INSTITUTO FEDERAL DE SANTA CATARINA

RONALDO JOÃO BORGES

Automatização de ensaios da RFC 7084 em roteadores IPv6 para certificações Anatel

São José - SC

Junho/2019

AUTOMATIZAÇÃO DE ENSAIOS DA RFC 7084 EM ROTEADORES IPV6 PARA CERTIFICAÇÕES ANATEL

Trabalho de conclusão de curso apresentado à Coordenadoria do Curso de Engenharia de Telecomunicações do campus São José do Instituto Federal de Santa Catarina para a obtenção do diploma de Engenheiro de Telecomunicações.

Orientador: Jorge Henrique Busatto Casagrande

Coorientador: Marcelo Maia Sobral

São José - SC

Junho/2019

Ronaldo João Borges
Automatização de ensaios da RFC 7084 em roteadores IPv6 para certificações Anatel/ Ronaldo João Borges. – São José - SC, Junho/2019-
50 p. : il. (algumas color.) ; 30 cm.

Orientador: Jorge Henrique Busatto Casagrande

Monografia (Graduação) – Instituto Federal de Santa Catarina – IFSC
Campus São José
Engenharia de Telecomunicações, Junho/2019.

1. Palavra-chave1. 2. Palavra-chave2. 2. Palavra-chave3. I. Orientador. II. Instituto Federal de Santa Catarina. III. Campus São José. IV. Título

RONALDO JOÃO BORGES

AUTOMATIZAÇÃO DE ENSAIOS DA RFC 7084 EM ROTEADORES IPV6 PARA CERTIFICAÇÕES ANATEL

Este trabalho foi julgado adequado para obtenção do título de Engenheiro de Telecomunicações, pelo Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina, e aprovado na sua forma final pela comissão avaliadora abaixo indicada.

São José - SC, 15 de outubro de 2015:

Jorge Henrique Busatto Casagrande, Dr.
Orientador
Instituto Federal de Santa Catarina

Professor, Roberto Matos Dr.
Instituto Federal de Santa Catarina

Professor
Instituto Y

Professor
Instituto Z

Este trabalho é dedicado às crianças adultas que,
quando pequenas, sonharam em se tornar cientistas.

AGRADECIMENTOS

Ao professor Casagrande, por ter me ajudado e incentivado a realizar meu Trabalho de Conclusão de Curso.

Agradeço ao meu pai, que mesmo ausente esteve sempre ao meu lado. E à minha mãe, a razão por eu enfrentar meus maiores desafios.

"Não vos amoldeis às estruturas deste mundo,
mas transformai-vos pela renovação da mente,
a fim de distinguir qual é a vontade de Deus:
o que é bom, o que Lhe é agradável, o que é perfeito.
(Bíblia Sagrada, Romanos 12, 2)

RESUMO

Este trabalho propõe o desenvolvimento de um software para automatização dos ensaios da norma RFC [1] 7084 aplicado a roteadores de acesso a rede visando a obtenção de certificação na Anatel [2]. Pretende-se implementar as principais características técnicas desses ensaios, através do estudo detalhado das normas envolvidas e do IPv6 [3]. Como primeiros passos, utilizou-se o software livre Scapy para desenvolvimento das rotinas de envio e análise de pacotes recebidos. Para validação do software será utilizado um roteador homologado na Anatel com diversas versões de firmware e diferentes comportamentos de operação, os quais apresentaram falha ou sucesso em ensaios realizados pelo laboratório CPqD [4]. A partir dos resultados obtidos, planeja-se implementar no IFSC [5] um computador com o software instalado, no intuito de oferecer às industrias que embarcam roteamento IPv6 em seus produtos ensaios de pré-certificação conforme RFC 7084.

Palavras-chave: IPv6, Certificação Anatel, RFC 7084.

[1] *Request For Comments* (RFC)
[2] Agência Nacional de Telecomunicações (Anatel)
[3] *Internet Protocol* (IP)
[4] Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPqD)
[5] Instituto Federal de Santa Catarina (IFSC)

ABSTRACT

Keywords: RFC 7084. IPv6, Anatel Certification.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE CÓDIGOS

LISTA DE ABREVIATURAS E SIGLAS

ICMPv6 *Internet Control Message Protocol version 6* 28

DAD *Duplicate Address Detection* 43

PA *Prefix Advertisement* 42

IETF *Internet Engineering Task Force* 28

ARPANET *Advanced Research Projects Agency Network* 31

WAN *wide area network* 28

DARPA *Defense Advanced Research Projects Agency* 28

IoT *Internet of Things* 28

RA *Router Advertisement* 30

RS *Router Solicitation* 44

ESE Equipamento Sob Ensaio 42

SUMÁRIO

1 INTRODUÇÃO

Exigências normativas são requisitos impostos a qualquer produto elétrico, eletrônico ou óptico que por ventura venha ser a comercializado. Tal processo, chamado de homologação, é um ato administrativo gerido por agências vinculadas ao governo que visam, de maneira geral, contribuir para o desenvolvimento tecnológico da nação onde estão estabelecidas. No Brasil a Anatel é uma dessas agências. Ela foi criada em sete de setembro de 1997 pelo decreto 2338, na competência de agência reguladora nos setores de telefonia fixa e celular. Sua missão é regulamentar e fiscalizar o uso do espectro eletromagnético, assegurar a interoperabilidade entre os dispositivos certificados, garantir a segurança e saúde do usuário e coibir que os equipamentos interfiram entre si (BRASIL, 1997).

Assim como a Anatel, há outras agências internacionais que também regularizam o setor de telecomunicações em seus respectivos países, como por exemplo, a americana *Federal Communications Commission* (FCC) que opera no Estados Unidos e *British Standards Institution Group* (BSIGroup) no Reino Unido. Cada agência estabelece suas próprias diretrizes de certificação, elenca as normas de certificação para cada produto com base em suas características próprias e no ambiente de instalação, o qual poderá implicar em testes normativos funcionais, elétricos, ópticos, mecânicos ou climáticos. Entretanto, as agências tentam operar sob a mesma base de normas a fim de criar um sistema homogêneo de certificação de produtos. Por exemplo, um aparelho homologado nos Estados Unidos tende a operar em território brasileiro sem qualquer degradação funcional ou de performance, pois a Anatel se baseia no mesmo escopo de normas da FCC para definir os requisitos de certificação dos produtos comercializados no Brasil. Tanto que, em alguns casos, dependendo da especificação do produto, a agência brasileira permite a homologação por Declaração de Conformidade, na qual é possível apresentar uma certificação estrangeira em substituição aos ensaios nacionais, sendo esta aceita pela Anatel.

Mesmo fundamentando-se no escopo de normas internacionais, a Anatel submete uma consulta pública antes de publicar qualquer norma em âmbito nacional, e os atos da consulta são levados ao conselho da agência para tomadas de decisões relativas. Tal processo pode resultar em normas nacionais, chamadas de resolução, que visam atender aspectos regionais de fornecimento de energia, espectro etc. Salvo exceções, as agências buscam se basear no mesmo conjunto de normas técnicas para garantir o funcionamento dos dispositivos em qualquer país. A propósito, as principais resoluções da Anatel para certificação de produtos de telecomunicações são a 506 (Equipamentos de Radiocomunicação de Radiação Restrita) (ANATEL, 2008), a 442 (Compatibilidade eletromagnética) (ANATEL, 2006) e a 529 (segurança elétrica) (ANATEL, 2009). São frutos de normas internacionais da *International Electrotechnical Commission* (IEC) e *International Telecommunication Union* (ITU), também adotadas pelas agências FCC e BSIGroup para avaliação de certificação de produtos eletrônicos.

1.1 Motivações

A exigência da Anatel referente à obrigatoriedade do protocolo IPv6 em roteadores de acesso a rede, impactou numa demanda crescente das empresas de tecnologia por laboratórios capazes de testar o protocolo IPv6 a fim de compatibilizar seus produtos com os novos requisitos. Atualmente, o CPqD é um dos poucos laboratórios acreditados pelo Instituto Nacional de Metrologia, Qualidade e Tecnologia (Inmetro) capaz de realizar os ensaios de certificação IPv6. A título de referência, os testes de desenvolvimento do IPv6 custam em torno de dez mil reais por ensaio, e o software de validação da RFC 7084 custa em torno de oitenta mil reais. No caso do software, ele é basicamente um script que analisa

os pacotes IPv6 transmitidos e recebidos por duas interface de rede acopladas em um computador e ao roteador sob ensaio.

Motivado pela recente inclusão dos requisitos de IPv6 aos roteadores de acesso a rede para obtenção da certificação compulsória da Anatel (ABRANET, 2016), além das dificuldades das empresas em entender a forma como é realizada a avaliação do IPv6 segundo a RFC e aliado aos respectivos custos de desenvolvimento dos ensaios, o foco do TCC será criar um software de validação conforme a norma RFC 7084 (SINGH et al., 2013). Assim, ao final do trabalho de conclusão do curso, existe a possibilidade de oferecer ao IFSC material técnico/científico e implementações suficientes para que o instituto possa ter a iniciativa de se tornar um centro de estudos de pré-certificação Anatel de roteamento IPv6.

1.2 Objetivos

Este trabalho tem por objetivo realizar o estudo da norma RFC 7084 a fim de criar um software capaz de automatizar os ensaios funcionais IPv6 exigidos pela Anatel para obtenção de certificação compulsória em roteadores de acesso a rede. Serão apresentados e analisados tais requisitos e também os mecanismos IPv6 avaliados em cada um dos ensaios. O software será aferido através de testes em um roteador IPv6 Intelbras homologado, que possui versões de firmware com comportamentos conhecidos de sucesso e falha nos ensaios da RFC 7084 executados pela Anatel durante os ensaios IPv6.

Como objetivo adicional, pretende-se implementar o software de teste com uma interface amigável, com o intuito de que o IFSC possa fornecer às empresas de telecomunicações um serviço de análise, testes e apoio na elaboração do protocolo IPv6 em seus produtos, em conformidade com a RFC 7084.

