Universidade de Brasília – UnB

Instituto de Ciências Exatas

Departamento de Ciência da Computação

Implantação e Análise do Protocolo IPv6 com Foco na Mobilidade

Democlydes Divino Pereira de Carvalho

Dissertação a apresentar como requisito parcial para conclusão do

Mestrado Profissional em Computação Aplicada

Orientador

Prof Dr. Eduardo Adilio Pelinson Alchieri

Brasília

2015

Universidade de Brasília – UnB
Instituto de Ciências Exatas
Departamento de Ciência da Computação
Mestrado Profissional em Computação Aplicada

Coordenador: Prof. Dr. Marcelo Ladeira

Banca examinadora composta por:

Prof. Dr. Eduardo Adilio Pelinson Alchieri (Orientador) — CIC/UnB
Prof. Dr. André Costa Drummond — CIC/UnB
Prof. Dr. Carlo Kleber da Silva Rodrigues – EXÉRCITO BRASILEIRO

CIP — Catalogação Internacional na Publicação

Carvalho, Democlydes Divino Pereira de

Implantação e Análise do Protocolo IPv6 com Foco na Mobilidade / Democlydes Divino Pereira de Carvalho: UnB, 2015.
200 p.: il.; 29,5 cm.

Dissertação (Mestrado) — Universidade de Brasília, Brasília, 2015.

1. IPv6, 2. *Internet*, 3. Mobilidade, 4. Pilha Dupla, 5. Análise de mecanismos.

C33li

Endereço: Universidade de Brasília
Campus Universitário Darcy Ribeiro — Asa Norte
CEP 70910-900
Brasília–DF — Brasil

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Implantação e Análise do Protocolo IPv6 com foco na Mobilidade

Democlydes Divino Pereira de Carvalho

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Prof. Dr. Eduardo Adilio Pelinson Alchieri (Orientador)
Departamento de Ciência da Computação

Prof. Dr. André Costa Drummond
Departamento de Ciência da Computação

Prof. Dr. Carlo Kleber da Silva Rodrigues
Exército Brasileiro

Prof. Dr. Marcelo Ladeira
Coordenador do Programa de Pós-graduação em Computação Aplicada

Brasília, 02 de julho de 2015

Dedicatória

Dedico este trabalho ao meu pai, grande mestre e exemplo de minha vida.

Agradecimentos

Agradeço a Deus por me guiar, de maneira incondicional, nos momentos que me exigiram sacrifícios pessoais.

Ao meu orientador, Prof. Dr. Eduardo Adilio Pelinson Alchieri, por ter acreditado em meu projeto, pela dedicação, confiança e ensinamentos no decorrer de todo o processo de orientação.

Agradeço de forma especial à minha esposa, Carla Andrade de Carvalho, por me apoiar e encorajar, sendo minha companheira nos bons e maus momentos, mantendo minha vontade sempre acesa, e filhos David e Danielle, que sempre souberam compreender minha ausência em função do esforço dedicado ao projeto.

Ao Prof. Dr. Marcelo Ladeira, por, além de coordenador do programa, ter sido um líder junto aos professores e alunos, dando um significado especial à nossa jornada.

Também meu agradecimento ao Prof. Dr. André Costa Drummond, pelo trabalho realizado junto aos alunos de Infraestrutura, proporcionando um ambiente adequado à pesquisa e desenvolvimento de nosso curso, sempre incentivando ao prosseguimento da missão.

Ao amigo Carlos Maurício de Borges Mello, por me apoiar e compartilhar o peso da caminhada pelo Mestrado em várias oportunidades de estudo e trabalho em conjunto.

Parágrafo especial, ao amigo e mentor, Prof. Dr. João Batista Simão, que plantou a semente acadêmica em minha mente e me fez despertar para a pesquisa e docência.

E, por fim, aos irmãos de farda do Exército Brasileiro, aos Chefes, em especial Cel Rodrigues e Cel Nunes que incentivaram e me permitiram partir em busca de meu objetivo e ao Tenente Fausto, colega de turma e demais companheiros da Seção de Redes do DGP, que estiveram firmes ao me apoiar, quando precisei me ausentar mais na conclusão de meu projeto.

“O insucesso é apenas uma oportunidade para recomeçar de novo com mais inteligência. ” (Henry Ford)

Resumo

A *Internet* tem crescido exponencialmente desde a sua implantação comercial em meados de 1980. A pilha de protocolo TCP / IP foi projetada para permitir a comunicação entre os *hosts* através de redes. Na sua versão 4, o protocolo IP foi capaz de suportar o crescimento da Internet até ao presente momento, mas o seu endereçamento de 32 bits está esgotado, e não há mais endereços disponíveis para uma redistribuição. Além deste fato, há o conceito de utilização de dispositivos com suporte a mobilidade, uma realidade que requer soluções robustas e acessíveis. Esse assunto é o cerne do desenvolvimento deste trabalho. O problema abordado nesta pesquisa é como implementar o protocolo IPv6 em uma rede corporativa, seguindo as normas, sem interferir com a sua capacidade operacional e fazer uso deste recurso de mobilidade, dando condições para alcançar uma otimização na transmissão de dados entre as Organizações Militares (OM), distribuídas por todo o país, realizando uma análise a respeito tanto a migração do IPv4 para o IPv6 nas infra-estruturas de rede do Exército Brasileiro, com foco em mobilidade no âmbito deste novo protocolo. Este trabalho pretende alertar os envolvidos nos setores brasileiros de tecnologia do Exército sobre o atraso atual em relação ao resto do mundo na adoção deste protocolo, estreitar o ponto sob conceitos de mobilidade para comunicação, seus laços dando uma atenção especial que com este aplicação, todo o pessoal poderia ser capaz de se conectar em diferentes organizações militares, usando suas credenciais de sua organização, permitindo que um único registro pode ser usado em diferentes pontos sem perda ou restrição de qualquer acesso aos serviços. Através do estudo e análise das normas e requisitos de transição do IPv4 para o IPv6, bem como o uso de IPv6 móvel, este estudo se concentra na identificação configurações físicas e lógicas que podem apoiar ou impedir a sua correta aplicação por meio de um ambiente simulado em uma organização específica exército brasileiro descrito como uma prova de conceito. Este ambiente teve uma análise topológica e verificação das métricas de *QoS* das aplicações instaladas sobre o meio ambiente e com isso foi possível avaliar a sua viabilidade e impacto sobre os ambientes envolvidos.

Palavras-chave: IPv6, *Internet*, Mobilidade, Pilha Dupla, Análise de mecanismos.

Abstract

The Internet has grown exponentially since its commercial deployment in the middle of 1980's. The stack of TCP / IP protocol was designed to enable communication between hosts over networks. In its version 4, the IP protocol was able to support the growth of the Internet until the present time, but its 32-bit addressability is exhausted, and there is no more addresses available to be redistributed. In addition to this fact there is the concept of using devices with mobility support, a reality that requires robust and affordable solutions. That subject is the core of the development of this work. The problem addressed in this research is how to deploy IPv6 protocol in a corporate network by following the standards, without interfering with its operational capacity and make use of this mobility feature, giving conditions to achieve an optimization in data transmission between the Military Organizations (OM), distributed all over the country, performing an analysis regarding both the migration from IPv4 to IPv6 in the Brazilian Army network infrastructures, focusing on under this new protocol mobility. This work intend to alert those involved in Brazilian Army technology sectors about the current delay in relation to the rest of the world in the adoption of this protocol, narrow the point under concepts of mobility to communication, their ties giving an special attention that with this implementation, all personnel could be able to connect in different military organizations, using their credentials from their organization, allowing a single register can be used in different points without loss or restriction of any access to services. Through the study and analysis of standards and requirements of transition from IPv4 to IPv6, as well as the use of mobile IPv6, this study is focused on identifying physical and logical configurations that may support or prevent the its correct implementation by using an simulated environment in an specific Brazilian Army organization described as a Proof of Concept. This environment had a topological analysis and verification of QoS metrics of applications installed on the environment and with this was possible to assess their feasibility and impact on the involved environments.

Keywords: IPv6 , *Internet* , Mobility, Dual Stack, mechanisms Analysis.

Sumário

Lista de Figuras

Lista de Tabelas

Abreviaturas e Siglas

AFRINIC - *African Network Information Center*

AP - *Access Point*

APF – Administração Pública Federal

ARIN - *American Registry for Internet Numbers*

AS - *Autonomous System*

APNIC - *Asia Pacific Network Information Centre*

ARPA – *Advanced Research Projects Agency*

BU - *Binding Update*

CIDR - *Classless Inter-Domain Routing*

CN - *Correspondent Node*

CoA - *Care-of Address*

CGI.br - Comitê Gestor da Internet no Brasil

DoD – *Department of Defense*

DHCP - *Dynamic Host Configuration Protocol*

DGP – Departamento-Geral do Pessoal

EB – Exército Brasileiro

ESP - *Encapsulating Security Payload*

FMIPv6 - *Fast Handover for Mobile IPv6*

FTP - *File Transfer Protocol*

HA - *Home Agent*

HIP - *Host Identity Protocol*

HMIPv6 - *Hierarchical Mobile IPv6*

HoA - *Home Address*

HTTP - *Hypertext Transfer Protocol*

IANA - *Internet Assigned Numbers Authority*

IEEE - *Institute of Electrical and Electronic Engineers*

IETF - *Internet Engineering Task Force*

IPng – *Internet Protocol Next Generetion*

IPv4 - *Internet Protocol Version 4*

IPv6 - *Internet Protocol Version 6*

IPSec - *Internet Protocol Security*

ISATAP - *Intra-Site Automatic Tunnel Addressing Protocol*

LACNIC - *Latin American and Caribbean IP Address Regional Registry*

LAN - *Local Area Network*

LISP - *Locator/ID Separation Protocol*

MAP - Mobility Anchor Point

MIP - Mobilidade IP

MIPV6 - Mobilidade IPv6

MN - *Mobility Node*

MTU - *Maximun Transmit Unit*

NAT - *Network Address Translation*

NCP - *Network Control Protocol*

NIC.br - *Núcleo de Informação e Coordenação do Ponto BR*

OM - Organizações Militares

OSI - *Open Systems Interconnection*

PDU - *Protocol Data Unit*

PMIPv6 - *Proxy Mobile IPv6*

PoC - *Proof of Concept*

QoS - Quality of Service

RFC - *Request For Comments*

RIPE NCC - *Réseaux IP Européens Network Coordination Centre*

RIR - *Regional Internet Registry*

ROAD - *ROuting and ADdressing*

SHIM6 - *Level 3 Multihoming Shim Protocol for IPv6*

SNMP - *Simple Network Management Protocol*

SSID - *Service Set Identifier*

TCP - *Transmission Control Protocol*

TI – Tecnologia da Informação

URL - *Uniform Resource Locator*

VLAN - *Virtual LAN*

VOIP - *Voice over IP*

WI-FI - *Wireless Fidelity*

1. Introdução

Neste capítulo é analisada a contextualização do problema de pesquisa, com sua delimitação. É apresentada também em qual justificativa se baseia a execução deste projeto, com a expectativa de contribuição ao ambiente estudado por meio do cumprimento aos objetivos que norteiam a dissertação.

1.1 Contextualização e Formulação do Problema

A demanda por redes de comunicação *wi-fi* segue crescendo, acompanhando a constante evolução da tecnologia. Para possibilitar que este aumento ocorra de forma progressiva foi proposto o novo protocolo IP (*Internet Protocol*), o IPv6, que apresenta, entre outras características, possibilidade de comunicação nativa entre redes fixas e móveis e o acesso à *Internet* a partir de uma rede sem fio, bem como a maior distribuição de endereços.

O conceito de mobilidade é requerido para variados tipos de dispositivos conectados a uma rede e, como consequência, vem a apresentar o problema de se endereçar dispositivos de forma simultânea em mais de uma rede, com o acréscimo de complexidade em se manter conexões e qualidade do serviço, não importando a posição e deslocamento de cada dispositivo.

O protocolo IP vem a ser o responsável pelo endereçamento e pela conexão dos dispositivos móveis à rede fixa. A versão que ainda predomina, o IPv4, possui endereçamento de 32 *bits*. O esgotamento dos endereços IP disponíveis é uma realidade e tendência irreversível, que já se apresenta como um problema global.

Para solucionar o problema dessa escassez, foi desenvolvida a versão 6 do protocolo IP, o IPv6. Com o seu lançamento, o Exército Brasileiro (EB), por meio de seus órgãos de Tecnologia da Informação (TI), busca se antecipar aos desafios, relativos à migração do IPv4 para o IPv6, especialmente no tocante à mobilidade.

A relativa novidade e a falta de conhecimento em torno do IPv6, leva a uma sequência de problemas de configuração, compatibilidade e desafios adicionais na implantação deste novo protocolo.

Em sua arquitetura, a mobilidade IP já está presente por meio da versão 4, ainda que, de forma não nativa. No IPv6, existe o conceito de mobilidade de forma nativa, com a implementação de otimização de rotas [1].

Prover endereçamento IPv6 válido aos dispositivos móveis não significa o efetivo uso de mobilidade. Por meio do uso de seus dispositivos em movimento, é preciso que se garanta conectividade ao usuário, sem a ocorrência de perda de conexão, de forma segura e transparente. Com o crescimento da demanda, novas propostas de mobilidade em ambientes implementados sobre IPv6 vão sendo apresentadas.

Neste contexto, este trabalho visa estudar algumas dessas propostas com vistas a evidenciar suas características e funcionalidades, obtendo como resultado, uma análise destes protocolos, em especial no que tange aos números de *QoS* (Qualidade de Serviço, do inglês *Quality of Service*) do ambiente e facilidade de implementação dos protocolos de mobilidade aplicados ao IPv6, abrindo caminho para o estudo de novas propostas que complementem e/ou melhorem as alternativas existentes.

1.1.1 *Problema de Pesquisa*

O problema abordado neste trabalho é como implantar o IPv6 numa rede corporativa seguindo as normas, sem interferir em sua capacidade operacional e fazer uso da mobilidade IPv6, dando condições de se alcançar uma transmissão de dados de com índices desejáveis de correção entre setores corporativos, aqui representados por Organizações Militares (OM) do Exército Brasileiro, distribuídas em determinadas faixas territoriais.

1.1.2 *Delimitação da pesquisa*

O presente trabalho se aplica ao Departamento-Geral do Pessoal (DGP), Órgão de Direção Setorial (ODS) do Exército Brasileiro (EB), que atua no Quartel General do Exército (QGEx), bloco E, 3º Piso, Setor Militar Urbano (SMU) - CEP 70.630-901 - Brasília-DF. O DGP tem como missão planejar, orientar, coordenar e controlar as atividades de pessoal decorrentes da Legislação de Pessoal vigente e do Sistema de Planejamento do Exército (SIPLEx), a fim de assegurar ao Exército Brasileiro condições para cumprir sua destinação constitucional e as atribuições subsidiárias explicitadas em Lei Complementar, e participar de Operações Internacionais.

Aqui não se busca a produção de um plano de implementação de mobilidade IPv6, com todas as características de projeto conforme descreve o Guia PMBOK [2], mas sim fornecer os quesitos para orientação de um experimento, através de análises de cenários

envolvendo a implantação do IPv6 em infraestrutura do EB. A criação de cenário proposta busca permitir o reuso de equipamentos e configurações para a consolidação do ambiente de mobilidade com a prova de viabilidade do modelo por meio de avaliação em ambiente experimental de rede confinada em laboratório, criando-se um *PoC* (*Proof of Concept*) no ambiente de produção da DGP, com base no modelo de referência técnica produzido neste trabalho.

1.1.3 *Justificativa*

Em 2011 os blocos remanescentes de endereço IPv4 foram distribuídos pelo *Internet Assigned Numbers Authority* (IANA) aos Registros Regionais de *Internet* (RIR). Com isto, um órgão como o Departamento-Geral do Pessoal (DGP) necessita montar, com antecedência, um plano de implantação de IPv6, para que venha a montar uma programação de atualizações e testes de laboratório, prevenindo a necessidade de gastos elevados com atualizações/implantações emergenciais e não programadas. Mudanças emergenciais também podem levar a erros e introduzir vulnerabilidades.

Mesmo havendo a implantação do IPv6 em função do esgotamento do IPv4, não haverá a desativação instantânea do protocolo. Haverá o processo de transição, onde IPv4 e IPv6 viverão mutuamente. Técnicas de transição já estão sendo experimentadas e aplicadas, conforme é apresentado neste trabalho.

Organizações já adotaram ou iniciaram o processo de adoção do IPv6. A *Internet Engineering Task Force* (IETF) desenvolveu mecanismos para dar suporte à coexistência do IPv4 e IPv6 e para mitigar a carga financeira da migração. Além disso, fabricantes de ativos de rede incorporaram o suporte para o IPv6 em produtos lançados no mercado.

O ambiente mais apropriado de adoção do IPv6 é o que se permite o uso duplo (IPv4 e IPv6) em todos os dispositivos por toda a organização [3]. Porém, o trajeto para conseguir uma instalação dupla da pilha dificilmente é o mesmo de organização para organização. Apesar das diferentes abordagens para se chegar ao estágio final, em todas as distribuições bem controladas devem constar abordagens de validação e teste de projetos realizados em laboratórios isolados e em seguida implantadas sistematicamente no ambiente da produção.

Um grande benefício da adesão ao IPv6 é a disponibilidade de um número extremamente maior de endereços se comparado ao IPv4. A alta disponibilidade de endereços e prefixos de rede fornece flexibilidade à arquitetura de rede possibilitando

organização hierárquica e geográfica. Além disso, o IPv6 tem suporte nativo do protocolo IPSec (*Internet Protocol Security*), bem como mecanismos de autenticação e encriptação.

O documento de referência do Governo Federal, denominado como e-PING (Padrões de Interoperabilidade de Governo Eletrônico) [4], determina que "os órgãos da Administração Pública Federal (APF) deverão se interconectar utilizando IPv4 e planejar sua futura migração para IPv6". Com isso, novas contratações e atualizações de redes devem prever suporte à coexistência dos protocolos IPv4 e IPv6 e a produtos que suportem ambos os protocolos.

O Comitê Gestor da *Internet* no Brasil, também aprovou e publicou recentemente uma nova resolução com recomendações sobre a implantação do IPv6 nas redes. Apontando os potenciais problemas ocasionados pelo atraso na implantação do protocolo e os principais pontos de atenção para a *Internet* brasileira [5] [6].

> Considerando que o atraso na disseminação do IPv6 dificultará sobremaneira a expansão sustentável da *Internet* e que, sem o IPv6 adequada e tempestivamente implementado surgirão diversos entraves na *Internet*, entre os quais notem-se:
>
> - Para usuários, uma experiência de navegação pior, eventual falha no funcionamento de serviços específicos como VoIP, jogos online, compartilhamento de arquivos *peer to peer*, streamings de vídeo etc.;
> - Para provedores de acesso *Internet*, uma complexidade maior em suas estruturas, com custos e complexidade crescentes;
> - Para provedores de conteúdo e serviços, necessidade de adaptação nos sistemas de autenticação baseados no endereço IP, em sistemas de geolocalização e medições de seus usuários e serviços;
> - Para segurança e estabilidade da *Internet*, dificuldade adicional na utilização de sistemas de segurança baseados em reputação dos IPs, como *blacklists*, e no uso do IPSec; e
> - Para desenvolvedores, eventual quebra da conectividade fim-a-fim, dificultando a inovação. [6]

Neste contexto, é imprescindível realizar uma análise a respeito tanto da migração do IPv4 para o IPv6 nas infraestruturas de rede do EB, com enfoque na mobilidade prevista neste novo protocolo. Tal análise também faz parte dos resultados obtidos das ações a realizar do PDTI 2011-2013 do DGP, no sentido de se apresentar as oportunidades de melhoria para o PDTI 2015-2016 [7].

O PDTI do DGP objetiva alinhar todas as ações desse Órgão de Direção Setorial (ODS) ligadas a Tecnologia da Informação (TI) ao determinado pelo Conselho Superior de Tecnologia da Informação (CONTIEX) [7].

Para o EB, instituição que vem, cada vez mais, fazendo uso e aprimorando sua infraestrutura de TI, o presente trabalho também dará respaldo à divulgação, no sentido de que se alerte para o atual atraso, em relação ao resto do mundo, na adoção do IPv6.

Devido à mobilidade implementada em IPv6, é possível que o militar se conecte em Organizações Militares diferentes, utilizando suas credenciais de sua OM de origem, permitindo uma flexibilidade de cadastro único para diferentes pontos sem perda de acesso aos serviços.

1.1.4 *Contribuição Esperada*

Este trabalho de pesquisa visa contribuir nos seguintes aspectos:

- A criação de um ambiente de rede experimental dentro do DGP, para estudo e avaliação do protocolo IPv6, na forma de prova de conceito;
- Realização de análises nesse ambiente, para o fornecimento de subsídios à implementação de método viável de migração do protocolo IPv4 para o IPv6 em ambiente de rede corporativo heterogêneo, com a avaliação das possibilidades de mobilidade, que possa servir de referência às OM do Exército;
- Avaliação de conjunto básico de protocolos, com métricas padronizadas e quantificação de resultados com possibilidade de comparação a outros ambientes.

1.2 Objetivos

1.2.1 *Objetivo geral*

O objetivo principal deste trabalho é implantar, como prova de conceito, o protocolo IPv6, com a implementação e a análise de mecanismo de suporte à mobilidade para o ambiente corporativo do Departamento-Geral do Pessoal, órgão de direção setorial do Exército Brasileiro.

1.2.2 *Objetivos específicos*

Visando atingir o objetivo geral, este trabalho se baseará no cumprimento dos seguintes objetivos específicos:

- Estudar e analisar os padrões e normas nacionais e internacionais relacionadas à transição IPv4 / IPv6, bem como o uso de mobilidade sobre IPv6;
- Identificar configurações físicas e lógicas que venham a suportar ou impedir a implementação adequada do protocolo IPv6;
- Implantar uma *PoC (*Prova de Conceito, do inglês *Proof of Concept)* para a realização do experimento, baseada no cenário topológico atual do DGP; e
- Analisar o ambiente com IPv6 implantado e o uso de mobilidade por meio de verificação de métricas de *QoS* de aplicações instaladas no ambiente.

1.3 Fases do Trabalho

Este projeto de pesquisa está dividido basicamente em quatro etapas:

1. Aprendizado do formato de implementação do protocolo IPv6 e definição de uma aplicação de mobilidade: Consiste na adaptação da configuração e topologia do DGP e na condução e teste de implementação dos conceitos de mobilidade ao escopo deste projeto. Estes dois processos são realizados em paralelo visto que um complementa o outro. Para definir a mobilidade é preciso ter conhecimento sobre quais informações são necessárias para o modelo de migração de protocolos de endereçamento de rede, por outro lado é preciso saber quais conceitos são englobados pela composição da rede de comunicação de dados para definir o modelo de mobilidade sobre IPv6.

2. Prova de Conceito:

Consiste na aplicação do modelo de migração definido aos membros da rede corporativa do DGP e na utilização da mobilidade para a agilização dos procedimentos de deslocamento nos seguimentos da EBnet.

3. Validação e Análise dos Resultados:

Após a implementação da migração em uma *PoC* e da implementação da mobilidade sobre o IPv6, estes são validados de forma a verificar a sua viabilidade, feito isso são analisados os resultados obtidos.

4. Escrita de artigo científico e do documento da dissertação:

O desenvolvimento de todas as etapas baseia-se em uma pesquisa bibliográfica e documental. Bibliográfica pois para a fundamentação teórico-metodológica do trabalho foram realizadas pesquisas sobre os seguintes assuntos: Redes TCP/IP sobre IPv4 e IPv6, migração de protocolos de endereçamento e técnicas de mobilidade. A pesquisa também é documental porque para atingir um dos objetivos deste trabalho foi necessário investigar

casos reais de aplicação do método de avaliação da rede, com a finalidade de validar o método de cálculo de mobilidade. O processo de trabalho deste projeto pode ser representado como na Figura 1.

.

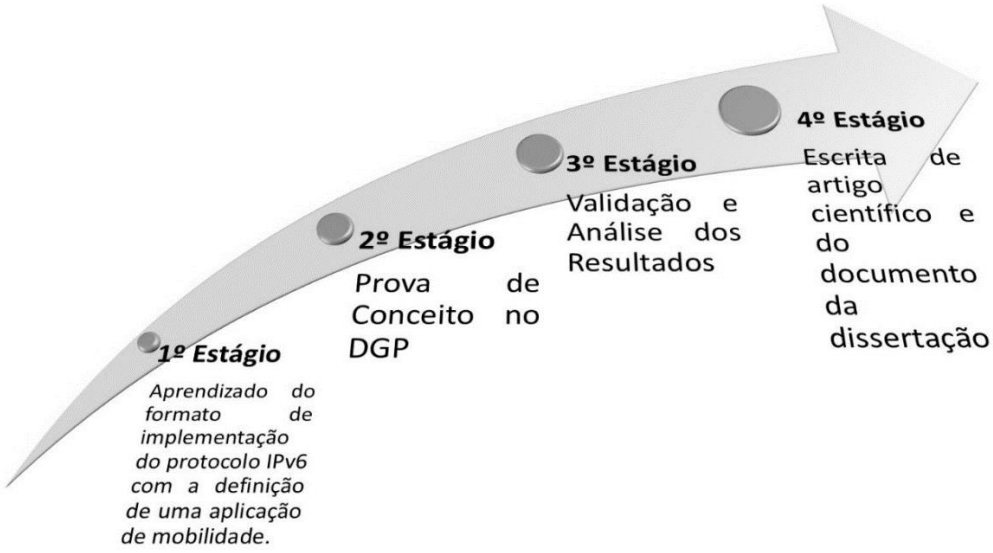


Figura 1 - Estágios do Projeto

1.4 Estrutura do Documento

O restante deste documento está organizado da seguinte forma:

- no Capítulo 2 é realizada uma introdução aos principais conceitos de *Internet*, arquitetura TCP/IP, Protocolos IPv4 e IPv6, Migração para IPv6 e formatos de implementação de Mobilidade sobre IPv6.
- o Capítulo 3 trata dos métodos de avaliação em redes de computadores, quais as métricas adequadas, os formatos de testes probatórios de qualidade e a observação de seus resultados.
- no Capítulo 4, são apresentadas observações realizadas a partir de outros trabalhos que trataram dos métodos e conceitos abordados nesta dissertação.
- no Capítulo 5 é apresentada a proposta de uma Prova de Conceito de migração para o protocolo IPv6 e implementação de mobilidade em ambiente formatado nos modelos do DGP com averiguação dos seus resultados, com validação e análise, destacando a viabilidade do modelo implementado;

- no Capítulo 6 são apresentadas as principais conclusões acerca do trabalho desenvolvido, incluindo sugestões de possíveis trabalhos futuros com novas implementações e expansões.

2. Fundamentação Teórica

Este capítulo discute os conceitos em que este projeto se baseia, descrevendo a base histórica e terminologias da arquitetura TCP/IP, com descrição das camadas de composição dessa referência, o protocolo IP em suas versões 4 e 6, as técnicas de transição entre esses protocolos e métodos de implementação de mobilidade, especialmente sobre o IPv6.

2.1. A *Internet* e o TCP/IP

O Departamento de Defesa (DoD – *Department of Defense*) do governo dos Estados Unidos da América iniciou em 1966, através de sua Agencia de Pesquisas e de Projetos Avançados (ARPA – *Advanced Research Projects Agency*), os estudos sobre o sistema de comunicação e controle distribuído com fins militares nomeado como ARPANET, objetivando formar uma arquitetura de rede sólida e robusta que pudesse trabalhar com os computadores e ligações de comunicação de maneira estável, mesmo com a queda de alguma estação. "Em 1969, são instalados os primeiros quatro nós dessa rede, localizados na Universidade de Los Angeles (UCLA), na Universidade da Califórnia em Santa Bárbara (UCSB), no Instituto de Pesquisas de Standford (SRI) e na Universidade de Utah" [5].

No início, essa rede funcionava com diversos protocolos de comunicação, com enfoque no NCP (*Network Control Protocol*). Já em janeiro de 1983, todas as máquinas da ARPANET, quando possuía um pouco mais de 550 *hosts*, passaram a adotar como padrão os protocolos TCP/IP ocasionando o crescimento ordenado da rede [5].

O protocolo IP foi definido para prover duas funções básicas [8]: a fragmentação, que permite o envio de pacotes maiores que o limite de tráfego estabelecido num enlace, dividindo-os em partes menores; e o endereçamento, que permite identificar destino e origem dos pacotes, por meio dos endereços armazenados no cabeçalho do protocolo [8]. A versão de protocolo IP utilizada desde aquela época até os dias atuais é a 4, comumente referenciada com o nome de IPv4. Apesar dessa versão se mostrar robusta, de fácil implantação e interoperabilidade, seu projeto original não previu alguns aspectos como: (1) o crescimento das redes com consequente esgotamento dos endereços IP; (2) o crescimento das tabelas de roteamento; (3) problemas de segurança dos dados transmitidos; e (4) aspectos de qualidade de serviço (prioridades) na entrega de pacotes específicos.

2.2. Arquitetura TCP/IP

Partindo do que vem a ser um protocolo, a sequência desta seção apresenta as camadas da arquitetura TCP/IP.

Protocolo é um conjunto de regras que definem uma comunicação. Como exemplo, o protocolo de *Internet* (IP) é a definição das regras que as máquinas devem possuir para realizar uma comunicação em nível de redes de computadores. O protocolo IP é definido na RFC[1] 791 [8].

2.2.1 *Camada de Aplicação*

Responsável por prover serviços, abstraindo a existência de comunicação entre processos em *hosts* diversos. No modelo TCP/IP, a Camada de Aplicação absorve as camadas de apresentação e sessão do modelo OSI (modelo de Interconexão de Sistemas Abertos, do inglês *Open Systems Interconnection model).* O PDU[2] relacionado à camada de aplicação é chamado de Mensagem [9].

2.2.2 *Camada de Transporte*

A camada de Transporte é responsável por receber os pacotes da camada de rede e remontar o dado original para enviá-lo à camada de aplicação, bem como receber a mensagem da camada de aplicação, encapsulá-la e enviar a camada de rede. A camada de transporte vem a ser a base da organização de protocolos ordenadamente. Com a função de prover o transporte econômico e confiável de dados, independentemente da rede física ou das redes atualmente em uso, a camada inclui controle de fluxo, ordenação dos pacotes e correção de erros, informando ao transmissor, com uma mensagem de recebimento, que o pacote foi recebido com sucesso. O PDU desta camada é chamado Segmento [9].

---

[1] RFC (*Requests for Comments*) são usadas pela comunidade Acadêmica e científica na definição de novos padrões para Rede [9].

[2] *Protocol Data Unit* (Unidade de Dados de Protocolo) descreve um bloco de dados que é transmitido entre duas instâncias da mesma camada. Cada camada recebe a PDU da camada superior como um bloco de dados, adiciona seus cabeçalhos (e em alguns casos, rodapés) de controle, criando a sua própria PDU, num processo chamado de encapsulamento. Embora seja comum o uso do termo "Pacote" para todas as informações trocadas numa rede, este termo só deve ser aplicado para as PDUs de camada de Rede [9].

2.2.3 *Camada de Rede*

Responsável por mover pacotes entre dispositivos, através do fornecimento da comunicação entre computadores que existem em diferentes redes. Tem como uma das principais funções desempenhadas o roteamento. A camada de rede controla a operação da sub-rede, decidindo qual caminho físico os dados devem seguir com base nas condições da rede, na prioridade do serviço e em outros fatores. A Camada de Rede fornece roteamento, controle de tráfego da sub-rede, fragmentação de quadros, mapeamento de endereços lógicos-físicos e contabilidade de uso da sub-rede. Os protocolos IPv4 e IPv6, estudados no contexto deste trabalho, fazem parte da composição da camada de rede. O PDU desta camada é geralmente conhecido como Datagrama [9].

2.2.4 *Camada de Enlace*

Aborda algoritmos que permitem uma comunicação eficiente e confiável entre dois computadores adjacentes em nível da camada de enlace de dados (adjacentes no sentido de estarem fisicamente conectadas). Possui controle, tanto de software para a placa de rede, quanto de firmware ou chipsets especializados, que executam as funções da camada de enlace de dados, que são: (1) adicionar um *header* de pacote para prepará-lo para transmissão; (2) transmitir o quadro através da camada física; (3) receber os quadros; (4) retirar os *headers* adicionados; e (5) encaminhar os pacotes para a camada de rede. O PDU desta camada é conhecido como Quadro [9].

2.3. O Protocolo IPv4

Os serviços da camada de rede do modelo TCP/IP, implementados por seu conjunto de protocolos, constituem o *Internet Protocol* (IP). Ainda hoje, o IPv4 é a versão mais utilizada de IP, sendo o único protocolo da camada de rede que carrega dados de usuários por meio da *Internet*.

A elaboração do protocolo não foi concentrada nas funções de rastreamento e gerenciamento do tráfego dos pacotes. Estas funções são realizadas por protocolos das camadas superiores, com suporte do TCP. Possui características básicas como ser sem conexão, baseado no melhor esforço, não confiável e independente de meios físicos [8].

2.3.1 *Cabeçalho de Pacote IPv4*

Conforme mostra a Figura 2, o protocolo IPv4 define uma série de campos no cabeçalho do pacote. Eles têm sua representação em binários para que os serviços IPv4 possam se referenciar quando fazem o envio pacotes por meio da rede [8].

<table>
<tr><td>Versão</td><td>IHL</td><td>Tipo de Serviço (ToS)</td><td colspan="2">Tamanho Total</td></tr>
<tr><td colspan="3">Identificação</td><td>Flags</td><td>Fragmentação</td></tr>
<tr><td>Tempo de Vida (TTL)</td><td colspan="2">Protocolo</td><td colspan="2">Verificação de Erros do Cabeçalho</td></tr>
<tr><td colspan="5">Endereço de Origem</td></tr>
<tr><td colspan="5">Endereço de Destino</td></tr>
<tr><td colspan="5">Opções (Extensões)</td></tr>
</table>

Figura 2 - Campos do Cabeçalho do Pacote IPv4 [9]

A seguir, os campos do cabeçalho no protocolo são descritos [8]:

- **Versão:** 4 bits. A versão é a 4.
- **IHL (Comprimento do Cabeçalho *Internet,* do inglês *Internet Header Length*):** Informa o comprimento do cabeçalho *Internet* em palavras de 32 bits (4 octetos ou 4 bytes).
- **TOS (Tipo de Serviço, do inglês *Type of Service*):** É utilizado para indicar o *QoS* (Qualidade de Serviço, do inglês *Quality of Service*).
- **Tamanho Total:** Informa o comprimento do datagrama, em octetos (bytes). O tamanho máximo do datagrama pode ser 65.535 octetos (64 kB).
- **Identificação**: Número de identificação do datagrama para permitir que o destino remonte os datagramas.
- ***Flags* (Sinalizadores)**: Bits que identificam a transmissão de sinais de controle.
- ***Flag* Mais Fragmentos:** é um único *bit* no campo *Flag* usado com o Deslocamento de Fragmentos na fragmentação e reconstrução de pacotes.
- ***Flag* Não Fragmentar:** É um único *bit* no campo *Flag* que indica que a fragmentação do pacote não é permitida. Com o *bit* da *flag* configurado como "Não Fragmentar", não permite a fragmentação do pacote [9].

- **Deslocamento de Fragmento:** na fragmentação, o pacote IPv4 usa o campo Deslocamento de Fragmento e a *flag* MF no cabeçalho IP para reconstruir o pacote quando o mesmo chega ao *host* de destino.
- **Tempo de Vida:** valor binário de 8 *bits* que indica o "tempo de vida" restante do pacote, que diminui em, ao menos, um a cada vez que o pacote é processado por um roteador (ou seja, a cada salto). Chegando a descrição desse valor igual a zero, o roteador se desligará do pacote (descartando-o ou abandonando-o) o retirando do tráfego de dados.
- **Protocolo:** valor binário de 8 *bits* que indica o tipo de *payload* de dados que o pacote está carregando. Este campo possibilita que a camada de rede passe os dados para o protocolo apropriado das camadas superiores.
- **Verificação de erros do Cabeçalho):** 16 bits. Esse *checksum* é calculado somente sobre o cabeçalho IP. Como alguns campos mudam frequentemente, como o TTL, esse valor tem que ser recalculado [10].
- **Endereços de Destino:** contêm um valor binário de 32 *bits* que representa o endereço do *host* de destino do pacote da camada de rede.
- **Endereço de Origem:** contém um valor binário de 32 *bits* representando o endereço do *host* de origem do pacote da camada de rede.
- **Opções:** Tamanho variável, entre 0 e 320 bits (40 octetos). O que é opcional é a transmissão ou não desse campo, não a implementação. Todo os roteadores e *gateways* devem implementar meios de codificação/decodificação desse campo. Pode haver mais de uma opção nesse campo [8].

2.3.2 *Endereçamento no IPv4*

Ao protocolo IPv4 são reservados 32 *bits* para o endereçamento, permitindo gerar mais de 4 bilhões de endereços distintos. Inicialmente, conforme mostra a Tabela 1, estes endereços foram divididos em três classes de tamanhos fixos da seguinte forma [8]:

- Classe A: definia o *bit* mais significativo como 0, utilizava os 7 *bits* restantes do primeiro octeto para identificar a rede, e os 24 *bits* restantes para identificar o *host*. Esses endereços eram determinados dentro da faixa de 1.0.0.0 até 126.0.0.0;
- Classe B: tem seus dois *bits* mais significativos como 10, utilizando os quatorze seguintes para identificar o endereçamento da rede, deixando os dezesseis *bits*

restantes identificando os endereços de *host*. Esses endereços estavam contidos dentro da faixa de 128.1.0.0 até 191.254.0.0; e

- Classe C: definia os 3 *bits* mais significativo como 110, utilizava os 21 *bits* seguintes para identificar a rede, e os 8 *bits* restantes para identificar o *host*. Esses endereços utilizavam a faixa de 192.0.1.0 até 223.255.254.0.

Tabela 1 – Classes de Endereçamento IPv4

Classe	Formato	Redes	*Host*
A	7 *bits* de Rede, 24 *bits* de *Hosts*	128	16.077.216
B	14 *bits* de Rede, 16 *bits* de *Hosts*	16.384	66.536
C	21 *bits* de Rede, 8 *bits* de *Hosts*	2.097.152	256

A classe A atendia um número pequeno de redes e ocupava metade de todos os endereços disponíveis por rede, enquanto que a classe C permitia criar muitas redes, só que, com poucos endereços disponíveis [5].

2.3.3 *Esgotamento do IPv4 e Busca de um Novo Protocolo*

Conforme dados extraídos de [3], abaixo é apresentada uma breve discussão a respeito da evolução da utilização dos endereços do protocolo IPv4.

- No segundo trimestre de 1992, tendo como motivo o crescimento da *Internet* e da política de distribuição de endereços, 38% das faixas de endereços classe A, 43% da classe B e 2% da classe C, já estavam alocados.
- Sendo criado o protocolo HTTP, em 1993, e a liberação, por parte do Governo dos EUA, para a utilização comercial da *Internet*, a rede cresceu de 2.056.000 de *hosts* em 1993, para mais de 26.000.000 de *hosts* em 1997.

Na Figura 3, retirada do site de Geoff Huston, onde publica estudos sobre o esgotamento do IPv4, o cientista chefe do APNIC (Registro Regional de IPs para a região da Ásia e Pacífico), ilustra o acelerado esgotamento do endereçamento IPv4 [3]. Na sequência é descrito um pouco sobre a atividade de cada ator envolvido no controle e distribuição de endereçamentos IP.

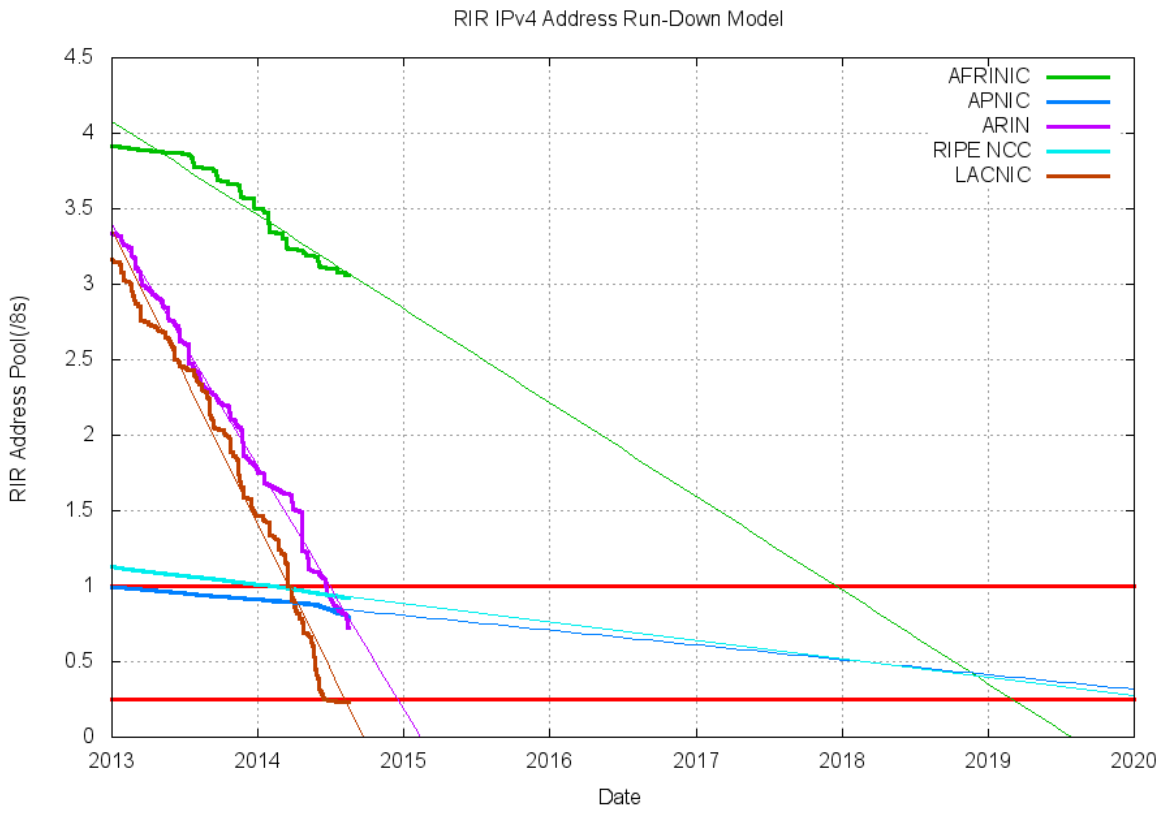


Figura 3 – Modelo de Esgotamento de Endereçamento IPv4 [3]

2.3.3.1 Registros Regionais da Internet - RIRs

Para melhor compreensão, Registros Regionais da *Internet* (do inglês *Regional Internet Registries* (RIRs)) são corporações sem fins lucrativos que administram e registram espaço de endereçamento de IP e números de Sistemas Autônomos (do inglês *Autonomous System* (AS)) dentro de uma região definida.

RIRs também trabalham em projetos comuns e são assim descritos:

(1) AFRINIC, que abrange a África e porções do Oceano Índico;

(2) APNIC, que abrange porções da Ásia e Oceania;

(3) ARIN, que abrange os EUA, Canadá, Caribe e ilhas do Atlântico Norte;

(4) LACNIC, que abrange a América Latina e porções do Caribe; e

(5) RIPE NCC, que vem a abranger a Europa, Oriente Médio e Ásia Central.

A Figura 4 mostra as suas áreas de atuação de cada uma.

Registry	Area Covered
AFRINIC	Africa Region
APNIC	Asia/Pacific Region
ARIN	North America Region
LACNIC	Latin America and some Caribbean Islands
RIPE NCC	Europe, the Middle East, and Central Asia

Figura 4 - Áreas de Atuação dos RIRs [11]

Os RIRs alocam os blocos IPs para os seus membros regionais ou LIR (Local *Internet* Registries), tais como o NIC/br responsável no Brasil, que por sua vez designa IPs para: Provedores de Serviços *Internet*, (ISPs); Organizações de Telecomunicações; Grandes Corporações; e até para usuários finais [10].

2.3.3.2 Comitê Gestor da Internet no Brasil - CGI.br

Criado em maio de 1995 pela Portaria Interministerial Nº 147 de 31/05/1995, alterada pelo Decreto Presidencial Nº 4.829 de 03/09/2003 é responsável pela coordenação e integração dos serviços *Internet* no país. Segue um modelo *multistakeholder* composto por membros do governo, e membros eleitos dos setores empresarial, terceiro setor e da comunidade acadêmica. O CGI.br não é órgão do governo e não tem personalidade jurídica.

O Comitê tem, como principais atribuições: fomentar o desenvolvimento de serviços *Internet* no Brasil; recomendar padrões e procedimentos técnicos operacionais para a *Internet* no Brasil; coordenar a atribuição de endereços *Internet* (IPs) e o registro de nomes de domínios usando **.br**; coletar, organizar e disseminar informações sobre os serviços *Internet* – indicadores e estatísticas [5].

2.3.3.3 Núcleo de Informação e Coordenação do Ponto BR - NIC.br

É uma entidade civil, sem fins lucrativos, criada em 2003 e começando a atuar em 2005, sob delegação do CGI.br. Possui um Conselho de Administração composto por 7 membros, sendo 3 do governo, escolhidos entre os componentes do CGI.br e 4 do setor privado indicados pelo CGI.br. A Assembleia Geral é formada pelo pleno do CGI.br e o NIC.br é um braço executivo do Comitê Gestor da *Internet* no Brasil, que coordena as atividades do Registro, do CERT, do CETIC e do CEPTRO, além de abrigar o escritório W3C Brasil [5].

A Figura 5, ilustra a disposição organizacional desses órgãos dentro do Governo Federal e Sociedade Civil. Com a seguinte distribuição de módulos:

1 – Min. da Ciência e Tecnologia
2 – Min. das Comunicações
3 – Casa Civil da Presidência da República
4 – Min. do Planejamento, Orçamento e Gestão
5 – Min. do Desenvolvimento, Indústria e Comércio Exterior
6 – Min. da Defesa
7 – Agência Nacional de Telecomunicações
8 – Conselho Nacional de Desenv. Científico e Tecnológico
9 – Conselho Nac. Secretários Estaduais p/ Assuntos de Ciência e Tecn.
10 – Notório Saber
11 – Provedores de acesso e conteúdo
12 – Provedores de infra de telecom
13 – Indústria TICs e software
14 – Empresas usuárias
15 – Terceiro setor
16 – Terceiro setor
17 – Terceiro setor
18 – Terceiro setor
19 – Academia
20 – Academia
21 – Academia

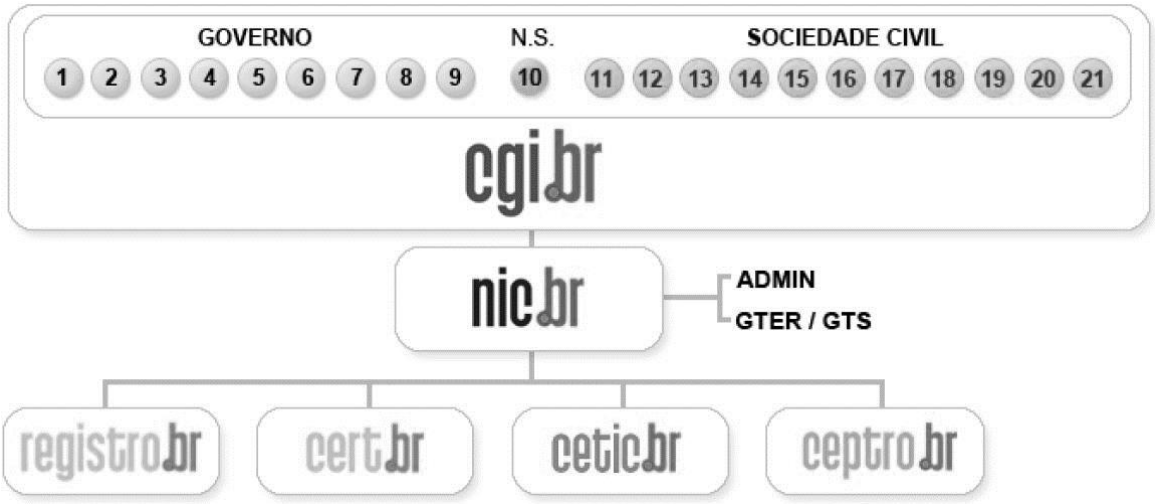


Figura 5 - Composição Organizacional do CGI.br e NIC.br [5]

2.3.3.4 Estratégias de Redução de Impacto em Virtude do Esgotamento do IPv4

A IETF, diante do cenário descrito anteriormente, passou a discutir estratégias para solucionar a questão do esgotamento dos endereços IP e do aumento da tabela de roteamento. No fim do ano de 1991, o grupo de trabalho ROAD (*ROuting and ADdressing*) teve sua formação oficializada, vindo a apresentar, como solução, o uso do CIDR (*Classless Inter-domain Routing*) [5].

Definido por meio da RFC 4632 [12], o CIDR, ou roteamento inter domínio sem classes, se baseia no fim do uso de classes de endereços, permitindo a alocação de blocos de

tamanho necessários de cada rede e a agregação de rotas, reduzindo o tamanho da tabela de roteamento. A técnica foi desenvolvida nos anos de 1990 como um esquema padrão de roteamento do tráfego de redes através da *Internet*. Em tal esquema, o valor de um endereço IP determina suas sub-redes para o propósito de roteamento [10].

Outra solução, proposta na RFC 2131 [13], foi o protocolo DHCP (*Dynamic Host Configuration Protocol*). Através deste protocolo, um *host* é capaz de obter um endereço IP automaticamente e adquirir informações de máscara de sub-rede, endereço do roteador padrão e endereço do servidor DNS local.

Outra técnica paliativa foi o desenvolvimento da NAT (*Network Address Translation*). Definida na RFC 3022 [14], permite que vários *hosts* possam trafegar na *Internet*, por meio de um único endereço IP, ou um pequeno número deles. Dentro de determinada rede, cada *host* recebe um endereço IP privado único, que é utilizado para o roteamento do tráfego interno e, quando um pacote precisa ser roteado para fora da rede, uma tradução de endereço é realizada, convertendo endereços IP privados em endereços IP públicos globalmente únicos.

Foram definidos três intervalos de endereços IP como privados [15], e nenhum pacote contendo estes endereços pode trafegar na *Internet* pública. As faixas reservadas foram 10.0.0.0 a 10.255.255.255 /8, com 16.777.216 *hosts*; 172.16.0.0 a 172.31.255.255 /12, com 1.048.576 *hosts*; e 192.168.0.0 a 192.168.255.255 /16, com 65.536 *hosts*.

A utilização da NAT permitiu a economia de endereços IP, simplificação da numeração interna das redes e transparência em relação à topologia das redes [5]. Porém a NAT interfere no modelo fim-a-fim da *Internet*, sem conexões diretas entre dois *hosts*, e infere baixa escalabilidade, além de exigir grande poder de processamento do dispositivo tradutor. A NAT, em adição, impossibilita o rastreamento de pacotes e dificulta a utilização de técnicas de segurança, como IPSec.

Mesmo com as medidas adotadas, somente a quantidade de equipamentos móveis capazes de acessarem a *Internet*, como celulares, *smartphones*, *netbooks* e *modems* 3G, podem chegar a 2,25 bilhões de aparelhos, ainda antes de 2015, segundo dados da *ABI Research* [10].

A adoção de técnicas, como as anteriormente citadas, reduziu em apenas 14% a quantidade de blocos de endereços solicitados à IANA [5]. Desta forma, através da RFC 1550 [16], a IETF formalizou pesquisas para uma nova versão do protocolo IP, em dezembro de 1993, solicitando o envio de projetos e propostas. O grupo de trabalho da IETF foi denominado *Internet Protocol next generation (IPng)* e as principais questões abordadas na

elaboração da próxima versão do protocolo IP deveriam ser: escalabilidade; segurança; configuração e administração de rede; suporte a *QoS;* mobilidade; políticas de roteamento; e transição [17].

