SERGIO EDUARDO NUNES

ANÁLISE DE IMPACTO NA TRANSIÇÃO ENTRE PROTOCOLOS DE COMUNICAÇÃO IPv4 E IPv6

CAMPINAS

2013

UNIVERSIDADE ESTADUAL DE CAMPINAS
Faculdade de Tecnologia

SERGIO EDUARDO NUNES

ANÁLISE DE IMPACTO NA TRANSIÇÃO ENTRE PROTOCOLOS DE COMUNICAÇÃO IPv4 E IPv6

Dissertação apresentada à Faculdade de Tecnologia da Universidade Estadual de Campinas, como parte dos requisitos exigidos para obtenção do título de Mestre em Tecnologia.

Área de concentração: Tecnologia e Inovação.

Orientador: PROF. PAULO SÉRGIO MARTINS PEDRO, Ph.D
Co-orientador: PROF. Dr. EDSON LUIZ URSINI

CAMPINAS
2013

Ficha catalográfica

Universidade Estadual de Campinas

Biblioteca da Faculdade de Tecnologia

Vanessa Evelyn Costa – CRB 8/8295

Nunes, Sergio Eduardo, 1977-

N922a Análise de impacto na transição entre os protocolos de comunicação IPv4 e IPv6 / Sergio Eduardo Nunes. – Limeira, SP : [s.n.], 2013.

Orientador: Paulo Sérgio Martins Pedro.

Coorientador: Edson Luiz Ursini.

Dissertação (mestrado) – Universidade Estadual de Campinas, Faculdade de Tecnologia.

1. Redes de computadores - protocolos. 2. Redes de computadores - simulação por computador. I. Martins Pedro, Paulo Sérgio. II. Ursini, Edson Luiz. III. Universidade Estadual de Campinas. Faculdade de Tecnologia. IV. Título.

Informações para Biblioteca Digital

Titulo em outro idioma: Evaluating the impact of the IPv4/IPv6 transition.
Palavras-chave em Inglês:
Computer networks - protocols
Computer networks – computer simulation
Área de concentração: Tecnologia e Inovação
Titulação: Mestre em Tecnologia
Banca examinadora:
Paulo Sérgio Martins Pedro [Orientador]
Omar Carvalho Branquinho
Andre Franceschi de Angelis.
Data da defesa: 28/08/2013.
Programa de Pós-Graduação: Tecnologia

DISSERTAÇÃO DE MESTRADO EM TECNOLOGIA

ÁREA DE CONCENTRAÇÃO: TECNOLOGIA E INOVAÇÃO

Análise de impacto na transição entre protocolos de comunicação IPv4 e IPv6.

Sergio Eduardo Nunes

A Banca Examinadora composta pelos membros abaixo aprovou esta Dissertação:

Prof. Dr. Paulo Sérgio Martins Pedro
FT-UNICAMP
Presidente

Prof. Dr. André Franceschi de Angelis
FT-UNICAMP

Prof. Dr. Omar Carvalho Branquinho
PUCCAMP

Resumo

Neste trabalho, efetuou-se a avaliação de desempenho em uma rede de pequeno escritório, SOHO (*Small Office Home Office*), a fim de se conhecer o impacto nas redes de computadores, devido à utilização dos protocolos IPv4, IPv6 ou técnica de transição. As medições realizadas observaram o comportamento da vazão, latência, *jitter* e perda de pacotes, em três diferentes cenários experimentais: Rede IPv4, Rede IPv6 e Rede Pilha dupla. Os valores numéricos obtidos na análise das redes foram utilizados de forma incremental no programa de simulação ARENA, sendo modelada uma rede multisserviços com condições especiais para teste do impacto. O objetivo desta simulação é conhecer o impacto no comportamento dos serviços *stream* e elástico devido à variação de desempenho dos protocolos. Tais estudos objetivam ajudar aos administradores de redes no planejamento do período de transição e coexistência, possibilitando com que essa mudança nas redes de computadores possa ocorrer de forma mais suave.

Palavra-Chave: Redes de computadores – protocolos; Redes de computadores – simulação por computador.

Abstract

This work evaluated a SOHO network (Small Office Home Office) in order to assess the impact of the IPv4, IPv6, and their transition protocols, on these networks. The experiments performed measured throughput, latency, jitter and packet loss in three experimental settings: IPv4, IPv6 and Dual Stack. The numeric values obtained in this experimental analysis were further applied, in an incremental fashion, to a multi-services network model built using the ARENA simulation software. The goal of this simulation was to obtain a better understanding of the behavior of both the stream and the elastic services as a function of the variation in protocol performance. This knowledge aims at supporting network managers in their task of planning the transitional period from IPv4 to IPv6, thus allowing for a smoother transition between these protocols.

Keyword: Computer networks – protocols; Computer networks – computer simulation.

SUMÁRIO

Agradecimentos

Primeiramente, gostaria de agradecer ao meu orientador, Professor Paulo Sérgio Martins Pedro, Ph.D, e, co-orientador, Professor Dr. Edson Luiz Ursini, por todas as orientações, paciência e comprometimento.

A todos os colegas de faculdade, funcionários e professores da FT UNICAMP, muito obrigado por compartilharem os seus conhecimentos.

Um agradecimento especial aos meus familiares, minha avó, Iolanda, a minha esposa, Tatiane e a minha mãe, Cristina, meu pai, Sergio, por todo apoio, carinho e incentivo.

A Deus por ter colocado todas essas pessoas no caminho da minha vida e formação.

Lista de Figuras

Lista de Tabelas

Lista de Quadros

Lista de Abreviaturas e Siglas

CGI	Comitê Gestor de Internet
IANA	*Internet Assigned Numbers Authority*
IETF	*Internet Engineering Task Force*
IPng	*Internet Protocol Next Generation*
ISO	*Open Systems Interconnection*
LACNIC	*Latin America and Caribbean Network Information Centre*
MTU	Unidade Máxima de Transmissão
NAT	*Network Address Translation*
RFC	*Request for Comments*
SOHO	*Small Office Home Office*

1. INTRODUÇÃO

O crescimento ao acesso da população à Internet, o desenvolvimento de novos serviços multimídia, a popularização da Internet móvel e, respectivamente, dos seus serviços, foram alguns motivos do esgotamento do IPv4 e da necessidade de substituição desse protocolo. O IPv6 possui características e funcionalidades diferentes do seu antecessor, gerando algumas dúvidas e controvérsias sobre a nova versão do protocolo IP.

Na segunda metade da década de 1990, as regras para o funcionamento do novo protocolo estavam descritas na RFC 1617. Segundo [Tanenbaum, 1997], as quatro principais mudanças: 1) Na nova versão do protocolo, a quantidade de *bits* reservados resolve a escassez de endereços; 2) O aperfeiçoamento e a simplificação do cabeçalho, com campos menores que permitem o processamento dos pacotes com mais rapidez e melhora significativa no *throughput* e retardo; 3) Um suporte melhor às opções oferecidas, fazendo com que alguns campos que eram obrigatórios passassem a ser opcionais, tornando mais simples o encaminhamento dos pacotes pelos roteadores; 4) A segurança, em que a IETF (*Internet Engineering Task Force* – Força Tarefa de Engenharia de Internet) teve grandes esforços para promover mudanças. As recomendações da criação de um protocolo (RFC 1752), que resolvesse as deficiências do IPv4, para que tivesse alguns aperfeiçoamentos e melhoria no desempenho, foram atendidas com a criação do IPv6 [Hagen, 2002].

Estamos vivendo no período de transição e coexistência entre os protocolos de comunicação. Conforme alguns autores já citavam, "IPv6 e IPv4 irão coexistir por muitos anos" [*Hagen*, 2002].

A IANA (*Internet Assigned Numbers Authority* – Autoridade para Atribuição de Números da Internet), responsável pela administração dos registros de endereços IP, vem alertando sobre a redução de endereços de Internet, em ritmo significativo, e com isso o seu esgotamento [Christian O'Flaherty (et al.), 2009].

Durante um tempo, adotou-se o NAT (*Network Address Translation*) para que os problemas de falta de endereçamento fossem resolvidos. Porém, o advento de mais dispositivos conectados à rede mundial e o acesso crescente à Internet nos países em desenvolvimento contribuíram significativamente para que o protocolo IPv6 se tornasse uma necessidade iminente.

Esse contexto acabou por gerar uma nova problemática, pois não há possibilidade de se "abandonar" imediatamente o protocolo IPv4 e começar a utilização de uma rede apenas com IPv6. Com isso, entramos em uma era de coexistência e interoperabilidade entre os protocolos [Fiorentino, 2012].

Na transição, os administradores de redes, e os provedores de Internet poderão sofrer algum tipo de impacto em suas redes, em um ou mais níveis de serviço. Os administradores de redes que utilizam o modelo de gerenciamento ISO (*International Organization for Standardization* – Organização Internacional para Padronização) entendem as mudanças ocorridas e os impactos que possam ser causados por elas, como descrito a seguir:

- **Gerenciamento de Falhas:** Efetuar um plano de contingência com características que permitam a continuidade dos serviços com IPv4 e IPv6, além de efetuar as correções.
- **Gerenciamento de Contabilização:** As novas características das redes mudam a forma como se contabilizam os limites de utilização dos seus recursos. Assim sendo, estabelecer novos parâmetros torna-se necessário.
- **Gerenciamento de Configuração:** A primeira mudança necessária pertence a essa área de gerenciamento. As redes que permitem comunicação entre os dois protocolos precisam efetuar algumas mudanças em sua estrutura como, troca de equipamentos, novos hardware e software. Em alguns casos, somente novas configurações podem proporcionar um ambiente com interoperabilidade.
- **Gerenciamento de Desempenho:** Com a mudança de cenário, as características de desempenho sofrem alterações. Parâmetros que medem o desempenho da rede necessitam de adequações para que seja garantido o acordo de nível de serviço (SLA – *Service Level Agreement*).
- **Gerenciamento de Segurança:** Questões como vulnerabilidades e ameaças ganham outras características com o uso dos dois protocolos. O administrador de rede deverá recorrer a algumas técnicas para permitir a interoperabilidade e estas podem gerar riscos à segurança da rede.

Embora não seja o objetivo deste trabalho analisar o impacto financeiro que essas mudanças irão causar, vale lembrar que o advento do IPv6 e a necessidade do chamado "Período de Coexistência" gerarão custos. É necessária a aquisição de novos equipamentos de rede, software e profissionais especializados, gerando gastos aos provedores de Internet e demais

empresas que dependam de alguma infraestrutura de rede para a continuidade do seu negócio. Dependendo do caso, será importante que tais custos sejam quantificados.

1.1 Objetivos

O objetivo deste trabalho é analisar o impacto que as redes sofrerão no período em que os protocolos de comunicação IPv4 e IPv6 necessitarem conviver e até quando elas se tornarem "IPv6 Pura".

Entende-se por impacto a avaliação de desempenho de latência, *throughput*, perda de pacotes e *jitter* (detalhados no Capítulo 6). Em uma Rede IPv4, Rede Pilha dupla e Rede IPv6. Para isso, foram enviadas mensagens do tipo cliente/servidor, com pacotes de tamanhos variados (conforme experimento).

Foi montado um ambiente com diferentes plataformas de sistemas operacionais, escolhidas com base na Figura 01 (07/2013), em três cenários experimentais de uma rede de pequeno escritório ou doméstica denominada *SOHO* (*Small Office Home Office*).

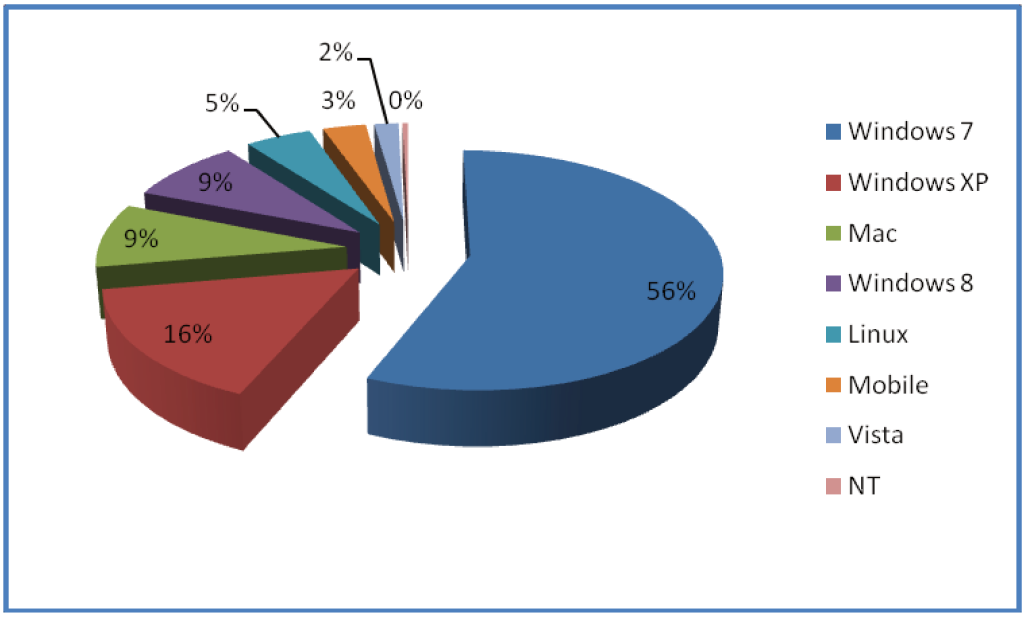

Figura 01 – Uso de Sistemas Operacionais (fonte w3counter.com)

Os cenários dos experimentos foram aplicados na topologia apresentada no Capítulo 5, sendo propostas situações que mais comumente são encontradas nas redes em convergência. Os roteiros dos experimentos propostos nesta dissertação estão descritos no diagrama da Figura 02:

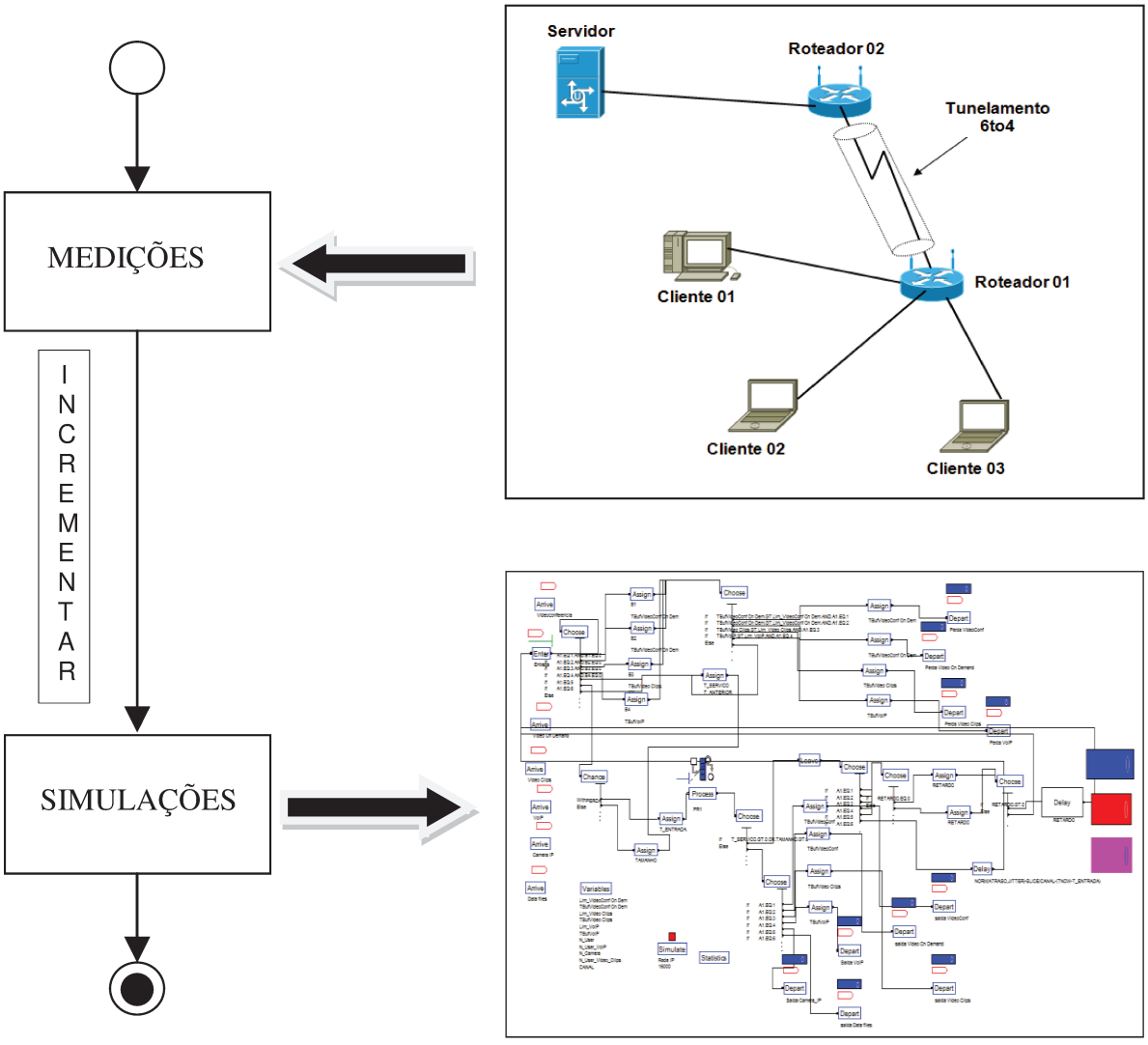

Figura 02 – Diagrama Simplificado de Atividades da Dissertação.

As medições efetuadas nos cenários experimentais, possibilitam estabelecer um comparativo de desempenho entre redes IPv4 x IPv6, IPv4 x Pilha dupla, IPv6 x Pilha dupla.

Após a coleta dos dados (vazão, latência, *jitter* e perda de pacotes), nos cenários experimentais, serão utilizados dados de forma incremental, na modelagem proposta na

Dissertação de Pinotti, F. (2011), no programa ARENA. As aplicações elásticas (TCP elástico) seguem o conceito de fluxo[1], em que, após um tempo (20 seg. de acordo com [Pinotti, 2001 – Pág. 07]) sem o usuário acessar um destino, para um determinado par origem-destino, considera-se o encerramento da transmissão, após um tempo sem tráfego, entre origem e destino.

O objetivo desta simulação é conhecer o comportamento que serviços *stream* e elástico terão devido à variação dos protocolos IPv4/IPv6 em um cenário com diversos tipos de serviços.

A metodologia de análise do impacto, em redes IPv4/IPv6, contribui no âmbito acadêmico para posteriores estudos em redes de maior complexidade física e/ou com mais serviços, com vistas a propostas de novas técnicas que possibilitem a coexistência.