1.3 Organização

Os capítulos 1 e 2 descrevem os efeitos causados pela escassez do IPv4 e quais foram as ações adotadas pelo governo brasileiro para regularização do IPv6 no Brasil, bem como demonstrar os problemas enfrentados pela indústria de telecomunicações na implementação do novo protocolo. Além do que já foi citado, no capítulo 2 é apresentado o estudo da arquitetura de rede de acesso e os grupos de testes da RFC 7084, a fim de identificar os mecanismos IPv6 avaliados nos ensaios e seus propósitos. Todos estes mecanismos são estudados durante o capítulo 2 como pré-requisito para o desenvolvimento do algoritmo que será abordado no capítulo 3. O capítulo 3 apresenta a metodologia de desenvolvimento da pesquisa, discute sobre as ferramentas disponíveis para a criação e análise de mensagens IPv6, contém um aprofundamento de cada um dos testes da RFC com o intuito de especificar o funcionamento das rotinas de envio e análise de mensagens IPv6. Ao final de cada item normativo da RFC 7084 implementado é apresentado o resultado dos testes no roteador IPv6 Intelbras homologado na Anatel com o objetivo de validar as implementações.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 A Homologação segundo as regras da Anatel

A Anatel dividiu os produtos em categorias I, II e III, a fim de determinar o conjunto de requisitos técnicos e procedimentos de ensaios aplicáveis(ANATEL, 2018) a uma família de produtos. Desta forma, a Anatel pode definir ensaios gerais de acordo com a categoria devido a similaridade dos produtos de uma determinada categoria. Por exemplo, desde 2018 o ensaio funcional de IPv6, estudado neste TCC, se tornou requisito de certificação de todos produtos da categoria I. Segue abaixo a descrição dos equipamentos que fazem parte de cada uma das categorias.

- Categoria I: equipamentos terminais destinados ao uso do público em geral para acesso a serviço de telecomunicações de interesse coletivo. Exemplos: telefone celular, baterias para telefone celular, cabos para uso residencial, etc.
- Categoria II: equipamentos não incluídos na definição da Categoria I, mas que fazem uso do espectro radioelétrico para transmissão de sinais. Exemplos: antenas, equipamentos com interfaces WiFi, bluetooth, etc.
- Categoria III: quaisquer produtos ou equipamentos não enquadrados nas definições das Categorias I e II, cuja regulamentação seja necessária à: garantia da interoperabilidade das redes de suporte aos serviços de telecomunicações; confiabilidade das redes de suporte aos serviços de telecomunicações; garantia da compatibilidade eletromagnética e da segurança elétrica. Exemplos: equipamentos e materiais utilizados nas redes das prestadoras de serviço de telecomunicação.

A determinação de qual categoria e os requisitos técnicos aplicáveis a determinado produto, por delegação da Anatel, é responsabilidade da Organismo de Certificação Designado (OCD) (ANATEL, 2015). Adicionalmente, a OCD tem o papel de avaliar a compatibilidade dos relatórios técnicos de conformidade de produtos de telecomunicações no âmbito da certificação compulsória.

Portanto, para obtenção da certificação compulsória, a primeira etapa é fazer uma consulta junto à OCD para definição dos requisitos. Por exemplo, considerando um roteador *Optical Network Terminal* (ONT), cujo produto é constituído basicamente de portas FXS, GPON, WiFi, fonte de alimentação e ethernet *Local Area Network* (LAN), a OCD classificará este produto na categoria I porque a interface *Gigabit Passive Optical Network* (GPON) pode se conectar com a provedora de internet. Os requisitos de certificação serão: Resolução 442, 506, IPv6, *Session Initiation Protocol* (SIP), *Foreign Exchange Subscriber* (FXS) e GPON baseados na ITU-T 984.x. Com base nestes requisitos, o solicitante deverá contratar um laboratório creditado pelo INMETRO para execução dos ensaios. E, por fim, enviar os resultados dos ensaios para avaliação dos analistas técnicos da OCD e Anatel. O processo de análise e publicação no sistema da Anatel poderá levar até 45 dias para ser concluído. Somente após a emissão do certificado no site da Anatel é que, de fato, o produtor pode comercializar o produto homologado.

2.2 A RFC 7084 - Ensaios para IPv6

O IPv6 foi criado para substituir o IPv4 principalmente devido ao esgotamento de endereços. Mesmo com a capacidade de endereçar mais de 4 bilhões de dispositivos, já era sabido desde 1998 que a quarta versão não supriria a demanda tecnológica por endereçamento de dispositivos conectados à Internet.

A versão 4 foi criada com propósito acadêmico e militar mas, posteriormente, foi cedida pela *Defense Advanced Research Projects Agency* (DARPA) para uso comercial. O sucesso foi tão grande que o IPv4 se tornou o principal protocolo para comunicação da rede de computadores no mundo e toda a estrutura da internet foi construída usando a versão 4 como base. Algumas técnicas foram adotadas para estender a vida do protocolo, no entanto, novas tecnologias como *Internet of Things* (IoT), aceleraram também o processo de esgotamento, em sua maioria operando somente em IPv6. Em resposta, a *Internet Engineering Task Force* (IETF) lançou a especificação da versão 6 do novo protocolo internet através da RFC 4291 (HINDEN; DEERING, 2006). Desde então, a IETF e operadoras alertam sobre os impactos econômicos e tecnológicos referentes a escassez da versão 4, de forma a sugerir que o país deveria adotar políticas de incentivo para adoção da nova versão. Porém, além das inciativas administrativas, era necessário superar aspectos técnicos, os quais são impostos pelos próprios equipamentos pois muitos deles necessitavam de mais espaço em memória para implementação do novo protocolo. Tal limitação oferecia abertura para implementações superficiais do protocolo em que a operadora acabaria saindo no prejuízo por não poder garantir a interoperabilidade da rede IPv6.

Preocupada com os riscos associados a uma baixa adotação do IPv6 e por sua falta de regulação, em dezenove de fevereiro de 2014 a Anatel criou um grupo de trabalho com o objetivo de coordenar as atividades necessárias à adoção do protocolo IP versão-6 (ANATEL, 2014) aos dispositivos que se conectam a rede de acesso (Por exemplo: par trançado, fibra óptica, coaxial, telefonia, satélite, rádio). O grupo foi composto por representantes das operadoras e pelo NIC (Núcleo de Informação e Coordenação), que além de definir o método de avaliação também avaliaram o método de transição da versão quatro para versão seis do IP com o objetivo de garantir a interoperabilidade da rede. Como resultado, no ano de 2016, a Anatel determinou que a partir de 2017, para obtenção de certificação compulsória, todos os produtos classificados como categoria I deveriam atender aos requisitos da RFC 7084 para validação dos aspectos funcionais do IPv6 (ABRANET, 2016).

2.3 Requisitos IPv6 para roteadores de acesso

Por delegação da Anatel, desde primeiro de janeiro de 2017, todos os produtos classificados como categoria I, devem atender aos ensaios funcionais da RFC 7084. A norma em si, especifica de que modo o roteador borda deve operar quando conectado a uma provedora de internet IPv6. Além disto, define o que é um roteador de acesso ao apresentá-lo na arquitetura de rede através da figura 1.

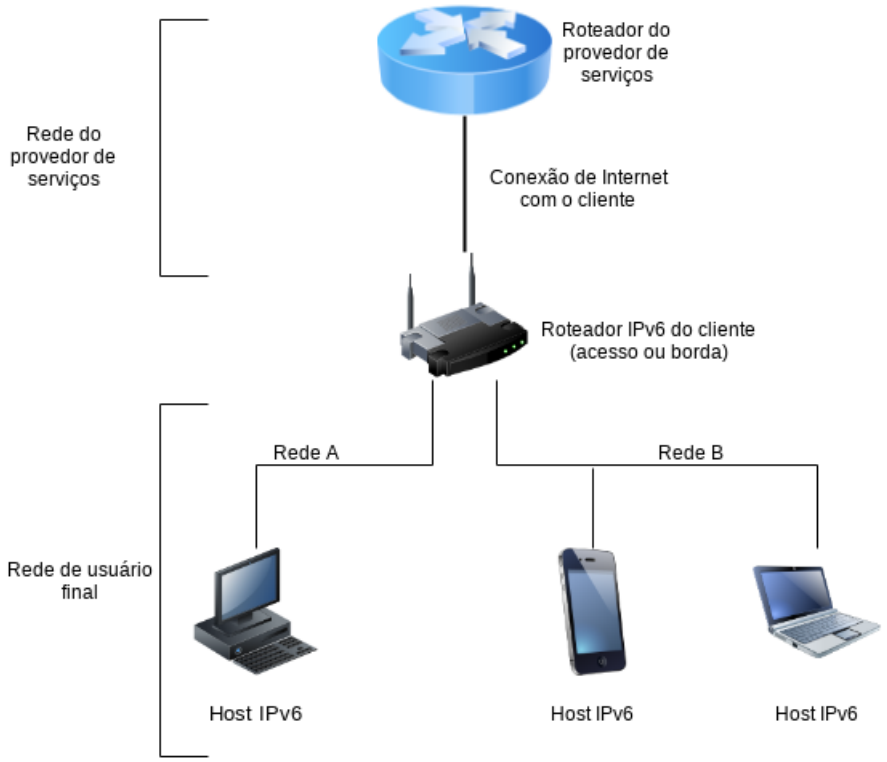
A figura 1 ilustra em que ponto da rede o roteador de acesso ou borda é instalado. Basicamente, o roteador é usado dentro da empresa ou residência do usuário final o qual está conectado ao provedor de internet. Assim, isso permite à Anatel categorizar se um roteador deverá atender aos requisitos IPv6 ao conferir as suas especificações e ponto de conexão na arquitetura de rede.

