UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO

CURSO DE ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDE

JOSÉ CARLOS BATISTA

ANÁLISE DO PROCESSO DE DESCOBERTA DE VIZINHANÇA DO PROTOCOLO IPv6

MONOGRAFIA

CURITIBA

2017

JOSÉ CARLOS BATISTA

ANÁLISE DO PROCESSO DE DESCOBERTA DE VIZINHANÇA DO PROTOCOLO IPv6

Monografia apresentada como requisito parcial para obtenção do grau de especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Rede, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná.
Orientador: Prof. Dr. Kleber Kendy Horikawa Nabas.

CURITIBA
2017

TERMO DE APROVAÇÃO

ANÁLISE DO PROCESSO DE DESCOBERTA DE VIZINHANÇA DO PROTOCOLO IPv6

por

JOSE CARLOS BATISTA

Esta Monografia foi apresentada em 27 de novembro de 2017 como requisito parcial para a obtenção do título de Especialista em Gerenciamento de Servidores e Equipamentos de Rede. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Augusto Foronda
Prof. Coordenador do Curso

_____
Kleber Kendy Horikawa Nabas
Prof. Orientador

_____
Omero Francisco Bertol
Membro titular

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

RESUMO

BATISTA, José Carlos. **ANÁLISE DAS MENSAGENS RA E RS DO PROTOCOLO ICMPv6**.2017. 37 f. Monografia – (Especialização em Gerenciamento de Redes) – Programa de Pós-Graduação em Tecnologia , Universidade Tecnológica Federal do Paraná. Curitiba, 2017.

Este trabalho tem como tema o *Internet Protocol version 6* (IPv6) mais especificamente sobre como se dá a troca de mensagens do protocolo de extensão ICMPv6. É apresentado também nessa pesquisa conceitos teóricos sobre os assuntos aqui tratados e também sobre os recursos utilizados. Para isso, será utilizado um simulador que trabalha com IOS real de roteadores o GNS3, nesse específico, o roteador da Cisco, e também máquinas virtuais criadas em um software próprio para tal, o Virtual Box. Uma série de recursos novos foram acrescidos no protocolo IPv6, uma delas é a possibilidade de se atribuir um endereço IP a um host de forma automática utilizando-se do *Stateless Address*, que será demonstrado nesse trabalho como um fundo para que seja possível a apresentação das trocas de mensagens do protocolo de extensão ICMPv6.

Palavras chave: IPv6. ICMPv6. Rede.

ABSTRACT

BATISTA, José Carlos. **ANALYSIS OF THE ROUTER ADVERTSEMENT AND ROUTER SOLICITATION MESSAGES OF THE ICMPv6**.2017. 37 f. Essay (Graduate Certificate in Networking and Systems Administration) - Graduate Programs in Technology, Federal Technological University of Paraná. Curitiba, 2017.

This work has the theme Internet Protocol version6 (IPv6) more specifically about how the ICMPv6 extension protocol messages are exchanged. Also presented in this research are theoretical concepts on the subjects discussed here and also on the resources used. For this, a simulator will be used that works with real routers IOS the GNS3, in that specific, the router of Cisco, as well as virtual machines created in its own software for such, Virtual Box. A series of new features were added in the protocol IPv6, one of them is the possibility of assigning an IP address to a host automatically using the Stateless Address, which will be demonstrated in this work as a background so that it is possible to present the message exchanges of ICMPv6 extension protocol.

Keywords: IPv6. ICMPv6. Network.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

1.1 TEMA

Devido ao enorme crescimento da demanda da utilização da internet nas últimas décadas uma preocupação ficou em evidência, os endereçamentos de protocolos *Internet Protocol* - protocolo de internet (IP) em sua versão atual não serão o suficiente para interligar todos os atuais novos usuários da rede global.

Mesmo com as mudanças sofridas, para a melhor utilização das suas classes e endereços, o IPv4 não atende mais à demanda e logo se esgotará. Restou então a evolução do protocolo IP para a versão 6 que resolverá o problema, se não definitivamente, por um longo período.

Este trabalho terá como tema o *Internet Protocol version 6* (IPv6), mais especificamente sobre o funcionamento e algumas vantagens do protocolo de extensão ICMPv6 em comparação ao seu antecessor, o ICMPv4, implantado em uma rede de computadores. O foco deste trabalho será a avaliação, assim como o método, de funcionamento de uma rede.

O trabalho visará a criação de uma topologia de uma rede local para a simulação e o estudo de situações em que sejam imprescindíveis a utilização de tal protocolo, o ICMPv6.

1.2 DELIMITAÇÃO DA PESQUISA

Será apresentado um exemplo de cenário com utilização de roteador, switch e host onde, em suas configurações, há a disponibilização da versão 6 do protocolo IP, o processo de endereçamento será demonstrado analisando as mensagens (RS e RA) trocadas entre roteador e host evidenciando assim a imprescindível necessidade do protocolo ICMPv6.

Nos primeiros capítulos serão exemplificados alguns conceitos sobre o IPv6, será descrito as suas funcionalidades proprietárias, maior número de redes e usuários, conta com datagramas mais simples e flexíveis.

No mundo há uma organização para a distribuição de endereços IP tanto o espaço de endereçamento do IPv4 como do IPv6 são delegados por um organismo central da Internet, chamado IANA (*Internet Assigned Numbers Authority*), que é subsidiado pelo governo. Para apoio na distribuição de números, o IANA conta com quatro regiões mundiais, chamados de *Regional Internet Registries* (RIR), sendo elas o LACNIC (*Latin-American and Caribbean IP Address Registry*) – América Latina e algumas ilhas do Caribe, ARIN (*American Registry for Internet Numbers*), responsável pela América do Norte, Caribe e África abaixo do Sahara, RIPE (*Reséau IP Européens*), responsável pela Europa, parte da África e países do oriente médio e APNIC (*Asia-Pacific Network Information Center*), responsável pela ásia e pacífico.

No Brasil, que fica sob responsabilidade do LACNIC, tem-se o Núcleo de Informação e Coordenação do ponto BR (NIC.br) que é responsável pela distribuição de endereços IP e registro de nomes de domínios a nível nacional. Estes órgãos por sua vez limitam os endereços para as empresas, órgãos públicos e demais usuários da internet, que façam solicitação de endereços IP válidos.

Figura 1 - RIR/NIC.BR [Autoria própria].

1.3 PROBLEMA

O problema constituiu em, a partir de uma rede IPv6, avaliar o funcionamento da descoberta de vizinhos e de roteadores por meio do protocolo ICMPv6, pois para que isso ocorra, é necessário utilizar o cabeçalho de extensão ICMPv6.

As mensagens RS e NS são enviadas por hosts e roteadores, respectivamente por meio de solicitações por meio de *multicast* e as mensagens RA e NA são as respostas a estas solicitações. A demanda deste trabalho veio da necessidade de se demonstrar na prática o que de fato acontece para que equipamentos que compartilham um mesmo nó conheçam seus vizinhos e recebam uma identificação, ou seja, um endereço IP.

A figura 1 apresenta a topologia que foi montada para efetuar as demonstrações de descoberta da vizinhança entre os equipamentos e as trocas dos protocolos e mensagens entre eles.

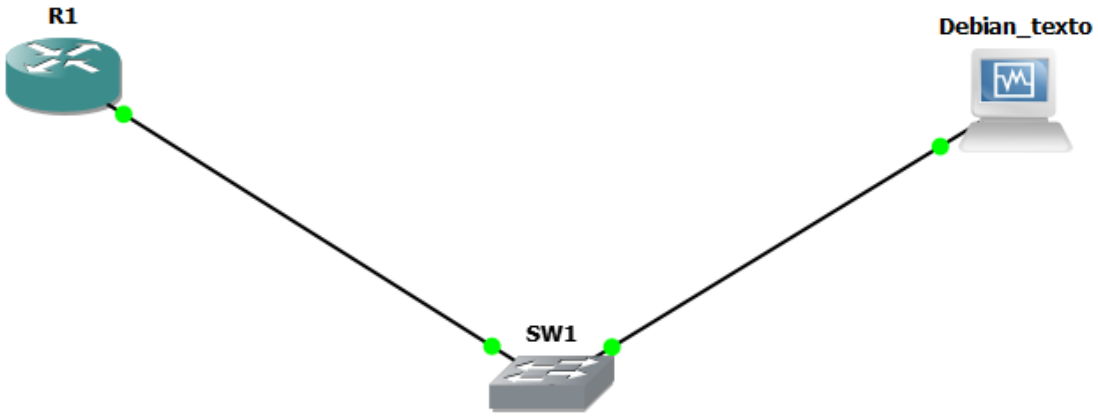

Figura 2 - Topologia [Autoria própria].

1.4 OBJETIVOS

A seguir é descrito o objetivo geral deste trabalho e as suas partes específicas.

1.4.1 Objetivo geral

Realizar um estudo sobre a nova versão do protocolo de extensão ICMPv6, visando a sua praticidade em relação à versão anterior o ICMPv4.

1.4.2 Objetivos específicos

- Estudar o estado da arte do protocolo IPv6;
- Estudar o estado da arte do protocolo ICMPv6;

- Explorar o uso do ICMPv6 no IPv6 no que cerne as trocas de mensagens RS e RA;
- Prospectar equipamentos de rede, assim como ferramentas que permitem a simulação de redes;
- Estruturar uma rede completamente IPv6, constituída de um roteador e um switch e host;
- Utilizar esta rede para realizar os testes de descoberta de IP e mensagens ICMPv6 para demonstrar trocas de mensagens;
- Fornecer a metodologia adotada para a realização dos experimentos.

1.4 JUSTIFICATIVA

O protocolo IPv6, mesmo sendo criado a mais de vinte anos, ainda é uma incógnita para muitos profissionais e estudantes que atuam na área de redes e por esse motivo deve ser estudado e testado em laboratório e os resultados devem ser apresentados para que ele se torne cada vez mais habitual e compreensível nos meios em que será aplicado. Percebo, no meio de trabalho, pouco ou nenhum interesse em desmistificar o protocolo IPv6, mesmo com os rumores de que seu antecessor, o IPv4 está no limite de sua utilização devido ao esgotamento dos seus endereços IP.

