FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Superior de Tecnologia em Segurança da Informação

Washington Osti Silva

IDENTIFICAÇÃO DE VULNERABILIDADES EM REDES IPv6

Americana, SP
2013

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Washington Osti Silva

IDENTIFICAÇÃO DE VULNERABILIDADES EM REDES IPv6

Trabalho monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Fatec Americana, sob orientação do Prof^{o} Dr. José Luis Zem.

Área temática: Segurança da Informação

Americana, SP
2013

FICHA CATALOGRÁFICA elaborada pela
BIBLIOTECA – FATEC Americana – CEETPS

Silva, Washington Osti
S584i Identificação de vulnerabilidade em redes IPv6. / Washington Osti Silva. – Americana: 2013.
60f.

Monografia (Graduação de Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Dr. José Luis Zem

1.Redes de computadores 2. Segurança em sistemas de informação I. Zem, José Luis II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.519
681.518.5

Bibliotecária responsável pela FC: Ana Valquiria Niaradi – CRB-8 região 6203

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Washington Osti Silva

IDENTIFICAÇÃO DE VULNERABILIDADES EM REDES IPv6

Trabalho de Conclusão de Curso apresentado à Fatec Americana como parte dos requisitos para obtenção do título de Tecnólogo em Segurança da Informação.

PUBLIQUE-SE

Banca examinadora:

_____

José Luis Zem – (Presidente)
Doutorado em Física Computacional
Faculdade de Tecnologia de Americana – FATEC

_____

Marcus Vinícius Lahr Giraldi – (Membro)
Graduado em Processamento de Dados
Faculdade de Tecnologia de Americana – FATEC

_____

Maria Cristina Luz Fraga Moreira Aranha – (Membro)
Mestrado em Ciência da Computação
Faculdade de Tecnologia de Americana – FATEC

Americana, 05 de Dezembro de 2013.

RESUMO

Numa era na qual a informação é um bem muito importante para todos, o principal meio de compartilhamento, a Internet, começa a sofrer de um problema crítico de endereçamento, que pode comprometer seu crescimento no futuro. Para resolver esse problema, as autoridades responsáveis pela Internet criaram um novo formato de endereçamento, o IPv6, mas a adesão está abaixo do que foi planejado inicialmente. Vulnerabilidades e falta de conhecimentos são alguns dos motivos dessa falta de interesse na migração para o novo padrão que pretende, entre outros aspectos, resolver este e outros problemas, além de trazer novas funcionalidades para o futuro da Internet que está em constante evolução. Este trabalho pretende, além de contribuir como mais uma fonte de informação sobre o IPv6, apontar as principais vulnerabilidades presentes nessa nova e necessária suíte de protocolos da Internet futura.

Palavras-chave: redes; *IPng*; endereçamento; Internet;

ABSTRACT

In times that the information is the very important for everyone, the primary means of sharing, the Internet begins to suffer from a critical problem addressing, which may hinder its future growth. To solve this problem, the authorities created a new Internet addressing format, IPv6, but acceptance is below that was originally planned. Vulnerabilities and lack of knowledge are some of the reasons for disinterest in migrating to the new standard that aims, among other things, solve this and other problems, and bring new functionalities to the future of the Internet, that is constantly evolving. This work intends to contribute as well as a source of information about IPv6, point out key vulnerabilities present in this new and necessary suite of Internet protocols for the future.

Keywords: *networks; IPng; addressing, Internet;*

SUMÁRIO

1. INTRODUÇÃO

Observando a linha cronológica da humanidade, é possível perceber que o Homem passou por muitas eras e na atual, denominada Era da Informação, encontra-se o bem mais valioso que é a informação. Porém, não a informação que está inacessível, mas pelo contrário, aquela que é divulgada, compartilhada, comunicada, conforme a necessidade. Todavia, essa comunicação precisa ser feita de maneira controlada, sabendo quem, quando e onde é acessada. Em resumo, precisa estar acessível e protegida ao mesmo tempo.

A Internet é, atualmente, o meio de comunicação mais utilizado para o acesso e compartilhamento dessas informações, uma vez que possui velocidade, facilidade e custo acessível e, por essa razão, é a mais utilizada. Para que essas informações sejam transmitidas, é necessário um protocolo de comunicação que defina formas e procedimentos sobre como as mesmas serão enviadas e recebidas e também como a origem e o destino serão identificados. Normalmente utiliza-se um endereço que, naturalmente, precisa ser único, o chamado endereço IP e que está definido no *Internet Protocol* (IP), e que, por sua vez, possui duas versões, o *Internet Protocol version 4* (IPv4) e *Internet Protocol version 6* (IPv6).

Até, aproximadamente, o ano de 2011, o IPv4 era considerado a forma de endereçamento nativa da Internet. Esse endereçamento é realizado através de 32 bits, que resulta em 2^{32}, ou 4.294.967.296 endereços. Esse número pode ser considerado grande, principalmente quando a Internet ainda não era vista como algo comercial e de grande escala como é hoje. Cabe ressaltar que, no início, faixas muito grandes de endereços foram fornecidas às grandes empresas e sem a possibilidade de flexibilizá-las, e isso levou ao desperdício de muitos endereços.

Atualmente, com a evolução comercial da Internet e para a chamada Internet das Coisas (*Internet Things*), na qual muitos dispositivos – celulares, *smartphones*, televisores, câmeras de segurança, lâmpadas, fechaduras, eletrodomésticos – que não tinham acesso à Internet, passaram a ter, sendo assim criada a necessidade de estar conectado ao mundo virtual. Com isso, o número de usuários cresceu consideravelmente e gerou uma necessidade grande de endereços, implicando assim no esgotamento dos endereços IPv4 (ano de 2011). A partir dessa data,

restaram apenas os endereços que os Registros Regionais[1] detêm, e que, segundo estimativas, para o Brasil devem restar endereços para aproximadamente dois anos, prevendo-se assim que os endereços se esgotem, definitivamente, por volta de 2014.

Para solucionar esse problema de limite de endereçamento, foi criado o formato de endereçamento IPv6, que utiliza 128 bits para formar o endereço, resultando em 2^{128} ou 340 undecilhões ($340x10^{36}$) endereços possíveis, quase 80 octilhões de vezes mais endereços que no protocolo IPv4. Com uma capacidade tão grande de endereçamento, o crescimento estará garantido para o futuro, mesmo em ritmo acelerado. No Brasil, através do NIC.br (Núcleo de Informação e Coordenação do ponto BR), desde 2007 existem programas de treinamentos para provedores, gestores de rede e usuários, com intuito de adequar o mercado à utilização do IPv6.

Atualmente, o IPv4 ainda é mandatório na Internet e torna-se difícil determinar quando o IPv6 se tornará a principal forma de endereçamento isso por ainda existir muitos mecanismos que ainda garantem uma sobrevida a ele. Outra questão é relacionada às equipes técnicas que relutam em migrar para o novo endereço, seja por falta de conhecimento ou por dúvidas na migração, nas vulnerabilidades, na coexistência de ambos, nos investimentos em equipamentos novos, entre outros fatores.

A cada dia, essa migração está mais próxima e ela terá que ocorrer, obrigatoriamente, para que a Internet continue crescendo e fazendo parte do dia-a-dia das pessoas e das organizações.

O trabalho aqui apresentado pretende apresentar o IPv6, identificando possíveis vulnerabilidades, apresentar formas de mitigação para as mesmas, colaborando na compilação de conhecimento sobre o IPv6, ao qual, a falta do mesmo é um dos responsáveis pela baixa taxa de adesão desse padrão. As vulnerabilidades tratadas são as que surgem com o novo protocolo; as que existem com a utilização em conjunto do IPv6 com o IPv4, durante o período de adequação, ou mesmo em sistemas que possuem o protocolo IPv6 ativado; as vulnerabilidades já existentes, como vulnerabilidades de camadas acima, como, por exemplo, alçapões e injeção de código malicioso, não serão exploradas, pois como estão

[1] Os Registros Regionais da Internet (*RIR*) são organizações que supervisionam e controlam o uso dos endereços e recursos da Internet. São subordinados ao *Internet Assigned Numbers Authority (IANA)*, que coordena os endereços a nível mundial. O LACNIC é o Registro Regional para a América Latina e Caribe.
No Brasil a organização que desempenha o mesmo papel é o Registro.br, por vez, subordinado ao LACNIC.

relacionadas às camadas de aplicação, não sofrem grandes alterações, exceto pelo fato de que passa a ser mais importante a utilização de mecanismos de controle de acesso e filtragem, pois essas vulnerabilidades passam a ser exploradas mais facilmente com a mudança no modelo de comunicação entre dois pontos na Internet, no qual esses pontos passam a se comunicar diretamente, fim-a-fim, como projetado inicialmente, mas que não foi possível, completamente, pelo uso de mecanismos para contornar o problema da limitação de endereçamento.

O método utilizado será a simulação a ser realizada a partir da criação de um ambiente virtual que permitirá estudar, em cenários presentes nas redes reais, as vulnerabilidades identificadas no levantamento teórico. Através de testes com ferramentas de auditoria de redes, as práticas necessárias para que essas vulnerabilidades sejam mitigadas na migração do protocolo IPv4 para IPv6.

2. LEVANTAMENTO BIBLIOGRÁFICO

Neste capítulo, será apresentada uma base de conhecimento necessária para um melhor entendimento sobre o novo formato de endereçamento que será utilizado no futuro da Internet, o IPv6, bem como o levantamento das novas vulnerabilidades presentes nas redes com endereços IPv6.

2.1 A Internet

No início da Internet, a rede, ainda chamada ARPANET, era composta apenas por quatros pontos interligados e localizados em universidades nos EUA. No contexto da época - Guerra Fria, no caso - a intenção dos militares era manter uma estrutura de comunicação descentralizada, na qual o funcionamento do sistema não dependesse de um elemento central, mas descentralizado onde, em caso de parada de algum elemento, (na época era temido um ataque da aliança soviética), a comunicação poderia acontecer entre os outros elementos que continuariam em funcionamento. Na época, o principal meio de comunicação era o telefone, o qual utiliza uma estrutura de funcionamento centralizada. Nesta estrutura, caso ocorresse um ataque no local onde existisse uma central telefônica, todos os pontos interligados a ela, ficariam sem comunicação, estratégia que poderia ser usada pelos inimigos como forma de ataque. Inicialmente este foi o principal argumento para a criação e manutenção de uma rede descentralizada que, futuramente, seria a principal forma de comunicação de toda uma Era (TANENBAUM, 2003).

Ao longo dos anos, com o crescimento da rede, a Internet passou por mudanças consideráveis, no tocante à importância do que é transmitido por ela e os principais elementos envolvidos na comunicação.

No inicio, os elementos mais importantes eram os computadores. Os primeiros computadores, ainda eram de grandes proporções, tinham o tamanho e o preço compatível com uma instituição de grande porte, como uma universidade, uma base militar ou uma grande empresa. Os usuários mais comuns da rede ARPANET, nessa ocasião eram os pesquisadores, governantes e pessoas ligadas à indústria. Segundo Brito (2013), esse período é denominado *Internet das Máquinas*. Posteriormente, com o lançamento do computador pessoal, o tamanho desses foi muito reduzido, sendo compatível com as residências, mas pelo preço ainda ser alto,

apenas em lares de famílias com poder aquisitivo maior, podia-se encontrá-los, e normalmente apenas um computador. Nesse momento, todas as pessoas utilizavam o mesmo equipamento e mesmo este sendo chamado de pessoal, ele era utilizado por todos e os dados não tinham teor comercial, normalmente educativo e de entretenimento. A Internet comercial, como é conhecida hoje, surgiu no início da década de 1990 com a criação do *World Wide Web (WWW)*. Esses marcos na história da tecnologia fizeram com que a Internet crescesse rapidamente, num ritmo exponencial (COMER, 2007).

Este período durou até o momento de expansão e globalização dos mercados mundiais, em meados da década de 2001, com o desenvolvimento de novas tecnologias, com maior capacidade de processamento e com a redução de preço dos computadores e também de *notebooks*. Nesse momento, o computador se torna muito mais acessível e ao mesmo tempo, surgem as redes sociais, reforçando essa característica mais pessoal, buscando uma identidade no mundo virtual, dessa forma, o elemento importante deixa de ser a máquina e passa a ser as pessoas como elemento central, que interpretam as informações, é a *Internet das Pessoas* conforme Brito (2013), ou a *Web 2.0* (BARBOSA *et al*, 2010).

A principal tecnologia que foi descoberta e desenvolvida nesse período – a nanotecnologia – que permitiu o aprimoramento dos processadores, aumentando a capacidade de processamento e reduzindo o tamanho, foi responsável pelo desenvolvimento de dispositivos móveis, como *tablets*, *smartphones*. Esses dispositivos também favoreceram o acesso mais pessoal, individualizado à Internet (SANTAELLA, 2008).

A partir daí, o estilo de vida das pessoas começa a mudar, sendo criada uma grande necessidade de estar conectado à Internet, de que tudo esteja *on-line*. Muitos dados que antes eram armazenados em discos, *pen-drives*, passam a ser armazenados na Internet, com o conceito de “nuvem” (BESERRA, 2011).

O desenvolvimento da nanotecnologia tornou possível a redução do tamanho dos processadores, que possibilitou a transformação de equipamentos, aparelhos eletrodomésticos e outros aparelhos do dia-a-dia. Esses, que antes faziam apenas suas funções básicas e de forma manual, agora têm a possibilidade de funcionamento automático, ou com controle pelo usuário de forma remota (BRITO, 2013). Conforme Pinheiro (2010), a domótica, que utiliza vários dispositivos, como sensores e módulos de atuação para prover a automação predial, precisam estar

todos em conexão, logo, na rede, cada um deles precisa de um endereço diferente. Podem ser citadas como exemplos, geladeiras que possuem acesso aos provedores de conteúdo e trazem na tela receitas para otimizar o tempo na cozinha, aparelhos de ar-condicionado que podem ser acionados pelo celular, para que o ambiente esteja na temperatura certa quando o morador chegar, câmeras com visualização remota para melhorar a segurança das residências (BRITO, 2013).

Esses elementos que antes não estavam conectados a Internet, precisam de conexão para que seja possível utilizar todos os seus recursos, ajudando as pessoas a economizar tempo em suas tarefas e ter mais praticidade e conforto neste novo estilo de vida. Nesse novo momento, denominado *Internet das Coisas*, ou a *Web²* (ao quadrado) conforme Barbosa *et al* (2010), a necessidade de conexões se torna muito grande, pois tudo precisa estar conectado, seja dentro ou fora das residências e estabelecimentos. Com toda essa necessidade, o modelo de endereçamento usado como padrão, já se esgotou, como previsto, aumentando a necessidade da adoção de um novo padrão que permita conectar um número muito maior de endereços, possibilitando o desenvolvimento dessa rede cada vez mais importante para a vida de todos (BRITO, 2013).

2.2 Segurança da Informação na Internet

No mundo atual, o bem mais importante para as organizações é a informação. Mas para que ela possa agregar valor aos produtos e serviços de empresas, bem como no dia-a-dia das pessoas, é necessário que essas informações estejam seguras. No âmbito da segurança é importante mencionar os riscos que são produtos de uma ameaça para um ativo (aqui, no caso, a informação), que pode ser um concorrente de uma empresa tentando obter a informação de um produto, e uma fragilidade presente no contexto relativo ao ativo, que no caso, pode ser uma falha no desenvolvimento de um sistema que o mantém ativo, por exemplo, um sistema de informação (FONTES, 2008).

Os sistemas possuem diversas fragilidades que são originadas de diferentes formas, podendo ser geradas por fatores externos ou serem intrínsecas do sistema, abrangendo todos os elementos envolvidos no armazenamento, processamento e transmissão da informação, incluindo desde os elementos de *hardware*, *software* e

elementos humanos. A essa fragilidade é dado o nome de vulnerabilidade, à qual está relacionada a uma ameaça, que possui um determinado risco de ocorrer.

Caso ocorra, passa a caracterizar-se como um incidente de segurança da informação. Na maioria das vezes, os incidentes causam perdas, seja ela concreta ou abstrata, como furto de dados, indisponibilidade de serviços, perda de capital financeiro, danos à imagem, entre outros (CICCO, 2008).