De modo geral, o objetivo dos testes é avaliar se o roteador suporta todos os tipos de mensagens ICMPv6 [1], serviço DHCPv6 [2], configuração da LAN, incluindo o gerenciamento de rotas, prefixos e múltiplos endereços na interface WAN [3], através de três grupos de testes. E todos eles devem ser aprovados para obtenção da certificação Anatel.

Todos os testes são citados pela RFC 7084, porém sua leitura é complexa e recheada de links para diversas normas que detalham os protocolos envolvidos no teste do IPv6. A fim de facilitar a compreensão dos requisitos para desenvolvedores e laboratórios, o grupo IPv6forum compilou os dados da RFC 7084 e produziu o documento chamado *Conformance Test Scenario CE Router*. Esse documento detalha, em

[1] *Internet Control Message Protocol version 6* (ICMPv6)
[2] *Dynamic Host Configuration Protocol version 6* (DHCPv6)
[3] *wide area network* (WAN)

Figura 1 – Exemplo de uma rede típica de usuário final



Fonte: os autores.

formato passo-a-passo, o comportamento das mensagens negociadas, dos procedimentos, cenários e os resultados esperados em cada item RFC 7084. A Anatel aproveitou este recurso para que sirva como uma espécie de manual aos laboratórios que realizam os ensaios para compatibilização do protocolo IPv6 em roteadores. Este manual também especifica os procedimentos dos ensaios da RFC 3315, 3646, 3363, 4861, 4862 e 1981 divididos em seções e grupos. Cada grupo representa uma RFC e cada seção um tipo de interface (WAN, LAN ou encaminhamento).

Primeiramente, são apresentados quais recursos IPv6 são avaliados pela RFC 7084, conforme seções 2.3.1, 2.3.2 e 2.3.3. Em seguida há o estudo mais aprofundado destes recursos na seção 2.4. No documento *Conformance Test Scenario CE Router* os ensaios da RFC 7084 estão citados nas seguintes seções: o grupo 7 da seção 1 avalia o IPv6 na interface WAN. O grupo 6 da seção 2, valida o protocolo na interface LAN e no grupo 2 da seção 3 são tratados os encaminhamentos das mensagens entre LAN e WAN. Estes ensaios serão apresentados neste TCC, porém, adotou-se uma numeração própria na identificação dos grupos, a fim de manter uma estrutura harmoniosa no trabalho. O propósito de cada ensaio também é descrito nos respectivos grupos, e tem o objetivo de tentar reconhecer quais recursos do protocolo IPv6 estão sendo validados na interface WAN, LAN e encaminhamento.

2.3.1 Grupo de testes 1: Ensaios da WAN

Este grupo de ensaios tem o objetivo de verificar se a interface WAN do roteador IPv6 oferece os recursos necessários do protocolo IPv6 para que se tenha o acesso de múltiplas arquiteturas conectadas a si. Não é especificada nenhuma arquitetura de acesso em particular, entretanto, deverá suportar as mais comumente usadas.

Os protocolos IPv6 *Neighbor Discovery* e DHCPv6 operam sobre qualquer tipo de camada de enlace suportada por IPv6, e não há necessidade de um protocolo na camada de enlace específico para configurar a camada de rede IPv6 opções como, por exemplo, Protocolo de Controle de IP PPP (IPCP) para IPv4. Os 7 ensaios do grupo WAN, fazem a suposição de que o mesmo mecanismo funcionará para qualquer camada de enlace, seja Ethernet, a *Data Over Cable Service Interface Specification* (DOCSIS), PPP ou outros (SINGH et al., 2013).

Valida-se o processamento das *flags* L e M, DHCP, delegação de prefixos e mensagens do processo de descoberta de hosts *Neighbor Discovery* do protocolo IPv6. A *flag* L ativa na mensagem *Router Advertisement* (RA) respondida pelo *ESE* indica que o prefixo contido nela pode ser usado para determinar um endereço válido na interface. Quando não está ativa significa que o roteador não dá declaração se o prefixo pode ser usado para isso ou não (NARTEN et al., 2007). A *Flag* M ativa indica que os endereços são disponibilizados através do serviço DHCPv6. Segue abaixo a descrição de cada um dos 7 ensaios do grupo WAN:

1. Transmissão de mensagem *Router Solicitation*: Verificar a capacidade do roteador em gerar um endereço de link-local e finalizar as mensagens *Duplicate Address Detection* antes de enviar qualquer *Router Solicitation*. O endereço de origem usado nas mensagens *Router Solicitation* subsequentes devem ser o endereço de link-local da interface WAN.

2. Processamento da *flag L*: Verificar se o roteador processa devidamente a *flag L* contida no campo *Prefix Information Options*.

3. Mensagem de reconfiguração: Verificar se o roteador implementa devidamente a opção *DHCPv6 Reconfigure Accept Option*.

4. Processamento da *flag M*: Verificar se o roteador implementa devidamente a *flag M* contida na mensagem *Router Advertisement*.

5. Tamanho do *Prefix Delegation*: Verifica se o roteador manipula corretamente o prefixo DHCPv6 delegado que são de diferentes tamanhos.

6. *Flag* M e O no *Prefix Delegation*: Verifica se o roteador manipula devidamente a *Flag M and O* para determinar a inicialização do processo de DHCPv6 *Prefix Delegation*.

7. Protocolo de roteamento dinâmico: Verifica se o roteador não inicializa qualquer protocolo dinâmico de roteamento.

2.3.2 Grupo de testes 2: Ensaios da LAN

Este grupo valida a capacidade do roteador em negociar, configurar, informar e prover endereçamento IPv6 aos dispositivos na interface LAN e assistência na obtenção do endereços IPv6. E também verificar que os dispositivos possuem conectividade na interface WAN. Esses ensaios são descritos abaixo:

1. Atribuindo prefixos para interfaces LAN: Verifica se o roteador atribui devidamente endereços a partir da delegação de prefixo para os dispositivos interface LAN do roteador.

2. Opção de informação de roteamento: Verificar se o roteador anuncia a si mesmo como roteador para os prefixos delegados através da mensagem *Route Information Option*.

3. Sem Delegação de prefixos: Verifica se roteador atribui endereços a partir da delegação de prefixo para interface LAN.

4. Informação de DNS no *Router Advertisement*: Verifica se o roteador transmite devidamente *Router Advertisement* informando o servidor a lista de pesquisa DNS.

5. Alteração prefixo: Verifica se o roteador anuncia devidamente a troca de prefixo.

6. Prefixo desconhecido: Verifica se o roteador transmite devidamente as mensagens ICMPv6 *Destination Unreachable* para os solicitantes que usaram um prefixo que está invalidado.

7. Prefixo de *Unique Local Address*: Verifica se o roteador gera e mantém prefixos ULA.

2.3.3 Grupo de testes 3 - Ensaios de Encaminhamento

Os testes neste grupo, validam as implementações IPv6 referente as especificações das mensagens *Neighbor Discovery*.

1. Encaminhamento IPv6 antes da aquisição de endereço: Verifica se o roteador devidamente não encaminha tráfego IPv6 antes do processo de aquisição de endereços ser realizada.

2. Sem rota padrão: Verifica se o roteador devidamente não anuncia a si mesmo como um roteador padrão na LAN enquanto não existir rota padrão na interface WAN.

3. Loop de encaminhamento: Verifica se o roteador devidamente previne loops de roteamento descartando pacotes que correspondem as rotas agregadas nos prefixos delegados.

4. Encaminhamento de *Unqiue Local Address Forwarding*: Verifica se o roteador devidamente faz o roteamento de prefixos ULA como um roteador de acesso.

2.4 Protocolos da camada de rede

Como pode-se observar nos itens da seção 2.3, a norma RFC 7084 enfoca sobre o provisionamento básico de um roteador IPv6 e o provisionamento de dispositivos conectados a ele, por meio mensagens ICMPv6, DHCPv6 com computador de teste. Nesta seção será abordado em detalhes a função dos campos e tipos de mensagens ICMPv6 e DHCPv6 usadas nos ensaios.

2.4.1 IPv4

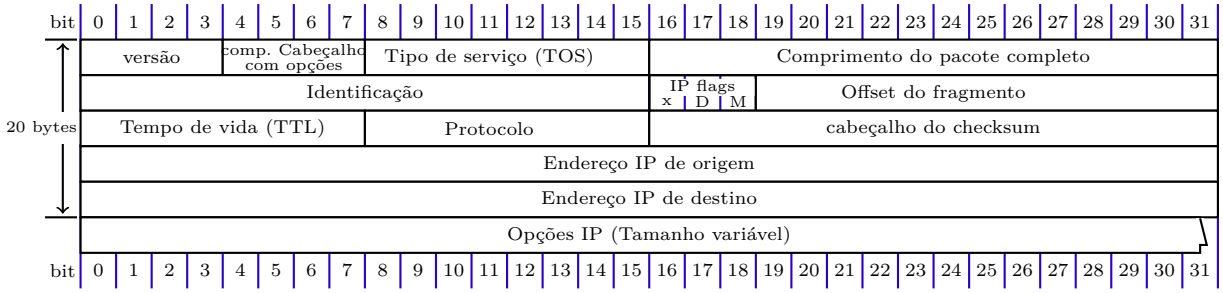
O Protocolo de Internet versão 4 (IPv4) é a quarta versão do Protocolo de Internet (IP). Ele é um dos principais protocolos de padrões baseados em métodos de interconexão de redes na Internet, e foi a primeira versão implementada para a produção da ARPANET [4], em 1983. Ele ainda roteia a maior parte do tráfego da Internet de hoje, apesar da contínua implementação de um sucessor do protocolo, o IPv6. O IPv4 está descrito no IETF publicação RFC 791 (setembro de 1981), em substituição a anterior definição (RFC 760, de janeiro de 1980).