Os administradores de redes necessitarão iniciar a implantação do IPv6 em sua estrutura de rede, conforme o define o CGI (Comitê Gestor da Internet no Brasil) em sua 4ª Reunião Ordinária em Maio/2012, na qual foi definido que: "As redes conectadas na Internet no Brasil considerem, com urgência necessária, a implantação do IPv6; Os provedores de acesso a Internet ofereçam conectividade IPv6 de forma nativa, para todos os seus usuários, a partir de 01 de Janeiro de 2013, juntamente com a conectividade IPv4", entre outras recomendações [CGI].

A metodologia baseada nas medições e simulações realizadas nesta dissertação permite aos profissionais de redes planejarem e dimensionarem os parâmetros determinantes no desempenho da rede, no período de implantação do novo protocolo, e, posteriormente, na coexistência dos protocolos IPv4/IPv6.

A hipótese geral levantada neste trabalho é que:

"*As redes deverão sofrer impacto, (latência, vazão,* perda de pacotes *e jitter) de certa magnitude, podendo ser irrelevante, moderado ou sensível ao tráfego elástico (menos prioritário), e ao tráfego "stream" (mais prioritário), devido à nova versão do protocolo, e/ou pela utilização dos mecanismos de transição".*

[1] Fluxo: conjunto de pacotes que correspondem a uma dada *especificação de fluxo* e que seguem um ao outro por intervalos de tempo não maiores que um dado limiar chamado de temporização (*time out*). A *especificação de fluxo* é determinada pela quíntupla: endereço de IP da origem, endereço IP do destino, número de porta da origem, número de porta do destino e protocolo de transporte. No modelo de simulação da rede do presente trabalho, o tráfego elástico é suposto modelado por fluxo, enquanto que o tráfego *stream* é modelado a partir do tipo de *codec* utilizado. Na verdade, a modelagem essencial do tráfego *stream* é baseada no nível 2 do modelo de referência OSI (enlace), mas modelada no nível 3 desse mesmo modelo como pequenos pacotes, e a do tráfego elástico no nível 3 do modelo OSI (mas com o conceito de fluxo de pacotes) [Oliver, 2001].

2. REVISÃO DE LITERATURA

O objetivo desta seção é apresentar trabalhos científicos relacionados ao tema proposto pela dissertação. Neste levantamento bibliográfico muitos trabalhos relacionados a redes IPv4/IPv6 estão disponíveis em acervos acadêmicos. Porém nenhum deles com ênfase na análise de impacto que os protocolos IPv4 e IPv6 poderão ocasionar, utilizando cenários experimentais e simulações.

Junior,L. *et al.* (2005) analisaram a segurança de redes puramente IPv6 em um ambiente Linux e Windows. Os autores utilizaram um programa do tipo *snnifer* para captura de pacotes e para testar a segurança nativa adotada pelos sistemas operacionais. Chegou-se à conclusão de que a segurança com IPSeg não está em conformidade ao determinado pela IETF, sendo os pacotes capturados facilmente, mesmo em redes puramente IPv6.

Ioan & Zeadally (2003) analisaram métricas como vazão (*throughput*), latência e taxa de utilização de processamento em dois mecanismos de transição entre roteadores, o 6to4, e o IPv4 *Tunneling*. Foi carregada a técnica de Pilha dupla no sistema operacional Windows 2000. Nesse tipo de cenário, foi concluído que a técnica de encapsulamento entre duas redes obteve um aumento no consumo de memória, porém, apresentou maior eficácia comparada ao IPv6 nativo. Embora as métricas utilizadas coincidam com a proposta desta dissertação (exceção à taxa de utilização de processamento). Este trabalho compara o desempenho das redes IPv4, IPv6 e Pilha dupla em uma rede SOHO e posteriormente, usa as medições em uma simulação de uma rede multisserviços.

Na fase de transição, as infraestruturas das redes terão que sofrer mudanças que possibilitem a comunicação entre as redes. Com isso, os mecanismos de transição entre os roteadores são necessários para a transferência dos pacotes; em Chang, Y. et al. (2004) foram feitas análises experimentais afim de se medir o desempenho, no mecanismo de tunelamento, entre roteadores que suportam pilha IPv4/IPv6. As métricas analisadas foram: a latência entre os enlaces, a taxa de utilização da CPU e a taxa de perda de pacotes. Os autores concluíram que o mecanismo 6to4 é o de mais fácil implementação; o túnel configurado é de mais rigorosa configuração por proporcionar mais controle ao *QoS, multicast e anycast*. Este artigo levou em consideração apenas o desempenho da rede pilha dupla. A dissertação proposta, compara o desempenho das redes IPv4, IPv6 e Pilha dupla.

Tatipamula & Grossetete (2004) indicaram boas práticas para implantação de mecanismos que permitam a coexistência entre os protocolos no tronco principal da rede (*backbone*), utilizando as técnicas de IPv6 em enlaces dedicados e prestadores de serviço de Internet. Os autores propuseram uma tabela comparativa para escolha estratégica, na infraestrutura da rede, na implantação do mecanismo de transição em *backbone*. O artigo apenas propõe praticas para o período de transição, enquanto a dissertação analisa o desempenho entre as redes IPv4, IPv6 e Pilha dupla.

Pinotti, F. (2011) propôs três modelos de simulação em ambiente multimídia, observando o *jitter* e latência e a degradação da qualidade de serviço ou bloqueio que esses parâmetros acarretam no tráfego dos serviços simulados. O autor considerou a influências dos serviços *stream* no tráfego TCP "elástico". Esse estudo foi utilizado como parte desta dissertação conforme descrito em mais detalhes nas seções seguintes.

3. PROTOCOLO DE COMUNICAÇÃO

O TCP é considerado um protocolo de transporte fim-a-fim, que garante a entrega confiável dos dados, livres de erro, na sequência certa e sem duplicações. "O *TCP/IP foi criado pensando em redes grandes e de longas distâncias, onde pode haver vários caminhos para o dado atingir o receptor*" [Torres, 2001]. Dentre os vários protocolos que compõem o conjunto TCP/IP (que abrangem apenas os níveis 3, 4 e 7 do protocolo OSI), destacam-se o TCP (Protocolo de Controle da Transmissão) e o IP (Protocolo de Internet). Ambos operam nas camadas de transporte e redes, respectivamente.

Em redes baseadas na comunicação TCP/IP, faz-se necessário que todos os dispositivos recebam endereços IP, sendo obrigatório esse identificador único, o qual permite a comunicação e a identificação dos dispositivos.

3.1 IPv4

O protocolo TCP foi definido na RFC 793, em setembro de 1981 [RFC 793]. É um protocolo usado no nível de transporte, juntamente com protocolos auxiliares. O IP fornece um serviço não confiável (*best effort*), podendo os pacotes chegarem fora de ordem, duplicados ou, ainda, ser perdidos. Isso simplifica a forma de transporte, o que facilita o roteamento. O endereçamento IPv4 contém 32 bits em sua estrutura, sendo divididos em quatro partes, cada parte contendo oito bits, como por exemplo 192.168.10.28 (onde cada ponto significa a separação de um byte). O protocolo IPv4 tem seu cabeçalho formado por 20 bytes obrigatórios e o restante destinado a uma série de opções. Na Figura 03, está mostrado o formato do cabeçalho e a descrição dos campos que o compõe.

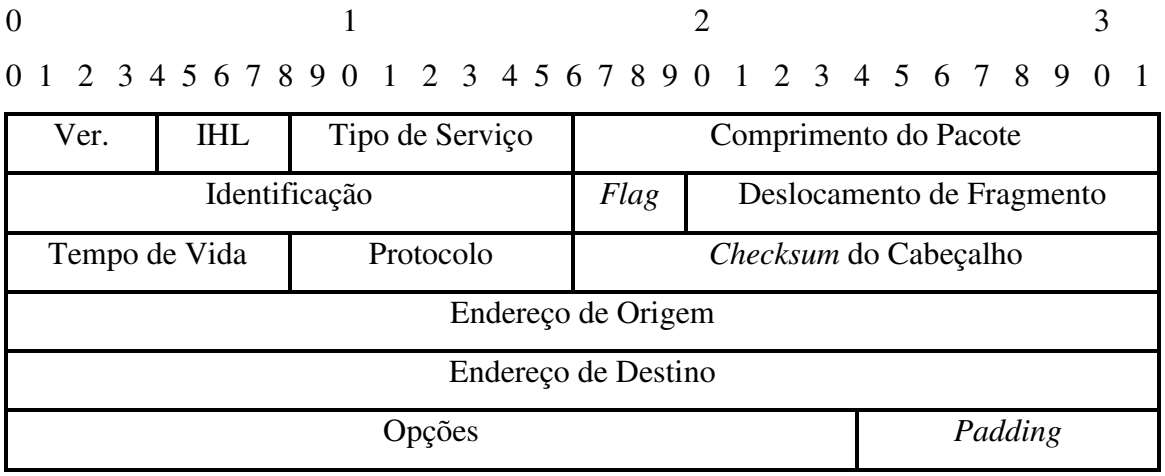

Figura 03 – Cabeçalho IPv4 [RFC 791].

- **Versão:** Este campo mostra a versão do protocolo IP.
- **IHL:** Especifica o tamanho do cabeçalho.
- **Tipo de Serviço:** Este campo tem 8 bits, permite determinar a prioridade do pacote, atuando, assim, diretamente na qualidade de serviço (QoS).
- **Comprimento do Pacote:** O campo fornece o tamanho total do pacote, incluindo o cabeçalho e os dados.
- **Identificação:** Os fragmentos do pacote IP original são identificados neste campo.
- ***Flag:*** Este campo é dividido em *Flag Mais Fragmentos (MF)*, que é representado por um bit, sendo usado para o deslocamento de fragmentos e posteriormente, na reconstrução dos pacotes. *Flag não Fragmentar (DF)*, indica que a fragmentação do pacote não é autorizada.
- **Deslocamento de Fragmento:** Este campo é responsável por identificar a ordem dos pacotes, sendo útil no momento da reconstrução.
- **Tempo de Vida:** Conhecido como TLL (*time to live*), possui 8 bits que indicam o "tempo de vida" que o pacote possui a cada salto pelos nós.
- **Protocolo:** Este campo possibilita, à camada de rede, repassar os dados para os protocolos corretos que estão nas camadas superiores.
- ***Checksum* do Cabeçalho:** É responsável por informar se há erros no cabeçalho.
- **Endereço de Origem:** Identifica o endereço do remetente.
- **Endereço de Destino:** Identifica o endereço do receptor.

- **Opções:** Campo que seria utilizado para implementaçoes opcionais.
- ***Padding:*** Preenchimento.

Com a utilização do protocolo de comunicação IPv4, o número de endereços possíveis é de 2^{32}, o que corresponde a 4.294.967.296 dispositivos. Estes endereços estão divididos em cinco classes (A, B, C, D e E). Na estrutura do IPv4, parte do endereço identifica a qual rede o pacote pertence (*Network Address*) e outra parte identifica o dispositivo. Conforme exemplo:

$$\underbrace{192.168.}_{\text{Endereço de Rede}}\underbrace{30.21}_{\text{Endereço de Dispositivo Final}}$$

Entre as principais vantagens do IPv4 estão: a) o protocolo não necessita de conexão antes dos pacotes serem enviados. b) o cabeçalho não é usado para garantir a entrega dos pacotes; c) o protocolo tem a capacidade de transportar os dados independentes do meio físico utilizado.

As desvantagens da primeira versão do protocolo podem ser apontadas como: a) o cabeçalho extenso; b) a quantidade de endereços insuficiente para atender a demanda atualmente; e c) a falta de autenticação de segurança.

3.2 IPv6

O protocolo IPv6 surgiu para suprir as deficiências do seu antecessor, o IPv4. Inicialmente, foi chamado de IPng (*Internet Protocol next generation*). Algumas de suas características se assemelham ao protocolo IPv4. A IETF (*Internet Engeeniring Task Force*) definiu algumas características por meio das RFCs relacionadas a seguir [Dados de RFCs disponíveis no site ipv6.br]:

RFC 2460 – Especificações do IPv6, de dezembro 1998.

RFC 2461 – Especificações de descoberta de vizinhos IPv6 (*Neighbor Discovery*).

RFC 4291 – Definições da arquitetura de endereçamento IPv6, em fevereiro de 2006.

RFC 4443 – Especificações do protocolo de controle de mensagem para Internet IPv6 (*Internet Control Message protocol*), chamado de ICMPv6.

O IPv6 tem endereçamento de 128 bits, o que possibilita 2^{128}, aproximadamente $3 * 10^{28}$ endereços possíveis. A forma como se escreve os endereços se distribuiu em oito grupos, cada um com quatro dígitos hexadecimais, como mostrado a seguir:

8000:0000:0010:0000:0123:4567:89AB:CDEF

Ao contrário do IPv4, a nova versão não possui endereço para fazer *broadcast.* O método utilizado para endereçar todos os nós, o endereço multicast do IPv6, que é representado por ff:0/8.

A IETF realizou um esforço para aumentar a segurança do IPv6. Para isso, o protocolo possibilita, em sua estrutura, autenticação e privacidade, oferecendo, consequentemente, uma melhora na qualidade de serviço (*QoS*). O cabeçalho teve uma simplificação, diminuiu para sete campos, facilitando o roteamento. Na Figura 04 são mostrados o cabeçalho IPv6 e as suas respectivas funções:

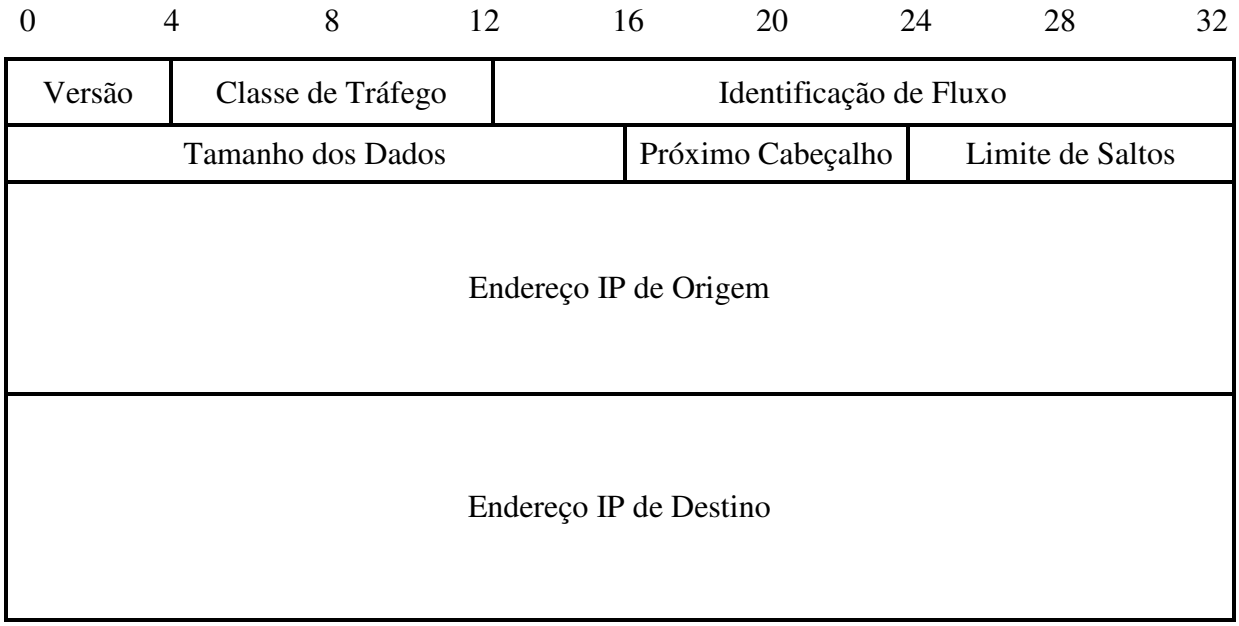

Figura 04 – Cabeçalho IPv6 [RFC 2460].

- **Versão:** Neste campo, é indicada a versão do protocolo IP utilizada.
- **Classe de Tráfego:** Indica qual o nível de prioridade.
- **Identificação de Fluxo:** Este campo faz o controle de fluxo de informação.

- **Tamanho dos Dados:** Neste campo, é calculado o tamanho total do datagrama.
- **Próximo Cabeçalho:** É utilizado para informar a presença de opções, chama-se de cabeçalhos de extensão.
- **Limite de Saltos:** Número máximo de nós que o pacote pode atravessar.
- **Endereço IP Origem:** Define o endereço do remetente.
- **Endereço IP destino:** Indica o endereço do destinatário.

3.3 Comparação dos Protocolos IPv4/IPv6

Os dois protocolos, quando comparados em sua estrutura, demonstram explicitamente os esforços para mudança das deficiências da versão antiga. Essas diferenças estão demonstradas no Quadro 01, baseadas em [Forouzan, 2006]:

Quadro 01 – Comparativo IPv4 e IPv6.

Versão / Itens	IPv4	IPv6
Quantidade de Endereços	2^{32}	2^{128}
Quantidade de Campos	14	8
MTU Mínimo	576 bytes	1.280 bytes
Representação do Endereço	4 Grupos com 8 bits	8 Grupos com 16 bits
Tamanho do Endereço (bits)	32	128
Roteamento	Tabela de roteamento grande	Efetuado pelo cabeçalho de extensão
Segurança	IPSeg facultativo	IPSeg Obrigatório
Qualidade de Serviço (QoS)	Sem Garantia	Através dos campos Classe de Tráfego e Identificação de Fluxo
Cabeçalho	Uso do Checksum	Mais simplificado

3.4 Esgotamento do IPv4

A LACNIC (*Latin American and Caribbean Internet Addresses Registry*) é a organização não governamental internacional responsável pelo registro e endereçamento de Internet da América Latina e Caribe. Há cinco dessas organizações pelo mundo afora: AfriNIC, APNIC, ARIN, LACNIC e RIPE NCC.

O site (http://www.lacnic.net) possui um serviço que fornece, em tempo real, a quantidade de IPv4 disponíveis para America Latina e Caribe. O site, foi acessado em 08/2013, informava ainda, que estava disponíveis para alocação aproximadamente 35.000.000 endereços IPv4, o que possibilita por volta de 265 dias até o seu esgotamento. A organização considera o estoque como esgotado quando a quantidade atingir 4.194.304 endereços. A Figura 05 demonstra a queda na quantidade de IPv4 disponível.

