

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANA
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE
SERVIDORES E EQUIPAMENTOS DE REDES

ANDRÉ HEIDRICH

IMPLEMENTANDO UM MECANISMO DE TRANSIÇÃO IPv4-IPv6

MONOGRAFIA

CURITIBA

2011

ANDRÉ HEIDRICH

IMPLEMENTANDO UM MECANISMO DE TRANSIÇÃO IPv4-IPv6

Monografia apresentada como requisito parcial para obtenção do grau de especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. MSc. Lincoln Herbert Teixeira

CURITIBA

2011

Á minha avó Anaites de Melo Andrade, cuja inspiração em seu exemplo de vida, me faz buscar ser uma pessoa melhor sempre.

E a minha mãe Ana Maria da Luz Simões Heidrich, no qual seu amor incondicional me traz harmonia e equilíbrio para toda a vida.

RESUMO

HEIDRICH, Andre. **Implementando um mecanismo de transição IPv4-IPv6**. 2011. 40 f. Monografia (Especialização em Gerenciamento de Redes) – Programa de Pós-Graduação em Tecnologia, Universidade Tecnológica Federal do Paraná. Curitiba, 2011.

O propósito desta monografia está em estudar a versão mais recente do protocolo de internet, onde o mesmo passará por um processo de transição que deverá ocorrer brevemente nas redes de computadores mundiais. A pesquisa apresenta conceitos teóricos juntamente com uma aplicação prática simulada em um ambiente real, demonstrando a viabilidade, as funcionalidades e as técnicas utilizadas para a aplicabilidade do protocolo na internet atual. O método mais recomendado para a transição de versões dos protocolos de internet é a chamada técnica de pilha dupla, pois esta apresenta um menor impacto nas redes atuais. Com base na tendência mundial a pesquisa está correlacionada a empresas de redes e telecomunicações, tais como a Global Village Telecom (GVT) onde a prática laboratorial foi realizada, a pesquisa também é de interesse empresarial e não somente para o meio acadêmico, onde futuramente a versão 6 do protocolo de internet será aplicada na empresa com a técnica de pilha dupla, mas também a versão deverá ser adotada a nível mundial pelas demais organizações da área de telecomunicações.

Palavras-chave: IPv6. Protocolo de internet. Pilha dupla. Transição. Redes.

ABSTRACT

HEIDRICH, Andre. **Implementing a IPv4-IPv6 transition mechanisms**. 2011. 40 f. Essay (Graduate Certificate in Networking and Systems Administration) - Graduate Programs in Technology, Federal Technological University of Paraná. Curitiba, 2011.

The goal of this essay is to study the most recent versions of the Internet protocol, which will soon go through a worldwide transition process. This research shows theoretical concepts along with a practical application simulated on a real environment, demonstrating its viability, functionality, and techniques used for adoption of the protocol in the current internet. The recommended method for the transition of the version of the internet protocol is called Dual IP Stack. This method is preferred due to the low impact it has in the existent network infrastructure. Based on a world trend this work is also related to networking and telecom companies such as Global Village Telecom (GVT) where the practical experiments took place. The value of this research is not limited to the academic community, it is also important to the industry where the internet protocol version 6 will soon be adopted using the same dual stack implementation, and eventually reach all other industries in the telecommunication field in the world.

Keywords: Internet Protocol. Dual Stack. Transition. Network.

LISTA DE FIGURAS

Figura 1 – Cabeçalho básico do IPv6 [Autoria própria].....	17
Figura 2 – Cabeçalho ICMPv6 [Autoria própria].....	18
Figura 3 – Posição do Cabeçalho ICMPv6 [Autoria própria].	18
Figura 4 – Primeira etapa do padrão EUI-64 [Autoria própria].	22
Figura 5 – Segunda etapa do padrão EUI-64 [Autoria própria].	23
Figura 6 – Roteador no padrão EUI-64 [Autoria própria].....	23
Figura 7 – Esboço da técnica de Pilha Dupla [Autoria própria].....	26
Figura 8 – Topologia da prática [Autoria própria].	28
Figura 9 – Endereço MAC da placa de rede do <i>Host</i> [Autoria própria].....	28
Figura 10 – Configuração da rede no sistema Linux [®] para IPv4 [Autoria própria].....	29
Figura 11 – Configuração da rede no sistema Linux [®] para IPv6 [Autoria própria].....	30
Figura 12 – Configuração da conexão do modem <i>Fritz!Box</i> [Autoria própria].	31
Figura 13 – Configuração das opções de IPv6 do modem <i>Fritz!Box</i> [Autoria própria].	32
Figura 14 – <i>Status</i> da conexão do modem <i>Fritz!Box</i> [Autoria própria].	33
Figura 15 – <i>Status</i> da conexão no <i>host</i> [Autoria própria].....	34
Figura 16 – Configuração do BRAS [Autoria própria].	35
Figura 17 – <i>Netstat</i> e rotas [Autoria própria].	36
Figura 18 – Comando “ <i>host</i> ” e conectividade [Autoria própria].....	36
Figura 19 – Ping endereço web [Autoria própria].	37
Figura 20 – Site www.ipv6.br [Autoria própria].	37
Figura 21 – Site www6.terra.com.br [Autoria própria].	38

LISTA DE TABELAS

Tabela 1 – Mensagens de Erros ICMPv6.....	19
Tabela 2 – Mensagens de Informações ICMPv6.....	20

SUMÁRIO

1 INTRODUÇÃO	8
1.1 TEMA	8
1.2 DELIMITAÇÃO DA PESQUISA	8
1.3 PROBLEMA	9
1.4 OBJETIVOS	10
1.4.1 OBJETIVO GERAL	10
1.4.2 OBJETIVOS ESPECÍFICOS	10
1.5 JUSTIFICATIVA	10
1.6 PROCEDIMENTOS METODOLÓGICOS	11
1.7 FUNDAMENTAÇÃO TEÓRICA.....	11
1.8 ESTRUTURA	12
2 CONHECENDO O PROTOCOLO	13
3 FUNCIONALIDADES IPV6.....	18
3.1 ICMPV6.....	18
3.2 DESCOBERTA DE VIZINHANÇA.....	20
3.3 ENDEREÇAMENTO <i>STATELESS</i>	21
3.4 DHCPV6.....	23
3.5 DNS	24
4 A TÉCNICA DE PILHA DUPLA.....	26
4.1 PILHA DUPLA.....	26
4.2 UTILIZANDO A TÉCNICA	27
5 CONCLUSÃO.....	39
REFERÊNCIAS	40

1 INTRODUÇÃO

1.1 TEMA

Com a massificação da internet e a demanda de usuários cada vez maior, uma preocupação começou a surgir de maneira mais evidente nesta última década. Os endereçamentos de protocolos *Internet Protocol* – protocolo de internet (IP) em sua versão atual não serão o suficiente para interligar todos os atuais e novos usuários da rede global.

Na atual versão 4 do IP apesar das mudanças sofridas durante o tempo para a melhor utilização das suas classes e endereços, o mesmo está se esgotando. As medidas paliativas que foram tomadas não estão suprindo à demanda que já é perceptível, sendo maior do que a entrega, para tal, a medida definitiva encontrada foi a evolução do protocolo.

Nesse trabalho é apresentada uma das possíveis implementações da versão 6 do protocolo de internet em conjunto com redes IPv4 até então globalmente utilizadas. A transição de uma versão para a outra deverá ocorrer de maneira gradual, onde neste tempo se faz necessário a existência prática das duas versões do protocolo, até por fim a troca ser efetivada.

Como as redes de computadores atualmente são muito vastas, não sendo possível a troca abrupta de todo o endereçamento dos *sites*, servidores, *host* e todos os componentes de todo a rede, esta transição e coexistência poderá ser dividida em 3 diferentes técnicas: i) Pilha dupla; ii) Tunelamento; e iii) Tradução. Como foco principal deste trabalho será descrito e estudado somente a técnica de pilha dupla.

1.2 DELIMITAÇÃO DA PESQUISA

Serão apresentados exemplos de cenários da utilização de modems com suporte a técnica de pilha dupla onde sua configuração disponibiliza as duas versões do protocolo IP e *sites* em que já se é possível navegar utilizando IPv6 com endereços e redes puramente IPv6.

Nos primeiros capítulos são explicados alguns conceitos sobre IPv6, que são importantes para fundamentação teórica do trabalho. Também serão abordadas as tecnologias envolvidas.

Como ponto principal sobre a nova versão do IP, será descrito as suas funcionalidades proprietárias, tais como também as diferenças encontradas em sua versão

anterior, onde além de maior número de redes e usuários, conta com datagramas mais simples e flexíveis.

Embora a internet seja uma rede mundial livre de uma coordenação central, existem órgãos responsáveis hierarquicamente pelas alocações e coordenação dos endereços IP's, sendo estes a *Internet Assigned Numbers Authority* – Autoridade dos números de endereçamento da internet (IANA) com nível mundial de coordenação de endereços; os órgãos, *Regional Internet Registries* - Registros regionais de internet (RIR) que são responsáveis por uma grande área demográfica e reconhecidos pelo IANA, como o *Latin American and Caribbean Internet Address Registry* – Registros de endereço de internet para a América latina e Caribe (LACNIC), responsável pela América latina e algumas ilhas do aríbe. E por fim para o Brasil 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's válidos.

1.3 PROBLEMA

Como consequência do grande crescimento de usuários e a necessidade de um número maior de endereços de internet, surgiu a necessidade de obter técnicas confiáveis e transparente ao usuário final, para que o tráfego seja gradativamente passado de redes IPv4 para redes IPv6. Além disso é necessário convergir de maneira eficaz e funcional a nova versão do protocolo com os equipamentos e protocolos de outras camadas já existentes, sem prejudicar as funcionalidades atuais.

Apesar da certa semelhança entre as versões, elas diferem não somente pela grande quantidade de endereços disponíveis no IPv6, mas também em técnicas mais simplificadas como, por exemplo, sempre poder efetuar conexões fim-a-fim, justamente por não requerer soluções paliativas encontradas no IPv4 para suprir a necessidade da falta de endereçamento.

Para responder a estas questões, necessita-se fazer um estudo do estado da arte da nova versão do protocolo de internet o, IPv6. Tal estudo é de grande valia para empresas, profissionais e estudantes de redes de computadores, pois permite que estes utilizem o IPv6 de forma adequada, atendendo à expectativa dos usuários.

1.4 OBJETIVOS

A seguir, serão apresentados os objetivos geral e específicos, que se pretende atingir com este projeto de pesquisa.