O trabalho aqui apresentado também se justifica pelo fato de que o protocolo de extensão do IPv6, o ICMPv6 não poderá ser barrado ou bloqueado nas redes em que será empregado, como é de praxe para se evitar ataques, se bloqueado não será possível a descoberta de vizinhança, a atribuição de endereços *Stateless* e a descoberta de roteadores e *gateways* em redes IPv6, pois exerce funções antes desempenhadas pelos protocolos ARP, RARP e IGMP. Segundo Florentino (2012, p. 50) “Dentre as várias mensagens lCMPv6 trocadas em um segmento de rede local, quatro delas são fundamentais para que a descoberta de hosts IPv6 vizinhos se realize.”), as mensagens as quais se refere Florentino são RS, RA, NS e NA, duas das quais (RS e RA) daremos ênfase no trabalho aqui apresentado.

1.5 PROCEDIMENTOS METODOLÓGICOS

Nesse projeto serão utilizadas referências bibliográficas sobre o assunto pressuposto, softwares e equipamentos virtuais conectados em rede e materiais virtuais e didáticos de apoio.

O estudo demonstrará também as funcionalidades do IPv6 e o protocolo de extensão ICMPv6 com ênfase nas trocas de mensagens RS e RA.

As diferenças entre o IPv4 e IPv6, tais como saber reconhecer a sintaxe dos cabeçalhos e características proprietárias, não faz parte do escopo desse trabalho, bem como as funcionalidades de QoS e segurança em IPv6.

1.6 FUNDAMENTAÇÃO TEÓRICA

Para descrever os conceitos, técnicas e diferenças que serão abordadas e estudadas no decorrer desta monografia, será utilizada a revisão de literatura relacionada à área de redes de computadores, baseadas nas obras de Santos (2010), Comer (2006), Florentino (2012), Filippetti (2014) e artigos regulamentadores da tecnologia como as *Request for Comments* – Requisições para Comentários (RFC's), regulamentada pela *Internet Engineering Task Force* – Força Tarefa de Engenharia para a Internet (IETF).

Estas bibliografias são essenciais para atender os objetivos específicos relacionados à tecnologia e utilização do protocolo de internet. Na parte que se destaca o escopo prático do trabalho, foram realizados ensaios laboratoriais utilizando equipamento próprio (*notebook*) munido de *softwares* de virtualização de equipamentos físicos, onde foram realizadas com sucesso a aplicação da tecnologia IPv6 em um cenário virtual de conexão de rede.

No que correspondem as atualidades e aplicações, a pesquisa baseia-se novamente em Santos (2010) por ser uma obra recente sobre o assunto relacionado, demonstrando assim conclusões mais precisas do escopo atual da utilização mundial do protocolo de internet.

1.7 ESTRUTURA DO TRABALHO

Esta monografia é estruturada por 5 capítulos que se complementam e que visam satisfazer os objetivos propostos. No primeiro capítulo, introdutório, a seguinte estrutura é formulada tendo início com : i) tema de pesquisa; ii) apresentação do problema; iii) objetivos; iv) justificativa; v) procedimentos metodológicos; vi) fundamentação teórica; vii) estrutura.

Para o desenvolvimento do tema proposto foram sugeridos os capítulos 2, 3 e 4 que englobam teorias e práticas dessa pesquisa. O capítulo 2 explana

conhecimentos do protocolo IP nas versões 4 e 6, demonstrando pontos que os diferenciam e apontando motivos para migrar para a versão mais atual do protocolo. O terceiro capítulo está embasado diretamente nas fundamentações e obras relacionadas à tecnologia do protocolo, estudando as funcionalidades do IPv6 das quais serão aplicadas nos testes do laboratório virtual, relacionando a teoria com a utilização da tecnologia e sua empregabilidade.

A parte de maior interesse para profissionais da área está contido no capítulo 4, onde será demonstrado de maneira prática a obtenção do endereço IP automaticamente pela placa de rede de um host com o sistema operacional Debian rodando de forma virtual em no Virtualbox, onde também serão apresentadas as trocas de mensagens RS e RA do protocolo de extensão ICMPv6 por meio de captura de pacotes utilizando o Wireshark.

No capítulo 5 será apresentada a conclusão da monografia e suas considerações futuras, descrevendo os resultados, aplicabilidade e utilização do protocolo. Se atendo as diretivas dos objetivos propostos.

2 O IPv6

É importante informar que a divisão dos blocos IPv4 não é nada ponderada, metade dos endereços foram destinados aos Estados Unidos (“criador do *backbone,* principal estrutura da Internet”) e a outra metade foi distribuída para as demais regiões geográficas do mundo.

Segundo Fillipetti (2014, p.128) “ Desde a sua criação, há mais de 40 anos, as redes de computadores só fazem crescer em tamanho, complexidade e apetite por banda.”

No início da distribuição dos endereços, existiram empresas e universidades que compraram 16 milhões de endereços. Hoje seria raro essas entidades devolverem o que adquiriram para uma melhor redistribuição dos endereços. Mas se essa divisão dos IPv4 fosse de forma igual para tal demanda de sua determinada região, não adiantaria em nada, estaríamos sujeitos do mesmo jeito aos esgotamentos dos IPs pois devido ao crescimento da população seguido pelas tecnologias a demanda também cresceu numa escala muito acima da esperada. Por esse e outros motivos que a IANA mais tarde necessitou de regras mais rígidas para a distribuição dos IPv4 para o mundo.

De acordo com Fillipetti (2014, p. 129) “ Os blocos de endereços IPv4 livres para atribuição a provedores de serviço já se esgotaram em praticamente todas as regiões do planeta. A previsão para o fim definitivo dos endereços IPv4 passíveis de alocação é no início de 2015, para a América Latina (o fim chegará antes em regiões com demandas maiores, como Ásia e América do Norte)”. A verdade é que os endereços IPv4 ainda não estão esgotados devido a uma série de técnicas e recursos para a otimização do uso destes endereços, foram criados e implementados com maestria por empresas e provedores de serviços.

A versão 4 do IP, que atualmente é utilizado para o endereçamento na internet é o endereço de 32 bits dividido em classes, por números de redes e números de host. Conforme Comer (2005, p. 370) “A versão 4 do *Internet Protocol* (IPv4) foi a primeira versão de trabalho; ela permaneceu quase inalterada desde o seu surgimento no final

da década de 1970.” Mostrando-se muito robusta e de fácil implementação, mas na década de 70 não foram levados em consideração alguns aspectos.

Segundo Santos et al (2010, p. 8) os aspectos não previstos para o IPv4 foram– “O crescimento das redes e um possível esgotamento dos endereços IP; O aumento da tabela de roteamento; Problemas relacionados a segurança dos dados transmitidos; e Prioridade na entrega de determinados tipos de pacotes.”

Atualmente estes fatores são levados em consideração uma vez que hoje é possível contar com internet não somente em computadores pessoais, mas em celulares *tablets*, *smartphones* e outros dispositivos eletrônicos que utilizam da rede mundial para a comunicação dos seus usuários.

Para Florentino (2012, p.20) “ Eu comparo a situação dos profissionais de redes de hoje a dos programadores de uns 20 anos atrás que se viravam com poucos *Kilobytes* de memória para fazer seus programas serem executados, pois memória era mito ara e difícil de obter. No futuro, cada usuário poderá receber um bloco de endereços em sua casa maior do que todo o bloco de endereços IP válidos existentes em toda a Internet hoje”.

O número de endereços certamente era mais do que suficiente nos primórdios da Internet, mas completamente inadequado para os tempos atuais, além de possuírem um computador em casa, muitos ainda levam consigo inúmeros outros dispositivos que também podem se conectar à Internet e, portanto, precisam de um endereço lógico como *tablets*, smartphones, iPods e muitos outros.

Segundo Filippetti (2014, p.128) “ O número de dispositivos que precisam de um endereço IP praticamente triplica a cada ano, e com isso, o número de endereços IPv4 disponíveis vai chegando ao fim”.

A solução definitiva encontrada foi a atualização da versão atualmente utilizada por uma que satisfaça as condições de crescimento atual da internet, foi então apresentada a versão 6 do protocolo de internet ou IPv6, especificada pela RFC 2460 em dezembro de 1998.

Em dezembro de 1988 foi especificada a FRC 2460 que trata da solução definitiva encontrada para a atualização da versão 4 do protocolo IP e que satisfaça as condições de crescimento da Internet.

De acordo Santos et al (2010, p. 18) “Como principais mudanças em relação ao IPv4 destacam-se: - Maior capacidade para endereçamentos, simplificação do formato do cabeçalho, suporte a cabeçalhos de extensão, capacidade de identificar fluxos de dados e suporte a autenticação e privacidade. ”

O IPv6 revisa o formato do datagrama em relação a sua versão anterior utilizando tamanhos fixos e simplificados, possui 128 bits com a denotação hexadecimal separada por dois pontos (:) as redes e hosts. Aumentando assim em mais do que suficiente da necessidade mundial tendo disponíveis bilhões de endereços.

A versão 6 do protocolo IP não necessita de técnicas para soluções paliativas, como seu antecessor, o IPv4, como o *Network Address Translator* – Tradutor de endereços de Rede (NAT) e o *Classless Interdomain Routing* – Roteamento de inter-domínio sem-classe (CIDR), que auxiliam na utilização mais otimizadas dos endereços IPv4, assim, evitando desperdícios de endereços que poderiam ser utilizados, mas ficavam “indisponíveis” na sua classe pela máscara de sub-rede. Devido à capacidade de endereços do IPv6, não há esta necessidade de recurso, melhorando assim o tempo de roteamento de pacotes, já que é um recurso a menos para ser processado pelo roteador.

