Instituto Superior de Engenharia do Porto

IPv6 – Integração, Transição e Segurança

André Filipe Costa Ribeiro

Dissertação para obtenção do Grau de Mestre

em

Engenharia Informática, Área de Especialização

em

Arquitetura, Sistemas e Redes

Orientador: Doutor Nuno Alexandre Magalhães Pereira

Júri:

Presidente:

Doutor Nuno Alexandre Pinto da Silva, ISEP

Vogais:

Doutor António Manuel Cardoso da Costa, ISEP

Doutor Nuno Alexandre Magalhães Pereira, ISEP

Porto, Julho 2015

"You have zero privacy anyway. Get over it"

Scott McNealy, CEO da Sun, 1999

Resumo

Ao longo dos anos a Internet tornou-se uma ferramenta fundamental para a sociedade e, nos dias de hoje, é praticamente inevitável não usufruir de algumas facilidades proporcionadas pela rede mundial. Devido à sua massificação nos últimos anos, os endereços de IP disponíveis esgotaram-se, pelo que tornou-se necessário a elaboração de uma nova versão do protocolo comunicação, utilizado para suportar todas as comunicações na Internet, o *Internet Protocol*, versão 6 (IPv6).

Apesar da ampla utilização da Internet, a maioria dos seus utilizadores está completamente alheia às questões de segurança, estando por isso exposta a uma diversidade de perigos. O aumento da segurança é também uma das principais missões do IPv6, tendo-se introduzido alguns mecanismos de segurança relevantes.

Este trabalho tem como objetivo estudar o IPv6, focando-se especialmente em questões relacionadas com os mecanismos de transição do IPv4 para IPv6 e em aspetos de segurança.

Proporcionando uma abordagem teórica ao protocolo e aos conceitos de segurança, este documento apresenta também uma perspetiva mais técnica da implementação do IPv6, pretendendo ser um manual de apoio aos responsáveis pela implementação da versão 6 do IP. Os três métodos de transição, que permitem a atualização do IPv4 para IPv6, são analisados de forma a apoiar a equipa na tomada de decisão sobre qual (ou quais) os métodos de transição a utilizar.

Uma parte substancial do trabalho foi dedicada à seleção e estudo de vulnerabilidades que se encontram presentes no IPv6, a forma como são exploradas por parte do atacante, a forma como podem ser classificadas e os processos que diminuem o risco de exposição a essas mesmas vulnerabilidades. Um conjunto de boas práticas na administração da segurança de redes é também apresentada, para melhorar a garantia de que problemas conhecidos não possam ser explorados por utilizadores mal intencionados.

Palavras-chave: IPv6, Rede, Segurança, Transição, Vulnerabilidade, Risco

Abstract

The Internet is a quite important tool, and nowadays it is almost impossible to go about our ordinary lives without using some of its functionalities. However, due to its widespread use, the available IP addresses are becoming scarce. This fact triggered the design of a new version of the Internet Protocol (IP), named IPv6.

Despite the Internet's pervasiveness, most of its users remain unaware of its security issues, becoming exposed to an array of dangers. Importantly, one of IPv6's objectives is to address these by including a set of important security features.

The objective of this dissertation is to explore the transition from the IPv4 to IPv6 and to address relevant security aspects related to the implementation of IPv6.

We carry out a theoretical overview of the IPv6 protocol concerning its implementation and security related aspects, providing a reference guide aimed at network administrators. In this line, we also analyze the three IPv4 to IPv6 transition methods, to support the networks administrator's decision and ease the transition process.

Focusing on network security, we built a catalogue of known vulnerabilities of IPv6, present information about how they can be explored, look into solutions to mitigate them, along with the proposal of several good security practices.

Keywords: IPv6, Network, Security, Transition, Vulnerability, Risk

Agradecimentos

Doutor Nuno Pereira, meu orientador, pela dedicação, disponibilidade, motivação, planeamento, conceção e correção desta dissertação.

Engº César Teixeira, pela motivação e debate de ideias para a elaboração deste projeto.

Doutor Filipe Pacheco, pela preocupação e conselhos.

Engº Bruno Saraiva, pelo incentivo e apoio na decisão do ingresso no mestrado e apoio ao longo do percurso.

Engº Ricardo Severino, pela ajuda dada ao longo de todo o trabalho.

Engº Cláudio Maia, pelo incentivo e motivação transmitidos.

Engº Bruno Ferreira, Engº Ricardo Moreira e Engº João Oliveira pelo apoio em diversas fases do meu percurso.

Amigos, que foram importantes neste trabalho, pelo apoio e pela partilha de bons momentos, que resultaram numa acrescida motivação para a elaboração desta Tese.

Joana, pelo tempo que a tese lhe roubou. Apesar disso reconheço o incondicional apoio, encorajamento, compreensão e motivação em todos os momentos. O carinho e a confiança foram dois importantíssimos fatores para a prossecução desta dissertação.

Drª Ágata Nicolau da Costa, que desde sempre fomentou em mim um espírito de ambição e determinação, incentivando-me sempre a prosseguir os estudos mostrando-me todas as oportunidades consequentes desse empenho académico.

Mãe, pelo suporte e compreensão.

Pai e esposa, pela motivação.

Irmãos, pelo apoio e orgulho demonstrados.

Família, por acreditarem nas minhas capacidades e pelo apoio transmitido na conclusão desta etapa do meu percurso académico.

E a todos a quem, embora não mencionados, deixo o meu agradecimento.

Índice

Lista de Figuras

Lista de Tabelas

Lista de Gráficos

Acrónimos e Símbolos

ACL	*Access Control List*
ARP	*Address Resolution Protocol*
DHCP	*Dynamic Host Configuration Protocol*
DMZ	*Demilitarized Zone*
DoS	*Denial of Service*
DNS	*Domain Name System*
DHCP	*Dynamic Host Configuration Protocol*
IANA	*Internet Assigned Numbers Authority*
ICANN	*Internet Corporation for Assigned Names and Numbers*
ICMP	*Internet Control Message Protocol*
IDS	*Intrusion Detection System*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
IPS	*Intrusion Protection System*
IPv4	*Internet Protocol versão 4*
IPv6	*Internet Protocol versão 6*
IPSec	*IP Security Protocol*
ISP	*Internet Service Provider*
LAN	*Local Area Network*
MAC	*Media Access Control*
MTU	*Maximum Transmission Unit*
MLD	*Multicast Listener Discovery*
NAT	*Network Address Translation*
ND	*Neighbor Discovery*

NDP	*Neighbor Discovery Protocol*
OS	*Operating System*
PPP	*Point-to-Point Protocol*
QoS	*Quality of Service*
RIR	*Regional Internet Registry*
SEND	*Secure Neighbor Discovery*
SHA	*Secure Hash Algorithm*
SLAAC	*Stateless Address Auto Configuration*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
VLAN	*Virtual LAN*
VoIP	*Voice over Internet Protocol*
VPN	*Virtual Private Network*
WAN	*Wide Area Network*

1 Introdução

1.1 Contexto e Motivação

A exaustão dos endereços do *Internet Protocol* versão 4 (IPv4) forçou, desde cedo, o planeamento de uma nova versão do IP. A versão IPv6 foi desenvolvida com o principal objetivo de disponibilizar uma gama maior de endereços. A par desta evolução foram também desenvolvidas funcionalidades que dizem respeito à segurança, reconhecimento de equipamentos vizinhos e otimização do desempenho da rede.

Apesar da sua baixa taxa de adoção [1], as organizações começaram a reconhecer que a mudança para o IPv6 é inevitável. O planeamento da implementação deve ser um processo cuidado e detalhado, uma vez que a infraestrutura de comunicação tem que manter o seu funcionamento, sem que seja prejudicado o fluxo habitual de trabalho.

A mudança da versão 4 para a versão 6 do IP deve basear-se nos mecanismos que foram definidos, aquando da conceção do IPv6 [2], com o objetivo de suportar a migração para a nova tecnologia de forma controlada. Estes mecanismos permitem que a transição seja feita de forma faseada, sem afetar os sistemas migrados, no entanto, para que possam ser corretamente aplicados, os mecanismos devem ser detalhadamente conhecidos e testados.

Atualmente, a segurança é um fator ao qual é dado primazia quando se fala de gestão de redes de comunicação. Devido à elevada dependência deste tipo de estruturas, por onde transitam diariamente informações de caráter altamente sigiloso e que caso seja acessível a pessoas externas às organizações em causa, poderá colocar alguns problemas à organização, quer de caráter legal que a nível do objeto de negócio, é um importante pilar nas mais diversas organizações.

Embora as questões de segurança tenham sido tomadas em conta na nova versão, existem ainda muitas falhas que podem ser exploradas a fim de atacar as redes, problemas esses que têm que ser detetados, analisados e corrigidos. As novas funcionalidades como as técnicas de transição, descoberta de vizinhos, autoconfiguração e mobilidade acarretam, seguramente, novos desafios no que diz respeito à segurança [3]. O facto de o IPv6 ser uma tecnologia recente, sugere que ainda existem vulnerabilidades por descobrir, o que indicia que os administradores de rede terão

que acompanhar os desenvolvimentos que surgirem acerca da segurança, na versão 6 do protocolo.

É fundamental que os responsáveis pela rede e implementação do novo protocolo dominem os conceitos associados à nova versão, bem como todas as técnicas e mecanismos que auxiliam a transição entre protocolos. No entanto, o levantamento desta informação exige uma árdua e morosa fase de pesquisa através da literatura, documentos técnicos, livros e sítios da especialidade.

No sentido de auxiliar os responsáveis na tarefa de reunir toda a informação necessária para um planeamento e respetiva implementação, este documento centra informação relativa à especificação do protocolo, detalha os aspetos fundamentais da segurança, enumera os mecanismos de transição e o processo de planeamento da transição, explora as vulnerabilidades consideradas mais relevantes, dada a sua fácil execução e elevado impacto no alvo, enumera técnicas para resolução das ameaças, bem como um conjunto adicional de boas práticas de segurança, para redes de comunicação.

1.2 Objetivos

Como já referido anteriormente, o processo de adaptação de uma organização para a migração do IPv4 para IPV6 irá necessitar de um trabalho de pesquisa, implementação e testes.

A elaboração deste relatório surge precisamente no sentido de proporcionar aos administradores de redes um compêndio que os auxilia na compreensão do protocolo, métodos de transição e técnicas para elevar o nível de segurança da infraestrutura. A importância da segurança em qualquer tecnologia é um fator primordial, pelo que a explicação das vulnerabilidades e apresentação de métodos que permitem a resolução das ameaças são fundamentais para uma implementação segura do protocolo. Este trabalho pretende cumprir os seguintes objetivos:

- Consolidar a informação sobre a arquitetura e funcionalidade do IPv6;
- Explorar as técnicas implementadas na versão 6 do IP, a fim de garantir mais segurança nas comunicações;
- Apresentar informação sobre o processo de implementação e transição para o IPv6;
- Sistematizar as vulnerabilidades mais relevantes descobertas até à data de realização deste documento;
- Recolher informação para a elaboração da análise de risco e avaliar as vulnerabilidades apresentadas;
- Reunir práticas e técnicas que permitam a resolução de algumas vulnerabilidades ou que reduzam o seu impacto;

1.3 Método

Numa primeira fase foi necessária uma exaustiva seleção da literatura disponível, permitindo desta forma expor os conceitos base do protocolo e todas as inovações que permitem aumentar o grau

de segurança conferido às redes que utilizem o IPv6. Os documentos técnicos, como RFC[1], foram uma grande fonte de informação visto que, muitos dos detalhes técnicos apresentados ao longo do documento estão exclusivamente detalhados nestes documentos. O resultado deste trabalho de rastreio e validação dos dados pode ser consultado nos Capítulos 2 e 3.

Livros da especialidade e outros documentos técnicos permitiram explicar os métodos de transição que foram disponibilizados pelas equipas de desenvolvimento, no sentido de auxiliar os responsáveis pelas infraestruturas de redes das organizações. O Capítulo 4 aborda os mecanismos de transição bem como todo o processo que deve ser seguido na implementação da tecnologia IPv6.

A elaboração do catálogo de vulnerabilidades teve por base diversos livros da matéria e alguns relatórios já existentes, bem como a recolha de informações em alguns sítios da especialidade. No que diz respeito à implementação, esta foi baseada no conhecimento adquirido ao longo da análise do catálogo de vulnerabilidades já referido. As vulnerabilidades apresentadas foram exploradas com base numa ferramenta denominada THC-IPv6 [4]. Foi criado um ambiente de testes baseado na tecnologia de virtualização, *Virtualbox*, tendo sido utilizadas três máquinas virtuais: uma com o Windows 8.1, como alvo dos ataques; a máquina atacante com a plataforma de testes de penetração Kali Linux [5]; e o *PFSense* como equipamento responsável por fazer o encaminhamento dos pacotes (*router*), servidor de nomes, de endereços e como meio de monitorização da rede [6].

Uma vez avaliado o impacto das vulnerabilidades, estes dados devem ser sistematizados de forma a tornar mais célere o processo de análise de risco de uma organização. Desta forma, convém definir os critérios pelos quais se irá reger esta classificação das vulnerabilidades, como apresentado no Capítulo 6.

No Capítulo 7 encontram-se documentadas as técnicas apuradas, durante o estudo, que reduzem ou solucionam a exploração das ameaças já analisadas. São ainda sugeridas algumas boas práticas que permitem aumentar a segurança da rede.

1.4 Estrutura do Documento

As alterações que se verificam ao nível dos cabeçalhos dos pacotes são também uma das grandes inovações da versão 6 do IP. A atualização do ICMP e o substituto do ARP, o *Neighbor Discovery Protocol* são elementos essenciais para que se entenda devidamente o protocolo. O novo mecanismo de atribuição de endereços é, também, uma peça fundamental que compõe uma introdução aos conceitos e funcionalidades do protocolo IPv6, que são apresentados no Capítulo 2.

Sendo um dos objetivos principais do documento a segurança do IPv6, é essencial que se forneça ao leitor alguns conceitos base da segurança, no âmbito geral, para que seja possível pormenorizar aspetos de segurança utilizados no IPv6, como o IPSec e o SEND, que são detalhados no Capítulo 3.

[1] Request for Comments (RFC) – Documentos de conteúdo técnico e organizacional da Internet [151].

No Capítulo 4 são apresentados os meios que permitem uma organização integrar o IPv6 na sua rede de comunicações. As 3 técnicas apresentadas: *Dual-Stack,* Túneis e Tradução têm vantagens e desvantagens que são apresentadas e discutidas. Ao longo do capítulo são ainda apresentadas algumas ideias chave que o administrador deve ter em atenção, quando se encontra a planear a mudança para a versão 6 do protocolo.

A apresentação de cada vulnerabilidade e a forma como cada uma é explorada encontram-se detalhadas no Capítulo 5. Onde se apresenta a vulnerabilidade e a forma como o atacante a pode explorar, bem como o impacto que esta poderá ter no sistema alvo, permitindo assim que administrador de redes consiga definir políticas de segurança que evitem a exploração das vulnerabilidades.

Tendo a informação das vulnerabilidades reunidas, importa tratar os dados e sumariá-los. A classificação do mecanismo usado pelo atacante, a dificuldade de execução do ataque e o impacto no alvo permite a sistematização de toda a informação relativa às vulnerabilidades num só quadro. No Capítulo 6 encontra-se toda a informação necessária para que o administrador de sistemas seja capaz de entender, de forma clara, a origem, o método e o impacto das vulnerabilidades num sistema.

A componente prática é, sem dúvida, fundamental pois trata-se do resultado de todo o estudo feito, e portanto pretende-se que todo ele obtenha bons resultados. Desta forma, são apresentadas as soluções para as vulnerabilidades apresentadas no Capítulo 5. A forma de resolução não é, nem pode ser igual para vulnerabilidades diferentes embora, em alguns casos, a mesma medida possa resolver dois problemas em simultâneo. No Capítulo 7 são apresentadas as medidas detalhadas para resolver as vulnerabilidades anteriormente apresentadas e classificadas. Consta ainda deste capítulo uma tabela semelhante à da categorização das vulnerabilidades, acrescida das principais medidas de resolução dessas mesmas vulnerabilidades. Finalmente, são apresentadas boas práticas aconselhadas a todos os administradores de sistemas, que estejam a ponderar a implementação de um sistema numa organização, seja este informático ou não.

2 Abordagem ao IPv6

2.1 Introdução

Com o intuito de substituir o IPv4, em 1998 foi apresentada a primeira especificação sobre IPv6, garantindo a continuidade da internet e do seu correto funcionamento, o que estava em risco uma vez que a exaustão dos endereços públicos IPv4 era inevitável [7].

As melhorias implementadas no IPv6 visam, principalmente, que esta versão consiga permanecer válida e útil por mais anos do que a precedente uma vez que, nos dias de hoje, a tecnologia avança a um ritmo vertiginoso e prevê-se que o número de dispositivos ligados à rede mundial continuem a crescer nos próximos anos. Estima-se que em 2019 existirão mais 73% dos equipamentos ligados à internet, do que em 2014 [8].

Aproveitando o desenvolvimento de uma nova versão do IP foram acrescentadas e/ou melhoradas algumas funcionalidades que passam agora a ser enumeradas:

- Mecanismo mais simples de autoconfiguração dos endereços [9];
- Endereços *multicast* e *anycast* [10];
- Formato do cabeçalho simplificado, com o intuito de reduzir o *overhead* [9];
- Melhoria do suporte de extensões e opções dos cabeçalhos [9];
- Permissão da distinção de tráfego, possibilitando distinguir tratamentos para os diversos tipos de tráfego (por exemplo *real-time*) [10];
- Criação de extensões que permitem autenticidade, integridade e confidencialidade dos dados [9].

Ao longo deste capítulo serão abordadas as novas formas de representação do endereço de IP, a forma como é constituído e a sua distribuição hierárquica. Os substitutos do *broadcast* são também apresentados, bem como as suas vantagens e impacto nos endereços. Os cabeçalhos nesta nova versão são um primeiro passo para o aumento da segurança no protocolo, pelo que são detalhados a fim de se perceber os objetivos e as vantagens da incorporação de cada um deles nos

pacotes. A evolução do ICMP para ICMPv6 e a introdução do *Neighbor Discovery Protocol*, em substituição do ARP (no IPv4), conferem mais estabilidade ao protocolo. O SEND é mais um mecanismo que confere um grau superior de segurança ao protocolo. A autoconfiguração sem estados e o DHCPv6 são explorados a fim de se apurarem as diferenças entre ambos. A inovação do *Mobile* IPv6 permite a comunicação com um determinado nó mesmo que este tenha, durante a comunicação, trocado a rede à qual se encontra ligado.

2.2 História

Por volta de 1990, a IETF[2] começaram a desenvolver-se todos os esforços a fim de se escolher um sucessor para o IPv4, uma vez que os dados, à data, indicavam que o número de endereços disponível viria a ser insuficiente no futuro [10]. As diversas equipas da IETF começaram a desenhar um sucessor, tendo também em conta a possibilidade de adicionar algumas funcionalidades e melhorias, nomeadamente, no que diz respeito à segurança [11].

No ano de 2000, metade dos endereços IPv4 já estavam a ser utilizados. No início de 2003 já 2/3 dos endereços estavam em utilização, o que demonstra o exponencial crescimento da adesão à Internet. A atribuição de endereços acompanhou o crescimento da utilização da Internet, o que levou a um rápido consumo de endereços, embora tenha sido desenvolvido o NAT, na tentativa de evitar o desperdício de endereços nas redes privadas.

Até que, a 3 de Fevereiro de 2011, a atribuição de IPv4 chegou ao seu limite. Foram esgotados todos os 16 777 216 endereços disponíveis para atribuir a entidades [12].

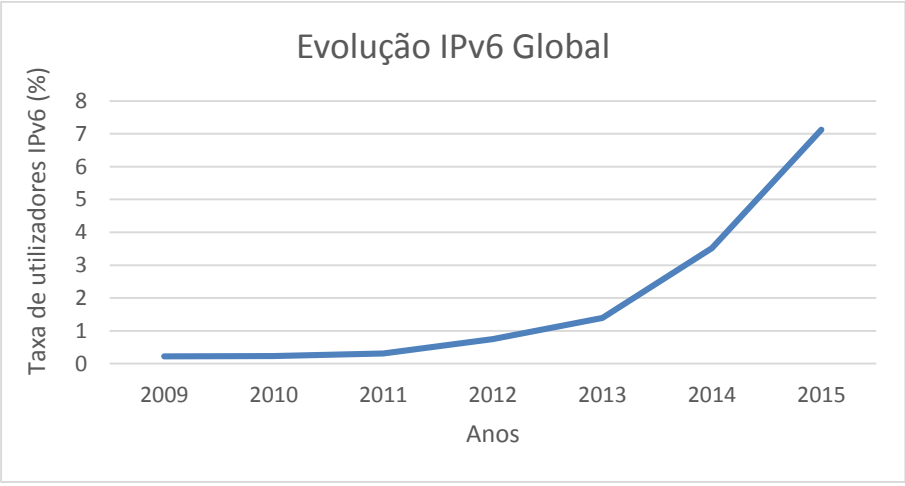

Gráfico 1 – Evolução da taxa de utilizadores IPv6, no Mundo

[2] IETF – Internet Engineering Task Force – Comunidade de investigadores, *designers*, técnicos que operam a internet. Esta equipa foi criada com a missão de garantir a evolução e o bom desempenho da internet [160, 5]

2.3 Evolução e Crescimento

O IPv6 tem tido uma adesão lenta. De acordo com as estatísticas disponibilizadas pela Google, em 2015, cerca de 7% da população internauta mundial utiliza o IPv6 [1], como demonstra o Gráfico 1 baseado em [13].

O crescimento nos últimos dois anos foi significativo, e tem tendência a intensificar-se, uma vez que os *Internet Service Providers* (ISP) têm vindo a aderir de forma massiva à utilização do IPv6 [14], o que levará certamente a que os seus clientes façam a migração, sem que a maioria se aperceba. Quanto aos clientes domésticos já há muito tempo que vêm sendo instalados equipamentos que suportam o IPv6, pelo que a migração para estes poderá ser praticamente transparente, se os restantes equipamentos da estrutura doméstica suportarem IPv6.

No que diz respeito a Portugal, a taxa de adoção da tecnologia IPv6 ronda os 10% [15]. Para tal muito tem contribuído a MEO, operadora que já tem o serviço IPv6 implementado em praticamente 25% dos seus clientes [14].

No que diz respeito aos países europeus, a adesão tem vindo a fazer-se sentir, embora que de forma gradual. Alguns países têm tido uma evolução mais lenta, o que se deve também à sua imensa dimensão geográfica.

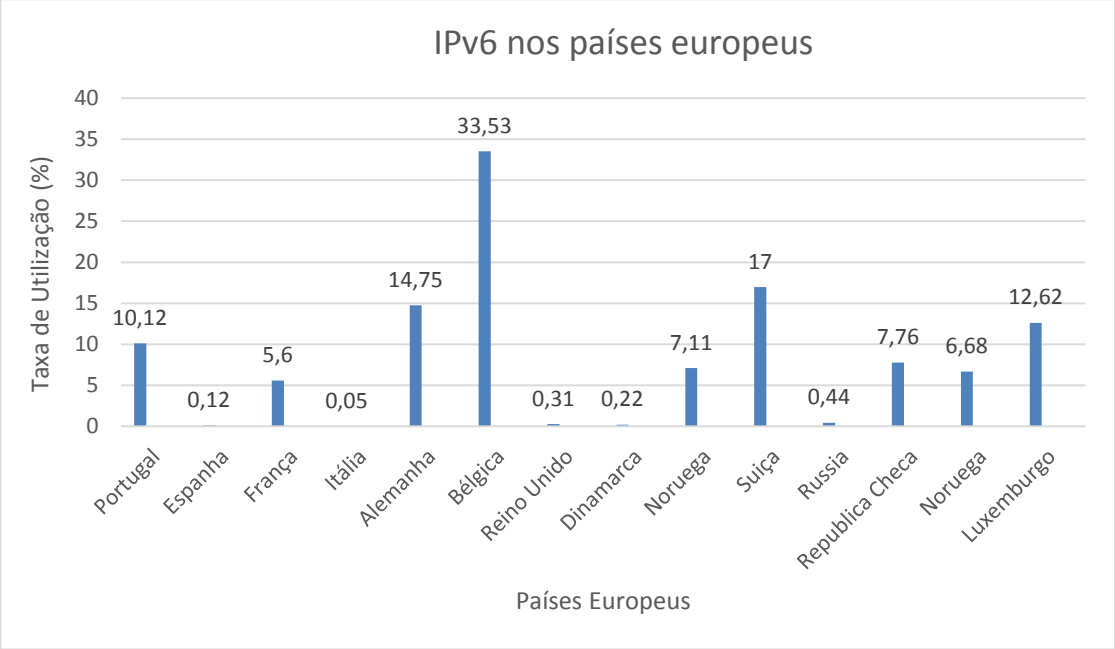

Gráfico 2 – Taxa de utilizadores IPv6 em países europeus, em junho 2015

Tal como pode ser analisado no Gráfico 2, a evolução nos países europeus não é equivalente [15] [16]. Alguns países têm uma grande taxa de adesão, ao contrário de outros que, apesar de fazerem parte do grupo de países desenvolvidos, têm uma taxa de adesão muito baixa. A operação de adesão é gerida pelos ISPs, pois são eles que providenciam a ligação aos clientes, sendo sua responsabilidade fornecer o serviço.

Os dados apurados são baseados no levantamento de equipamentos (*routers)* e consequentes ligações, que já se encontram preparadas para utilizar o IPv6.

Apesar das taxas de adesão díspares apresentadas anteriormente, a média de adoção europeia à tecnologia é de cerca de 7%. A Europa é o continente que lidera a lista dos continentes, no que diz respeito à preparação das infraestruturas para adoção do IPv6, como pode ser comprovado pelo Gráfico 3.

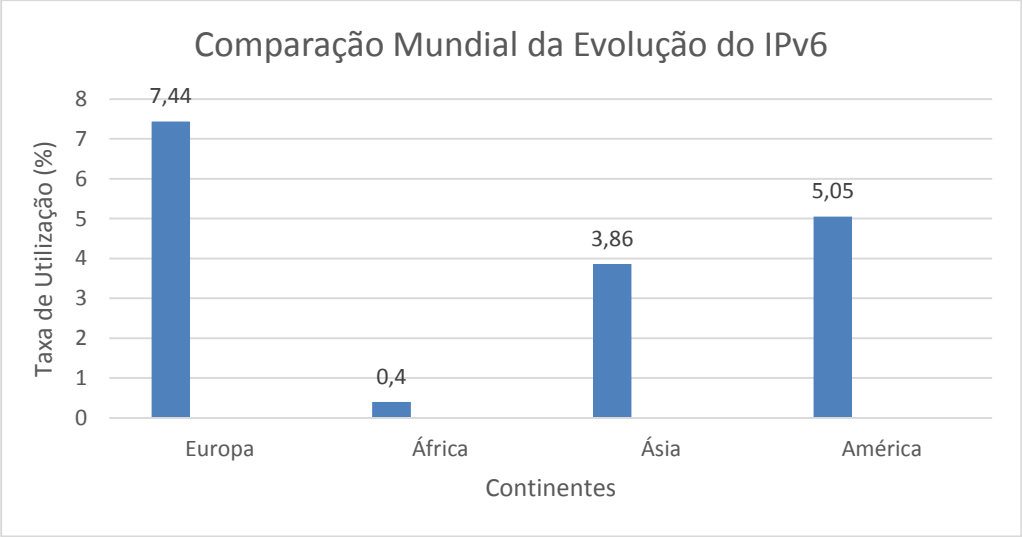

Gráfico 3 – Comparação entre as taxas de utilização entre continentes

Numa análise mais global à adesão ao IPv6, podemos concluir que a Europa é a região mais evoluída, no que diz respeito à utilização da nova tecnologia IPv6 [15].

Com a exaustão da gama de endereços do IPv4, torna-se inevitável que o IPv6 seja implementado. Até ao momento o grau de adesão tem tido um crescimento modesto motivo pelo qual, até à data, não são ainda conhecidas muitas vulnerabilidades. No entanto, à semelhança de outras tecnologias, quando se verifica a sua massificação, torna-se expectável que o crescimento de vulnerabilidades detetadas aumente substancialmente. Espera-se que nos próximos anos a quantidade de vulnerabilidades cresça de uma forma, até ao momento, incalculável.

2.4 Endereçamento

2.4.1 Endereços

Um endereço IPv6 é constituído por 128 *bits* (= 16 *bytes*), disponibilizando no total 340 282 366 920 938 463 463 374 607 431 768 211 456 endereços. No entanto, seria muito difícil, ou praticamente impossível representar 128 algarismos, desta forma, foi à semelhança do que

aconteceu com o IPv4, convencionada uma representação para os IPs da versão 6. Os IPs serão representados através de hexadecimais, recorrendo a 8 blocos de 4 números hexadecimais.

Em binário:

0010000000000001 0000110110111000 0000000000000000 0010111100111011
0000001010101010 0000000011111111 1111111000101000 1001110001011010

Em hexadecimal:

2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A

Possibilidades de Representação
2001:0dbf**:0000:0000:**0432:0621:ad32:14d6
2001:0dbf**:0:0:**0432:0621:ad32:14d6
2001:0dbf**::**0432:0621:ad32:14d6
2001:**dbf::432:621**:ad32:14d6

Tabela 1 - Compressão de zeros na representação de endereços IPv6

Estas diversas formas de representação podem trazer um problema relacionado com a pesquisa em bases de dados, folhas de cálculo, ficheiros de texto, comando "whois" e em diagramas de rede, pelo que a forma de representação mais utilizada é a substituição de blocos de zeros por um par de dois pontos "::". Com base em [17], a utilização desta abreviação obriga a que sejam seguidas algumas recomendações sob pena de o endereço poder ser confundido com outro, ou tornar-se incorreto:

i) Um bloco de 16 *bits*, ou seja, 0000, não deve ser representado por "::", mas sim por um único 0;
ii) O "::" só pode aparecer uma vez por endereço, em lugar da maior sequência de blocos a 0;
iii) Usar o ponto anterior sempre que possível;
iv) No caso de existirem duas sequências de blocos a 0 com o mesmo tamanho, só a primeira deverá ser representada por "::", ficando os restantes blocos, com um 0, por cada bloco;
v) Usar letra minúscula a, b, c, d, e, f.

A melhor forma para representar um endereço IPv6, seguido de uma porta, deverá acontecer com recurso à utilização de parêntesis retos, assim:

[2001:0dbf::0432:0621:ad32:14d6]:22

2.4.2 Gestão de Atribuição dos Endereços

A IANA (*Internet Assigned Numbers Authority*) é um Departamento da ICANN *(Internet Corporation for Assigned Names and Numbers)*, responsável por coordenar a atribuição de endereços de IPs e números de portas.

No sentido de garantir uma melhor gestão dos recursos, sentiu-se necessidade de criar 5 entidades responsáveis pela atribuição de endereços RIR (*Regional Internet Registry*), cada uma encarregue de uma área geográfica diferente. A distribuição da área geográfica de cada RIR encontra-se representada na Figura 1 [18].

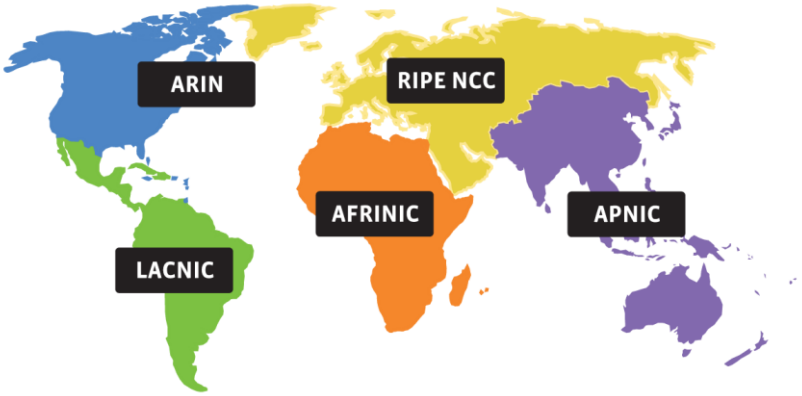

Figura 1 - Mapa-mundo com a distribuição das RIR

Por forma a sistematizar a área geográfica pela qual é responsável cada uma das RIR, a Tabela 2 descrimina essa informação [18].

