INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MINAS GERAIS
CAMPUS SÃO JOÃO EVANGELISTA
Curso Superior de Bacharelado em Sistemas de Informação

Alex Wesley Gonçalves dos Santos
Juliano de Moura Pinto
Lucas Barroso Marques

IPv6
CABEÇALHO, ENDEREÇAMENTO E TÉCNICAS DE TRANSIÇÃO

São João Evangelista
2013

Alex Wesley Gonçalves dos Santos
Juliano de Moura Pinto
Lucas Barroso Marques

IPv6
CABEÇALHO, ENDEREÇAMENTO E TÉCNICAS DE TRANSIÇÃO

Monografia apresentada como requisito para obtenção do título de Bacharel em Sistemas de Informação do Instituto Federal de Minas Gerais – Campus São João Evangelista.

Orientador: Fernando Henriques Mafra
Coorientador: Ricardo Bittencourt Pimentel

São João Evangelista
2013

FICHA CATALOGRÁFICA
Elaborada pelo Serviço Técnico da Biblioteca do
Instituto Federal Minas Gerais – Campus São João Evangelista

S237i SANTOS, Alex Wesley Gonçalves dos , 1990 -

IPv6 cabeçalho, endereçamento e técnicas de transição./ Alex Wesley Gonçalves dos Santos; Lucas Barroso Marques Juliano de Moura Pinto. São João Evangelista, MG: IFMG – Campus São João Evangelista, 2013.
73 p.: il.

Trabalho de Conclusão de Curso - TCC (graduação) apresentado ao Instituto Federal Minas Gerais – Campus São João Evangelista – IFMG, Curso de Bacharelado em Sistemas de Informação, 2013.
Orientador: Prof. Me. Fernando Henriques Mafra
Coorientador: Prof. Esp. Ricardo Bittencourt Pimentel

1. Rede. 2. Protocolo. 3. IP. 4. Cabeçalho. I. Instituto Federal Minas Gerais – Campus São João Evangelista. Curso de Bacharelado em Sistemas de Informação. II. Título.

CDD 004.6

Alex Wesley Gonçalves dos Santos
Juliano de Moura Pinto
Lucas Barroso Marques

IPv6
CABEÇALHO, ENDEREÇAMENTO E TÉCNICAS DE TRANSIÇÃO

Monografia apresentada como requisito para obtenção do título de Bacharel em Sistemas de Informação do Instituto Federal de Minas Gerais – Campus São João Evangelista.

Fernando Henriques Mafra – IFMG

Ricardo Bittencourt Pimentel – IFMG

Ronan Dutra Mendonça – IFMG

São João Evangelista, 12 de novembro de 2013

"Eu jamais me engano. Só me enganei uma vez: quando acreditei estar enganado!" (Prof. Girafales).

RESUMO

O presente projeto aborda o esgotamento do IPv4 e a implantação da nova versão do protocolo, o IPv6. O trabalho consiste em identificar as diferenças entre as versões do protocolo de comunicação, o IPv4 e o IPv6. São apresentadas as características referentes ao cabeçalho, endereçamento e funcionalidades do IPv6. Para que a implantação do novo protocolo seja de forma gradual, será necessário o uso das técnicas de transição, que possibilitam a coexistência das duas versões. O trabalho tem por objetivo mostrar a técnicas mais indicadas para o uso do protocolo IPv6 juntamente com o IPv4 no momento em que o IPv6 se tornar majoritário na rede. A pesquisa apresenta conceitos teóricos e testes que simulam o uso das técnicas de transição indicadas para o atual momento da transição no Brasil. Foram avaliadas a técnica de transição Pilha Dupla, onde todos os equipamentos da rede utilizam ambos os protocolos, um em cada pilha, a técnica DSLIte e NAT64/DNS64, que são indicadas para sub-rede majoritariamente IPv6 mas ainda possuem ilhas IPv4 que necessitam ser acessadas, sendo que a técnica DSLite utiliza túneis para encapsulamento de cabeçalho IPv4 em IPv6, enquanto a técnica NAT64/DNS64 utiliza tradução de endereço IPv4 em IPv6. Por fim, os testes realizados possibilitaram a conclusão do cenário especifico em que cada técnica pode ser aplicada.

Palavras Chave: IPv4, IPv6, técnicas de transição.

ABSTRACT

This following project addresses the ending of IPv4 and the deployment of new protocol version, IPv6. The work is to identify the differences between versions of communication protocols, both IPv4 and IPv6. Shows the IPv6 characteristics for the header, addressing, and features. For the implementation of the new protocol be gradually, you will need to use the techniques of transition, enabling the coexistence of the two versions. The paper aims to show the techniques most suitable for use IPv6 together with IPv4 when IPv6 become the majority in the network. The research presents theoretical concepts and tests that simulate the use of the techniques indicated of transition for the current time of transition in Brazil. We evaluated the technique of Dual Stack Transition, where all network equipment using both protocols, one in each cell, the technique and DSLite NAT64/DNS64, which are indicated for IPv6 subnet mostly but still have IPv4 islands that need to be accessed. Since the technique uses DSLite tunnels for encapsulation of IPv6 in IPv4 header, while the technical NAT64/DNS64 uses translation of IPv4 over IPv6. Finally, tests have enabled the conclusion of setting where each specific technique can be applied.

Keywords: IPv4, IPv6, techniques of transition.

LISTA DE FIGURAS

Tabela Página

LISTA DE TABELAS

LISTA DE SIGLAS

AFTR	Address Family Transition Router
ALGs	Aplication level Gateways
ARP	Address Resolution Protocol
B4	DSLite Basic Bridging BroadBand
BIND	Berkeley Internet Name Domain
CGI	Comitê Gestor da Internet no Brasil
CIDR	Classless Inter-DomainRouting
CPE	Customer Premise Equipment
DHCP	Dynamic Host Configuration Control
DNS	Domain Name System
DSlite	Dual Stack Lite
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICMPv6	Internet Control Message Protocol version 6
IETF	Internet Enginnering Task Force
IHL	Header Length
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISC	Internet System Consortium
ISO	International for Standartion
ISP	Internet service provider
MAC	Media Control Acess
MLD	Multicast Listener Discovery
MTU	MaximumTransmit Unit
NAT	Network Address Translation
NA	Neighbor Advertisement
NICbr	Núcleo de Informação e Coordenação do Ponto BR
NS	Neighbor Solicitation
NTP	Network Time Protocol
OSFv2	Open Shortest Path First
OSI	Open Systems Intenconection
QoS	Quality of service
RA	Router Advertisement
RS	Router Solicitation
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TTL	Time to live
UDP	User Datagrama Protocol
ULA	Unique Local Address

SUMÁRIO

1. INTRODUÇÃO

Com a necessidade de comunicação, que é essencial tanto para o meio corporativo quanto para o meio pessoal, as pessoas dependem cada vez mais das soluções oferecidas pela tecnologia da informação. Como exemplo de evolução no campo da comunicação, os dispositivos eletrônicos ganharam espaço nas atividades comuns da rotina das pessoas. Um marco que serve como exemplo é a telefonia, que hoje tem a capacidade de trafegar voz, imagem e dados com o uso de um telefone celular por meio das redes integradas à *Internet*.

Anteriormente os aparelhos eletrônicos disponíveis no mercado eram específicos: televisão era usada somente para transmissão de imagens; telefones, para realizar chamadas, e os computadores, para atividades comuns (executar aplicativos, reprodução de músicas, vídeos e uso básico da *Internet)*. Atualmente esses equipamentos são multitarefas e exercem qualquer uma dessas funções. Eles ainda têm a capacidade de comunicar-se entre si, criando então a chamada rede de computadores ou rede de comunicação. Isso é possível por meio da função do protocolo *Internet Protocol* (IP), que permite a interação entre os dispositivos físicos e sistemas de diferentes tecnologias. (TORRES, 2001).

Tendo em vista que o número de possibilidades de acesso à *Internet* aumenta, e que cada um desses dispositivos necessita de um endereço para se identificar na rede mas o protocolo atual, versão 4, não possibilita atender o crescimento exponencial desses dispositivos e que o IPv4(*Internet Protocol version 4*), ainda que disponibilize cerca de 4 bilhões de endereços distintos mas não o suficiente para a demanda futura. Foi desenvolvido no final de 1995, uma nova versão do protocolo IP, um protocolo que promete atender a essa necessidade. A versão oficial desse modelo é o IPv6(*Internet Protocol version 6)*, que substituirá a atual IPv4. Esse protocolo possibilita 4 bilhões de vezes mais endereços que o IPv4, além desse aumento significativo o IPv6 oferece um melhor aproveitamento do tráfego de informações. (SCRIMGER, 2002).

Como o IPv6 e o IPv4 não são compatíveis, houve a necessidade da criação de uma forma para que ambos pudessem trabalhar de forma simultânea, compartilhando os mesmos equipamentos. Tendo isso em vista, os órgãos que gerenciam os padrões estabelecidos na *Internet* e nas redes de computadores desenvolveram técnicas para que a transição fosse feita de forma gradual. Mas o

assunto não é disseminado entre os profissionais da área, e de muito pouco conhecimento dos usuários finais. Diante disso tem-se a necessidade de mostrar quais as técnicas indicadas tanto para usuários finais como para provedores de *Internet* para a coexistência dos protocolos IPv4 e o IPv6. (COMER, 2006).

O trabalho se justifica em demonstrar as soluções para que haja a coexistência e interoperabilidade entre ambos os protocolos e para isso é necessário o uso de tecnologias auxiliares, conhecidas como técnicas de transição. A necessidade dessa coexistência ocorre em diferentes cenários, assim sendo**,** será apresentado um estudo das técnicas de transição desenvolvidas pelo órgão responsável por especificar os padrões que serão utilizados na *Internet* o IETF(*Internet Enginnering Task Force*).

O trabalho tem como objetivo demonstrar as técnicas mais indicadas para o uso do protocolo IPv6 juntamente com o IPv4 no momento em que o IPv6 se tornar majoritário na rede. As técnicas são: Pilha dupla, DSlite e NAT64/DNS64 , técnicas essas que são indicadas para um cenário futuro no qual a rede será majoritariamente IPv6 mas ainda com várias ilhas IPv4 ainda em uso. Para comprovar a compatibilidade do uso dos dois protocolos simultaneamente na rede serão realizados laboratórios utilizando as técnicas citadas, tendo como objetivos específicos: a) fazer um estudo dos principais autores; b) apresentar as mudanças de maior relevância do IPv6 em relação ao IPv4, que são o formato do cabeçalho, padrão de endereçamento e as funcionalidades adicionadas ao IPv6; c) apresentar as técnicas de transição e demonstrar o cenário em que cada uma se aplica.

O método utilizado será o de estudo bibliográfico das técnicas de transição entre as versões, e demonstração de laboratórios realizados pela NICbr (Núcleo de Informação e Coordenação do Ponto BR) para comprovar a aplicabilidade de cada técnica em determinado cenário e a compatibilidade entre os protocolos.

2. FUNDAMENTAÇÃO TEÓRICA

Para realizar um estudo sobre IPv6, tem-se a necessidade de conhecer como foi implementada a rede de comunicação. Portanto, este capítulo apresenta o estudo básico sobre os protocolos de comunicação, que são: Modelo OSI (*Open Systems Interconnection)*, TCP (*Transmission Control Protocol)*, IPv4 e IPv6.

2.1. Modelo OSI

O tráfego de rede é gerado quando ocorre uma solicitação na rede. A solicitação tem de ser alterada daquilo que o usuário vê para um formato que possa ser utilizado na rede. Essa transformação é possível por meio do modelo de referência (OSI), desenvolvido pela *International Organization for Standartion*(ISO). O trafego de rede é enviado na forma de pacotes de dados, que é a informação de um usuário, ou seja o pacote, transformado em um formato entendido pela rede. Todas as transformações derivam do modelo OSI de sete camadas. (SCRIMGER, 2002).

A camada OSI é composta basicamente por 7 camadas, apresentadas na tabela 1 a seguir:

Tabela 1: Descrição das camadas do Modelo OSI (continua)

Camada	Descrição
Camada 1: Física	Hardware de rede básico, que fornece a especificação detalhada do hardware de LAN.
Camada 2: Enlace	Especifica como organizar os dados em quadros e como transmiti-los através de uma rede.
Camada 3: Rede	Especifica como são atribuídos endereços e como são encaminhados pacotes de uma ponta a outra da rede.

Tabela 1: Descrição das camadas do Modelo OSI (conclusão)

Camada 4: Transporte	Especifica como tratar os detalhes de transferência confiável.
Camada 5: Sessão	Especifica como estabelecer uma sessão de comunicação com o sistema remoto.
Camada6: Apresentação	Especifica como representar os dados**. São** necessários para traduzir da representação de um computador para representação do outro.
Camada 7: Aplicação	Especifica como um aplicativo em particular usa uma rede, mostra como um programa aplicativo faz um pedido e como um aplicativo em outra **máquina** responde.

Fonte: COMER, 2007

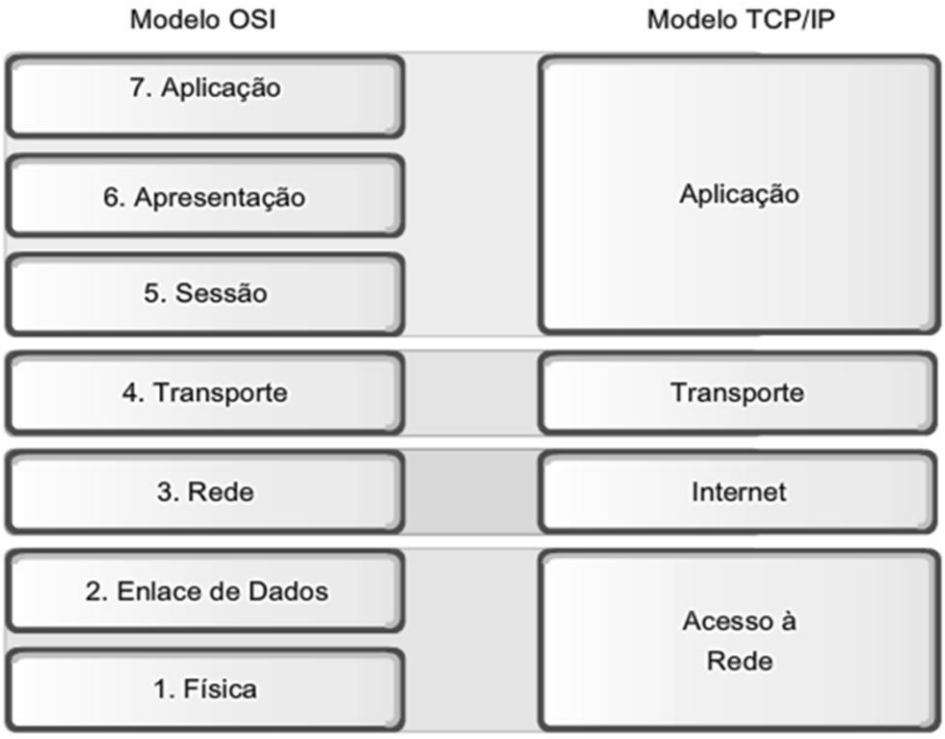
De acordo com Tanenbaum (2003), o modelo OSI possui princípios aplicados para se chegar às sete camadas, veja o resumo dos princípios a seguir:

a) Uma camada deve ser criada onde houver necessidade de um grau de abstração adicional;
b) Cada camada deve executar uma função bem definida;
c) A função de cada camada deve ser escolhida tendo em vista a definição de protocolos padronizados internacionalmente;
d) Os limites de camadas devem ser escolhidos para minimizar o fluxo de informações pelas interfaces;
e) O número de camadas deve ser grande, o bastante para que funções distintas não precisem ser desnecessariamente colocadas na mesma camada; e pequeno, o suficiente para que a arquitetura não se torne difícil de ser controlado.

2.2. TCP/IP

Segundo Torres (2001), o TCP/IP é, na realidade, um conjunto de protocolos. Os mais comuns são justamente o nome desse conjunto: TCP (Protocolo de controle da Transmissão) e IP(*Internet Protocol*), que operam nas camadas Transporte e *Internet*, respectivamente. A arquitetura do TCP/IP é mostrada na figura 1, como pode ser observado é um protocolo de quatro camadas, fazendo correlação das camadas do TCP/IP com as camadas do modelo OSI.

Figura 1: Modelo OSI x Modelo TCP



Fonte: SCRIMGER, 2002

2.2.1. Camada de aplicação

O modelo TCP/IP não possui as camadas de sessão e apresentação. Como não foi percebida nenhuma necessidade, elas não foram incluídas. As experiências com o modelo OSI demonstraram a correção dessa tese: elas são pouco usadas na maioria das aplicações segundo Tanenbaum(2002).

A camada de aplicação faz a comunicação entre os aplicativos e o protocolo de transporte. Existem vários protocolos que operam na camada de aplicação. Os

mais conhecidos são o HTTP (*HyperText Tranfer Protocol*), SMTP (*Simple Mail Transfer Protocol*), o FTP (*File Transfer Protocol*), o SNMP (*Simple Network Management Protocol*), o DNS (*Domain Name System*) e o Telnet (TORRES, 2001).

2.2.2. Camada de Transporte

A camada de transporte é responsável por pegar os dados enviados pela camada de aplicação e transformá-los em pacotes a serem repassados para a camada de *Internet* (Torres,2001).

Segundo Scrimger (2002) dois protocolos são utilizados na camada de Transporte: *Transmission Control Protocol* (TCP), comunicação confiável orientada para a conexão, que é mais lenta na transmissão e *User Datagrama Protocol* (UDP), comunicação não garantida, que é mais rápida na transmissão.

2.2.3. Camada de Internet

Principal responsável pelo endereçamento e roteamento de rede. Além disso, essa camada é responsável pela fragmentação do pacote. Os pacotes de dados são montados e remontados para transmissão nessa camada (SCRIMGER,2002).

Datagramas é o nome dado aos pacotes divididos. São adicionadas a ele informações sobre o caminho que deverá percorrer. São enviados para camada de interface com a rede, onde são transmitidos pelo cabeamento da rede através de quadros. Essa camada não verifica se eles chegaram ao destino (TORRES, 2001).

O endereçamento de IP permite que o TCP/IP escalone desde redes muito pequenas, ate grandes empresas de host de milhões de dólares utilizando um único esquema de endereçamento. Atualmente, o *Internet Protocol* versão 4(IPv4) está em utilização. O IPv4 consiste em 5 classes de endereços, rotuladas pelas letras A até E, gerando assim em torno de 4 bilhões de endereços disponíveis.(SCRIMGER, 2002).

2.2.4. Camada Física

Primeira camada do modelo TCP/IP, corresponde as camadas de Enlace e as camadas físicas do modelo OSI, e é responsável pelo acesso a rede. Essa camada

se comunica diretamente com a rede, é a ligação entre a topologia de rede e a camada de *Internet* (Scrimger, 2002).

2.3. Endereçamento IP

O protocolo TCP/IP é roteável, isto é, foi criado pensando-se na interligação de diversas redes – por meio das quais podemos ter diversos caminhos interligando o transmissor e o receptor – culminando assim na rede mundial que hoje conhecemos por *Internet*. Por isso, utiliza-se um esquema de endereçamento lógico chamado endereçamento IP. Em uma rede TCP/IP cada dispositivo conectado em uma rede necessita usar pelo menos um endereço IP, endereço que permite identificar o dispositivo e a rede à qual ele pertence (Torres, 2001).

O endereço IP é especifico que para cada host é atribuído um numero de 32 bits conhecido como endereço de Protocolo *Internet* do host. Cada endereço IP de 32 bits é dividido em duas partes: prefixo e sufixo; hierarquia projetada para fazer uso eficiente de roteamento. O prefixo do endereço identifica a rede física à qual o computador esta acoplado, enquanto o sufixo identifica um computador individual naquela rede (COMER, 2007).

2.4. IPv6

A evolução da arquitetura TCP/IP sempre esteve interligada à evolução da *Internet* global. Hoje em dia**,** centenas de milhões de usuários dependem da *Internet* em seu ambiente de trabalho diário. No inicio da década de 1990, os pesquisadores argumentaram que o IPv4 seria insuficiente para as novas aplicações, visto que a expansão global da rede seria dada de maneira desenfreada. Isso porque o crescimento da *Internet*, que dobrava de tamanho em media a cada nove meses, logo esgotaria o conjunto de endereços disponíveis (COMER, 2006).

O IPv6 introduz varias alterações no protocolo IPv4. Essas alterações tornaram o protocolo muito mais flexível e confiável, e fornece um espaço de endereçamento quase ilimitado. Dentre as alterações se destaca: a) capacidade de roteamento e endereçamento expandido; b) simplificação do formato do cabeçalho; melhor suporte de opções; capacidade para autenticação e privacidade. (SCRIMGER, 2002).

