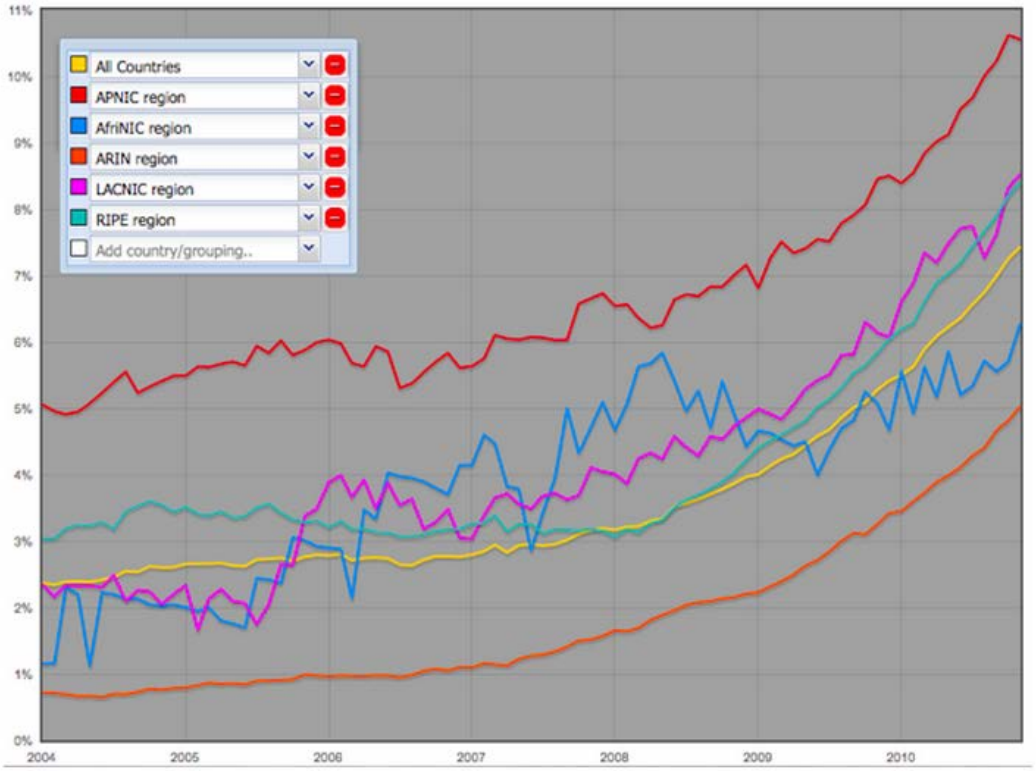

Figure 1.3: Percentage of IPv6-enabled Autonomous Systems registered in each RIR.

With IPv4 shortage rapidly progressing and IPv6 adoption becoming a priority for many ISPs, this growth rate is expected to increase in the following years. The Internet Society has already declared publicly that the Internet has run out of IPv4 addresses. However, due to backwards-compatibility with systems and networks that remain IPv4 only, it is expected that for several years both protocols will have to co-exist and ISPs will have to adapt with the following two constraints:[Soca]

1. IPv6 deployment in their internal networks and availability as a service to customers

2. efficient use of IPv4 addresses, to reduce costs and enable IPv4 conectivity

The path to a IPv6-only Internet is far from complete and there are significant challenges ahead. First, the transition period will bring a mix of partial and full-transitioned networks online to coexist with the current IPv4 networks and provision of online services

is expected not to be disrupted. Secondly, IPv6 as a protocol has several security misconceptions and vulnerabilities by design, which adds to the challenge of transitioning the Internet to a new routing protocol in a safe and cost-effective way.

1.2.3 Information security industry

The Internet started as an academic research project, under the name Advanced Research Projects Agency Network (ARPAnet), linking few universities internal networks. At the time, it was meant as a tool to facilitate colleagues' collaboration and information exchange through the use of computer systems. When the United States Defense department took interest, the project received additional funding, direction and changed its name to Defense Advanced Research Projects Agency Network (DARPAnet), growing rapidly to become more device independent and information focused. On 1988, with the Internet's (at the time, National Science Foundation Network (NSFNET)) first availability to commercial uses[9], there were still few concerns with security and little expertise in the field of internetworking security; until then, only academic and government institutions were allowed to connect to the network and its Acceptable Use Policy (AUP) contemplated only research and education.[Dae, SK, Zak]

The Internet evolution, fueled by new and old businesses reaching out to worldwide customers, saw a dramatic increase in sensitive information and financial transactions over network links, bringing along security concerns. As the "Internet underground" developed in the late 80s and 90s, with enthusiasts and professionals pushing computer systems to their limits, discovering and actively exploiting vulnerabilities, those concerns quickly spun a spring of different businesses around computer security. A relevant and big industry grew, producing security software (e.g. anti-virus, firewalls, intrusion detection software), services (e.g. penetration testing[10], SSL certificates) and professional certification, used to protect and attack networks and computer systems ranging from the simplest home workstation to bank and military networks.[Day]

1.2.3.1 A note on wearing different kinds of hats

Legislation for these kind of actions is very different from country to country, making regulation of online security activities difficult. While many experts and professionals offer or sell their services publicly and lawfully, others do so anonymously, either for

[9] Curious fact: the term internet derives from its use as a shorthand for internetwork in RFC 675 (first draft of the Transmission Control Protocol (TCP)) in December 1974. Since then, other RFCs started using it and by January 1, 1983 TCP/IP became the standard protocol suite on the ARPANET.

[10] Penetration testing is the process of testing a software or computer network for security vulnerabilities, using tools and attacks in the same way a malicious attacker would.

fun or profit, and commonly break laws. In many countries (Portugal is such an example), the law is ambivalent towards what exactly constitutes legal or illegal actions, which complicates matters.

By mid-80s, a need to clearly contextualize such activities became clear and the terms “hacker” and “cracker” were coined. Both stand for highly skilled technologists, the difference being that crackers use their knowledge to break into other people’s systems, without their consent. Another form of designation arised, distinguishing between three types: “white hats”, the equivalent to hackers; “black hats”, equivalent to crackers; and “grey hats”, who mostly act lawfully but will circumvent security in illegal ways ocasionally.[Ray]

1.2.3.2 Profession

From the beginning, two distinct approaches to network security clearly arised and persist to this day: defensive and offensive. The latter focuses on penetrating networks and compromising systems, developing and leveraging software to attack and exploit vulnerabilities in protocols, operating systems or software. Defensive security provides the tools, processes and knowledge to defend networks and computer systems against attacks or mitigate the consequences of a successful attack. Furthermore, attacks and techniques are usually very specific to the system being tested: web application attacks such as Cross-site Scripting (XSS) and Cross-site Request Forgery (CSRF) are perpetrated in very different ways than software reverse engineering[11] or remote network intrusion, and require very different skillsets.[NKKK09]

Different roles emerged in organizations to support this responsibilities, and a myriad of tools (both software and standard practices) emerged. Nowadays, the role of protecting an organization’s information assets rests highly on the organization’s ability to protect their networks and computer systems and is most commonly shared between systems operations and a Chief Security Officer (CSO), dictating policies, auditing processes, monitoring usage and activity patterns, etc.
The software tools [12] of the trade are spread accross the following categories:

Information gathering Dedicated to find out more information about a specific target or to identify possible targets in a given network. These include network scanners, fingerprinting tools, web and vulnerability scanners, as well as standard UNIX network tools.

[11] The process of deciphering a software executable file into assembly language for analysis. This can be useful to identify potential security holes and is widely known as a license evasion technique for shareware software.

[12] A comprehensive and extensive list of the most popular information security tools is at `https://sec-tools.org`.

Traffic manipulation In order to cause a Denial of Service (DoS), manipulate network packets, replicate behaviour or simply to test unexpected inputs to a network or application.

Proactive defense Anti-virus, firewalls, intrusion detection systems, honeypots and forensic tools help prevent, detect, stop and analyse attacks.

Exploiting Used for exploiting vulnerabilities and gaining or maintaning privileged access to systems or networks. These include automated frameworks, collections of published exploits, privilege escalation and log cleaning tools, as well as compilers, etc for exploit development.

Aside from the software, it's worth mentioning other common assets on a security team:

Security Policies This is an instrumental tool for any team managing security in a corporate environment. A security policy clearly states and defines rules for managing assets (e.g. routers, servers, user accounts) and provides a framework for consistent security across all devices and activities. An example of its utility is when adding a new router to the network: default configuration steps, allowed networks in and out and other similar settings are most useful when properly standardized across all routers.[Insb, Insc, Dep]

Certifications and training Most hardware and enterprise software vendors provide security certifications and/or training, illustrating the security features and settings available in their products. Aside from that, online certifications provide virtual network labs and exams to allow students to progress at their own pace.[Off, Secb, Cisc]

Vulnerabilities disclosure There are several online vulnerabilities databases and mailing lists which allow security professionals to keep updated concerning publicly disclosed vulnerabilities, security fixes and ongoing "in the wild" attacks. Most vendors also keep their own channels to communicate security advisories to their customers or users.[Secc, seca, Sym, Mit, osv]

1.2.3.3 High profile security breaches

This past few years have witnessed a rise in security breaches and public disclosure of private data - personal, financial and other sensitive information. These attacks were perpretated by many different organizations, under code names, and with various goals: political, public disclosure of secret or illegal actions by governments or businesses, or simply to create chaos.[wik, Gol11, CM, Hon11, Dwy11, Sch11]

An infographic of the high profile attacks and the public disclosed information can be seen on Figure 1.4. These attacks gathered a great deal of attention from the media and the general public, improving the overall concern from consumers about security and privacy of their information with online retailers and businesses, but did so by disclosing much private information and with high costs for the businesses in cause.

A significant and serious (yet not so circulated events) trend of attacks is targeting Supervisory Control And Data Acquisition (SCADA) and Industrial Control Systems (ICS). Attacks like the famous 'stuxnet' worm are becoming increasingly common and target critical infra-structure of any country, like energy powerplants and water distribution systems, showing a glimpse into (an almost science fiction-like) cyberwar between nations.[Sch10, Sai13, Neg12]

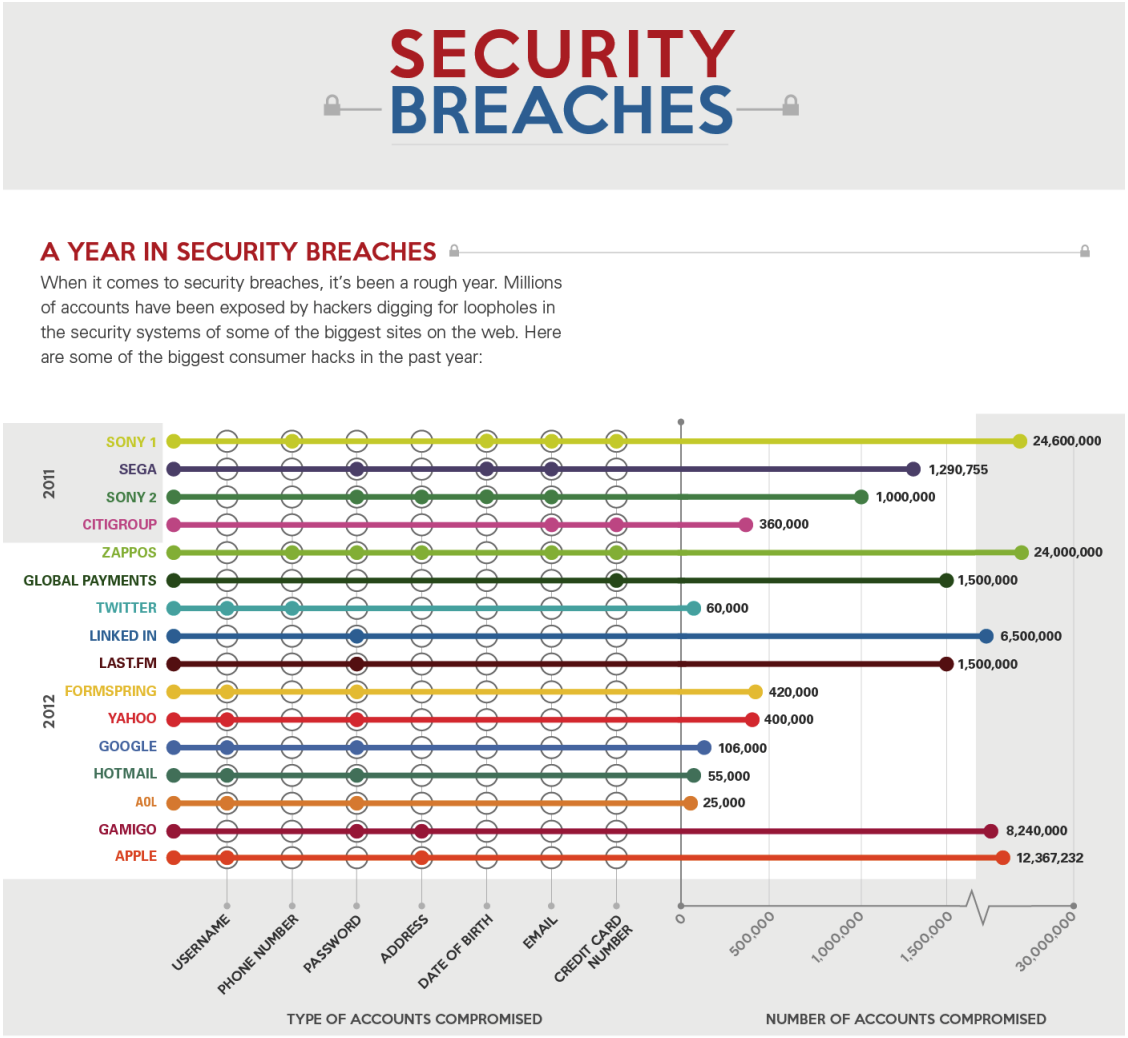

Figure 1.4: High profile attacks and public disclosed information (2011 & 2012).[Bil]

1.2.3.4 Underground community

Apart from public actions described in the sections above, there are two other significant and highly profitable parts of this industry that operate in private channels and contribute to its growth.