Projetos de composições diversas vieram a levantar os resultados do crescimento da *Internet*. Foram projetos como o CNAT, o *IP Encaps*, o Nimrod e o *Simple* CLNP, o *TCP and UDP with Bigger Addresses* (TUBA (evolução do *Simple* CLNP)), e o *IP Address Encapsulation* (IPAE (evolução do *IP Encaps)*). Alguns meses depois foram apresentados os projetos *Paul's Internet Protocol (PIP),* o *Simple Internet Protocol* (SIP) e o TP/IX. Uma nova versão do SIP, que englobava algumas funcionalidades do IPAE, foi apresentada antes de agregar-se ao PIP, resultando no *Simple Internet Protocol Plus* (SIPP) [17].

A recomendação final para o novo protocolo IP baseou-se em uma versão revisada do SIPP, que passou a incorporar endereços de 128 *bits*, com os elementos de transição e autoconfiguração do TUBA, o endereçamento baseado no CIDR e os cabeçalhos de extensão, vindo a nomeação "IPv6" passando a ser oficialmente usada [17].

2.4. O Protocolo IPv6

O objetivo do IPv6 não foi apenas realizar mudanças no tamanho do endereçamento, mas também a implementação de um novo protocolo, com um novo cabeçalho e novas funcionalidades.

2.4.1 *Fatores Promovem a Lentidão da Adoção do IPv6*

A demora na adoção do IPv6 ocorre principalmente pela necessidade de investimento em serviços e na substituição de equipamentos, principalmente nos *Backbones* das operadoras de telefonia e provedores de *Internet*. Para contornar esta necessidade eminente, fabricantes como Cisco implantaram o protocolos *Carrier Grade NAT*44 [18] em seus equipamentos, que permite o uso de NAT na borda da rede, capacitando um Sistema Autônomo a trabalhar inteiramente com endereços inválidos, o que permite postergar ainda mais a migração para o IPv6, preservando investimentos feitos com os equipamentos existentes e postergando a necessidade de mudanças nos equipamentos, mas ao mesmo tempo impedindo que usuários alcancem outras vantagens oriundas deste novo protocolo.

Neste contexto, os governos e órgãos responsáveis pela distribuição de endereços estão tomando algumas atitudes. No Brasil o incentivo para implantação do IPv6 é realizado

pelo Núcleo e Informação e Coordenação do Ponto BR (NIC.br), através de treinamentos e eventos, estimulando as instituições a solicitarem blocos de endereços IPv6 [5].

O tráfego de *Internet* no Brasil em IPv6 chegou a marca de 2% no mês de junho de 2015, revelando um crescimento maior no ano de 2015, em relação aos anteriores. Como pode ser observado na Figura 6 [19].

De acordo com os dados levantados para o monitoramento realizado pela Cisco sobre a adesão de IPv6 em escala mundial, em janeiro de 2015 era de 0,11%, com um salto para 1% no final do mês de março, chegando a 2% em junho [19], gerando a expectativa de aumento no número de tráfego em protocolo IPv6.

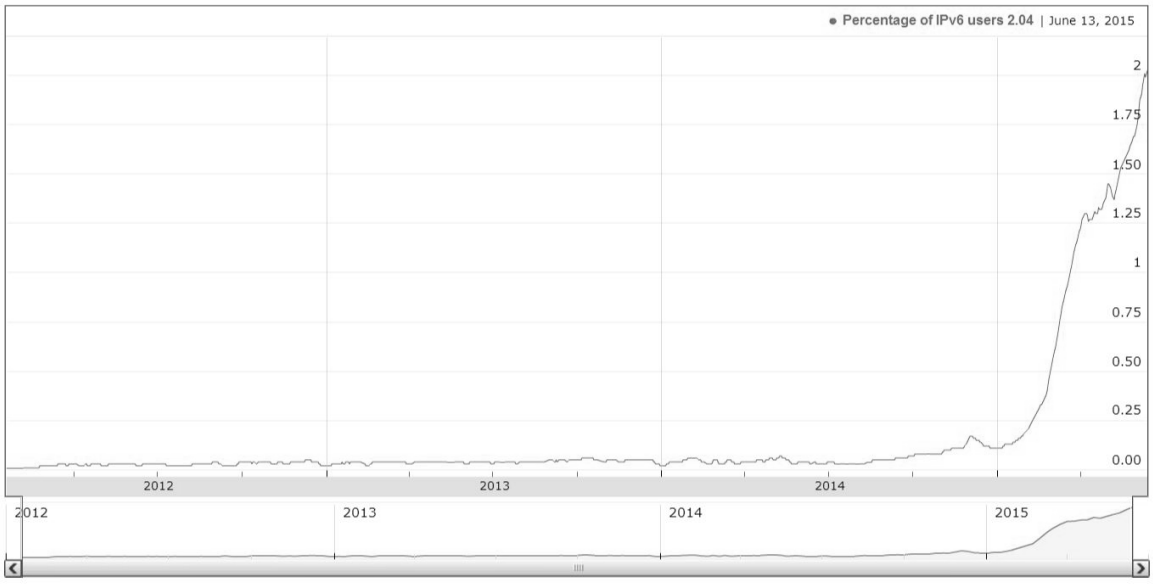


Figura 6 - Percentual de usuários IPv6 no Brasil [19]

Ilustrando melhor a expectativa de crescimento, a Bélgica tem 32,3 de seu tráfego em IPv6, os Estados Unidos possuem 18,3%, a Alemanha tem 14,3%, Portugal 11,3% e o Japão tem a marca de 6,8%. A Figura 7 ilustra a distribuição de tráfego IPv6 no Globo [19].

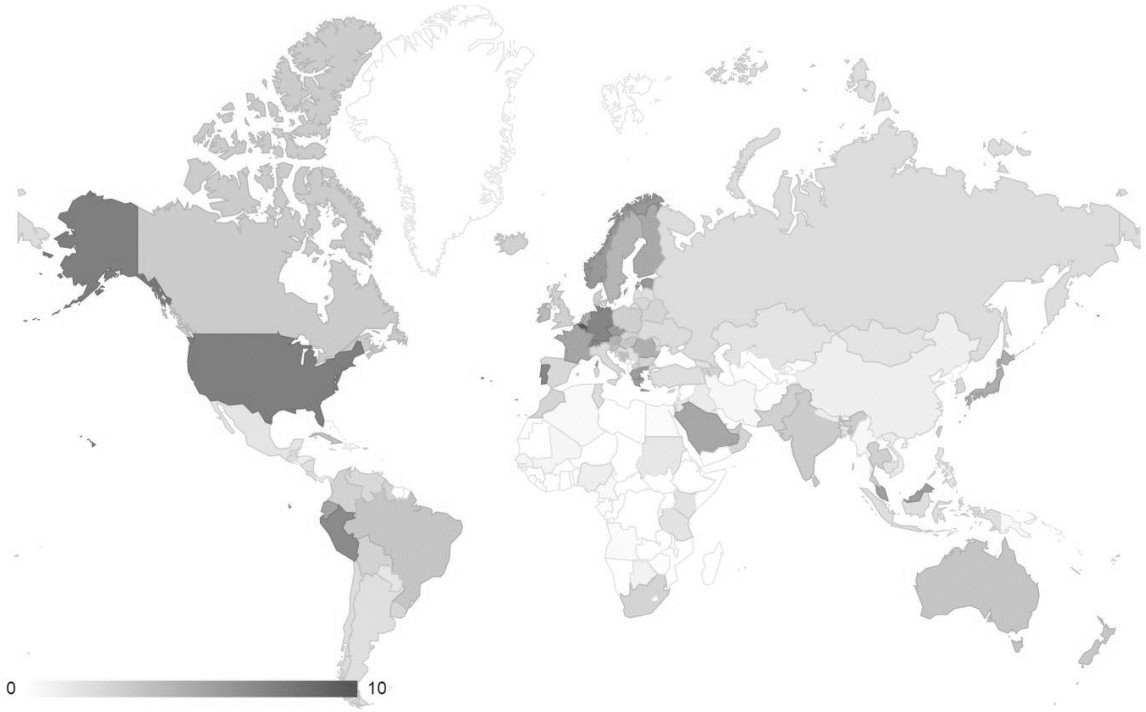


Figura 7 - Tráfego IPv6 no Mundo [19].

2.4.2 *Cabeçalho de Pacote IPv6*

O cabeçalho IPv6 ficou mais simples em relação ao IPv4, pois apesar do aumento em quatro vezes no seu tamanho de endereçamento, seu cabeçalho possui apenas o dobro de tamanho. Para isto alguns campos foram retirados e outros tiveram seus nomes alterados. Cinco campos do cabeçalho IPv4 foram removidos do cabeçalho IPv6 [20]:

header length: o cabeçalho IPv6 tem tamanho fixo de 40 bytes;

identification, flags e fragment offset: informação de fragmentação não aparece no cabeçalho IPv6, uma vez que existe o cabeçalho de extensão *Fragment,* específico para quando a fragmentação for necessária;

header checksum: foi removido para melhorar a velocidade de processamento dos pacotes IP. Além disso, a detecção de erros no nível de bit é realizada pela camada de enlace, assim como existe *checksum* na camada de transporte UDP e TCP.

A Tabela 2 demonstra os campos que tiverem seus nomes alterados.

Tabela 2– Diferenças do cabeçalho IPv4/IPv6

IPv4	IPv6
Tipo de Serviço	Classe de Tráfego
Tamanho Total	Tamanho de Dados
Tempo de Vida (TTL)	Limite de Encaminhamento
Protocolo	Próximo Cabeçalho

A grande alteração em comparação ao IPv4 está no uso dos cabeçalhos de extensão. No IPv4 todas as informações do pacote estavam em um cabeçalho de tamanho fixo. No IPv6, havendo necessidade, múltiplos cabeçalhos de extensão podem ser incluídos em um único pacote, onde cada cabeçalho de extensão possui um campo próximo cabeçalho, que pode ser ou não processado pelos nós intermediários de uma rede. O cabeçalho IPv6 ficou com a estrutura apresentada na Figura 8:

- **Versão** (4 bits): indica a versão do protocolo IP, no caso de IPv6 o número é 6;
- **Classe de Tráfego** (1 byte): indica a classe ou prioridade do pacote IPv6;
- **Identificador de Fluxo** (*Flow Label***)** (20 bits): indica que este pacote pertence a uma sequência específica de pacotes entre uma origem e um destino, exigindo tratamento especial pelos roteadores IPv6 intermediários;
- **Tamanho da Carga de Dados** (*Payload Length*) (2 bytes): indica o comprimento da carga do pacote IPv6, o que inclui os cabeçalhos de extensão e a unidade de dados da camada superior;
- **Próximo Cabeçalho (***Next Header*) (1 byte): indica qual é o próximo cabeçalho após o cabeçalho base IPv6, podendo ser tanto os cabeçalhos de extensão como os protocolos da camada superior, como TCP, UDP ou ICMPv6;
- **Limite de Saltos (***Hop Limit*) (1 byte): indica o número máximo de saltos que o pacote IPv6 pode dar antes de ser descartado;
- **Endereço de Origem (***Source Address*) (16 bytes): armazena o endereço IPv6 da máquina origem; e
- **Endereço de Destino (***Destination Address*) (16 bytes): armazena o endereço IPv6 da máquina destino.

Figura 8– Cabeçalho IPv6 [9]

Segundo a RFC 2640 [21], os cabeçalhos de extensão definidos são:

- ***Hop-by-Hop*:** informa aos roteadores a necessidade de analisar o restante dos cabeçalhos de extensão. Não havendo o cabeçalho, o pacote é encaminhado diretamente ao seu destino;
- ***Destination Options*:** utilizado em pacotes enviados por um nó móvel, enquanto fora de sua rede, para informar ao destinatário seu *home address*;
- ***Routing Header:*** era utilizado para definir por quais saltos que o pacote deverá passar antes de chegar ao seu destino. Se tornou um problema de segurança e, por consequência, obsoleto [22];
- ***Fragmentation:*** informações sobre pacote fragmentado, como a posição do fragmento atual em relação ao pacote original;
- ***Authentication Header:*** utilizado para a implementação de IPSec sobre IPv6; ***e***
- ***Encapsulation Security Payload Header (ESP):*** usado para garantir a confidencialidade, autenticidade da origem dos dados e integridade da conexão.

A Figura 9 ilustra a ordem dos cabeçalhos de extensão em um pacote IPv6, onde se pode observar que o cabeçalho de extensão *destination options* aparece em dois lugares [20]:

(1) para ser analisado por nós intermediários, quando o cabeçalho *Routing* estiver presente: e

(2) para ser analisado pelo destino final do pacote.

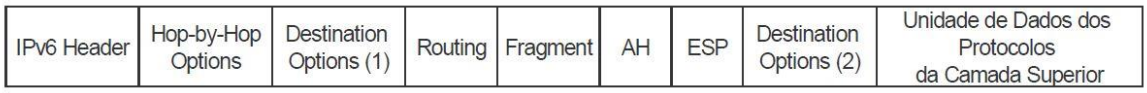


Figura 9 - Ordem dos Cabeçalhos de Extensão no IPv6 [20]

Também surgiram características e funcionalidades como: Descoberta de Vizinhança; Descoberta Automática do *Maximun Transmit Unit* (MTU); alteração no protocolo de roteamento RIP para RIPng [23]; OSPFv3 [24] ; DHCPv6 [25] ; endereços com 128 *bits* de tamanho; autoconfiguração ("*plug and ping*"); implementação de IPSec "mandatório"; e melhor suporte para *Mobile* IP que o IPv4, além da criação de um cabeçalho mais simples, em que, apesar do endereçamento ser 4 vezes maior, o cabeçalho é apenas 2 vezes maior.

2.4.3 *Fragmentação no IPv6*

No IPv6, diferentemente do IPv4, a fragmentação é assim interpretada pelos hosts: os roteadores não têm que processar ou considerar a fragmentação; e somente o nó de destino necessita lidar com a remontagem dos fragmentos.

O Path MTU é descoberto dinamicamente pela técnica padronizada, "Path MTU Discovery", através de mensagens do Protocolo ICMPv6 e a descoberta do Path MTU suporta destinos *Unicast* assim como *Multicast* [10].

2.4.4 *O Protocolo ICMPv6*

O ICMPv6 tem fator crucial no funcionamento IPv6. Ele está localizado logo após o cabeçalho do IPv6 e suas extensões, possui apenas quatro campos (tipo, código, *checksum* e dados), mas sua importância está relacionada com os tipos de mensagens possíveis [26]:

As mensagens de erros possuem as seguintes funcionalidades:

- *Destination Unreachable* - problemas em localizar destino;
- *Packet Too Big* - tamanho do pacote maior que o MTU;
- *Time Exceeded* - limite de encaminhamento; e
- *Parameter Problem* - problema em algum campo dos cabeçalhos do IPv6.

Já as mensagens de informações contêm os conhecidos *Echo Request* e *Echo Reply* utilizados pelo comando *ping*. Todas estas mensagens são definidas entre o tipo 1 e o tipo 129 do pacote ICMPv6, as diferenças estão nas mensagens entre os tipos 130 e 255 onde são definidos os tipos de mensagens para realização de ações como: Descoberta do Tamanho do MTU, Descoberta de Vizinhança (*Neighbor Discovery*), Gerência de Grupos *Multicast* e Mobilidade.

2.4.5 *O Protocolo Neighbor Discovery*

Este protocolo substitui o protocolo ARP e inclui as seguintes funcionalidades ao IPv6 [27]:

2.4.5.1 Autoconfiguração de endereços

Diferentemente do protocolo IPv4, o IPv6 possibilita que um dispositivo gere automaticamente seus endereços através da configuração *Stateless* sem o uso de um serviço de DHCP, onde o host gera um IP com o prefixo FE80::/64 concatenado com seu MAC *Address*, chamado de endereço link-local, onde automaticamente passa a fazer parte dos grupos *multicast*: *solicited-node* e *all-node*. Posteriormente este host envia uma mensagem *Router Solicitation* (RS) para o grupo *multicast all-routers*, recebendo uma mensagem *Router Advertisement* (RA) do roteador padrão da rede, contendo como informações o MTU do enlace de rede; a rota default; o limite de encaminhamento; os prefixos da rede; e outras mais.

Através das informações recebidas, o *host* passa a ter um endereço *stateful* roteável na *Internet*. Outra forma de obtenção de endereços é através de um servidor DHCPv6, onde o *host* usando seu endereço *stateless* envia uma solicitação de endereço para o grupo *multicast* FF02::1:2, o qual é respondido por um servidor de DHCPv6, informações como servidor de DNS, NTP e outras. Estes processos também são utilizados quando um nó móvel entra em uma rede remota.

2.4.5.2 Descoberta de vizinhança

A mensagem *Neighbor Solicitation* (NS) é enviada do host a um grupo *multicast* da rede informando seu endereço MAC e obtém como resposta a mensagem *Neighbor Advertisement* (NA), contendo como parte da mensagem o endereço MAC de seus vizinhos.

Estas mensagens substituem o protocolo ARP do IPv4 e inibem a necessidade de uso de *broadcast* na rede.

2.4.5.3 Redirecionamento de pacotes

Os roteadores que recebem pacotes de determinados *hosts*, têm a possibilidade de enviar mensagens de *redirect* informando outro caminho de saída do enlace local.

2.4.5.4 Endereços duplicados

Após um host receber seu endereço, ele deve verificar se o mesmo já não está em uso na rede. Para isto, ele envia uma mensagem de *Neighbor Solicitation* informando no campo de destino o seu próprio endereço de origem, isto é, se ele receber uma resposta NA, significa que o endereço já está em uso. Este processo é sempre executado quando um nó móvel recebe um endereço ao entrar em uma rede estrangeira.

2.4.6 *Endereçamento no IPv6*

O protocolo IPv6 apresenta como principal característica o aumento no espaço para endereçamento. Com um espaço para endereçamento de 128 *bits*, representando aproximadamente 79 octilhões (7,9×1028) de vezes a quantidade de endereços IPv4 [5].

Os endereços IPv6 divididos em oito grupos de 16 *bits*, separando-os por ":", escritos com dígitos hexadecimais (0-F). Regras de abreviação podem ser aplicadas e é permitido omitir os zeros a esquerda de cada bloco de 16 *bits*, além de substituir uma sequência longa de zeros por "::" [28], ver a Figura 10.

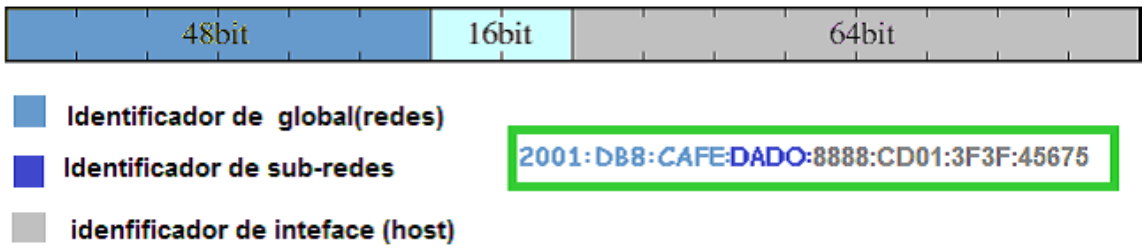


Figura 10 - Endereçamento IPv6 [29]

Em endereços IPv6, a representação de prefixos de rede continua sendo escrita de forma análoga ao IPv4, com a notação CIDR representada no formato "endereço-

IPv6/tamanho do prefixo", onde "tamanho do prefixo" é um valor decimal que especifica a quantidade de *bits* contíguos à esquerda do endereço que compreendem o prefixo [5].

Esse formato de representação possibilita a agregação dos endereços de forma hierárquica, identificando a topologia da rede através de parâmetros como posição geográfica, provedor de acesso, identificação da rede, divisão da sub-rede, etc. Assim, há a possibilidade de diminuição do tamanho da tabela de roteamento, agilizando o encaminhamento dos pacotes.

A representação dos endereços IPv6 em URLs (*Uniform Resource Locators*) passa a se dar entre colchetes, eliminando ambiguidades no caso de ser preciso indicar o número de uma porta juntamente com a URL.

A arquitetura do IPv6 o *multicast* passou a ter papel fundamental no seu funcionamento, assim como o *Anycast* e o *Unicast* conforme detalhados a seguir [21].

2.4.6.1 Unicast [30]

Também no IPv6 identifica o endereço de uma interface de rede de forma única e possui tipos (faixas reservadas) para certas funcionalidades. No IPv6 utiliza-se o endereço de rede FC00::/7 para redes não roteáveis. Esta mesma reserva de IPs existe para representar diferentes serviços, como:

- FE80::/10 endereço utilizado para a distribuição de IPv6 *stateless*;
- 2000::/3 faixa de endereços onde se iniciou a alocação dos endereços IPv6 roteáveis; e
- ::1/128 endereço de *loopback* .

2.4.6.2 Multicast [31]

Identifica um grupo de interfaces através de um endereço reservado FF00::/8, onde uma interface pode pertencer a mais de um grupo *multicast*. Os próximos oito bits 00 após o FF (FF00::/8) são utilizados para *flags* e delimitação da área de abrangência do grupo *multicast*, que pode variar da interface local até a rede externa. Sendo que a abrangência referente a rede externa é limitada pelo TTL (Time to Live) do pacote.

Como exemplo exemplifica-se alguns grupos *multicast* pré-definidos, tais como:

- FF01::1 Grupo *all-nodes*, referente a todas as interfaces do dispositivo;
- FF01::2 Grupo *all-routers*, referente a todos os roteadores do dispositivo;

- FF02::1 Grupo *all-nodes*, referente a todos os dispositivos do enlace da rede (*linklocal*); e outros, mostrados na Tabela 3.

Tabela 3 - Endereços *Multicast* permanentes [10].

Endereço	Escopo	Descrição
FF01::1	Interface	Todas Interfaces em um Nó (all-nodes)
FF01::2	Interface	Todos Roteadores em um Nó (all-routers)
FF02::1	Enlace	Todos os Nós do Enlace (all-nodes)
FF02::2	Enlace	Todos Roteadores do Enlace (all-routers)
FF02::5	Enlace	Roteadores OSPF
FF02::6	Enlace	Roteadores OSPF Designados
FF02::9	Enlace	Roteadores RIP
FF02::D	Enlace	Roteadores PIM
FF02::1:2	Enlace	Agentes DHCP
FF02::1:FFXX:XXXX	Enlace	Solicited-node
FF05::2	Site	Todos os Roteadores de um Site
FF05::1:3	Site	Servidores DHCP em um Site
FF05::1:4	Site	Agentes DHCP em um Site
FF0X::101	Variado	NTP (Network Time Protocol)

2.4.6.3 Anycast [32]

Utilizado para identificar um grupo de interfaces como, por exemplo, uma subclasse de rede. É possível assemelhar-se ao *broadcast*. A diferença é que no *Anycast* a mensagem é enviada apenas a uma interface escolhida por proximidade. É usado no balanceamento de carga, na descoberta de serviços na rede (onde ocorrendo a primeira resposta considera-se satisfatório) e na mobilidade, no processo de descoberta do *Home Agent*.

2.4.7 *Estrutura Hierárquica do Endereçamento IPv6*

O IPv6 tem uma Estrutura Hierárquica, pois os endereços IPs serão fornecidos obedecendo também uma Hierarquia no poder de concessão destes IPs. E Como os RIRs alocam os blocos IPs para os seus membros regionais ou LIR (*Local Internet Registries*).

Cada RIR recebe da IANA um bloco **/12**. O bloco **2800::/12** corresponde ao espaço reservado para o LACNIC, já o NIC.br trabalha com um **/16** que faz parte deste **/12**. A alocação mínima para ISPs é um bloco **/32**, podendo chegar até **/35** [10].

Alocações maiores podem ser feitas mediante apresentação de justificativa de utilização. A Figura 11 mostra a divisão hierárquica do endereçamento, ilustrando a gama de atribuição de cada organismo, com os campos mais escuros indicando a atribuição de cada organização.

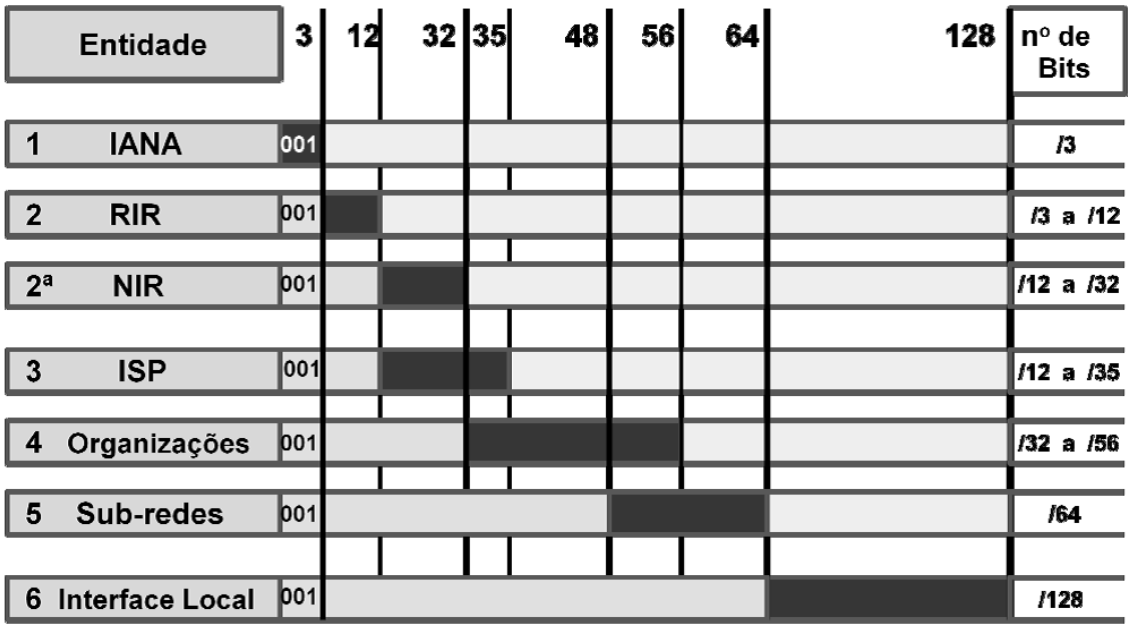


Figura 11 - Estrutura de Alocação de endereços IPv6 [10]

2.4.8 *Recomendações para Designação de Endereços Ipv6*

Existem recomendações no NIC.br, para a designação de endereços IPv6, e é uma boa prática seguir as políticas que estão sendo adotadas pelos RIRs aceitando as decisões de administração dos Blocos IPv6 [5]. Ao se seguir tais recomendações, o administrador obtém facilidade na renumeração da rede em caso de troca de prefixo (mudança de provedor) e pode expandir a rede sem solicitar mais endereços ao provedor, entre outros benefícios que facilitem a administração. A distribuição usual dos prefixos de endereçamento IPv6 é resumida na Tabela 4.

- Redes **/48** são recomendadas para todos os tipos de usuários, sejam usuários domésticos, pequenos ou grandes empresas;
- Grandes empresas podem receber um **/47**, prefixos um pouco menores, ou múltiplos de **/48**;
- Redes **/64** são recomendadas quando houver certeza que uma e apenas uma sub-rede é necessária [10]; e

- Uma rede **/128** pode ser utilizada quando houver absoluta certeza que uma e apenas uma interface será conectada.

Tabela 4 - Distribuição usual dos prefixos de endereçamento IPv6 [33]

Prefixo	Alocado para	Redes /64
/32	Provedores de acesso	2^{32}
/48	Organizações	2^{16}
/56	Usuários domésticos	2^{8}
/64	Segmentos individuais de rede (sub-redes, vlans)	1

2.4.9 *Identificadores de interface*

Utilizados para distinguir as interfaces dentro de um enlace, os identificadores de interface (IID), devem ser únicos dentro do mesmo prefixo de sub-rede. O mesmo IID pode ser usado em múltiplas interfaces em um único nó, porém, elas devem estar associadas a deferentes sub-redes.

Normalmente utiliza-se um IID de 64 bits, que pode ser obtido de diversas formas. Ele pode ser configurado manualmente, a partir do mecanismo de autoconfiguração *stateless* do IPv6, a partir de servidores DHCPv6 (*stateful*), ou formados a partir de uma chave pública (CGA). Embora eles possam ser gerados randomicamente e de forma temporária, recomenda-se que o IID seja construído baseado no endereço MAC da interface, no formato EUI-64 [5].

2.4.10 *Endereços especiais*

Utilizados para fins determinados, são utilizados alguns endereços IPv6 especiais, descritos a seguir:

- **Endereço Não-Especificado (*Unspecified*):** representado pelo endereço 0:0:0:0:0:0:0:0 ou ::0 (equivalente ao endereço IPv4 *unspecified* 0.0.0.0). Não

deve ser atribuído a nenhum nó, indicando apenas a ausência de um endereço e não deve ser utilizado como endereço de destino de pacotes IPv6 [21];

- **Endereço *Loopback***: representado pelo endereço *unicast* 0:0:0:0:0:0:0:1 ou ::1 (se equivale ao endereço IPv4 *loopback* 127.0.0.1) e é utilizado para referenciar a própria máquina, sendo muito utilizado para teste internos. [21]; e
- **Endereços IPv4-mapeado**: 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:192.168.100.1. [5]

Também existem algumas faixas de endereços também são reservadas para uso específicos [5]:

- **2002::/16**: prefixo utilizado no mecanismo de transição 6to4;
- **2001:0000::/32**: prefixo utilizado no mecanismo de transição TEREDO; e
- **2001:db8::/32**: prefixo utilizado para representar endereços IPv6 em textos e documentações.

2.4.11 *Roteamento no IPV6*

O IPv6 inclui extensões de roteamento simplificadas que suportam novas funcionalidades poderosas, como: *Provider Selection* - seleção de provedor, baseada em políticas, desempenho, custo, etc; *Host Mobility* - roteamento até a localização atual do host, quando este pode se deslocar; e o *Auto-Readdressing* - roteamento para um novo endereço [10].

A funcionalidade de roteamento é obtida criando sequências de endereços IPv6 usando a opção ***Routing*** e essa opção é usada por um equipamento de origem para listar um ou mais nós intermediários a serem visitados no caminho de destino de um pacote do protocolo.

No IPv6, assim como no IPv4, os endereços IP não são roteáveis e o que é roteado em cada Protocolo é, no IPv4 - o endereço de Rede e no IPv6 - o Prefixo.

Como no IPv4, também é a máscara quem determina qual parte do endereço IP é Rede e qual parte é Host. Todas as máscaras contidas nas Tabelas de Rotas são aplicadas

para cada endereço de destino e o resultado da maior máscara que traduz uma rota contida na tabela, é a que será usada.

Os mais importantes protocolos de roteamento RIP, OSPF e BGP são todos utilizados para roteamento em redes IPv6, com pouca ou nenhuma modificação e o encaminhamento em uma rede IP, seja o IPv6 ou IPv4, é realizado utilizando os mesmos mecanismos, as maiores diferenças são: o maior recurso, a agregação e os endereços mais longos (128 bits); e uma vez ajustados estes fatores através dos protocolos de roteamento o roteamento IPv6 também é ajustado [5].

2.4.11.1 Protocolo de Roteamento RIPng ou Rip Next Generation

A tabela de roteamento RIP [23] contém uma entrada para cada destino alcançável e a cada entrada contém pelo menos as seguintes informações:

- o prefixo IPv6 de destino;
- uma métrica que representa o custo total de obtenção de um datagrama a partir do roteador para esse destino. Esta métrica é a soma dos custos associados com as redes que seriam percorridas para chegar ao destino;
- endereço IPv6 do próximo roteador no caminho para o destino (ou seja, o próximo salto). Se o destino for uma das redes conectadas diretamente, este item não é necessário;
- um sinalizador para indicar que as informações sobre o percurso foram alteradas recentemente. Este será referido como a "*route change flag*"; e
- vários "*timers*" associados com o percurso, em particular relacionados aos anúncios que devem ser enviados e quando as rotas devem ser consideradas com "*time out*".

O protocolo RIPng é um protocolo IGP de implantação e configuração simplificada e possui ainda as seguintes características [10]:

- Protocolo do tipo Vetor de Distância (Bellman-Ford);
- Baseado no RIPv2 (IPv4);
- Específico para IPv6, como suporte ao novo formato de endereço;
- Utiliza o endereço *multicast* FF02::9 (*All RIP Routers*) como destino;

- O endereço do próximo salto deve ser um endereço *link* local;
- Em um ambiente IPv4+IPv6 é necessário usar RIP (IPv4) e RIPng (IPv6);
- Tem como limitações: alcançar no máximo 15 saltos; utilizar apenas a distância para determinar o melhor caminho; e possuir a possibilidade de criar *loops* de roteamento e contagem até o infinito.
- A atualização das tabelas de rotas trabalha com envio automático a cada 30 segundos, independentemente de haver mudanças ou não; quando detecta mudanças na topologia da rede, envia apenas a linha afetada pela mudança; e ocorrem quando recebem uma mensagem do tipo *Request*.

Roteadores utilizando RIPng devem enviar e receber mensagens UDP na porta UDP 521 [23].

2.4.11.2 Protocolo de Roteamento OSPFng ou OSPF Next Generation

Desenvolvido como resposta a algumas das deficiências do RIP, o OSPF propaga informações de roteamento mais rapidamente e é mais estável que o RIP, lida adequadamente com Sub-redes, realiza balanceamento de carga onde houver rotas equivalentes, suporta os tipos de serviços de roteamento e utiliza *multicasting*, caracterizando as vantagens sobre o RIPv1.

O OSPFng [24], ou "OSPF para IPv6", fornece as especificações para o OSPF, que se adapta ao uso com IPv6.

Em sua maior parte, o OSPF para IPv6 usa os mesmos mecanismos utilizados no IPv4, "OSPFVersion 2" e como qualquer protocolo de roteamento IP, o OSPF foi modificado para acomodar os 128 bits do IPv6 [24].

O *Open Shortest Path First version* 3 (OSPFv3) - protocolo IGP (trabalha internamente ao AS) é do tipo link-state, os roteadores descrevem seu estado atual ao longo do AS enviando mensagens LSAs (*flooding*), utiliza o algoritmo de caminho mínimo de Dijkstra, agrupa roteadores em áreas e em um ambiente IPv4+IPv6 é necessário usar OSPFv2 (IPv4) e OSPFv3 (IPv6) [10].

O OSPF agrupa os roteadores em áreas, onde cada roteador pertencente a cada área deve ter na sua configuração referência a esta área, sempre devendo haver uma Área “0”, que é chamada de área *backbone*, sendo que todas as outras áreas devem ter conexão com a mesma. A Figura 12 mostra topologia ilustrando o conceito e as designações dos roteadores que fazem parte destas áreas [10], onde:

- **ASBR**- Roteador de Borda do Sistema Autônomo (se liga a outro AS)
- **ABR**- Roteador de Borda da Área (liga uma Área à outra)
- **BR**- Roteador do Backbone (todo Roteador que está no Backbone)
- **IR**- Roteador Interno (Todo Roteador que se interliga a outro dentro da Área)

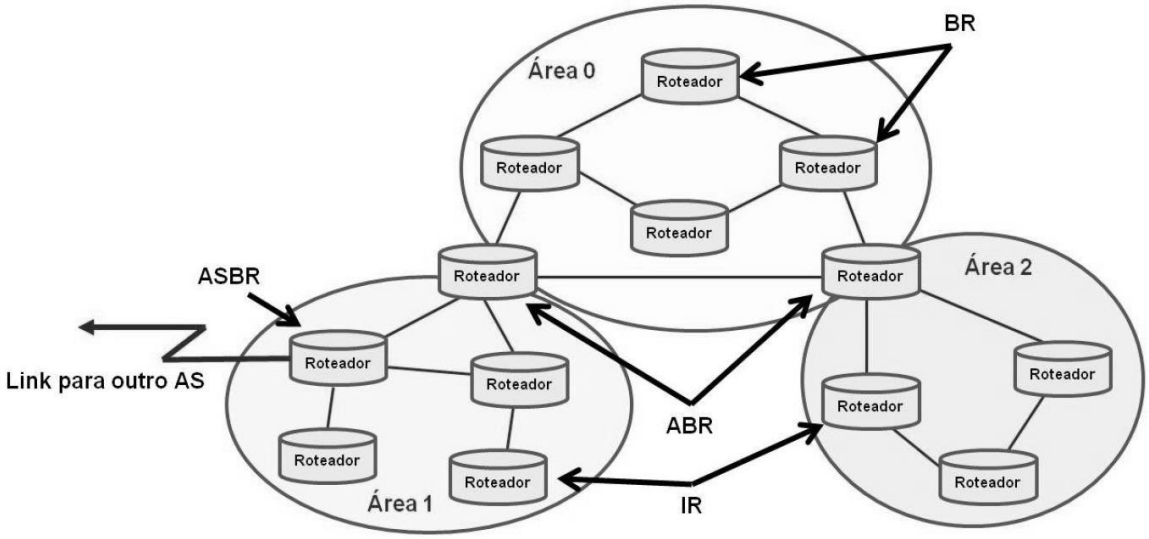


Figura 12 - Representação do conceito de Áreas [10]

O protocolo OSPFng apresenta algumas diferenças do OSPFv2, como, entra elas:

- OSPFv3 roda por enlace e não mais por sub-rede;
- Foram removidas as informações de endereçamento;
- Adição de escopo para *flooding* (fluxo);
- Suporte explícito a múltiplas instâncias por enlace;
- Uso de endereços *link*-local;
- Mudanças na autenticação e no formato do pacote;
- Identificação de vizinhos pelo *Router* IDs; e
- Utiliza endereços *Multicast* (AllSPFRouters FF02::5 e AllDRouters FF02::6).

2.4.11.3 Protocolo BGP 4 - Border Gateway Protocol Versão 4

Os Protocolos RIP e OSPF, anteriormente citados, são classificados como protocolos IGP (*Interior Gateway Protocol*) por trocarem informações somente dentro de um Sistema Autônomo (AS). Já entre ASs, o BGP [34] é o protocolo padrão utilizado, sendo

BGP 4 a versão mais aplicável em Redes IPv6 até agora. É essencialmente um Protocolo Vetor de Distância com características de um Protocolo *Link State*. E tem como função primária a troca das informações sobre rotas entre Sistemas Autônomos.

O BGP 4 utiliza o TCP, porta 179, como protocolo de transporte, que implementa fragmentação, retransmissão e está virtualmente implementado em todos os hosts comerciais. Dois sistemas autônomos formam uma conexão de protocolo de transporte, isto é, uma conexão TCP e trocam mensagens para abrir e conferir os parâmetros de conexão sendo que inicialmente, trocam todas as tabelas de roteamento entre si, e após, apenas atualizações destas tabelas são enviadas [10].

2.4.12 *IPv6 DNS*

A resolução de nomes DNS para nós IPv6 funciona de forma praticamente idêntica a IPv4, com algumas mudanças, o sistema no IPv4 exige atualização manual toda vez que um host é adicionado, alterado ou retirado numa rede, já o serviço DNS, elaborado no IPv6, providencia um banco de dados centralizado, onde a tradução entre nomes e endereços é armazenada. Para o DNS no IPv6 não existe algum novo conceito fundamental e para a resolução de nomes no IPv6 são usados os registros AAAA (quádruplo A), os quais apontam para uma entidade que é quatro vezes do tamanho do registro A (IPv4) [35].

O DNS usa os registros de requisição e resposta (*Request/Response Records* - abreviados como RRs) em suas consultas, como os descritos abaixo:

- **SOA - *Start Of Authority*** – descrevendo as propriedades do domínio;
- **NS - *Name Server*** – informando quais são os servidores de nomes para o domínio;
- **A - *Address*** – endereços IPv4;
- **AAAA - *Address*** – endereços IPv6;
- **CNAME** - *alias names*; e
- **PTR - *pointer*** – normalmente apontando de um endereço de volta para o nome (DNS reverso) [10].

Na resolução de nomes, para efetivar a tradução do nome de um host para um endereço IP, os RRs (*Resource Records*) disponíveis com suporte a IPv6 são o AAAA ou A6, mas, existe um estudo que sugere que o A6 seja descontinuado [36].

Na resolução de Nomes utilizando registros de recursos AAAA, O IETF recomenda o uso o uso do registro de recurso AAAA RR para o mapeamento direto (*forward mapping*) e PTR RRs para mapeamento reverso (*reverse mapping*) quando se estiver definindo redes IPv6.

2.4.13 *DHCPv6*

O protocolo DHCP é basicamente o mesmo para ambos, IPv4 e IPv6, esse protocolo é utilizado na Autoconfiguração *Stateful* e possui duas características do IPv6 que melhoraram muito o DHCPv6 [25]:

1) *Hosts* IPv6 têm o endereço "*link*-local". Toda interface de rede possui um endereço único, que pode ser usado para enviar e receber apenas no *link* e os *hosts* IPv6 usam este endereço para enviar pedidos de endereços Globais.
2) Os sistemas IPv6 suportam *multicast*. Todos os servidores DHCPv6 recebem pacotes *multicast* DHCPv6 com endereços: FF02::1:2 e FF05::1:3

Em uma troca de informações entre Cliente e o Servidor DHCP, configura todas as interfaces. A utilização de DHCPv6 oferece um controle maior na atribuição de endereços, visto que, além de fornecer opções de configuração de rede, é possível definir políticas de alocação de endereços e atribuir endereços aos hosts que não sejam derivados do endereço MAC. Em uma rede IPv6, é possível combinar o uso de autoconfiguração *stateless* com servidores DHCP.

Os protocolos DHCPv6 e DHCPv4 são independentes, de modo que, em uma rede com Pilha Dupla, será necessário rodar um serviço para cada protocolo [10]. Com DHCPv4, é preciso configurar no cliente se este usará DHCP, enquanto que com o DHCPv6, sua utilização é indicada através das opções das mensagens RA e o servidor DHCPv6 pode fornecer várias informações, dentre elas: endereço IPv6, prefixo IPv6, Opções de Extensão, servidores DNS e servidores SNTP (data e hora atualizada na rede) [10].

2.4.14 *IP Security Protocol (IPSec)*

O IPSec, que fornece uma arquitetura de segurança para o Protocolo da Camada *Internet*, não é uma arquitetura de segurança para a *Internet* em si [37]. O protocolo define

os serviços de segurança para ser utilizado na camada IP, tanto para IPv4 e IPv6. E a diferença é que o IPSec é obrigatório nos nós IPv6 e opcional para nós IPv4.

O IP *Security Protocol* (IPSec) fornece um padrão aberto e interoperável para a construção da segurança na camada de rede, no lugar da camada de aplicação ou camada de transporte. Ele permite a criação de redes virtuais privadas (VPNs) [38], capaz de levar, com segurança, dados da empresa através da *Internet* aberta.

O IPSec é geralmente usado em conjunto com os protocolos de gestão do túnel, incluindo o *Layer 2 Tunneling Protocol* (L2TP) [39], o *Layer 2 Forwarding* (L2F) [40] protocolo criado pela Cisco Systems e o *Point to Point Tunneling Protocol* (PPTP) [41] da Microsoft.

O IPSec pode operar em dois modos:

1) **Modo de Transporte**: protege somente os protocolos das camadas superiores, pois o cabeçalho de segurança aparece logo após o cabeçalho IP e antes dos cabeçalhos dos protocolos de camada superior.
2) **Modo Túnel (VPN de camada 3)**: protege todo o Pacote, encapsulando somente o cabeçalho IP externo [42].

E o protocolo IPSec utiliza os seguintes recursos independentes para realizar suas funções [10]:

- *Authentication Header* (AH): que garante a integridade do pacote, a autenticação da origem, proteção contra o reenvio do pacote, é adicionado após os Cabeçalhos *Hop-by-Hop*, *Routing* e *Fragmentation* e pode ser usado em ambos os modos de operação.
- *Encapsulating Security Payload* (ESP): que vem a garantir a confidencialidade do Pacote, integridade do Interior do Pacote, autenticação da Origem, proteção contra o reenvio, é responsável pela Criptografia, pode ser combinado com o AH e também pode ser usado em ambos os modos de operação.

2.5. Desafios da Migração do IPv4 para o IPv6

Nesta seção são abordadas as diferentes técnicas de transição e coexistência entre protocolos IPv4 e IPv6. Além de uma abordagem conceitual, são descritos os possíveis cenários no qual essas técnicas poderão ser aplicadas. Esta seção serve como base para a seção onde é realizado um estudo acerca da viabilidade de implementação IPv6 na atual topologia do DGP.

2.5.1 *Cenários de coexistência de IPv6 e IPv4*

Na transição do IPv4 para o IPv6 é necessária a coexistência e interoperabilidade entre ambos os protocolos e para isso é necessário o uso de tecnologias auxiliares, conhecidas como técnicas de transição [5]. A necessidade de coexistência ocorre em diferentes cenários, cada qual com características e demandas singulares e uma técnica de transição isoladamente normalmente não é capaz de atender simultaneamente a todos.

A enumeração dos cenários a seguir é uma generalização feita pelo IPv6.br [5] e extensão da enumeração feita na RFC 6144 [43], pois a RFC citada trata apenas de cenários utilizados com soluções de tradução, aqui os cenários descrevem também soluções de tunelamento.

- Cenário 1: Rede IPv6 para *Internet* IPv4: Devido à falta de endereços IPv4 ou outras limitações técnicas ou econômicas a rede cliente possui somente IPv6, mas necessita conectar-se à *Internet* IPv4. Este cenário também pode ocorrer em projetos totalmente novos, aos quais não se aplicam as restrições normalmente encontradas em tecnologias já em uso. Algumas empresas têm se decidido por criar redes somente IPv6 nesse caso, por motivos de simplicidade, facilidade de gerência e outros, mas necessitam ainda acessar servidores de clientes e fornecedores que estão na *Internet* IPv4. Este cenário possui uma complexidade simples e é de fácil solução, sendo suportado por tanto por técnicas *statless* quanto *stateful*, que serão explicadas mais adiante [5].
- Cenário 2: *Internet* IPv4 para Rede IPv6: Mesma rede, mas que necessita receber conexões da *Internet* IPv4, para o caso, por exemplo, de haver servidores IPv6 na rede, que devem atender solicitações de clientes na *Internet* IPv4 [5]. Este cenário é muito mais complexo que o cenário 1, pois

normalmente não se consegue fazer um mapeamento 1:1 de todos endereços IPv6 existentes na rede para endereços IPv4 válidos. Exige soluções *stateful*, mas pode ser também atendido por soluções *stateless*, desde que suportem conexões iniciadas via IPv4 para um subconjunto dos endereços IPv6 na rede.

- Cenário 3: *Internet* IPv6 para Rede IPv4: Este é um típico cenário onde uma rede legada, onde não é possível fazer uma atualização para IPv6, necessita continuar em uso e responder requisições da *Internet* IPv6 e neste cenário só cabe soluções *stateful*, já que a rede IPv4 deve comunicar-se com toda a *Internet* IPv6.
- Cenário 4: Rede IPv4 para *Internet* IPv6: Este cenário só deve ser encontrado em estágios bem avançados da implementação do IPv6, quando a maior parte dos serviços na *Internet* já tiverem migrado para o novo protocolo. Técnicas de tradução na própria rede provavelmente não conseguirão solucionar esse problema [5].
- Cenário 5: Rede IPv6 para Rede IPv4: Ambas as redes deste cenário estão na mesma organização e os endereços IPv6 e IPv4 podem ser públicos e válidos na *Internet* ou privados e válidos somente dentro da organização [5]. Este cenário é bastante similar ao cenário 1 e os mesmos tipos de técnicas aplicadas a ele podem ser aplicadas a este.
- Cenário 6: Rede IPv4 para Rede IPv6: Conforme o cenário anterior, essa é uma situação semelhante ao cenário 2, mas com ambas as redes dentro da mesma organização. Os endereços IPv6 e IPv4 podem ser públicos e válidos na *Internet* ou privados e válidos somente dentro da organização. Os mesmos tipos de técnicas aplicadas ao cenário 2 podem ser aplicadas a este.
- Cenário 7: *Internet* IPv6 para *Internet* IPv4: Este cenário, necessita da técnica de transição perfeita, que também seria capaz de resolver todos os cenários anteriores, mas infelizmente ela não existe [5]. A grande diferença na quantidade de endereços torna, até este momento, uma solução para este cenário tecnicamente improvável.
- Cenário 8: *Internet* IPv4 para *Internet* IPv6: Mesma dificuldade técnica de implementação do cenário anterior.
- Cenário 9: Rede IPv6 para Rede IPv6 bidirecional via *Internet* IPv4: Este cenário apresenta o caso em que a comunicação entre duas redes com IPv6

necessita ser feita através da *Internet* IPv4 ou de Rede IPv4 [5]. A comunicação pode ser iniciada por ambas as Redes IPv6.

- Cenário 10: Rede IPv4 para Rede IPv4 bidirecional via *Internet* IPv6: Este cenário apresenta o caso em que a comunicação entre duas redes com IPv4 necessita ser transmitida através da *Internet* IPv6 ou de Rede IPv6. A comunicação pode ser iniciada por ambas as Redes IPv4 [5].

2.5.2 *Técnicas de Transição do Protocolo IPv4 para o IPv6*

Em função da estrutura da *Internet*, que é baseada no IPv4, não seria possível uma mudança total e imediata, daí o IPv6 foi projetado para ser implantado gradualmente.

E o período de transição e de coexistência dos dois protocolos exigiu o desenvolvimento de técnicas auxiliares. Problemas conectar redes IPv6 a outras redes IPv6 por meio de equipamentos ou de uma *Internet* que só suportassem IPv4, foram surgindo e soluções, como na forma de diversos tipos de túneis IPv6 sobre IPv4 para atender tal necessidade, usando diferentes técnicas, estabelecidos manualmente ou automaticamente, começaram a ser criadas. Técnicas de tradução vieram a ser empregadas [5].

Em virtude da variedade, pode-se classificar as técnicas de transição segundo sua funcionalidade, como na Tabela 5.

Tabela 5 - Técnicas de Transição [5]

TÉCNICA DE TRANSIÇÃO	DESCRIÇÃO
Pilha dupla	Convivência do IPv4 e do IPv6 nos mesmos equipamentos, de forma nativa, simultaneamente. Essa é a técnica padrão escolhida para a transição para IPv6 na *Internet* e deve ser usada sempre que possível.
Túneis	Permite que diferentes redes IPv4 comuniquem-se através de uma rede IPv6, ou vice-versa.
Tradução	Permite que equipamentos usando IPv6 comuniquem-se com outros que usam IPv4, por meio da conversão dos pacotes.

Os túneis e as técnicas de tradução podem ser *stateful* ou *stateless*:

- *Stateful*: em que é necessário manter tabelas de estado com informações sobre os endereços ou pacotes para processá-los.
- *Stateless*: em que não é necessário guardar informações, cada pacote é tratado de forma independente.

As técnicas *stateful* são mais caras: gastam mais CPU e memória, não vindo a escalar bem. É recomendável que sempre se busque dar a preferência a técnicas *stateless*.

Conforme consta em [5], existem casos em que a comunicação entre IPv4 e IPv6 se faz necessária para um, ou alguns tipos de aplicações. Também situações em que, no uso de uma técnica de tradução, ela venha a funcionar para quase todas as aplicações, mas falha naquelas que carregam endereços IP literais no protocolo, na camada de aplicação. Se fazendo necessário fazer o uso de *gateways* específicos, na camada de aplicação, os chamados *Application Level Gateways* (ALGs).

Existem diversos tipos de técnicas para túneis hoje padronizadas, ou em discussão na IETF e, de forma geral, recomenda-se critérios na escolha da técnica a ser utilizada, como:

- preferir técnicas que impliquem na utilização de IPv6 nativo pelos usuários finais, de forma que túneis IPv4 dentro de IPv6 venham a ser preferidos em detrimento de túneis IPv6 sobre IPv4;
- evitar técnicas para prolongar o uso do protocolo IPv4, sem a adoção concomitante do IPv6; e
- analisar a maturidade da técnica e as opções de implantação.

2.5.3 *Pilha Dupla (Dual-Stack)*

Para funcionamento em paralelo (IPv4 e IPv6), esta técnica deve ser aplicada em todos os dispositivos da rede. Cada nó da rede é configurado para trabalhar com endereços IPv4 e IPv6 e protocolos de roteamento de forma simultânea executam sua pilha de aplicações com as decisões de roteamento sendo tomadas baseadas na versão de cabeçalho IP em que o IPv6 é o protocolo preferencial dos roteadores. A técnica de pilha dupla é exemplificada na Figura 13 [5].