Segundo Tanenbaum (2001), um aperfeiçoamento importante no IPv6 é a simplificação do cabeçalho. Ele contém apenas **7** campos, enquanto o cabeçalho de IPv4 possui 13. Essa mudança permite aos roteadores processarem os pacotes com mais rapidez e, dessa forma, melhorar *a* taxa de transferência e o retardo. Outra grande mudança foi o melhor suporte para as opções oferecidas. Essa mudança é fundamental para o novo cabeçalho, pois os campos que até então obrigatórios, agora são opcionais.

O endereçamento do IPv6 foi expandido, agora possui 128 bits diferentemente do IPv4 que possuía 32 bits. O número de endereços aumentou exponencialmente, passando de 4 bilhões de endereços existentes na versão 4, para (3,4 x 10^38) de endereços na versão 6.

3. REVISÃO DE LITERATURA

Conforme LAKATOS E MARCONI (2006), revisão de literatura “é uma pesquisa teórica que tem por objetivo estudar um foco ou um assunto, não apenas citando partes desses textos, repetindo o que já está escrito, mas sim, conseguir ter uma visão crítica daquilo que está escrito, é uma atividade científica que ajuda a descobrir e entender a realidade.”

Neste capitulo são apresentados trabalhos relacionados ao tema principal, visando destacar as principais características relacionadas ao trabalho a ser desenvolvido.

3.1. TCC IPv6 versus IPv4, características, instalação e compatibilidade

O trabalho de Prazer (2007) faz referência às diferenças entre as versões 4 e 6 do protocolo, comparando o modelo didático com pacotes coletados em uma comunicação de dados entre os sistemas operacionais mais utilizados no mercado, onde haja comunicação entre IPs de mesma versão (v6) e versões diferentes (v6 e v4) utilizando algumas técnicas que comprovam a compatibilidade entre elas. Explica o surgimento do protocolo IP e como foi incorporado ao protocolo TCP, em qual modelo esse protocolo foi baseado, dando algumas informações sobre o modelo de camadas OSI.

Prazer (2007) demonstra em sequência, as características do protocolo IPv6, que, de início, mostra que o motivo básico no qual a versão atual do protocolo precisava ser renovada é a necessidade do aumento de endereços, trazendo informações sobre o novo cabeçalho do datagrama, detalhando a função de cada campo do cabeçalho. Como o aumento no número de endereços é a característica de maior impacto da nova versão do protocolo, é tratada com bastante ênfase, mostrando todas as mudanças do tipo de endereço que o IPv6 passou a ter, citando também os endereços *multicast* e o novo *anycast*. Prazer (2007) cita as compatibilidades entre as versões e faz alguns testes de configuração do IPv6, apresentando um laboratório prático com alguns dos sistemas operacionais mais utilizados mostrando o funcionamento e a compatibilidade técnica entre estes protocolos IPv6 e IPv4, o que poderá servir de base para montagem de laboratórios de estudo e planejamento, como alternativa de diminuição dos impactos,

principalmente com a substituição de *hardware* e ajustes de *softwares* ainda não compatíveis.

Prazer(2007) conclui que mesmo com as vantagens da implementação do IPv6, são necessários certos cuidados com o inicio da utilização. As empresas que produzem softwares e hardwares já desenvolvem produtos com compatibilidade entre a versão 4 e 6 do protocolo.

3.2. IPv6 – Funcionalidades e Métodos de Transição

Araújo *et. al* (2011), apresenta as características do IPv4 e IPv6. No início de seu trabalho ele introduz alguns fundamentos teóricos que são importantes para entender a evolução ocorrida no conceito de rede de computadores e protocolos de comunicação. Ele demonstra os principais conceitos relacionados à rede de computadores e ao protocolo TCP/IP, começando pelo surgimento da *Internet*. Cita os fatores que colaboraram para o crescimento no número de computadores e endereços, como o aumento no uso da *Internet*. Devido à expansão da rede chamada *Internet*, surge o problema da escassez de endereços de IP. Este problema levanta a hipótese de se ter outro protocolo de comunicação que atenda as novas necessidades, surgindo assim uma nova versão do IP, que é o IPv6. (ARAÚJO *et. al,* 2011)

Este trabalho apresenta características do IPv6, assim como as melhorias ocorridas em relação ao IPv4. Foram demonstradas em especial, as mudanças ocorridas no cabeçalho em comparação à versão 4, um novo campo foi incluído no cabeçalho do IPv6. Com a transição dos protocolos e a criação de um novo, algumas características de IPv4 entraram em desuso e foram removidas da nova versão. (ARAÚJO *et. al,* 2011)

Apresentou-se também as características das técnicas de comunicação/transição entre as versões do protocolo que serão usados para possibilitar a comunicação entre os diferentes protocolos, IPv4 e IPv6. As técnicas baseiam-se em modelos de pilha dupla, tunelamento e tradução. O autor concluiu com as demonstrações quais as vantagens e as desvantagens existentes em cada um destas técnicas que devem ser levadas em consideração antes de escolher qual implementar. (ARAÚJO *et. al,* 2011)

3.3. TCC – Rede IPv6 com integração IPv4

No trabalho de Silveira (2012), são citadas algumas características do IPv4 e o esgotamento de seus endereços. Houve então a necessidade de ser desenvolvido um novo protocolo, que suprisse as limitações geradas com o esgotamento da versão 4, não somente isso, foram adicionadas melhorias nesta nova versão do protocolo, o IPv6. Com o surgimento e a implantação do IPv6, será nativa a comunicação entre a nova versão e a antiga, mas o contrário não acontece, tendo a necessidade então de aplicar técnicas que realizem essa comunicação. Essa necessidade ocorre pelo fato de que a nova versão vai ser implantada, mas a antiga não irá parar de funcionar de imediato, e com isso, a comunicação entre elas deverá existir até o momento em que seja possível o uso apenas da nova versão.

As técnicas para a comunicação/transição são Pilha Dupla, Tradução e Tunelamento. Este trabalho faz um estudo de tais técnicas, suas características e exemplifica como cada uma funciona, com exceção da técnica de tunelamento, por não existir a possibilidade de se criar um ambiente de comunicação entre redes IPv4 e IPv6, exceto por encapsulamento de datagramas IPv6 em datagramas IPv4. A técnica de transição Pilha dupla é explicada assim como os processos para a sua implantação. Implementando testes com o intuito de mostrar como a técnica funciona. O mesmo ocorre com a técnica NAT64/DNS64, que também é explicada e exemplificada através de testes de funcionalidade. (SILVEIRA, 2012).

Ao fim do trabalho, Silveira (2012), chegou a conclusão de que o método Pilha dupla é o melhor a ser usado para a comunicação entre os protocolos IPv4 e IPv6, por se adaptar facilmente às duas versões. Os testes com NAT64/DNS64 mostraram uma boa eficiência, porém apresentaram problemas com alguns aplicativos, como AMSN, TORRENT, SKYPE. Esse problema se deu pelo fato de gerar requisições e esperar um endereço IPV4 como resposta. Mesmo não sendo realizados testes com a técnica IVI, por limitações de hardware, pôde ser observado que é uma boa alternativa para redes apenas com máquinas de endereçamento IPv6, por ter acesso nativo a esta versão do protocolo e pela possibilidade de acesso a máquinas com endereçamento IPv4 através de técnicas de mapeamento.

4. METODOLOGIA

Diante da enorme necessidade de novas formas de transmissão de informação em diversos meios, tende-se a necessitar de novas soluções oferecidas pelas tecnologias da informação. Todos os aparelhos eletrônicos que participam dessa comunicação necessitam de um endereço físico, endereço este nomeado de *Internet Protocol(*IP).

> A metodologia é o conjunto de atividades sistemáticas e racionais que permite alcançar o objetivo, traçando o caminho a ser seguido, detectando erros e auxiliando as decisões do cientista. (LAKATOS; MARCONI, 2001, p.83).

A metodologia usada baseia-se no estudo de várias bibliografias relacionadas e trabalhos conexos ao tema para um melhor entendimento do assunto. No estudo de trabalhos de Silveira (2012),Araújo (2011) e Prazer (2007) foi visto que nenhum aborda todas as características do IPv6 e que para realizar um entendimento amplo do novo protocolo teríamos que abordar todas essas alterações e funcionalidades.

Um dos grandes fatores da necessidade de um novo protocolo é a escassez de endereços físicos da versão 4. Inicialmente abordar-se-á, de forma sucinta ,algumas características da versão antecessora do IPv6, como: modelo OSI, cabeçalho e datagrama.

Após o breve estudo sobre o IPv4, demonstrar-se-á todas as mudanças que o IPv6, novo modelo de protocolo, acarretará na nova concepção de comunicação. As características dessa nova versão serão ressaltadas, desde as mudanças relacionadas ao endereço, passando pelos campos do cabeçalho, tamanho do datagrama do protocolo e as novas funcionalidades agregadas . Explicar-se-á como as técnicas de transição serão usadas em diferentes cenários, onde os protocolos coexistem e se comunicam. Nesta perspectiva, enfatizará os problemas que podem ocorrer neste processo.

Diante de tal necessidade, para os testes laboratoriais serão utilizados o Sistema Operacional Linux Ubuntu 11.04, juntamente com o *Software* emulador de redes Core 4.3 para apresentar as técnicas DSLite e NAT64/DNS64, para apresentar a técnica Pilha Dupla utilizar-se-á uma máquina com Sistema Operacional *Windows* 8 e navegador *Internet Explorer* 10 e conexão banda larga. Os

testes tem como finalidade exemplificar as técnicas Pilha Dupla, Tradução e Tunelamento, que realizam a comunicação entre protocolos IPv4 e IPv6 e também a comunicação dos protocolos de forma individual . O intuito da realização destes testes laboratoriais é mostrar como é feita a configuração para que as técnicas sejam utilizadas, bem como comprovar a eficácia e demonstrar o funcionamento das técnicas de transição.

5. RESULTADOS

Este capítulo apresenta as mudanças mais significativas do IPv6 em relação ao IPv4, como: cabeçalho, endereçamento, funcionalidades e as técnicas utilizadas para o coexistência dos protocolos IPv4 e IPv6 e testes laboratoriais que demonstram em qual cenário a técnica se aplica. Os cenários de aplicação das técnicas são cenários futuros nos quais a rede em sua maior parte é constituída por IPv6 mas ainda possuem algumas de suas partes possuindo IPv4.

5.1. Cabeçalho

Nesta sessão, de acordo com as especificações, apresentam-se as principais do IPv6 a começar pela análise das mudanças ocorridas na estrutura de seu cabeçalho, seguido da apresentação das diferenças entre os cabeçalhos de ambas as versões, destacando o que foi aprimorado no funcionamento do protocolo. Também, detalhará a utilização dos cabeçalhos de extensão e, o porquê de ela melhorar o desempenho dos roteadores.

5.1.1. Cabeçalho IPV4

Segundo Scrimger (2002), o cabeçalho IPv4 é composto por 13 campos fixos, que podem ou não conter opções responsáveis por fazer com que o tamanho varie de 20 a 60 Bytes. Estes campos são destinados a transmitir informações sobre:

Vers: Versão (*version*) é o primeiro campo do cabeçalho de um datagrama IPv4 e é um campo de 4 bits.

IHL: O segundo campo, de 4 bits, é o IHL (*Header Length)*, isto é, Comprimento do Cabeçalho da *Internet* com o número de *words* de 32 bits no cabeçalho IPv4.

Service Type: No RFC791 (1991), os 8 bits seguintes são alocados para um campo Tipo de Serviço (TOS). A intenção original era para um *host* especificar uma preferência do modo como os datagramas poderiam ser manuseados assim que circulassem pela rede.

Total Length: Tamanho Total (*total length*) é o campo de 16 bits seguinte do IPv4 e define todo o tamanho do datagrama. O datagrama de tamanho mínimo é de 20 bytes e o máximo é 65535 (64 Kbytes).

Identification: O campo seguinte de 16 bits é um campo de identificação. Este campo é usado principalmente para detectar fragmentos identificadores do datagrama IP original.

Flags: O campo de 3 bits que segue é usado para controlar ou identificar fragmentos.

Fragment Offset: O campo offset do fragmento tem 13 bits, e permite que um receptor determine o local de um fragmento em particular no datagrama IP original.

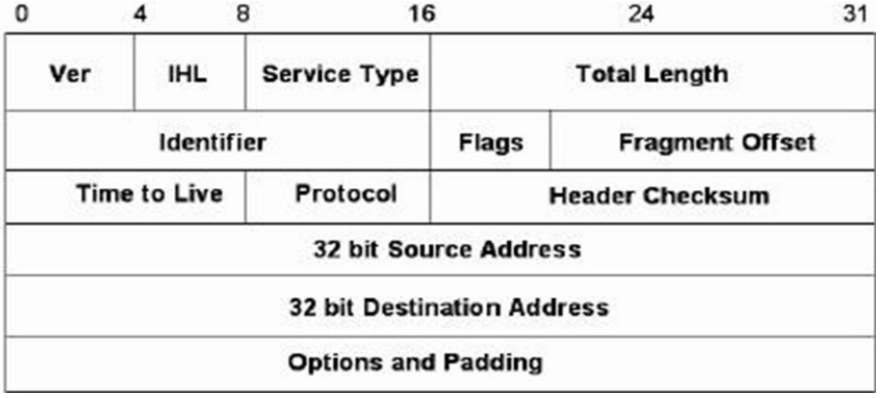
Time to Live: Um campo de 8 bits, o TTL (*time to live*, ou seja, tempo de vida) ajuda a impedir que os datagramas permaneçam numa rede (ex. andando aos círculos).

Protocol: O campo Protocolo é formado por 8 bits. Este campo define o protocolo seguinte usado numa porção de dados de um datagrama IP.

Header Checksum: O campo seguinte é um campo de verificação (*checksum*) do cabeçalho do datagrama IPv4. Um pacote em trânsito é alterado por cada router (hop) que atravesse. Um desses routers pode comprometer o pacote, e o checksum é uma simples forma de detectar a consistência do cabeçalho.

Adress Source / Destination: O Endereço de Origem / Destino encontra-se a seguir ao campo de verificação e cada um é de 32 bits. Na figura 2 a seguir é possível visualizar todos os campos.

Figura 2: Cabeçalho IPv4

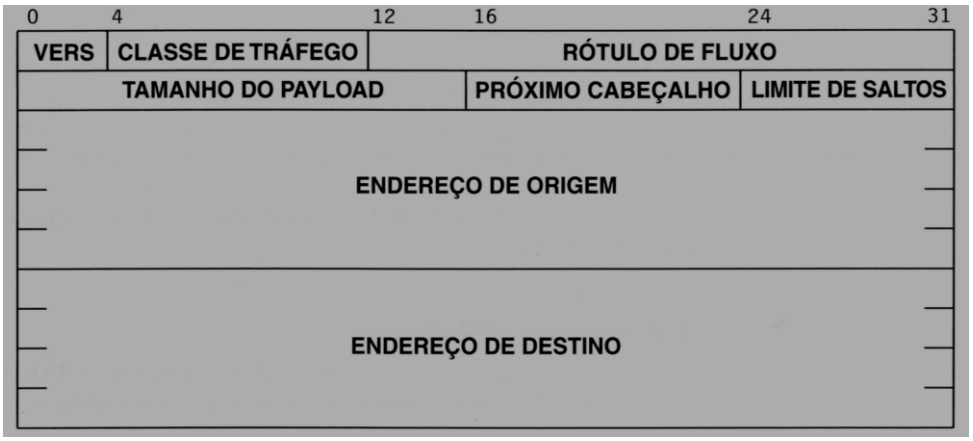


Fonte: SCRIMGER, 2002

5.1.2. *Cabeçalho IPv6*

O IPv6 altera o formato do datagrama em relação ao IPv4. Ele apresenta um cabeçalho base simplificado que utiliza somente campos essenciais, sendo que outros campos opcionais também podem ser adicionados ao datagrama através de cabeçalhos de extensão. Tais alterações permitiram que, mesmo com um espaço de endereçamento quatro vezes maior que o do IPv4, o tamanho total do cabeçalho IPv6 fosse apenas duas vezes. O cabeçalho na figura 3 a seguir. (COMER, 2006).

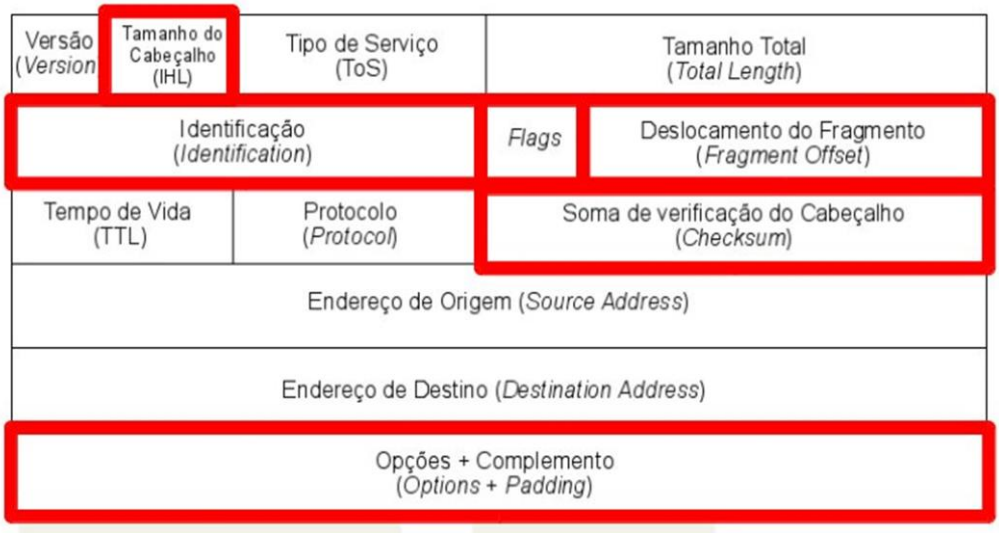
Figura 3: Formato do cabeçalho IPv6



Fonte: COMER, 2006

Dentre essas mudanças, pode-se destacar a retirada de seis dos campos que constituíam o cabeçalho IPv4, como decorrência da inutilização das funções quanto a implantação do uso de cabeçalhos de extensão. A figura 4 a seguir identifica esses campos.

Figura 4: Campos retirados do cabeçalho IPv4



Fonte: SANTOS et al, 2010

A primeira retirada foi a do campo “Tamanho do Cabeçalho” que por ter seu valor fixado tornou-se desnecessário. A seguir, os campos “Identificação”, “Flags”, “Deslocamento do Fragmento” e “Opções e Complementos” estes passam a ter indicação de suas informações em cabeçalhos de extensão. Por fim, o campo “Soma de Verificação” foi removido objetivando deixar o protocolo mais eficiente já que outras validações são realizadas pelos protocolos das camadas superiores da rede.(SANTOS *et al*, 2010).

Outra alteração realizada com o intuito de melhorar o processamento foi a troca de nome e e indicação de nova posição de quatro campos conforme a tabela 2 a seguir:

Tabela 2: Campos reposicionados

IPv4	IPv6
Tipo de serviço	Classe de serviço
Tamanho total	Tamanho dos dados
Tempo de vida(TTL)	Limite de encaminhamento
Protocolo	Próximo cabeçalho

Fonte: SANTOS et al, 2010

5.1.3. Campos do cabeçalho IPv6

Conforme pode ser visto na figura 3, o cabeçalho IPv6 é dividido nos seguintes campos de acordo com o RFC5095 (2007).

a. Versão: Este campo define a versão do IP.

b. Classe de Tráfego: Este campo define o nível de prioridade do pacote para uso em políticas de QoS (*Quality of service)* opcionalmente implementadas em redes.

c. Rótulo de fluxo: Identifica e diferencia pacotes do mesmo fluxo na camada de rede, sem a necessidade de verificar sua aplicação.

d. Tamanho do payload: Este campo define o tamanho total do datagrama IP, excluindo o cabeçalho base.

e. Próximo cabeçalho: Identifica o cabeçalho que vem após o cabeçalho básico do IPv6, estes cabeçalhos podem ser os cabeçalhos de extensão estudados na próxima seção.

f. Salto limite:Indica o numero máximo de saltos que o datagrama IPv6 deve dar antes de ser descartado.

g. Endereço de Origem: Identifica o host de origem do datagrama.

h. Endereço de Destino: Este campo usualmente identifica o destino final do datagrama. Entretanto, se o esquema de roteamento da origem for utilizado, este campo irá conter o endereço do próximo salto (roteador).