Alguns aspectos devem ser considerados no desenvolvimento e manutenção da operação de sistemas de informação para que seja garantida a segurança, (COMER, 2007) como:

1. *Confidencialidade*: que garante que as informações são acessadas apenas por pessoas previamente autorizadas. Em organizações, essas autorizações se dão de acordo com o setor e cargo ocupado. Um exemplo de quebra de confidencialidade seria: um ativo, por exemplo, a folha de pagamento de uma empresa, que a principio, só poderia ser acessada pelo setor de recursos humanos e setor financeiro, um atacante, que pode ser um funcionário do setor de produção, conseguir acessar uma planilha contendo os dados sobre os funcionários e seus respectivos salários, através de uma vulnerabilidade presente no sistema de armazena os arquivos, que pode ser uma falha na configuração do controle de acesso, ele poderia divulgar esses dados para outros e gerar um descontentamento interno.
2. *Integridade*: é o que garante a exatidão das informações e se essas são manipuladas da forma correta de acordo com um controle de mudanças, bem como se estão legíveis. Seguindo o exemplo anterior, o funcionário (atacante), além de conseguir acessar a planilha (ativo), pode alterá-la para que seu próprio salário seja calculado incorretamente. Se o sistema não tiver um mecanismo que verifique o cálculo novamente (vulnerabilidade), o valor incorreto trará prejuízo para a empresa.
3. *Disponibilidade*: é o que garante que um ativo ou informação estará disponível sempre que os autorizados precisarem. Um exemplo de indisponibilidade poderia ser a parada do sistema que armazena a planilha de salários no momento do pagamento dos funcionários da empresa, o que resultaria em atraso e descontentamento.

4. *Autenticidade*: é o que garante que o conteúdo é proveniente da fonte informada. É comum que os mecanismos que garantem a autenticidade, também garantam a integridade, pois, para que realmente seja garantida a fonte, a informação não pode ser alterada sem um controle. Está também relacionada ao aspecto de *auditabilidade*, que garante o rastreamento dos acontecimentos relativos à informação. No exemplo utilizado, seria necessário um mecanismo garantindo que as alterações tivessem a assinatura dos responsáveis por elas.
5. *Irretratabilidade ou não-repudio*: é o que garante a impossibilidade de negação do autor de uma ação. Pode ser relativo à criação ou, normalmente, está vinculada ao controle de mudanças da informação. De acordo com o que foi exemplificado no item anterior, os responsáveis que tivessem suas assinaturas nas alterações, não poderiam negar ter feito tais alterações.

2.3 Arquitetura TCP/IP

Como mencionado anteriormente, hoje a Internet é a forma de comunicação mais utilizada no mundo pela sua facilidade e velocidade.

Aos olhos de um usuário, realmente ela é muito rápida e fácil, mas para que seja dessa forma, existe uma estrutura que é muito complicada, considerando muitos pontos como meios de comunicação, tipos de dispositivos utilizados para conectar, os *hardwares* como servidores, *laptop*, dispositivos móveis, computadores, sendo que cada um utiliza um sistema operacional diferente e os programas e serviços que fazem as comunicações podem ser desenvolvidos de várias formas (TANENBAUM, 2003).

Para resolver um problema muito complicado, normalmente ele é dividido em partes e, no caso do problema "*Redes de Computadores*", ele foi dividido em camadas. À esta divisão inicial foi dado o nome de modelo de referência ISO/OSI, que é um modelo padrão, no qual, cada parte que compõe o modelo, corresponde a uma camada, na qual existe a abstração de um par de elementos de cada lado que se comunicam diretamente. Essa camada se preocupa em receber os dados, processá-los, resolvendo a complexidade da camada em questão e entregar o mínimo possível de dados para a próxima camada (COMER, 2007).

Essa comunicação entre as camadas é chamada de interface. A forma como cada um dos elementos responsáveis por esse processamento é construída, pode ser diferente, basta que esse entregue os dados para a próxima cada, de acordo com um padrão. Esse padrão é o protocolo, que é um tipo de comunicação adotado em cada interface que viabiliza o entendimento entre elas, sem importar como foram implementadas, bem como as características de cada uma, bastando apenas que o protocolo seja o mesmo nos dois lados envolvidos na comunicação (TANENBAUM, 2003).

Esses protocolos são definidos pelo *Internet Engineering Task-Force* (IETF) por meio de *Request for Comments (*RFCs) (IETF, 1999), que consistem em documentos que definem os requisitos para cada elemento envolvido no processo de comunicação. As RFCs são usadas, por exemplo, para a implementação de um novo dispositivo de rede, ou para o desenvolvimento de um *software* que faça envio e recebimento de dados pela rede, assim, elas podem ser consideradas como manuais de implementação dos padrões e protocolos existente, e quem desenvolve, deve utilizá-las como base, pois, estarão "*falando a mesma língua*", possibilitando que qualquer dispositivo ou aplicação construído possa funcionar em conjunto com outro (IETF, 1999).

Nessa estrutura, os dados na origem são inseridos na camada superior e esta, à medida que processa, coloca informações de controle e empacota tudo em novos dados que serão passados para a camada inferior, que fará o mesmo processo, até chegar à camada mais inferior que é responsável pelo transporte físico dos dados até o destino. Ao chegar o processo começa no sentido contrário, pela camada inferior, recebendo os pacotes, retirando as informações de controle relativas àquela camada e passando os dados para a camada superior. Em cada camada esses pacotes de dados podem receber um nome diferente, como quadro, datagrama, de acordo com a arquitetura utilizada, mas como existe a ideia de empacotamento dos dados, comumente é encontrado o termo pacote (TANENBAUM, 2003). A partir desse ponto, este termo será usado para facilitar essa referência.

Como o modelo ISO/OSI é um padrão de referência, existem outros modelos derivados dele, em implementações práticas, como o modelo TCP/IP. Os pares envolvidos na comunicação devem utilizar o mesmo modelo e, portanto, possuem as mesmas camadas. Sendo assim, os pares das mesmas camadas na origem e no

destino, também precisam se comunicar “falando a mesma língua”. Os protocolos também são usados na comunicação entre as camadas. Como as camadas estão todas interligadas e seguem uma ordem formando uma pilha, a todo esse conjunto de camadas e protocolos é dado o nome de arquitetura (BRITO, 2013).

A partir deste ponto, onde é mencionada a arquitetura TCP/IP, entende-se pelo modelo híbrido, conforme Tanenbaum (2003), a fim de facilitar o entendimento, mantendo as camadas do modelo TCP/IP, que é implementado na prática, mas usando uma abordagem que facilita a abstração para os elementos concretos ao qual cada camada se refere. Na Figura 1, seguem os modelos para efeitos de ilustração e comparação, adaptados de TANENBAUM (2003).

Na arquitetura TCP/IP existem camadas – física e enlace – que resolvem a complexidade referente a elementos físicos, como equipamentos de conexão, dispositivos para transmissão, meios de comunicação que podem ser guiados, como cabeamento da rede telefônica, televisão a cabo, fibra ótica; e meios não guiados, como redes móveis através da rede de telefonia celular e redes sem fio (*WiFi*) ou via satélite. Os elementos principais dessas camadas consistem basicamente em componentes eletrônicos, que caracterizam os *hardwares*. Exemplos de equipamentos que funcionam nessas camadas são chaveadores, repetidores, conversores de mídia, moduladores, que são encontrados facilmente no mercado como, respectivamente, *switches*, *hubs*, conversores de fibra ótica, *modems ADSL/CABLE*. Nessas camadas existem protocolos específicos, como o ARP (PLUMMER, 2013), ETHERNET, 1000BASE-SX (BEILI e NETWORKS, 2013) e ATM (SINGH, 2013) (TANENBAUM, 2003).

Outra parte das camadas – transporte e aplicação – tem a finalidade de fazer com que os elementos de *hardware* tenham utilidade, assim como prover alguns aspectos como integridade, segurança, adaptação sobre limitações do hardware, entre outros. Nessas camadas os elementos principais são os *softwares* que podem ser, como exemplos, os que compõem a pilha de protocolos TCP/IP, que normalmente são nativos nos sistemas operacionais atuais. Da mesma forma que nas camadas mais baixas, existem protocolos específicos para essas camadas, como *Transmission Control Protocol* (TCP, 2013), UDP (POSTEL e ISI, 2013), HTTP (FIELDING, 2013), SMTP (POSTEL, 2013) (TANENBAUM, 2003).

Um ponto comum entre todas as camadas, e que é fundamental para a comunicação e no qual todas elas se afunilam, é a camada que cuida do

endereçamento. Nessa camada também existem vários protocolos de comunicação, mas o padrão adotado para a Internet é o protocolo IP (*Internet Protocol*), daí o nome TCP/IP. A Figura 2 ilustra o modelo TCP/IP (híbrido) e o destaque para a camada de rede, a qual faz a fronteira entre os elementos de hardware, normalmente relacionados à infraestrutura de redes (cor verde) e os elementos de *software*, relacionados aos serviços (cor azul) (BRITO, 2013).

Figura 1 - Modelos de arquiteturas.

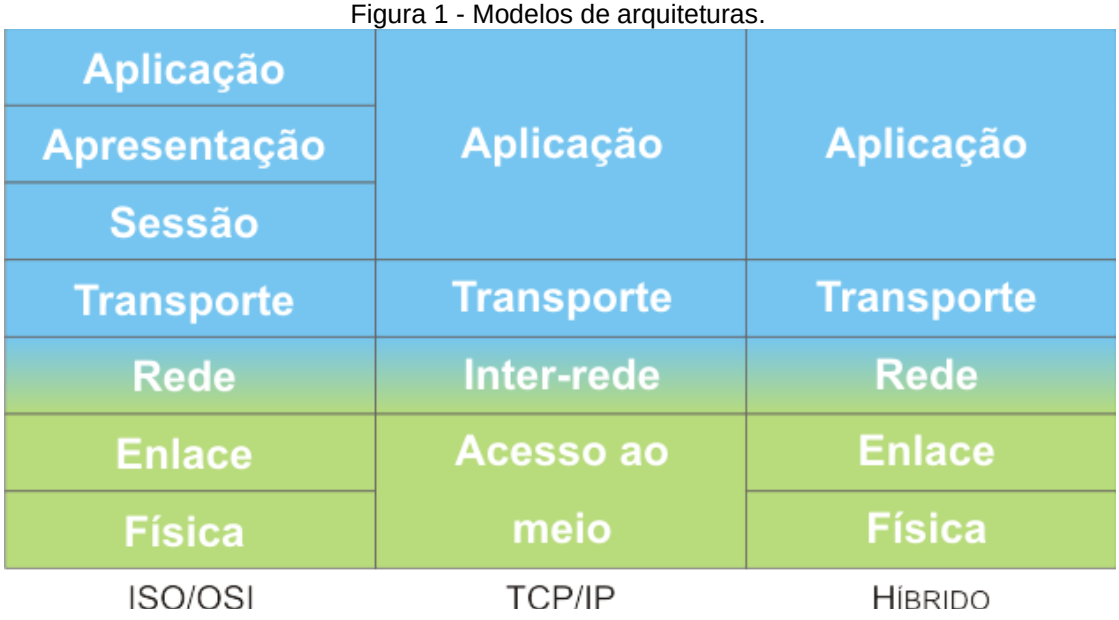
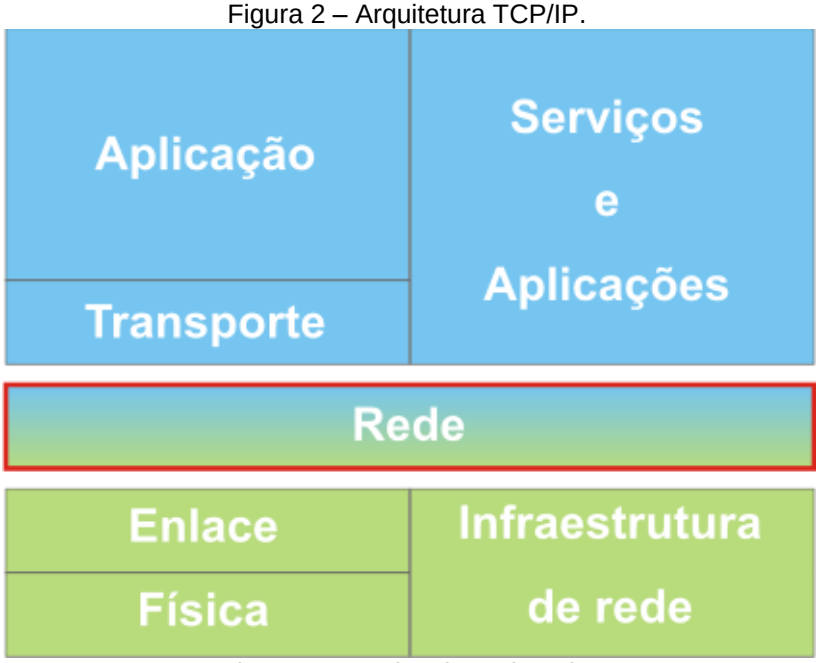


Figura 2 – Arquitetura TCP/IP.



Fonte: (BRITO, 2013), adaptado pelo autor.

Nas especificações desse protocolo, estão previstos vários aspectos e o que é relativo a este trabalho é o endereçamento, que até então se tem como padrão o IPv4.

2.4 Endereçamento IPv4

Assim como todos os moradores de uma cidade têm um endereço único em suas residências, que possibilita receber suas correspondências sem ter problemas de entrega, os usuários da Internet também precisam ter um endereço único, pois, para cada comunicação que se pretende fazer, é necessário estabelecer uma conexão que passa por vários caminhos e para que ela não se perca, é necessário ter um endereço de origem e um de destino.

O padrão de endereçamento para as residências costumam variar de acordo com o país. Se o endereçamento no mundo virtual também variasse dessa maneira, a complexidade da conexão entre um cliente e um servidor em outro país seria um agravante para a velocidade e facilidade que a Internet exige, visto que, por exemplo, uma empresa situada no Brasil pode ter seu site hospedado no exterior e ainda, esse site pode conter elementos que estejam hospedados em servidor de um terceiro país (TANENBAUM, 2003).

Por isso existe um padrão de endereçamento que foi definido na RFC 791, o IPv4, que ainda é mandatório na Internet. Nele está definido que os endereços são compostos por quatro grupos de oito bits, chamados octetos, o que totaliza 32 bits, portanto a quantidade total de endereços possíveis no IPv4 é igual a 2^{32} ou 4.294.967.296 endereços. Excluindo desse número os endereços referentes às dezenas de blocos que foram alocados para grandes empresas antes da existência do CIDR (*Classless Interdomain Routing – RFC 4632*), desperdiçando uma quantidade muito grande de endereços, e também as faixas de endereços reservados para uso especial, o número resultante de endereços disponíveis para alocação é de aproximadamente 3 bilhões de endereços. Na teoria, esse valor já pode ser considerado pequeno, visto que, é estimado que existam aproximadamente 2,4 bilhões de usuários conectados (*Internet World States*, 2012) e até final de 2013, o numero de usuários deve chegar a 2,7 bilhões (ITU, 2013). Na Tabela 1 segue os dados da União Internacional de Telecomunicações sobre o uso da Internet no mundo.

Tabela 1 - União Internacional de Telecomunicações – Indicadores para países desenvolvidos e em desenvolvimento sobre o uso da Internet

	(milhões)								
	2005	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012***	**2013***
Assinaturas de telefones fixos									
Desenvolvidos	570	565	546	544	562	552	542	531	520
Em desenvolvimento	673	696	708	705	691	676	662	655	652
Mundial	1.243	1.261	1.254	1.249	1.253	1.228	1.204	1.186	1.171
Assinaturas de telefones móveis									
Desenvolvidos	992	1.127	1.243	1.325	1.383	1.418	1.475	1.538	1.600
Em desenvolvimento	1.213	1.618	2.125	2.705	3.257	3.901	4.487	4.872	5.235
Mundial	2.205	2.745	3.368	4.030	4.640	5.320	5.962	6.411	6.835
Assinaturas de banda larga móvel									
Desenvolvidos	N/D	N/D	225	336	450	529	683	788	934
Em desenvolvimento	N/D	N/D	43	86	165	249	472	768	1.162
Mundial	N/D	N/D	268	422	615	778	1.155	1.556	2.096
Assinaturas de banda larga fixa									
Desenvolvidos	148	188	219	251	271	291	306	322	340
Em desenvolvimento	71	96	127	159	197	236	282	316	357
Mundial	220	284	346	411	468	527	588	638	696
Uso individual da Internet									
Desenvolvidos	616	649	719	750	773	830	875	913	958
Em desenvolvimento	408	502	645	807	974	1.193	1.398	1.584	1.791
Mundial	1.024	1.151	1.365	1.556	1.747	2.023	2.273	2.497	2.749

Retirado de http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/ITU_Key_2005-2013_ICT_data.xls (10/2013)

Na prática os blocos de endereços são distribuídos e alocados de acordo com o continente e região, através dos RIRs. Portanto, em algumas regiões, que possuem um número maior de usuários, como na Ásia e Pacífico, América do Norte, Europa, o número de endereços disponíveis é ainda menor, sendo que os últimos blocos disponíveis foram alocados para os RIRs em 2011 e no mesmo ano, os estoques do APNIC[2] já se esgotaram. A quantidade de endereços disponíveis por usuários é cada vez menor, considerando que a quantidade de usuários é crescente e a quantidade de endereços IPv4 não pode mais aumentar (BRITO, 2013).