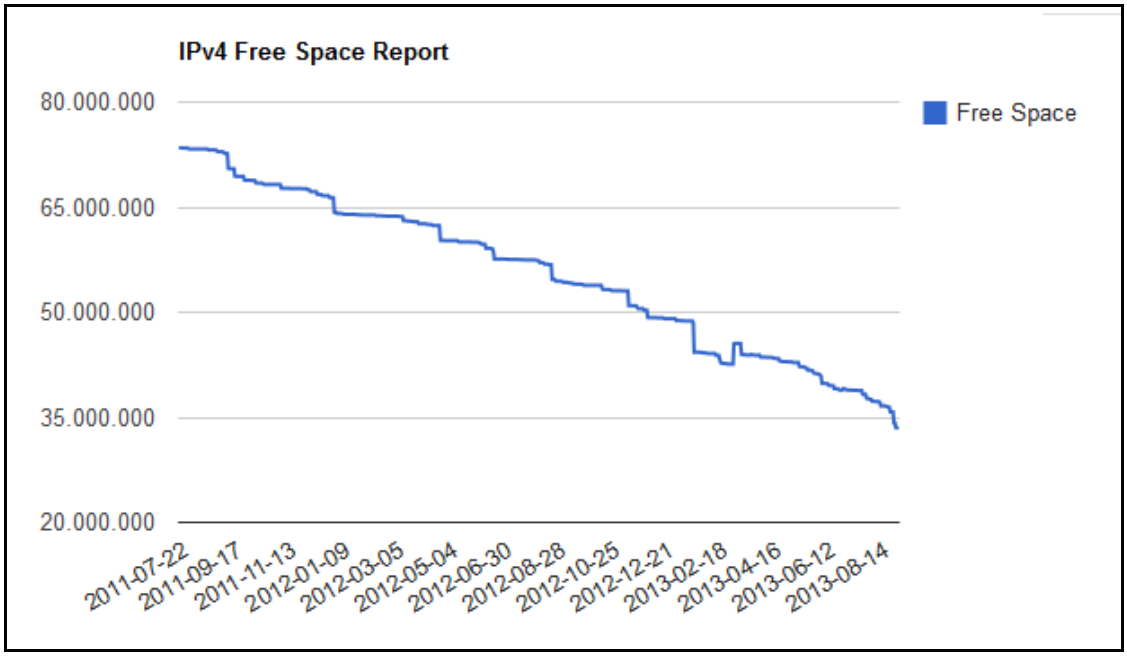

Figura 05 – Quantidade de IPv4 disponível. (Fonte LACNIC)

Por esses motivos, a IETF vê em caráter de urgência a migração do IPv4 para IPv6. Considera o cronograma atrasado, pois a migração deveria ter se iniciado entre os anos de 2009 e 2010. Empresas como Google, Yahoo! e Facebook começaram a migração em meados de 2010.

4. ESTRATÉGIA DE MIGRAÇÃO

Para que o IPv6 possa trabalhar melhor, todos os computadores da rede devem migrar para o novo protocolo. Porém, como isso não é possível instantaneamente, os engenheiros e administradores de redes têm trabalhado no intuito de permitir a coexistência dos dois protocolos. A estratégia para migração dos protocolos tem que ser feita de forma cautelosa para que o impacto produzido não seja sentido pelos usuários, a fim de se manter a qualidade do serviço.

Para isso, a IETF conta com o grupo de trabalho *IPv6 Operations,* cuja a finalidade foi, desenvolver diretrizes para a operação de Internet compartilhada IPv4/IPv6. As técnicas de mecanismos de transição, que permitem a interoperabilidade entre os protocolos, estão divididas em duas categorias:

1- RFC 1933, onde são definidos os mecanismos de transição de Pilha dupla e tunelamento [Gilligan & Nordmark, 1996].
2- RFC 2766, com as definições dos mecanismos de tradução [Tsirtsis, 2000].

As duas técnicas permitem a coexistência dos dois protocolos. Porém, na RCF 2766 a infraestrutura da rede pode conter as seguintes características físicas:

- Nó IPv4: Suporta apenas comunicação com IPv4; a maioria dos nós de redes ainda tem essa característica. O IPv4 *only node*.
- Nó IPv6: Suporta comunicação com IPv6. O IPv6 *only node*.
- Nó IPv4/IPv6: Nó que tem suporte aos dois tipos de protocolo, fazendo assim a comunição sem necessidade de nenhuma técnica de transição.

4.1 Técnica de Pilha Dupla

A técnica de Pilha dupla permite a comunicação de ambos os protocolos simultaneamente. Os dispositivos de rede que têm habilitada a Pilha dupla terão dois endereços de rede, um IPv4 e

outro IPv6, permitindo, assim que o datagrama seja processado conforme a versão do protocolo. A Figura 06 mostra como os datagramas IPv4 e IPv6 são transmitidos através da Pilha dupla:

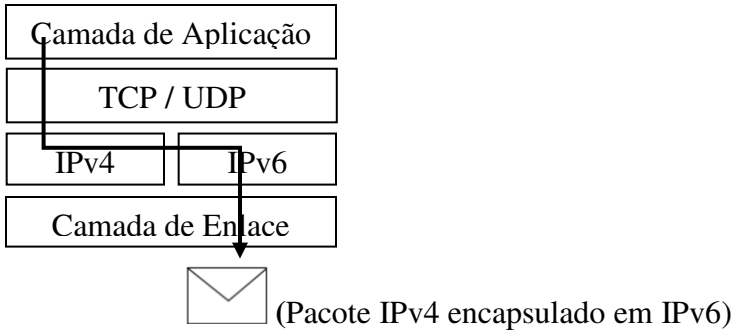

Figura 06 – Exemplo 01 de Pilha dupla.

> "Pilha dupla habilitada será aplicada para o *Tunnel End Point* (TEP) nos mecanismos de interconexão. Nós de Pilha dupla podem suportar Túnel Automático, Túnel Configurado, ou ambos. Existem três instâncias de assistência a túnel em um *host* IPv4/IPv6, assim como rodando apenas o Túnel Automático, rodando apenas o Túnel Configurado, e rodando ambos mecanismos de tunelamento." [Mun & Lee, 2005].

Os roteadores e demais nós que tenham por função permitir o tráfego, ainda que seja apenas ligar os segmentos da rede, e que possuam a opção de Pilha dupla em sua configuração, poderão operar de três formas:

- Pilha IPv4 habilitada e pilha IPv6 desabilitada.
- Pilha IPv6 habilitada e pilha IPv4 desabilitada.
- Ambas as pilhas habilitadas.

Tais configurações podem mudar conforme a topologia, a tecnologia dos dispositivos que compõem a rede, ou, ainda, por alguma questão estratégica e/ou administrativa.

4.1.1 Pilha Dupla no Sistema Operacional Windows XP

No sistema operacional Windows XP *Service Pack* 2, o IPv6 não é nativo. Para isso é necessário instalá-lo; o comando "ipconfig" retorna o endereço IPv4, IPv6 e a técnica de transição que o sistema operacional utiliza, como apresentado na Figura 07:

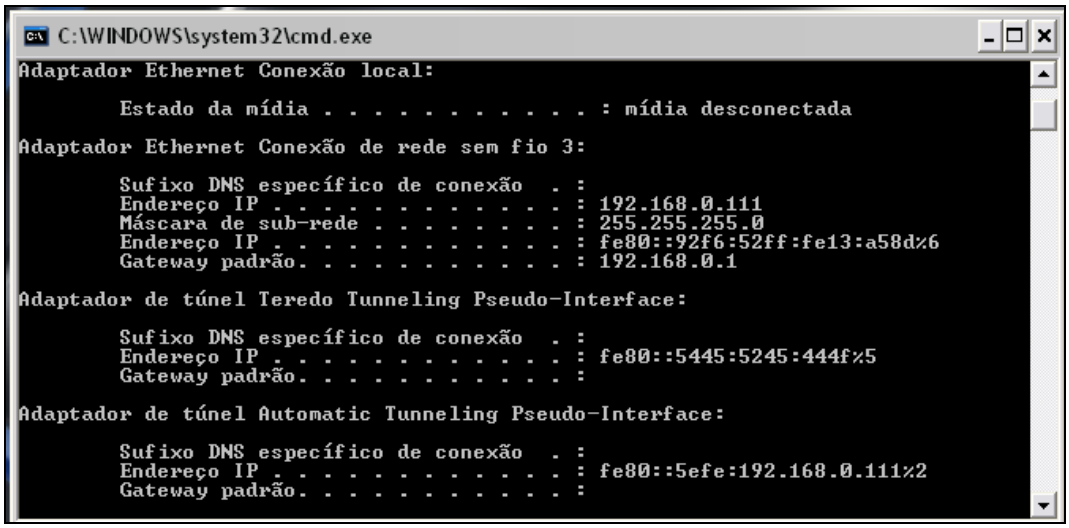

Figura 07 – Configuração IPv6, Windows XP.

O DHCP (para a rede sem fio) atribuiu o Endereço *IPv4: 192.168.0.111* e *IPv6: fe80::92f6:52ff:fe13:a58d%6.* A técnica adotada foi o *túnel Teredo* (mais detalhes no capítulo 4.2.3).

Para testar se o protocolo IPv6 está habilitado, nos sistemas operacionais, foi utilizado o comando *ping* para IPv6, o "ping6". Tal comando é definido como: ping –n 5 ::1.

O endereço da interface de *loopback* para IPv6 foi definido "0:0:0:0:0:0:0:1", que abreviado é escrito como "::1", possibilitando testar o funcionamento correto do IPv6, como mostrado na Figura 08:

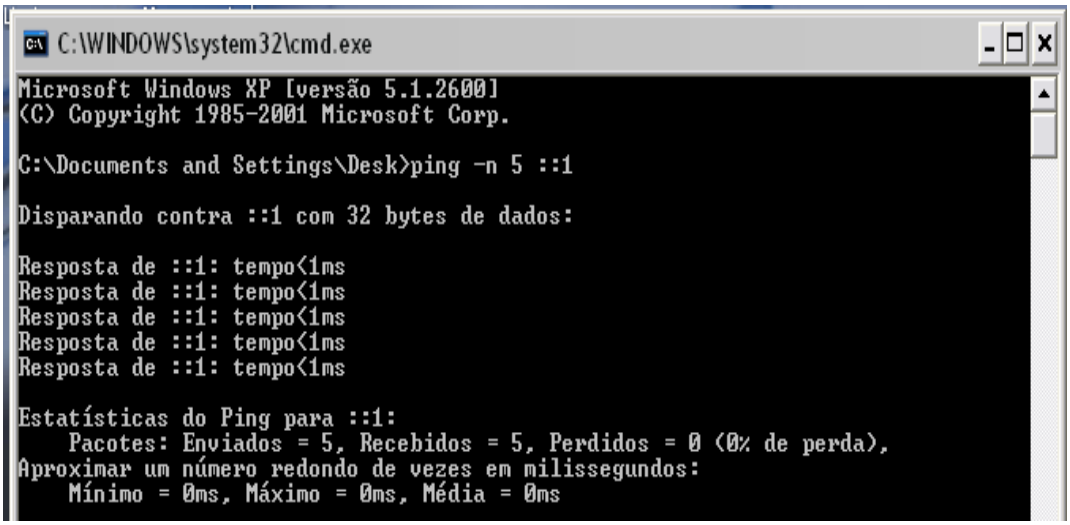

Figura 08 – Teste IPv6, Windows XP.

No teste mostrado na Figura 08 demonstra o funcionamento correto no Windows XP.

4.1.2 Pilha Dupla no Sistema Operacional Windows 7

Ao contrário das versões anteriores, o Windows 7 tem suporte ao IPv6, "com novas melhorias: o IP-HTTPS (IP *over Security* HTTP), que permite que os computadores atravessem redes privadas dentro de túneis HTTPS, com segurança dos dados" [*Microsoft Developer Network*]. Nessa Pilha dupla, a compatibilidade a IPseg, DHCPv6, o identificador de interface aleatório e os demais suportes demonstram que a versão mais recente da Microsoft possui nativamente mais recursos. A Figura 09 mostra as configurações do IPv6:

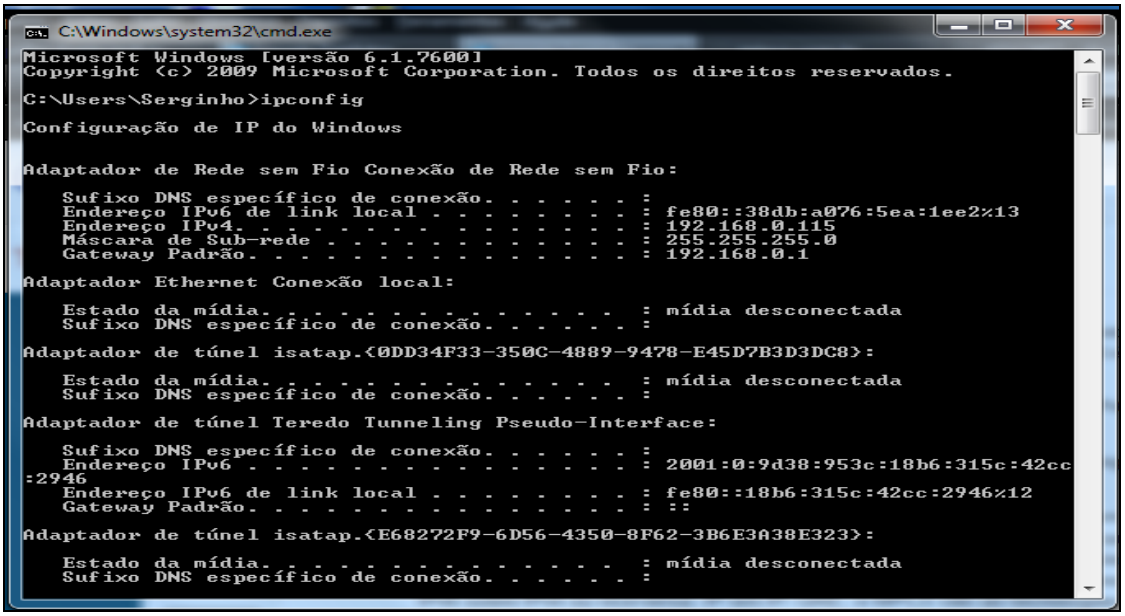

Figura 09 – Configuração IPv6, Windows 7.

Na figura anterior o IPv4 atribuído foi 192.168.0.115, o endereço IPv6: fe00::30db:a076:5ea:1ee2%13.

O teste de funcionamento do IPv6 no *Windows 7,* é mostrado a seguir:

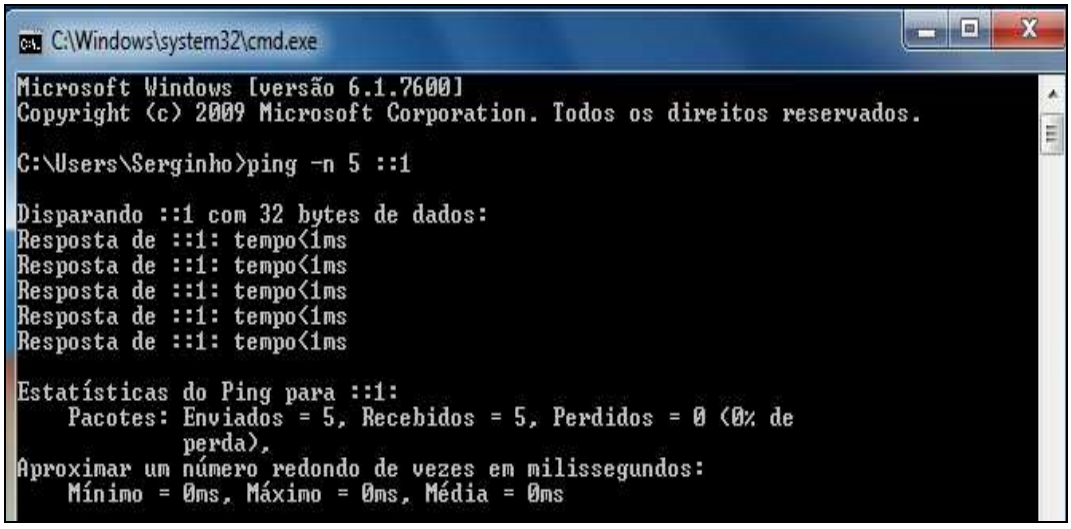

Figura 10 – Teste IPv6, Windows 7.

4.1.3 Pilha Dupla no Sistema Operacional Linux (Ubuntu)

O sistema operacional Ubuntu, dá suporte ao protocolo IPv6 a partir da versão 2.4.x do seu Kernel. O comando “ifconfig” informa as configurações no Linux, como mostrado na Figura 11:

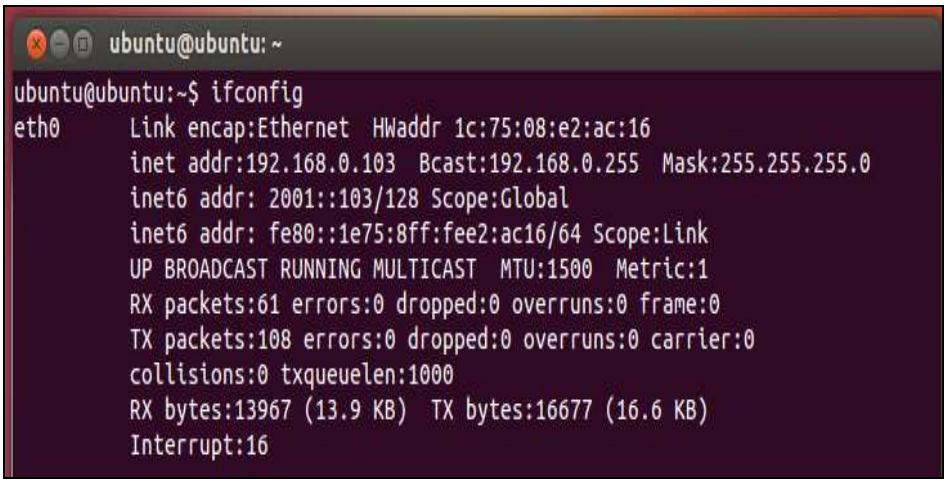

Figura 11 – Configuração Ubuntu.

Nesse sistema operacional, foi atribuído em IPv4 o endereço 192.168.0.103. Para o endereço IPv6, fe80::1e75:8ff:fee2:ac16/64. Conforme observado na Figura 11.

O teste de funcionamento do IPv6 no Ubuntu, é mostrado na Figura 12:

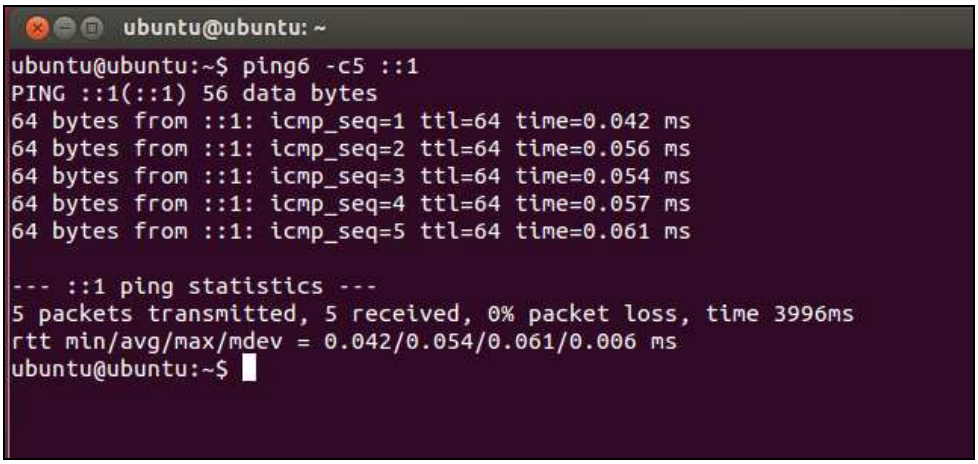

Figura 12 – Teste IPv6, Ubuntu.