O IPv6 possui 128 bits de campo para seus endereços, conseguindo atingir um tamanho mais do que necessário para futuras gerações durante anos, conforme Florentino (2012, p.20) “Esta fartura de endereços permite uma mudança radical na forma de atribuição e gerenciamento do plano de endereços IP”. A sua denotação hexadecimal com dois pontos, fornece uma melhor e mais compacta visualização e utilização quando comparada a denotação decimal do IPv4.

Para exemplificar, será utilizado o endereço IPv6 a seguir:

2001:0DB8:CAFE:DAD0:FACA:CA5A:F0CA:DEAD/128

No exemplo, cada parcela de 16 bits é representada por 4 dígitos hexadecimais (0 – F), podendo ser maiúsculas ou minúsculas e separados entre si por dois pontos. Como são oito grupos de 16 bits nos dá um total de 128 bits. Para tornar o exemplo ainda mais fácil de ser compreendido, é permitida a notação tipo CIDR com a

utilização da barra transversal seguida de um número inteiro representando a parcela de bits que está sendo utilizada para endereço de rede, assim como é no IPv4.

Conforme Florentino (2012, p. 37) “ Não se costuma informar uma máscara de sub-rede para fazer a operação AND binário como ocorre no IPv4”.

Para facilitar sua representação, algumas regras de nomenclatura foram definidas, como por exemplo, zeros à esquerda em cada duocteto, assim também chamado um rupo de 16 bits, podem ser omitidos, dessa forma o endereço utilizado como exemplo abaixo:

2001:0DB8:00AD:000F:0000:0000:0000:0001

Pode ser representado da seguinte forma:

2001:DB8:AD:F:0:0:0:1

Blocos vazios contínuos podem ser representados pelos caracteres :: uma única vez dentro do endereço, o valor que se apresenta antes do primeiro sinal de dois pontos representa os primeiros bits, e o que está posicionado após o segundo sinal de dois pontos representa os últimos bit do endereço conforme está representado abaixo:

2001:DB8:AD:F::1

Assim como no IPv4 o IPv6 possui endereços básicos definidos, sendo eles: *unicast*, *anicast* e *multicast*. O *unicast* é o endereço de destino que especifica um único host ou roteador e o pacote é entregue somente a esse destinatário utilizando o caminho mais curto; o *anycast* cujo destino é identificado por um conjunto de hosts ou interfaces onde o pacote é encaminhado a um dos membros deste conjunto, levando como padrão o mais próximo, segundo Santos et al (2010, p. 54) “Um endereço *anycast* é utilizado em comunicações de um-para-um-de-muitos.”

O endereço *multicast* tem como destino um conjunto de computadores, possivelmente em vários locais, contudo o pacote não é encaminhado a somente um destes computadores do conjunto, mas as todas as interfaces que compõem o mesmo endereço, conforme Santos et al (2010, p .54) “Um endereço *multicast* é utilizado em comunicações de um-para-muitos”.

No IPv6 não apresenta o endereço de *broadcast* (que envia pacotes para todos os nós de um mesmo domínio) sendo este muito utilizado na versão 4, na nova versão esta função foi atribuída ao endereço de *multicast*, mas em tipos específicos de *multicasting*.

De acordo com Florentino (2012, p. 45) “Em redes IPv6 não existem mais endereços de broadcast. Este recurso agora é realizado por diversos grupos *multicast* específicos.”

Mantendo-se os últimos 64 bit do endereços IPv6 destinado à criação de hosts, pode-se utilizar um recurso chamado *Stateless auto-configuration* (configuração sem estado), que permite a geração automática do ID do host baseado em seu endereço físico (*MAC Address* – endereço físico de um dispositivo).

Segundo Comer (2005, p. 382), sobre o recurso *Stateless*:

> O IPv6 admite a autoconfiguração e a renumeração. Cada host em uma rede isolada gera um endereço local ao enlace exclusivo, que usa para comunicação. O host também usa o endereço local ao enlace para descobrir roteadores e informações de prefixo global.

Para uma melhor visualização e compreensão do formato, na figura 3 abaixo é demonstrada a estrutura do cabeçalho básico do IPv6 de 40 octetos.

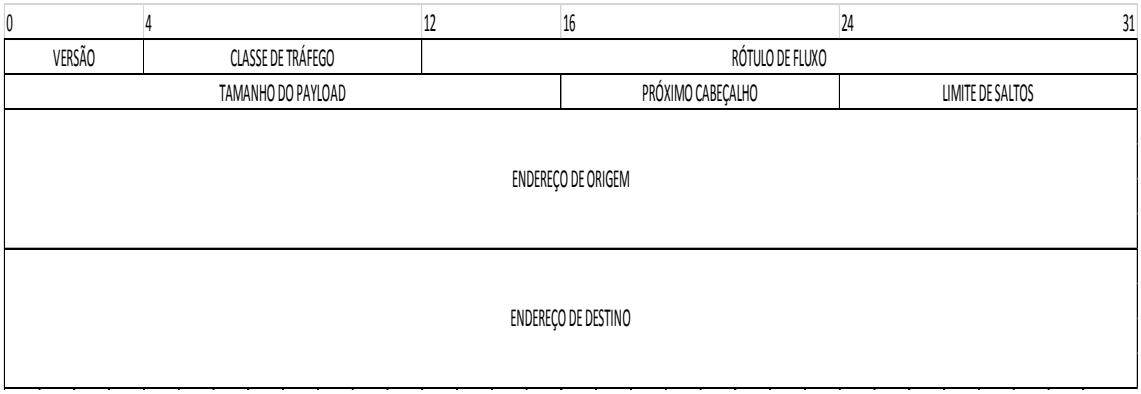

Figura 3 - Cabeçalho básico do protocolo IPv6 [Autoria própria].

Segundo Comer (2005, p. 372), sobre datagrama IPv6 básico é importante salientar que:

> Cada datagrama IPv6 começa com um cabeçalho básico de 40 octetos, que inclui campos para os endereços de origem e destino, o limite máximo de saltos, a classe do tráfego, o rótulo de fluxo e o tipo do próximo cabeçalho. Assim, um datagramaIPv6 precisa conter pelo menos 40 octetos além dos dados.

3 FUNCONALIDADES DO IPv6

Nesse capítulo, serão abordadas as funcionalidades essenciais da nova versão do protocolo IP que será utilizada nesse trabalho, tanto na aplicação prática quanto para o conhecimento teórico.

3.1 ICPMv6

Para que a funcionalidades do protocolo sejam colocadas em prática é necessário um protocolo auxiliar e fundamental para a execução das demais ferramentas, esse protocolo auxiliar é o Protocolo de Controle de Mensagens de Internet versão 6 – Internet *Control Message Protocol version 6* (ICMPv6).

Essas mensagens são utilizadas como troca de informações para que a ferramenta desejada seja aplicada, tendo como objetivo: i) informar tipos de rede; ii) diagnosticar a rede; iii) relatar erros onde sejam encontrados erros nos processamentos.

Esta função está identificada no campo "*Próximo Cabeçalho*" do datagrama e com o valor 58, haja vista que, para que a mensagem seja corretamente direcionada, o ICMPv6 deve ser implementado em todos os nós da rede e não é compatível com a versão 4 do protocolo IP. Os cabeçalhos do protocolo são de estruturas simples conforme demonstrada na figura 4.

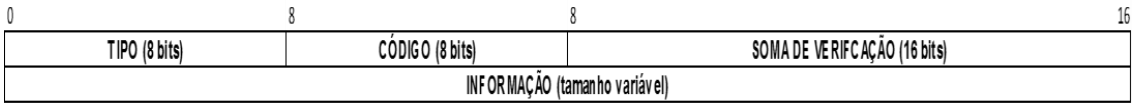

Figura 4 - Cabeçalho ICMPv6 [Autoria própria].

As informações das mensagens estão sempre precedidas do cabeçalho básico do IPv6 e dos cabeçalhos de extensão, a seguir na figura 5 é apresentada a posição do cabeçalho ICMPv6.

Figura 5 - Posição do Cabeçalho ICMPv6 [Autoria própria].

Para o funcionamento da versão 6 o protocolo de mensagens é fundamental na arquitetura e estrutura de comunicação como um todo. Ele gerencia as seguintes funções:

- Grupos de endereços *Multicast*;
- Resolução de endereços da camada inferior, substituindo o antigo Protocolo de resolução de Endereços – *Address Resolution Protocol* (ARP);
- Mensagens para a função de Descoberta de Vizinhança;
- Tipos de endereçamentos sendo eles *Stateless* ou *Statefull*; e
- Descoberta da Máxima Unidade de Transmissão – *Maximum Transmit Unit* (MTU) do pacote, a partir dos saltos da origem até o destino, sendo este dinâmico podendo ser alterado de enlace para enlace.

No gerenciamento de grupos *multicast*, conforme já mencionado o protocolo utiliza um dispositivo de descoberta para saber qual dos grupos de devem sem enviados as mensagens *multicast*, este protocolo é denominado de Descoberta de Ouvintes *Multicast* – *Multicast Listener Discovery* (MLD).

Outro fator essencial para o funcionamento é o processo de Descoberta de Vizinhança, que executa a função da camada de enlace do modelo Aberto de Sistemas de Interconexão – *Open Systems Interconnection* (OSI), responsável pela descoberta dos *hosts* diretamente conectados ao seu de conexão.

O ICMPv6 é dividido em dois grupos de mensagens, as mensagens de erros (tabela 1) e mensagens informativas (tabela 2), das quais serão demonstradas as que têm no escopo do trabalho.

Tabela 1 - Mensagens de Erros ICMPv6.