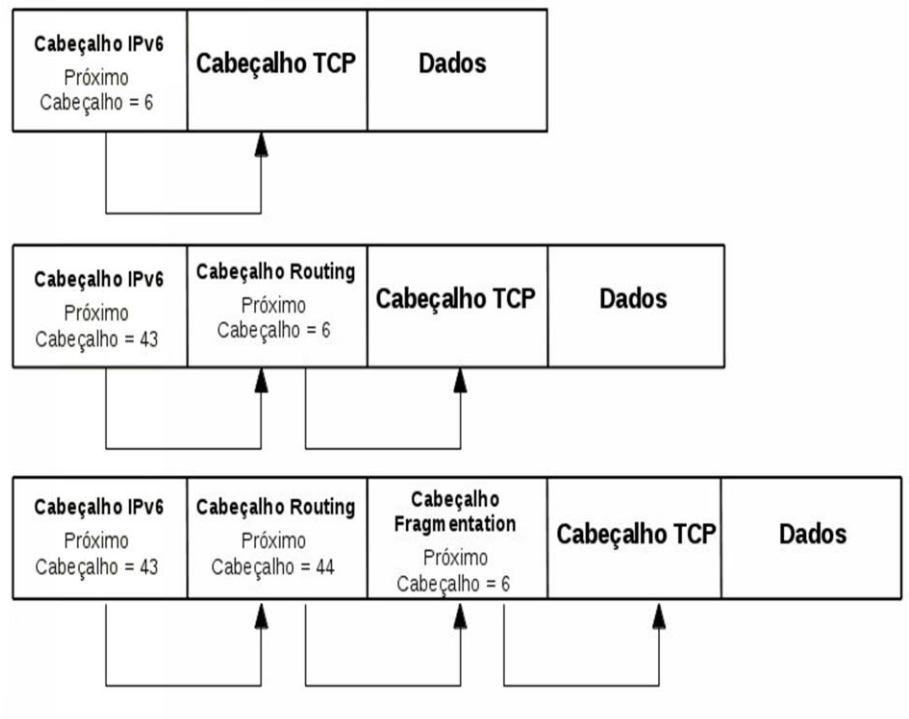
5.1.4. Cabeçalhos de extensão

Segundo Cruz (1999) os cabeçalhos de extensão do IPv6 funcionam de forma idêntica às opções do cabeçalho do IPv4 - um transmissor pode optar por indicar que cabeçalhos de extensão serão inclusos num determinado datagrama e quais não serão. Deste modo, os cabeçalhos de extensão proveem máxima flexibilidade possível.

De modo a tratar opções, o IPv6 apresenta um esquema de módulos: a informação adicional é transmitida através dos cabeçalhos de extensão. Este esquema fornece ao IPv6 flexibilidade para transportar informação relevante para encaminhamento e aplicações, bem como fornecer mecanismos de segurança, fragmentação, qualidade de serviço e gestão de rede, com escalabilidade ilimitada. Na medida em que estes módulos são opcionais, este esquema ajuda ainda a reduzir o custo de processamento de pacotes IPv6.

Os cabeçalhos de extensão são colocados entre o cabeçalho IPv6 e o cabeçalho do protocolo de transporte, estando ligados entre si pelo campo *Próximo Cabeçalho* (*Next Header*), formando uma cadeia. (CRUZ, 1999). A figura 5, a seguir, exemplifica essa situação.

Figura 5: Lista de cabeçalhos



Fonte: SANTOS et al, 2010

As especificações do IPv6 definem seis cabeçalhos de extensão segundo o RFC2460 (1998):

a. Opções de cabeçalho nó-a-nó (*Hop-by-Hop Options Header*): Usado para transportar informação opcional que tem de ser examinada por cada nó ao longo do caminho do pacote.
b. Opções de Destino *IPv6*(*Destination Options Header*): Usado para transportar informação opcional a ser analisada apenas no destino do pacote.
c. Cabeçalho de Roteamento (*Routing Header*): Usado por uma fonte IPv6 para listar um ou mais nós intermediários que devem ser visitados até o pacote chegar ao destino.
d. Fragmentação do cabeçalho (*Fragment Header*): Usado para enviar módulos de dados maiores do que a *MaximumTransmit Unit* (MTU) de um caminho.
e. *Autenticação* do cabeçalho (*Authentication Header*): Usado para fornecer confidencialidade, autenticação e integridade do conteúdo do datagramaIPv6.

f. Encapsulamento de dados de segurança (*Encapsulating Security Payload Header*): fornecer confidencialidade, autenticação e integridade do conteúdo do datagrama transmitido.

5.2. Endereçamento

O protocolo IPv6 apresenta como principal característica e como prioridade maior para o seu desenvolvimento, a ampliação no número de endereços válidos de IP (*Internet* Protocol). Com isso é necessário identificar as diferenças entre a representação dos endereços IPv4 e IPv6, saber diferenciar a sintaxe dos endereços IPv4 e IPv6 e conhecer os tipos de endereços IPv6 existentes e suas principais características.

No IPv4, o campo do cabeçalho reservado para o endereçamento possui 32 bits. Este tamanho possibilita em torno de 4 bilhões endereços distintos. Sendo que sua notação representada da seguinte forma, os endereço IP são compostos por 4 blocos de 8 bits, que são representados através de números de 0 a 255, como "192.16.0.12 ou "10.156.0.8". Esse número de endereços válidos era satisfatório para atender a necessidade quando o protocolo foi desenvolvido e suportar o surgimento de novas sub-redes. Porém, com o exponencial crescimento da *Internet*, surgiu o problema da escassez dos endereços IPv4, motivando o desenvolvimento de uma nova concepção do protocolo IP, o IPv6. (COMER, 2006).

O IPv6 possui um espaço para endereçamento de 128 bits, sendo possível obter 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços. Este valor representa aproximadamente 4 bilhões para cada endereço existente no protocolo IPv4 e representa, também, mais de 56 octilhões (5,6×1028) de endereços por ser humano na Terra, considerando-se a população estimada em 6 bilhões de habitantes. (RFC3513, 2003).

5.2.1. Representação de endereços

A notação mais utilizada é a:a:a:a:a:a:a:a, onde os "a" são números hexadecimais, ou seja, o endereço é dividido em oito partes de 16 bits, como no seguinte exemplo: **1080:0:0:0:8:800:200C:417A**

De todo espaço de endereçamento IPv6, apenas 15% está antecipadamente reservado para uso, ficando os 85% restantes reservados para o futuro. Na forma abreviada, as sequências de zeros podem ser substituídas pela string “::”. No entanto, esta substituição só pode ser feita uma única vez em cada endereço. A tabela 3 a seguir mostra alguns exemplos na forma completa e na forma abreviada. (CRUZ, 1999).

Tabela 3: Exemplos de abreviação de endereços

Endereço	Representação completa	Representação abreviada
Unicast	1080:0:0:0:8:800:200C:417A	1080::8:800:200C:417A
Multicast	FF01:0:0:0:0:0:0:43	FF01::43
Loopback	0:0:0:0:0:0:0:1	::1
Unspecified	0:0:0:0:0:0:0:0	::

Fonte: CRUZ, 1999

De acordo com Cruz (199) a terceira forma de representação, mais conveniente quando em ambientes mistos com nós IPv4 e IPv6, é da forma f:f:f:f:f:f:d:d:d:d, onde os "f" são números hexadecimais (16 bits) e os "d" são valores decimais de 8 bits referentes à representação padrão já bem conhecida do IPv4. Por exemplo:

0:0:0:0:0:0:192.168.10.25

0:0:0:0:0:FFFF:172.17.10.25

ou, na forma abreviada:

::192.168.10.25

::FFFF:172.17.10.25

Esta forma de notação será bastante útil durante a migração do IPv4 para o IPv6 e na coexistência entre ambos. Outra notação importante, a que se refere à representação textual dos prefixos e que é similar à notação CIDR (*ClasslessInter-DomainRouting)* do IPv4: endereço/prefixo, ou seja, o prefixo representa a sub-rede

à qual o endereço pertence. Para se exemplificar isso, é bom que se considere um prefixo de 60 bits sendo 12AB00000000CD3 em hexadecimal, as seguintes representações são válidas:

12AB:0:0:CD3:0:0:0:0/60

12AB::CD3:0:0:0:0/60

12AB:0:0:CD3::/60

5.2.2. Tipos de endereços

De acordo com a (RFC3513, 2003) existem no IPv6 três tipos de endereços definidos:

a) *Unicast* – este tipo de endereço identifica uma única interface, de modo que um pacote enviado a um endereço *unicast* é entregue a uma única interface;
b) *Anycast* – Identifica um conjunto de interfaces. Um pacote encaminhado a um endereço *anycast* é entregue à interface pertencente a este conjunto mais próxima da origem (de acordo com distância medida pelos protocolos de roteamento). Um endereço *anycast* é utilizado em comunicações de um-para-um-de-muitos.
c) *Multicast* – também identifica um conjunto de interfaces, entretanto, um pacote enviado a um endereço *multicast* é entregue a todas as interfaces associadas a esse endereço. Um endereço *multicast* é utilizado em comunicações de um-para-muitos. Diferente do IPv4, no IPv6 não existe endereço broadcast, responsável por direcionar um pacote para todos os nós de um mesmo domínio. No IPv6, essa função foi atribuída a tipos específicos de endereços *multicast.*

No protocolo IPv6 os prefixos de rede mantêm a mesma representação que possuíam no IPv4. A representação se dá da seguinte forma endereço-IPv6/tamanho do prefixo, com isso o tamanho do prefixo é o valor na forma decimal que representa a quantidade de bits localizados à esquerda do endereço que compõem o prefixo. A seguir o prefixo de sub-rede que é apresentado mostra que dos 128 bits de endereço, 64 bits são para identificar a sub-rede0. (RFC3513, 2003).

Ex: Prefixo 2001:FACA:1234:1::/64
Prefixo Global: 2001:FACA::/32
ID da sub-rede: 1234:1

De acordo com Cruz (1999), os endereços IPv6 na sua grande maioria são endereços *unicast* globais (podem equivaler aos endereços públicos IPv4), que na maioria das situações seu uso é valido. Entretanto foram reservados para uso específicos determinados intervalos de endereços. A tabela 4 a seguir apresenta alguns desses intervalos de endereços atualmente em uso:

Tabela 4: Intervalos de endereços

0:0:0:0:0:0:0:0 ou ::	Endereços não especificados
0:0:0:0:0:0:0:1 ou ::1	Endereços de loopback
2001(...)::/32	Endereços globais
::FFFF:192.168.0.2	Endereço IPv4 mapeado em IPv6
FE80::/64	Endereço Link-local
FEC0::/10	Endereços de site-local
FF00::/8	Endereço Multicast

Fonte: CRUZ, 1999

De acordo com Cruz (1999)**,** os endereços ilustrados na tabela 3 podem ser descritos como:

a) Endereço Não-Especificado (*Unspecified*): é representado pelo endereço 0:0:0:0:0:0:0:0 ou ::0 (equivalente ao endereço IPv4 *unspecified* 0.0.0.0). Ele nunca deve ser atribuído a nenhum nó, indicando apenas a ausência de um endereço. Ele pode ser utilizado no campo Endereço de origem de um pacote IPv6 enviado por um *host* durante o processo de inicialização, antes que este tenha seu endereço exclusivo determinado. O endereço *unspecified* não deve ser utilizado como endereço de destino de pacotes IPv6;
b) Endereço de *loopback* (::1): representado pelo endereço *unicast* 0:0:0:0:0:0:0:1 ou ::1 (equivalente ao endereço IPv4 *loopback* 127.0.0.1). Este

endereço é utilizado para referenciar a própria máquina, sendo muito utilizado para testes internos. Este tipo de endereço não deve ser atribuído a nenhuma interface física, nem usado como endereço de origem em pacotes IPv6 enviados para outros nós. Além disso, um pacote IPv6 com um endereço *loopback* como destino não pode ser enviado por um roteador IPv6, e caso um pacote recebido em uma interface possua um endereço *loopback* como destino, este deve ser descartado;

c) Endereços Globais(2001(...)/16): podem ser vistos como os endereços públicos IPv4, o endereço global *unicast* é globalmente roteável e acessível na *Internet* IPv6.

d) Endereço IPv4 mapeado em IPv6 (::FFFF:wxyz): representado por 0:0:0:0:0:FFFF:wxyz ou ::FFFF:wxyz, é usado para mapear um endereço IPv4 em um endereço IPv6 de 128-bit, onde wxyz representa os 32 bits do endereço IPv4, utilizando dígitos decimais. É aplicado em técnicas de transição para que nós IPv6 e IPv4 se comuniquem. Ex. ::FFFF:192.168.0.2.

e) Endereços de link-local (FE80::/64): podendo ser usado apenas no enlace específico onde a interface está conecta da, o endereço link local é atribuído automaticamente utilizando o prefixo FE80::/64. Os 64 bits reservados para a identificação da interface são configurados utilizando o formato IEEE EUI-64. Vale ressaltar que os roteadores não devem encaminhar para outros enlaces, pacotes que possuam como origem ou destino um endereço *link-local Unique Local Address* (ULA) – endereço com grande probabilidade de ser globalmente único, utilizado apenas para comunicações locais, geralmente dentro de um mesmo enlace ou conjunto de enlaces.

f) Endereços de site-local (FEC0::/10): desenvolvidos para serem utilizados dentro de uma rede específica sem a necessidade de um prefixo global, equivalente aos endereços privados do IPv4. Sua utilização foi substituída pelos endereços ULA;

g) Endereços *multicast* (FF00::/8): Um endereço *multicast* identifica várias interfaces. Com a topologia de encaminhamento *multicast* apropriada, os pacotes dirigidos a um endereço *multicast* são enviados para todas as interfaces identificadas pelo endereço.

5.3. Funcionalidades IPv6

Esta sessão aborda as funcionalidades essenciais do IPv6. Funcionalidades que fazem com que o protocolo IPv6 se diferencie do IPv4.

5.3.1. ICMPv6

Para colocar as funcionalidades em prática necessita-se de um protocolo auxiliar e fundamental para execução de outras ferramentas, esse protocolo auxiliar é o ICMPv6 - *Internet Control Message Protocol version 6 (Protocolo de controle de mensagens da Internet versão 6).* As mensagens enviadas são usadas para troca de informações para que o instrumento desejado seja aplicado, tem como objetivo: a) informar topologia de rede; b) fazer diagnóstico da rede; c) caso seja encontrado falhas no processamento, seja relatada. SANTOS *et al* (2010).

De acordo com Santos *et al* (2010) o protocolo de mensagens é essencial na arquitetura e estrutura de comunicação, isso leva ao funcionamento da versão 6, esse protocolo gerencia as funções de: Grupos de endereços *Multicast*, substitui o antigo protocolo de resolução de endereço *Address Resolution Protocol* (ARP) na resolução de endereços da camada inferior, mensagens para descoberta de vizinhos e diferenciando os tipos de endereçamento sendo *Stateless* ou *Statefull.* Nos grupos *multicast* o gerenciamento utiliza um dispositivo de descoberta para identificar para quais grupos as mensagens *multicasts* devem ser enviados, é identificado como *Multicast Listener Discovery* (descoberta de ouvintes multicast - MLD). A descoberta de vizinha é fundamental para o funcionamento**,** pois é a que executa a função da camada 2 do modelo OSI, tem a responsabilidade de descobrir quais *hosts* estão diretamente interligados a rede. A tabela 5 a seguir apresenta as mensagens informativas do ICMPv6.

Tabela 5: Mensagens informativas ICMPv6

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

Fonte: SANTOS *et al*, 2010

5.3.2. Descoberta de vizinhança

Segundo RFC4861 (2007) a descoberta de vizinhança é responsável pela comunicação entre os nós da rede IPv6, semelhante ao IPv4 que utilizava o protocolo ARP, mas necessitava de métodos adicionais na sua estrutura. Possui diversas características dentre essas estão: a) determinar o endereço de enlace, camada 2 do modelo OSI, conhecida como MAC-*Address,* sendo constituído pelo formato hexadecimal, identificando o código do fabricante e o equipamento; b) localizar roteadores dentro do mesmo enlace, roteadores vizinhos; c) determina parâmetros relacionados à autoconfiguração de endereços e seus prefixos; d)

detectar e existência de endereços de IP duplicados em um nó dentro do enlace; e) detecção de vizinhos inacessíveis.

De acordo com a RFC4862 (2007), a autoconfiguração de endereços *Stateless* permite que endereços IPv6 possam ser atribuídos às interfaces sem a exigência de configuração manual, sem utilizar servidores DHCP (*Dynamic Host Configuration Control*), usando apenas as mínimas configurações existentes nos roteadores. Para gerar esse endereço o host utiliza combinações entre dados locais, como endereço físico do host (MAC) ou um valor aleatório para criar o ID, e informações oriundas de roteadores que possuem diversos prefixos. Caso não existam roteadores identificados, o host utiliza apenas o endereço *link local* com o prefixo **FE80::.**

5.3.3.DHCPv6

Dynamic Host Configuration Protocol (DHCP) é um protocolo de autoconfiguração *Statefull,* através de um servidor DHCP que distribui os endereços IP utilizados de forma dinâmica na rede, onde se pode obter assim um maior controle na atribuição de endereços pelos hosts. O DHCPv6 tem como função o fornecimento de informações de rede quando não se tem a presença de roteadores, ou quando seu uso é indicado nas mensagens RA (*Router Advertisement)*, fornecendo endereço IPv6 e outros parâmetros de rede, como endereços de servidor DNS, NTP(*Network Time Protocol*), etc. O protocolo UDP é responsável pela troca de mensagens entre cliente e servidor quando utilizado o DHCPv6. Os hosts utilizam troca de mensagens *multicast* e endereços *link-local* para realizar a troca de mensagens DHCP. (RFC 3315, 2003).

De acordo Santos *et al* (2010) o DHCP é “um protocolo de autoconfiguração *Statefull* 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 *hosts*.”

5.3.4. DNS(Domain Name System)

De acordo com o RFC3596 (2003), o protocolo DNS tem importante função para quem utiliza a *Internet*, pois é o DNS o responsável por traduzir os endereços de IP para nome de domínios como de sites e equipamentos de rede e vice-versa. Sua arquitetura é hierárquica, com seus dados organizados em uma árvore invertida, distribuída de forma eficiente em um sistema descentralizado e com cache (armazena domínios pouco tempo antes acessado pelo cliente).

Algumas mudanças foram estabelecidas para que o IPv6 pudesse trabalhar juntamente com o IPv4. Como o tamanho do endereço da versão 6 é de 128 bits um registro foi criado para armazenar os endereços IPv6, esse registro chamado de AAAA ou Quad-A. Sua função se é equivalente ao registro A do endereço IPv4, fazer a tradução do endereços IPv6. O protocolo DNS começa a traduzir o endereço sempre no inverso do endereço IP ou nome do domínio, caso ele acesse o endereço www.google.com o DNS começa a tradução pelo ".com" em seguida ".google", chama-se tradução do reverso, para o IPv6 foi introduzido ao DNS o registro PTR *ip6.arpa*, responsável pela tradução, no IPv4 o registro que tinha a responsabilidade de traduzir é o *in-addr.arpa.*(RFC3596, 2003)

Para cada endereço IPv6 que o host possua ele possuirá um registro Quad-A. A forma de representação dos registros e a resolução do inverso é representados na tabela 6 a seguir:

Tabela 6: Representação e resolução dos registros

Website	Endereço IPv4	Endereço IPv6
www.google.com	71.125.234.200	2800:3f0:4001:806::1005
Website	Inverso IPv4	Inverso IPv6
www.google.com	200.234.125.71.in-addr.arpa PTR www.google.com	1.0.0.5.0.0.0.0.0.0.0.0.0.0.0.0.8.0.6.0.4.0.0.1.3.f0.0.2.8.0.ip6.arpa PTR www.google.com

Fonte: Elaborado pelos autores

5.4. Técnicas de Transição

Como toda estrutura da rede mundial de computadores ainda se baseia no IPv4, existe a necessidade da coexistência dos dois protocolos para que a mudança seja feita de forma gradual, devido ao tamanho que a rede possui. O período de transição e coexistência foi iniciado no ano de 1998 e era previsto que a implantação fosse concluída juntamente com o esgotamento de endereços do protocolo IPv4. Os endereços foram esgotados e o IPv6 não foi implantado por completo, diante disso as técnicas transição foram desenvolvidas para que a rede IPv4 pudesse comunicar com rede IPv6 e vice-versa e manter a compatibilidade de toda a base das redes instaladas sobre o IPv4 como o protocolo IPv6. Cada uma dessas técnicas desenvolvidas apresentam características especificas, tendo a possibilidade de ser empregada de forma individual ou associada a outras técnicas, desse modo suprindo a necessidade de cada uma das situações encontradas. (MOREIRAS *et al.* , 2012).