O funcionamento a 100% do IPv6 é apresentado no Ubuntu.

4.2 Tunelamento (*Tunneling*)

A RFC 2983 estabelece as regras para a técnica de tunelamento, que dizem: “Tunelamento fornece uma maneira de utilizar uma infraestrutura IPv4 existente para encaminhar pacotes IPv6”. Esse tipo de técnica permite que pacotes IPv6 se comuniquem em uma rede IPv4. A RFC desta técnica estabelece três tipos de comunicação:

- Roteador-a-Roteador: Pacotes oriundos de rede IPv6 atravessam redes IPv4 enxergando-as como túneis. O pacote é encapsulado no início de sua transmissão, dentro de um pacote IPv4, posteriormente tunelado, chegando finalmente ao seu destino e sendo desencapsulado, conforme mostrado na Figura 13:

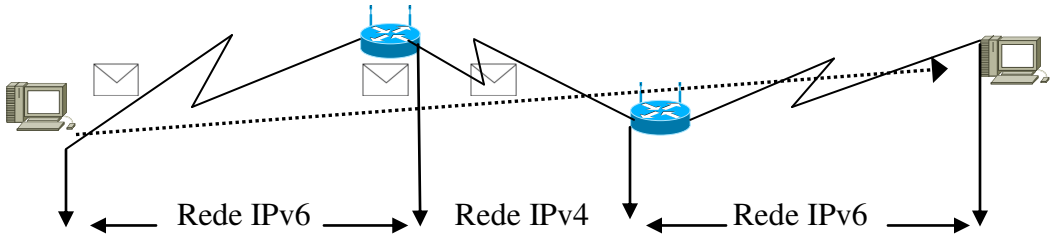

Figura 13 – Túnelamento entre Roteadores.

- Roteador-a-*Host*: Um computador estando numa rede IPv4 envia um pacote a um computador situado em uma rede IPv6. Esse pacote atravessa um roteador com suporte à Pilha dupla e chega ao destino. Para isso, é necessário um túnel entre o roteador e o computador destino. Como mostrado na Figura 14:

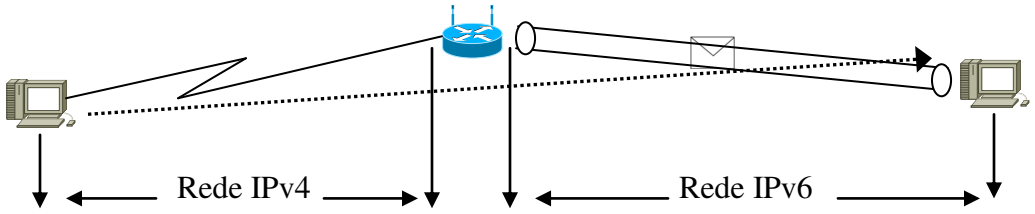

Figura 14 – Tunelamento entre roteadores e Computadores.

- *Host-a-Host*: Computadores com Pilha dupla se comunicam em uma rede IPv4, para isso, o tunelamento ocorre entre os dois computadores, conforme mostrado a seguir:

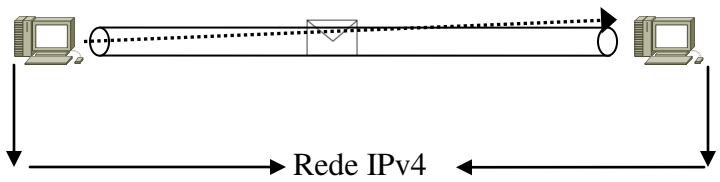

Figura 15 – Túnelamento entre Computadores.

Nas figuras anteriores, o pacote IPv6 puro, para ser transmitido, é colocado dentro do pacote IPv4. Em seguida, é colocado o endereço do destinatário no cabeçalho do pacote; os túneis criados entre os roteadores encaminham o pacote independentemente da versão do protocolo IP. O roteador receptor recebe o pacotes IPv4, extrai do seu interior o pacote IPv6 e em seguida envia o pacote IPv6 para o computador destino. A técnica de tunelamento é dividida em:

- **Tunelamento manual (Configurado):** "Pacotes IPv6 são encapsulados em IPv4 para serem transportados sobre uma infraestrutura IPv4. Esses túneis são ponto-a-ponto que necessitam ser configurados manualmente" [Hagen, 2002].
- **Tunelamento automático:** Túneis automáticos têm a capacidade de permitir a comunicação de pacotes, a passagem de pacotes IPv6 em uma estrutura de rede IPv4, em enlaces entre roteador-a-computador e computador-a-computador. Como nesse tipo de mecanismo são utilizados endereços privados, o túnel automático funciona apenas em tunelamento IPv6 sobre IPv4 (*IPv6 over IPv4*) [Mun & Lee, 2005].

A IETF adotou, por meio das RFCs, diversas técnicas de tunelamento, algumas já em desuso. As técnicas atualmente mais utilizadas em redes que requerem interoperabilidade são:

- Túnel *Broker*
- 6to4
- Teredo
- ISATAP

4.2.1 Túnel *Broker*

As definições desse tipo de mecanismo estão na RFC 3035. Nesse tipo de túnel, o pacote IPv6 é encapsulado dentro do pacote IPv4 para ser roteado através do túnel. Essa técnica é utilizada em sites IPv4/IPv6 ou em computadores que estejam em uma rede IPv4 e necessitem de interoperabilidade em seus acessos. Esse tipo de túnel é representado na Figura 16:

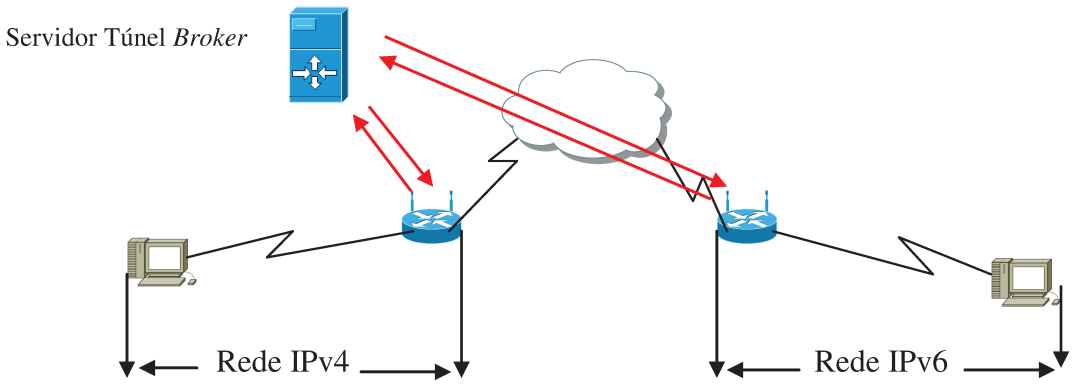

Figura 16 – Esquema Túnel *Broker*.

Essa técnica permite que uma rede IPv4 pura, com provedor de acesso sem suporte a IPv6, consiga alcançar redes IPv6. Para isso, é necessário se cadastrar em um provedor de *Tunnel Broker* como exemplo, www.sixxs.net. Para escolher o tipo de túnel:

- **6in4-static:** No caso de possuir um endereço IPv4 dedicado.
- **6in4-heartbeat:** Esta técnica é usada quando o provedor fornece o endereço por DHCP, ou possui o NAT configurado. É preciso ter a possibilidade de configurar o IP local, na DMZ (*DeMilitarized Zone*) do roteador, para que os pacotes roteados encontrem o IPv4 fornecido pelo provedor da rede.
- **AYIYA:** Esse túnel é utilizado quando o NAT está habilitado na rede e não há possibilidade de configuração de DMZ no roteador [Martinez, 2011].

4.2.2 ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*)

Essa técnica é definida pelas RFCs 5214 e 4213. O mecanismo utiliza o endereço atribuído pelo DHCPv4 aos computadores, ou, ainda, o endereço do roteador de borda, como parte do endereçamento, possibilitando que um nó ISATAP determine a entrada e a saída do túnel IPv6. Conforme mostrado na Figura 17:

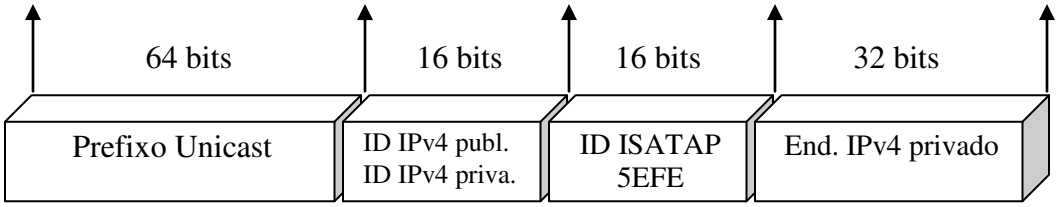

Figura 17 – Estrutura do pacote ISATAP.

Fonte: www.teleco.com.br

Quando a comunicação ocorre entre dois computadores de uma mesma rede, não se necessita de um roteador ISATAP, pois os pacotes são encapsulados e desencapsulados nos próprios computadores. Tais pacotes são estruturados como:

- **Prefixo Unicast:** Enlace local (fe80::/64), ou fornecido pela operadora.
- **ID IPv4 público ou privado:** Nesse local é definido o tipo de IP; dependendo da faixa de IP que é utilizada pode ser diferenciado por público ou privado.
- **ID ISATAP:** Este campo tem valor fixo, 5EFE (em hexadecimal).
- **Endereço IPv4:** Formato normalmente utilizado, como por exemplo, 192.168.0.1.

4.2.3 Teredo

O desenvolvimento desse mecanismo, definido pela RFC 4338, permite que computadores clientes, alocados em uma rede IPv4 e localizados em sua infraestrutura atrás do NAT, possam se comunicar com redes IPv6. A técnica de transição Teredo envia os pacotes pelo tunelamento com

pacotes encapsulados UDP, assim, possibilitando atravessar o NAT instalado no nó da rede. Tais pacotes são encapsulados no computador cliente e enviados para um servidor Teredo, com o servidor da rede pré-configurado com o endereço Teredo. A função desse servidor é prover o endereço IPv6 para os computadores clientes. A Figura 18 exemplifica o Teredo habilitado em um sistema operacional.

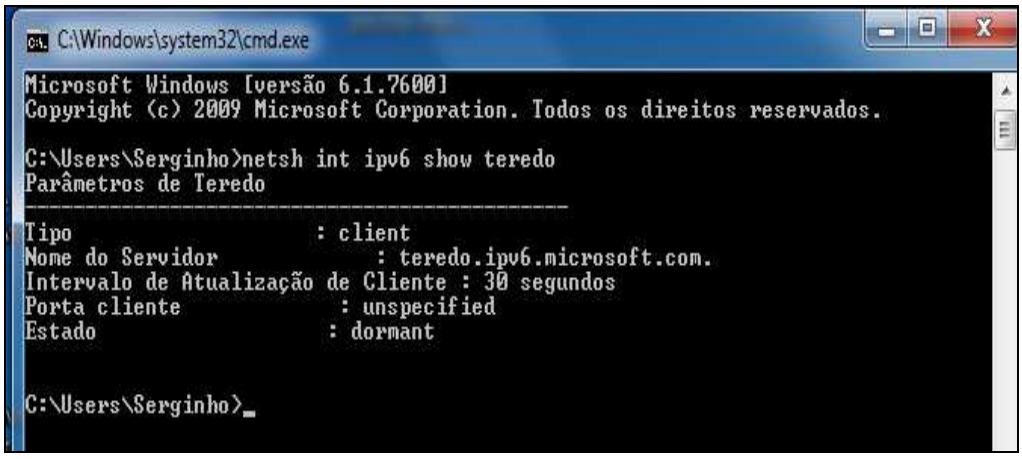

Figura 18 – Teredo no windows 7

O mecanismo Teredo é divido em três componentes:

- **Servidor Teredo:** Permite conexão entre computadores em redes IPv4 com redes IPv6.
- **Retransmissor Teredo:** Responsável por criar enlaces entre redes IPv4/IPv6, permitindo um enlace para um servidor Teredo, encaminhando o pacote encapsulado.
- **Cliente Teredo:** Responsável por encapsular o pacote e enviar para o servidor Teredo, possibilitando o alcance a redes IPv6.

O formato do endereço para uma comunicação usando o mecanismo de transição Teredo é definido pela RFC 4380, conforme mostrado na Figura 19:

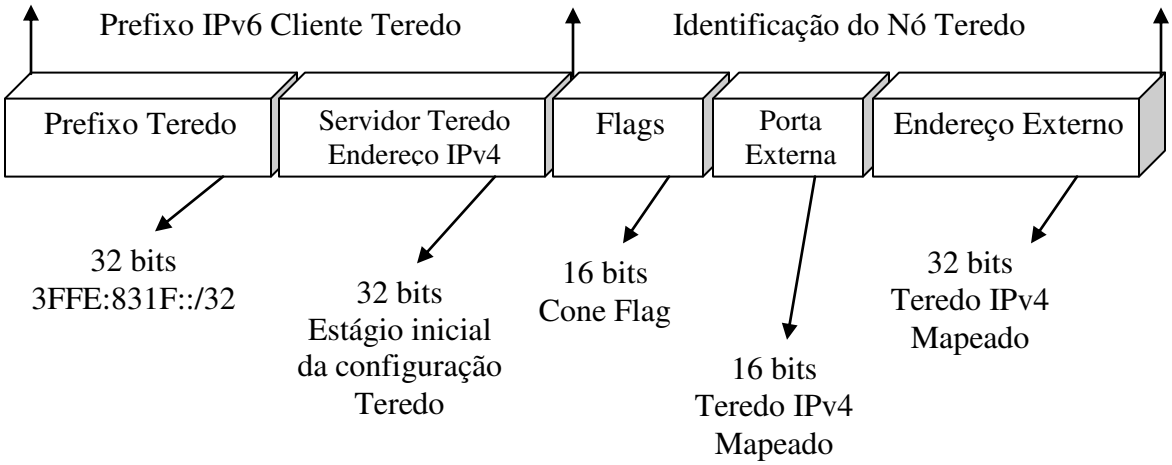

Figura 19 – Formato do Endereço Teredo

Fonte: www.teleco.com.br

4.2.4 6to4

A técnica de 6to4 é uma das primeiras técnicas adotadas que permitiram a transição IPv4/IPv6. O 6to4 é descrito na RFC 3056. Essa técnica serviu de inspiração na criação da técnica 6rd.

O seu mecanismo é utilizado para Internet, ou seja, entre roteadores. Permite que pacotes IPv6 sejam transmitidos através de uma rede IPv4. Também sendo possível que redes IPv6 isoladas consigam se comunicar roteador-a-roteador por túnel automático. No envio dos pacotes, o IPv6 é encapsulado com cabeçalho IPv4. As definições dessa técnica (RFC 3056) seguem os seguintes termos:

- Roteadores 6to4: devem encaminhar ambos os endereços dos dispositivos clientes.
- Dispositivos Clientes: devem estar configurados, pelo menos, com o endereço IPv4.

O Cenário Experimental III – Rede Pilha dupla, possui um tunelamento entre os roteadores 6to4. Foi observado que o roteador, que tem suporte a 6to4 na extremidade da Rede IPv4, tem conectividade quando usados ambos os protocolos para se comunicar. Nos dispositivos clientes, foi observado que os endereços IPv6 obtidos via 6to4, ou de *link-local,* respondem da mesma forma à outra rede.

5. MATERIAIS E MÉTODOS

As seções apresentadas neste capitulo descrevem os cenários experimentais, as configurações e funções dos dispositivos que compõem as redes.

5.1 Topologia dos Experimentos

Procurou-se representar os cenários experimentais propostos por meio das topologias no formato que mais comumente são utilizadas por administradores de redes. “A topologia de uma rede é a apresentação geométrica do relacionamento entre todos os *links* e dispositivos conectados uns aos outros (usualmente os nós)” [Forouzan, 2006].

O Servidor é o dispositivo responsável pela coleta dos dados. O software foi instalado como “modo servidor”, sem a habilitação da função de DNS (*Domain Name System* – Sistema de Nomes de Domínio) e DHCP (*Dynamic Host Configuration Protocol* – Protocolo de Configuração Dinâmica de Endereços de Rede). Tais funções são exercidas pelo Roteador 01 e 02.

A Tabela 01 demonstra o hardware dos dispositivos utilizados nas topologias representadas nas Figuras 20 e 21:

Tabela 01 – Descrição do Hardware dos Experimentos.

NOME	***DESCRIÇÃO***
ROTEADOR 01	TP-link – TL-WDR 4300 (N750)
ROTEADOR 02	Linksys Wi-fi Router E2500
SERVIDOR	PCCHIPS A33G – AMD Semprom; 1,5 GB.
CLIENTE 01	Acer Aspire 5750 – Intel i3 2310M; 2GB.
CLIENTE 02	Gigabyte GA-81865GME-775 – Intel Dual Core; 1,5GB.
CLIENTE 03	SIM 2012 – Intel Celeron; 1,5GB.

As Figuras 20 e 21 representam a topologia utilizada nos cenários experimentais:

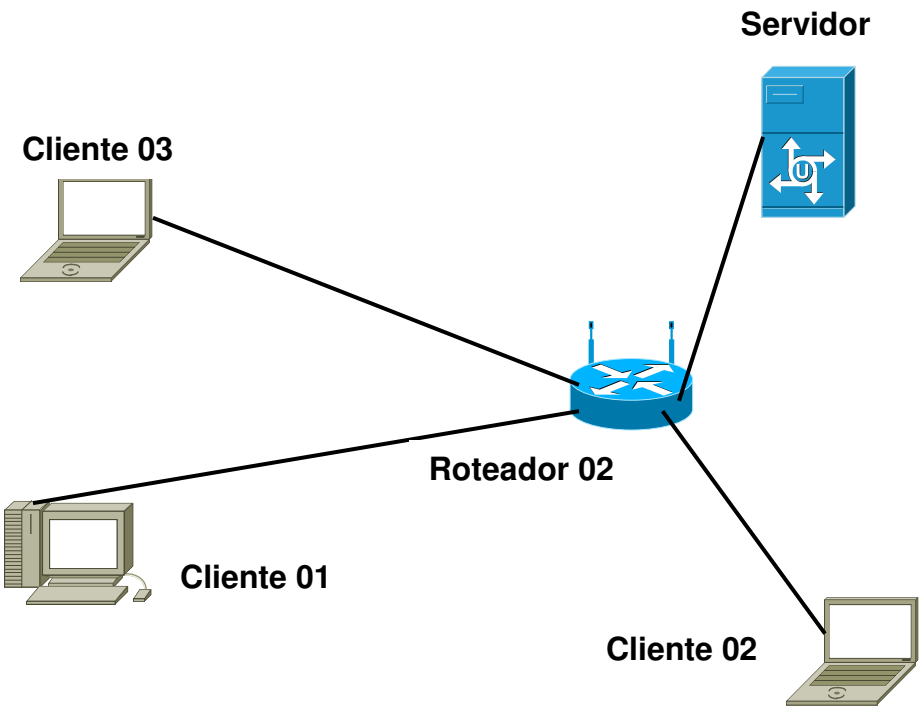

Figura 20 – Topologia da Rede SOHO 01 (Cenário I e II).