2.4.2 IPv6

IPv6, (Internet Protocol versão 6) é a versão mais atual do protocolo IP. Sua criação é fruto do esforço do IETF para criar a "nova geração do IP"(IPng: *Internet Protocol next generation*), cujas linhas mestras foram descritas por Scott Bradner e Allison Marken, em 1994, na RFC 1752 (BRADNER; MANKIN, 1995). Sua principal especificação encontra-se na RFC 2460. O protocolo está sendo implantado gradativamente na Internet e deve funcionar lado a lado com o IPv4, numa situação tecnicamente chamada

[4] *Advanced Research Projects Agency Network* (ARPANET)

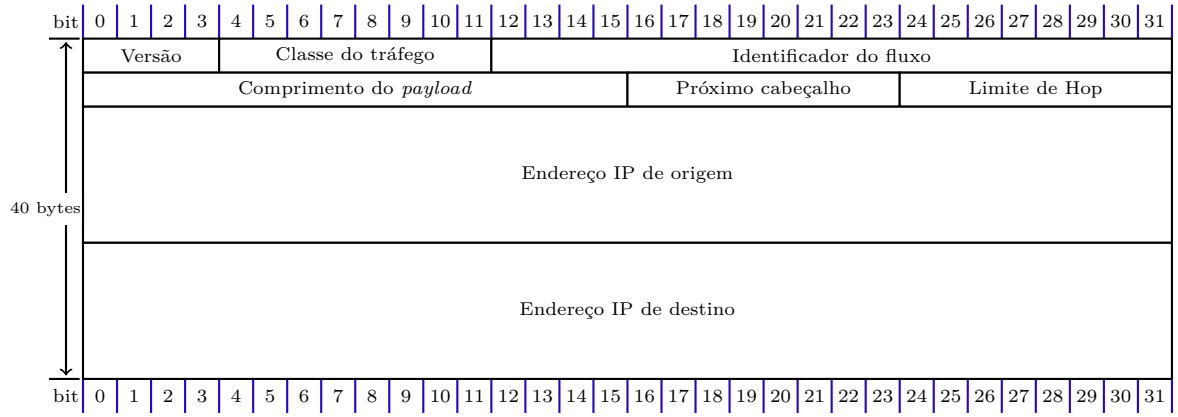
Figura 2 – Cabeçalho do quadro IPv4



Fonte: Tabascoeye (2014)

de "pilha dupla"ou "*dual stack*", por algum tempo. A longo prazo, o IPv6 tem como objetivo substituir o IPv4, que só suporta cerca de quatro bilhões de endereços IP, contra cerca de 3,4x10 38 endereços do novo do protocolo. A previsão para a exaustão de todos os endereços IPv4 livres para atribuição a operadores era de julho de 2011, o que significa que a implantação do IPv6 vem ocorrendo de forma gradativa através de diferentes técnicas como, por exemplo, tunelamento, pilha dupla ou tradução.

Figura 3 – Cabeçalho IPv6



Fonte: Tabascoeye (2014)

A figura 5 apresenta os campos do cabeçalho IPv6. Com tamanho de 40 bytes, é duas vezes maior que o IPv4. A razão é que boa parte do cabeçalho é alocado aos 16 bytes dos endereços de origem e destino. Todos os campos são descritos a seguir:

Versão(4 bits): Este campo contém a versão do protocolo. No caso de IPv4 o valor será 6.

Classe do tráfego (1 Byte): Mesmo recurso do IPv4 (QoS) usado para classificar os diferentes tipos de pacotes dando priorização de banda e recurso entre os nós e roteadores.

Identificador do fluxo (20 Bits): Por meio deste recurso quando associado ao endereço de destino, permite que o roteador não abra cada pacote recebido, assim oferecendo melhor performance para serviços de tempo real.

Comprimento do *Payload* (2 Bytes): Comprimento dos dados transportados. No IPv6 não é considerado o tamanho do cabeçalho.

Próximo cabeçalho (1 Byte): Indica próximo cabeçalho (protocolo) após o fim do cabeçalho IPv6.

Ex: ICMPv6, DHCPv6, TCP, UDP.

Limite de *Hop* (1 Byte): Representa o número de encaminhamentos antes do pacote ser destruído.

Endereço IP de origem(16 Bytes): Este campo contém o endereço IP de 128 bits do originador do pacote.

Endereço IP de destino (16 Bytes): Este campo contém o endereço pretendido do receptor do pacote. Pode ser o endereço do destino final ou do próximo roteador.

2.4.3 Tipos e grupos de endereços IPv6

Há três tipos de endereço no IPv6. O tipo de endereço *unicast* é destinado para comunicações nodo um-a-um, já o *multicast* é usado para comunicação de um nodo para vários nodos e o *anycast* para endereçar um nodo configurado em múltiplos locais. Já as faixas de endereços especiais do IPv6 são apresentadas na tabela .

Tabela 1 – Faixas de endereços especiais.

Endereço	**Descrição**
::/0	Rota padrão
::/128	Não especificado
::1/128	*loopback*
::FFFF:0:0/96	Endereços IPv4 mapeados
2001::/32	Teredo
2001:DB8::/32	Documentação
2002::/16	Transição IPv6 para IPv4
FC00::/7	Endereço local único
FE80::/10	Prefixo de endereço de link local
FF00::/8	Prefixo de endereços multicast

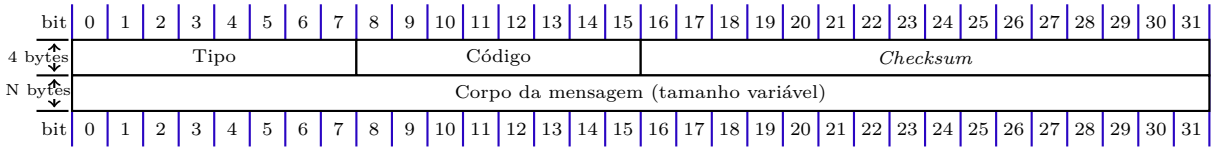
Fonte: Stretch (2016)

Os grupos e tipos de endereços são fortemente manipulados durante os ensaios na detecção de endereços duplicados, atribuição de endereços globais e locais.

2.4.4 ICMPv6

ICMPv6 é mais poderoso que o ICMPv4 e seu propósito é fornecer mecanismos de interação entre os nós conectados no mesmo enlace (HAGEN, 2006). Suas características e mecanismos serão estudadas nesta seção. Toda mensagem ICMPv6 possui a seguinte estrutura de cabeçalho:

Figura 4 – Cabeçalho mensagem ICMPv6



Fonte: os autores.

- tipo (1 byte): indica o tipo da mensagem ICMPv6 de informação ou de erro.
- Código (1 Byte):
- Checksum (2 Bytes): depende dos demais campos para ser definido seu valor, porém serve para determinar se houve algum erro na mensagem ICMPv6.

- Corpo da mensagem (tamanho variável):

No corpo da mensagem ICMPv6, pode-se transportar dois tipos de classes de mensagens. A primeira são mensagens de relatórios e a outra são mensagens de erros com seus respectivos tamanhos dependendo do tipo. Entretanto, não devem exceder o limite do MTU do IPv6 de 1280 Bytes. Toda mensagem ICMPv6 é precedida de um cabeçalho IPv6, conforme reportado na seção 2.4.2.

2.4.5 Os tipos de mensagens ICMPv6

A função do protocolo ICMPv6 é fazer o controle e manutenção da rede com o objetivo de mantê-la operacional através de mensagens de descoberta dos hosts e reporte de erro (NARTEN; NORDMARK; SIMPSON, 1998). Os mecanismos de controle são providos através de mensagens descritas no corpo da mensagem ICMPv6 e identificada através de um código no cabeçalho ICMPv6.

As mensagens ICMPv6 usadas nos testes são descritas abaixo. Consulte a RFC 2461 para mais detalhes referentes à especificação dos campos de cada mensagem.

Tabela 2 – Tipos de mensagens ICMPv6.

Mensagens ICMPv6	**Descrição**
Router Discovery	Mecanismo para que os hosts descubram os roteadores conectados no mesmo link
Prefix Discovery	Mecanismo no qual os hosts descobrem o conjunto de prefixo de endereços conectados no mesmo link.
Parameter Discovery	Mecanismo no qual um nó aprende os parâmetros como por exmeplo: MTU, Hop Limit para ser usado nos pacotes de saída da rede.
Address Autoconfiguration	Mecanismo no qual os nós podem configurar um endereço automaticamente na interface.
Address resolution	Mecanismo para que os nós possam determinar o endereço de link de um nó dando apenas o endereço IP do destino.
Duplicate Address Detection	Mecanismo para determinar que um endereço pretendido já não está em uso por outro nó.
Router Solicitation	Desde quando a interface esteja ativa, os hosts podem enviar *Router Solicitations* para que os roteadores gerem imediatamente mensagens *Router Advertisements*.
Router Advertisement	O roteador anuncia a sua presença junto de vários parâmetros de link e internet periodicamente, ou em resposta para uma mensagem *Router Solicitation*.
Neighbor Solicitation	Mensagem enviada por um nó para determinar o endereço MAC dos nós vizinhos ou verificar se um vizinho ainda estão acessível através do endereço de link armazenado na tabela de endereços de link.
Neighbor Advertisement	Resposta na presença de uma mensagem *Neighbor Solicitation*.

Fonte: Hagen (2006)

2.4.6 DHCPv6

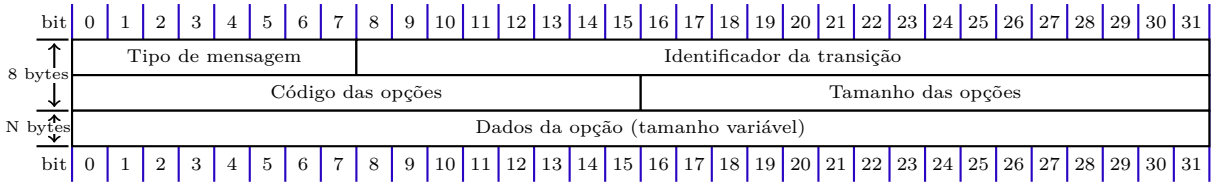
O DHCP é um serviço para configurar endereços de rede aos hosts. No entanto, numa rede IPv6, os hosts podem configuram o próprio endereço de rede sem a necessidade de um servidor DHCP através do mecanismo *stateless autoconfiguration* especificado na RFC 3736 (DROMS, 2004). Nas redes com servidor DHCPv6 chamado *Stateful autoconfiguration* ou *Stateful DHCPv6*, há um protocolo de mensagens de configuração de parâmetros e outras informações definidos pela RFC 3315 (DROMS et al., 2003). A Anatel exige que os roteadores IPv6 suportam ambos mecanismos.