Na atual fase de implantação do IPv6, órgãos governamentais, instituições de ensino, entidades ligadas a *Internet* e empresas buscando inovação começaram a implantar maciçamente o IPv6, formando assim ilhas IPv6 flutuantes em uma *Internet* majoritariamente IPv4 este cenário implicará na convivência entre os protocolos IPv6 e IPv4, pois os novos *hosts* IPv6 terão a necessidade de acessar servidores que ainda usam o IPv4. Para que *hosts* IPv6 possam acessar servidores IPv4 é necessário o uso de técnicas que possibilitem a convivência entre os dois protocolos. (MOREIRAS *et al.* , 2012).

Segundo Moreiras *et al*. (2012) a primeira grande questão que surgiu era como conectar redes IPv6 por meio de equipamentos que só suportavam IPv4. Diante disso houve a necessidade de se criar diversos tipos de túneis IPv6 sobre IPv4, usando diversos modos de comunicação, estabelecidos de forma manual ou automática. Também foram desenvolvidas técnicas de tradução que pudessem interoperar redes IPv6 e IPv4,o método utilizado consistia em tradução de pacotes. Essa técnica objetiva traduzir um cabeçalho IPv6 em IPv4 e vice-versa. Outro problema que surgiu foi a necessidade de implantar o IPv6 em um cenário em que o IPv4 não esteja disponível, mas ainda assim seja necessário para a utilização dos usuários à rede. Para que o problema pudesse ser resolvido por completo, uniu-se o uso das técnicas de tunelamento IPv4 sobre IPv6 às técnicas de tradução.

As técnicas de transição e suas funcionalidades são:

Pilha dupla: Equipamentos possuem nativamente IPv4 e IPv6 convivendo juntos e simultaneamente. A pilha dupla deve ser usada sempre que possível, por ser definida pelos órgãos que regulamentam a *Internet* como a técnica padrão para a transição para o IPv6.(MOREIRAS *et al.* , 2012).

Túneis: Permite que redes IPv6 tenham comunicação entre si utilizando uma rede IPv4, ou vice-versa.(MOREIRAS *et al.* , 2012)

Tradução: Permite que redes IPv6 possa realizar comunicação com redes IPv4, através de conversão de pacotes. (MOREIRAS *et al.* , 2012).

De acordo com o RFC4862 (2007), ambas as técnicas de tradução e tunelamento podem ser do tipo *Statefull* ou *Stateless*. As técnicas do tipo *Stateless* não exigem o armazenamento das informações, pois cada pacote é tratado de forma individual. As técnicas do tipo *Statefull* necessitam armazenar tabelas com informações acerca dos endereços ou pacotes a serem processados. De modo geral, sempre se deve dar preferência às técnicas com a funcionalidade *Stateless*, devido ao uso das técnicas *Statefull* exigirem um tempo maior de processamento e um grande consumo de memória.

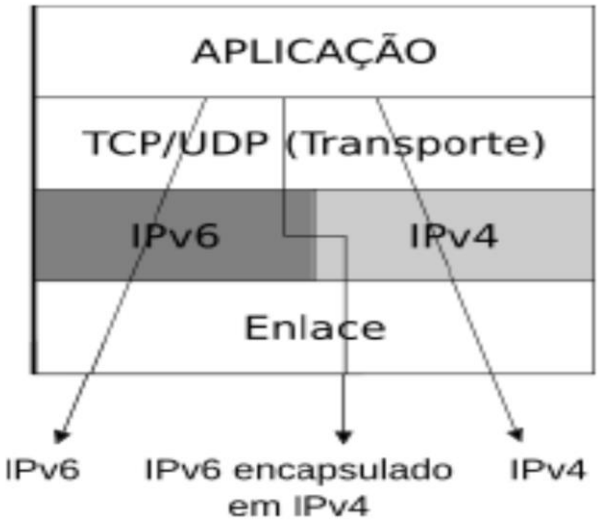
5.4.1. Pilha Dupla

A técnica Pilha Dupla ou *Dual Stack* deve ser utilizada quando for possível, pois na etapa de transição que a rede se encontra não é indicado ter nós com suporte exclusivo do IPv6, pois a maior parte da rede ainda utiliza o IPv4. Diante disso é preciso manter o IPv4 funcionando de forma estável e implantar o IPv6 nativo para que coexistam utilizando o mesmo hardware. Os datagramas de ambos protocolos são tratados no nó de uma rede que utiliza a técnica de pilha dupla, ao entrar em comunicação com uma rede IPv6 esse nó assume um comportamento de no IPv6, e se comporta como um nó IPv4 ao entrar em comunicar-se com uma rede IPv4. Isso é possível devido a pilha dupla possuir ambos endereços atribuídos a sua interface.(RFC6333, 2011).

Para Filippetti (2008) “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.”

Esta técnica de transição permite que a implantação seja de forma gradual, com a configuração de pequenas redes, não havendo a necessidade de configurar toda grande rede. Além disso, caso no futuro o IPv4 não seja mais usado, basta simplesmente desabilitar a pilha IPv4 em cada nó. Na figura 6 a seguir é possível visualizar como é o funcionamento da Pilha Dupla.

Figura 6: Funcionamento da pilha dupla



Fonte: SANTOS et al, 2010

Mas como desvantagem tem-se que nem todos os sistemas operacionais possuem suporte para IPv6, isso também acontece com alguns hardwares existentes nas rede que são utilizadas. Para configuração de uma rede que utilizará a técnica da pilha dupla, deve-se considerar aspectos relacionados ao DNS e ao *Firewall*.

Segundo Moreiras *et al*. (2012), “Em relação ao DNS, é preciso que este esteja habilitado para resolver nomes e endereços de ambos os protocolos. No caso do IPv6, é preciso responder a consultas de registros do tipo AAAA (Quad-A), que armazenam endereços no formato do IPv6, e para o domínio criado para a resolução de reverso, o ip6.arpa.” A resposta não sofre interferência do protocolo no qual foi feita a consulta DNS, ao receber a resposta da consulta obtendo endereços IPv6 ou IPv4, a aplicação decide qual protocolo utilizar. O padrão é a utilização do IPv6, mas caso falhe, deve-se tentar utilizar o protocolo IPv4, mas isso gera alguns problemas de lentidão na conexão. Diante disso, foi desenvolvido um comportamento chamado *happy eyeballs*, usado nos principais navegadores utilizados atualmente. Essa

técnica consiste em fazer tentativas simultâneas de conexão, e opta pela que der a resposta mais rápida. Isso resolve alguns problemas da utilização do IPv6, pois alguns usuários ao fazerem a tentativa de se conectarem com um site que já possui IPv6 gera uma longa espera. Esse tempo de espera é conhecido como *time out* que pode ser muito longo, fazendo com que o usuário desista da consulta. Essa técnica resolve o problema do *time out*, pois se a resposta do protocolo IPv4 for mais rápida será dada a preferência a ele, ao invés de serem feitas duas tentativas para conseguir uma conexão. Nos protocolos de roteamento é independente a configuração de roteamento IPv6 em relação à configuração do roteamento do protocolo IPv4. Porém, no caso da rede, antes de ser configurada a Pilha Dupla, utilizava-se unicamente o protocolo de roteamento OSFv2 (*Open Shortest Path First*), que possui suporte apenas para IPv4, tem-se a necessidade de atualizar o protocolo de roteamento para uma versão que suporte ambos protocolos, tendo como exemplo IS-IS ou executar o OSPFv3 juntamente com OSPFv2.

No caso dos firewalls a configuração de filtragem de pacotes pode depender da plataforma que se encontra em uso, no caso da plataforma Linux. Esses filtros são independentes uns dos outros, de modo que o filtro iptables filtra apenas pacotes IPv4, e, no caso do IPv6, o filtro ip6tables filtra apenas os pacotes da rede IPv6. No caso da utilização dos dois protocolos, deve-se, sempre, manter os dois filtros configurados, pois, caso o filtro do IPv6 não esteja, a porta para entrada de terceiros se manterá aberta. (MOREIRAS, 2012).

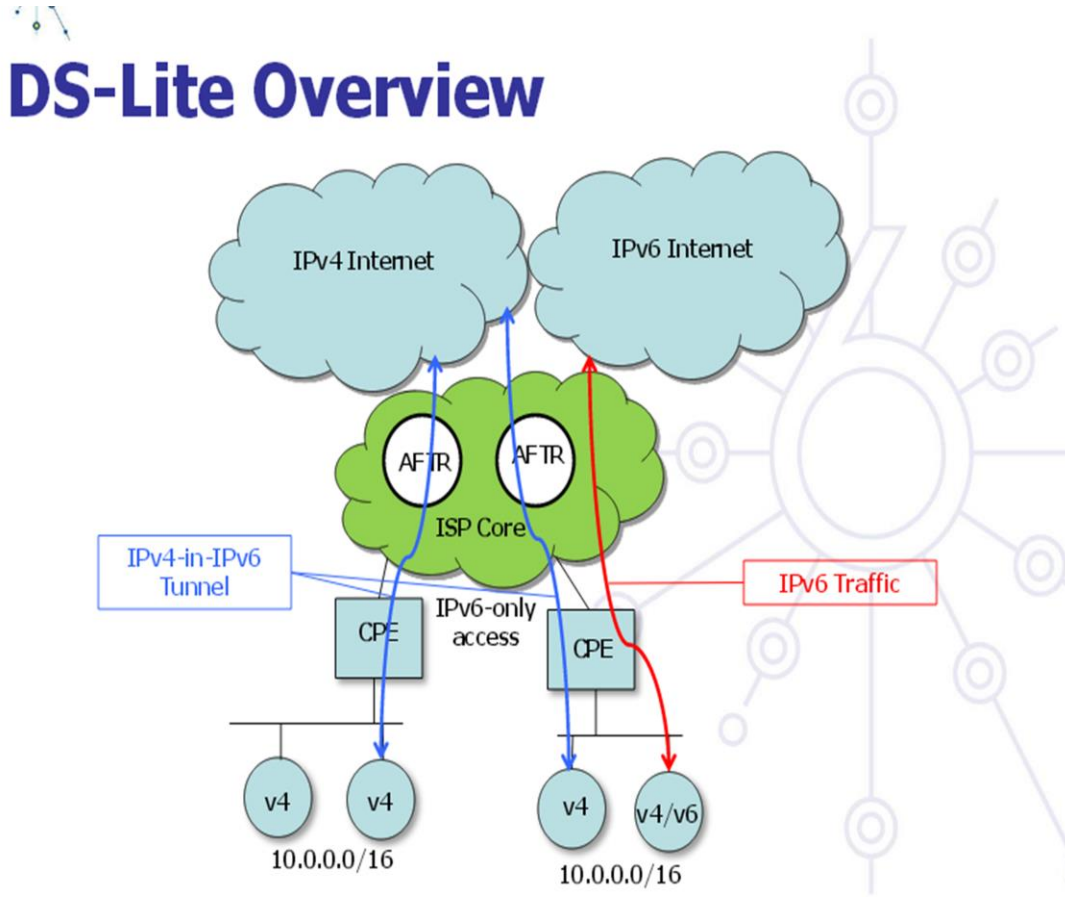
Na plataforma *Windows* o protocolo IPv6 é habilitado nativamente, dessa forma, o firewall também possui a configuração nativa da mesma forma como é feito no IPv4. Ao ser habilitado o IPv6, o sistema operacional atribui endereço IPv6 *link local*, endereços não roteáveis para placa de rede. São utilizados apenas em um mesmo segmento da rede, dessa forma, não são registrados pelo DNS, não causando nenhum problema de segurança. (RODRIGUES, 2013).

5.4.2. DSLite

DSLITE (Dual-Stack Lite) é uma técnica de transição que permite um provedor de serviços de banda larga compartilhar endereços IPv4 entre os clientes através da combinação de duas tecnologias bem conhecidas: IP em IP (IPv4-em-IPv6) e *Network Address Translation* (NAT). (RFC6333, 2011)

De acordo Moreiras (2012) a técnica de transição DS-LITE é destinada para um cenário onde não existem mais IPv4 disponíveis, todo o tráfego de informações é realizado em redes IPv6 mas muitos provedores e serviços ainda utilizam o IPv4, e precisam de alguma forma serem acessados. Na figura 7 a seguir é possível visualizar como é tráfego quando se utiliza a técnica.

Figura 7: Cenário DSLite



Fonte: 6DEPLOY, 2013

O acesso a estes provedores ou serviços é feito através de um túnel IPv4 sobre a rede IPv6. Se o usuário for realizar uma conexão à *Internet* onde existe a possibilidade de conexão IPv6, esta conexão será realizada normalmente através da rede IPv6. Já se o usuário for realizar uma conexão à *Internet* onde só seja possível a comunicação via IPv4, de acordo com o RFC6333 (2011), a conexão será realizada entre o CPE (*Customer Premise Equipment*) do lado do usuário, e o AFTR

(*Address Family Transition Router*) do lado do provedor. O CPE do usuário é chamado de B4 (*DSLite Basic Bridging BroadBand*). Esse dispositivo é muitas vezes uma porta de entrada da rede do usuário. Em alguns casos, os computadores são ligados diretamente ao prestador de serviço de rede, o que faz com que estes computadores sejam vistos como CPEs. O DS-Lite utiliza a técnica de tunelamento para encapsular um cabeçalho IPv4 em um cabeçalho IPv6. Nas extremidades desses tuneis é usado o endereço de faixa 192.0.0.0/29.

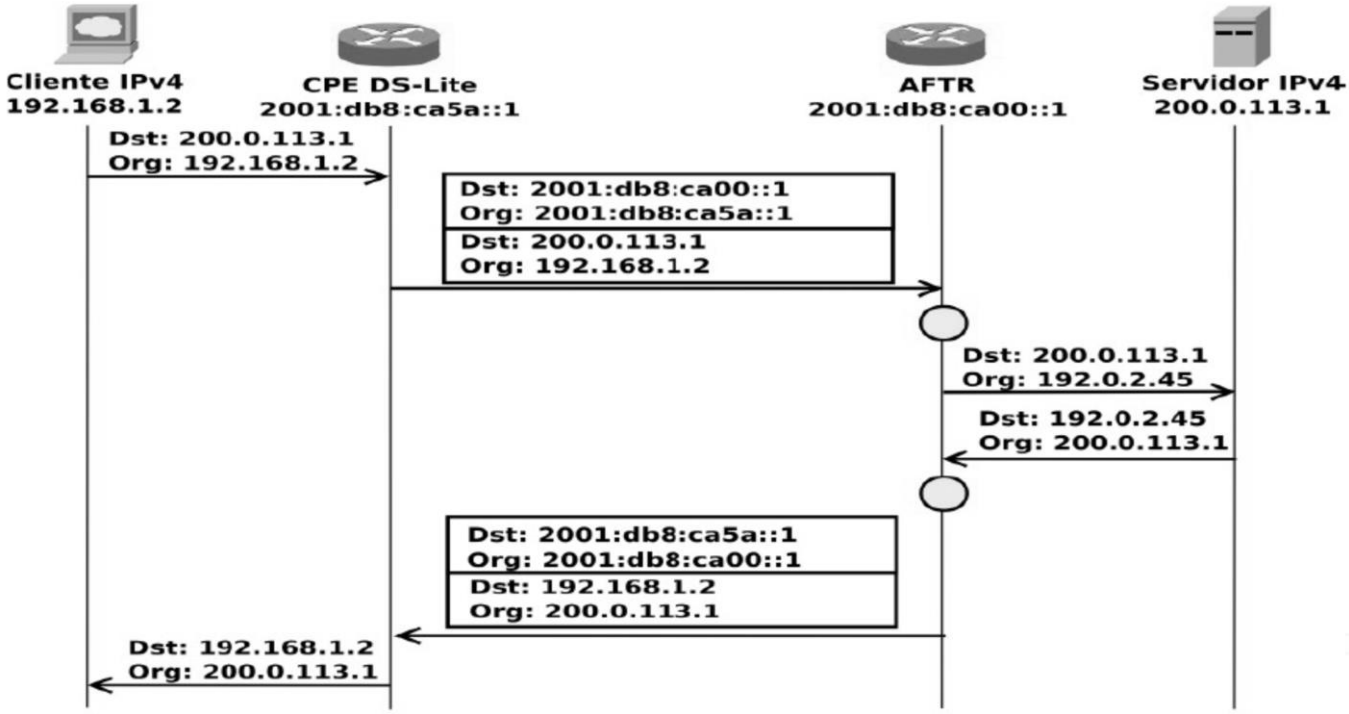
O elemento B4 é uma função implementada em um nó dual-stack-capable, ou um dispositivo ligado diretamente a um CPE, que cria um do túnel a uma AFTR. (RFC 6333, 2011).

Já o AFTR é um software desenvolvido pela ISC(*Internet* System Consortium) a pedido da *Comcast* que é utilizado pelos provedores e tem a função de fechar o túnel IPv4 IPv6 que se inicia do lado do cliente, além de realizar a função de NAT na versão 4 sobre a rede IPv6 do provedor. Isso permite que antigos locais com IPv4 finais, como PCs domésticos possam interagir com provedores e serviços de conteúdo que ainda utilizam IPv4. Esta comunicação é realizada através de uma infra-estrutura de rede IPv6. (6DEPLOY, 2013).

De acordo com Moreiras (2012) na CPE do usuário deve ter um DHCPv4 para que seja feita a distribuição de endereços dentro da rede com IPv4, juntamente com um proxy DNS, que possibilite consultas usando IPv4.

O funcionamento da técnica se dá da seguinte forma: um cliente faz uma requisição de um serviço IPv4, mas a rede é majoritariamente IPv6, dessa forma o CPE recebe a solicitação encapsula o cabeçalho IPv4 em um cabeçalho IPv6, e cria um túnel através da rede IPv6 para transmissão dos pacotes. Quando a informação chega até o AFTR, o túnel é fechado e o cabeçalho é desencapsulado e entregue à rede IPv4. A resposta do servidor é feita com cabeçalho IPv4, no momento que atingem o AFTR esse cabeçalho é encapsulado em um pacote IPv6, e é enviado ao CPE pelo o túnel aberto. Chegando ao CPE o túnel é fechado e o cabeçalho é desencapsulado e entregue ao cliente IPv4. Sempre que for necessário o acesso à um serviço IPv4, este processo se repetirá, caso o acesso for via IPv6, ocorrerá normalmente, devido o fato de a rede ser em sua maior totalidade IPv6. A figura 8 a seguir mostra a sequência do funcionamento da técnica.

Figura 8: Funcionamento DSLite



Fonte: MOREIRAS, 2012

5.4.3. NAT64/DNS64

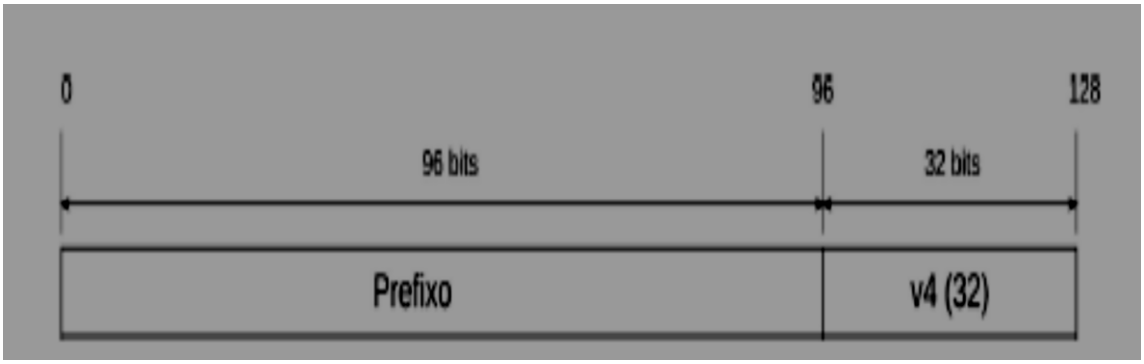
A transição do protocolo IPv4 para o IPv6 é iminente. Gradativamente, empresas já realizam testes de compatibilidade entre os protocolos, visando diminuir ou extinguir os impactos negativos para quando a transição for efetivamente realizada. Com isso as técnicas de transição, responsáveis pela comunicação entre IPv4/IPv6 vão ganhando forma.

Dentre as técnicas existentes, a NAT64/DNS64 é uma técnica que consiste na tradução de endereços e pode ser exemplificada como um dispositivo na rede que contém as duas interfaces, IPv6 e IPv4. Assim a configuração da rede é dada para enviar e receber tanto pacotes IPv6 e IPv4, delegando então a tradução desses pacotes ao dispositivo de rede, que irá fornecer assim compatibilidade para comunicação entre os dois protocolos. NAT64/DNS64 são técnicas *Statefull*. Nas técnicas *Statefull*, é necessário manter algumas tabelas contendo informações sobre o estado da rede. Essas informações são referentes aos endereços e também aos

pacotes. Dessa maneira, o custo de processamento das técnicas *Statefull* são maiores do que das *Stateless*, já que na primeira, será gasto CPU e também memória para armazenar e processar essas tabelas. (RFC6147, 2011).