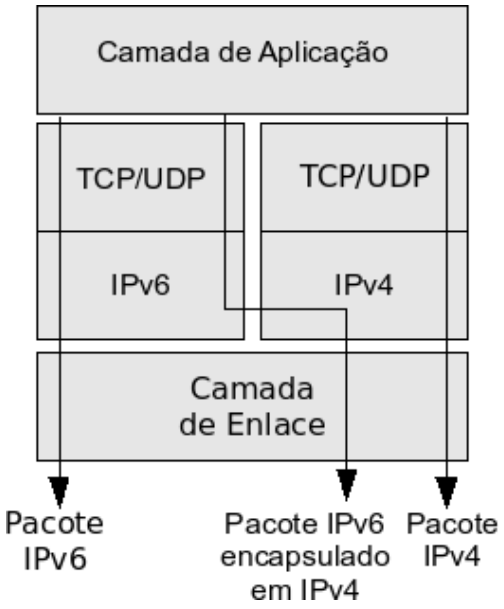


Figura 13– Implementação Pilha Dupla [5]

Nesta técnica deve-se deixar o IPv4 nativo em funcionamento e implantar o IPv6 em um formato de coexistência nos equipamentos, de acordo com [5] "A utilização deste método permite que dispositivos e roteadores estejam equipados com pilhas para ambos os protocolos, tendo a capacidade de enviar e receber os dois tipos de pacotes, IPv4 e IPv6. "

Em cada nó (que funciona IPv4/IPv6) é configurado o endereçamento de cada versão (ex. DHCP e/ou DHCPv6) [5].

Medidas, como a aplicação de filtragem de pacotes IPv6 e habilitação do serviço DNS para IPv6 são necessárias e o método é suportado por todos os sistemas operacionais. Como os equipamentos terão que trabalhar com IPv4 e IPv6 simultaneamente, surge uma carga maior de processamento [5]. Na proposta apresentada neste documento, será realizada uma distribuição dos endereços IPv6, bloco 2804:7a8::/32, dentro da topologia do DGP. Para isso serão seguidas as seguintes recomendações do Comitê Gestor da *Internet* no Brasil e do Núcleo de Informação e Coordenação do Ponto BR [44]:

- Para clientes domésticos fornecer, no mínimo, um bloco /64 ou até um bloco /56. Isso permite ao cliente formar de uma a 256 redes;
- Reservar 64 *bits* para porção de endereço de *host*. Isso garante o bom funcionamento do serviço de autoconfiguração;
- Para clientes corporativos, que justifiquem a necessidade, ofertar um bloco /48. Tal bloco possibilita ao cliente 65.536 redes; sempre considerar as necessidades de expansão futuras, bem como qual será a estratégia de roteamento dentro do provedor (no caso o DGP).

Quanto ao DNS, responder os endereços IPv6 (registros AAAA) quando disponíveis para um determinado nome de domínio é o comportamento padrão do servidor DNS, mesmo ele operando com IPv4. O protocolo por meio do qual é feita a consulta não interfere na resposta. Ao receber endereços IPv6 e IPv4 como resposta a uma consulta no DNS a aplicação decide qual protocolo usar, normalmente optando pelo IPv6, tentando o IPv4 no caso de falha. Ocorrem atualmente experimentos que resultam tentativas de conexão IPv6 e IPv4 simultâneas com opção da que for mais rápida [5].

A configuração do roteamento IPv6 costuma se apresentar independente da configuração do roteamento IPv4, implicando na necessidade de migração para um protocolo de roteamento que suporte tanto IPv6 quanto IPv4 ou optar pela execução do OSPFv3 paralelamente ao OSPFv2.

No caso da filtragem dos pacotes que trafegam na rede, em ambiente Linux os filtros de pacotes são totalmente independentes uns dos outros, de modo que o *iptables*[3] filtra apenas pacotes IPv4 e o *ip6tables*[4] apenas IPv6, não compartilhando nenhuma configuração. Já no FreeBSD[5], as regras são aplicadas a ambos os protocolos no mesmo arquivo de configuração enquanto que a aplicação de regra, além de maneira simultânea aos dois protocolos, pode ser a somente um, bastando utilizar o parâmetro *inet* ou *inet6*, dependendo do protocolo, sendo necessário configurar no *firewall*, de qualquer forma, ao implantar-se o IPv6. A atenção deve estar concentrada nas configurações independentes para IPv4 e IPv6, que são necessárias para diversos aspectos da rede, como: informações nos servidores DNS autoritativos; protocolos de roteamento; *Firewalls*; e gerenciamento das redes [5].

Utilizar pilha dupla pode não ser possível em todos os cenários, como quando não há mais IPv4 disponíveis e o provedor precisa atender a usuários novos com IPv6 e IPv4. Já em redes corporativas que já utilizam NAT isso não é um impedimento: o IPv6 nativo pode ser utilizado em conjunto com o IPv4 compartilhado.

---

[3] O *iptables* é o *firewall* padrão incluído na maioria das distribuições Linux, e ele é na verdade um front *end* para o *netfilter*, que pode manipular a pilha de rede do Linux. Há uma variante chamada *nftables* que pode vir a substituí-lo no futuro. Ele funciona verificando os pacotes que atravessam as interfaces de rede, comparando-os com um conjunto de regras pré-definidas para descobrir o que fazer com esses pacotes [106].

[4] O *ip6tables* também faz parte do pacote *iptables* e é usado para configurar o filtro de pacotes para IPv6 [106].

[5] O FreeBSD é um sistema operacional livre do tipo Unix descendente do BSD (*Berkeley Software Distribution*) desenvolvido pela Universidade de Berkeley. Ele é um sistema operacional multiusuário, que foi desenvolvido para ser compatível com a norma POSIX, assim como outros clones do Unix [107].

2.5.4 *Túneis 6over4 (IPv6-over-IPv4)*

As técnicas de Tunelamento (*Tunneling*), definas pela RFC 4213 [45], que consistem em encapsular um pacote IPv6 dentro de um pacote IPv4, permitindo que *hosts* puramente IPv6 comuniquem-se através de uma infraestrutura IPv4 já implantada, são frequentemente utilizadas, quando partes ou toda infraestrutura de rede não é capaz de prover conectividade IPv6. Portanto, tunelamento permite que o tráfego IPv6 seja carregado sobre a infraestrutura de rede IPv4.

É o processo pelo qual a informação de um protocolo é encapsulada dentro do pacote de outro protocolo, permitindo que a informação original seja carregada sobre o segundo protocolo. Um exemplo: o pacote IPv6, que é transmitido desta forma, é encapsulado em um pacote IPv4 (usando IP protocolo 41), tunelado até o destino, onde é desencapsulado e o pacote original IPv6 encaminhado [5].

A motivação para o 6over4 é permitir que máquinas IPv6 isoladas, localizadas num link físico sem conectividade direta com roteador IPv6, se tornem máquinas IPv6 completamente funcionais usando um domínio IPv4, que suporte *multicast* IPv4 como seu enlace local virtual. Endereços *multicast* IPv6 são mapeados para endereços *multicast* IPv4 para permitir *Neighbor Discovery*. O método está em desuso por várias razões, incluindo a ausência geral de suporte *multicast* IPv4 em várias redes.

Uma das formas de utilizar-se túneis é criando-os manualmente. A técnica 6over4 [46] utiliza um túnel manual estabelecido entre dois nós IPv4 para enviar o tráfego IPv6. Todo o tráfego IPv6 a ser enviado é encapsulado em IPv4 usando 6in4. A configuração manual consiste em definir os IPs v4 de origem e destino. No nó de destino, ao ocorrer a entrega, o pacote é desencapsulado e tratado de forma adequada. Como mostra a Figura 14, esse tipo de túnel pode ser utilizado para contornar um equipamento ou enlace sem suporte ao protocolo IPv6, ou para criar túneis estáticos entre duas redes IPv6 através da *Internet* em IPv4 [5].

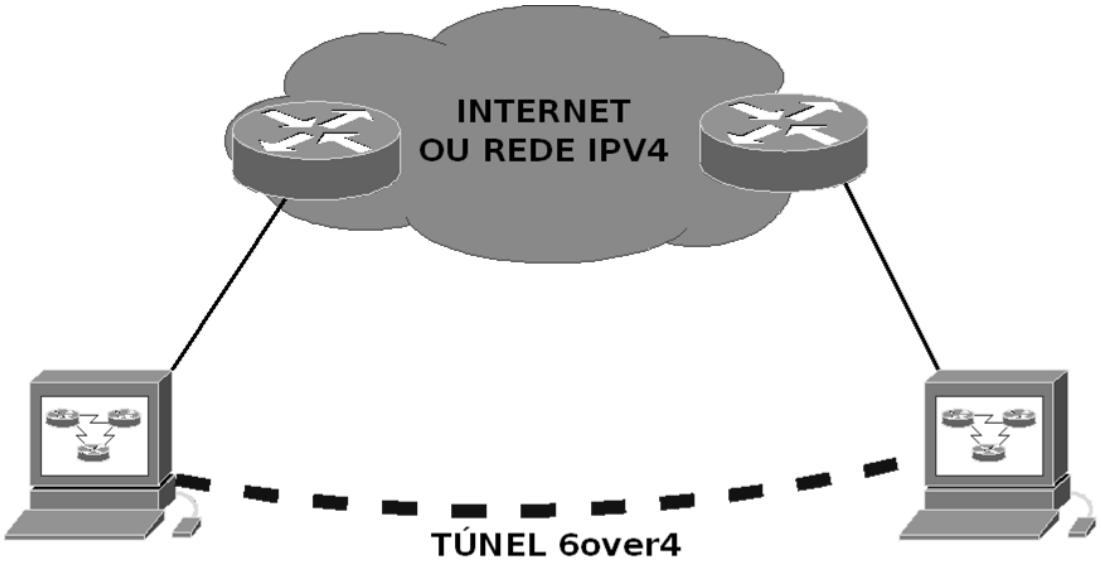


Figura 14 - túnel manual 6over4 [5]

Para se reforçar a diferença de procedimentos, o túnel 6over4 é estabelecido manualmente e tem o objetivo de permitir conexão IPv6 entre dois nós conectados por uma rede via IPv4 e faz o uso do encapsulamento 6in4. Já o encapsulamento 6in4, com a utilização do tipo 41, pode ser utilizado também em outras técnicas de transição que transportam pacotes IPv6 em redes IPv4.

2.5.5 *Túneis GRE*

O GRE (*Generic Routing Encapsulation*) [47] é outra forma de túnel estático para o transporte de IPv6 em redes IPv4. Ele é um túnel estático entre dois nós originalmente desenvolvido pela Cisco com a finalidade de encapsular vários tipos diferentes de protocolos. Este tipo de encapsulamento é suportado na maioria do sistemas operacionais e roteadores e possibilita a criação de um link ponto a ponto. Sua configuração também é manual com crescimento de complexidade proporcional à quantidade de túneis.

O funcionamento deste túnel consiste em pegar os pacotes originais, adicionar o cabeçalho GRE e o cabeçalho IPv4 e enviar ao IP de destino. Quando o pacote encapsulado chegar na outra ponta do túnel (IP de destino) remove-se dele os cabeçalhos IPv4 e GRE, restando apenas o pacote original, que é encaminhado normalmente ao destinatário.

2.5.6 *Tunnel Broker*

Apresentada na RFC 3053 [48], a técnica basicamente permite o acesso de *hosts* IPv6/IPv4 isolados em uma rede IPv4, a redes IPv6, vindo a consistir de um túnel IPv6 dentro da rede IPv4, criado do roteador, mais a frente nomeada, como *Home Agent*, até o provedor que irá fornecer a conexão IPv6.

É necessário, no início do processo, realizar um cadastro, normalmente via *Web*, em um provedor que ofereça esse serviço, o provedor realizará de maneira automática, ou semiautomática, a configuração do seu lado do túnel e permitirá o *download* de instruções, ou de um software ou script de configuração, para configurar o lado do usuário. Os *Tunnel Brokers* normalmente oferecem blocos fixos IPv6 que variam de /64 a /48.

Dentre as opções existentes, este projeto fez uso do http://tunnelbroker.net/ que vem a ser um serviço oferecido pela *Hurricane Electric*, que provê túneis para usuários domésticos ou corporativos, inclusive com a possibilidade de se fechar sessões BGP para provimento de trânsito IPv6 via túnel [5]. O NIC.br ainda está com estudo em andamento para a implantação do serviço de *Tunnel Broker*.

Sistemas Autônomos brasileiros têm utilizado com sucesso túneis com a *Hurricane Electric* para anunciar seus blocos em caráter de teste. A Figura 15 ilustra a topologia lógica.

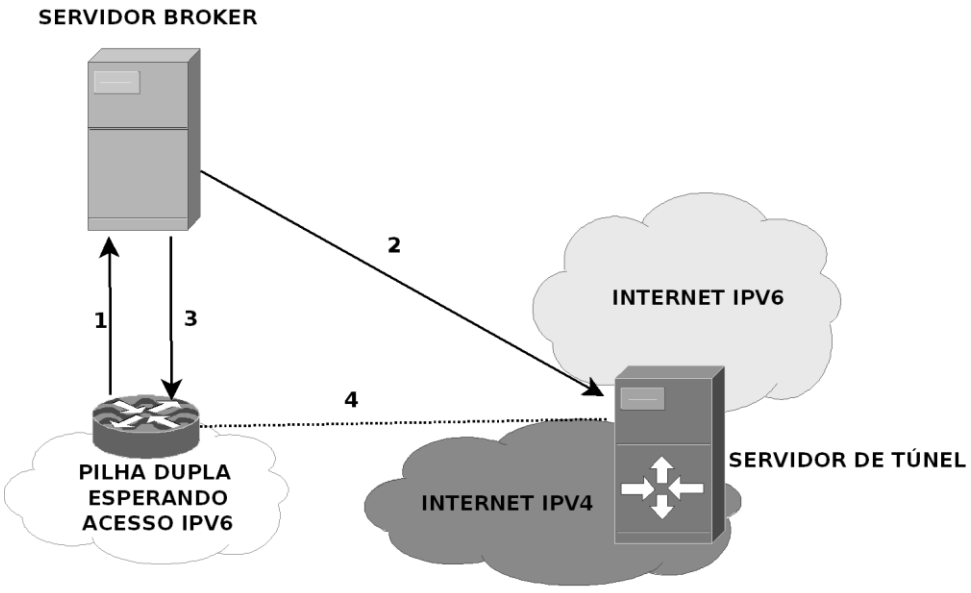


Figura 15 - Topologia lógica do *Tunnel Broker* [5]

1 – O cliente pilha dupla solicita túnel via IPv4
2 – O provedor cadastra usuário no servidor de túnel
3 – O provedor informa ao cliente os parâmetros para criação do túnel
4 – Túnel estabelecido

2.5.7 *Dual Stack Lite (DS-Lite)*

Esta técnica de tunelamento é uma das que é adequada para um cenário em que não há mais protocolos IPv4 disponíveis, mas a base de usuários do provedor continua a crescer e ainda há muitos serviços exclusivamente disponíveis em IPv4 na *Internet*. Sendo assim, o provedor não pode oferecer exclusivamente conectividade IPv6 ao usuário final, sendo forçado a oferecer também conectividade IPv4, mas com IPs de alguma forma compartilhados.

Dual Stack Lite (Pilha dupla simplificada) [49] pode ser aplicada em situações em que o provedor já oferece IPv6 nativo para seus usuários. Sua implementação necessita de um equipamento denominado AFTR (*Address Family Transition Router*), que implementa um CGN (*Carrier Grade NAT*), que vem a ser um NAT de grande porte, na rede do provedor. É usado um túnel IPv4 sobre IPv6 para transportar o tráfego IPv4. Na padornização do DS-Lite, o roteador do usuário é chamado de B4, abreviação para *DS-Lite Basic Bridging BroadBand* e nas extremidades desses túneis são usados endereços da faixa 192.0.0.0/29, especialmente reservada para este fim. Na rede do usuário são utilizados IPs da RFC 1918 [15] e não há problema se diferentes usuários utilizarem faixas de IPs repetidas, uma vez que é realizada a identificação dos diferentes túneis com base no IPv6 de origem dos pacotes encapsulados. Na CPE do usuário deve existir um DHCP v4 para a distribuição dos endereços na rede interna. Deve existir também um proxy DNS, que permita consultas via IPv4, mas realizando as consultas ao DNS recursivo do provedor via IPv6, evitando traduções desnecessárias no AFTR [5].

2.5.8 *IVI, dIVI e dIVI-pd*

O dIVI (draft-xli-behave-divi-04) e o dIVI-pd (draft-xli-behave-divi-pd-01) são alternativas de solução com a vantagem de usar técnicas *stateless* baseadas numa dupla tradução de pacotes, diferentemente do DS-Lite, que é *stateful* e baseado em tunelamento.

São métodos de tradução *stateless* que são capazes de manter a transparência fim a fim do endereço IP, não necessitando de técnicas auxiliares como tradução de DNS ou gateways para aplicações específicas. Ambos os protocolos usam compartilhamento de IPv4 com restrição de portas. As soluções são extensões do IVI [50], que é um mecanismo de tradução *stateless* 1:1, desenvolvido por pesquisadores da CERNET2, a rede acadêmica chinesa, que é somente IPv6 [5]. A China optou por criar uma rede acadêmica IPv6 pura,

totalmente nova, no lugar de implantar o IPv6 em pilha dupla na rede já existente. Essa estratégia permitiu o desenvolvimento da indústria nacional de equipamentos de rede e alavancou a implantação do IPv6 nas universidades e o desenvolvimento de diversas aplicações. Em muitas universidades chinesas, na atualidade, o tráfego IPv6 é maior do que o IPv4.

O IVI foi criado inicialmente para permitir que servidores IPv6, ligados à CERNET2, pudessem comunicar-se com a *Internet* IPv4. Para isso um endereço IPv4 é atribuído virtualmente ao dispositivo, utilizando-se um mecanismo de tradução de pacotes *stateless*. As soluções, IVI, dIVI e dIVI-pd são experimentais. Para o IVI há código disponível publicamente, na forma de um *patch* para o *kernel* do Linux, mas os outros não são disponíveis.

Para um entendimento mais prático, conforme demonstrado na Figura 16, visualiza-se que ele cria um nó IPv6 espelho[6] para o IPv4 e um nó IPv4 espelho para o IPv6, sendo que um nó espelho é. O servidor ou usuário IPv6 nativo na rede atendida pelo IVI, embora não tenha um endereço IPv4 atribuído a si, é visto por um nó IPv4 na *Internet* por meio de seu "endereço espelho" e, de forma análoga, enxerga um nó IPv4 qualquer na *Internet* por meio de seu "endereço IPv6 espelho".

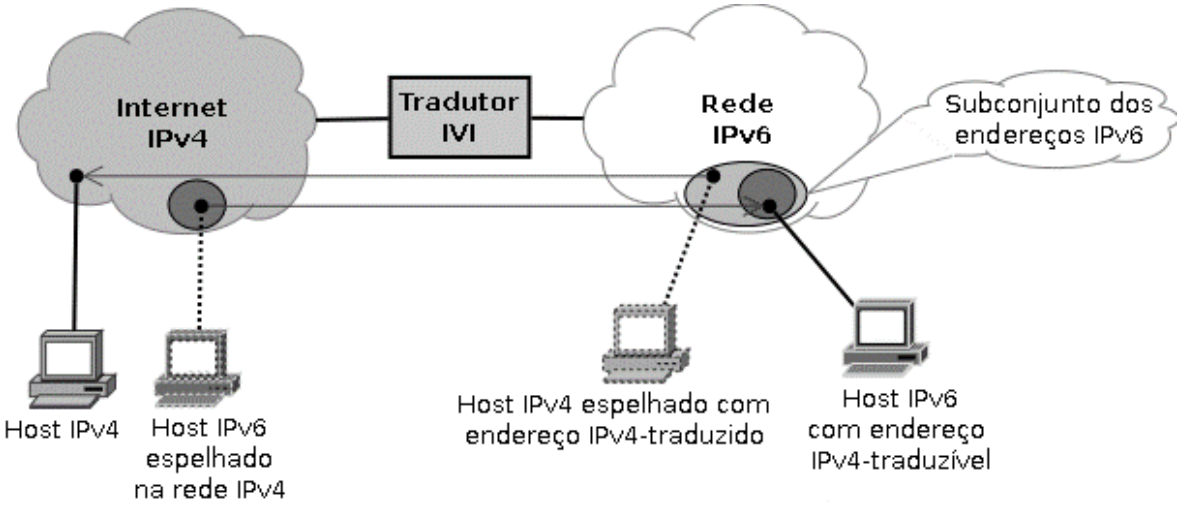


Figura 16 - Funcionamento do método IVI [50]

A aplicação mais prática para o IVI é dar visibilidade IPv4 para servidores somente IPv6 dentro de uma rede, mas ele pode ser utilizado também para usuários, com a mesma

[6] Endereço que vem a simular a presença do dispositivo na rede, mas que na verdade encaminha os pacotes enviados a ele para o dispositivo real através da tradução *stateless.*

finalidade, desde que haja uma quantidade suficiente de endereços IPv4 disponíveis. Os dispositivos que utilizarem o IVI devem usar endereçamento manual ou DHCPv6, pois o endereço precisa seguir um padrão específico que não pode ser obtido pela autoconfiguração IPv6.

2.5.9 *NAT64 e DNS64*

O NAT64 também é uma técnica de tradução, e aplicável em situações similares as do IVI, dIVI e dIVI-pd, ou seja, para nós somente IPv6 acessarem a *Internet* IPv4. O NAT64 é uma técnica *stateful* de tradução de pacotes IPv6 em IPv4 [51]. Ele necessita de uma técnica auxiliar para a conversão do DNS, chamada de DNS64 [52]. São sistemas distintos, mas que trabalham em conjunto para permitir a comunicação entre as redes IPv6 e IPv4.

O NAT64 necessita fazer a tradução de endereços IPv4 em IPv6, esta tradução é feita conforme ilustrado na Figura 17. O processo é definido em detalhes em [53]:

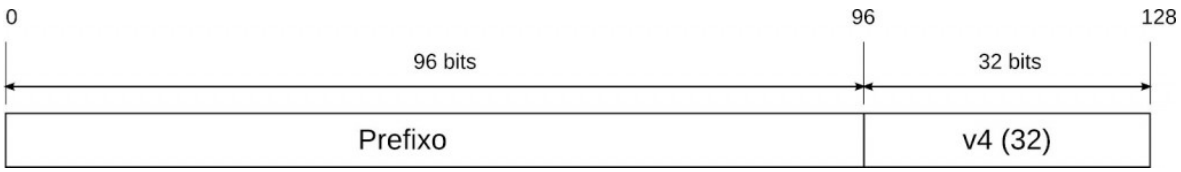


Figura 17 - Endereçamento IPv6 traduzido do IPv4 pelo NAT64 [5]

Os bits 64 a 71 são reservados para a compatibilidade de identificação de host conforme [54] e devem ser zeros. O prefixo IPv6 pode ser escolhido pela operadora, mas é recomendada a utilização do prefixo 64:ff9b::/96, reservado especificamente para a utilização em algoritmos de mapeamento de endereços IPv4 em IPv6. Já a tradução do cabeçalho IPv6 em cabeçalho IPv4 e vice-versa é feita da mesma maneira que no IVI.

2.5.10 *6to4*

Técnica de tunelamento que visa o provimento de conexão a domínios IPv6 isolados sobre uma rede conexão a domínios IPv6 isolados sobre uma rede IPv4, isso sem a necessidade de configuração dos túneis nos roteadores situados nos limites destes domínios. Essa técnica funciona através de endereços IPv6 únicos e formados pelo prefixo de endereço global 2002:wwxx:yyzz::/48, onde wwxx:yyzz é o endereço IPv4 global representado no formato hexadecimal, ver Figura 18.

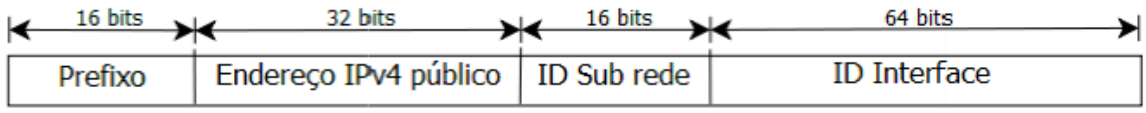


Figura 18 - Endereço 6to4

Descrição dos campos do endereço 6to4.

- Prefixo: 2002::/16 é reservado pela IANA para uso exclusivo do 6to4.
- Endereço IPv4 público: é convertido para hexadecimal.
- ID Sub rede: Usado para segmentação da rede 6to4 em várias sub redes, onde 216 sub redes são possíveis.
- ID Interface: Identifica a interface, com 264 combinações possíveis.

2.5.11 *ISATAP*

O tipo de tunelamento *Intra-Site Automatic Tunnel Addressing Protocol* (ISATAP) [55], se fundamenta em túneis criados pelo roteador ISATAP com prefixos definidos para clientes IPv4 se comunicarem com hosts IPv6. O prefixo definido no roteador ISATAP é associado ao endereço IPv4 do cliente formando assim um endereço IPv6, facilitando ao host ISATAP determinar os pontos de entrada e saída dos túneis.

Clientes ISATAP usualmente efetuam autoconfiguração *stateless* de endereço IPv6 com descoberta de roteador ISATAP automática, porém eles também podem opcionalmente usar endereços designados estaticamente, quando exigido por circunstâncias especiais. É um método compatível com mecanismos que atuam dentro de um domínio como 6to4 [5].

2.5.12 *Teredo*

É uma técnica de tunelamento automática criada pela Microsoft, permite que nós localizados atrás de *Network Address Translations* (NAT), obtenham conectividade IPv6 utilizando tunelamento em IPv4, usando o protocolo UDP [56].

A técnica apresenta alta taxa de falhas e observações de segurança. Está implementada e é fornecida por padrão em algumas versões do *Windows*.

Seu funcionamento sob túneis automáticos implica que usuários podem ter endereços IPv6 em seus dispositivos, mesmo que a rede não tendo IPv6 implantado. Tem a formatação baseada no Servidor Teredo e o *Relay* Teredo e a conexão é realizada através de do Servidor Teredo, que a inicia após determinar o tipo de NAT usado na rede do cliente. Na sequência, caso o nó destino possua IPv6 nativo, um *Relay* Teredo é utilizado para criar uma interface entre o cliente e o nó destino. Os Servidores Teredo utilizam a porta UDP 3544 para comunicar-se com os dispositivos [5].

2.6. Mobilidade no IPV6

Com a popularidade dos dispositivos móveis, tem se tornado comum a disponibilidade de redes sem fio que permitem que os usuários estejam sempre conectados na *Internet*. Em cada rede que o dispositivo se conectar, ele recebera um novo endereço IP. A mudança de endereço provoca a perda de todas as conexões e os serviços do dispositivo não podem mais ser localizados pelo seu endereço IP de origem. Com a finalidade de resolver esses problemas e permitir que o usuário mantenha seu endereço IP de origem em qualquer rede conectada, foi criado o conceito de Mobilidade IP. De acordo com essa definição, ao mudar de rede, o dispositivo sempre manterá o mesmo endereço IP da sua rede de origem.

O processo de mobilidade inter-redes foi proposto inicialmente para funcionar em IPv4 e foi chamado de *Mobile* IPv4 [57]. No *Mobile* IPv4, a comunicação entre o nó móvel e o nó correspondente sempre passa pela rede de origem do nó móvel, existindo um roteamento triangular. No IPv6 é possível executar uma otimização de rota, criando um canal de comunicação direto entre o nó móvel e o nó correspondente, utilizando para isto o cabeçalho de extensão *Mobility*.

As mensagens de controle do protocolo de mobilidade em IPv4, necessárias para registrar e controlar o nó móvel, são enviadas em pacotes UDP, já no IPv6 pode-se utilizar cabeçalhos de extensão próprios para estas ações.

Uma das maiores vantagens da implementação de mobilidade em IPv6 é a possibilidade de uma única interface de rede possuir *n* endereços (um em cada rede), facilitando a troca e o retorno do nó móvel entre as redes. Esta vantagem, aliada ao uso de endereços de grupos *multicast*, o qual permite a um nó móvel descobrir os agentes de mobilidade existentes na rede de forma dinâmica, permite ao IPv6 prover mobilidade de uma forma mais simples que o IPv4.

Em questões de segurança, o IPv6 possui uma implementação nativa de IPSec, facilitando o estabelecimento de uma comunicação segura inter-redes. Contudo, se a necessidade for aumentar o *throughput*, com o uso dos cabeçalhos de extensão do IPv6 é possível diminuir o *overhead* por não necessitar do tunelamento requerido pelo *Mobile* IPv4.

Devido a essas vantagens, em 2004 foi criada a especificação de suporte à mobilidade em IPv6, através da RFC 6275 [58], que utiliza esses novos recursos para implementação de mobilidade.

Para uma melhor compreensão de conceitos de protocolos de mobilidade, é necessário fazer uma apresentação da terminologia. A RFC 2002 [59] define algumas entidades referenciadas neste trabalho de pesquisa, incluindo: O *Mobile Node* (MN) como um *host* ou dispositivo que migra de uma rede para outra, mantendo a comunicação com um *Correspondent Node* (CN), que se refere ao par com o qual um nó móvel está se comunicando. Quando o nó móvel está trocando de rede, a partir de uma *Home Network* (HN) a uma *Foreign Network* (FN), a comunicação é controlada por um agente de mobilidade, conhecido como *Home Agent* (HA), que recebe e encaminha todos os pacotes enviados entre o nó móvel e o nó correspondente.

Existem dois tipos de protocolos de mobilidade, o primeiro chamado de protocolo IPv6 "puros" e o segundo de protocolos "híbridos". Os protocolos IPv6 "puros" são classificados dessa maneira porque utilizam apenas os recursos nativos oferecidos pelo IPv6, como: *Mobile* IPv6, *Fast Handover for Mobile* IPv6, *Hierarchical Mobile* IPv6 e o *Proxy Mobile* IPv6 [29]. Já os protocolos "híbridos" sugerem a separação entre a identificação e a localização de um dispositivo na rede.

2.6.1 *Mobile IPv6*

O protocolo de mobilidade inicialmente concebido, *MIPv6* [58], permite o uso de mobilidade sem a necessidade de qualquer agente externo nas redes estrangeiras.

A RFC 6275 [58] apresenta alguns elementos:

- *Mobile Node* (MN) - Nó móvel, que alterna de uma rede de origem a uma rede estrangeira, preservando a comunicação.
- *Home Network* (HN) - Rede de origem do nó móvel.
- *Foreign Network* (FN) - Rede remota onde se encontra MN após sair da sua HN.

- *Home Agent* (HA) - Roteador da rede de origem responsável pela mobilidade.
- *Correspondent Node* (CN) - *Host* externo a rede, que está realizando a comunicação com o nó móvel.
- *Care-of Address* (CoA) - Endereço recebido pelo MN na rede remota.
- Para o estabelecimento da comunicação entre o MN na rede estrangeira e o nó correspondente,

Pode-se trabalhar de duas maneiras para o estabelecimento da comunicação entre o MN na rede estrangeira e o nó correspondente: através de um tunelamento entre o MN e o HA ou diretamente do MN para CN, através de otimização de rotas. Na primeira forma, o CN não necessita saber que o host MN é um nó móvel, pois CN continua enviando seus pacotes para a rede de origem (HN) de MN, onde o HA fica responsável por encaminhar os pacotes para o MN através de um túnel bidirecional. Na segunda forma, CN precisa ter suporte à mobilidade, pois necessita conhecer a mudança de rede realizada por MN utilizando o cabeçalho de extensão *mobility* do IPv6. Este cabeçalho deve ser informado no campo próximo cabeçalho do pacote e possui o seguinte formato [58]:

- *Payload proto* – se refere ao número do próximo cabeçalho, com o uso atual do valor 59 para informar a ausência de próximos cabeçalhos;
- *Header len* - tamanho do cabeçalho em múltiplos de 8 bytes;
- MH *Type* - Tipos de mensagens;
- *Reserved* - Reservado para uso futuro;
- *Checksum* - Soma de verificação;
- *Message* data - Dados do cabeçalho. Variável em tipo e tamanho de acordo com o campo MH *type*.

Os tipos de mensagens (MH *Type*) trocadas entre CN e MN durante o processo de negociação e estabelecimento da comunicação são:

- *Binding Update* - Mensagem enviada pelo MN para o HA ou para o CN informando seu novo IP remoto (CoA);
- *Binding Acknowledgement* - Confirmação de recebimento de uma mensagem de *Binding Update*;

- *Binding Refresh Request* - Mensagem enviada pelo CN ao MN solicitando uma atualização de seus endereços atuais;
- *Binding Error* - Utilizada pelo CN para informar a ocorrência de erros.

Ao migrar para outra rede, o nó móvel (MN) solicita um endereço IPv6 na nova rede e informa ao seu *Home Agent* (HA) sobre o seu novo local. A partir deste momento, um túnel IPv6 é estabelecido entre o *Mobile Node* (MN) e seu *Home Agent* (HA). Assim, a comunicação entre *Mobile Node* (MN) e *Correspondent Node* (CN) continua a fluir por meio do HA. A Figura 19 detalha todos os passos do processo de troca de rede, chamado de *handover*:

- Passo (1), o *Mobile Node* (MN) possui um endereço em sua *Home Network* e uma comunicação estabelecida com o *Correspondent Node* (CN).

- Passo (2), MN inicia o processo de troca de rede, movendo-se a uma *Foreign Network* (FN). Neste momento ele irá receber um novo endereço IPv6 chamado *Care-of Address* (CoA), esta designação é apenas para distinguir seus dois endereços IPv6.

- Passo (3), como o MN mantém seu antigo endereço, deve enviar um pacote para o seu *Home Agent* (HA) por meio da rede estrangeira, registrando o novo endereço através de uma mensagem de *Binding Update*, onde o HA responde com *Binding Acknowledgement*.

- Passo (4), MN atualiza seu endereço com o CN e, dependendo do suporte à mobilidade de CN, pode estabelecer a comunicação através do túnel, como se pode observar no passo (5), ou diretamente com MN, como no passo (6) [60].

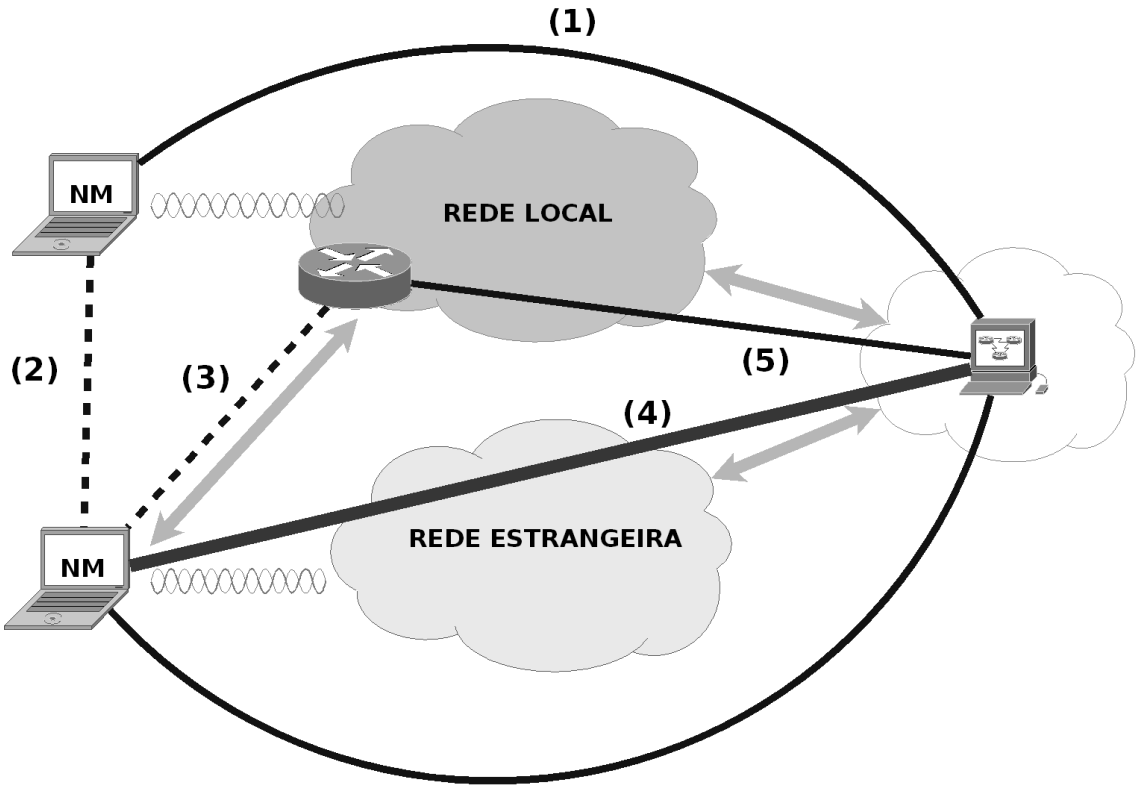


Figura 19 - MIPv6 - Arquitetura e operação [29]

2.6.2 *Fast Handover for Mobile IPv6*

O protocolo *Fast Handover for Mobile IPv6* (FMIPv6) foi padronizado em 2008 [61] e atualizado em 2009 [62]. Este protocolo tem o intuito de transformar o MIPv6 em um protocolo funcional, pois no MIPv6 existe uma latência muito alta durante o processo movimentação e registro do nó móvel na nova rede, chamado de tempo de *Handover*. Durante alguns segundos, o nó móvel fica incomunicável, isto é, não tem acesso à sua rede de origem e ainda não recebeu o IP na nova rede. Mesmo depois de possuir o novo IP, o nó móvel necessita aguardar a resposta referente ao seu *Binding Update* realizado na sua rede de origem.

Novos elementos fazem parte do processo de mobilidade deste protocolo, entre eles relacionam-se:

- *Access Point* (AP): Dispositivo da camada dois que provê a conexão sem fio;
- *Access Router* (AR): Roteador default do MN;
- *Previous Access Router* (PAR): Roteador default do MN antes de realizar o *Handover*;

- *New Access Router* (NAR): Roteador default do MN logo após realizar o *Handover*;
- *Previous CoA* (PCoA): O endereço *Care-of Address* do MN na antiga rede;
- *New CoA (NCoA)*: O endereço *Care-of Address* do MN na nova rede.

O protocolo aproveita informações da camada de enlace do modelo de referência OSI para sinalizar a troca de uma rede. Isto é, quando um dispositivo móvel reconhece que o sinal existente com o seu atual AP está enfraquecido e que existe um novo AP na área de cobertura, ele inicia o processo de conexão com esta nova rede, utilizando as mensagens introduzidas no FMIPv6 [62]:

- *Router Solicitation for Proxy Advertisement* (RtSolPr);
- *Proxy Router Advertisement* (PrRtAdv);
- *Fast Binding Update* (FBU);
- *Fast Binding Acknowledgment* (FBack);
- *Handover Initiate* (HI);
- *Handover Acknowledgment* (HAck) e
- *Fast Neighboor Advertisement* (FNA).

Iniciado o processo de h*andover*, existem dois modos de operação possíveis: o modo preditivo e o reativo. A diferença está no momento que o nó móvel recebe a última mensagem do processo de *handover*, antes ou depois de perder a conectividade com a sua rede atual.

No modo Preditivo, quando o MN realiza a negociação com o novo *Access Point*, ele envia ao seu AR uma mensagem *RtSolPr*, recebendo como retorno a mensagem *PrRtAdv*, inicia o processo de obtenção de endereço IP (*stateful* ou *stateless*) para configuração de um *New CoA*. Em posse de seu novo endereço, mas ainda se comunicando através de seu *Previous Access Router* (PAR), MN encaminha um *Fast binding Update* (FBU) a ele, solicitando que seu tráfego seja redirecionado através do *New Access Router* (NAR).

Já no modo Reativo, o processo inicial é idêntico ao modo Preditivo até o momento do FBU. A diferença está na falta de comunicação devido à mobilidade do MN, onde a mensagem de resposta *FBack*, que deveria ser enviada do PAR ao MN não ocorre. A Figura 20 mostra uma ilustração dos dois modos descritos.

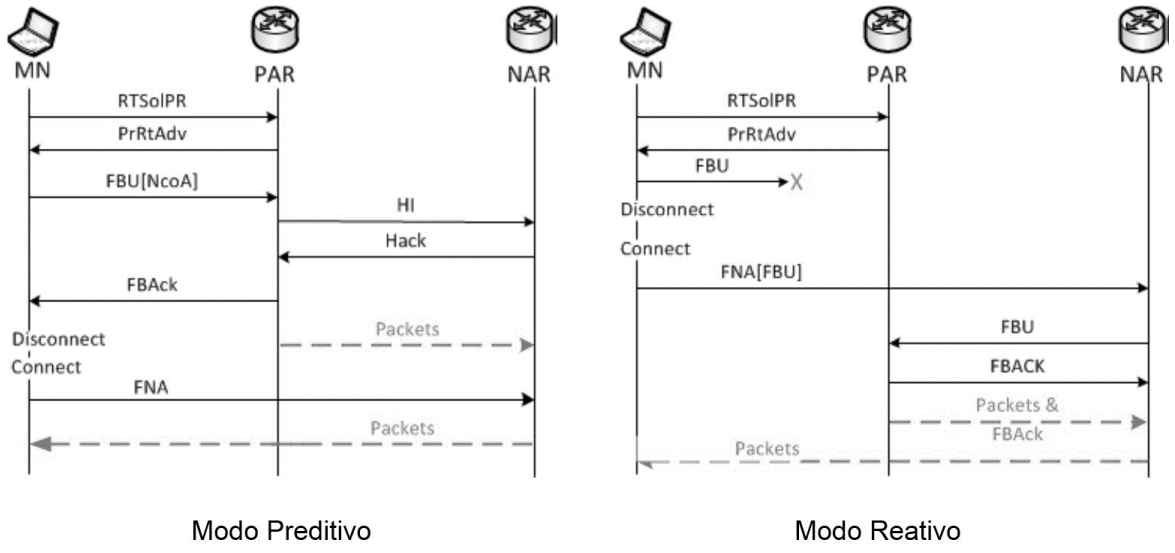


Figura 20 - FMIPv6. Troca de mensagens [62]

2.6.3 *Hierarchical Mobile IPv6*

No FMIPv6, a quantidade de sinalização existente no processo de *Handover* aumenta consideravelmente a complexidade do processo em comparação ao MIPv6. Para reduzir estas sinalizações foi desenvolvido o *Hierarchical* MIPv6 (HMIPv6), que para atingir seu objetivo, incluiu mais um agente no processo, chamado de *Mobility Anchor Point* (MAP) [63]. Esse agente é responsável pelo controle da mobilidade existente no domínio da rede, isto é, possui o mesmo MAP para todo o *Autonomous System* (AS), independente dos números de redes existentes. Com isto, passam a existir dois tipos de *Handover*: o local dentro do mesmo domínio e o externo quando ocorre a troca de domínios de rede.

2.6.4 *Proxy Mobile IPv6*

Definido em [64], PMIPv6 tem o intuito de incluir um ponto central no controle da mobilidade. Com isso, o nó móvel (MN) não precisa realizar os controles de entradas e saídas de rede, esta responsabilidade passa a ser exercida por duas novas entidades: *o Mobile Access Gateway* (MAG), que está na rede pelo qual o MN está entrando e pelo *Local Mobility Anchor* (LMA), que se encontra na sua rede de origem.

MAG é a primeira camada que detecta um *host* móvel (MN) associando-se a esse *host* e oferecendo uma conectividade IP. O LMA é a entidade que irá atribuir um ou mais *Home Network Prefixes* (HNPs) para o nó móvel.

A base fundamental do PMIPv6, ilustrado na Figura 21, está no MIPv6, estando o método utilizando conceitos como a funcionalidade do *home agent* (HA). O LMA e o MAG estabelecem um túnel bidirecional para encaminhamento de todo o tráfego de dados pertencente aos nós móveis. A gerência de mobilidade suporta uma liberdade de mobilidade dentro do domínio do PMIPv6, ou seja, um host móvel pode circular livremente dentro do domínio PMIPv6 sem alterar o seu endereço IP [65].

O MAG tem a função de detectar a chegada de um MN e realizar os procedimentos necessários para oferecer o serviço de mobilidade a ele. Por outro lado, o LMA tem uma função similar a do HA (Home Agent) no MIPv6, controlando a disponibilidade do serviço de mobilidade. Pelo LMA passam todos os pacotes da comunicação entre o MN e dispositivos externos ao domínio. Quando estiver no domínio do PMIPv6, o MN manterá sempre o mesmo endereço IPv6, ainda que mude seu ponto de acesso, sem se preocupar com qualquer sinalização de mobilidade, que diferente do MIPv6, é realizada pelo núcleo da rede [66].

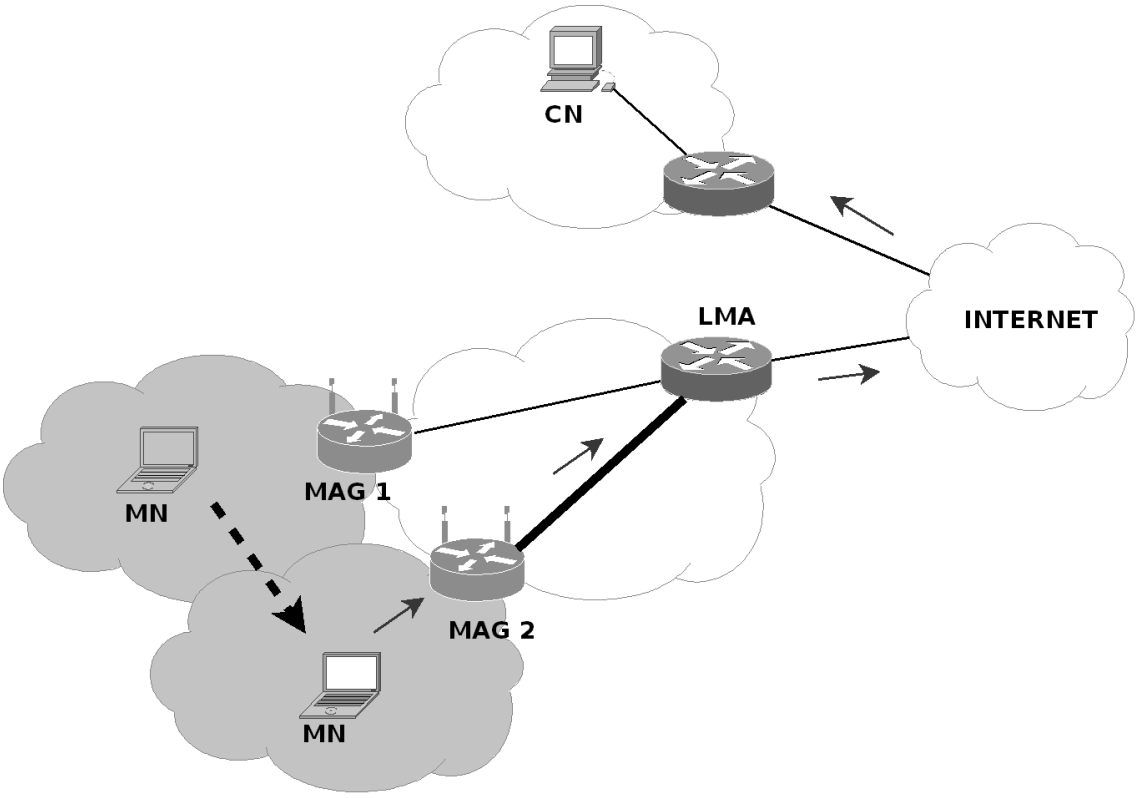


Figura 21 - Visão geral do PMIPv6 [66]

3. Métricas para Avaliação de Redes

Este capítulo trata dos métodos de avaliação em redes de computadores, baseados em métricas que dão suporte à realização de testes probatórios de qualidade. Como vem a ser a sistemática de análise em determinados cenários de operação, e a observação de seus resultados, oferecendo elementos para a viabilidade ou não de implementação de determinadas implementações. Também são observados formatos de testes de desempenho, como podem ser executadas simulações de tráfego na rede e, por consequência, a análise da resposta da rede a este tráfego.

3.1. *QoS - Quality of Service*

Com o aumento de demanda, nos anos 90, para que serviços de voz, vídeo e dados) tivessem sua infraestrutura isolada, crescendo o custo da comunicação, os serviços passaram a ser transportados via IP, surgindo o desafio dessas redes integradas garantirem que aplicações com características e requisitos diferentes pudessem compartilhar a mesma estrutura, mantendo a mesma qualidade e desempenho.

Sendo o protocolo IP um protocolo de *Best Effort*, todo tráfego é tratado da mesma forma, sem distinção, portanto, aplicações sensíveis ao atraso, por exemplo Voz e Vídeo, seriam tratadas da mesma forma que um tráfego de *e-mail*, FTP e qualquer aplicação P2P, provocando uma baixa qualidade na transmissão de Voz e Vídeo.

Neste contexto, entra o *QoS* (*Quality of Service*) [67], que consiste em tratar de uma forma diferente, fluxos que são diferentes.

Portanto, a Qualidade de Serviço em uma rede pode ser definida como a habilidade de uma rede fornecer o melhor serviço para determinados usuários ou aplicações, em detrimento de outros usuários e aplicações, ou seja, uma forma especial de dar um tratamento diferenciado para algumas aplicações.

A *QoS* é garantida pela rede, suas componentes e equipamentos utilizados. Do ponto de vista dos programas de aplicação, a *QoS* é tipicamente expressa e solicitada em termos de uma "Solicitação de Serviço" ou "Contrato de Serviço". A solicitação de *QoS* da aplicação é denominada tipicamente de SLA (*Service Level Agreement*) [68].

A SLA deve definir claramente quais requisitos devem ser garantidos para que a aplicação possa executar com qualidade.

Do ponto de vista dos usuários, tem-se normalmente que a qualidade obtida de uma aplicação pode ser variável e, a qualquer momento, pode ser alterada ou ajustada (para melhor qualidade ou pior qualidade). A alteração numa SLA implica normalmente numa nova solicitação de qualidade de serviço à rede em questão.

QoS se trata de uma funcionalidade para designar um conjunto de algoritmos capazes de fornecer vários níveis de tratamentos para diferentes tipos de tráfego na rede. O propósito dessa tecnologia é otimizar o uso da banda passante provendo um tráfego fim-a-fim eficaz e econômico. O *QoS* resolve a necessidade da aquisição de mais banda para a rede, pois supre a demanda de tráfego das LANs/WANs de forma inteligente e organizacional através dos mais diversos mecanismos que ele dispõe e é muito importante para as redes convergentes, pois as tornam capazes de transportar, de maneira bem próximo ao ideal, os mais diversos tráfegos, como: vídeo, voz e dados, de modo simultâneo sem interferências mútuas.

Cada tráfego recebe tratamento especial conforme suas características e é necessário que os cuidados especiais sejam obedecidos. A economia de banda é um dos principais benefícios do *QoS.*

É necessário considerar que não são todas as aplicações que realmente necessitam de garantias fortes e rígidas de qualidade de serviço para que seu desempenho seja satisfatório. Dentre as aplicações identificadas anteriormente, as aplicações multimídia são, normalmente, aquelas que têm uma maior exigência de *QoS.*

No mínimo, as aplicações sempre precisam de vazão (banda) e, assim sendo, este é o parâmetro mais básico e certamente mais presente nas especificações de *QoS.* Este parâmetro da qualidade de serviço é normalmente considerado durante a fase de projeto e implantação da rede e corresponde a um domínio de conhecimento bem discutido e relatado na literatura técnica.

Os fatores que determinam a qualidade na transmissão são: latência, *jitter*, perda de pacotes e banda passante, detalhados a seguir [67]:

- Latência ou *delay*, é o tempo gasto para iniciar outro procedimento de dados. O *delay* é subdividido em sensível ou não ao tráfego. O menor *delay* ocorre no sensível aa tráfego e existem variados tipos de *delays*, como: serialização, propagação e encaminhamento. De maneira geral define os bits do pacote dentro da interface física até a saída.