Os endereços IPv4 já teriam se esgotado há vários anos, se não tivessem sido criados alguns mecanismos para contornar o problema, como o NAT (*Network*

[2] APNIC – *Asia-Pacific Network Information Centre*. Registro Regional, subordinado à IANA, responsável pela distribuição e gerenciamento de endereços da Ásia e da costa do Pacífico.

Address Translation), DHCP e CIDR, que possibilitaram que este padrão continuasse em utilização até hoje. (BRITO, 2013)

2.5 Esgotamento dos endereços IPv4

A partir de 1990, iniciaram alguns estudos sobre o esgotamento dos endereços IPv4. Com a exploração comercial da Internet, que se iniciou por volta de 1993, a quantidade de endereços atribuídos pela IANA (*Internet Assigned Numbers Authority*) aumentou consideravelmente e intensificou a discussão sobre o esgotamento dos endereços. Em 1992, o IETF criou o grupo de trabalho *ROuting and ADdress* (RFC 2131) que propôs o desenvolvimento de algumas soluções paliativas para o problema de esgotamento de endereços, na tentativa de minimizar o problema. (BRITO, 2013)

Entre as soluções estão o CIDR (RFC 4632) que põe fim à utilização das classes padrão para atribuição, definindo que nos endereços atribuídos, a parte que identifica a rede e os *hosts*, deixa de ser fixa e passa a variar de acordo com a necessidade do tamanho da rede a ser alocada. Como passa a ser variável, é necessário apontar qual *bit* identifica a rede (prefixo) e a partir deste, identifica os *hosts* (sufixo). Para isso é usado a notação IP/x, onde x representa o bit que faz a fronteira entre a identificação da rede e dos *hosts* (RFC 4632). Com essa definição do CIDR, é possível também diminuir as tabelas de roteamento nos roteadores do núcleo da Internet. Outro problema advindo do crescimento da rede, pois a atribuição dos endereços se torna hierárquica. Sendo assim, não é necessário identificar a rota para uma rede menor, no caso um cliente, atribuída a partir de uma rede maior, no caso um provedor, basta conhecer a rota para este, e o mesmo saberá a rota para o seu cliente, pois o endereço da rede menor é derivado do endereço da rede maior (BRITO, 2013).

Outra solução proposta foi o DHCP (RFC 2131), que permite uma alocação dinâmica de endereços, ou seja, os endereços disponíveis podem ser alocados de forma automática e variável, contendo as informações necessárias para a configuração da rede de acordo com a necessidade. Em conjunto com a outra solução proposta pelo grupo ROAD tornaram-se os principais responsáveis pela utilização do IPv4 até hoje.

A solução proposta foi o NAT (RFC 3022), que possibilita a conexão de vários *hosts* à Internet através de apenas um (ou poucos) endereço público, com a implantação de um dispositivo tradutor na rede, que faz a conversão do endereço do *host* na rede interna, que não é roteável na Internet, portanto privado em um endereço público. Essa conversão é feita com o armazenamento do endereço privado de um *host* que fez uma requisição para Internet numa tabela, a requisição então é feita pelo tradutor, que tem o endereço público em uma das interfaces. Quando recebe a resposta, ele deve entregar para o endereço privado que está na tabela.

Apesar de ser necessário, o NAT possui várias desvantagens. Uma delas é a carga de processamento da tabela pelo tradutor, que pode diminuir o desempenho da rede no caso de muitas traduções simultâneas, outro problema é a quebra do modelo fim-a-fim. A arquitetura original da Internet foi pensada para que todos os *hosts* conectados a ela, possam se comunicar diretamente, escondendo a complexidade intermediária da rede, facilitando a comunicação cliente-servidor. Com essa quebra, algumas aplicações passam a ser inviáveis como aplicações de fluxo, que requerem um bom desempenho, de voz e multimídia e também inviabiliza mecanismos de segurança como o *IPSec* (RFC 4301), além de aumentar a complexidade da rede e afetar aspectos como rastreabilidade (TANENBAUM, 2003).

Outro problema gerado é a sensação de segurança causada pela ocultação da topologia de rede atrás do NAT. Muitos o defendem como ferramenta de proteção e não se preocupam com outras que normalmente são mais eficientes, como um *firewall* com regras bem definidas. O NAT acaba sendo uma proteção por obscuridade, significando que, por esconder, se torna mais difícil de encontrar, mas não impossível de se alcançar. Como o tradutor permite a entrada de uma resposta a uma solicitação da rede interna, existem ataques que são iniciados a partir daí e o atacante consegue invadir, pois essa recepção é permitida como resposta á solicitação da rede interna (BRITO, 2013).

O fato de uma rede estar inteiramente atrás de um dispositivo, não significa que ele a protege, pois logicamente, a rede possui várias conexões externas, mas, fisicamente, está conectada por apenas uma ou algumas conexões (*links*) e é nesse ponto que há a necessidade da existência de dispositivos de proteção como os *firewalls*, pois este pode analisar melhor o tipo de tráfego que pode passar pelo *link*, baseado em regras definidas a partir de uma política de segurança. Para que essa

técnica seja usada e mostre-se efetiva, não há necessidade de que toda a rede interna esteja escondida, ela pode ser bem controlada e transparente, diminuindo a complexidade, facilitando a rastreabilidade e a solução de problemas (BRITO, 2013).

A associação das técnicas de NAT e DHCP possibilitou que os provedores alocassem um endereço público para seus clientes, independente do tamanho de suas redes internas e que esse endereço ficasse alocado apenas enquanto estivesse sendo utilizado, podendo ser alocado para outro cliente posteriormente. (IPV6BR, 2013)

Mesmo com essas soluções, o problema inicial do esgotamento de endereços não seria resolvido, visto que a quantidade de usuários da Internet era crescente, cenário presente atualmente, conforme foi abordado. Para a resolução do problema, o IETF criou em 1992, o *IPng* (IP *Next Generation*), um grupo de trabalho com a missão de desenvolver uma nova versão do IP considerando escalabilidade, segurança, mobilidade, qualidade de serviço e configuração da rede. Depois de algumas propostas, em 1998, foi apresentado como solução, o IPv6 com comunicação fim-a-fim, cabeçalho simplificado, identificação de fluxo de dados, mecanismo de segurança incorporado, configuração automática (IPV6BR, 2013).

2.6 IPv6

O IPv6 é definido na RFC 2460, tomando como base os requisitos da IETF definidos na criação do *IPng*. Algumas características principais que podem ser citadas, além do endereçamento muito maior que o do IPv4, são: (i) cabeçalho mais simplificado e de tamanho fixo trazendo maior facilidade e melhor desempenho; (ii) cabeçalhos de extensão, garantindo uma boa escalabilidade e flexibilidade; (iii) mecanismos de autoconfiguração, que facilitam a configuração e administração das redes; (iv) comunicação fim-a-fim, pois não há mais a necessidade do uso de NAT; (v) protocolo *IPSec* nativo, possibilitando segurança na camada de endereçamento; (vi) identificação do fluxo de dados, melhorando a qualidade de serviço de aplicações.

Nessas características estão presentes vários protocolos, ferramentas e mecanismos novos, e como toda tecnologia nova, gera incertezas, dúvidas e consequente resistência à migração. Mesmo com todo esforço das autoridades de Internet no mundo e nos países, favorecendo a comunidade quanto à documentação

e treinamento, a adoção ainda é pequena, considerando que, pelo esgotamento dos endereços IPv4 em alguns RIRs e o crescimento da Internet, a migração, como foi proposta inicialmente, já deveria estar numa fase avançada. Segundo o NIC.BR, o planejamento era de que, à medida que os endereços IPv4 fossem diminuindo, a adoção do IPv6 iria aumentando junto com o crescimento da Internet, com os dois protocolos sendo utilizados em conjunto, como pilha dupla. Esse início deveria ocorrer por volta do ano 2000 e o período de transição deveria durar de 6 a 10 anos. Mas, ao contrário, está atrasada, os endereços IPv4 estão se esgotando e a utilização do IPv6 ainda é pequena.

Entre todos os blocos já alocados mundialmente, apenas 7,5% são usados efetivamente. Na América Latina, os blocos atribuídos, correspondem a 1,8% dos alocados mundialmente, e desse valor, 36% estão alocados no Brasil, mas apenas 20% são realmente utilizados.

Esse atraso e a pouca adoção e utilização colaboram para a falta de amadurecimento da tecnologia e dificuldade na elaboração de boas práticas que podem ajudar numa migração com menores custos e maior velocidade. Mesmos assim, a migração será necessária e quanto mais ela for postergada, haverá menos tempo para planejamento, aumentando as chances de erros e a existência de vulnerabilidades, afetando a rotina dos usuários e as ameaças para a segurança dos sistemas computacionais (BRITO, 2013).

2.7 Estrutura do IPv6

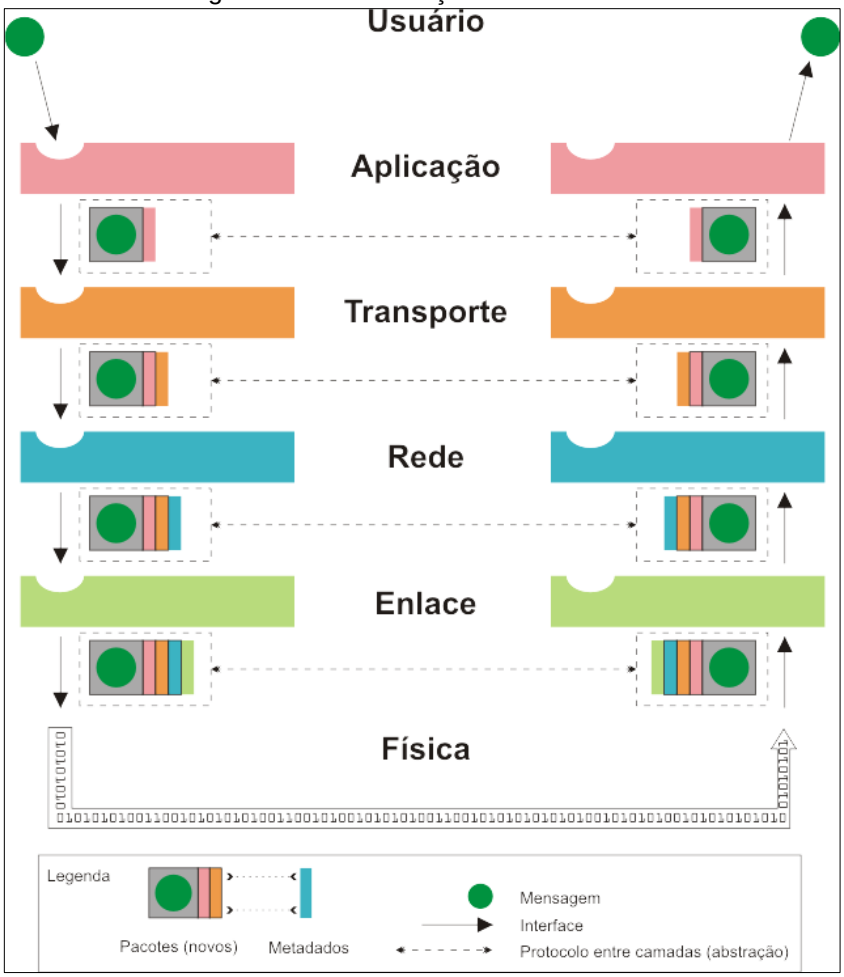
Neste capítulo, serão abordadas as questões técnicas planejadas para garantir os requisitos do projeto *IPng*. Aqui a abordagem será mais aprofundada nas características e funcionalidades referentes ao IPv6.

2.7.1 Cabeçalho

Como abordado anteriormente, na estrutura de camadas, como a utilizada na arquitetura TCP/IP, a comunicação entre elas é feita diretamente, como se não houvesse camadas abaixo destas. Isso se deve à utilização de informações de controle que são denominadas metadados. À medida que os dados são passados para a camada inferior, esses metadados são vistos apenas como dados e

empacotados seguindo o funcionamento da camada em questão e são inseridos nesses novos pacotes, novos metadados. No destino, o processo é o contrário, a camada inferior recebe os dados, desempacota, retira os dados de controle, processa e entrega apenas os dados para a camada superior. Nas camadas, a comunicação é feita através de protocolos e os dados de controle são inseridos conforme um padrão, que recebe o nome de cabeçalho, no qual, as posições, definidas por campos, contém várias informações relevantes ao protocolo e à camada em questão (TANENBAUM, 2003). O processo é ilustrado na Figura 6.

Figura 6 – Comunicação entre camadas

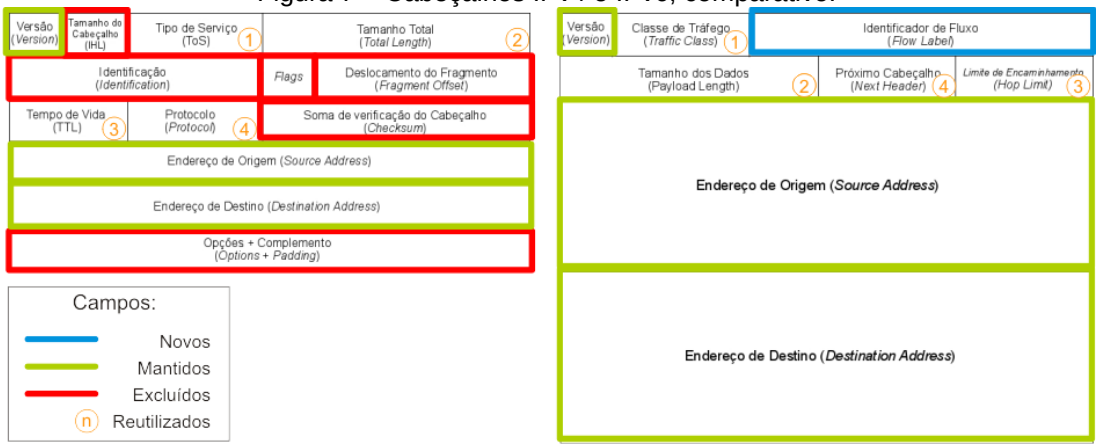


Fonte: TANNENBAUM, adaptado pelo autor.

No caso do protocolo IPv6, em comparação com o IPv4, o cabeçalho, apesar de ser maior, por conta do tamanho dos endereços, 128 bits contra 32 bits no IPv4, o tamanho não varia, o que representa um aumento de desempenho, pois não é necessário verificar o tamanho do cabeçalho, que era variável no IPv4, tornando-o mais eficiente (BRITO, 2013).

Na Figura 7, é mostrada a comparação entre os cabeçalhos do IPv4 e IPv6, com as alterações ilustradas, como é explicado a seguir.

Figura 7 – Cabeçalhos IPv4 e IPv6, comparativo.



Fonte: IPv6.br, adaptado pelo autor.

Com relação aos campos, alguns como o campo “*IHL*” deixam de existir exatamente porque este determinava o tamanho do cabeçalho que no IPv6 é fixo. O campo de “*verificação de erros*” é eliminado, pois em outras camadas essa verificação já ocorreu, sendo desnecessária. Os campos “*identificação*”, “*flags*”, “*fragmentação*” e “*opções*” também foram excluídos, pois foram implementados os cabeçalhos de extensão, permitindo, além dessas funções, a utilização de outras que foram criadas no IPv6 para garantir alguns fatores propostos no projeto, e são indicados no campo “*Próximo Cabeçalho*”, renomeado a partir do campo “*Protocolo*” no IPv4.

Outros campos alterados do IPv4 são “*TTL”*, “*Tamanho Total”* e “*Tipo de Serviço”*. No IPv6 eles recebem, respectivamente, os nomes “*Limite de Hops*”, “*Tamanho do Payload de Dados*” e “*Classe de Tráfego*”.

O campo “*Limite de Hops*” (ou saltos) é usado por uma função que descarta o pacote se esse número chegar à zero, evitando que um pacote “perdido” fique trafegando pela rede. A cada nó que ele passa, o valor é decrementado de 1 e, se ele entrar em um segmento da rede que não consiga sair, por falha na rota ou erro, quando o valor chegar a 0, ele é descartado por exceder o limite de saltos. Esse campo é essencial para que pacotes perdidos não trafeguem desnecessariamente pela rede, diminuindo o desempenho.