Type		
Valor	Nome	Descrição
1	Destination Unreachable	Indica falhas na entrega do pacote
2	Packet Too Big	Indica que o tamanho do pacote ultrapassou o limite do enlace.
3	Time Exceeded	Indica que o limite de encaminhamento ou o tempo de remontagem do pacote foi excedido.
4	Parameter Problem	Indica erro em algum campo do cabeçalho ipv6 ou que o tipo indicado no próximo cabeçalho não foi reconhecido.
127	--	Reservado para expansão das mensagens de erro
255	--	Reservado para expansão das mensagens de erro

Fonte: Autoria Própria.

Tabela 2 - Mensagens de Informações ICMPv6

Type		
Valor	Nome	Descrição
128	Echo Request	Utilizadas no comando ping
129	Echo Reply	
130	Multicast Listener Query	Utilizadas no gerenciamento de grupos multicast
131	Multicast Listener Report	
132	Multicast Listener Done	
133	Router Solicitation	Utilizadas com o protocolo Descoberta de vizinhança
134	Router Advertisement	
135	Neighbor Solicitation	
136	Neighbor Advertisement	
137	Redirect Message	
138	Router Renumbering	Utilizada no mecanismo de re-endereçamento de roteadores
139	ICMP Node Information Query	Utilizadas para descobrir informações sobre nomes e endereços, são atualmente limitadas a ferramentas de diagnóstico, depuração e gestão de rede
140	ICMP Node Information Reponse	
141	Inverse ND Solicitation Message	Utilizadas em uma extensão do protocolo de descoberta de vizinhança
142	Inverse ND Advertisement Message	
143	Version2 Multicast Listener Report	Utilizada no gerenciamento de grupos multicast
144	Ha Address Discovery Request Message	Utilizadas no mecanismo de mobilidade IPv6
145	HA Address Discovery Reply Message	
146	Mobile Prefix Solicitation	
147	Mobile Prefix Advertisement	
148	Certification Path Solicitation Message	Utilizadas pelo protocolo SEND
149	Certification Path Advertisement Message	
150	--	Utilizada experimentalmente com protocolos de mobilidade Seamoby
151	Multicast Router Advertisement	Utilizada pelo mecanismo multicast router discovery
152	Multicast Router Solicitation	
153	Multicast Router Termination	
154	FMIPv6	Utilizada pelo protocolo de mobilidade FAST Handovers

Fonte: Autoria Própria

3.2 DESCOBERTA DE VIZINHANÇA

O protocolo *Neighbor Discovery Protocol* (Protocolo de descoberta de vizinho) definida pela RFC 4861 é responsável por descobrir os endereços IP das máquinas e roteadores presentes na rede. Ele é o equivalente ao protocolo ARP, que não existe em redes IPv6, más também possui recursos que no IPv4 eram efetuados pelo protocolo ICMP.

Suas principais características são: i) determinar o endereço de camada de enlaço de dados do modelo OSI, denominada Controle de Media de Acesso – *Media Access Control* (MAC), mais conhecido por MAC-*Address*, representado no formato hexadecimal, sendo os três primeiros identificando o código do fabricante e os três últimos o equipamento; ii) encontrar roteadores diretamente conectados (vizinhos) e a acessibilidade dos mesmos; iii) determinar configurações de rede e autoconfiguração de endereços; e iv) alertar endereços de IP duplicados na mesma rede.

3.3 DESCOBERTA DE ROTEADORES E PREFIXOS

Esta funcionalidade do protocolo de Descoberta de Vizinhança é utilizada para localizar roteadores vizinhos dentro do mesmo enlace, bem como aprender prefixos e parâmetros relacionados à autoconfiguração de endereço.

Estas informações enviadas a partir de um roteador local, através de mensagens RA encaminhadas para o endereço *multicast all-notes*, fazendo um comparativo, no IPv4, o mapeamento dos endereços de rede local são realizados através de mensagens ARP *request*.

No caso de um *host* enviar uma mensagem ao roteador vizinho e este através da sua tabela de roteamento, verificar que no enlace há uma rota mais apropriada para o destino do pacote do *host*. O roteador redireciona automaticamente o pacote recebido ao *host*, utilizando a mensagem do tipo 137 (redirecionamento). Com esta função o *host* subsequentemente passa a enviar seus pacotes com o mesmo destino do pacote redirecionado.

3.4 ENDEREÇAMENTO STATELESS

Esta função tem como principal tarefa atribuir automaticamente o endereço de IP para o *host*, chamada de Autoconfiguração de Endereços *Stateless* ou configuração automática de endereço. Não havendo a necessidade de configurações manuais ou mesmos de um servidor de endereços, como os servidores DHCP.

Segundo Florentino (2012, p. 49) “O IPv6 traz uma série de novos recursos em relação à sua versão anterior, dentre elas a possibilidade de se atribuir endereços IP ao host automaticamente aravés do *Stateless Address*”.

Para tal configuração o *host* utiliza suas próprias informações e atribuem elas como informações de *Host-Id*, juntamente ao prefixo da rede, combinado o prefixo IPv6 com as informações de hardware do fabricante (MAC-*Address*).

Na configuração *Stateless* é utilizado o padrão do Identificador Único Estendido de 64-*bits* – *64-bits Extended Unique Identifier* (EUI-64), para autoconfigurar o endereço IPv6 em redes onde 64 *bits* são destinados a prefixos de rede e os 64 *bits* restante para interface de usuários dado aqui como exemplo o 2001:DB8:1:1::/64.

Para que um IP seja criado o roteador deve ser configurado com o padrão EUI-64 e fornecer o prefixo ao *host*, para se chegar a esse resultado, o processo segue duas etapas, a primeira é separar o endereço MAC em duas partes iguais e inserir entre elas o endereço hexadecimal FFFE, valores esses que são reservados para o padrão EUI-64, não podendo conter em endereços MAC de fabricantes. Na segunda etapa a informação do *bit* 6 do octeto da alta ordem é alterado de 0 para 1, garantindo assim um endereço IPv6 globalmente exclusivo.

Veremos logo a frente que o endereço MAC da máquina virtual que será utilizada em testes de laboratório é o 08:00:27:62:DB:9E e que após a atuação do recurso *stateless* seu endereço IP Global ficará sendo 2001:DB8:1:1:A00:27FF:FE62:DB94/64, onde se percebe claramente a inclusão dos 16 bit FFFE na metade do endereço físico e a alteração do valor 8 para A.

4 DEMONSTRANDO AS TROCAS DE MENSAGENS

Baseando-se nos conceitos teóricos e referências de autores da área de redes foi elaborado um ensaio utilizando-se de equipamentos simulando equipamentos de rede conectados para demonstrar as trocas de mensagens do protocolo de extensão ICMPv6.

4.1 FERRAMENTAS DE VIRTUALIZAÇÃO

Para a realização de testes com diferentes topologias de redes, é necessário o uso de diversos tipos de equipamentos de redes. O custo de adquirir estes equipamentos e o espaço físico necessário podem impossibilitar a realização de experimentos de redes. Logo, há disponíveis certos tipos de softwares que permitem a construção de redes simuladas em computadores.

Utilizaremos aqui para a virtualização de uma rede o GNS3 e para a virtualização de um *host* utilizaremos o Virtualbox, o que possibilita a montagem de um cenário ideal para a análise dos dados trocados entre equipamentos.

O GNS3 trabalha com a emulação do sistema operacional de roteadores, o *Internetwork Operating System* (IOS), que é obtido dos próprios roteadores físicos.

A respeito da análise dos pacotes IP que trafegam em uma rede, é possível com a utilização da ferramenta denominada Wireshark, que é um analisador de protocolos de rede inclusa no GNS3. Permite-se verificar detalhadamente cada pacote, e, por isso, esta ferramenta é destinada tanto para as empresas como para o ensino de redes.

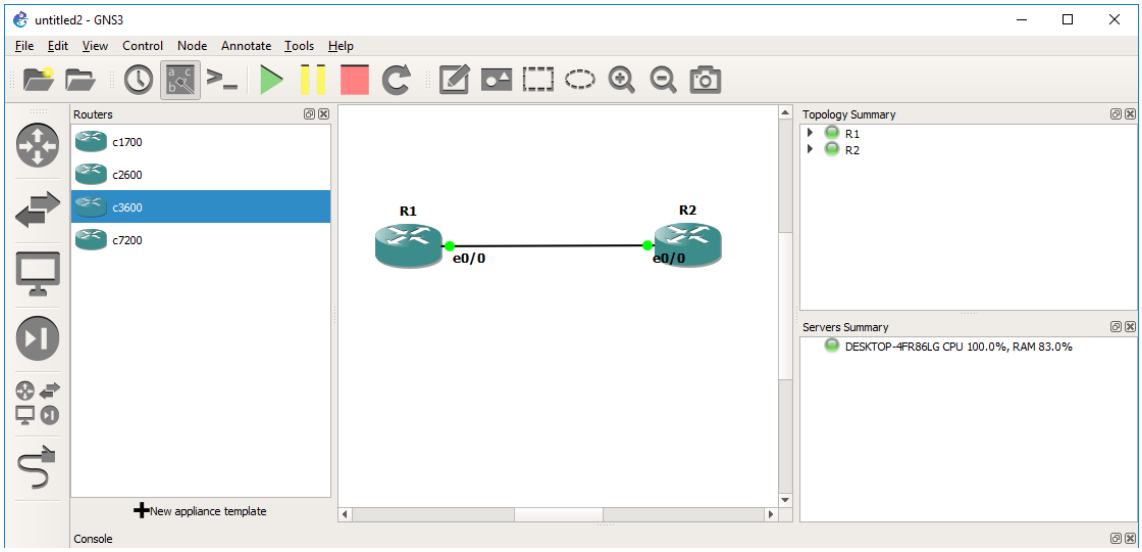

Figura 6 - Emulador de Redes GNS3 [Autoria própria].