Os campos do cabeçalho DHCPv6 são descritos a seguir:

Tipo de mensagem (1 byte): define o tipo de mensagem transmitida pelo cliente ou servidor e já detalhado na tabela 3.

Identificador da transição (3 bytes): número gerado pelo cliente a cada nova transação para relacionar específicas requisições.

Figura 5 – Cabeçalho mensagem DHCPv6



Fonte: os autores.

Código de opções (2 bytes): As principais opções utilizadas na RFC 7084 são descritas na tabela 4. Consulte a RFC 3315 para acessar a lista completa de opções.

Tamanho do campo dados das opções (2 bytes): Este campo indica o tamanho do campo de dados de opções.

Dados da opção: Finalmente as informações para configuração definida no campo código da opção e seu tamanho é variável.

2.4.7 Os tipos de mensagens DHCPv6

DHCP define os seguintes tipos de mensagens detalhados na RFC 3315 e avaliados nos ensaios de certificação da Anatel nos roteadores IPv6.

Tabela 3 – Tipos de mensagens DHCPv6.

Mensagens DHCPv6	**Descrição**
Solicit	Usado pelo cliente para localizar servidores DHCP
Adivertise	Usado pelo servidor DHCP em resposta para o *Solicit*
Resquest	Usado pelo cliente para coletar informações do servidor.
Confirm	Usado pelo cliente para verificar se seus os parâmetros de configuração e endereços estão validos em seu link
Renew	Usado pelo cliente estender as configurações de endereço IP e renova-las com o servidor quando estão expirarem
Rebind	Usado pelo cliente quando não recebe a confirmação de recepção da mensagem *Renew*. Nela reinforma os parâmetros de configuração de endereço IP e sua renovação
Reply	Usado pelo servidor para responder as mensagens dos clientes: *solicit*, *request*, *renew* e *rebind*
Release	Usado pelos clientes para liberar seu endereço IP. Esta mensagem é enviada para o servidor do qual o endereço foi recebido
Decline	Usado pelos clientes para indicar para o servidor que um ou mais endereços foram atribuídos a eles estão já sendo usado no link
Reconfigure	Usado pelo servidor DHCP para informar aos clientes que o servidor tem uma nova informação de configuração. Neste caso, os clientes devem enviar as mensagens de *renew request* para obter a nova informação do servidor
Information Request	enviado pelos clientes para solicitar informação adicional dos parâmetros de configuração (Sem informação de endereço IP)
Relay Forw	Usado pelos agentes DHCP *relays* para encaminhar informações dos clientes para os servidores. Os agentes *relays* encapsulam as mensagens dos clientes para serem enviadas diretamente ao servidor DHCP ou a outros agentes *relays*
Relay-Repl	Usada pelos servidores DHCP para enviar mensagens para os clientes através dos agentes DHCP *relays*

Fonte: Hagen (2006)

Todas mensagens listadas na tabela 3 são negociadas e avaliadas nos ensaios dos grupos descritos nas subseções 2.3.1, 2.3.2 e 2.3.3. Além de manipular o campo código de opção detalhados na tabela 4. Para maiores detalhes sobre a arquitetura dos campos e *flags* referente aos tipos de mensagens ICMPv6 e DHCPv6 utilizadas nos ensaios consulte as RFC's 3315 (DROMS et al., 2003) e 4443 (CONTA; DEERING; GUPTA, 2006).

Tabela 4 – Tipos de informações DHCPv6 no campo código de opções.

Opção	**Descrição**
Identificador de cliente	Usado pelo cliente como DHCP *Unique Identifier* DUID
Identificador de servidor	Usado pelo servidor como DUID
Associação de Identidade para endereço não-temporários (IA_NA)	Usado para indicar o IA_NA, os parâmetros, e endereços não-temporários associados com ele.
Associação de Identidade para endereço temporários (IA_TA)	Usado para indicar o IA_TA, os parâmetros, e endereços temporários associados com ele. Todos os endereços com está opção são usados como endereços temporários pelo cliente.
Pedido de opções	Usado na troca de mensagens entre o cliente e o servidor para identificar uma lista de opções.

Fonte: Hagen (2006)

Todos estes recursos do DHCPv6 são garantidos através dos ensaios da RFC 7084.

2.5 Arquitetura do software de teste

O grande desafio do projeto será o desenvolvimento das sub-rotinas, em especial da primeira rotina, pois a nível de software as demais rotinas se baseiam no desenvolvimento da primeira. Nesta etapa, serão pesquisados bibliotecas e softwares, de preferência código fonte aberto, que ofereçam funções que permitam criar, enviar, manipular e analisar quadros IPv6 e que sejam desvinculados do hardware, podendo ser instalado em qualquer computador com arquitetura comercial x86 ou amd64. Com base nesta proposta foram estudados três ferramentas: Pcap, Scapy e Ostinato.

A Ostinato é um gerador de pacotes e gerador de tráfego de rede com uma GUI amigável. Também uma poderosa API Python para automação de testes de rede. Permite criar e enviar pacotes de vários fluxos com protocolos diferentes em taxas diferentes. A Ostinato tem como objetivo fornecer um gerador de tráfego e uma ferramenta de teste de rede para cada engenheiro e desenvolvedor de rede - algo que não é possível atualmente com os equipamentos de teste de rede comercial existentes. Com a ferramenta certa, os desenvolvedores e engenheiros de rede podem melhorar seu trabalho e melhorar a qualidade dos produtos de rede (P, 2019). O software atende quase todos os requisitos do projeto, no entanto, há custos para baixar o software e a API em python usada para automatização dos ensaios. Os custos totais podem chegar em torno de cento e nove dólares para versões Linux.

O Scapy é uma poderosa ferramenta de manipulação interativa de pacotes. Ele é capaz de forjar e decodificar um grande número de protocolos (802.11, Ethernet, VLAN, IPv4, IPv6,etc) conforme discutido na seção 3.1.5. Além disso, permite *sniffar* os pacotes recebidos, o qual é um recurso fundamental para o desenvolvimento do software. Escrito em Python, oferece os recursos necessários para desenvolvimento das rotinas e criação de novos laços para implementação da própria rotina. (BIONDI; COMMUNITY, 2015).

Em contraste, apesar da biblioteca Pcap ser também licenciada em código aberto, oferece somente recursos para sniffar para análise dos campos do pacote. Entretanto, não possui implementadas funções para forjar pacotes, necessitando assim de implementação. Por ser desenvolvido em C, apesar de ter melhor performance, seria necessário despender um grande esforço comparado a outras linguagens para implementação das rotinas de envio. Por exemplo, para criar o algoritmo de um pacote em C, em média são 60 linhas e através do aplicativo Scapy apenas 2 linhas (BIONDI; COMMUNITY, 2015).

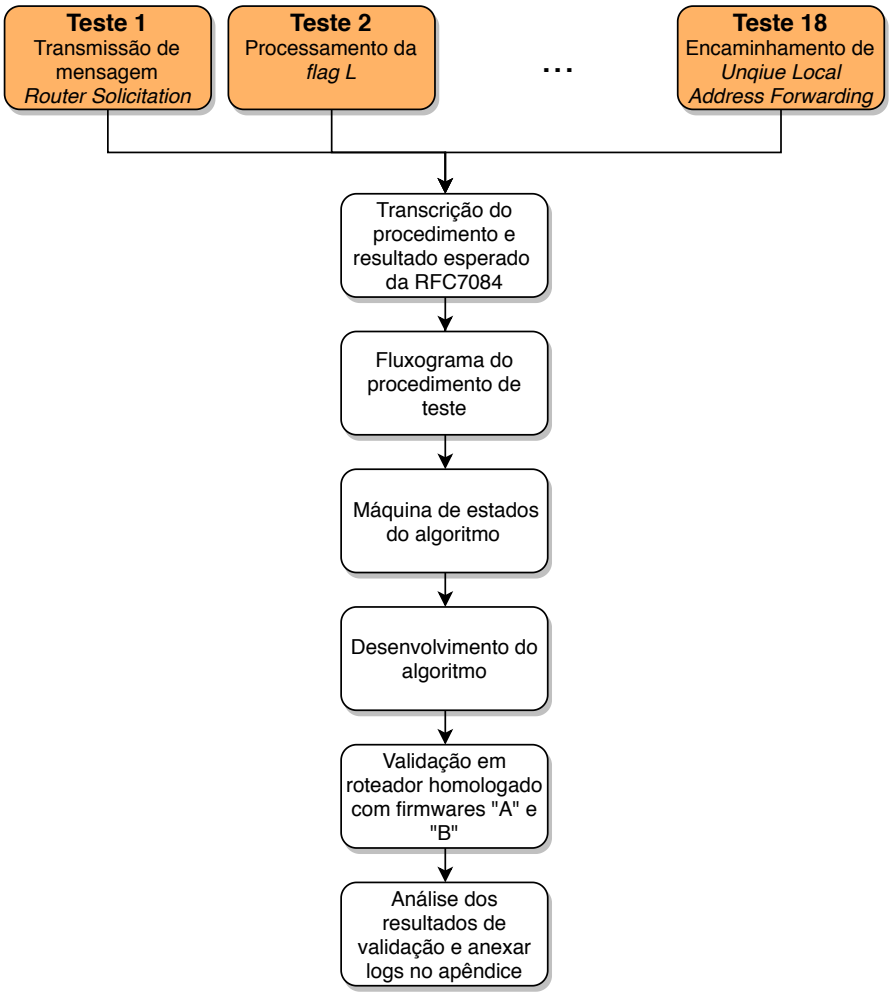
A vantagem do Scapy em relação ao Pcap é possuir vários protocolos mapeados nos quais pode-se manipular todos os campos, além de conter classes e métodos para sniffar qualquer campo dos pacotes recebidos.