O campo “*Tamanho do Payload de Dados*” representa o tamanho da carga de dados depois do cabeçalho principal, considerando neste tamanho, os cabeçalhos de extensão.

O campo “*Classe de Tráfego*” é usado pelos nós e roteadores ao longo do caminho para identificar o tipo e priorizar o tráfego dos pacotes de acordo com esse tipo, desempenhando qualidade de serviço para aplicações que precisam desse tipo de priorização.

Outro campo que está relacionado com a priorização de pacotes é o novo “*Identificador de fluxo*” que associa os pacotes da mesma natureza para que estes possam ser direcionados como um fluxo e não como pacotes isolados. Estas funcionalidades de qualidade de serviço (*QoS*) são úteis para aplicações em tempo real, voz, vídeo, multimídia.

Os campos “*Versão*”, “*Endereço de Origem*” e “*Endereço de Destino*” são mantidos, apenas alterando o valor do campo “Versão” para “0110” em binários (6 em decimal) e os campos de endereços passam a ter 128 bits (IPV6BR, 2013).

No total o cabeçalho tem 40 bytes, o dobro do mínimo do cabeçalho IPv4, mas como esse tamanho é fixo, diminui o custo de processamento, principalmente em dispositivos de rede, que tem capacidades limitadas, aumentando quantidade de pacotes processados e diminuindo o retardo (BRITO, 2013).

2.7.2 Cabeçalhos de Extensão

Como abordado anteriormente, a otimização do cabeçalho do IPv4, foi possível eliminando-se alguns campos que tinham seus espaços reservados, mas eram usados de forma opcional ou que poderiam ser inseridos conforme uma necessidade específica, como identificação. Esses campos tinham seus espaços definidos, e se fosse necessária a implementação de uma funcionalidade nova, esta teria que ser feita através de outro campo, por exemplo, o campo “*Opções*”. Como esse campo é usado opcionalmente, contendo informações auxiliares de outros campos, funcionalidades padronizadas precisariam ter um campo específico para elas, iguais às demais funcionalidades, que se torna inviável pela necessidade de alteração do cabeçalho principal.

Portanto, esse modelo, além de ter campos fixos desnecessários, não tem um mecanismo que garanta a escalabilidade para que no futuro, com uma utilização

maior, as soluções para problemas possam ser adotadas de forma padronizada para garantir o bom funcionamento das redes, a segurança, entre outros aspectos.

No IPv6, essas opções, identificações e controles relacionados às funções complementares foram eliminados do cabeçalho principal e inseridos, juntamente com novas opções, através de cabeçalhos de extensão e são referenciados através do campo "*Próximo Protocolo*". Esses cabeçalhos funcionam em forma de "cascata", sendo que um pode referenciar outro, e esse subsequentemente, até que não haja mais cabeçalhos de extensão. Essa referência ocorre através de um valor que representa cada cabeçalho de extensão.

Então o destinatário do pacote irá verificar as informações de controle contidas nesse cabeçalho, fazem o processamento relacionado, e como nesse cabeçalho também existe o campo "*Próximo Protocolo*", essa sequência é repetida, podendo haver vários cabeçalhos de extensão envolvidos, até que, quando não houver mais nenhum, o valor indica um protocolo como UDP, TCP ou ICMP, que são da camada de transporte, portanto, significa que junto com esse cabeçalho estão os dados que realmente foram transmitidos (BRITO, 2013).

Alguns cabeçalhos e suas funções são: (IPV6BR, 2013)

1. *Hop-by-Hop*: este cabeçalho corresponde ao valor 0 no campo "*Próximo Protocolo*", e é o único cabeçalho que é interpretado por todos os roteadores do núcleo da Internet. Ele é utilizado por recursos que precisam interagir com esses roteadores intermediários, visto que, no IPv6, apenas a origem e o destino são quem processam os pacotes. Atualmente estão definidos dois tipos que são: *Router Alert*, que utiliza o cabeçalho para informações aos roteadores referentes ao roteamento *multicast* e reserva de recursos, através do protocolo MLD (*Multicast Listener Discovery*) e RSVP (*Resource Reservation Protocol*) respectivamente; e *Jumbogram* que são pacotes que podem ser enviados pela rede com tamanho maior que 64KB, normalmente utilizados em redes de alta velocidade. Neste caso, o cabeçalho informa o tamanho do pacote IPv6, para que não haja o descarte do pacote já no primeiro roteador.

2. *Routing Header*: identificado pelo valor 43, inicialmente este cabeçalho (*Routing Type 0*) indicava endereços de roteadores que um determinado pacote precisaria passar ao longo do caminho, determinando previamente

uma rota, similar ao *Loose Source* no IPv4, mas por problemas de segurança foi descontinuado. Atualmente *Routing Type 2* é usado pela solução de mobilidade do IPv6, o MIPv6 que também utiliza um cabeçalho de extensão *Mobility* (código 135), que determina dois endereços para um nó móvel, um sendo um de origem (HoA – *Home-of-Address*), no qual se autentica e outro dinâmico quando esta em trânsito (CoA – *Care-of-Address*), por isso os campos de endereços, que possuem 128 bits, foram reaproveitados desse e de outros cabeçalhos.

3. *Fragment Header*: identificado pelo valor 44, este cabeçalho é usado para vincular pacotes fragmentados pela origem para que o destino consiga recuperá-los. Essa fragmentação é necessária quando é ultrapassado o MTU (*Maximum Transfer Unit*) de um ponto entre a origem e o destino, que é um limite intrínseco da tecnologia em questão. Normalmente ocorre quando há sobreposição de tecnologias, como túneis, protocolos de autenticação, de conexão, quando existe um cabeçalho além do cabeçalho padrão. No IPv4, essa fragmentação era feita pelos roteadores intermediários, que consumia mais processamento destes. No IPv6, quando um pacote ultrapassa o MTU, o roteador sinaliza para a origem, e esta fragmenta os pacotes e mantém o vínculo dos fragmentos através deste cabeçalho para que o destino consiga reconstruí-los.

4. *Authentication Header*: identificado pelo valor 51, esse cabeçalho é parte da solução nativa de segurança do IPv6, o IPSec. Com a utilização desse cabeçalho, é possível garantir a integridade e autenticidade dos pacotes transmitidos. Como esse protocolo funciona já na camada de rede, o nível de segurança é maior do que os protocolos de segurança das camadas acima, como o SSL, por exemplo.

5. *Encapsulation Security Payload*: identificado pelo valor 52 e utilizado também pela solução IPSec garantindo a integridade e confidencialidade dos dados transmitidos, em conjunto com o cabeçalho AH. Essa *suíte* de protocolos será mais detalhada no capítulo sobre segurança.

6. *Destination Options*: identificado pelo valor 60, é usado para prover informações ao destino. Essas informações dependem da aplicação dos pacotes, e podem conter opções que serão processadas pelo primeiro destino, caso o endereço de destino seja um grupo, sendo indicado antes do cabeçalho de roteamento, e pode conter opções para o endereço de destino final, sendo indicado antes do protocolo de camada superior. Atualmente é usado no suporte à mobilidade, transmitindo o endereço de origem de um nó móvel, quando este está fora da sua rede de origem.

Para que o desempenho seja otimizado, a ordem dos cabeçalhos é importante para que os elementos de rede que processam os pacotes, apenas precisem fazê-lo nos cabeçalhos que têm importância para cada um deles, economizando processamento, evitando cabeçalhos que não têm relevância para esses, e passando o pacote para o próximo elemento. No caso do IPv6, a ordem apresentada acima é a recomendada, pois, o cabeçalho *Hop-by-Hop* e processado por todos os roteadores ao longo do caminho e todos os outros são processados no destino.

Como esses cabeçalhos são apontados apenas por um código, se futuramente, houver a necessidade de criar uma nova funcionalidade através de um novo cabeçalho de extensão, basta apenas referenciá-lo no campo "*Próximo Protocolo*" e definir o formato do cabeçalho de extensão. Essa expansão pode ser feita até mesmo de forma experimental, bastando que seja definido um padrão entre as partes envolvidas no teste, já que, com exceção o cabeçalho *Hop-by-Hop*, todos os outros são processados no destino, portanto não implicaria no funcionamento da rede. Depois de testado, seria necessário padronizar o código, a ordem de referência e o novo cabeçalho de extensão numa RFC, através do IETF, como é o procedimento para todos os protocolos.

Essa ferramenta traz para o IPv6, flexibilidade e escalabilidade, que eram aspectos previstos no projeto do IPv6 para a continuidade do crescimento da Internet. Além desses aspectos, como abordado no início desta sessão, o desempenho foi melhorado, pois, eliminou informações desnecessárias do cabeçalho e também, como os únicos que processam os cabeçalhos de extensão são a origem e o destino, retira-se uma carga de trabalho considerável dos roteadores (BRITO, 2013).

2.7.3 Endereçamento

A principal mudança, que está relacionada à principal justificativa do IPv6 é o endereçamento, pois desde 1992 já existem estudos sobre o esgotamento de endereços e limitação no crescimento da Internet.

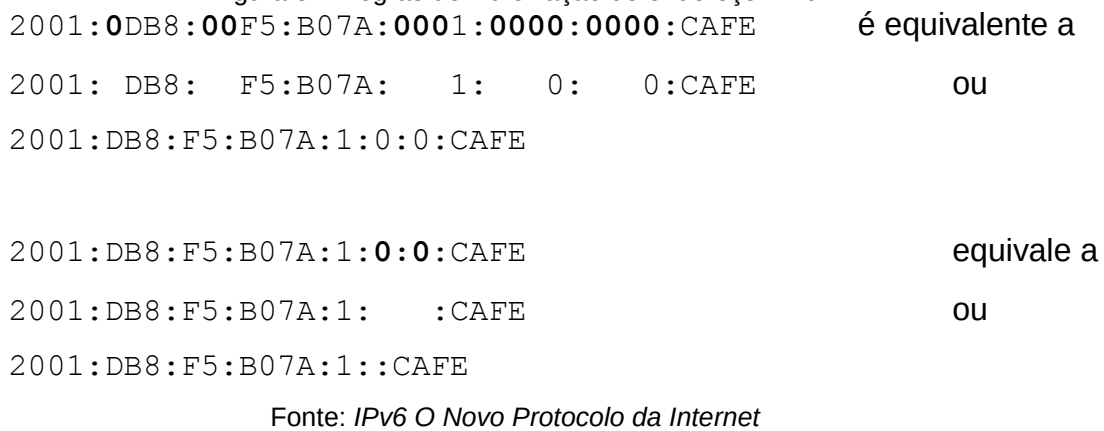
Enquanto o IPv4 utiliza 32 bits, o endereço IPv6 é formado por um endereço de 128 bits, portanto 2^{128} combinações de endereços possíveis. Para efeitos de comparação, um endereço IPv4 possui 2^{32} (4.294.967.296) combinações possíveis. O dobro de 2^{32} é 2^{33} e a cada acréscimo do expoente, o número dobra novamente, portanto a quantidade de endereços IPv6 é astronomicamente maior, difícil de ser assimilada.

Para ilustrar a dimensão desse número, assumindo que a superfície terrestre possui, aproximadamente, 510 milhões de km². Em cada metro quadrado da Terra caberiam, aproximadamente, 155 trilhões de redes IPv4 que possuem mais de 4 bi de endereços cada. Se cada endereço IPv6 ocupasse o espaço equivalente a um milímetro, a quantidade de endereços possíveis seria igual a 340 tri de vezes o diâmetro estimado da Via-Láctea.

Como a quantidade de bits é quatro vezes maior que no IPv4, que usava notação decimal e, em algumas situações, em binário nos endereços, no IPv6, a forma decimal seria inviável, e até mesmo na forma decimal seriam muitos números. Foi adotado o formato hexadecimal, que é representado pelos algarismos de 0 a 9 e letras de A a F, sem distinção entre maiúsculas e minúsculas, facilitando a escrita em oito partes de 16 bits, sendo que cada parte equivale a quatro algarismos hexadecimais (decahexateto). A separação dos grupos, que no IPv4 era feita pelo ponto (.), passa a ser feita pelos dois pontos (:). Como, mesmo com a adoção do formato hexadecimal, o endereço ainda fica extenso, existem regras que permitem abreviar os endereços como as que seguem:

É permitido suprimir o(s) zero(s) em sequência mais a esquerda no grupo. Logo, um grupo composto apenas por uma sequência de zeros pode ser suprimido. Outra regra permite suprimir apenas uma sequência de grupos com valor zero, portanto é recomendado que seja suprimida a maior sequência, representada por "::". Seguem exemplos das regras aplicadas para visualização na figura 8:

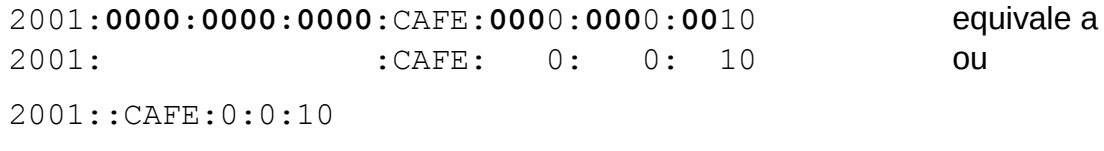
Figura 8 – Regras de Abreviação do endereço IPv6



Fonte: *IPv6 O Novo Protocolo da Internet*

No caso de duas sequências de grupos com zeros, apenas uma delas pode ser suprimida, preferencialmente a maior, podendo ser aplicada normalmente a regra que suprime os zeros à esquerda na outra sequência. Segue o exemplo na figura 9:

Figura 9 - Regras de Abreviação do endereço IPv6 com duas sequências de grupos com zero



Fonte: *IPv6 O Novo Protocolo da Internet*

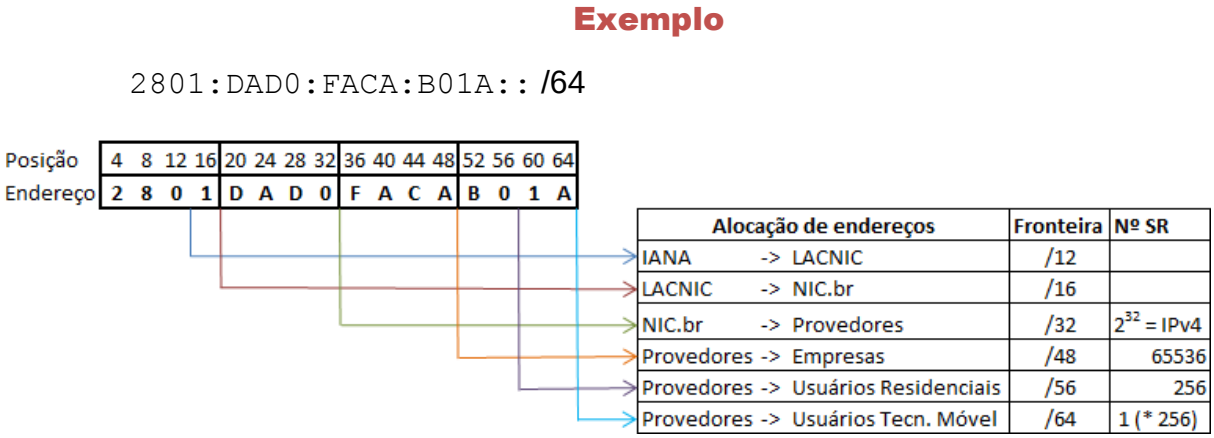
A fronteira entre os bits que identificam a rede e a que identificam os *hosts* é identificada, por padrão, com a notação CIDR, ou seja, o endereço seguido de barra (/) e o número do bit que faz a fronteira. A notação de máscara de rede, como era opcional no IPv4, se tornaria muito extensa, inviabilizando-a. E adotando um padrão, fica mais fácil e menos custoso para usuários e sistemas.

É recomendado que a parte que identifica a rede não ultrapasse /64, sendo assim, basicamente os grupos do endereço IPv6 são divididos em duas partes iguais de quatro grupos, os primeiros têm a finalidade de identificar a rede, e os últimos, identificam os *hosts* (RFC 4291).