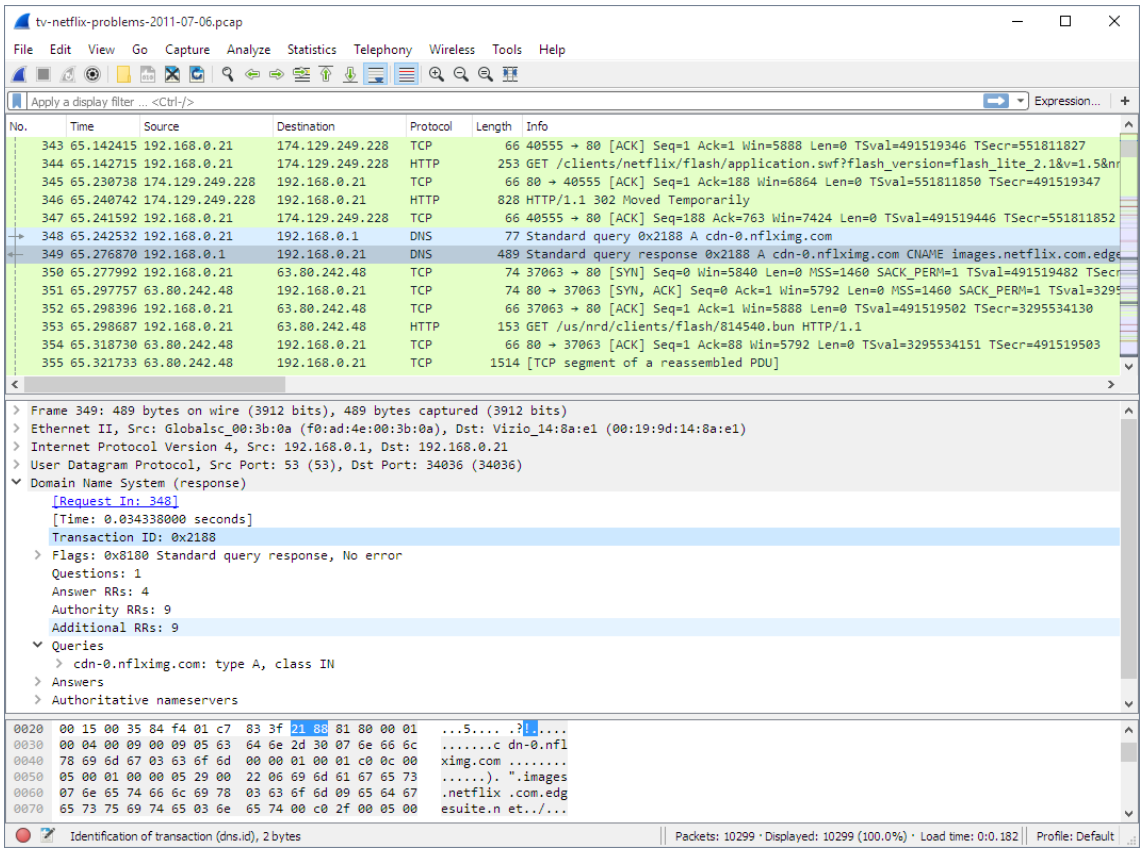

Figura 7 – Wireshark.

Fonte: https://www.wireshark.org/docs/wsug_html/

VirtualBox é um software de virtualização desenvolvido pela empresa Innotek depois que visa criar ambientes para instalação de sistemas distintos. Ele permite a instalação e utilização de um sistema operacional dentro de outro, assim como seus respectivos softwares, como dois ou mais computadores independentes, mas compartilhando fisicamente o mesmo hardware.

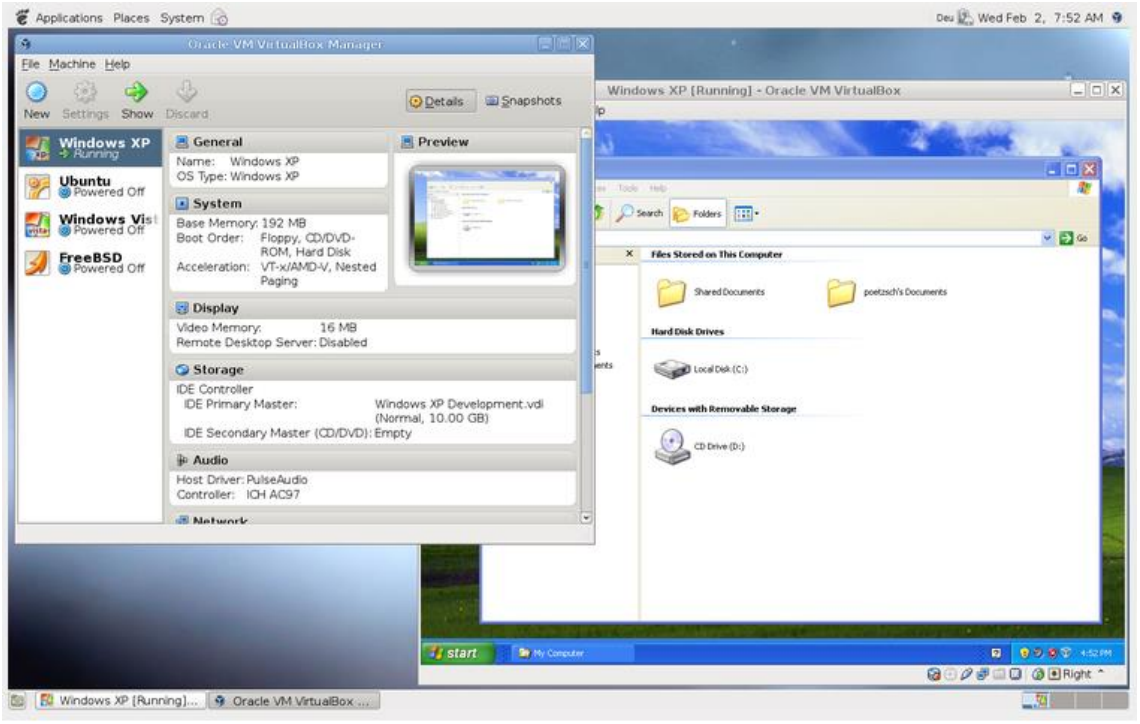

Figura 8 - Software de Virtualização Virtualbox.

Fonte: https://www.virtualbox.org/wiki/Screenshots

Para os testes foi utilizado um notebook da marca Dell Vostro 1310, equipamento não muito atual que possui um processador Intel Core 2 Duo T8100 com 2.1GHz e 4GB de memória RAM que atende aos requisitos de instalação do Software GNS3. O sistema operacional é o Windows 10 Pro 64bits.

A figura 9 exibe as configurações do equipamento utilizado para a instalação dos softwares de virtualização e também os testes efetuados.

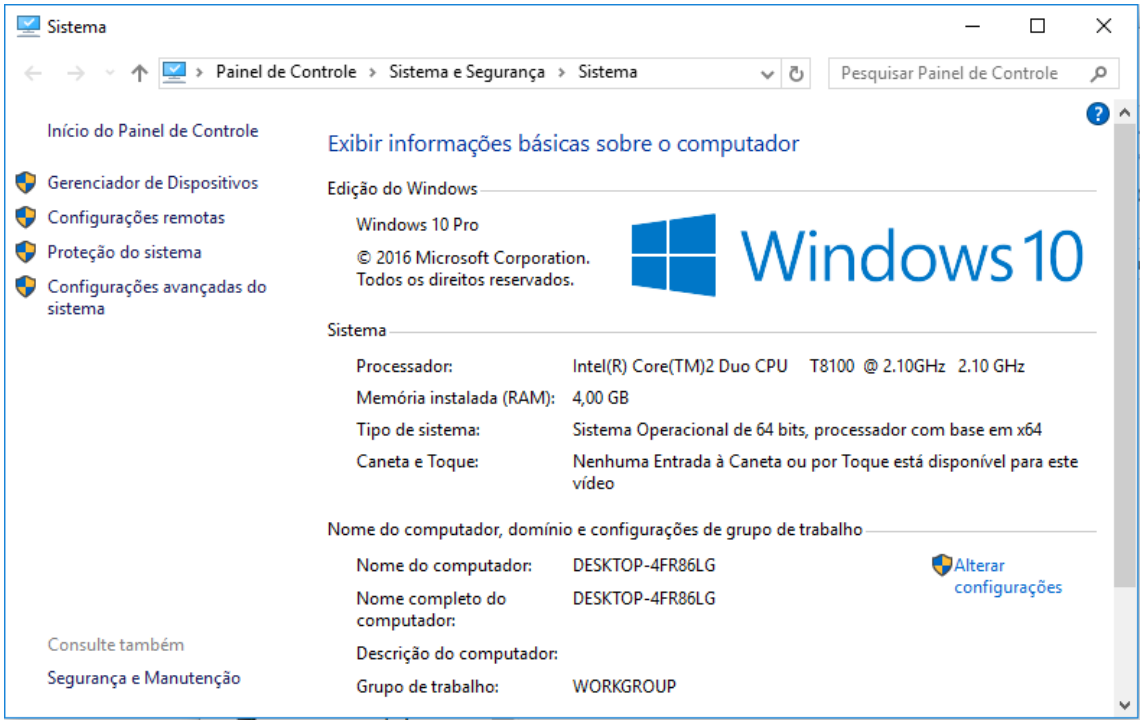

Figura 9 - Equipamento [Autoria própria].

O GNS3 foi então utilizado para os testes sem o apoio de equipamentos físicos de rede devido à sua flexibilidade para emular os roteadores Cisco utilizando-se para isso dos IOS dos mesmos, para o presente trabalho foram testados vários IOS, alguns apresentaram alguns problemas que vão desde não disponibilizarem a versão 6 do protocolo IP como é o caso do Cisco 2610. O modelo Cisco 3640 da família Cisco 3600 foi quem atendeu aos requisitos para que os testes fossem efetuados como interfaces de rede ethernet e suporte ao protocolo IPV6.

4.2 PROCEDIMENTOS

Nesta seção é descrita como a rede IPV6 foi implantada, como o ICMPv6 é imprescindível e como os experimentos para a visualização dos processos de descoberta de vizinhança e distribuição de endereço IP foram realizados. A figura 10 mostra uma apresentação da rede que foi montada para que os testes fossem efetuados.