A topologia proposta na Figura 20 é utilizada nos Cenários I – Rede IPv4 Pura e II – Rede IPv6 Pura.

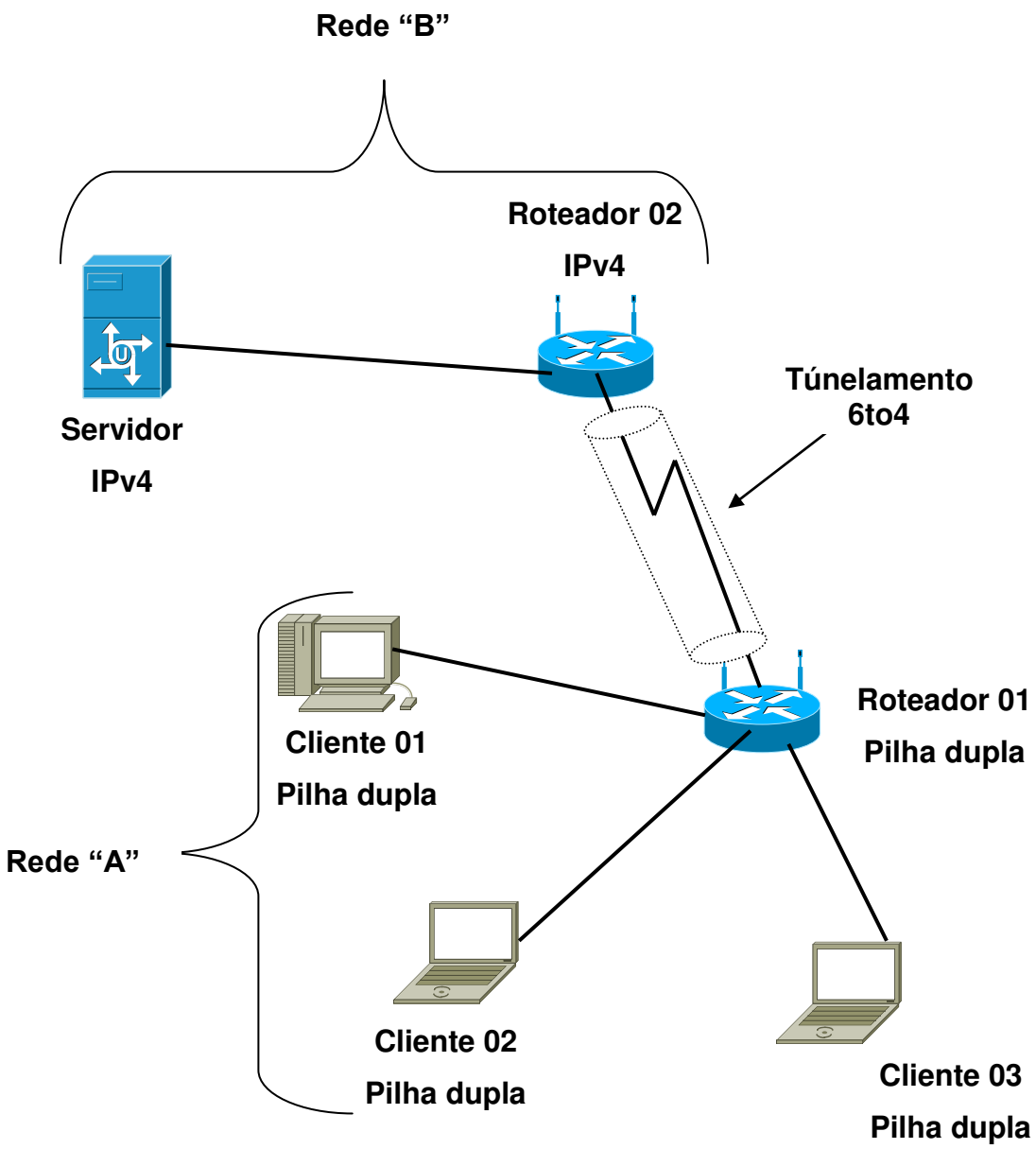

Figura 21 – Topologia da Rede SOHO 02 (Cenário III).

A topologia representada na Figura 21 é útilizada no Cenário III – Rede Pilha dupla.

5.2 Cenários Experimentais

As configurações dos dispositivos são modificadas conforme os experimentos descritos nos Cenários I, II e III:

- **Cenário I - Rede IPv4 Pura:**

A topologia desse cenário está representada pela Figura 20, nomeada como "Rede IPv4 Pura".

O Roteador 02 possui suporte para IPv4. Assim, a função DHCPv4 ficou habilitada, porém, todas as funções de suporte a IPv6 foram desabilitadas no roteador.

O Servidor tem o suporte a IPv6 desinstalado. Os dispositivos Clientes tem o suporte IPv6 desinstalados dos sistemas operacionais.

Após a garantia de que todos os dispositivos da rede tenham suporte apenas para IPv4, são efetuadas as medições de latência, *jitter*, vazão e perda de pacotes. As características apresentadas acima são as mais comumente encontradas nas redes SOHO.

- **Cenário II - Rede IPv6 Pura:**

Nesse cenário, também é utilizada a topologia representada na Figura 20.

O Roteador 02 tem todas as funções IPv4 desabilitadas. Todos os dispositivos foram conectados ao Roteador 02, ficando este responsável por distribuir endereço através do DHCPv6.

No Servidor, é instalado o suporte para IPv6 e são desabilitadas as funções IPv4. Nos dispositivos Clientes, é instalado o suporte para IPv6 e são desabilitadas as funções IPv4.

Este cenário permitiu conhecer o comportamento de latência, vazão, *jitter* e perda de pacotes em uma rede em que todos os dispositivos são configurados com IPv6. Caracterizando, assim, uma Rede IPv6 Pura.

- **Cenário III - Rede com Pilha dupla:**

Neste cenário, a topologia está representada na Figura 21.

O Roteador 01 encontra-se na Rede "A" as funções DHCPv4 e DHCPv6 ficam habilitadas, podendo, assim, rotear mensagens nos dois protocolos. O Roteador 02 encontra-se na Rede "B",

a qual possui apenas a função DHCPv4 e, portanto, atribui aos dispositivos nele conectados endereço do tipo IPv4.

Para que os dispositivos que estão em redes distintas pudessem se comunicar, foi feito o tunelamento entre os roteadores. O tunelamento permitido é o 6to4.

No Servidor, a Pilha dupla fica habilitada. Como o Roteador 02 não atribui IPv6, é utilizado o endereço de Link Local IPv6, atribuído automaticamente.

Nos dispositivos clientes, a Pilha dupla é carregada, recebendo endereço IPv4 e IPv6 pelo Roteador 01.

Os cenários experimentais I, II e III representam uma rede SOHO (*Small Office Home Office*). As topologias física e lógica, em que os roteadores, servidores e computadores assumem possíveis funções dentro da rede, estão representadas conforme descreve o Quadro 02:

Quadro 02 – Configurações dos dispositivos nos cenários.

Cenário / Dispositivos	**Cenário I Rede IPv4 Pura**	**Cenário II Rede IPv6 Pura**	**Cenário III Rede Pilha dupla**
Roteador 01	DHCPv4	DCHPv6	DHCPv4 / DHCPv6
Roteador 02	Não utilizado	Não utilizado	DHCPv4
Servidor	IPv4	IPv6	Pilha dupla
Cliente 01	IPv4	IPv6	Pilha dupla
Cliente 02	IPv4	IPv6	Pilha dupla
Cliente 03	IPv4	IPv6	Pilha dupla

6. TESTES DE DESEMPENHO E MÉTRICA

Os testes de desempenho propostos nas redes SOHO foram efetuados pelo *software* Iperf, chamado Jperf em Linux (mais informações it.engineering.illinois.edu). O programa efetua análise de rede e desempenho, por meio de suas ferramentas disponíveis e configuradas, para enviar pacotes de tamanhos variáveis conforme o experimento a ser realizado.

No Quadro 03, estão descritos os comandos utilizados nos experimentos e suas respectivas funções:

Quadro 03 – Comandos do Software Iperf.

COMANDO	FUNÇÃO
-b	Define a banda a ser utilizada.
-c	Executa o Iperf em modo cliente.
-f	Define a unidade do relatório de saída.
-i	Define o relatório de tempo de registro de saída.
M	Exibe, na saída, o tamanho máximo do MTU.
-p	Define a porta a ser utilizada.
-s	Executa o Iperf em modo servidor.
-t	Define o tempo de duração dos testes.
-u	Utiliza o protocolo UDP.
-P	Define o número de conexões paralelas.
-S0x02	Define a saída da comunicação com menor custo.
-T	Define o numero de saltos.
-V	Utilizado para conexões IPv6.

Para que seja possível efetuar as medições com o software Iperf, um dos computadores da rede deve ser programado no modo "*Server*", como feito na topologia do experimento no Servidor. Nos demais computadores da rede, o Iperf deve ser executado no modo "*Client*".

O *link* do site mantido pela NLANR/DAST (user.informatik.haw-hamburg.de/~scotty/pub/Rechnernetze/iperf/iperfdocs.html), possui documentação sobre os comandos e suas funções.

Ao término dos testes, o Iperf gera um arquivo ".txt" com os resultados experimentais. Para todos os resultados obtidos neste trabalho, deve-se consultar o DVD anexo.

O software possui também modo gráfico, que permite efetuar análise de desempenho, enquanto os testes estão sendo executados. A Figura 22 mostra um exemplo de gráfico gerado pelo Iperf.

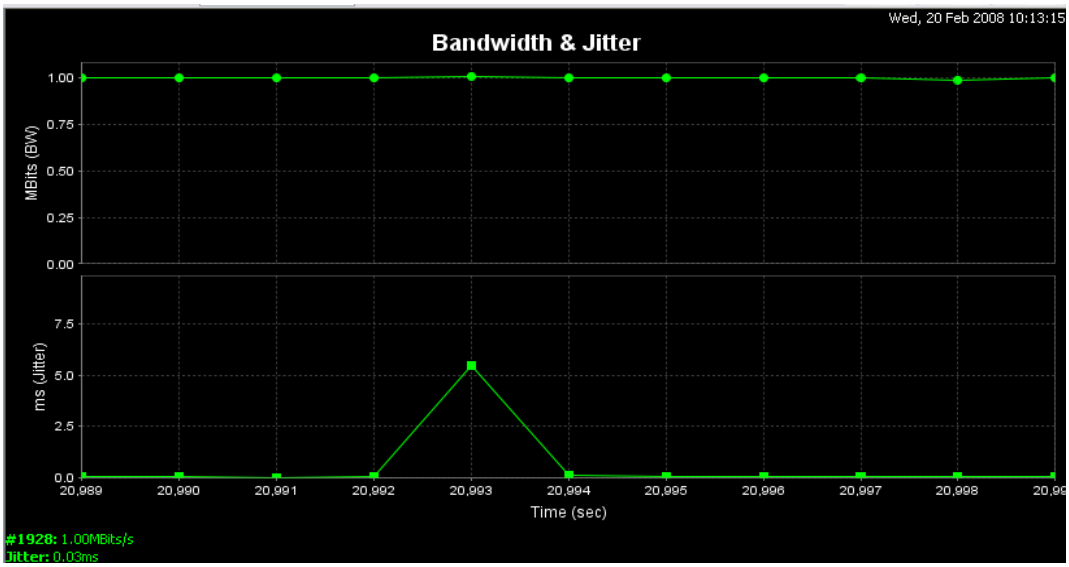

Figura 22 – Exemplo de saída em Modo Gráfico.

6.1 Latência

"Latência é o tempo decorrido após uma operação de envio ser executada e antes que os dados comecem a chegar a seu destino. Ela pode ser medida como o tempo necessário para transferir uma mensagem" [Coulouris, 2005]. Segundo Carissimi [2009] em redes de computadores, latência é o tempo em que o emissor enviou o pacote e o momento em que este

recebe a confirmação do receptor de que o pacote foi recebido. No cálculo da latência é excluído o tempo em que o receptor gasta processando o pacote.

Segundo Filippetti [2008], pode-se expressar latência em redes de computadores como:

Latência = *Tempo de Transmissão* + *Tempo de Propagação*

Sendo,

- Tempo de Transmissão = *Dimensão do pacote (bits) / Velocidade da Transmissão (bps).*
- Tempo de Propagação = *Dimensão do Canal (Km) / Velocidade de Propagação (Km/s).*

Segundo Kurose [2006], há dois outros tipos de atrasos que podem provocar latência: o tempo de processamento e o tempo de enfileiramento. No entanto, esses dois tempos só podem ser aferidos em uma rede com utilização de tráfego significativamente elevado.

Nos experimentos, utiliza-se o comando *ping*. Os comandos são enviados dos Clientes ao Servidor, com *ping* de 750 bytes. Foram enviadas por volta de 21.000 mensagens em cada cenário experimental, em média 7000 mensagens para cada sistema operacional.

No Cenário I – Rede IPv4 Pura, foram utilizados os seguintes comandos:

- **Windows XP, 7:** ping 192.168.0.100 –s 750 –c 7000
- **Ubuntu 11.10:** ping 192.168.0.100 –n 750 –l 7000

No Cenário II – Rede IPv6 Pura, foram utilizados os seguintes comandos:

- **Windows XP, 7:** ping -6 fe80::216:ecff:fec1:8476 –s 750 –c 7000
- **Ubuntu 11.10:** ping6 fe80::216:ecff:fec1:8476 –n 750 –l 7000

No Cenário III – Rede Pilha dupla, as duas versões do comando respondem. Foram efetuadas por volta de 15.000 medições IPv4 e IPv6, na rede Pilha dupla. Foram selecionadas as 21.000 medições que apresentaram o menor custo.

- **Windows XP, 7:** ping 192.168.0.100 –s 750 –c 3500
- **Windows XP, 7:** ping -6 fe80::216:ecff:fec1:8476 –s 750 –c 3500
- **Ubuntu 11.10:** ping 192.168.0.100 –n 750 –l 3500
- **Ubuntu 11.10:** ping6 fe80::216:ecff:fec1:8476 –n 750 –l 3500

6.2 Vazão (*Throughput*)

A quantidade de dados transferidos entre redes ou computadores, ou mesmo a quantidade de dados processados em determinado tempo, normalmente é expressa por *bits per second* (*bps*). "Ou seja, se considerarmos o ponto como sendo um plano que secciona o meio, o *throughput* é o número de bits que atravessa esse plano" [Forouzan, 2006]. Os fatores que interferem no *throughput* são:

- Topologia de rede;
- Número de usuários;
- Sistema operacional;
- Taxa das interfaces de rede.

Resumidamente a vazão, poderia ser descrita como a velocidade em que os dados realmente trafegam pela rede. Essa taxa de transferência pode ser menor do que a *largura de banda,* devido às perdas e atrasos.

Para efetuar as medições nos cenários experimentais, é necessário programar o software Jperf:

- Servidor: coloca-se o número de IP, variando conforme o dispositivo testado. O número da porta é 5001, padrão do programa. A saída é configurada em Mbits/seg. O *TCP window size* é colocado em 8 Kbytes (Padrão).
- Cliente: coloca-se o número IP do Servidor (a versão utilizada depende do cenário). O número da porta é 5001, padrão do programa. Foram gerados pacotes de tamanho médio de 10,46 Mbytes, enviados a cada segundo, durante 21000 segundos. O formato de saída foi Mbits.

No Cenário I – Rede IPv4 Pura, foram utilizados os seguintes comandos:

- **Servidor IPv4:** -s –P0 –i1 –p5001 –fm –t 7000
- **Cliente IPv4:** -c 192.168.0.100 –P3 –i1 –p5001 –fm –t7000

No Cenário II – Rede IPv6 Pura, foram utilizados os seguintes comandos:

- **Servidor IPv6:** -s –P0 –i1 –p5001 –V –fm

- **Cliente IPv6:** -c fe80::216:ecff:fec1:8476 –P3 –i1 –p5001 –V –fm –t7000 –T1

No Cenário III – Rede Pilha dupla, foram utilizados os seguintes comandos:

- **Servidor Pilha dupla:** -s –P0 –i1 –p5001 –V –fm
- **Cliente Pilha dupla:** -c fe80::216:ecff:fec1:8476 192.168.0.100 –P3 –i1 –p5001 –V –fm –t7000 –T1 –S0x02

As medições realizadas nos experimentos permitiram conhecer o desempenho de Vazão em redes IPv4 Pura, IPv6 Pura e Pilha dupla. Assim, possibilitando estabelecer um comparativo entre os tipos de redes.

6.3 Perda de Pacotes

Os fatores citados, nos capítulos anteriores, influenciam diretamente neste quesito. Pelo fato de os roteadores não terem a capacidade de armazenamento de pacotes infinita, após o esgotamento, os pacotes são descartados.

À medida que a rede cresce ou a exigência de processamento aumenta devido às aplicações, o nó passa a ter maiores solicitações e, consequentemente, pode ocorrer perda de pacotes.

As configurações do software Jperf, para as medições de perda de pacotes, são feitas conforme descrito a seguir:

- Servidor: coloca-se o número de IP, variando conforme o dispositivo testado. O número porta é 5001, padrão do programa. A saída é configurada em Mbits/seg.
- Cliente: é colocado o número IP do Servidor. Os testes são realizados com 21000 mensagens, sendo enviados, a cada um segundo, com tamanho médio de 0,12 MBytes. O formato de saída é em Mbits.