Os primeiros quatro grupos também são divididos para identificação dos endereços para alocação dos RIRs e endereços reservados especiais. Os endereços são subdivididos por NICs, por provedores, empresas, clientes e podem ainda ser subdivididos em outras sub-redes. Inicialmente a IANA alocou endereços /12 para os RIRs, que possuem autonomia para planejar a distribuição desses

endereços. Uma recomendação de divisão que é adotada pelo NIC.br é mostrada na Figura 10. Nela são mostrados os 64 primeiros bits de um endereço fictício e as posições que são feitas as divisões em sub-redes, que serão alocadas aos diversos tipos de clientes e organizações (coluna Alocação de endereços, lado direito), os bits que fazem a fronteira entre a rede e as sub-redes, na notação CIDR, e uma coluna (Nº SR) que demonstra a quantidade de sub-redes possíveis, a partir da fronteira até o /64 que delimita a identificação das redes. Nessa recomendação é determinado que usuários de tecnologias móveis recebam redes /64, mas que seja reservado um espaço de rede /56 para uso futuro (* 256) (IANA).

Figura 10 – Recomendações de atribuições de endereço



Fonte: IPv6.br, adaptado pelo autor.

Os últimos quatro grupos identificam os *hosts*. Os protocolos de autoconfiguração, por padrão, utilizam um algoritmo para gerar o endereço do *host* que é baseado endereço físico da interface de rede (*MAC Address*), que em uma rede, pode-se assumir que ele é único. Para a geração do endereço, o *MAC Address*, que possui 48 bits, passa por um processo chamado EUI-64, expandindo-o para 64 bits e resultando em um endereço único, favorecendo a função de mobilidade, que mantêm a parte de identificação do *host* inalterada em qualquer rede que a interface se conectar. Como esse endereço pode ser atribuído manualmente, é recomendado que fosse utilizado um algoritmo que gera um endereço único, para que, o *host* possa conectar-se em qualquer rede sem que haja endereços duplicados, favorecendo assim, a mobilidade (BRITO, 2013).

Com essas recomendações, a quantidade de sub-redes possíveis diminui bastante, e novas comparações são válidas, perante o novo cenário, com uma

distribuição e planejamento melhores para a alocação dos endereços. Considerando apenas um RIR para todo o globo terrestre, que possui endereço /12 e assumindo que nem todos os clientes serão empresas (/48), e também não serão clientes residenciais (/56), assumindo uma fronteira média situada em /52. Assumindo esse valor, ainda restam 40 bits no intervalo para identificação, o que resulta ainda em 2^{40} (1.099.511.627.776) endereços possíveis, 256 vezes a quantidade de endereços IPv4 possíveis. Se a área emersa da Terra, que corresponde a aproximadamente 150 milhões de km², for dividida pelo número de endereços possíveis, resultará em um endereço para cada 136 m², equivalente a um terreno de uma casa popular no Estado de São Paulo. Analisando, esse valor pode se concluir que, em determinada situação ou época, não seja suficiente, mas, no exemplo foram considerados apenas os endereços de um RIR, e no mundo existem atualmente cinco RIRs, lembrando que, apenas cinco blocos /12 foram alocados pela IANA e ainda está disponível, aproximadamente, 500 blocos para alocação futura, concluindo que a quantidade de endereços é totalmente suficiente para a evolução da Internet, mesmo em cenários com distribuições demográficas diferentes.

2.7.4 Tipos de endereços

No IPv6, os endereços podem ser de três tipos, *Unicast*, *Multicast* e *Anycast*. Em comparação com o IPv4, deixa de existir o tipo *broadcast* e passa a existir o tipo *Anycast*, que significa, *um para um de muitos*, e não substitui o tipo *broadcast*. Ele consiste em endereços replicados e distribuídos, para os quais os pacotes são direcionados para os nós de menor custo, melhorando o desempenho e redução de tráfego.

Os endereços *Unicast*, *um para um*, podem ser de outros três tipos, *Link Local*, *Unique Local* e *Global Unicast*. O *Link Local* é um endereço para comunicação apenas em nível de enlace e tem importância na funcionalidade de autoconfiguração e descoberta de vizinhança. Os endereços são iniciados em FE80::/10 e são equivalente aos endereços 169.254/16 no IPv4. O tipo *Unique Local* é equivalente aos endereços privados no IPv4 (192.168/16). Estes são roteados localmente e não são válidos na Internet. Eles são utilizados para o caso de uma máquina na rede local que não necessita ou não pode ser vista na Internet. Esses endereços são iniciados por FC00::/7, divididos em dois blocos FC00::/8 e FD00::/8,

os quais o primeiro é atribuído por uma autoridade e o segundo é atribuído manualmente. E finalmente existe o tipo *Global Unicast*, que são os endereços públicos e roteáveis na Internet, definidos e atribuídos como abordado acima.

O tipo *Multicast*, *um para muitos*, além das primícias de roteamento *multicast*, no IPv6 são usados em grupos *multicast* que tem por finalidade agrupar *hosts* do mesmo tipo ou com mesmas características e serviços. Esses endereços iniciam-se por FF00::/8. Um exemplo de grupo *multicast* é o *multicast-all-nodes* (FF02::1) que representa todos os *hosts* que se conectam na rede. Este grupo substitui o tipo *broadcast* do IPv4, e passa a ser um grupo de *hosts* conhecido que receberão os pacotes enviados a este grupo, evitando tráfego desnecessário pela rede, melhorando o desempenho. Outros grupos *multicast* são utilizados, principalmente, pelas funções de descoberta de rede e vizinhança, como o grupo *multicast-all-routers* (FF02::2), composto por todos os roteadores que ingressam na rede.

No IPv6, um novo tipo de endereços denominado *Anycast* passa a ser adotado. Esse tipo faz a comunicação de natureza *um para um de muitos*, usado no contexto do IPv6 para agrupar diversos *hosts* através do mesmo endereço *unicast*, de forma redundante ou replicada, localizados em locais diferentes. Essa característica faz com que, um cliente localizado em um ponto possa acessar o endereço de destino através de uma rota mais curta para esse cliente, enquanto que, para outro cliente em outra localização, a rota mais curta para o mesmo endereço pode ser outro ponto mais próximo dele, diminuindo a quantidade de saltos, o tráfego na rede e, consequentemente, o desempenho (BRITO, 2013).

2.7.5 Protocolos

Nas redes IPv4 estão presentes vários protocolos na camada de rede e adjacentes como ARP, RARP, IGMP. No IPv6, a maioria deles deixaram de serem utilizadas e suas funções passam a ser responsabilidade de apenas um protocolo, tornando mais simples o seu uso, o entendimento e o gerenciamento. Existe também um protocolo que foi criado para prover a segurança no modelo fim-a-fim da Internet IPv6, o IPSec.

2.7.6 ICMPv6

O ICMP (*Internet Control Message Protocol*) é um protocolo que tem grande importância na rede, pois, possibilita o diagnóstico e informação sobre problemas e erros que podem ocorrer na rede. Com o uso de ferramentas baseadas nesse protocolo, como o *ping* e o *traceroute* é possível detectar se um destino é alcançável, tempo de resposta, distancia de saltos, entre outros parâmetros que são importantes para o funcionamento da rede e detecção e resolução de problemas relacionados.

No IPv6, o ICMP(v6) ganha maior importância no funcionamento da rede, visto que, além das funções de informação e diagnóstico, esse protocolo é essencial para outras funcionalidades como gerenciamento de grupos *multicast* essenciais para o funcionamento de algumas funcionalidades presente no IPv6, mobilidade, que consiste no fato de um nó móvel poder visitar outra rede e ter a mesma identificação associada a ele, descoberta do MTU do caminho (*Path MTU*), no IPv6 a fragmentação não ocorre mais nos roteadores ao longo do caminho e sim na origem, portanto esta precisa saber o valor máximo do MTU para que o máximo de informação chegue ao destino em menor tempo, sem que seja negada por algum roteador num trecho de MTU menor.

Entre todas as funções, a de autoconfiguração e descoberta de vizinhança que funcionam por meio do NDP (*Neighbor Discovery Protocol*) são as que trazem maior nível de complexidade e, portanto, requerem maior atenção quanto às configurações que envolvem o protocolo ICMPv6 e também as vulnerabilidades que passam a existir em decorrência de seu funcionamento (IPV6BR, 2013).

Essas funções resolvem problemas de interação entre os *hosts* vizinhos da rede, fazendo a solicitação e anúncio de vizinhança e roteadores, detecção de endereços duplicados, parâmetros de rede, resolução de endereços físicos (MAC), verificação de atividades na vizinhança, redirecionamento de pacotes, autoconfiguração de endereços. Assim como é considerada uma prática de proteção, por obscuridade, com o uso do NAT, no ICMPv4 essa prática também é comum, normalmente bloqueando totalmente os pacotes nas regras de *firewall*.

No caso do IPv6, o ICMPv6 não pode ser majoritariamente bloqueado, já que algumas funções desempenhadas por ele são cruciais para o funcionamento correto de funções nas redes IPv6, portanto é necessário avaliar melhor as regras que são

configuradas no *firewall* para evitar um mau funcionamento da rede e também para garantir a segurança, considerando que a maioria das vulnerabilidades que surgem com o IPv6, são exploradas a partir das funções do ICMPv6.

O ICMPv6 é identificado no IPv6 por meio do campo "*Próximo Cabeçalho*" com o código 58. Esse cabeçalho tem um formato muito simples, contendo campos tipo e código que definem uma função, um campo de verificação de integridade e um para mensagem.

Segue abaixo as funcionalidades desempenhadas pelo *Neighbor Discovery Protocol* (NDP) (IPV6BR, 2013):

1. *Descoberta de Rede – Roteadores*: A descoberta de redes é uma função de autoconfiguração, na qual o protocolo descobrirá qual o roteador e os parâmetros da rede automaticamente, de forma nativa. Existe um grupo multicast padrão que identifica os roteadores, favorecendo o desempenho. A máquina que tenta ingressar na rede envia um pacote *Router Solicitation* (RS – ICMPv6 tipo 133) para grupo *multicast-all-routers.* Automaticamente, se existir um roteador na rede ele fará parte desse grupo, e responderá com uma mensagem *Router Advertisement* (RA – ICMPv6 tipo 134) com o endereço dele e com as informações sobre a rede, incluindo o prefixo da rede, que será utilizado para obter o endereço unicast da máquina solicitante, juntamente com o sufixo gerado pelo processo de expansão do endereço físico da interface ou atribuído por outro método. Periodicamente o roteador envia essas mensagens para o grupo *multicast-all-nodes*, ao qual pertencem todos os *hosts* que ingressam na rede, para que, se ocorrer alguma alteração nos parâmetros, esses sejam atualizados nos *hosts*. Para esta função, passam a existir algumas vulnerabilidades que podem ser exploradas, por exemplo, a partir de uma falsificação de roteadores na rede, um atacante começa a responder com RA próprio, podendo fazer um ataque de monitoramento de pacotes (*sniffing*) ou um ataque de *homem do meio*, com a possibilidade de interceptar os pacotes que trafegam na rede. Outro ataque, de negação de serviço, consiste na manipulação das mensagens RA para que indiquem um endereço desconhecido ou para que os *hosts* percam a configuração aprendida

anteriormente, anulando a validade do RA, causando um ataque de negação de serviço.

2. *Resolução de Endereços Físicos* : Apesar de existir o endereço IP que é lógico, no nível de enlace, a identificação dos *hosts* é feita através de endereços físicos chamados de MAC. O NDP cuida da associação entre endereços lógicos e físicos, assim como acontecia com o protocolo ARP no IPv4, que deixa de existir no IPv6. A resolução de endereços ocorre através de mensagens ICMPv6 do tipo 135 (*Neighbor Solicitation* – NS) e do tipo 136 (*Neighbor Advertisement* – NA). Uma maquina presente na rede, para conseguir se comunicar diretamente com outra, esta precisa saber o endereço físico desta. Então, ela envia uma mensagem NS para um grupo *multicast-solicited-node* seguido dos 24 últimos bits do endereço IPv6 que deseja saber o endereço físico. Ao receber a mensagem, o *host* vizinho envia uma mensagem NA informando seu endereço MAC. Esse endereço é armazenado pelo sistema operacional em uma tabela *Neighbor Cache*, que posteriormente terá as associações de todos os *hosts* da rede.

3. *Detecção de endereços duplicados*: No NDP existe uma função que garante a unicidade de um endereço *unicast*, seja ele definido de forma automática, dinâmica ou estática. Ela funciona basicamente enviando uma mensagem NS tendo como destino, o endereço que se pretende atribuir à interface. Se existir um *host* com o endereço, este não será atribuído, caso contrário, significa que não existe esse endereço ainda e este pode ser atribuído normalmente à interface. Nessa função existe uma vulnerabilidade que pode ser explorada através de um ataque de negação de serviço, consistindo em enviar resposta NA para todas as mensagens NS recebidas, fazendo com que os dispositivos considerem que os endereços já estão sendo utilizados, impedindo novos dispositivos ingressarem na rede.

4. *Detecção de inatividade dos vizinhos*: Essa função serve para identificar a inacessibilidade de algum nó vizinho. Um nó identifica que um vizinho esta acessível através da confirmação de entrega de algum pacote a esse

vizinho, que pode ser através da resposta NS que deve ocorrer em um intervalo determinado nos parâmetros da rede, informado pelo roteador através de mensagens RA ou através de conexão estabelecida na camada de transporte. Se uma dessas confirmações não for recebida dentro do tempo determinado, o nó é considerado inacessível e a informação é atualizada na tabela *Neighbor Cache*. Essa função é importante para que não haja uma tentativa de comunicação desnecessária para um *host* inacessível, economizando tempo e tráfego na rede.

5. *Redirecionamento*: O redirecionamento é uma função usada pelos roteadores para indicar a um *host* o melhor caminho para um destino. Um roteador, identificando que existe um roteador no mesmo enlace que seja mais apropriado para o destino, envia um pacote ICMPv6 do tipo 137 (*Redirect*) para o *host*. A partir daí, os pacotes seguintes serão enviados para o roteador indicado. Esses pacotes podem ser enviados pelo roteador, também para informar ao *host* que o destino encontra-se no mesmo enlace, para que este possa se comunicar diretamente com o destino, eliminando um tráfego desnecessário no roteador.

6. *Autoconfiguração de endereços*: No IPv6 existe um mecanismo nativo de configuração automática de endereços do tipo *stateless,* ou seja, sem estado ou sem armazenamento de informações, elas são geradas a partir de informações obtidas e atribuídas às interfaces, por isso tem uma natureza automática e independente. Esse mecanismo é responsável pela atribuição dos endereços aos *hosts* ingressantes na rede mesmo sem a existência de um serviço de atribuição de endereços, como o DHCP e sem a necessidade de configuração manual, dada a complexidade do endereçamento e a necessidade de não existir endereços duplicados, bem como o fato de existir uma organização de regras para atribuição de endereços, mesmo no contexto local.

Como abordado anteriormente, os endereços são compostos pelo prefixo, que é obtido dos roteadores através de mensagens RA, e pelo sufixo, obtido através

do processo EUI-64 que faz a expansão do endereço físico da interface para 64 bits e é usado para compor o endereço IPv6 completo (/128) do *host*.

Inicialmente as interfaces recebem um endereço *link-local* (FE80::/64) como prefixo e o *Host-id,* como explicado acima, como o sufixo. Este endereço ingressa nos grupos *multicast-solicited-node* e *multicast-all-node*.

Esses endereços passam pelo processo de identificação de endereços duplicados, e se for encontrada duplicação, este deve ser definido manualmente. Se não, ele é atribuído à interface e é enviada uma mensagem RS para o grupo *multicast-all-routers*. Os roteadores respondem com mensagens RA informando parâmetros como prefixos da rede, rota padrão, MTU, se existem outras configurações de natureza *stateful* que precisam ser aprendidas, como servidores DNS, NTP. E finalmente, o prefixo anunciado é usado para atribuição de um endereço válido para a interface. Se não existirem roteadores na rede, a interface terá apenas o endereço *link-local* que não é válido na Internet.

Nos roteadores, essa função de autoconfiguração só é utilizada para gerar endereços do tipo *link-local*, pois o endereço da rede precisa ser atribuído por uma entidade responsável e configurado por outros métodos, por exemplo, manualmente.

Existe outra forma de atribuição de endereços para os *hosts* da rede, como o DHCPv6 *stateful* que atribui todos os parâmetros às interfaces, assim como no IPv4. Nesse caso, há a necessidade de um servidor responsável pelo serviço, que armazena os endereços cedidos e o endereço físico da interface numa tabela. Os clientes recebem a informação de que a configuração deve ser aprendida através desse serviço, por mensagem RA com essa instrução (BRITO, 2013).