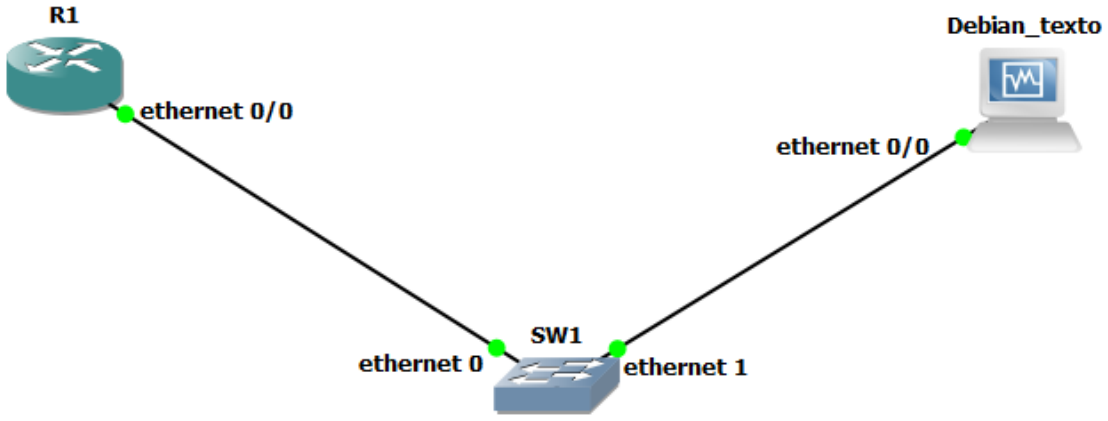

Figura 10 - Topologia Virtual [Autoria própria].

Antes da implantação de uma rede completamente IPv6, fez-se necessário a instalação do GNS3, em conjunto com o Dynamips (emulação de roteadores), Wireshark (análise dos pacotes IP) e o VirtualBox (virtualização de sistema operacional).

O R1 é o roteador o qual será interligado ao computador Debian_texto por meio de um switch, o SW1, os procedimentos para a configuração dos equipamentos seguem no decorrer deste trabalho, com textos explicativos e figuras que ajudarão na compreensão dos procedimentos adotados nas configurações dos equipamentos Roteador R1 e Host Debian_texto.

Na configuração do Roteador R1 a seguinte configuração foi executada:

#ipv6 unicast-routing

#interface ethernet0/0

#ipv6 address 2001:db8:1:1::/64 eui-64

#ipv6 enable

Os passos acima foram efetuados para que primeiramente na caixa do roteador fosse habilitado o IPV6 com o comando “ipv6 unicast-routing”, logo em seguida, dentro da interface ethernet 0/0 configurado um prefixo IPV6, nesse caso 2001:db8:1:1::/64 e por fim habilitado o IPV6 na interface ethernet0/0 com o comando “ipv6 enable”. Na figura 11 é apresentada a interface ethernet após os passos descritos.

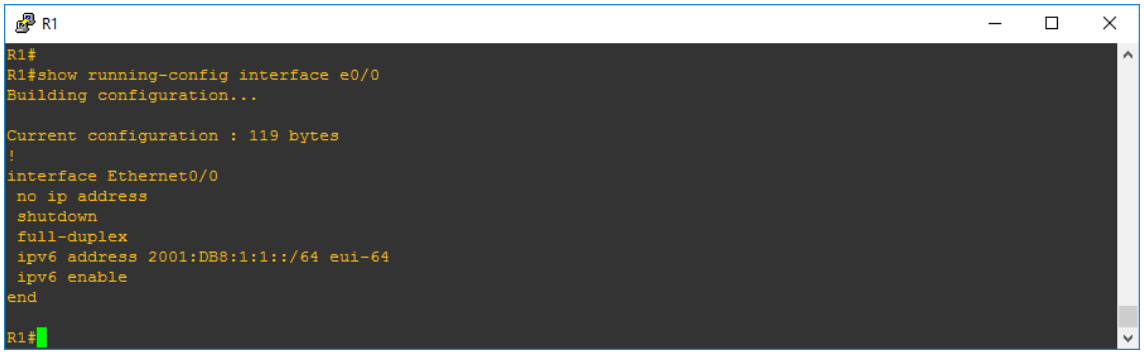

Figura 11 - Ethernet R1 [Autoria própria].

O host que foi utilizado para o laboratório, que roda de forma virtual no programa VirtualBox tem como sistema operacional Debian, foram necessárias as configurações na interface de rede desse host para que o mesmo trabalhasse com o protocolo IPv6, as quais seguem descritas.

Para utilizar poucos recursos da máquina física, o sistema operacional foi apresentado em forma de CLI, interface de linha de comando.

O arquivo interfaces que se encontra no caminho /etc/network foi editado e as linhas “auto eth0” e “iface eth0 inet6 auto” foram inclusas.

Abaixo a figura 12 que ilustra a configuração da interface de rede do host:

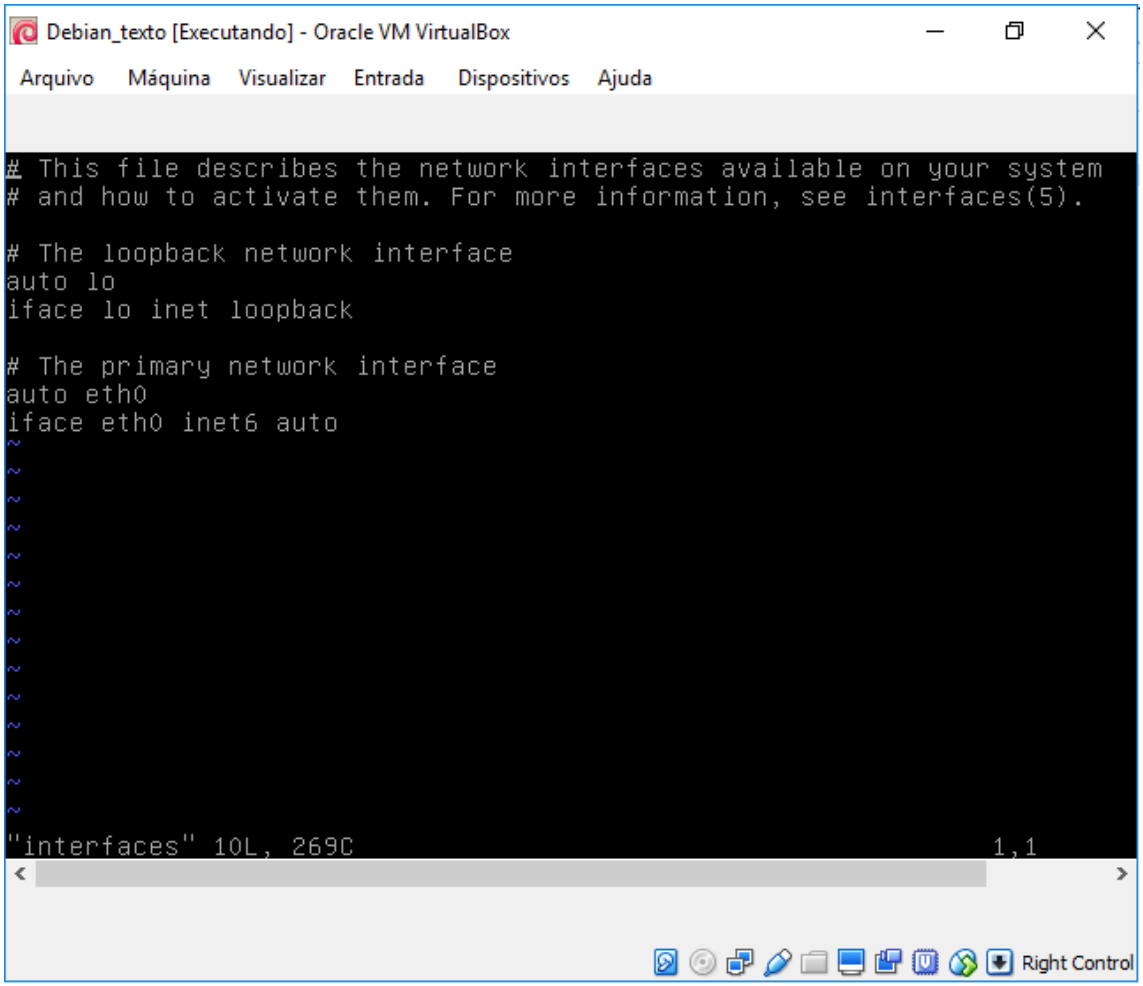

Figura 12 - Ehternet Debian [Autoria própria].

Com o comando ifconfig é possível verificar a situação da interface naquele determinado momento, a figura 13 apresenta essa situação.