3 METODOLOGIA

3.1 Metodologia

O software contemplará os 18 casos da RFC 7084 citados na seção 2.3 usados na validação do protocolo IPv6 nas interfaces WAN e LAN, além de certificar conectividade entre elas. Será apresentado nesta seção um fluxograma com a proposta de concepção desses 18 casos. Nele constará as seguintes etapas: transcrição do procedimento de testes descritos pela RFC7084, a montagem de um fluxograma do procedimento e mensagens negociadas, descrição do comportamento do algoritmo de testes por meio de máquinas de estado, desenvolvimento do algoritmo baseado nestas máquinas de estados, validação do algoritmo através de testes em um roteador devidamente homologado com duas versões de firmware (A e B) com sucesso e falha no respectivo ensaio e, por fim, análise das mensagens obtidas com as duas versões de firmware, que serão anexadas no apêndice deste trabalho de conclusão de curso. Todas estas etapas estão representadas no fluxograma da figura 6.

Figura 6 – Fluxograma de desenvolvimento do software



Fonte: os autores.

Essencialmente, este software será composto por subrotinas que forjarão mensagens IPv6, DHCPv6 e ICMPv6 além de manipular seus respectivos campos antes de enviá-las ao ESE. Além disso, contém as implementações para análise de mensagens de resposta do ESE, que serão usadas para checar se o roteador cumpre as exigências normativas. Como preparação do ambiente de teste, cada grupo possui um conjunto comum de mensagens IPv6 negociadas previamente antes de cada teste específico. Este conjunto de mensagens predefinidos fazem parte da negociação inicial do teste específico e portanto também deverão ser contemplados pelo software. Antes de iniciar o desenvolvimento das rotinas, faz parte deste trabalho estudar o escopo destas mensagens IPv6 negociadas em cada item da RFC 7084. Desta forma, será importante explorar os ensaios durante seu desenvolvimento, apresentar os cenários, as mensagens negociadas e a sequência em que elas ocorrem, além de descrever cada resposta esperada do ESE no software de teste, para então poder especificar o funcionamento do robô de teste. Quando conveniente será descrito qual a função de uma determinada flag manipulada em alguns casos de teste.

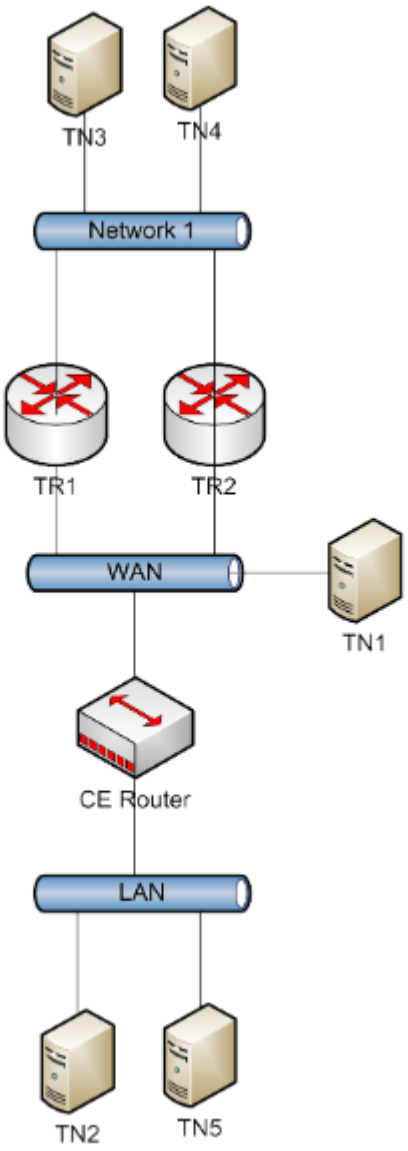
O produto a ser usado na validação do software, será um roteador ONT GPON com portas 2 FXS, 4 LAN e uma interface WLAN 2,4 GHz, modelo ONT 142 NW da fabricante Intelbras. Este produto foi submetido a uma extensa e repetida bateria de testes na RFC 7084, totalizando 9 testes no laboratório CPqD antes de ser aprovado nos 18 casos de teste da RFC. Cada um destes ensaios foi realizado com uma nova versão de firmware na tentativa de corrigir os problemas reportados pelo laboratório CPqD no final de cada teste completo da RFC7084. A nona versão foi aprovada em todos os dezoito casos de testes da RFC. O histórico das mensagens IPv6 negociadas em item da RFC 7084 reprovado e aprovado sob cada versão de firmware estarão apresentados no apêndice X.

A primeira sob-rotina a ser implementada será para testar o item 1 do grupo WAN, que será aferido a partir de duas versões de firmware da ONT142NW no qual a versão "A"reprova e a "B"aprova no respectivo ensaio. Neste primeiro momento, os logs dos pacotes a serem transmitidos e recebidos serão avaliados manualmente para confirmar se apresentarão o comportamento esperado conforme determinado pela RFC descrito na seção 3.1.8. Além disso, se verificará se os logs de mensagens de resposta de ESE, coincidem com o comportamento apresentado nos ensaios executados pelo CPqD durante a certificação IPv6 do roteador ONT142NW sob as mesmas versões de firmware "A"e "B".

3.1.1 Cenário de testes RFC 7084

Todos os grupos de teste (WAN, LAN e encaminhamento) usam a mesma topologia apresentada na figura 7. A infraestrutura do ensaio é composta pelo roteador sob ensaio (*CE router*) e dois links conectados nas interfaces de rede LAN e WAN do ESE.

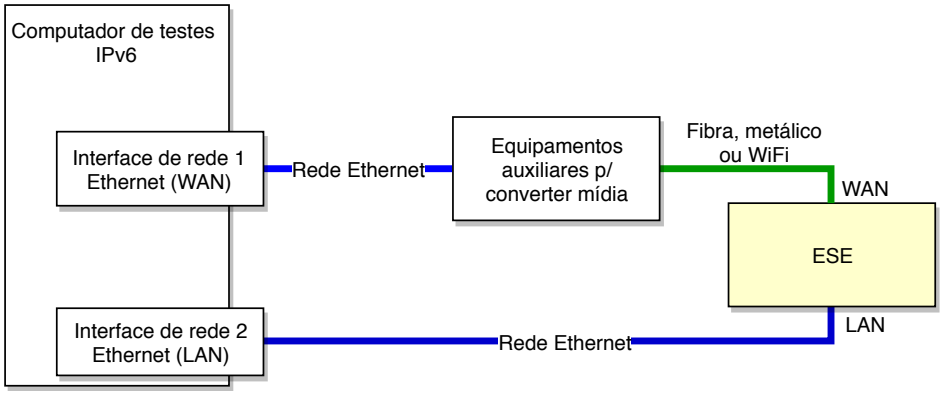
Figura 7 – Topologia dos ensaios IPv6 em roteadores de acesso a rede conforme RFC 7084.



Fonte: Universidade Hampshire

A topologia apresentada na figura 7 pode ser simplificada através da emulação por software dos TN's e TR's. Como resultado, o cenário de teste final é constituído por um computador de teste IPv6, uma placa de rede que simula a rede WAN da operadora de serviços, uma placa de rede LAN para simular os dispositivos da rede de usuário final, o roteador IPv6 sob ensaio e os equipamentos auxiliares que convertem a mídia da interface WAN do roteador sob ensaio para o padrão ethernet do computador de teste IPv6. Portanto, a topologia completa de teste exibida na figura 7 fica reduzida conforme a figura 8.

Figura 8 – Cenário de teste aplicado nos ensaios IPv6



Fonte: os autores.

3.1.2 Desenvolvimento do software

O software de teste para roteadores IPv6 será desenvolvido sob um sistema operacional baseado em Linux, escolhido principalmente por ser de código fonte aberto e oferecer ampla documentação como suporte de desenvolvimento e contar com a colaboração de programadores ao redor do mundo que mantém o sistema atualizado. O hardware do computador de teste será um processador Intel Core i5, 500 GBytes de disco rígido, 4 GBytes de memória RAM, com duas placas de rede gigabit ethernet modelo TP-Link TG3468.

3.1.3 Interface gráfica de usuário

O usuário terá acesso a uma interface gráfica para selecionar o item da norma a ser testado. Em cada item constará a numeração e o título do teste conforme RFC. Haverá um botão iniciar para dar início ao conjunto de itens selecionados. No final da mensagem deverá ser exibido um resultado de aprovado ou reprovado.

3.1.4 Script com as Rotinas de teste da RFC 7084

O script contém o conjunto de mensagens pré-definidas do protocolo IPv6 a serem enviados para o ESE. Através do Scapy também serão capturadas as respostas provenientes do roteador e analisadas. Ao final deste processo, será enviado um sinal à camada Interface Gráfica de Usuário (IGU) para informar se as respostas estão conforme definido pela norma. Mensagens não correspondentes dentro do escopo do protocolo IPv6, ICMPv6, DHCPv6 ou da norma RFC 7084 serão ignoradas. Mensagens de resposta do ESE que não atendem aos requisitos exigidas pela norma serão consideradas como descumprimento do item avaliado e será enviado um sinal de reprovado para a interface de usuário.

3.1.5 Biblioteca Scapy

O Scapy é um framework desenvolvido em Python que permite forjar pacotes da camada enlace e transporte, através de classes e atributos que representam o tipo de pacote/quadro/mensagem e seus respectivos campos. O comando `explore()` exibe todos os protocolos e mensagens suportados pelo software. Por exemplo, na figura 9, são exibidos todos os campos e *flags* configuráveis da mensagem ICMPv6 *Neighbor Advertisement* usada em diversos testes da RFC.