Entidade	Área Geográfica
AFRINIC	África
APNIC	Oceânia e Ásia Oeste
ARIN	América do Norte
LACNIC	América Central e do Sul
RIPE NCC	Europa e Ásia Central e Nordeste

Tabela 2 - Distribuição das áreas geográficas pelas RIR

2.4.3 Prefixos

Os primeiros *bits* de um endereço dizem respeito ao prefixo. Este prefixo é constituído por valores associados à entidade responsável pela distribuição dos endereços (RIR), ao ISP, à rede da organização e até à sub-rede que pode eventualmente ser criada. Na Figura 2 são apresentados os *bits* que representam cada uma das entidades [19].

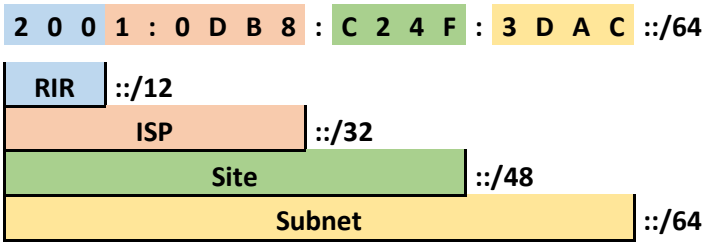

Figura 2 - Constituição do prefixo de um endereço IPv6

Vamos agora entender o que significa cada um dos componentes do prefixo, com base em [19]:

- **RIR** – a cada RIR são atribuídos blocos de endereços, que são representados nos primeiros três carateres hexadecimais do endereço;
- **ISP** (*Internet Service Provider*) – em cada país ou região existem as empresas que são responsáveis por distribuir o sinal de internet aos clientes particulares ou coletivos. Em Portugal temos, por exemplo, MEO, Nos e Vodafone;
- ***Site*** – Quando uma empresa ou um cliente final solicita ao seu ISP um endereço ou um bloco de endereços e cria a sua própria rede interna da organização, a essa rede chama-se Site. Com estes 48 *bits* completa-se o endereço fornecido pelo ISP;
- ***Subnet*** – Os 16 *bits* ficam à responsabilidade do administrador de redes para fazer a gestão das suas sub-redes internas.

2.5 Tipos de Endereços

No IPv6, podem ser distinguidos três tipos de endereços: *unicast, multicast* e *anycast* que são de seguida abordados.

2.5.1 Unicast

Um endereço *unicast* identifica de forma unívoca uma interface IPv6 de um equipamento [20].

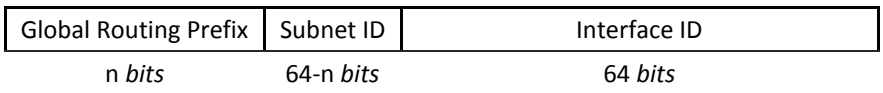

Figura 3 - Estrutura do endereço *unicast*

Os endereços *unicast* podem ainda ser categorizados: *global, link local e unique local*.

Global

Equivalentes aos IPs públicos IPv4, são globalmente encaminhados e atingíveis sobre a rede de IPv6 [21]. A estrutura destes endereços encontra-se definida em [22].

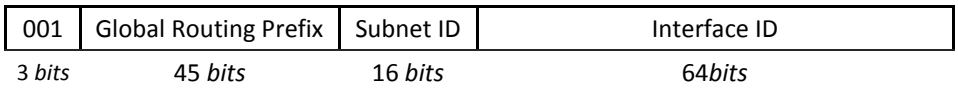

Figura 4 - Estrutura de um endereço global

De seguida são apresentadas as descrições de cada um das partes que compõem o endereço [21] :

001 – Os três *bits* mais significativos são colocados a 001;

Global Routing Prefix – Representa o prefixo atribuído pela IANA para cada *site*. Juntamente com os três *bits* mais significativos forma o *site prefix,* que é atribuído a cada organização;

Subnet ID – Utilizado dentro de uma organização para definir as sub-redes. Tendo em conta que para a definição das sub-redes existem 16 *bits* disponíveis, possibilita a criação de 65536 sub-redes diferentes;

Interface ID – Identifica uma determinada interface numa sub-rede da organização.

Link Local

Este tipo de endereços distingue-se pelos 64 *bits* mais à esquerda serem fixos, com este prefixo é possível os *routers* saberem que este tipo de tráfego não deve ser passado para o exterior. Utilizado somente para a comunicação entre *hosts* dentro da mesma ligação [22].

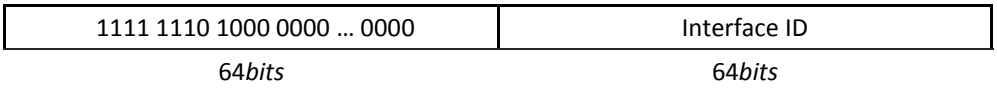

Figura 5 - Estrutura de um endereço *link local*

Numa rede na qual não existam *routers,* estes endereços são utilizados para comunicar entre os nós da rede. Este tipo de endereços é ainda necessário para alguns processos de *Neighbor Discovery* e é sempre configurado de forma automática.

Uma vez que este endereço se carateriza pelos 64 *bits* terem o valor apresentado na Figura 5, a sua representação será sempre iniciada por FE80, com o número de *bits* que identificam a rede igual a 64. Estes endereços só são encaminhados dentro da rede [21].

Unique Local

Concebidos com a ideia de garantir que são realmente endereço único, dentro de uma determinada rede (mas sem garantias de 100%).

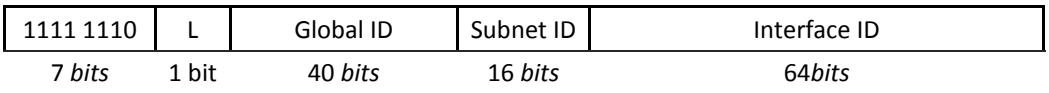

Figura 6 - Estrutura de um endereço *unique local*

1111 1110 – Combinação de *bits* que identificam o endereço;

L – Indica que o endereço é atribuído localmente;

Global ID – identifica um *site* numa organização gerado de forma aleatória;

Subnet ID – identifica uma sub-rede dentro de um *site*.

Estando os primeiros 7 *bits* definidos a 1, a representação hexadecimal do prefixo deste tipo de endereços começa sempre com FC [21].

2.5.2 Anycast

Um endereço *anycast* identifica um grupo de interfaces. Um pacote enviado para um endereço *anycast* será, normalmente, processado pelo nó mais próximo [23].

Estes endereços foram pensados com o intuito de criar redundância quando se fala de dispositivos que disponibilizem algum tipo de serviços. Não foi criado com o fim de ser aplicado no IPv6, mas sim no IPv4, o que não se veio a verificar [21].

Este tipo de endereços é, na sua maioria utilizado para identificar *routers* [22].

Subnet-Router Anycast Address
A representação de um endereço de *subnet router anycast* é a apresentada na Figura 7 [22].

Subnet Prefix	000 … 000
n *bits*	128 - n *bits*

Figura 7 - Sub-rede *router anycast address*

O *Subnet Prefix* é sintaticamente muito semelhante a um endereço *unicast*, a distinção poderá ser feita pelos *bits* menos significativos que são colocados todos a “0” [22].

2.5.3 Multicast

Os endereços *multicast* identificam interfaces que se encontram num mesmo grupo. Um pacote enviado para um endereço *multicast* será recebido e tratado por todos os nós deste grupo. Um nó pode fazer parte de diversos grupos *multicast*.

Nunca pode ser utilizado como endereço de origem em qualquer comunicação.

Um endereço *multicast* pode facilmente ser identificado, uma vez que os 8 *bits* iniciais ou as duas primeiras representações hexadecimais não são, por motivo algum, alteradas.

Desta forma, os 8 *bits* mais significativos têm sempre o valor 1, assim um endereço *multicast* é sempre iniciado por “ff” [21]. A estrutura do endereço e aplicação da constituição dos endereços apresenta-se de seguida na Figura 8 [24].

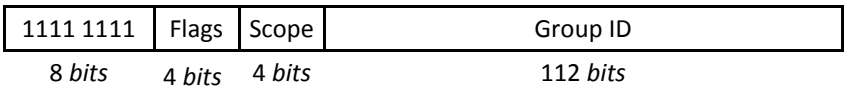

Figura 8 - Representação de um endereço *Multicast*

Flags – Composto por 4 *bits* dos quais, os três primeiros se encontram reservados, devendo ser definidos como 0. No entanto, o bit menos significativo define, no caso de ser:

- 0 -> Endereço permanente, atribuído pela IANA;
- 1 -> Endereço não permanente.

Scope – Serve, tal como o nome indica, para definir qual o âmbito em que estes IPs podem ser utilizados. Os códigos que se destinam a especificar o âmbito do endereço encontram-se previamente definidos e são apresentados na Tabela 3 [21] [24];

Bits	**Hexa**	**Sope**
0000	0	*reserved*
0001	1	*node-local*
0010	2	*link-local*
0011	3	(não atribuído)
0100	4	*admin-local*
0101	5	*site-local*
0110	6	(não atribuído)
0111	7	(não atribuído)
1000	8	*organization-local*
1001	9	(não atribuído)
1010	A	(não atribuído)
1011	B	(não atribuído)
1100	C	(não atribuído)
1101	D	(não atribuído)
1110	E	*global scope*
1111	F	*reserved*

Tabela 3 - Âmbitos *Multicast*

Group ID – Identifica o endereço *multicast*, dentro de um determinado *scope*.

A Tabela 4 apresenta o sumário dos endereços de *multicast* existentes [25] [26].

Endereço *Multicast*	Finalidade
FF01::1	Interface-Local All Nodes
FF01::2	Interface-Local All Routers
FF02::1	Link-Local All Nodes
FF02::2	Link-Local All Routers
FF05::1	Site-Local All Nodes
FF05::2	Site-Local All Routers
FF05::1:3	Site-Local All DHCP Servers

Tabela 4 - Âmbito a que se destinam os endereços *multicast*

2.5.4 Loop Back

Este endereço é vulgarmente conhecido como *localhost* e permite indicar o endereço do próprio computador. Em IPv6 representa-se por 0:0:0:0:0:0:0:1. Este tipo de endereços não é encaminhado pelo *router* [21].

2.5.5 Unspecified

O *unspecified address* significa que não existe IP atribuído aquela interface. Este endereço é muito semelhante ao endereço 0.0.0.0, com o mesmo objetivo existente no protocolo IPv4 [21].

2.6 Subnetting

Tal como no IPv4, no IPv6 é também possível fazer uma segmentação da rede. No entanto, no IPv4, e com base na máscara de rede, o administrador da rede pode escolher os *bits* que ficam destinados a identificar o *host*. No caso do IPv6, o número de *bits* destinado a identificar o nó é fixo, são 64 *bits* [21].

Ao contrário do IPv4, a possibilidade de criar endereços de rede privados no IPv6, não se restringe a classes, como A, B e C.

Conforme a Figura 9, podemos constatar que é possível utilizar 16 *bits* para definir a sub-rede, assim, é possível criar 65536 sub-redes (= 2^{16}) [27].

As fontes [28] e [27] defendem que, com o objetivo de promover a organização e a melhor interpretação dos endereços, pode fazer-se uma divisão utilizando os 16 *bits*. Entre diversas sugestões destacam-se a segmentação através da localização e dos departamentos. Demonstra-se agora uma possibilidade de subdivisão. No entanto, o administrador da rede pode optar por uma outra metodologia.

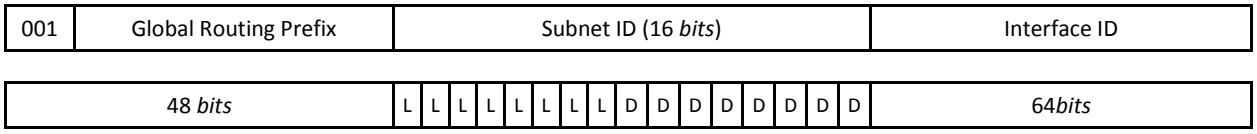

Figura 9 - Criação de uma sub-rede

Desta forma ficam atribuídos os 8 *bits* mais significativos para identificar a localização e os restantes 8 para identificar o departamento. Permite, assim, 256 localizações diferentes e, em cada uma destas, 256 departamentos.

2.7 Cabeçalhos

À semelhança do IPv4, o IPv6 também utiliza um cabeçalho por pacote, o qual contém informação necessária para permitir uma comunicação entre nós. De seguida, iremos analisar cada campo que constitui o cabeçalho de um pacote, cujo tamanho fixo é de 40 *bytes* [23].

Sendo o IPv6, uma evolução do IPv4, foi concebido com o objetivo de otimizar a comunicação e a segurança. Nesse sentido foram feitas alterações significativas no cabeçalho, começando pela remoção dos seguintes campos:

Header Lenght – Uma vez que no IPv4 o tamanho do cabeçalho não era fixo (mínimo de 20 bytes, máximo de 60 bytes, se fossem adicionadas opções);

Identification, Flags, Fragment Offset – Estes três campos estão relacionados com a fragmentação de pacotes, que ocorre quando um pacote enviado é demasiado grande para a rede a que se destina. No IPv6 esta opção é gerida pelas extensões de cabeçalhos;

Header Checksum – Com o principal objetivo de incrementar a velocidade de processamento da informação, este campo destinava-se a verificação de erros. Uma vez que no IPv6 a verificação de erros no *UDP* é obrigatória, a verificação de erros nesta camada foi considerada desnecessária.

2.7.1 Estrutura do Cabeçalho

Um cabeçalho de um pacote IPv6 é, de seguida, apresentado na Figura 10.

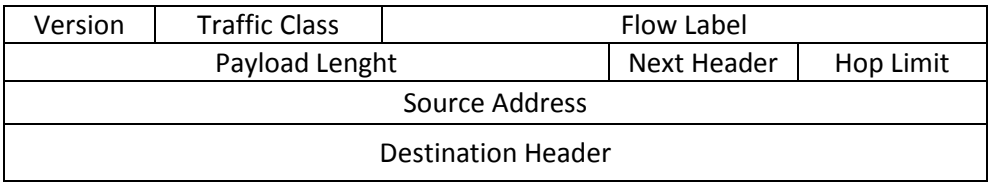

Figura 10 - Cabeçalho IPv6

Version [4 *bits*] – Indica a versão do protocolo, no caso do IPv6, o número é 6. No caso do IPv4, é 4;

Traffic Class [8 *bits*] - Permite a classificação do conteúdo do pacote, por classes ou por prioridades. Semelhante ao campo *Type of Service*, no IPv4 [29];

Flow Label [20 *bits*] – Definido para pacotes que pertençam a uma sequência de pacotes, que necessitam de um tratamento especial por parte dos *routers* IPv6. Por exemplo: *real time* (áudio/vídeo): os *routers*, ao identificarem que o pacote seguinte contém a mesma identificação do *Flow Label*, não necessitam de processar o cabeçalho novamente, economizando processamento. Importa destacar que é necessário que os campos *Source* e *Destination* sejam iguais em todos os pacotes que pertencem à mesma sequência;

Payload Lenght [16 *bits*] – Permite definir o tamanho da informação que segue no pacote, incluindo as extensões dos cabeçalhos. Possibilita, através dos 16 *bits*, indicar 65535 *bytes* de tamanho da informação. No entanto, se houver necessidade deste valor ser superior, é possível defini-lo, na extensão Hop-by-Hop Header, através da opção *Jumbogram Option*;

Next Header [8 *bits*] – Com recurso a representação numérica é possível identificar se o pacote contém extensão de cabeçalho, ou qual o protocolo do próximo pacote. Na Tabela 5 são listados os valores e a respetiva descrição do campo *Next Header* [23] [30];

Valor	**Descrição**
0	IPv4: reservado
	IPv6: Hop-by-Hop Header
1	ICMPv4
2	IGMPv4
4	IPv4
6	TCP
17	UDP
41	IPv6
43	Routing Header
44	Fragmentation Header
50	Encapsulating Security Payload Header
51	Authentication Header
58	ICMPv6
59	Não existe um pacote seguinte IPv6
60	Destination Options Header
88	EIGRP
89	OSPF
115	L2TP
135	Mobile IPv6

Tabela 5 - Valores do campo Next Header

Hop Limit [8 *bits*] – Indica o número máximo de *hosts* pelos quais o pacote irá viajar, até ser descartado;

Source Address [128 *bits*] – Contém o endereço IP da interface da qual é proveniente a mensagem;

Destination Address [128 *bits*] – Endereço de IP da interface à qual se destina o pacote.

2.7.2 Extensões de Cabeçalhos

A introdução de extensões de cabeçalhos é uma das grandes inovações desta nova versão do *Internet Protocol*. Fiabilidade, desempenho e segurança são alguns dos conceitos que são aprimorados com a criação desta funcionalidade.

A estrutura de uma extensão de cabeçalho, independentemente do tipo, é a que se pode verificar na Figura 11 [31].

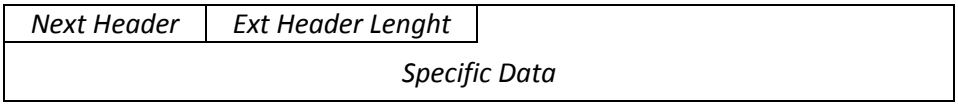

Figura 11 - Estrutura da extensão de cabeçalhos

***Next Header* [8 *bits*] –** Identifica o cabeçalho que sucede o atual;

***Extension Header Lenght* [8 *bits*] –** Define o tamanho dos dados do presente cabeçalho;

***Specific Data* [variável] –** O seu conteúdo depende do tipo de cabeçalho.

Hop-by-hop Options Header

Com base em [23] quando existe, este tipo de cabeçalho deve ser examinado por todos os nós, pelo qual passa ao longo do seu caminho. Surge imediatamente a seguir ao cabeçalho IPv6, é necessário que no pacote IPv6 o valor de *Next Header* esteja a 0, utilizado no caso do MLD[3], RSVP[4] e como *Jumbogram*[5].

O formato da extensão *Hop-by-Hop Options* é demonstrado na Figura 12.

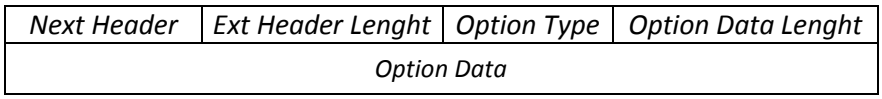

Figura 12 - *Hop-by-Hop Options Header*

***Next Header* [8 *bits*] –** Explicado na secção 2.7.2;

***Extension Header Lenght* [8 *bits*] –** Explicado na secção 2.7.2;

[3] *Multicast Listener Discover* (MLD) – Sub protocolo do ICMPv6. Concebido com o propósito de ativar no *router* a presença de nós que pertençam a grupos de *multicast*, garantindo que os pacotes *multicast* são entregues a todos os membros do respetivo grupo [48].
[4] *Resource Reservation Protocol* (RSVP) – Protocolo que permite a um determinado posto solicitar requisitos específicos para uma determinada transmissão de dados. Os *routers* utilizam-no em resposta ao solicitado pelo posto, servindo também como ferramenta de controlo e manutenção da qualidade de serviço concedida [127].
[5] *Jumbogram* – Acrescido ao pacote base IPv6 permite uma extensão do *payload* [128] [152].

***Option Type* [8 *bits*] –** Este octeto encontra-se subdividido em três partes, as quais são apresentadas de seguida;

Option Type (8 *bits*)		
XX	Y	ZZZZZ

XX) Os primeiros dois *bits* informam a ação que será tomada e encontram-se representados na Tabela 6 [25];

Valor	**Descrição**
00	Ignora e continua o processamento
01	Descarta o pacote
10	Descarta o pacote e envia um ICMP, com o código 2, para o nó emissor da mensagem
11	Descarta o pacote e envia um ICMP, com o código 2, para o nó emissor da mensagem, se o destinatário não for um endereço multicast

Tabela 6 – *Option Type*

Y) Se o *bit* estiver a 1, indica que o valor pode alterar a *en-route*. No caso de estar ativo, os dados da *Option Data* não serão analisados [32];

ZZZZZ) Os últimos 5 *bits*, ou os 5 *bits* menos significativos contêm informação muito importante, como é descrito na Tabela 7 [25];

Hex	**Binário**			**Descrição**
	XX	**Y**	**ZZZZZ**	
0	0	0	00000	Pad1
1	0	0	00001	PadN
C2	11	0	00010	Jumbo Payload
C3	11	0	00011	NSAP Address
4	0	0	00100	Tunnel Encapsulation Limit
5	0	0	00101	Router Alert
C6	1	0	00110	Binding Update
7	0	0	00111	Binding Acknowledgment
8	0	0	01000	Binding Request
C9	11	0	01001	Home Adress
8A	10	0	01010	Endpoint Identification

Tabela 7 - Descrição da combinação dos valores do campo *Option Type*

Com vista a otimizar o processamento da *Option Data,* destas extensões de cabeçalhos, a sua informação é alinhada com base nos octetos. Este ajuste é feito com base na inserção de *bits* com valor 0. Ou seja, quando há alguma informação que só ocupa três *bits*, torna-se

necessário inserir mais 5 *bits*, com o valor 0, para que a informação relativa àquela opção ocupe um octeto inteiro [25].

Pad1 – Esta opção é utilizada quando só um octeto precisa de ser preenchido com 0, para que acerte o limite com o octeto. É utilizado somente quando a ação é aplicada sobre um só octeto;

PadN – Quando é necessário efetuar o alinhamento a mais do que um octeto, é utilizada esta opção [32];

Router Alert – Todos os routers devem processar esta informação sempre que um pacote passa por eles;

Jumbo Payload option header – Indica se é ou não um pacote Jumbo.

***Option Data Lenght* [variável] –** Indica, em octetos, o tamanho do *Option Data;*

***Option Data* [variável] –** O seu conteúdo depende do tipo de cabeçalho.

Routing Header

Com base em [33] este tipo de cabeçalho é utilizado com o objetivo de criar uma lista de nós, os quais devem ser visitados no seu caminho até ao destinatário. O valor que o *Next Header* deverá ser 43. A estrutura do *routing header* é a seguir descrita na Figura 13.

Next Header	*Ext Header Lenght*	*Routing Type*	*Segments Left*
Type Specific Data			

Figura 13 - *Routing Header*

***Next Header* [8 *bits*] –** Explicado na secção 2.7.2;

***Extension Header Lenght* [8 *bits*] –** Explicado na secção 2.7.2;

***Routing Type* [8 *bits*] –** Explicado na secção 2.7.2;

***Segments Left* [8 *bits*] –** Neste campo constam quantos nós "obrigatórios" ainda faltam visitar, segundo a lista, até chegar ao destinatário;

***Type Specific Data* [variável] –** Esta informação depende do campo *Routing Type.*

Se um nó não conseguir interpretar a informação contida no *Routing Type*, será verificado o número de *Segments Left*, no caso de ser 0, o cabeçalho é ignorado pelo nó. No caso de ser diferente de 0, o pacote deve ser descartado e enviado um ICMP, com código de 0.

Fragment Header

Com base [33] este cabeçalho foi concebido com o objetivo de facilitar o envio e o tratamento de pacotes que excedam o MTU do nó destino. Ao contrário do que se passa no IPv4, no IPv6 os

routers pelos quais os pacotes passam até chegar ao nó destino, não são fragmentados e construídos sempre que passam por um router; os pacotes passam pelos *routers* fragmentados, sendo fragmentados no nó de origem e assemblados no nó de destino.

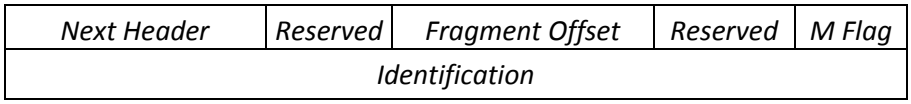

Figura 14 - Fragment Header

***Next Header* [8 *bits*] –** Explicado na secção 2.7.2;

***Reserved* [8 *bits*] –** Inicializado a 0;

***Fragment Offset* [13 *bits*] –** Contém o valor inicial do pacote original;

***Reserved* [2 *bits*] –** Inicializado a 0;

***M Flag* [1 *bits*] –** Com o valor 1 significa que este é precedido de mais fragmentos. O valor 0 indica que se trata do último fragmento;

Identification [32 *bits*] – O nó do qual é originário o pacote deve, de forma aleatória, gerar um valor que identifica o fragmento. Este valor deve ser diferente dos últimos fragmentos enviados entre a mesma origem e o mesmo destino.

Destination Options Header

Com base [33] por vezes, torna-se necessário, por parte do emissor, enviar alguma informação adicional para o recetor da mensagem, no entanto, no IPv4 essa informação podia ser enviada, mas era processada por todos os pontos pelos quais a mensagem passava até chegar ao seu destino. Com esta extensão de cabeçalho o processamento da informação nele contido é feito, única e exclusivamente pelo nó ao qual se destina o pacote.

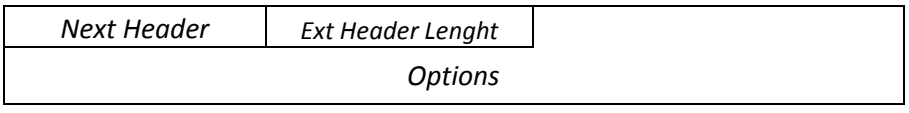

Figura 15 - Cabeçalho Destination Options

***Next Header* [8 *bits*] –** Explicado na secção 2.7.2;

***Extension Header Lenght* [8 *bits*] –** Explicado na secção 2.7.2;

***Options* [variável] –** Contém uma ou mais opções, o seu tamanho é definido no *Extension Header Lenght.*

Authentication Header

Com base em [34] e [35] uma grande inovação e um enorme avanço no que diz respeito à segurança da informação trocada sobre uma rede IP, é conferida por esta extensão de cabeçalho que é responsável pela autenticidade, integridade e o não-repúdio da informação. Não confere o princípio da confidencialidade, uma vez que a informação não é encriptada, mas garante a proteção contra alteração dos dados dos pacotes.

<table>
<tr><td>Next Header</td><td>Ext Header Lenght</td><td>Reserved</td><td>Security Parameters Index</td></tr>
<tr><td colspan="2">Sequence Number Field</td><td colspan="2">Integrity Check Value</td></tr>
</table>

Figura 16 - Estrutura do *Authentication Header*

Next Header **[8 *bits*] –** Explicado na secção 2.7.2;

Extension Header Lenght **[8 *bits*] –** Explicado na secção 2.7.2;

Reserved **[16 *bits*] –** Para utilização futura. Deve ser colocado todo a 0;

Security Parameters Index (SPI) **[32 *bits*] –** Valor aleatório que identifica as *security associations* (SA);

Sequence Number Field **[32 *bits*] –** Número sequencial, que deve ser incrementado pelo emissor da mensagem, sempre que envia um pacote;

Integrity Check Value (ICV) **[variável] –** Com base num algoritmo, este valor é gerado de forma a que o destinatário do pacote possa garantir a integridade do respetivo pacote [34].

Encapsulating Security Payload Header

Com base [36] o cabeçalho ESP confere aos pacotes Integridade, Confidencialidade, Não-Repúdio e dificulta a análise de tráfego da rede. A negociação deste mecanismo de segurança é baseada em *Security Associations,* como descrito na Figura 17 [36].

<table>
<tr><td colspan="3">SPI</td></tr>
<tr><td colspan="3">Sequence Number</td></tr>
<tr><td colspan="3">Payload Data</td></tr>
<tr><td>Padding</td><td>Pad Lenght</td><td>Next Header</td></tr>
<tr><td colspan="3">Authentication Data</td></tr>
</table>

Figura 17 - Encapsulating Security Payload Header

SPI **[4 bytes] –** Valor aleatório que identifica as *security associations.* Utilizado pelo recetor para associar os SA aos pacotes. É obrigatório, devendo ser suportado por todas as implementações de ESP;

***Sequence Number* [4 bytes]** – Tal como o nome indica trata-se de um número sequencial que é utilizado pelo recetor para garantir que não existe uma tentativa de envio de pacotes repetidos;

***Payload Data* [variável] –** Onde seguem os dados devidamente encriptados;

***Padding* [0 - 255 *bits*] –** Em caso de necessidade, utilizado para alinhar o conteúdo ao *byte;*

***Pad Lenght* [1 byte] –** Indica por quantos *Paddings* é precedido;

***Next Header* [1 byte] –** Explicado na secção 2.7.2;

***Integrity Check Value (ICV)* [variável] –** Com base num algoritmo este valor é gerado de forma a que o destinatário do pacote possa garantir a integridade do respetivo pacote [34].

2.8 ICMPv6

Já existente no IPv4, o Internet *Control Message Protocol* (ICMP) foi concebido com o objetivo de permitir obter, de forma simples, mais informação sobre a rede de comunicações e os equipamentos que a compõem [37].

Com o acréscimo de novas funcionalidades, o ICMPv6 apresenta-se como um protocolo muito mais poderoso.

O que é o ICMP? Para que serve?

O ICMP permite:

- Reportar erros ocorridos durante a comunicação e processamento dos dados;
- Diagnosticar a rede;
- Mapear endereços IP em endereços físicos (ARP no IPV4);
- Mapear endereços físicos em endereços IP (RARP no IPv4);
- Gestão dos membros de endereços *multicast* (IGMP no IPv4).

As mensagens ICMP são enviadas em diversas situações, tais como, quando um pacote não consegue chegar até ao seu destino; quando um *gateway* não tem, no momento, capacidade para encaminhar uma determinada mensagem; quando o MTU do nó destino é inferior ao do nó de origem. É também utilizado para verificar se um determinado nó se encontra ligado ou não à rede. [38]

É fundamental para a compreensão do restante capítulo entender que o ICMP pode emitir dois tipos diferentes de mensagens: as mensagens de erro e as mensagens de informação, cuja distinção é feita pelo *bit* mais à esquerda do campo *Type.*

2.8.1 Estrutura

O ICMP baseia-se, tal como toda a comunicação sobre IP, num cabeçalho, cuja estrutura é apresentada na Figura 18 [23].

Type	*Code*	*Checksum*
Message Body		

Figura 18 - Estrutura de um pacote ICMP

***Type* [8 *bits*] –** Tal como noutros cabeçalhos IP, identifica o tipo de mensagem que se segue;

***Code* [8 *bits*] –** Depende do anterior, no entanto, maioritariamente é utilizado para aumentar a granularidade da informação do campo *Type;*

***Checksum* [16 *bits*] –** Campo responsável por detetar informação corrompida. Este valor é criado com base nos endereços IPv6 do emissor e do destinatário das mensagens;

***Message Body* [variável] –** Dependendo do campo *Type* e *Code* o conteúdo deste campo varia.

2.8.2 Mensagens de Erro

Nas mensagens de erro, o *bit* mais significativo (mais à esquerda) do campo *Type* (que é constituído por 8 *bits*, no total) tem o valor 0, permitindo tipos de mensagens de 0 a 127 [23].

Type	Descrição	Code	Descrição
1	*Destination Unreacheable*	0	Não foi encontrada uma rota até ao destinatário
		1	Endereço inatingível
		2	Protocolo desconhecido
		3	Porta inatingível
		4	Fragmentação necessária
		5	Falha na rede do remetente
		6	Rede de destino desconhecida
		7	Erro no cabeçalho de *routing*
2	*Packet to Big*	0	Ignorado pelo recetor
3	*Time Exceeded*	0	*Hop Limit* atingido
		1	Assemblagem de fragmentos excedida
4	*Parameter Problem*	0	Erro encontrado no cabeçalho
		1	Cabeçalho do próximo pacote desconhecido
		2	Opção IPv6 não reconhecida

Tabela 8 - Mensagens de erro de ICMP

As mensagens de erro mais comuns são agora apresentadas de forma sumária na Tabela 8 [23] [39] [40] [41], algumas das quais serão abordadas com mais detalhe nas secções seguintes deste capítulo.