Exploit development is one of them. Security experts test various software of all kinds, from routers operating systems to web applications and Portable Document Format (PDF) readers to find vulnerabilities and develop programs to exploit those flaws in order to gain control over the systems, bypass authentication or validation or have the program execute another set of actions than those predetermined.
Upon finding a vulnerability, a security expert has to make a choice to publicly disclose it, to reach out to the vendor or to sell it privately - this is mostly a balance between ethics and exploit value (according to popularity/deployment rate of the software and usefulness of the exploit). There are professionals who publicy release details for every vulnerability they find, while others always sell that information and target the most valuable systems.[Sch00]
Relevant vendors have started to publicly address this by offering bounties for vulnerabilities made available to them in private so they can quickly patch the vulnerabilities before the exploit is published.[Neg12]

Another business kept usually on a low-profile note is the activity of botnets. A botnet consists of a big set of computer systems which are infected with a malicious program (zombie hosts) and respond to a central authority (command & control center) by automated means. Typically, this involves infecting hundreds or thousands of computer systems - unaware users install malicious software or a worm uses vulnerabilities to gain access and infect - with a program that then connects to some channel of communication with the master (the entity controlling the botnet); examples include Internet Relay Chat (IRC) channels or twitter accounts.[Insa, Kri, Bot05]
After building a sufficient large botnet, the master(s) usually rent “computing time” to leverage the botnet(s). This involves unsolicited bulk email (SPAM) sending, Distributed Denial of Service (DDoS) attacks and other similar activities which require distributed, exposable, unidentifiable (or unrelatable) hosts.

1.3 Problem Description

The problem addressed in this thesis is twofold. First, the transition to IPv6 is a complex feat that requires skilled effort and investment from ISPs; it is not only a technical challenge with very different and intricate transitional protocols but also a business constraint due to the implications it has on service availability to customers, expected lifetime of a

dual-protocol situation and cost of transition (acquisition of compatible hardware, training, etc). [Hus11a, Hus11b]
Secondly, IPv6 brings along many security issues with its renewed pool of IP addresses. It's a fundamental paradigm change in the way we think about internetworking, due to its security features and the impact on current industry standard practices.

A worldwide transition of the Internet to IPv6 is on its way and besides the technical challenge, there is also a limited and uncertain time frame to actively deploy, test and roll out IPv6 solutions before new IPv4 address allocation becomes unfeasible for ISPs. No one can tell for sure when adresses will effectively "run out" in a given region, so there is a need for proactive deployment of IPv6 addresses, transition solutions and migration methodologies.

Adopting IPv6 brings along several security concerns. It is foreseeable that operating systems will have problems supporting IPv6 robustly, when compared to our current IPv4 network stacks implementations. The latter have been developed, tested and scrutinized for more than two decades and have had time to mature. The IPv6 network stacks of the different operating systems are not only relatively new (beginning 10 years ago)[Bie, Kos] but also lack testing performance and security as *the* network stack actively in use. Many of the security products in use to actively secure networks (firewalls, intrustion detection systems (IDS), etc) are in a similar situation as their support for IPv6 (when available) has little testing. Limited use of IPv6 leads to few networks with real traffic available for testing of IPv6 features, both in the protocol and in the network software and devices available.

Aside from software support, IPv6 is also a liability for the technical staff in charge of network operations. Many are still not knowledgeable about IPv6, even having IPv6-enabled systems already connected (even unknowingly) to their networks as a result of operating systems' default settings - all modern operating systems enable IPv6 by default, so the majority of users has IPv6 support enabled without any knowledge of it. Finally, a lack of understanding of the new security features will allow for misconfigurations and incomplete security policies that easily create the opportunity for local-link traffic hijacking, denial of service and other attacks.

Moving to an IPv6 world will effectively transform our Internet into a dual-stack network, where we'll have to be wary of IPv4 vulnerabilities, IPv6 vulnerabilities, transition protocols vulnerabilities and even vulnerabilities caused by weak IPv6-support from commonly deployed software.

1.4 Motivation and Contributions

This is one of the biggest challenges the Internet has faced since it started. From its inception to this day, starting with first four Network Access Points (NAPs), its growth

has followed a quantitative strategy, adding more routers, servers, networks, Network Operations Centers (NOCs) and all the other necessary components to the infra-structure. However, that is no longer a viable solution and a global coordinated effort is needed to upgrade networks in a smart and scalable way.
To pursue that goal, a protocol designed in the 1990s is being used for the first time in the Internet of 2012. Not only is the protocol immature, but it's design has already demonstrated some faults.

This is an important time for both internetworking and information security, and the two must come together to enable a safe path for adoption in corporate and personal networks, in a way that is as simple as possible to the unknowingly user.[Hus11b] To fulfill that, a missing step is the study of different transition paths in terms of overall network security during and after the transition.
To that end, an infographic will be created, depicting and analysing different paths with security in mind, measuring consequences in security policies and industry best practices.

Learning with the lessons from the past, creating the network is not enough and steps must be taken to keep a safe environment throughout its growth. To that end, new threats need to be discovered, addressed and mitigated. As with every new protocol, only through creating the tools to quickly implement countermeasures and uncover new threats being used without public knowledge can we achieve preventive and defensive security effectively.

This thesis aims to clearly illustrate how ready (or not) is the Internet to move to the IPv6 protocol. This includes an analysis of the IPv6 protocol, transition strategies and security issues that have arised. While the IPv6 protocol was clearly not designed with security in mind, it's the near future of the Internet and by being prepared proactive action can be taken to mitigate at least some of its flaws.

Chapter 2

The IPv6 Protocol

2.1 Features

The IPv6 protocol introduces a fundamental shift in the way we see networks and Internet connectivity, and can not be mistaken for a simple extension of our pool of IP addresses. IPv6 features a large address space, endpoint-to-endpoint full connectivity (e.g. no Network Address Translation (NAT)), simplified address allocation and network segmenting.

2.1.1 Address space

In a pure IPv4 network, nodes are identified by a single IPv4 address, whereas some nodes (commonly routers and servers) are bound with more than one address. On an IPv6 network, the default condition is for any node (be it a workstation, a router, etc) to bind to several addresses.
An address is one of:

Unicast address uniquely identifies an interface on a given node. Any packet directed towards this address is delivered to that interface.

Multicast address identifies a collection of IPv6 interfaces - packets sent to this address are processe by every element of the multicast group.

Anycast address identifies a collection of IPv6 interfaces; however, differently from the multicast addresses, each packet is delivered only to one of the interfaces - the one which is closest (in terms of hops).

Note: whereas in IPv4 there were broadcast addresses, in IPv6 these are replaced by multicast addresses.

IPv6 uses a 128-bit long address, which yields a large address space: 2^{128} in total, compared to 2^{32} in IPv4. This allows for planning sub-networks configuration (i.e. subnetting) in terms of number of subnets required rather than the number of addresses required for a subnet, which brings a /64 prefix as the default and recommended option - some features of IPv6 like Stateless Address Auto-Configuration (SLAAC) even depend upon it.[TN98, Jus12]

As defined in RFC 4291, an IPv6 address is represented by eight groups of one to four 16-bit hexadecimal digits, separated by colons. Leading zeros can be ommited, provided there is at least one numeral in each field. Abbreviations are also possible for two or more 16-bit sequences of all zeros.[HD98, HS06]
For example, the IPv6 counter-part for IPv4 address 8.8.8.8 is shown in abbreviated, short and full form:

- 2001:4860:4860::8888
- 2001:4860:4860:0:0:0:0:8888
- 2001:4860:4860:0000:0000:0000:0000:8888

2.1.2 Packet format

The IPv6 packet format is show in Figure 2.1 side by side with the IPv4 packet format for comparison. Though it is outside of this thesis scope to thoroughly detail the changes, the packet structure was designed to simplify processing.[Wal99]
As an example, fragmentation processing was moved to the endpoints of a connection instead of the routers and extension headers were added to provide an easy way of adding options for routers - both these changes are meant to improve performance of packet processing and inspection.

As of RFC 2460, the available extension headers are shown in table 2.1. [DH98, KR98a, KR98b]

2.1.3 Multicast support

Multicast is an essential feature of IPv6, effectively replacing and superseding broadcast addresses, available in IPv4. While multicast was added in IPv4, mostly for delivery of multimedia, it's instrumental in IPv6.[Johb]
The IPv6 range FF00::/8 is reserved for multicast, and introduces fixed addresses for communicating messages to different scopes like global, network-local and link-local, conveying easy access to all local nodes on the same Local Area Network (LAN), all routers, etc.

Multicast is required for local configuration of addresses, both via SLAAC and Dynamic Host Configuration Protocol version 6 (DHCPv6): when using DHCPv6, a query

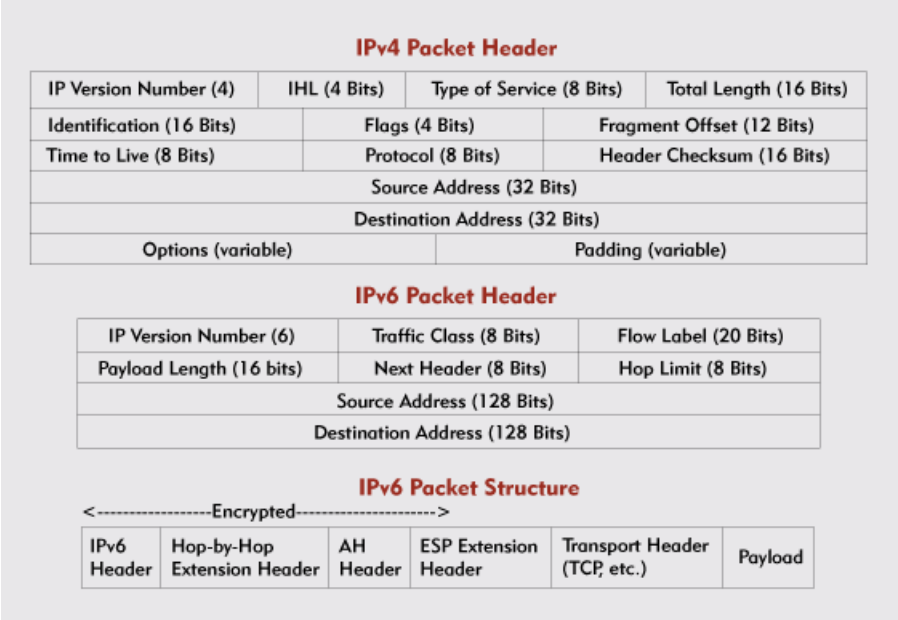

Figure 2.1: IPv4 and IPv6 packet header/structure comparison

Hop-by-hop options	optional information that must be examined by every node along a packet's delivery path
Routing	list one or more intermediate nodes to be "visited" on the way to a packet's destination
Fragment	to send a packet larger than would fit in the path maximum transmission unit (MTU) to its destination
Destination options	optional information that need be examined only by a packet's destination node(s)
No next	indicates that there is nothing following that header (payload is ignored)
Authentication header	provide connectionless integrity and data origin authentication for IP datagrams and protection against replays
Encapsulating Security Payload	provide a mix of security services in IPv4 and IPv6

Table 2.1: IPv6 extension headers and their purpose

to check for address clashing is emitted to a specific DHCPv6 multicast address; a similar query is made through Neighbor Discovery Protocol (NDP) (using a multicast address) when using SLAAC.