1.4.1 Objetivo Geral

Realizar um estudo sobre a nova versão do protocolo de internet o IPv6, visando a praticidade de sua aplicação nas redes atuais.

1.4.2 Objetivos Específicos

Os objetivos específicos são:

- Configurar e programar IPv6 em modems residenciais;
- Utilização e interoperabilidade da técnica de Pilha Dupla;
- Descrever os recursos do IPv6 e suas vantagens;
- Demonstrar as diferenças e vantagens do IPv6 em relação a sua versão anterior.

1.5 JUSTIFICATIVA

Ao final deste projeto de pesquisa onde seus objetivos sejam alcançados, o mesmo poderá servir de orientação para usuários que queiram conhecer sobre como implementar esta nova versão do protocolo IP, visando a real necessidade para inserir nas já existentes redes de computadores, o novo modo de endereçamento. Sendo possível diferenciar as técnicas e funcionalidades em questão, que este estudo demonstrará de maneira específica para a técnica de pilha dupla, mas envolvendo todos os aspectos particulares da tecnologia empregada no IPv6, desde sua gradual adoção até a sua total utilização nas atuais redes.

1.6 PROCEDIMENTOS METODOLÓGICOS

Para o desenvolvimento deste projeto, utilizar-se-á referências bibliográficas sobre o assunto pressuposto, equipamentos de redes conectados em rede e materiais virtuais e didáticos de apoio.

O estudo também demonstrará as funcionalidades do IPv6 e a técnica de transição conhecida como Pilha Dupla. Não será abordado as demais técnicas como: Tunelamento e Tradução.

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.

Para as práticas de protocolos de roteamentos será apresentado as compatíveis com a nova versão do protocolo IP.

1.7 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 nas áreas de telecomunicações e redes de computadores, baseadas nas obras de Santos (2010), Comer (2006), Colcher (2005) 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 nas instalações da empresa de Telecomunicações Global Village Telecom (GVT), onde foi realizado com sucesso a aplicação da tecnologia do IPv6 em cenários reais de estruturas de conexões com a internet.

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.

1.8 ESTRUTURA

Esta monografia é estruturada por 5 capítulos complementares entre si, que visam satisfazer os objetivos propostos. No capítulo 1, 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 teoria; vii) estrutura.

Para desenvolvimento do tema proposto foram sugeridos os capítulos 2, 3 e 4 que englobam as teorias e práticas desta pesquisa. No capítulo 2 demonstra uma prévia de conhecimento da versão 4 e 6 do protocolo de internet, fazendo uma diferenciação e apontando motivos para migrar para a versão mais atual do protocolo. O capítulo 3 está embasado diretamente nas fundamentações e obras relacionadas à tecnologia do protocolo, estudando as funcionalidades da versão 6 do IP das quais serão aplicadas nos ensaios práticos, relacionando a teoria com a utilização da tecnologia e sua empregabilidade.

A parte de maior interesse para profissionais da área concentra-se no capítulo 4, onde será aplicada a técnica de pilha dupla, simulada em um ambiente real de utilização da internet demonstrando os passos das configurações entre modem, *Digital Subscriber Line Access Multiplexer* – Multiplexador Digital de Linha de Acesso a Assinante (DSLAM) e roteador de borda com a função de *Broadband Remote Access Server* – Servidor de Acesso Remoto a Banda Larga – (BRAS). No capítulo 4 além das configurações nos equipamentos de rede, são explicadas as funções do protocolo e sua utilidade na aplicação em questão, de acordo descrito nos capítulos anteriores e fundamentada nas obras relacionadas ao protocolo de internet e tecnologias convergentes, que auxiliam no funcionamento do IPv6 mas aqui não descritas, pois fogem ao escopo dos objetivos da pesquisa.

No capítulo 5 é 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 CONHECENDO O PROTOCOLO

Como o crescimento faz parte da evolução humana, assim como população, recursos/tecnologias e crescimento de cidades dentre outros, a rede mundial de computadores também não ficou para trás. O aumento de usuários de internet teve um rápido crescimento na última década fazendo surgir uma preocupação sobre um possível esgotamento dos endereços de protocolos IP, estes endereços precisam ser únicos para cada usuário a nível mundial na rede.

De acordo com Filippetti (2011, p. 11) “Espera-se que o Brasil zere o seu estoque de endereços IPv4 até meados de 2012. A verdade é que os endereços IPv4 só não se esgotaram ainda porque uma série de técnicas e recursos para otimização do uso destes endereços, foram criadas 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 (com a telefonia 3G), tablets, smartphones e outros dispositivos eletrônicos que utilizam da rede mundial para a comunicação dos seus usuários.

Para Comer (2005, p. 370), o argumento dos pesquisadores foi que:

No início da década de 1990, os pesquisadores argumentaram que a Internet atual era insuficiente para as novas aplicações, como voz e vídeo. Eles argumentaram ainda que o crescimento da Internet, que estava dobrando de tamanho a cada nove meses ou mais rápido ainda, logo esgotaria o conjunto de endereços disponíveis.

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.

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.

Para Colcher et al (2005, p. 73), “cada endereço é formado por um prefixo (denominado *Net-Id*), que identifica a rede, e um sufixo (denominado *Host-Id*), que identifica a interface da estação com aquela rede em particular.”

Diferente da versão 4 o IPv6 não precisa de técnicas de soluções paliativas como o *Network Address Translator* – Tradutor de endereços de rede (NAT) e o *Classless Inter-domain Routing* – Roteamento de inter-domínio sem-classe (CIDR), que auxiliam na utilização mais otimizadas dos endereços IPv4, evitando assim desperdícios de endereços que poderiam ser utilizados, mas ficavam “presos” na sua classe pela máscara de sub-rede. Já o IPv6 pela sua capacidade de endereços, não há esta necessidade de recurso melhorando assim o tempo de roteamento de pacotes, uma vez que é um recurso a menos para o roteador processar.

Nos dias atuais a IANA já recebeu diversas solicitações de blocos de endereços IPv6 o mais usual é o bloco da classe /32 que é fornecido as *Internet Services Provider* – Provedor de serviço de internet (ISP). Diferente do IPv4 a utilização dos endereços é medida em relação à necessidade de alocação de designações /48 para usuários finais e não ao número de endereços designados ao usuário final. Já em redes locais o tamanho recomendado é o /64 para o melhor funcionamento das facilidades do protocolo, como o endereçamento *stateless* para dispositivos conectados a *Local Area Network* – Rede local (LAN).

Segundo Santos et al (2010, p. 30), o cenário mundial do IPv6 se reflete:

Blocos de endereços IPv6 vêm sendo alocados pelos RIRs há aproximadamente dez anos. No entanto, o fato dos RIRs alocarem endereços aos Registros Nacionais ou aos ISPs, não significa que estes endereços estejam sendo utilizados. Ao cruzar os dados sobre a quantidade de blocos /32 IPv6 já alocados com o número de rotas anunciadas na tabela de roteamento, nota-se que apenas 3% desses recursos estão sendo efetivamente utilizados, isto é, dos 73.000 blocos já alocados, apenas pouco mais de 2.500 estão presentes na tabela global de roteamento.

O IPv6 possui 128 bits de campo para seus endereços, conseguindo assim atingir um tamanho mais do que o necessário para futuras gerações durante anos. A sua denotação hexadecimal com dois pontos, fornece uma melhor e mais compacta visualização e utilização se utilizar a denotação decimal como no IPv4.

Como exemplo, será apresentado o endereçamento a seguir:

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

Onde 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 facilitar ainda mais é permitido como no exemplo acima a notação tipo CIDR com a utilização da barra transversal seguida de um número inteiro representando a parcela de bits que está sendo utilizado para endereço de rede, semelhante a sua versão anterior.

Conforme Santos et al (2010, p. 54) “ Esta notação é representada de forma endereço-IPv6/tamanho do prefixo, onde o “tamanho do prefixo” é um valor decimal que especifica a quantidade de bits contíguos à esquerda do endereço que compreende o prefixo.”

Outra maneira que auxilia muito na utilização da denotação de endereço IPv6 seria a compactação de números 0 (zeros) consecutivos por um par de sinais de dois pontos, como por exemplo o endereço:

2001:0A26:0:0:0:0:fff8

Pode ser escrito da seguinte maneira reduzida,

2001:A26::fff8

Note que para não haver ambiguidade este recurso só pode ser utilizado somente uma vez. Percebe-se também que ao invés de se utilizar zeros na sequência “0000” é utilizado somente um, pois os “zeros” à esquerda podem ser abreviados para facilitar a sua escrita.

Demais endereços especiais como *loopback* e endereços não-especificados, estão presentes para nova versão, onde os endereços não-especificados inicialmente todos os dígitos zeros (0:0:0:0:0:0:0:0 ou ::0) são utilizados como endereços de origem de computadores que estão autenticando na rede e ainda não receberam seu endereçamento IPv6 ou ausência de

endereço. Assim como no IPv4 o endereço de *loopback* que é utilizado para testar a própria placa de rede do computador local que envia um pacote para si mesmo, é representado por zeros com final 1 (0:0:0:0:0:0:0:1 ou ::1).

Outro endereço específico é o endereço de IPv4-mapeado (::wwxx:yyzz), onde a sua denotação final “wx:yz” representa um endereço IPv4 de 32 bits, convertidos de decimal para hexadecimal e aplicado na técnica de transição *6to4* entre nós IPv6 e IPv4, técnica da qual não será abordada neste projeto de pesquisa.

Assim como no IPv4 o IPv6 possui endereços básicos definidos, sendo eles: *unicast*, *anycast* e *multicast*. O *unicast* é o tipo de endereço que identifica um único host e o pacote é entregue somente a este host pelo caminho mais curto; O *anycast* cujo destino é identificado por um conjunto de hosts ou interfaces onde o pacote é encaminhado a uma dos membros deste conjunto (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.”

Por último o endereço de *multicast* que também representa um conjunto de hosts ou interfaces, contudo o pacote não é encaminhado a somente um destes hosts do conjunto, mas a todas as interfaces que compõem o mesmo endereço, segundo 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 Comer (2005, p. 378), a relação entre *broadcast* e *multicast* pode ser relacionado da seguinte maneira:

O IPv6 não usa os termos *broadcast* ou *broadcast direcionado* para se referir à entrega a todos os computadores em uma rede física ou a uma sub-rede IP lógica. Em vez disso, ele usa o termo *multicast*, e trata do *broadcast* como uma forma especial de *multicast*.