Destination Unreacheable
Esta mensagem é normalmente gerada por um *router* que se encontre nada rede. Tal como o nome indica, informa que o destino não pode ser alcançado não podendo a mensagem ser entregue [39].

Packet Too Big
Um *router* emite uma mensagem deste tipo quando o pacote que tenta enviar excede o MTU da rede a qual se destina o pacote [39].

Time Exceeded
Quando uma mensagem chega a um *router* e o *Hop Limit* encontra-se com o valor 0, o *router* emite uma mensagem que o pacote atingiu o número máximo de "saltos" definidos na emissão do pacote até à sua chegada ao destinatário [39].

Parameter Problem
Esta mensagem não tem que ser emitida por um *router*, pode ser emitida por um qualquer nó que se encontre na rede. Este erro é lançado quando um nó não consegue processar toda a informação contida num pacote indicando, ao emissor da mensagem danificada, o tipo de erro e a sua localização [39].

2.8.3 Mensagens de Informação

Nas mensagens de informação, o *bit* mais à esquerda do campo *Type* tem o valor 1, permitindo tipos de mensagens de 128 a 255 [23].

Echo Request
Estas mensagens são utilizadas para, principalmente, diagnosticar e monitorizar a rede [39]. Consistem, basicamente, numa mensagem simples, como por exemplo: "Estás vivo?".

Echo Reply
Em resposta ao pedido Echo Request, é necessário dar uma resposta. Desta forma, o *Echo Reply* consiste nessa resposta direcionada ao emissor do *Echo Request* [39].

Redirect Message
Mensagem enviada para o emissor de um determinado pacote, informando-o que deverá optar por outra rota para atingir o destinatário pretendido. Este tipo de mensagens não deve ser emitida por nós, uma vez que é responsabilidade dos *routers* [39].

Com base em [23] [39] [40] [42] [43] [44] [45] [46] [47] [48] resumem-se, na Tabela 9, as mensagens de informação do protocolo ICMP.

Type	Descrição
128	Echo Request
129	Echo Reply
130	Group Membership Query
131	Group Membership Report
132	Group Membership Reduction
133	Router Solicitaion
134	Router Advertisement
135	Neighbor Solicitation
136	Neighbor Advertisement
137	Redirect Message
138	Router Renumbering
139	ICMP Node Information Query
140	ICMP Node Information Response
141	Inverse Neighbor Discovery Solicitation Message
142	Inverse Neighbor Discovery Advertisement Message
143	Multicast Listener Discovery
144	Home Agent Address Discovery Request Message
145	Home Agent Discovery Response Message
146	Mobile Prefix Solicitation
147	Mobile Prefix Advertisement
148	Certification Path Solicitation
149	Certification Path Advertisement
151	Multicast Router Advertisement
152	Multicast Router Solicitation
153	Multicast Router Termination
155	RL Control Message

Tabela 9 - Mensagens de Informação de ICMP

2.9 Atribuição de Endereços

2.9.1 Stateless Address AutoConfiguration (SLAAC)

Como sabemos, para qualquer equipamento que esteja ligado a uma rede IP se habilitar a comunicar necessita, imprescindivelmente, de um identificador, conhecido como endereço IP. A sua configuração de forma manual já tinha sido praticamente erradicada com o aparecimento do DHCP, no IPv4, o que levou a uma extrema dependência dos servidores de DHCP. Uma vez que,

num futuro muito próximo, se prevê a extensão da tecnologia IP a frigoríficos e ar condicionado, torna-se necessário minimizar a dependência das comunicações do servidor DHCP.

À semelhança do DHCP, não é necessária qualquer configuração por parte dos nós na rede para se conseguir obter endereço de IP, através do SLAAC. No entanto, o *router* tem que ser configurado de forma a permitir essa configuração [49].

O endereço de IP é gerado com base nas seguintes variáveis:

- MAC Address;
- ID de interface escolhido de forma aleatória;
- Informação recebida por parte dos *routers.*

Os *routers* na rede podem anunciar um ou mais prefixos, cada nó adota os seus prefixos com base nas mensagens de *advertisement* dos *routers*. Este mecanismo permite uma muito rápida e eficaz alteração de IPs nos postos que se encontram ligados àquela rede, uma vez que os nós, em caso de ordem por parte do *router* só mudam o prefixo, mantendo-se todos os outros elementos constituintes do endereço. No caso de alteração do ISP, este novo irá atribuir um novo prefixo para se proceder em conformidade com esta alteração, só será necessário alterar configuração do *router* que irá alterar o prefixo e, posteriormente, difundirá pela rede a alteração do prefixo, mas manterá o *subnet ID*.

Stateless e *Statefull* podem ser combinados, sendo que a responsabilidade de atribuir IPs é conferida ao SLAAC e informação adicional fica ao cargo do *Statefull*, como por exemplo NTP e DNS servers.

Sempre que um endereço de rede é atribuído, ele tem um prazo de validade, que após ser expirado, torna-se um endereço inválido. Uma vez que não existe na rede, um servidor responsável pela emissão de endereços de IP, sempre que um nó gera o seu endereço, terá que validar se, na restante rede, existe um outro nó que já esteja a utilizar IP pretendido. Foi então criado o *Duplicate IP Address Detection* (DAD), que será abordado mais à frente [23].

Em jeito de balanço, os passos a serem dados num processo de SLAAC devem ser:

1. Obter o identificador da interface;
2. Aplicar a função de criptografia;
3. Utilizar o resultado da função na comparação feita através do DAD;
4. Definir os tempos de vida apropriados e associar-se aos grupos *multicast* pretendidos;
5. Continua a utilizar o antigo endereço de IP para comunicações anteriores, mas não para novas [50].

Este processo dever-se-á repetir todas as vezes que uma interface se conectar pela primeira vez a uma rede ou que se tenham esgotado os tempos de vida do endereço, definidos no ponto 4 [51].

2.9.2 Statefull Address AutoConfiguration (DHCPv6)

À semelhança da versão 4, o IPv6 tem também a possibilidade de atribuir de forma mais centralizada os endereços de IP às interfaces que assim o solicitarem [52]. Neste caso deixa de ser necessária a utilização de mecanismos como o DAD, uma vez que o endereço é sempre atribuído pelo servidor, conforme pode ser analisado na seguinte descrição do processo:

1. O nó liga-se à rede e, utilizando o seu endereço *link-local* envia um pedido, *Information-Request,* para o *multicast All_DHCP_Relay_Agents_and_Servers*;
2. O servidor de DHCP responde com base nos endereços que tem disponíveis na sua *pool*, assim como associa ao endereço outras informações para enviar para o cliente, como por exemplo informação relativa a DNS e NTP;
3. O cliente recebe a resposta por parte do servidor e envia uma mensagem confirmando a receção do seu endereço;
4. Por último o servidor envia um *acknowledge* informando que o registo está guardado no servidor [52] [53].

2.9.3 Configuração Manual

Já conhecida do IPv4, a configuração manual de endereços de rede é por norma posta de lado na maior parte das organizações, uma vez que obriga a uma configuração computador a computador, o que é indesejado pelos administradores de redes.

Utilizada em ambientes mais específicos, a definição do IP, número de *bits* que pertencem ao prefixo e a definição do endereço do *gateway* são colocados diretamente no computador que se vai ligar à rede, dependendo dos sistemas operativos pode ser feito através de um interface gráfico, ou alterando estas configurações num ficheiro de texto, onde as configurações de rede são armazenadas.

2.10 Neighbor Discovery Protocol

O *Neighbor Discovery Protocol* (NDP) é utilizado por nós, para descobrir endereços dos seus vizinhos na rede; para encontrar *routers* que possam encaminhar os seus pacotes para os destinatários corretos; e para manter uma lista atualizada de quais são ou não os nós que se encontram ainda alcançáveis [47].

O protocolo *Neighbor Discovery* baseia o seu funcionamento nas mensagens disponibilizadas pelo ICMPv6 [23].

Este protocolo é dotado de diversas funcionalidades, explicadas em [54]:

- Stateless Autoconfiguration de endereços IPv6 (SLAAC);
- Duplicate IP Address Detection (DAD);
- Router Discovery (RD);

- Neighbor Unreachability Detection (NUD);
- Secure Neighbor Discovery (SEND);
- Inverse Neighbor Discovery (IND).

2.10.1 Duplicate IP Address Detection (DAD)

Tendo em conta que o processo SLAAC é descentralizado, torna-se necessária a existência de um mecanismo que permite validar se um endereço pode ou não ser utilizado. Surge assim o *Duplicate IP Address Detection (DAD)*.

Durante este processo de validação os endereços passam por diferentes estados, que são descritos na Tabela 10 [55] [49].

Endereço	Descrição
Tentative Address	Endereço que ainda não foi atribuído. Existe enquanto está a ser verificado se existe outro endereço. Este endereço só permite troca de mensagens no processo de Neigbhor Discovery
Preferred Address	Endereço válido, que é utilizado para comunicar sem quaisquer restrições
Deprecated Address	Desaconselhado mas não proibido. Pode ser utilizado enquanto decorre uma comunicação, embora não seja mais utlizado como *source address*
Valid Address	Engloba os endereços *preferred* e *deprecated*
Invalid Address	Quando um endereço *valid* expira o seu tempo de vida
Optimistic Address	Endereço atribuído a uma interface, no entanto sujeito a algumas restrições uma vez que aguarda conclusão do processo de DAD.

Tabela 10 - Estados dos endereços durante o processo de DAD

O processo de autoconfiguração segue as seguintes fases:

1. O endereço é gerado com base na combinação do prefixo com o identificador gerado pelo próprio, denominado *tentative address;*
2. O nó começa a fazer parte dos grupos de *mulicast: all-nodes* e *solicited-node;*
3. Um pacote *Neighbor Solicitation* é enviado com o *tentative address*. Este pacote tem como destinatário o endereço *multicast solicited-nodes*. Se alguma interface já estiver a utilizar esse endereço como seu identificador, emitirá um *Neighbor Advertisement* avisando que o endereço já está em utilização. Caso o nó que pretende definir o seu IP receba um *Neighbor Advertisement* e se o ID tiver sido gerado de forma aleatória, será gerado um novo identificador. Caso o endereço seja definido com base em EUI-64, a configuração do endereço será parada e será necessária intervenção humana para proceder a uma configuração manual do equipamento. Caso não exista uma resposta ao *Neighbor Solicitation,* o posto adota o endereço que anteriormente se denominava *tentative address*, mas que a partir deste momento se chama *preferred address;*
4. O nó envia um *Router Solicitation* para o grupo *multicast* de *all-routers*, na tentativa de adquirir o prefixo.

Todos os *routers* respondem com um *router Advertisement.* Para cada resposta o nó gera um endereço, ficando cada um destes registados na lista de endereços para a respetiva interface.

2.10.2 Neighbor Unreachability Detection (NUD)

Tal como o nome indica, esta função tem como responsabilidade a deteção de vizinhos que se encontram disponíveis para aceitar comunicações. Este tipo funcionalidade aplica-se a todas as comunicações, quer sejam de nó para nó, nó para *router* ou de *router* para nó. Pode também ser utilizado entre *routers.* Importa referir que este tipo de verificações só são feitas para endereços de *unicast* e não é aplicável a endereços *multicast.*

A atuação em caso de falha de comunicação com outro nó depende do papel que este último desempenha na comunicação. Se se tratar de um *router*, o procedimento mais adequado é trocar de *router*. A confirmação da indisponibilidade de comunicação com outro nó, por norma, resulta na remoção da entrada da *Neighbor Cache* [55].

2.10.3 Secure Neighbor Discovery (SEND)

O protocolo *Neighbor Discovery* contém algumas falhas no que diz respeito à segurança, potenciando que sejam realizados alguns ataques através deste protocolo. Na tentativa de minimizar as ameaças ao ND foi definido o *Secure Neighbor Discovery* (SEND). Este protocolo será analisado mais adiante neste relatório.

2.10.4 Inverse Neighbor Discovery (IND)

Esta extensão ao protocolo *Neighbor Discovery* surgiu como substituto do RARP (protocolo que pertence à versão 4 do IP). No entanto, à semelhança de outras funcionalidades o *Inverse Neighbor Discovery* permite que um determinado nó, que pretenda saber o endereço IP de um outro, com base no seu MAC *Address*, o interrogue diretamente, sem necessidade de enviar uma mensagem para um endereço *multicast*, como acontecia no IPv4 [43]. Este processo permite uma redução na sobrecarga da rede uma vez que, sempre que um nó pretende enviar uma mensagem para outro, não necessita de enviar uma mensagem que chegue a todos os nós que se encontram nessa mesma rede.

As mensagens utilizadas têm o formato das mensagens usadas no protocolo ND. Para que esta extensão ao ND funcione convenientemente, torna-se necessário utilizar dois tipos de mensagens [43]:

Inverse Neighbor Discovery Solicitation
Esta mensagem é despoletada pelo nó que pretende saber o IP de um determinado equipamento na rede. Este tipo de mensagem é rotulado com o *Type* a 141 [23].

O nó que pretende obter a informação gera então um pacote, cujo objetivo é questionar o seu destinatário sobre qual o endereço IPv6, que corresponde ao seu endereço MAC [43].

Inverse Neighbor Discovery Advertisement
Como resposta ao *Inverse Neighbor Discovery Solicitation* o nó gera um pacote *Inverse Neighbor Discovery Advertisement*, que envia a informação relativa a todos os endereços de IP, que se encontram associados àquela interface [43].

2.10.5 Multicast Listener Discovery (MLD)

Concebido com o propósito de permitir a cada *router* na rede descobrir a presença de nós que subscrevam um determinado endereço *multicast*, este mecanismo garante que quando é enviada uma mensagem para um determinado endereço *multicast,* que a mesma chega a todos os devidos destinatários. Para tal, cada *router* guarda uma lista para cada *link* de quais os endereços *multicast* e quais os seus nós à escuta [45].

Estas mensagens podem ser emitidas com dois objetivos distintos:

- *General Query*, para saber quais os endereços *multicast* que têm nós à escuta na rede;
- *Multicast-Address-Specific Query,* emitida com o intuito de saber, para um dado endereço *multicast*, se existem alguns nós à escuta na rede.

A estrutura dos pacotes encontra-se representada na Figura 19 [45].

Type	*Code*	*Checksum*
Maximum Response Delay		*Reserved*
Multicast Address		

Figura 19 - Estrutura do pacote do protocolo MLD

***Type* [1 byte] –** Explicado na secção 2.8.1. Com o valor 130;

***Code* [1 byte]** – Explicado na secção 2.8.1- Inicializado a 0;

***Checksum* [2 bytes] –** Explicado na secção 2.8.1;

***Maximum Responde Delay* [2 bytes] –** Tal como o nome indica é o tempo máximo no qual deve chegar uma mensagem até ao *router*. Este é expresso em milissegundos;

***Reserved* [2 bytes] –** Inicializado a zero e ignorado pelos recetores;

***Multicast Address* [32 bytes] –** No caso de *General Query* segue com o valor 0. No caso de *Multicast-Address-Specific Query* este campo vai preenchido com o endereço *multicast* pretendido.

2.10.6 Mensagens

Router Solicitation (RS)

Mensagem enviada por um determinado nó com o intuito de saber quais os *routers* disponíveis na rede. Quando um *router* recebe um pedido destes, emite uma resposta através de um *Router Advertisement* [47].

Definidas no protocolo, encontram-se algumas regras que permitem a validação de RS válidos. Desta forma, caso os RS não cumpram os requisitos de seguida listados, os pacotes devem ser descartados, por razões de segurança [47].

- Caso o *Hop Limit* seja 255, significa que o valor ainda não foi decrementado por nenhum *router;*
- O código ICMP esteja a 0;
- O cumprimento do ICMP seja superior a 8 octetos;
- Se contiver o campo *options* com valor superior a 0;
- Caso o endereço de emissão do pacote não esteja definido.

Router Advertisement (RA)

Esta mensagem é gerada pelos *routers* periodicamente, com o intuito de informar os *hosts* na rede de que o *router* existe e que está apto a encaminhar pedidos. Por vezes, esta mensagem é gerada em resposta a um *Router Solicitation*, uma vez que o intervalo entre o envio de cada RA pode ser muito grande [47].

À semelhança de todas as mensagens que fazem parte do protocolo *Neighbor Discovery* existem regras que permitem a validação de RA. Caso os RA não cumpram os requisitos de seguida listados, os pacotes devem ser descartados:

- Caso o *Hop Limit* seja 255, significa que o valor ainda não foi decrementado por nenhum *router;*
- O código ICMP esteja a 0;
- O cumprimento do ICMP seja superior a 16 octetos;
- Se contiver o campo *options* com valor superior a 0;

Esta mensagem difunde informação de extrema importância para os nós que se encontram nessa rede, como por exemplo [56]:

- Anuncia que ele próprio (o *router*) se encontra disponível como rota alternativa;
- Informa os nós de qual é o prefixo atribuído e das respetivas alterações, com a respetiva *lifetime*;
- Indica o tipo de configuração permitida na rede;
- Disponibiliza informação como: H*op Limit,* MTU.

A estrutura do pacote encontra-se expressa na Figura 20 [23].

Type	Code					Checksum
Cur Hop Limit	M	O	H	DRP	Reserved	Router Lifetime
Reachable Time						
Retrans Timer						
Options						

Figura 20 – Estrutura de um pacote de *Router Advertisement*

***Type* [1 byte] –** Explicado na secção 2.8.1;

***Code* [1 byte] –** Explicado na secção 2.8.1;

***Checksum* [2 bytes] –** Explicado na secção 2.8.1;

Cur Hop Limit [1 byte] – Valor máximos de "saltos" possíveis até o pacote ser descartado;

Managed Address Configuration Flag [1 bit] – Quando com o valor 1 indica que o nó deve obter o seu IP através do serviço de DHCPv6;

Other Stateful Configuration Flag [1 bit] – Quando com o valor 1 indica que o nó deve solicitar ao servidor DHCPv6 restante informação, como DNS, etc;

Home Agent Flag [1 bit] – Este campo encontra-se reservado à gestão do IPv6 *mobile*

Default Router Preference [2 *bits*] – Indica o nível de preferência que deve ser dado ao *router* emissor do RA. Uma vez que vários *routers* podem responder ao RS com RA. Para o nó poder definir uma ordem de preferência de utilização dos *routers,* estes informam através deste valor: 01 (preferência máxima); 00 (média); 11 (baixa). Quando o DRP contém o valor 10 o *router* deve ser desativado, colocando a 0 o *router lifetime* [21]*;*

***Reserved* [3 *bits*] –** Reservado para utilização futura;

Router Lifetime [16 *bits*] – Informação relativa ao *default router*

Reachable Time [32 *bits*] – Especifica, em milissegundos, o tempo o qual deve ser necessário para alcançar o nó

Retrans Time [32 *bits*] – Tempo, em milissegundos, entre a emissão de mensagens *Neighbor Solicitation*

***Options* [Variável] -** Source link-layer address; MTU; Prefix Information [47].

Neighbor Solicitation (NS)

Esta mensagem, à semelhança do *Router Solicitation* é gerada por um nó que pretende obter informações acerca dos vizinhos. A geração desta mensagem pode ter como objetivo três tipos

distintos de respostas: (1) solicitar a tradução de um endereço IP, enviando para tal uma mensagem para o endereço *multicast all-nodes*; (2) a verificação da disponibilidade de um determinado vizinho, para obter esta informação o pacote é enviado com o campo destinatário contendo um endereço *unicast*; (3) para efetuar a verificação de endereços repetidos é esta a mensagem enviada para o endereço *multicast solicited-nodes* [23].

Com base em [47] é fundamental que exista um mecanismo primário de deteção de pacotes corrompidos, esse mecanismo funciona através da análise dos campos que constituem o pacote NS. O pacote deve ser descartado caso:

- O *Hop Limit* seja 255, significa que o valor ainda não foi decrementado por nenhum *router;*
- O código ICMP esteja a 0;
- O cumprimento do ICMP seja superior a 24 octetos;
- O endereço destino seja *multicast*.

Neighbor Advertisment (NA)

Em resposta a *Neighbor Solicitation* surge um *Neighbor Advertisement*.

Os NA são descartados [47] caso:

- O *Hop Limit* seja 255, significa que o valor ainda não foi decrementado por nenhum *router;*
- O código ICMP esteja a 0;
- O cumprimento do ICMP seja superior a 24 octetos;
- Se contiver o campo *options* com valor superior a 0;
- Se o endereço destino for um endereço *multicast*.

A estrutura do pacote *Neighbor Advertisement* é apresentada na Figura 21 [47].

Type	Code	Checksum
Reserved		
Target Address		
Options		

Figura 21 – Formato do pacote *Neighbor Advertisement*

***Type* [8 *bits*] –** Explicado na secção 2.8.1;

***Code* [8 *bits*] –** Explicado na secção 2.8.1;

***Checksum* [16 *bits*] –** Explicado na secção 2.8.1;

***Reserved* [4 bytes] –** Este octeto encontra-se reservado para utilização futura;

***Target Address* [16 bytes]** – Endereço de destino;

***Options* [Variável] –** Informações adicionais.

Redirect Message

Esta mensagem é também gerada nos *routers*, tem como objetivo informar o nó que emitiu uma determinada mensagem que chegou a este *router*, que pode utilizar um melhor caminho para atingir o destino que pretende [47].

Estas mensagens devem ser descartadas caso [47]:

- O *Hop Limit* seja 255, significa que o valor ainda não foi decrementado por nenhum *router;*
- O código ICMP esteja a 0;
- O cumprimento do ICMP seja superior a 40 octetos;
- Se contiver o campo *options* com valor superior a 0;
- O endereço de origem deve ser um endereço *link-local*.

Desta forma, na mensagem enviada ao nó, consta o endereço do próximo salto que deverá ser executado na próxima comunicação a fim de otimizar a comunicação.

2.11 DNSv6

Este é um dos mais importantes serviços providenciados nas redes, nomeadamente na Internet. Este é o serviço responsável por traduzir os nomes dos *websites* ou nós de uma rede, em endereços de IP.

O funcionamento é muito similar ao do IPv4, em vez de um registo ser do tipo A, passa agora a ser AAAA. Como o servidor não tem forma de saber qual o protocolo utilizado pelo cliente que solicita a tradução do nome, serão providenciados ao cliente os registos tipo A e AAAA.

A versão 6 é tomada como preferencial face à versão 4 [57].

2.12 Mobile IPv6

O IPv6 suporta uma funcionalidade que permite que um determinado nó troque de rede à qual se encontra ligado, sem que os interlocutores se apercebam da alteração [58]. Desta forma permite-se que um nó IPv6 não esteja restringindo a uma determinada localização, para que possa estar acessível [59].

Para que tal mecanismo funcione são essenciais 3 componentes, que podem ser graficamente identificados na Figura 22:

- ***Mobile Node*** – Nó que muda de localização, mas continua a ser alcançável;

- ***Home Agent*** – O *router* que se encontra no local onde o nó faz, pela primeira vez, uma ligação;
- ***Home Address*** – Endereço do *Mobile Node* enquanto ligado ao *Home Agent;*
- ***Correspondent Node*** – Nó com o qual o *Mobile Node* se encontra a comunicar fora da rede original;
- ***Care-of address*** – Endereço *unicast,* no *Home Agent,* enquanto o *Mobile Node* se encontra numa rede diferente.

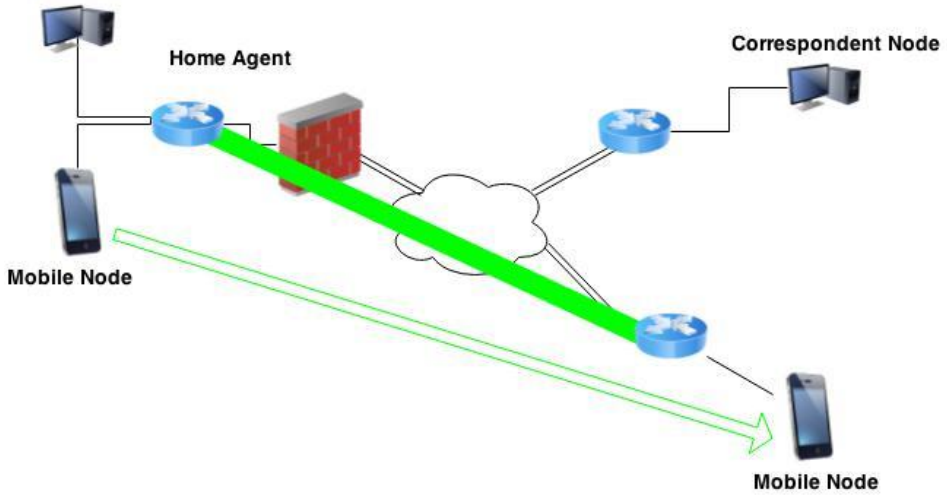

Figura 22 - Funcionamento do Mobile IPv6

Um *mobile node* deve ser sempre acessível através de sua "casa", quer se encontre ligado em casa ou noutro local qualquer. Enquanto o nó se encontra em "casa" a comunicação através dos pacotes IPs funciona como uma convencional comunicação.

Quando o *mobile node* se encontra fora da *home agent*, será posteriormente alcançável através do *care-of address*, que pode ser adquirido através de SLAAC ou DHCPv6.

O *mobile node*, depois de adquirido o seu endereço, informa o *home agent* do seu novo endereço de *IP* através de um *Binding Update,* passando todo o tráfego a ser encaminhado para o Mobile Node, onde quer que ele se encontre [58].

3 Abordagem à Segurança no IPv6

3.1 Introdução

Na definição e conceção da anterior versão do *Internet Protocol*, os aspetos de segurança não foram particularmente contemplados, mas com a evolução desta tecnologia e a respetiva globalização, a segurança tornou-se num dos mais importantes aspetos do protocolo. A introdução de mecanismos de autenticação foi o primeiro sinal dessa preocupação, mais tarde a introdução do IPSec sobre IPv4 foi também uma solução adotada, a fim de conferir um maior grau de segurança à informação que circula sobre a rede mundial.

Naturalmente, uma evolução de qualquer tecnologia tenta colmatar as falhas existentes na sua versão anterior. No que diz respeito à segurança, o IPv6 propõe alterações que visam aumentar as políticas que permitem garantir maior confidencialidade, integridade e autenticidade no acesso aos dados, tendo por base o IPSec, que já existia, mas não era amplamente utilizado na versão 4 do *Internet Protocol* [60]. A alteração na estrutura dos cabeçalhos dos pacotes tem um grande impacto na segurança do protocolo, uma vez que erradica alguns dos problemas que existiam baseados nos cabeçalhos no IPv4 [3].

Antes de avançarmos para os mecanismos e para que a sua interpretação seja a mais correta, torna-se fundamental que os conceitos sobre a matéria sejam assimilados. Os termos utilizados ao longo deste relatório relativos a segurança ficam aqui explicados. São detalhadas as duas principais inovações que vieram dotar o IPv6 de uma maior capacidade de garantir segurança: o IPSec e o SEND.

3.2 Conceito de Segurança

Quando se fala de segurança informática é necessário estarmos familiarizados com os seus princípios. À pergunta “O que é a segurança da informação?” provavelmente iriam ser dadas respostas muito diversas, podendo estar todas elas corretas.

Foi definida, universalmente, a resposta para essa pergunta: "*Information security is the protection of information and systems from unauthorized access, disclosure, modification, destruction or disruption*." [61].

Especialistas em matéria de segurança informática têm apontado dois conjuntos de conceitos base para facilmente identificar os pilares da segurança:

CIA

- **Confidencialidade (Confidentiality)** – Confere que a informação não é lida nem alterada por entidades não autorizadas;
- **Integridade (Integrity)** – Garante que qualquer alteração ao conteúdo da mensagem consegue ser detetada pelos intervenientes da comunicação;
- **Disponibilidade (Availability)** – Permite que a informação esteja sempre disponível aos utilizadores que têm autorização para lhe aceder [62].

AAA

- **Autenticação (Authentication) –** Certifica-se que um utilizador ou um grupo são realmente quem dizem ser, para tal são utilizados meios de verificação tais como: palavra-chave, PIN, dados biométricos, cartões de identificação, etc;
- **Autorização (Authorization)** - É possível garantir que cada utilizador ou grupo de utilizadores só acede ao conteúdo que lhe permitido;
- **Registo (Accounting)** - O registo e recolha de informação e recursos utilizados, quando e por quem [63].

O conceito de **não repúdio (non-repudiation)** é um dos outros pilares que não se encontra incluído em nenhum dos anteriores grupos, no entanto, não lhe confere menos importância que os restantes. Por não-repúdio entende-se a impossibilidade de negar uma ação, por exemplo: o envio de um email, cujo contenha assinatura digital, torna-o impossível de ser negado pelo seu emissor [64].

3.2.1 Terminologia Relevante

É fundamental, antes de abordar qualquer assunto relativo a vulnerabilidades, garantir que estão extintas todas as dúvidas que possam existir relacionadas com os conceitos base presentes neste tema.

Falha

Erro de uma aplicação ou sistema. Este conceito encontra-se diretamente ligado à conceção de um sistema, seja um *software*, uma rede ou outro ambiente. Uma falha poderá não resultar numa vulnerabilidade [65].

Vulnerabilidade

Por vulnerabilidade entende-se uma falha que permita a violação da política de segurança definida na entidade em questão [65] [66] [67].

Ataque

O ataque é a concretização ou exploração de uma ameaça, com base numa determinada técnica, por via de uma vulnerabilidade [65] [67].

3.2.2 Mecanismos

A fim de conferir os principais fundamentos da segurança de uma comunicação, são normalmente utilizados dois mecanismos distintos, que podem ser utilizados em parceria: cifragem e *checksums.* [23]

Criptografia

Para garantir que a informação não poderá ser acedida por terceiros, caso consigam ter acesso indevido aos dados, estes podem ser cifrados. Por cifragem entende-se uma codificação, no emissor, e descodificação no recetor da mensagem, com base num algoritmo deixando a mensagem de ter um formato legível [68]. No que diz respeito à cifragem, esta ainda se subdivide em duas:

- ***Criptografia de Chave Secreta*** **–** também chamada de simétrica, determina que o emissor e o recetor devem conhecer previamente uma determinada chave que é utilizada para cifrar os dados na origem e utilizada para decifrar os dados no destino. Destacam-se alguns dos mais comuns algoritmos: AES, DES e 3DES.

- ***Criptografia de Chave Pública*** – também chamada de assimétrica, utiliza um par de chaves para cada interveniente na comunicação, uma chave pública e uma chave privada. Alguns dos algoritmos mais utilizados são: RSA, ElGamal e ECC. As chaves podem ser utilizadas como se apresenta na Tabela 11.

Chave na Origem	Chave no Destino	Resultado
Chave Publica do Destinatário	Chave Privada do Destinatário	Só o destinatário conseguirá ler a mensagem
Chave Privada do Remetente	Chave Publica do Remetente	Garante que a mensagem é daquele remetente
Chave Publica do Destinatário + Chave Privada do Remetente	Chave Publica do Remetente + Chave Privada do Destinatário	Garante que a mensagem é daquele remetente e que só o destinatário a irá ler

Tabela 11 - Combinações de Chaves Assimétricas

Checksums
Usados em larga escala, com o objetivo de garantir a integridade dos dados. Com a introdução de uma mensagem com um tamanho variável, resulta numa *string* de tamanho fixo, chamada *hash* ou *message digest.* Os protocolos mais utilizados são: SHA-1 e MD-5 [23].

3.3 IPSec

O *Internet Protocol Security* (IPSec) foi proposto pela IETF, inicialmente na RFC 2401, atualizado na RFC 4301, que tem como objetivo a circulação de informação sensível através de redes desprotegidas, como por exemplo, a *Internet* [69] [70]. O IPSec tem três modelos de proteção: *gateway-to-gateway, host-to-gateway* e *host-to-host* [51].