De acordo com a RFC 6052 (2013), NAT64 é responsável pela tradução de datagramas IPv4 para IPv6, para que a tradução seja possível tem-se a necessidade de traduzir também os endereços, isso pode ser visto na figura 9 a seguir.

Figura 9: Tradução de um endereço IPv4 em IPv6



Fonte : MOREIRAS, 2012

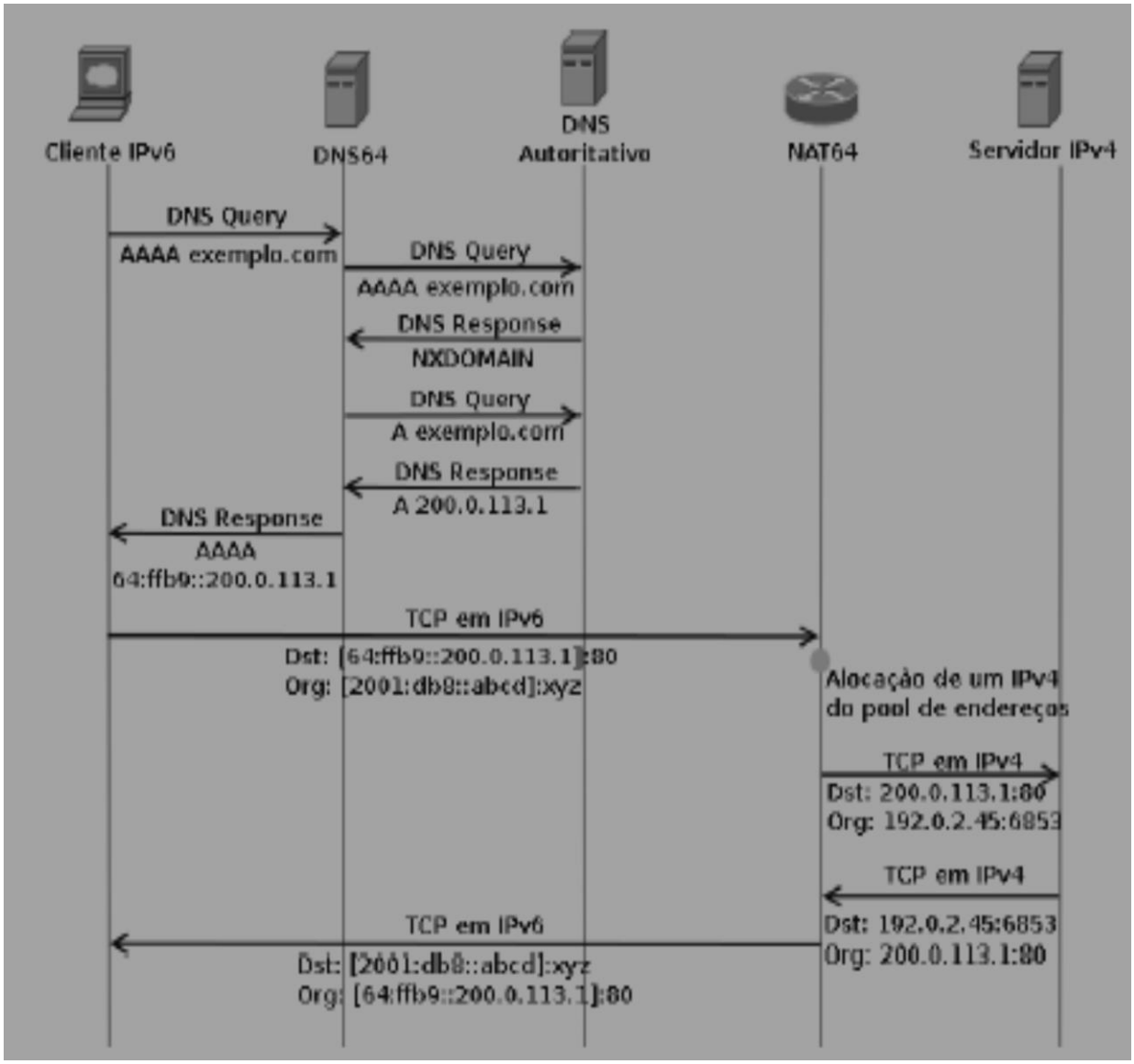
O prefixo utilizado pode ser escolhido pelo provedor, mas recomenda-se a utilização do prefixo 64::ff9b::/96, prefixo especifico reservado para ser utilizado em algoritmos de mapeamento de endereços IPv4 em IPv6. Por exemplo endereço IPv4 192.0.3.100 seria convertido para o endereço IPv6 64::ff9b::/c000:0364.

Segundo tradução livre da RFC6147 (2011) “DNS64 é um mecanismo para a síntese de Registros AAAA para registros A. Um registro sintético AAAA criado pelo DNS64 a partir de um registro A original, contém o nome do proprietário do registro A original, mas ele contém um endereço IPv6 em vez de um endereço IPv4. O endereço IPv6 é uma representação do endereço IPv4 contido no registro A original. A representação IPv6 do endereço IPv4 é algoritmicamente gerada a partir do endereço IPv4 retornado no registro A e um conjunto de parâmetros configurados no DNS64 (tipicamente, um prefixo IPv6 usado por representações IPv6 de endereços IPv4 e, opcionalmente, outros parâmetros).”

Conforme a RCF6147 (2013) DNS64 responsável por converter as solicitações de DNS IPv4 em solicitações de DNS IPv6 e vice-versa, tendo como resposta para *host* IPv6 resposta do tipo AAAA (Quad-A) e para *hosts* IPv4 resposta

do tipo A. O funcionamento é simples, um *host* IPv6 ao fazer um consulta DNS a registros Quad-A usando um IPv4 mapeado tendo prefixo IPv6, o DNS64 fará uma consulta ao servidor DNS autoritativo da rede com registro A, e a reposta da solicitação Quad-A com a conversão da resposta A do servidor autoritativo. No caso do uso unicamente de endereço IPv6 o próprio DNS autoritativo que fará as consultas, sem a necessidade do DNS64, para realizar as consultas os servidores DNS consultados pelo servidor DNS autoritativo necessariamente tem que possuir a capacidade de resolver consultas do tipo Quad-A. a figura 10 a seguir mostra a sequência do funcionamento do NAT64 juntamente com o DNS64.

Figura 10: Funcionamento do NAT64/DNS64



Fonte: SANTOS et al, 2012

De acordo com o RCF2694 (1999) Com essa técnica é possível realizar a tradução IPv6 para IPv4 e vice e versa. Mas na tradução de IPv4 para IPv6 são necessários ALGs (*Aplication level Gateways*), pois o NAT64 é unidirecional. Os AGLs têm a responsabilidade de fazer uma ponte entre os protocolos, a fim de permitir a conexão entre aplicações específicas, um exemplo dessas aplicações é o próprio DNS64, pois utiliza registros Quad-A para uma conversão em registros A. Essa técnica é bem volátil, permitindo implementações para Linux, *Windows* e até para roteadores domésticos baseados em Linux.

.

5.5. Laboratórios

Os laboratórios apresentados à seguir têm como objetivo apresentar a configuração necessária para utilização da pilha dupla por usuários finais, simular um ambiente onde será implantada a técnica DS-lite e simular um ambiente onde será feita a configuração da técnica NAT64/DNS64.

5.5.1. *Laboratório Pilha Dupla*

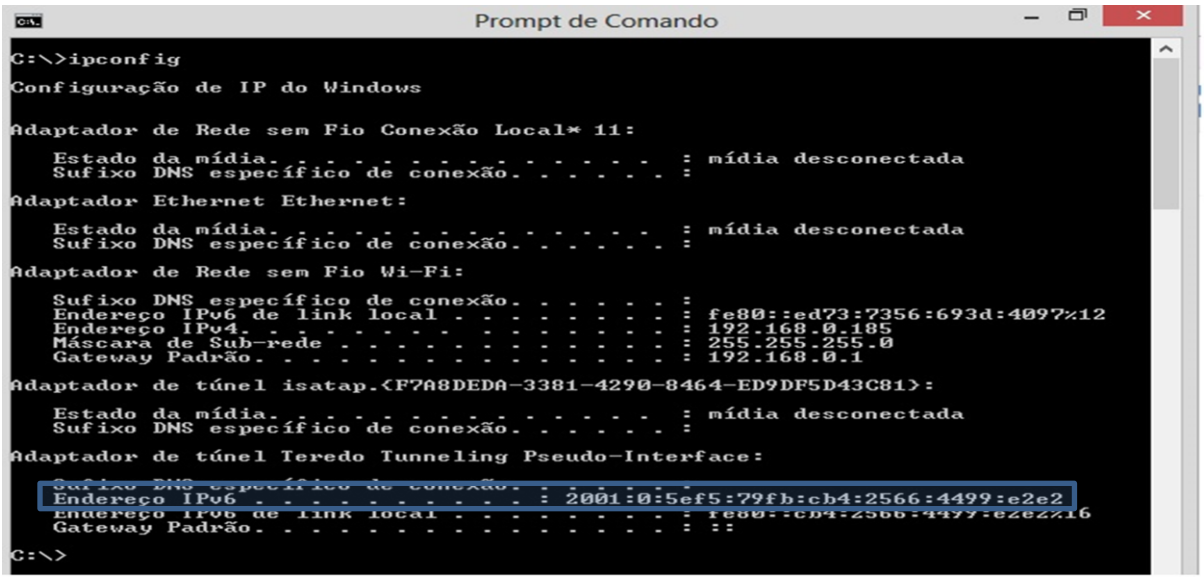
O cenário deste laboratório consiste em testar a conexão de uma máquina que possui a Pilha Dupla, ou seja, protocolo IPv4 e IPv6 habilitados nativamente. O sistema operacional a ser usado é o Windows 8, e o navegador utilizado para os testes realizado é o *Internet* Explorer 10.

O objetivo é apresentar a compatibilidade de conexão do *host* através dos dois protocolos utilizados. Para isso, usando teste para verificação da conectividade e, por meio disso, visualizar o resultado dessas conexões realizadas.

Realizaram-se os seguintes procedimentos, iniciou-se com o comando ipconfig para comprovar que o protocolo IPv6 está habilitado de forma nativa, mostrar qual protocolo o navegador utiliza para fazer a conexão com sites que utilizam IPv6, além de buscar determinar a conectividade IPv6 e aferir o nível de compatibilidade com a nova versão do protocolo.

Através do comando ipconfig é possível visualizar que o IPv6 é nativo no Windows 8, isso porque desde o Windows Vista, a Microsoft oferece IPv6 já instalado nos Sistemas Operacionais. Na figura 11 a seguir é possível visualizar essa configuração nativa e o endereço gerado pelo sistema operacional.

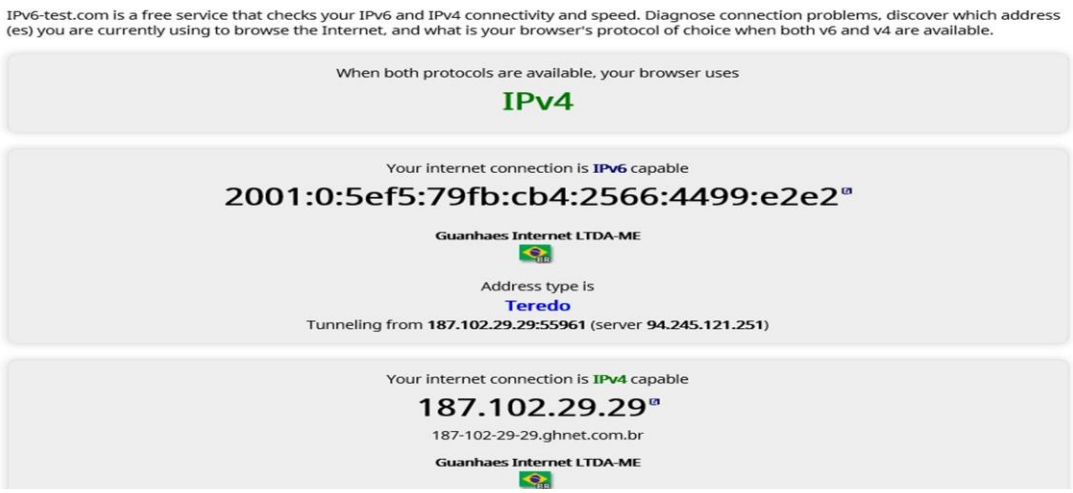
Figura 11: Comando ipconfig



Fonte: Elaborado pelos autores

Após verificar a configuração nativa do IPv6 demonstra-se a conectividade, na figura 12 através do teste de conectividade utilizando o site IPv6-test.com, um serviço gratuito para verificar a conectividade quando se utiliza ambos protocolos; e, a seguir, pode visualizar por qual protocolo a conexão é estabelecida, o endereço IPv6, o provedor de acesso a *Internet*, técnica de tunelamento utilizada para realizar a conexão e o endereço IPv4.

Figura 12: Teste realizado através do site IPv6-test.com

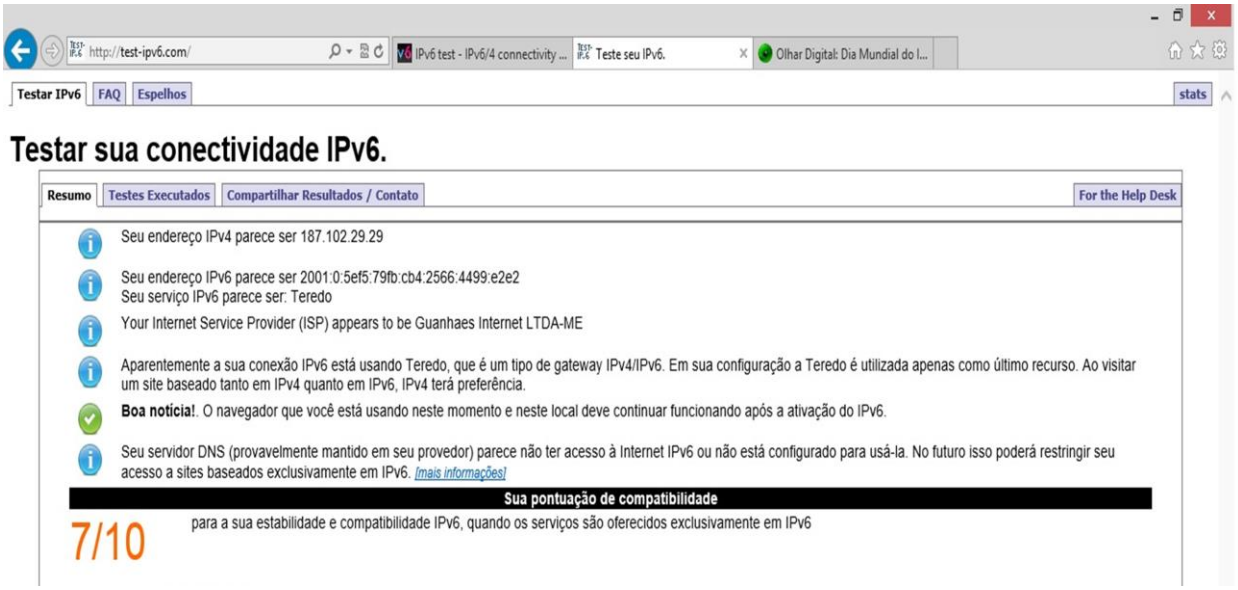


Fonte: Elaborado pelos autores

É possível identificar na figura 12 qual protocolo é escolhido pelo navegador quando ambos os protocolos estão disponíveis. Neste caso foi utilizado o protocolo IPv4, isso acontece devido aos equipamentos do provedor não possibilitarem conexão puramente IPv6, a conexão é realizada através da técnica de tunelamento Teredo, técnica -- implementada de forma automática pelos sistemas operacionais da *Microsoft.* Mas o uso dessa técnica esta obsoleto, uma vez que utiliza o protocolo UDP, mais especificamente a porta 3544, para fazer o encapsulamento de pacotes. Se uma rede coorporativa tem a intenção de utilizar IPv6 é aconselhável que seja desabilitada a técnica Teredo, pois gera túneis automáticos, e que sejam implementadas outras variações de túneis, caso não haja IPv6 na borda da rede.

Mas diante da resposta positiva da possibilidade de conexão IPv6 existe a necessidade de se conhecer mais detalhes desta conexão, como mostrado na figura 13 a seguir, onde são mostrados ambos endereços utilizados, IPv4 e IPv6, qual técnica utilizada, o provedor de *Internet*, informações sobre navegador utilizado, informações sobre o servidor DNS e a pontuação de estabilidade e compatibilidade para serviço exclusivamente IPv6, o teste realizado no site test-IPv6.com, um serviço gratuito que testa a acessibilidade do lado do cliente, determinando o tempo de conexão em determinados serviços quando ambos protocolo estão habilitados.

Figura 13: Teste realizado através do site test-IPv6.com - Resumo



Fonte: Elaborado pelos autores

A figura 14 a seguir apresenta os testes realizados para chegar a tais resultados apresentados na figura 13.

Figura 14: Teste realizado através do site test-IPv6.com – Testes Executado

Fonte: Elaborado pelos autores

Na figura 14 é possível ver com mais precisão a comparação entre a conectividade IPv6 e IPv4, a primeira comparação é a resposta do Servidor DNS no IPv4 é feita a busca por um objeto que utiliza apenas A no DNS, no IPv6 é feita a busca por um objeto que utiliza um registro AAAA no DNS, neste caso, para usuários que possuem IPv6 habilitado essa tentativa de conexão irá falhar. Tido como mais importante, o teste com um registro de DNS duplo, esse teste verifica se o navegador possui registro tanto para IPv4 quanto para IPv6 e com registro de DNS duplo e pacote grande, verifica-se se pode enviar pacotes grandes nessa conexão.

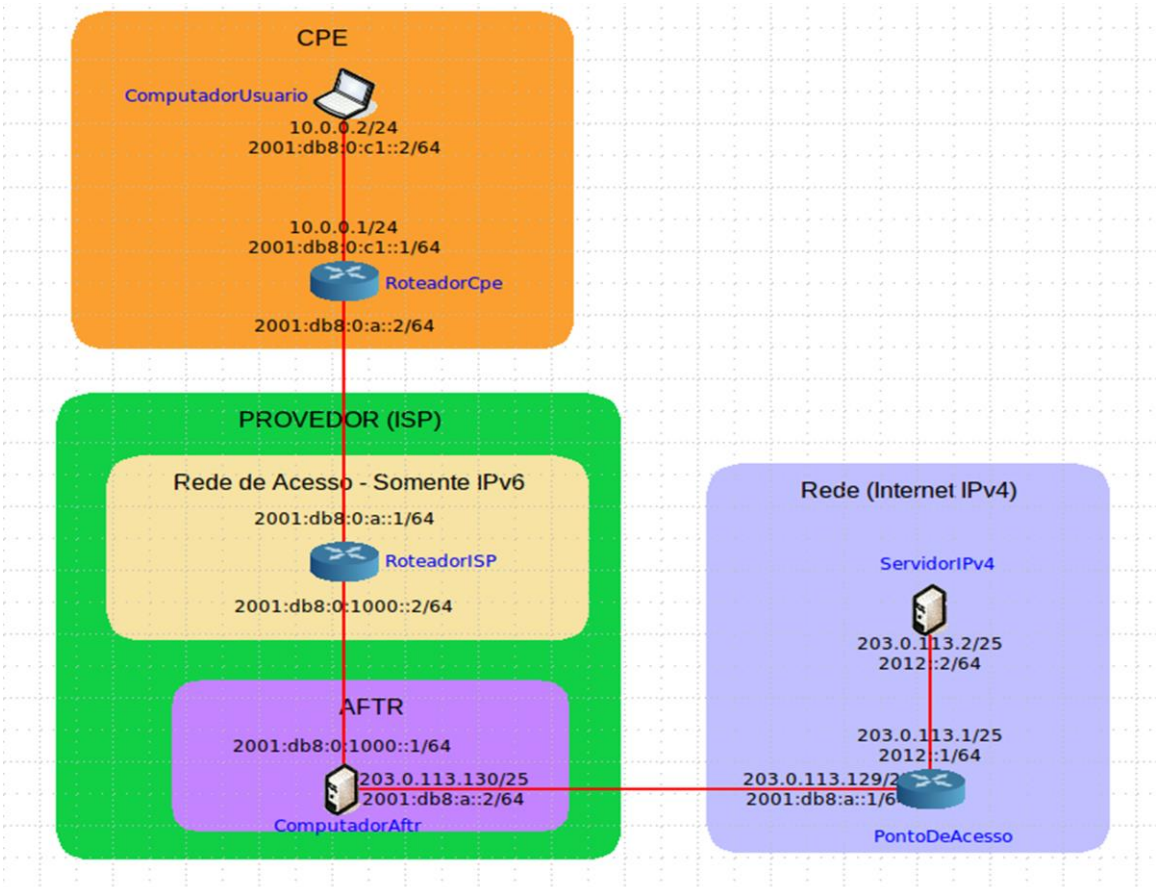
O teste IPv4 sem DNS, tenta estabelecer uma conexão usando um endereço IPv4, o que deve funcionar para todos, a não ser que seja utilizado exclusivamente IPv6. Teste IPv6 sem DNS tenta estabelecer uma conexão usando o endereço IPv6; a ideia, neste caso, é fazer a separação da conectividade IPv6 de sua capacidade de utilizar o DNS para estabelecer a conexão. Teste de pacote grande usando IPv6 Teredo verifica o funcionamento do protocolo para a transmissão de pacotes grandes. Caso a conexão falhe, possivelmente, existem problemas envolvendo o túnel utilizado. Testa se o provedor DNS utiliza IPv6, a resposta com *time out* indica que o servidor DNS mantido pelo provedor não é capaz de acessar servidores DNS autoritativo, baseados exclusivamente em IPv6.