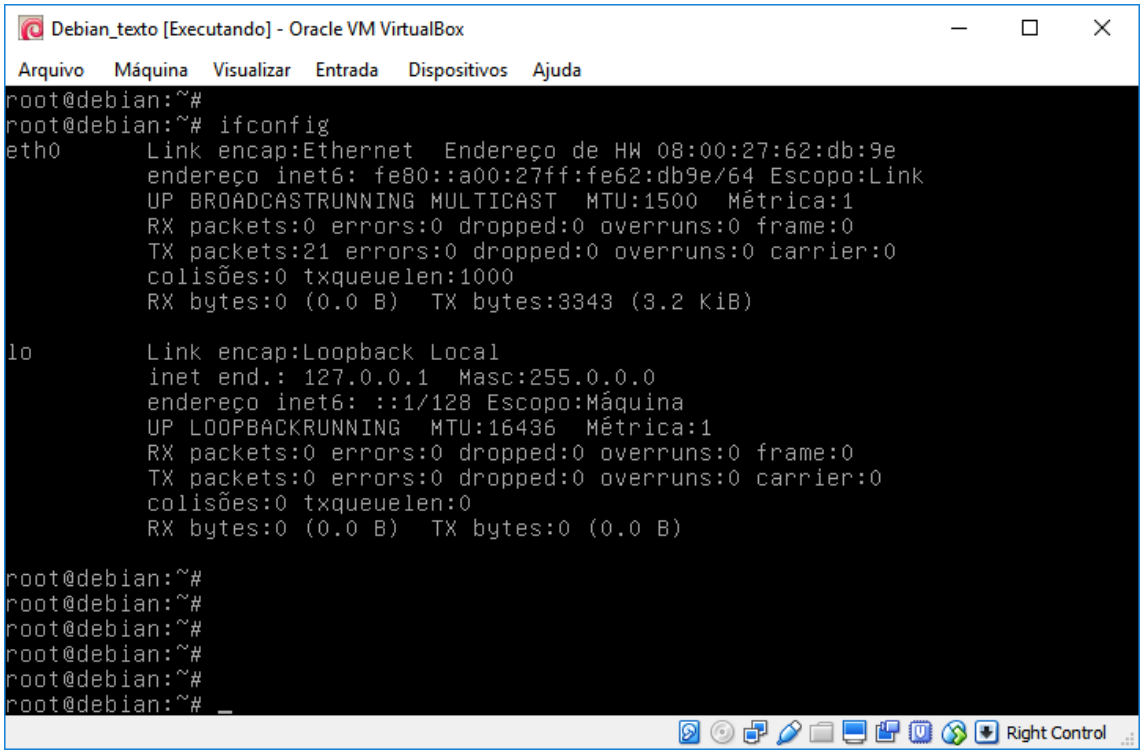

Figura 13 - Ifconfig Debian [Autoria própria].

Após efetuadas as configurações nas interfaces de rede de R1 e Debian_texto é possível acompanhar as atividades do protocolo IPv6 e o protocolo de extensão ICMPv6 como demonstrado nas figuras abaixo com o resultado dos comandos “show ipv6 interface brief” e “ifconfig”.

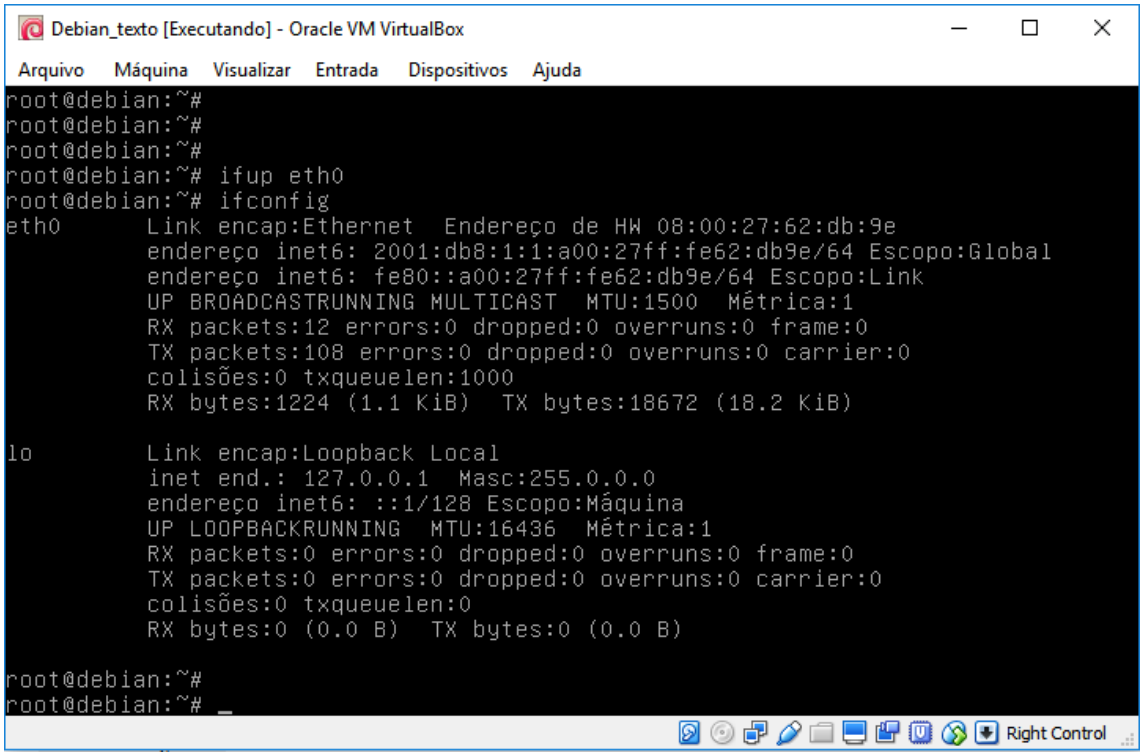

Figura 14 - Status Eth0 Debian [Autoria própria].

Na figura acima é possível identificar o endereço IPv6 Global 2001:db8:1:1:a00:27ff:fe62:db9e/64 atribuído à interface eth0 do host Debian_texto, assim como também na figura 15 abaixo é possível identificar o endereço IPv6 Global da interface Ethernet0/0 de R1.

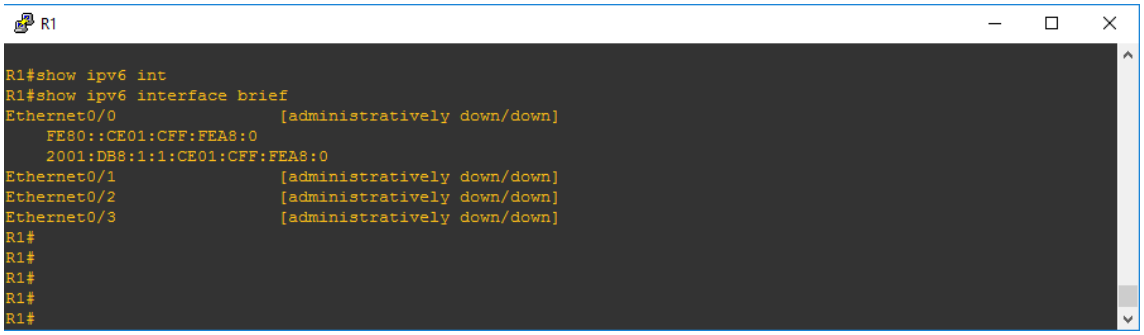

Figura 15 - Estado eth0 R1 [Autoria própria].

O endereço da Eth0 do host Debian_texto foi atribuído devido ao mecanismo de endereçamento *Stateless* que utiliza-se de mensagens trocadas entre o roteador e o host em questão, as mensagens são RS e RA, as quais serão detalhadas a frente com o auxílio da ferramenta de análise de pacotes Weireshark, demonstrando assim

todo o processo de troca das mensagens nas camadas II e III para a descoberta de vizinhança.

4.3 ANÁLISE DOS EXPERIMENTOS REALIZADOS

No laboratório apresentado, onde se conectaram roteador (R1) e host (Debian_texto) também foi possível analisar a troca de mensagens do protocolo de extensão ICMPv6 por meio da ferramenta de captura de pacotes Wireshark onde seguem abaixo com o passo a passo no que se refere às trocas de mensagens.

Na figura 16 é mostrada a mensagem RS (*Router Solicitation*) que é enviada por uma estação (Debian_texto) que deseja aprender informações de um roteador dentro de um seguimento de rede local (prefixo, comprimento do prefixo, *gateway*...)

O computador gera uma mensagem ICMPv6 *Router Solicitation*. Na camada 2, o endereço MAC de origem é o da placa de rede do *host*, aqui, 08:00:27:62:db:9e, e o endereço de destino é o MAC 33:33:00:00:00:02, esse é o endereço *multicast* associado ao grupo designado para o IPv6 *All Routers*).

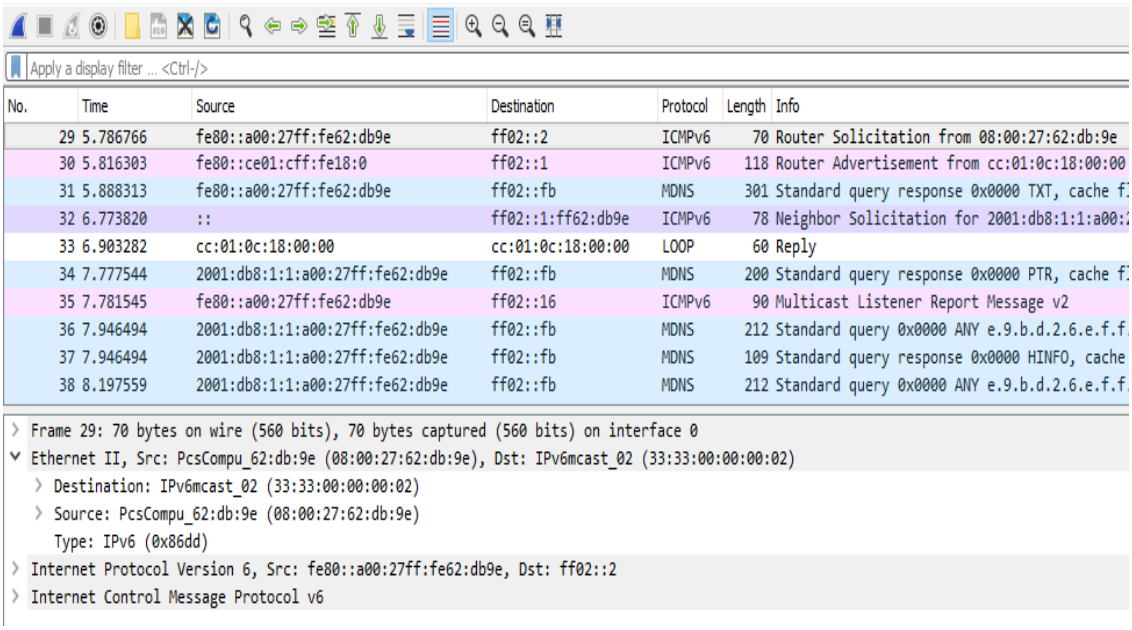

Figura 16 - *Router Solicitation* Camada 2 [Autoria própria].