O IPSec surgiu durante o crescimento do IPv4 para conferir a este protocolo algumas medidas de segurança. Trata-se de uma combinação de mecanismos referidos na secção anterior, criptografia simétrica, criptografia assimétrica e *Cheksums.* Este protocolo foi concebido com o objetivo de proporcionar interoperabilidade, qualidade em comunicação cifrada, tanto no IPv4, como no IPv6. Garante controlo de acessos, gestão da integridade da ligação, origem dos dados, confidencialidade, entre outros. A maioria dos serviços fornecidos pelo IPSec baseiam-se em: *Authentication Header* (AH) e *Encapsulating Security Payload* (ESP) [71].

Importa salientar que o IPSec é implementado como um módulo independente, querendo com isto garantir que não deverá interferir na comunicação de clientes que não estejam a utilizar a comunicação sob este protocolo. A modularidade permite a escolha de algoritmos de cifragem diferentes [71].

Para que seja possível estabelecer uma comunicação entre dois pontos utilizando IPSec é necessário que sejam definidas, previamente, algumas configurações. Estes tipos de comunicações chamam-se *Security Associations* (SA)*,* tais como a chave de cifra, mecanismo de autenticidade e parâmetros adicionais, que podem não ter caráter obrigatório.

O IPSec pode operar de duas formas distintas:

- ***Transport mode*** – O cabeçalho dos pacotes não é cifrado. A negociação é feita entre dois nós e define a cifragem ou autenticidade para o conteúdo do pacote (*payload)* [71].

- ***Tunnel mode*** – Por norma, entre dois *gateways*, onde todo o pacote incluindo o cabeçalho se encontra cifrado, sendo gerado um novo cabeçalho IP. Este caso é o fundamento base das V*irtual Private Network* (VPN) [71].

Uma vez que a cifragem simétrica tem por base uma chave e um algoritmo de criptografia, é necessário que exista um mecanismo que permita essa negociação, que acontece sobre comunicações desprotegidas. Foi então definido o Internet Key Exchange (*IKE),* cujo objetivo é gerir o processo de negociação das chaves. A versão vigente é a *IKEv2* [23].

As comunicações sobre este protocolo fazem-se sempre com base num par de mensagens, um pedido e a respetiva resposta a este conjunto de duas mensagens chama-se e*xchange* [72].

3.3.1 IPSec no IPv6

No IPv6 são definidos dois novos protocolos: *Authentication Header (AH)* e *Encapsulatiing Security Payload Header (ESP)* que surgem como *Extensions Headers* [73].

Authentication Header (AH)

Tem como missão garantir a integridade dos dados e a respetiva autenticidade do emissor da mensagem [74]. Os cabeçalhos dos pacotes IP também vêem garantida a sua integridade através do AH [69]. A Figura 23 mostra a estrutura de um cabeçalho de autenticidade [75].

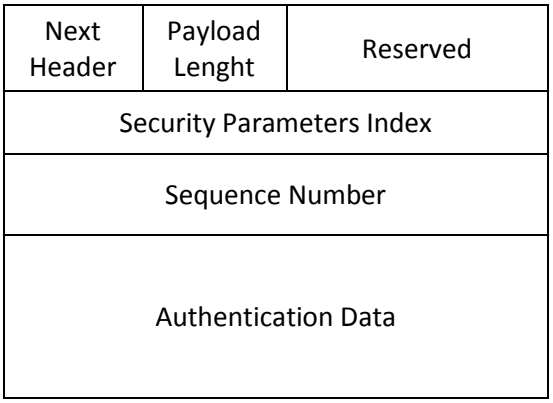

Figura 23 - *Authentication Header*

Next Header – Identifica o próximo cabeçalho;

Payload Lenght – Indica o tamanho do pacote;

Security Parameters Index – Contém o *Security Parameters Index* utilizado para a identificação das *SA;*

Sequence Number – Para evitar a repetição de pacotes;

Authentication Data – Contém informação relativa ao *Integrity Check VAlue (ICV)* que permite a autenticidade e a integridade dos dados [75].

Encapsulating Security Payload Header (ESP)

O ESP, quando aplicado, confere confidencialidade, integridade, não-repúdio e *Traffic Flow Confidentiality* [6] da mensagem [69]. ESP utiliza algoritmos de cifragem para garantir a

[6] *Traffic Flow Confidentiality* (TFC) - Mecanismo que permite mascarar/esconder os padrões de tráfico na rede, que previne a realização de análise estatística do tráfego e consequentes ataques [163].

confidencialidade do *payload* da mensagem [74]. A Figura 24 explica a estrutura do Encapsulating Security Payload [75].

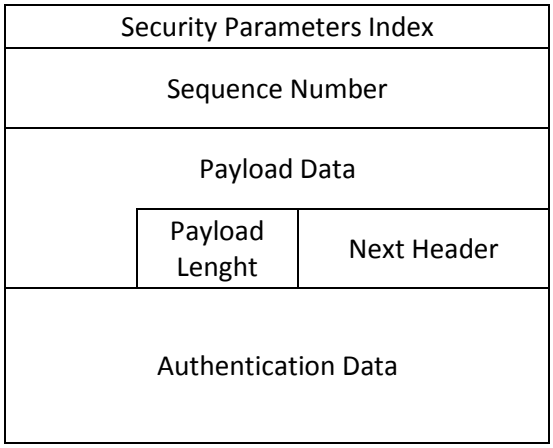

Figura 24 - *Encapsulating Security Payload*

***Security Parameters Index* –** Contém o *Security Parameters Index* utilizado para a identificação das *Security Associations;*

***Sequence Number* –** Para evitar a repetição de pacotes;

Payload Data – Campo cifrado com base num algoritmo de cifragem, identificado por um SA;

***Payload Lenght* –** Indica o tamanho do pacote;

***Next Header* –** Identifica o próximo cabeçalho;

Authentication Data – Contém informação relativa ao *Integrity Check VAlue (ICV)* que permite a autenticidade e a integridade dos dados [75].

Combinação de AH e ESP

Embora possam ser usados de forma independente o AH e o ESP podem também ser utilizados em simultâneo, desta forma o AH garante a autenticidade e a integridade mesmo antes do pacote ser decifrado [23]. Já o ESP tem a responsabilidade de garantir confidencialidade do pacote [74].

O *Internet Key Exchange (IKE)* é um protocolo concebido com o objetivo de gerir a troca de chaves (*Security Assocciations* [SA]) que cooperam com o IPSec. O IKE adiciona ao IPSec flexibilidade e ainda facilita a sua configuração [69].

O IPSec dispõe de dois modos de atuação:

Modo de Transporte

A configuração do IPSec deverá ser realizada em cada um dos pontos da comunicação, tendo a configuração que ser aplicada a cada um dos dispositivos, tal como apresenta a Figura 25 [70].

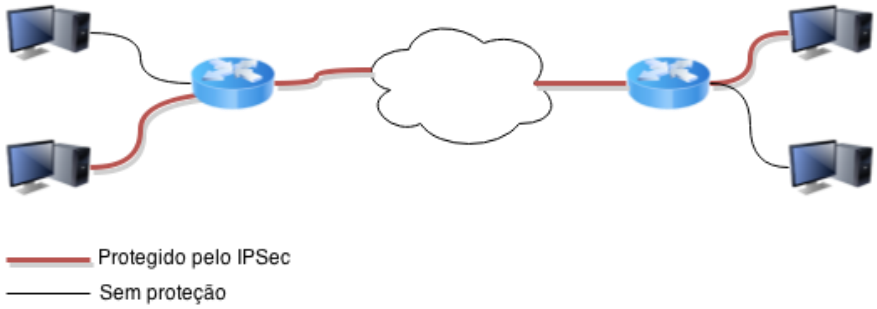

Figura 25 - IPSec – Modo de transporte

Modo de Túnel

O principal objetivo deste modo de operação é garantir que todo o tráfego que sai da rede local irá ser protegido pelo IPSec, enquanto "atravessa" a *Internet*. Ao contrário do que acontece no modo anteriormente apresentado, aqui a configuração só será feita uma única vez em cada um dos *routers*, no ponto onde começa e onde acaba a rede protegida pelo IPSec [70].

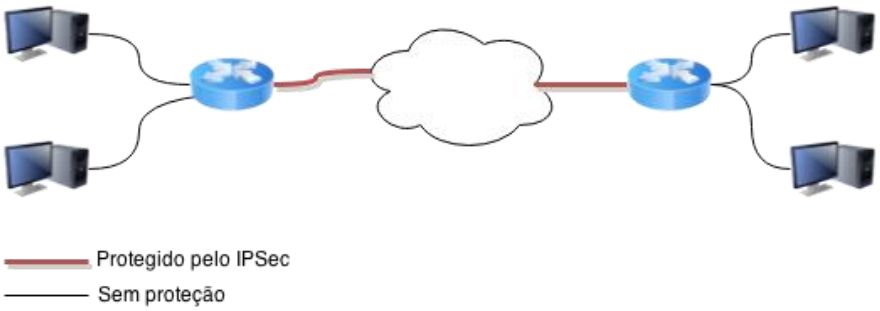

Figura 26 - IPSec – Modo de Túnel

3.4 SEND

O protocolo SEND foi concebido com o objetivo de reduzir o risco de ataques, conforme podem ser consultados mais à frente neste documento ou na RFC 3756 [76], ficando assim o SEND responsável por combater algumas das ameaças inerentes ao mecanismo de descoberta de vizinhos (*Neighbor Discovery – ND)* [54].

Um nó que trabalha sob SEND, dispõe de um par de chaves, pública e privada [74]. A fim de proporcionar as funções de segurança para o ND, foram introduzidas algumas novas opções ao protocolo, que passam agora a ser descritas [77].

No entanto, a utilização de criptografia implica um aumento da carga de computação dos equipamentos que operarem com este protocolo, o que pode resultar num problema de desempenho, caso o equipamento tenha pouca capacidade de processamento, ou seja

responsável por intermediar muitas comunicações. As validações de assinaturas, bem como a sua construção, são tarefas computacionalmente pesadas [78].

3.4.1 Cryptographically Generated Addresses (CGA)

Com a utilização do SEND não é permitido aos *hosts* escolher o próprio endereço de IP (os últimos 64 *bits*, ou menos significativos), o identificador será gerado com base em algumas variáveis. Este processo encontra-se representado na Figura 27.

A geração de uma CGA depende de três componentes:

- *Modifier* (número aleatório);
- Chave Pública;
- Prefixo da sub-rede.

Recorrendo ao algoritmo de cifragem SHA-1[7], é gerado o identificador da interface que, juntamente com o prefixo da sub-rede onde o nó se encontra, irá formar o endereço IPv6.

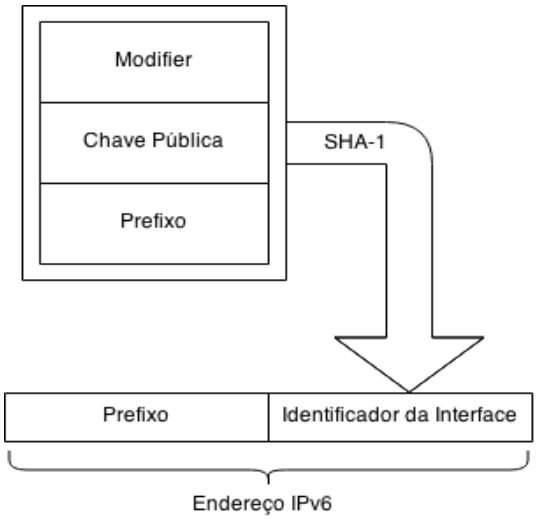

Figura 27 - CGA

Nas comunicações, quando um pacote é enviado, a chave pública do emissor passa também a fazer parte do pacote sendo este, posteriormente, assinado com a chave privada do emissor. Do lado do recetor é possível, com recurso à chave pública do emissor, validar a assinatura do pacote [51].

Em suma, o processo de comunicação utilizando SEND baseia-se nos seguintes passos:

[7] Secure Hash Algorithm 1 (SHA-1) – Algoritmo de encriptação [155].

- O emissor
  1. Gera o par de chaves e o respetivo endereço;
  2. Insere a chave pública do recetor no pacote;
  3. Assina com a sua chave privada;
- O recetor
  4. Recorrendo à sua chave pública do emissor acede à informação;
  5. Verifica com a sua chave privada a publica colocada pelo emissor;

É fundamental entender que este mecanismo só garante que a entidade que emitiu a chave e o pacote a analisar é a mesma, bem como que o pacote não foi alterado por nenhuma outra entidade.

A implementação deste tipo de mecanismos deve ser bem ponderada pois, em caso de uso excessivo de mecanismos de cifragem pode-se incorrer num acréscimo de *overheads* completamente desnecessários à comunicação [51].

3.4.2 Router Adverstisement Guard (RA-Guard)

O RA-Guard enquadra-se como uma subfunção do SEND, neste caso exclusivamente direcionado para filtrar pacotes RA, com base num conjunto de critérios. A seleção de quais os RAs legítimos, não se encontra ao cargo dos nós da rede, é responsabilidade de um membro de confiança da rede, um *router*, por exemplo.

Ao contrário do SEND o RA-Guard não valida as assinaturas ou certificados, pelo que não poderá ser garantida a autenticidade dos dados [78].

4 Transição e Implementação do IPv6

4.1 Introdução

Para a maioria das organizações é praticamente impossível implementar uma rede IPV6 de uma vez só. É necessário um passo intermédio que permita que a rede funcione em simultâneo com os dois protocolos, até que o processo de transição esteja completamente concluído.

Aquando do planeamento do IPv6 foram definidos três métodos que permitem auxiliar esta transição:

- **Dual-Stack**, quando os dois protocolos são usados em simultâneo na mesma rede, os equipamentos, como *routers,* têm os dois protocolos implementados, estando assim capazes de comunicar através dos dois protocolos;
- **Túneis** são criados túneis IPv6 sobre uma rede IPv4, permitindo assim que a comunicação IPv6 não fique isolada em ilhas em consequência da evolução do IPv6;
- **Tradução** é o mecanismo que a faz tradução entre protocolos. Quando um pacote IPv4 chega a uma rede IPv6, o dispositivo responsável pela tradução irá converter o pacote IPv4 em IPv6, à saída o pacote IPv6 é convertido num pacote IPv4.

Não existe uma especificação que permita qualificar qual a melhor das implementações, pois o sucesso da implementação depende muito de todo o cenário da organização. É fundamental que qualquer organização que pretenda implementar esta nova tecnologia prepare os seus responsáveis e técnicos para o processo de transição. Este processo de preparação exige formação e treino exaustivos, por parte dos intervenientes no processo [51].

Neste capítulo são abordados os três mecanismos que estão à disposição do administrador de redes para serem implementados durante a transição entre protocolos. Cada um dos métodos apresenta também algumas opções que são exploradas e demonstradas na respetiva subsecção. Para auxiliar na decisão de qual o mecanismo a adotar, no fim da explicação dos três mecanismos surge um quadro resumo que contém as vantagens e desvantagens de cada uma das opções. No entanto, o planeamento da transição do IPv4 para o IPv6 obriga a ponderar diversas variáveis que

são também apresentadas neste capítulo, onde é necessário ponderar a decisão com base no equipamento e *software* disponíveis, nos endereços de IP necessários e na forma como estes irão ser distribuídos.

4.2 Dual Stack

4.2.1 Funcionamento

Para uma organização pode ser vantajoso manter os dois protocolos em funcionamento, permitindo que os *hosts* consigam utilizar serviços IPv4 e IPv6, em simultâneo. Pode ainda tornar-se praticamente uma imposição, pois equipamentos mais antigos não suportarão o IPv6. Este método de coexistência de protocolos denomina-se *Dual Stack*. No entanto, para que funcione corretamente é necessário que esta funcionalidade seja suportada pelos equipamentos que compõem a rede da organização, que basicamente são capazes de entender, processar e enviar pacotes de ambos os protocolos.

Apesar de operarem em simultâneo e na mesma rede, o IPv4 e IPv6 são independentes. A migração de aplicações, redes e *hosts* pode ser feita de forma gradual [79]. No que diz respeito ao desempenho, escalabilidade e à eficiência, esta é o melhor dos três métodos apresentados [23].

Um nó pode ter três comportamentos distintos, que podem ser alterados ativando ou desativando cada uma das suas duas *stacks*, os modos de operação são IPv4-*only node*, IPv6-*only node* e IPv4/IPv6 *node*, que são abaixo descritos [23], podem também ser vistos na Figura 28.

IPv4-only node
Desta forma, o nó encontra-se com o IPv4 ativo e o IPv6 desativo. O nó comporta-se como se fosse um simples nó IPv4, sem que se apercebam que este tem uma *stack* IPv6.

IPv6-only node
O nó encontra-se com o IPv6 ativo e o IPv4 desativo. À semelhança do referido para o IPv4-only node, os seus interlocutores não sabem que este tem uma *stack* IPv4.

IPv4/IPv6 node
Tanto o IPv4, como o IPv6 se encontram ativos no nó. Assim sendo, o nó configurado como IPv4/IPv6 tem que ter, no mínimo, um endereço de IP para cada uma das suas interfaces. A definição do endereço pode, em IPv4 ser conseguida através de configuração manual ou DHCP e na interface IPv6 através de configuração manual, SLAAC ou DHCPv6.

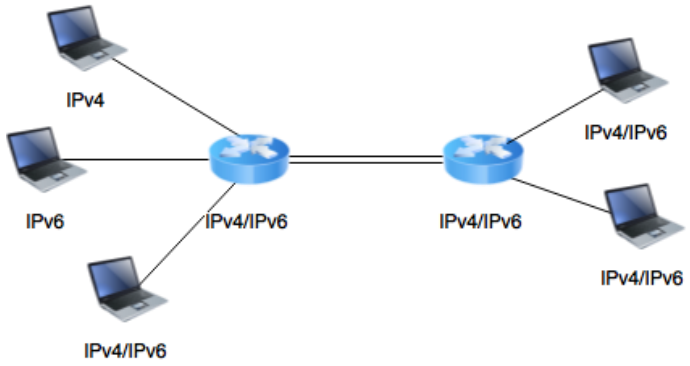

Figura 28 - Dual Stack

Servidor de DNS
No que diz respeito ao serviço de resolução de nomes, é possível que o administrador de rede dê preferência a um dos protocolos, preferencialmente, o IPv6, ordenando a prioridade dos registos, pelo protocolo a que pertencem.

Servidor de Endereços
Um serviço de DHCP pode ser configurado para suportar os dois protocolos em simultâneo, não sendo necessário ter dois servidores diferentes, com o mesmo objetivo, fornecer endereços aos *hosts* que o solicitem, independentemente do seu protocolo.

4.2.2 Implementação

Durante a implementação deste método de transição importa destacar que:

- Os dois protocolos terão que partilhar a largura de banda existente na rede;
- Os *routers* têm que:
  - Manter a tabela de encaminhamento para cada protocolo;
  - Executar protocolos de *routing* para cada uma das versões.
- O planeamento do endereçamento é autónomo;
- Se devem implementar políticas de segurança independentes;
- Os sistemas de deteção e prevenção de intrusão devem ser atualizados para cada um dos protocolos;
- A atualização a nível de *hardware* é fundamental uma vez que o processamento do IPv6 é mais exigente do que o do IPv4.

De forma a evitar a exposição a mais riscos, todos os serviços desnecessários devem ser desativados. Como este é considerado um protocolo de transição, assim que for possível aos nós, *routers* e servidores comunicar através do IPv6, os serviços de IPv4 devem, de imediato, ser desativados [51].

No que diz respeito aos *hosts*, dependendo do sistema operativo que esteja ativo, poderão existir diferentes comandos para executar determinadas operações, é possível que haja uma maior exigência de processador e maior necessidade de memória disponível.

Numa perspetiva de suporte desta solução, a missão detetar e corrigir problemas é dificultada, uma vez que obriga a que os responsáveis pela infraestrutura de comunicação dominem os dois protocolos e que estejam devidamente formados e treinados para operarem com ambos.

4.2.3 Problemas Associados

Um dos maiores problemas do Dual Stack é mesmo a sua introdução nos sistemas operativos. Nas plataformas da Microsoft, o IPv6 começou a ser introduzido no Windows Vista, no entanto, esta informação não é do conhecimento da maior parte dos utilizadores, deste e de outros sistemas operativos. Sem o conhecimento do *Dual-Stack* ativo os utilizadores, enquanto utilizadores de IPv4 assumem-se exclusivamente como clientes da versão 4, no entanto, se o *Dual-Stack* for suportado na rede a que se encontra ligado o computador, o equipamento na realidade encontra-se ligado aos dois protocolos em simultâneo, mas sem a perceção do utilizador. Esta falta de conhecimento por parte do utilizador leva a que as políticas de segurança se centrem no IPv4, deixando algumas vulnerabilidades prontas a serem exploradas por um atacante [74] [80].

4.3 Túneis

4.3.1 Funcionamento

A implementação deste método de transição tem vindo a aumentar de forma gradual. Derivada da ainda pouca adesão ao IPv6, surgem ilhas de IPv6, ou seja, redes ondem existe IPv6, mas que se encontram rodeadas por rede IPv4, o que tornaria impossível a comunicação aos nós que já utilizam a versão mais recente do protocolo. A solução passa por encapsular um protocolo dentro do outro. Ao longo do "caminho", o número de *hops* não será incrementado ao protocolo encapsulado [51].

Na sua essência, este método consiste no encapsulamento de pacotes IPv6, em pacotes IPv4,ou vice-versa, os quais são transportados até ao destino, onde são desencapsulados e "voltam a ser" pacotes do protocolo original.

Esta técnica tem como enorme vantagem a sua extrema flexibilidade, uma vez que permite que seja utilizado:

- Em paralelo com o *Dual-Stack;*
- De forma completamente autónoma;
- Juntamente com métodos de tradução.

Existem diversas formas deste mecanismo ser implementado, que passam agora a ser apresentadas e posteriormente detalhadas, com base [52]:

- 6over4 – comunicação entre nó-*router* ou *router*-nó;
- 6to4 e 6rd – comunicação entre *router-router;*
- ISATAP – túneis dentro de um *site;*
- Teredo – encapsulamento UDP para NATs IPv4.

6over4

Um dos mais simples mecanismos permite que uma ilha IPv6 comunique com outra, com base numa rede virtual criada sobre o protocolo IPv4 [81]. Devido à sua elevada dependência do IPv4, não é utilizado para "ligar" um nó IPv6 ao restante mundo IPv6.

A cada interface são atribuídos dois endereços, um *unicast* e um *link-local.* Recorre-se à utilização de um prefixo de 64 *bits*, e utiliza-se o IPv4 como identificador da *interface*, para completar a constituição do endereço [51].

6to4

Connection of IPv6 Domains via IPv4 Clouds é o verdadeiro nome deste mecanismo. O 6to4 não requer que as redes ou nós ligados sejam compatíveis com IPv4, ou que sejam configurados túneis de forma explícita; o seu funcionamento baseia-se na dependência de *routers* que se encontram nos limites das redes. Esta é uma das enormes vantagens deste tipo de *tunneling,* pois todos os restantes equipamentos da rede vão "pensar" que toda a comunicação tem por base rede IPv6.

Os endereços utilizados têm como prefixo 2002::/16.

A implementação deste mecanismo jamais deve ser encarada com caráter permanente [23].

De seguida é apresentada uma imagem que permite observar o processo no qual se baseia o 6to4.

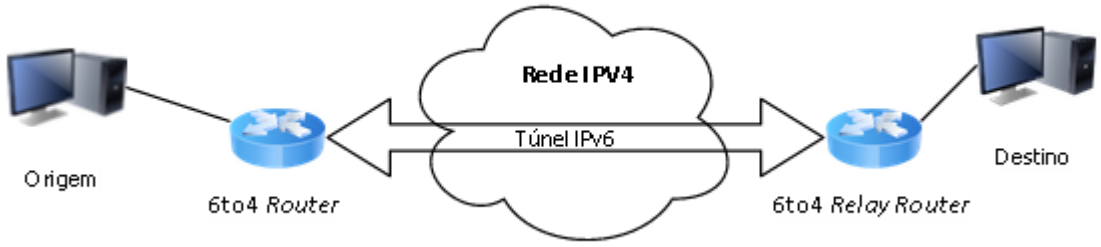

Figura 29 - Túnel 6to4

6rd

Com base no já existente 6to4, este mecanismo diferencia-se do anterior na constituição do endereço [82]. Em alternativa à utilização do prefixo determinado para o 6to4, neste é utilizado um prefixo definido pelo ISP [83]. O que elimina alguns problemas relacionados com a utilização de prefixos conhecidos pelos atacantes [57]. Desta forma, o domínio 6rd é tão grande como a rede do

seu ISP, o que lhe permite um controlo sobre a rede. Já do ponto de vista dos clientes, trata-se de toda uma rede IPV6 nativa [84].

ISATAP
Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) permite isolar nós IPv6 de uma rede que funciona em IPv4. É, normalmente, utilizado dentro das organizações, em casos onde o ISP fornece IPv6, mas este protocolo não é suportado dentro das organizações [85].

Teredo
De todas as alternativas de *tunneling* anteriormente apresentadas, nenhuma consegue lidar com o NAT [86]. É no sentido de colmatar esta falha que surge o Teredo.

4.3.2 Implementação

Quando um administrador de rede tem que gerir este tipo de mecanismo, tem que distinguir dois cenários [74]:

- Quando o túnel tem o seu ponto de entrada e de saída dentro da rede;
- Quando o ponto de entrada no túnel se encontra na rede, mas o ponto de saída se encontra fora da rede gerida pelo administrador.

Todo o tráfego deve, obrigatoriamente, ser inspecionado para ser considerado confiável, caso contrário, poderá ser facilitado o trabalho de um atacante.

Os pontos de entrada e saída dos túneis devem ser o maior foco da segurança na implementação desta técnica, pois os atacantes tentam atacar estes pontos para “entrarem” no túnel. Os túneis devem ser tratados como se de um acesso externo se trateasse, de forma a evitar riscos maiores.

Filtragem de pacotes e sistemas de deteção e proteção devem estar sempre ativos, analisando o protocolo que chega encapsulado [51].

A utilização de algoritmos de criptografia obriga a que ou o ponto de término do túnel se encontre antes do mecanismo de análise de tráfego, ou então o dispositivo responsável por analisar o tráfego terá que decifrar o tráfego, analisá-lo e posteriormente encapsulá-lo de novo, causando um impacto negativo no desempenho da comunicação [51].

4.3.3 Problemas Associados

Um atacante consegue forjar endereços e esconder a origem do seu ataque, isto porque nos pontos de saídas dos túneis descartam o cabeçalho IPv4, acoplando o cabeçalho IPv6, deixando assim de ser possível ter conhecimento dos endereços de entrada e de saída do túnel. Na tentativa de proteger as redes destas falhas, os pontos de saída do túnel devem ser configurados para validarem se o endereço de origem do pacote coincide com o ponto de entrada do túnel. O IPSec também é recomendado neste ambiente [78].

O *Denial-of-Service* não é também um novo tipo de ataque, no entanto, pode ser implementado recorrendo à injeção de pacotes falsificados num dos pontos do túnel [7].

4.4 Tradução

4.4.1 Funcionamento

Network Address Translation (NAT) é já um conceito conhecido do IPv4. No IPv4 é responsável pela comunicação de uma rede privada, com a rede pública. Ao NAT foi acrescentado o *Protocol Translation*, passando a designar-se por NAT-PT [87]. Por norma, o dispositivo que suporta esta funcionalidade encontra-se instalado entre a rede IPv4 e a rede IPv6. Este equipamento, que poderá ser uma *firewall* ou um *router*, dispõe de uma gama de endereços IPv4 para poder atribuir de forma dinâmica aos nós IPv6 [74].

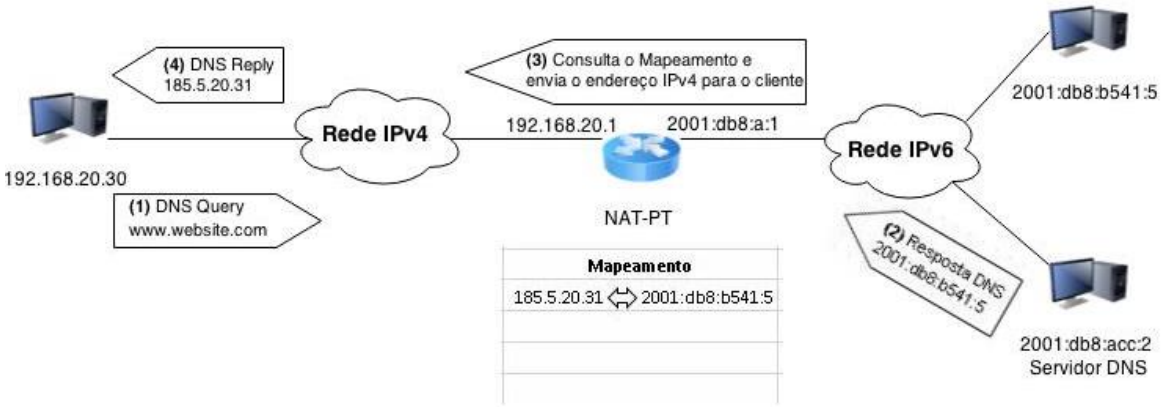

Figura 30 – Túnel NAT-PT

4.5 Comparação de mecanismos

Os três mecanismos analisados possibilitam uma transição de IPV4 para IPv6 de forma a que se afete o menos possível o normal funcionamento das redes. Os três devem ser utilizados, cada um numa determinada fase.

Sem dúvida que o *Dual-Stack* seria o meio de eleição, no entanto, esta implementação acarreta custos elevados. Tendo em conta o cenário económico nacional e mundial, não é preferência das empresas fazer este tipo de investimentos na sua tecnologia de rede, pelo que a implementação exclusiva de *Dual-Stack* deixa de ser válida. Aliados aos custos de implementação, problemas de segurança aumentam o grau de receio por parte das organizações em pôr em prática este mecanismo, uma vez que tem que haver, por parte do *staff*, um profundo conhecimento de ambos os protocolos.

Na Tabela 12 são apresentados os pontos mais fortes e mais frágeis de cada um dos métodos [23].

Dual-Stack	
Vantagens	• Muito flexível • Nós da rede nem se apercebem da presença do mecanismo (facilidade) • Fácil de desativar
Desvantagens	• Gestão de dois protocolos, em simultâneo • Nós da rede nem se apercebem da presença do mecanismo (segurança) • As tabelas de ambos os protocolos têm que ser guardadas • Protocolo de *routing* e regras de segurança para cada um dos protocolos • Resolução de problemas mais complexos, pois têm que ser analisados dois protocolos • Deve ser temporário
Túneis	
Vantagens	• Permite a migração faseada da rede • O ISP não necessita de suportar IPv6 • Permite interligar ilhas IPv6
Desvantagens	• Aumenta o *load balance* dos *routers* • Os pontos de entrada e de saída do túnel necessitam de mais CPU, uma vez que têm que encapsular e desencapsular o tráfego • Ponto de falha sem redundância • Os clientes IPv4 não podem comunicar com clientes IPv6 e vice-versa
Tradução	
Vantagens	• Permite a comunicação direta entre *hosts* IPv6 e *hosts* IPv4, e vice-versa
Desvantagens	• As funcionalidades introduzidas pelo IPv6 não podem ser utilizadas • Limita o desenho das topologias de rede

Tabela 12 – Vantagens e Desvantagens dos Mecanismos de Transição

	Serviços têm que ser atualizados (ex DNS, DHCP …)	**Custos**	**Complexidade**	**Interoperabilidade**
Dual Stack	✓	⇧	⇩	✓
Túneis	×	⇩	⇧⇩	×
Tradução	✓	⇩	⇧	✓

Tabela 13 – Comparação de Mecanismos de Transição

4.6 Implementação IPv6

Para implementar qualquer tecnologia, é primordial que os técnicos que irão operacionalizar a implementação estejam preparados para os desafios que vão encontrar ao longo do processo.