Com este laboratório, conclui-se que é real a possibilidade da coexistência das duas versões do protocolo IP. Na rede utilizada para o teste foi visto que o provedor de *Internet* não possui técnica de transição atribuída em seus equipamentos, esse procedimento é feito pelo sistema operacional através da técnica de tunelamento automático do Windows, Teredo. Fica provado que se o IPv6 for desabilitado, a conexão não poderá ser estabelecida através do protocolo.

5.5.2. *Laboratório DSLite*

O cenário deste laboratório apresenta um momento onde o IPv4 já está escasso, já existe o tráfego de informações via IPv6 mas ainda existem serviços que estão disponíveis apenas em IPv4. A técnica de transição DS-LITE é uma solução para que seja possível a comunicação com estes pontos que só possuem IPv4 como pode ser visto na figura 15 a seguir.

Figura 15: Apresentação do ambiente DS-LITE



Fonte: Elaborado pelos autores

Neste ambiente temos um cenário onde a comunicação IPv6 é realizada naturalmente, ou seja, os provedores fornecem IPv6 nativo aos usuários, que podemos identificar na figura como RoteadorISP. No ambiente, temos um cliente com IPv4 e IPv6 configurados, o ComputadorUsuario; um CPE que também possui IPv4 e IPv6, identificado como RoteadorCpe.

No ambiente 2, temos o ISP(*Internet Service Provider)* que é a rede do provedor, utilizando apenas com IPv6. Juntamente temos o AFTR, identificado como ComputadorAftr, que possui em uma interface apenas IPv4 e na outra interface, IPv4 e IPv6. O ComputadorAftr é o responsável por realizar a função de NAT para a *Internet* IPv4.

O objetivo deste laboratório é demonstrar como funciona a técnica DSLITE na prática, apresentando as características dos elementos que fazem parte desta técnica. Para a realização desta técnica, é preciso realizar configurações por parte do provedor de serviço e por parte do usuário.

Os procedimentos iniciaram-se com as configurações dos dispositivos do lado cliente, que são uma máquina de um usuário e um CPE, e do lado do provedor uma ilha onde só existem endereços IPv4, um aftr, que é o responsável por disponibilizar uma maneira de usuários acessarem esta ilha IPv4 em uma rede IPv6.

A simulação do ambiente será realizada no software CORE 4.3, um software open source utilizado para simulações de rede. Juntamente com o CORE, é necessário a utilização do AFTR. Todo o Laboratório foi realizado em um Sistema Operacional Ubuntu, na versão 11.04.

Inicialmente é necessário realizar o download e a compilação do AFTR. Para a realização deste laboratório foi utilizada a versão aftr1.1. Para a compilação do AFTR temos os seguintes comandos:

Estes comandos são usados para descompactar o aftr no diretório atual do usuário e entrar no diretório, respectivamente:

$ tar xf aftr1.1.tar.gz

$ cd aftr1.1

Os próximos comandos são utilizados para a compilação do AFTR

$ chmod +x configure

$ ./configure

$ make

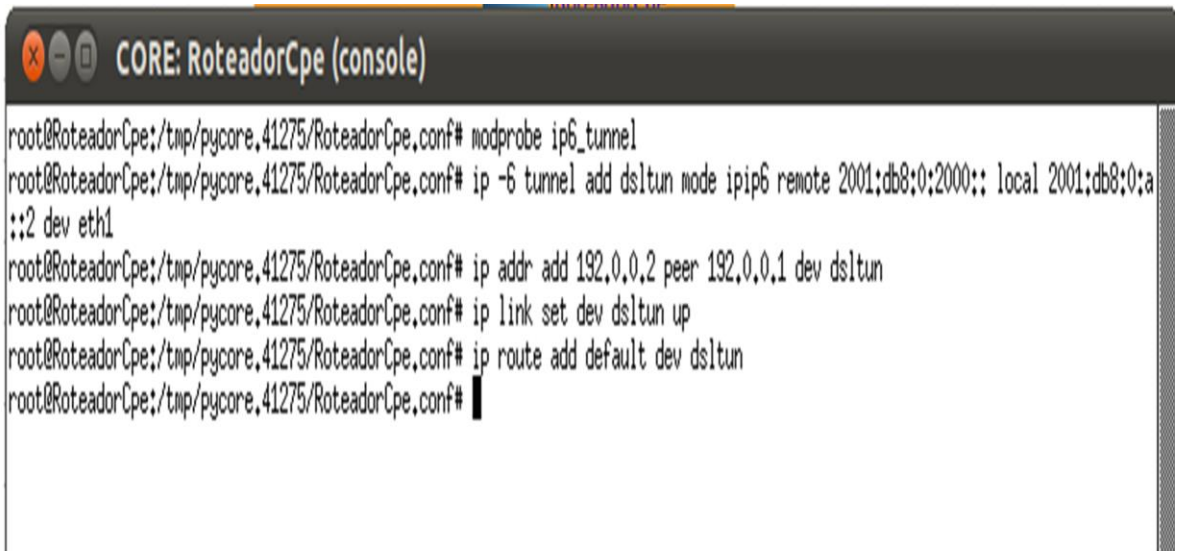
$ sudo ln s /home/core/aftr1.1/aftr/usr/bin/aftr

Inicialmente, neste cenário só é possível realizar comunicação via IPv6, para que seja possível a comunicação com um serviço que é fornecido apenas em IPv4 é necessário a implantação da técnica DS-LITE, onde será criado um túnel onde os pacotes IPv4 serão encapsulados em cabeçalhos IPv6. Este túnel se estende do CPE até o AFTR do provedor, onde será realizada a função de NAT e permitir a comunicação com o serviço IPv4.

É necessário realizar a configuração de um túnel a partir do CPE, que será ligado até o AFTR do provedor, com o intuito de possibilitar a comunicação IPv4 sobre a rede IPv6.

A configuração é realizada com comandos na interface RoteadorCpe ilustrados na figura 16 a seguir:

Figura 16: Demonstração de criação do túnel IPv4 sobre IPv6



Fonte: Elaborado pelos autores

A configuração é iniciada com o comando modprobe ip6_tunnel

 # modprobe ip6_tunnel

Neste ponto é definido que o túnel é do tipo IPv4 sobre IPv6, nomeado dsltun com o endereço local definido como 2001:db8:0:a::2 e o link remoto como 2001:db8:0:2000::

 # ip -6 tunnel add dsltun mode ipip6 remote 2001:db8:0:2000:: local 2001:db8:0:a::2 dev eth1

Este comando define a ligação do túnel do lado do CPE com o AFTR. O IP 192.0.0.2 é utilizado pelo CPE, enquanto o 192.0.0.1 é utilizado pelo AFTR. De acordo com o RCF 6333, a faixa de IP 192.0.0.0/29 foi reservada pela IANA (*Internet Assigned Numbers Authority*) para a configuração das interfaces de túnel nas implementações do DSLite.

 # ip addr add 192.0.0.2 peer 192.0.0.1 dev dsltun

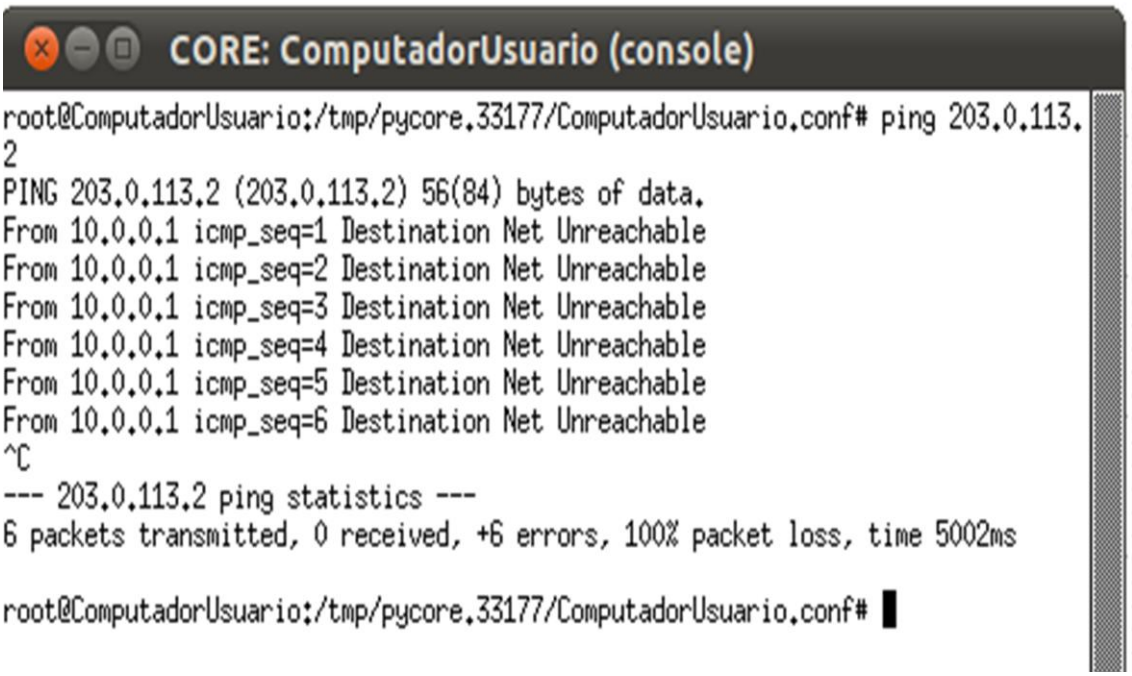
Os próximos comandos dão inicio ao funcionamento dos túneis.

 # ip link set dev dsltun up

 # ip route add default dev dsltun

Com o túnel configurado do lado do cliente, é necessário configurar o ponto de saída do túnel, que é realizado no AFTR pelo provedor, caso contrário, a comunicação com a ilha IPv4 não será realizada. Na figura 17 a seguir, pode-se visualizar a tentativa de comunicação entre o ComputadorUsuario e o ServidorIPv4, utilizando endereço do protocolo IPv4, mas sem sucesso.

Figura 17: Demonstração de falha de acesso via IPv4.



Fonte : Elaborado pelos autores

Temos neste ponto os comandos necessários para a configuração do túnel no AFTR, e para isso é necessário a criação de um script nomeado como aftr-script. Clique na interface do ComputadorAftr para realizar a criação do script e realizar a configuração. Na figura 18 a seguir pod-se visualizar o conteúdo do script criado.

Figura 18: Script de fechamento do túnel IPv4 sobre IPv6

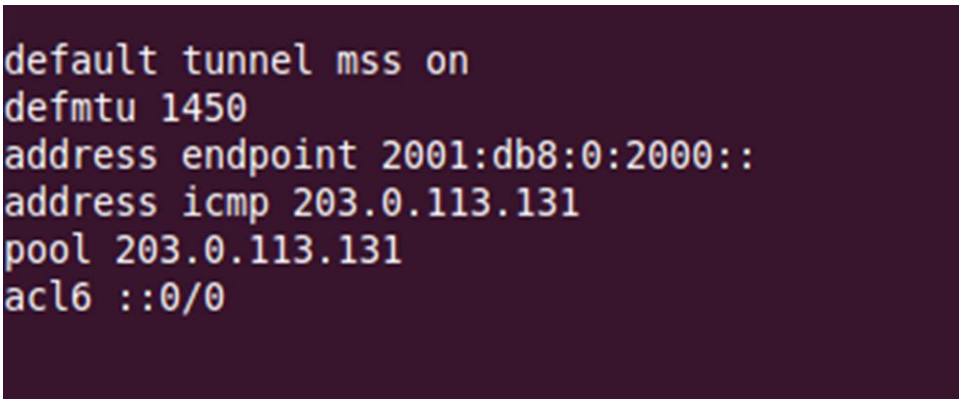
```
#!/bin/sh

aftr_start() {
    set -x
    ip link set tun0 up
    ip addr add 192.0.0.1 peer 192.0.0.2 dev tun0
    ip route add 203.0.113.131/32 dev tun0
    ip -6 addr add fe80::1 dev tun0
    ip -6 route add 2001:db8:0:2000::/64 dev tun0
    arp -i eth0 -s 203.0.113.131 0a:0b:0c:0d:0e:f0 pub
}

aftr_stop() {
    set -x
    ip link set tun0 down
}

case "$1" in
start)
        aftr_start
        ;;
stop)
        aftr_stop
        ;;
*)
        echo "Usage: $0 start|stop"
        exit 1
        ;;
esac

exit 0
```

Fonte: Elaborado pelos autores

Neste documento temos a definição dos endereços 192.0.0.1 e 192.0.0.2 que são utilizados para este tipo de implementação DSLITE. O endereço 203.0.113.131 é o endereço público utilizado para a realização do NAT na rede interna do ISP. O endereço 2001:db8:0:2000:: foi escolhido para o fechamento do túnel no servidor AFTR. Esse endereço não pode ser utilizado nas interfaces de rede do servidor ou por qualquer outro equipamento de rede.

É necessário também a criação de um documento para se realizar a configuração de fechamento do túnel aberto pelo RoteadorCpe. O documento é nomeado como aftr.conf. Para este documento temos o seguinte conteúdo, que pode ser visualizado na figura 19 a seguir:

Figura 19: Conteúdo do arquivo aftr.conf

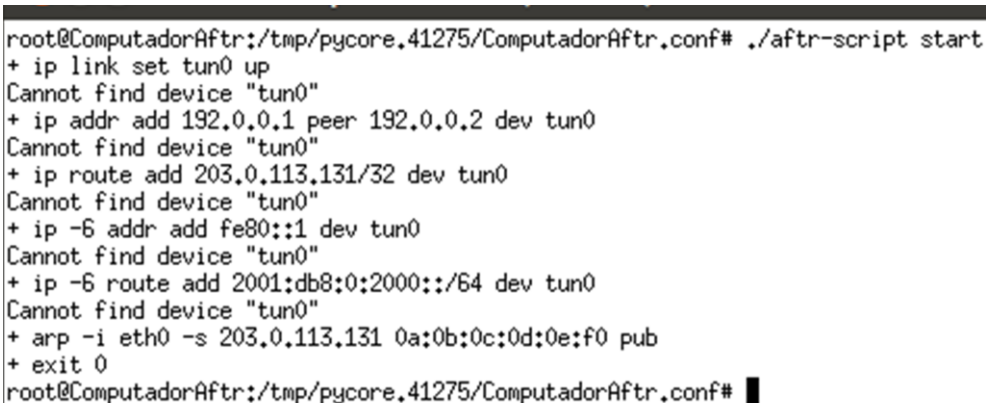


Fonte: Elaborado pelos autores

Neste documento temos a definição do endereço do ponto final do túnel, assim como a definição do MTU dos pacotes trafegados no túnel, um endereço de icmp e uma faixa de endereços.

Após isso, é necessário iniciar o serviço AFTR na interface do ComputadorAftr com o comando *aftr. Pode-se visualizar na* figura 20 a seguir a resposta do comando.

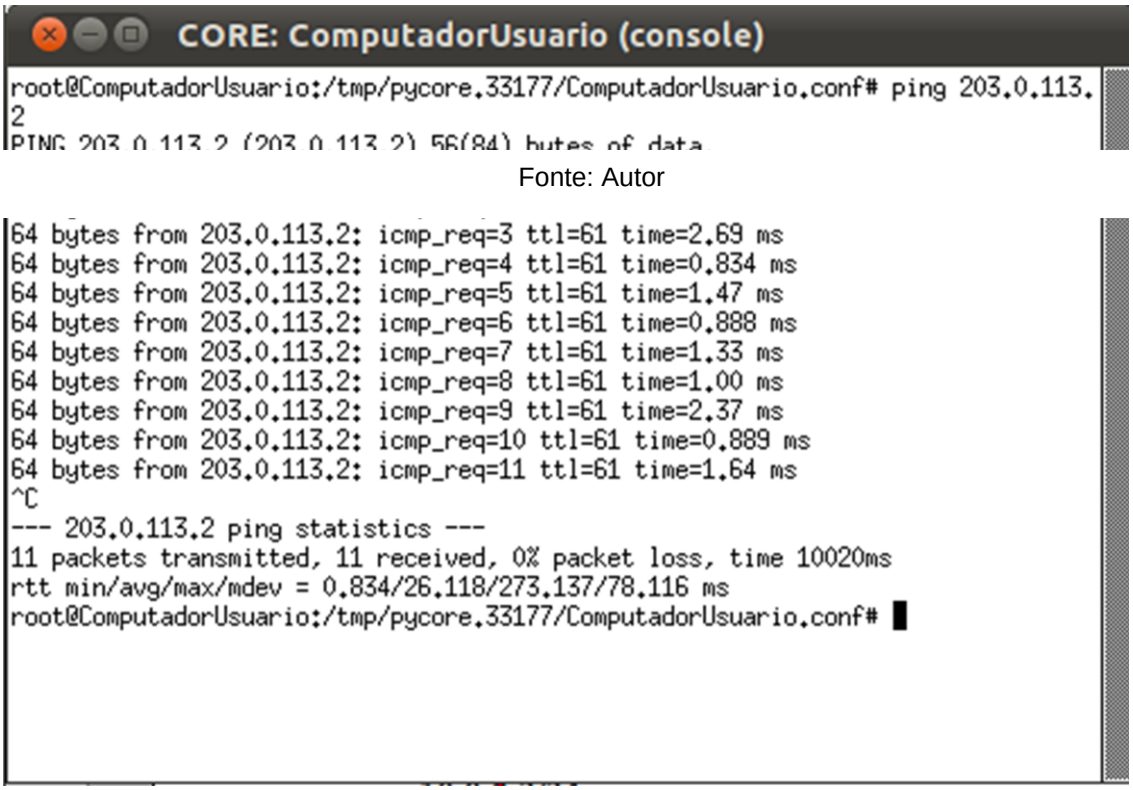
Figura 20: Concretização da configuração do túnel IPv4 sobre IPv6



Fonte: Elaborado pelos autores

Sendo assim, temos o túnel criado e a implementação do DSLITE realizada. Agora é possível que o cliente acesse serviços que possuem somente IPv4, através de um túnel entre o RoteadorCpe e o ComputadorAftr. Esta comunicação é possível ser visualizada na figura 21 através do comando *ping.*

Figura 21: Demonstração de ping via IPv4

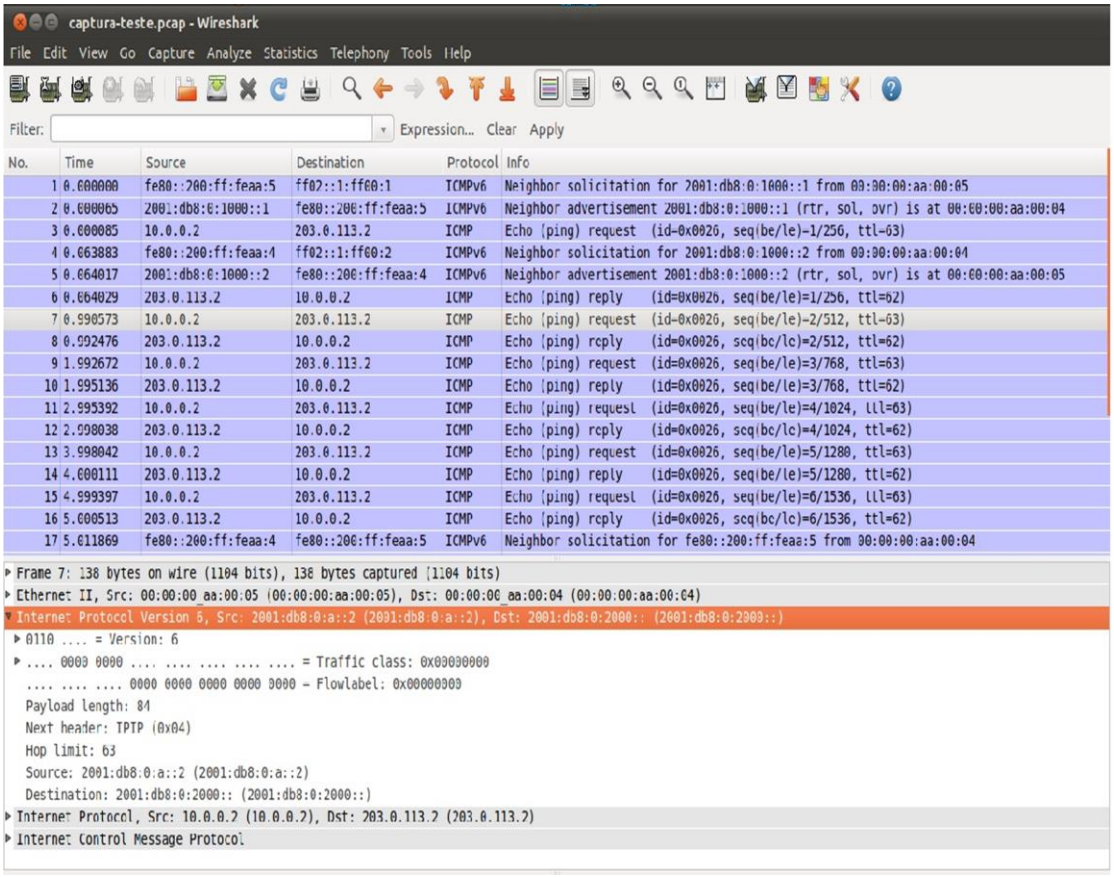


Fonte: Autor

Fonte: Elaborado pelos autores

Para provar que o encapsulamento do pacote IPv4 em um pacote IPv6 pode-se observar na figura 22 que mostra através da captura realizada através do *Wireshark*, *software* que analisa o tráfego de rede, e o organiza por protocolos. Na linha 7 vemos a requisição feita pelo ComputadorUsuario para o ServidorIPv4. Na linha em destaque, pode-se observar que o cabeçalho IPv4 é encapsulado em um cabeçalho IPv6 e então é realizado a trafego através de um túnel na rede de acesso IPv6.