Como a utilização principal da internet nos dias atuais é predominantemente IPv4, é necessário fazer a transição de maneira gradual e adequada. Não se pode simplesmente trocar em pouco tempo todos os sites, servidores e equipamentos que utilizam o endereçamento IPv4 por IPv6, onde acarretaria um prejuízo para diversas corporações e usuários, para isto foram desenvolvidas as técnicas de transição.

Segundo Filippetti (2008, p. 179) “Entretanto, esta migração já teve início faz algum tempo. Se não percebemos, é porque o que quer que seja que estão fazendo, estão fazendo certo”.

A técnica de pilha dupla consiste em utilizar o endereçamento IPv4, até então já em uso, em conjunto com o IPv6, ou seja, o modem e/ou roteador suporta ambos os protocolos. Sendo assim o equipamento utiliza o protocolo IPv4 quando for comunicar com redes IPv4 e protocolo IPv6 para redes IPv6, mantendo a compatibilidade e comunicação durante o período de coexistência.

Para Santos et al (2010, p. 178) “A utilização deste método permite que hosts e roteadores estejam equipados com pilhas para ambos os protocolos, tendo a capacidade de enviar e receber os dois pacotes, IPv4 e IPv6”.

Esta técnica utiliza também mecanismos proprietários para cada versão do protocolo para atribuir seu endereço, seja via *Dynamic Host Configuration Protocol* – Protocolo de configuração dinâmica de hosts (DHCP) nas versões 4 e 6 ou pelo mecanismo de autoconfiguração para inserir o endereço IPv6.

Para uma melhor visualização e compreensão do formato, na figura 1 abaixo é demonstrado o do cabeçalho básico IPv6 de 40 octetos.

0	4	12	16	24	31
Versão	Classe de Tráfego	Rótulo de Fluxos			
Tamanho do Payload			Próximo Cabeçalho	Limite de Saltos	
Endereço de Origem					
Endereço de Destino					
Dados					

Figura 1 – Cabeçalho básico do 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 datagrama IPv6 precisa conter pelo menos 40 octetos além dos dados.

3 FUNCIONALIDADES IPv6

Neste capítulo, será abordada as funcionalidades essenciais da nova versão do protocolo IP que será utilizada neste trabalho, tanto na aplicação prática quanto para o conhecimento teórico.

3.1 ICMPv6

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

Estas mensagens são utilizadas como troca de informações para que a ferramenta desejada seja aplicada, tendo como objetivo: i) informar tipos da rede; ii) diagnosticar a rede; e iii) relatar casos 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 sua versão anterior. Os cabeçalhos do protocolo são de estruturas simples conforme demonstrada na figura 2.

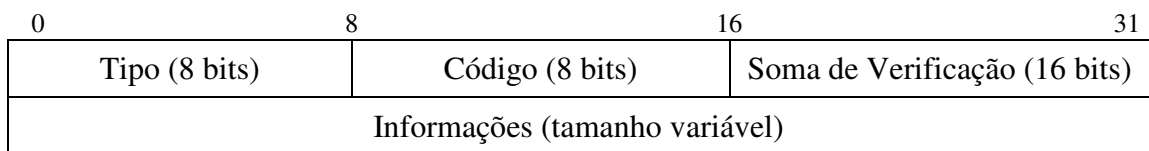


Figura 2 – Cabeçalho ICMPv6 [Autoria própria].

As informações das mensagens vem precedidas do cabeçalho básico do IPv6 e do(s) cabeçalho(s) de extensão(ões), a seguir na figura 2 é apresentada a posição do cabeçalho ICMPv6.

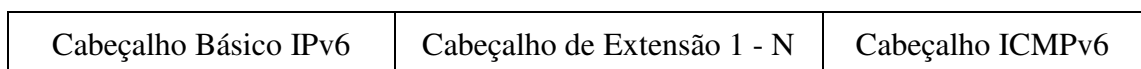


Figura 3 – Posição do Cabeçalho ICMPv6 [Autoria própria].

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 grupo 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.

Tipo	Nome	Descrição
1	<i>Destination Unreachable</i>	Indica que o destino para o qual um pacote foi enviado não está acessível ou há uma falha na transmissão.
2	<i>Packet Too Big</i>	Mensagem recebida quando o pacote excede o tamanho máximo da MTU do enlace.
3	<i>Time Exceeded</i>	Semelhante ao campo de tempo de vida da versão anterior, onde o limite máximo para os saltos no enlace ou o tempo de remontagem dos pacotes nos enlaces foi excedido.
4	<i>Parameter Problem</i>	Problemas de cabeçalhos, onde os parâmetros, tipos e tamanhos não foram reconhecidos pelo protocolo.

Fonte: Santos et al (2010).

Tabela 2 – Mensagens de Informações ICMPv6.

Tipo	Nome	Descrição
128	<i>Echo Request</i>	Utilizadas pelo comando <i>ping</i> .
129	<i>Echo Reply</i>	
130	<i>Multicast Listener Query</i>	Para o gerenciamento de grupos <i>multicast</i> . Proprietárias do protocolo MLD.
131	<i>Multicast Listener Report</i>	
132	<i>Multicast Listener Done</i>	
133	<i>Router Solicitation (RS)</i>	Protocolo de Descoberta de Vizinhança.
134	<i>Router Advertisement (RA)</i>	
135	<i>Neighbor Solicitation (NS)</i>	
136	<i>Neighbor Advertisement (NA)</i>	
137	<i>Redirect Message</i>	
141	<i>Inverse ND Solicitation Message</i>	Utilizadas também na Descoberta de Vizinhança mas como mensagens de extensão.
142	<i>Inverse ND Advertisement Message</i>	
151	<i>Multicast Router Advertisement</i>	Mensagens utilizadas nas descobertas dos roteadores vizinhos.
152	<i>Multicast Router Solicitacion</i>	
153	<i>Multicast Router Termination</i>	

Fonte: Santos et al (2010).

3.2 DESCOBERTA DE VIZINHANÇA

Definida pela RFC 4861 a Descoberta de Vizinhança, faz toda a tarefa de comunicação entre os nós de uma rede IPv6, similar a sua versão anterior que utilizava o protocolo ARP, mas com métodos adicionais na sua estrutura.

Suas principais características são: i) determinar o endereço de camada de enlace 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.

Segundo Santos et al (2010, p. 93) “ As mensagens de Descoberta de Vizinhança são configuradas com um limite de encaminhamento de 255 para assegurar que as mensagens

recebidas são originadas de um nó do mesmo enlace, descartando as mensagens com valores diferentes.”

De acordo a tabela 2 com as mensagens de informações do ICMPv6, as mensagens dos tipos 133 a 137 são trocadas pelos *hosts* durante a comunicação, para que o enlace seja conectado.

Como exemplo será utilizado um *host A* e um *host B*, o A envia uma mensagem tipo 135 (solicitação de vizinho) ao endereço de *multicast solicited node* do B, informando seu MAC. Assim que receber a mensagem 135 o B responde a A através da mensagem ICMPv6 tipo 136 (anúncio de vizinho) informando o seu endereço MAC e atribuindo o endereço de MAC de A.

Quando se tem nesta rede um roteador o mesmo utiliza mensagens do tipo 133 (solicitação de roteador) e 134 (anúncio de roteador) para localizar roteadores vizinho, bem como efetuar configurações de prefixos de redes IPv6 e dados relacionados à autoconfiguração de endereço, chamada de *Stateless*. Neste contexto a mensagem tipo 134 é encaminhada ao endereço *multicast all-nodes*, ou seja, enviada a todos os nós vizinhos.

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* subseqüentemente passa a enviar seus pacotes com o mesmo destino do pacote redirecionado.

3.3 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.

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).

De acordo Filippetti (2008, p. 178) “O host determina a informação do prefixo por meio de um router na rede, uma vez de posse desta informação, ele adiciona como Interface ID o endereço MAC de sua placa de rede.”

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 como exemplo de prefixo o endereço IPv6 2001:470:e0ae:6::/64, prefixo este de posse da operadora GVT.

Para que o IP seja criado o roteador deve estar configurado para o padrão EUI-64 e fornecer o prefixo ao *host* que segue duas etapas. A primeira etapa separa o endereço de MAC em duas partes iguais e insere entre elas um endereço hexadecimal de 16 bits com valores FFFE, estes 16 bits são a diferença de 48 bits do endereço de MAC, para um total necessário de 64 bits para a interface de usuário, tendo assim 64 bits de rede mais 64 bits de interface, resultando no total de 128 bits que é o tamanho do IPv6.

Os valores FFFE são valores reservados para o padrão EUI-64, não podendo conter em endereços MAC de fabricantes. Para exemplo de MAC será utilizado o valor 00:18:71:8C:0D:D9, na figura 4 é demonstrada a primeira etapa do padrão EUI-64, depois de executada a primeira etapa, o endereço de 64 bits resultante é 00:18:71:FF:FE:8C:0D:D9. Como o processo ainda não está completamente concluído o *host* passa para a etapa seguinte.

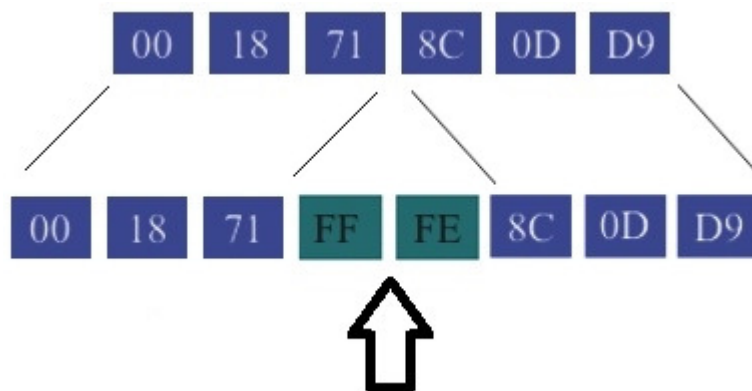


Figura 4 – Primeira etapa do padrão EUI-64 [Autoria própria].

Na segunda etapa a informação do *bit 6* do octeto de alta ordem é alterado de 0 para 1, garantindo assim que o endereço IPv6 seja globalmente exclusivo. Então o endereço de interface 02:18:71:FF:FE:8C:0D:D9 é criado e anexado ao prefixo da rede IPv6 segundo o exemplo já descrito, resultando assim o endereço IPv6 2001:470:e0ae:6:218:71ff:fe8c:dd9. Este sendo um IP válido para acesso a internet e exclusivo para este *host* neste prefixo de rede, a figura 5 abaixo demonstra a segunda etapa do padrão EUI-64.



Figura 5 – Segunda etapa do padrão EUI-64 [Autoria própria].