2.1.4 IPsec

Internet Protocol Security is a suite of protocols designed to secure communication, authenticate and safely exchange cryptographic keys over IP. [KS05, FS11]

Implementation of IPsec was initially and until recently mandatory for any IPv6 implementation. This is not to be confused with required: every implementation of IPv6 must support IPsec communication, but packet transit over IPv6 links needs not use IPsec.[J. 06]

In December 2011, RFC 6434 was published obsoleting the previous RFC for IPv6 Node Requirements and removing the requirement for IPv6 implementations to support IPsec.[JLN11]

2.2 Companion protocols

The IPv6 protocol brings along several new protocols, both at the Link layer and the Internet layer. Following, a brief analysis of the most relevant ones is shown, since they are required to fully understand what implementing IPv6 in our networks brings along.

2.2.1 Internet Control Message Protocol version 6 (ICMPv6)

The Internet Control Message Protocol (version 4) was designed to enable diagnostic and error control for network devices. As an example, it is used to signal a packet's Time-To-Live (TTL) exceeded[1]. Ping, a common utility in network diagnosis, uses Internet Control Message Protocol's (ICMP) ECHO request and reply messages to check host reachability.[Pos81, Bra89, Ope12])

A *shell* designates a computer program which allows control over a computer system through command line commands. In network security, a shell represents one of two kinds:

bind shell the program binds itself to a network address on the computer system, allowing remote access (optionally authenticated) and control. Connecting to a bind shell from outside a given network can be difficult due to firewall filtering.

reverse shell the program connects to a predefined host to receive commands, allowing for remote control and bypassing inbound firewall filtering (since it connects to the outside).

ICMP has become a popular protocol for reverse shells communication, since it is rarely filtered in firewalls, compared to TCP and User Datagram Protocol (UDP) communication.[SNL+]

ICMPv6 plays an instrumental part in IPv6, as features such as automated address configuration and neighbor discovery rely on it to operate correctly.

[1] The Time To Live field in the IPv4 header marks how many hops the packet is allowed to go before failing to reach its destination, and is decremented by one on each hop.

2.2.1.1 Neighbor Discovery

There are several problems regarding neighbor (e.g. nodes on the same link or network) interaction on IPv4 networks, forcing hosts to rely on Address Resolution Protocol (ARP) and ICMP to discover and keep a current list of near-by nodes and routing tables. [NNSS07, Orab]
IPv6 is designed to provide local network discovery inherently, with key features such as:

Router discovery which allows nodes to locate routers on an attached link (i.e. LAN);

Prefix discovery to discover the collection of prefixes available on-link; nodes use prefixes to distinguish destinations on the attached link from those available only through attached routers;

Parameter discovery for learning sensible values for local link parameters (e.g. MTU) or Internet parameters (e.g. hop limit);

Address autoconfiguration for stateless (e.g. automatic) configuration of an IPv6 unicast address when joining a network;

Address resolution allows discovery of the link-layer address of on-link neighbor given only the destination's IP address. Note: this does not work with multicast addresses;

Next-hop determination maps IP destination into an IP address of the next neighbor to which the traffic should be sent: a router on the path or the destination itself;

Neighbor unreachability detection tests connectivity host-to-host, router-to-host and host-to-router. It allows an alternative path to be chosen if there is a problem reaching a router, by trying alternate default routers;

Duplicate address detection to check whether a desired address is already in use by another node;

Redirect for routers to provide a better alternative than itself to reach a given destination.

The Neighbor Discovery Protocol defines five different ICMP packet types to achieve these features: a pair of Router Solicitation and Router Advertisement, a pair of Neighbor Solicitation (NS) and Neighbor Advertisement (NA) and a Redirect message: [NNSS07]

Router Solicitation is used by hosts when joining a network to request immediate generation of Router Advertisements (RAs);

Router Advertisement is issued by routes either periodically or in response to a Router Solicitations (RS); it serves the purpose of announcing a router's presence, various link parameters, and various Internet parameters;

Neighbor Solicitation is sent by a node to determine the link-layer address of a neighbor or to confirm a cached address is still reachable. Neighbor Solicitations are also used for Duplicate address detection.

Neighbor Advertisement is sent either as a reply to a NS or to announce a link-layer address change.

Redirect is sent by routers to inform hosts of a better first hop for a destination.

2.2.1.2 StateLess Address Auto Configuration

StateLess Address Auto Configuration (SLAAC) allows a host to perform a series of operations when it joins an IPv6 network.
It's through SLAAC the host obtains a link-local address, information for configuring its address and confirms the address it is about to assign for itself isn't already in use in the network. [TNJ07, Oraa]

SLAAC enables a host to generate its own addresses by using prefixes advertised by local routers combined with a self-generated interface identifier, reaching unique addresses for the given subnet. [Oraa]
Before assigning a generated address, a host follows the duplicate address detection algorithm, by issuing NS messages to the link-local network and checking for replies. This technique can be abused, as is detailed in Section 4.2.

2.2.2 DHCPv6

DHCP is a protocol for providing nodes with network configuration information through network links. Configured addresses are "leased" for a period of time after which they need to be renewed or changed to a different one. [RBV+03a]

DHCPv6 takes advantage of IPv6 features for better performance and usefulness: [Ker06]

- communication happens via link-local addresses and facilitates obtaining required network configuration information
- multicast allows for easier direct communication, instead of broadcast requests.

DHCPv6 is radically different from DHCP, and adds several relevant features to an IPv6 network: [RBV+03a, Joha]

operating mode DHCP can operate together in different modes:

stateless mode to provide additional information to stateless address auto configuration

stateful mode to provide network configuration information and addresses to nodes.

relaying a node can act as an intermediary for DHCP messages between clients and servers on different links

unique identification DHCP introduces DHCP Unique Identifier (DUID) and Internet Association identifier (IAID) as tokens for uniquely identifying clients and interfaces on a link; this is in line with IPv6 expectation for nodes to configure multiple addresses.

privacy support Temporary Addresses are introduced and assigned outside the IAID number space.

authentication of messages built-in support for authenticating messages between clients and servers.

SLAAC interoperability, as can be easily guessed from the list above, is possible and easily achievable. However, the following two problems may arise [Ker06]:

- SLAAC provides a limited amount of information to nodes. DHCPv6 was designed to allow for extension as the need arises and its flexibility can be an advantage in some scenarios;
- unmanaged allocation of addresses can be problematic in corporate networks or in an auditing situation, for example. DHCPv6 allows more control over this when compared to SLAAC

Overall, implementing DHCPv6 and/or SLAAC needs to be put in the context of the network for correct evaluation of the better solution. There is not one clearly better than the other.

2.2.3 DNS support

2.2.3.1 Quick introduction to the Domain Name System (DNS)

The Domain Name System allows users to type `iamto.me` instead of 195.200.253.133 - essentially making the World-wide Web (WWW) available to common people since it's much easier to memorize and navigate.

DNS works as an hierarchical structure of servers responsible for keeping updated records for a given DNS zone. These servers provide a public DNS service who listens to queries in the form of hostnames and replies with the correspondent address if it is in its records or if it can get the information from another DNS server.[Zyt]

DNS zones are split by TLDs (top-level domains) like .com, .org and .net and ccTLDs (country-code TLDs) like .pt, .es or .me. Keeping updated ccTLD records is the responsibility of each country, through one specific entity (Foundation for National Scientific Computing (FCCN) in the case of Portugal, for example). This entity keeps a main registry of all the existent domains under that country code and provides services for registration, renewals and dispute about those domains.[IAN]
Additionally, each domain has two or more authoritative nameservers. These servers are the ones which keep the most up-to-date information of the DNS records for that domain and are regularly queried by others to propagate changes throughout the network. As a side-effect of this, if the address for *google.com* changes, it will take a few hours before it is fully propagated throughout the Internet.[Zyt]

2.2.3.2 DNS and IPv6

DNS is a very important part of the daily interaction between users and the Internet, and that relevance has only gotten bigger with the introduction of IPv6. An enormous address space compared to IPv4 and long, difficult to remember IPv4 addresses turn DNS records into essential tools to reach hosts.

In addition to public records, network operators may also adopt existing or new solutions for keeping a list of internal, non-publicly reachable hosts to help with network maintenance and operation. As an example of this, network printers are commonly searched on the network by scanning the current subnet, which is unfeasible in an IPv6 network. As such, it's expectable that DNS will be used much more heavily on IPv6 than it currently is. [Zyt, Mic, Don]

In related work, DNSSEC is a set of DNS extensions to add data origin authentication and data integrity to the Domain Name System. The importance of this work is related not only to IPv6, as it is currently deployed for example to fight SPAM with success, but the need to employ IPv6 DNS servers and DNSSEC extensions correctly is of utmost importance for laying the infrastructure for the Internet transition to IPv6. [AAL$^+$05, Ica, Dav08, Viv03]

2.2.3.3 IPv6 records

To support IPv6, DNS was extended with new kinds of records and a new domain for reverse lookup. However, multiple RFCs exist leaving us with: [CH00, iH01, THKS03]

AAAA record (since 1995) a new resource record type, to map a domain name to an IPv6 address. Equivalent to the A record for IPv4 addresses.
Example form:

```
$ORIGIN X.EXAMPLE.
```

```
N            AAAA 2345:00C1:CA11:0001:1234:5678:9ABC:DEF0
```

A6 record (since 2000) a new resource record type, to do the same as the AAAA record, but with a different design approach.
Example form:

```
$ORIGIN X.EXAMPLE.
N            A6 0 2345:00C1:CA11:0001:1234:5678:9ABC:DEF0
```

IP6.ARPA domain a new domain to look up IPv6 addresses. The intent is to provide a mechanism to map an IPv6 address to a host name, similar to IN-ADDR.ARPA for IPv4.
Example for address *4321:0:1:2:3:4:567:89ab* is:

```
b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4
                                                    .IP6.ARPA.
```

The other record types are now expected to return results for both IPv4 and IPv6 addresses for the queried host name.

Chapter 3

Transition Strategies

The path to full IPv6 adoption and deprecation of IPv4 is not straightforward. Each network operator must deliberately choose when to start the transition, taking account availability consequences, migration strategies, business constraints and operational constraints.
In such diverse environments as computer networks are, this raises many questions and delays the natural transition to the new protocol. Different strategies are adopted: IPv6 traffic tunneling, dual-stack networks or reuse of IPv4 addresses in "smarter" ways. While some parts of the Internet (and the World) are cruising full-speed towards IPv6 operation, others are still learning what that can mean for their networks.[Husa]

The fact that this stack of new protocols is still actively being worked on[1] complicates matters. People are naturally afraid of implementing insecure and/or untested solutions, waiting for more mature solutions to emerge before adopting one.
Vendors play a key role in this, as they are commonly the bridge between the scientific world - where the IETF fits - and the business world. Their acknowledgment of new protocol extensions, active deployment of corresponding products or firmware updates and communication with their customers influences the evolution of this scenario.[Too]
An interesting point was made by Huston (Asia-Pacific Network Information Centre (APNIC)) and Kolkman (NLnet Labs) at Latin American and Caribbean Network Information Centre (LACNIC) XVI (Oct. 2011), illustrating vendors and ISPs might have business interests in keeping IPv4 as the main protocol of the Internet for years to come, which explains all the information about how slow the transition must be and how important IPv4 still is. After all, giant corporations showed us with the World IPv6 Launch day that dual-stack is possible to implement successfully at large-scale networks.[HK]

Lastly, the transition path for a network needs to be considered carefully according to its context: what kind of traffic it serves or traverses it, what are the technical capabilities of end-users, and other operational requisites. Business constraints must also be taken

[1] Curious fact: if you take a look at the references, you'll find current IETF I-D documents which will expire in 2013 and are currently being discussed.

into account, conveying expected return-of-investment figures for invested hardware and human resources' time.[Husb]

3.1 Client-side support

Client-side support for IPv6 is always going to be the hardest part of transitioning to IPv6. Most end-users are non-technical and unable to troubleshoot simple network problems, and naturally have no desire to do so - they just want connectivity and availability at all times.

Software and services both direct and depend upon user engagement, creating a chicken-and-egg problem: while one does not move to IPv6, the other will not follow.

3.1.1 Dual-stack

The optimum scenario for a end-user wanting to connect to an IPv6 network and access IPv6 resources is the dual-stack network. This allows for IPv4 and IPv6 connectivity at the same time, allowing requests to fall back on IPv4 if a connection fails, a good approach while some resources are not available through IPv6. [Husb]

Recently there has been a new Internet Draft (I-D) proposal, "Happy Eyeballs", which takes this even further, recommending a different algorithm for requesting resources from the network to satisfy dual-stack network users: [WY12]

- when a node needs to request a network resource, it first finds both IPv6 and IPv4 addresses for the given node through DNS or other means
- it initiates connections in parallel, through both network stacks
- the fastest connection to be established is elected to retrieve the resource, and the other connection is cancelled.