Figura 9 – Exemplo da mensagem ICMPv6 *Neighbor Advertisement* e seus campos dos editáveis da através da interface do software Scapy

```
>>> ls(ICMPv6ND_NA)
type       : ByteEnumField                    = (136)
code       : ByteField                        = (0)
cksum      : XShortField                      = (None)
R          : BitField (1 bit)                 = (1)
S          : BitField (1 bit)                 = (0)
O          : BitField (1 bit)                 = (1)
res        : XBitField (29 bits)              = (0)
tgt        : IP6Field                         = ('::')
```

Fonte: os autores.

A primeira coluna representa o nome do campo ou *flag*, a segunda coluna detalha o tipo da variável e seu tamanho, e a última coluna apresenta seu valor padrão.

No caso do Scapy, a montagem do quadro Ethernet a ser transmitido pela interface de rede é feita de forma manual. Portanto, deverá ser implementada a automatização da confecção das mensagens de acordo com a RFC. A figura 10 demonstra como é feita montagem no Scapy de um quadro ethernet para transmissão de uma mensagem ICMPv6 *Neighbor Advertisment* e também exibe seu conteúdo antes de ser transmitido pela interface de rede.

Figura 10 – Exemplo de um quadro Ethernet forjado via software Scapy para envio de uma mensagem ICMPv6 *Neighbor Advertisment*

```
>>> pkt = Ether()/IPv6()/ICMPv6ND_NA()
>>> pkt.show()
WARNING: No route found for IPv6 destination ff02::1 (no default route?)
WARNING: No route found for IPv6 destination ff02::1 (no default route?)
###[ Ethernet ]###
  dst= 33:33:00:00:00:01
  src= 00:00:00:00:00:00
  type= 0x86dd
###[ IPv6 ]###
     version= 6
     tc= 0
     fl= 0
     plen= None
     nh= ICMPv6
     hlim= 255
     src= ::
     dst= ff02::1
###[ ICMPv6 Neighbor Discovery - Neighbor Advertisement ]###
        type= Neighbor Advertisement
        code= 0
        cksum= None
        R= 1
        S= 0
        O= 1
        res= 0x0
        tgt= ::
```

Fonte: os autores.

O software incluirá uma interface de usuário para administração e conferência dos resultados dos testes. Por esta interface, serão executados os scripts com as rotinas para cada item da RFC. O script monta o cabeçalho, e o corpo das mensagens ICMPv6 ou DHCPv6 que serão enviadas pela API do *framework* Scapy. O Scapy é capaz de forjar os pacotes e acessar interface de rede para transmissão e recepção de mensagens IPv6. A especificação do Scapy é estudada em detalhes a partir da seção 3.1.5. A estrutura do software é apresentada em forma de camadas através da tabela 5.

Tabela 5 – Arquitetura do software de teste RFC 7084

Interface gráfica de usuário
Script de teste rotinas de teste RFC7084
Scapy Libs Socket (transporte, IP, enlace)
Drivers dos dispositivos
Interface física

Fonte: os autores.

3.1.6 Ensaios de validação do software

Ao implementar a primeira rotina, o software será avaliado ao testá-lo sob um ESE (equipamento sob teste) com comportamento de falha e também de sucesso previamente conhecido, conforme citado na seção 3.1. O teste "Transmissão de *Router Solicitation*"é o primeiro ensaio da RFC 7084 aplicado sob o Equipamento a ser ensaiado no processo de certificação IPv6, e será apresentado em detalhes no item na seção 3.1.8. Se apresentar o comportamento esperado, conforme descrito na seção 3.1.8, o roteador estará apto para realizar o teste 2 (Processamento da flag L) do grupo de testes 1 (WAN) (HAMPSHIRE; LABORATORIES, 2015), conforme mencionado na seção 2.3.

3.1.7 Setup básico 1 de teste IPv6(Possível apêndice)

Neste seção é exposto o conjunto básico de mensagens negociadas entre o ESE e os TN's conectados na porta WAN do Equipamento Sob Ensaio (ESE) para validação do IPv6 na interface WAN.

1. TR1 transmite uma mensagem *Router Advertisement* (RA) para todos endereços do grupo *all-node multicast* com as *flags* M e O ativas. O limite *hop* do RA é definido em 64. O *Router Advertisement* inclui parâmetro *Prefix Advertisement* (*Prefix Advertisement* (PA)) com o prefixo global com a flag L com nível lógico "1"e a flag B em "0". Isso deverá adicionar o TR1 em sua lista de roteamento padrão e calcular o tempo de alcance. O parâmetro *Router Lifetimes* é grande o suficiente que não expira durante o teste.

2. O TR1 transmite uma mensagem *Echo Request* para o *NUT* e ele responde aos *Neighbor Solicitations*. E os NS esperam pelo *Echo Reply* do NUT. O resultado esperado é que o NUT seja capaz de resolver o endereço do TR1 e criar uma entrada *Neighbor Cache* com estado alcançavel.

3. O ESE transmite um DHCPv6 *Solicit Message* para todos *"DHCP_Relay_agents_and_Servers"* para o endereço *multicast* (FF02::1:2). O TN1 responde com uma mensagem DHCPv6 *Advertise*. O ESE envia um mensagem DHCPv6 *Resquest* para o TN1 pedindo para confirmar o endereço e a configuração. O TN1 responde com uma mensagem *Reply* contendo a confirmação do endereço e configuração. A mensagem DHCPv6 *Reply* contém as opções IANA e IADP T1 definidas em 50 segundos e a T2 para 80 segundos. O DHCPv6 *Reply* também contém um DNS *Recursive Name*

Server Option que inclui o TN3's com endereços globais e a lista com domínio de pesquisa que inclui "text.example.com"

3.1.8 Teste 1 - Transmissão de *Router Solicitation*

Propósito:

Verificar a capacidade do roteador em gerar um endereço de link-local e finalizar as mensagens *Duplicate Address Detection* antes de enviar qualquer *Router Solicitation* através das etapas a seguir:

Referência: RFC 7084 item W-2.

Procedimento:

1. Inicializar todos os dispositivos na interface WAN.
2. Observar os pacotes transmitidos pelo roteador sob certificação.

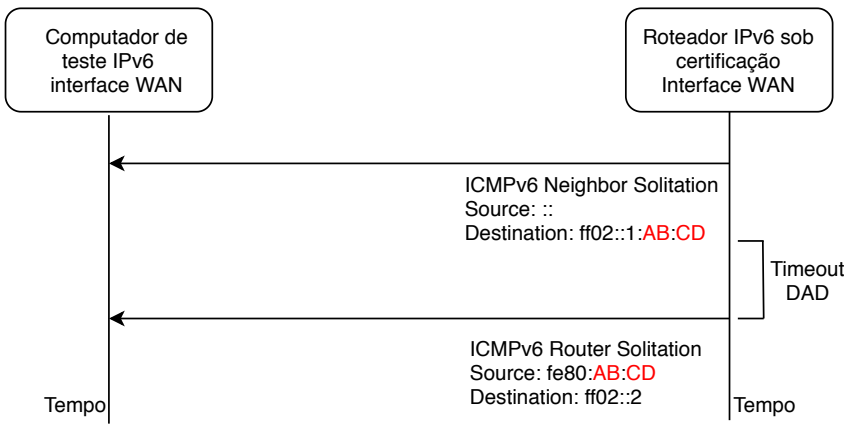
Resultados esperados:

- No **Passo 2:** O Roteador sob certificação deve concluir a *Duplicate Address Detection* nos endereços de link locais antes de Transmitir *Router Solicitation*. As mensagens de *Router Solicitations* devem ser transmitidas com uma fonte de endereço de link local e o endereço *multicast* de todos os roteadores (ff02::2).

3.1.8.1 Fluxograma do procedimento de teste

Conforme figura 11, o processo de *Duplicate Address Detection* (DAD) é iniciado assim que roteador envia uma mensagem ICMPv6 do tipo *Neighbor Solicitation* para endereço de *multicast* do nodo solicitado (o próprio endereço do ESE), com o propósito de verificar se algum nodo responderá como dono deste endereço. Se nenhum nodo responder dentro de um determinado tempo, aquele endereço será considerado como único e o processo de DAD é finalizado.

Figura 11 – Diagrama de mensagens do teste 1 conforme RFC 7084



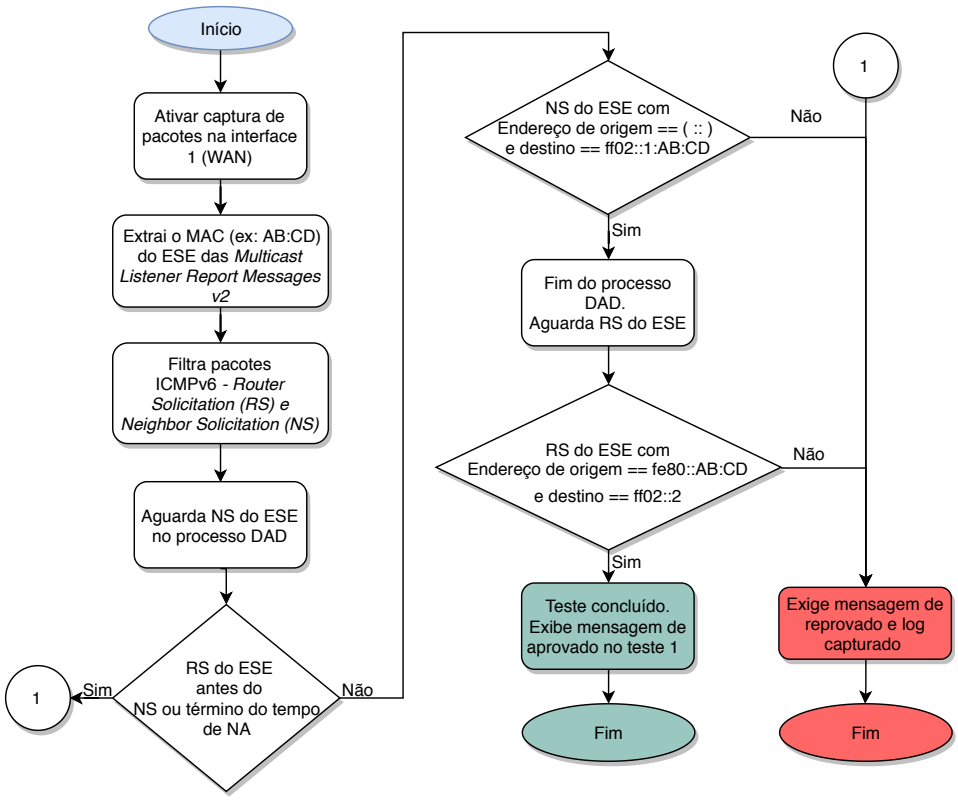
Fonte: os autores.