Para que um roteador esteja configurado no padrão EUI-64 é necessário inserir na linha de comando do endereço IPv6 a palavra “eui-64” após o endereço do prefixo da rede IPv6 em sua interface. A seguir na figura 6 é realizado um exemplo das linhas de comando para a configuração do roteador e a saída do comando.

```
Router(config)# interface f0/0
Router(config-if)# ipv6 address 2001:470:e0ae:6::/64 eui-64
Router(config-if)# do show ipv6 interface f0/0
FastEthernet0/0 is up, line protocol is down
  IPv6 is enabled, link-local address is 2001:470:E0AE:6:218:71FF:FE8C:DD9 [TEN]
  No Virtual link-local address(es):
  Global unicast address(es):
  2001:470:E0AE:6:218:71FF:FE8C:DD9, subnet is 2001:470:e0ae:6::/64 [EUI/TEN]
  ...
```

Figura 6 – Roteador no padrão EUI-64 [Autoria própria].

3.4 DHCPv6

A função do servidor DHCPv6 é fornecer informações de redes quando não há a presença de roteadores, utilizando as mensagens RA (tipo 134), ou quando é habilitado pelo usuário a sua utilização. Além do endereço IPv6 outros parâmetros da rede como endereços de outros servidores como o Sistema de Nome de Domínio – *Domain Name System* (DNS).

Conhecido como autoconfiguração *Stateful* do protocolo IPv6 o DHCPv6 utiliza a troca de mensagens *multicast* reservadas e endereços de *link-local* para trocarem informações DHCP. Os clientes utilizam as mensagens de link-local para enviarem ou receberem informações. Os servidores o endereço de multicast reservado, sendo eles FF02::1:2 ou FF05::1:3 para receberem mensagens dos clientes.

De acordo Santos et al (2010, p. 106) o DHCP é “um protocolo de autoconfiguração *Stateful* utilizado na distribuição de endereços IP dinamicamente em uma rede, a partir de um servidor DHCP, fornecendo um controle maior na atribuição de endereços aos *host*.”

Na utilização do DHCPv6 tem-se a possibilidade de combinar o estados *stateful* com *stateless*, a atribuição do endereço IPv6 se utiliza o estado *stateless* e para os demais parâmetros de rede como endereços de servidores DNS seria realizada pelo servidor DHCP.

A versões de DHCP 4 e DHCPv6 são independentes para tanto em sua utilização na técnica de Pilha Dupla, será necessário atribuir o serviço do servidor para cada protocolo.

Contudo este endereçamento precisar ser renovado na rede de acordo com o tempo estipulado pelo roteador para que um *host* tenha o endereço como válido. Este mecanismo ajuda a não deixar que endereços não mais utilizados ou que *hosts* que já não estejam ativos na rede ainda façam parte das listas dos roteadores, otimizando a funcionalidade e tráfego da rede.

Segundo Comer (2006, p. 382), a idéia por trás da renumeração é simples:

Ao anunciar um novo prefixo (ou seja, adicional), esperar um pouco e desativar o uso do prefixo antigo. Porém, na prática, essas transições são difíceis. Conexões de transporte de longa duração serão terminadas quando houver mudança; um servidor que se vincula a um endereço existente não receberá contato no novo endereço; e o roteamento precisa ser alterado.

3.5 DNS

O protocolo DNS é de grande apoio dentro para usuários da internet, pois ele faz a tradução de endereço IP's para nomes de domínios como *website* e dispositivos de redes e vice-versa.

Sendo uma vasta base de dados com abrangência global o DNS possui: i) hierarquia; ii) dados dispostos em uma árvore invertida; iii) descentralizada ; e iv) com *cache*, ou seja, salva domínios acessados recentemente pelo usuário.

Para que o IPv6 trabalhasse em conjunto com a versão 4, foram definidas algumas mudanças no protocolo de DNS.

Como o tamanho da versão 6 é de 128 bits um novo registro foi criado para dar suporte a este número mais de endereçamentos, denominado “AAAA” ou “*quad-A*”, para traduzir domínios IPv6 em endereços e vice-versa. Para versões 4 de 32 bits até então era utilizado somente o registro “A”.

O DNS inicia a sua tradução sempre com sentido inverso do endereço IP ou nome de domínio, se o usuário quiser acessar como exemplo o endereço de web www.ipv6.br o DNS

iniciará a sua tradução pelo “.br” e em seguida “.ipv6”, chamado de resolução de reverso. Para a versão 6 foi adicionado ao DNS o registro chamado PTR *ip6.arpa*, este responsável para traduções IPv6, na versão 4 o registro responsável pela tradução é o *in-addr.arpa*.

Exemplo de diferença entre A e *Quad-A*:

- www.ipv6.br IN A 200.160.4.22;
- www.ipv6.br IN AAAA 2001:12ff:0:4::22.

Exemplo de resolução de reverso PTR entre IPv4 e IPv6:

- 22.4.160.200.in-addr.arpa PTR www.ipv6.br;
- 2.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2.ip6.arpa PTR www.ipv6.br (não é permitida a omissão dos zeros “0”).

Para Santos et al (2010, p. 118), o suporte a IPv6 do DNS deve ser observado por dois aspectos:

O primeiro, é que um servidor DNS deve ser capaz de armazenar registros *Quad-A* para endereços IPv6. O segundo aspecto, é se um servidor DNS é capaz de transportar consultas e respostas através de conexões IPv6. Isto é, a base de dados de um servidor DNS pode armazenar tanto registro IPv6 quanto IPv4, independentemente da versão de IP que este servidor opera.

4 A TÉCNICA DE PILHA DUPLA

Neste capítulo, será demonstrada a técnica de pilha dupla utilizada para a coexistência e transição das versões dos protocolos. A técnica consiste em utilizar ambas as versões sendo assim uma técnica de maior aceitação e com um nível menos complexo de aplicação.

Uma vez que, esta técnica por utilizar as duas versões do protocolo em simultâneo evita que um *host* fique ilhado dentro de uma só rede seja ela IPv4 ou IPv6.

4.1 PILHA DUPLA

Este método de transição pode facilitar o gerenciamento entre as versões dos protocolos, por possuir pilhas distintas e funcionais cada uma em seu método de comunicação assim que a pilha do protocolo IPv4 e sua redes forem se tornando obsoletas, basta desativá-la.

De acordo Santos et al (2010, p. 178) “ A utilização deste método permite que *hosts* e roteadores estejam equipados com pilhas para ambos os protocolos, tendo a capacidade de enviar e receber os dois pacotes, IPv4 e IPv6.”

A configuração de cada mecanismo para adquirir seu endereçamento é realizada pelas funcionalidades de cada protocolo, para IPv4 é utilizado o DHCP e IP Fixo. No IPv6 a configuração é realizada por Link Local, Autoconfiguração e DHCPv6. Na figura 7 é esboçado o conceito da técnica de Pilha Dupla.

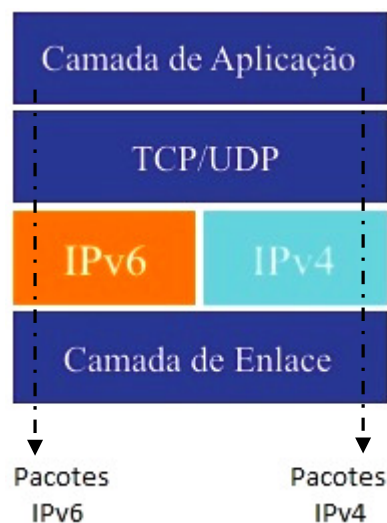


Figura 7 – Esboço da técnica de Pilha Dupla [Autoria própria].

Para Filippetti (2008, p. 179) “A vantagem deste método é que novos elementos de rede já podem ser endereçados em IPv6, e os elementos já existentes podem ser migrados em fases sem grandes impactos.”

Mas haja vista que uma das desvantagens é que nem todos os equipamentos de rede suportam o IPv6, e há sistemas operacionais que também não tem suporte à este protocolo.

Conforme visto no capítulo anterior sobre as funcionalidades do protocolo IPv6, para a aplicação da técnica de Pilha Dupla alguns aspectos relacionados as estas funcionalidades devem ser considerados.

Para o DNS é necessário que o servidor esteja habilitado para a resolução dos nomes para endereços e vice-versa, com a nomenclatura *Quad-A*. Para o armazenamento dos endereços do IPv6 no domínio de resolução de reverso, conhecido por *ip6.arpa*.

Como os roteamentos devem ser feitos de maneira independente, como também versões diferentes dos protocolos da camada superior de transporte. No IPv4 é utilizado protocolo com roteamento interno conhecido como Abrir Primeiro o Menor Caminho – *Open Shortest Path First* (OSPF) na versão 2, ou comumente utilizado OSPFv2.

Esta versão acima mencionado não possui compatibilidade com o IPv6, sendo necessário a migração/utilização da versão atual OSPFv3, que distribui e encaminha pacotes de ambos os protocolos IP's, ou outra solução proposta é forçar o funcionamento das versões dos protocolos de roteamento em paralelo, para atender a necessidade do IPv6 tanto como a do IPv4.

Uma última adequação que deve ser levada em consideração é a plataforma que o host está executando, seja ela sobre segurança, proteção e *firewall* de um sistema operacional Linux[®] ou Windows[®], a filtragem dos pacotes são realizadas de maneiras diferentes. Podendo ou não compartilhar os filtros entre os protocolos IP's ou tratá-los de maneira independentes.

4.2 UTILIZANDO A TÉCNICA

Com base nos conceitos teóricos e referências de autores da área de redes foi elaborada um ensaio prático demonstrando a utilização da técnica de Pilha Dupla e do funcionamento atual com redes utilizando o Protocolo IPv6.

Regras de endereçamento, protocolos e configurações de equipamentos serão realizadas para que o resultado seja satisfatório aos objetivos específicos propostos no capítulo 1.

Foi utilizado o laboratório da engenharia de acesso da GVT e dentre os equipamentos necessários estão: i) o *host*; ii) o modem ADSL do fabricante AVM[®], modelo: *Fritz!Box* com suporte a IPv6; iii) DSLAM da marca *Keymile*[®], modelo *Milegate*; e iv) o roteador com a função de BRAS da fabricante *Ericsson*[®], modelo *Smart Edge 800* este com saída para a Internet. Os equipamentos foram conectados conforme a figura 8 – Topologia da prática.