No Cenário I – Rede IPv4 Pura, foram utilizados os seguintes comandos:

- **Servidor IPv4:** -s –u –P0 –i1 –p5001 -fm
- **Cliente IPv4:** -c 192.168.0.100 –u –P3 –i1 –p5001 –fm –b1.0M –t7000 –T1

No Cenário II – Rede IPv6 Pura, foram utilizados os seguintes comandos:

- **Servidor IPv6:** -s –u –P0 –i1 –p5001 –V -fm
- **Cliente IPv6:** -c fe80::216:ecff:fec1:8476 –u –P3 –i1 –p5001 -V –fm –b1.0M –t7000 –T1

No Cenário III – Rede Pilha dupla, foram utilizados os seguintes comandos:

- **Servidor Pilha dupla:** -s –u –P0 –i1 –p5001 –V -fm
- **Cliente Pilha dupla:** -c fe80::216:ecff:fec1:8476 192.168.0.100 –u –P3 –i1 –p5001 -V –fm –b1.0M –t7000 –T1 –S0x02

Foi analisada a taxa de Perda de pacotes em redes IPv4, IPv6 e Pilha dupla. Normalmente essas medições são representadas pelo percentual de pacotes perdidos, demonstrando maior eficiência do quesito a rede com menor perda de pacotes.

6.4 *Jitter*

A influência do *jitter* é mais sensível para a qualidade de serviço quando se tem a necessidade da garantia na entrega dos pacotes em períodos definidos e a observação do *Jitter* torna-se um parâmetro importante. "*Jitter* pode ser definido como a variação no tempo e na sequência de entrega dos pacotes (Packet-Delay Variation) devido à variação da latência (atrasos) na rede" [Comer, 2004]. O *Jitter* é analisado na periodicidade na transmissão dos pacotes, como também na variação da entrega dos pacotes (na origem e no destino, mas, geralmente é mais significativa sua variação no destino). A Figura 23 é um exemplo de *jitter* em uma rede.

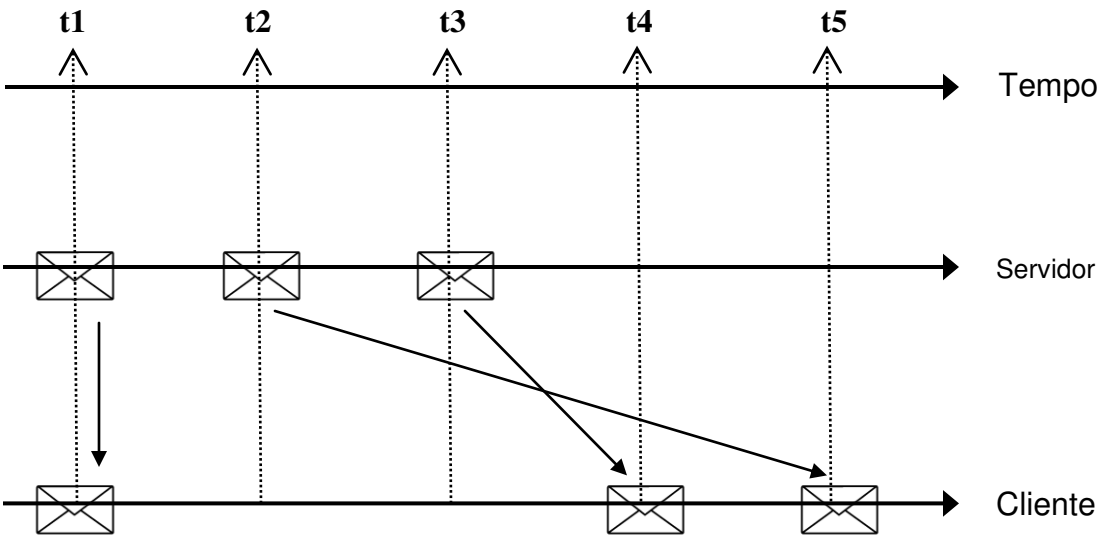

Figura 23 – *Jitter* na entrega de pacotes.

Na Figura 23, o pacote transmitido pelo Servidor, no tempo 1, é recebido no período certo pelo Cliente. O pacote enviado pelo Servidor no Tempo 2 tem sua ordem trocada e chega ao Cliente no Tempo 5, e o pacote enviado pelo Servidor no Tempo 3 tem sua ordem trocada e chega ao Cliente no Tempo 4.

A medição do *jitter,* no software Jperf, é efetuada juntamente com a perda de pacotes. Portanto, as configurações são as mesmas descritas no Capítulo 6.3.

7. RESULTADOS EXPERIMENTAIS

Os resultados dos experimentos permitiram comparar o desempenho de redes com os protocolos de comunicação IPv4, IPv6 e Pilha dupla. As medições de vazão, *jitter*, perda de pacotes e latência foram efetuadas seguindo todas as configurações de dispositivos, frequência e tamanho de pacotes, apresentadas no Capítulo 6.

Os resultados serão apresentados por ordem de cenários experimentais I, II e III:

Cenário I – Rede IPv4 Pura: Para a realização do teste de vazão, foram efetuadas 20.988 repetições, uma por segundo. A taxa de transferência média foi de 11,16 MBytes/seg. A **vazão** média obtida, neste tipo de rede, foi de **91,32 Mbits/seg.**

No teste de latência, foram efetuados 20.998 segundos. O tamanho dos pacotes enviados foi de 758 bytes. A **latência** média na Rede IPv4 foi de **0,355 ms.**

Para os testes de *jitter* na Rede IPv4, foram efetuadas 15.296 repetições com taxa de transferência média de 0,11 MBytes/seg. O ***jitter*** médio dessa rede foi de **0,349 ms.**

Para medições de perda de pacotes foram gerados 437.075 pacotes. A perda registrada foi de **113 pacotes**, que representam **0,026%** dos pacotes perdidos.

Cenário II – Rede IPv6 Pura: Os testes de vazão em Rede IPv6, foram realizados por 20.995 segundos. A taxa de transferência média foi de 10,75 MBytes/segundo. A **vazão** média obtida foi de **87,79 Mbits/seg.**

A medição do teste de latência foi realizada por 20.997 segundos. O tamanho dos pacotes enviados foi de 758 bytes. A média de **latência,** na Rede IPv6, foi de **0,355 ms.**

Para as medições de *jitter*, na Rede IPv6, foram feitas 20.937 repetições, a taxa de transferência média foi de 0,12 MBytes/seg. O ***jitter*** médio foi de **0,259 ms.**

Em medições de perda de pacotes foram gerados 1.780.479 pacotes, não havendo registro de Perda de pacotes.

Cenário III – Rede Pilha dupla: Para a realização do teste de vazão, nesse cenário, foram efetuadas 20.990 repetições, uma por segundo. A taxa de transferência média foi de 10,60 MBytes/seg. A **vazão** média obtida, nesse tipo de rede, foi de **91,06 Mbits/seg.**

O teste de latência foi efetuado por 20.999 segundos. O tamanho dos pacotes enviados foi de 758 bytes. A **latência** média na Rede Pilha dupla foi de **0,637 ms.**

Para os testes de *jitter*, na Rede Pilha dupla, foram efetuadas 20.497 repetições, com taxa de transferência média de 0,12 MBytes/seg. O ***jitter*** médio dessa rede foi de **0,287 ms.**

Para medições de perda de pacotes foram gerados 892.457 pacotes. A perda de pacotes registrada foi de **2 pacotes**, que representam **0,0002%** dos pacotes perdidos.

O Quadro 04 mostra os resultados dos experimentos.

Quadro 04 – Resultados Experimentais

Redes/Métricas	Vazão (Média)	Latência (Média)	Jitter (Média)	Perda de Pacotes (%)
Rede IPv4	91,32 Mbits/seg	0,355 ms	0,349 ms	0,026%
Rede Pilha dupla	91,06 Mbits/seg	0,637 ms	0,287 ms	0,0002%
Rede IPv6	87,79 Mbits/seg	0,355 ms	0,259 ms	0%

7.1 Análise de Desempenho dos Experimentos

A Figura 24 ilustra um comparativo de desempenho de vazão entre as redes. Os cenários experimentais das redes IPv4 e Pilha dupla tiveram desempenho próximos. Porém, na Rede IPv6 houve queda no desempenho.

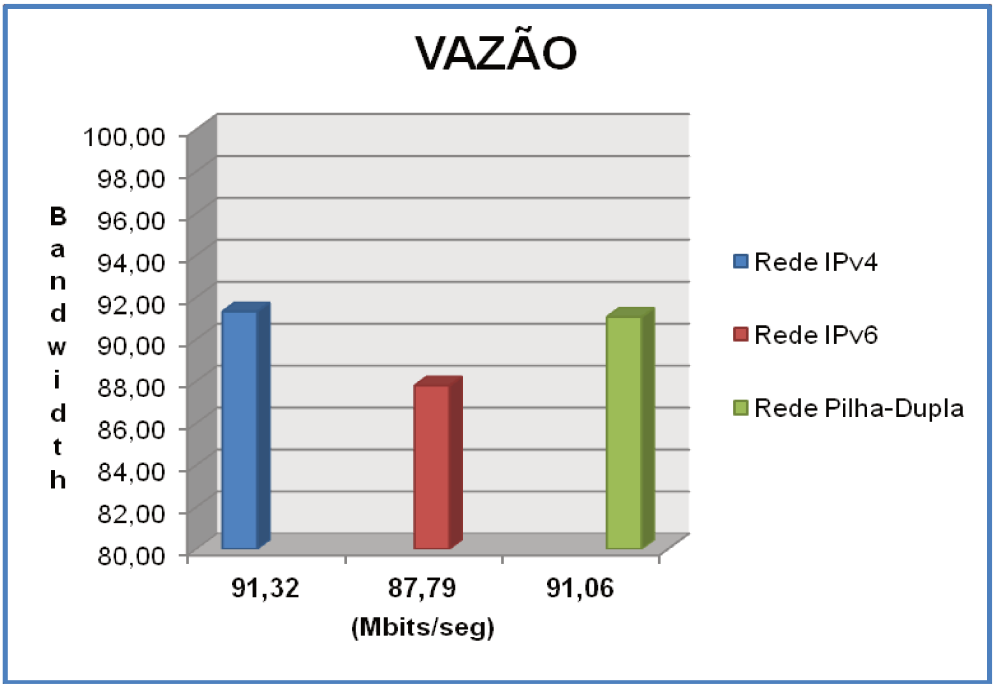

Figura 24 – Comparativo de Vazão entre as Redes

A Rede IPv4, em comparação com a Rede Pilha dupla, teve o desempenho de 0,26 Mbits/seg. superior a esta.

A Rede IPv4, quando comparada à Rede IPv6, teve o desempenho superior em 3,53 Mbits/seg.

Quando compara-se a Rede Pilha dupla com a Rede IPv6, seu desempenho foi de 3,27 Mbits/seg. superior.

Com isso, foi concluido que, no período de interoperabilidade e coexistência, as redes poderão ter uma queda de desempenho em vazão de 0,28 % em relacão as redes IPv4, maioria atualmente.

No momento em que não houver mais a necessidade de usar as técnicas que permitam coexistência, e as redes se tornarem IPv6 Pura, a queda de desempenho será de 3,59 %.

Por fim, quando comparado as redes atuais (IPv4) à Rede IPv6, a queda de desempenho de Vazão foi de 3,86 %.

As análises de desempenho de latência estão representadas na Figura 25.

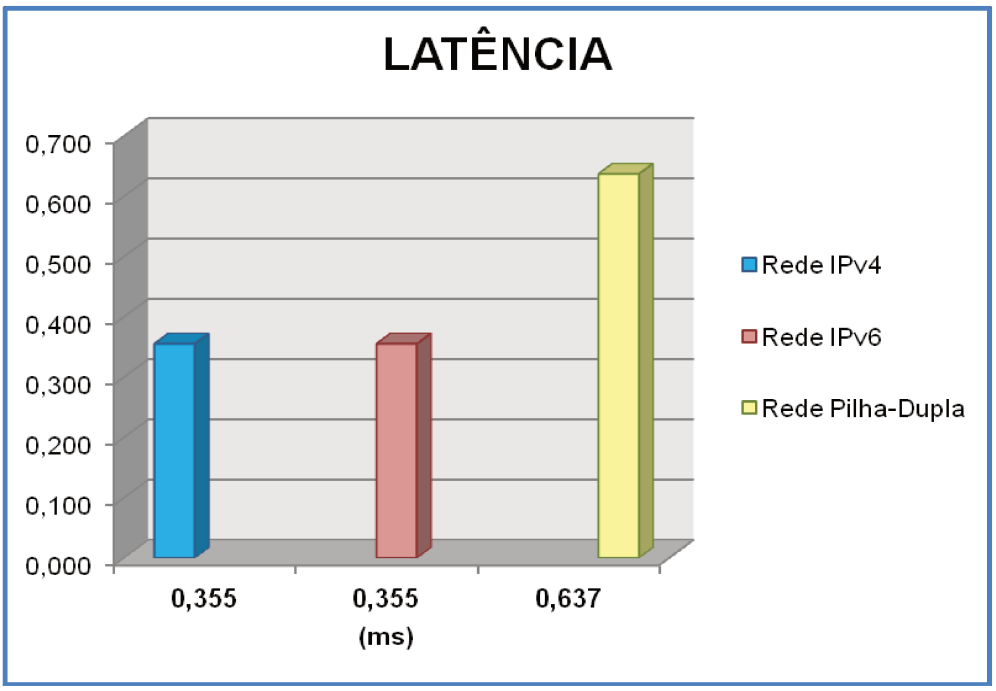

Figura 25 – Comparativo de Latência entre as Redes

As Redes IPv4 e IPv6 tiveram o mesmo desempenho de 0,355 ms.

A Rede IPv4 e IPv6, quando comparadas com a Rede Pilha dupla, tiveram o desempenho superior em 0,282 ms.

Conclui-se que a Rede Pilha dupla teve queda de desempenho em latência de aproximadamente 79,43 % em relacão às redes IPv4 e IPv6. Isto ocorreu nos experimentos devido à necessidade de coexistência e/ou devido a utilizacão de mecanismos de transição.

Os testes realizados para a perda de pacotes apresentou, na rede IPv4, o desempenho menor do que as outras redes conforme a Tabela 02.

Tabela 02 – Comparativo de Perda de pacotes entre as Redes

	GERADOS	PERDIDOS	PORCENTAGEM
Rede IPv4	437075	113	0,0260 %
Rede IPv6	1780479	0	0,0000 %
Rede Pilha dupla	892457	2	0,0002 %

Embora a Rede IPv4 tenha tido uma Perda de pacotes superior as outras redes, todas as redes tiveram perdas menores a 1%, não degradando, de maneira geral, a qualidade de serviço (QoS).

O desempenho nos cenários experimentais, no qual foi medido o *jitter*, demonstra que as Redes IPv6 e Pilha dupla tiveram desempenho próximos. Já na Rede IPv4, houve queda no desempenho, conforme a Figura 26:

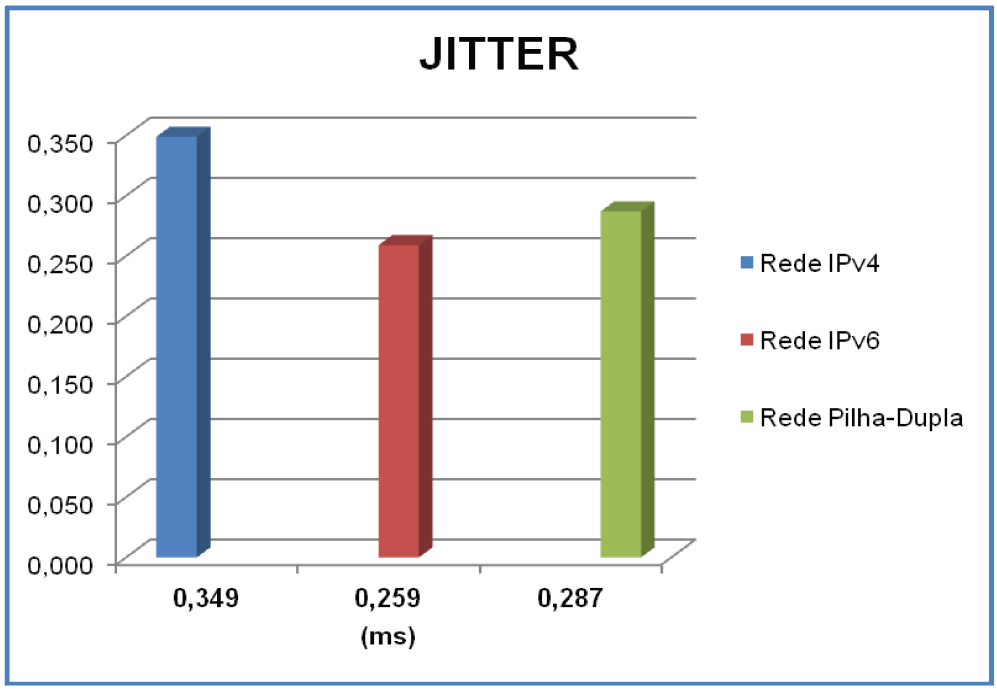

Figura 26 – Comparativo de *Jitter* entre as Redes

A Rede IPv4, em comparação com a Rede Pilha dupla, obteve queda no desempenho de 0,062 ms.

A Rede IPv4, quando comparada com a Rede IPv6, teve o desempenho inferior em 0,090 ms.

Quando comparada a Rede Pilha dupla à Rede IPv6, o desempenho foi de 0,028 Mbits/seg. superior.

A Figura 26 permite efetuar um comparativo entre as redes IPv4 x Pilha dupla, IPv4 x IPv6 e Pilha dupla x IPv6:

Após análise do desempenho entre as redes no quesito *Jitter*, conclui-se que a Rede IPv4 teve um desempenho 17,76 % menor em relação à Rede Pilha dupla. Em relação com a rede IPv6, o desempenho foi 25,78 % menor.

A Rede Pilha dupla obteve um desempenho 9,75 % menor do que a Rede IPv6.

7.2 Discussão dos Experimentos

No momento em que as redes IPv4, entrarem no período de transição e coexistência, em que os protocolos IPv4 e IPv6 necessitarão conviver, as medicões apresentaram queda de desempenho no tráfego elástico (menos prioritário), porém, nas transmissões de tráfego *stream* (mais prioritário), é que o impacto poderá ser mais sensível, gerando maior degradação do serviço. Pois, a caracteristica desse tipo de tráfego não admite atraso.

No futuro, quando não for mais necessario utilizar as tecnicas adotadas no periodo de coexistencia e as redes forem definidas como "IPv6 pura", as medicões demonstram, que a queda no desempenho das redes, poderá ser de maior impacto em transmissões de tráfego elástico (menos prioritário). Nos serviços *stream* (mais prioritário) observou-se melhora no desempenho quando se utiliza o protocolo IPv6.

A fim de se comparar as redes IPv4 (maioria nas redes atuais) com as redes IPv6 (futuro), o desempenho das redes IPv4, em transmissão de tráfego elástico, poderá ser superior quando comparado com a rede IPv6. Na comunicão *stream*, a rede IPv6 mostrou-se mais eficaz que a rede com o protocolo IPv4, podendo proporcionar uma melhora considerável para esses tipos de serviços.

Embora não seja o foco do trabalho analisar a implementação do protocolo IPv6, sua configuração mostrou-se de fácil nos sistemas operacionais, quando não nativos.