- *Jitter* é conhecido como: “Variação de *Delay*”, ou seja, é a variação do atraso entre os pacotes consecutivos e quanto menor o *Jitter*, maior sua prioridade, pois os pacotes vão estar nas filas cada vez mais juntos. O *Jitter* influencia reduzindo o *delay*, reduzindo também o prazo para entrega dos pacotes. Ele pode ser suavizado através das técnicas de compressão e das técnicas de *delay*.
- Perda de pacote é realmente inevitável, mas existem mecanismos de controle de perda de pacotes como: Controle de Bits com Erros - que varia de protocolo para protocolo, no TCP existe o controle de FCS (*Frame Check Sequence*) minucioso e que garante menores taxas de erros; e controle da falta de espaço em uma fila: É outra técnica importante para a correção do ajuste incorreto do pacote com *jitter*.
- *Bandwidth* se refere ao número de bits por segundo que pode, controladamente, ser expedido para sucesso na entrega. Se trata do “gargalo” do tráfego dos dados, da voz ou do vídeo. É importante usar técnicas de *bandwidth* para otimizar os processos de entrega dos pacotes. Essas normas usam de enfileiramentos extras para garantir um equilíbrio no percentual de transporte dos dados.

Os parâmetros de confiabilidade, retardo, flutuação (*jitter*) e largura de banda estão expostos na Tabela 6 [42].

Tabela 6 - Rigidez dos requisitos de *QoS* [42]

Aplicação	Confiabilidade	Retardo	Flutuação	Largura de banda
Correio eletrônico	Alta	Baixa	Baixa	Baixa
Transferência de arquivos	Alta	Baixa	Baixa	Média
Acesso à Web	Alta	Média	Baixa	Média
Login remoto	Alta	Média	Média	Baixa
Áudio por demanda	Baixa	Baixa	Alta	Média
Vídeo por demanda	Baixa	Baixa	Alta	Alta
Telefonia	Baixa	Alta	Alta	Baixa
Videoconferência	Baixa	Alta	Alta	Alta

3.1.1 Componentes do QoS

Existem dois princípios básicos para se aplicar uma política de qualidade de serviço adequada em redes IP, sendo eles: Serviços integrados (*Intserv*) e Serviços diferenciados (*Diffserv*).

3.1.1.1 Serviços integrados (Intserv)

O *Intserv* é uma arquitetura de qualidade de serviço, que tem o propósito de garantir níveis de qualidade de serviço fim a fim, através de recursos reservados e estabelecimento de chamada. Ele utiliza-se do protocolo RSVP (*Resource Reservation Protocol*) para sinalizar as necessidades de *QoS* para cada dispositivo ao longo da rede, permitindo que vários transmissores enviem os dados para vários grupos de receptores, eliminando o congestionamento da rede.

Esse protocolo é empregado para fazer as reservas; outros protocolos são usados para transmitir os dados. O RSVP permite que vários transmissores enviem os dados para vários grupos de receptores, torna possível receptores individuais mudarem livremente de canais e otimiza o uso da largura de banda ao mesmo tempo que elimina o congestionamento. [42].

Os serviços integrados (*Intserv*) possuem duas classes de serviços: serviço de carga garantido e serviço de carga controlada. O serviço de carga garantido: estabelece limites rígidos (que podem ser provados matematicamente) para atrasos de fila que um pacote sofrerá em um roteador, definida no RFC 2212 [69].

Serviço de rede de carga controlada: tem como foco as aplicações multimídia, permitindo com que pacotes com taxas muito altas passem pelo roteador sem que haja descarte de pacotes, por outro lado, não a garantias de desempenho. Portanto a um bom funcionamento apenas quando a rede está descongestionada, definida no RFC 2211 [70].

3.1.1.2 Serviços diferenciados (*Diffserv*)

É baseado no tratamento diferenciado de classes, podendo manipular diferentes tipos de classes de várias maneiras dentro da rede. Este tratamento é repetido nó-a-nó, ou seja, os pacotes de uma aplicação prioritária quando chegam a um nó (roteador) são separados e recebem um tratamento diferenciado.

Para obter serviços diferenciados, a rede tenta entregar um determinado tipo de serviço com base no *QoS* especificado por cada pacote, sendo assim, classificados, marcados, policiados, priorizados, descartados, e enviados pelo roteador de origem, até o roteador de destino [67].

3.1.2 O Serviço de Melhor Esforço

O protocolo IP oferece um serviço sem conexão baseado em datagramas, que não garante a entrega dos datagramas a tempo, não garante que eles cheguem ao destino na ordem correta e nem mesmo garante que eles cheguem no destino. As características citadas anteriormente são importantes para compreender esse comportamento. Os roteadores fazem o melhor que podem, se esforçam ao máximo, mas não podem fazer garantias a respeito da entrega dos pacotes. Esse tipo de serviço sem conexão é conhecido como serviço de Melhor Esforço (*Best Effort,* BE).

No serviço de melhor esforço, a rede tenta encaminhar todos os pacotes o mais rápido possível, mas não pode fazer qualquer tipo de garantia quantitativa sobre a Qualidade de Serviço. Além disso, o tráfego de dados é por natureza imprevisível e em rajadas, de modo que surge o problema de congestionamento, pois não é economicamente viável prover a rede para satisfazer as demandas de pico [71]. No entanto, bons resultados podem ser obtidos com o serviço de melhor esforço, se políticas de gerenciamento de filas e técnicas de controle de congestionamento apropriadas forem utilizadas [72].

3.1.3 QoS em Ambientes IPv6

Recursos como níveis de serviço garantido, segurança hierárquica e maior nível de confiabilidade foram adicionados às especificações do IPv6 através do comitê IETF.

Um sistema baseado puramente em IPv4 não possui capacidade de diferenciar os dados que são sensíveis a atraso, tais como streaming de vídeo ou de áudio, e aqueles que não são sensíveis ao tempo, tais como relatórios e transferência de arquivos. Streaming de áudio e aplicações de vídeo são muito sensíveis ao atraso de alguns pacotes.

Em ambientes IPv6, o *QoS* atua de maneira diferenciada para que as aplicações façam suas solicitações evitando uma demora desnecessária no link de WAN. O termo frequentemente utilizado para descrever este fenômeno é baixa latência [71].

Um aplicativo pode vir a compartilhar várias conexões a partir da utilização de níveis de prioridade e a sua distribuição pode ser feita em até sete níveis, da seguinte forma:

- Nível 0 - Sem prioridade de especificar;
- Nível 1 - O tráfego secundário (notícias);
- Nível 2 - de transferência de dados automática (email);
- Nível 3 - Reservado;

- Nível 4 - Com a presença de transferência em massa (FTP);
- Nível 5 - Reservado;
- Nível 6 - O tráfego Interativo (Telnet, janela); e
- Nível 7 - Controle de tráfego (roteamento, gerenciamento de rede).

A fragmentação de um pacote IP, é, ainda hoje, uma grande fonte de atrasos de pacotes, ou alta latência, sob o protocolo IPv4. Cada dispositivo conectado a uma rede possui um limite de dados definido dentro do pacote Ethernet e o IPv6 utiliza uma abordagem mais sofisticada para lidar com dados de aplicações solicitando tratamento prioritário. O dispositivo de origem fará uma consulta o destino, a fim de determinar o tamanho máximo da carga que exige ser tratada através de todo o caminho determinado pela conexão, ou seja, é feita uma análise ponto a ponto, para garantir que não haja pontos de congestionamento, o que pode aumentar o tempo de resposta de um sistema ou eventualmente causar a perda de um pacote. Realizada a checagem, o IPv6 ajusta os seus próprios parâmetros de modo a não gerar pacotes com um volume de dados superior a menor célula por onde este pacote trafegará (com o cuidado de não subutilizar os recursos) [73]. Esta abordagem, traz como benefícios a redução da fragmentação e também a latência, mas também pode resultar em uma utilização ineficiente [5].

Este mecanismo garante que, com um menor envio de dados por frame, ele irá conseguir uma maior largura de banda com redução de delay. A funcionalidade *QoS,* assim como o IPSec, terá de ser incluída em cada dispositivo de rede, a fim de ser implementada de forma otimizada, garantindo assim uma melhor utilização dos recursos da rede como um todo. Sem a utilização desta funcionalidade em determinados dispositivos, resultará em um tratamento de pacotes sem priorização, ou seja, de uma forma padrão com apenas uma camada adicional para passar, aumento o tempo de entrega, diminuindo a qualidade da rede.

3.1.4 QoS e computação móvel

Uma das características fundamentais que diferencia os sistemas móveis dos fixos é que eles têm que ser capazes de se adaptar a alterações de *QoS* resultantes da mobilidade, em vez de tentar oferecer garantias rígidas de *QoS* [71]. Algumas questões devem ser consideradas com relação ao impacto da mobilidade nos níveis de garantias que as estações móveis podem esperar:

- Efeitos do tipo do enlace: dispositivos móveis podem se conectar através de uma rede local, via modem ou então um enlace sem fio.
- Efeitos do movimento: Um dos principais problemas do movimento é devido ao *handoff*, que ocorre quando uma estação móvel se move de uma célula para outra célula adjacente.
- Restrições dos dispositivos portáteis: a principal limitação dos dispositivos móveis diz respeito ao seu tamanho e peso e a curta duração das baterias.

3.1.5 Qualidade de Experiência (QoE – Quality of Experience)

Os aspectos e métricas de *QoS*, não possuem um alcance em termos de percepção humana. Ao se referir às aplicações multimídia, a experiência ou percepção humana é importante para determinar a qualidade de tais aplicações. Existe aqui no tema desta seção a relevância da aplicação ou serviço estar satisfazendo à necessidade ou desejo do usuário.

Acompanhando a tendência, as novas arquiteturas não estão sendo mais avaliadas apenas em termos de aspectos de *QoS*, mas também em quanto ao suporte à *QoE* [66]. As métricas de *QoE* servem como extensão aos parâmetros do *QoS*, permitindo avanços nas transmissões de aplicações de áudio e vídeo em redes IP, permitindo a se proporcionar melhorias nos protocolos.

Na Tabela 7 [66] são apresentadas, por estarem em uso no artigo referenciado, as métricas PSNR (*Peak Signal to Noise Ratio*) e SSIM (*Structural Similarity Index).*

O PSNR é uma métrica de *QoE*, que estima a qualidade do vídeo em decibéis, comparando o vídeo original com o vídeo recebido pelo usuário e, para cada faixa de valores de PSNR, há uma qualificação para o vídeo que foi recebido pelo usuário, conforme é apresentado na tabela.

Tabela 7 - Valores de classificação do PSNR [66]

PSNR (dB)	**> 37**	**31 – 37**	**25 – 31**	**20 – 25**	**< 20**
Qualidade	Excelente	Bom	Aceitável	Pobre	Péssimo

A métrica SSIM (*Structural Similarity Index*), também utilizada para avaliação de *QoE*, baseia-se na medição quadro a quadro do vídeo original com o vídeo recebido pelo usuário. O SSIM compara a similaridade entre os vídeos nos seguintes aspectos: contraste,

luminosidade e estrutura. O SSIM é expresso como um valor decimal entre 0 e 1 e quanto mais próximo do valor 1, mais apurada é a qualidade do vídeo.

3.2. Métricas de Redes

Uma das principais dificuldades encontradas em projetos de redes é o atendimento das características de desempenho almejadas. Uma vez testada, pode ser essencial a realização de testes probatórios de qualidade. Muitas vezes, os engenheiros precisam analisar determinados cenários de operação, mais críticos, e observar se os resultados obtidos atendem às métricas desejadas ou são compatíveis com as validações realizadas [72].

Os testes de desempenho, são executados com a injeção de um determinado tráfego na rede e, por consequência, a análise da resposta da rede a este tráfego.

Existem três fatores principais envolvidos na determinação de qual o tipo de serviço a ser disponibilizado: largura de banda, atraso e perda de dados [72].

A largura de banda é cada vez mais exigida sendo contratadas maiores velocidades fim a fim. A transferência de dados, e-mail, seminários e discussões pela Web, além de voz sobre IP, estão exigindo mais largura de banda dos provedores de serviços. Para poder prestar suporte a estes serviços, a largura de banda contratada é normalmente estabelecida no SLA e comumente exige-se uma prova de que a conexão fornecida pelo provedor de serviços fornecera o valor acordado.

O atraso é outro fator de suma importância em um SLA, especialmente quando serviços em tempo real estão sendo usados. Estes serviços podem compreender seminários e palestras pela Web e voz sobre IP (VoIP). Tempos de atraso longos na rede podem fazer com que esses serviços sejam paralisados ou tenham sua qualidade reduzida. Quando o utilizando um serviço VoIP, tempos longos de atrasos podem interferir significativamente em uma conversa telefônica normal, o que é inaceitável para o usuário final. Outro fator limitante que está relacionado com o atraso é o grau de variação do mesmo. Se o atraso for razoavelmente pequeno, mas tiver uma variação considerável durante a transmissão, haverá problemas no uso de serviços em tempo real.

A perda de dados é obviamente mal vista em qualquer rede. O provedor de serviços precisará ter certeza de que o serviço Ethernet que está sendo fornecido não perderá quadros quando estes forem transmitidos pela rede.

3.2.1 *Benchmarking*

É o processo de comparação entre dois ou mais sistemas através de medições. Esta avaliação permite medir o desempenho de um sistema (ou subsistema), quando realizando uma tarefa ou conjunto de tarefas bem definidas [73].

O resultado de cada avaliação deve ser representado em forma de gráfico, onde a coordenada "x" deve conter o tamanho do quadro e a coordenada "y" deve fornecer o resultado dos testes. Deve haver pelo menos duas linhas para cada gráfico, uma teórica e outra com os resultados dos testes [74].

3.2.1.1 Request for Comments 2544

Apresenta testes que podem ser usados para descrever as características de desempenho de dispositivos de rede e a forma como os resultados devem ser apresentados. Possui embasamento na RFC 1242, que introduz as terminologias para interconexão de dispositivos de rede [73].

A RFC 2544 [75] define que sejam utilizados para teste quadros com tamanhos variados e que sejam enviados por um determinado intervalo de tempo e por um número definido de vezes. Isso porque todos esses tamanhos de quadro poderão ser usados na rede, sendo necessário verificar os resultados de cada um [76].

Os testes mencionados na RFC 2544 são definidos por vazão, latência, perda de quadros e análise fim-a-fim. O teste tráfego de quadros entre equipamentos trata de enviar ao DUT[7] um *Burst*[8] com espaços mínimos entre quadros e contar o número de quadros que forem encaminhados pelo DUT. Se o número de quadros encaminhados for igual ao número de quadros transmitidos, o comprimento do *Burst* será aumentado e o teste será executado novamente. Se o número de quadros encaminhados for menor do que o número transmitido, o comprimento do *Burst* será reduzido e o teste será executado novamente. O valor fim-a-fim será o número de quadros do *Burst* mais longo que o DUT consegue tratar sem perder nenhum quadro [75]. O teste embasado nesta RFC recomenda que os resultados de todos estes testes sejam apresentados nos formatos de texto e gráfico. Os

[7] DUT: Nome designado ao componente, equipamento ou sistema que deve ser testado.

[8] *Burst*: Rajada de tráfego de curta duração.

resultados poderão então fornecer dados concretos de desempenho para o provedor de serviço e o cliente.

Com relação à taxa de transferência, a vazão de dados expressa a quantidade máxima de dados que pode ser transportada de uma origem até o seu respectivo destino. Em qualquer sistema Ethernet, a banda passante máxima absoluta será igual à taxa de dados, em termos reais, os números não são exatamente como previstos, devido aos campos adicionais para que os quadros possam ser transportados e pelo espaçamento entre quadros, necessário para o funcionamento da rede. Os pacotes menores têm uma vazão efetiva menor do que o dos pacotes maiores, devido à inclusão dos bytes de preâmbulo e do espaço entre pacotes, que não contam como dados. A vazão máxima que pode ser obtida para os variados tamanhos de quadro são é verificada em: Tabela 8, 9 e 10 [76].

Tabela 8 - Vazão máxima para pacotes de sistema de 10 Mbit/s [76]

Tamanho do Quadro	Vazão de Dados	Preâmbulo e IGP	Quadros por Segundo
64 bytes	7,62 Mbit/s	2,38 Mbit/s	**14,88**
128 bytes	8,65 Mbit/s	1,35 Mbit/s	**8,45**
256 bytes	9,28 Mbit/s	0,72 Mbit/s	**4,53**
512 bytes	9,62 Mbit/s	0,38 Mbit/s	**2,35**
1024 bytes	9,81 Mbit/s	0,19 Mbit/s	**1,20**
1280 bytes	9,85 Mbit/s	0,15 Mbit/s	**0,96**
1518 bytes	9,87 Mbit/s	0,13 Mbit/s	**0,81**
1522 bytes	**9,87 Mbit/s**	**0,13 Mbit/s**	**0,81**

Tabela 9 - Vazão máxima para pacotes de sistema de 100 Mbit/s [76]

Tamanho do Quadro	Vazão de Dados	Preâmbulo e IGP	Quadros por Segundo
64 bytes	76,19 Mbit/s	23,81 Mbit/s	**148,81**
128 bytes	86,49 Mbit/s	13,51 Mbit/s	**84,46**
256 bytes	92,75 Mbit/s	7,25 Mbit/s	**45,29**
512 bytes	96,24 Mbit/s	3,76 Mbit/s	**23,50**
1024 bytes	98,08 Mbit/s	1,92 Mbit/s	**11,97**
1280 bytes	98,46 Mbit/s	1,54 Mbit/s	**9,62**
1518 bytes	98,70 Mbit/s	1,30 Mbit/s	**8,13**
1522 bytes	**98,70 Mbit/s**	**1,30 Mbit/s**	**8,11**

Tabela 10 - Vazão máxima para pacotes de sistema de 1000 Mbit/s [76]

Tamanho do Quadro	Vazão de Dados	Preâmbulo e IGP	Quadros por Segundo
64 bytes	761,90 Mbit/s	238,10 Mbit/s	**1488,10**
128 bytes	864,86 Mbit/s	135,14 Mbit/s	**844,59**
256 bytes	927,54 Mbit/s	72,46 Mbit/s	**452,90**
512 bytes	962,41 Mbit/s	37,59 Mbit/s	**234,96**
1024 bytes	980,84 Mbit/s	19,16 Mbit/s	**119,73**
1280 bytes	984,62 Mbit/s	15,38 Mbit/s	**96,15**
1518 bytes	987,00 Mbit/s	13,00 Mbit/s	**81,27**
1522 bytes	**987,03 Mbit/s**	**12,97 Mbit/s**	**81,06**

A largura de banda expressa a maior capacidade que pode ser obtida através da transferência. A vazão representa a taxa na qual a informação trafega nivelado pelo menor valor de transferência. A Tabela 11 apresenta os valores indicados para cada tipo de aplicação no serviço Ethernet:

Tabela 11 - Vazão típica de algumas aplicações [77]

Aplicação	Vazão
Aplicações Transacionais	**1 Kbps a 50 Kbps**
Quadro Branco (*Whiteboard*)	**10 Kbps a 100 Kbps**
Voz	**10 Kbps a 120 Kbps**
Aplicações Web (WWW)	**10 Kbps a 500 Kbps**
Transferência de Arquivos (Grandes)	**10 Kbps a 1 Mbps**
Vídeo (Streaming)	**100 Kbps a 1 Mbps**
Videoconferência	**500 Kbps a 1 Mbps**
Vídeo MPEG	**1 Mbps a 10 Mbps**
Aplicação para Imagens Médicas	**10 Mbps a 100 Mbps**
Aplicação para Realidade Virtual	**80 Mbps a 150 Mbps**

- A vazão é uma das métricas mais importantes quando se avalia qualidade de serviço de uma rede e é necessária para a operação correta de qualquer aplicação. Em termos práticos as aplicações geram vazões que devem ser atendidas pela rede.
- Ao se referir à latência, trata-se do tempo total gasto por um quadro desde a origem até o destino. Esse tempo absoluto é a soma dos atrasos do processamento nos elementos da rede e o atraso de propagação ao longo do meio de transmissão [76]. Para medi-la, um quadro de teste contendo uma marca de tempo (*timestamp*) é transmitido pela rede. A marca de tempo é então analisada quando o quadro é recebido de volta. Uma grande latência não indica que pode ocorrer uma perda de sincronização. A variação de tempo entre chegadas de pacotes do endereço de origem caracteriza-se como *Jitter*. O mesmo pode resultar em intervalos de tempo vazios dentro de um *Burst* de voz, de forma que a diminuição, ou até mesmo a perda destes intervalos, resultaria na falta de interpretação da informação no destino. Um valor máximo tolerado, sem que haja comprometimento da qualidade de voz, calculado segundo uma

média Gaussiana[9], considera que os valores devem ser menores do que 225 ms.

A Figura 22 demonstra o efeito do *jitter* entre o envio de pacotes na origem e o seu processamento no destino, causando uma entrega com a chamada "Variação de Pacotes por Atraso" e a entrega de pacotes fora de ordem.

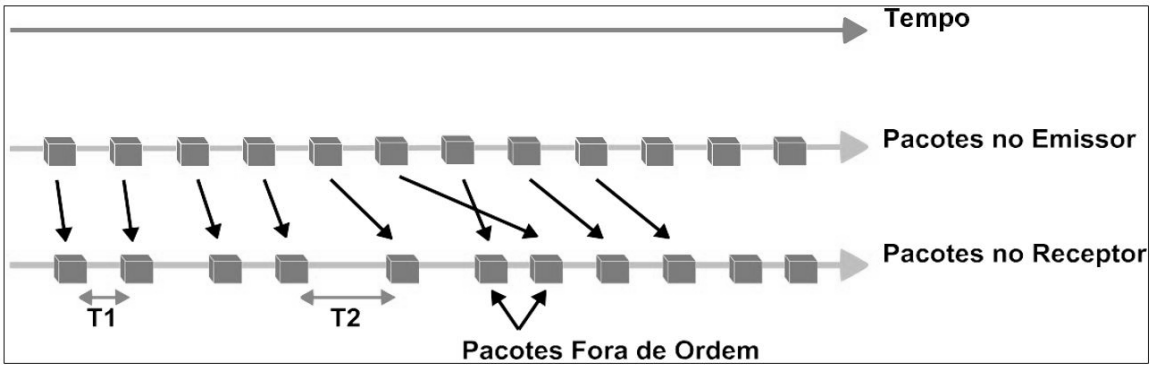


Figura 22- Efeito causado pelo *Jitter* [72]

- A perda de quadros analisa o número de quadros que foram transmitidos pelo transmissor e que nunca foram recebidos em seu destino. É normalmente chamada de taxa de perda de quadros, sendo expressa como uma porcentagem do número total de quadros transmitidos e os quadros podem ser perdidos ou descartados por várias razões, incluindo erros, assinatura excessiva e atraso excessivo [76]. Pacotes perdidos em aplicações que utilizam o protocolo UDP e RTP[10] não podem ser retransmitidos.
- Sobre os erros: a maioria dos dispositivos da camada de enlace descartará um quadro que tiver o valor de verificação do quadro incorreto, o FCS (*Frame*

[9] Gaussiana ou Distribuição Normal: Descreve uma série de fenômenos físicos e financeiros, possui grande uso na estatística de inferência. É inteiramente descrita por seus parâmetros de média e desvio padrão, permitindo se determinar qualquer probabilidade em uma Normal.

[10] RTP (*Real-time Transport Protocol*) é um protocolo utilizado em aplicações de tempo real e define como deve ser feita a fragmentação do fluxo de dados áudio, adicionando a cada fragmento informação de sequência e de tempo de entrega. O controle é realizado pelo RTCP (*Real Time Control Pro*tocol) e ambos utilizam o UDP como protocolo de transporte, que não oferece qualquer garantia de entrega em determinado intervalo. Os protocolos RTP/RTCP são definidos pela RFC 3550 do IETF.

Check Sequence). Assim, um único erro de bit na transmissão fará com que todo o quadro seja descartado. Esse é um dos motivos que faz com que o BER[11], que é fundamental em um serviço SONET/SDH[12], não tenha significado em Ethernet, pois a relação entre bits corretos e incorretos não pode ser averiguada [76].

- O fator mais comum para a perda de quadros é a sobrecarga excessiva da largura de banda disponível. Quando o limite for atingido, pode haver descarte de quadros [76].
- O atraso excessivo pode ser entendido assim: o atraso na rede varia do atraso em cada nó e na quantidade de nós entre origem e destino. A natureza das redes *Ethernet* torna possível o atraso de quadros por períodos consideráveis de tempo. Isso é importante para a análise, pois o testador estará "esperando" que todos os quadros transmitidos sejam recebidos e contados. Em algum momento, o testador tem que decidir que o quadro transmitido não será mais recebido e contar esse quadro como perdido. O intervalo de tempo mais comum usado para tomar essa decisão é a especificação RFC de dois segundos.
- Em uma análise fim-a-fim (*back-to-back*), a análise de quadros entre equipamentos envolve enviar ao equipamento testado (DUT) um *Burst* com espaços pequenos entre quadros e contar o número de quadros conduzidos por este. Se o número de quadros encaminhados for igual ao número de quadros transmitidos, o tamanho do *Burst* será aumentado e o teste será executado novamente [76]. Caso o número de quadros encaminhados for menor do que o número de quadros transmitidos, o comprimento do *Burst* será reduzido e o teste será executado novamente. O valor fim-a-fim será o número de quadros do *Burst* mais longo que o DUT consegue tratar sem perder nenhum quadro. O atraso fim-a-fim possui componentes de natureza fixa e de natureza variável. Estes componentes são definidos como:

[11] BER (*Bit Error Ratio*) é a taxa de número incorreto de bits, elementos, caracteres ou blocos recebidos do número total de bits, elementos, caracteres ou blocos enviados durante um intervalo de tempo especificado.

[12] SONET / SDH (*Synchronous Digital Hierarchy*): São padrões para a transferência de fluxo de bits sobre fibra óptica através de lasers ou luz altamente coerente LEDs.

- Atraso de Propagação: Este atraso é diretamente relacionado com o tempo de propagação do sinal no meio de transmissão, sendo este, função da velocidade da luz no meio. O atraso de propagação depende do tipo de meio, da distância percorrida e é considerado atraso fixo;
- Atraso de Empacotamento: Tempo necessário para se gerar um número suficiente de quadros de voz para preencher o *payload* do pacote IP. Para que esse atraso não atinja valores muito altos, os pacotes enviados podem conter somente um quadro, porém, isto reduz a eficiência do sistema;
- Atraso nos Nós da Rede: O atraso de enfileiramento é o principal atraso que os pacotes sofrem dentro da rede. Este atraso é composto de duas parcelas: uma fixa, referente ao tempo de transmissão do pacote, e outra variável, correspondente ao tempo de espera na fila até que o pacote seja atendido. Este atraso é responsável pela aleatoriedade do atraso total ao qual o pacote é exposto, assumindo valores inaceitáveis quando a rede estiver congestionada; e
- Atraso devido ao "*Dejitter Buffer*": O *jitter* é introduzido no sistema através do comportamento aleatório do tempo de enfileiramento dos pacotes nos roteadores. Uma das soluções que podem ser usadas para compensar esta variação é a introdução de *Buffers*[13] ("*Dejitter Buffers*"), com a função de armazenar os pacotes que chegam com atraso variável e entregá-los ao receptor. Se a variação do atraso for muito alta, o atraso adicional necessário para compensar a variação pode resultar em um atraso fim-a-fim inaceitável. É definido, então, um valor máximo de atraso aceitável para o "*Dejitter Buffer*". Qualquer pacote que chegar após esse tempo será descartado.

O alcance máximo de atraso fim-a-fim é firmado em 300 ms pela recomendação G.114. Sendo esse valor um limite máximo, isto quer dizer que acima desse valor a qualidade da transmissão se torna inaceitável. O limite confortável é estabelecido em 150 ms. Atrasos entre esses dois valores

[13] *Buffer*: Região de memória temporária utilizada para escrita e leitura de dados. Os dados podem ser originados de dispositivos (ou processos) externos ou internos ao sistema.

delimitam uma região de qualidade marginal, que pode ser aceitável para algumas aplicações de voz.

- A largura de banda para a transmissão de voz depende de vários fatores e pode ser calculada com facilidade de acordo com informações de diagnóstico, quantização da voz, algoritmos de compressão, etc. Além da transmissão de voz, as redes também são usadas com outras finalidades. Como a transmissão de voz em uma conversação telefônica deve ocorrer em tempo real, tais dados devem possuir uma prioridade em relação a outros dados com menor importância, obviamente, a decisão de se usar uma largura de banda maior ou menor deve ser tomada conforme as necessidades e prioridades da rede. Vale ressaltar que uma banda muito estreita para a transmissão de voz influencia negativamente na qualidade do serviço.

3.2.1.2 Request for Comments 2889

Esta RFC [78] fornece uma metodologia para avaliação de dispositivos para redes LAN (*Local Area Network*). Ela estende a metodologia da RFC 2544 [76], definida para a análise comparativa de redes interligando dispositivos, visando a análise de Switches e Roteadores. Ela define parâmetros para dispositivos que alteraram os quadros da camada MAC (Controle de Acesso ao Meio). A RFC 2889 fornece uma metodologia para avaliação comparativa de *switches*, analisando o desempenho, o controle de congestionamento, a latência, a manipulação e a filtragem de endereços. Além de apresentar testes já definidos, a RFC também descreve formatos específicos para a comunicação dos resultados dos testes.

Enquanto a RFC 2544 foi escrita como uma metodologia geral para todos os tipos de dispositivos de rede, a RFC 2889 foi escrita para abranger técnicas de avaliação de desempenho de equipamentos que desempenham tarefas de controle da Qualidade de Serviço (*QoS)*.

- O tamanho do *cache* de endereçamento (*Memory Fault*), analisa a capacidade de armazenamento de endereços para cada porta testada. Os quadros são transmitidos a uma taxa determinada de modo que seja verificado se o DUT aprendeu corretamente todos os endereços. A finalidade do teste é verificar o número máximo de endereços MAC suportados pelo DUT. Existindo um

endereço para ser atualizado na tabela, então o teste deve ser executado em uma porta que transmita para todas as demais portas do receptor. Caso exista uma tabela de endereçamento em cada porta, então o ensaio deve ser executado para cada porta [78]. O teste é executado com um mapeamento de tráfego "Um para Muitos". Os resultados do teste devem mostrar o tamanho da memória obtida para cada tamanho de quadro. Este teste exige, no mínimo, três portas.

- O teste taxa de endereçamento é muito parecido com o teste de vazão da RFC2544 [76]. A cada ensaio, quadros com múltiplos endereços baseados numa especificação de tamanho inicial são transmitidos a uma taxa especificada pelo usuário. O número de quadros recebidos em cada porta é contado e a taxa de recepção é calculada [78]. Este teste usa um mapeamento de tráfego "Um para Muitos", mas apenas uma porta é usada para transmissão de uma só vez. Os resultados do teste devem mostrar as taxas obtidas para cada tamanho de quadro.
- A taxa de *broadcast* especifica a taxa máxima com que o DUT recebe e encaminha quadros de *broadcast*[14] sem perda. Quadros são inicialmente enviados com uma taxa especificada pelo usuário. Geralmente é utilizada a taxa máxima teórica da porta. Este teste é configurado com um mapeamento de tráfego "Um para Muitos", mas apenas uma porta por vez é usada para a transmissão. Os resultados do teste devem mostrar as taxas obtidas para cada tamanho de quadro [78].
- O congestionamento determina o controle de congestionamento exercido quando múltiplas portas estão transmitindo em uma única porta, o que deve causar a sobrecarga do meio. Este teste é configurado para um mapeamento de tráfego "Muitos para Um". O resultado do teste deve determinar o número de quadros recebidos, o número de colisões e o número de pacotes perdidos e recebidos para cada tamanho de quadro [78].
- O bloqueio de entrada principal determina o atraso adicionado em uma interface de saída não saturada, quando os quadros são recebidos de uma interface de entrada, que também está tentando transmitir quadros para uma interface de saída congestionada. A configuração mínima é de duas portas, "A" e "B", transmitindo para uma terceira porta, "C", gerando o congestionamento

[14] *Broadcast*: É o processo pelo qual se transmite ou difunde determinada informação, tendo como principal característica que a mesma informação está sendo enviada para muitos receptores ao mesmo tempo.

da interface enquanto a porta "A" também transmite para a porta "D" de forma inconsistente. O resultado do teste deve mostrar o número de quadros recebidos, o número de colisões e os pacotes perdidos e obtidos para cada tamanho de quadro [72].

- O filtro de quadros com erro determina se o DUT aplica o filtro de quadros corretamente para alguns tipos de erros como quadros não reconhecidos, quadros com tamanho desproporcional, erros de CRC, fragmentação e erros de alinhamento. Este teste é configurado com um mapeamento de tráfego "Um para Muitos". Os resultados do teste devem determinar o tipo de erro de transmissão, o número de quadros transmitidos, o "*Interframe Gap*[15]" e o número de erro nos pacotes para cada tamanho de quadro [72],
- O entrelaçamento total (*Fully Meshed*) vem a especificar o número total de quadros suportados pelo DUT durante tráfego de todas as portas em teste. Para este ensaio, todas as portas devem transmitir e receber o tráfego a uma taxa específica onde cada uma das interfaces do DUT possa transmitir e receber quadros a partir de todas as outras interfaces sob teste, além disso, em cada porta são enviados quadros para todas as demais portas de forma uniforme e distribuída (*Round-robin*[16]). Os resultados do teste devem determinar o número total de quadros transmitidos a partir de todas as portas, o número total de quadros recebidos em todas as portas, bem como o percentual de perda de pacotes para cada tamanho de quadro [78].
- Muitos para muitos entrelaçamentos (*Many to Many Mesh*) determina o número total de quadros perdidos durante transmissão em todas as portas e o número total de quadros recebidos em todas as portas. Existem dois tipos de testes disponíveis: *Round-robin* e *Peak-load*[17] (pico de carga). Assume-se que o número de quadros que uma determinada entrada está recebendo, a partir de

[15] *Interframe Gap*: Dispositivos Ethernet devem permitir um período ocioso mínimo entre a transmissão de quadros Ethernet.

[16] *Round-robin*: Algoritmo usado em projetos de sistemas operacionais multitarefa, e foi projetado especialmente para sistemas *time-sharing*, pois ele depende de um temporizador.

[17] *Peak-load*: A máxima demanda de carga em um determinado período de tempo.

todas as portas, é o mesmo que será transmitido pela porta de entrada, ou seja, para transmitir em todas as portas deve-se transmitir de todas as entradas.

A taxa de transmissão é ajustada com base em dois parâmetros [73]:

  - a taxa mínima em que as portas podem receber devem ser utilizadas em todas as portas de transmissão; e
  - a taxa deve ser a metade do valor máximo, se a porta transmitir em modo h*alf-duplex*[18].

- Muitos para um (*Many to one*) determina a taxa máxima em que o DUT recebe e encaminha quadros de muitas interfaces com uma interface sem qualquer perda de quadros [78]. Apenas um grupo (contendo uma porta de recepção e múltiplas portas de transmissão) pode ser executado por vez. Os resultados do teste devem determinar as taxas obtidas para cada tamanho de quadro.
- Um para muitos (*One to many*) determina a taxa máxima em que o DUT recebe e transmite quadros de uma interface de saída para várias interfaces de recepção, sem quaisquer perdas de quadros. Apenas um grupo (contendo múltiplas portas de recepção e uma porta de transmissão) pode ser executado por vez. Os resultados do teste devem determinar as taxas obtidas para cada tamanho de quadro [78].
- O Entrelaçamento parcial (*Partially meshed*) é usado para determinar a taxa máxima do DUT, através do envio de quadros de múltiplas portas de recepção para múltiplas portas de transmissão, onde as portas de transmissão não recebem e as portas de recepção não transmitem. O teste deve utilizar um protocolo específico (Protocolo Servidor).

[18] *Half-duplex*: Quando se tem um dispositivo transmissor e outro receptor, e transmitem e recebem dados, porém não simultaneamente, a transmissão tem sentido bidirecional.

3.2.1.3 Request for Comments 3918

Descreve uma metodologia específica para a análise comparativa dos dispositivos de encaminhamento *multicast* IP [79]. É baseada em princípios estabelecidos na RFC 2544 [76], RFC 2432 [80] e nos esforços do Grupo de Trabalho para Metodologias por Benchmarking (*Benchmarking Metodology Working Group* – BMWG) [79].

Um cenário típico de teste é definido através de protocolos *multicast* (IGMP v1, 2, 3; PIM-SM; SSM), além do número dos grupos *multicast*, que deverão ser encaminhados.

- No teste de acúmulo é especificada, em seu ensaio, a vazão do DUT quando o cliente envia um grande número de grupos em uma determinada taxa. Este ensaio de estresse força a rápida atualização do grupo IGMP / DML na memória e, em seguida, encaminha o tráfego para todos os grupos. Os resultados devem incluir a perda de quadros por grupo [79].
- O teste de agregamento avalia a capacidade do DUT em manter a taxa de tráfego *multicast* IP constante quando se tem um número fixo de clientes que aderiram ao IGMP / DML e que foram redistribuídos entre sub-redes menores. Este teste utiliza uma estrutura de mapeamento "um para muitos" e requer pelo menos quatro portas sendo uma para transmitir e três para receber. Os resultados devem revelar o número de quadros perdidos e a vazão de quadros por grupo [72].
- A sobrecarga de grupo, por meio de seu ensaio, determina o tempo que o DUT leva para registrar clientes *multicast* para um novo grupo ou um grupo já existente na tabela de encaminhamento. Este teste utiliza dois tipos de estrutura de mapeamento sendo a primeira "um para muitos", para o tráfego *multicast* tal como nos outros testes, e "Muitos para Muitos", para o tráfego Unicast[16] como sobrecarga de tráfego [79]. Seus resultados devem indicar a recepção e transmissão de quadros por porta, o tempo que leva para um grupo ser adicionado à lista de encaminhamento e a taxa de carga.
- A sobrecarga de latência avalia a capacidade do DUT para transmitir o tráfego *multicast* com uma latência aceitável. Este teste utiliza duas estruturas de mapeamento sendo a primeira "um para muitos", para o tráfego *multicast* tal como nos outros testes, e o segundo "muitos para muitos" para o tráfego *unicast* como sobrecarga de tráfego. Seus Os resultados devem

demonstrar a perda de quadros por porta, a recepção e transmissão de tráfego por porta, a média de latência por endereço de grupo *multicast* e a taxa de carga [79].

- O teste de distribuição determina a capacidade do DUT para encaminhar o tráfego, de forma correta, para clientes *multicast* numa base por fluxo de porta (*Per-port*) [79]. No teste, cada porta de entrada dará entrada, IGMP / DML, a diferentes conjuntos de grupos *multicast*. Os resultados devem incluir perda de quadros e vazão de quadros [72].
- O teste de capacidade do grupo determina o número máximo de grupos *multicast* que podem ser registrados em um DUT, usando IGMP / DML, e quantos quadros *multicast* podem ser transmitidos. Este ensaio exige pelo menos duas portas, uma para transmitir e uma para receber, e usa a estrutura de tráfego "um para muitos". O resultado determina o número de grupos cadastrados.
- O teste para atraso em registro de grupo especifica o tempo que o DUT leva para registrar um cliente na tabela *multicast*. O teste mede o tempo decorrido entre o momento em que o DUT recebe a solicitação de registro de um grupo de IGMP / DML até o tempo em que os clientes *multicast* recebem a confirmação de registro no grupo. O teste exige no mínimo quatro portas sendo uma para transmitir, pelo menos duas portas para receber e uma porta para contagem, que permite que o teste possa derivar ao longo do tempo as informações para validação do tráfego. Os resultados devem determinar o tempo de atraso do grupo [79].
- O teste para atraso em cancelamento de grupo determina o tempo que o DUT leva para remover um cliente de uma tabela *multicast*. O teste mede o tempo decorrido entre o momento em que o DUT recebe a solicitação de cancelamento de envio de tráfego para o cliente e o momento em que o cliente deixa de receber o tráfego *multicast* [79]. Ele exige, no mínimo, quatro portas sendo uma para transmitir, pelo menos duas portas para receber e uma porta para contagem, que permite que o teste possa derivar ao longo do tempo as informações para validação do tráfego. Os resultados devem incluir o tempo de atraso do grupo.
- O teste de latência mede a latência média de quadros *multicast* enviados para clientes em várias sub-redes. O ensaio revela a quantidade de processamento

por *overhead*[19] é exigido pelo DUT para a transmissão de quadros *multicast*. Os resultados devem revelar a latência por grupo.

- O teste de entrelaçamento mede a taxa de tráfego do DUT por fluxo de tráfego (*Per-port*) durante a recepção e o encaminhamento de quadros em todas as suas portas. É semelhante ao teste de entrelaçamento total (*Fully Meshed*), referenciado na RFC 2889, exceto que este teste utiliza quadros *multicast* [72]. Este ensaio exige, no mínimo, três portas e a estrutura de mapeamento pode ser definida como "Muitos para muitos". O resultado demonstra a perda de quadros.
- O teste de vazão por mistura de classes avalia a vazão do DUT quando há uma mistura de tráfego *unicast* e *multicast* simultaneamente em várias portas. Para o tráfego *unicast*, o teste usa uma estrutura de tráfego "um para um". Para o tráfego *multicast*, é utilizada a estrutura de tráfego "um para muitos" e pelo menos três portas. Os resultados incluem vazão e perda de quadros [79].
- O teste de escala de grupo determina a vazão de *multicast* utilizando uma quantidade fixa de tráfego e aumento ou diminuindo o número dos grupos de *multicast*. O mesmo faz uso de uma estrutura de mapeamento "um para muitos", exigindo, no mínimo, três portas. Os resultados incluem vazão e perda de quadros.
- O teste para vazão de tunelamento determina a vazão de *multicast* quando as interfaces de um DUT ou de um conjunto de DUTs estão agindo com características de tunelamento. Aqui, o encapsulamento ou tunelamento refere-se a um pacote que contém um protocolo não suportado em um formato suportado pelo DUT. "um para muitos", é a estrutura de mapeamento utilizada, com um mínimo de duas portas exigidas [73].

[19] *Overhead*: É qualquer processamento ou armazenamento em excesso, seja de tempo de computação, de memória, de largura de banda ou qualquer outro recurso que seja requerido para ser utilizado ou gasto para executar uma determinada tarefa.

3.2.2 *Características Avançadas de Avaliação de Desempenho*

Com o crescimento da *Internet*, o projeto, a instalação e o gerenciamento de redes de computadores de alta velocidade possibilitaram o aparecimento de novas aplicações distribuídas, como as aplicações multimídia, vindo a exigir a aproximação destas duas áreas. Por padrão, a *Internet* trabalha com a "filosofia do melhor esforço"[20], onde os usuários compartilham largura de banda e têm a transmissão de seus dados concorrendo entre si [72].

Com o uso *QoS* , é possível oferecer maior garantia e segurança para aplicações avançadas, de forma que o tráfego destas aplicações passa a ter prioridade em relação a aplicações tradicionais. As redes estão se tornando cada vez mais complexas, usando tecnologias diversificadas (*Ethernet* sobre ATM, *Frame Relay* sobre ATM, *Ethernet* sobre POS)

O aumento de demanda de performance aliada à complexidade da convergência das redes tem começado a demonstrar deficiências na utilização do IP, pois não fez parte do projeto do protocolo garantir características necessárias para o correto funcionamento de serviços embasados em aplicações de voz e multimídia e esta fragilidade tem impulsionado a necessidade de *QoS* sobre IP [73].

3.2.3 *Novas Métricas de Teste*

Os ensaios de desempenho tradicionais executam medições com base no modelo de "fluxo de porta" (*Per-port*), que aborda questões como: desempenho de cada porta; vazão máxima; e média de *Jitter*.

Testes tradicionais, mesmo que necessários, não são suficientes para o modelo de rede atual, e, para isso, os testes devem abordar fluxos individuais de tráfego e fluxos.

As redes convergentes atuais, multiplexam diferentes aplicações num só dispositivo, combinando diferentes classes de tráfego. Cada tipo de tráfego pode ter um conjunto distinto de requisitos de desempenho. Os ensaios devem simular diferentes tipos

[20] Atualmente, a rede trabalha com a **filosofia do melhor esforço**, que implica em ausência de organização dos diversos tipos de fluxos de dados que trafegam e, consequentemente, falta de condições para garantir o desempenho das aplicações quando há congestionamento.

de tráfego determinando o impacto que este possui sobre o desempenho da rede e determinar a capacidade da rede para lidar com um alto fluxo de dados [72].

O fluxo de dados atual não pode ser testado em uma base por fluxo de porta (*Per-port*). Para determinar o verdadeiro *QoS,* deve-se abordar: todas as camadas de rede; os fluxos individuais e fluxos IP; e a transição entre as tecnologias de rede. Existe a necessidade, por quem opera a rede, de uma ferramenta que aborde um complexo conjunto de métodos de otimização e priorização que trabalhe em todas as camadas de rede. Esta ferramenta deverá ter a capacidade de medir:

- Rede Local Virtual (VLAN), Tipos de Serviço IP (TOS), *Diffserv*, *Multiprotocol Label Switching* (MPLS), voz e multimídia;
- Chamadas e conexões (Funções de Sinalização);
- Aplicações de rede; e
- Transição de dados entre diferentes tecnologias.

3.2.4 *Teste sobre Camadas*

A otimização do tráfego pode ser analisada conforme modelo de camadas, através dos seguintes conceitos:

- Camada 2 (*Data Link*): IEEE 802.1Q (*Virtual LAN*) e 802.1p;
- Camada 3 (Rede): *Diffserv*, TOS, MPLS RSVP; e
- Camada 4 (Transporte): Otimizar o tráfego com base em vários critérios, incluindo TCP ou UDP.

Na camada 2, os testes sobre 802.1p e 802.1Q possuem embasamento sobre a *tag* de VLAN do *frame Ethernet*. Na camada 3, verifica-se o correto funcionamento dos diferentes métodos de otimização (*Diffserv* e TOS, VLAN baseada em sub-rede ou endereço IP) e protocolos RSVP e até mesmo MPLS. Já para a camada 4, deve-se utilizar medidas baseadas na priorização de portas UDP ou TCP (por exemplo, FTP, TELNET e fluxos de tráfego http) [72].

Para garantir *QoS*, importantes fatores devem ser levados em consideração: A verificação das capacidades da rede; o comportamento do tráfego IP *multicast*; o

desempenho do *firewall* sob altas cargas; a movimentação de cargas com base em redes virtuais privadas (VPN); eficiência e a proteção contra condições extremas.

De acordo com a Tabela 12, testar todas as camadas de rede ajuda a determinar como as próprias camadas funcionam, como estas interagem com o usuário e a qualidade de serviço necessária.

Tabela 12 - Métricas de avaliação para camadas de rede diversas [72]

Camada	Análise	Métrica
Layer 2 - Data Link	Velocidade de dados entre dispositivos; Atraso entre pacotes; Habilidade para lidar com	*Throughput*; Latência; Perda de pacotes.
Layer 3 - Rede	Variação de atraso no fluxo de transferência da rede; Ordenamento dos pacotes; Acompanhamento do fluxo de pacotes; VLAN's (segmentação do *tráfego*).	*Jitter*; Monitoramento; *Throughput*, latência, e perda pacotes; Teste de protocolos e serviços.
Layer 4 - Transporte	Manipulação de rajadas (burst) para chamadas e conexões; Tempo de resposta da aplicação (vídeo, voz, FTP, HTTP, e-mail); Desempenho da rede (firewall,	Taxa máxima; Categoria de conexão; *Jitter*.

3.2.5 *Métrica por Fluxo de Dados (Per-flow)*

Um típico usuário de rede pode estar executando vários aplicativos simultaneamente. Isso significa que inúmeros utilizadores podem ter seus pedidos multiplexados em uma única porta, combinando várias classes de serviços ou fluxos de tráfego. Cada tráfego pode ter um conjunto distinto de desempenho (*QoS)*, que precisam ser medidos [73].

A métrica por *Per-flow*, faz uma avaliação além dos ensaios tradicionais por fluxo de porta (*Per-port*), fazendo com que haja uma avaliação real do fluxo do usuário.

Além dos testes de vazão, latência, *jitter*, perda de quadros e monitoramento de sequência, as métricas de *QoS* por *per-flow* incluem:

- Otimização dos fluxos de tráfego;
- Priorização dos fluxos de tráfego;
- Priorização de tráfego baseado em políticas como TOS / *Diffserv*, RSVP, MPLS ou IEEE 802,1;
- Segmentação dos fluxos de tráfego ou fluxos (*Virtual LAN's*); e
- Encaminhamento de tráfego apenas para endereços que atendam aos critérios de VLAN.

A perda de pacotes consecutivos caracteriza outro importante fator nas métricas de avaliação de redes com tráfego VOIP. Uma perda de vários pacotes em uma fila afetará a qualidade de voz e irá impor retransmissão de pacotes, assim, retardando ainda mais a rede.

Outra medida fundamental é o monitoramento de sequência de fluxo. Este monitoramento permite verificar se os pacotes enviados chegam em boa ordem. O desordenamento consecutivo faz com que a rede retransmita muitos pacotes, o que aumenta o tráfego e provoca uma maior degradação.

A avaliação de desempenho em *QoS* é importante tanto para medir a capacidade da rede para deslocar os dados (plano de dados), como a capacidade da rede para gerir aplicações (plano de controle). Estas análises incluem avaliações de desempenho de roteamento (RIP e OSPF) e da capacidade da rede para realizar a convergência no caso de uma falha. É importante também mensurar o efeito que a gestão de filas e políticas têm sobre o poder de transformação do indivíduo e, em última instância, o desempenho de dispositivos da rede.

3.3. Prova de Conceito

Prova de Conceito (do inglês *Proof of Concept* - PoC), se trata de um modelo prático que venha a auxiliar a coleta de dados e auxiliar em se provar o conceito estabelecido por uma pesquisa ou artigo técnico. Em Tecnologia da Informação (TI), o termo costuma ser relacionado ao desenvolvimento de um protótipo como ferramenta para provar a viabilidade de um projeto. Ela permite a constatação prática de uma metodologia, os conceitos e tecnologias envolvidas na elaboração de um projeto, com a característica de ser de curto

prazo, geralmente restrita a um segmento de rede, para se captar a experiência junto ao cliente, de forma antecipada [81].

Alterações do projeto de uma rede de computadores devem ser testadas antes de qualquer imposição ao usuário, com oportunidade de se testar dispositivos existentes, novos equipamentos e versões de sistemas, sempre antes em ambiente que não seja o de produção, ou, quando não for possível, como esse projeto de dissertação, realizar em segmento a parte da rede que se encontra funcionando. De acordo com [81] a prova de conceito, entre outras, pode assumir formas como:

- Lista de tecnologias (frameworks, padrões, arquiteturas etc.) conhecidas que pareça adequada ao projeto;
- Esboço de modelo conceitual de uma solução;
- Simulação de uma solução através de ferramentas de software; e
- Protótipo executável.

A partir da prova de conceito pode se partir para a avaliação dos resultados dos testes de aceitação e certificação e, com eles, se orientar nas realizações de alterações na estrutura lógica e física.

Para iniciar a prova de conceito, o primeiro passo é avaliar o que será validado inicialmente durante a etapa de testes, se as tecnologias condizem com as necessidades do cliente e com a finalidade a qual se propõe o projeto. No segundo passo, definido o ambiente de teste, deve-se identificar o segmento de rede menos crítico ou aquele onde os usuários serão menos afetados para a construção de um protótipo. O terceiro passo é instalar e configurar os equipamentos e sistemas necessários no ambiente do cliente. No quarto passo, definem-se os testes pertinentes, segundo o modelo de protótipo definido anteriormente. Neste momento, scripts de teste devem ser construídos para satisfazer as possibilidades de funcionamento da rede. No quinto passo temos a análise dos resultados dos testes que servirão como referência para possíveis correções no modelo do protótipo e, posteriormente, irão compor a documentação final do projeto.

No caso de um protótipo executável, a prova de conceito pode ser feita com uma demonstração. No caso de um protótipo conceitual, por meio de argumentação, inspeção e raciocínio. No caso de uma simulação, requer a configuração e a execução do modelo simulado com dados informados ou obtidos dos critérios de avaliação e, em seguida, da coleta e análise dos dados resultantes do modelo.