Na camada 3, o pacote utiliza como endereço de origem seu IP link Local, aqui fe80::a00:27ff:fe62:db9e, e de destino o endereço ff02::2, esse último sendo o endereço *All Routers* onde o switch recebe a mensagem por uma interface ICMPv6 e a encaminha para todas as outras interfaces conectadas. Somente o rotador pode

responde-la, por isso os demais hosts a ignoram conforme demonstrado na figura 17 seguinte.

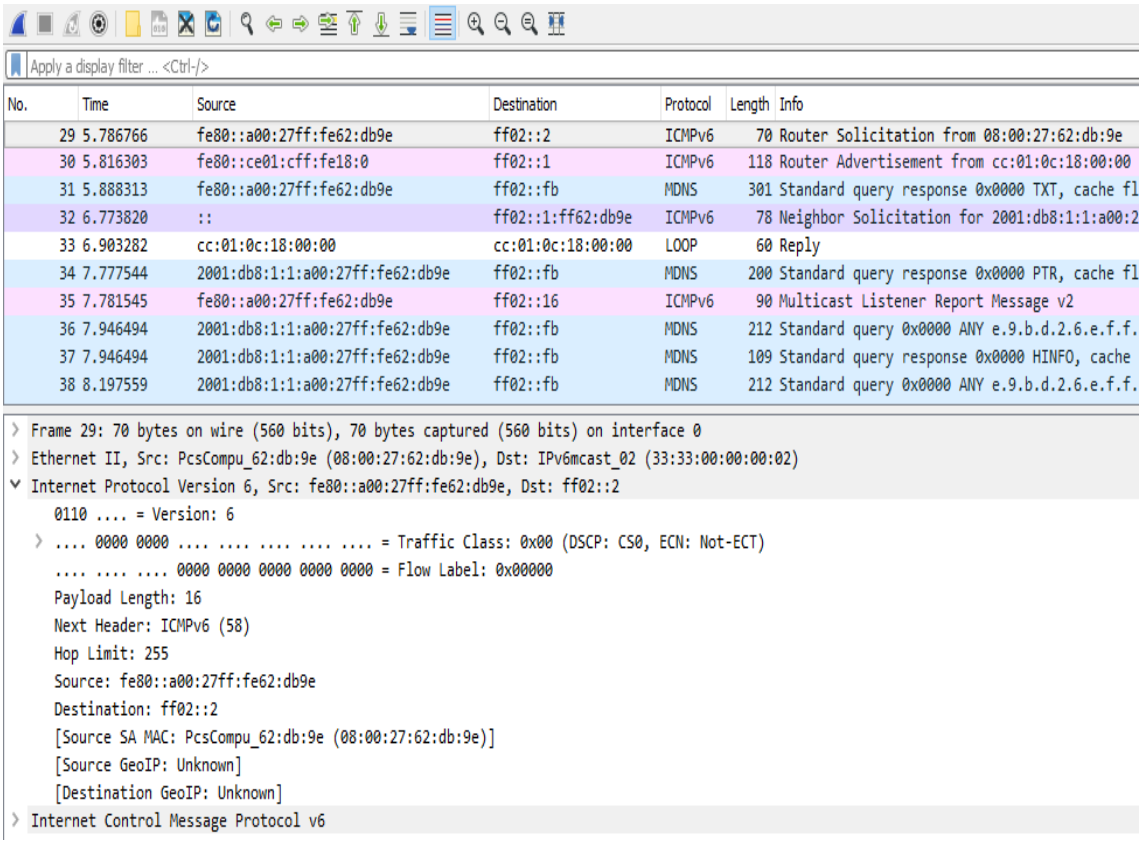

Figura 17 - *Router Advertsement* Camada 2 [Autoria própria].

O Roteador, por sua vez, em resposta a mensagem RS do host (Debian_texto) gera uma mensagem RA (*Router Advertisement*), mensagem essa que nem sempre é enviada como resposta à uma solicitação, ela pode ser configurada no roteador para ser disseminada em um período de tempo predeterminado. Quando o anúncio RA é feito de forma automática, a origem é o endereço *unicast* da interface do roteador e o destino é o endereço *Multicast All-Node* ff02::1. No caso aqui apresentado o RA foi criado em resposta a uma solicitação RS *unicast*, o endereço de destino é o mesmo endereço *unicast* da origem da solicitação, ou seja fe80::a00:27ff:fe62:db9e, conforme demonstrado na figura 18 abaixo, finalizando assim o processo de endereçamento automático do host e as trocas de mensagens RA e RS entre os dois equipamentos.

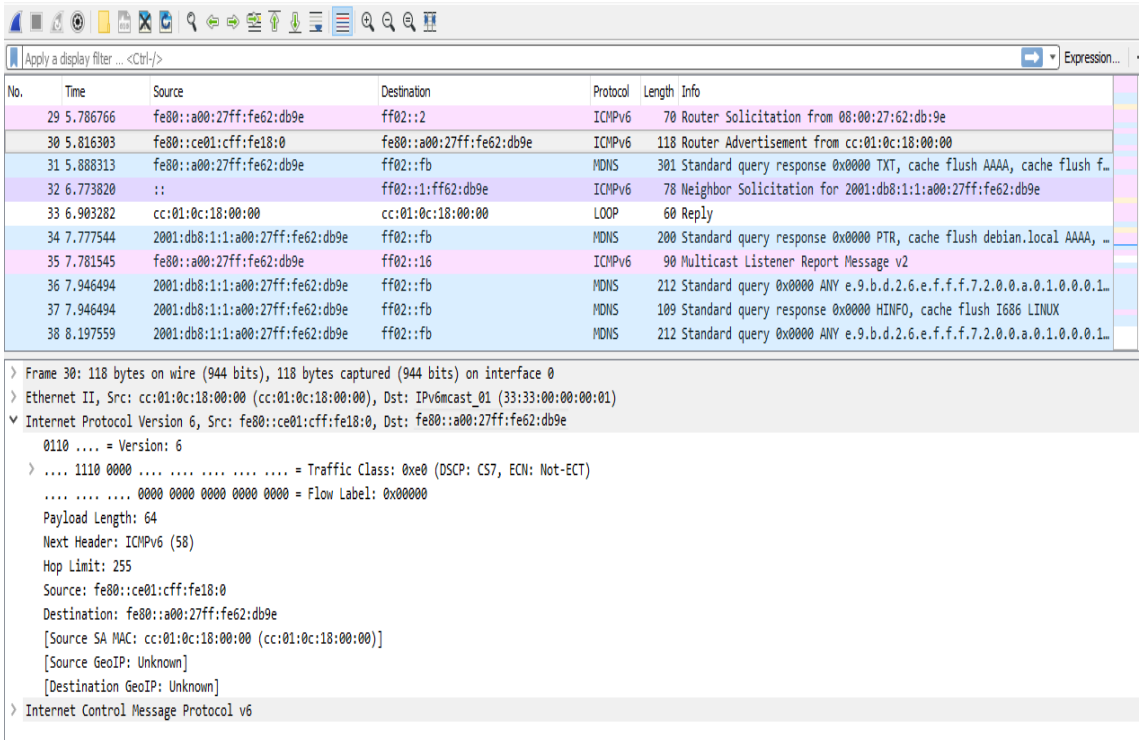

Figura 18 - *Router Advertsement* Camada 3 [Autoria própria]

5 CONCLUSÃO

Com a crescente demanda por endereços IP devida a disponibilidade cada vez maior de equipamentos que podem acessar outros e serem acessados pela internet, viu-se o esgotamento desse recurso na sua versão 4 e por esse motivo a necessidade de um estudo, o qual resultou na versão 6 do protocolo IP.

O IPv6 trouxe consigo algumas inovações, dentre elas protocolos de extensão, os quais são anexados ao cabeçalho IP conforme a necessidade, como por exemplo o Protocolo de extensão ICMPv6 que agregou para si várias funcionalidades da versão anterior, o ICMPv4, e outras indispensáveis para o correto funcionamento do protocolo, como a de descoberta de vizinhança (NDP)

Com isso é notória a importância desse protocolo e o mesmo não poderá mais ser bloqueado ou inativado na nova versão pois isso impossibilitaria a comunicação entre equipamentos como roteadores e computadores.

Como demostrado no capítulo 4, as trocas de mensagens RS e RA do protocolo de extensão ICMPv6 acontecem de forma automática, conforme o processo de endereçamento *stateless* onde um host solicita o prefixo da rede a um roteador e é atendido com mensagem RA direcionada somente a ele por meio de um endereço único na rede.

É importante conhecer o protocolo IPv6 pois é iminente a sua propagação nos meios de comunicação mundial, trabalhos como esse aqui apresentado ajudam a desmistificar e até incentivar a sua utilização.

REFERÊNCIAS BIBLIOGRÁFICAS

COMER, Douglas E. **Interligação de Redes com TCP/IP, vol. 1** – Princípios, protocolos e arquitetura. 5ª ed. Rio de Janeiro: Elvesier, 2006.

DEERING, S; HINDEN, R. **RFC 2460**. Disponível em: <http://www.ietf.org/rfc/rfc2460.txt>. Acesso em: 02 out. 2017.

FILIPPETTI, Marco A. **CCNA 5.0 – Guia Completo de Estudo.** 1ª ed. Florianópolis: Visual Books, 2014. 544p.

FLORENTINO, Adilson A. **IPv6 na Prática.** 1ª ed. São Paulo: Linux New Media do Brasil Editora Ltda, 2012.165p.

SANTOS, Rodrigo Regis dos, et al. **Curso IPv6 Básico.** 1ª ed. São Paulo: Ceptro.br, 2010.315p.