This way, the end-user will always see content retrieved the fastest way possible, providing a seamless experience whether resources are available through IPv6 in a satisfying way or not.

From the security point-of-view, this is the best scenario because its the simplest one to manage and audit. However, users must be prepared and educated about the absence of NAT in IPv6. Most customer premise equipments (CPEs) automatically share one IPv4 address - the outbound assigned address - with the hosts of the internal network through NAT, and filter almost every traffic inbound except for ongoing sessions.
In IPv6 this is no longer the situation as end-to-end connectivity is expected, leaving dual-stack users in a mixed situation: NAT and a default firewall on IPv4, directly accessible in IPv6.[Husb]

3.1.2 Tunnels

Network tunnels are a solution for technical users to access IPv6 resources even if their ISP does not provide IPv6 connectivity at this point. These are not a long term solution, as connectivity can become problematic due to firewall filtering, etc..

3.1.2.1 6to4 tunnels

6to4 is a tunneling protocol supported by an addressing structure - IPv6 addresses for 6to4 hosts use the 2002::/16 IPv6 prefix, and embed the 32-bit IPv4 address of the host in the next 32 bits, effectively carrying the IPv4 address inside the IPv6 address.[Husb]

These encapsulated IPv6 packets are tunneled through IPv4 networks through encapsulating: each packet gets an outer IPv4 packet which uses IP protocol type 41, reserved for IPv6 packets tunneling. Through an IPv4-to-IPv6 relay, which must be assigned a public IPv4 address and is always 192.88.99.1 on the local network, the original IPv6 packets are stripped of the IPv4 temporary encapsulation and sent to the IPv6 network, where normal routing and operations take over.[CM01, CD98]
As the destination address of the returning packet is on the 2002::/16 prefix, which is an anycast relay address, an IPv6-to-IPv4 relay will pick up the packet from the network, extract the IPv4 destination from the IPv6 destination address, encapsulate the IPv6 packet with an IPv4 packet for protocol 41 and then route it to the IPv4 destination address, which will be the 6to4 host on the originating network.

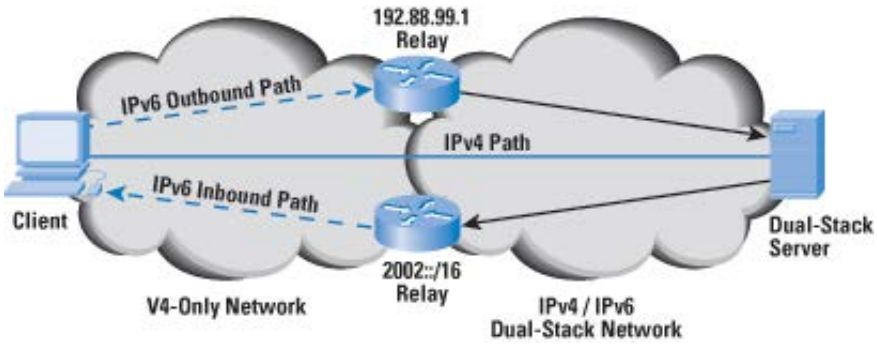

Figure 3.1: 6to4 Tunneling Architecture[Husb]

Overall, given that 6to4 depends upon complicated operation of traffic relays for successfully traversing the network, and the strong possibility of encountering filtering issues given the uncommon type 41 packets, 6to4 is not a recommended solution for users wanting to connect to IPv6 through IPv4 networks.[Car11]

3.1.2.2 Teredo tunnels

Some networks enforce a local IPv4 NAT and do not support 6to4 traffic. Teredo, much like 6to4, is a tunneling protocol supported by an addressing architecture, except it is designed to support NAT traversal.[Hui06, Husb]
All Teredo addresses share the common 2001:0000::/32 prefix, followed by the 32-bit IPv4 address. The IPv6 interface identifier encodes NAT-related information - the NAT type, the external UDP port number to reach this client (to the relay's knowledge, this the NAT binding port) and the external IPv4 address to reach this client (again, to the relay's knowledge, this is the external IPv4 the NAT bounds this client to).

A Teredo network consists of:

Teredo client a host connected to an IPv4 network and behind a NAT, which initiates the connection;

Teredo server a host on a publicly reachable IPv4 address, which facilitates communication with the relay;

Teredo relay which bridges traffic to the IPv6 networks

The Teredo traffic exchange relies on ICMPv6 for the initial packet exchange negotiating a connection according to the type of NAT. Further traffic is based on UDP (as most NAT devices filter anything non-TCP or UDP): packets are encapsulated with an IPv4 and UDP header, and the IPv6 packet travels as the UDP payload. Figure 3.2 shows an example traffic exchange for a Teredo connection.

Teredo suffers from the same challenges as 6to4 in operating supporting infra-structure, making it a viable alternative to 6to4 in restricted NAT environments. By using UDP as its transport protocol, it also reduces the risk of filtering interference and raises the chance of successful communicating over IPv6 networks.[Hui06, TKH10, Tha11]

3.1.2.3 Tunnel brokers

For more technical users, the foolproof way of configuring IPv6 connectivity (even if somewhat limited) is by using tunnel brokers[2].
Manual configuration provides a greater depth of understanding of the network configuration and direct tweaking of necessary settings according to the network context.

Traffic is simply prefixed with a IPv4 packet header which contains:

- the source address of the tunnel ingress point
- the destination address of the tunnel egress point

[2]Like SixXS: http://www.sixxs.net/

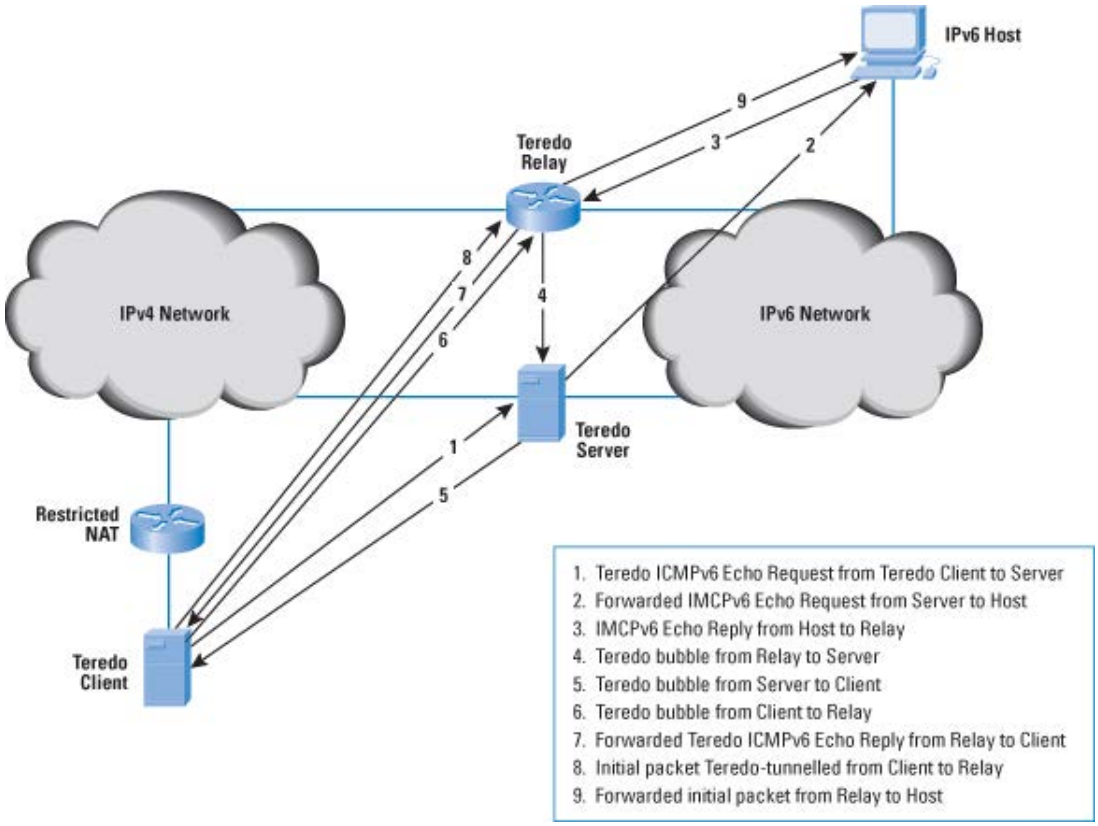

Figure 3.2: Teredo Tunneling Architecture[Husb]

- the IP protocol field contains 41, marking the packet as an IPv6 tunneling packet.

Routing is operated normally for IPv4 packets, and the IPv4 packet header is removed or added accordingly at the endpoints of the tunnel.

3.2 Internet Service Providers

3.2.1 Dual Stack

Adopting a dual stack environment is clearly the best path for any ISP wishing to adopt IPv6 at this time; however it is not a trivial operation.
For dual-stack operation it is essential that feature-parity is provided for every service the ISP provides on IPv6 and IPv4. This does not mean only the customer services and resources, but also internal accounting, routing systems, peer-exchange partnerships, datacenter hardware, monitoring and everything else involved in operating an ISP.[Husb]

Significant costs in both hardware, training, human resources' time and effort are to be expected of such an enormous set of tasks. It means doing a complete rework of all the ISPs infrastructure and processes, and this process can take months or even years to accomplish successfully.[Husb]

Since time is a factor, most ISPs are opting for a segmented, layered transition and investing in one of the solutions below as an intermediate solution for doing business.

3.2.2 IPv4 address sharing

Reusing current IPv4 networks in a more efficient way is a possibility for ISPs to extend their time window to (fully) implement IPv6 on their networks. As such, there are several methods to do so currently in use:

3.2.2.1 Dual Stack Lite

Dual Stack Lite allows ISPs to continue to provide IPv4 addresses to customers while moving all the ISPs network infrastructure to IPv6-only. IPv4 packets need to be encapsulated in IPv6 at the customer's CPE as they enter the ISPs network and decapsulated as they exit through the routers gateway into the public IPv4 network.[DDWL11, Dua10]

The NAT translation, now commonly placed at the customer's CPE moves to the ISPs gateway, providing an extended possibility for reuse of addresses by the ISP. This approach eliminates common NAT problems with deep packet inspection and allows for flexible scaling as customers do not require an IPv4 address anymore. It can, however, disrupt applications that rely on Universal Plug and Play (UPnP) or otherwise port forwarding configurations.[Doy10]
Another significant constraint of Dual-Stack lite (DS-Lite) is that it will require CPE replacement for ISPs using non-IPv6 capable equipment, which can be a big investment upfront.

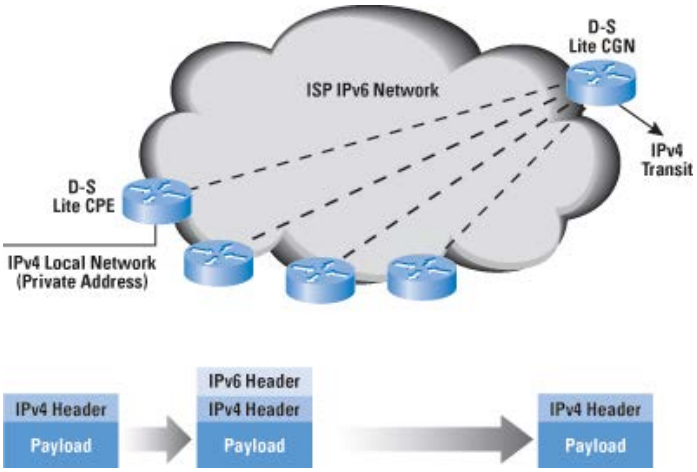

Figure 3.3: Dual Stack Lite Architecture[Husb]

Security wise, this is twofold: while the carrier NAT provides a first layer of security from traffic outside the ISPs network, it creates a single point of failure where all customers can be affected if the ISPs gateway fails.