A prova de conceito inclui a análise e discussão de questões específicas de cada teste, definido e executado segundo o modelo definido no protótipo. Os resultados dessa avaliação são analisados não apenas para determinar se os requisitos importantes para o projeto podem ser atendidos, mas também para verificar a validade desses requisitos. Nesse momento, tais requisitos podem ser modificados se ainda não estão necessariamente bem entendidos pelos envolvidos.

E os resultados dos testes devem ser utilizados para fazer alterações na estrutura atual do projeto, desde a infraestrutura, segurança e gerenciamento de especificações desenvolvidas até o momento de avançar para a proposta final do projeto. Caso sejam necessárias alterações na configuração da rede, o projetista deve ter o discernimento necessário para identificar quais dispositivos ou sistemas correlatos devem ter suas configurações alteradas a fim de manter o estado de consistência da rede. Neste ponto, entende-se por correlação o fato de haver dois ou mais dispositivos ou sistemas que possuem a característica de uma alteração no estado ou configuração em um deles, implicar em uma ação nos demais.

A metodologia é recomendada para evitar imprevistos durante a execução do projeto, comprovando o bom entendimento do escopo, que os requisitos de projeto são bem definidos e o seu desenvolvimento pode ser avaliado como tendo baixo risco para o cliente [81].

4. Trabalhos Relacionados

Neste capítulo, são apresentadas observações realizadas a partir de projetos, dissertações e artigos que tratem e serviram de referências relativas à transição entre protocolos IPv4 e IPv6, mobilidade e avaliações de cenários de testes de rede.

4.1. Principais Contribuições na Área.

Como foi possível observar, os novos mecanismos incorporados pelo IPv6 visam suprir as deficiências apresentadas pelo IPv4 ao longo dos anos. Neste sentido os trabalhos descritos a seguir abordam aspectos relacionados com a migração do IPv4 para o IPv6 e aplicação de mobilidade no mesmo ambiente, e representam o estado da arte.

Finney, J. Schmid, S. e Scott, A [1] tratam da probabilidade que, mesmo após a implantação do IPv6 no mundo real, um número considerável de aplicações e dispositivos IPv4 "legados" permanecerão em uso regular por muitos anos. Mesmo com os trabalhos focados no desenvolvimento de protocolos e ferramentas para facilitar a transição do IPv4 para o IPv6, os protocolo e ferramentas, à época, estavam projetadas para operar em um ambiente móvel. O artigo documenta a motivação, *design*, implementação e avaliação experimental da mobilidade 4 em 6 (*mobile 4-in-6*), tecnologia de transição IPv4 / IPv6 4 em 6 com base no padrão IPv6 móvel, que fornece suporte transparente para aplicações somente em IPv4 em ambientes somente IPv6.

Em sua dissertação de mestrado, C. R. dos Santos [20] analisou as implicações da adoção de IPv6 em Ambientes Cooperativos Seguros. Considerando que uma rede IPv6 não será efetivamente útil se não permitir a ocorrência de comunicação com outras redes na Internet, tanto IPv4 quanto IPv6, seu trabalho estudou os cenários de integração entre redes IPv6 e IPv4 bem como os mecanismos de transição aplicáveis a cada cenário.

César A. H. Loureiro, Liane M. R. Tarouco, Lisandro Z. Granville e Leandro M. Bertholdo [29] , em seu artigo, analisaram e avaliaram algumas implementações usadas no provimento de mobilidade em IPv6, medindo o desempenho, dificuldade de implantação e estabilidade das implementações. Constataram que nos protocolos "híbridos", o HIP se mostrou o protocolo mais viável a utilização, por implementar segurança de dois níveis (de endereçamento e de comunicação). No entanto, verificaram que é necessário analisar melhor o impacto da criação de túneis entre cada nó móvel e sua *home network*, pois uma grande

quantidade de túneis podem gerar problemas de escalabilidade em grandes redes e concluíram que a mobilidade sobre IPv6 como uma solução fim-a-fim, precisava ainda evoluir. Identificraram também que mais estudos eram necessários para prover serviços utilizando mobilidade sobre IPv6 para o usuário final, avançando os estudos sobre mobilidade utilizando protocolos de *layer-2* do modelo de referência OSI, como MPLS e OpenFlow.

C. E. Perkins [57] citou o *Mobile IP*, protocolo baseado no IP, proposto por um grupo de trabalho dentro do IETF (*Internet Engineering Task Force)*; baseado na possibilidade de se utilizar dois endereços IP: um endereço residencial fixo e um *care-of address* que muda a cada novo ponto de ligação. O artigo apresenta o padrão *Mobile IP* em detalhe técnico moderado e disponibiliza ao leitor uma riqueza de informações complementares.

Deguang Le, Xiaoming Fu e Dieter Hogrefe, no artigo "*A review of mobility support paradigms for the internet"* [60] observaram a forte necessidade de proporcionar dispositivos de conectividade para a comunicação entre os dispositivos na Internet, a qualquer momento e em qualquer lugar. Neste artigo, revisaram a pilha de protocolos TCP/IP, analisando os problemas associados no ambiente de mobilidade. Também investigaram as técnicas de apoio à mobilidade e soluções existentes de apoio à mobilidade na Internet. Classificaram as soluções propostas com base nas camadas de protocolo e apresentaram paradigmas para cada categoria da camada. Seus resultados mostraram que não existe uma solução única que combina perfeitamente endereços e apoio à mobilidade para a Internet. Por fim, concluiu-se a pesquisa com recomendações de recursos que devem ser atendidas em suporte à mobilidade Internet.

Wang, Li e Yan [63], em seu trabalho, compararam o Handover HMIPv6 e MIPv6. Um esquema que suporta uma transferência rápida de forma eficaz em redes IPv6 móveis hierárquicas (HMIPv6) é apresentado. Em HMIPv6 quando um nó móvel (MN) se move a partir de um domínio do mapa para outro, pode enfrentar interrupção de comunicação, bem como perda de pacote devido a uma transferência de longa latência. Para lidar com esses problemas, o esquema de entrega rápida de FMIPv6 é adotada para otimizar o desempenho da transferência. A latência para vários protocolos de transferência foi comparada com o esquema proposto com o modelo de análise.

No artigo de R. I. Meneguette, L. F. Bittencourt e E. R. M. Madeira [65], a fim de tirar proveito de todas as interfaces de rádio do veículo e para dar boa qualidade de serviço para aplicações veiculares, desenvolveram uma política de seleção de *handover* baseada na

lógica fuzzy, que indica qual é a melhor interface a um determinado fluxo. Utilizaram o simulador NS3 para analisar a política de seleção de interface. E compararam a mesma a uma política baseada em limiares. Observamos que o mecanismo proposto apresentou um tempo de troca de fluxo baixo, com menor perda de pacotes e menor atraso.

E. A. M. AVELAR, L. L. MARQUES, T. Bemerguy e K. L. Dias [66] citam, em seu artigo, que o gerenciamento de mobilidade eficiente é um aspecto fundamental para o sucesso de aplicações móveis multimídia. Seu trabalho descreve e avalia uma implementação do PMIPv6 com a avaliação sendo realizada através de um *testbed* IEEE 802.11 considerando métricas de QoS e QoE para avaliar o suporte do protocolo para tráfego multimídia. Além disso, propuseram uma otimização baseada no nível de sinal do terminal para antecipar o *handoff*.

D. Chalmers e M. Sloman [72] em seu artigo, realizam o levantamento de conceitos e técnicas de *QoS* para ambientes de computação distribuída móveis. Os requisitos de computação móvel atual e futura são examinados e os serviços necessários para apoiar a mobilidade são discutidas. Conceitos genéricos de especificação e gestão de *QoS* são estudados e seguido por uma análise dos trabalhos de *QoS* específicos para ambientes de computação móvel.

Em L. Zimu, P. Wei e L. Yujun [82] são apresentados fundamentos da tecnologia de Tradução IVI [50] seguido de exposição de um modelo para implementação do método de transição entre os protocolos IPv4 e IPv6 em servidores de um ISP (*Internet Service Provider*).

No artigo de Oliveira, E. R. de, Cascardo, T. L. de S. e Loureiro, A. A. F. [83], foi citado que o IPv6 Móvel (MIPv6) foi proposto como solução para permitir que estes dispositivos se comunicarem com a Internet, mas o protocolo não diferencia mobilidade global de local, adicionando carga à rede e não realizando rápidos handoffs. Para superar este mau desempenho, mecanismos hierárquicos de gerenciamento de mobilidade foram propostos, realizando uma análise comparativa entre estes diferentes mecanismos.

Menth, Klein e Hartmann [84] demonstram as oito conjunções de agentes necessários para prover mobilidade sobre LISP, no relacionamento entre redes LISP e redes Não-LISP.

Kong e Lee [85] compararam o tempo de *Handover* dos protocolos MIPv6, HMIPv6, FMIPv6 e PMIPv6, através de simulações e análise das mensagens dos protocolos.

No artigo de H. Hou, Q. Zhao e Y. Ma [86], foram expostos os principais mecanismos de transição, propondo uma solução para suavizar a transição para IPv6 baseado em túneis e tecnologia de tradução.

Da Silva , Douglas Chagas e Monteiro, Claudio de Castro [87], também trabalharam com análise de desempenho de rede sobre mobilidade, e em seu trabalho eles realizaram medições com a avaliação dos os valores de latência de *handover* do protocolo SMIP (*Specialized Mobile IP*), que vem a ser uma implementação *open source* baseada no MIP, e o protocolo mostrou-se mais eficiente em razão principalmente do mecanismo de sinalização utilizado, seus valores obtidos, mensuram apenas o desempenho dos algoritmos do protocolo SMIP e não foram considerados no cenário: tráfego de fundo, disputa no canal de acesso a rede, ou a utilização de serviços de rede TCP ou UDP.

Observou-se também, a partir dos resultados encontrados, que sua utilização em ambientes que requerem valores de latência muito pequenos (voz e vídeo), são viáveis. O protocolo pode ainda trabalhar de forma conjunta com alguma métrica de decisão de *handover*, tendo seu acionamento implementado através de gatilhos.

Ressalta-se, mais uma vez, o fato de não avaliarem o comportamento do protocolo quando utilizado em ambiente de "stress" computacional, bem como não foram considerados os atrasos provenientes das conexões de *Internet*.

No artigo de Loureiro, César A. H. [88], o trabalho se concentra em três propostas para utilização de mobilidade sobre IPv6: MIPv6, PMIPv6 e DMMS (*Decentralized Mobility Management Service*), com abordagem em suas características e funcionalidades.

4.2. Lições Aprendidas

Nesta seção são descritas as lições aprendidas através dos conceitos e trabalhos anteriormente descritos. Estas lições auxiliam na elaboração e desenvolvimento deste trabalho.

Dentre as estratégias de transição do IPv4 para o IPV6, a Pilha Dupla se mostrou a mais viável em função da determinação do documento de referência *e-Ping* [4], que deve ser usado, em um primeiro momento, a longo prazo pela Administração Pública Federal.

Não é possível implementar IPv6 e economizar IPv4 sem algum tipo de perda no lado do usuário, a não ser que refira a apenas *backbone* e/ou plano de controle (gerência).

Deve-se buscar identificar pessoas que possam contribuir e convidá-las a fazer parte do projeto, os treinamentos no assunto, como os do NIC.br, colaboram com a criação de uma cultura de aceitação ao projeto. Também é necessário compreender que migrar tudo para IPv6 não será a solução dos problemas sem a disponibilização de conteúdo disponível, se o cliente não estiver preparado para a migração e se a operação, assim como o suporte, estará pronta para operar esta rede.

A pilha dupla se mostra ser, ainda hoje, a melhor escolha para provedores e redes corporativas, isso se não ocorrer a falta de endereços IPv4 válidos e for possível utilizá-la.

O rápido esgotamento dos endereços IPv4, a existência de equipamentos legados onde não é possível utilizar IPv6 e a presença de equipamentos somente IPv6, por falta de IPv4 livres, criaram a demanda por outras técnicas de transição.

A convergência tecnológica, que se apresenta no decorrer das décadas, com atualizações e mudanças de padrões, é um processo natural por ela facilitar o gerenciamento das redes, a interoperabilidade, o desenvolvimento de novas aplicações e serviços, reduzindo custos, de forma geral.

É importante avaliar se é preciso investir agora em equipamentos que suportam uma determinada técnica, para serem usados daqui a um ou dois anos, ou se é melhor esperar algum tempo até que tecnologias melhores e mais baratas, do ponto de vista financeiro e computacional, estejam mais maduras. Um dos pontos a considerar na escolha das técnicas de transição a serem utilizadas é se elas são *stateless* ou *stateful*, sendo as *stateless* preferíveis, por escalarem melhor possuir custo mais baixo. No caso de uso de técnicas *stateful*, é recomendável que estejam implantadas nos equipamentos dos usuários e não no provedor.

No geral, as técnicas de tradução, tanto quanto as de túneis, provocam a redução do MTU no escopo em que são usados na rede. As técnicas baseadas em tradução aparentemente vêm a oferecer vantagem por não encapsularem o pacote novamente, elas apenas traduzem e trocam os cabeçalhos na camada IP.

O tunelamento deve ser empregado juntamente com a Pilha Dupla para infraestrutura externa à organização que não suporta IPv6. Já a tradução deve ser evitada por:

(1) não suportar características avançadas de IPv6, como segurança fim-a-fim;

(2) impor limitações à topologia da rede, pois as respostas de qualquer mensagem enviada pelo roteador de tradução devem retornar para o mesmo; e

(3) pelo roteador de tradução se apresentar como um ponto único de falha.

Além das atualizações de softwares ou possíveis substituições de equipamentos, e da forma de distribuição dos endereços, deve-se habilitar um servidor DNS com suporte à resolução de nomes para IPv6; habilitar o serviço de DNS reverso; habilitar o modo pilha dupla em servidores e roteadores; e escolher um protocolo de roteamento no lugar de rotas estáticas.

Foram testadas algumas propostas de provimento de mobilidade para IPv6, demonstrando a usabilidade de cada protocolo estudado [29]. Na análise realizada por transferência de dados não houve problemas de perda de conexão. Na análise do tempo de *handover*, FMIPv6 tem o menor tempo, no entanto, é incomum a existência de duas interfaces wireless em dispositivos móveis hoje em dia, o que elege a implementação do protocolo PMIPv6 como o melhor resultado a este respeito, com um tempo aceitável de *handover*, baixa utilização do pacote de controle e compatibilidade com qualquer sistema operacional utilizado no *Mobile Node*, pois o *Mobile Node* não precisa realizar qualquer gestão sobre a mobilidade. Porém, este protocolo não implementa a segurança advinda do IPSec, implementada nos outros protocolos classificados como "puros".

No entanto, é necessário analisar melhor o impacto da criação de túneis entre cada nó móvel e sua *home network* [89], pois uma grande quantidade de túneis podem gerar problemas de escalabilidade em grandes redes [29].

A mobilidade sobre IPv6 como uma solução fim-a-fim, ainda se encontra em evolução.

5. Ambiente e Experimentos realizados

Este capítulo propõe a apresentar a prática do trabalho, baseada nos conceitos e experimentos citados nas seções anteriores, bem como a descrição do ambiente que serve de modelo para a *PoC*, a coleta de dados de operação, resultados e avaliação dos mesmos.

Este trabalho se baseia na implementação do Departamento-Geral do Pessoal, com vistas a se adquirir experiência de projeto, não sendo possível, neste caso, comparar os resultados com arquiteturas e tecnologias existentes, pois as composições são diversas não se pode assumir um padrão, em virtude do risco ao se empregar as alterações diretamente no ambiente operacional e o mesmo é baseado em duas principais atividades:

a) Implantação, no formato prova de conceito, a migração de IPv4 para IPv6 e ativação de um protótipo de mobilidade nesse ambiente.
b) Análise do comportamento, por meio de métricas *QoS*, do ambiente experimental.

Para o item (a), são utilizados os conceitos teóricos apresentados no Capítulo 2, com a opção de uso da estratégia de Pilha Dupla, conforme justificativa apresentada anteriormente, que permita a implementação da mobilidade no DGP.

Para o item (b) é implementada uma *PoC* onde são desenvolvidos testes práticos de análise de desempenho de rede, fazendo uso de experimentos por meio de transferência de arquivos em rede local, em meios físicos diversos, uso da medida de tempo de latência, uso do protocolo ICMP, por meio do comando *ping*, levantando o tempo de reposta em uma consulta, na análise de funcionamento do Tunnel Broker, por meio de teste de latência em sites operarando sobre pilha dupla, cáluculo de Round-Trip Time (RTT) em busca da variação de delay obtido entre MN e CN em comunicações com e sem mobilidade e captadação dos tempos de Handover durante a troca de Rede DGP (HA) para Rede EBNet (FN), a fim de aproximar a teoria com a prática e demonstrar os processos de configurações de equipamentos.

5.1. Ambiente de Análise.

A configuração lógica de rede do DGP compreende: uma conexão de provisão de acesso dedicado à *Internet* de 100 Mbps; hospeda 160 servidores virtuais configurados de forma heterogênea. Os sistemas operacionais e servidores de aplicação atendem mais de 200

sistemas para usuários militares da ativa e reserva, servidores civis, dependentes e pensionistas, que também é parte integrante da Intranet do Exército Brasileiro. Existe um sítio de contingência em organização externa ao Quartel General do Exército que conta com 1100 clientes desktop/notebooks em sua rede local.

Em sua estrutura, a segurança se apresenta por meio de dispositivos *Aker Firewall UTM*, versão 6.7, que também reúne funções de VPN, detecção e prevenção de intrusões de rede, *antispam*, antivírus, filtragem de conteúdo *web*, FSense (filtro de conteúdo e prevenção de invasões), além de serviços regulares de ambiente data center, que podem forçar alterações em análises de desempenho e volume de tráfego, que não podem ser descartadas.

5.1.1 *Arquitetura e Configuração do Ambiente de Testes*

Para composição da *PoC* A arquitetura de rede compreende a divisão lógica em sub-redes como a DMZ Intranet – serviços de rede (DNS, AD, IIS, BD), DMZ *Internet* – sistemas e sites, Rede Administrativa – tráfego de backup, Rede DRAC – Rede de acesso remoto aos servidores, Rede Interna – estações de trabalho e Intranet PUB – rede pública para visitantes (SIH-EB), com uma faixa reservada de endereçamento IPv4, segmentadas em faixas isoladas entre si, como se vê na Figura 23. A mesma se encontra mais detalhada em Anexo IV - Topologia Física Interna do DGP e Anexo V - Topologia Lógica Interna do DGP.

Baseando-se nas recomendações do Comitê Gestor da *Internet* no Brasil e do Núcleo de Informação e Coordenação do Ponto BR [44] propõe-se que para a distribuição dos recursos de endereçamento dentro do DGP, com seu porte de topologia mais reduzida, seja oferecido um bloco /64; seguirão o mesmo formato de distribuição de servidores de autenticação, Firewall, DNS e a rede de voz, que será configurada com endereços de nível local.

A Tabela 13 descreve a distribuição de pools de endereços, distribuídos ao Departamento, bem como a faixa disponibilizada em cadastro realizado em servidor *Tunnel Broker*.

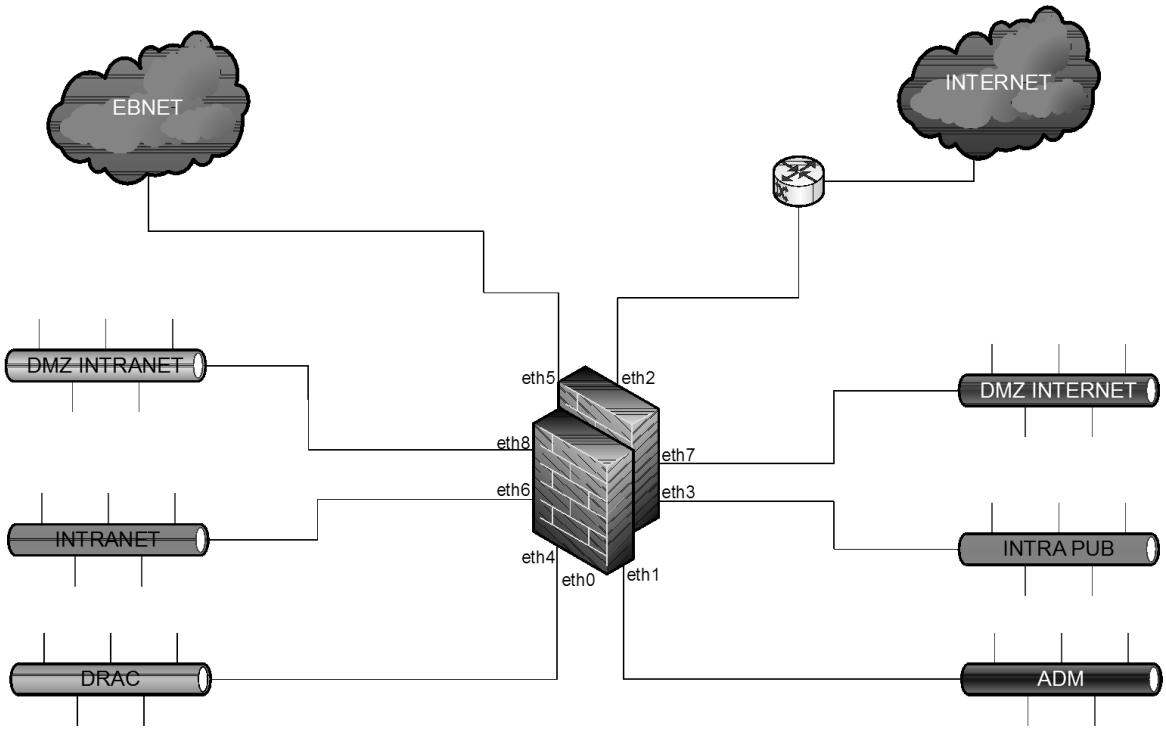


Figura 23 - Arquitetura lógica de rede do DGP

Os endereços IPv6 *unicast* são utilizados para comunicação entre dois nós, por exemplo, telefones VoIPv6, computadores em uma rede privada, etc., e sua estrutura foi definida para permitir agregações com prefixos de tamanho flexível, similar ao CIDR do IPv4.

Dos tipos de endereços *unicast* IPv6, se faz uso do tipo Global Unicast, como os apresentados na Tabela 13 e também os de tipo *Link-Local*, que são usados em enlace específico onde a interface está conectada, recorda-se aqui que o mesmo é atribuído automaticamente utilizando o prefixo FE80::/64, sendo que os 64 bits reservados para a identificação da interface são configurados utilizando o formato IEEE EUI-64, sem serem encaminhados pelo roteador para outros enlaces.

O pool utilizado neste projeto é apresentado na Tabela 14.

Tabela 13 - Endereçamento IP do ambiente.

Provedora	Rede	Descrição
Telebrás	Endereçamento IPv4 *Internet*	Endereço/Rede: 177.15.75.32/27 Prefixo CIDR: /27 Máscara de sub-rede: 255.255.255.224 IP da Rede: 177.15.75.32/27 Broadcast da Rede: 177.15.75.63 Range de IPs: 177.15.75.32 - 177.15.75.63 Total de IPs: 32
CITEx	Endereçamento IPv4 Intranet	Endereço/Rede: 10.67.64.0/22 Prefixo CIDR: /22 Máscara de sub-rede: 255.255.252.0 IP da Rede: 10.67.64.0/22 Broadcast da Rede: 10.67.67.255 Range de IPs: 10.67.64.0 - 10.67.67.255 Total de IPs: 1024
Hurricane *Eletric*	Endereçamento IPV6	Endereço/Rede: 2001:470:4:d2b::/64 Prefixo CIDR: /64 IP da Rede: 2001:470:4:d2b::/64 Prefixo: FFFF:FFFF:FFFF:FFFF:0000:0000:0000:0000 Range de IPs: 2001:0470:0004:0d2b:0000:0000:0000:0000 - 2001:0470:0004:0d2b:ffff:ffff:ffff:ffff Total de IPs: 18446744073709551616

Tabela 14 - Endereços tipo Link Local do Experimento

Endereço IP	fe80::ac1e:4359/64
Tipo	Link-Local Unicast (Linked-Scoped Unicast) (fe80::/10) [rfc4291][IANA])
Rede	fe80::
Tamanho do Prefixo	64
Faixa de Rede	fe80:0000:0000:0000:0000:0000:0000:0000- fe80:0000:0000:0000:ffff:ffff:ffff:ffff
Total de Endereços	18446744073709551616

As faixas de endereços fornecidas pelo CITEx (IPv4) e pelo *Tunnel Broker* (Global IPv6), foram alocadas, como forma de experiência, de forma que se permita a distribuição dos blocos em sub-redes conforme o estabelecido na RFC 3531 [90].

Essa RFC propõe três métodos para ordenar a distribuição de endereços e blocos IP. Existe dessa forma a possibilidade de se alocar um bloco adicional para alguém que já tenha recebido um, de forma que possa anunciá-lo de forma agregada no roteamento.

Com o método acima citado, há a possibilidade de eventualmente mudar a quantidade de blocos, sem alterar as alocações já realizadas. Para tal cálculo, o site IPv6.br oferece um simulador *on line* no endereço *http://ipv6.br/rfc3531demo* [44], dos algoritmos apresentados na RFC (*Rightmost, Leftmost e Centermost*) [90].

O simulador divide os blocos na quantidade de subredes se deseja, e mostra a ordem em que devem ser alocados, segundo o algoritmo escolhido. Com a faixa recebida por *Tunnel Broker*, se a tem a seguinte possibilidade de segmentação, ilustrada na Tabela 15 sem perdas e com capacidade de conexão. No caso do endereçamento IPv6, ele será mantido no formato em que foi entregue.

Tabela 15 - Alocação dos Endereços IPv6

Endereço IPv6	Endereço IPv4
2001:470:4:d2b::/64	**10.67.64.0/22**
2001:470:4:d2b:0000::/68	10.67.64.0/26
2001:470:4:d2b:1000::/68	10.67.64.64/26
2001:470:4:d2b:2000::/68	10.67.64.128/26
2001:470:4:d2b:3000::/68	10.67.64.192/26
2001:470:4:d2b:4000::/68	10.67.65.0/26
2001:470:4:d2b:5000::/68	10.67.65.64/26
2001:470:4:d2b:6000::/68	10.67.65.128/26
2001:470:4:d2b:7000::/68	10.67.65.192/26
2001:470:4:d2b:8000::/68	10.67.66.0/26
2001:470:4:d2b:9000::/68	10.67.66.64/26
2001:470:4:d2b:a000::/68	10.67.66.128/26
2001:470:4:d2b:b000::/68	10.67.66.192/26
2001:470:4:d2b:c000::/68	10.67.67.0/26
2001:470:4:d2b:d000::/68	10.67.67.64/26
2001:470:4:d2b:e000::/68	10.67.67.128/26
2001:470:4:d2b:f000::/68	10.67.67.192/26

Para o desenvolvimento dos testes foi montado um laboratório que oferece os recursos físicos e lógicos, necessários ao experimento e a Tabela 16 esclarece mais o formato

de infraestrutura utilizada, deixando os detalhes da implementação na descrição de configuração.

Tabela 16- Informações de configurações dos ativos.

NOME DO ATIVO	OS	IPV4	IPV6	FINALIDADE
DGP HA	Linux / IOS	SIM	SIM	Roteador
EXT 1 FN	Linux / IOS	SIM	SIM	Roteador
HN Server	Linux / IOS	SIM	SIM	Roteador/Servidor/*Firewall*
Ar base 01	Proprietário (embutido)	SIM	SIM	*Access-Point*
Ar base 02	Proprietário (embutido)	SIM	SIM	*Access-Point*
Summit x650	Proprietário (embutido)	SIM	SIM	*SWITCH* GERENCIÁVEL
Host CN	Linux	SIM	SIM	Desktop
Host i1	Linux	SIM	SIM	Desktop
Host i2	Win 7	SIM	SIM	Desktop
Observer	Linux	SIM	SIM	Desktop/Sniffer

Os dispositivos de comutação, configurados com as funções específicas, que permitam o suporte ao tunelamento IPv6 e protocolos de roteamento IPv6 com a alocação, para os testes, de endereçamento IPv4 privado, além desse ambiente ser produzido em aplicativo de virtualização *Vmware*, detalhado no Apêndice C – Configuração do MIPv6, auxiliando na configuração de dispositivos com suporte IPv6 para simular clientes em redes pilha dupla e IPv6 nativo.

Roteadores de diferentes portes devem ser observados em função da versão de seu sistema operacional. No caso de se fazer uso do mesmo no formato da CISCO, de fácil implementação em caso de simulações, ou em customizado como uma *apppliance*[21], deve-se atentar para a versão de sistema operacional, no caso dos CISCO, em novas versões, o sistema IOS (*Internetwork Operating System*). Versões mais antigas apresentam severos problemas às aplicações IPv6, não foi considerado válido se manter versões anteriores para se observar o comportamento da rede, em função do incômodo que produz as seguidas mensagens e reações aos *bugs*, com isso é recomendável o uso de sistemas da família 720, como os roteadores Cisco 7206VXR [91], que têm plataformas modulares, formatados para operar em pilha dupla. O IOS deve trabalhar com suporte tanto a RIPng quanto a OSPFv3, ideal para o ambiente trabalhado, sem esquecer de se habilitar o protocolo escolhido e atribuir endereços IPv6 às interfaces.

[21] Na computação, a *appliance* se trata de um *hardware* com características de arquitetura específicas, com um sistema operacional, recursos e configuração específica, que roda um software (roteador, firewall, IDS, etc.) com finalidade definida.

O procedimento deve iniciar com o comando "*ipv6 unicast-routing*" no roteador, fazendo ele ser ativado modo de configuração global. Para começar a se encaminhar os pacotes, o protocolo IPv6 tem que ser habilitado também nas interfaces, com o comando por meio do comendo "*ipv6 enable*" e usar o comando "*ipv6 address*" atribuir o endereço IPv6 na interface, manualmente ou automaticamente usando a autoconfiguração.

Para a obtenção de endereço, o IPv4 utilizará mecanismos IPv4, como DHCP, como exemplo e o IPv6 utilizara mecanismos próprios de seu protocolo (IPv6), como DHCPv6 ou autoconfiguração. Algumas mudanças também têm que ser feitas em relação ao firewall e ao DNS. O firewall tem que ser configurado para IPv6 e o serviço DNS tem que estar habilitado para resolução de endereços IPv6. A configuração dessas entidades se encontra mais detalhada no Apêndice A**,** é exemplificada genericamente no trecho de código para uso nos roteadores da Figura 24.

```
router(config)#ipv6 unicast-routing
router(config)#int f0/0
router(config-if)#ip address 10.67.64.1 255.255.255.192
router(config-if)#ipv6 address 2001:470:4:d2b::1/64 eui-64
```

Figura 24 - Configurando o Método Pilha Dupla nos Roteadores

Para a interconexão deste laboratório com a *Internet* foram criadas seguidas implementações de tunelamento com base nos endereços fornecidos pelo provedor público *Hurricane Electric* – (*http://tunnelbroker.net/*), conforme descrito no Apêndice A - Procedimentos de Configuração do *Tunnel Broker*, possibilitando a criação de túneis via *Internet* IPv4 para trafegar IPv6. Neste cenário é criado um túnel IPv6 sobre a *Internet* e fornecida à VLAN, que representa o DGP, tanto acesso IPv4, através de NAT, como acesso IPv6.

A configuração se realiza em poucos passos, isso para o túnel estar atendendo a conectividade IPv6, recebendo um endereço IPv6 válido e podendo navegar pela *Internet*. O teste é simples, executando o comando *ping* no site *www.ipv6.br*, que possuí versão IPv6, a Figura 25 ilustra como se apresenta a tela de resposta ao teste.

Na *PoC*, o servidor DNS, DHCPv4, DHCPv6, cliente *Broker*, Firewall (IPv4 e IPv6) e Gateway NAT estão agrupados na máquina **HN *Server***.

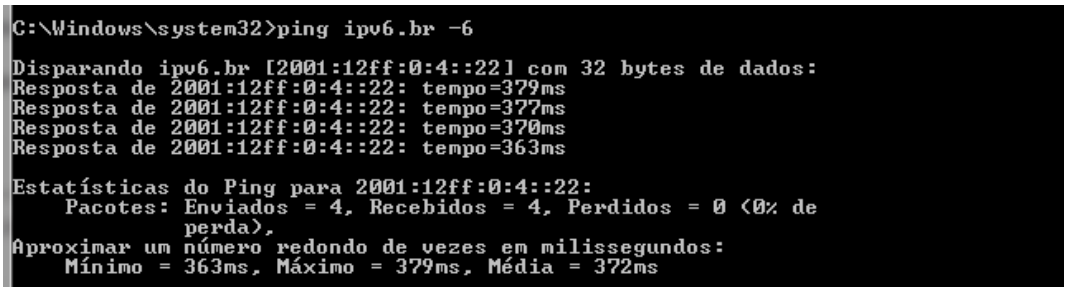


Figura 25 - Teste ICMP (*ping*) em site IPv6

Para a rede DGP, que vem a ser *o Home Network* do experimento de mobilidade, a técnica de transição pilha dupla é estabelecida se configurado os equipamentos que a suportam. Para a saída WAN, interface externa do roteador de borda, foi adotada a saída pública IPv4 com apenas um endereço IP e o *Broker* IPv6 com um "prefixo" /48. A técnica utilizada na parte WAN, apesar fazer uso do *Broker*, pode ser considerada também como de pilha dupla, pois, para o roteador de borda é como se ele possuísse também as duas versões de IP em sua pilha.

Na interface do roteador *Internet* são configuradas duas subinterfaces, cada uma com um endereço válido diferente. Na rede interna serão configurados endereços IPv4 e IPv6, o primeiro utilizando endereços de nível local e o segundo utilizando um bloco /64 fornecido pelo servidor do túnel *broker*.

No ambiente da *PoC*, foi utilizado o pool 10.67.64.1 - 62/26, o servidor DNS foi configurado como 10.67.64.1 (o próprio firewall), e o gateway padrão foi configurado como 10.67.64.1.

O prefixo "2001:470:4:d2b::/64" foi inserido pelo cliente do *Tunnel Broker* ao arquivo de configuração, de forma que *o Router Advertisement* enviado aos clientes IPv6 da rede sempre possuam o prefixo fornecido pelo *Broker*. Para que os clientes IPv6 da rede acessem e busquem algumas configurações do DHCPv6, nesse exemplo o endereço do Servidor DNS, foram feitas configurações no cliente do *Túnel Broker* que são descritas no Apêndice A - Procedimentos de Configuração do *Tunnel Broker*. Sua inicialização é feita, automaticamente por "*script*" linux.sh executado pelo cliente do *Broker*.

Ocorre também a habilitação do roteamento no IPv6, sendo independente do IPv4 que já estava habilitado. Vindo a caracterizar a independência das duas pilhas, é realizada a customização das regras e procedimentos para o IPv4 de maneira à parte das regras e procedimentos para o IPv6.

O *kernel* compilado na máquina **HN Server** possui suporte à IPv6, assim a interface é inicializada com um IPv6 montado pelo próprio sistema, através do prefixo *link local* (não roteável) “FE80::2”, e, no resto, do endereço MAC da interface de rede.

O primeiro endereço da interface “eth1” em HN Server é o IPv4 10.67.64.1/26, que faz parte da pilha dupla IPv4/IPv6 dessa máquina e o segundo é um IPv6, recebido pelo *Broker* e totalmente construído pelo mesmo e o ultimo endereço é o “link local”, montado com o prefixo “fe80::2” e o MAC da interface de rede.

Existe também uma referência a uma interface virtual, criada no sistema operacional pelo script linux.sh e associada virtualmente à interface física eth1. Ela mostra as palavras “IPv6-in-IPv4” que vem a ser o encapsulamento no protocolo 41 para o tunelamento utilizado pelo *Broker*. Essa interface recebe um IPv6 de Escopo Global com máscara 64 através da interface do *Broker*, sem fazer qualquer modificação no mesmo, servindo como indicação ponto-a-ponto do túnel IPv6. Também é produzido o endereço de *loopback*, tanto em IPv4 como em IPv6, de acordo com os conceitos de Pilha dupla.

Um teste do funcionamento do túnel é realizado com o comando *Ping6* (versão IPv6 do comando *ping*) com o envio de pacotes ICMPv6 [26] para o site *ipv6.google.com*. Se verifica na Figura 26 que o endereço é resolvido em IPv6 e que a latência de resposta é consideravelmente alta, isso em função do *Broker* ser sediado no Hemisfério Norte. Sendo assim, o pacote salta mais redes até chegar ao destino.

```
Hnserver - # ping6 -n ipv6.google.com
PING ipv6.google.com(ee-in-x64.1e100.net) 32 data bytes
40 bytes from ee-in-x64.1e100.net: icmp_seq=0 ttl=57 time=4.75 ms
40 bytes from ee-in-x64.1e100.net: icmp_seq=1 ttl=57 time=4.84 ms
40 bytes from ee-in-x64.1e100.net: icmp_seq=2 ttl=57 time=4.81 ms
40 bytes from ee-in-x64.1e100.net: icmp_seq=3 ttl=57 time=5.13 ms
^C
--- ipv6.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3011ms
rtt min/avg/max/mdev = 4.755/4.886/5.137/0.170 ms, pipe 2

 ---- Finished ------
```

Figura 26 - Teste de ping versão 6

Como ainda não se dispõe de um provedor com um *Broker* no Brasil, não foi possível realizar essa comparação.

Um desafio dessa realização de Prova de Conceito foi, se ver satisfeito com alguma combinação entre os elementos, os mecanismos e as funções de *QoS* , AAA e Mobilidade, ideais, para que se aproximassem de uma arquitetura que se pudesse considerar optimizada, foram usados experimentos em artigos científicos e relatórios acadêmicos, com foco na

realidade do ambiente trabalhado, foi colhido bastante dados, sendo exigida também uma pesquisa em conceitos estatísticos para se obter o equilíbrio da relação quantidade/qualidade das informações obtidas. Que ainda permitem uma infinidade de análises, a serem abordadas em futuras submissões de artigos em busca da correta quantificação de indicadores para monitorar e planejar o uso de processos de migração IPv6 e de implantação me mobilidade.

Sendo fundamental para a migração e funcionamento da rede IPv6, serviço de DNS tem atuação destacada, uma vez que a administração dos endereçamentos se torna tarefa muito complexa, em sua forma numérica, no modelo IPv6. O BIND[22], também precisa ser compilado com suporte a "IPv6".

As zonas IPv6 e IPv4 e os arquivos de resolução reversa devem ser separadamente configuradas para a utilização pelo DNS, e depois, por meio do comando `# /./etc/ini.d/named start,` inicializar o serviço de DNS. O detalhamento das configurações são vistas no Apêndice B.

Poucas configurações são realizadas no DHCPv6 são mínimas cabendo somente enviar para os clientes que o requisitarem o endereço do DNS, mas, mesmo assim, é necessário configurar um pool de endereços para o funcionamento do serviço, sem o qual, o serviço não inicializa.

Quanto ao firewall Aker, a aplicação funciona naturalmente com entidades e conjuntos no padrão do protocolo IPv6, suportando as RFCs abaixo [92]:

RFC2460 - *Internet Protocol, Version* 6 (IPv6) *Specification*;

RFC4291 - IP *Version* 6 *Addressing Architecture*;

RFC3484 - *Default Address Selection for Internet Protocol version* 6 (IPv6);

RFC4443 - *Internet Control Message Protocol* (ICMPv6) *for the Internet Protocol Version 6 (IPv6) Specification*;

RFC4862 - *IPv6 Stateless Address Autoconfiguration*;

RFC1981 - *Path MTU Discovery for IP version 6*;

RFC4861 - *Neighbor Discovery for IP version* 6 (IPv6); e

RFC4213 - *Basic Transition Mechanisms for IPv6 Hosts and Routers*.

[22] *Berkeley Internet Name Domain - Name Server* (BIND), desenvolvido e mantido pela *Internet Systems Consortium (ISC)* é um servidor DNS disponibilizado e bastante utilizado na *Internet*, em funçãode sua estabilidade e robustez.

É importante também a atenção aos detalhes, como na criação de regras quando selecionada as entidades, deve-se observar a origem e o destino destas. Tanto em IPv4, quanto IPv6 e que não é possível remover o módulo de IPv6 uma vez que ele tenha sido instalado. Também, se o módulo não estava instalado no *kernel*, os *daemons* todos do firewall estavam escutando um socket IPv4 [92].

Na próxima seção é realizada a abordagem de testes sobre o funcionamento do método Pilha Dupla, o ambiente elaborado para permitir a realização dos testes comparativos de desempenho do roteador utilizando os protocolos IPv4 e IPv6. Neste ambiente o host cliente encaminha pacotes gerados por uma aplicação Java ao host servidor. O roteador recebe estes pacotes em um dispositivo de rede diretamente conectado ao host cliente e os encaminha ao host servidor através de outro dispositivo. O tráfego dos pacotes é medido no roteador, e os dados processados e representados em gráficos e tabelas comparativas.

Após a afirmação de funcionamento da Pilha Dupla, demonstrada mais a frente, os testes se baseiam em realizar, no cenário definido, a movimentação de um nó móvel (MN) de sua rede origem, *Home Network* (HN) para uma rede estrangeira (FN), no caso aqui representando a Intranet do Exército Brasileiro, em Brasília, apenas atuando em IPv4. As redes são separadas pela *Internet* e são providas por roteadores de acesso.

Enfim, a estrutura para a avaliação de mobilidade, conforme visto na Figura 27, terá um *host* para atuar como CN; outro *host* para atuar como MN; *Access Point;* e roteadores, desempenhando atividades de suporte à mobilidade do MN entre as redes, conforme já foi descrito nas seções de exposição de conceitos. O processo de mobilidade completo tem a seguinte sequência: existe uma comunicação normal entre o MN o CN (nó correspondente); MN movimenta-se para a EBnet; o próprio MN registra seu novo *CoA* (Endereço recebido na rede remota) no seu HA (*Home Agent*), na origem da mobilidade estudada, e que é o responsável de fato pela mobilidade; ocorre a atualização das novas informações (*Binding Update*) entre o MN e o CN; fechando o circuito de comunicação [93]. Em relação ao CN, um cenário natural seria a existências de vários nós correspondentes na rede, realizando o estabelecimento de circuitos com NM, mas, de acordo com [94], apenas um CN torna o teste suficientemente pronto para a demonstração do conceito.

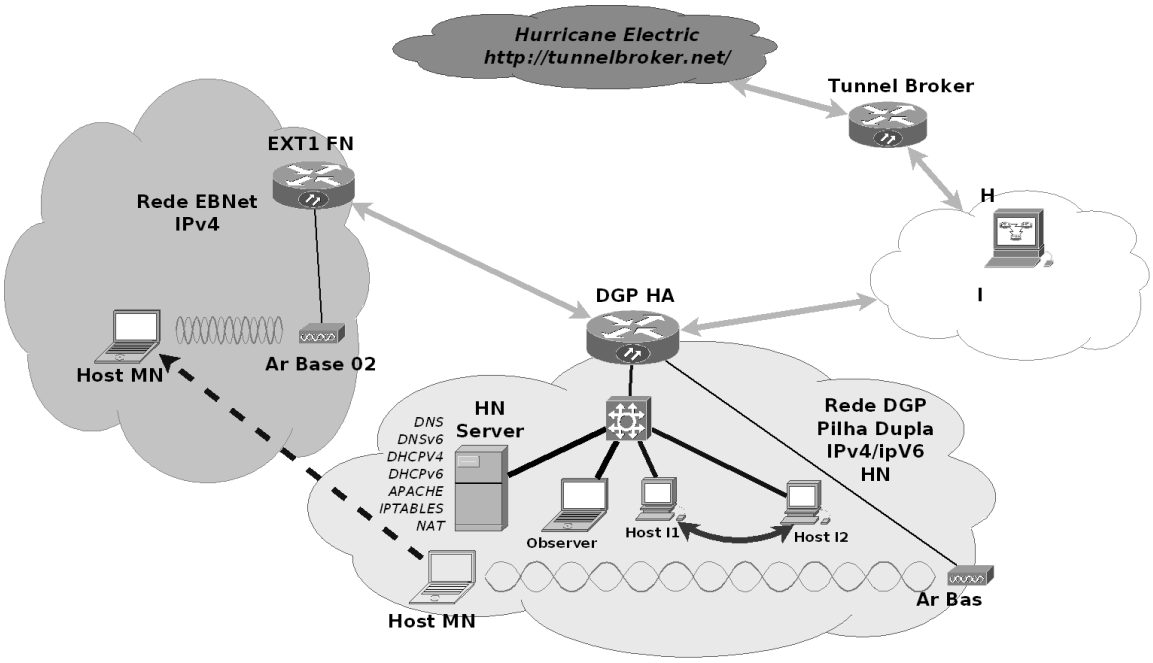


Figura 27 - Estrutura de rede utilizada no experimento

5.2. Formato da Análise

Nesta estrutura, baseada em Pilha Dupla de IP, foi analisada a implementação MIPv6. Como forma de métricas, para analisar o tempo de *handover*, foram utilizadas medições por meio de coleta de dados de transferência de arquivos, avaliando seu comportamento de uso de banda, *delay* e perda de pacotes, tanto na estrutura interna, configurada no método Pilha Dupla de trabalho conjunto de protocolos IP versões 4 e 6, quanto na situação de otimização de rede, na condição de mobilidade em rede local e em rede estrangeira, configurada apenas em IPv4. Essas métricas serão comparadas com os valores de referência de cada aplicação [95].

A estrutura de testes acrescenta a proposta de [94], onde se visa analisar durante a otimização de rede (*handover*): (1) o comportamento das ligações entre o NM e o CN; (2) se existem perdas de dados das comunicações TCP; e (3) a manutenção das sessões TCP.

Para a composição do cenário, para analisar os protocolos supracitados, foi realizado o uso da estrutura mostrada, onde se executaram as seguintes ações como forma de esforço de testes: (1) estabelecimento de troca de mensagens do CN para o MN analisando se a comunicação permanece no MN após a movimentação da rede móvel (DGP) para a rede visitada (EBNET/CITEX); (2) estabelecimento de uma sessão SSH entre o MN e um

servidor da *Internet* analisando se, após o *handover*, a sessão SSH será mantida, em conjunto com a correspondente sessão TCP; e (3) transferência de um arquivo entre o CN e o MN durante seguidos deslocamentos da rede móvel, analisando se o arquivo será integralmente recebido. Ao se implementar as configurações previstas para a ativação MIPv6, ocorre a perda de tráfego entre a rede interna, que funciona em Pilha Dupla e a *Internet*. A rede interna tem seu funcionamento normal, com alterações praticamente imperceptíveis, sem a implementação da mobilidade. Foi estudada a possibilidade de necessidade de ajuste no *Switch layer* 3, que vem sendo utilizado como HA da presente implantação. A implementação em Pilha Dupla, exige a correta manipulação do *Switch* para ativar ou desativar uma das pilhas, sendo assim, o método possui três tipos de operações: quando a pilha IPv4 é habilitada, a pilha IPv6 é desabilitada, o *host* se comporta como IPv4; no caso da pilha IPv6 estar ativada, a pilha IPv4 é desativada, levando o *host* a trabalhar como IPv6; e no caso de os dois protocolos estarem habilitados, o *host* pode usar os dois.

A "simplicidade" de implementação do modelo pode servir também como uma forma de "armadilha" para quem opta pelo modelo para conseguir velocidade na conclusão do serviço porque não se pode negligenciar a necessidade de configurações independentes para IPv4 e IPv6, importantes para aspectos variados no ambiente trabalhado, como nas informações nos servidores DNS autoritativos; nos métodos de roteamento; nos firewalls; e no gerenciamento das redes.

Na RFC 4977 [96] são abordadas questões relacionadas com a gestão de mobilidade para nós sob Pilha Dupla. Atualmente, são definidos dois protocolos de gestão de mobilidade para IPv4 e IPv6. A implantação múltipla em um nó sob pilha dupla acaba apresentando alguns problemas. Tais problemas de implantação e questões operacionais acabam por motivar o uso de um único protocolo de gerenciamento de mobilidade. O documento aborda tais motivações. O documento também descreve os requisitos para os protocolos de mobilidade IPv4 (MIPv4) e IPv6 (MIPv6) poderem apoiar a gestão da mobilidade para um nó de pilha dupla.

5.3. Experimentos e Resultados

Com a finalidade de se avaliar o implementado, houve a realização dos testes concentrada no desempenho do tráfego de dados IPv6 em relação ao IPv4 e também houve o teste em cima da mobilidade e do tunelamento *Tunnel Broker*. Tendo como base ao pesquisado em [97], foi observada a diferença de velocidade na transmissão de dados na rede

local, para ser avaliada a diferença de transmissão dos pacotes IPv6 ao IPv4 e analisada a diferença de performance do processamento e encaminhamento tunelado do IPv6 ao IPv4.

Como suporte aos experimentos, podem ser observados os procedimentos de configurações do *Tunnel Broker* estão descritos no **Apêndice A - Procedimentos de Configuração do *Tunnel Broker,*** bem como os procedimentos de configuração dos servidores DNS e DHCP, estão detalhados no **Apêndice B - Procedimentos de Configuração do Servidor DNS e DHCP**, o detalhamento de configuração do MIPv6 no ambiente de Prova de Conceito são encontrados no **Apêndice C – Configuração do MIPv6**, e configurações e testes preliminares dos dispositivos são descritos no **Apêndice D – Procedimentos de Configuração e Testes dos Dispositivos que compõem a *PoC*.**

Conforme visto em Métricas de Redes, testes de desempenho, são executados com a injeção de um determinado tráfego na rede e, por consequência, a análise da resposta da rede a este tráfego. Existem três fatores principais envolvidos na determinação de qual o tipo de serviço a ser disponibilizado: largura de banda, atraso e perda de dados [72]. Com relação à taxa de transferência, a vazão de dados expressa a quantidade máxima de dados que pode ser transportada de uma origem até o seu respectivo destino. Ao se referir à latência, trata-se do tempo total gasto por um quadro desde a origem até o destino. Esse tempo absoluto é a soma dos atrasos do processamento nos elementos da rede e o atraso de propagação ao longo do meio de transmissão [76]. A variação de tempo entre chegadas de pacotes do endereço de origem caracteriza-se como Jitter.

Nos experimentos a seguir foram realizadas medições por meio de transferência de arquivos em rede local, em meios físicos diversos, uso da medida de tempo de latência, descartando outras métricas em função de não se ter controle sobre fatores externos, presentes nos pontos de conexão entre o ambiente de testes e o servidor de *Broker*. Fazendo uso do protocolo ICMP, por meio do comando ping, levantando o tempo de reposta em uma consulta.

Na análise de funcionamento do *Tunnel Broker*, foi realizado um teste de latência em sites operarando sobre pilha dupla, tanto na versão IPv4 quanto na IPv6 [97].

Foi feito cáluculo de Round-Trip Time (RTT) em busca da variação de delay obtido entre MN e CN em comunicações com e sem mobilidade e captados os tempos de *Handover* durante a troca de Rede DGP (HA) para Rede EBNet (FN).

5.3.1 *Experimento 1*

Como primeiro teste de coleta de dados, foi realizada a transferência de arquivos em rede local, arquitetura IEEE 802.3u (*Fast Ethernet*), meio físico 100baseT4 (par-trançado de 4 pares, codificação 8B6T), de alcance de 100m com garantia de performance, avançando em relação à pesquisa realizada em publicação anterior. Tendo como base a quantidade de tráfego transmitido e considerando que duas máquinas estão no mesmo segmento de rede.

Foram executadas 50 medições em cada dia de experimento, com padrão de execução às segundas, quartas e sextas-feiras, durantes os meses de abril a junho de 2015.

Não houve fuga dos padrões de taxa de transferência e dispersão da mesma em dias sem expediente, mas sim a apresentação de melhor taxa de transferência. Com isso pode-se caracterizar, já nesse experimento, a influência da carga de uso dos sistemas do DGP, mesmo executando a *PoC* em rede de segmento isolado.

Conforme visualizado na Figura 28, se verifica a média das 50 medições a cada experimento com o cálculo de desvio padrão. Foram testados os dois protocolos, IPv6 e IPv4, no início foi feito um teste de transferência de arquivo dentro da rede local com as estações configuradas somente com IPv4 e conectadas em uma mesma comutadora e o protocolo IPv6 desabilitado.