7. *Descoberta do MTU do caminho*: outra função que utiliza pacotes ICMPv6 é o Path MTU Discovery. No IPv6, a fragmentação dos pacotes maiores do que o MTU da tecnologia de qualquer trecho do caminho, necessariamente é feito pela origem, ao contrário do IPv4, no qual a fragmentação de pacotes ocorre ao longo do caminho, feito pelos próprios roteadores. Quando o pacote, com seu tamanho determinado pelo MTU do primeiro salto, chega a um trecho no qual o MTU da tecnologia do enlace é menor do que ele, o roteador descarta e envia uma mensagem ICMPv6 tipo 2 (*Packet too big*) para a origem com o valor do MTU, a qual irá reduzir os pacotes para esse tamanho. Essa

operação pode se repetir várias vezes até que a origem diminua o tamanho do pacote para que ele trafegue por todos os enlaces até o destino.

8. *Gerenciamento de grupos multicast*: o gerenciamento de grupos multicast através do protocolo MLD, equivalente ao IGMP no IPv4, utiliza mensagens tipo 130,131,132 para gerenciar a entrada e saída de nós a um grupo e para localizar nós pertencentes a determinados grupos.

9. *Mobilidade*: a função de mobilidade também utiliza mensagens RA para que roteadores informem que estão operando como Agentes de Origem, que mantém a relação entre a rede de origem e o endereço da rede remota de um nó móvel.

10. *Renumeração de rede*: Como o prefixo dos endereços das redes são baseados no provedor, no caso de troca de provedor, possivelmente haverá a troca do prefixo que, através da função de renumeração de rede pode ser feito com maior facilidade. Essa função utiliza mensagens ICMPv6 tipo 138 (Router Renumbering) enviadas aos roteadores, informando a alteração dos parâmetros, que por sua vez, enviam as novas configurações da rede para os *hosts* através do NDP, com mensagens RA.

2.8 Segurança para redes IPv6

Na criação da ARPANET e no posterior surgimento da Internet, o interesse desses projetos eram apenas viabilizar a comunicação entre os nós, não se atentando a outros aspectos como mobilidade, qualidade de serviço, endereçamento e principalmente com a segurança.

No projeto IPng, o qual deu origem ao IPv6, o aspecto da segurança foi considerado de forma constante e obrigatório. Sendo assim, o IPv6, de certa forma, poderia ser considerado mais seguro do que o IPv4, mas existem fatores como as técnicas de transição, as funcionalidades novas, como a descoberta de vizinhança, o modelo de comunicação fim-a-fim que carregam vulnerabilidades próprias, assim como a falta de conhecimento, maturidade e boas práticas provocadas pela baixa taxa de adoção, comparada com as planejadas no inicio do projeto. Atualmente

esses fatores contribuem para que a adoção do IPv6 seja ainda mais adiada por conta de mitos e equívocos sobre, entre outros aspectos, a segurança do novo padrão de endereçamento da Internet.

2.8.1 IPSec

O IPSec é uma solução de segurança fim-a-fim baseada em criptografia que visa garantir os aspectos de autenticidade, integridade e confidencialidade dos dados que trafegam na rede. Essa solução é oferecida na camada de rede, enquanto que soluções semelhantes, como o SSL (*Secure Socket Layer*), são implementadas na camada de aplicação. Como só a origem e o destino conseguem manipular os pacotes, o ideal é a comunicação fim-a-fim. O fato do IPv6 seguir esse modelo, facilita o uso dessa ferramenta, o que não era viável no IPv4.

No IPv6, o IPSec é nativo, que significa que todos os dispositivos compatíveis com IPv6, automaticamente oferecem suporte à IPSec. Esse suporte oferece ao IPv6 uma predisposição a ser seguro, pois, se em uma rede IPv6 for adotado o IPSec como padrão em todos os dispositivos de uma rede, com certeza todos terão suporte a ele, assim como novos dispositivos que ingressarão posteriormente à rede. O fato de oferecer suporte não significa que o IPSec estará protegendo a comunicação. Pelo contrário, para que ele possa funcionar, é necessária uma série de configurações que o profissional de rede precisa definir e implementar, normalmente a partir de uma política de segurança da informação (BRITO, 2013).

O IPSec funciona com uma configuração de confiabilidade entre as partes que podem ser considerados com uma “conexão” prévia, chamada Associação de Segurança (SA – *Security Association*), na qual são definidos índices e identificadores de segurança que completam os campos dos cabeçalhos de extensão e determinam a autenticidade e a confidencialidade, dependendo da combinação de cabeçalhos utilizados. Essa associação é válida apenas em um sentido da comunicação e é feita através de assinatura digital e criptografia de chaves simétricas.

A criptografia garante a confidencialidade, ou seja, que apenas os pares envolvidos na comunicação terão acesso aos dados. A autenticidade, ou seja, a garantia de que os dados realmente pertencem àquele remetente, é conseguida através da autenticação. A integridade também é garantida através dos mesmos

processos. A criptografia de chaves simétricas possui um desempenho muito maior, comparado com a de chaves assimétricas e por isso é utilizada. Nesse tipo de criptografia, os pares utilizam a mesma chave para criptografar e descriptografar os dados. Essa chave precisa ser trocada na associação e para isso existem métodos seguros de troca de chaves, que é feito através da criptografia de chave pública, o qual, seu gerenciamento das chaves criptográficas é feito através do *Internet Key Exchange (IKE)*. Utiliza-se também métodos de assinatura digital para garantir a autenticidade, que é feito através de *hash* criptográfico (OLIVEIRA, 2012).

O IPSec funciona no IPv6 através de dois cabeçalhos de extensão denominados Authentication Header, com o código 51 no campo “Próximo Protocolo” e *Encapsulation Security Payload*, com código 52 no mesmo campo. O primeiro garante a autenticidade e integridade, mas não utiliza criptografia os dados, que é responsabilidade do segundo cabeçalho, que garante a confidencialidade e também integridade.

O IPSec pode ser implementado através de dois modos, sendo eles, modo transporte e modo túnel. No modo transporte, o cabeçalho principal referencia os cabeçalhos de extensão subsequentes se existirem, ou diretamente os cabeçalhos AH e/ou ESP e estes referenciam o cabeçalho da próxima camada, assim como acontece com os outros cabeçalhos de extensão. Esse modo é utilizado para prover a segurança entre os pontos finais da comunicação. O segundo é o modo túnel, que é usado quando os pontos envolvidos não são os fins, como em VPN´s (*Virtual Private Network*), normalmente implementadas entre *gateways*. Nesse caso todo o pacote é encapsulado em um novo pacote IP (IPV6BR, 2013).

2.8.2 Vulnerabilidades

O NDP no IPv6 traz funcionalidades importantes para o correto funcionamento das redes. Os mecanismos utilizados fazem com que sejam observadas algumas vulnerabilidades.

As mensagens RA e NA que anunciam os roteadores e vizinhos podem ser manipuladas para que os demais acreditem em informações falsas.

Quando um *host* tenta ingressar na rede e frequentemente, para manter uma situação do funcionamento da rede, este envia mensagens NS para todos os *hosts*. Essas mensagens podem ser alteradas para forjar uma informação falsa sobre a

rede, ou para tentar limitar o acesso a ela, se fazendo acreditar que o endereço proposto está em uso. Esse problema abrange qualquer tipo de configuração de endereços, pois, a função de detecção de endereços duplicados (DAD) é executada para qualquer tipo de configuração de endereços.

No caso do roteador, também é possível interceptar as mensagens RA e manipulá-las para tentar bloquear o acesso a Internet, pois as informações são aprendidas pelos *hosts* a partir dessas mensagens.

No caso da descoberta de vizinhança, um dos problemas está relacionado à como essa descoberta é feita, no caso, a partir dos próprios vizinhos, portanto, é necessário que os vizinhos sejam confiáveis. Se isso não puder ser garantido, então é necessária a utilização de mecanismos criptográficos que possam garantir a autenticidade dos vizinhos (IPV6BR, 2013).

Outras vulnerabilidades, que estão presentes nas camadas superiores, continuam ameaçando da mesma forma, exceto pelo fato de, no IPv6, o modelo de comunicação é fim-fim, portanto, algumas vulnerabilidades já presentes, podem ser exploradas mais facilmente, pois o NAT como tradutor, não permite acesso direto da Internet para a rede interna. Nesse modelo, o *firewall* é um equipamento que ganha maior importância, porém ainda não é muito empregado, principalmente em ambientes domésticos e de pequenas empresas (BEZERRA, 2011).

As técnicas de transição, as quais o tunelamento é muito importante para redes em migração, também carregam com si vulnerabilidades. Um exemplo delas é o *Tunnel Broker*, que depende do serviço disponibilizado por terceiros, aos quais é necessária uma boa relação de confiança, pois tudo o que passa pelo tunelamento, se afunila em um ponto que pode inspecionar todo o tráfego de uma rede. Existem também tuneis automáticos que são instalados por padrão em sistemas operacionais, que também podem trazer problemas parecidos. Nesse caso o *firewall* com regras bem definida é um elemento chave na segurança.

Como o IPv6 ainda é novo, portanto não é uma tecnologia madura, como o IPv4, para apontar boas práticas em redes IPv6. O fator humano é um agravante para a segurança das redes IPv6, que pode ser resolvido com informação, treinamento e políticas bem definidas. Na Tabela 2 são mostradas as principais vulnerabilidades em redes IPv6.

Tabela 2 – Vulnerabilidades IPv6

Falha	Ataque	Defesa
Possibilidade de falsificação do Neighbor Discovery	Negação de serviço impedindo obtenção de endereço IPv6 válido	SEND, NDPmon
Possibilidade de falsificação do Router Advertisement	Man-in-the-middle ou negação de serviço por configuração inválida	SEND, RA Guard, NDPmon
Conteúdo exposto e falta de autenticação	Man-in-the-middle ou falsificação de pacotes	IPsec
	Varredura de Rede	Crypto-generated Address
	Varredura de Rede	Unique Local Addresses
	Varredura de Rede	Privacy Addresses
	Varredura de Rede	Grande quantidade de endereços
Utilizar MAC na definição do IP	Rastreabilidade de Dispositivos	RFC4941 (random address) e hash por prefixo de rede
Ignorar ou mal implementar o IPv6	Novidade / Complexidade	Treinamento de equipes
Ignorar ou mal implementar o IPv6	Falta de políticas, treinamentos e ferramentas	Treinamento de equipes
Ignorar ou mal implementar o IPv6	Túnel automático	
Túnel automático	Contornar segurança IPv4	Firewall, desabilitar túneis automáticos
6to4, Teredo	Fake relay, man in the middle	Firewall, Tunnel Broker, Túnel Manual
Falta de Familiaridade com o Modelo Fim a Fim	Ataques diretos a vulnerabilidades	Firewall, IDS

Fonte: IPv6.br

3. DESENVOLVIMENTO

A etapa de testes tem como objetivo observar numa rede implementada, o funcionamento do NDP e as vulnerabilidades, demonstrando os ataques relacionados a elas. O objetivo dos testes é simular uma rede IPv6 e avaliar o impacto das vulnerabilidades existentes, explorando-as e propor uma solução para o problema em questão, para tanto foi criado um ambiente para se realizar tais simulações.

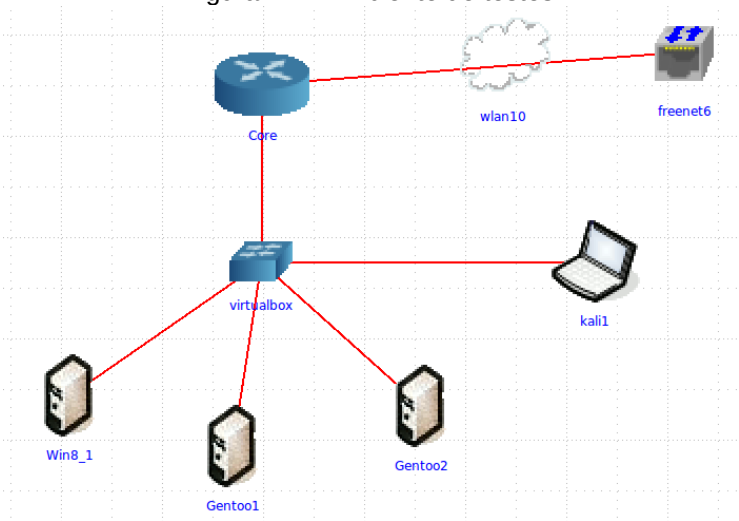
3.1 Descrição do ambiente de teste

O ambiente criado para realização dos testes consiste em um ambiente virtual, implementado através do *software* emulador de máquinas virtuais VirtualBox, o qual é desenvolvido pela empresa Oracle, sob a versão 4.2.12. Foi escolhido este *software* porque é de uso gratuito e sua utilização é muito disseminada, também no ambiente acadêmico, contando com grande disponibilidade de sistemas operacionais prontos para uso como máquinas virtuais (*appliances*). Este *software* foi instalado sobre um sistema operacional *Microsoft Windows 8*, tendo como interfaces de rede uma placa de rede sem fio, que dá acesso à Internet através de roteador e modem ADSL com endereço dinâmico e com IPv4 nativo.

No ambiente virtual, o cenário montado para realização dos testes é apresentado na Figura 11.

Core: é o roteador da rede IPv6. Consiste em um sistema operacional (SO) Linux Ubuntu 11.04, personalizado pela equipe do IPv6.BR, no qual possui a ferramenta *Common Open Research Emulator* (CORE), que é um *software* para simulação de rede de computadores. Nesse roteador existe (i) a interface de rede (eth1) que se conecta ao *switch* virtual emulado pelo VirtualBox que fará o anuncio do roteador para a rede; e (ii) outra interface (eth0) que se conecta à Internet, através da qual será feito o acesso ao servidor Freenet6.net da empresa Gogoc, no qual será montado um túnel para a rede IPv6 (*tunnel broker*). Esta distribuição foi escolhida por ter os serviços relacionados ao NDP já instalados, necessitando apenas da configuração dos mesmos e por ser uma distribuição personalizada para ambientes de testes IPv6. Outra ferramenta instalada é o *software* Wireshark que faz a captura de pacotes na rede.

Figura 11 – Ambiente de testes



Win8_1: *host* virtual com sistema operacional *Microsoft Windows 8* com IPv6 nativo e habilitado com uma interface de rede. Foi escolhido para o ambiente de testes porque a maioria das redes existentes possuem computadores que utilizam o SO.

Gentoo1 e *Gentoo2*: *hosts* virtuais com o sistema operacional *Linux Gentoo* com IPv6 nativo e habilitado com uma interface de rede cada. Foi escolhido o sistema operacional para efeitos de testes com outros *hosts* na rede e não requer muitos recursos de hardware para execução.

Kali1: *host* virtual com sistema operacional Linux Kali 1.0.2 com IPv6 nativo e habilitado com uma interface de rede. Este terá o papel de atacante e foi escolhida esta distribuição por conter uma grande variedade de ferramentas para ataques e auditoria de redes, portanto, não é necessária a instalação de tais ferramentas. É uma distribuição baseada no *BackTrack* e que é muito conceituada na área de *Penetration Test* (Pentest) e auditoria.

Wlan10: rede física existente no local de execução dos testes com a topologia básica com acesso à Internet contendo modem ADSL, roteador com NAT sem encaminhamento de portas e sem DMZ configurada, *Firewall* do tipo *statefull* habilitado e DHCP. O *link* de Internet dispõe apenas de IPv4.

3.2 Configuração e preparação

Inicialmente, o roteador precisa receber algumas configurações para conexão com o *tunnel broker*. Para realizar esta conexão foi necessário efetuar um cadastro

no site da empresa responsável pelo *tunnel broker*, instalar o cliente de conexão disponível no site e configurar as opções no arquivo "*/usr/local/gogoc/bin/gogoc.conf*", alterando os campos "*userid*", "*passwd*", "*server*" e "*auth_method*" (conforme cadastro no site), os campos "*host_type*" (como "*router*", pois a interface será usada para roteamento do tráfego IPv6) e "prefixlen" (com o tamanho do prefixo de rede, no caso, "64") e o campo "if_prefix" (com o nome da interface que anunciará o roteador para a rede, no caso, "eth"), como mostra a Figura 12.

Figura 12 – Configuração do *tunnel broker*

```
userid=<cadastrado_no_site>
passwd=<cadastrado_no_site>

server=<anonymous.freenet6.net>
auth_method=<anonymous|any>

host_type=router
prefixlen=64
if_prefix=eth1
```

Foi necessário configurar o serviço RADvd, responsável por responder às solicitações de RS na rede e fornecer as informações de prefixo de rede. Para isso é necessário editar o arquivo "*/etc/radvd.conf*", conforme a Figura 13.