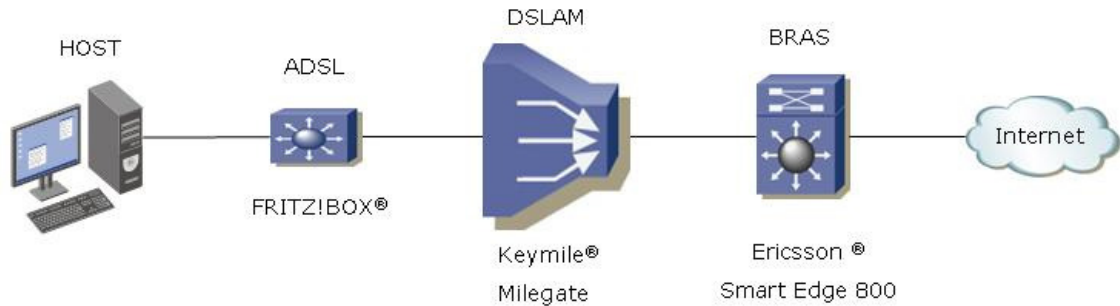


Figura 8 – Topologia da prática [Autoria própria].

Inicialmente como o padrão a ser utilizado para a configuração do endereço IPv6 será o padrão EUI-64, é verificado o endereço de hardware do dispositivo da placa de rede do *host*, conforme a figura 9, este utilizando o sistema operacional Linux[®].

O endereço HWaddr 00:18:71:8c:0d:d9 que é demonstrado na saída do comando, irá formar subsequentemente o endereço IPv6 - EUI-64 da LAN entre o *host* e o modem.

```

g0200787@notctaro1-5205: ~
g0200787@notctaro1-5205:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:18:71:8c:0d:d9
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:16

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:66 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:5088 (5.0 KB)  TX bytes:5088 (5.0 KB)

g0200787@notctaro1-5205:~$ _

```

Figura 9 – Endereço MAC da placa de rede do *Host* [Autoria própria].

Ainda na configuração do *host* para que a técnica da pilha dupla seja efetuada a configuração do endereçamento IPv4 é realizada com o auxílio do protocolo DHCP para a LAN do *host* de endereço versão 4, segundo a figura 10.

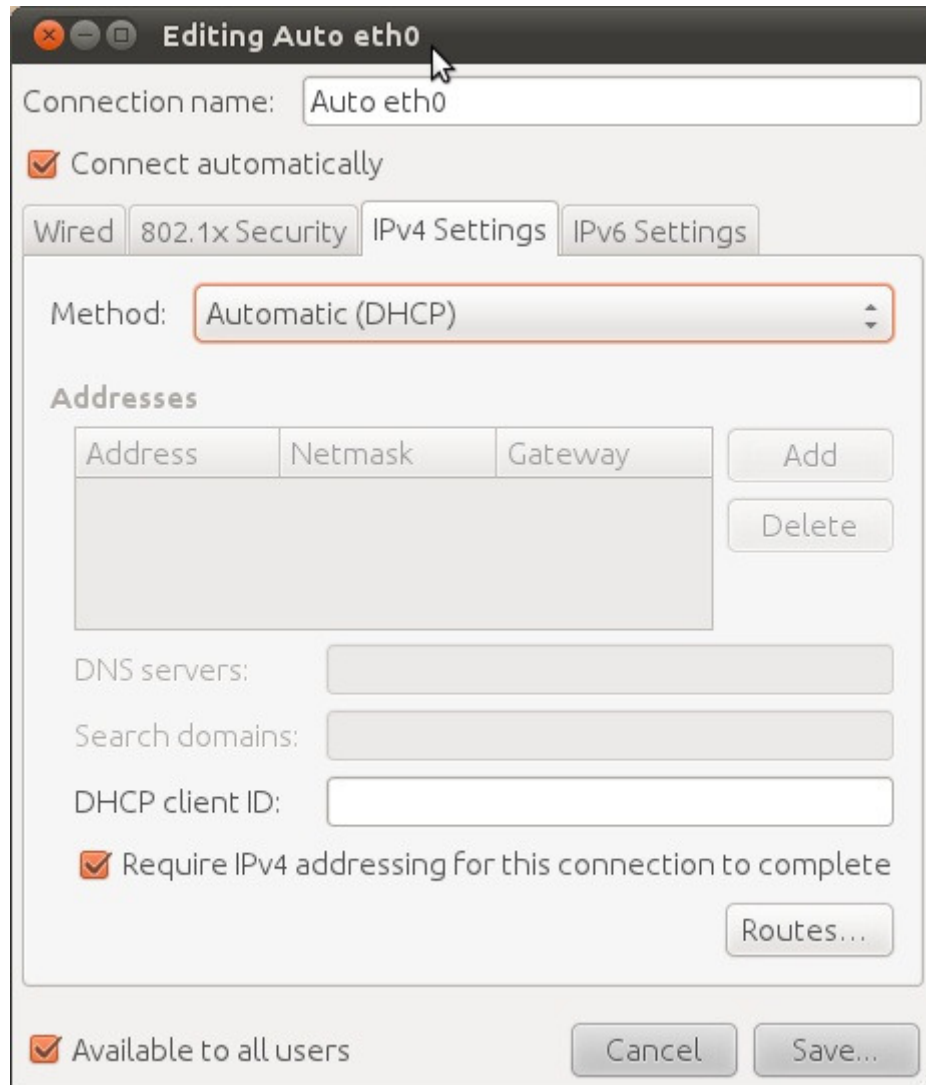


Figura 10 – Configuração da rede no sistema Linux® para IPv4 [Autoria própria].

Com a funcionalidade de auto-endereçamento *Stateless* para o IPv6, a configuração da placa de rede do *host* será configurada no padrão automático, para que o mesmo auto configure o endereço IPv6. Na figura 11 é demonstrado o padrão da configuração.

No ambiente em que o teste foi realizado o modem *Fritz!Box* não tem suporte ao protocolo DHCPv6, por este motivo que a autoconfiguração *Stateless* foi utilizada neste cenário de teste.

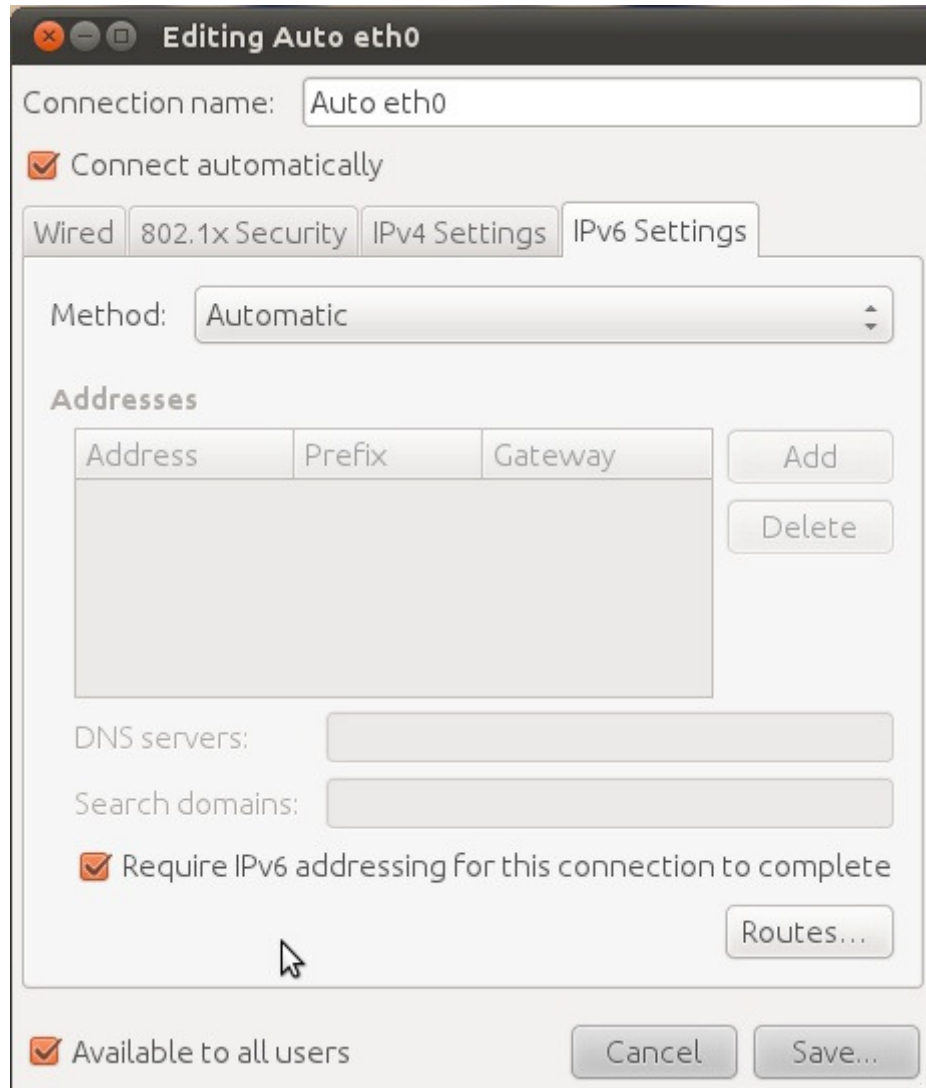


Figura 11 – Configuração da rede no sistema Linux® para IPv6 [Autoria própria].

Depois das configurações do *host*, a próxima etapa foi configurar o modem para as condições de testes em laboratório. Os padrões de configuração foram conforme a figura 12, sendo elas os padrões em que a rede da GVT tem suporte e viabilidade.

A conexão é realizada via Linha Digital de Assinantes – *Digital Subscriber Line* (DSL) no modo de operação de roteador. Usuário `ipv6@turbonet` com padrões de Modo de Transferência Assíncrono – *Asynchronous Transfer Mode* (ATM), sendo este VPI: 1 e VCI: 32, no padrão de banda larga de usuários de internet conhecido como Protocolo de Ponto-a-ponto sobre *Ethernet* – *Point-to-Point Protocol over Ethernet* (PPPOE).

Settings IPv6

Enter your account information here.

Connecting

Select whether your Internet connection should be established via DSL or LAN.

- Internet connection via DSL**
Select this kind of connection if FRITZ!Box is to connect directly using your DSL line.
- Internet connection via LAN 1**
Select this kind of connection if FRITZ!Box is to be connected to an already existing network (LAN), a cable modem or a DSL router.

Operating Mode

- Use one Internet connection for all computers (router)**
All connected network devices share one connection to the Internet
- Use FRITZ!Box as a DSL modem**
Each connected computer establishes its own Internet connection using its own access software

Account Information

Specify whether account information such as a 'User name' and 'Password' is required for Internet access.

- Account information required (PPPoE/PPPoA connection)**
- No account information required (in accordance with RFC 1483/RFC2684)**

Connection Settings

User name:

Password:

Password confirmation:

- Maintain Internet connection permanently**
 - Delay disconnection by provider to the period between o'clock
 - Clear Internet connection automatically after seconds.