Porém, o suporte dos roteadores, mostram-se em fase de aprimoramento. Quando foram necessários criar túneis entre os roteadores, a configuração dos mesmos foi difícil. Isso ocorreu devido às limitações de técnicas de tunelamento nos equipamentos e à falta de opções de equipamentos que possibilitassem a utilização do IPv6 ou, ainda, para a criação de túneis.

8. MODELO DE SIMULAÇÃO DO CENÁRIO HIPOTÉTICO DE REDE

O modelo de simulação tem o objetivo principal de avaliar o impacto dos parâmetros obtidos na rede SOHO em uma rede hipotética com vários serviços *stream* (mais prioritários) e um serviço elástico (o *Data files*, menos prioritário). A suposição do modelo em atribuir prioridade aos serviços *stream* está no fato de se ter controle das conexões como numa VPN. Além de avaliar de forma mais ampla um possível impacto da mudança IPv4-IPv6, também se colocou um controle de admissão para os diversos serviços do tipo *stream* (com exceção do Camera IP), que poderia ser bastante útil para dimensionar essa rede. Em uma rede corporativa essa função seria realizada por um servidor centralizador quando da geração dos serviços.

Após as medições realizadas nos cenários experimentais, foi utilizado de forma incremental o modelo de simulação, no software Arena 14.0, versão estudante (limitada em 150 entidades).

O modelo proposto por Pinotti [2011] permite simular os serviços como Vídeo Conferência, *Vídeo on Demand*, *Vídeo Clips*, VoIP, Câmera IP e *Data Files* (serviço de dados tais como serviço FTP, serviços HTTP (WEB), etc).

Inicialmente, foi utilizada a ferramenta *trace router* do *windows* em um site do Brasil e outro da Rússia para medir o tempo de propagação em uma conexão *wan* (Rede de Longa Distância).

Os valores obtidos pelo *tracer route,* foram utilizados no Arena, como se os sites fossem acessados através de uma VPN. A proposta para o cenário com os 5 serviços *stream* e com o serviço elástico seguem na Tabela 03:

Tabela 03 - Parâmetros de intervalo, duração e trafego de serviços.

Serviço	***Intervalo entre Requisições***	***Duração (s)***
Videoconferência	1 chamada/h	900
Vídeo on Demand	0.25 chamada/h	7200
Dados	1 arquivo/300s	(*)
Vídeo Clips	4 chamadas/h	300
VoIP	100 chamadas/h	180
Câmera IP	1 quadro/s	1

Fonte: Pinotti, (2011). Pag. 60

A simulação proposta nesta Dissertação utilizou de forma incremental os resultados obtidos nas medições das redes SOHO. Tal fato possibilitou o planejamento de uma rede em convergência, definir as limitações e as necessidades para manter os índices de QoS em níveis aceitáveis.

A Figura 27 mostra o cenário com todos os seus blocos e serviços. Para maior compreensão do modelo, os blocos e suas funções foram explicados separadamente, conforme mostrado nos próximos capítulos.

* O serviço Dados (*Data Files*) não possui período de duração como os serviços *stream*. Portanto, sua duração dependerá do volume de dados a ser transmitido e dá condição do sistema (filas, canal, etc.)

Nessa Página é colocado a Folha A3 (arquivo em corel).

Figura 27 – Modelo de Simulação (Pinotti)

8.1 Bloco *Arrive*

Estes blocos são responsáveis pela geração dos serviços, os tipos de serviços gerados estão descritos na Figura 28:

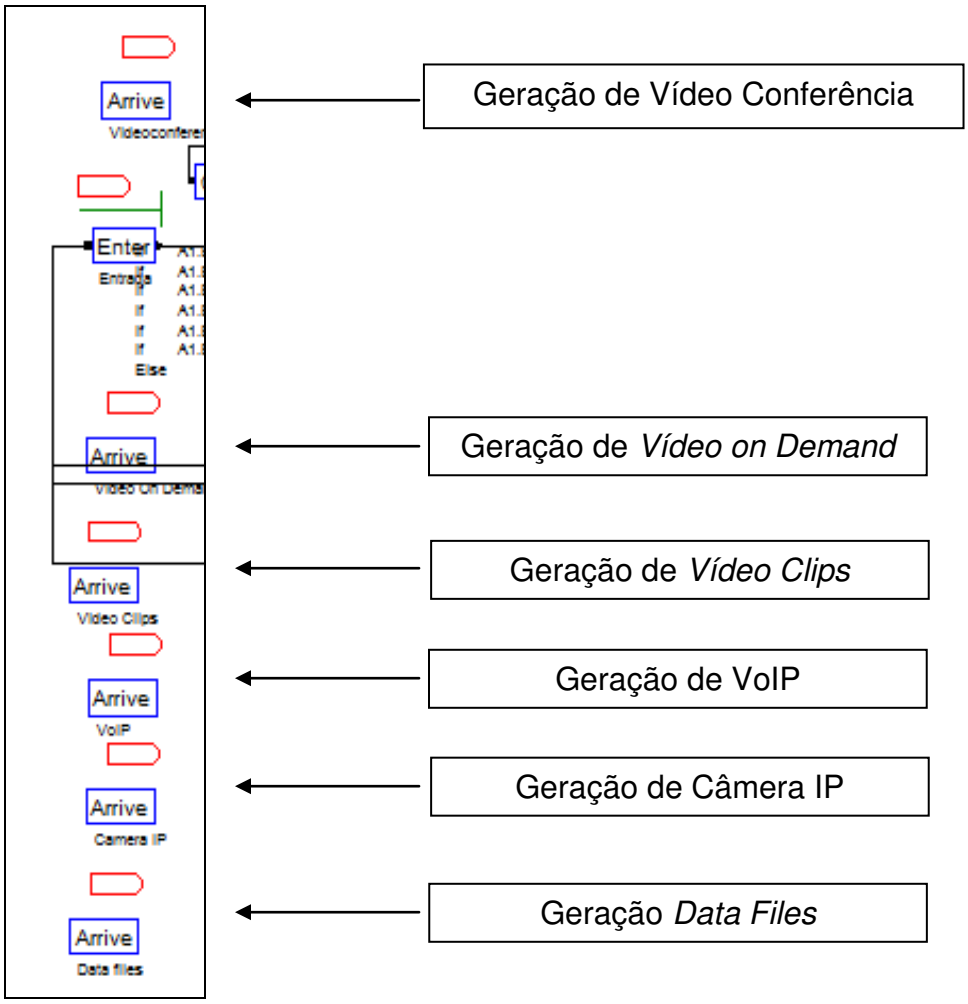

Figura 28 – Bloco *Arrive*.

Os serviços gerados, nos blocos anteriormente descritos, podem resultar em dois tipos de saídas:

- Serviços Permitidos: Quando o serviço gerado atende às requisições pré-estabelecidas, como número de usuários (CAC) caso sejam serviços *stream*[2].
- Serviços Rejeitados: Nos casos em que não haja disponibilidade no sistema para um dado tipo de serviço *stream*, o serviço é rejeitado nesse bloco.

As medições de Latência, *Jitter* e Perda de pacotes, que foram realizadas nos Cenários experimentais I, II e III, são incrementadas nos blocos *Arrive* de cada serviço.

8.2 Bloco *Choose* (1)

Após a geração dos serviços, os pacotes são encaminhados para o bloco *Choose*. Esse bloco recebe a demanda dos blocos anteriores (Bloco *Arrive*) e analisa qual o tipo do serviço gerado, além de encaminhar o pacote ao bloco *Assign* do respectivo serviço.

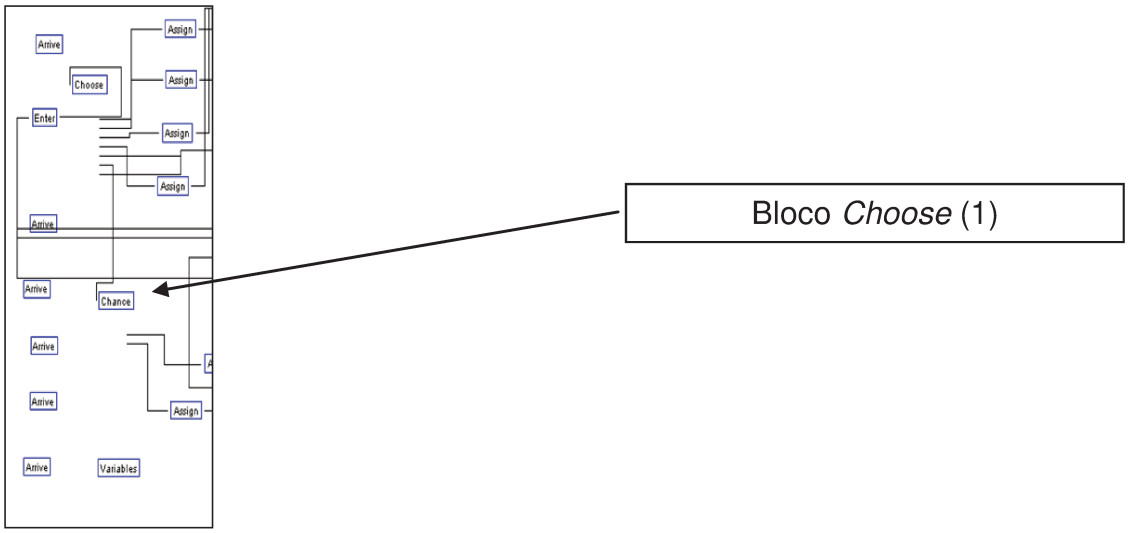

Figura 29 – Bloco *Choose* (1).

[2] Com relação ao único serviço elástico, chamado genericamente de *Data Files*, seu encaminhamento se dá por meio de pacotes de quantidade bits preestabelecida e, dependendo do tamanho (em bits) do serviço de *Data Files* sorteada pelo bloco *Arrive*, vai requerer maior ou menor número de pacotes para completá-lo. Esse serviço pode sofrer atraso e não há controle de admissão para ele (não tem perda). Tanto o serviço *stream* Câmera IP quanto o serviço elástico *Data Files* não tem o controle de admissão.

8.3 Bloco *Assign*

Esse bloco recebe o pacote encaminhado pelo bloco *Choose,* e adiciona a variável relativa ao serviço gerado no começo do processo, indicando que o serviço ocupará um espaço no sistema. Posteriormente, o pacote é encaminhado ao segundo bloco *Choose (2)*. Abaixo são demonstrados os blocos *Assign,* e suas respectivas variáveis relacionadas ao serviço gerado:

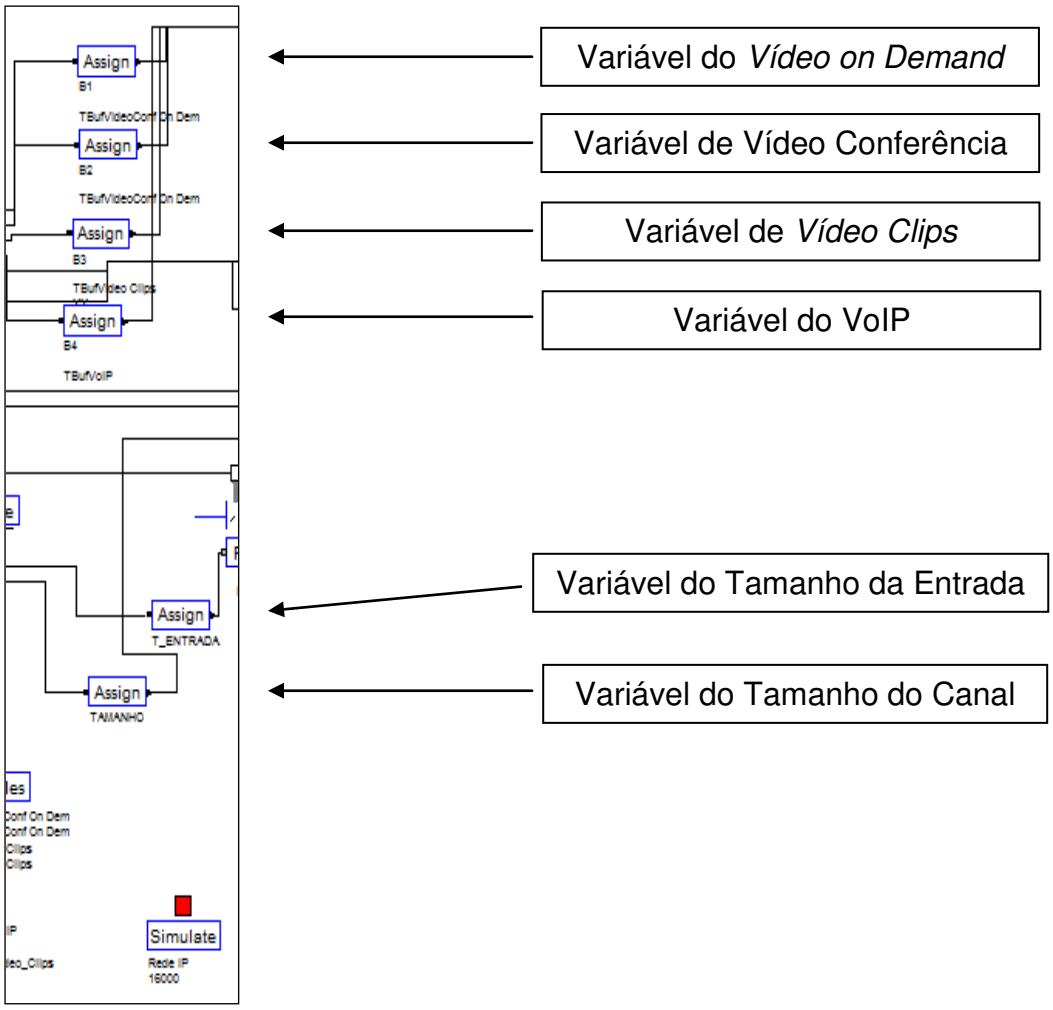

Figura 30 – Bloco *Assign*.

8.4 Bloco *Choose* (2)

As informações oriundas do bloco *Assign,* são encaminhadas ao bloco *Choose* (2) o qual verifica as variáveis inseridas no bloco *Assign* responsável pelo controle de admissão de chamadas (CAC).

Quando o valor da variável for menor que o valor do CAC, a chamada é contemplada e encaminhada ao bloco *Assign* responsável por verificar o tempo total da duração do serviço quando este foi gerado pelo bloco *Arrive*. Em situações em que o valor da variável for maior que o CAC, a chamada é rejeitada. O pacote rejeitado é encaminhado ao bloco *Assign* de serviços rejeitados, sendo incrementada ao contador uma chamada bloqueada.

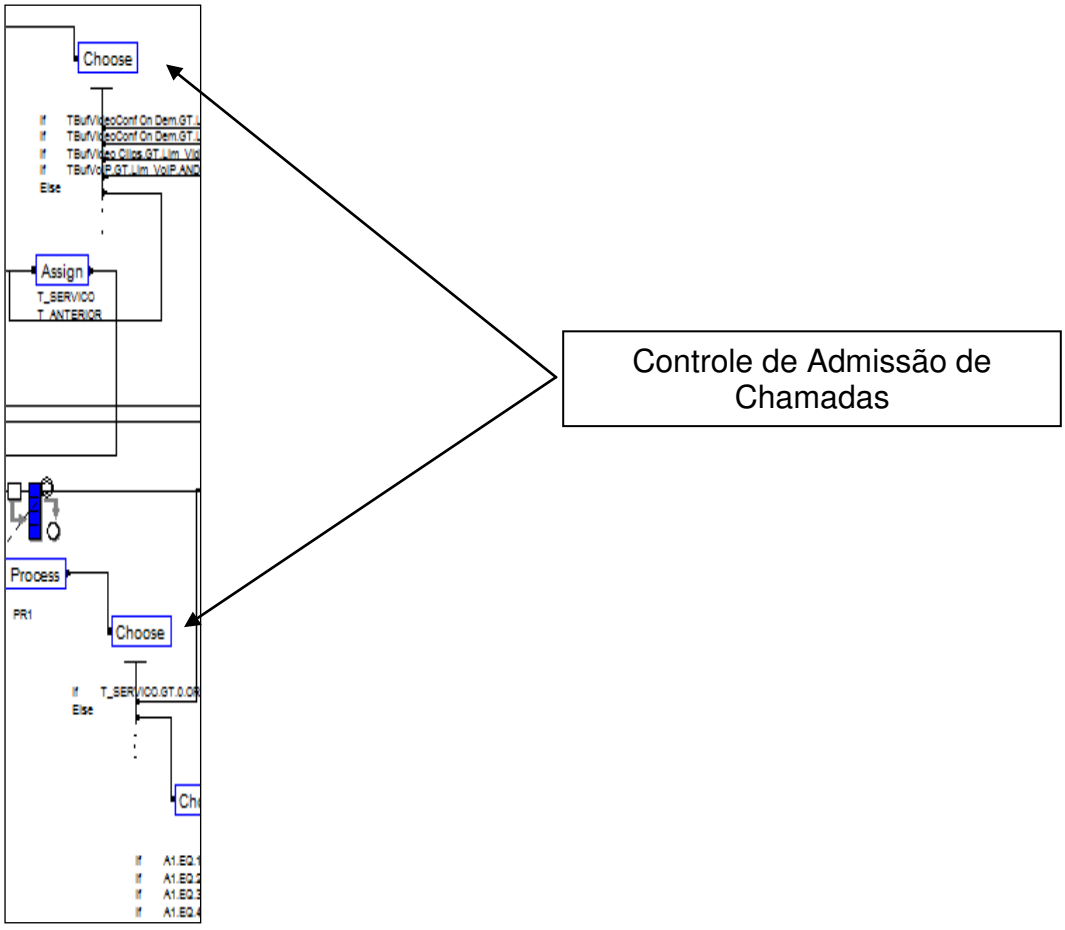

Figura 31 – Bloco *Choose* (2).

8.5 Bloco *Process*

Nesse bloco, é realizado todo o processamento do sistema. Variáveis, como *codec*, capacidade de processamento e regras de fila, interferem diretamente no processamento do pacote. Após processado, a solicitação é encaminhada ao bloco *Choose* (3).