3.2.2.2 CGNs

Carrier Grade NATs, or CGNs for short, take from the current *status quo* for deploying customer premises networks: a NAT-capable CPE allows for sharing one address across all users of that link. So why not build a NAT-upon-NAT? [JH11]

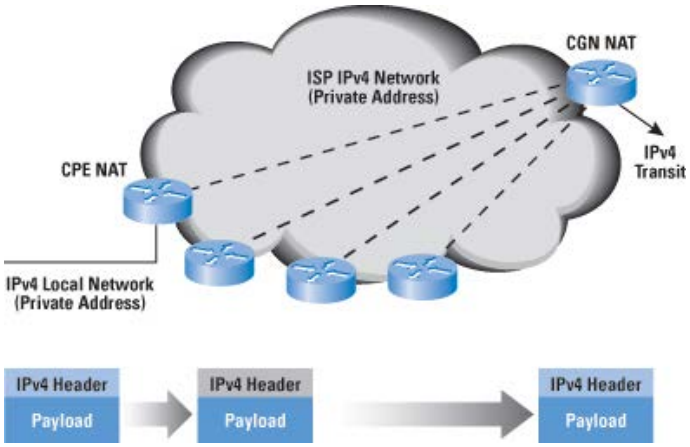

Figure 3.4: CGN example Architecture[Husb]

Using a CGN allows to share one public address across multiple customers, which in turn share that address with their internal network. Nothing changes for the customers, and the investment for the ISP would be minimum when compared to other alternatives.[jun11]
There are operational costs to be considered, though: [SYM+12]

- NAT over NAT can complicate or disrupt application behavior
- NAT binding times can become problematic in managing address allocation within the ISPs network
- as it's not easy to move NAT clients from one device to another, service resilience becomes critical
- security attacks (inside or outside) can have disastrous effects if they consume available NAT resources
- scalability is a concern within a somewhat short timeframe

CGNs, although popular, are merely a band-aid solution and not a cure for IPv4 exhaustion. As more and more addresses are needed, scalability and resilience will become critical issues and other solutions will have to be devised.

3.2.2.3 Address-plus-Port

The Address-plus-Port approach reuses an IPv4 address by limiting the range of ports a given CPE has assigned to it and can communicate on. Given minor changes to CPE

software, an ISP internal NAT can be configured for all customers, with several customers sharing the same address but with different port ranges. [R. 11]

Network traffic flows the same way as today IPv4 networks with the following exceptions: [R. 11, Husb]

1. CPEs are assigned an (internal) address and port range by the ISP, mapped to an ISP external address through NAT
2. the customer address identifier on the NAT is a combination of address and port range
3. CPEs must emit outgoing traffic only using the assigned range of ports

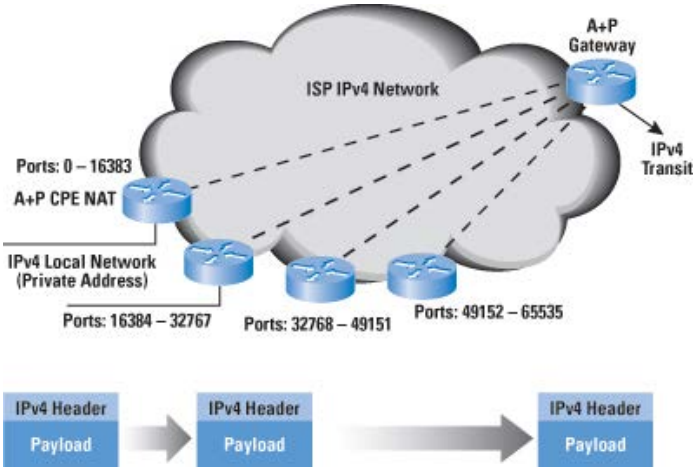

Figure 3.5: Address-plus-Port Architecture[Husb]

This architecture can be enhanced (according to context) in several ways, by combining other address sharing techniques to optimize scalability. However, security, scalability and usability must be weighed with appropriate context before mixing address-sharing techniques instead of focusing on IPv6 adoption.[Husb]

3.2.3 Protocol translation

Different approaches to protocol translation between IPv4 and IPv6 have been attempted, with variable popularity, but still worth mentioning. A short list shows different approaches: [Orac, Husb, Nor00]

SIIT Protocol Stateless IP/ICMP Translation Algorithm[Nor00, LBB11]

NAT-PT Network Address Translation - Protocol Transition (now deprecated)[TS00, AD07]

NAT64 Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers, a similar approach to NAT-PT [BMvB11]

Chapter 4

IPv6 Security

Designing an Internet Protocol is a daunting task, which few dare to attempt. Even though several people typically collaborate to produce a document and there is sufficient peer-review, some errors happen to slip by. When they do so in such important RFCs, they are bound to be discovered and updated in later specifications.[Hou10]

Since the first IPv6 protocol RFC, several other RFCs and drafts have appeared to correct specific vulnerabilities or to enhance operation issues. While this is good to formalize improvements of the protocol, it brings along a major problem when the updates are specific to protocol implementation: it means every implementation of IPv6 (or any other protocol, for that matter) ever made needs to be updated accordingly.[ASNN07, Kri09, KWK+12, ACJR11, AB10]

In order for protocol specification updates to work, every vendor, network software producer, operating system developer team, etc. must take care to stay up to date with this information, and be proactive to implement the changes and roll them out to customers and/or users.

Since this is not feasible for many scenarios, updating a protocol RFC or even obsoleting it is no guarantee it will be deployed to every network stack. As such, vulnerabilities in the protocol design are very hard to mitigate properly.

4.1 Design flaws

4.1.1 Design goals

The design of IPv6, at the time of its proposal, contemplates network operations and security with the mindset of 1995. It contemplates the following changes regarding IPv4: [DH95, DH98]

Expanded Addressing Capabilities redesign the IP packet to provide a (much) larger address space; this was the main goal given the predicted IPv4 address depletion;

Header Format Simplification in order to simplify processing and enhancing performance;

Improved Support for Extensions and Options which allowed to simplify the header, options to be moved to extension headers and leave room for further extensions;

Flow Labeling Capability for easy labeling of streams of packets which need special handling;

Authentication and Privacy Capabilities which lay groundwork for security mechanisms, but essentially reduced to encryption-equivalent features.

4.1.2 Multicast and IPSEC

At the time, the IPv6 protocol RFC (2460) was compliant with the "Security Architecture for the Internet Protocol" RFC (2401), which does not support multicast in a standard way and left room for further definition in later documents.[KA98, HD98]
The IPv6 Protocol relies on multicast communication for local-link operations (explained earlier) and also states IPSEC as mandatory. Since IPSEC multicast operations was not clearly defined at the time, this leaves a huge gap in the specification.[HD98]

Further development of multicast support for IPSEC continued but was only resolved definitively a decade later, with RFCs 4301 (2005) and 5374 (2008).[KS05, WGI08, BCHW02]

4.1.3 Private addresses

The first attempt to define private addresses for IPv6 were Local-User IPv6 Unicast Addresses, later deprecated due to the ambiguity of addresses and fuzzy definition of *sites*, which defined the boundaries for routing these addresses. [HD98, HD03, HC04]

Private addresses are now defined through Unique Local Addresses, for use in context of: [HH05, Hus05]

- addressing for isolated networks (e.g. IPv4 private networks)
- persistent local-context addresses (e.g. IPv4 DHCP fixed leases)
- interconnection of local network contexts

4.1.4 Stateless Address Auto-configuration

Stateless Address Automatic Configuration is one of the major new features of IPv6. It moves address allocation to the core of network protocols instead of an upper layer alternative (i.e. DHCP in IPv4). [TNJ07]

Security concerns of network operators about automatic assignment of addresses in their networks need to be balanced against network availability, and automatic configuration is a huge step forward in the direction of connectivity everywhere for any device.

4.1.4.1 DNS configuration

The first major problem of SLAAC is DNS configuration. DNS information is not provided by SLAAC's first draft, leaving two options for hosts [TN98, TNJ07, RBV+03a]:

1. use locally-configured DNS servers in every network or reach hosts through their IPv6 addresses
   - using IPv6 addresses instead of DNS records is not acceptable for most users
   - using the same public DNS servers everywhere creates a great dependency upon them
   - setups in which network operator maintain a private set of DNS records for their domains (for internal hosts) can't work unless network nodes use local DNS servers[1]
2. obtain an address through DHCPv6 or similar protocol
   - will automatically revert the address allocation being part of the Internet layer
   - complicates ubiquitous connectivity since hosts need to be configured or somehow discover what sort of address allocation method is in-place when connecting to a network

4.1.4.2 Privacy issues

The second issue raised by SLAAC is a privacy issue in address allocation. The algorithm used to devise a node's address generates predictable addresses for nodes which have a network interface with an embedded Institute of Electrical and Electronics Engineers (IEEE) identifier, which may be used to track a host activity and mobility through different networks. [ND01]

To fix this problem Privacy Extensions for SLAAC were developed, to the purpose of: [ND01, NDK07, Gon12d]

interoperability by not changing the basic behavior of addresses generated via SLAAC

short-lived random addresses generated based on a common (random) identifier, to use for outgoing connections. Any address will expire after a few hours or days, not being used for further outgoing connections

[1] Example: Berkeley Internet Name Domain's (BIND) view clause - http://ftp.isc.org/isc/bind9/cur/9.9/doc/arm/Bv9ARM.ch06.html

hindering address prediction by producing random identifiers in a way that makes it difficult to give educated guesses on possible generated identifiers

performance by setting a common identifier as a boundary for address generation in order to prevent joining too many multicast groups which could cause the network interface to enter promiscuous mode[2]

Using DHCPv6 with randomly assigned addresses is also a possible solution to this privacy issue. [ND01]

Predictable addresses can be beneficial for configuring access control, debugging network problems, tracking malicious activity and other similar scenarios where the goal is to associate and/or allow or disallow network activity with a given node.
Privacy addresses can highly difficult such activities, so an algorithm to generate stable privacy addresses is currently undergoing discussion by an IETF working group. This algorithm essentially aims to substitute IEEE identifiers in the context of SLAAC, and declares that: [Gon12d, Gon13a]

- the generated interface identifiers remain fixed on a given subnet
- the generated interface identifiers must not depend on underlying hardware
- different prefixes result in different generated interface identifiers
- interface identifiers generation prediction must be difficult

4.2 Relevant vulnerabilities

In this section the most relevant vulnerabilities for the IPv6 protocol and companion protocols are presented. Most of the attacks require an attacker to have a local-link, but there are some remotely exploitable vulnerabilities.

Most attacks result in protocol updates or extension, yet as stated previously that does not mean automatic corrective measures in existent devices and operating networks.

To test and attack IPv6 networks there are two main software toolkits available: [Hau13, Si6, Gon13h]

THC IPv6 toolkit is a set of tools for exploiting specific attack vectors in a straightforward way and is penetration testing oriented

SI6 Networks' IPv6 Toolkit is a flexible set of tools designed to allow different vectors (user provided) in a research oriented way

[2] A network interface in promiscuous mode listens to all traffic that it "sees", giving inferior performance than in normal operation mode.

4.2.1 Neighbor Discovery attacks

Neighbor Discovery is vulnerable to many attacks, targeting both hosts and routers. Some attacks result in DoS attacks, others threaten network performance and yet another set focuses on traffic hijacking. [PKN04]

These attacks can be mitigated by implementing solutions like RA Guard and Secure Neighbor Discovery protocol (SeND) following best practices, as well as Layer-2 switches filtering of NA and RA messages accordingly. None of these solutions is foolproof, but each step enhances security and reduces the risk of having compromised nodes in a network. [Gon13f]

Duplicate address detection tampering When configuring a new address or renewing a current one, a host sends a NS to confirm it is not currently in use. An attacker can simply respond to such NS messages, causing the requesting node to fail in assigning an address to itself.[Gon13g]

Default router hijack An attacker can send unsolicited RAs or respond to RSs and advertise a given address as the default router. This can result either in a DoS, when the address is an inexistent or unresponsive address, or in traffic hijacking by assigning the address of a compromised node.[Gon13e]

Address spaces By sending unsolicited RAs or responding to RSs, an attacker can advertise both on-link prefixes as well as SLAAC address configuration prefixes. These actions will result in DoS attacks as the traffic originating from these bogus addresses will either be filtered or have an invalid return-path for the emitting node. [Gon13c, Gon13b]

Disable routers Sending crafted RAs, NA or RSs while spoofing the source address as a given router on the network can result in nodes removing the impersonated router from their routing table upon receiving these packets. This would would work together with other attacks to facilitate traffic hijacking or as a DoS attack. [Gon13d]

Forwarding loops Using neighbor cache poisoning and multicast communication (actually the Ethernet broadcast address), a forwarding loop can be achieved causing two (or more) routers to enter a chain reaction of emitting traffic until the Hop Limit is reached. This can result on a DoS of the network link or of the routers affected. [Gon13f]

4.2.1.1 ND protections' attacks

Rogue RAs are a problem in IPv6 networks not only due to malicious attacks but also of unknowing users who misuse resources. In an attempt to fix these problems, RA Guard was developed as an Internet Standard. [CV11, LAdVPM11, Ipv07]

However, it is still possible to circumvent it so a secure deployment of RA Guard continues to be studied and proposed. Two ways of evading RA Guard are currently known: [Gon12b, Gon12a]

IPv6 Extension Headers By using IPv6 Extension Headers in RA messages (even though there are currently no legitimate uses), some RA Guard can be evaded by prefixing an RA message with any Extension Header because of the way they identify RA packets. See Figure 4.1 for an example.