Prioritization of the network devices requires data about the speed of your DSL line:

- Set the speeds of the DSL line automatically**
- Set the speeds of the DSL line manually**
 - Upstream: kBit/s
 - Downstream: kBit/s

DSL ATM Settings

Your DSL provider can tell you which values are required.

VPI:

VCI:

Encapsulation: PPPoE
 PPPoA/LLC
 PPPoA/VC-Mux

Apply Cancel Help



Figura 12 – Configuração da conexão do modem *Fritz!Box* [Autoria própria].

Seguindo as configurações do *Fritz!Box* é necessário a adequação do suporte ao IPv6, iniciando com a ativação do protocolo na caixa de seleção “*Enable support for IPv6*”. Note se que o prefixo do endereçamento da LAN utilizado é o prefixo de utilização proprietário da GVT com o prefixo: 2001:470:e0ae:6::/64 e MTU de 1492 de acordo o padrão utilizado pela prestadora.

Para conectividade IPv6 foi selecionado a 2ª opção da caixa de seleção “*Always use a native IPv6 connection*” que ao selecionar este tipo de configuração, o modem deve forçar a sua conexão, utilizando um provedor de serviço de internet.

Na conexão IPv6 a caixa de seleção “*Derive global address using only the assigned prefix*” ativa a função de autoconfiguração utilizando apenas o prefixo da operadora designado para a sua LAN. Na figura 13 estas configurações estão destacadas.

The screenshot displays the IPv6 configuration interface of a Fritz!Box. On the left, a sidebar lists various settings categories. The main panel is titled 'IPv6' and shows the current connection status as 'connected since 01/07/2011 at 15:44'. A table lists key IPv6 parameters:

Global IPv6 address of the FRITZ!Box:	2001:470:e0ae:5:224:feff:fec6:c4b3/64
Global IPv6 address obtained via:	Router Advertisement
Global Address Lifetimes (Valid/Preferred):	4294967295/4294967295 s
IPv6 MTU:	1492
Global IPv6 prefix for LAN:	2001:470:e0ae:6::/64
Global Prefix for LAN Lifetimes (Valid/Preferred):	7191/3591 s
Primary IPv6 DNS server:	2001:470:20::2
Secondary IPv6 DNS server:	

Below the table, the 'IPv6 support' section is highlighted in yellow. It includes the following configuration options:

- Enable support for IPv6
- IPv6 Connectivity**
 - Detect settings automatically (recommended)
First the system will attempt to negotiate native IPv6. If this fails, a 6to4 tunnel will be established.
 - Always use a native IPv6 connection
For this operation mode your Internet Service Provider must support native IPv6 on your line.
 - Always use a tunnel protocol for the IPv6 connection
Use IPv6 with a tunnel protocol over a conventional IPv4 connection. For this operation mode your Internet Service Provider does not have to support native IPv6.
- Connection Settings**
 - Automatically negotiate a global address
First FRITZ!Box attempts to determine the global address from the router advertisement of the provider. Then an address is requested via DHCPv6. If this fails, an address from the first /64 subnet of the determined prefix is used.
 - Obtain global address only via DHCPv6
The global IPv6 address of the FRITZ!Box is requested only via DHCPv6. Use this setting if you use an Internet connection via TV cable.
 - Derive global address using only the assigned prefix.
First FRITZ!Box attempts to determine the global address from the router advertisement. If this fails, an address from the first /64 subnet of the determined prefix is used.
- Additional Settings**
 - Set MTU manually: Bytes
 - Also announce DNS server via router advertisement (RFC 5006)
- Unique Local Addresses**

If no IPv6 Internet connection is active, FRITZ!Box can assign unique local addresses (ULA) to local network devices so that they can communicate with each other.

 - do not assign unique local addresses (ULA) (not recommended)
 - Assign unique local addresses (ULA) so long as no IPv6 connection exists (recommended)
 - Always assign unique local addresses (ULA)

Set ULA prefix manually:
fd 00 : : : /64

Unique Local Address of your FRITZ!Box: fd00::224:feff:fec6:c4b1/64

Buttons for 'Apply', 'Cancel', and 'Help' are located at the bottom right of the configuration area.

Figura 13 – Configuração das opções de IPv6 do modem *Fritz!Box* [Autoria própria].

Para fins de constatações da conexão, a figura 14 demonstra a saída da tela inicial do modem, contendo o *status* das conexões, sinalizadas pela coloração verde, onde é possível verificar o endereçamento IPv4 válido de endereço 201.86.86.223 e o prefixo IPv6 2001:470:e0ae:6::/64, ambos ativos.

Com esta verificação é possível afirmar que a técnica de pilha dupla foi aceita pelo modem e está com o *status* operacional.

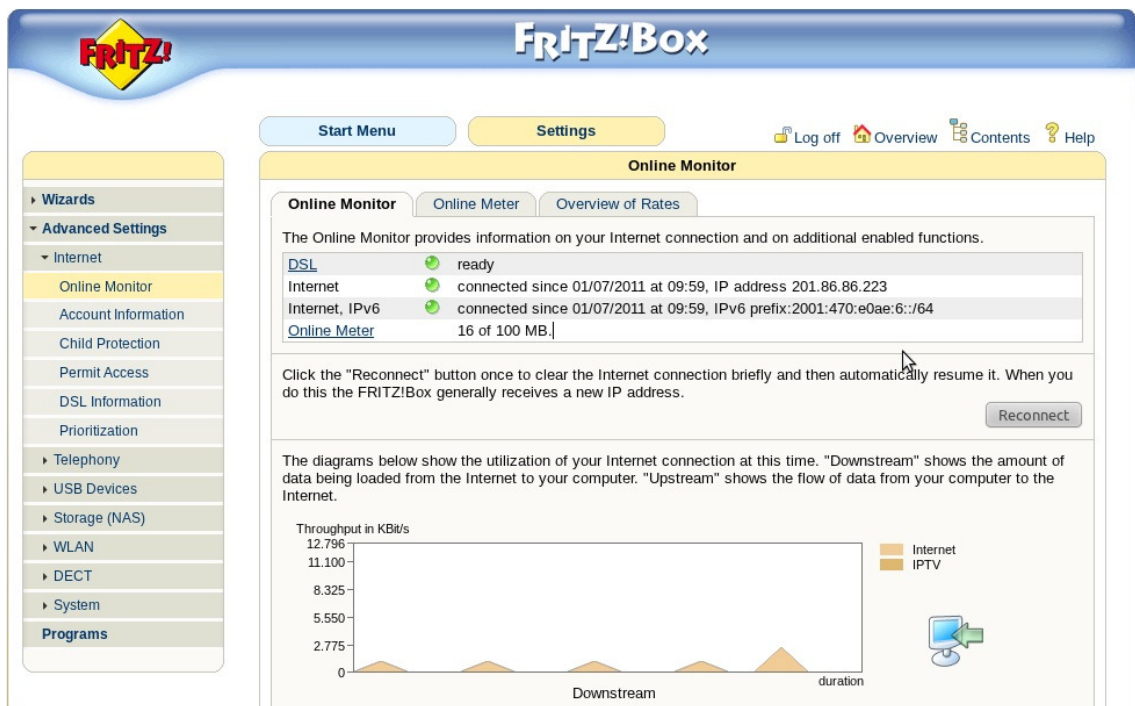


Figura 14 – Status da conexão do modem *Fritz!Box* [Autoria própria].

Voltando ao *host*, após as configurações do modem, neste deve ser observado os endereços de LAN entre o *host* e o modem. Seguindo a configuração do modem, para IPv4 é atribuído o endereçamento *inet addr*: 192.168.78.31 da rede 192.168.178.0/24 destinada a oferecer endereços IPv4 nas portas de LAN do modem, sendo este passando pelo processo de NAT, onde é utilizado o endereço 201.86.86.223 válido da internet.

Conforme as funcionalidades do IPv6, é atribuído ao *host* o endereço *inet6 addr*: 2001:470:e0ae:6:218:71ff:fe8c:dd9/64 que representa o padrão EUI-64, com a junção do prefixo delegado do BRAS – 2001:470:e0ae:6, com a transformação de endereço único global (vide capítulo 3) do endereço MAC da placa de rede do *host* – 218:71ff:fe8c:dd9.

Na figura 15 é observada a saída do comando *ifconfig*, demonstrando os endereços de *ethernet* (eth0) tanto quanto os endereços de loop local (lo) nas versões IPv4 - 127.0.0.1 e IPv6 - ::1/128, certificando assim que este *host* está equipado com a técnica de Pilha Dupla.

```

g0200787@notctarol-5205: ~
g0200787@notctarol-5205:~$ ifconfig
eth0      Link encap:Ethernet  Hwaddr 00:18:71:8c:0d:d9
          inet addr:192.168.178.31 Bcast:192.168.178.255 Mask:255.255.255.0
          inet6 addr: 2001:470:e0ae:6:218:71ff:fe8c:dd9/64 Scope:Global
          inet6 addr: fe80::218:71ff:fe8c:dd9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:150 errors:0 dropped:0 overruns:0 frame:0
          TX packets:193 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:28824 (28.8 KB)  TX bytes:24648 (24.6 KB)
          Interrupt:16

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:40 errors:0 dropped:0 overruns:0 frame:0
          TX packets:40 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2400 (2.4 KB)  TX bytes:2400 (2.4 KB)

g0200787@notctarol-5205:~$ _

```

Figura 15 – Status da conexão no *host* [Autoria própria].