Assim que o processo de DAD é concluído o roteador sob certificação deverá enviar a mensagem ICMPv6 de *Router Solicitation* para que ele seja aprovado no teste 1.

3.1.8.2 Máquina de estados do algoritmo

O script do teste 1 valida dois processos: o processo DAD e a subsequente recepção da mensagem RS. O algoritmo reprova se o ESE receber mensagens ICMPv6 de *Router Solicitation* (RS) antes ou durante o processo DAD. Ao fim do DAD, o script aguarda mensagens RS do ESE para concluir o teste 1. Nesse teste, os campos avaliados são: o cabeçalho Ethernet e ICMPv6 para leitura dos endereços MAC e identificação o tipo de mensagem, o endereço IPv6 de origem e destino para atender os requisitos do teste.

Figura 12 – Diagrama do algoritmo para o teste 1



Fonte: os autores.

Fica entendido que o software contempla todas as temporizações para atuar automaticamente em caso de inoperabilidade do ESE durante o ensaio. Neste caso, o software encerra com reporte de falha do ESE e volta ao seu estado inicial.

3.1.8.3 Validação dos resultados no roteador certificado

No teste 1 não há transmissão de mensagens pelo computador de teste. As mensagens transmitidas pelo roteador homologado com versão de firmware "A"produziu as mensagens apresentadas na figura 13.

Figura 13 – Mensagens capturadas pelo computador de teste durante ensaio do teste 1

No.	Time	Source	Destination	Protocol	Length	Info
2	0.529993000	::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
3	0.573337000	::	ff02::1:ff2d:3b8e	ICMPv6	78	Neighbor Solicitation for fe80::221:6aff:fe2d:3b8e
8	1.576722000	fe80::221:6aff:fe2d:3b8e	ff02::2	ICMPv6	70	Router Solicitation from 00:21:6a:2d:3b:8e
9	1.577519000	fe80::221:6aff:fe2d:3b8e	ff02::2	ICMPv6	62	Router Solicitation

Fonte: os autores.

Pode-se observar que as diretrizes de aprovação do teste 1 foram atendidas, de forma que houve o processo de DAD concluído sem anomalias e a subsequente conclusão do teste com transmissão do RS pelo ESE conforme RFC7084.

3.1.9 Cronograma

1. Elaboração da proposta de TC.
2. Estudo detalhado dos cenários de teste com IPv6.
3. Definição do fluxo de testes segundo uma máquina de estados.
4. Criação da rotina de validação do primeiro cenário segundo a RFC usando o framework Scapy.
5. Aplicação da rotina sobre equipamento com comportamento conhecido de falha e sucesso em cenário controlado.
6. Implementação das demais rotinas para conclusão de todos os ensaios de validação.
7. Validação do software através do produto homologado com a versão de firmware "A"e "B".
8. Escrita do TC I.
9. Desenvolvimento automação das rotinas.
10. Teste e correções.
11. Escrita do TC II.

	2019					2019				
	MAR	ABR	MAI	JUN	JUL	AGO	SET	OUT	NOV	DEZ
1	√	√								
2		√	√	√						
3			√	√	√					
4			√	√	√					
5				√	√	√				
6					√	√	√			
7					√	√	√			
8						√	√	√		
9						√	√	√	√	
10						√	√	√	√	
11								√	√	√

4 CONCLUSÕES

Este trabalho tem o desafio de realizar a implementação de um software capaz de automatizar os ensaios da RFC 7084 em roteadores para obtenção de certificação da Anatel. No capítulo 2, procurou-se apresentar os recursos dos protocolos IPv6 avaliados pela RFC 7084 descrevendo suas respectivas características. No Capítulo 3, procurou-se descrever a especificação do software a ser desenvolvido e quais recursos e estratégias adotados para sua implementação. Em seguida, apresentou-se a forma de validação do software e as análises dos resultados através de um roteador homologado Anatel. Por fim, apresentou-se o software através de um computador, o qual faz a validação do IPv6 em conformidade pela Anatel, instalado nas dependências do laboratório de testes do IFSC campus São José.

REFERÊNCIAS

ABRANET, R. *Anatel define para novembro exigência de certificação IPv6 para redes fixas*. 2016. Disponível em: <http://www.abranet.org.br/Noticias/Anatel-define-para-novembro-exigencia-de-certificacao-IPv6-para-redes-fixas-1157.html?UserActiveTemplate=site#.XQgKa3VKiPQ>. Acesso em: 20 mai 2019. Citado 2 vezes nas páginas 26 e 28.

ANATEL. *Regulamento para certificação de equipamentos de telecomunicações quanto aos aspectos de compatibilidade eletromagnética*. [S.l.], 2006. Citado na página 25.

ANATEL. *Regulamento sobre equipamentos de radiocomunicação de radiação restrita*. [S.l.], 2008. Citado na página 25.

ANATEL. *Regulamento para certificação de equipamentos de telecomunicações quanto aos aspectos de segurança elétrica*. [S.l.], 2009. Citado na página 25.

ANATEL. *Grupo de Trabalho para implantação do protocolo IP- Versão 6 nas redes das Prestadoras de Serviços de Telecomunicações*. 2014. Disponível em: <http://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=325769&assuntoPublicacao=null&caminhoRel=null&filtro=1&documentoPath=325769.pdf>. Acesso em: 20 mai 2019. Citado na página 28.

ANATEL. *Organismos de Certificação Designados (OCD)*. 2015. Disponível em: <http://www.anatel.gov.br/setorregulado/organismos-de-certificacao-designados-ocds>. Acesso em: 20 mai 2019. Citado na página 27.

ANATEL. *Homologação de produtos de telecomunicações importados para uso próprio*. 2018. Disponível em: <http://www.anatel.gov.br/setorregulado/orientacoes/forum-de-certificacao/2-uncategorised/431-importacao-para-uso-proprio>. Acesso em: 20 mai 2019. Citado na página 27.

BIONDI, P.; COMMUNITY, S. *About Scapy*. 2015. Disponível em: <https://scapy.readthedocs.io/en/latest/introduction.html#about-scapy>. Acesso em: 20 mai 2019. Citado na página 36.

BRADNER, S.; MANKIN, A. *The Recommendation for the IP Next Generation Protocol*. [S.l.], 1995. Citado na página 31.

BRASIL. *Lei nº 9.472, de 16 de julho de 1997: Lei Geral de Telecomunicações*. 1997. Citado na página 25.

CONTA, A.; DEERING, S.; GUPTA, M. *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*. [S.l.], 2006. <http://www.rfc-editor.org/rfc/rfc4443.txt>. Disponível em: <http://www.rfc-editor.org/rfc/rfc4443.txt>. Citado na página 35.

DROMS, R. *Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6*. [S.l.], 2004. Citado na página 34.

DROMS, R. et al. *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*. [S.l.], 2003. <http://www.rfc-editor.org/rfc/rfc3315.txt>. Disponível em: <http://www.rfc-editor.org/rfc/rfc3315.txt>. Citado 2 vezes nas páginas 34 e 35.

HAGEN, S. *IPv6 Essentials*. 2. ed. [S.l.]: O'Reilly Media, 2006. ISBN 0-596-10058-2. Citado 4 vezes nas páginas 33, 34, 35 e 36.

HAMPSHIRE, U. of N.; LABORATORIES, C. T. *IPv6 READY Conformance Test Scenario CE-Router*. 2015. Disponível em: <https://ipv6ready.org/docs/CE_Router_Conformance_Latest.pdf>. Acesso em: 20 mai 2019. Citado na página 42.

HINDEN, R.; DEERING, S. *IP Version 6 Addressing Architecture*. [S.l.], 2006. <http://www.rfc-editor.org/rfc/rfc4291.txt>. Disponível em: <http://www.rfc-editor.org/rfc/rfc4291.txt>. Citado na página 28.

NARTEN, T.; NORDMARK, E.; SIMPSON, W. *Neighbor Discovery for IP Version 6 (IPv6)*. [S.l.], 1998. Citado na página 34.

NARTEN, T. et al. *Neighbor Discovery for IP version 6 (IPv6)*. [S.l.], 2007. <http://www.rfc-editor.org/rfc/rfc4861.txt>. Disponível em: <http://www.rfc-editor.org/rfc/rfc4861.txt>. Citado na página 30.

P, S. *Ostinato - Gerador de pacotes*. 2019. Disponível em: <https://ostinato.org/>. Acesso em: 20 mai 2019. Citado na página 36.

SINGH, H. et al. *Basic Requirements for IPv6 Customer Edge Routers*. [S.l.], 2013. Citado 2 vezes nas páginas 26 e 30.

STRETCH, J. *IPv6*. 2016. Disponível em: <http://packetlife.net/media/library/8/IPv6.pdf>. Acesso em: 10 mai 2019. Citado na página 33.

TABASCOEYE. *Repositório de cabeçalhos de protocolos de rede em latex*. 2014. Disponível em: <https://github.com/tabascoeye/TikZ-diagrams/tree/master/networking>. Acesso em: 10 jun 2019. Citado na página 32.