De seguida, são apresentados os principais passos para a implementação do novo protocolo IP.

4.6.1 Processo

Com base no levantamento de literatura [51] [57] [88] e na experiência própria durante este estudo, foi definido um processo sequencial que permite aos responsáveis ter por base um conjunto de práticas a seguir:

1º. Verificar o suporte de IPv6 por parte do ISP;
2º. Analisar a situação atual da organização:
    1. Tecnologia existente;
    2. Identificar equipamentos, aplicações, dados e serviços existentes.
3º. Elaborar um estudo do impacto da migração para a organização;
4º. Estimar os custos da migração;
5º. Elaborar o plano de migração:
    1. Atualizar ou substituir o equipamento que não suporta IPv6;
    2. Estratégia de transição;
    3. Plano de endereçamento;
    4. Definição do plano de segurança e de emergência.
6º. Testar a implementação: identificar e resolver problemas;
7º. Documentação;
8º. Implementação:
    1. Implementação faseada de serviços IPv6;
    2. Desativação de serviços IPv4.
9º. Monitorização e atualização;

Verificar o suporte de IPv6 por parte do ISP

Não precisa de ser obrigatoriamente o primeiro passo, uma vez que esta verificação poderá ser feita em qualquer altura, antes da implementação propriamente dita. No entanto, caso o ISP não disponha do serviço pretendido, a mudança de operador poderá demorar algum tempo, pelo que é aconselhado que seja a primeira verificação do processo. Em Portugal, os principais ISPs já dispõe de serviço IPV6 [89].

Analisar a situação atual da organização

Como prática aconselhável antes de qualquer procedimento informático, deve sempre ser analisado o contexto, antes de se partir para o planeamento. Desta forma, nesta primeira fase o conhecimento sobre tecnologia, neste caso IPV4, deve ser bem sólido, para que se entenda toda a estrutura já existente na organização.

A inventariação de todos os equipamentos, aplicações, serviços e dados que compõem a rede são também uma ação fundamental para que, posteriormente, se possa planear o que irá ser substituído por IPv6, ou o que terá de ser compatibilizado com a nova tecnologia.

Elaborar um estudo do impacto da migração para a organização

Depois de bem identificados os equipamentos, serviços e dados das aplicações, é possível identificar as vantagens e desvantagens que esta poderá trazer para a organização.

Estimar os custos da migração

Nos dias de hoje, a maioria das empresas tem um fator que influencia, de forma determinante, todos os seus setores, a questão financeira. A empresa tem que garantir, para esta mudança de protocolo, um orçamento que suporte todo este processo. Esta estimativa de custos deve ser sempre apresentada para apreciação, juntamente com o estudo do impacto da migração na organização, que por si só fundamenta a necessidade da migração para a nova versão do protocolo.

Elaborar o plano de migração

Equipamento

Numa primeira análise é fundamental saber se os equipamentos e *firmwares* suportam o IPV6. No entanto, o suporte para IPv6 não é suficiente. É preciso analisar se os dispositivos suportam a estratégia de transição escolhida pelo administrador de rede.

Alguns equipamentos que suportam IPv4 podem suportar nativamente IPv6. No entanto, outros exigem uma atualização ao seu *firmware* para que o protocolo mais recente seja suportado. Embora alguns equipamentos de IPv4 suportem nativamente ou através de *update* o IPv6, para que se tire proveito de todos os benefícios da nova versão do IP, é necessário que o *hardware* seja também atualizado, principalmente de equipamentos como *routers, switches* e *firewalls.* Só desta forma será possível explorar todas as vantagens inerentes à utilização do IPv6, nomeadamente a nível do desempenho, uma vez que este irá necessitar de mais poder de processamento e também de mais memória disponível. Uma vez que o *upgrade* para equipamentos de IPv6 não é obrigatório, mas sim aconselhável, a substituição do equipamento antigo poderá ser incorporada nos habituais ciclos de renovação de equipamento, que as organizações devem planear [90].

Software

Na sua maioria, o *software* poderá ser atualizado nos ciclos de renovação mencionados no *hardware*, não havendo, à partida, uma necessidade urgente de atualização. No entanto, é altamente aconselhável que todo o *software* envolvente (servidores, *workstations*, ferramentas de administração de redes entre outras aplicações que possam depender do protocolo de rede) suportem o novo protocolo de forma a que este funcione na sua plenitude [90].

Estratégia

Com base na informação dada anteriormente neste capítulo, é fundamental que se decidam quais os métodos de transição a adotar para cada ambiente da organização: *dual-stack*, túneis ou tradução.

Endereçamento

No que diz respeito ao plano de endereçamento, o IPv6 vem resolver um enorme problema que existia no IPv4, a falta de endereços. O prefixo atribuído a cada entidade que solicita um endereço ocupa 48 *bits* dos 64 *bits* disponíveis para o prefixo que, juntamente com os 64 *bits* do endereço da interface, constituam os 128 *bits* do endereço. Como podemos entender pelos valores apresentados se o prefixo do endereço são 64 *bits* e o endereço atribuído a uma organização são 48 *bits*, sobram 16 *bits*. Estes 16 *bits* podem ser utilizados para fazer uma divisão lógica e/ou operacional da organização.

De seguida é apresentado, na Figura 31, um exemplo da forma como podem ser utilizados estes 16 *bits* restantes [28].
A título de exemplo considera-se que o endereço atribuído à organização é : 2001:db8:cafe::/64

Prefixo																::/64
Endereço atribuído à organização pelo ISP												*Bits* disponíveis				
2	**0**	**0**	**1**	**0**	**d**	**b**	**8**	**c**	**a**	**f**	**e**	**L**	**T**	**S**	**S**	
0010	0000	0000	0001	0000	1100	1010	1000	1011	1001	1111	1110	LLLL	TTTT	SSSS	SSSS	

Figura 31 – Proposta de 16 *bits* destinados à definição da sub rede num endereço IPv6

L – Localização. A utilização destes 4 *bits* permite uma combinação de 16 localizações

T – Categoria ou Tipo. Podem ser criados 16 tipos/categorias (por exemplo: servidores, técnicos, docentes, alunos, público, etc)

S – Sub-rede. Os 8 *bits* disponíveis permitem a criação de 256 sub-redes

A atribuição dos "L", "T" e "S" terá que se adaptar às necessidades em causa. É fundamental que quando se está a planear esta distribuição que se tenha em conta um crescimento futuro.

Naturalmente que a ordem sugerida no exemplo não é obrigatória, podendo o administrador de rede segmentar os endereços de uma outra forma. No entanto, importa referir que caso a segmentação seja baseada na localização e tipo, deve ser tida em conta a ordem dos elementos, que é agora brevemente explicada:

- Localização primeiro (2001:db8:café:LTSS::/64): Com esta opção permite-se que nas tabelas de endereçamento as entradas para cada edifício possam ser agregadas num só endereço, mantendo assim as tabelas compactas;

- Tipo primeiro (2001:db8:café:TLSS::/64): Com esta sequência torna-se mais simples a implementação de políticas de segurança, na *firewall* [28].

No que diz respeito à configuração de endereços de IP nos clientes, como já foi abordado anteriormente, existem três formas de o fazer [19] [28]:

- *Stateless Address Autoconfiguration* (SLAAC);
- *Dynamic Host Configuration* Protocol versão 6 (DHCPv6);
- Configuração Manual.

Plano de segurança e recuperação

Para que se possa avançar com qualquer um destes planos, é fundamental entender que deverá existir na organização uma política de segurança convenientemente elaborada e aprovada por todos os órgãos da organização. Definir planos de segurança e de recuperação em caso de emergência é também uma tarefa essencial embora que, por norma, estes são descartados da sua importância por alguns dos responsáveis pela infraestrutura informática das empresas.

Testar a implementação: Identificar e resolver problemas

Nesta fase pretende-se que os responsáveis criem um ambiente que lhes permita testar a implementação, baseando-se num ambiente virtual ou até num ambiente real, mas restrito. Pretende-se que as práticas sejam encaradas como se de um ambiente real se tratasse, para possibilitar uma maior facilidade na deteção de erros e sua respetiva resolução.

Documentação

Uma das maiores dificuldades da implementação de qualquer estratégia ou outro processo é a fase de documentação. Embora surja como a 7ª fase, esta é uma fase que começa desde a primeira fase e que, na realidade, não mais termina. Neste documento pretende-se que estejam assentes todas as decisões, planeamentos, sugestões, dúvidas, implementações, testes, correções, alterações, configurações, procedimentos, etc. Em suma, toda a informação que diz respeito ao processo de migração.

Surge nesta posição, por ter um papel determinante na fase seguinte, ou seja, para partir para a implementação propriamente dita, é altamente aconselhável que a documentação se encontre bem estruturada para que, em caso de dúvida, a equipa que se encontra a implementar possa recorrer à documentação e esclarecer qualquer questão que surja.

Implementação

Esta fase, encarada como a mais crítica, deverá ser a fase mais simples de todas as anteriores, uma vez que todos os procedimentos devem estar descritos detalhadamente na documentação elaborada na fase anterior. No entanto, é nesta fase que qualquer erro pode colocar em causa a produtividade de uma empresa. Uma falha pode acarretar prejuízos bastante elevados para uma organização.

A implementação deve ser faseada, com testes unitários, para que seja possível atestar que os procedimentos anteriores se encontram corretamente implementados. Depois de atestada a correta implementação dos procedimentos, os serviços IPv4 devem ir sendo também desativados, para que, não fiquem na rede serviços IPv4 “perdidos”.

Monitorização e atualização

Esta é a fase que não permite que a elaboração da documentação possa ser dada por concluída pois a rede, os equipamentos e serviços devem constantemente ser monitorizados, tornando possível a rápida resolução pois, em caso de falhas, devem também ser documentadas.

Como é do conhecimento geral, todos os serviços, aplicações ou *frameworks* vão, ao longo do tempo, sendo atualizados. As atualizações não devem ser descuradas pois, por norma, estas vêm resolver problemas que são encontrados ao longo do tempo, em que os sistemas se encontram em produção. Todas as atualizações e processos consequentes devem ser também documentados.

5 Catálogo de Vulnerabilidades

5.1 Introdução

Os problemas que comprometem a segurança de uma rede informática podem ter as mais diversas origens. Para além do aumento do espaço de endereços, o IPv6 tem também, desde a sua origem, um grande foque na segurança. No entanto, alguns dos problemas do IPv4 são herdados pelo IPv6.

Algumas das principais falhas dos sistemas citadas na literatura são [91] [23]:

- Inexistência ou falhas de segurança em *software*, *firmware e hardware* utilizado numa rede;
- Inexistência de um plano com os possíveis ataques e as respetivas medidas a implementar, em caso de ataque;
- Incorreta atribuição de privilégios;
- Roubo de identidade;
- *Trojan horses* e vírus;
- Vulnerabilidades da arquitetura da tecnologia como: *IP spoofing, Denial of Service, man-in-the-middle, DNS poising e DHCP snooping.*

A integração do IPv6 em ambientes onde anteriormente se encontrava implementado o IPv4 implica um aumento da complexidade da rede, uma vez que ambos os protocolos se encontram presentes. Obriga a um cuidado extremo na implementação do processo de transição, bem como na alteração de configurações [92].

O aparecimento do IPv6 complicou algumas tarefas dos sistemas de segurança existentes no IPv4, ainda que algumas possam ser temporárias:

- No IPv4 a reputação dos IPs permitia filtrar IPs conhecidos como maliciosos. Na nova versão, para já, não existe uma base de dados com os IPs potencialmente perigosos, visto que esta se constrói ao longo dos anos;

- Outro dos problemas que pode comprometer o sucesso da segurança é o facto de o IPv6, na maioria dos equipamentos, vir ativo por omissão. Desta forma, quando se julga estar a trabalhar só sobre IPv4, a interface IPv6 pode estar ativa sem ser monitorizada, ficando mais vulnerável a ataques;
- A pesquisa num registo de eventos ficará também mais dificultada, uma vez que no IPv6 um endereço pode ser representado de diversas formas, como por exemplo, 2001:db8:babe::cafe e 2001:db8:babe:0:0::café;
- Por ainda ser uma tecnologia recente, a versão 6 do IP poderá contemplar ainda problemas desconhecidos, podendo ser exploradas vulnerabilidades que não tenham, até à data, sido identificadas [93].

Dada a importância que a segurança tem numa rede de comunicações, é fundamental identificar as vulnerabilidades e as respetivas consequências. Naturalmente, é impossível catalogar todas as vulnerabilidades existentes na versão 6 do protocolo, pelo que serão abordadas 18 vulnerabilidades consideradas mais relevantes, dada a sua fácil execução e elevado impacto no alvo. Ficam excluídas desta análise as vulnerabilidades que se cingem a um determinado fabricante.

Ao longo do capítulo serão analisadas as vulnerabilidades, partindo dos métodos utilizados pelos atacantes até ao impacto que o ataque surte no alvo.

5.2 Contextualização

O principal objetivo da enumeração de vulnerabilidades é, sem dúvida, a correção ou a implementação de medidas que impeçam a sua exploração. Para que sejam definidas medidas preventivas ou corretivas, é fundamental entender a forma como o ataque é executado e as consequências que este terá no alvo. Em alguns casos, o custo da aplicação das medidas de correção poderá não justificar perante um leve impacto no alvo do ataque.

Ao longo deste relatório todas as vulnerabilidades que serão analisadas foram desenvolvidas em contexto de simulação em ambiente virtual, para tal foi utilizada uma máquina Windows, um *Router PFSense* e uma máquina com a *framework* Kali.

Optou-se por manter a designação das vulnerabilidades em inglês, para facilitar a identificação junto de outras fontes de informação.

5.3 Sumário de Vulnerabilidades

Na Tabela 14 apresenta-se um resumo com as 18 vulnerabilidades detalhadas ao longo deste capítulo. Esta tabela será completada ao longo do relatório, conforme forem analisados os assuntos que irão compor a tabela final de análise de vulnerabilidades. As vulnerabilidades foram divididas em 4 categorias, estando esta divisão associada a diferentes funcionalidades que incorporam o IPv6.

Manipulação de extensões de cabeçalhos	V1	Covert Channel on Hop-by-Hop and Destination Options
	V2	Router Alert DoS Attack in Hop-by-Hop Options Header
	V3	Firewall Evasion with Fragment Header
	V4	Cabeçalhos Desconhecidos
Ataques baseados no ICMPv6	V5	Router Advertisement Spoofing
	V6	Router Advertisement Flooding
	V7	Neighbor Solicitation Flooding
	V8	Neighbor Solicitation Spoofing
	V9	Duplicate Address Detection
	V10	Redirect Spoofing
	V11	Broadcast amplification attacks (smurf)
	V12	Secure Neighbor Discovery (SEND) Flooding
DHCPv6	V13	DHCP Starvation
	V14	Rogue DHCPv6 Server
Outro tipo de ataques	V15[(a)]	Reconnaissance
	V16[(a)]	Privacy unfriendly Stateless Address Autoconfiguration
	V17	Unsupported and unsafety IPv6 features
	V18	Neighbor Discovery table exhaustion

Tabela 14 – Resumo das Vulnerabilidades

(a) Estas vulnerabilidades não se tratam propriamente de ataques, uma vez que as consequências que advêm da sua execução são meramente informativas, podendo o atacante obter o historial de localização do equipamento visado.

De seguida são apresentadas, em detalhe, cada uma das vulnerabilidades, assim como o respetivo processo através do qual é possível explorar a vulnerabilidade.

5.4 Manipulação de Extension Headers

5.4.1 V1 - Covert Channel on Hop-by-Hop and Destination Options Header

Ambas as extensões de cabeçalhos têm estruturas muito similares, no entanto, uma caraterística bastante importante, entre outras, as distingue: o *Hop-by-Hop Options Header* é analisado a cada nó que passa até chegar ao seu destino, ao contrário do que acontece com o *Destination Option Header*, uma vez que este pacote só deverá ser analisado pelo nó ou nós a que se destina a informação [74].

As *firewalls* têm como missão proteger a rede na qual se encontram instaladas, como tal, analisam todos os cabeçalhos que por ela passam, uma vez que estes podem contrariar as normas de segurança impostas pela *firewall*. Já os *routers*, que têm como objetivo o correto encaminhamento da informação, analisam somente o endereço IP de destino e o *Hop-by-Hop Options Header.*

Os *Hop-by-Hop Options Header* podem aparecer apenas uma vez por cada pacote IPv6, mas não existe qualquer limite para o número de opções que cada cabeçalho pode conter [94].

É no campo PadN (utilizado para que os limites do pacote coincidam com um octeto) que pode ser introduzida informação que não pertença ao pacote, criando um canal dissimulado. Desta forma, pode ser propagada informação que não seja pretendida através da normal comunicação, podendo até violar as políticas de segurança da organização.

Esta comunicação permite ainda que se utilize o próprio IPv6 como canal de comunicação, utilizando campos como endereços de IP, mensagens de controlo e erro [92].

Este não é, na sua essência, um problema novo uma vez que, no IPv4 já existiam formas de criar *covert channels*, tais como: *covert timing channel* e *covert storage channel* [7].

Implementação

```
scapy6
dest = ’2001:db8:51e5:30dd:8dac:c860:67f0:91fa’
hbhpkt        =        IPv6(dst=dest,        nh=0)        /IPv6ExtHdrHopByHop(nh=6,
options=[ PadN(optdata=(“ X” *1 50) ) ] ) /TCP(sport=1 080, dport=80) /(“ X” *1 50)
ans, unans=sr(hbhpkt)
```

A ferramenta utilizada para explorar esta vulnerabilidade é o scapyy6.

2001:db8:51e5:30dd:8dac:c860:67fa:91fa -> endereço da máquina alvo do ataque
X -> Valor que irá ser incluído no pacote
50 -> Quantidade de vezes que será repetido o valor a introduzir

Quando o atacante executa o código acima apresentado, o alvo irá receber no PadN a informação lá contida. Neste caso, para efeitos de teste da vulnerabilidade, foram colocados 150 “X”.

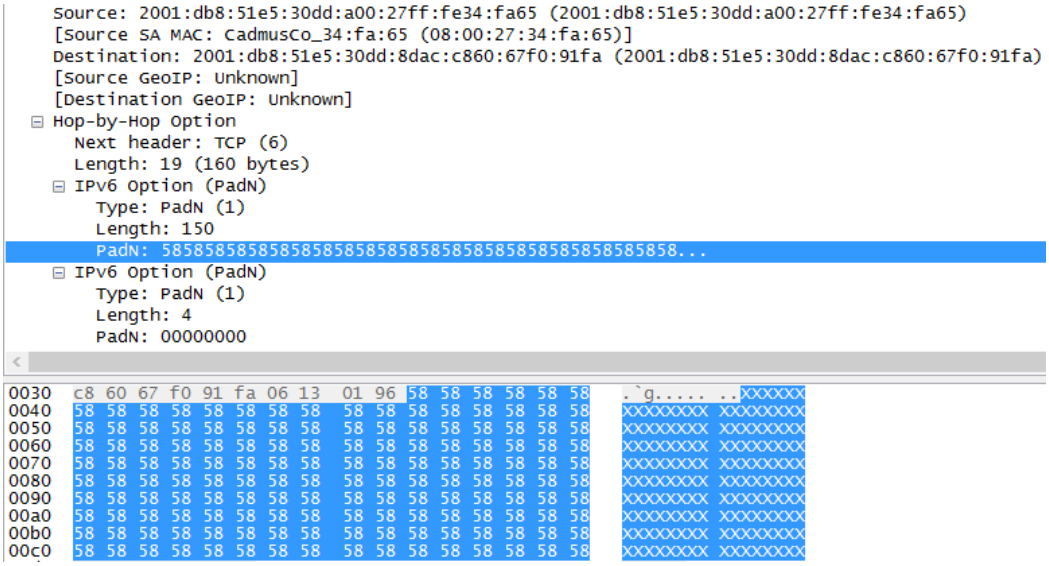

Figura 32 - Valor PadN após Covert Channel

5.4.2 V2 - Router Alert DoS Attack in Hop-by-Hop Options Header

A extensão do cabeçalho pode conter, numa das suas opções, a informação de que aquele pacote deve ser analisado por todos os *routers* por onde passe, colocando o valor 5 no *Option Type* [25].

Com a opção *router alert* ativa um *router* no qual passe o pacote é forçado a capturar o pacote e a analisá-lo. Caso o equipamento não tenha um *hardware* capaz de fazer esta análise num tempo curto, o *router* fica vulnerável a um ataque de *Denial of Service,* caso receba muitos pacotes com a opção ativa [95].

Esta inundação de pacotes com conteúdo falsificado pode acarretar enormes problemas de desempenho para o *router* [7].

Implementação

O scapy6 é também utilizado para explorar esta vulnerabilidade, desta vez criando um pacote rapkt.

```
scapy6
dest = ’2001:db8:51e5:30dd:8dac:c860:67f0:91fa’
rapkt = IPv6(dst=dest, nh=60) /IPv6ExtHdrDestOpt(nh=6, options=[ RouterAlert()
])/TCP(sport=1080, dport=80)
ans, unans=sr(rapkt, timeout=2)
```

2001:db8:51e5:30dd:8dac:c860:67fa:91fa -> endereço da máquina alvo do ataque

Como pode ser comprovado pela Figura 33 o valor do *Router Alert* chega ativo ao destinatário do ataque.

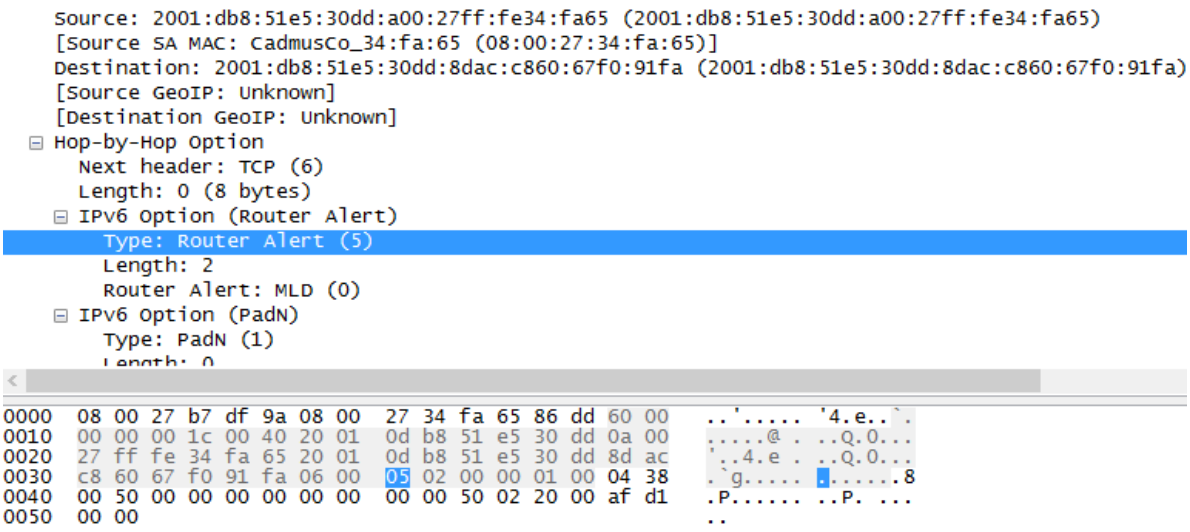

Figura 33 - Impacto do Router Alert DoS Attack

5.4.3 V3 - Firewall Evasion com Fragment Header

No IPv6 a fragmentação pode ser feita exclusivamente pelo nó de origem [33], não sendo possível a nós intermédios, tais como a *firewall*. O facto de esta operação só ser permitida aos nós de origem permite um incremente significativo no desempenho da transmissão de dados.

No IPv6, o MTU mínimo são 1280 bytes, excetuando o último fragmento que poderá ser menor, tendo a *flag* M (*more fragments*) desativada (= 0) [7]. Por norma, fragmentos muito pequenos tornam-se suspeitos, principalmente se forem em grande número.

O uso da fragmentação é comum entre os atacantes que tentam, com base na segmentação de pacotes, ultrapassar limitações impostas por medidas de segurança, nas *firewalls* [74].

Dependendo do tipo de ataque feito através desta vulnerabilidade, surtem impactos diferentes, tais como:

- *Evasion* – Quando o IDS rejeita o pacote, mas este é aceite no destinatário;
- *Insertion* – O IDS aprova o conteúdo, mas o destinatário rejeita-o [96];
- *Overlapping fragments* – Poderá causar DoS durante o processo de assemblagem dos fragmentos;
- Tiny fragmentation – Muitos pacotes muito pequenos, é sinal de ataque;
- Disordered arrival of fragments – Esta técnica usa-se com o objetivo de, devido ao facto dos pacotes estarem desordenados, que estes não sejam inspecionados de forma minuciosa [26].

Implementação

```
scapy6
ragpkt = IPv6(dst=dest, nh=44) /IPv6ExtHdrFragment(nh=6, offset=1 00, id=2,
m=1)/TCP(sport=1080, dport=80, flags="S")/Raw(load=("X"*150))
ans, unans=sr(fragpkt)
```

X -> Informação a introduzir no pacote

150 -> Número de vezes que a informação se irá repetir

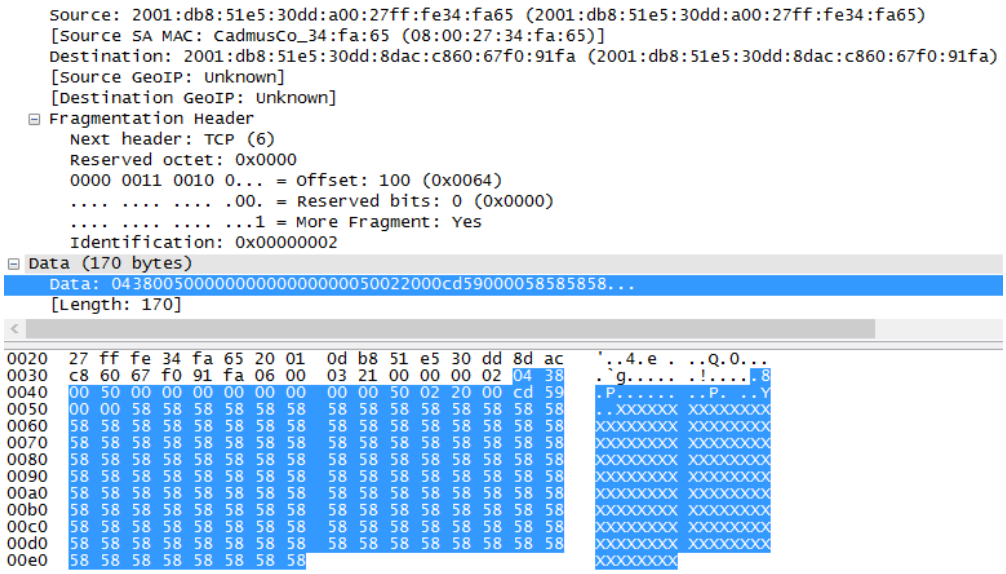

Figura 34 - Inspeção de pacote alterado através do F*ragment Header*

5.4.4 V4 - Cabeçalhos Desconhecidos

Todos os equipamentos devem descartar todos os cabeçalhos que sejam desconhecidos, respondendo ao emissor do pacote com um ICMPv6, com o código 1 "unrecognized next header type encountered". O problema surge quando alguns dispositivos, numa determinada rede ignoram as extensões de cabeçalhos, podendo assim retransmitir pacotes com erros ou propositadamente alterados [74].

Implementação

Através da alteração de um qualquer pacote pode ser simulada a utilização de um cabeçalho não existente.

5.5 Ataques baseados no ICMPv6

Numa determinada rede, um *router* deve ser capaz de receber *Router Solicitation* e enviar um *Router Advertisement*, assim como cada interface de um nó deve ser capaz de receber *Neighbor Solicitation* e de enviar *Neighbor Advertisement*. Estes quatro tipos de mensagens são fundamentais numa rede, no entanto, o seu encaminhamento para fora da rede deve ser

devidamente bloqueado. Existem outros tipos de mensagens, também no âmbito ICMPv6, que devem ser propagadas para fora da rede, nomeadamente *destination unreachable, packet to big, time exceeded* e *parameter problem*. Todas estas mensagens são absolutamente necessárias para o correto funcionamento do *Internet Protocol* versão 6 [7].

No entanto, o IPv6 apresenta vulnerabilidades muito semelhantes ao ARP em IPv4. Existem, na versão 6, técnicas que permitem mitigar algumas vulnerabilidades, no entanto, muito menos testadas e conhecidas, tais como a implementação de ACLs estáticas que permitam que determinada informação só seja aceite se for proveniente das portas indicadas [97].

5.5.1 V5 - Router Advertisement Spoofing

Router Advertisement (RA) é uma mensagem que pertence ao protocolo ICMPv6, que tem como objetivo informar todos os nós que se encontrem ligados a uma determinada rede, que aquele *router* se encontra na rede.

<table>
<tr><td colspan="2">Type (8 bits)</td><td colspan="3">Code (8 bits)</td><td colspan="2">Checksum (16 bits)</td></tr>
<tr><td colspan="2">Cur Hop Limit (8 bits)</td><td>M bit</td><td>O bit</td><td>Reserved (6 bits)</td><td colspan="2">Router Lifetime (16 bits)</td></tr>
<tr><td colspan="7">Reachable Time (32 bits)</td></tr>
<tr><td colspan="7">Retrans Timer (32 bits)</td></tr>
<tr><td colspan="7">Options (tamanho variavel)</td></tr>
</table>

Figura 35 - Estrutura do *Router Advertisement*

Neste caso, o atacante tem que estar ligado dentro da rede, podendo fazer-se passar por um *router*; para isso basta enviar um *RA* falsificado para o endereço *multicast* dos *all-nodes*, indicando que aquele "*router*" poderá ser utilizado para encaminhar os pedidos de qualquer nó da rede. O atacante, através de um equipamento, ou mesmo através de ferramentas criadas para o efeito envia, periodicamente, RAs para o endereço *all-nodes*. Desta forma, o tráfego quando sai do nó vai seguir para o seu *router* "preferido", assim o atacante tem o poder de fazer o que pretender com a informação, pode [7]:

a) Não definir uma rota para o exterior, ficando assim todos os equipamentos que usarem este *router* como *default*, impedidos de ter acesso externo. O atacante tem acesso à informação que o nó dentro da rede solicitou, conforme se encontra descrito na Figura 36;

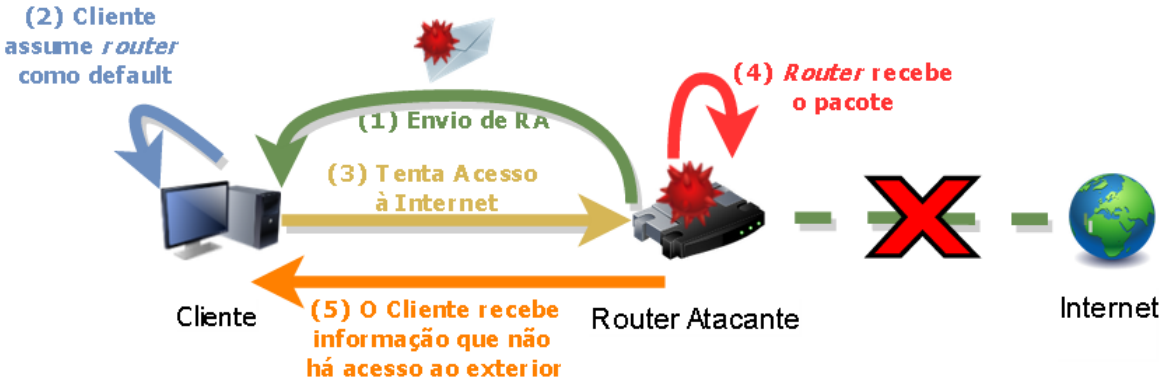

Figura 36 - Router Advertisement DoS

b) Pode definir uma rota para o exterior. Redireciona o pacote para o endereço destino definido, originalmente, pelo nó de origem, passando assim a informação pelo atacante e sendo entregue ao destino. Neste caso, o atacante tem acesso à informação que o nó dentro da rede solícita, mas também tem acesso à resposta que vem do exterior. Como é possível constatar na Figura 37;

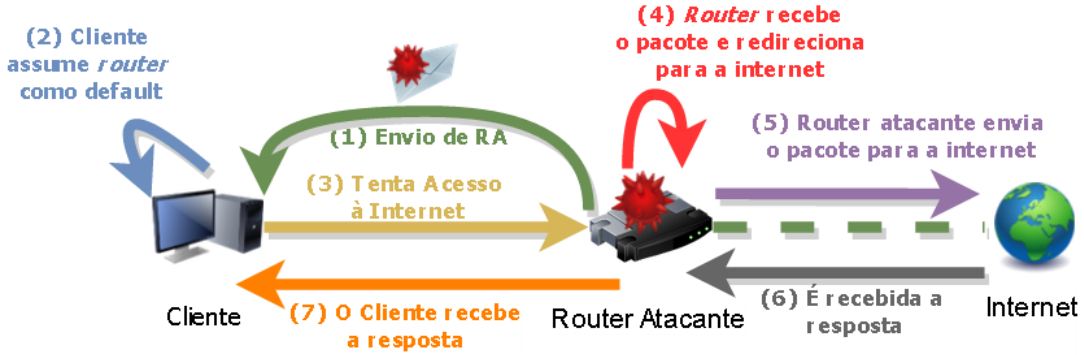

Figura 37 - Router Advertisement Man-in-the-Middle

c) Pode ainda ser executado um outro tipo de ataque, no qual os RAs são enviados com o *lifetime* com o valor 0, mas com o endereço do *router* "verdadeiro". Logo que os clientes recebam esta informação, irão descartar a rota definida para esse *router*, uma vez que a informação que lhes chega, indica que o router deixou de existir [98].