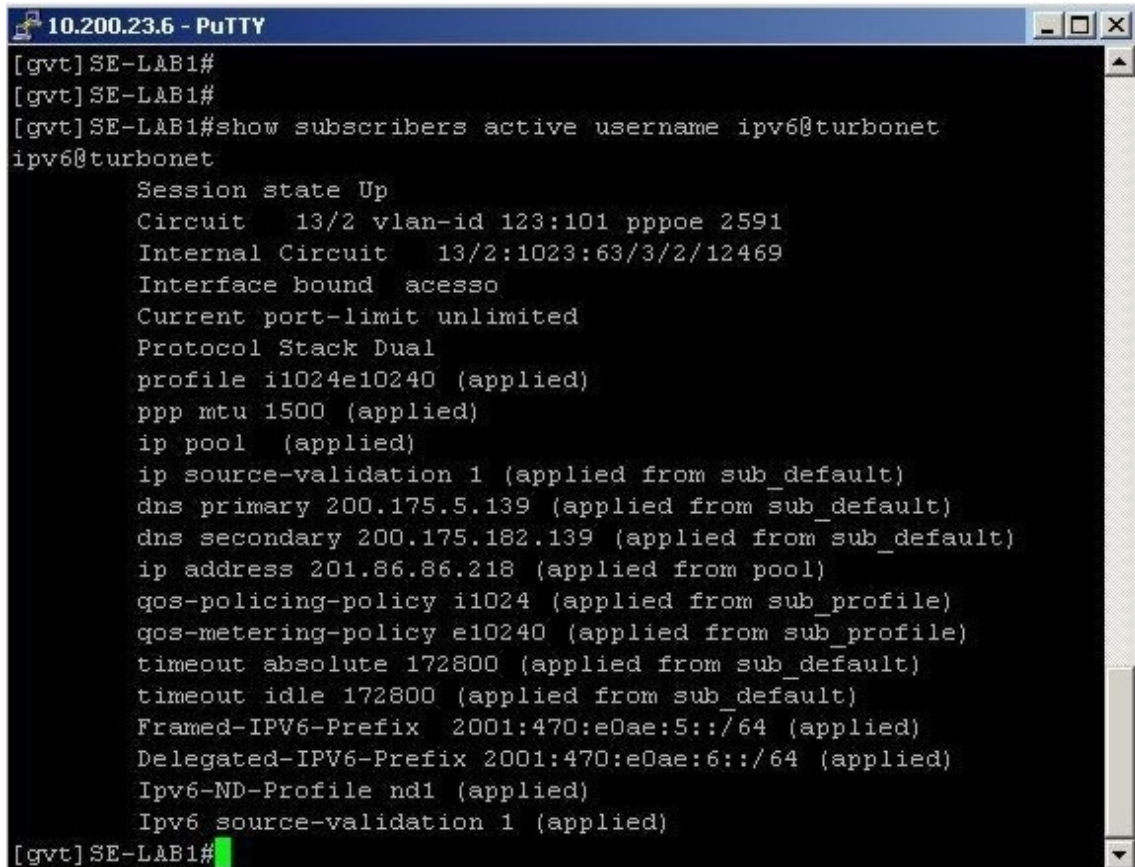
Outro equipamento envolvido na topologia é o DSLAM modelo: *Milegate*. Este equipamento é o responsável pelo sincronismo, pela conexão física e de enlace entre o modem e o BRAS. Por ser um equipamento de camada 2 não sofre configurações adicionais para IPv6 e técnica de Pilha Dupla.

O roteador de borda com a funcionalidade de BRAS do modelo: Smart Edge 800 necessita ser configurado para ter a funcionalidade de IPv6 e da técnica de Pilha Dupla. Na saída do comando realizado na figura 16, observamos o assinante: *ipv6@turbonet* e suas atribuições de rede e endereçamentos.

Principal observação de acordo o objetivo desta monografia é verificada na linha 6 “*Protocol Stack Dual*” no circuito PPPOE 2591, que representa a técnica de Pilha Dupla ativa para o assinante.

Endereços de DNS nas linhas 11 e 12, endereço de rede para a versões 4, na linha 13 de “*Ip address*” para IPv4. Linhas 18 “*Framed-IPV6-Prefix*” para Rede de Longa Distância – *Wide Area Network* (WAN) e 19 “*Delegated-IPV6-Prefix*” endereços delegados para a atribuição de endereços de um respectiva LAN, representando os prefixos válidos para redes IPv6.

Demais configurações como MTU, políticas de qualidade de serviço e *profile* de velocidade da linha de banda larga, também podem ser verificadas.



```

10.200.23.6 - PuTTY
[gvt] SE-LAB1#
[gvt] SE-LAB1#
[gvt] SE-LAB1#show subscribers active username ipv6@turbonet
ipv6@turbonet
  Session state Up
  Circuit      13/2 vlan-id 123:101 pppoe 2591
  Internal Circuit  13/2:1023:63/3/2/12469
  Interface bound  acesso
  Current port-limit unlimited
  Protocol Stack Dual
  profile i1024e10240 (applied)
  ppp mtu 1500 (applied)
  ip pool (applied)
  ip source-validation 1 (applied from sub_default)
  dns primary 200.175.5.139 (applied from sub_default)
  dns secondary 200.175.182.139 (applied from sub_default)
  ip address 201.86.86.218 (applied from pool)
  qos-policing-policy i1024 (applied from sub_profile)
  qos-metering-policy e10240 (applied from sub_profile)
  timeout absolute 172800 (applied from sub_default)
  timeout idle 172800 (applied from sub_default)
  Framed-IPV6-Prefix 2001:470:e0ae:5::/64 (applied)
  Delegated-IPV6-Prefix 2001:470:e0ae:6::/64 (applied)
  Ipv6-ND-Profile nd1 (applied)
  Ipv6 source-validation 1 (applied)
[gvt] SE-LAB1#

```

Figura 16 – Configuração do BRAS [Autoria própria].

Retornando ao *host* e suas atribuições de rede pode-se também ser demonstrado as tabelas de roteamento dos protocolos IPv4 e IPv6.

Na figura 17 com as saídas dos comandos “*netstat -RN*” para IPv4 e “*netstat -rn6*” para IPv6, proprietários do sistema operacional Linux[®], é possível verificar as rotas padrões, locais e de *loopback*.


```

g0200787@notctarol-5205: ~
g0200787@notctarol-5205:~$
g0200787@notctarol-5205:~$ netstat -rn
Kernel IP routing table
Destination      Gateway          Genmask         Flags   MSS Window  irtt Iface
192.168.178.0    0.0.0.0         255.255.255.0  U       0  0        0 eth0
169.254.0.0     0.0.0.0         255.255.0.0   U       0  0        0 eth0
0.0.0.0         192.168.178.1  0.0.0.0       UG      0  0        0 eth0
g0200787@notctarol-5205:~$
g0200787@notctarol-5205:~$
g0200787@notctarol-5205:~$
g0200787@notctarol-5205:~$
g0200787@notctarol-5205:~$ netstat -rn6
Kernel IPv6 routing table
Destination      Next Hop          Flag Met Ref Use If
2001:470:e0ae:6::/64      ::                UAe  256 0   0 eth0
fe80::/64                ::                U   256 0   0 eth0
::/0                    fe80::224:feff:fec6:c4b1 UGDA 1024 0   30 eth0
::/0                    ::                !n  -1  1  239 lo
::1/128                 ::                Un   0  1   29 lo
2001:470:e0ae:6:218:71ff:fe8c:dd9/128 ::                Un   0  1   18 lo
fe80::218:71ff:fe8c:dd9/128 ::                Un   0  1   7 lo
ff00::/8                ::                U   256 0   0 eth0
::/0                    ::                !n  -1  1  239 lo
g0200787@notctarol-5205:~$ _

```

Figura 17 – Netstat e rotas [Autoria própria].

A seguir com o comando “*host*” (ferramenta proprietário do sistema operacional Linux® para resolução de nomes), seguido do endereço do nome de um *website*, pode se obter as informações de endereços dos mesmo. Quando este website tiver suporte a endereço IPv4 e IPv6 o comando retornará com os endereços físicos (IP’s) do *website*, nas versões 4 e 6.

Além do comando *host* foi verificado a conectividade IPv6 do *host* pelo comando *ping6* (proprietário para redes IPv6) no endereço de IP do website conforme exemplo demonstrado na figura 18, www.ipv6.br, teste este realizado com sucesso.

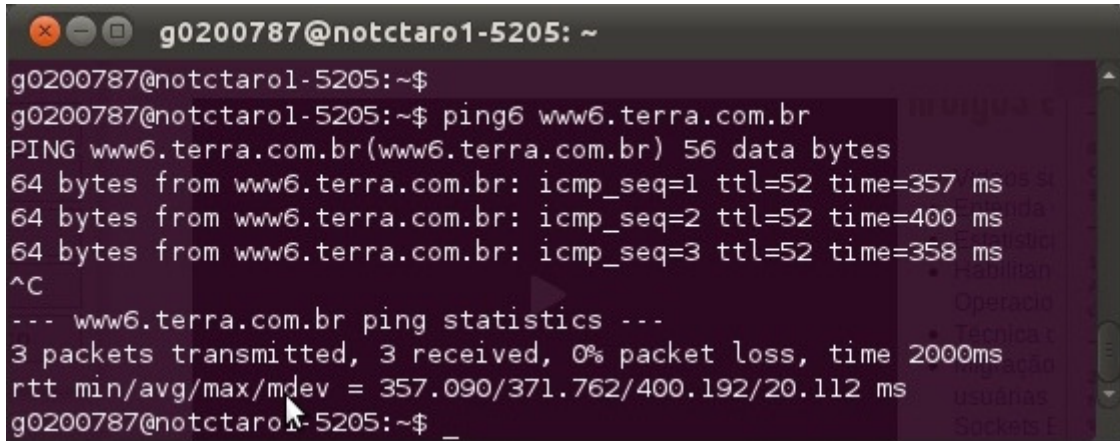
```

g0200787@notctarol-5205: ~
g0200787@notctarol-5205:~$
g0200787@notctarol-5205:~$ host www.ipv6.br
www.ipv6.br has address 200.160.4.22
www.ipv6.br has IPv6 address 2001:12ff:0:4::22
g0200787@notctarol-5205:~$
g0200787@notctarol-5205:~$ ping6 2001:12ff:0:4::22
PING 2001:12ff:0:4::22(2001:12ff:0:4::22) 56 data bytes
64 bytes from 2001:12ff:0:4::22: icmp_seq=1 ttl=55 time=388 ms
64 bytes from 2001:12ff:0:4::22: icmp_seq=2 ttl=55 time=388 ms
64 bytes from 2001:12ff:0:4::22: icmp_seq=3 ttl=55 time=388 ms
64 bytes from 2001:12ff:0:4::22: icmp_seq=4 ttl=55 time=388 ms
^C
--- 2001:12ff:0:4::22 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 388.071/388.335/388.578/0.234 ms
g0200787@notctarol-5205:~$ _

```

Figura 18 – Comando “*host*” e conectividade [Autoria própria].

Para demonstrar a funcionalidade de DNS foi executado também um comando "ping6" no endereço de nome do site `www6.terra.com.br`, retornado com sucesso a sequência de envio e resposta do comando. Conforme demonstrado na figura 19.



```

g0200787@notctaro1-5205: ~
g0200787@notctaro1-5205:~$
g0200787@notctaro1-5205:~$ ping6 www6.terra.com.br
PING www6.terra.com.br(www6.terra.com.br) 56 data bytes
64 bytes from www6.terra.com.br: icmp_seq=1 ttl=52 time=357 ms
64 bytes from www6.terra.com.br: icmp_seq=2 ttl=52 time=400 ms
64 bytes from www6.terra.com.br: icmp_seq=3 ttl=52 time=358 ms
^C
--- www6.terra.com.br ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 357.090/371.762/400.192/20.112 ms
g0200787@notctaro1-5205:~$ _

```

Figura 19 – Ping endereço web [Autoria própria].