Figura 22: Demonstração de encapsulamento de pacotes



Fonte: Elaborado pelos autores

Conclui-se a partir da execução deste laboratório, o quão fácil é a implantação desta técnica, o que deve ser levado em consideração pelos provedores, para que a implantação seja iniciada o quanto antes.

É importante citar que a implantação desta técnica é de baixo custo, o que deve ser considerado como uma vantagem. Outro ponto que deve ser considerado na hora da decisão de qual técnica implantar, é que esta é uma técnica bem madura atualmente, com vários documentos contendo informações sobre a implantação, facilitando assim o processo.

Além destes pontos, o DSLITE é uma técnica que visa o prolongamento necessário de acesso às redes IPv4, juntamente com a rede IPV6 nativa, visto que a

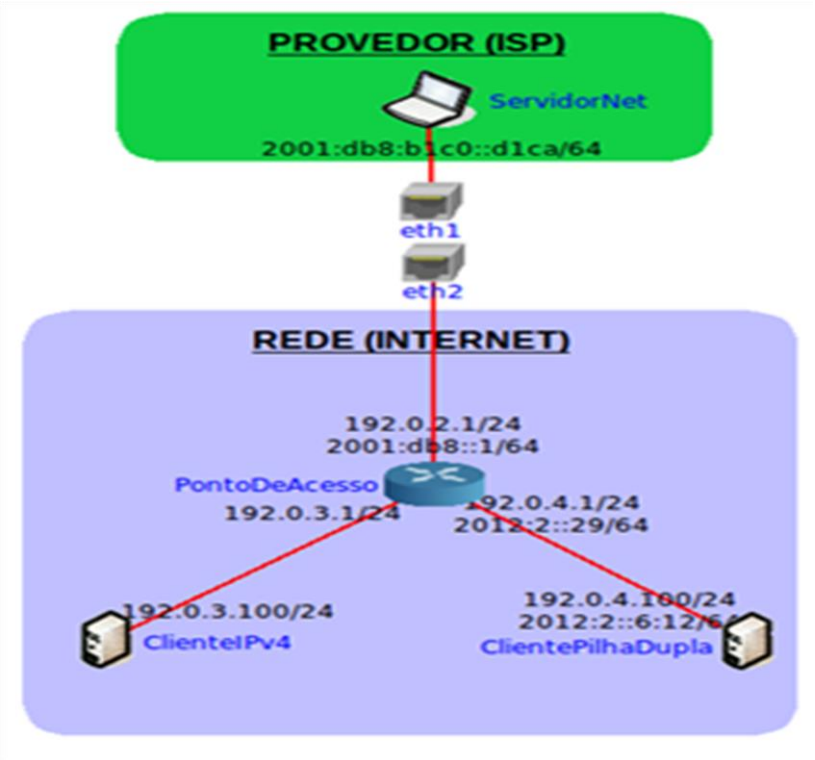
preferência é a implantação de técnicas que não preservem o IPv4, mas sim que deem acesso concomitante a ambos os protocolos, IPv4 e IPv6, que é a recomendação do Comitê Gestor da *Internet* no Brasil(CGI).

5.5.3. Laboratório NAT64/DNS64

O cenário deste laboratório apresenta um momento onde o IPv4 já está escasso, já existe o tráfego de informações via IPv6 mas ainda existem serviços que estão disponíveis apenas em IPv4. A técnica de transição NAT64/DNS64 é uma solução para que os nós somente IPv4 possam acessar uma rede IPv6

O cenário utilizado é exemplificado pela figura 23 a seguir. Existem 02 (dois) ambientes, o ambiente do PROVEDOR (ISP) e o da REDE (*INTERNET*).

Figura 23: Cenário para implantação do NAT64/DNS64



Fonte: Elaborado pelos autores

O ambiente 1, PROVEDOR (ISP) é composto por 01 (um) computador denominado ServidorNet, que tem atribuído a ele 01 (uma) interface de rede que utiliza o protocolo de comunicação IPv6.

O ambiente 2, REDE (*INTERNET*) é composto por 02 (dois) computadores. O computador ClienteIPv4, tem atribuído a ele 01(uma) interface de rede que utiliza o protocolo de comunicação IPv4. Já o computador ClientePilhaDupla, tem atribuído a ele 01 (uma) interface de rede que utiliza os protocolos de comunicação IPv4 e IPv6, através de uma técnica conhecida como Pilha Dupla.

Por fim, o ambiente é composto também por 01 (um) roteador denominado PontoDeAcesso, que tem atribuído a ele 03 (três) interfaces de rede. Sendo a primeira *Eth0*, utilizando IPv4 e IPv6, interligada ao ServidorNet; A segunda *Eth1*, utilizando IPV4, interligada ao ClienteIPv4; A terceira *Eth2*, utilizando IPv4 e IPv6, interligada ao ClientePilhaDupla. De acordo com a estrutura do ambiente 002, temos então, um cliente que utiliza apenas IPv4 e outro cliente que tem pilha dupla habilitada, sendo capaz de receber informações tanto IPv4 quanto IPv6. O roteador PontoDeAcesso é configurado para fazer a comunicação com ambos os protocolos.

O objetivo deste laboratório é demonstrar como são feitas as configurações de uma máquina inserida em um provedor de *Internet* para que esta faça a entrega de endereços IPv6 com sucesso em uma rede majoritariamente IPV4. Para isso é apresentada a técnica de transição NAT64/DNS64. Os testes são realizados em um cenário que é composto por um provedor de *Internet* e seus clientes. Para tal foi utilizado o Sistema Operacional Ubuntu 11.04 e o software CORE 4.3.

Nos procedimentos o download e instalação do modulo do kernel do Linux desenvolvido pelo projeto ecdysis. (ECDYSIS, 2013). E criação do ambiente no simulador CORE, configuração do computador ServidorNet e do roteador PontoDeAcessoutilizadas para desenvolver o cenário.

Logo após a criação do cenário, o primeiro passo é integrar o CORE com o sistema utilizado, no caso o Ubuntu 11.04 rodando a partir de uma máquina virtual. Para tal, é necessário executar o script de comandos denominado **simulacao-nat-64.sh** que realiza o roteamento necessário para estabelecer comunicação entre o CORE e o sistema. O conteúdo desse script pode ser visualizado na figura 24 a seguir:

Figura 24: Script usado para integrar os Host ao CORE

Fonte: Elaborado pelos autores

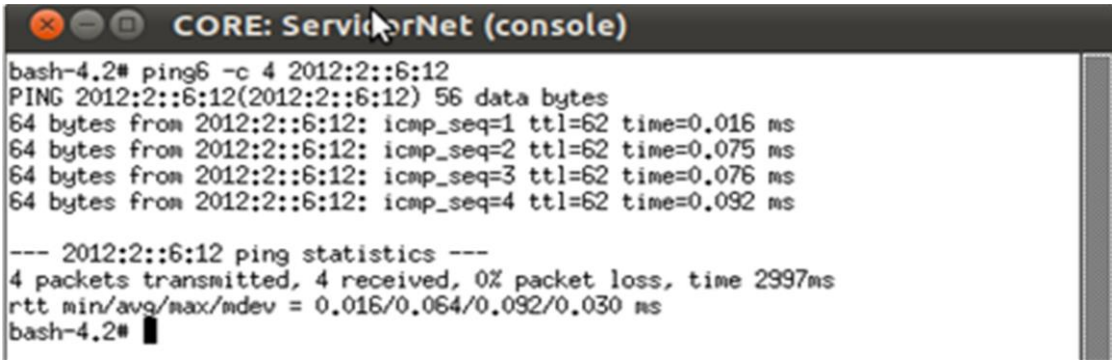
Na figura 25 a seguir temos o retorno da execução do script de integração simulacao-nat-64.sh e o comando ***sudo sysctl w net.ipv6.conf.all.forwarding=1***, o retorno será:

Figura 25: Resposta da execução do script

Fonte: Elaborado pelos autores

Agora é necessário verificar a conectividade entre o ServidorNet e o ClientePilhaDupla, através do protocolo IPv6. Conforme figura 26 a conexão foi estabelecida com sucesso:

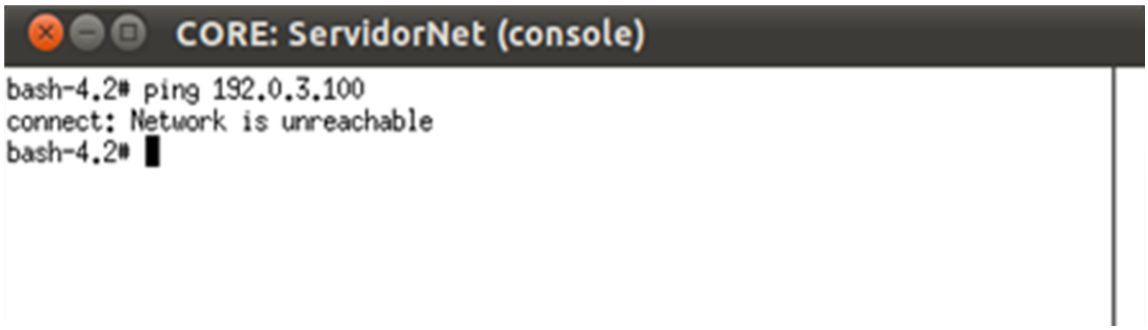
Figura 26: Ping IPv6 no ClientePilhaDupla



Fonte: Elaborado pelos autores

A conectividade entre ServidorNet e ClientePilhaDupla existe pois o computador ClientePilhaDupla tem conectividade IPv6. Em seguida é feito o teste de conectividade com o computador ClienteIPv4, que retorna erro, pois ainda não há tradução de endereços IPv4, conforme a figura 27 a seguir:

Figura 27: Ping IPv4 no ClientePilhaDupla

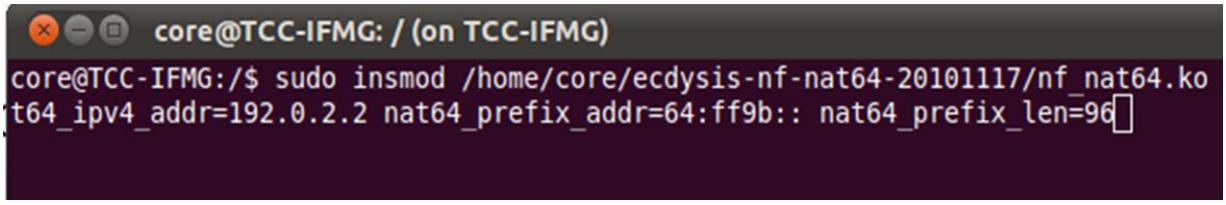


Fonte: Elaborado pelos autores

Para solucionar essa falta de conectividade, o NAT64 deve ser configurado na máquina utilizada como *host*, no caso, Ubuntu 11.04. Sua configuração envolve subir um módulo para kernel do Linux desenvolvido pelo projeto Ecdysis, (Ecdysis, 2013) que possibilita definir alguns parâmetros como o prefixo utilizado pelo NAT64

para tradução do endereço e tamanho desse prefixo, o comando pode ser visualizado na figura 28 a seguir:

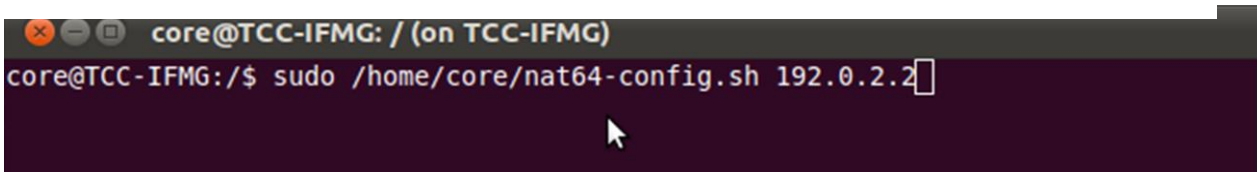
Figura 28: Definição do prefixo utilizado na tradução



Fonte: Elaborado pelos autores

Para resolver o problema de falta de conectividade, ainda é necessário habilitar o NAT64 e configurar a rota para tradução, conforme figura 29 a seguir:

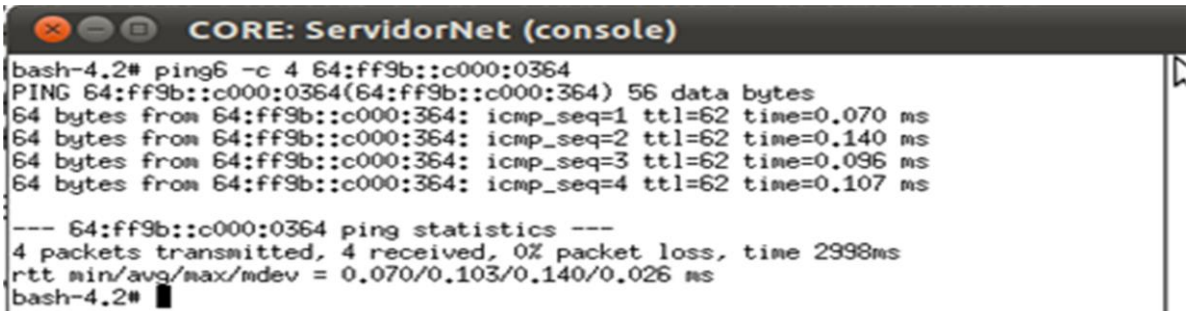
Figura 29: Definindo endereço da rota para tradução



Fonte: Elaborado pelos autores

Após configurar o NAT64 e subir os módulos do de configuração ecdsys o NAT64 deve estar funcionando na maquina host. É verificado o sucesso da conectividade IPv6 entre ServidorNet e ClienteIPv4, onde os endereços IPv4 agora são acessíveis, via NAT64, utilizando o prefixo configurado 64:ff9b::/96 e também o endereço IPv4 do ClienteIPv4 escrito em forma hexadecimal, c0:00:03:64, resultando em um novo endereço IPv6 64:ff9b::c000:0364, de acordo com a figura 30 a seguir é visualizar a conexão, mas o Servidor Net enxerga apenas endereços IPv6 assim como o ClienteIPv4 enxerga apenas endereços IPv4.

Figura 30: Ping IPv6 com endereço traduzido



Fonte: Elaborado pelos autores

Desta forma o NAT64 esta funcionando, mas é apenas a metade de todo processo que deve ser realizado. Agora deve-se configurar o DNS64.

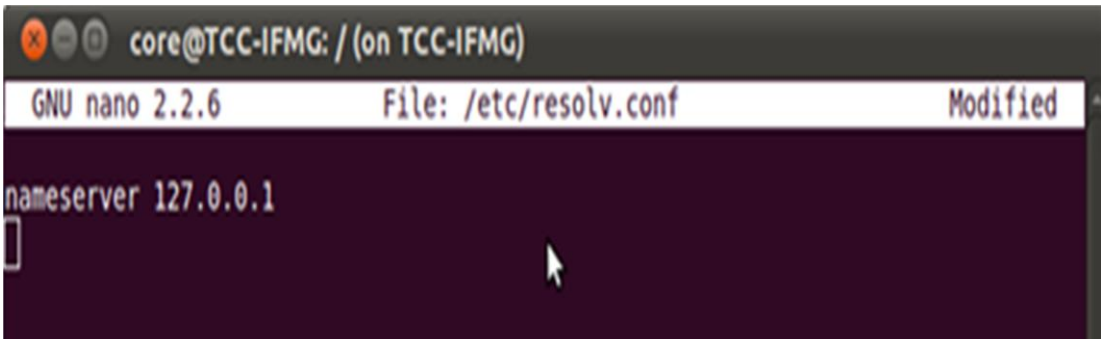
Na máquina *host* deve ser editado o *resolv.conf* , esse arquivo no Linux é que diz onde estão os *nameserves,* comando para editar o arquivo pode ser visualizado na figura 31 a seguir:

Figura 31: Comando para abrir o arquivo resolv.conf

Fonte: Elaborado pelos autores

A edição deste arquivo se dá apagando todo seu conteúdo e indicando que o *nameserver* é o *localhost,* e endereçado por 127.0.0.1 conforme a figura 32 a seguir:

Figura 32: Arquivo resolv.conf editado



Fonte: Elaborado pelos autores

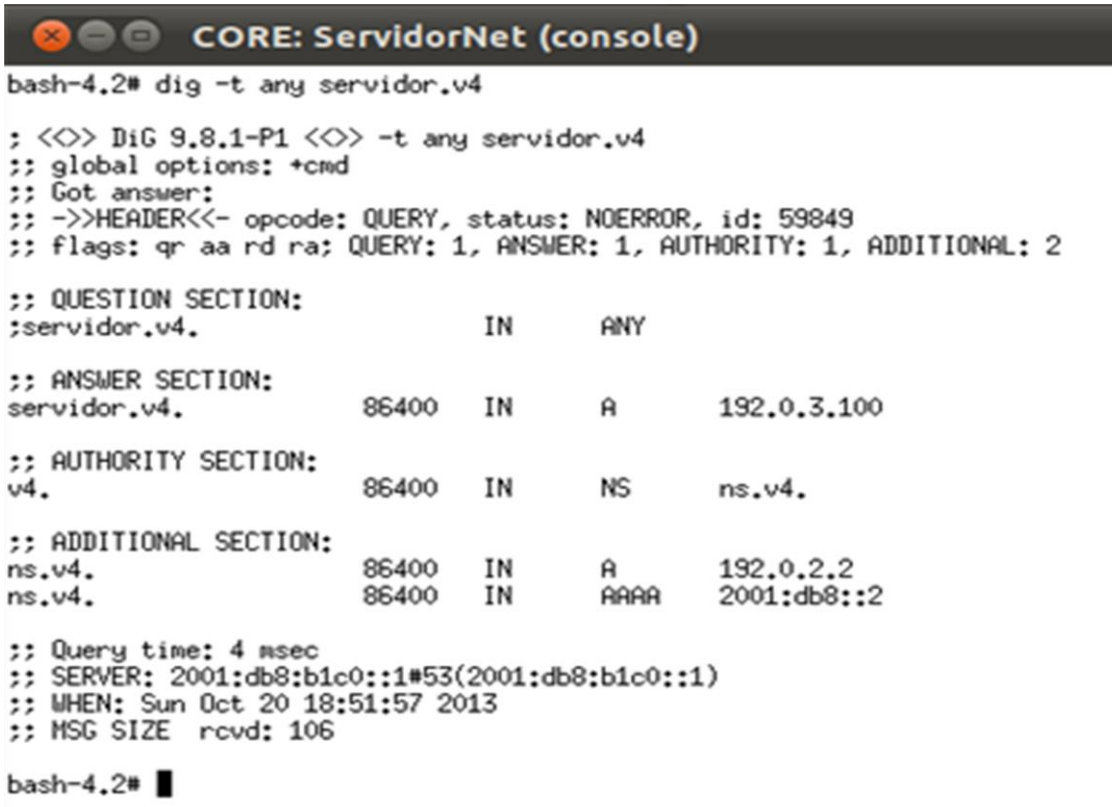
Após a edição do resolv.conf é inicializado o BIND (Berkeley *Internet* Name Domain) principal servidor para o protocolo DNS do Linux, pode ser visto na figura 33 a seguir.