Realizou-se a operação de transferência de arquivo de 115 MB da estação de nome **Host I1**, com endereço IP 10.67.64.2/26 para a estação **Host I2**, com o endereço IP 10.67.64.4/26.

A comunicação se deu através do endereçamento de escopo link-local, para tráfego interno na rede LAN, e estes pacotes não passaram por roteamento saindo da rede. Em seguida, foram alteradas as configurações das estações, agora para IPv6 puro e se promoveu a transferência do mesmo arquivo. Houve medição em outros arquivos com tamanhos diversos, que não vieram a motivar a apresentação de seus resultados, por não apresentarem variação significativa.

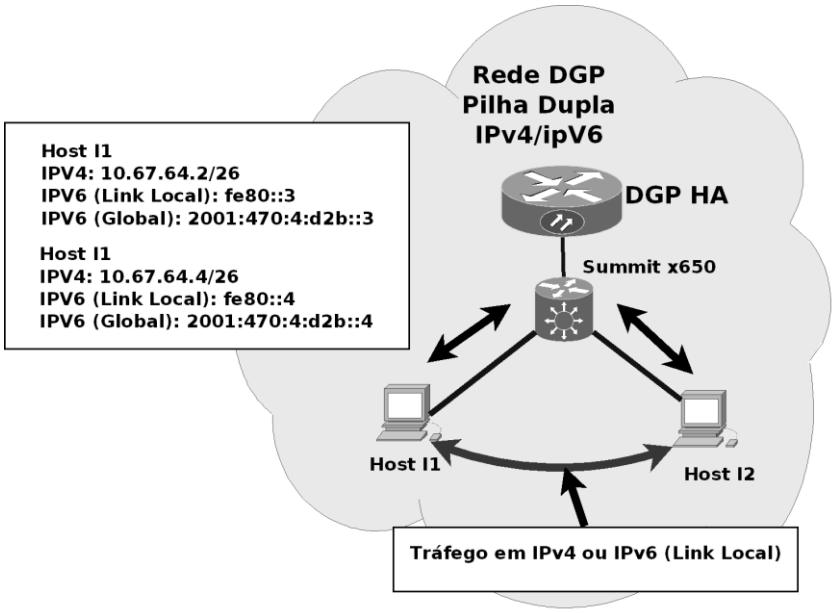


Figura 28 - Topologia do experimento 1

Aqui, verificou-se o padrão de taxa de transferência média semelhante ao ambiente de testes usado como base. Em comparação, a variação foi muito pouca entre o IPv4, com média de 15,70 MB/s, e o IPv6, mantendo uma média muito próxima, a 12,99 MB/s, destacando uma queda em função do *overhead* do pacote IPv6, fazendo a diferença (Figura 29).

Porém ao se observar a dispersão das taxas de transferência, apresentada na Figura 30, foi um fator que se repetiu nos experimentos a distribuição mais estável no protocolo IPv6 com média de desvio padrão a 1,12 MB/s, enquanto que no protocolo IPv4 a média de desvio padrão a 2,38 MB/s, ratificando uma melhoria em relação ao projeto do IP versão 4.

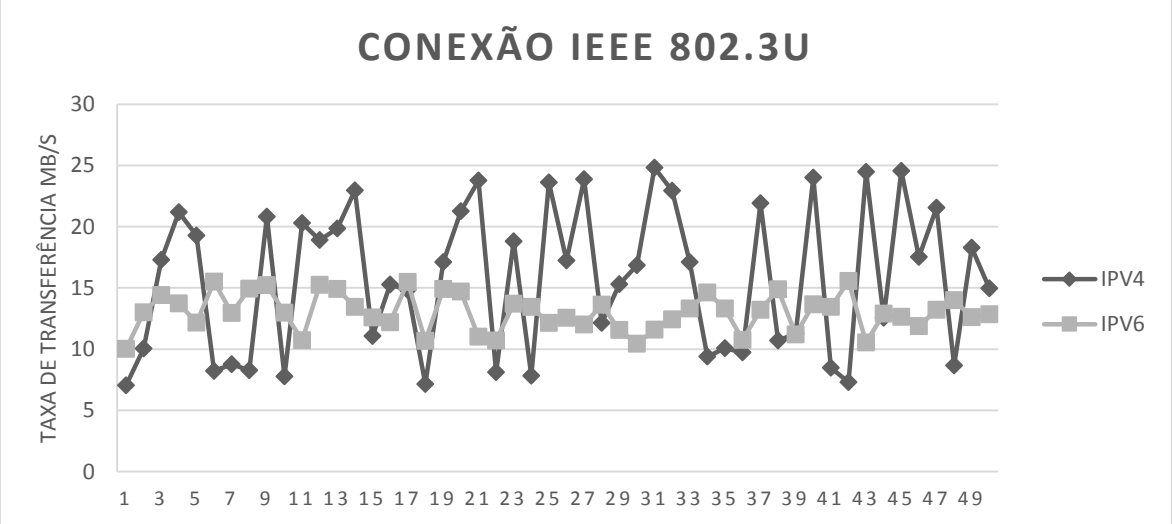


Figura 29 - Experimento 1 - comparação IPv4 x IPv6 – Via Cabo

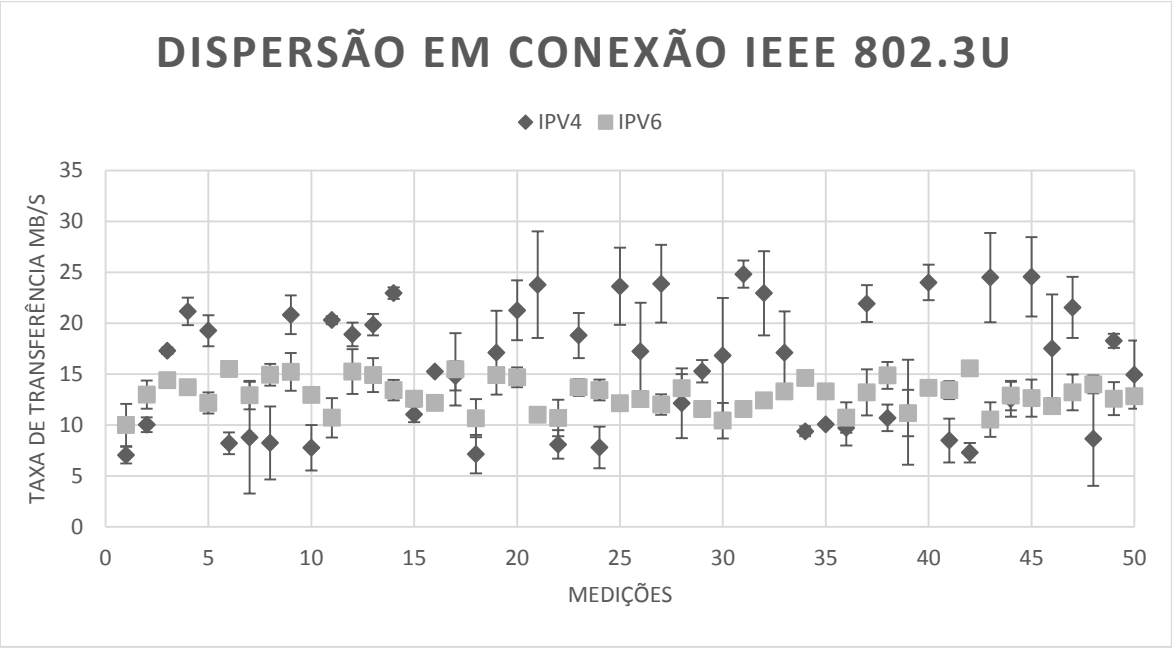


Figura 30 - Medida de dispersão e desvio padrão de Taxa de Transmissão.

5.3.2 *Experimento 2*

Neste experimento, a transferência de arquivo, agora se deu em rede sem fio, IEEE 802.11n, se ligando o *Access-Point* (AP), e as estações se comunicando por meio do *AP*, de acordo com o demonstrado na Figura 31.

Mantendo o padrão, e se respeitando a distância determinada do fabricante do AP, foram executadas 50 medições em cada dia de experimento, com padrão de execução às segundas, quartas e sextas-feiras, durantes os meses de abril a junho de 2015. O teste foi iniciado com as estações configuradas somente com IPv4. Foi realizada a transferência do mesmo arquivo da estação **Host I1** para a estação **Host I2**, sendo verificada a taxa de transferência média de 679 KB/s. Em seguida, também se alterou a configuração das estações para IPv6, desabilitando o protocolo IPv4 e se realizou a transferência do arquivo com taxa de transferência média de 590 KB/s.

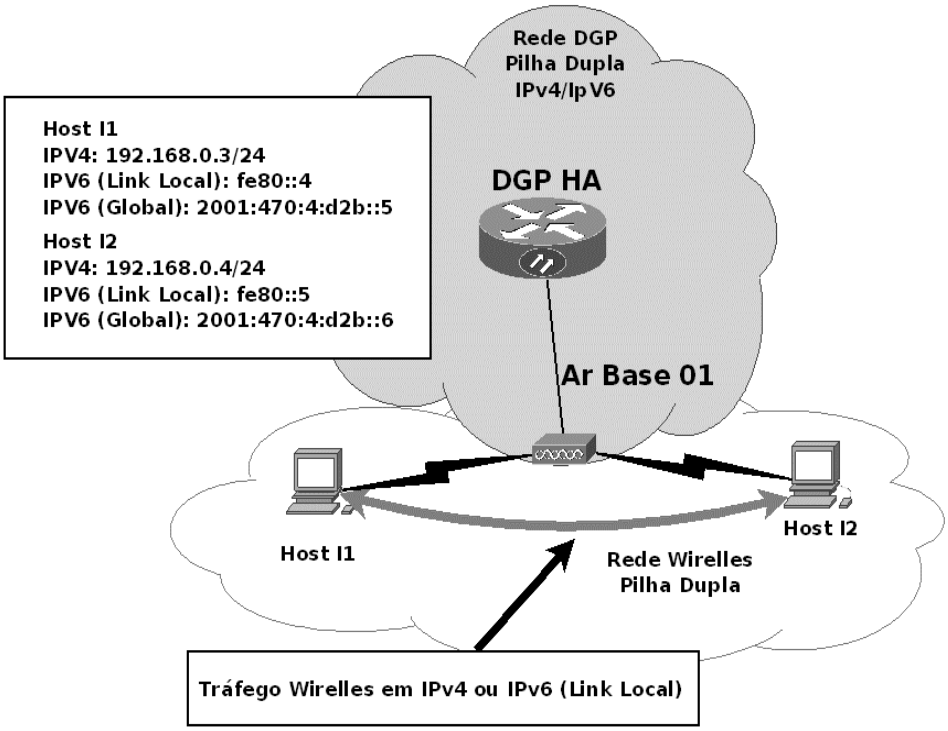


Figura 31 - Topologia do experimento 2

Da mesma forma que o teste anterior, como mostra a, o desempenho obtido em *Wireless* também foi compatível entre as estações, não acrescentando muitas informações, inclusive no quesito dispersão de taxas de transferência (Figura 33), que sofre um tratamento do firmware do ponto de acesso sem fio, com o correr das avaliações a conexão se manteve um pouco mais uniforme nos dois protocolos, com média de desvio padrão de 112KB/s em IPv4 e 93KB/s em IPv6.

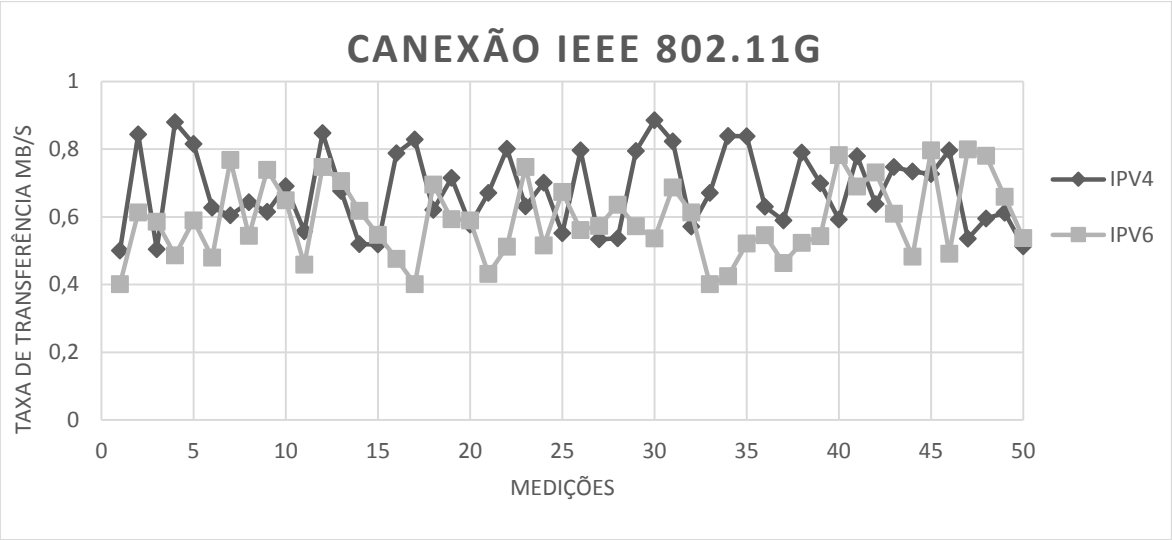


Figura 32 - Experimento 2 - comparação IPv4 x IPv6 – Via *Wirelles*

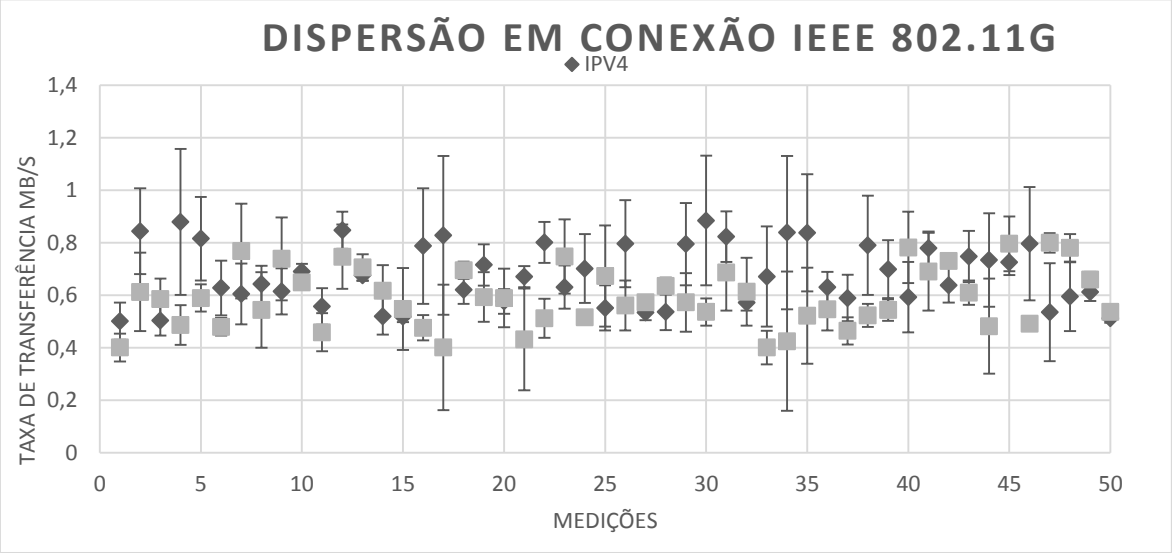


Figura 33 - Medida de Dispersão em Conexão *Wirelles*

5.3.3 *Experimento 3*

Neste teste, foi considerado o uso da medida de tempo de latência, descartando outras métricas em função de não se ter controle sobre fatores externos, presentes nos pontos de conexão entre o ambiente de testes e o servidor de *Broker*. Sendo assim, se faz o uso do protocolo ICMP, por meio do comando *ping*, se levantando o tempo de reposta em uma consulta.

Para analisar o funcionamento do *Tunnel Broker*, foi, de acordo com o seu formato de configuração, realizado um teste de latência (com o comando *ping*) no site do

www.freenet6.net, por ele operar em pilha dupla, com a aceitação de requisições ICMP, tanto na versão IPv4 quanto na IPv6 [97].

Com o uso das duas versões de IP, seguindo a lógica para comparação ao realizado em [97], foram realizados 16 saltos em 30 repetições a cada dia de coleta de dados. E para alcançar o servidor do *Freenet6* mas o teste do IPv6 é mascarado com o comando *tracepath6*, por apresentar apenas um salto, que é a interface do *Tunnel Server* do *Broker*. De forma transparente o pacote é transportado tunelado através de uma rede IPv4 encapsulado (protocolo "41")

Para, então, determinar o caminho e saltos percorrido pelo pacote do túnel na *Internet* IPv4, foi utilizado o comando *tracepath* para IPv4 [97] ,comparando o tempo médio de um pacote ICMP (v4 e v6), se verifica uma ainda pequena diferença no desempenho entre os dois protocolos, no teste da *PoC*, como ilustra a Figura 34, os resultados apresentam as médias dos experimentos com desvio padrão calculado e não se percebe uma dispersão significativa nos resultados, com média de 173,01 ms em IPv4 e 197,74 ms em IPv6, um pouco maior, também a média do desvio padrão segue a tendência, 9,51 ms no IPv4 e 17,73 ms no IPv6, mas tal elevação em IPv6 pode ser levada em conta pelo estabelecimento do túnel entre o servidor de destino e o *Tunnel Broker*.

Existe o fato de não ser medida a diferença do processamento já que os pacotes IPv6, por estarem encapsulados em IPv4 são considerados como IPv4 e são roteados pela *Internet* como IPv4 (até a ponta do *Broker*), daí a falta de parâmetros mais precisos.

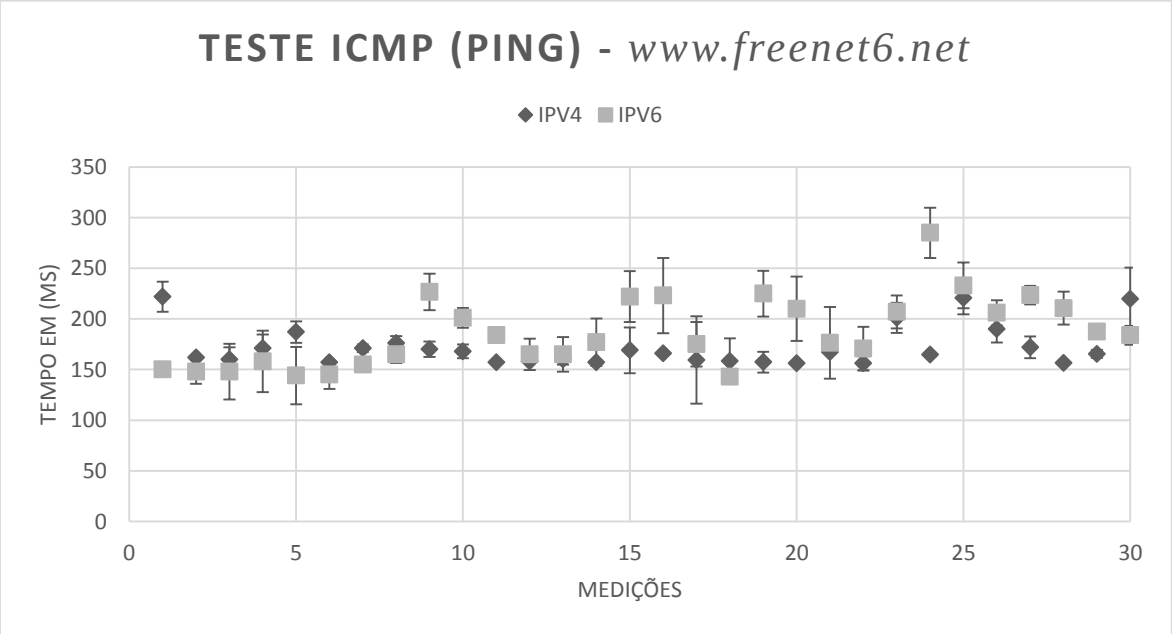


Figura 34 - Teste de ICMP – IPv4 x IPv6 – Servidor *Freenet6*

5.3.4 *Experimento 4*

Este teste considerou o site *www.IPv6.br*, que suporta os dois protocolos (IPv4 e IPv6 em pilha dupla) para se medir o desempenho dos dois protocolos. Aqui, como mostra a Figura 35, se confirma o experimentado em [97], no mesmo padrão apresentando as médias dos resultados com cáculo de desvio padrão, pois a latência média adquirida foi de 227 ms, com média de desvio padrão de 2,14 ms para IPv6 e de 29 ms, com média de desvio padrão de 3,20 ms para IPv4, tendo agora uma diferença considerável de comparação, isso porque o *Broker* utilizado está na América do Norte, como consequência, só de latência, são gastos quase 90% do resultado.

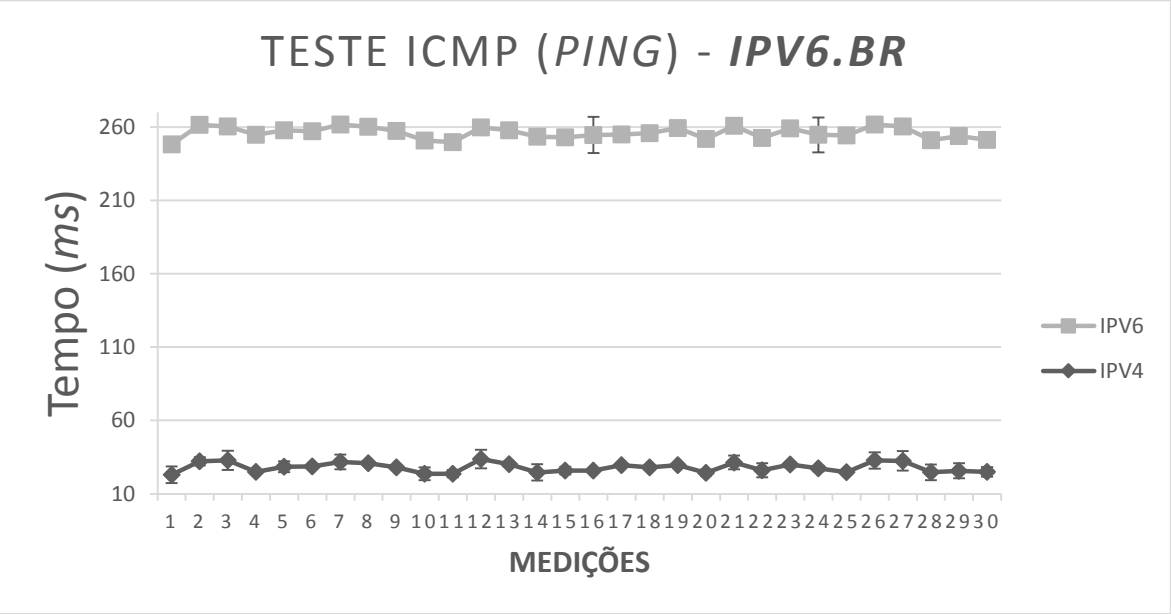


Figura 35 - Teste de ICMP – IPv4 x IPv6 – Servidor Ipv6.br

5.3.5 *Experimento 5*

Este vem a ser um experimento de Mobilidade, ocorrida logo após a instalação do pacote de mobilidade no *Home Agent* (HA) e no *Mobile Node* (MN) para que, durante a movimentação do MN para a FN, se constituísse um canal seguro entre MN e HA, utilizado para encaminhar os pacotes até CN. Para a configuração dos endereços foram instalados o serviço de *Router Advertisement* (RA) no HA e na FN, conforme a Figura 36.

A atividade se iniciou pela averiguação de qual a utilização do canal sem a transferência de dados, isto é, a utilização do canal de comunicação por pacotes inerentes ao protocolo estudado.

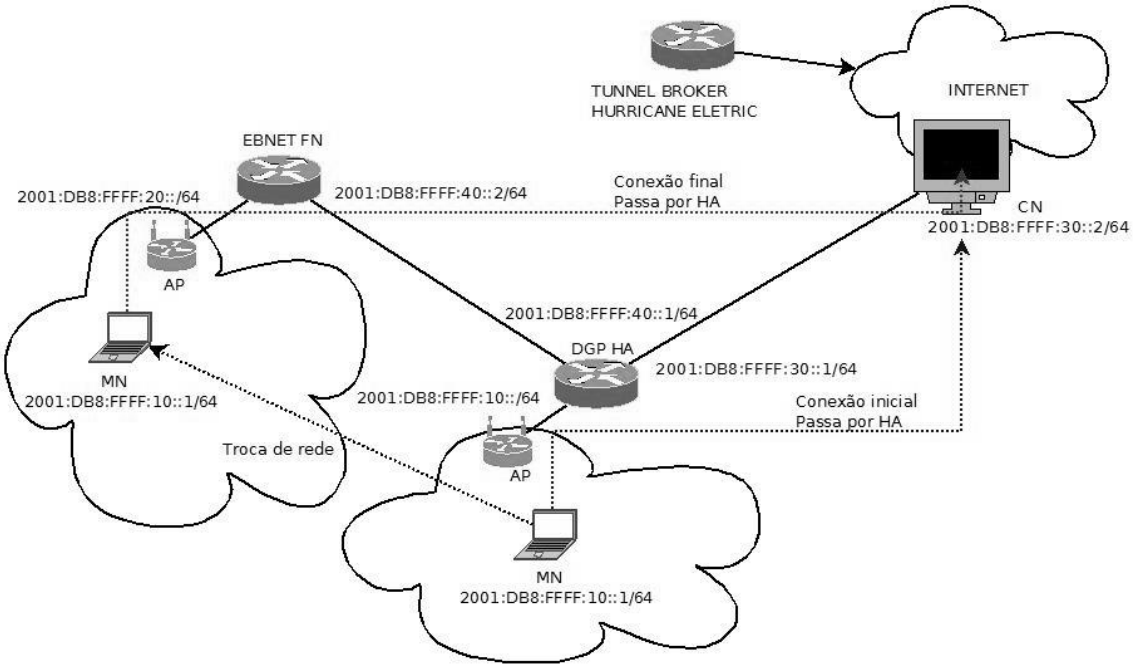


Figura 36 - Configuração da rede nos experimentos com Mobilidade

Dessa forma se seguiu ação de realizar três capturas de MN, de 120 segundos cada:

- Na primeira captura, sem o uso de MIPv6, foram recebidos 42 pacotes, referentes a anúncios de *neighbor discovery*, gerando 0,310 pacotes por segundo e 3.241 *Bytes*.
- Foi habilitado, aa segunda captura o anúncio de *Router Advertisement* (RA) realizado pelo *Home Agent* (HA), obtendo como resultado 116 pacotes, gerando 0,7 pacotes por segundo e 9.877 *bytes*. Esta quantidade de pacotes no início de contagem de tempo se deve à configuração de *Router Advertisement* existente em *Home Network*, configurado para enviar mensagens de RA, a cada três segundos no máximo. Há uma rápida convergência, no momento em que o agente de mobilidade (HA ou FN) percebe a existência do *Mobile Node* na rede. Este tempo de envio de *Router Advertisement* pode ser reduzido a um intervalo de 300 ms, porém não é usual esta configuração em redes IPv6.
- Habilitado o processo de mobilidade *mip6d* em MN, com isto obteve-se um aumento inicial de pacotes referente ao registro do MN em seu HA de 133

pacotes, com uma média de 1,09 pacotes por segundo e 42.201 *bytes*. Esta quantidade de pacotes de controle representa 0,02 % da taxa de transferência de *bits/s* permitida neste canal de comunicação, conforme a mensuração da capacidade de transferência executada, abordada no tópico sobre taxa de transferência.

O Cálculo de *Round-Trip Time* objetiva verificar qual a variação de *delay* obtido entre MN e CN utilizando o MIPv6 em uma *Foreign Network*, em comparação a uma comunicação sem o uso de protocolos de mobilidade. Para isto foram realizadas coletas com e sem o uso do MIPv6, utilizando pacotes de 65 bytes realizadas em 3 amostras de 100 pacotes cada.

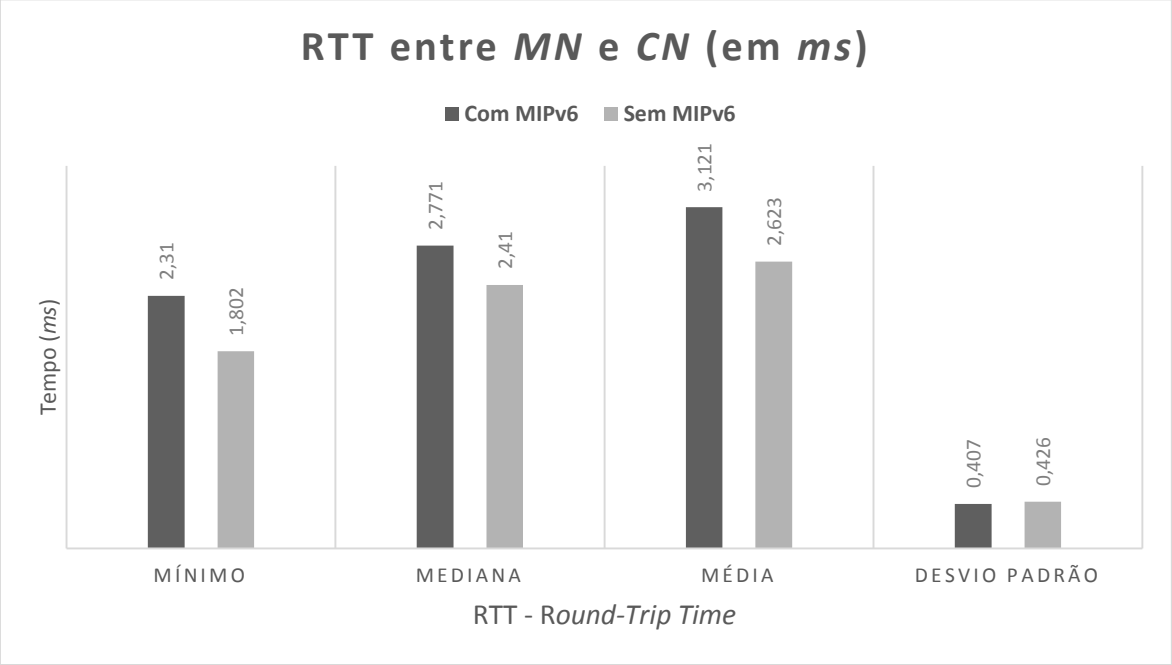


Figura 37 - RTT entre *Mobile Node* e *Correspondent Node* (em ms)

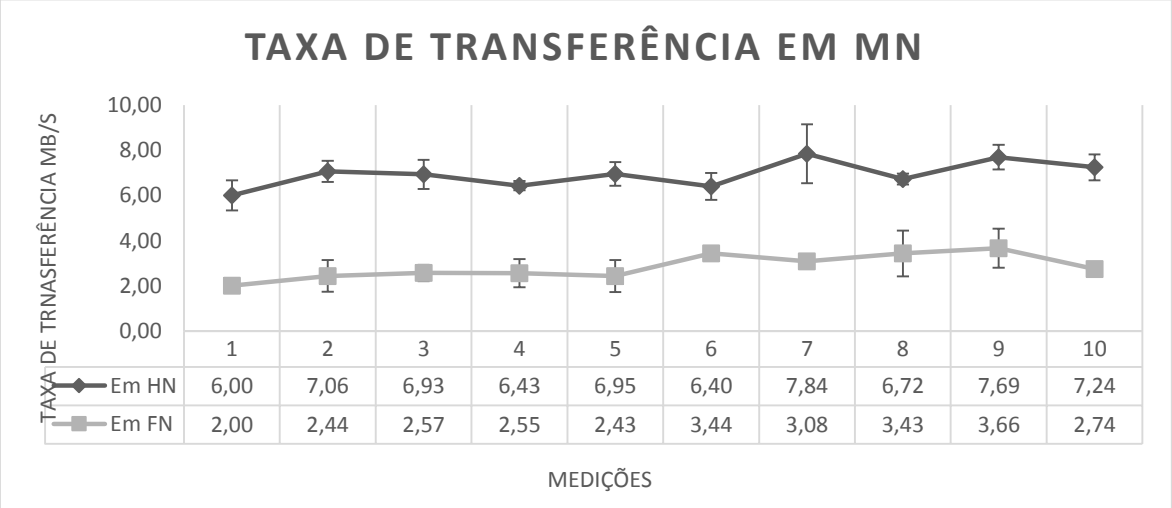
Acima, na Figura 37, se observa uma elevação de 20% com o uso do MIPv6, após a criação do túnel entre MN e CN, devido ao canal de comunicação estabelecido entre MN e o HA utilizar o protocolo IPSec.

Após a implementação da mobilidade, voltou-se a medir a Taxa de Transferência, dessa vez mensurando a taxa de transferência de dados por TCP, utilizando o *iperf*, enviando tráfego de MN ao CN, realizando 10 (dez) atividades de duas capturas: uma com MN em sua rede local e outra com MN na rede estrangeira.

Nos testes, se manteve o AP foi utilizando o protocolo 802.11n, permitindo taxa de transferência com possibilidade de alcance à taxa de 300 Mbps, mas limitado pelas interfaces de rede de HA e CN, do tipo *FastEthernet* (100 Mbps).

Apesar de a estrutura física ser idêntica entre as redes, quando MN está na rede estrangeira, ele tem reduzida a sua capacidade de transferência, realizando a comunicação por IPSec, devido a implementação de criptografia. Também se constatou que a CPU não passou de picos de 6% em sua carga de uso, ocasionados pela criptografia dos pacotes, o que não influenciou nos experimentos.

Como se observa na Figura 38, foi obtida uma taxa média de transferência de 6,92 MB/s, quando realizada a medição na rede local e uma taxa média de 2,83 MB/s na rede estrangeira, devido a utilização de IPSec e do aumento da rota dos pacotes.



	1	2	3	4	5	6	7	8	9	10
Em HN	6,00	7,06	6,93	6,43	6,95	6,40	7,84	6,72	7,69	7,24
Em FN	2,00	2,44	2,57	2,55	2,43	3,44	3,08	3,43	3,66	2,74

Figura 38 - Taxa de Transferência em Mobilidade de MN

Os tempos de *Handover* durante a troca de Rede DGP (HA) para Rede EBNet (FN), na transferência de dados por TCP, resultaram entre 12,321 e 15,011 segundos nos dez experimentos realizados. Esta variação ocorreu devido ao tempo de recebimento do endereço IPv6 através de RA na FN, o qual estava configurado para ser realizado no intervalo de um a três segundos.

Assim, para desconsiderar o tempo de endereçamento durante a troca da rede (recebimento de RA), foi realizado o processo de mobilidade várias vezes entre as redes em um curto espaço de tempo, dessa forma MN não necessitou solicitar um novo endereço, ou aguardar o recebimento de *Router Advertisement*, pois já possuía os endereços em sua interface. Neste experimento, obteve-se 13,201 segundos de *Handover*, na transferência de dados por TCP entre MN e CN.

Em um terceiro teste foi analisado o tempo de *Handover* através do envio de pacotes ICMP a uma taxa de um pacote por milissegundo, com a mesma estrutura do experimento anterior. Nesse experimento, obteve-se uma melhora no tempo de *Handover*, passando a ser realizado em 7,4 segundos, pois não ocorreu o processo de negociação de conexão necessário na comunicação por TCP, porém, incluindo o tempo de endereçamento (recebimento de RA) esse intervalo foi de 9,673 segundos.

Enfim, foi mensurado separadamente o tempo de *Handover* da camada de enlace do MN, isto é, o tempo que o *hardware* a e pilha TCP/IP do Sistema Operacional demora para desconectar de um *Access Point* e conectar ao outro através da interface *Wireless*, este experimento com um tempo de 4,882 segundos.

Encerrando o teste, estabelece-se a composição conceitual de tempo de *Handover*, composto por três partes: *Handover* de enlace, de endereçamento e de registro no HA. Apresentando assim o estabelecimento da implementação de mobilidade do ambiente estudado.

5.4. Análise dos Experimentos

Mesmo diante da pouca diferença nos Experimentos 1 e 2, pode-se concluir que existe um aumento da utilização da banda, quando se faz a troca de IPv4 por IPv6, justificado em função do *overhead* proporcionado pelo desenvolver do IPv6 que, mesmo com um cabeçalho de tamanho fixo, é superior que a maioria dos de IPv4. O *throughput* para o mesmo tipo de informação fica maior em IPv6 do que no IPv4, vindo a gerar aumento de uso da banda. O conceito indica como vantagem que, em relação ao IPv4, no IPv6 o tamanho máximo dos pacotes é de até 4Gb, contra os 64Kb do IPv4. Sendo assim, a diferença tende a reduzir à medida que se utilizar mais o IPv6, porém o aspecto não foi apresentado em grande diferença ao IPv4, o que pode indicar alguma falha de configuração na implementação do ambiente.

Com base no resultado do Experimento 4, pode-se afirmar que a utilização de *Broker* IPv6 no Brasil só terá um desempenho próximo ao do IPv4 no momento em que se disponibilizar, um serviço de *Broker* local, possibilitando se atenuar o tempo gasto pelo pacote no túnel.

Ocorrido logo após a instalação do pacote de mobilidade no Home Agent (HA) e no *Mobile* Node (MN), o Experimento 5 foi direcionado para que, durante a movimentação do MN para a FN, se constituísse um canal seguro entre MN e HA, utilizado para encaminhar

os pacotes até CN. Assim foram realizados teste de delay, por meio do cálculo de *Round-Trip Time*, e a implementação ainda não se encontra pronta, apesar de realizar o programado no quesito mobilidade, ainda se observa uma elevação de 20% com o uso do MIPv6, após a criação do túnel entre MN e CN, devido ao canal de comunicação estabelecido entre MN e o HA utilizar o protocolo IPSec, além do crescimento na taxa média de transferência em função do uso de IPSec e do aumento da rota dos pacotes.

Com os testes de *Handover* durante a troca de Rede DGP (HA) para Rede EBNet (FN), na transferência de dados por TCP, apresentaram uma significativa devido ao tempo de recebimento do endereço IPv6 através de RA na FN, algo que pode ser otimizado por meio de novas experiências.

6. Conclusões e Trabalhos Futuros

Este trabalho, foi direcionado a um ambiente específico, sendo promovido o estudo e pesquisa de modelos de migração de protocolos IP e implementação estendida de mobilidade aplicados a redes corporativa. Em formato de Prova de Conceito, foi simulada a rede do DGP, Organização Departamental do Exército Brasileiro, o qual possui como desafio a integração de um grande volume de dados provenientes de diferentes repositórios, bem como o gerenciamento e a disponibilização do conhecimento militar. A importância e continuidade do mesmo é um ponto passivo na Força Terrestre, como se pode atestar no Anexo I, em declaração quanto à Relevância da dissertação, assinada pelo Chefe da Assessoria de Planejamento e Gestão do DGP, órgão de gestão e controle do Exército Brasileiro.

Seguindo a orientação governamental de se aplicar o IPv6, que diferentemente de seu protocolo antecessor, possui características direcionadas a atender as demandas dos novos serviços de comunicação em tempo real. E com uma implementação complexa, o mesmo segue do caminho de ser mais estudado e desvendado, coexistindo assim, com o IPv4 durante um longo período. Este buscou ser conduzido, dentro das práticas que preveem a coexistência entre os dois protocolos, assim como a manutenção de sistemas e aplicações que ainda não sejam atendidas pelo IPv6.

A adoção do IPv6 é irreversível e os resultados apresentados promoveram a interoperação entre os protocolos IPv4 e IPv6 de forma consistente sem a interrupção do IPv4, servindo, a dissertação final, como referência didática ao aprendizado do corpo técnico envolvido no processo de transição para que os serviços e softwares sejam alcançados tanto pelo protocolo IPv4, quanto o IPv6. Em adição, a avaliação da mobilidade, em um formato ainda de implementação básica, é fornecida, com a busca de garantia de interoperabilidade entre dispositivos, se mantendo sempre conectado, independente de localização física.

Neste projeto, o estudo de mobilidade em IPv6 apresentado foi centrado no protocolo MIPv6, mas foram conhecidas outras tecnologias associadas à mobilidade, como os protocolos envolvidos com micromobilidade e macromobilidade e como métrica de evolução, foi também abordado o comportamento destas tecnologias em IPv4, assim, apresentam-se os avanços mais recentes realizados, com base nos estudos e pesquisas, sendo configurados diversos cenários de teste.

Neste contexto, o objetivo deste trabalho que era implantar, como prova de conceito, o protocolo IPv6, com a implementação e a análise de mecanismo de suporte à mobilidade para o ambiente corporativo do Departamento-Geral do Pessoal, órgão de direção setorial do Exército Brasileiro, foi alcançado, com a prática do estudo e análise dos padrões e normas, nacionais e internacionais, relacionadas à transição IPv4 / IPv6, bem como o uso de mobilidade sobre IPv6 realizando a identificação de configurações físicas e lógicas que promovem o suporte, bem aqueles que impedem a implementação adequada do protocolo IPv6.

No decorrer deste trabalho, também foram elucidados temas relacionados ao domínio acadêmico, bem como conceitos que envolvem redes convergentes, migração de protocolos *Internet* e mobilidade baseada no IPv6. Foi também possível conhecer os recursos que os métodos de qualidade de serviço e experiência oferecem, assim como suas diversas aplicações, na melhoria e análise de ambientes de comunicação.

A implantação de um modelo de mobilidade, mesmo que complexa, em razão de ainda ser considerada recente e pouco difundida, segue em uma direção de amadurecimento, com o sucesso de sua implantação no DGP no formato de Prova de Conceito.

O modelo de migração pode ser aprimorado a partir da inclusão de novos elementos importantes para a medição da comunicação, bem como a partir da realização de novas validações e será possível, com o último experimento apresentado nesta dissertação, se partir para um novo ciclo de estudos e experiências que vão surgir, em condições de serem testadas em um ambiente totalmente diferente do Exército Brasileiro, e também, como forma de incentivo a trabalhos futuros, novas funcionalidades podem vir a ser incorporadas ao DGP.

Como novas funcionalidades de migração IPv4/IPv6 sugere-se, como continuação de estudos e uso da *PoC*, a aplicação de modelos, em conjunto com a implementação pilha dupla, como Túneis 6over4 (IPv6-over-IPv4), o Dual Stack Lite (DS-Lite) e os métodos de tradução IVI, dIVI e dIVI-pd [5]. Já para o conceito de mobilidade, recomenda-se promover pesquisas sobre o modelo NEMO, conceito de mobilidade dos equipamentos IPv6 que é assegurada por um conceito de *router* móvel (*Mobile Router* – MR). Este *router* móvel, que pode ser um computador portátil com ligação simultânea à rede local e à *Internet*, é capaz de alterar o seu ponto de ligação à *Internet* de forma transparente para os dispositivos a que está diretamente ligado, já a partir do MIPv6 [94].

Referências

[1] S. S. S. A. FINNEY JOE, "Mobile 4-in-6: a novel IPv4 / IPv6 transitioning mechanism for mobile hosts," em *Conference: Wireless Communications and Networking Conference, 2005 IEEE, Volume: 3*, South Drive, Lancaster, 2005.

[2] Project Management Institute, Um Guia do Conhecimento Em Gerenciamento de Projetos - Guia Pmbok®, 5ª ed., PMI, Ed., 2014, p. 496.

[3] G. Huston, "IPv4 Address Report," 9 agosto 2013. [Online]. Available: http://www.potaroo.net/tools/ipv4/. [Acesso em 06 junho 2015].

[4] COMITÊ EXECUTIVO DE GOVERNO ELETRÔNICO, *e-PING – Padrões de Interoperabilidade de Governo Eletrônico, Documento de Referência Versão 2011*, G. Brasileiro, Ed., Brasília:, DF, 2010.

[5] Equipe do CEPTRO - NIC.br , "IPv6.br," Centro de Estudos e Pesquisas em Tecnologia de Redes e Operações, junho 2012. [Online]. Available: http://ipv6.br/. [Acesso em 23 junho 2013].

[6] C. G. D. I. N. B. –. CGI.br, *Resolução CGI.br/RES/2013/033 – Ações para fomentar a adoção do IPv6*, CGI.br, Ed., Brasília, DF, 2013.

[7] Departamento- Geral do Pessoal (DGP) - Exército Brasileiro - Ministério da Defesa., *Plano Diretor de Tecnologia da Informação - 2015/2016*, BRASÍLIA, DF: DGP, 2015, p. 113.

[8] INTERNET ENGINEERING TASK FORCE (IETF)., *RFC 791 – Internet Protocol – Protocol Specification*, 1981.

[9] CISCO, Networking Academy, *CCNA Exploration – Fundamentos de Rede. Cisco Systems*, 2007-2009.

[10] A. F. G. R. R. Fey, Dominando o IPv6 a partir do IPv4, 2ª ed., Caxias do Sul, RS: ITIT, 2015.

[11] The Internet Assigned Numbers Authority (IANA), "IANA - Number Resources," Internet Corporation for Assigned Names and Numbers (ICANN), 2015. [Online]. Available: https://www.iana.org/numbers. [Acesso em 12 Janeiro 2015].

[12] T. L. V. Fuller, *Request for Comments: 4632 - Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan*, N. W. Group, Ed., 2006.

[13] R. Droms, *Request for Comments: 2131 - Dynamic Host Configuration Protocol*, N. W. Group, Ed., 1997.

[14] K. E. P. Srisuresh, *Request for Comments: 3022 - Traditional IP Network Address Translator (Traditional NAT)*, N. W. Group, Ed., 2001.

[15] B. M. D. K. G. J. d. G. E. L. Y. Rekhter, *Request for Comments: 1918 - Address Allocation for Private Internets*, 1996.

[16] A. M. S. Bradner, *Request for Comments: 1550 - IP: Next Generation (IPng) White Paper Solicitation*, N. W. Group, Ed., 1993.

[17] A. M. S. Bradner, *Request for Comments: 1752 - The Recommendation for the IP Next Generation Protocol*, N. W. Group, Ed., 1995.

[18] CISCO, "Implementing the Carrier Grade IPv6 on," 2013.

[19] CISCO, “6lab - The place to monitor IPv6 adoption,” 2012. [Online]. Available: http://6lab.cisco.com/stats/cible.php?country=BR&option=all. [Acesso em 15 Junho 2015].

[20] C. R. dos Santos, “Integração de IPv6 em um Ambiente Cooperativo Seguro,” UNICAMP, Campinas, 2004.

[21] S. DEERING e R. HINDEN, “Request for Comments: 2460 - Internet Protocol, Version 6 (IPv6),” Network Working Group, RFC 2460, 1998.

[22] J. P. S. A. G. N.-N. ABLEY, *Request for Comments: 5095 (Updates RFC 2460 and RFC 4294),* 2007.

[23] R. M. G. Malkin, *Request for Comments: 2080 - RIPng for IPv6,* N. W. Group, Ed., 1997.

[24] D. F. J. M. R. Coltun, *RFC 5340. OSPF for IPv6.*, 2008.

[25] J. B. B. V. T. L. C. P. M. C. R. Droms, *Request for Comments: 3315 - Dynamic Host Configuration Protocol for IPv6 (DHCPv6),* 2003.

[26] . A. C. . S. D. e M. G. E. , *Request for Comments: 4443 - Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification,* Network Working Group - The Internet Society, 2006.

[27] T. Narten, E. N. W. S. e H. S. , *Request for Comments: 4861 - Neighbor Discovery for IP version 6 (IPv6),* N. W. Group, Ed., 2007.

[28] R. H. e . S. D. , *Request for Comments: 3513 - Internet Protocol Version 6 (IPv6) Addressing Architecture,* N. W. Group, Ed., 2003.

[29] L. M. R. T. L. Z. G. L. M. B. CÉSAR A. H. Loureiro, “Uma análise das implementações de protocolos IPv6 puros e híbridos para provimento de mobilidade em IPv6,” *SBRC,*, pp. 321-334, 2012..

[30] R. H. . S. D. e E. N. , *Request for Comments: 3587 - IPv6 Global Unicast Address Format*, N. W. Group, Ed., Aug, 2003.

[31] R. H. e S. D. , *Request for Comments: 2375 - IPv6 Multicast Address Assignments*, N. W. Group, Ed., 1998.

[32] D. J. e S. D. , *Request for Comments: 2526 - Reserved IPv6 Subnet Anycast Addresses*, N. W. Group, Ed., 1999.

[33] A. F. G. R. R. Fey, Dominando Sub-redes no IPv4 e no IPv6, Caxias do Sul, 2014.

[34] Y. R. E. T. L. E. e S. H. E. , *Request for Comments: 4271 - A Border Gateway Protocol 4 (BGP-4)*, 2006.

[35] S. T. C. H. V. K. e M. S. , *Request for Comments: 3596 - DNS Extensions to Support IP Version 6*, N. W. Group, Ed., 2003.

[36] S. J. D. C. e . B. C. , *Request for Comments: 6563 - Moving A6 to Historic Status*, I. E. T. F. (IETF), Ed., 2012.

[37] . S. K. e K. S. , *Request for Comments: 4301 - Security Architecture for the Internet Protocol*, N. W. Group, Ed., 2005.

[38] L. A. e T. M. , *Request for Comments: 4026 - Provider Provisioned Virtual Private Network (VPN) Terminology*, N. W. Group, Ed., 2005.

[39] W. T. A. V. A. R. G. P. G. Z. e . B. P. , *Request for Comments: 2661 - Layer Two Tunneling Protocol "L2TP"*, N. W. Group, Ed., 1999.

[40] A. V. M. L. e T. K. , *Request for Comments: 2341 - Cisco Layer Two Forwarding (Protocol) "L2F"*, N. W. Group, Ed., 1998.

[41] K. H. G. P. . W. V. J. T. W. L. e . G. Z. , *Request for Comments: 2637 - Point-to-Point Tunneling Protocol (PPTP),* N. W. Group, Ed., 1999.

[42] D. J. Wetherall e A. S. Tanenbaum, Redes de Computadores, 5ª ed., São Paulo: PEARSON EDUCATION - BR, 2011, p. 600.

[43] . F. B. X. L. C. B. e K. Y. , *Request for Comments: 6144 - Framework for IPv4/IPv6 Translation,* I. E. T. F. (IETF), Ed., 2011.

[44] E. IPv6.br, "Recomendações do nic.br," CEPTRO., 2012.

[45] E. N. e . R. G. , *Request for Comments: 4213 - Basic Transition Mechanisms for IPv6 Hosts and Routers,* N. W. Group, Ed., 2005.

[46] . B. C. e C. J. , *Request for Comments: 2529 - Transmission of IPv6 over IPv4 Domains without Explicit Tunnels,* Network Working Group , 1999.

[47] D. F. T. L. . S. H. D. M. e P. T. , *Request for Comments: 2784 - Generic Routing Encapsulation (GRE),* 2000.

[48] D. A., P. Fasano, I. Guardini e D. Lento, "Request for Comments: 3053 - IPv6 Tunnel Broker," Network Working Group - Internet Engineering Task Force (IETF), janeiro 2001. [Online]. Available: https://tools.ietf.org/html/rfc3053. [Acesso em 22 julho 2014].

[49] A. D. R. D. . J. W. e Y. L. , *Request for Comments: 6333 - Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion,* Internet Engineering Task Force (IETF), 2011.

[50] C. B. M. C. H. Z. J. W. X. Li, *Request for Comments: 6219 - The China Education and Research Network (CERNET) IVI Translation - Design and Deployment for the IPv4/IPv6 Coexistence and Transition,* I. E. T. F. (IETF), Ed., 2011.

[51] . M. B. P. M. e I. v. B. , *Request for Comments: 6146 - Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers,* Internet Engineering Task Force (IETF), 2011.

[52] . M. B. . A. S. P. M. e I. v. B. , *Request for Comments: 6147 - DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers,* Internet Engineering Task Force (IETF), 2011.

[53] . C. B. C. H. . M. B. M. B. e X. L. , *Request for Comments: 6052 - IPv6 Addressing of IPv4/IPv6 Translators,* I. E. T. F. (IETF), Ed., 2010.

[54] R. H. e S. D. , *Request for Comments: 4291 - IP Version 6 Addressing Architecture,* Network Working Group, 2006.

[55] F. T. . T. G. e D. T. , *Request for Comments: 5214 - Intra-Site Automatic Tunnel Addressing Protocol (ISATAP),* Network Working Group, 2008.