Figura 13 – Configuração serviço RADvd

```
interface eth1 {
 AdvSendAdvert on;
 AdvOtherConfigFlag on;
 MinRtrAdvInterval 30;
 MaxRtrAdvInterval 300;
 AdvLinkMTU 1280;
 prefix 2001:5c0:1101:ef00::1/64 {
      AdvOnLink off;
      AdvAutonomous on;
      AdvRouterAddr on;
      AdvPreferredLifetime 91;
      AdvValidLifetime 121;
      };
 };
```

Nesse arquivo é necessário configurar o nome da interface que fará os anúncios para a rede, no caso "*eth1*", e o prefixo informado no cadastro feito no site Freenet6. Este prefixo é válido na Internet e será distribuído na rede interna virtual para os *hosts*.

Como o Linux não se comporta por padrão como um roteador, foi necessário habilitar o encaminhamento de pacotes entre sub-rede, editando o arquivo "*/proc/sys/net/ipv6/conf/all/forwarding*".

Em sequência, foram executados os serviços RADvd ("*/etc/init.d/radvd start*) e executado o processo "gogoc" para efetivar o túnel ("*/usr/local/gogoc/bin/gogoc*").

Após a conexão, é criada uma interface "*tun*" que corresponde a uma das pontas do túnel entre o roteador e o servidor Freenet6, e a interface "*eth1*" recebe um endereço IPv6 válido (tipo *Global Unicast*), como na Figura 14.

Figura 14 – Conexão de rede "eth1"

```
eth1      Link encap:Ethernet  HWaddr 08:00:27:21:dd:31
          inet6 addr: fe80::a00:27ff:fe21:dd31/64 Scope:Link
          inet6 addr: 2001:5c0:1101:ef00::1/64 Scope:Global
```

3.3 Execução dos testes – Ataques

Os seguintes ataques foram executados no ambiente de teste, com a descrição sobre como foram realizados.

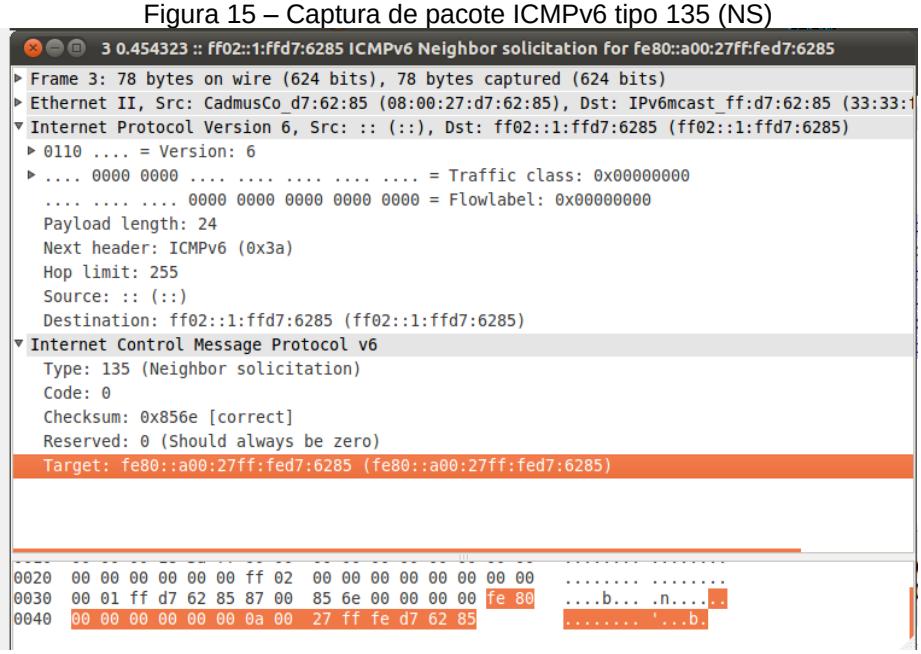
3.3.1 Negação de serviço com DAD

Esse ataque consiste simplesmente em responder a todas as solicitações NS (*Neighbor Solicitation*), que são feitas no momento que o *host* ingressa na rede, com uma resposta NA (*Neighbor Advertisement*). Nesse momento, sua interface não tem nenhum endereço e é enviada uma mensagem NS com o endereço que será configurado na interface. O atacante automaticamente responde essa mensagem, e o *host* admite que já possua esse endereço na rede, portanto, o endereço não é configurado e o *host* não ingressa na rede.

No ambiente de teste o ataque foi feito a partir da maquina virtual Kali1 usando a ferramenta *dos-new-ip 2.0* do projeto *The Hackers Choice* (HAUSER, 2013). No roteador Core é executado o *software Wireshark* (COMBS, 2013) "ouvindo" os pacotes na interface da rede interna *VirtualBox*.

Na inicialização do *host* Gentoo1, o endereço IPv6 foi atribuído normalmente à interface de rede, que pode ser observado na Figura 15.

Figura 15 – Captura de pacote ICMPv6 tipo 135 (NS)

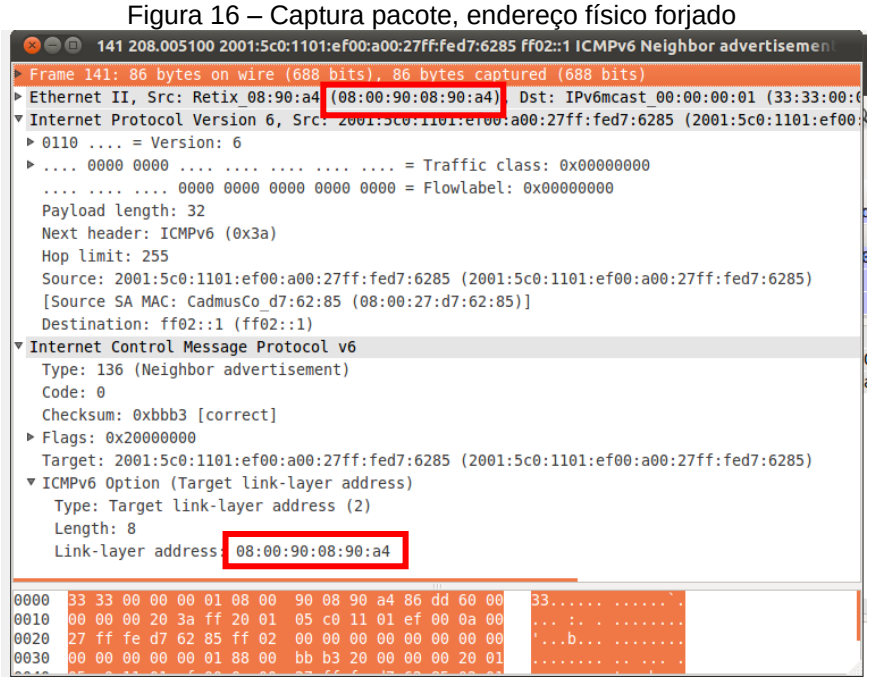


Para monitorar o tráfego na rede é executado o comando *ping* como destino o endereço "*2001:4860:4860::8888*" (servidor DNSv6 da empresa Google), obtendo resposta normalmente, no *host* Gentoo1.

É iniciado o ataque executando o comando "*dos-new-ip6 eth1*" na máquina Kali1.

A resposta continua normalmente no *hos*t Gentoo1 até ser enviada na rede uma mensagem NS que é respondida. Logo em seguida a resposta do comando *ping* é interrompida. Segue na Figura 16, o pacote capturado com endereço físico falso.

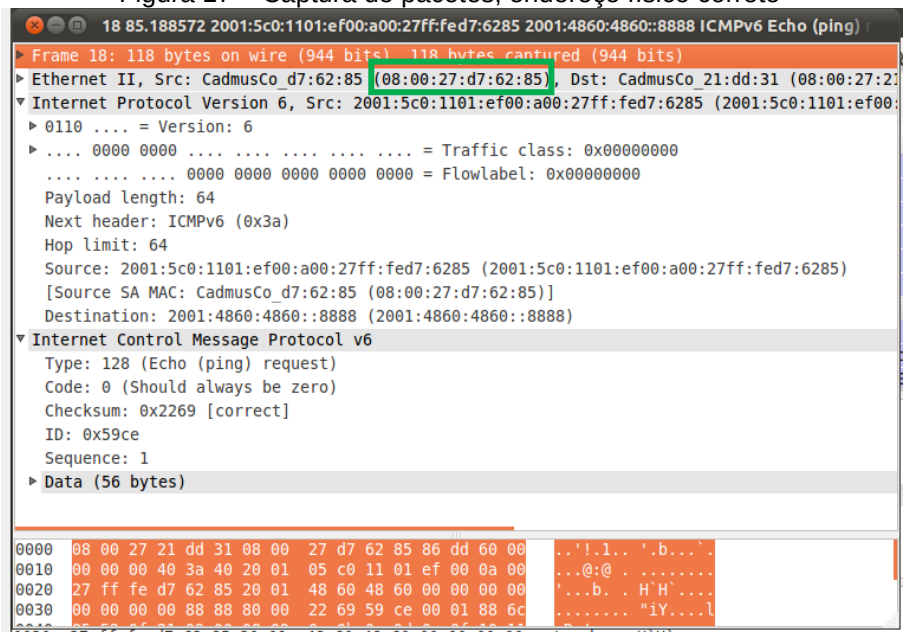
Figura 16 – Captura pacote, endereço físico forjado



O *host* Gentoo1 não perde sua configuração de endereço *Link-Local*, mas não é mais possível a comunicação com nenhum endereço na rede. O *host* Gentoo2 é iniciado e não acorre a atribuição de endereço IPv6 a ele, portanto, também não é possível se comunicar na rede.

Após o encerramento do processo que executa o ataque "*dos-new-ip6*", a resposta do comando *ping* é restabelecida, como mostra a Figura 17.

Figura 17 – Captura de pacotes, endereço físico correto



O endereço é atribuído ao *host* Gentoo2 e este ingressa na rede.

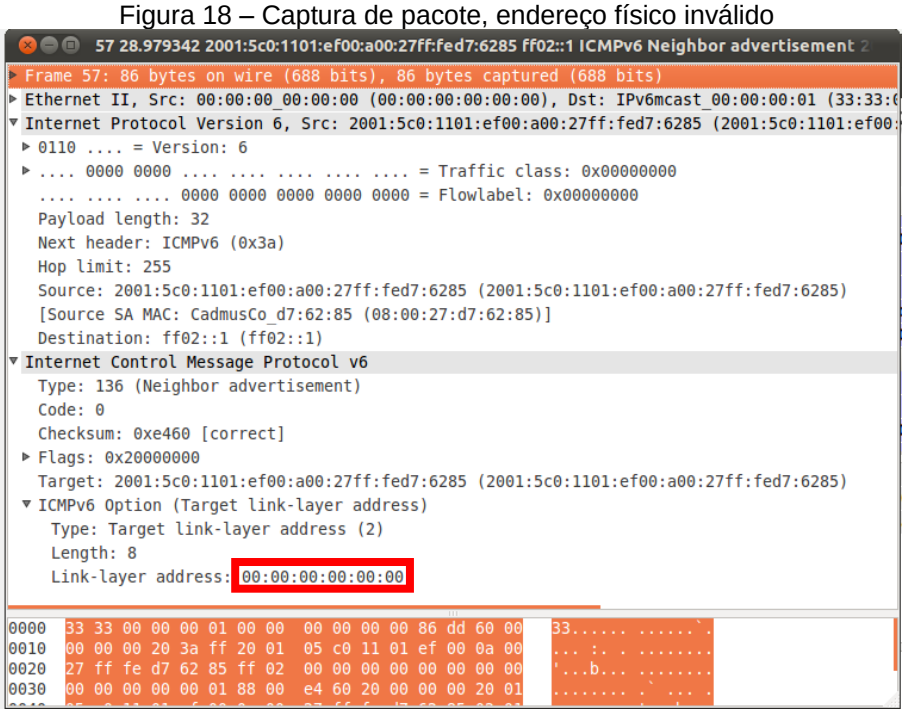
3.3.2 Envenenamento das tabelas de vizinhança

Esse ataque consiste na geração de muitas mensagens NA com endereços forjados com o objetivo de acrescentar entradas alteradas pelo atacante, com finalidade de escuta de tráfego. Esse ataque pode ser considerado também de negação de serviço, pois, aumentar o tamanho da tabela de vizinhança, que pode ocasionar o estoura do cache da tabela em dispositivos e aumentar o tempo para pesquisa de *hosts* autênticos, além de aumentar o tráfego na rede, pois se trata de um ataque de inundação.

No teste foi utilizada a ferramenta "*fake_advertise6*" que envenena as tabelas de vizinhança com mensagens NA com um endereço existente na rede, ao qual se deseja atacar, e um endereço físico no qual será feita a escuta do tráfego. Existe a opção de usar um endereço físico inválido, como na Figura 18.

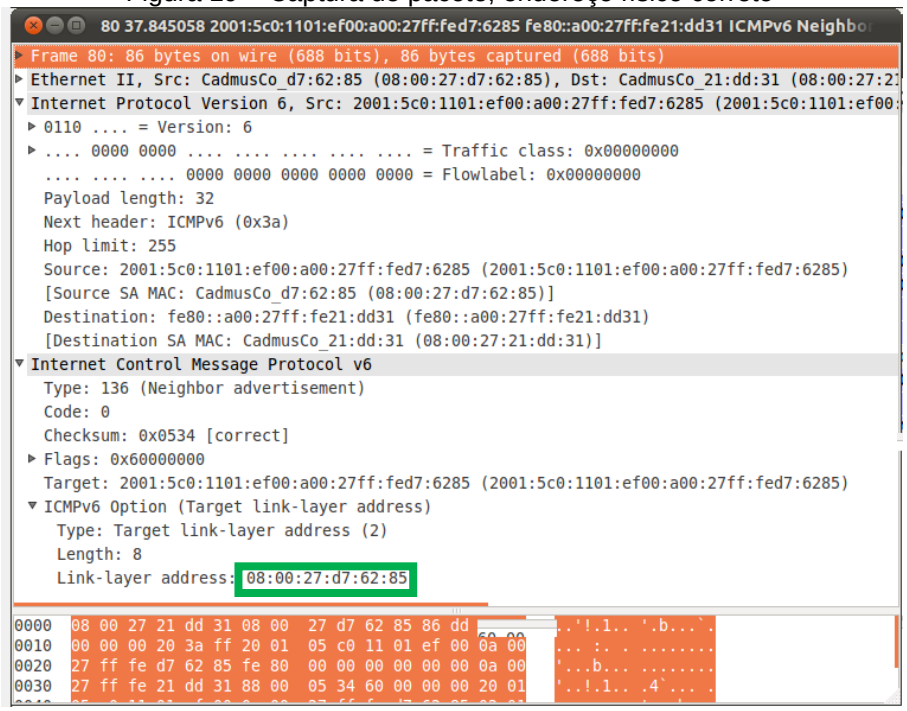
Foi executado o processo tendo como alvo o *host* Gentoo1, que no teste de *ping* com um endereço externo, apresentou grande quantidade de perda de pacotes, enquanto que o *host* Gentoo2 estava respondendo normalmente.

Figura 18 – Captura de pacote, endereço físico inválido



Encerrando o programa atacante, a resposta do *host* volta ao normal, como observado na Figura 19.