Para fins de tráfego pela internet utilizando a Pilha Dupla, um website foi acessado através de um navegador de internet. Como exemplo na figura 20, é acessado o site com endereço comum IPv4 `www.ipv6.br`, mas este fornecendo no campo "Seu IP:" o endereços da LAN da pilha IPv6. É verificado que este não sofre NAT, pois o endereço da LAN é também o endereço válido para uma rede IPv6.

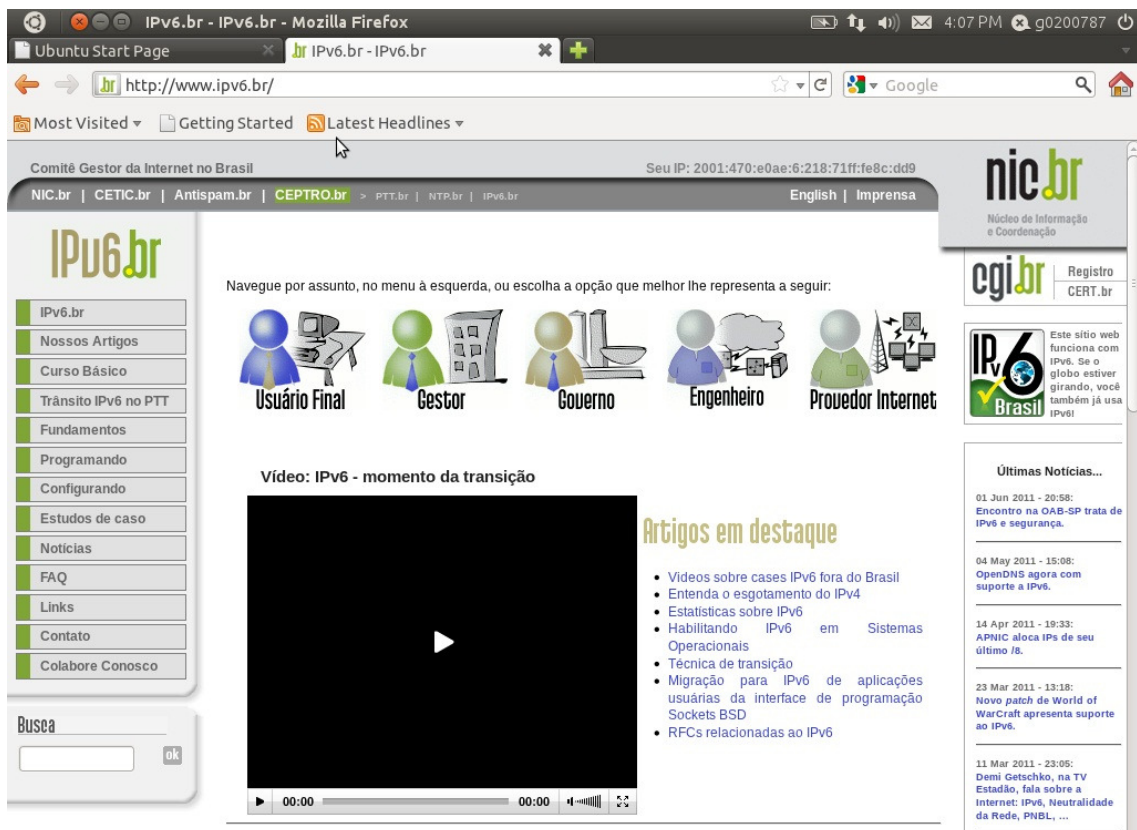


Figura 20 – Site `www.ipv6.br` [Autoria própria].

Como teste final de conectividade, foi realizada uma navegação com um domínio de nomenclatura IPv6, conforme o acesso na figura 20, o endereço inserido no navegador de internet, foi um endereço de acesso próprio IPv6.

Este *website* pode ser acessado via IPv4 digitando o endereço: www.terra.com.br ou conforme o exemplo para redes IPv6 no endereço: www6.terra.com.br.

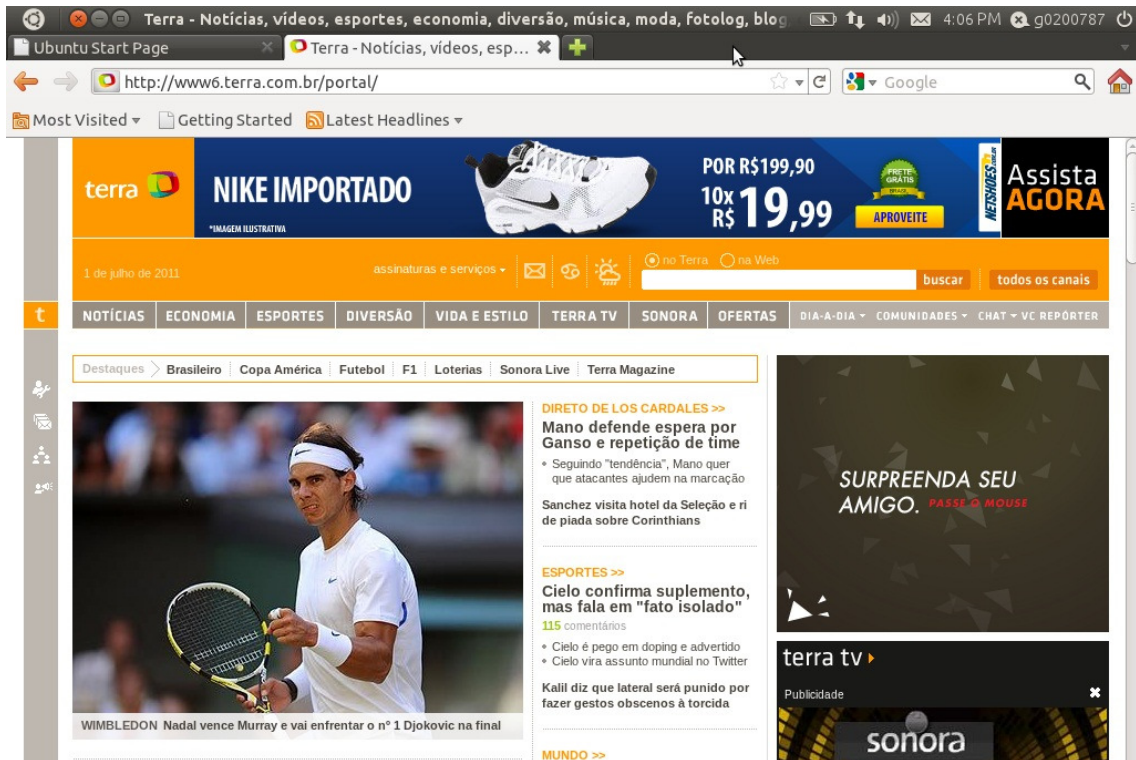


Figura 21 – Site www6.terra.com.br [Autoria própria].

Conforme descrito neste capítulo a técnica de Pilha Dupla pode ser configurada nos equipamentos envolvidos e testada em um ambiente real de internet.

Obtendo acesso a *websites* e respondendo a comandos de teste de conectividade suportados pelo sistema operacional, dentro da topologia estabelecida e de acordo as configurações necessárias para realizar esta simulação, suportadas pela rede da operadora de banda larga.

5 CONCLUSÃO

A necessidade da transição de versão do protocolo de internet dar-se-á em um futuro muito breve, pois a escassez da versão 4 está cada vez maior, onde foi visto que não há mais blocos novos disponíveis para a alocação de endereços e sim somente os já existentes.

Nos dias atuais além dos computadores pessoais, há uma gama muito vasta de novos componentes de redes e equipamentos que possam a vir utilizar endereçamento de internet, como *tablets*, *smartphones* e celulares. Tornando assim a internet cada vez mais dinâmica e com uma necessidade maior de disponibilidade de endereços.

Conforme abordado nesse trabalho o IPv6 não somente tem a vantagem de disponibilizar endereços válidos para toda a necessidade atual, mas também com a previsão futura. Dentre suas funcionalidades são relatados diversos protocolos de auxílio e funcionamento como o OSPFv3, ICMPv6 e DHCPv6. Conforme estudado a opção de autoconfiguração - *Stateless* facilita aos coordenadores de redes a obtenção de endereço IPv6, onde sua fácil compreensão pode ser observada no capítulo 3.

Uma desvantagem atual que foi abordada no capítulo 4, é que apesar de novos dispositivos e equipamentos de redes tendem a trazer o suporte ao IPv6, outros que já estão em utilização, como modems, *switches* e roteadores que não possuem suporte a IPv6 ou protocolos de camada superior como o OSPFv3. Outro ponto em desvantagem seria os Sistemas Operacionais que ainda não trazem suporte a versão 6 em suas configurações de rede.

Na simulação foi realizada a técnica de Pilha Dupla, onde são configuradas nos equipamentos de rede as duas versões de protocolos. Estes equipamentos então permitem aos usuários acessarem redes em IPv4 utilizando seu endereço IPv4 e redes IPv6 utilizando seu endereço IPv6. Tornando assim a transição de uma maneira menos impactante, sendo assim, este serviço mostra ser exequível e promissor.

A viabilidade para realizar a transição entre as versões do protocolo, nos tempos atuais, não requer um alto custo de modificações da estrutura das redes de computadores. Mas se os provedores de serviços não disponibilizarem suas estruturas para o IPv6 de uma maneira gradual, a mudança poderá ocorrer de forma brusca no momento em que a escassez atingir pontos críticos.

REFERÊNCIAS

COLCHER, Sérgio, et al. **VoIP – Voz sobre IP**. 3ª tiragem. Rio de Janeiro: Elsevier Editora, 2005. 288p.

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: 22 jul. 2011.

FILIPPETTI, Marco A. **CCNA 4.1 – Guia Completo de Estudo**. 5ª ed. Florianópolis: Visual Books, 2008. 480p.

FILIPPETTI, Marco A. IPv6 – O Futuro do Pretérito. **Admin Magazine**, São Paulo, v. 1, n. 2, p. 10-11, jun. 2011.

SANTOS, Rodrigo Regis dos, et al. **Curso IPv6 Básico**. 1ª ed. São Paulo: Ceptro.br, 2010. 315p.