[56] C. Huitema, *Request for Comments: 4380 - Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs),* Network Working Group, 2006.

[57] C. E. Perkins, "Mobile Networking Through Mobile IP," em *Journal IEEE Internet Computing*, NJ, USA, 1998.

[58] C. J. D. a. J. A. PERKINS, *Request for Comments: 6275 - Mobility Support in IPv6,* Internet Engineering Task Force (IETF), 2011.

[59] C. E. PERKINS, *Request for Comments: 2002 - IP Mobility Support,* Network Working Group , 1996.

[60] D. F. X. a. H. D. LE, “A review of mobility support paradigms for the internet,” *Communications Surveys & Tutorials, IEEE (Volume:8 , Issue: 1)*, vol. 8, nº 1, pp. 38 - 51, 5 Mar 2007.

[61] E. R. Koodli, *Request for Comments: 5268 - Mobile IPv6 Fast Handovers,* N. W. Group, Ed., 2008.

[62] E. R. Koodli, *Request for Comments: 5568 - Mobile IPv6 Fast Handovers,* N. W. Group, Ed., 2009.

[63] Z. L. X. a. Y. B. WANG, “Fast inter-MAP handover in HMIPv6,” em *Education Technology and Computer Science, 2009. ETCS '09. First International Workshop on*, Wuhan, Hubei, 2009.

[64] S. G. E. K. L. V. D. K. C. e B. P. , *Request for Comments: 5213 - Proxy Mobile IPv6,* Network Working Group, 2008.

[65] R. I. Meneguette, L. F. Bittencourt e E. R. M. Madeira, “Uma Política de Handover de Gerência de Mobilidade de Fluxo baseada em Lógica Fuzzy,” em *31º Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, Brasília - DF, 2013.

[66] E. A. M. AVELAR, L. L. MARQUES, T. Bemerguy e K. L. .. Dias, “Avaliando o protocolo PMIPv6 quanto ao Suporte à Qualidade de Experiência para Tráfego de Vídeo em um Testbed 802.11,” em *9th International Information and Telecommunication Technologies Symposium*, Rio de Janeiro., 2010.

[67] . J. K. . H. T. M. A. M. J. E. e A. L. , *Request for Comments: 5777 - Traffic Classification and Quality of Service (QoS) - Attributes for Diameter,* I. E. T. F. (IETF), Ed., 2010.

[68] J. D. McCabe, Practical Computer Network Analysis and Design (The Morgan Kaufmann Series in Networking), 1ª ed., Morgan Kaufmann, 1997, p. 367.

[69] S. S. C. P. e R. G. , *Request for Comments: 2212 - Specification of Guaranteed Quality of Service*, N. W. Group, Ed., 1997.

[70] J. Wroclawski, *Request For Comments: 2211 - Specification of the Controlled-Load Network Element Service,* 1997.

[71] D. Chalmers e M. Sloman, "A survey of quality of service in mobile computing environments," em *Communications Surveys, IEEE,* 1999.

[72] G. H. DA COSTA, "Métricas para Avaliação de Desempenho em Redes QoS sobre IP," Porto Alegre, RS, 2008..

[73] S. L. CECHIN, "Avaliação de Desempenho em Redes de Computadores," Porto Alegre, RS, 2005.

[74] E. T. L. MELO, "Qualidade de Serviço em redes IP com DiffServ: Avaliação," Florianópolis, SC, 2001.

[75] S. B. e J. M. , *Request for Comments: 2544 - Benchmarking Methodology for Network Interconnect Devices,* Network Working Group, 1999.

[76] N. Burgess, *Testing of Ethernet Services in Telecom Networks: RFC 2544,* Agilent Technologies, 2004.

[77] J. A. S. MONTEIRO, L. SAMPAIO e M. FIGUEREDO, "GT QoS relatório de avaliação dos pilotos," RNP - Rede Nacional de Ensino e Pesquisa, Rio de Janeiro , 2003.

[78] R. M. e J. P. , *Request for Comments: 2889 - Benchmarking Methodology for LAN Switching Devices,* Network Working Group, 2000.

[79] D. S. e B. H. , *Request for Comments: 3918 - Methodology for IP Multicast Benchmarking*, Network Working Group , 2004.

[80] K. Dubray, *Request for Comments: 2432 - Terminology for IP Multicast Benchmarking*, Network Working Group , 1998.

[81] J. M. Santos Pinheiro, "Prova de Conceito no Projeto de Redes de Computadores," Volta Redonda, 2010.

[82] P. W. E. L. Y. L. ZIMU, "Na Innovative IPv4-IPv6 Transition Way for Internet Service Provider," *Robotics and Applications (ISRA), 2012 IEEE Symposium on*, pp. 672 - 675, 03 Jun 2012.

[83] E. R. d. C. T. L. d. S. a. L. A. A. F. OLIVEIRA, "Análise dos Mecanismos de Gerenciamento de Mobilidade no IPv6," em *XXI Simpósio Brasileiro de Redes de Computadores*, Natal, CE, 2003.

[84] M. K. D. a. H. M. Menth, "Improvements to LISP Mobile Node," em *22nd International Teletraffic Congress (ITC)*, 2010.

[85] K. a. L. W. KONG, "Mobility management for all-IP mobile networks: mobile IPv6 vs. proxy mobile IPv6," *Wireless Communications, IEEE* , vol. 15, pp. 36 - 45, 18 Apr 2008.

[86] Q. Z. E. Y. M. H. HOU, "Design and Implementation of a Solution to Smooth IPv6 Transition.," *Advanced Intelligence and Awarenss Internet (AIAI 2010), 2010 International Conference on*, pp. 157 - 161, 25 out 2010.

[87] D. C. da Silva e C. d. C. Monteiro, "Análise da Latência de Handover do Protocolo SMIP," em *VII CONNEPI 2012*, PALMAS - TO, 2012.

[88] C. A. H. Loureiro, “Protocolos de Mobilidade sobre IPv6: Uma análise sobre MIPv6 x PMIPv6 x DMMS,” em *XIV SEMINÁRIO INTERMUNICIPAL DE PESQUISA*, GUAÍBA-RS, 2011.

[89] X. P. M. M. T. a. H. H. COSTA, “performance comparison of Mobile IPv6, Hierarchical Mobile IPv6, fast handovers for Mobile IPv6 and their combination,” *Sigmobile,*, pp. 5-19, 2003.

[90] M. Blanchet, *Request for Comments: 3531 - A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block*, Network Working Group - The Internet Society (2003), 2003.

[91] Cisco Systems, Inc., “Cisco 7206VXR Router,” 2015. [Online]. Available: http://www.cisco.com/c/en/us/products/routers/7206vxr-router/index.html. [Acesso em 11 maio 2015].

[92] Aker Security Solutions, *Manual Firewall Aker*, 2014.

[93] D. J. C. P. e J. A. , *Request for Comments: 3775 - Mobility Support in IPv6*, N. W. Group, Ed., 2004.

[94] A. M. V. N. SANTOS V., “Testes de mobilidade de rede (NEMO) em IPv6,” em *CISTI'2007 - 2ª Conferência Ibérica de Sistemas e Tecnologias de Informação*, Porto, Portugal, 2007.

[95] T. F. a. N. Y. YAN Chen, “QoS Requirements of Network Applications on the Internet,” *Management, Information-Knowledge-Systems*, vol. 4, pp. 55 - 76, Jan 2004.

[96] H. S. G. Tsirtsis, *RFC 4977. Problem Statement: Dual Stack Mobility*, 2007.

[97] A. J. Camilo Gomes, “Rede IP II: Melhores Práticas de Migração de Rede IPv4 para IPv6,” 13 fevereiro 2012. [Online]. Available:

http://www.teleco.com.br/tutoriais/tutorialredeipmig2/. [Acesso em 01 fevereiro 2015].

[98] E. Bergamin e J. O. Ferreira, "Técnica de utilização do mecanismo de transição "Tunnel Broker" para a comunicação do protocolo IPv6 em redes IPv4.," *Curso de Pós Graduação em Redes e Segurança de Sistemas - Pontifícia Universidade Católica do Paraná,* p. 10, Fev 2013.

[99] Hurricane Electric Internet Services, "Hurricane Electric Free IPv6 Tunnel Broker," Hurricane Electric, 1994. [Online]. Available: https://www.tunnelbroker.net/.

[100] R. Maia, "ENDEREÇAMENTO IPv6 - Tabela auxiliar ao Guia Didático do Projeto IPv6.br," 28 Nov 2014. [Online]. Available: http://diatinf.ifrn.edu.br/lib/exe/fetch.php?media=corpodocente:ronaldo:ipv6:tabela_auxiliar_ao_guia_didatico_do_ipv6.pdf. [Acesso em 20 Mar 2015].

[101] J. JAYANTHI, H. C. C. T. I. DEPT. OF COMPUT. SCI. e S. RABARA, "Transition and mobility management in the integrated IPv4 and IPv6 network - A systematic review," *Electronics and Information Engineering (ICEIE), 2010 International Conference On (Volume:1),* vol. 1, pp. V1-162 - V1-166, 13 Aug 2010.

[102] C. A. H. Loureiro, "Estudo e classificação de propostas e protocolos para provimento," UFRGS, Porto Alegre, 2012..

[103] . R. C. . D. F. e J. M. , *Requests for Comments: 2740 - OSPF for IPv6,* N. W. Group, Ed., 1999.

[104] T. L. e Y. R. , *Request for Comments: 2430 - A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE),* Network Working Group, 1998.

[105] B. B. . D. C. J. C. B. D. S. D. . D. E. S. F. V. J. G. M. C. P. L. P. K. R. . S. S. J. W. e L. Z. , *Request for Comments: 2309 - Recommendations on Queue Management and Congestion Avoidance in the Internet,* Network Working Group , 1998.

[106] R. E. Ferreira, Linux Guia do Administrador do Sistema, 2 ed., São Paulo, SP: Novatec, 2008, p. 720.

[107] FreeBSD Foundation, "The FreeBSD Project," FreeBSD Foundation, 2015. [Online]. Available: https://www.freebsd.org/. [Acesso em 21 março 2015].

[108] B. C. e K. M. , *Request for Comments: 3056 - Connection of IPv6 Domains via IPv4 Clouds,* Network Working Group, 2001.

[109] B. v. S. E. Hansen, "Redes IPv6: QoS em Ambientes IPv6 -," 08 Abr 2013. [Online]. Available: http://www.teleco.com.br/tutoriais/tutorialipv6seg/pagina_7.asp. [Acesso em 18 Dez 2014].

Apêndice A - Procedimentos de Configuração do *Tunnel Broker*

A funcionalidade *Tunnel Broker* é uma alternativa para se conseguir conectar à *Internet* via IPv6, quando ela ainda não está disponível em sua rede ou em seu provedor de *Internet* [48] .

Tunnel Server é um roteador de pilha dupla (IPv4 e IPv6) conectado à *Internet*. Após a recepção de uma ordem do *Tunnel Broker*, o *Tunnel Serve*r atua na manutenção de cada túnel, podendo também manter as estatísticas dos mesmos. Ele é o servidor que fecha o túnel com o cliente do túnel, trabalhando para fazer o interfaceamento entre o IPv6 e o IPv4.

O usuário do *Tunel Broker* é um roteador IPv6 de Pilha-Dupla conectado à *Internet* IPv4 e antes do usuário se conectar, o cliente deve se identificar e inserir as credenciais de autenticação do usuário, de modo que o túnel seja adequado conforme a configuração.

Na configuração do *Tunnel Broker*, após a autorização do cliente ao acesso do serviço, caso a máquina cliente rode um serviço de roteamento IPv6, a mesma estará pronta a realizar a distribuição de endereços de IPv6 para os pontos de rede.

Já o *Tunnel Server*, gerencia o cliente escolhendo o prefixo IPv6 a ser alocado para o cliente; determinando uma vida útil para o túnel; registrando automaticamente no DNS os endereços de IPv6 globais; configurando o *Tunnel Broker*; e notificando as informações relevantes para a configuração do cliente, incluindo parâmetros do túnel e registros de DNS.

Dentro do formato apresentado pela Figura 15, na página 60, o cliente deve especificar a quantidade desejada de endereços IPv6, possibilitando assim, que o roteador possa resolver a conectividade para os *hosts* na rede. Serão entregues endereços de tipo *unicast global*, o mesmo que receberia diretamente do provedor de *Internet* e após as etapas de configuração serem concluídas, o túnel IPv6 sobre IPv4 estará ativado e operando, acessando qualquer rede IPv6 [98].

O túnel é então estabelecido entre o *Tunnel Cliente* e o *Tunnel Server* e em seguida ao tunelamento nas duas pontas, no *Tunnel Cliente*, os pacotes IPv6 são encapsulados e enviados no túnel via *Internet* IPv4 utilizando o protocolo 41, o protocolo é utilizado tanto para o *Tunnel Server* quanto para o *Broker Cliente*; a partir deste ponto as estações da rede local podem utilizar o prefixo e autoconfigurar seus endereços IPv6 de escopo global para

que possam se comunicar com o servidor WEB IPv6 como se estivessem conectados ao *backbone* IPv6;

É importante salientar que toda a comunicação interna em IPv6 da LAN continua a ser realizada normalmente pelo endereço "FE80::/10" de escopo *link-local* possibilitando seu uso juntamente com o cenário de pilha-dupla (IPv4/IPv6) e todos os recursos e serviços IPv6 disponíveis.

Os túneis utilizados para os testes aqui conduzidos foram disponibilizados por meio da *Hurricane Eletric* (HE) – *Internet Service* [99]. A mesma provê túneis de maneira livre e gratuita, fornecendo o serviço de acesso à *Internet* por IPv6. Os serviços de *Tunnel Broker* da Hurricane são orientados para desenvolvedores e pesquisadores que querem utilizar um túnel estável nos estudos e implementação em seus aplicativos oferecendo vantagens como disponibilização de prefixo /48; a visão das tabelas de roteamento; suporte aos problemas através do email: ipv6@he.net; faz a habilitação e utilização do túnel em poucos instantes; possui Tunnel Servers em diversas áreas geográficas; e fornece até cinco túneis para cada usuário cadastrado [98].

Para a criação de Túneis Regulares a *Hurricane Eletric*® é um provedor de serviços de tunelamento sobre redes IPv4 possibilitando o alcance do IPv6 aos hosts e após a realização do cadastro e ativação da conta, o usuário pode solicitar até cinco túneis pelo site [99].

Na seção *User Functions*, se acessa o *link Create Regular Tunnel*. A página vai redirecionada para configuração do túnel. Nesta etapa, será informado no campo IPv4 *endpoint* o endereço de IP valido do utilizador na *Internet*. Será direcionado um túnel mais próximo e será realizado um teste de *ping* em cada servidor para saber o tempo de resposta e analisar o servidor mais próximo e com respostas mais rápidas. Para o Brasil tem sido direcionado o servidor de Miami, FL, EUA [209.51.161.58] [98].

No link *http://ipv6.br/tunnel-broker-via-hurricane-electric/* em [5] o usuário encontra um tutorial, de fácil entendimento, para a execução dos primeiros passos de criação de seu *Tunnel Broker*.

A ativação do túnel e configuração do endereço IPv6 no Linux segue a formatação descrita a seguir:

- Configuração *Linux-net-tools*

```
root@linuxA:/# ifconfig sit0 up
root@linuxA:/# ifconfig sit0 inet6 tunnel ::209.51.161.58
root@linuxA:/# ifconfig sit1 up
root@linuxA:/# ifconfig sit1 inet6 add 2001:470:4:d2b::/64
root@linuxA:/# route -A inet6 add ::/0 dev sit1
```

- Configurando o IPv6 no Linux como *router Ipv6*:

```
root@linuxA:/# modprobe ipv6
root@linuxA:/#  ip  tunnel  add  he-ipv6  mode  sit  remote
209.51.161.58 local 177.15.75.33 ttl 255
root@linuxA:/# ip link set he-ipv6 up
root@linuxA:/# ip addr add 2001:470:4:d2b::/64 dev he-ipv6
root@linuxA:/# ip route add ::/0 dev he-ipv6
root@linuxA:/# ip -f inet6 addr
```

- A configuração é seguinte:

```
root@linuxA:/# ifconfig
eth0 Link encap:Ethernet Endereço de HW 08:00:27:b0:a0:38
inet      end.:      128.67.64.1      Bcast:      128.67.64.255
Masc:255.255.252.0
endereço inet6: fe80::a00:27ff:feb0:a038/64 Escopo:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Métrica:1
pacotes RX:141175 erros:0 descartados:0 excesso:0 quadro:0
Pacotes TX:108851 erros:0 descartados:0 excesso:0 portadora:0
colisões:0 txqueuelen:1000
RX bytes:39466100 (39.4 MB) TX bytes:14141214 (14.1 MB)

he-ipv6 Link encap:IPv6 sobre IPv4
endereço inet6: fe80::/64 Escopo:Link
endereço inet6: 2001:470:4:d2b::/64 Escopo:Global
UP POINTOPOINT RUNNING NOARP MTU:1480 Métrica:1
pacotes RX:0 erros:0 descartados:0 excesso:0 quadro:0
Pacotes TX:0 erros:60 descartados:0 excesso:0 portadora:60
```

```
colisões:0 txqueuelen:0
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
lo Link encap:Loopback Local
inet end.: 127.0.0.1 Masc:255.0.0.0
endereço inet6: ::1/128 Escopo:Máquina
UP LOOPBACK RUNNING MTU:16436 Métrica:1
 pacotes RX:70 erros:0 descartados:0 excesso:0 quadro:0
Pacotes TX:70 erros:0 descartados:0 excesso:0 portadora:0
colisões:0 txqueuelen:0
RX bytes:9368 (9.3 KB) TX bytes:9368 (9.3 KB)

sit0 Link encap:IPv6 sobre IPv4
endereço inet6: ::127.0.0.1/96 Escopo:Desconhecido
endereço inet6: ::192.168.1.115/96 Escopo:Compat
UP RUNNING NOARP MTU:1480 Métrica:1
pacotes RX:0 erros:0 descartados:0 excesso:0 quadro:0
Pacotes TX:0 erros:0 descartados:0 excesso:0 portadora:0
colisões:0 txqueuelen:0
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

sit1 Link encap:IPv6 sobre IPv4
endereço inet6: fe80::/64 Escopo:Link
endereço inet6: 2001:470:4:d2b::/64 Escopo:Global
UP POINTOPOINT RUNNING NOARP MTU:1480 Métrica:1
pacotes RX:54025 erros:0 descartados:0 excesso:0 quadro:0
Pacotes TX:53575 erros:0 descartados:0 excesso:0 portadora:0
colisões:0 txqueuelen:0
RX bytes:15871634 (15.8 MB) TX bytes:5555652 (5.5 MB)
```

É necessário que o *router* esteja habilitado para encaminhar o Protocolo 41, condição essencial para o funcionamento do *Tunnel Broker*. Dentro do cabeçalho IPv4, o Protocolo 41 é definido para encapsular o pacote IPv6. O firewall deve estar habilitado para este protocolo [98].

Pode ser utilizado o DHCPv6 para encaminhar endereços IPv6 automático na rede privada, também é possível fazer NAT na versão para IPv6, a rede privada com o NAT6 ficaria com escopo de *link-local* “FE80::/10”.

Para a checagem do funcionamento do *Tunnel Broker*, são sificientes a realização dos testes de *ping6* e *traceroute6* via *shell*.

Apêndice B - Procedimentos de Configuração do Servidor DNS e DHCP

Instalação e Configuração do DNS

Instalação simples, bastando utilizar o comando para iniciar.

 # apt-get install bind9

Após realizadas alterações no arquivo *`/etc/bind/named.conf.local`*, onde são configuradas as zonas de domínio do DNS Reverso e do DNS, para isto é necessária a criação um arquivo de configuração para cada um. Estes, foram criados com os nomes de *`db.rdns`* (DNS Reverso) e *`db.dns`* (DNS), os quais recebem os endereços e configurações necessárias para seu funcionamento e são encontrados no diretório */etc/bind/*. Dentro do arquivo *`named.conf.local`* são inseridas as seguintes informações:

```
zone
"8.a.0.c.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.2.a.0.3.1.0.2.ip6.arpa"
{
type master;
notify no;
file "/etc/bind/db.rdns";
allow-query { any; };
};
zone "dgp.eb.mil.br" {
type master;
file "/etc/bind/db.dns";
allow-query { any; };
};
O arquivo db.rdns, que é a configuração do DNS Reverso, foi
configurado da seguinte
forma:
; Arquivo reverso do dominio dgp.eb.mil.br
$TTL 800
$ORIGIN
8.a.0.c.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.2.a.0.3.1.0.2.ip6.arpa.
@ IN SOA ns.dgp.eb.mil.br. maq4.dgp.eb.mil.br. (
2013111201 ; Serial
604800 ; Refresh
4000 ; 86400 Retry
2419200 ; Expire
```

```
800 ) ; 604800 Negative Cache TTL
@ IN NS ns.
;@ IN NS dgp.
a.0.a.0 IN PTR maquina4.dgp.eb.mil.br.
```

Por fim, o arquivo *db.dns*, foi configurado desta forma:

```
; Arquivo dns do dominio dgp.eb.mil.br
;
$TTL 800
@ IN SOA ns.dgp.eb.mil.br. maq4.dgp.eb.mil.br. (
2013111201 ; serial
604800 ; refresh
4000 ; 86400 retry
2419200 ; expire
800 ) ;
@ IN NS ns.
@ IN NS dgp.eb.mil.br.
@ IN AAAA 2013:0a26::c0a8:0a0a
@ IN AAAA ::1
maquina4 IN AAAA 2013:0a26::c0a8:0a0a
```

Para testar o serviço, deve ser feita a reinicialização do *bind9*, com o comando apresentado a seguir:

 # service bind9 restart

Instalação e Configuração DHCPv6

O primeiro passo para instalação do serviço inicia-se com o pacote *isc-dhcp-server*, instala-se o mesmo através do comando abaixo:

 # apt-get install isc-dhcp-server

Ao fechar a instalação, deve-se efetuar a criação do arquivo de configuração do servidor DHCPv6, denominado *dhcpd6.conf*. Este deve estar localizado no diretório */etc/dhcp/*.

Tal arquivo serve para adição dos parâmetros para execução do servidor.

```
# Configuration file DHCPv6 server
# The ddns-updates-style parameter
ddns-update-style none;
update-static-leases off;
# option definitions common to all supported networks...
#option domain-name "example.org";
#option domain-name-servers ns1.example.org, ns2.example.org;
#max-lease-time 7200;
#default-lease-time 2592000;
#preferred-lifetime 604800;
#option dhcp-renewal-time 3600;
```

```
#option dhcp-rebinding-time 7200;
#allow leasequery;
option dhcp6.name-servers 2001:470:4:d2b::7;
option dhcp6.domain-search "dgp.eb.mil.br";
#option dhcp6.info-refresh-time 21600;
# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;
# Use this to send dhcp log messages to a different log file
#log-facility local7;
# Subnets DHCP server
#subnet 10.5.5.0 netmask 255.255.255.224 {
time 600;
# max-lease-time 7200;
#}
# Hosts Pool for Dynamic Addresses
shared-network IPv6 {
subnet6 2013:0a26:: /64 {
range6 2013:0a26::c0a8:2 2013:0a26::c0a8:ffff;
}
}
# Hosts Fixed Addresses
# host IPv6clientFixed {
# host-identifier option dhcp6.client-id 00:01:00:02:08:00:27:d2:2e:3e;
# fixed-address6 2001:470:4:d2b::700;
#}
# Hosts Dynamic Addresses with assigned DNS Server
# host IPv6client {
# host-identifier option dhcp6.client-id 00:01:00:02:08:00:27:d2:2e:3e;
# host-identifier option dhcp6.client-id 00:01:00:02:MAC;
# option dhcp6.name-servers 2001:470:4:d2b::7;
#}
```

Definição da interface para distribuição de endereços IPs. Para este estudo a interface definida foi a interface *eth1*, tal
Procedimento é configurado no arquivo */etc/default/isc-dhcp-server*.

```
#Defaults for dhcp initscript
#sourced by /etc/init.d/dhcp
#installed at /etc/default/isc-dhcp-server by the maintainer scripts
#
#This is a POSIX shell fragment
#
#On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#Separate multiple interfaces with spaces, e.g. “eth0 eth1”.
INTERFACES="eth1"
```

PARA FINALIZAR O DHCPv6, deve-se efetuar a inicialização do mesmo. Tal etapa é concluída com a execução do comando à seguir, como superusuário no terminal do servidor.

```
# /etc/init.d/isc-dhcp-server6 start
```

Apêndice C – Configuração do MIPv6

O Mobile IPv6 está implementado como módulo do *kernel*.

Este é introduzido no *source code* do *kernel* através de um sistema de *patch*, que vai adicionar um conjunto de diretórios ao *source code* e vai modificar outros diretórios para que esta opção possa ser ativada durante o processo de configuração.

Esta implementação do Mobile IPv6 foi preparada para a versão 2.4.4 do *kernel*.

Para aplicar o patch, deve-se obter o Mobile IPv6
Para instalar, devem-se executar as seguintes etapas:

• Descompactar o diretório do Mobile IPv6 com o comando "tar – zxvf mipv6-0.8.1-v2.4.2.tar.gz".

• Copiar o diretório"mipv6-0.8.1-v2.4.2.patch" que está dentro da pasta "mipv6-0.8.1-v2.4.2" para a pasta do *source code* do *kernel*.

• Testar se há existência de problemas com o comando "patch -p1 -- dry-run < mipv6-0.8.1-v2.4.2.patch".

• Se o comando anterior não indicar qualquer problema, pode-se correr o comando "patch -p1 < mipv6-0.8.1-v2.4.2.patch".

Depois de ter o *kernel* compilado e instalado em todas as máquinas, é necessário copiar a pasta dos módulos ("/lib/modules/2.4.2") para todas as máquinas.

O Mobile IPv6 é também constituído por ferramentas ao nível do utilizador, assim como *scripts* de inicialização do módulo. Para instalar estes diretórios, deve-se:

- Entrar na pasta "mipv6-0.8.1-v2.4.2/src/userspace"
- Executar o comando "make"
- Executar o comando "make install"

Para integrar a configuração do IPv6 no sistema já existente para o IPv4. É necessário instalar em todos os *routers*, que neste caso são o HA e o CN, o *radvd – Router advertisement Daemon*. Este software gera as mensagens que são utilizadas pelo MN para se auto-configurar quando muda de rede.

Para utilizar o Mobile IPv6 é necessário que o IPv6 esteja configurado com os endereços e rotas suficientes para que haja conectividade entre as 3 máquinas.
Foram criados endereços com um *escopo* do tipo *site local*, e utilizou-se os últimos 64 bits dos endereços que são criados automaticamente quando o

IPv6 inicia na máquina. O IPv6 pode ser ativado pelo comando "insmod ipv6" ou no *boot* da máquina, configurando os *scripts* obtidos anteriormente.

É necessário configurar o radvd para que o Mobile IPv6 funcione.
Ao instalar uma versão em RPM, pode-se encontrar o diretório de configuração em "/etc/radvd.conf". Nas versões de *source code*, existe um diretório dentro da pasta principal do radvd com o nome de "radvd.conf.example". Pode-se copiar este diretóriopara "/etc/radvd.conf" e editá-lo.

```
A configuração do CN é a seguinte:
interface eth1
{
AdvSendAdvert on;
MinRtrAdvInterval 3;
MaxRtrAdvInterval 10;
AdvHomeAgentFlag off;
#
# new EUI-64 prefixes
#
prefix fec0:0:0:3::0/64
{
AdvOnLink on;
AdvAutonomous on;
AdvRouterAddr on;
};
};
A configuração do HA é a seguinte:
interface eth1
{
AdvSendAdvert on;
MinRtrAdvInterval 3;
MaxRtrAdvInterval 10;
AdvHomeAgentFlag on;
prefix fec0:0:0:2::0/64
{
       AdvOnLink on;

AdvAutonomous on;
AdvRouterAddr on;
};
};
```

É importante observar que no HA o campo "AdvHomeAgentFlag" está com o valor de "on". Por omissão, vem definido a interface "eth0", mas há o entendimento nesse projeto que ao trabalhar, o MN liga-se ao "eth1" do HA e do CN.

O campo "AdvRouterAddr" também foi mudado para "on". O prefixo tem de acabar com um "0".
Configuração do Mobile IPv6

A configuração do Mobile IPv6 baseia-se em apenas dois diretórios:
• "/etc/mip6_acl.conf" - lista de acessos do HA

• "/etc/sysconfig/network-mip6.conf" – configuração do HA / MN / CN.

A lista de acessos do HA é configurada pelo seguinte sistema: • Para permitir o acesso de todos os MN com um endereço que tenha o prefixo fec0::2::/64, adiciona-se a seguinte linha: "ALLOW fec0::2::/64"

Para negar o acesso a todos cujos endereços têm o prefixo fec0::3:abcd::/80, adiciona-se "DENY fec0::3:abcd::/80" Os três elementos do Mobile IPv6 são configurados num único ficheiro. São ignorados os parâmetros que não dizem respeito a essa máquina.

Configuração do CN

O CN é configurado apenas pelo primeiro parâmetro do ficheiro, ou seja, basta indicar no início o seguinte: "FUNCTIONALITY=cn"

Ao activar o *Authentication Header* no *kernel* é necessário definir pelo menos um dos dois campos:
"MD5KEY="
"SHA1KEY="

O MD5 pode ter até 22 caracteres e o SHA1 até 27. É possível utilizar os algarismos, as letras minúsculas e maiúsculas e ainda o "." e o espaço.

Configuração do HA.

O HA é configurado por 6 parâmetros, sendo 2 opcionais. O primeiro é o seguinte: "FUNCTIONALITY=ha"

Para indicar o nível de *debug* que se pretente, utiliza-se o seguinte parâmetro: "DEBUGLEVEL=0"

Os valores possíveis são de 0 a 7. Este valor não tem qualquer significado se o *kernel* não tiver a opção de *debug* do Mobile IPv6 ativada.

Para escolher se os pacotes com um e*scopo* do nível *site local* são enviados para o MN, define-se o seguinte parâmetro: "TUNNEL_SITELOCAL=yes"

Ao ativar o *Authentication Header* no *kernel* é necessário definir pelo menos um dos dois campos:
"MD5KEY="
"SHA1KEY="

Estes campos devem ser iguais em todas as máquinas. O último parâmetro é normalmente sempre igual, um vez que indica a localização da lista de acessos do HA. "MOBILENODEFILE=/etc/mipv6_acl.conf"

Configuração do MN

O MN é configurado por 8 parâmetros, sendo 2 opcionais. O primeiro é o seguinte: "FUNCTIONALITY=mn"

"DEBUGLEVEL=1"

É necessário indicar o endereço do MN:
"HOMEADDRESS=3ffe:2620:6:1234:abcd::2/64"

Também é preciso indicar o endereço do HA:
"HOMEAGENT=3ffe:2620:6:1234:abcd::1/64"

Este endereço tem de ser acessível pelo CN.
Ao activar o *Authentication Header* no *kernel* é necessário definir pelo menos um dos dois campos:
"MD5KEY="
"SHA1KEY="

Estes campos devem ser iguais em todas as máquinas.
O MN pode solicitar mensagens de anúncio do *router* com um intervalo mínimo definido por: "RTR_SOLICITATION_INTERVAL=1"

Este valor está definido em segundos.
As solicitações contínuas ao *router* pelo MN, vão aumentando o seu intervalo de tempo entre elas até ao valor máximo de: "RTR_SOLICITATION_MAX_SENDTIME=5"

Este valor está definido em segundos.

Utilizar o Mobile IPv6

O Mobile IPv6 inicia com o *script* de inicialização que é instalado na pasta "/etc/rc.d/init.d", com o nome de "mobile-ip6". Se o IPv6 iniciar no *boot* do Linux, pode-se incluir este *script* no conjunto de serviços que arrancar na máquina. Caso contrário, arranca-se o Mobile IPv6 com o comando "/etc/rc.d/init.d/mobile-ip6 start". É necessário proceder do mesmo modo em todas as máquinas.

O "mipdiag" é um programa de interação com o Mobile IPv6. Este programa é instalado normalmente em "/usr/sbin". Existe documentação referente a este executável no sistema de ajuda do Linux.

Apêndice D – Procedimentos de Configuração e Testes dos Dispositivos que compõem a *PoC*.

EXPERIMENTO nº01

Configuração dos equipamentos (roteamento estático)

Comandos para os roteadores DGP e EXT1

- Habilitando o roteamento IPv6:

```
DGP#
DGP#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DGP(config)#ipv6 unicast-routing
DGP(config)#
```

- Configuração de endereço IPv6 *global-unicast* numa interface serial:

```
EXT1#
EXT1#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
EXT1(config)#interface serial [nº da interface]
EXT1(config-if)#ipv6 enable
EXT1(config-if)#ipv6 address [endereço IPv6*] [prefixo de
rede**]
EXT1(config-if)#clock rate [Banda***]
EXT1(config-if)#
```

Obs:

* notação do endereço configurado IPv6 tipo Global

** - refere-se ao no de bits que fazem parte do prefixo de rede.

*** - refere-se a taxa de transmissão de bits utilizada na .

- Configuração de endereço IPv6 *global-unicast* numa interface ethernet:

```
EXT1#
EXT1#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
EXT1(config)#interface ethernet [no da interface]
EXT1(config)#ipv6 enable
EXT1(config-if)#ipv6 address [endereço IPv6] [prefixo de
rede]
EXT1(config-if)#
```

- Configuração de uma rota default:

```
DGP#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DGP(config)#ipv6 route  ::/0 [interface de saída*]
DGP(config-if)#
```

Obs:

* - refere-se a interface pela qual o roteador comunica-se com seu ISP

SHOW RUNNING-CONFIG

- Este comando é utilizado para verificar a configuração do roteador. Observar se a interface está UP/DOWN, quais os endereços IPv6 de cada interface e a rota default.

Resultados DGP

```
DGP#show running-config
Building configuration...

Current configuration : 587 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname DGP
!
enable secret 5 $1$53N9$VIUVRghlRRihc/1yd2Q9r1
enable password router
```

```
!
ip subnet-zero
!
ipv6 unicast-routing
!
!
!
interface Ethernet0
 no ip address
 ipv6 address 2001:470:4:d2b::1/64
 ipv6 enable
!
interface Serial0
 no ip address
 shutdown
 no fair-queue
!
interface Serial1
 no ip address
 ipv6 address 2001:470:4:d2b::2/64
 ipv6 enable
!
ip classless
ip http server
ip pim bidir-enable
!
ipv6 route ::/0 2001:470:4:d2b
!
!
line con 0
 password router
line aux 0
line vty 0 4
!
end
```

Resultados EXT1

```
EXT1#show running-config
Building configuration...

Current configuration : 598 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname EXT1
!
enable secret 5 $1$KNqz$FJlrixXvAm.bMEfz5y0m7.
enable password router
!
ip subnet-zero
!
ipv6 unicast-routing
!
!
!
interface Ethernet0
```

```
 no ip address
 ipv6 address 2001:470:4:d2b::1/64
 ipv6 enable
!
interface Serial0
 no ip address
 ipv6 address 2001:470:4:d2b::1/64
 ipv6 enable
 clockrate 2000000
!
interface Serial1
 no ip address
 shutdown
!
ip classless
ip http server
ip pim bidir-enable
!
ipv6 route ::/0 2001:470:4:d2b::2
!
!
line con 0
 password router
line aux 0
line vty 0 4
 login
!
end
```

Para avaliação serão usados três comandos que são fundamentais para que se possa tirar as conclusões a respeito do correto funcionamento de nossa rede de testes. São eles os comandos ***ping6*** (que verifica a conectividade da rede IPv6), ***traceroute6*** (que mostra por quais roteadores um pacote enviado passa até alcançar seu destino) e o ***show ipv6 route*** (que apresenta a tabela de rotas de cada roteador).

PING6

- Verifica a conectividade entre a estação Linux A (de onde é executado o programa ping6) e a estação Linux B. O programa ping6 envia um pacote ICMP com 64 bytes de dados para o endereço indicado (neste caso testado 2001:470:4:d2b::2– endereço IPv6 do Linux A) e aguarda o retorno do mesmo, calculando o tempo gasto para execução desta tarefa.

```
[root@linuxA democlydes]# ping6 -c 5 2001:470:4:d2b::2
PING 2001:470:4:d2b::2 (2001:470:4:d2b::2) 56 data bytes
64 bytes from 2001:470:4:d2b::2: icmp_seq=1 ttl=62 time=7.88 ms
64 bytes from 2001:470:4:d2b::2: icmp_seq=2 ttl=62 time=7.15 ms
64 bytes from 2001:470:4:d2b::2: icmp_seq=3 ttl=62 time=7.25 ms
64 bytes from 2001:470:4:d2b::2: icmp_seq=4 ttl=62 time=7.09 ms
64 bytes from 2001:470:4:d2b::2: icmp_seq=5 ttl=62 time=6.98 ms

--- 2001:470:4:d2b::2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4044ms
rtt min/avg/max/mdev = 6.986/7.274/7.880/0.323 ms
```

- Verifica a conectividade entre a estação Linux B e a estação Linux A.

```
[root@linuxB carvalho]# ping6 -c 5 2001:470:4:d2b::2
PING 2001:470:4:d2b::1(2001:470:4:d2b::1) 56 data bytes
64 bytes from 2001:470:4:d2b::1: icmp_seq=1 ttl=62 time=8.08 ms
64 bytes from 2001:470:4:d2b::1: icmp_seq=2 ttl=62 time=6.94 ms
64 bytes from 2001:470:4:d2b::1: icmp_seq=3 ttl=62 time=7.05 ms
64 bytes from 2001:470:4:d2b::1: icmp_seq=4 ttl=62 time=7.04 ms
64 bytes from 2001:470:4:d2b::1: icmp_seq=5 ttl=62 time=6.92 ms

--- 2001:470:4:d2b::1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4042ms
rtt min/avg/max/mdev = 6.924/7.208/8.082/0.452 ms
```

TRACEROUTE6

- Mostra o caminho percorrido da estação Linux A até alcançar o destino, a estação Linux B. Podemos verificar que o pacote enviado do Linux A para o Linux B passa por 2001:470:4:d2b::1 - roteador DGP, interface ethernet 0, passa por 2001:470:4:d2b::1 - roteador EXT1, interface serial 0, e alcança seu destino ao chegar em 2001:470:4:d2b::2 – estação Linux B.

```
[root@linuxA democlydes]# traceroute6 2001:470:4:d2b::2
traceroute to 2001:470:4:d2b::2 (2001:470:4:d2b::2) from
2001:470:4:d2b::1, 30 hops max, 16 byte packets
 1  2001:470:4:d2b::1 (2001:470:4:d2b::1)  2.983 ms  2.537 ms *
 2  2001:470:4:d2b::1 (2001:470:4:d2b::1)  6.019 ms  27.437 ms *
 3  2001:470:4:d2b::2 (2001:470:4:d2b::2)  7.284 ms  7 ms  6.963
ms
```

- Mostra o caminho percorrido da estação Linux B até alcançar o destino, a estação Linux A. Podemos verificar que o pacote enviado do Linux B para o Linux A passa por 2001::1 - roteador EXT1, interface ethernet 0, passa por 2001:470:4:d2b::2- roteador DGP, interface serial 1, e alcança seu destino ao chegar em 2001:470:4:d2b::1 – estação Linux A.

```
[root@linuxB carvalho]# traceroute6 2001:470:4:d2b::1
traceroute to 2001:470:4:d2b::1 (2001:470:4:d2b::1) from
2001:470:4:d2b::2, 30 hops max, 16 byte packets
 1  2001::1 (2001::1)  2.748 ms  2.63 ms *
 2  2000::2 (2000::2)  7.256 ms  6.29 ms *
 3  2001:470:4:d2b::1  (2001:470:4:d2b::1)    7.696  ms    7.061
ms  6.914 ms
```

SHOW IPV6 ROUTE

- DGP – Pode-se verificar na tabela de rotas IPv6 do roteador DGP, que existem 3 tipos de rotas L, C, S. As rotas L (locais) são as rotas configuradas manualmente nas interfaces ou aquelas autoconfiguradas pelo protocolo IPv6. Por exemplo, as rotas para 2000::2/128 (1) - (endereço da interface serial 1) e 2001:470:4:d2b::1/128 (3) - (endereço da interface ethernet 0) são rotas do tipo "L" configuradas manualmente e são aprendidas pelas próprias interfaces. Já as rotas FE80::/10 (5)-(prefixo de endereço link local) e FF00::/8 (6)-(prefixo de endereço *multicast*) são rotas do tipo "L" configuradas automaticamente pelo protocolo. Essas rotas são necessárias para configurar equipamentos que não estão possuem endereços, para reconhecimento de vizinhos e reconhecimento de grupos *multicast*. As rotas do tipo "C" para 2000::/16 (2) e 2002::/16 (4) são de redes diretamente conectadas e aprendidas

respectivamente através das interfaces serial 1 e ethernet 0. A rota do tipo “S” para ::/0 (7) é uma rota default, isto é, indica o roteador para qual todos os pacotes enviados para redes que ele não conhece devem ser enviadas, neste caso para 2001:470:4:d2b::1 (endereço da rede 2000::/16 – diretamente conectada), entrada (2) da tabela de rotas.

```
DGP#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
Timers: Uptime/Expires

L   2000::2/128 [0/0]
     via ::, Serial1, 00:22:07/never      (1)

C   2000::/16 [0/0]
     via ::, Serial1, 00:22:10/never      (2)
L   2001:470:4:d2b::1/128 [0/0]

     via ::, Ethernet0, 00:15:02/never         (3)
C   2002::/16 [0/0]
     via ::, Ethernet0, 00:15:05/never    (4)
L   FE80::/10 [0/0]
     via ::, Null0, 00:35:09/never        (5)
L   FF00::/8 [0/0]
     via ::, Null0, 00:35:09/never        (6)
S   ::/0 [1/0]

     via 2001:470:4:d2b::1, Null, 00:22:10/never         (7)
```

- EXT1 – Verificamos que a tabela de rotas é bem semelhante a tabela do DGP, as diferenças se devem somente aos endereços das interfaces e a rota *default*.

```
EXT1#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
Timers: Uptime/Expires

L   2001:470:4:d2b::1/128 [0/0]
     via ::, Serial0, 00:26:38/never
C   2000::/16 [0/0]
     via ::, Serial0, 00:26:41/never
L   2001::1/128 [0/0]
     via ::, Ethernet0, 00:22:22/never
C   2001::/16 [0/0]
     via ::, Ethernet0, 00:22:25/never
L   FE80::/10 [0/0]
     via ::, Null0, 00:53:33/never
L   FF00::/8 [0/0]
     via ::, Null0, 00:53:33/never
S   ::/0 [1/0]
     via 2000::2, Null, 00:26:41/never
```

EXPERIMENTO nº02 (roteamento dinâmico)

Configuração dos equipamentos

Comandos para os roteadores DGP e EXT1

- Habilitando o roteamento IPv6:

```
DGP#
DGP#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DGP(config)#ipv6 unicast-routing
DGP(config)#
```

- Configuração de endereço IPv6 *global-unicast* numa interface serial:

```
EXT1#
EXT1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
EXT1(config)#interface serial [nº da interface]
EXT1(config-if)#ipv6 enable
EXT1(config-if)#ipv6 address [endereço IPv6*] [prefixo de rede**]
EXT1(config-if)#clock rate [Banda***]
EXT1(config-if)#
```

Obs:

* - refere-se a notação do endereço a ser configurado, padrão Global IPv6

** - refere-se ao no de bits que fazem parte do prefixo de rede

*** - refere-se a taxa de transmissão de bits utilizada nesta interface

- Configuração de endereço IPv6 *global-unicast* numa interface ethernet:

```
EXT1#
EXT1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
EXT1(config)#interface ethernet [nº da interface]
EXT1(config)#ipv6 enable
EXT1(config-if)#ipv6 address [endereço IPv6] [prefixo de rede]
EXT1(config-if)#
```

- Criação de um processo do protocolo RIPv6 e anuncio das redes conectadas:

```
DGP#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DGP(config)#ipv6 router rip [nome*]
DGP(config-router)#
```

Obs:

* - refere-se ao nome dado ao processo criado para o funcionamento do protocolo RIPv6, Ex: ipv6 *router rip* "**teste2"**.

- Habilitação do protocolo RIPv6 numa interface qualquer:

```
DGP#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DGP(config)#interface [tipo da interface] [nº da interface]
DGP(config-if)#ipv6 rip [nome] enable
```

- Anuncio das redes conectadas e habilitadas no processo do RIPv6:

```
DGP#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DGP(config)#ipv6 router rip [nome]
DGP(config-router)#redistribute connected
DGP(config-router)#
```

SHOW RUNNING-CONFIG

- Este comando é utilizado para verificar a configuração do roteador. Observar se a interface está UP/DOWN, quais os endereços IPv6 de cada interface, as interfaces que estão habilitadas e anunciadas no processo RIPv6.

Resultados DGP

```
DGP#show running-config
Building configuration...

Current configuration : 748 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname DGP
!
enable secret 5 $1$53N9$VIUVRghlRRihc/1yd2Q9r1
enable password cisco
!
ip subnet-zero
!
```

```
ipv6 unicast-routing
!
!
!
interface Ethernet0
 ip address 152.84.50.1 255.255.255.0
 ipv6 address 2001:470:4:d2b::1/64
 ipv6 enable
 ipv6 rip teste2 enable
!
interface Serial0
 no ip address
 shutdown
 ipv6 rip teste2 enable
 no fair-queue
!
interface Serial1
 no ip address
 ipv6 address 2001:470:4:d2b::2/64
 ipv6 enable
 ipv6 rip teste2 enable
!
ip classless
ip http server
ip pim bidir-enable
!
ipv6 router rip teste2
 redistribute connected
!
!
!
line con 0
 password cisco
line aux 0
line vty 0
 password cisco
 login
line vty 1 4
 login
!
end
```

Resultados EXT1

```
EXT1#show running-config
Building configuration...

Current configuration : 700 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname EXT1
!
enable secret 5 $1$KNqz$FJlrixXvAm.bMEfz5y0m7.
enable password cisco
!
ip subnet-zero
!
ipv6 unicast-routing
!
!
!
interface Ethernet0
 no ip address
 ipv6 address 2001:470:4:d2b::1/64
 ipv6 enable
 ipv6 nd managed-config-flag
 ipv6 rip teste2 enable
!
interface Serial0
 no ip address
 ipv6 address 2001:470:4:d2b::1/16
 ipv6 enable
 ipv6 rip teste2 enable
 clockrate 2000000
!
interface Serial1
 no ip address
 shutdown
!
```

```
ip classless
ip http server
ip pim bidir-enable
!
ipv6 router rip teste2
 redistribute connected
!
!
!
line con 0
 password cisco
line aux 0
line vty 0 4
 login
!
end
```

Neste item são apresentados três comandos fundamentais para que se possa tirar as conclusões a respeito do correto funcionamento de rede de testes. São eles os comandos ***ping6*** (que verifica a conectividade da rede IPv6), ***traceroute6*** (que mostra por quais roteadores um pacote enviado passa até alcançar seu destino) e o ***show ipv6 route*** (que apresenta a tabela de rotas de cada roteador).

PING6

- Verifica a conectividade entre a estação **Linux A** (de onde é executado o *program* a ping6) e a estação **Linux B.** O programa ping6 envia um pacote ICMP com 64 bytes de dados para o endereço indicado (neste caso 2001:470:4:d2b::1 – endereço IPv6 do Linux A) e aguarda o retorno do mesmo, calculando o tempo gasto para execução desta tarefa.

```
[root@linuxA democlydes]# ping6 -c 5 2001:470:4:d2b::2
PING 2001:470:4:d2b::2(2001:470:4:d2b::2) 56 data bytes
64 bytes from 2001:470:4:d2b::2: icmp_seq=1 ttl=62 time=6.77 ms
64 bytes from 2001:470:4:d2b::2: icmp_seq=2 ttl=62 time=6.69 ms
64 bytes from 2001:470:4:d2b::2: icmp_seq=3 ttl=62 time=6.91 ms
64 bytes from 2001:470:4:d2b::2: icmp_seq=4 ttl=62 time=6.79 ms
64 bytes from 2001:470:4:d2b::2: icmp_seq=5 ttl=62 time=6.75 ms

--- 2001:470:4:d2b::2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4042ms
rtt min/avg/max/mdev = 6.690/6.785/6.915/0.104 ms
```

- Verifica a conectividade entre a estação **Linux B** e a estação **Linux A.**

```
[root@linuxB carvalho]# ping6 -c 5 2001:470:4:d2b::1
PING 2001:470:4:d2b::1(2001:470:4:d2b::1) 56 data bytes
64 bytes from 2001:470:4:d2b::1: icmp_seq=1 ttl=62 time=6.87 ms
64 bytes from 2001:470:4:d2b::1: icmp_seq=2 ttl=62 time=6.69 ms
64 bytes from 2001:470:4:d2b::1: icmp_seq=3 ttl=62 time=6.65 ms
64 bytes from 2001:470:4:d2b::1: icmp_seq=4 ttl=62 time=7.08 ms
64 bytes from 2001:470:4:d2b::1: icmp_seq=5 ttl=62 time=6.81 ms

--- 2001:470:4:d2b::1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4037ms
rtt min/avg/max/mdev = 6.657/6.824/7.085/0.151 ms
```

TRACEROUTE6

- Mostra o caminho percorrido da estação **Linux A** até alcançar o destino, a estação **Linux B**. Podemos verificar que o pacote enviado do **Linux A** para o **Linux B** passa por 2001:470:4:d2b::1 - roteador **DGP**, interface ethernet 0, passa por 2001:470:4:d2b::1 - roteador **EXT1**, interface serial 0, e alcança seu destino ao chegar em 2001:470:4:d2b::2 – estação **Linux B**.

```
[root@linuxA democlydes]# traceroute6 2001:470:4:d2b::2
traceroute to 2001:470:4:d2b::2 (2001:470:4:d2b::2) from
2001:470:4:d2b::1, 30 hops max, 16 byte packets
 1  2001:470:4:d2b::1 (2001:470:4:d2b::1)  8.617 ms  2.403 ms *
 2  2001:470:4:d2b::1 (2001:470:4:d2b::1)  5.78 ms  6.277 ms *
 3  2001:470:4:d2b::2 (2001:470:4:d2b::2)  8.948 ms  6.787 ms  6.608
ms
```

- Mostra o caminho percorrido da estação **Linux B** até alcançar o destino, a estação **Linux A**. Podemos verificar que o pacote enviado do **Linux B** para o **Linux A** passa por 2001::1 - roteador **EXT1**, interface ethernet 0, passa por 2000::2 - roteador **DGP**, interface serial 1, e alcança seu destino ao chegar em 2001:470:4:d2b::1 – estação **Linux A**.

```
[root@linuxB carvalho]# traceroute6 2001:470:4:d2b::1
traceroute to 2001:470:4:d2b::1 (2001:470:4:d2b::1) from
2001:470:4:d2b::2, 30 hops max, 16 byte packets
 1  2001::1 (2001::1)  2.823 ms  2.273 ms *
 2  2000::2 (2000::2)  5.619 ms  5.739 ms *
```

```
 3  2001:470:4:d2b::1 (2001:470:4:d2b::1)  6.945 ms  6.84 ms  6.524
ms
```

SHOW IPV6 ROUTE

- DGP – Se pode verificar na tabela de rotas IPv6 do roteador DGP, que existem 3 tipos de rotas L, C, R. As rotas do tipo "L" são as rotas configuradas manualmente nas interfaces ou aquelas autoconfiguradas pelo protocolo IPv6. Por exemplo, as rotas para 2000::2/128 (1)-(endereço da interface serial 1) e 2001:470:4:d2b::1/128 (4)-(endereço da interface ethernet 0) são rotas do tipo "L" configuradas manualmente e são aprendidas pelas proprias interfaces. Já as rotas FE80::/10 (6)-(prefixo de endereço *link local*) e FF00::/8 (7)-(prefixo de endereço *multicast*) são rotas do tipo "L" configuradas automaticamente pelo protocolo. Essas rotas são necessárias para configurar equipamentos que não estão possuem endereços, para reconhecimento de vizinhos e reconhecimento de grupos multicast. As rotas do tipo "C" para 2000::/16 (2) e 2002::/16 (5) são de redes diretamente conectadas e aprendidas respectivamente através das interfaces serial 1 e ethernet 0. A rota do tipo "R" para 2001::/16 (3) é uma rota aprendida pelo protocolo RIPv6, através de sua interface serial 1(interface de comunicação com o EXT1), note que ele aprende essa rota através de um endereço *link local* (*), que o o endereço deste tipo para a interface serial 1 (cada interface é automaticamente configurada com um endereço desse tipo quando o protocolo IPv6 é habilitado na mesma).

```
DGP#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
Timers: Uptime/Expires

L   2000::2/128 [0/0]
     via ::, Serial1, 01:23:19/never                              (1)
C   2000::/16 [0/0]
     via ::, Serial1, 01:23:22/never                              (2)
R   2001::/16 [120/2]
                        via    FE80::200:CFF:FE46:DEBC*,    Serial1,
00:10:21/00:02:48       (3)
L   2001:470:4:d2b::1/128 [0/0]
     via ::, Ethernet0, 01:16:13/never                            (4)
C   2002::/16 [0/0]
     via ::, Ethernet0, 01:16:17/never                            (5)
L   FE80::/10 [0/0]
     via ::, Null0, 01:36:21/never                                (6)
L   FF00::/8 [0/0]
```

```
via ::, Null0, 01:36:21/never                                    (7)
```

- EXT1 – Verifica-se que a tabela de rotas é bem semelhante a tabela do DGP, as diferenças se devem somente aos endereços das interfaces e a rota aprendida por RIPv6.

```
EXT1#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
Timers: Uptime/Expires

L   2001:470:4:d2b::1/128 [0/0]
     via ::, Serial0, 01:22:30/never
C   2000::/16 [0/0]
     via ::, Serial0, 01:22:33/never
L   2001::1/128 [0/0]
     via ::, Ethernet0, 00:28:11/never
C   2001::/16 [0/0]
     via ::, Ethernet0, 00:28:14/never
R   2002::/16 [120/2]
     via FE80::200:CFF:FE46:DE08, Serial0, 00:09:48/00:02:53
L   FE80::/10 [0/0]
     via ::, Null0, 01:49:24/never
L   FF00::/8 [0/0]
     via ::, Null0, 01:49:24/never
```

EXPERIMENTO nº 03

Objetivos

Para este experimento foram utilizados equipamentos com suporte ao protocolo IPv6 (roteadores e estações) e um roteador com IOS sem suporte IPv6. Foram configuradas as interfaces *Ethernet* dos roteadores DGP e EXT1 e as estações Linux com endereços de rede IPv6 e também endereços IPv4. As interfaces Seriais dos roteadores DGP, EXT1 e IPv4 possuem apenas endereçosIPv4. Desta forma, se pode verificar no diagrama abaixo a formação de duas ”ilhas” IPv6. Para uni-las utilizou-se uma conexão através de um *Tunnel* entre os roteadores DGP e EXT1.