Implementação a) ou b)

```
Scapy6
q=IPv6()/ICMPv6ND_RA()/ICMPv6NDOptPrefixInfo(prefix=bad:bad:bad::',prefixlen=64)
/ICMPv6NDOptSrcLLAddr(lladdr='00:00:65:23:12:00')
ans, unans=sr(q)
```

bad:bad:bad:: -> Prefixo a atribuir

64 -> Número de *bits* do prefixo

00:00:65:23:12:00-> Endereço MAC do *router* "criado" pelo atacante

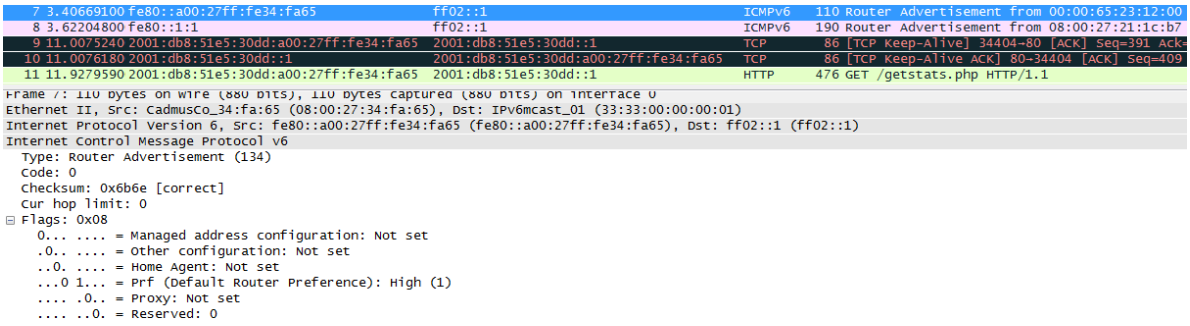

Figura 38 - Resultado RA Spoofing

```
Windows IP Configuration
Ethernet adapter Ethernet:
   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . . . . : 2001:db8:51e5:30dd:8dac:c860:67f0:91fa
   Temporary IPv6 Address. . . . . . . . . :
2001:db8:51e5:30dd:5966:a68a:e9f1:4454
   Link-local IPv6 Address . . . . . . . . : fe80::8dac:c860:67f0:91fa%3
```

5.5.2 V6 - Router Advertisement Flooding

O envio sucessivo de RAs com informação de um novo prefixo (enviado através do campo *options* do pacote de RA) pode causar problemas de desempenho nos equipamentos alvo do ataque. Ao receber a informação de um novo prefixo atribuído pelo *router* da rede, um nó tem de alterar o seu endereço de IP uma vez que, como descrito na secção 2.9.1 o IP é, em parte, constituído pelo prefixo enviado pelo *router*. Com base na informação recebida insere também informação relativa ao encaminhamento de pacotes.

A exploração desta vulnerabilidade pode resultar numa negação de serviço, *DoS.*

O impacto deste ataque depende do Sistema Operativo que estiver a ser usado pelo computador alvo do ataque. Num equipamento com o Sistema Operativo Windows (2003 Server, 2008 Server, XP, Vista e 7 [99]) a consequência deste ataque é uma ocupação de 100% do CPU, e mesmo que o atacante pare de enviar RA, o computador não consegue voltar ao seu normal funcionamento. Já em sistemas operativos Unix, o impacto do ataque, quando interrompido pelo atacante é diferente, a ocupação do CPU decresce de imediato, uma vez que em sistemas Unix só são criados um número limite de IPs. Desta forma, o equipamento Unix insere também na sua tabela de encaminhamento a informação de *routing*, mas não altera o seu IP (mais do que o limite previamente configurado, por *default* 16) [7].

Implementação

```
fake_advertise6      eth0      2001:db8:51e5:30dd:8dac:c860:67f0:91fa      ff02::1
00:11:22:33:44:55
```

eth0 -> Interface local pela qual seguirá o ataque
2001:db8:51e5:30dd:8dac:c860:67f0:91fa -> Endereço da máquina alvo
ff02::100:11:22:33:44:55-> Endereço fictício

```
 4 0.91349800 2001:db8:51e5:30dd:8dac:c860:67f0:91fa ff02::1                ICMPv6    86 Neighbor Advertisement 2001:db8:5
 5 0.91349900 2001:db8:51e5:30dd:8dac:c860:67f0:91fa ff02::1                ICMPv6    86 Neighbor Advertisement 2001:db8:5
Frame 4: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
Ethernet II, Src: Cimsys_33:44:55 (00:11:22:33:44:55), Dst: IPv6mcast_01 (33:33:00:00:00:01)
Internet Protocol Version 6, Src: 2001:db8:51e5:30dd:8dac:c860:67f0:91fa (2001:db8:51e5:30dd:8dac:c860:67f0:91fa), Dst: ff02::1 (ff02::1)
Internet Control Message Protocol v6
  Type: Neighbor Advertisement (136)
  Code: 0
  Checksum: 0xef1e [correct]
⊟ Flags: 0x20000000
    0... .... .... .... .... .... .... .... = Router: Not set
    .0.. .... .... .... .... .... .... .... = Solicited: Not set
    ..1. .... .... .... .... .... .... .... = Override: Set
    ...0 0000 0000 0000 0000 0000 0000 0000 = Reserved: 0
  Target Address: 2001:db8:51e5:30dd:8dac:c860:67f0:91fa (2001:db8:51e5:30dd:8dac:c860:67f0:91fa)
⊟ ICMPv6 Option (Target link-layer address : 00:11:22:33:44:55)
    Type: Target link-layer address (2)
    Length: 1 (8 bytes)
    Link-layer address: Cimsys_33:44:55 (00:11:22:33:44:55)
```

Figura 39 - Surgem diversos pacotes iguais com vista a colocar o CPU em *overload*

Muito habitualmente uma máquina Windows que esteja a ser alvo de um ataque deste género poderá apresentar os conhecidos "*blue screen*" [100].

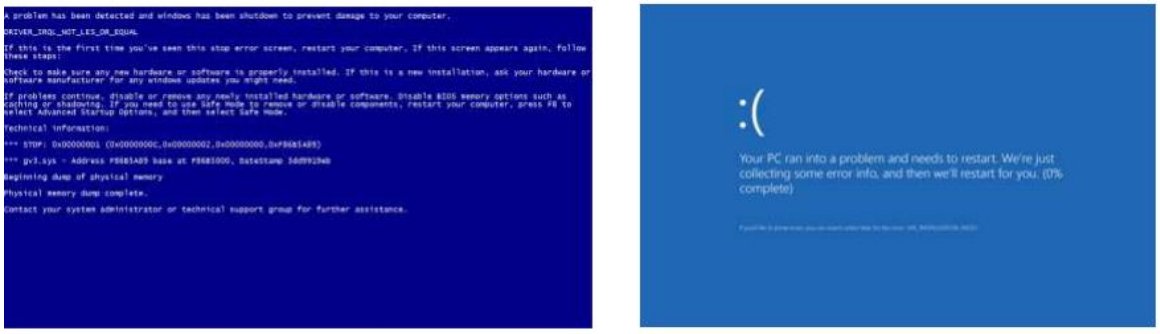

Figura 40 - Impactos em computadores Windows 7 e 8.1

5.5.3 V7 - Neighbor Solicitation Flooding

A inserção de um número elevado de mensagens numa rede não será, certamente, favorável ao desempenho dessa rede. O envio massivo pode comprometer não só o desempenho da rede, bem como dos equipamentos que a ela se encontram ligados.

Implementação

```
flood_solicitate6 eth0
```

eth0 -> Interface local pela qual seguirá o ataque

Neste caso o comando executado irá enviar milhares de *Neighbor Solicitations* para o endereço *multicast all-nodes*, utilizando como emissor das mensagens IPs e MACs aleatórios [7].

```
5.95885300 fe80::218:11ff:fe67:3c39  ff02::1            ICMPv6    86 Neighbor Solicitation for fe80::218:1eff:fe9e:6545
5.95885300 fe80::218:cbff:fedb:a359  ff02::1            ICMPv6    86 Neighbor Solicitation for fe80::218:11ff:fe67:3c39
5.95885400 fe80::218:b9ff:fea5:61fc  ff02::1            ICMPv6    86 Neighbor Solicitation for fe80::218:cbff:fedb:a359
5.95885400 fe80::218:58ff:fea9:2ab5  ff02::1            ICMPv6    86 Neighbor Solicitation for fe80::218:b9ff:fea5:61fc
5.95885500 fe80::218:6bff:fe3c:3f77  ff02::1            ICMPv6    86 Neighbor Solicitation for fe80::218:58ff:fea9:2ab5
5.95885500 fe80::218:57ff:fe0a:be07  ff02::1            ICMPv6    86 Neighbor Solicitation for fe80::218:6bff:fe3c:3f77
5.95885500 fe80::218:21ff:fe55:263f  ff02::1            ICMPv6    86 Neighbor Solicitation for fe80::218:57ff:fe0a:be07
5.95885500 fe80::218:f3ff:fe8c:8504  ff02::1            ICMPv6    86 Neighbor Solicitation for fe80::218:21ff:fe55:263f
5.95885600 fe80::218:f3ff:fec1:3dbe  ff02::1            ICMPv6    86 Neighbor Solicitation for fe80::218:f3ff:fe8c:8504
5.95885600 fe80::218:9cff:fee1:1756  ff02::1            ICMPv6    86 Neighbor Solicitation for fe80::218:f3ff:fec1:3dbe
5.95885600 fe80::218:86ff:fe78:52de  ff02::1            ICMPv6    86 Neighbor Solicitation for fe80::218:9cff:fee1:1756
5.95885700 fe80::218:21ff:fe7c:948c  ff02::1            ICMPv6    86 Neighbor Solicitation for fe80::218:86ff:fe78:52de
5.95885800 fe80::218:b9ff:fed3:310   ff02::1            ICMPv6    86 Neighbor Solicitation for fe80::218:21ff:fe7c:948c
5.95886200 fe80::218:ddff:fec1:18fe  ff02::1            ICMPv6    86 Neighbor Solicitation for fe80::218:b9ff:fed3:310
5.95886300 fe80::218:16ff:fe3e:3d09  ff02::1            ICMPv6    86 Neighbor Solicitation for fe80::218:ddff:fec1:18fe
5.95886300 fe80::218:caff:fec2:ebd   ff02::1            ICMPv6    86 Neighbor Solicitation for fe80::218:16ff:fe3e:3d09
```

Figura 41 – Resultado do Neighbor Solicitation Flooding

```
[zone: pf states] PF states limit reached
```

Figura 42 - Mensagem do GW

5.5.4 V8 - Neighbor Solicitation Spoofing

O tipo de mensagens *Neighbor Solicitation* é enviado em três cenários: (1) quando o nó de origem pretende saber qual é o endereço MAC de um determinado endereço IP; (2) quando um vizinho se encontra em *cache* com o estado a "*probe*"; (3) e quando valida a existência de um IP igual ao que se candidata a adquirir, durante o processo de SLAAC.

(1) Neste caso o nó que emite o pedido com o endereço de IP, do qual pretende obter o endereço MAC, envia o NS para o endereço multicast *solicited-node* [23], uma vez que se fosse enviada para o *all-nodes* seria, automaticamente, descartada segundo RFC 4861 [47];

(2) Cada nó guarda, em memória própria, informação relativa aos seus vizinhos, no entanto, este tipo de registos tem, a fim de permitir o controlo da sua validade, um estado. O processo de confirmação da existência de nó que se encontra na lista de outro é despoletado com um *Neighbor Solicitation*;

(3) Num processo de verificação da existência de IPs iguais, esta é também uma mensagem utilizada durante o processo.

Um atacante infiltrado na rede pode gerar, com o apoio de ferramentas, uma quantidade megalómana de mensagens e com isso provocar uma elevada carga nos processadores dos nós que se encontram na rede, o que pode levar a um ataque de DoS.

No entanto, caso o NS seja dirigido a um endereço *unicast*, o nó destino ao processá-lo vai, caso ainda não exista, criar uma nova entrada na sua tabela de vizinhos [47].

Implementação

```
fake_solicitate6 eth0 2001:db8:51e5:30dd:8dac:c860:67f0:91fa
```

eth0 -> Interface local pela qual seguirá o ataque
2001:db8:51e5:30dd:8dac:c860:67f0:91fa -> Endereço da máquina alvo

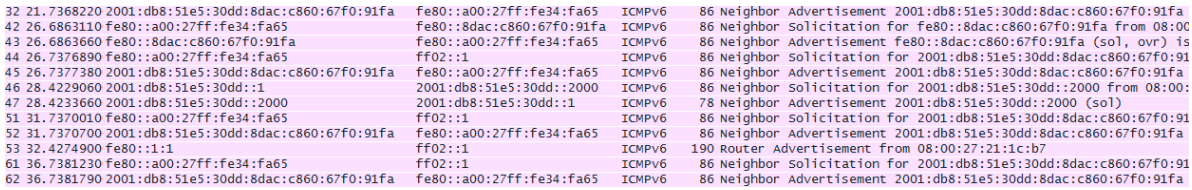

Figura 43 – Adulteração do Neighbor Solicitation

5.5.5 V9 - Duplicate Address Detection

Quando se utiliza configuração de IPs através do SLAAC, é indispensável que um novo nó, a fim de validar o endereço que gerou, envie um *Neighbor Solicitation* para saber se já alguém está a utilizar o IP pretendido. Este processo pode ser utilizado com vista a negar o acesso à rede deste novo nó [101].

Num processo de DAD, o nó que se submete ao processo de aprovação do novo endereço necessita de enviar para toda a rede um *Neighbor Solicitation*, a fim de apurar se já existe naquela rede algum nó com o endereço IP, para que os endereços não se repitam. A responder a estes *Neighbor Solicitation* pode estar um atacante, que se faz passar por um nó que detém o endereço pretendido pelo novo nó, para isso envia um *Neighbor Advertisement* informando que o IP já está a ser usado. Repetindo esta ação para cada pedido da nova máquina, resulta numa negação de serviço, uma vez que a máquina se vê impedida de ter o seu endereço IP validado, não podendo assim fazer o *join* à rede [98].

Implementação

```
fake_advertise6 eth0 2001:db8:51e5:30dd:8dac:c860:67f0:91fa
```

eth0 -> Interface local pela qual seguirá o ataque
2001:db8:51e5:30dd:8dac:c860:67f0:91fa -> Endereço da máquina alvo

Figura 44 - Gateway recebe a resposta de IP já em utilização

5.5.6 V10 - Redirect Spoofing

A mensagem *redirect* foi introduzida no ICMPv6 com o objetivo de um *router* poder informar nós IPv6 que estes podem/devem alterar as suas rotas, em virtude, de existir um caminho melhor para chegar a um determinado destino.

A indicação dada pelo atacante indicará que o melhor caminho passará por um *router* que será controlado pelo atacante, possibilitando assim que tenha acesso a toda a informação e que decida se pretende provocar um DoS, não permitindo que o tráfego vá para o exterior, ou simplesmente inspecionar toda a informação, provocando assim um ataque de *man-in-the-middle* [7].

Implementação

```
redir6     eth0     2001:db8:51e5:30dd:8dac:c860:67fa:91fa     cafe:deca:cace:0162
2001:db8:51e5:30dd::1 2001:db8:51e5:30dd:a00:27ff:fe34:fa65
```

eth0 ->interface com a qual comunica a máquina do atacante
2001:db8:51e5:30dd:8dac:c860:67fa:91fa -> endereço da máquina alvo do ataque
cafe:deca:cace:0162 -> endereço para o qual a rota irá ser alterada
2001:db8:51e5:30dd::1 -> endereço do *router* por omissão
2001:db8:51e5:30dd:a00:27ff:fe34:fa65 -> endereço do *router* atacante

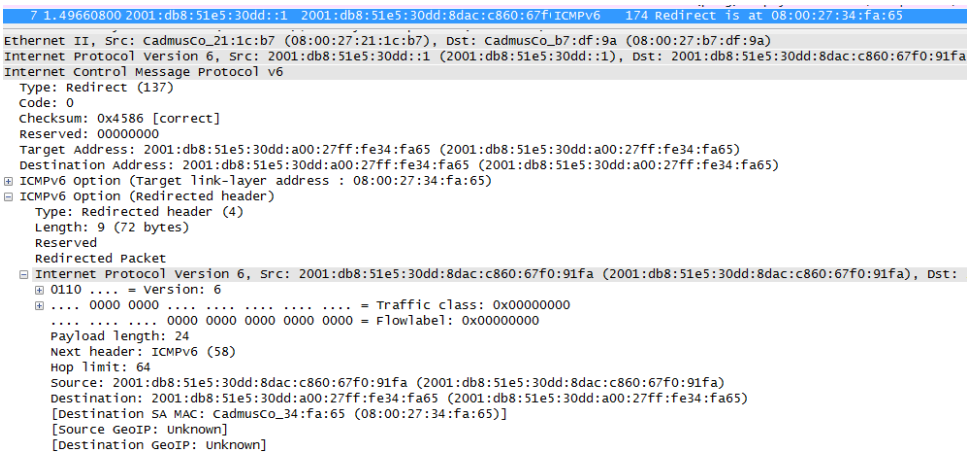

Figura 45 - Resultado de um Redirect Spoofing

5.5.7 V11 - Broadcast amplification attacks (smurf)

Este tipo de ataque tem origem na troca de pacotes ICMP. Consiste na emissão de pacotes do tipo E*cho Request* que são enviados para endereços *multicast*, no entanto, é no endereço do remetente do pacote que é possível alterar o pacote, substituindo o endereço de origem correto, por um outro endereço, de um determinado nó. Desta forma, o que irá acontecer é que todos os *hosts* que pertencerem ao grupo do *multicast* irão responder ao *Echo Request*¸*com um* Reply, enchendo o nó "atacado" de respostas, o que pode provocar, para além de um grande constrangimento na rede, a impossibilidade de comunicação por parte do nó atacado [92] [102].

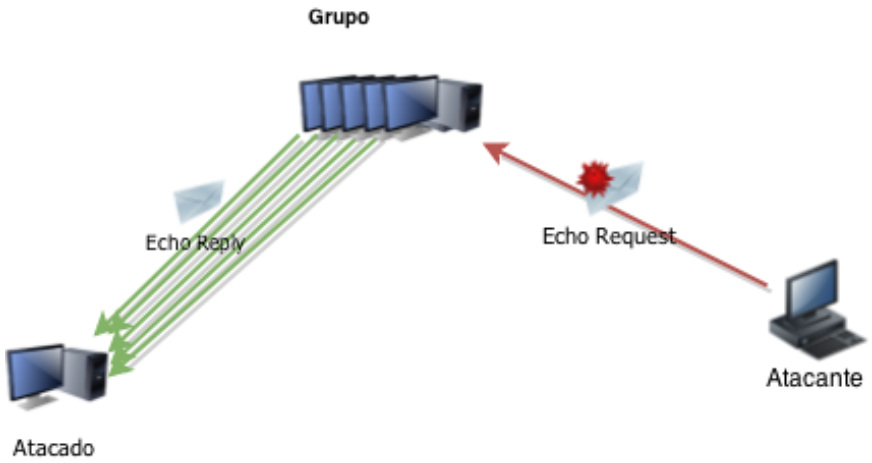

Figura 46 - Exemplo de um cenário de ataque

Implementação

```
smurf6 eth0 2001:db8:51e5:30dd:8dac:c860:67f0:91fa
```

2001:db8:51e5:30dd:8dac:c860:67f0:91fa -> Endereço da máquina alvo

A imagem abaixo surge após o término do ataque, uma vez que enquanto o ataque dura, a máquina fica completamente inutilizável [7].

```
1300 0.09753700 2001:db8:51e5:30dd:8da ff02::1                ICMPv6    78 Echo (ping) request id=0xface, seq=47806, hop limit=255
1301 0.09753700 2001:db8:51e5:30dd:8da ff02::1                ICMPv6    78 Echo (ping) request id=0xface, seq=47806, hop limit=255
1302 0.09753800 2001:db8:51e5:30dd:8da ff02::1                ICMPv6    78 Echo (ping) request id=0xface, seq=47806, hop limit=255
1303 0.09753800 2001:db8:51e5:30dd:8da ff02::1                ICMPv6    78 Echo (ping) request id=0xface, seq=47806, hop limit=255
1304 0.09753800 2001:db8:51e5:30dd:8da ff02::1                ICMPv6    78 Echo (ping) request id=0xface, seq=47806, hop limit=255
1305 0.09753900 2001:db8:51e5:30dd:8da ff02::1                ICMPv6    78 Echo (ping) request id=0xface, seq=47806, hop limit=255
1306 0.09753900 2001:db8:51e5:30dd:8da ff02::1                ICMPv6    78 Echo (ping) request id=0xface, seq=47806, hop limit=255
1307 0.09753900 2001:db8:51e5:30dd:8da ff02::1                ICMPv6    78 Echo (ping) request id=0xface, seq=47806, hop limit=255
1308 0.09754000 2001:db8:51e5:30dd:8da ff02::1                ICMPv6    78 Echo (ping) request id=0xface, seq=47806, hop limit=255
1309 0.09754000 2001:db8:51e5:30dd:8da ff02::1                ICMPv6    78 Echo (ping) request id=0xface, seq=47806, hop limit=255
1310 0.09754000 2001:db8:51e5:30dd:8da ff02::1                ICMPv6    78 Echo (ping) request id=0xface, seq=47806, hop limit=255
```

Figura 47 - Pacotes que a máquina alvo recebe

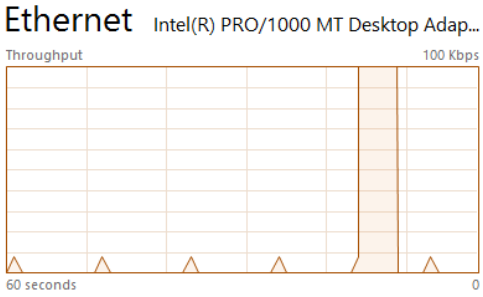

Figura 48 - Estado da interface de rede durante o ataque

5.5.8 V12 – Secure Neighbor Discovery (SEND) Flooding

O SEND, como já analisado anteriormente, utiliza *Cryptographically Generated Addresses* (CGA), que é um identificador da interface encriptado com a chave privada da própria interface. Desta forma, um atacante não pode usar CGAs já existentes, mas poderá criá-las. Esta criação massiva de CGAs irá levar a que o computador alvo use, de forma intensiva, o CPU na tentativa de decifrar o CGA, podendo levar a um DoS.

Implementação

```
sendpees6 eth0 1024 dead:: 2001:db8:51e5:30dd:8dac:c860:67f0:91fa
```

eth0 -> Interface local pela qual seguirá o ataque
1024 -> Tamanho da chave
dead:: -> Prefixo
2001:db8:51e5:30dd:8dac:c860:67f0:91fa -> Endereço da máquina alvo

```
    1 0.00000000 dead::1862:d8f3:a1f 2001:db8:51e5:30dd ICMPv6    454 Neighbor Solicitation for 2001:db8:51e5:30dd:8dac:c860
    2 0.00000100 dead::1862:d8f3:a1f 2001:db8:51e5:30dd ICMPv6    454 Neighbor Solicitation for 2001:db8:51e5:30dd:8dac:c860
    3 0.00000100 dead::1862:d8f3:a1f 2001:db8:51e5:30dd ICMPv6    454 Neighbor Solicitation for 2001:db8:51e5:30dd:8dac:c860
5456 13.3536220 dead::1862:d8f3:a1f 2001:db8:51e5:30dd ICMPv6    454 Neighbor Solicitation for 2001:db8:51e5:30dd:8dac:c860
5457 13.3536220 dead::1862:d8f3:a1f 2001:db8:51e5:30dd ICMPv6    454 Neighbor Solicitation for 2001:db8:51e5:30dd:8dac:c860
5458 13.3536230 dead::1862:d8f3:a1f 2001:db8:51e5:30dd ICMPv6    454 Neighbor Solicitation for 2001:db8:51e5:30dd:8dac:c860
```

Figura 49 - Impacto do SEND Flooding

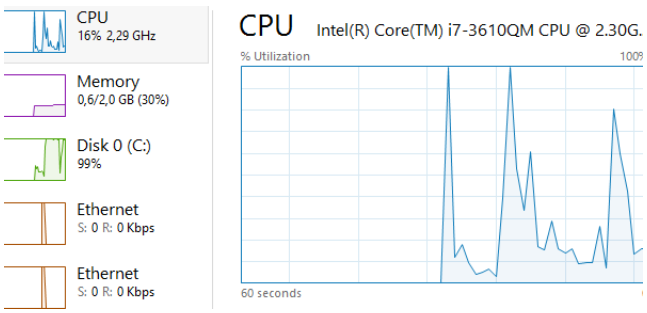

Figura 50 - Impacto no processador e disco

5.6 DHCPv6

De seguida são apresentados dois ataques aos quais uma estrutura que utilize DHCPv6 fica vulnerável [103].

5.6.1 V13 - Starvation

Semelhante ao DHCPv4, um atacante poderá proceder à tentativa de "gastar" os endereços de IP disponíveis o que, com o DHCPv6 dir-se-á que é praticamente impossível [104], dado o elevado número de endereços disponíveis.

Por norma, este tipo de ataques só terá sucesso caso o administrador da rede defina pequenos intervalos de endereços disponíveis para atribuir aos clientes. Aliado a cada atribuição de IP, é guardada, no lado servidor, alguma informação relativa ao nó cliente, o que pode levar a um transbordo da memória [7].

Implementação

```
flood_dhcpc6 eth0
```

eth0 -> Interface local pela qual seguirá o ataque

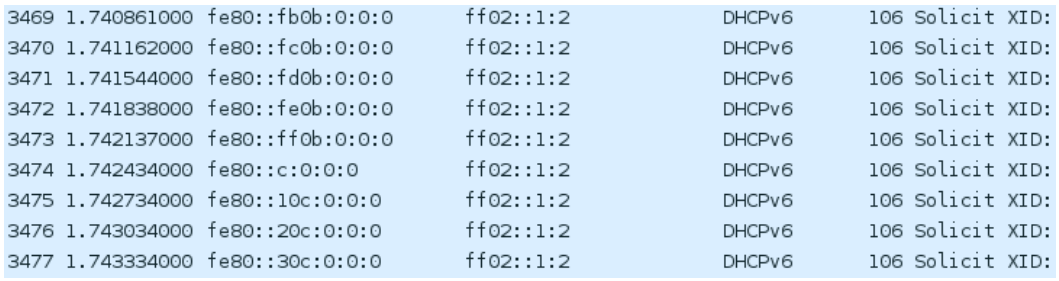

Figura 51 - Solicitação de muitos endereços de IP

5.6.2 V14 - Rogue DHCPv6 Server

Com base no serviço de DHCPv6, um atacante pode ainda fazer-se passar pelo respetivo servidor que atribui os endereços aos seus clientes, [26] subscrevendo o endereço *multicast* ff05::1:2. A partir daqui responderá às mensagens *Solicit* emitidas pelos clientes que pretendem endereços IP, fazendo-se passar por um servidor DHCP legítimo [78].

O atacante atribui as informações que mais lhe convêm, nomeadamente, no que diz respeito aos servidores DNSv6. Aceitando esta atribuição, os pedidos dos clientes passam a ser manipulados pelo atacante, que poderá redirecionar os pedidos para sítios seus, ou limitar o acesso alguns sítios [104].

Implementação

```
fake_dhcpc6 eth0 2001:db8:bad:dddd:8923 2001:db8:dead:daaa:342a
```

eth0 -> Interface local pela qual seguirá o ataque
2001:db8:bad:dddd:8923 -> Endereço falso do Servidor de DHCP
2001:db8:dead:daaa:342a -> Endereço falso do Servidor de DNS

```
Received DHCP6 Solicitate packet from fe80::c85d:ee0b:2d78:a208
Sent DHCP6 Advertise packet to fe80::c85d:ee0b:2d78:a208 (offer: 2001:db8:51e5:30dd:500::)
Received DHCP6 Solicitate packet from fe80::4c1a:6946:4aea:4a46
Sent DHCP6 Advertise packet to fe80::4c1a:6946:4aea:4a46 (offer: 2001:db8:51e5:30dd:600::)
Received DHCP6 Request packet from fe80::c85d:ee0b:2d78:a208
Sent DHCP6 Reply packet to fe80::c85d:ee0b:2d78:a208 (address accepted)
Received DHCP6 Request packet from fe80::4c1a:6946:4aea:4a46
Sent DHCP6 Reply packet to fe80::4c1a:6946:4aea:4a46 (address accepted)
```

Figura 52 - Atacante faz-se passar por servidor DHCP

```
2612 150.9373040( fe80::a00:27ff:fe34:fa65          fe80::c85d:ee0b:2d78:a208          DHCPv6      166
Frame 2612: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits) on interface 0
Ethernet II, Src: CadmusCo_34:fa:65 (08:00:27:34:fa:65), Dst: CadmusCo_aa:53:1f (08:00:27:aa:53:1f)
Internet Protocol Version 6, Src: fe80::a00:27ff:fe34:fa65 (fe80::a00:27ff:fe34:fa65), Dst: fe80::c85d:ee0b:2d78:a208
User Datagram Protocol, Src Port: 37837 (37837), Dst Port: dhcpv6-client (546)
DHCPv6
   Message type: Reply (7)
   Transaction ID: 0x6674b2
 ⊞ Client Identifier
 ⊞ Server Identifier
 ⊞ Identity Association for Non-temporary Address
 ⊟ DNS recursive name server
      Option: DNS recursive name server (23)
      Length: 16
      Value: 20010db851e530dd0a0027fffe34fa65
      DNS server address: 2001:db8:51e5:30dd:a00:27ff:fe34:fa65 (2001:db8:51e5:30dd:a00:27ff:fe34:fa65)
```

Figura 53 - Servidor DNS indicado pelo falso servidor DHCP

5.7 Outros tipos de ataques

5.7.1 V15 - Reconnaissance

Este é o primeiro processo utilizado por um atacante que consiste, tal como o nome indica, num reconhecimento da rede[8], tomando conhecimento de que equipamentos existem na rede. Numa primeira fase o atacante efetua uma análise de quais os *hosts* que se encontram na rede, utilizando um, ou vários, das seguintes possibilidades:

[8] Os atacantes mais cuidadosos fazem este ataque lentamente, para que não possam ser detetados pelos mecanismos de deteção de intrusão da rede alvo (IDS) [74].