IPv6 Fragmentation An attack vector which has been found to work against all RA Guard implementation is by fragmenting the RA message, which would lead to Layer-2 devices being unable to identify it as such. See Figure 4.2 for an example.

Figure 4.1: RA Guard Evasion - Fragmentation technique[Netb]

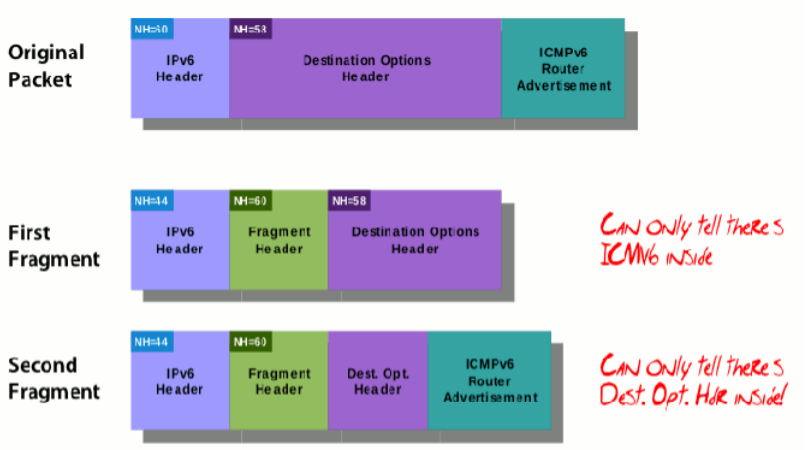

Figure 4.2: RA Guard Evasion - Fragmentation technique[Netb]

SeND was designed to counter the threats of the Neighbor Discovery by standardizing a set of different messages and techniques. [JKZN05, PKN04]

Operating SeND relies in the Cryptographically Generated Addresses (CGAs) feature. This technique uses a cryptographic hash of a public key associated with a given IPv6 address to generate a unique identifier.[KGAS02, Aur05]

Although CGAs are generated only once for each address, given this is a resource-greedy process and key length is variable (the client node can choose the strength of the key), sending crafted packets to cause heavy CGA calculation causes a Denial of Service. [Sta11, CISb, Bow11, CISa]

4.2.2 Routing Header Type 0 attack

The IPv6 Protocol standard includes the "Routing Header" extension header, which has several types: [Cis07, BE07, Sav02a, DKS07, ASNN07]

Type 0 which includes intermediate routing addresses

Type 1 currently unused, a legacy type from a DARPA project

Type 2 used for Mobile IPv6

Type 0 Routing Header (RH), commonly referred to as RH0, can be abused to keep a stream of packets oscillating between two RH0-processing routers or hosts many times. Moreover, since RH0 allows for including multiple intermediate node addresses and the same address multiple times, this stream of packets affects not only the two hosts in question but all hosts in between possibly causing a DoS.
This possibility and its implications were considered severe enough to warrant deprecation of RH0 entirely, as of RFC 5095.

4.2.3 DHCPv6

DHCPv6 is, by design, inherently open to several kinds of attacks by local network nodes and possibly remote ones. Attacks can target client nodes, server nodes or both, causing a DoS or helping with man-in-the-middle (MITM) attacks. [RBV+03b, A.J]

Most attacks can be mitigated by following good security practices and combining with other security measures like SeND. Furthermore, the IETF working groups continue to develop safety enhancements for DHCPv6 or companion techniques like DHCPv6-Shield.[JS12, GL12]

4.3 Other issues

Aside from the problems detailed in the previous sections, IPv6 presents other challenges for current networks and affects networking security in other ways. Other issues currently being researched or actively exploited: [GT12, Gon12c, OvVdBP, Heu12, Gon12e, Ant, Atl12, DKS, Sav02b]

Address and host enumeration with such a large address space, subnet scanning is no longer feasible (time constraint), so new techniques must be developed. Currently, work has been done by using Autonomous Systems registries and DNS enumeration through wordlist bruteforcing for enumerating remote hosts. There is also a problem in most ICMP implementations, allowing easy detection of alive nodes on the local link.

Firewalls rules bypassing clever use of IPv6 fragmentation options and the way network router devices process them can cause light packet inspection allowing IPv6 packets that would otherwise be dropped to be accepted by a firewall for protected networks.

ACL bypassing using extension headers sometimes allows complete ACL bypassing

Dual-stack environments the combined operation of IPv4 and IPv6 in the same environment can cause several issues of sensitive traffic (e.g. Virtual Private Network) leakage from one environment to the other and interference between the networks.

Chapter 5

Conclusions

This chapter tries to expose the current state of transition, what can be expected to follow as the IPv6 transition continues and highlights possible research paths taking the current state of the industry into account.

5.1 Findings

5.1.1 Transition challenges

For most networks, the biggest problem will be client-side configuration. In a home environment, a campus network or in a corporate network alike, network configuration can be a challenge for most users when trying to connect to IPv6. Many different options exist for linking a host to an IPv6 network and troubleshooting can be hard. This is the biggest challenge IPv6 adoption faces: providing the end-user with ubiquitous and easy, ready-to-go network access.

Content providers and ISPs also face a whole other set of challenges: which strategy to adopt, when to make a transition and when to unplug IPv4 links. Besides the technological challenges of making the transition, concerns build up as customers and users can't access some hosts or take too long, or when enabling IPv6 effectively disables their communication channel with the Internet. Business wise, these are risky - if not unacceptable - side effects, easily leading to postponing IPv6 adoption, hardware purchasing, etc.

A challenge further down the road awaits for networks adopting address-sharing solutions like Carrier-Grade NAT and Address-plus-Port: these approaches will delay transitioning for IPv6 to a point where the network must be rapidly and efficiently adapted for IPv6 support. Moving a "simple" network to IPv6 is already a challenge, so address-sharing will only complicate matters in terms of availability and Quality of Service (QoS) during the transition.

5.1.2 Security and IPv6

The IPv6 protocol is not secure by default and care must be taken to implement appropriate security measures for address and router configuration. Secure deployment of IPv6, both in dual-stack and IPv6-only networks, is a difficult task prone to error and it's easy to misconfigure some host or device.
This new protocol stack is being actively developed upon to improve functionality and remove liabilities, with many IETF working groups and individuals contributing drafts improving recommendations, implementation requirements and proposing new protocols or protocol enhancements. Governments (like the United States of America and the United Kingdom) have had experimental IPv6 programs and recommendations issued for several years now, granting a minimum level of security of the IPv6 deployments in critical infra-structures like military and government networks.

The information security industry is less concerned, as attention flees to more easily executed attack vectors at the application layer, such as web application frameworks bugs and Structured Query Language (SQL) injections.
A few, notably Marc Van Heuse[1] and Fernando Gont[2], have actively researched and repeatedly publicly disclosed vulnerabilities, protocol enhancement proposals and IPv6 security testing tools.
Open-source projects like Metasploit[3] and Nmap[4], commonly in a penetration tester's or security professional toolchain, have incorporated support for IPv6 into their products which in turn encouraged more active IPv6 security research. These efforts seem to be making their way to the generic professional security tester, as IPv6 deployments become more common and a required set of their skills. A good example of this are the security conferences around the world, which nowadays almost always include IPv6-related keynotes and sometimes workshops.

5.1.3 Industry response

The industry response to the need for transition has mostly been positive and initiatives like IPv6 World Launch day have proven the major content providers are developing actions to make IPv6 generally available to the public. ISPs have also started to deploy IPv6 CPEs to their customers, and vendors have rallied in summits to discuss and promote IPv6 adoption.

These kind of initiatives show that the core network and Internet community is aware, engaged and prepared for IPv6 adoption, but it's a long way from public IPv6 consumption; the goal is still to achieve IPv6 support in conjunction with IPv4. Until content

[1] van Hauser, of mh-sec and The Hackers Choice fame
[2] see his website, SI6 Networks and Hacking IPv6 networks
[3] http://www.metasploit.com/
[4] http://nmap.org/

providers, datacenters and vendors treat IPv4 as a deprecated protocol, real progress will be delayed.

5.2 Future research

Even though the protocol is quite a few years old, since it's usage in a more broad way is relatively new there are plenty of open opportunities for security and network research in several fields.

As an under researched topic, even the smallest contribution can amount to raising the awareness level and lead to more proactive measures or research from other people or entities. On the other hand, with so many new protocols and changes, it doesn't take much to be on the verge of ground breaking research if attention is devoted to bold goals.

5.2.1 Transition paths

While detailed work as been done on different approaches to transitioning networks between the two protocol stacks, most of this work has been done from the network-savvy and technological point-of-view. Though much necessary and valuable work, this still leaves three big challenges.

Firstly, the public education on the subject is very low, as is expected when it comes to deep technology topics. This means ISPs customer support teams will be dealing with IPv6-related queries as time goes by and IPv6-only networks become dominant.
This won't affect ISPs only, and will be a symptom of old software which is only IPv4-enabled, routing failures for IPv4 hosts trying to connect to sites which choose to discontinue IPv4 availability, etc.. The research of technological assets to smooth the transition process for the end-user (e.g. firewalls, peer-to-peer (P2P), IPv6 tunnels configuration, etc) will help minimize this problem.

In second place, addressing identification solutions for the total address space available in IPv6. In IPv4, we mostly rely on the DNS to provide easy name to address configuration, and most network professionals are used to knowing a few IP addresses by heart. However, in IPv6 with such long and so many addresses, these solutions may not be feasible. The DNS protocol is quite mature but lacks strong security mechanisms by default and can be a burden to manage in such a large address space, so better solutions are needed in the long term.

Finally, with NAT no longer being the default configuration for small home and small-medium businesses (SMBs) networks, security concepts for these kind of networks need to be reassessed.
All kinds of software currently trust communication with local network hosts implicitly

and relax security rules, openly share private information and make things more easy for possible attackers.

5.2.2 Security

Although many of the possible research topics listed in the following topics can be (and are) also applied to IPv4 networks, please keep in mind that they are given here in the context where they pertain to IPv6 or dual-stack networks.

5.2.2.1 Offensive security

As with any new technology, the possibility for security vulnerabilities and attacks is present. The fact that the new stack of protocols is composed of core network protocols, adds to the importance of a thorough security analysis. Given that IPv6 and its companion protocols will take the place of IPv4 and related protocols on our networks and the Internet makes it crucial and essential to properly address their security.

An entry path and first concern into IPv6 security should be the protocol itself and related protocols (ICMPv6 et alii). This should address both the protocols design and implementation stacks across different devices: routers, desktop operating systems, server operating systems, etc. Any network-enabled that is to be connected to an IPv6 network must implement (or reuse) some sort of network stack and these should endure significant security research.
Enhanced mobility of users must not be forgotten and is more and more relevant and with it new protocols emerge (example: Mobile IPv6).

A second target are the service daemons used to provide us with things like webpages, network file sharing and remote access control. Examples include important, daily-use services like web servers, DNS servers, email related servers (Simple Message Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), Post Office Protocol (POP)), File Transfer Protocol (FTP) servers and Secure Shell (SSH).

5.2.2.2 Defensive techniques

As a network administrator, security researcher or simply a network enthusiast, it is our responsibility to gather tools and techniques to help in the task of trying to protect networks and users.

At first glance, and taking from current practice, an obvious place to start is with packet inspection and ACLs. Packet inspection is used to filter and transform network traffic in border-gateway routers, and can help immensely in dropping bogus or malicious traffic. Advanced packet inspection techniques (and software) for IPv6 networks are still very early and need to be improved in terms of performance, proven as secure and researched on new possible approaches.

Monitoring network hosts, devices and services for perfomance, attacks and disruptions plays a valuable part in keeping a network's QoS and security. Currently, software exists for various related topics: availability checks, intrusion detection, and attack misdirection (i.e. honeypots) and is at various (sometimes none at all, sometimes great) stages of support for the IPv6 protocol. New approaches and improvement of current ones would help a more rapid cycle between security vulnerabilities discovery, disclosure and patching.

A step further from monitoring, traffic analysis can also be relevant to find new attacks, and accelerate migitation. Whether it's Border-Gateway Protocol (BGP) peer-exchanged traffic or local network traffic, (static) pattern analysis of protocol types, flags and extension headers used can transform raw network data into valuable information about what kind of activity is going on in a network.

Conclusions

References

[AAL+05] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. DNS Security Introduction and Requirements. http://tools.ietf.org/html/rfc4033, 2005.

[AB10] J. Arkko and S. Bradner. IANA Allocation Guidelines for the IPv6 Routing Header. http://tools.ietf.org/html/rfc5871, 2010.