Configuração dos equipamentos

Comandos para os roteadores DGP e EXT1

- Habilitando o roteamento IPv6:

```
DGP#
DGP#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DGP(config)#ipv6 unicast-routing
DGP(config)#
```

- Configuração de endereço IPv6 global-unicast numa interface ethernet:

```
EXT1#
EXT1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
EXT1(config)#interface ethernet [nº da interface]
EXT1(config)#ipv6 enable
EXT1(config-if)#ipv6 address [endereço IPv6*] [prefixo de rede**]
EXT1(config-if)#
```

Obs:

* - refere-se a notação do endereço a ser configurado padrão IPv6 tipo Global

** - refere-se ao no de bits que fazem parte do prefixo de rede

- Configuração de endereço IPv6 *global-unicast* numa interface *tunnel*:

```
EXT1#
EXT1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
EXT1(config)#interface tunnel [nº da interface]
EXT1(config-if)#ipv6 enable
EXT1(config-if)#ipv6 address [endereço IPv6] [prefixo de rede]
EXT1(config-if)#
```

- Configuração de Tunnel entre dois roteadores para encapsulamento IPv6 sobre IPv4:

```
EXT1#
EXT1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
EXT1(config)#interface tunnel [nº da interface]
EXT1(config-if)#tunnel source [tipo da interface de saída*] [nº da interface]
EXT1(config-if)#tunnel destination [endereço de destino**]
EXT1(config-if)# tunnel mode ipv6ip***
```

Obs:

* refere-se a interface usada como fonte do *tunnel* Ex: Serial.

** refere-se ao endereço IPv4 da interface de destino do *tunnel* Ex: a interface serial 0 do roteador DGP, 200.20.20.2.

*** - refere-se ao modo de encapsulamento usado pelo *tunnel* Ex: neste caso usaremos IPv6 sobre IPv4.

- Criação de um processo do protocolo RIPv6 e anuncio das redes conectadas:

```
DGP#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DGP(config)#ipv6 router rip [nome*]
DGP(config-router)#
```

Obs:

* - refere-se ao nome dado ao processo criado para o funcionamento do protocolo RIPv6, Ex: ipv6 router rip "**teste3"**.

- Habilitação do protocolo RIPv6 numa interface qualquer:

```
DGP#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DGP(config)#interface [tipo da interface] [nº da interface]
DGP(config-if)#ipv6 rip [nome] enable
```

- Anuncio das redes conectadas e habilitadas no processo do RIPv6:

```
DGP#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
DGP(config)#ipv6 router rip [nome]
DGP(config-router)#redistribute connected
DGP(config-router)#
```

SHOW RUNNING-CONFIG

- Este comando é utilizado para verificar a configuração do roteador. Observar se a interface está *UP*/*DOWN*, quais os endereços IPv6 e IPv4 de cada interface. Verificar na interface as configurações do Tunnel e do processo RIPv6. Ainda é importante observar as configurações para IPv4 existente em toda rede, utilizando protocolo de roteamento RIP.

Resultados DGP

```
DGP#show running-config
Building configuration...

Current configuration : 598 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname DGP
!
!
ip subnet-zero
!
ipv6 unicast-routing
!
!
!
interface Tunnel0
 no ip address
 ipv6 address 3000::1/64
 ipv6 enable
 ipv6 rip 1 enable
 tunnel source Serial0
```

```
 tunnel destination 200.20.10.2
 tunnel mode ipv6ip
!
interface Ethernet0
 ip address 152.84.50.1 255.255.255.0
 ipv6 address 2001::1/64
 ipv6 enable
 ipv6 rip 1 enable
!
interface Serial0
 ip address 200.20.20.2 255.255.255.0
 no fair-queue
!
interface Serial1
 no ip address
 shutdown
!
router rip
 network 152.84.0.0
 network 200.20.20.0
!
ip classless
ip http server
ip pim bidir-enable
!
ipv6 router rip 1
 redistribute connected
!
!
!
line con 0
line aux 0
line vty 0 4
!
end
```

Resultados EXT1

```
EXT1#show running-config
Building configuration...
Current configuration : 598 bytes
```

```
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname EXT1
!
!
ip subnet-zero
!
ipv6 unicast-routing
!
!
!
interface Tunnel0
 no ip address
 ipv6 address 3000::3/64
 ipv6 enable
 ipv6 rip 1 enable
 tunnel source Serial0
 tunnel destination 200.20.20.2
 tunnel mode ipv6ip
!
interface Ethernet0
 ip address 200.20.30.1 255.255.255.0
 ipv6 address 2003::1/64
 ipv6 enable
 ipv6 rip 1 enable
!
interface Serial0
 ip address 200.20.10.2 255.255.255.0
 no fair-queue
!
interface Serial1
 no ip address
 shutdown
!
router rip
 network 200.20.10.0
 network 200.20.30.0
```

```
!
ip classless
ip http server
ip pim bidir-enable
!
ipv6 router rip 1
 redistribute connected
!
!
!
line con 0
line aux 0
line vty 0 4
!
end
```

Resultados IPV4

```
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname IPv4
!
!
!
!
!
!
ip subnet-zero
!
!
!
!
interface Ethernet0
 no ip address
 shutdown
 media-type 10BaseT
```

```
!
interface Ethernet1
 no ip address
 shutdown
 media-type 10BaseT
!
interface Serial0
 ip address 200.20.10.1 255.255.255.0
 no fair-queue
 clockrate 2000000
!
interface Serial1
 ip address 200.20.20.1 255.255.255.0
 clockrate 2000000
!
interface Serial2
 no ip address
 shutdown
!
interface Serial3
 no ip address
 shutdown
!
router rip
 network 200.20.10.0
 network 200.20.20.0
!
ip classless
no ip http server
!
!
line con 0
line aux 0
line vty 0 4
!
end
```

Neste item são apresentados três comandos fundamentais para que se possa tirar as conclusões a respeito do correto funcionamento da rede de testes. São eles os comandos ***ping6*** (que verifica a conectividade da rede IPv6), ***traceroute6*** (que

mostra por quais roteadores um pacote enviado passa até alcançar seu destino) e o ***show ipv6 route*** (que apresenta a tabela de rotas de cada roteador).

PING6

- Verifica a conectividade entre a estação **Linux A** (de onde é executado o programa ping6) e a estação **Linux B.** O programa ping6 envia um pacote ICMP com 64 bytes de dados para o endereço indicado (neste caso 2003::201:2ff:febf:a56b – endereço IPv6 do Linux B) e aguarda o retorno do mesmo, calculando o tempo gasto para execução desta tarefa.

```
[root@linuxA brasil]# ping6 2003::201:2ff:febf:a56b
PING 2003::201:2ff:febf:a56b(2003::201:2ff:febf:a56b) from
2001:470:4:d2b::2a0:c9ff:fec8:e0c2 : 56 data bytes
64 bytes from 2003::201:2ff:febf:a56b: icmp_seq=1 ttl=62 time=12.8 ms
64 bytes from 2003::201:2ff:febf:a56b: icmp_seq=2 ttl=62 time=11.9 ms
64 bytes from 2003::201:2ff:febf:a56b: icmp_seq=3 ttl=62 time=11.9 ms
64 bytes from 2003::201:2ff:febf:a56b: icmp_seq=4 ttl=62 time=11.9 ms
64 bytes from 2003::201:2ff:febf:a56b: icmp_seq=5 ttl=62 time=11.9 ms
64 bytes from 2003::201:2ff:febf:a56b: icmp_seq=6 ttl=62 time=12.6 ms

        --- 2003::201:2ff:febf:a56b ping statistics ---
        6 packets transmitted, 6 received, 0% loss, time 5010ms
        rtt min/avg/max/mdev = 11.908/12.225/12.874/0.410 ms
```

- Verifica a conectividade entre a estação **Linux B** e a estação **Linux A.**

```
[root@linuxB brasil]# ping6 2001:470:4:d2b::2a0:c9ff:fec8:e0c2
PING   2001:470:4:d2b::2a0:c9ff:fec8:e0c2(2001:470:4:d2b::2a0:c9ff:fec8:e0c2)   56
data bytes
64 bytes from 2001:470:4:d2b::2a0:c9ff:fec8:e0c2: icmp_seq=1 ttl=62 time=12.7 ms
64 bytes from 2001:470:4:d2b::2a0:c9ff:fec8:e0c2: icmp_seq=2 ttl=62 time=12.3 ms
64 bytes from 2001:470:4:d2b::2a0:c9ff:fec8:e0c2: icmp_seq=3 ttl=62 time=12.9 ms
64 bytes from 2001:470:4:d2b::2a0:c9ff:fec8:e0c2: icmp_seq=4 ttl=62 time=12.2 ms
64 bytes from 2001:470:4:d2b::2a0:c9ff:fec8:e0c2: icmp_seq=5 ttl=62 time=12.0 ms
64 bytes from 2001:470:4:d2b::2a0:c9ff:fec8:e0c2: icmp_seq=6 ttl=62 time=12.6 ms
64 bytes from 2001:470:4:d2b::2a0:c9ff:fec8:e0c2: icmp_seq=7 ttl=62 time=12.0 ms

--- 2001:470:4:d2b::2a0:c9ff:fec8:e0c2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6056ms
rtt min/avg/max/mdev = 12.073/12.434/12.929/0.325 ms
```

TRACEROUTE6

- Mostra o caminho percorrido da estação **Linux A** até alcançar o destino, a estação **Linux B**. Podemos verificar que o pacote enviado do **Linux A** para o **Linux B** passa por 2001::1 - roteador **DGP**, interface ethernet 0, passa por 3000::3 - roteador **EXT1**, interface tunnel 0, e alcança seu destino ao chegar em 2003::2201:2ff:febf:a56b – estação **Linux B**. Podemos verificar que os pacotes passam pela nuvem IPv4, sem serem percebidos, isto é, utiliza Tunnel com encapsulamento IPv6 sobre IPv4.

```
[root@linuxA brasil]# traceroute6 2003::201:2ff:febf:a56b
traceroute to 2003::201:2ff:febf:a56b (2003::201:2ff:febf:a56b)
 from 2001:470:4:d2b::2a0:c9ff:fec8:e0c2, 30 hops max, 16 byte packets
1  2001::1 (2001::1)  2.476 ms *  2.396 ms
2  3000::3 (3000::3)  10.843 ms *  11.007 ms
3   2003::201:2ff:febf:a56b (2003::201:2ff:febf:a56b)  12.227 ms  11.705
 ms  12.058 ms
```

- Mostra o caminho percorrido da estação **Linux B** até alcançar o destino, a estação **Linux A**. Podemos verificar que o pacote enviado do **Linux B** para o **Linux A** passa por 2003::1 - roteador **EXT1**, interface ethernet 0, passa por 3000::1 - roteador **DGP**, interface tunnel 0, e alcança seu destino ao chegar em 2001:470:4:d2b::2a0:c9ff:fec8:e0c2 – estação **Linux A**. Podemos verificar que os pacotes passam pela nuvem IPv4, sem serem percebidos, isto é, utiliza Tunnel com encapsulamento IPv6 sobre IPv4.

```
[root@multicast brasil]# traceroute6 2001:470:4:d2b::2a0:c9ff:fec8:e0c2
traceroute to 2001:470:4:d2b::2a0:c9ff:fec8:e0c2
(2001:470:4:d2b::2a0:c9ff:fec8:e0c2) from 2003::201:2ff:febf:a56b, 30 hops
max, 16 byte packets
 1  2003::1 (2003::1)  2.975 ms  2.617 ms *
 2  3000::1 (3000::1)  10.953 ms  11.091 ms *
 3  2001:470:4:d2b::2a0:c9ff:fec8:e0c2 (2001:470:4:d2b::2a0:c9ff:fec8:e0c
2)  13.746 ms  12.076 ms  11.593 ms
```

SHOW IPV6 ROUTE

- DGP – Pode-se verificar na tabela de rotas IPv6 do roteador DGP, que existem 3 tipos de rotas L, C, S. As rotas L (locais) são as rotas configuradas manualmente nas interfaces ou aquelas autoconfiguradas pelo protocolo IPv6. Por exemplo, as rotas para 2001::1/128 (1)-(endereço da interface ethernet 0) e 3000::1/128 (4)-(endereço da interface tunnel 0) são rotas do tipo "L" configuradas manualmente e são aprendidas pelas proprias interfaces. Já as rotas FE80::/10 (6)-(prefixo de endereço *link local*) e FF00::/8 (7)-(prefixo de endereço *multicast*) são rotas do tipo

"L" configuradas automaticamente pelo protocolo. Essas rotas são necessárias para configurar equipamentos que não estão possuem endereços, para reconhecimento de vizinhos e reconhecimento de grupos multicast. As rotas do tipo "C" para 2001::/64 (2) e 3000::/64 (5) são de redes diretamente conectadas e aprendidas respectivamente através das interfaces serial 0 e tunnel 0. A rota do tipo "R" para 2003::/64 (3) é uma rota aprendida pelo protocolo RIPv6, através de sua interface tunnel 0(interface de comunicação com o EXT1), note que ele aprende essa rota através de um endereço *link local* (*), que o o endereço deste tipo para a interface tunnel 0 (cada interface é automaticamente configurada com um endereço desse tipo quando o protocolo IPv6 é habilitado na mesma).

```
DGP#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
Timers: Uptime/Expires

L   2001::1/128 [0/0]
     via ::, Ethernet0, 00:00:15/never                (1)
C   2001::/64 [0/0]
     via ::, Ethernet0, 00:00:18/never                (2)
R   2003::/64 [120/2]
     via FE80::C814:A02, Tunnel0, 00:08:26/00:02:59   (3)
L   3000::1/128 [0/0]
     via ::, Tunnel0, 00:08:28/never                  (4)
C   3000::/64 [0/0]
     via ::, Tunnel0, 00:08:31/never                  (5)
L   FE80::/10 [0/0]
     via ::, Null0, 00:09:25/never                    (6)
L   FF00::/8 [0/0]
     via ::, Null0, 00:09:25/never                    (7)
```

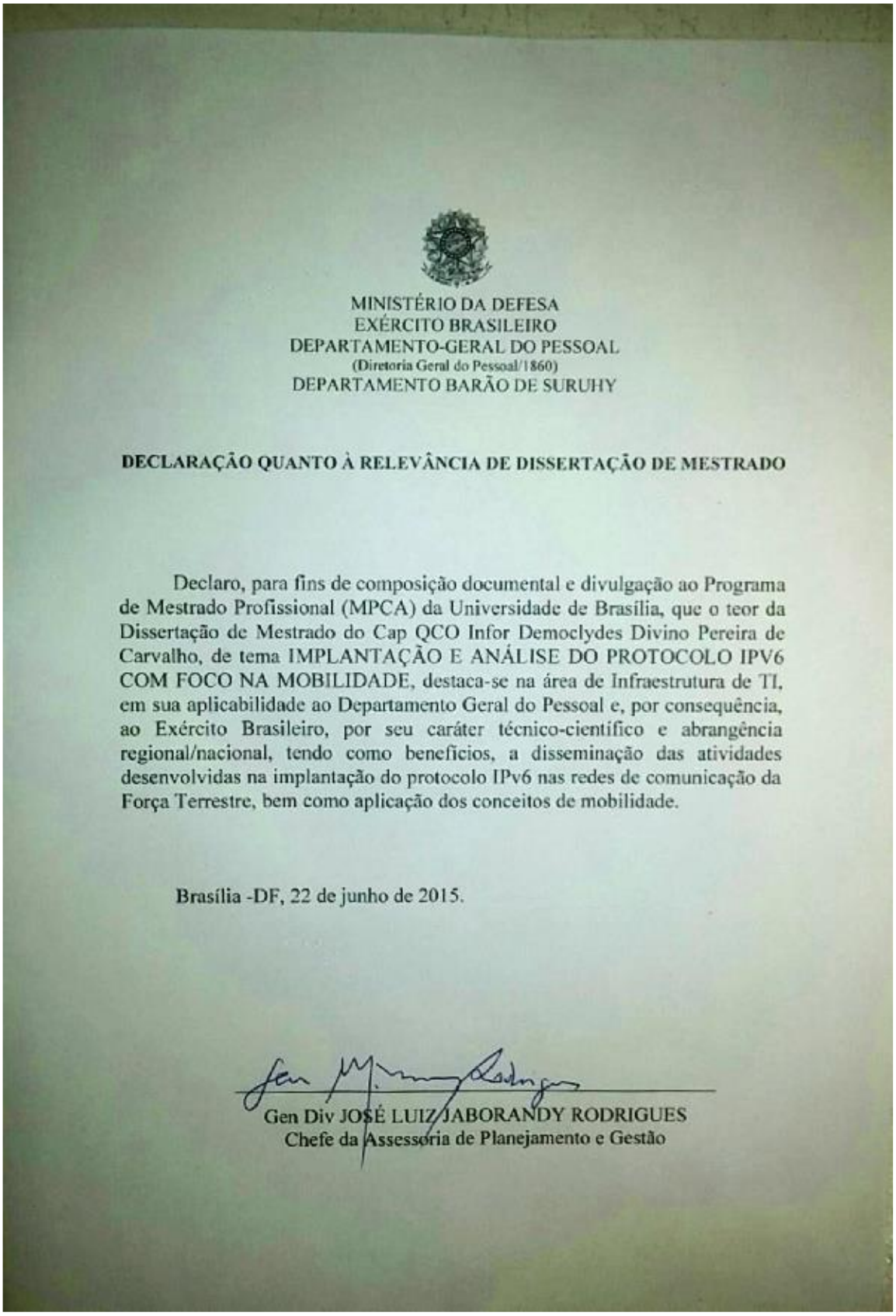
- EXT1 – Verifica-se que a tabela de rotas é bem semelhante a tabela do DGP, as diferenças se devem somente aos endereços das interfaces e a rota aprendida por RIPv6.

```
EXT1#sh ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
Timers: Uptime/Expires

R   2001::/64 [120/2]
     via FE80::C814:1402, Tunnel0, 00:05:54/00:02:03
L   2003::1/128 [0/0]
```

```
     via ::, Ethernet0, 00:06:47/never
C    2003::/64 [0/0]
     via ::, Ethernet0, 00:06:50/never
L    3000::3/128 [0/0]
     via ::, Tunnel0, 00:05:55/never
C    3000::/64 [0/0]
     via ::, Tunnel0, 00:05:58/never
L    FE80::/10 [0/0]
     via ::, Null0, 00:06:51/never
L    FF00::/8 [0/0]
     via ::, Null0, 00:06:51/never
```

Anexo I - Declaração quanto à Relevância



MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DEPARTAMENTO-GERAL DO PESSOAL
(Diretoria Geral do Pessoal/1860)
DEPARTAMENTO BARÃO DE SURUHY

DECLARAÇÃO QUANTO À RELEVÂNCIA DE DISSERTAÇÃO DE MESTRADO

Declaro, para fins de composição documental e divulgação ao Programa de Mestrado Profissional (MPCA) da Universidade de Brasília, que o teor da Dissertação de Mestrado do Cap QCO Infor Democlydes Divino Pereira de Carvalho, de tema IMPLANTAÇÃO E ANÁLISE DO PROTOCOLO IPV6 COM FOCO NA MOBILIDADE, destaca-se na área de Infraestrutura de TI, em sua aplicabilidade ao Departamento Geral do Pessoal e, por consequência, ao Exército Brasileiro, por seu caráter técnico-científico e abrangência regional/nacional, tendo como benefícios, a disseminação das atividades desenvolvidas na implantação do protocolo IPv6 nas redes de comunicação da Força Terrestre, bem como aplicação dos conceitos de mobilidade.

Brasília -DF, 22 de junho de 2015.

Gen Div JOSÉ LUIZ JABORANDY RODRIGUES
Chefe da Assessoria de Planejamento e Gestão

Figura 39 - Declaração de Relevância de Dissertação de Mestrado.

Anexo II Guia Didático de Endereçamento IPv6

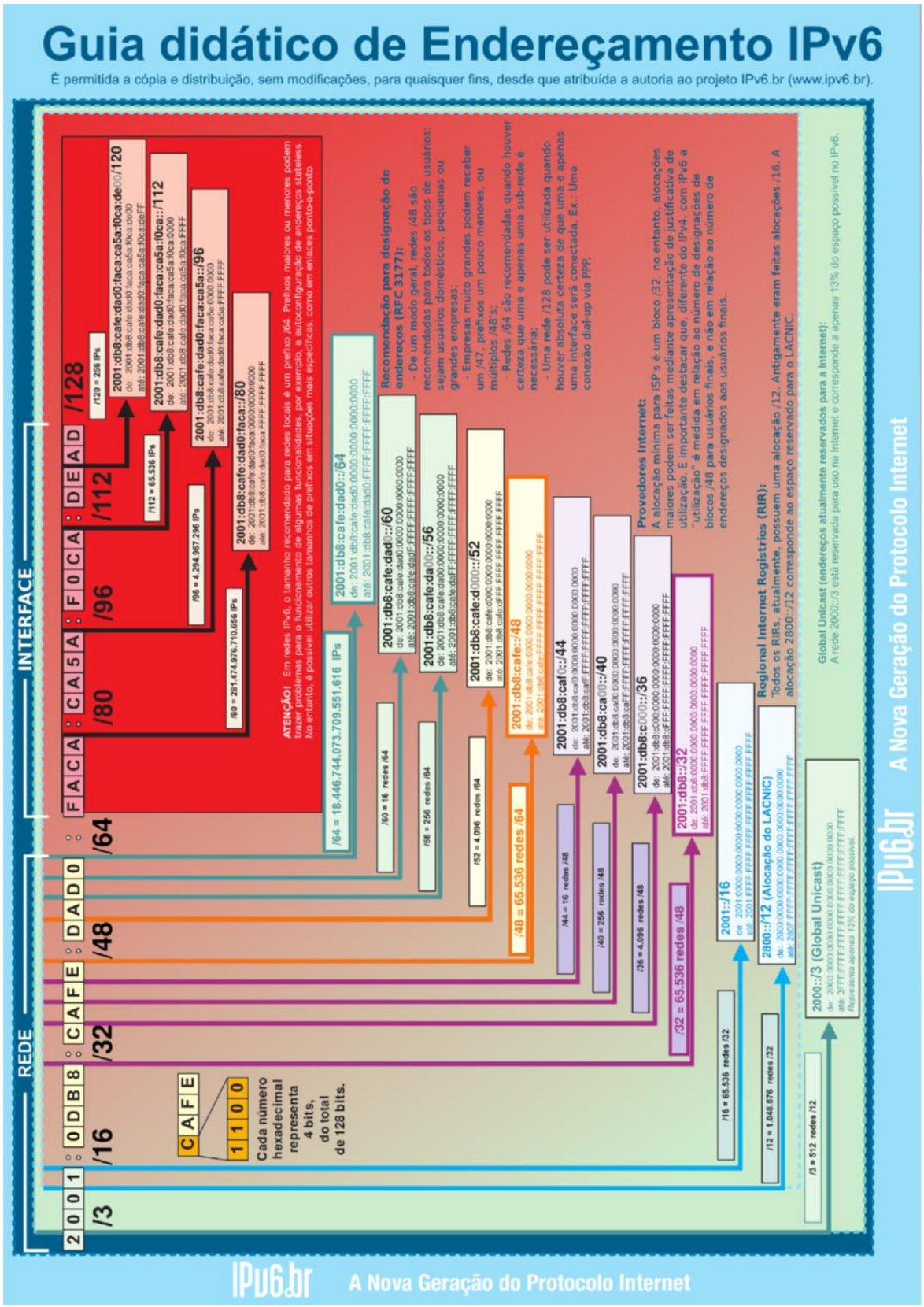
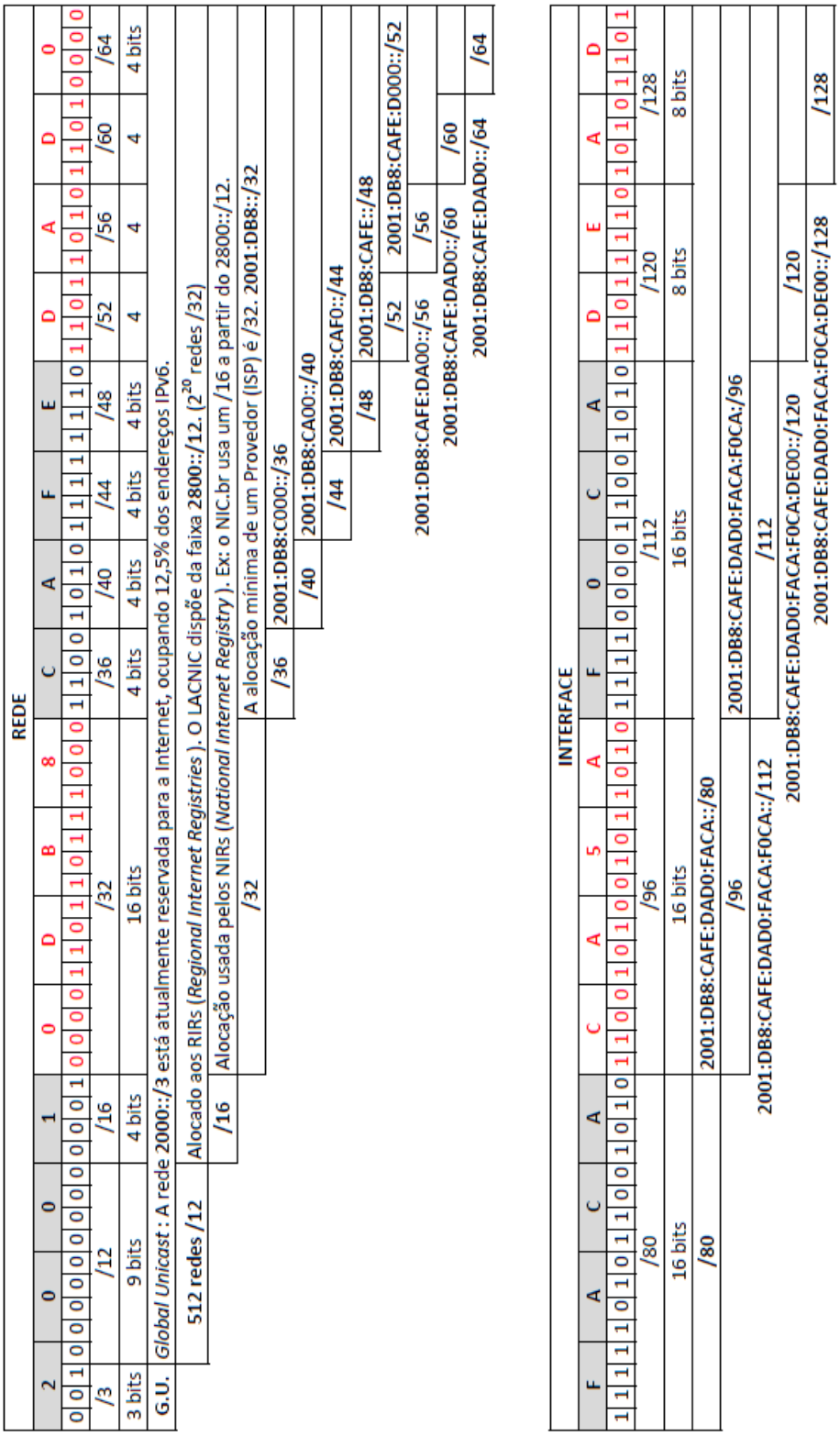


Figura 40 - Guia Didático de Endereçamento IPv6 [5]

Anexo III - Guia Didático de Endereçamento IPv6

Tabela 17 - ENDEREÇAMENTO IPv6 - Tabela auxiliar ao Guia Didático do Projeto IPv6.br [100]



Anexo IV - Topologia Física Interna do DGP

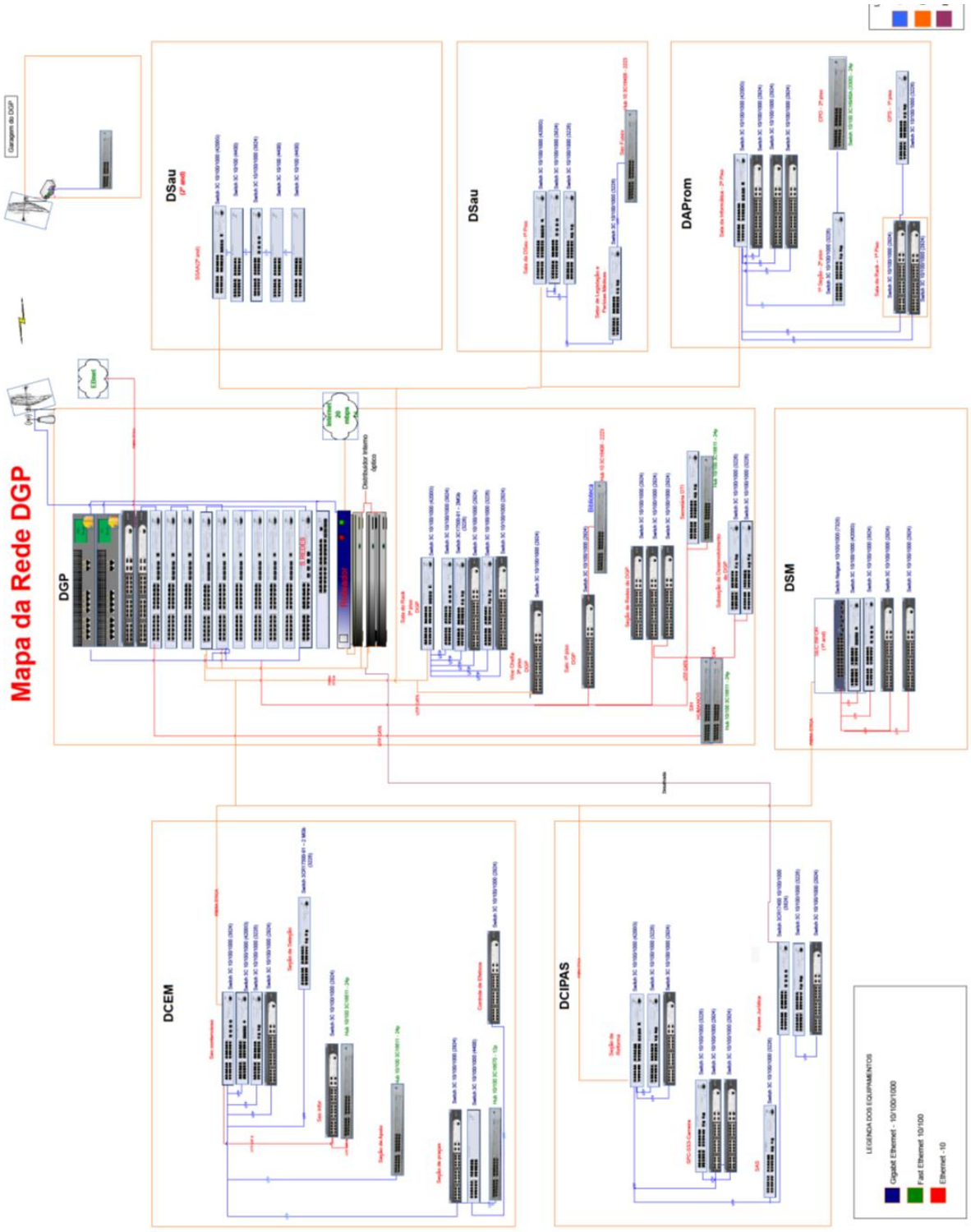
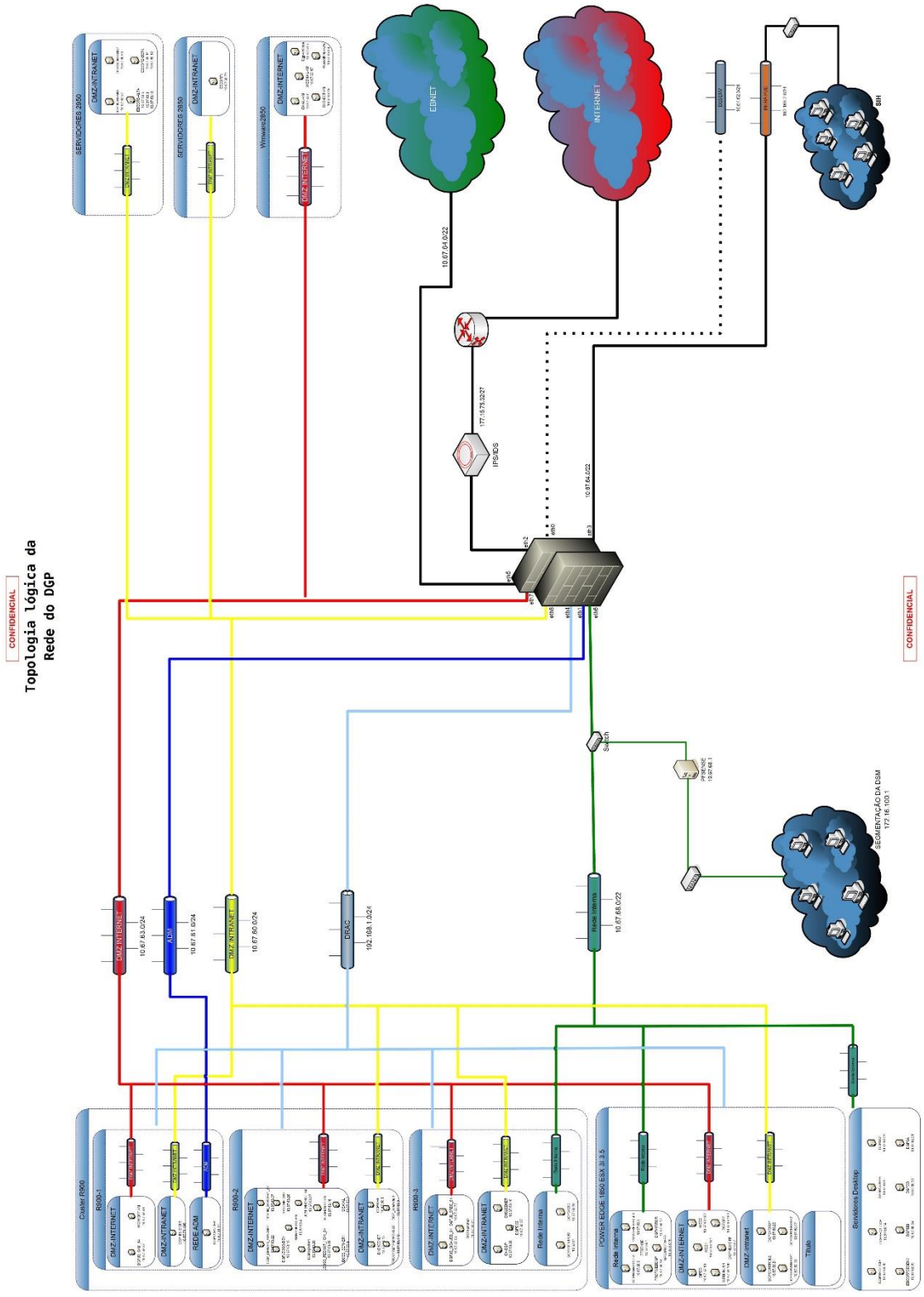


Figura 41 - Topologia Física Interna do DGP

Anexo V - Topologia Lógica Interna do DGP



Anexo VI - Resolução CGI.br/RES/007

O COMITÊ GESTOR DA *INTERNET* NO BRASIL – CGI.br, em sua 4ª Reunião Ordinária de 2012, realizada em 18 de maio de 2012, na sede do NIC.br, e no uso das atribuições que lhe confere o Decreto nº 4.829/2003, resolve aprovar esta Resolução, da seguinte forma:

Resolução CGI.br/RES/2012/007/P – Recomendação para Implantação do Protocolo IPv6

Considerando que:

– a *Internet* vem se expandindo e desenvolvendo continuamente, desde sua criação, e que essa expansão necessita ser preservada, tornando universal o acesso à rede;

– que à *Internet* estão sendo incorporados cada vez mais, diferentes tipos de dispositivos e equipamentos;

– que o IP (*Internet* Protocol) é o protocolo responsável por identificar cada um dos dispositivos presentes na *Internet* e por encapsular toda a informação que flui pela mesma, podendo ser considerado como a base tecnológica que separa a *Internet* dos outros serviços existentes sobre as redes de telecomunicações, sendo, portanto, de vital importância para seu funcionamento;

– que a versão 4 do IP, ou IPv4, que vem sendo usada na *Internet* desde janeiro de

1983, está em vias de se esgotar, não podendo mais sustentar o crescimento da rede e desenvolvimento futuros;

– que mesmo soluções paliativas, para a compartilhamento e preservação dos endereços IPv4, e que vêm sendo usadas com sucesso desde 1994 também alcançaram o seu limite de aplicação;

– que deste 1998 com o padrão RFC 2460 o IETF (*Internet Engineering Task Force*) desenvolveu uma nova versão do protocolo IP, a versão 6 - IPv6;

– que o IPv6 foi testado com sucesso em diversos ambientes de laboratório e em produção;

– que hoje o suporte ao IPv6 está disponível na maioria dos equipamentos usados no núcleo das redes, que os principais sistemas operacionais o suportam, e que muitos provedores de conectividade, acesso e serviços já o implantaram com sucesso;

– que o NIC.br tem capacitado técnicos, engenheiros e administradores de redes para que implantem e operem redes com suporte ao IPv6 ao longo dos últimos anos, por meio de diversas ações, como palestras, cursos e publicação de material pertinente em português; e

– que o NIC.br tem coordenado esforços com provedores de acesso, serviços e conteúdo na *Internet*, no sentido de realizar a implantação do IPv6 e que, como resultado destes esforços delineou-se um cronograma para nortear a implantação do IPv6 no Brasil.

Recomenda:

– que todas as redes conectadas à *Internet* no Brasil considerem, com a urgência necessária, a implantação do IPv6;

– que Sistemas Autônomos que proveem trânsito *Internet* para outros Sistemas Autônomos suportem o protocolo IPv6 à partir da segunda metade de 2012, em caráter de produção e em todas as localidades onde operam;

– que provedores de hospedagem, conteúdo e serviços na *Internet*, que incluem sítios Web, serviços de "e-mail", comércio eletrônico, serviços bancários e de governo prestados pela *Internet*, suportem o IPv6 antes de 01 de Janeiro de 2013;

– que provedores de acesso *Internet* ofereçam conectividade IPv6 de forma nativa, para todos os seus novos usuários, à partir de 01 de Janeiro de 2013, juntamente com conectividade IPv4, usando sempre que possível números IPv4 válidos ou, em caso de carência, IPv4 compartilhados ou mesmo técnicas de tradução que permitam ao usuário nativo de IPv6 acesso aos serviços que só respondem a IPv4;

– que provedores de acesso *Internet* ofereçam suporte ao IPv6 para todos os usuários antes de 01 de Janeiro de 2014;

– que provedores de acesso não utilizem técnicas para preservação e compartilhamento de IPs versão 4 de forma isolada sem a implantação concomitante do IPv6;

– que os fabricantes de equipamentos usados na *Internet*, incluindo-se mas não limitados a modems, roteadores e roteadores sem fio, ofereçam equipamentos compatíveis com IPv6, à partir da segunda metade de 2012;

– que as empresas usuárias da *Internet* realizem a implantação do IPv6 tanto em seus serviços expostos na *Internet*, como em sua rede interna, conforme as datas recomendadas, de forma planejada e com a urgência possível;

– que o governo, considerando-os aqui os três poderes e em suas diversas instâncias, estabeleça normas internas com cronograma conforme as datas aqui previstas e com metas claras para a implantação do IPv6, em especial nos serviços oferecidos aos cidadãos através da *Internet*; e

– que as universidades e centros de pesquisa, em especial os relacionados às disciplinas de redes, computação e *Internet*, implantem o IPv6 em suas redes com urgência.

Anexo VII - Resolução CGI.br/RES/033

O COMITÊ GESTOR DA *INTERNET* NO BRASIL – CGI.br, em sua 8ª Reunião Ordinária de 2013, realizada em 20 de setembro de 2013, na sede do NIC.br, e no uso das atribuições que lhe confere o Decreto nº 4.829/2003, resolve aprovar esta Resolução, da seguinte forma:

Resolução CGI.br/RES/2013/033 – Ações para fomentar a adoção do IPv6

Considerando que a disponibilidade de números IP, protocolo básico da *Internet*, em sua versão 4 (IPv4) e utilizada para comunicação entre todos os dispositivos da *Internet* desde janeiro de 1983, tem o seu esgotamento previsto para o primeiro semestre de 2014, e que isso gera a necessidade urgente da implantação da versão 6 do referido protocolo, o IPv6;

Considerando que o atraso na disseminação do IPv6 dificultará sobremaneira a expansão sustentável da *Internet* e que, sem o IPv6 adequada e tempestivamente implementado, surgirão diversos entraves na *Internet*, entre os quais notem-se:

Para usuários, uma experiência de navegação pior, eventual falha no funcionamento de serviços específicos como VoIP, jogos online, compartilhamento de arquivos *peer to peer*, streamings de vídeo etc;

- **Para provedores de acesso *Internet,*** uma complexidade maior em suas estruturas, com custos e complexidade crescentes;

- **Para provedores de conteúdo e serviços,** necessidade de adaptação nos sistemas de autenticação baseados no endereço IP, em sistemas de geolocalização e medições de seus usuários e serviços;
- **Para segurança e estabilidade da *Internet,*** dificuldade adicional na utilização de sistemas de segurança baseados em reputação dos IPs, como *blacklists*, e no uso do IPSec;
- **Para desenvolvedores,** eventual quebra da conectividade fim-a-fim, dificultando a inovação;

Considerando ainda que:

- Alguns dos **principais fornecedores de acesso** *Internet* ainda não oferecem conectividade IPv6 para os demais Sistemas Autônomos em toda sua área de abrangência, nem serviços completos de conectividade *Internet* com suporte a IPv6 para empresas e outras redes interessadas em usar IPv6 imediatamente;
- **Equipamentos** são comercializados no mercado nacional, sem suporte a IPv6, ou com funcionalidade diminuída em relação ao IPv4, incluindo-se aí telefones móveis e roteadores para uso doméstico;
- **"*Datacenters*" e serviços de hospedagem ("*hosting*"),** mesmo tendo conectividade externa IPv6, nem sempre a oferecem aos clientes de seus produtos e serviços;
- **Sítios de comércio eletrônico, bancos e instituições do governo** ainda não oferecem IPv6, dificultando a utilização do protocolo pelos novos usuários que venham com IPv6;
- Grande parte das **universidades** ainda não efetuou a implantação do IPv6 mesmo quando há a possibilidade de obtenção de conectividade externa, nem inclui o tema em seus cursos cabíveis, dificultando a formação de técnicos;
- **Não existe um cronograma de consenso** entre os setores envolvidos para a implantação do IPv6.

Resolve:

- Enviar ofício para SBC e sua Comissão Especial em Redes de Computadores e Sistemas Distribuídos (CE-ReSD), LARC, ANDIFES, ABRUEM, FEBRABAN, Câmara-e.net, principais operadoras de telecomunicações, principais empresas e entidades representativas ou com destaque, em diferentes setores, reforçando a urgência da implantação do IPv6 e questionando sobre que medidas estão sendo adotadas ou planejadas, e seu cronograma de implementação;

- Instruir o NIC.br para que incremente a produção de vídeos educativos e materiais didáticos sobre o assunto, com o objetivo de informar: (i) os gestores não familiarizados com tecnologia, (ii) os profissionais da área de TIC em geral, (iii) os profissionais de *Internet*, integrando uma campanha extensiva de conscientização sobre IPv6;
- Apoiar a Secretaria de Logística e Tecnologia da Informação, do Ministério de Planejamento, Orçamento e Gestão na criação de um plano de metas para a adoção do IPv6 nas entidades do Governo Federal.

E, recomenda, ainda, que:

- A Rede Nacional de Pesquisa apoie e incentive, utilizando os Pontos de Presença existentes, gestores de TI dos diferentes campi universitários na implantação do IPv6;
- As universidades ofereçam cursos de formação, capacitação ou educação continuada em IPv6.

  Os docentes de disciplinas de computação e redes utilizem em suas aulas estudos de casos, exemplos e laboratórios com IPv6.
- O Governo, considerando aqui os três poderes e suas instâncias Federal, Estadual e Municipal, inclua IPv6 como requisito na compra de equipamentos e em seu provimento de acesso à *Internet*, e estabeleça normas internas com cronograma e com metas claras para a implantação do IPv6, em especial nos serviços oferecidos aos cidadãos através da *Internet*.

Anexo VIII - Resolução CGI.br/RES/008

O COMITÊ GESTOR DA *INTERNET* NO BRASIL – CGI.br, em sua 3ª Reunião Ordinária de 2014, realizada em 04 de abril de 2014, na sede do NIC.br, no uso das atribuições que lhe confere o Decreto nº 4.829/2003, resolve aprovar a Resolução que segue:

Resolução CGI.br/RES/2014/008 – Recomendação para o suporte ao IPv6 em equipamentos que usam protocolos *Internet*

Considerando que, para os efeitos desta resolução, Sistemas Autônomos são todas as redes de *Internet* sob um bloco contíguo de endereços numéricos IPv4 ou IPv6 conforme definido na BCP6/RFC1930, "*Guidelines for creation, selection, and registration of an Autonomous System* (AS) ", e que recursos de endereçamento para os protocolos *Internet* IPv4 e IPv6, são requeridos pelos Sistemas Autônomos;

Considerando que Sistemas Autônomos são atribuídos a redes de universidades e instituições de pesquisa, e que hoje todas as instituições de certo porte podem requerer designação de Sistema Autônomo para suas redes, tal como o fazem as empresas de telecomunicações;

Considerando o esgotamento iminente dos endereços livres do Protocolo *Internet* versão 4 (IPv4), já ocorrido na região da Ásia e da Europa, e o processo em curso, de migração para o Protocolo *Internet* versão 6 (IPv6) na *Internet*, envolvendo a adaptação de todos os elementos e equipamentos envolvidos na *Internet*, citando-se como exemplo os utilizados por indivíduos, em residências, em equipamentos "inteligentes", jogos eletrônicos etc.;

Considerando os termos das Resoluções CGI.br/RES/2012/007/P e CGI.br/RES/2013/033, do Comitê Gestor da *Internet* no Brasil, que recomendam a aceleração da adoção do IPv6;

Considerando os princípios que fundamentam o desenvolvimento da *Internet*, tais como: a livre iniciativa do mercado; o processo colaborativo na definição de padrões, parâmetros e diretrizes; e a adoção de melhores práticas, todos já consagrados na Resolução CGI.br/RES/2009/003/P, do Comitê Gestor da *Internet* no Brasil (CGI.br);

Considerando, finalmente, que o braço operacional do CGI.br, o NIC.br tem se dedicado há mais de cinco anos na propagação do IPv6, seja com numerosos cursos periódicos, seja com palestras ou com geração de material técnico,

RESOLVE

- Recomendar que todos os equipamentos que podem ser conectados à *Internet*, fabricados ou vendidos no Brasil, tenham suporte aos protocolos IPv4 e IPv6, com paridade de funcionalidades, atendendo aos requisitos mínimos definidos no Anexo XIX desta resolução;
- **Recomendar a todos os usuários de *Internet*, empresas, órgãos do governo e outras instituições que oferecem serviços de acesso à *Internet* e, em particular, aos Sistemas Autônomos, que passem a adquirir apenas equipamentos com suporte aos protocolos IPv4 e IPv6, permitindo dessa forma a necessária adoção do protocolo IPv6;**
- Recomendar aos órgãos competentes de normatização e regulamentação nas áreas pertinentes, e aos órgãos e instituições de defesa dos interesses dos consumidores, que colaborem com ações que fomentem a inclusão do suporte ao IPv6 em todos os equipamentos pertinentes, e que facilitem a identificação de equipamentos compatíveis ou não pelos consumidores;
- Ratificar a continuidade do grupo de trabalho permanente de IPv6 no CGI.br/NIC.br, reforçando-o com convites para inclusão de representantes do MCTI, *MiniCom*, MDIC, Anatel, bem como outros órgãos envolvidos e interessados no processo de disseminação do IPv6.

Anexo XI - Resolução CGI.br/RES/2014/008

Requisitos mínimos para compatibilidade com IPv6.

Recomenda-se que todos os equipamentos conectados à *Internet*, para uso por indivíduos, em redes domésticas e de pequenas empresas, suportem o protocolo IPv6, em adição aos protocolos legados, conforme especificações em:

- RFC 2460 - *Internet Protocol, Version* 6 (IPv6) *Specification*

Em particular, recomenda-se que os equipamentos com função de terminal de acesso à *Internet*, incluindo, mas não se limitando a computadores, *tablets*, telefones móveis, *smart* TVs, discos para armazenamento de informações e backup em rede, servidores multimídia, e videogames, atendam aos requisitos especificados em:

- RFC 6434 – IPv6 *Node Requirement*s e
- RFC 7066 – IPv6 *for Third Generation Partnership Project* (3GPP) Cellular Host

Para os equipamentos com função de roteamento, em particular os utilizados para interligar a rede do usuário com a do provedor de acesso, recomenda-se que atendam aos requisitos definidos em:

- RFC 7084 – *Basic Requirements for IPv6 Customer Edge Routers*

Os documentos aqui especificados buscam representar um conjunto mínimo de funcionalidades para garantir o bom funcionamento e interoperabilidade dos equipamentos em redes e na *Internet* utilizando o protocolo IPv6. Funcionalidades diferentes ou adicionais podem ser necessárias em casos específicos, e devem ser consideradas pelos fabricantes.