Figura 33: Inicialização do BIND

Fonte: Elaborado pelos autores

Em seguida são verificados os arquivos de endereçamento de DNS do ServidorIPv4, através do arquivo servidor.v4 conforme figura 34 a seguir abaixo:

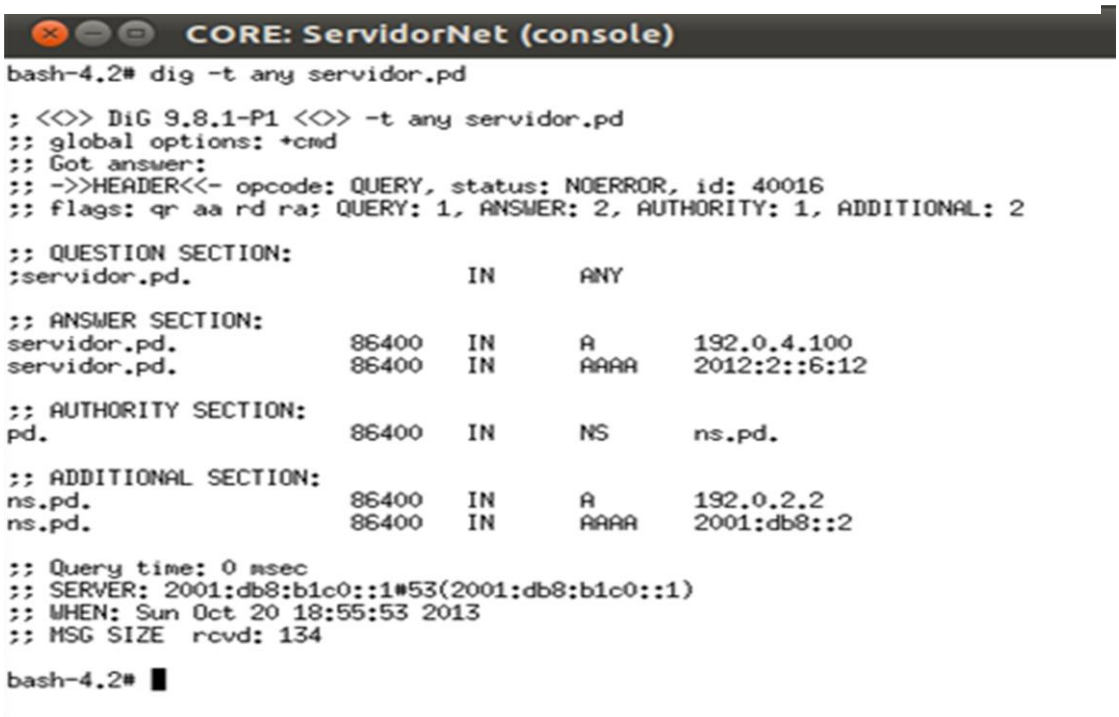
Figura 34: Consulta do endereçamento de DNS v4



Fonte: Elaborado pelos autores

Na figura 35 a seguir podemos visualizar os arquivos de endereçamento de DNS do ServidorPilhaDupla.

Figura 35: Consulta do endereçamento de DNS Pilha Dupla

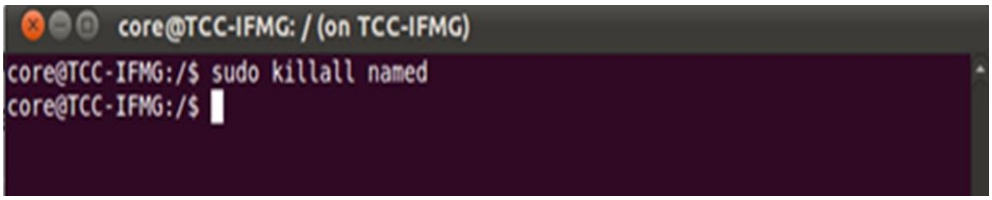


Fonte: Elaborado pelos autores

Nestas consultas, podemos observar que apenas o domínio servidor.pd possui endereçamento IPv4 e IPv6 (pilha dupla) e que o servidor.v4 possui apenas endereço IPv4.

Devemos alterar a configuração do BIND para que o NAT64 possa estar ativo, dessa forma é utilizado o comando killall named para encerrar o BIND para que possa ser inserido o prefixo que será utilizado pelo DNS, assim habilitando a técnica conjunta ao NAT64, o DNS64. Na figura 36 a seguir o encerramento o serviço DNS:

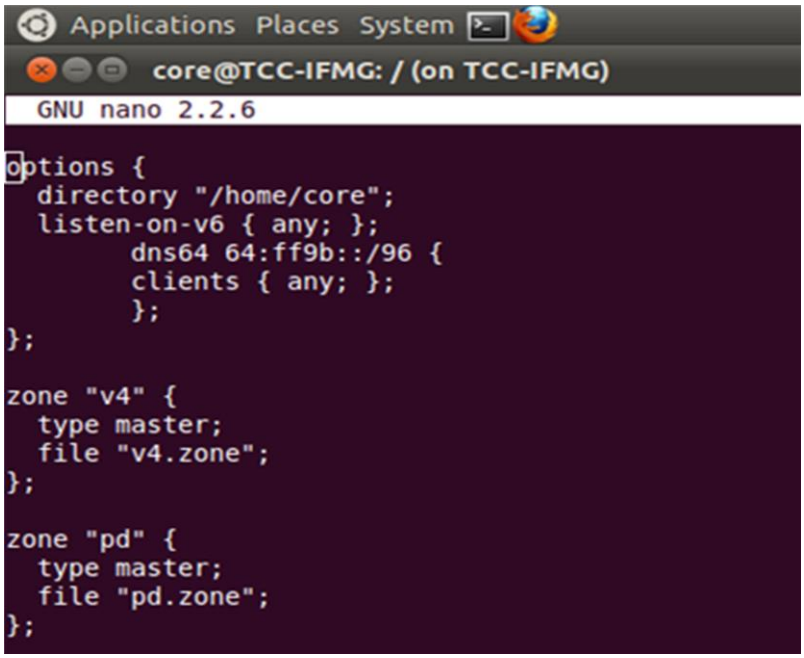
Figura 36: Encerrando o BIND



Fonte: Elaborado pelos autores

E a edição do arquivo DNS do cenário se dá a partir do comando // *vim named.conf,* o arquivo a ser editado é visto na figura 37 a seguir, é necessário a adição do endereço IP do prefixo do dns64 64:ff9b::/96:.

Figura 37: Arquivo *named.conf* editado



Fonte: Elaborado pelos autores

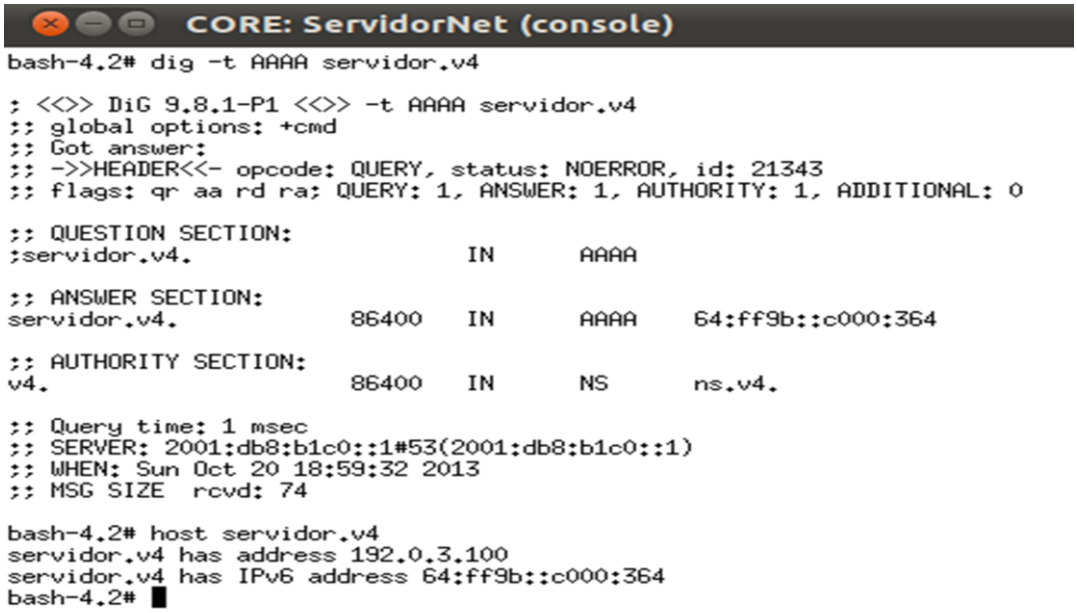
Iniciando o serviço DNS novamente através do BIND, comando a ser executado exibido na figura 38 a seguir:

Figura 38: Inicializando o BIND

Fonte: Elaborado pelos autores

Após o DNS64 configurado, pode ser observado que a consulta ao domínio servidor.v4 agora possui como resposta um endereço IPv4 mapeado, conforme figura a seguir:

Figura 39: Consulta do endereçamento de DNS v4



Fonte: Elaborado pelos autores

Concluiu-se com este laboratório que foram demonstradas as configurações necessárias para que uma rede predominantemente IPv6 possa realizar a comunicação com nós IPv4, por meio da técnica de tradução denominada NAT64/DNS 64. Com algumas configurações na máquina principal da rede, no caso o servidor que entrega os serviços, pode-se então enviar e receber pacotes IPv4, de forma *Statefull*, sem necessariamente depender de uma configuração para cada máquina da rede. Com base nos testes realizados, a técnica de transição NAT64/DNS64 mostrou-se extremamente eficaz no cenário de um provedor de serviços e/ou *Internet*.

5.6. Avaliação de resultados

As técnicas Pilha Dupla, DSLite e NAT64/DNS64 não são as únicas disponíveis, existem ainda outras técnicas que prometem até melhores desempenhos e maiores facilidades de implementação, porém as técnicas abordadas na pesquisa trazem maior confiabilidade por serem técnicas já maduras e possuírem documentação de referência, tornando seu uso mais indicado no momento.

A técnica Pilha Dupla é indicada para ser usada sempre que possível, pois, quando a rede não mais possuir endereços IPv4, basta apenas desabilitar o protocolo. A grande vantagem dessa técnica é que é nativa na maioria dos sistemas operacionais atuais e requer o mínimo de conhecimento do usuário para que possa acessar sites que possuam IPv6, como pode ser visto no laboratório 1, no qual foi utilizado um sistema operacional que possui IPv6 nativo no acesso à rede é simples. Mas a sua desvantagem mais clara é o gasto adicional de memória e de processamento por utilizar duas pilhas rodando separadamente, cada uma fazendo a tradução de determinados pacotes. Outra desvantagem é a necessidade de ter firewall, DNS configurados separadamente para cada protocolo.

Essa técnica é considerada com a maior versatilidade e simplicidade, pois a técnica escolhe qual protocolo utilizar em determinada situação, a escolha é feita pela aplicação.

A técnica DS-LITE é indicada para o momento em que a transição do IPv4 para o IPv6 já esteja em fase final, onde a maioria dos serviços disponíveis já podem ser acessados via protocolo IPv6 e uma pequena parte ainda necessita de acesso IPv4.

Com a técnica DS-LITE a comunicação com serviços disponíveis apenas em IPv4 é possível, de modo que favorece a transição para o IPv6, possibilitando somente acesso aos serviços IPv4 sem prolongar mais que o necessário. Mesmo com a possibilidade de acesso a estes serviços via IPv4 por meio da técnica DS-LITE, é necessário que estes serviços possam ser disponibilizados também através do acesso via IPv6, para que a transição do protocolo IPv4 para o protocolo IPv6 seja finalizada o quanto antes.

A técnica NAT64/DNS64 é indicada para quando a rede for IPv6 em grande parte mas houver necessidade de prover acesso IPv4. A técnica NAT64 consiste em mapear tradução de pacotes que permitem nós de uma rede IPv6 acessarem *Internet* IPv4, e necessita de uma técnica auxiliar DNS64, essa técnica converte o DNS utilizando um prefixo básico 64:ff9b::/96.

A vantagem de sua utilização é o baixo custo de implantação, pois a configuração é realizada em apenas um dispositivo, que pode ser um roteador ou como no caso do laboratório da técnica realizada em um *host.*

O problema desse tipo de tradução é por ser incompatível com algumas aplicações com esse tipo de NAT. Para serviços como correio eletrônico e

navegação HTTP não há grandes problemas, mas para soluções que envolvam balanceamento de carga ou algo do gênero, pode acarretar problemas.

6. CONSIDERAÇÕES FINAIS

Durante o desenvolvimento do trabalho pôde-se constatar que o IPv6 apesar de não ser uma tecnologia recente, finalizado em 1995, é um assunto pouco disseminado entre os profissionais na área de TI, e a migração anda a passos lentos, como algo para o futuro e não uma necessidade real.

Diante da iminência do esgotamento do IPv4 existe a grande necessidade de migrar as redes existentes para o IPv6, mas a migração está sendo feita de forma gradual, pois o custo para mudança de toda infraestrutura da rede demandaria recursos muito altos. Como pôde ser visto o caminho a ser seguido é a coexistência dos dois protocolos, mas a grande questão é disponibilizar meios que se ajustem a cada cenário. A recomendação da CGI.br é que a partir de janeiro de 2014 os provedores de *Internet* disponibilizem para novos usuários apenas endereços IPv6, que nas Universidades e centros de Pesquisa relacionadas às disciplinas de redes implantem o IPv6 em suas redes com urgência. Visto isso, pressupõem-se, que ao longo do tempo, a rede se tornará majoritariamente IPv6, mas existindo ilhas IPv4 que devem ser acessadas. Dessa forma foram estudadas as mudanças em relação ao IPv4 e as funcionalidades do IPv6 e as técnicas que possibilitem a coexistência dos dois protocolos no futuro.

Durante os estudos e os laboratórios realizados pôde ser constatado que a técnica que se encaixa em todos os cenários é a Pilha Dupla, pois sua adaptação é fácil em qualquer cenário, e a preferência sempre é que o usuário possua a técnica de transição, mas como para seu funcionamento demanda obrigatoriamente ter um endereço IPv4 válido, e a configuração do *host* deve ser individual para cada versão do protocolo, e alguns usuários tendem a desabilitar, o que não é indicado. Mas com o esgotamento de IPv4, e a existência de equipamento onde utilizasse unicamente IPv4, e equipamentos que utilizam apenas IPv6, teve a necessidade da criação de outras técnicas que auxiliassem na transição, considerando que inevitavelmente a *Internet* caminha pra o uso do IPv6.

As técnicas DSLite e NAT64/DNS64 são indicadas para o futuro, onde a rede em sua maior parte é constituída por IPv6. O uso dessas técnicas vai de acordo com a recomendação da CGI.br, que é a não preservação da rede IPv4.

REFERÊNCIAS

6DEPLOY**, IPv4 and IPv6 Transition & Coexistence,** 2013 Disponivel em <http://www.6deploy.org/tutorials2/130-6deploy_ipv6_transition_20120207_v2_0.pdf > Acesso em 29 de setembro de 2013.

Araujo, Bruno Oliveira; Almeida, Igor Sousa; Silva, Lucas Araújo. **IPv6 – Funcionalidade e métodos de transição.** Universidade de Salvador, 2011.

COMMER, Douglas E..**Interligação de redes com TCP/IP**. Vol.1, 5 ed. TraduçãoDaniel Vieira. Rio de Janeiro: Campus,2006.

COMMER, Douglas E..**Redes de Computadores e *Internet***. 4 ed. tradução Álvaro Strube de Lima. Porto Alegre: Bookman,2007.

CRUZ, Ademar. IPv6 – **Características**, 1999 Disponível em: < http://civil.fe.up.pt/acruz/Mi99/asr/Caracteristicas.htm>. Acesso em: 05 agosto 2013.

ECDYSIS. **Ecdysis: open-source implementation of a NAT64 gateway,** 2013 Disponível em http://ecdysis.viagenie.ca/download/ecdysis-nf-nat64-20101117.tar.gz >. Acesso em 10 setembro de 2013.

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

LAKATOS, Eva Maria; MARCONI, Marina de Andrade, **Fundamentos de metodologia científica**. 4. ed. rev. e ampl. São Paulo: Atlas, 2001.

GIRAFALES, Prof; **Pensador**, Disponível em: < http://pensador.uol.com.br/frase/NTM1MTU5/ >. Acesso em: 12 de outubro de 2013.

MOREIRAS, Antonio M., et al. **Técnicas de Transição do IPv4 para o IPv6**, 2012 Disponível em: <http://www.IPv6.br/download>. Acesso em: 26 julho de 2013.

PRAZER, Elisnaldo. **IPv4 versus IPv6, características, instalação e compatibilidade**. Professor orientador MSc. André Calazans Barreira. – Guará: [s. n.], 2007. 120f. : il.

(RFC791)J. POSTEL. **PROTOCOL SPECIFICATION**, 1981 Disponível em: < http://www.ietf.org/rfc/rfc791.txt >. Acesso em: 06 julho de 2013.

(RFC2460)S. DEERING. ***Internet* Protocol, Version6 (IPv6)**, 1998 Disponível em: < http://www.ietf.org/rfc/rfc2460.txt >. Acesso em: 03 setembro de 2013.

(RFC2694) P. Srisuresh. **DNS extensions to Network Address Translators (DNS_ALG),** 1999 Disponivel em < http://www.ietf.org/rfc/rfc2694.txt> . Acesso em 27 de setembro de 2013.

(RFC3315) R. Droms, Ed.. **Dynamic Host Configuration Protocol for IPv6 (DHCPv6)** 2003 Disponível em: < http://www.ietf.org/rfc/rfc3315.txt >. Acesso em: 20 de setembro de 2013.

(RFC3513) R. Hinden. ***Internet* Protocol Version 6 (IPv6) Addressing Architecture**, 2003 Disponível em: < http://www.ietf.org/rfc/rfc3513.txt >. Acesso em: 28 de julho de 2013.

(RFC3596) S. Thomson. **DNS Extensions to Support IP Version 6**, 2003 Disponível em: < http://www.ietf.org/rfc/rfc3596.txt >. Acesso em: 03 de setembro de 2013.

(RFC4861) T. Narten. **Neighbor Discovery for IP version 6 (IPv6)**, 2007 Disponível em: < http://www.ietf.org/rfc/rfc4861.txt >. Acesso em: 20 de junho de 2013.

(RFC4862) S. Thomson. **IPv6 *Stateless* Address Autoconfiguration** 2007 Disponível em: < http://www.ietf.org/rfc/rfc4862.txt >. Acesso em: 20 de setembro de 2013.

(RFC6052) C. Bao. **IPv6 Addressing of IPv4/IPv6 Translators,** 2010 Disponivel em < http://www.ietf.org/rfc/rfc6052.txt> . Acesso em 27 de setembro de 2013.

(RFC6147) M. Bagnulo. **DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers,** 2011 Disponivel em < http://www.ietf.org/rfc/rfc6147.txt> . Acesso em 26 de setembro de 2013.

(RFC6333) A. Durand. **Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion,** 2011 Disponível em: < http://www.ietf.org/rfc/rfc6333.txt >. Acesso em: 30 de setembro de 2013.

RODRIGUES A. **Porque não desabilitar o IPv6 no Windows ,** 2013 Disponível em http://blogs.technet.com/b/arturlr/archive/2012/09/20/porque-n-227-o-desabilitar-o-IPv6-no-windows-e-na-sua-rede.aspx >. Acesso em 01 de outubro de 2013.

SANTOS, Rodrigo R., et al. **Curso IPv6 básico**, 2010 Disponível em: <http://www.IPv6.br/download. Acesso em: 04 de maio de 2013.

SCRIMGER, Rob..**TCP/IP, A Bíblia.** Tradução Edson Furmankievicz. Rio de Janeiro: Campus,2002.

SILVEIRA, André Manoel da.**Rede IPv6 com integração IPv4.** Centro Federal de Educação Tecnológica de Santa Catarina. 2012.

TANENBAUM, Andrew S.. **Rede de Computadores.** Tradução VandenbergD. de Souza. Rio de Janeiro: Elsevier,2003.

TORRES, Gabriel..**Rede de Computadores, Curso Completo.** Axcel Books do Brasil Editora,2001.