- nmap
- Ping
- Whois
- Sobre o DNS (Nslookup, dig, vários pedidos de resolução)
- Traceroute

Estas ferramentas permitem efetuar um levantamento das máquinas existentes. Os ataques de recolha de informação são, muitas vezes, protagonizados tendo como alvo os servidores de DNS, pois estes servidores detêm grande parte de informação relativa à rede [92]. Para os humanos é muito difícil conseguir memorizar um IP da versão 6, portanto os DNS são um forte alvo quando se trata de rastreio da rede, ao contrário do que acontecia com a versão 4, [74].

Na sua maioria, os administradores de rede não valorizam muito os *scans* da rede, no entanto, se forem executados de forma exaustiva, podem provocar um excessivo consumo de largura de banda; ou até um impacto negativo no desempenho dos equipamentos de gestão da rede e serviços.

Este tipo de explorações torna-se bem mais difícil de ser aplicado ao IPv6, uma vez que é disponibilizada, para cada rede, uma enorme gama de endereços.

Implementação

```
nmap -6 -v -Pn 2001:8a0:7d1f:3801:415c:2e80:e6ad:b37

Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2015-06-11 21:50 Hora de Verão de GMT
Initiating System DNS resolution of 1 host. at 21:50
Completed System DNS resolution of 1 host. at 21:50, 0.00s elapsed
Skipping SYN Stealth Scan against AndreRibeiroHP.lan (2001:8a0:7d1f:3801:415c:2e80:e6ad:b37) b
Nmap scan report for AndreRibeiroHP.lan (2001:8a0:7d1f:3801:415c:2e80:e6ad:b37)
Host is up.
PORT      STATE   SERVICE
1/tcp     unknown tcpmux
3/tcp     unknown compressnet
4/tcp     unknown unknown
6/tcp     unknown unknown
7/tcp     unknown echo
9/tcp     unknown discard
13/tcp    unknown daytime
17/tcp    unknown qotd
19/tcp    unknown chargen
20/tcp    unknown ftp-data
21/tcp    unknown ftp
22/tcp    unknown ssh
23/tcp    unknown telnet
24/tcp    unknown priv-mail
25/tcp    unknown smtp
26/tcp    unknown rsftp
30/tcp    unknown unknown
32/tcp    unknown unknown
33/tcp    unknown dsp
37/tcp    unknown time
42/tcp    unknown nameserver
43/tcp    unknown whois
49/tcp    unknown tacacs
53/tcp    unknown domain
```

Figura 54 - Comando NMAP

Os atacantes podem acelerar o processo de descoberta de *hosts*. Sabendo o prefixo da rede [78] e caso consiga descobrir qual a marca e o tipo de placas de rede utilizadas pela organização alvo, consegue descobrir qual o OUI[9], sabe os primeiros 24*bits* do MAC *Address*¸ que caso esteja a ser utilizado EUI-64, é usado na geração do endereço de rede. O atacante reduz assim, significativamente, a gama de IPs a analisar [74].

5.7.2 V16 – Privacy unfriendly Stateless Address Autoconfiguration (SLAAC)

Uma das formas de gerar endereços IPv6 (EUI-64) utilizando o SLAAC recorre ao MAC *address* da interface de rede, para preencher os 64 *bits* menos significativos. Com a utilização do MAC *address* no endereço IPv6 é possível:

- Que qualquer pessoa ligada à internet consiga, através da parte do IP, manter um registo das redes pelas quais aquele equipamento passou;
- É também possível deslindar qual o fabricante da placa de rede utilizada, o que pode comprometer a segurança por uma vulnerabilidade conhecida do fabricante [105].

5.7.3 V17 – Funcionalidades não suportadas ou inseguras do IPv6

Desde as primeiras propostas de desenho do Protocolo IPv6 que foram sugeridas, implementadas, alteradas e removidas muitas funcionalidades do protocolo. Algumas, embora renovadas, fazem parte de implementações anteriores, o que permite que atacantes explorem as ditas fraquezas [105]. Alguns breves exemplos de funcionalidades que foram desativadas mas que ainda são encontradas em alguns sistemas:

- Site Local Address [106];
- Source routing type 0 (RH0) [107];
- DNS: A6 Records [108].

5.7.4 V18 – Neighbor Discovery table exhaustion

À semelhança do ARP, no IPv4, o IPv6 mantém, nos *routers,* uma tabela com a lista dos seus vizinhos. Um atacante pode fazer um *scan* a um muito vasto número de *hosts*, analisando um determinado prefixo. Os *routers* vão tentar adicionar novas entradas à sua *cache* [105].

Este ataque pode ter diferentes impactos [105] :

- O dispositivo perder a capacidade de guardar novos vizinhos;

[9] *Organizational Unique Identifier* (OUI) – Identificador único, para cada fabricante de placas de rede, que faz parte do *MAC Address* da placa.

- Sobre utilização do CPU;
- O equipamento pode mesmo bloquear e ser necessário reiniciá-lo.

```
alive6 –s 80 eht0 2001::0-ffff:0-ffff:0-ffff:0-ffff
```

Implementação

80 -> porto a ser analisado

eth0 -> interface pela qual é feito o ataque

2001::0-ffff:0-ffff:0-ffff:0-ffff -> gama de endereços a analisar

6 Análise de Risco e Classificação de Vulnerabilidades

6.1 Introdução

Não existe perfeição quando se fala de segurança, pelo que é necessário avaliar os problemas que podem comprometer a segurança de um sistema e avaliar as soluções [109].

Quando se fala em ameaças à segurança, torna-se necessário definir mecanismos para permitir diferenciar os tipos de ataques. Esta diferenciação permite que as vulnerabilidades sejam avaliadas, podendo assim ser definida uma lista de prioridades para que possa ser elaborado um plano de intervenção, para resolver ou minimizar as consequências dos ataques.

A análise do impacto ou do risco das vulnerabilidades é fundamental para que se possa definir quais as medidas que podem ser aplicadas para proteger a rede. Deve ser tido em conta a vantagem económica na aplicação de medidas, ou seja, para se aumentar a proteção de um serviço simples, que não é crucial ao funcionamento da empresa, não faz sentido despender uma elevada quantidade de dinheiro, uma vez que caso o ataque surja, a informação perdida não tem praticamente valor, para a entidade atacada.

Neste capítulo serão apresentadas as etapas que devem ser seguidas a fim de se elaborar uma correta análise de risco. Dada a especificidade de cada infraestrutura são apresentados procedimentos que podem ser utilizados para todas as redes. Importa, depois de elaborada a análise de risco, avaliar e compreender as vulnerabilidades a que pode estar exposta a rede da organização em causa. Esta avaliação permitirá identificar os equipamentos ou serviços mais expostos, permitindo que a elaboração da política de segurança da entidade tenha um maior foco nos pontos mais sensíveis da rede de comunicação.

6.2 Análise de risco

Para se poder analisar o risco, convém ter bem presente o seu significado: "Risco é a possibilidade de haver perda ou dano em dados" [109].

A análise de risco não é um processo isolado, nem pode ser limitado no tempo. A análise de risco inicia-se juntamente com o desenho da estrutura da rede e acompanhá-la-á enquanto a rede funcionar. Novas ameaças podem surgir e, como tal, são necessárias novas medidas para as conter que, depois de planeadas, são testadas e consequentemente implementadas.

A análise de risco varia de organização para organização. Os atributos a analisar ou a categorização das vulnerabilidades deverão adaptar-se a cada organização, cumprindo as necessidades de cada infraestrutura.

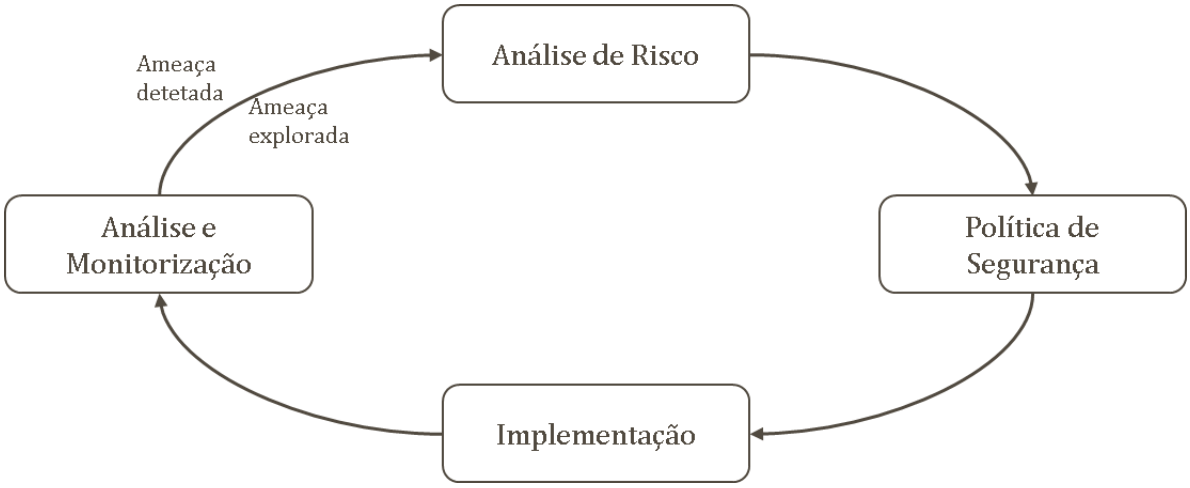

Figura 55 - Processo da Análise de Risco

Na Figura 55 é possível constatar o processo cíclico, no qual se baseia uma análise de risco [109].

Após ser efetuado o levantamento das ameaças a que se encontra sujeita a rede de uma organização, devem ser cuidadosamente definidas quais as políticas de segurança a implementar, para garantir que a exploração das ameaças não resultará em efeitos negativos na rede. Após a implementação das regras de segurança, é necessária uma constante monitorização e testes à infraestrutura, das quais podem resultar a descoberta de novas ameaças, para as quais devem ser definidas novas regras de segurança. Sendo necessário voltar à fase de testes e monitorização, processo este que deverá ser mantido ativo enquanto o sistema existir.

No caso de haver alguma exploração de uma ameaça, esta deve ser avaliada e devem ser definidos os meios que impedem ou reduzem a possibilidade da sua exploração, é implementada e novamente se passa à fase de testes e monitorização.

Para que seja elaborada uma condigna análise de risco é necessário reunir uma diversidade de dados, que são agora enumerados:

a) **Inventariar equipamento, aplicações e dados**
   Para que possa ser efetuado um correto e pormenorizado levantamento das ameaças e vulnerabilidades é necessário conhecer todos os equipamentos, aplicações e dados que fazem parte da organização. Uma vez que, determinada aplicação pode, ao nível da sua implementação, conter alguma ameaça que possa comprometer a restante organização. É fundamental que para cada um destes seja definido um grau de importância, que permita implementar ou não medidas de contenção;
b) **Ameaças e Vulnerabilidades**
   Com base no levantamento previamente realizado e nas mais diversas fontes de informação sobre segurança informática, devem ser enumeradas todas ameaças e vulnerabilidades a que o sistema possa estar sujeito;
c) **Probabilidades**
   Depois de elaborada a lista de ameaças e vulnerabilidades, é fundamental avaliar a probabilidade que cada uma das ameaças de ser explorada por atacantes;
d) **Consequências**
   Para que possam ser aplicadas medidas de recuperação do sistema após um ataque, é muito importante saber qual o impacto que este ataque poderá ter no sistema, que dados ou sistemas poderá afetar;
e) **Recuperação**
   A vulnerabilidade não é o grande problema, o problema consiste sim na sua exploração e nas consequências que podem advir da exploração. Desta forma, e com base nas consequências previamente analisadas, é fundamental definir políticas que permitam a rápida recuperação do sistema, de forma a afetar o mínimo possível o normal funcionamento do sistema;
f) **Medidas de segurança**
   A melhor alternativa para um sistema é reduzir as possibilidades de ser atacado aos valores mais baixos possíveis e é na implementação de medidas de segurança que se devem centrar esforços para evitar que existam ameaças prontas a explorar, pelos atacantes [109].

Serão analisados ao longo deste capítulo os parâmetros que permitem avaliar as vulnerabilidades, de forma a tornar possível a elaboração de uma síntese das vulnerabilidades. Como primeiro passo, serão definidas as categorias nas quais se dividem os ataques com base em informação da literatura. A restante classificação foi baseada na experiência adquirida durante o estudo das vulnerabilidades, utilizando também alguns documentos técnicos para elaborar esta classificação. No fim deste capítulo consta uma tabela resumo com todas as vulnerabilidades apresentadas no Capítulo 5, com a respetiva categorização e classificação.

6.3 Classificação de Vulnerabilidades

No sentido de tornar possível uma sistematização das vulnerabilidades, torna-se fundamental classifica-las no que diz respeito às consequências provocadas pela execução de um ataque numa rede [110].

Para que seja possível uma interpretação mais simplificada de todo o trabalho desenvolvido neste relatório, torna-se imprescindível a classificação das vulnerabilidades quanto à sua dificuldade de execução e quanto ao impacto que este ataque terá no seu alvo.

6.3.1 Método de ataque

Esta classificação pode ser feita em conformidade com as necessidades da entidade em causa. No entanto, na Tabela 15 é apresentada uma possível categorização das vulnerabilidades, que poderá ou não ser utilizada como guia na avaliação das vulnerabilidades [111] [110].

EV	**Eavesdropping**	O atacante monitoriza as comunicações com o objetivo de capturar mensagens e credenciais
MIM	**Man-in-the-Middle**	O atacante interceta um canal de comunicação entre dois nós legítimos
MASQ	**Masquerading "Spoofing"**	O atacante faz-se passar por uma entidade ou nó autorizado
RA	**Routing Attack**	Quando o ataque resulta na manipulação de tabelas de encaminhamento
DOS	**Denial of Service**	O ataque a uma máquina ou serviço, que devido ao elevado número de pedidos faz com que este deixe de responder
MM	**Message Modification**	A mensagem a ser enviada é propositadamente alterada pelo atacante
MR	**Message Replay**	O atacante envia mensagens e responde como se fosse um utilizador legítimo para tal

Tabela 15 - Categorização das Vulnerabilidades

6.3.2 Dificuldade de execução

A dificuldade de execução pode ser analisada tendo em conta dois diferentes pontos de vista, os conhecimentos técnicos requeridos ao atacante e os meios necessários à execução propriamente dita do ataque.

A **Alto –** Quando é requerido ao atacante elevados conhecimentos de programação e do sistema alvo do ataque;

M **Média** – Para a concretização do ataque são necessárias aplicações específicas e conhecimento do sistema alvo do ataque;

B **Baixa** – Com base em aplicações existentes é possível executar um ataque, sem que haja um conhecimento prévio do sistema a atacar.

6.3.3 Técnica utilizada

Para executar um ataque, o atacante pode utilizar diversas técnicas [102], como já analisamos na secção anterior. Procura-se agora resumir as técnicas para facilitar a interpretação da tabela final.

Send O atacante envia o pacote diretamente para o alvo;
Flood O atacante emite uma grande quantidade de informação;
Spoof O atacante cria informação, fazendo-se passar por outro;
Scan O atacante "percorre" uma gama ou todos os endereços;
Assign O atacante faz-se passar pelo alvo;
Listen O atacante está à escuta da informação.

6.3.4 Impacto no alvo do ataque

Como impacto no alvo do ataque vamos considerar a facilidade de deteção do ataque e também a aplicação de medidas corretivas de forma a que o alvo consiga repor a comunicação e a reposição dos dados, caso seja necessário [64].

 Acesso não autorizado a dados;

 Alteração de dados;

 Impedimento de acesso a informação ou serviços;

 Atraso do desempenho da máquina alvo ou da rede;

 Alteração da tabela de *routing.*

6.3.5 Alvo do ataque

Os ataques, independentemente do resultado pretendido, podem ter diversos alvos.

 Computador individual

 Serviços

 Grupo de computadores

 Router/Firewall

 Endereço *multicast*

 Largura de Banda

6.4 Resumo das Vulnerabilidades

Tendo por base as classificações anteriormente apresentadas, a Tabela 16 contempla as vulnerabilidades apresentadas no Capítulo 5, bem como a forma como o ataque é elaborado, a dificuldade de execução do ataque, o impacto que terá no alvo e ainda o tipo de equipamento que é o alvo do ataque.

	Tipo	Método	Dificuldade Execução	Impacto	Alvo
V1 - Covert Channel on Hop-by-Hop and Destination Options Header	MM	Send	M		
V2 - Router Alert DoS Attack in Hop-by-Hop Options Header	MM	Flood	M		
V3 - Firewall Evasion with Fragment Header	MM	Send	B		
V4 - Cabeçalhos Desconhecidos	MASQ	Spoof	A		
V5 - Router Advertisement Spoofing	RA	Spoof	M		
V6 - Router Advertisement Flooding	RA	Flood	M		
V7 - Neighbor Solicitation Flooding	RA	Flood	B		
V8 - Neighbor Solicitation Spoofing	RA	Spoof	M		
V9 - Duplicate Address Detection	RA	Spoof	M		
V10 - Redirect Spoofing	MASQ	Spoof	M		
V11 - Broadcast amplification attacks (smurf)	RA	Flood	M		
V12 - Secure Neighbor Discovery (SEND) Flooding	DOS	Flood	M		
V13 - DHCP Starvation	DOS	Flood	B		
V14 - Rogue DHCPv6 Server	MR	Spoof	M		
V15 - Reconnaissance	MASQ	Scan	B		

	Tipo	Método	Dificuldade Execução	Impacto	Alvo
V16 - Privacy unfriendly Stateless Address Autoconfiguration (SLAAC)			A		
V17 - Unsupported and unsafety IPv6 features	MASQ	Spoof	M		
V18 - Neighbor Discovery table exhaustion	RA	Scan	M		

Tabela 16 - Classificação das Vulnerabilidades

7 Técnicas para Resolução e Boas Práticas

7.1 Introdução

A elaboração da análise de risco tem como objetivo a implementação de medidas que aumentem o grau de segurança e proteção de equipamentos, aplicações e dados. Neste capítulo serão abordadas técnicas a implementar para se diminuir ou erradicar o risco de exposição à ameaça. Será ainda enumerada uma lista de práticas comuns que devem ser tidas em conta pelos administradores de redes das organizações.

A análise de risco permite ao responsável pela rede identificar, de forma mais rigorosa, os problemas mais suscetíveis de ataque, bem como a forma como podem ser resolvidos.

Neste capítulo são apresentadas as propostas de resolução para cada uma das vulnerabilidades apresentadas e detalhadas no Capítulo 5. Será elaborada uma proposta de categorização no que diz respeito à resolução das vulnerabilidades. No fim do capítulo será apresentada uma tabela resumo com o tipo de resolução proposta para cada vulnerabilidade, no sentido de tornar a compreensão das medidas mais sintética.

7.2 Manipulação de Extensões de Cabeçalhos

7.2.1 V1 - Covert Channel no Hop-by-Hop e Destination Options Header

Resolução
Para que se possa evitar a criação de *covert channels* é necessário que se defina se se pretende eliminar ou limitar esta vulnerabilidade, acarretando, cada uma das medidas, as respetivas consequências.

A *firewall* deverá rejeitar:

- PadN que contenham *payload* [92]*;*
- Pacotes que tenham mais de 5 bytes de *padding* [94] [7]*;*
- Pacotes cujo *padding* contenha *bits* que não sejam 0 [7] [112].

7.2.2 V2 - Router Alert DoS Attack in Hop-by-Hop Options Header

Resolução
Com base na RFC 6398 (IP Router Alert Considerations and Usage) [95] não existem atualmente métodos para distinguir pacotes cujo *router alert* seja falsificado, ou não.

Uma implementação que tem vindo a ser adotada é a limitação do número de pacotes ou simplesmente a rejeição dos ditos pacotes [7].

Para tal, num *router* pode recorrer-se à utilização de ACL.

```
ipv6 access-list DenyRA
       deny ipv6 any any dest-option-type 5 log
       permit ipv6 any any
       interface FastEthernet 0/2
```

[74]

7.2.3 V3 - Firewall Evasion com Fragment Header

Resolução
Com o objetivo de resolver o problema criado com os fragmentos, é possível proibir a aceitação de pacotes fragmentados [74].

```
ipv6 access-list DenyFragments
       deny ipv6 any 2001:db8:cafe::/64 fragments
       permit ipv6 any any
       interface FastEthernet 0/2
```

7.2.4 V4 - Cabeçalhos Desconhecidos

Os pacotes que contenham cabeçalhos desconhecidos devem ser automaticamente descartados.

7.3 Ataques baseados no ICMPv6

7.3.1 V5 - Router Advertisement Spoofing

Resolução

Uma definição rigorosa de quais os *routers* confiáveis e a respetiva aceitação, em exclusivo de RA destes *routers* dificultará a tarefa dos atacantes, mas ainda assim este poderá fazer-se passar por um *router* de confiança.

É ainda possível desativar a funcionalidade de *router discovery* passando a distribuição da informação a ser da responsabilidade do servidor DHCPv6, caso este serviço se encontre disponível na rede.

A utilização do IPSec e do SEND são altamente recomendáveis [78].

No entanto, soluções mais elaboradas podem ser aplicadas. Os RA só devem ser aceites nos switches quando vêm da interface que liga o *switch* ao *router*, garantindo assim que só através dessa interface é que poderão ser disseminados *Router Advertisements*. A entrada de RA deve estar impedida em todas as outras portas do equipamento.

Utilização de RA Guard.

RA Guard é uma funcionalidade que permite ao administrador da rede bloquear e rejeitar RAs indesejados. O RA Guard analisa e filtra os pacotes e descarta os que foram emitidos por dispositivos que não foram autorizados. Esta análise baseia-se na comparação da informação de *Layer* 2 com a informação que consta no pacote de RA [113].

`configure terminal`	
`ipv6 nd raguard policy policy-name`	Definir o nome do RA Guard
`device-role {host | router}`	Identificar o tipo de dispositivo
`hop-limit {maximum | minimumlimit}`	Ativa a verificação do campo *hop-limit*
`managed-config-flag {on | off}`	Ativa a verificação da *flag* M
`match ipv6 access-list ipv6-access-list-name`	Valida o prefixo em conformidade com uma acl
`match ra prefix-list ipv6-prefix-list-name`	Valida o prefixo em conformidade com uma lista
`other-config-flag {on | off}`	Ativa a validação de outros parâmetros dos pacotes
`router-preference maximum {high | low | medium}`	Ativa a validação do R*outer Preference* que descarta os RAs com Router Preference superior à escolhida.
`configure terminal`	
`interface type number`	Seleciona a interface pretendida
`show ipv6 nd raguard policy [policy-name]`	Aplica a RA Guard definida anteriormente

[56]

7.3.2 V6 - Router Advertisement Flooding

Resolução
Uma definição rigorosa de quais os *routers* confiáveis e a respetiva aceitação, em exclusivo de RA destes *routers* dificultará a tarefa dos atacantes, mas ainda assim este poderá fazer-se passar por um *router* de confiança.

É ainda possível desativar a funcionalidade de *router discovery*, passando a distribuição da informação a ser responsabilidade do servidor DHCPv6.

A utilização do IPSec e do SEND são altamente recomendáveis [78].

A limitação do número de pacotes é também aconselhável [114].

A utilização de *RA Guard* explicada no ponto anterior permite também a resolução deste problema [113].

7.3.3 V7 - Neighbor Solicitation Flooding

Resolução
A utilização do mecanismo de proteção SEND auxilia a resolução do problema [105].

Utilização do IPSec [78].

A limitação do número de pacotes é também aconselhável [114].

7.3.4 V8 - Neighbor Solicitation Spoofing

Resolução
SEND ajuda a resolver este problema [105].

Utilização do IPSec [78].

7.3.5 V9 - Duplicate Address Detection

Resolução
O SEND soluciona este problema [115]. A combinação com o IPSec praticamente erradica a possibilidade deste ataque [78].

7.3.6 V10 - Redirect Spoofing

Resolução
Uma primeira abordagem a este tipo de tráfego deverá passar por analisar se a mensagem reencaminhada contém o cabeçalho do pacote que é redirecionado. Esta ação previne, mas não erradica a possibilidade do ataque. No entanto, e como esta funcionalidade tem como único objetivo a otimização da rede, esta função poderá, em último caso, ser desativada [78].

A utilização do SEND é uma forma de garantir proteção contra este ataque [7].

7.3.7 V11 - Broadcast amplification attacks (smurf)

Resolução
Não enviar respostas ICMP quando o destinatário do pacote é um endereço *multicast,* para tal, pode-se recorrer à utilização de regras de bloqueio de pacotes na *firewall* [105].

Os atacantes que se encontram numa rede têm que fazer os seus pacotes ser propagados através do *router/firewall*, por norma, estes equipamentos só validam os endereços de destino. No entanto, se o endereço de origem for também analisado permite que só sejam aceites pacotes da sub-rede que se encontra ligada ao *router*, bloqueado e descartando quem não pertence a essa sub-rede [64].

7.3.8 V12 – Secure Neighbor Discovery (SEND) Flooding

Resolução
Em sistemas com pouca capacidade de computação o SEND deve ser desativado, no entanto, terá que haver uma decisão entre o compromisso de ficar exposto a SEND *flooding* ou a Neighbor/Router Discovery (*Solicitation/Advertisement*) *flooding* [105].