[ACJR11] S. Amante, B. Carpenter, S. Jiang, and J. Rajahalme. IPv6 Flow Label Specification. http://tools.ietf.org/html/rfc6437, 2011.

[AD07] C. Aoun and E. Davies. Reasons to Move the Network Address Translator - Protocol Translator - (NAT-PT) to Historic Status. http://tools.ietf.org/html/rfc4966, 2007.

[A.J] A.J.N. Fake DHCPv6 attack. http://ccniethebeginning.wordpress.com/2012/01/27/dhcpv6-fake-attack/.

[ALM+05] David Alderson, Lun Li, Student Member, Walter Willinger, and John C Doyle. Understanding Internet Topology :. 13(6):1205–1218, 2005.

[Ant] Antonios Atlasis. Security Impacts of Abusing IPv6 Extension Headers. https://media.blackhat.com/ad-12/Atlasis/bh-ad-12-security-impacts-atlasis-wp.pdf.

[ASNN07] J. Abley, P. Savola, and G. Neville-Neil. Deprecation of Type 0 Routing Headers in IPv6. https://tools.ietf.org/html/rfc5095, 2007.

[Atl12] Antonios Atlasis. ATTACKING IPV6 IMPLEMENTATION USING FRAGMENTATION. http://media.blackhat.com/bh-eu-12/Atlasis/bh-eu-12-Atlasis-Attacking_IPv6-Slides.pdf, 2012.

[Aur05] T. Aura. Cryptographically Generated Addresses (CGA). http://tools.ietf.org/html/rfc3972, 2005.

[BCHW02] Mark Baugher, Ran Canetti, Thomas Hardjono, and Brian Weis. IP Multicast issues with IPsec. http://tools.ietf.org/html/draft-ietf-msec-ipsec-multicast-issues-01, 2002.

[BE07] Philippe BIONDI and Arnaud EBALARD. IPv6 Routing Header Security. http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf, 2007.

[Bie] Peter Bieringer. History of IPv6 in Linux. http://tldp.org/HOWTO/Linux+IPv6-HOWTO/basic-history-ipv6-linux.html.

[Bil] Ricardo Bilton. 2012: A big, bad year for online security breaches (infographic). http://venturebeat.com/2012/09/17/2012-security-breaches/.

[BMvB11] M. Bagnulo, P. Matthews, and I. van Beijnum. Stateful NAT64: Network Address and Protocol Translation - from IPv6 Clients to IPv4 Servers. http://tools.ietf.org/html/rfc6146, 2011.

[Bot05] Botnets. http://www.shadowserver.org/wiki/pmwiki.php/Information/Botnets, 2005.

[Bow11] Sam Bowne. Project 13x: IPv6 DoS with sendpees6 (10 pts.). http://samsclass.info/ipv6/proj/proj-124-13x-sendpees6.html, 2011.

[Bra89] R. Braden. Requirements for Internet Hosts – Communication Layers. http://tools.ietf.org/html/rfc1122, 1989.

[Car11] B. Carpenter. Advisory Guidelines for 6to4 Deployment. http://tools.ietf.org/html/rfc6343, 2011.

[CD98] A. Conta and S. Deering. Generic Packet Tunneling in IPv6 - Specification. http://tools.ietf.org/html/rfc2473, 1998.

[CH00] M. Crawford and C. Huitema. DNS Extensions to Support IPv6 Address Aggregation and Renumbering. http://tools.ietf.org/html/rfc2874, 2000.

[CISa] CISCO. Cisco IOS Software Release 12.2(50)SY New Features and Hardware Support. http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6970/ps6017/product_bulletin_c25-661245.html.

[CISb] CISCO. Implementing First Hop Security in IPv6. http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security.html.

[Cisc] Cisco Systems Inc. Training & Certifications. http://www.cisco.com/web/learning/certifications/index.html.

[Cis07] Cisco. IPv6 Routing Header Vulnerability. http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070124-IOS-IPv6, 2007.

[CM] Josh Corman and Brian Martin. Building a Better Anonymous. http://attrition.org/security/rants/building_a_better_anonymous/.

[CM01] B. Carpenter and K. Moore. Connection of IPv6 Domains via IPv4 Clouds. http://tools.ietf.org/html/rfc3056, 2001.

[CV11] T. Chown and S. Venaas. Rogue IPv6 Router Advertisement Problem Statement. http://tools.ietf.org/html/rfc6104, 2011.

[Dae] Inet Daemon. History of the Internet. http://www.inetdaemon.com/tutorials/internet/history.shtml.

[Dav08] Kim Davies. Saving the Internet from doom. http://www.iana.org/about/presentations/davies-sofia-dnssec+ipv6-080909.pdf, 2008.

[Day] Bhavya Daya. Network Security : History , Importance , and Future.

[DDWL11] A. Durand, R. Droms, J. Woodyatt, and Y. Lee. Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion. http://tools.ietf.org/html/rfc6333, 2011.

[Dep] Enterprise & Regulatory Reform Department for Business. INFORMATION SECURITY: HOW TO WRITE AN INFORMATION SECURITY POLICY. http://www.bis.gov.uk/files/file49963.pdf.

[DH95] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) - Specification. http://tools.ietf.org/html/rfc1883, 1995.

[DH98] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) - Specification. http://tools.ietf.org/html/rfc2460, 1998.

[DK06] Libor Dostálek and Alena Kabelováa. Understanding TCP/IP. *Network*, 2006.

[DKS] E. Davies, S. Krishnan, and P. Savola. IPv6 Transition/Coexistence Security Considerations. https://tools.ietf.org/html/rfc4942.

[DKS07] E. Davies, S. Krishnan, and P. Savola. Routing Headers and Hosts. https://tools.ietf.org/html/rfc4942#section-2.1.1, 2007.

[Don] Lutz Donnerhacke. How IPv6 and DNSSEC change the Intranets. http://altlasten.lutz.donnerhacke.de/mitarb/lutz/vortrag/ICANN40-Intranets-with-IPv6-DNSSEC.pdf.

[Doy10] Jeff Doyle. Understanding Dual-Stack Lite. ttp://www.networkworld.com/community/node/46600, 2010.

[Dua10] Overview of Dual-Stack Lite. http://www.juniper.net/techpubs/en_US/junos10.4/topics/concept/ipv6-ds-lite-overview.html, 2010.

[Dwy11] Paul C. Dwyer. Rebuttal: Paul C Dwyer, ICTTF and LulzSec. http://attrition.org/security/rebuttal/rebuttal-paul_dwyer-icttf.html, 2011.

[Fio] Alain Fiocco. World IPv6 Launch: Impact on the Web. http://blogs.cisco.com/news/ipv6webimpact/.

[FS11] S. Frankel and S. Krishnan. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. https://tools.ietf.org/html/rfc6071, 2011.

[GL12] F. Gont and W. Liu. DHCPv6-Shield: Protecting Against Rogue DHCPv6 Servers - draft-gont-opsec-dhcpv6-shield-01. http://tools.ietf.org/html/draft-gont-opsec-dhcpv6-shield-01, 2012.

[Gol11] David Goldman. LulzSec and Anonymous are the least of your hacker worries. http://money.cnn.com/2011/07/25/technology/lulzsec_anonymous_hackers/, 2011.

[Gon12a] F. Gont. Evasion techniques for some Router Advertisement Guard (RA Guard). http://tools.ietf.org/html/draft-ietf-v6ops-ra-guard-implementation-07#section-2, 2012.

[Gon12b] F. Gont. Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard) - draft-ietf-v6ops-ra-guard-implementation-07. http://tools.ietf.org/html/draft-ietf-v6ops-ra-guard-implementation-07, 2012.

[Gon12c] F. Gont. Virtual Private Network (VPN) traffic leakages in dual-stack hosts/-networks - draft-ietf-opsec-vpn-leakages-00. http://tools.ietf.org/html/draft-ietf-opsec-vpn-leakages-00, 2012.

[Gon12d] Fernando Gont. Recent Advances in IPv6 Security, 2012.

[Gon12e] Fernando Gont. Recent Advances in IPv6 Security, 2012.

[Gon13a] F. Gont. A method for Generating Stable Privacy-Enhanced Addresses with IPv6 Stateless Address Autoconfiguration (SLAAC) draft-ietf-6man-stable-privacy-addresses-03. http://tools.ietf.org/html/draft-ietf-6man-stable-privacy-addresses-03, 2013.

[Gon13b] F. Gont. Bogus address configuration prefixes. http://tools.ietf.org/html/draft-gont-opsec-ipv6-nd-security-01#section-6.1.7, 2013.

[Gon13c] F. Gont. Bogus on-link prefixes. http://tools.ietf.org/html/draft-gont-opsec-ipv6-nd-security-01#section-6.1.6, 2013.

[Gon13d] F. Gont. Disabling routers. http://tools.ietf.org/html/draft-gont-opsec-ipv6-nd-security-01#section-6.1.8, 2013.

[Gon13e] F. Gont. Rogue Router. http://tools.ietf.org/html/draft-gont-opsec-ipv6-nd-security-01#section-6.3.2, 2013.

[Gon13f] F. Gont. Security Assessment of Neighbor Discovery (ND) for IPv6 - draft-gont-opsec-ipv6-nd-security-01. http://tools.ietf.org/html/draft-gont-opsec-ipv6-nd-security-01, 2013.

[Gon13g] F. Gont. Tampering with Duplicate Address Detection (DAD). http://tools.ietf.org/html/draft-gont-opsec-ipv6-nd-security-01#section-6.1.2, 2013.

[Gon13h] Fernando Gont. The state of IPv6 (pen)testing and the future. http://lists.si6networks.com/pipermail/ipv6hackers/2013-January/000925.html, 2013.

[GT12] F. Gont and T. Chown. Network Reconnaissance in IPv6 Networks - draft-gont-opsec-ipv6-host-scanning-02. http://tools.ietf.org/html/draft-gont-opsec-ipv6-host-scanning-02, 2012.

[Har97] Gary Zergo Ltd Hardy. The relevance of penetration testing to corporate network security. *Information Security Technical Report*, 2(3):80–86, 1997.

[Hau13] Van Hauser. A complete tool set to attack the inherent protocol weaknesses of IPV6 and ICMP6, and includes an easy to use packet factory library. http://thc.org/thc-ipv6/, 2013.

[HC04] C. Huitema and B. Carpenter. Deprecating Site Local Addresses. http://tools.ietf.org/html/rfc3879, 2004.

[HD98] R. Hinden and S. Deering. IP Version 6 Addressing Architecture. http://tools.ietf.org/html/rfc2373, 1998.

[HD03] R. Hinden and S. Deering. Internet Protocol Version 6 (IPv6) Addressing Architecture. http://tools.ietf.org/html/rfc3513, 2003.

[Heu12] Marc "van Hauser" Heuse. IPv6 Insecurity Revolutions. http://conference.hitb.org/hitbsecconf2012kul/materials/D1T2-MarcHeuse-IPv6InsecurityRevolutions.pdf, 2012.

[HH05] R. Hinden and B. Haberman. Unique Local IPv6 Unicast Addresses. http://tools.ietf.org/html/rfc4193, 2005.

[HK] Geoff Huston and Olaf Kolkmann. IPv4 Address Exhaustion: A Progress Report. http://lacnic.net/documentos/lacnicxvi/viernes/04-Huston-2011-10-06-exhaustion.pdf.

[Hon11] Brian Honan. LulzSec Ups The Ante. http://attrition.org/security/rebuttal/rebuttal-lulzsec_ups_the_ante.html, 2011.

[Hou10] R. Housley. Guidelines to Authors of Internet-Drafts. http://www.ietf.org/ietf-ftp/1id-guidelines.txt, 2010.

[HS06] R. Hinden and S. Deering. IP Version 6 Addressing Architecture. http://tools.ietf.org/html/rfc4291, 2006.

[Hui06] C. Huitema. Teredo: Tunneling IPv6 over UDP - through Network Address Translations (NATs). https://tools.ietf.org/html/rfc4380, 2006.

[Husa] Geoff Huston. Transitional Myths. http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_14-1/141_myths.html.

[Husb] Geoff Huston. Transitioning Protocols. http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_14-1/141_protocols.html.

[Husc] Geoff (APNIC) Huston. IPv4 Address Report. ipv4.potaroo.net.

[Hus05] Geoff Huston. IPv6 Unique Local Addresses Update on IETF Activity. http://www.apnic.net/__data/assets/pdf_file/0019/33427/arin-vx-v6-ula.pdf, 2005.

[Hus11a] Geoff (APNIC) Huston. Transitional Myths. *Internet Protocol Journal*, 14(1), 2011.

[Hus11b] Geoff (APNIC) Huston. Transitioning Protocols. *The Internet Protocol Journal*, 14(1):181, February 2011.

[IAN] IANA. Root Zone Database. http://www.iana.org/domains/root/db.