Figura 19 – Captura de pacote, endereço físico correto

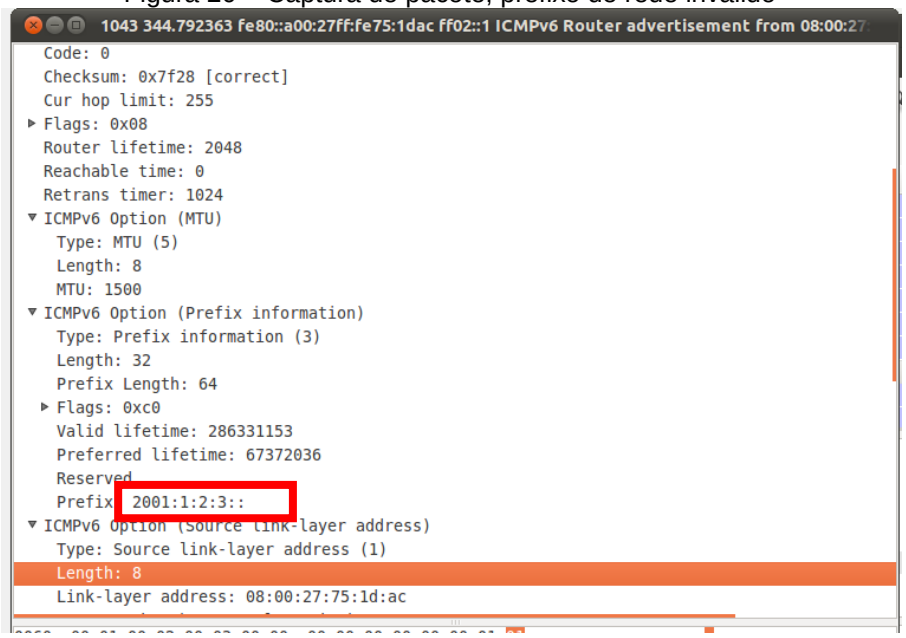


3.3.3 Falsificação de roteadores

Esse ataque consiste na falsificação de mensagens RA, enviadas pelos atacantes com os objetivos de (i) assumirem a posição de roteador da rede, possibilitando a interceptação do tráfego, caracterizando um ataque de homem-do-meio (*man-in-the-middle*); (ii) forjar um prefixo falso, impossibilitando o roteamento entre as sub-redes e, consequentemente, o tráfego, caracterizando um ataque de negação de serviço; e também (iii) zerar a validade das mensagens RA dos roteadores autênticos, fazendo com que os *hosts* percam suas configurações sobre a rede, como, por exemplo, o prefixo.

Foi utilizada a ferramenta "*fake_router6*" e um prefixo de rede inválido. A partir da descoberta da rede através das mensagens RA, os *hosts* aprendem os novos endereços e passam a fazer parte dessa sub-rede inválida, conforme a Figura 20, por isso não consegue acessar a Internet.

Figura 20 – Captura de pacote, prefixo de rede inválido



3.3.4 Pilha dupla nos sistemas operacionais

Nos testes, foram observados que todos os *hosts* envolvidos possuíam as duas pilhas de protocolo e que estavam habilitadas por padrão.

Na inicialização dos respectivos sistemas operacionais, o endereço *Link-Local* foi atribuído conforme o padrão, e na inicialização do roteador Core, ocorreu a

atribuição dos endereços IPv6 automaticamente, de acordo com o funcionamento do mecanismo de descoberta de rede.

3.3.5 Mecanismos de tunelamento

Nos testes, foi utilizado um túnel através de um NAT e um *Firewall* simples ativado, do tipo *stateful*, disponível no roteador de Internet. O roteador é uma solução completa com modem ADSL e roteador sem fio num único equipamento da marca ZTE, modelo ZX V10 W300. Mesmo o ambiente utilizando maquinas virtuais, a conexão com o túnel pela Internet, era feita através de uma rede física utilizando apenas IPv4.

O túnel foi estabelecido sem qualquer alteração na configuração do roteador.

4. DISCUSSÃO DOS RESULTADOS

4.1 Negação de serviço com DAD

O ataque teve eficiência e impediu que os *hosts* ingressassem na rede. Embora o ataque cause uma negação de serviço, mantendo os *hosts* inacessíveis, essa ferramenta se baseia no envenenamento das tabelas de vizinhança, enviando um endereço físico inválido (Figura 16) na mensagem NA. Dessa forma, o ataque não impede que o endereço *Link-Local* seja atribuído, fazendo com que a vítima acredite que ingressou na rede e que o problema pode ser outro, por exemplo, no roteamento.

O ataque não começa a surtir efeito imediatamente ao se executar o processo, mas sim, quando algum *host* envia uma mensagem NS, que é feito com uma periodicidade por causa do recurso de identificação de atividade da vizinhança. Sem que a vítima que tenta ingressar consiga se comunicar na rede, não consegue obter o prefixo da rede e, portanto, não é atribuído um endereço *Global-Unicast*.

4.2 Envenenamento das tabelas de vizinhança

A ferramenta é funcional e possui grande variedade de aplicação. O ataque foi efetivo, mesmo tendo um caráter de negação de serviço. O ataque pode ser realizado com intuito de “escutar” o trafego destinado a um *host*, desviando o tráfego para o atacante, como um ataque de homem-do-meio. Uma solução para o problema de relação de confiança entre os vizinhos é a utilização de endereços gerados criptograficamente (CGA) que utiliza o sistema de chaves públicas para a geração dos endereços, porém, possui uma implantação mais trabalhosa.

4.3 Falsificação de roteadores

As validades das mensagens possuem um valor alto, e os *hosts* aprendem essa nova rede, assumindo endereços relativos a essa. A ferramenta envia, além do prefixo da rede, outras informações como servidores DNS. Essas informações também podem ser forjadas para incrementar um ataque de interceptação. O simples fato de anunciar uma nova rede, que provavelmente será inválida já

caracteriza um ataque de negação de serviço grave, pois afeta o acesso a Internet de toda a sub-rede que depende do roteador.

Existem *switches* com uma funcionalidade chamada RAguard que consiste em determinar a porta que o roteador está conectado e permitir o envio de mensagens RA apenas por essa porta, bloqueando o envio nas outras portas.

Uma prática comum é a utilização do DHCPv6 para gerenciar os endereços na rede, mesmo que represente a perda da facilidade da autoconfiguração.

4.4 Pilha dupla nos sistemas operacionais

Os sistemas operacionais atuais, além de possuírem suporte ao IPv6, trazem a pilha de protocolo habilitada por padrão. Como a maioria das redes atuais possuem apenas endereços IPv4 e, portanto, a segurança está concentrada ou apenas é suportada para IPv4, um atacante executando um ataque de falsificação de roteador pode forjar uma rede IPv6 e conseguir acesso aos *hosts*.

No caso de sistemas que não utilizam o IPv6, é recomendado desativar a pilha de protocolos para que não haja tráfego desnecessário ou mal intencionado na rede. Nos sistemas que utilizam a Internet IPv6 nativamente ou parcialmente, os esforços devem ser concentrados no intuito de resolver os problemas referentes ao NDP, que desempenha um papel de muita importância na rede e, por isso, quando são atacados, o impacto é considerável. É necessária a viabilização de mecanismos de defesa, que tenham uma implantação menos problemática.

4.5 Mecanismos de tunelamento

Como os túneis são mecanismos de transição entre IPv4 e IPv6, existem vários serviços que possibilitam diversas técnicas de tunelamento, incluindo técnicas que passam por tradutores de rede (NAT) e *firewalls* simples, normalmente encontrados em formato de *appliances* em residências e pequenos negócios. Um atacante conseguindo ativar um túnel dentro de uma rede IPv4 e que possui *hosts* em pilha dupla, contorna a segurança do perímetro da rede e consegue acesso a partir de um *host* mais vulnerável.

O cenário enquadrou-se numa situação de tunelamento e que pode ser implementada na maioria das residências e negócios de pequeno porte que

possuem equipamentos de rede do tipo apresentado no parágrafo anterior. Esse cenário trás vulnerabilidades, pois se um processo sendo executado na rede interna conseguir estabelecer um túnel e atuar como roteador IPv6, este disponibilizará um endereço *global-unicast* para os *hosts* que trabalham em pilha dupla. Com o modelo fim-a-fim do IPv6, esses *hosts* estariam acessíveis na Internet. Como (i) a segurança na instalação de *softwares*, (ii) a configuração do *firewall* presente no SO, (iii) a falta de *softwares* antivírus eficazes não são práticas comuns entre os usuários, outras vulnerabilidades, principalmente as de camadas acima da rede, podem oferecer grande risco aos sistemas.

5. CONSIDERAÇÕES FINAIS

A partir do levantamento bibliográfico foi possível apresentar o IPv6 baseado em materiais do principal órgão relacionado à gerência de Internet e ao IP da próxima geração e também de fonte certificada em IPv6 no Brasil. Esse levantamento resultou numa síntese dos principais pontos sobre os aspectos relacionados ao funcionamento do IPv6 e suas vulnerabilidades, que visa colaborar para a disseminação de conhecimento a respeito do IPv6. Através dos testes executados foi possível observar o funcionamento do mecanismo de descoberta de vizinhança e apontar as vulnerabilidades que acompanham esse mecanismo. Ao mesmo tempo foi possível, através do ambiente criado, a observação do mecanismo de tunelamento usado na migração e coexistência das redes.

As vulnerabilidades advindas do IPv6 oferecem grande risco de serem exploradas com conhecimentos e ferramentas largamente difundidos. Essa exploração pode resultar num grave incidente, colocando em risco o funcionamento das redes, considerando, principalmente, os aspectos de disponibilidade e confidencialidade. Faz-se necessário o aprimoramento de mecanismos que estabeleça a confiança entre os vizinhos nas redes, preferencialmente através de recursos criptográficos, que são mais seguros e garantem a autenticidade dos envolvidos. Ao mesmo tempo é necessário o aprimoramento dos mecanismos de detecção e prevenção a esses ataques através de ferramentas de monitoramento das mensagens de controle relacionadas ao protocolo de descoberta de vizinhança, com a possibilidade de validação das mensagens e anúncios feitos pelos *hosts* da rede.

Entre as técnicas de coexistência, o tunelamento possui vulnerabilidades que não podem ser testadas e confirmadas, pois a infraestrutura pela qual este túnel é estabelecido é de natureza privada e não é possível determinar se há algum tipo de interceptação ou ação que infrinja os aspectos de segurança. Essas vulnerabilidades são inferidas a partir de práticas comuns de servidores virtuais relacionados, principalmente, a serviços gratuitos na Internet. Mecanismos criptográficos, como o IPSec em modo transporte, podem ser adotados nessa situação a fim de diminuir as chances de interceptação do conteúdo.

Na utilização de *host*s que possuem redes em pilha dupla, as falhas normalmente ocorrem a partir do suporte nativo dos sistemas operacionais mais

modernos. É necessária uma conscientização sobre a utilização da mesma, pois, se a rede não possui IPv6, é aconselhável desabilitar a pilha referente a este no SO, para evitar que possíveis ataques contornem a segurança implementada sobre o IPv4. Se realmente a rede utilizar o IPv6 em conjunto com o IPv4, é necessário que a segurança abranja ambos. Nesse ponto, deve haver uma conscientização da importância de aplicações de *firewall*, sendo executadas, inclusive nos computadores, na tentativa de cultivar uma prática parecida com a que é cultivada para os *softwares* antivírus, pois usuários domésticos nem sempre dão a devida importância ao *firewall* nativo dos sistemas operacionais e muitas vezes este é entendido como um problema, principalmente quando há a falta de conhecimento sobre o mau funcionamento de algum recurso.

Para contribuir com a minimização de tais vulnerabilidades, alguns trabalhos podem ser desenvolvidos futuramente, abordando questões sobre:

- Novas formas de estabelecer confiança entre os vizinhos da rede
- Utilização de terceiros para estabelecer essa confiança
- Encriptação de mensagens de controle
- Mecanismos de detecção e prevenção de ataques relacionados ao mecanismo de descoberta de rede
- Utilização de criptografia de forma amigável ao usuário
- Desenvolvimento da inteligência de *softwares* de filtragem (*firewall*), detecção e prevenção de ataques (IDS/IPS)

REFERÊNCIAS

BATHRICK, G. *et al*. **Definitions of Managed Objects for the ADSL Lines RFC 2662** – Disponível em < http://tools.ietf.org/html/rfc2662 > - Acessado em 20 de setembro de 2013.

BARBOSA et al. In: Web Colaborativa - Evolução ou Revolução? **5ª Conferencia Ibérica de Sistemas y Tecnologías de Información**, 2010.

BEILI, E; NETWORKS A. - **Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs) RFC 4836** – Disponível em <http://www.ietf.org/rfc/rfc4836.txt>. Acessado em 21 de setembro de 2013.

BESERRA, Bruno Y. In: Cloud Computing . **Revista Científica Computação em Evolução**. Cuiabá, 2011

BEZERRA, Marcelo. In: Segurança das Redes. **Revista RTI**. p. 56. Maio, 2010

BRITO, Samuel H. B. **IPv6 O Novo Protocolo da Internet**. São Paulo: Novatec, 2013

CICCO, Francesco De. **Iso 27005**. Disponível em <http://www.qsp.org.br/artigo_27005.shtml> - Acessado em 30 de agosto de 2013.

COMBS, Gerald. – **Wireshark** – Disponível em < http://www.wireshark.org/>. Acessado em 03 de novembro de 2013.

COMER, Douglas. **Redes de Computadores e Internet**. 4. ed. São Paulo: Bookman, 2007

DEERING, S. *et al*. **Internet Protocol, Version 6 (IPv6) RFC 2460**. Disponível em <http://www.ietf.org/rfc/rfc2460.txt> - Acessado em 19 de setembro de 2013.

DROMS, R. **Dynamic Host Configuration Protocol RFC 2131**– Disponível em <http://www.ietf.org/rfc/rfc2131.txt>- Acessado em 30 de outubro de 2013.

ETHERNET - **Ethernet Interfaces and Hub MIB (hubmib)** – Disponível em <http://www.ietf.org/wg/concluded/hubmib.html> - Acessado em 16 de setembro de 2013.

FIELDING, R. *et al*. **Hypertext Transfer Protocol RFC 2616** - Disponível em <http://www.ietf.org/rfc/rfc2616.txt> - Acessado em 16 de setembro de 2013.

FONTES, Edison. **Praticando a Segurança da Informação**. 1. ed. Rio de Janeiro: Brasport, 2008

FULLER, V. *et al*. **Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan RFC 4632** – Disponível em <http://tools.ietf.org/html/rfc4632> - Acessado em 18 de setembro de 2013.

HAUSER, V. – **The Hacker´s Choice THC-IPV6** – Disponível em <https://www.thc.org/thc-ipv6/>. Acessado em 03 de novembro de 2013.

IANA - **Internet Assigned Numbers Authority** – Disponível em <http://www.iana.org/> - Acessado em 29 de setembro de 2013.

IETF - **The Internet Engineering Task Force** – Disponível em <http://www.ietf.org> - Acessado em 15 de setembro de 2013.

Internet World States – Disponível em <www. internetworldstats.com/stats.htm> 06/2012 - Acessado em 19 de setembro de 2013.

IP – **Internet Protocol RFC 791** – Disponível em <http://www.ietf.org/rfc/rfc791.txt> - Acessado em 18 de setembro de 2013.

IPV6BR - **Curso IPv6.br (EAD 2013)**. Disponível em <http://ipv6.br>. Acessado em 08 de outubro de 2013.

ITU – **Committed to Connecting The Word** – Disponível em <http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/ITU_Key_2005-2013_ICT_data.xls>*(10/2013)*. Acessado em 21 de setembro de 2013.

KENT, S. *et al*. **Security Architecture for the Internet Protocol RFC 4301** – Disponível em <http://tools.ietf.org/html/rfc4301> - Acessado em 01 de novembro de 2013.

LAUBACH, M. *et al***. Classical IP and ARP over ATM RFC 4454** – Disponível em <http://tools.ietf.org/html/rfc4454>. Acessado em 16 de setembro de 2013.

OLIVEIRA, Ricardo Sato. In: Estudo de Vulnerabilidades do IPSEC em Redes IPv6. **CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA.** Marília, 2013

PINHEIRO, J.M. In: Domótica- Princípios da Automação Predial. **Revista RTI**. p. 98-107. Outubro, 2010

POSTEL, J; ISI. **User Datagram Protocol RFC 768** – Disponível em <http://www.ietf.org/rfc/rfc768.txt> - Acessado em 16 de setembro de 2013.

POSTEL, J.B. **Simple Mail Tranfer Protocol RFC 821** - Disponível em <http://tools.ietf.org/html/rfc821> - Acessado em 16 de setembro de 2013.

PLUMMER, D. C. **Address Resolution Protocol RFC 826**. Disponível em <http://www.ietf.org/rfc/rfc826.txt> - Acessado em 16 de setembro de 2013.

RFC - **Request for Comments –** Disponível em <http://www.ietf.org/rfc.html> - Acessado em 15 de setembro de 2013.

SANTAELLA, Lucia. In: Artigo sobre Nanotecnologia e Dispositivos Móveis. **Revista FAMECOS**. n. 35. Porto Alegre, p.95-101, Abril 2008

SRISURESH, P. *et al*.- **Traditional IP Network Address Translator (Traditional NAT) RFC 3022**. Disponível em < http://www.ietf.org/rfc/rfc3022.txt> - Acessado em 30 de outubro de 2013.

TANENBAUM, Andrew S. **Redes de Computadores**. 4. ed. Rio de Janeiro: Campus (Elsevier), 2003

TCP – **Transmission Control Protocol RFC 793**– Disponível em <http://www.ietf.org/rfc/rfc793.txt> - Acessado em 15 de setembro de 2013.