7.4 DHCPv6

7.4.1 V13 - Starvation

Resolução

A utilização do *Port Security* permite limitar o número de *leases* DHCP que atravessam cada porta, num *switch.* No entanto, no caso de uma rede sem fios, esta opção não é válida uma vez que não é possível controlar quantos clientes se poderão ligar à rede [116] [117].

```
switchport port-security
switchport port-security maximum 1
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

No entanto, existe uma outra alternativa, o DHCP snooping, que em vez de necessitar de configuração porta a porta, define simplesmente quais as portas que permitem a entrada de pacotes de DHCP [116].

`enable`	
`configure terminal`	
`ip dhcp snooping`	Ativar a funcionalidade
`ip dhcp snooping vlan 1`	Definir qual para qual *vlan* a funcionalidade deverá atuar
`interface FastEthernet 0/2`	Escolher a porta na qual se pretende confiar
`ip dhcp snooping trust`	
`ip dhcp snooping limit rate 25`	Limita o número de pacotes de portas sem serem de confiança (*trust)*. O limite é expresso em pacotes por segundo

7.4.2 V14 - Rogue DHCPv6 Server

Resolução

Uma das medidas que pode ser determinante para o decréscimo de possíveis ataques através do servidor e serviço DHCP é a utilização da opção de autenticação no DHCP. O mecanismo *Delayed Authentication Protocol* utiliza a *Hash-based Message Authentication Code (HMAC)* para garantir a autenticidade e integridade das mensagens [78]. Com recurso a uma chave simétrica [97] este mecanismo permite identificar o emissor da mensagem e confirmar que esta não foi adulterada [52]. Nenhuma mensagem DHCP deve conter mais do que uma opção de autenticação [52]. Importa notar que a autenticação em DHCP requer custos associados à gestão de chaves e à sua respetiva distribuição, pelo que não é utilizada na maior parte dos cenários [97].

Pode também ser tido em atenção o DUID que é enviado pelo cliente quando envia a mensagem de *Solicit* para o servidor, uma vez que é único, independentemente da sub-rede ou da rede onde se encontra o equipamento. No entanto, permite que haja a possibilidade de um atacante manter o *tracking* da *interface* [78].

7.5 Outros tipos de ataques

7.5.1 V15 - Reconnaissance

Resolução

No que diz respeito a este tipo de prática não existe uma solução propriamente dita, até porque não se trata de um ataque no seu sentido mais literal. No entanto, podem ser definidas algumas medidas que podem dissuadir os atacantes de executarem este tipo de análises.

- Deve ser evitado o uso do SLAAC, no caso de serem utilizados os endereços gerados devem socorrer-se de CGA [78];

- Utilização do DHCPv6, mas a gama atribuída não deve começar nos primeiros endereços de nós disponíveis;
- A atribuição de endereços de forma aleatória.

Utilizando SLAAC podem também utilizar-se endereços temporários, para os quais se define um período máximo de validade, ao fim do qual é gerado um novo endereço [78].

7.5.2 V16 – Privacy unfriendly Stateless Address Autoconfiguration (SLAAC)

Resolução
No SLAAC é também possível obter os últimos 64 *bits* do endereço através da geração de um número aleatório. Desta forma, torna-se impossível para um utilizador da *internet* manter o registo de quais as redes por onde um determinado equipamento transitou [105].

7.5.3 V17 – Funcionalidades não suportadas ou inseguras do IPv6

Resolução
Ao contrário de outas, esta solução não é de extrema complexidade. Alguns princípios são suficientes para que estas vulnerabilidades sejam rapidamente anuladas [105], tais como:

- Remover as funcionalidades das implementações e configurações
- Rejeitar tráfego relativo às funcionalidades nos *routers* e *firewalls*

7.5.4 V18 – Neighbor Discovery table exhaustion

Resolução
O tráfego de envio de mensagens relativas à descoberta de vizinhos pode ser limitado nos dispositivos de rede [105].

7.6 Classificação da Resolução de Vulnerabilidades

Naturalmente que é fundamental percebermos a origem e o impacto que uma vulnerabilidade explorada poderá ter. No entanto, esta informação de forma isolada torna-se pouco relevante. É necessário relacionar a informação anteriormente recolhida com uma proposta ou método de resolução, ou no limite, uma noção de quais as práticas que poderão ajudar a conter este tipo vulnerabilidades.

Router/Firewall	Aplicação de regras nos *routers* e *firewall*
Informação Estática	Informação estática nos clientes
IPSec	Utilização de IPSec
SEND	Utilização de SEND
RA-Guard	RA-Guard
Limitação pacotes	Limitação do número de pacotes
DHCP	Aplicação de regras no DHCP

7.7 Resumo das Vulnerabilidades

A Tabela 17 contempla a informação relevante para um administrador de redes, quando este ponderar a implementação do IPv6. São apresentadas as caraterísticas das vulnerabilidades, bem como métodos que auxiliam a contenção dos ataques.

		Tipo	Método	Dificuldade Execução	Impacto	Alvo	Tipo de Resolução
V1 - Covert Channel on Hop-by-Hop and Destination Options Header	V1	MM	Send	M			*Router/Firewall*
V2 - Router Alert DoS Attack in Hop-by-Hop Options Header	V2	MM	Flood	M			*Router/Firewall*
V3 - Firewall Evasion with Fragment Header	V3	MM	Send	B			*Router/Firewall*
V4 - Cabeçalhos Desconhecidos	V4	MASQ	Spoof	A			*Router/Firewall*
V5 - Router Advertisement Spoofing	V5	RA	Spoof	M			Informação Estática IPSec SEND RA-Guard
V6 - Router Advertisement Flooding	V6	RA	Flood	M			Informação Estática IPSec SEND RA-Guard Limitação pacotes
V7 - Neighbor Solicitation Flooding	V7	RA	Flood	B			IPSec SEND Limitação pacotes
V8 - Neighbor Solicitation Spoofing	V8	RA	Spoof	M			IPSec SEND
V9 - Duplicate Address Detection	V9	RA	Spoof	M			IPSec SEND
V10 - Redirect Spoofing	V10	MASQ	Spoof	M			*Router/Firewall* SEND
V11 - Broadcast amplification attacks (smurf)	V11	RA	Flood	M			*Router/Firewall*
V12 - Secure Neighbor Discovery (SEND) Flooding	V12	DOS	Flood	M			*Router/Firewall*

		Tipo	Método	Dificuldade Execução	Impacto	Alvo	Tipo de Resolução
V13 - DHCP Starvation	V13	DOS	Flood	B			*Router/Firewall*
V14 - Rogue DHCPv6 Server	V14	MR	Spoof	M			DHCP
V15 - Reconnaissance	V15	MASQ	Scan	B			DHCP
V16 - Privacy unfriendly Stateless Address Autoconfiguration (SLAAC)	V16			A			*Router/Firewall*
V17 - Unsupported and unsafety IPv6 features	V17	MASQ	Spoof	M			*Router/Firewall*
V18 - Neighbor Discovery table exhaustion	V18	RA	Scan	M			*Router/Firewall*

Tabela 17 – Resumo das Vulnerabilidades com ações de resolução

7.8 Sumário de Boas Práticas

Para além das já estudadas vulnerabilidades, com a massificação da versão 6 do *Internet Protocol* vão surgir novas ameaças, no futuro, o que implica uma constante monitorização da rede e dos recursos que a ela se encontram ligados.

Algumas medidas podem ser tomadas previamente com vista a prevenir ou a reduzir o impacto de futuros ataques, que são ainda desconhecidos. Nesse sentido, de seguida, são apresentadas algumas regras que permitem incrementar o nível de segurança das redes onde forem aplicadas.

Essas medidas podem ser categorizadas [65] [118] [119] em 10 categorias:

- Segurança do elo mais fraco;
- Defesa em profundidade;
- Falha segura;
- Privilégio mínimo;
- Compartimentação;
- Simplicidade;
- Promoção da privacidade;
- Guardar segredos é difícil;
- Desconfiar por omissão;
- Utilizar fontes de informação públicas.

Segurança do elo mais fraco

1. Os sistemas mais sensíveis têm, obrigatoriamente, que ser protegidos de uma forma mais cuidada do que os restantes;

Defesa em profundidade

2. A utilização de mecanismos em série, como a utilização de uma *firewall* seguida de um *router* aumenta o grau de dificuldade de invasão dos sistemas;

Falha segura

3. Os pacotes compostos por extensões de cabeçalhos desatualizados devem também ser descartados [120]*;*
4. Bloquear todo o tráfego que não pertença ao protocolo vigente na rede [121];
5. Existência de cópia da configuração de equipamentos fundamentais como *routers* e servidores;

Privilégio mínimo

6. Utilizadores num sistema devem deter as permissões necessárias para executarem as suas tarefas, jamais um utilizador deve ter mais permissões do que as extremamente necessárias

Compartimentação

7. Na interface exterior de uma rede devem ser descartados pacotes como *Router Solicitation* e *Advertisement, Neighbor Solicitation* e *Adverstisement, Redirect* [122];
8. Pacotes como *Destination Unreachable, Packet Too Big, Time* Exceeded e *Parameter Problem* jamais devem ser descartados na interface externa de um *gateway* [122];
9. Com o intuito de permitir a correta utilização do IPSec, os pacotes que contenham um endereço legítimo e o cabeçalho "*Authentication Header*" ou *"Encapsulatin Security Payload"* devem poder entrar e sair da rede [34] [36];
10. Utilização de gama de endereços a atribuir, pouco comuns [121];
11. Utilização de tabela estática para manter a informação dos vizinhos na rede, em sistemas críticos [123];

Simplicidade

12. Fragmentos de pacotes com menos de 1280 octetos devem ser descartados (exceto o último, que se determina com base na *flag* M) [123];

Promover a privacidade

13. Os pacotes que têm como IP emissor um endereço *multicast* não devem ser encaminhados nem transmitidos por nenhuma interface [120]*;*

14. Pacotes nos quais os endereços de origem sejam *unique local* não devem sair nem entrar na rede [120]*;*
15. Os pedidos de DNS recebidos nas interfaces exteriores não devem ser processados pelo DNS que se encontra dentro da rede [120]*;*
16. Os pedidos de DHCP recebidos do exterior não devem ser processados pelo servidor de DHCP que se encontra "dentro" da rede [52];

Guardar segredos é difícil

17. Utilização do IPSec no máximo de processos possíveis, desde que sejam garantidas condições de processamento pelo equipamento que compõe a rede [121];

Desconfiar por omissão

18. Todo o tráfego que entra ou sai para a internet deve ser verificado de uma forma básica, procurando *spoofs* [120]*;*
19. Limitar o *hop limit* para garantir que os pacotes ao fim de alguns "saltos" são descartados [3];
20. Qualquer tráfego UDP que tenha como destino a porta 500 deve ser bloqueado, uma vez que esta porta se encontra destinada ao *Internet Key Exchange* [124];
21. No caso de utilização do DHCPv6, este deve utilizar autenticação [92];
22. Determinar que extensões de cabeçalhos são permitidas na rede [123];
23. Todos os serviços, mesmo que do protocolo em utilização, que não estejam a ser utilizados devem ser bloqueados através de regras na *firewall* [125];

Utilizar fontes de informação públicas

24. O *firmware* do *gateway* deve manter-se sempre devidamente atualizado [120]*;*
25. Elaboração de documentação de todas as tomadas de decisão e implementações na rede [121].

8 Conclusões e Trabalho Futuro

Atualmente, a segurança da informação é uma das maiores preocupações para os administradores de redes. A nova versão do IPv6, inicialmente desenvolvida principalmente para resolver o problema da exaustão de endereços, também introduz novos mecanismos de segurança e apresenta um conjunto relevante de desafios relacionados com a implementação e maturação da tecnologia que importa estudar.

Neste relatório foi apresentada uma análise ao IPv6 focada nas questões relacionadas com a sua implementação, mecanismos de migração e aspetos de segurança mais relevantes.

O mecanismo de transição escolhido pelo administrador de rede tem um papel muito importante no resultado final da migração. De entre os 3 mecanismos apresentados, Dual-Stack, Túneis e Tradução, não podemos eleger uma melhor opção. A decisão de qual o mecanismo a implementar dependerá muito do cenário atual da organização e dos objetivos definidos a atingir, como o caráter definitivo ou não do mecanismo, os equipamentos ou redes a interligar. Naturalmente que o processo de migração obriga a uma determinada sequência de verificações e ações, desde a garantia, por parte do ISP, do suporte de IPV6, até à fase monitorização e atualização da documentação, são diversos os procedimentos a atender para que o processo de migração seja completado com sucesso.

Para que um responsável por uma determinada rede possa mais facilmente avaliar os riscos a que potencialmente está exposto, é importante que tome um contacto mais próximo com as consequências que podem advir de ataques a sistemas que não se encontram devidamente protegidos. Desta forma, as 18 vulnerabilidades que foram consideradas as mais relevantes, pela sua facilidade de implementação e pelo seu pesado impacto nos sistemas alvo, são detalhadas, sendo explicada a vulnerabilidade, apresentada a forma como um ataque a pode explorar e demonstrado o impacto que esta terá no sistema alvo.

A análise de risco é uma ferramenta imprescindível para avaliar riscos de segurança e consiste num processo de catalogação do equipamento, serviços, dados e aplicações que constituem o capital tecnológico da entidade, definindo para cada um destes o grau de risco, ou de importância. A informação apresentada permite facilitar a avaliação das consequências de

ataques, compreender quais as vulnerabilidades que podem causar maior impacto em determinados sistemas, bem como as medidas de recuperação a implementar após o ataque. Desta forma é facilitada a elaboração mais eficaz de um plano de segurança.

Após detalhadas todas as vulnerabilidades, elaborada a análise de risco e classificadas as vulnerabilidades devem ser tomadas medidas de segurança e proteção contra a exploração de ameaças. Para as definir é crucial que se perceba o método utilizado pelo atacante para explorar a vulnerabilidade. É fundamental compreender que estas medidas não garantem que o ataque não possa ser executado, mas sim que há menos probabilidade de ser executado e que, em caso de execução, o impacto possa ser menorizado. As boas práticas apresentadas podem ser consideradas como medidas padrão a utilizar sempre que possível nas diversas redes, pois ajudarão a prevenir futuros ataques.

Pretende-se assim que um administrador de redes que necessite de planear um processo de migração tenha, neste documento, ao seu dispor informação fundamental para que possa tomar decisões ponderadas, conhecendo as alternativas existentes, bem como as consequências de cada uma das opções tomadas.

Trabalho Futuro

Naturalmente que muitas mais vulnerabilidades de relevo irão surgir com a evolução do protocolo, pelo que a lista apresentada deverá crescer tão rapidamente como a massificação da nova versão do protocolo. Poderão ser seguidos caminhos adicionais no prolongamento deste trabalho, dos quais se destacam os seguintes:

- A aplicação de medidas de segurança ao nível da implementação, uma vez que cada fabricante apresenta meios distintos de permitir a implementação de mecanismos de segurança;
- A exploração de sistemas de IDS e IPS que aumentam significativamente a segurança das redes onde são incorporados;
- Avaliação de vulnerabilidades que irão surgir com a utilização mais intensiva do protocolo.

9 Referências

[1] Google, “Google IPv6 Statistics,” 2015. [Online]. Available: http://www.google.com/intl/en/ipv6/statistics.html.

[2] R. Gilligan e E. Nordmark, “[RFC 1933] Transition Mechanisms for IPv6 Hosts and Routers,” 1996.

[3] A. Moreiras, “Segurança e IPv6 - Aspectos teóricos e práticos,” Núcleo de Informação e Coordenação do Ponto BR - Comité Gestor da Internet no Brasil.

[4] THC, “The Hacker's Choice,” 2015. [Online]. Available: www.thc.org/thc-ipv6. [Acedido em 05 2015].

[5] Kali, “KALI - Penetration Testing Redefined with the Kali Linux Distribution,” [Online]. Available: www.kali.org. [Acedido em 05 2015].

[6] PFSense, “PFSense,” [Online]. Available: www.pfsense.org.

[7] J. Weber, “IPv6 Security Test Laboratory,” 2013.

[8] Cisco, “VNI Forecast Highlights,” [Online]. Available: http://www.cisco.com/web/solutions/sp/vni/vni_forecast_highlights/index.html. [Acedido em 06 2015].

[9] S. Deering e R. Hinden, “[RFC 1883] Internet Protocol, Version 6 (IPv6) Specification,” 1995.

[10] K.-T. Seo, M. Balitanas, E.-s. Cho, M.-k. Choi e S. Kim, “Security Issues and Preventive Measuers for IPv6 on Systems Control and Data Acquisition,” 2009.

[11] S. Brander e A. Mankin, “[RFC 1752] The Recommendation for the IP Next Generation Protocol,” 1995.

[12] APNIC, “IPv4 exhaustion details,” [Online]. Available: https://www.apnic.net/community/ipv4-exhaustion/ipv4-exhaustion-details.

[13] Cisco, “6lab - The place to monitor IPv6 adoption,” [Online]. Available: http://6lab.cisco.com/stats/cible.php?country=world&option=prefixes.

[14] APNIC, “IPv6 Country Deployment for Portugal (PT),” [Online]. Available: http://stats.labs.apnic.net/ipv6/PT?c=PT&x=1&p=1&r=1&w=400. [Acedido em 06 2015].

[15] Google, “Google IPv6 - Per-Country IPv6 adoption,” 2015. [Online]. Available: https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption.

[16] Akamai, “State Of The Internet - IPv6 Adoption Visualization,” [Online]. Available: http://www.stateoftheinternet.com/trends-visualizations-ipv6-adoption-ipv4-exhaustion-global-heat-map-network-country-growth-data.html. [Acedido em 6 2015].

[17] S. Kawamura e M. Kawashima, “[RFC 5952] A Recommendation for IPv6 Address Text Representation,” 2010.

[18] Internet Assigned Numbers Authority, “Internet Assigned Numbers Authority - Number Resources,” [Online]. Available: http://www.internetassignednumbersauthority.org/numbers. [Acedido em 2015].

[19] “IPv6 Addressing,” Cisco Systems, Inc, 2007.

[20] S. Deering, R. Hinden e E. Nordmark, “[RFC 3587] IPv6 Global Unicast Address Format,” 2003.

[21] J. Davies, Understanding IPv6, 3ª Edição, 9780735659148, Microsoft, 2012.

[22] S. Deering e R. Hinden, “[RFC 4291] IP Version 6 Addressing Architecture,” 2006.

[23] S. Hagen, IPV6 Essentials - Integrating IPv6 into your IPv4 network, 3ª ed., O'REILLY, 2014.

[24] S. Deering e R. Hinden, “[RFC 2373] IPv6 Addressing Architecture,” 1998.

[25] P. Loshin, IPv6 Theory, Protocol and Practice, Elsevier, 2004.

[26] P. Fojtu, “Vulnerabilities and Threats in IPv6 Environment,” 2013.

[27] M. Morowczynski, “IPv6 for the Windows Administrator: More IPv6: Subnetting, Zones, Address Autoconfiguration, Router Advertisements and IPv4 comparisons,” 2015. [Online]. Available: http://blogs.technet.com/b/askpfeplat/archive/2013/07/08/ipv6-for-the-windows-administrator-more-ipv6-subnetting-zones-address-autoconfiguration-router-advertisements-and-ipv4-comparisons.aspx.

[28] SurfNet, “Preparing An IPv6 Addressing Plan,” 2013.

[29] K. Nichols, S. Blake, F. Baker e D. Black, “[RFC 2474] Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers,” 1998.

[30] R. Moskowitz, P. Nikander, P. Jokela e T. Henderson, “[RFC 5201] Host Identity Protocol,” 2008.

[31] S. Krishnan, J. Woodyatt, E. Kline, J. Hoagland e M. Bhatia, “[RFC 6564] A Uniform Format for IPv6 Extension Headers,” 2012.

[32] S. Racherla e J. Daniel, IPv6 Introduction and Configuration, 1ª Edição, 9780738450551, IBM, 2012.

[33] S. Deering e R. Hinden, "[RFC 2460] Internet Protocol, Version 6 (IPv6) Specification," 1998.

[34] S. Kent, "[RFC 4302] IP Authentication Header," 2005.

[35] "Microsoft TechNet - Authentication Header," Microsoft, [Online]. Available: http://technet.microsoft.com/en-us/library/cc959507.aspx. [Acedido em 2015].

[36] S. Kent, "[RFC 4303] IP Encapsulating Security Payload," 2005.

[37] M. Véstias, Redes Cisco para Profissionais, 3ª Edição, 9789727224821, FCA - Editora de Informática, 2005.

[38] J. Postel, "[RFC 792] Internet Control Message Protocol," 1981.

[39] A. Conta, S. Deering e M. Gupta, "[RFC 4443] Internet Control Message Protocol (ICMPv6)," 2006.

[40] A. Conta e S. Deering, "[RFC 2463] Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification," 1998.

[41] J. Postel, D. Johnson, T. Markson, B. Simpson e Z.-S. Su, "Internet Control Message Protocol (ICMP) Parameters," [Online]. Available: http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml#icmp-parameters-codes-3. [Acedido em 2015].

[42] S. Gai, Internetworking IPv6 with Cisco Routers, 1ª Edição, 978-0070228368, 1998.

[43] A. Conta, "[RFC 3122] Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification," 2001.

[44] M. Crawford, "[RFC 2894] Router Renumbering for IPv6," 2000.

[45] S. Deering, W. Fenner e B. Haberman, "[RFC 2710] Multicast Listener Discovery (MLD) for IPv6," 1999.

[46] B. Haberman e J. Martin, "[RFC 4286] Multicast Router Discovery," 2005.

[47] T. Narten, E. Nordmark, W. Simpson e H. Soliman, "[RFC 4861] Neighbor Discovery for IP version 6," 2007.

[48] R. Vida, L. Costa, S. Fdida, S. Deering, B. Fenner, I. Kouvelas e B. Haberman, "[RFC 3810] Multicast Listener Discovery Version 2 (MLDv2) for IPv6," 2004.

[49] S. Thomson, T. Narten e T. Jinmei, "[RFC 4862] IPv6 Stateless Address Autoconfiguration," 2007.

[50] T. Narten, R. Draves e S. Krishnan, "[RFC 4941] Privacy Extensions for Stateless Address Autoconfiguration in IPv6," 2007.

[51] S. Frankel, R. Graveman, J. Pearce e M. Rooks, "Guidelines for the Secure Deployment of IPv6," 2010.

[52] J. Bound, B. Volz, C. Perkins e M. Carney, "[RFC 3315] Dynamic Host Configuration Protocol for IPv6," 2003.

[53] S. Kerr, "DHCPv6," 2006.

[54] Y. C. R. Gelogo e B. Park, “Threats and Security Analysis for Enhanced Secure Neighbor Discovery Protocol (SEND) of IPv6 NDP Security,” International Journal of Control and Automation Vol. 4, No. 4, December, 2011, 2011.

[55] T. Narten, E. Nordmark e W. Simpson, “[RFC 2461] Neighbor Discovery for IP Version 6,” 1998.

[56] I. Cisco Systems, IPv6 Configuration Guide, Cisco IOS - Release 15.2M&T, 2012.

[57] P. Castro, “Process for IPv6 Migration in Large Organizations,” Instituto Superior Técnico de Lisboa, 2013.

[58] D. Johnsin, C. Perkins e J. Arkko, “[RFC 3775] Mobility Support in IPv6,” 2004.

[59] “IPv6 MOBILITY AT–A–GLANCE,” Cisco Systems, Inc. , 2005.

[60] K. Das, “IPSec & IPv6 - Securing the NextGen Internet,” [Online]. Available: http://www.ipv6.com/articles/security/IPsec.htm.

[61] CMU, “Security 101 - Computing Services Information Security Office”.

[62] U.S. DEPARTMENT OF COMMERCE, “Standards for Security Categorization of Federal Information and Information Systems,” 2004.

[63] L. Gommans, J. Vollbrecht e D. Spence, “[RFC 2903] Generic AAA Architecture,” 2000.

[64] H. Haijian, “Network Security Threats and Defense,” 2013.

[65] A. Costa e N. Pereira, “Princípios de Segurança Informática na Programação,” 2014.

[66] G. E. d. Andrade, “Riscos, Ameaças e Vulnerabilidades”.

[67] C. Pfleeger, “Security in Computing,” Prentice Hall, 2006.

[68] Kaspersky, “O que é a encriptação?,” [Online]. Available: http://www.kaspersky.com/pt/internet-security-center/definitions/encryption. [Acedido em 06 2015].

[69] “Implementing IPsec in IPv6 Security,” Cisco Systems, Inc., 2012.

[70] “Segurança em IPv6,” IPv6.br, 2012.

[71] S. Kent e K. Seo, “[RFC 4301] Security Architecture for the Internet Protocol,” 2005.

[72] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen e T. Kivinen, “[RFC 7296] Internet Key Exchange Protocol Version 2,” 2014.

[73] E. Jankiweicz, J. Loughney e T. Narten, “[RFC 6434] IPv6 Node Requirements,” 2011.

[74] S. Hogg e E. Vyncke, IPv6 Security, Cisco Press, 2009.

[75] S. Institute, “Security Features of IPv6,” 2002.

[76] P. Nikander, J. Kempf e E. Nordmark, “[RFC 3756] IPv6 Neighbor Discovery (ND) Trust Models and Threats,” 2004.

[77] J. Arkko, J. Kempf, B. Zill e P. Nikander, “[RFC 3971] SEcure Neighbor Discovery (SEND),” 2005.

[78] A. Herrera, “How Secure is the Next-Generation Internet? An Examination of IPv6,” Departmnet of Defence of Australian Government, 2013.

[79] I. Cisco Systems, “Dual Stack Network,” 2010. [Online]. Available:

http://www.cisco.com/web/strategy/docs/gov/IPV6at_a_glance_c45-625859.pdf.

[80] E. Carter, “IPv6 Security Considerations,” Cisco Services.

[81] B. Carpenter e C. Jung, “[RFC 2529] Transmission of IPv6 over IPv4 Domains without Explicit Tunnels,” 1999.

[82] H. Zuleger, 6to4 & 6rd Explained, http://www.hznet.de/ipv6/ipv6-6rd.pdf, 2010.

[83] R. Despres, “[RFC 5569] IPv6 Rapid Deployment on IPv4 Infrastructures (6rd),” 2010.

[84] M. Towsley e O. Troan, [RFC 5969] IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification, 2010.

[85] F. Templin, T. Gleeson e D. Thaler, “[RFC 5214] Intra-Site Automatic Tunnel Addressing Protocol (ISATAP),” 2008.

[86] C. Huitema, “[RFC 4380] Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs),” 2006.

[87] G. Tsirtsis e P. Srisuresh, [RFC 2766] Network Address Translation - Protocol Translation (NAT-PT), 2000.

[88] S. Burwell, “Enhancing the Security of Federal Information and Information Systems,” Office of Management and Budget, Executive Office of the President of United States, 2013.

[89] ipv6 test, “IPv6 in Portugal,” 5 2015. [Online]. Available: www.ipv6-test.com/stats/country/PT. [Acedido em 6 2015].

[90] “Technical and Economic Assessment of Internet Protocol Version 6 (IPv6),” U.S. DEPARTMENT OF COMMERCE, 2006.

[91] S. Feruza e T.-h. Kim, “IT Security Review: Privacy, Protection, Access Control, Assurance and System Security,” International Journal of Multimedia and Ubiquitous Engineering, 2007.

[92] V. Leitão, “IPv6 - A New Scurity Challenge,” 2011.

[93] P. Rubens, “eSecurity PLanet,” 2012. [Online]. Available: www.esecurityplanet.com/network-security/7-ipv6-security-risks.html. [Acedido em 2015].

[94] M. Mavani e L. Ragha, “Covert channel in IPv6 Destination option Extension Header,” 2014.

[95] R. Rahman, D. Ward, A. Narayanan, A. Farel, T. Li e F. Faucher, “[RFC 6398] IP Router Alert Considerations and Usage,” 2011.

[96] A. Atlasis, “Attacking IPv6 Implementation using Fragmentation,” 2012.

[97] M. Shutte, “Design and Implementation of an IPv6 Plugin for the Snort Intrusion Detection System,” Potsdam University - Institute for Computer Science Operating Systems and Distributed Systems, 2011.

[98] “IPv6 Security Assessment and Benchmarking Abstract Test Suite,” EANTC AG, 2013.

[99] CVE Details, “CVE Details CVE-2010-4669,” [Online]. Available: http://www.cvedetails.com/cve/CVE-2010-4669.

[100] J. Small, “IPv6 Attacks and countermeasures,” CDW Advanced Technology Services.

[101] H. Dawood, “IPv6 Security Vulnerabilities,” International Journal of Information Security Science, vol. 1.

[102] J. Ullrich, K. Krombholz, H. Hobel, A. Dabrowski e E. Weippl, “IPv6 Security: Attacks and Countermeasures in a Nutshell”.

[103] C. Carpene e A. Woodward, “Exposing Potential Privacy Issues with IPv6 Address Construction,” 2012.

[104] A. Zamani e S. Zubair, “Deploying IPv6: Security and Future,” International Journal of advanced studies in Computer Science and Engineering, vol. 3, 2014.

[105] S. Degen, A. Holtzer, B. Kluit, H. Schotanus, H. Oije, D.-J. Bartels, M. Ramesdonk, G. Groot, F. Kolle, D. Keuper, T. Stols, C. Ottow, G. Bij, C. Mune e A. Spruyt, “Testing the security of IPv6 implementations,” 2014.

[106] C. Huitema e B. Carpenter, “[RFC 3879] Deprecating Site Local Addresses,” 2004.

[107] J. Abley, P. Savola e G. Neville-Neil, “[RFC 5095] Deprecation of Type 0 Routing Headers in IPv6,” 2007.

[108] S. JIang, D. Conrad e B. Carpenter, “[RFC 6563] Moving A6 to Historic Status,” 2012.

[109] R. Weaver, D. Weaver e D. Farwood, Guide to Network Defense and Countermeasures Second Edition, 2ª Edição, 978-1133727941, Thomson Course Technology, 2013.

[110] S. Plósz, A. Farshad, M. Tauber, C. Lesjak, T. Ruprechter e N. Pereira, “Security Vulnerabilities And Risks In Industrial Usage Of Wireless Communication,” 2014.

[111] European Telecommunications Standards Institute, “Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 1: Threat Analysis,” 2003.

[112] E. Davies, S. Krishnan e P. Savola, “[RFC 4942] IPv6 Transition/Coexistence Security Considerations,” 2007.

[113] E. Levy-Abegnoli, G. Vlde, C. Popoviciu e J. Mohacsi, “[RFC 6105] IPv6 Router Advertisement Guard,” 2011.

[114] R. Radhakrishnan, M. Jamil e S. M. Mehfuz, “Security issues in IPv6,” Third International COnference on Networking and Services 2007 IEEE, 2007.

[115] N. Moore, “[RFC 4429] Optimistic Duplicate Address Detection (DAD) for IPv6,” 2006.

[116] N. Tripathi, “Can anyone tell me the latest solutions to prevent DHCP starvation attacks and Rogue DHCP Server attacks?,” 2015. [Online]. Available: https://www.researchgate.net/post/Can_anyone_tell_me_the_latest_solutions_to_prevent_DHCP_starvation_attacks_and_Rogue_DHCP_Server_attacks.

[117] Y. Bhaiji, “Understanding, Preventing, and Defending Against Layer 2 Attacks,” Cisco, 2007.

[118] OWASP, “Secure Coding Principles,” [Online]. Available: https://www.owasp.org/index.php/Secure_Coding_Principles. [Acedido em 06 2015].

[119] J. Saltzer e M. Schroeder, “The Protection of Information in Computer Systems,” Project MAC and the Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology Cambridge, 1975.

[120] J. Woodyatt, “[RFC 6092] Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service,” 2011.

[121] THe Government of the Hong Kong, “IPv6 Security,” THe Government of the Hong Kong Special Administrative Region, 2011.

[122] E. Davies e J. Mohacsi, “[RFC 4890] Recommendations for Filtering ICMPv6 Messages in Firewalls,” 2007.

[123] Cisco, “IPv6 Security,” 2006.

[124] C. Kaufman, P. Hoffman, Y. Nir e P. Eronen, “[RFC 5996] Internet Key Exchange Protocol Version 2 (IKEv2),” 2010.

[125] W. Maia, “IPv6 Security,” 2012.

[126] R. Hinden e B. Haberman, “[RFC 4193] Unique Local IPv6 Unicast Addresses,” 2005.

[127] B. Braden, L. Zhang, S. Berson, S. Herzog e S. Jamin, “[RFC 2205] Resource ReSerVation Protocol (RSVP),” 1997.

[128] D. Borman, S. Deering e R. Hinden, “[RFC 2147] IPv6 Jumbograms,” 1999.

[129] J. Arkko, T. Aura, J. Kempf, V.-M. Mantyla, P. Nikander e M. Roe, “Securing IPv6 Neighbor and Router Discovery”.

[130] S. Kent e R. Atkinson, “[RFC 2402] IP Authentication Header,” 1998.

[131] P. Nikander, J. Kempf e E. NOrdmark, “[RFC 3756] IPv6 Neighbor Discovery (ND) Trust Models and Threats,” 2004.

[132] S. Plósz, A. Farshad, M. Tauber, C. Lesjak, T. Ruprechter e N. Pereira, “Security Vulnerabilities And Risks In Industrial Usage Of Wireless Communication,” 2014.

[133] A. Conta e S. Deering, “[RFC 2473] Generic Packet Tunneling in IPv6 Specification,” 1998.

[134] B. Carpenter e K. Moore, “[RFC 3056] Connection of IPv6 Domains via IPv4 Clouds,” 2001.

[135] C. Marsan, “IPv6 tunnel basics,” Network World, 6 5 2010. [Online]. Available: http://www.networkworld.com/article/2208835/lan-wan/ipv6-tunnel-basics.html. [Acedido em 2015].

[136] S. JIang, D. Guo e B. Carpenter, [RFC 6264] An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition, 2011.

[137] M. Bagnulo, P. Matthews e I. Beijnum, [RFC 6146] Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers, 2011.

[138] “IPv6Now,” 2015. [Online]. Available: http://www.ipv6now.com.au/primers/IPv6RoutingSecurity.php.

[139] W. Maia, “Layer II Security,” 2010.

[140] I. Gashinsky, J. Jaeggli e W. Kumari, “[RFC 6583] Operational Neighbor Discovery

Problems," 2012.

[141] "IPv6 First-Hop Security Concerns," Cisco, [Online]. Available: http://www.cisco.com/web/about/security/intelligence/ipv6_first_hop.html. [Acedido em 2015].

[142] E. Yardley, "CCNP Studies: Configuring DHCP Snooping," 2012. [Online]. Available: http://packetpushers.net/ccnp-studies-configuring-dhcp-snooping/.

[143] R. Lopes, "Instalação e Administração de uma Rede Local de Comunicação de Dados," Universidade de Aveiro, 1998.

[144] S. Basílio, "A Evolução dos Computadores e da Internet," 2006. [Online]. Available: http://www1.ci.uc.pt/diglit/DigLitWebCdeCodiceeComputadorEnsaio29.html#bOrigemdaInternet.

[145] V. Dumas, "A origem da internet," [Online]. Available: http://www2.uol.com.br/historiaviva/reportagens/o_nascimento_da_internet.html.

[146] DARPA, "DARPA History," [Online]. Available: [http://www.darpa.mil/About/History/History.aspx.

[147] IANA, "Introducing IANA," [Online]. Available: www.iana.org/about.

[148] K. Das, "IPv6 - The History and Timeline," [Online]. Available: http://www.ipv6.com/articles/general/timeline-of-ipv6.htm.

[149] What's a Byte, "Megabytes, Gigabytes, Terabytes... What Are They?," [Online]. Available: www.whatsabyte.com/.

[150] Kali, "Kali," [Online]. Available: www.kali.org.

[151] IETF, "Request for Comments (RFC)," [Online]. Available: www.ietf.org/rfc.html.

[152] D. Borman, S. Deering e R. Hinden, "[RFC 2675] IPv6 Jumbograms" 1999.

[153] National Instituto of Standards and Technology, "National Vulnerability Database" 2015. [Online]. Available: https://web.nvd.nist.gov/view/vuln/search-results?query=IPv6&search_type=all&cves=on. [Acedido em 11 6 2015].

[154] National Institute of Standards and Technology, "National Vulnerability Database" 2015. [Online]. Available: https://web.nvd.nist.gov/view/vuln/statistics-results?adv_search=true&query=ipv6. [Acedido em 2015].

[155] P. DesAutels, "W3C," [Online]. Available: http://www.w3.org/PICS/DSig/SHA1_1_0.html. [Acedido em 2015].

[156] S. Brander e A. Mankin, "[RFC 1550] IP: Next Generation (IPng) White Paper Solicitation" 1993.

[157] S. Zander, G. Armitage e P. Branch, "A survey of covert channels and countermeasures in computer network protocols," IEEE Communications Surveys & Tutorials, Melbourne, Austrália, 2007.

[158] G. Morais, "Análise e Implementação de Sistemas de IDS e IPS," 2011.

[159] J.-W. Kim, H.-H. Cho, G.-J. Mun e J.-H. Seo, "Experiments adn Countermeasures of Security Vulnerabilities on Next Generataion Network," Ministry of Information and

Communication of Korea.

[160] IETF, “About the IETF,” [Online]. Available: https://www.ietf.org/about/. [Acedido em 2015].

[161] T. Hain, IPv6 Deployment - Security Issues Thinking outside the NAT box, Cisco Systems, 2005.

[162] T. Smith e W. Sean, CCNP Security Secure 642-637 Official Cert Guide, 1ª Edição, 978-1-58714-280-2, 2011.

[163] C. Kiraly, S. Teofili, G. Bianchi, R. Lo Cigno, M. Nasrdelli e E. Delzrei, “Traffic Flow Confidentiality in IPsec: Protocol and Implementation,” em The Future of Identity in the Information Society, 1ª Edição, 978-0-387-79026-8, Springer Boston, 2008, pp. 311-324.

[164] Cisco, “The Zettabyte Era — Trends and Analysis,” Cisco, Maio 2015. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html.