[Ica] Icann. DNSSEC – What Is It and Why Is It Important? http://www.icann.org/en/about/learning/factsheets/dnssec-qaa-09oct08-en.htm.

[IET] IETF. Internet Protocol. http://www.ietf.org/rfc/rfc791.txt.

[iH01] Jun-ichiro itojun Hagino. Comparison of AAAA and A6 (do we really need A6?) - draft-ietf-dnsext-aaaa-a6-01.txt. http://tools.ietf.org/html/draft-ietf-dnsext-aaaa-a6-01, 2001.

[Insa] SANS Institute. Bots and Botnet: an Overview.

[Insb] SANS Institute. Information Security Policy Templates.

[Insc] SANS Institute. Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines.

[Ipv07] Ipv6samurais.com. I have a problem with rogue RAs in my IPv6 network. http://ipv6samurais.com/ipv6samurais/demystified/rogue-RA.html, 2007.

[J. 06] Ed. J. Loughney. IPv6 Node Requirements. http://tools.ietf.org/html/rfc4294, 2006.

[JH11] S. Jiang and Huawei. An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition, 2011.

[JKZN05] Ed. J. Arkko, J. Kempf, B. Zill, and P. Nikander. SEcure Neighbor Discovery (SEND). http://tools.ietf.org/html/rfc3971, 2005.

[JLN11] E. Jankiewicz, J. Loughney, and T. Narten. IPv6 Node Requirements. http://tools.ietf.org/html/rfc6434, 2011.

[Joha] Olle E. Johansson. DHCPv6 – an introduction to the new host configuration protocol. http://ipv6friday.org/blog/2011/12/dhcpv6/.

[Johb] Olle E. Johansson. IPv6: Goodbye to broadcast, say hello to Multicast. http://ipv6friday.org/blog/2011/12/ipv6-multicast/.

[Jor07] Jordi Palet. *The Choice: IPv4 Exhaustion or Transition to IPv6*. 2007.

[JS12] Sheng Jiang and Sean Shen. Secure DHCPv6 Using CGAs - draft-ietf-dhc-secure-dhcpv6-07.txt. http://tools.ietf.org/html/draft-ietf-dhc-secure-dhcpv6-07, 2012.

[jun11] Carrier Grade NAT Implementation Guide. http://www.juniper.net/us/en/local/pdf/implementation-guides/8010076-en.pdf, 2011.

[Jus12] Justin Franks. IPv6. Think Big, Really Big. http://www.inetassociation.com/ipv6subnetdesign.htm, 2012.

[KA98] S. Kent and R. Atkinson. Security Architecture for the Internet Protocol. http://tools.ietf.org/html/rfc2401, 1998.

[Ker06] Shane Kerr. DHCPv6. http://meetings.ripe.net/ripe-53/presentations/dhcpv6.pdf, 2006.

[KGAS02] James Kempf, Craig Gentry, Alice, and Silverberg. Securing IPv6 Neighbor Discovery Using Address Based Keys (ABKs). http://tools.ietf.org/html/draft-kempf-secure-nd-01, 2002.

[Kos] Joseph Koshy. IPv6 in FreeBSD. people.freebsd.org/~jkoshy/images/ipv6.tex.

[KR98a] S. Kent and R. Atkinson. IP Authentication Header. http://tools.ietf.org/html/rfc2402, 1998.

[KR98b] S. Kent and R. Atkinson. IP Encapsulating Security Payload (ESP). http://tools.ietf.org/html/rfc2406, 1998.

[Kri] John Kristoff. NANOG 32 - Botnet.

[Kri09] S. Krishnan. Handling of Overlapping IPv6 Fragments. http://tools.ietf.org/html/rfc5722, 2009.

[KS05] S. Kent and K. Seo. Security Architecture for the Internet Protocol. http://tools.ietf.org/html/rfc4301, 2005.

[KWK+12] S. Krishnan, J. Woodyatt, E. Kline, J. Hoagland, and M. Bhatia. A Uniform Format for IPv6 Extension Headers. http://tools.ietf.org/html/rfc6564, 2012.

[LAdVPM11] E. Levy-Abegnoli, G. Van de Velde, C. Popoviciu, and J. Mohacsi. IPv6 Router Advertisement Guard. http://www.ietf.org/rfc/rfc6105.txt, 2011.

[LBB11] X. Li, C. Bao, and F. Baker. IP/ICMP Translation Algorithm. http://tools.ietf.org/html/rfc6145, 2011.

[MBD04] M Malli, C Barakat, and W Dabbous. A Survey on Internet Topology Inference. Technical Report December, INRIA, 2004.

[Mic] How Network Printing Works. http://technet.microsoft.com/en-us/library/cc783789(v=ws.10).aspx.

[Mit] Mitre. Common Vulnerabilities and Exposures. http://cve.mitre.org/.

[ND01] T. Narten and R. Draves. Privacy Extensions for Stateless Address Autoconfiguration in IPv6. http://tools.ietf.org/html/rfc3041, 2001.

[NDK07] T. Narten, R. Draves, and S. Krishnan. Privacy Extensions for Stateless Address Autoconfiguration in IPv6. http://tools.ietf.org/html/rfc4941, 2007.

[Neg12] Ajay Singh Negi. List of Bug Bounty Programs. http://computersecuritywithethicalhacking.blogspot.pt/2012/09/web-product-vulnerabilty-bug-bounty.html, 2012.

[Neta] Lean Networking. The TCP/IP Stack and the OSI Model.

[Netb] SI6 Networks. Router Advertisement Guard (RA-Guard) Evasion. http://blog.si6networks.com/2011/09/router-advertisement-guard-ra-guard.html.

[NKKK09] Nitin A Naik, Gajanan D Kurundkar, Santosh D Khamitkar, and Namdeo V Kalyankar. Penetration Testing: A Roadmap to Network Security. *Journal of Computing*, 1(1):187–190, 2009.

[NNSS07] T. Narten, E. Nordmark, W. Simpson, and H. Soliman. Neighbor Discovery for IP version 6 (IPv6). http://tools.ietf.org/html/rfc4861, 2007.

[Nor00] E. Nordmark. Stateless IP/ICMP Translation Algorithm (SIIT). http://tools.ietf.org/html/rfc2765, 2000.

[Off] Offensive Security. Offensive Security Certified Professional.

[Ope12] OpenBSD System Manager's Manual. http://www.openbsd.org/cgi-bin/man.cgi?query=ping&sektion=8, 2012.

[Oraa] Oracle Corporation. IPv6 Administration Guide. http://docs.oracle.com/cd/E19683-01/817-0573/chapter1-42/index.html.

[Orab] Oracle Corporation. IPv6 Neighbor Discovery. http://docs.oracle.com/cd/E19683-01/817-0573/chapter1-40/index.html.

[Orac] Oracle Corporation. Other Transition Mechanisms. http://docs.oracle.com/cd/E19683-01/817-0573/transition-9/index.html.

[osv] The Open Source Vulnerability Database. http://www.osvdb.org/.

[OvVdBP] Christiaan Ottow, Frank van Vliet, Pieter-Tjerk de Boer, and Aiko Pras. The Impact of IPv6 on Penetration Testing. http://doc.utwente.nl/81276/1/Ottow12impact.pdf.

[PKN04] Ed. P. Nikander, J. Kempf, and E. Nordmark. IPv6 Neighbor Discovery (ND) Trust Models and Threats. https://tools.ietf.org/html/rfc3756, 2004.

[Pos81] J. Postel. INTERNET CONTROL MESSAGE PROTOCOL. http://tools.ietf.org/html/rfc792, 1981.

[R. 11] Ed. R. Bush. The Address plus Port (A+P) Approach to the IPv4 Address Shortage. https://tools.ietf.org/html/rfc6346, 2011.

[Ray] Eric S. Raymond. The Jargon File. http://catb.org/jargon/.

[RBV+03a] Ed. R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). http://tools.ietf.org/html/rfc3315, 2003.

[RBV+03b] Ed. R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney. Security Considerations. http://tools.ietf.org/html/rfc3315#section-23, 2003.

[RIP] RIPE. IPv6 Act Now: Allocation and routing statistics. http://www.ipv6actnow.org/info/statistics/.

[Sai13] Anne Saita. Malware Infects Two Power Plants Lacking Basic Security Controls. http://threatpost.com/en_us/blogs/malware-infects-two-power-plants-lacking-basic-security-contro 2013.

[Sav02a] P. Savola. Security of IPv6 Routing Header and Home Address Options. https://tools.ietf.org/html/draft-savola-ipv6-rh-ha-security-03, 2002.

[Sav02b] P. Savola. Security of IPv6 Routing Header and Home Address Options. https://tools.ietf.org/html/draft-savola-ipv6-rh-ha-security-03, 2002.

[Sch00] Bruce Schneier. Crypto-Gram Newsletter. http://www.schneier.com/crypto-gram-0009.html#1, 2000.

[Sch10] Bruce Schneier. Schneier on Security. http://www.schneier.com/blog/archives/2010/10/stuxnet.html, 2010.

[Sch11] Mathew J. Schwartz. Sony Hacked Again, 1 Million Passwords Exposed. http://www.informationweek.com/security/attacks/sony-hacked-again-1-million-passwords-ex/229900111, 2011.

[seca] SecLists.Org Security Mailing List Archive. http://seclists.org/.

[Secb] ELearn Security. Penetrating Testing Course Pro.

[Secc] Offensive Security. Exploit-DB. http://www.exploit-db.com/.

[Si6] Si6networks. SI6 Networks' IPv6 Toolkit. http://www.si6networks.com/tools/ipv6toolkit/.

[SK] Rajiv C Shah and Jay P Kesan. The Privatization of the Internet ' s Backbone Network. (217):1–25.

[SNL+] Abhishek Singh, Ola Nordstrom, Chenghuai Lu, Andre L.M. dos Santos, and O. Malicious ICMP Tunneling: Defense against the Vulnerability. http://www.2factor.us/icmp.pdf.

[Soca] Internet Society. Everyday Users: A Short Guide to IPv6.

[Socb] Internet Society. World IPv6 Launch. http://www.worldipv6launch.org/participants/.

[Sta11] IT Security StackExchange. IPV6 Cryptographically Generated Address implementation. http://security.stackexchange.com/questions/3384/ipv6-cryptographically-generated-address-implementation, 2011.

[Sym] Symantec. Security Focus. http://www.securityfocus.com/.

[SYM+12] Ed. S. Perreault, I. Yamagata, S. Miyakawa, A. Nakagawa, and H. Ashida. Common requirements for Carrier Grade NATs (CGNs) - draft-ietf-behave-lsn-requirements-10. http://tools.ietf.org/html/draft-ietf-behave-lsn-requirements-10, 2012.

[Tha11] D. Thaler. Teredo Extensions. http://tools.ietf.org/html/rfc6081, 2011.

[THKS03] S. Thomson, C. Huitema, V. Ksinant, and M. Souissi. DNS Extensions to Support IP Version 6. http://tools.ietf.org/html/rfc3596, 2003.

[TKH10] D. Thaler, S. Krishnan, and J. Hoagland. No Title Teredo Security Updates. 2010.

[TN98] S. Thomson and T. Narten. IPv6 Stateless Address Autoconfiguration. http://tools.ietf.org/html/rfc2462, 1998.

[TNJ07] S. Thomson, T. Narten, and T. Jinmei. IPv6 Stateless Address Autoconfiguration. http://tools.ietf.org/html/rfc4862, 2007.

[Too] Ietf Tools. Internet-Draft Archive. http://tools.ietf.org/id/draft-ietf-6man.

[TS00] G. Tsirtsis and P. Srisuresh. Network Address Translation - Protocol Translation (NAT-PT). http://tools.ietf.org/html/rfc2766, 2000.

[Viv03] Álvaro Vives. Management of DNS and DNSsec in IPV6. http://www.ist-ipv6.org/presentations/madrid03/alvaro_vives.pdf, 2003.

[Wal99] Cheryl Walton. IPv6: At the Starting Line. http://support.novell.com/techcenter/articles/nc1999_05a.html, 1999.

[WGI08] B. Weis, G. Gross, and D. Ignjatic. Multicast Extensions to the Security Architecture for the Internet Protocol. https://tools.ietf.org/html/rfc5374, 2008.

[wik] wikileaks. http://wikileaks.org/.

[WY12] D. Wing and A. Yourtchenko. Happy Eyeballs: Success with Dual-Stack Hosts. http://tools.ietf.org/html/rfc6555, 2012.

[Zak] Robert H'obbes' Zakon. Hobbes' Internet Timeline. http://www.zakon.org/robert/internet/timeline/.

[Zyt] Zytrax. DNS for Rocket Scientists. http://www.zytrax.com/books/dns/.