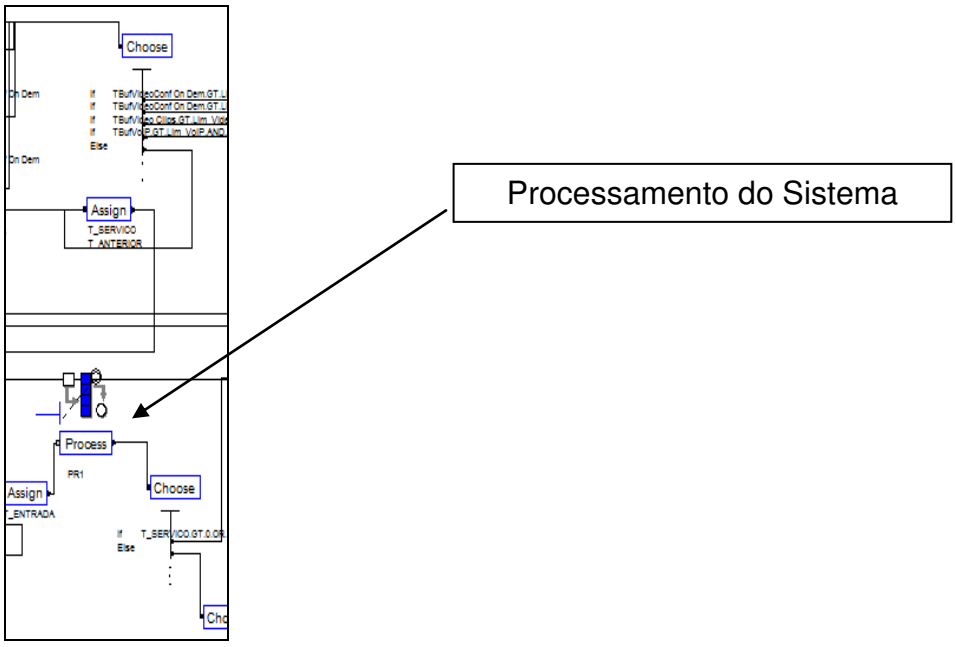

Figura 32 – Bloco *Process*.

8.6 Bloco *Choose* (3)

Esse bloco verifica o tempo de duração para completar o serviço do pacote enviado pelo bloco *Assign* de serviços permitidos. Se o serviço não tiver finalizado todo o processo, então, é feito *loopback*[3] ou retorno ao sistema.

[3] No caso dos serviços *stream*, o retorno ao sistema ocorre quando o tempo previsto para a duração do serviço não foi ainda completado; para o serviço elástico (*Data Files*), o retorno ocorre quando a quantidade de bytes prevista para o serviço ainda não foi completada. A ideia do retorno do serviço é simples: no nível de aplicação temos a duração do serviço, que é fundamental para os serviços *stream*, ou o seu tamanho em bytes, que é fundamental para o

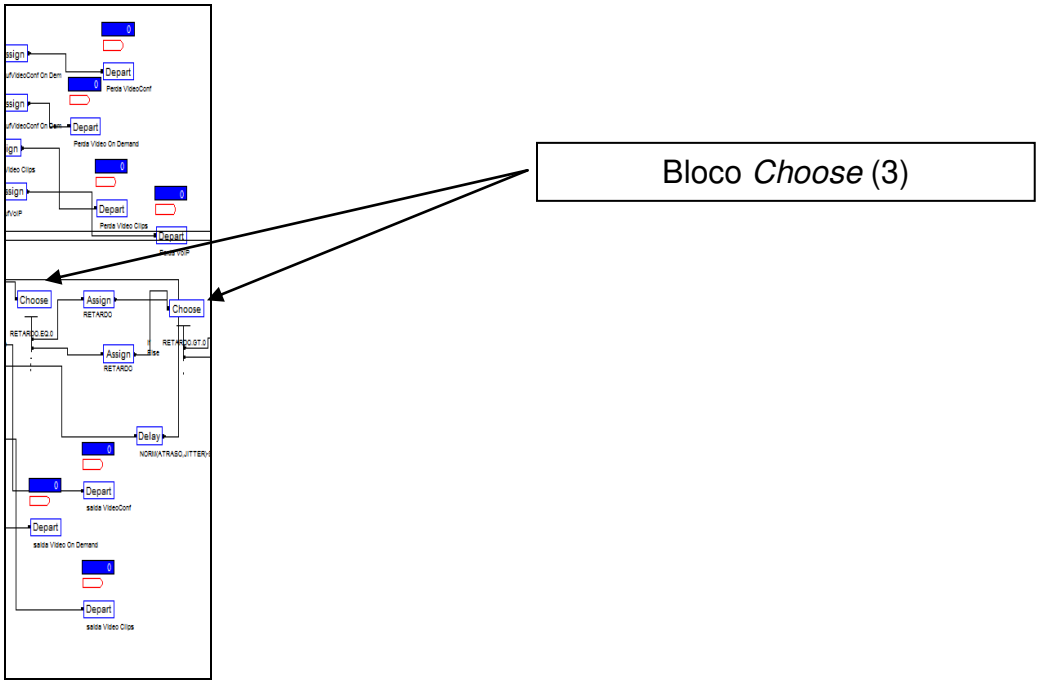

Figura 33 – Bloco *Choose* (3).

8.7 Bloco *Variables*

No bloco *variables*, são definidas variáveis de abrangência global (ao contrario dos atributos que são específicos de cada instância ou processo), como o limite do CAC, o tamanho do canal e o *Buffer* disponível para um dado serviço *stream*, para todos os serviços gerados inicialmente no bloco *Arrive*.

serviço elástico (características que são sorteadas no bloco *Arrive*). Esse nível de aplicação é convertido para os níveis mais baixos (de pacotes) por meio do envio de pacotes durante o tempo previsto para o serviço ou enquanto houver seus bytes para serem enviados.

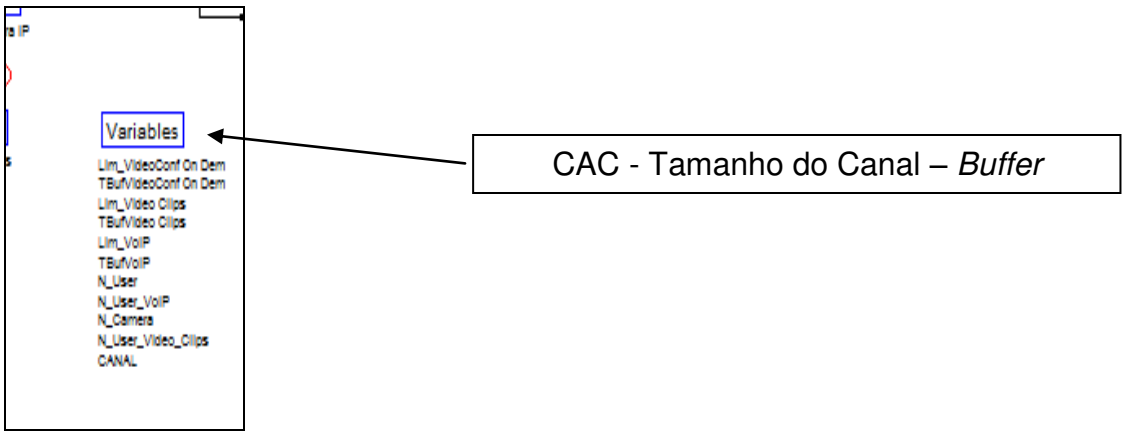

Figura 34 – Bloco *Variables*.

As medições de Vazão realizadas nos Cenários experimentais I, II e III são implementadas nesse bloco.

8.8 Bloco *Depart*

As saídas de todos os serviços gerados, contemplados ou rejeitados ocorrem nestes blocos.

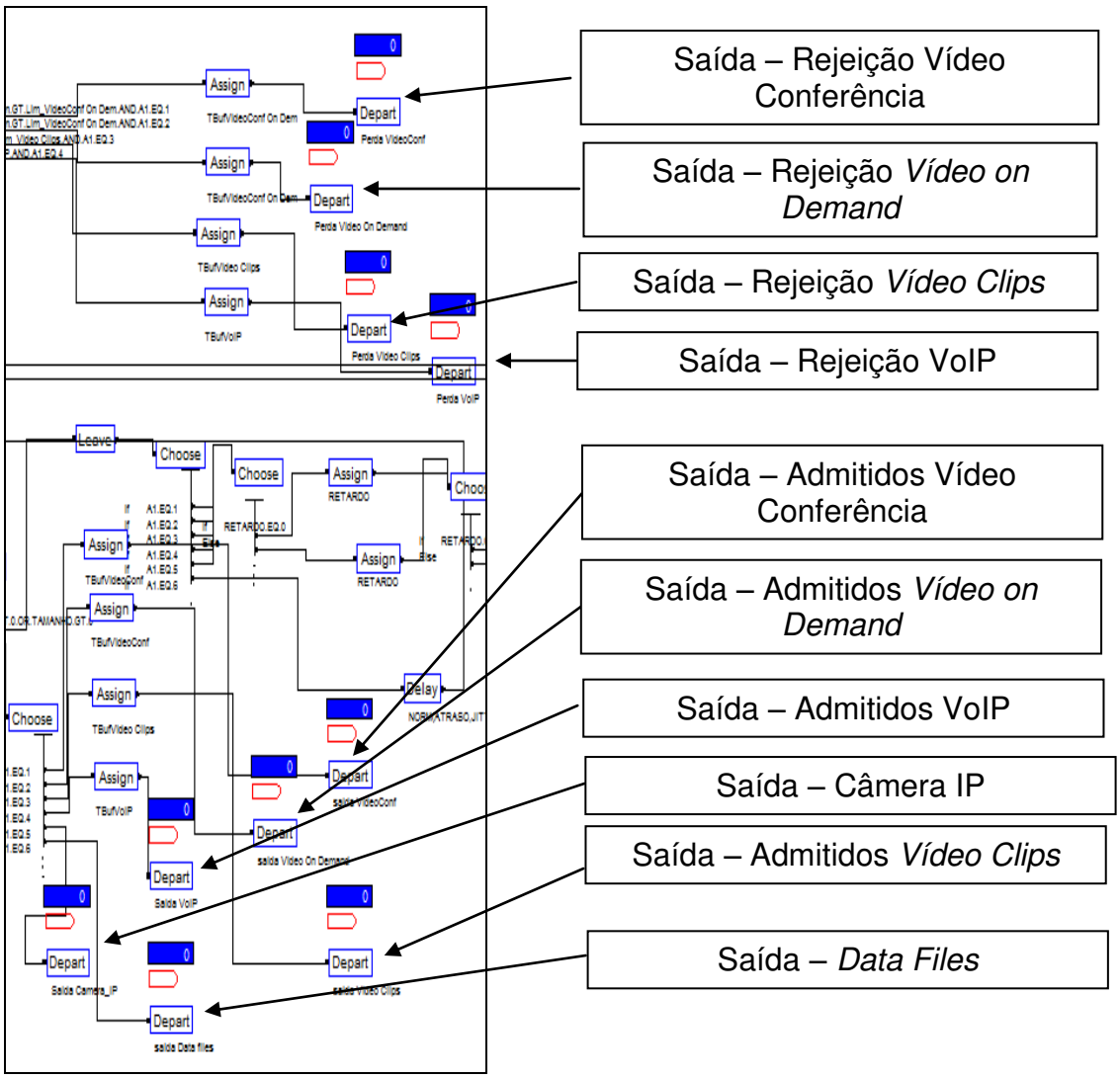

Figura 35 – Bloco *Depart*.

9. RESULTADOS DAS SIMULAÇÕES

A proposta das simulações é de observar o comportamento dos serviços *stream* e elástico, em função das variações promovidas pelos protocolos de comunicação IPv4, IPv6 e as técnicas que permitem coexistência e interoperabilidade.

Foram efetuadas 10 replicações de 100.000 segundos. O período de aquecimento (*warm-up period*) configurado no Arena, foi suposto de 10% do tempo de cada uma das três simulações. Segundo Freitas (2008), o período de aquecimento, deve ser definido quando os resultados das simulações atingirem um comportamento estável do sistema.

Na primeira simulação realizada, as medições do Cenário I – Rede IPv4 Pura, foram utilizados os seguintes valores:

- Vazão: 91,32 Mbits/seg.
- Latência: 0,355 ms.
- *Jitter*: 0,349 ms.
- Perda de pacotes: 0,026%.

Na segunda simulação, as medições do Cenário II – Rede IPv6 Pura foram utilizados os seguintes valores:

- Vazão: 87,79 Mbits/seg.
- Latência: 0,355 ms.
- *Jitter*: 0,259 ms.
- Perda de pacotes: 0%.

Na ultima simulação, as medições do Cenário III – Rede Pilha dupla foram utilizados os seguintes valores:

- Vazão: 91,06 Mbits/seg.
- Latência: 0,637 ms.
- *Jitter* : 0,287 ms.
- Perda de pacotes: 0,0002%.

Os resultados das simulações no Arena geram um arquivo ".txt". As replicações realizadas nos experimentos receberam tratamento estatístico, sendo possível estabelecer o intervalo de confiança para cada serviço gerado. Estes se encontram no DVD anexo.

9.1 Análises de Desempenho das Simulações

Os resultados das simulações foram analisados pelo tipo de serviço. Os dados provenientes das diferenças geradas pela utilização das versões dos protocolos de comunicação IPv4, IPv6 ou Pilha dupla foram comparadas. Os serviços estão separados em *stream* (*Vídeo on Demand*, Câmera IP, Videoconferência, VoIP, *Vídeo Clips*) e elástico (*Data Files*).

As Tabelas a seguir exibem o comparativo entre as simulações:

Tabela 04 – Comparação de Perda de Serviço em *Vídeo on Demand*

VÍDEO ON DEMAND		
REDE	**Bloqueio de Serviço - Valor Mínimo (%)**	**Bloqueio de Serviço - Valor Máximo (%)**
IPv4	91,96	99,78
IPv6	95,25	100
Pilha dupla	90,26	100

Devido à limitação de canal e o tempo de duração do serviço, o canal ocupado vai gerar um maior número de perda de serviços. Nesse tipo de serviço, pode-se observar que os resultados obtidos nas simulações IPv4 e Pilha dupla obtiveram valores máximos e mínimos muito próximos. Porém ao comparar o desempenho do IPv6, houve aproximadamente 4 % a mais de serviços bloqueados. O alto valor de perdas observado é forçado no modelo porque foi alocado ao controle de admissão um valor muito baixo em relação à duração do serviço e ao *codec* utilizado. Na prática, para conviver com um QoS satisfatório, esses valores terão que serem aumentados.

Tabela 05 – Comparação das Simulações de Câmera IP

CÂMERA IP			
REDE	**MÉDIA (Seg.)**	**MÍNIMO (Seg.)**	**MÁXIMO (Seg.)**
IPv4	1,0394	1,0394	1,0395
IPv6	1,0391	1,0390	1,0391
Pilha dupla	1,0392	1,0392	1,0392

No serviço de Câmera IP, os valores obtidos ficaram próximos, sendo concluindo-se que as versões dos protocolos não interferiram no desempenho desse tipo de tráfego *stream*.

Tabela 06 – Comparação de Perda de Serviço em Vídeoconferência

VIDEOCONFERÊNCIA		
REDE	**Bloqueio de Serviço - Valor Mínimo (%)**	**Bloqueio de Serviço - Valor Maximo (%)**
IPv4	95,51	98,48
IPv6	97,05	99,34
Pilha dupla	95,27	98,07

Assim, como os resultados do serviço de *Video on Demand*, os resultados obtidos das Redes IPv4 e Pilha dupla ficaram com desempenho próximos. A rede IPv6 obteve um desempenho aproximadamente 2 % inferior. Também neste caso, o alto valor de perdas observado é forçado porque foi alocado ao controle de admissão (descrito no Capítulo 8.4) um valor muito baixo em relação à duração do serviço e ao *codec* utilizado. Na prática, para conviver com um QoS satisfatório, esses valores terão que serem aumentados.

Tabela 07 – Comparação de Perda de Serviço em VoIP

VoIP		
REDE	Perdas **Valor Mínimo (%)**	Perdas **Valor Maximo (%)**
IPv4	0	0
IPv6	0	0
Pilha dupla	0	0

O serviço VoIP não obteve perdas, assim sendo, não houve degradação desse serviço *stream.*

Tabela 08 – Comparação de Perda de Serviço em *Vídeo Clips*

VÍDEO CLIPS		
REDE	Perdas **Valor Mínimo (%)**	Perdas **Valor Máximo (%)**
IPv4	1,09	1,71
IPv6	0,69	1,46
Pilha dupla	1,02	1,50

Na análise dos resultados do serviço *Video Clips*, o desempenho da rede IPv6 mostrou melhor desempenho em comparação aos resultados de valores mínimos obtidos pelas outras redes.

Tabela 09 – Comparação das Simulações de *Data Files*

DATA FILES			
REDE	**MÉDIA (Seg.)**	**MÍNIMO (Seg.)**	**MÁXIMO (Seg.)**
IPv4	5,8340	5,6120	6,0560
IPv6	5,8630	5,7091	6,0169
Pilha dupla	5,8217	5,6616	5,9819

Os valores médios simulados, nas três redes, ficaram próximos, assim como os valores máximos. A rede IPv6, embora com média ligeiramente maior que as outras duas, apresentou menor dispersão que as outras duas (mais estável com relação à variância dos atrasos).

9.2 Discussão sobre as Simulações

As simulações, com o cenário proposto, possibilitaram comparar o comportamento de seis serviços presentes nas redes com a variação dos protocolos, gerando resultados semelhantes ao de um ambiente real.

As medições de vazão, latência, j*itter* e perda de pacotes influenciaram no comportamento do modelo conforme a versão do protocolo.

Observou-se em todos os serviços das simulações IPv4 e Pilha dupla resultados próximos. Assim, concluí-se que o impacto no período de transição e coexistência, poderá ser irrelevante nas redes multisserviços. Não houve sua melhora sensível ou degradação do serviço prestado ao usuário.

Nas simulações IPv6, com base nos resultados apresentados, foi observado que as redes multimídia poderão ser impactadas com maior grau de significância no desempenho, como nos serviços de *Vídeo on Demand* e Vídeo Conferência, respectivamente 4% e 2% inferiores às simulações IPv4 e Pilha dupla. Nos outros serviços *stream* a melhora não foi sensível ou relevante. Nas simulações do serviço elástico (*Data Files*) observadas, houve uma pequena queda de desempenho nos valores mínimos.

A quantidade de perdas apresentadas nas simulações dos três cenários, ficaram abaixo de 1%, não degradando os serviços. Com exceção dos serviços de *Vídeo on Demand* e de Vídeo Conferência, pois o número de serviços bloqueados ficou bastante alto devido à propositalmente grande duração desses serviços, ou seja, pelo tempo em que o usuário utiliza o serviço o canal.

10. CONCLUSÕES E TRABALHOS FUTUROS

Conhecido como a versão empregada em maior escala nas redes atuais, o protocolo IPv4 não contempla todas as necessidades dos serviços mais utilizados (*stream*) e, portanto, sua substituição torna-se essencial para os fluxos de informação multimídia. Os experimentos demonstraram que os serviços *stream* obtiveram melhor desempenho em redes IPv6, baseado nas medições/simulações.

A metodologia aplicada nesta dissertação analisou as redes IPv4, IPv6 e pilha dupla e, a partir dos resultados das medições experimentais e simulações, levando-se em conta que a coexistência entre os dois protocolos poderá ocorrer por um longo período, recomenda-se o aumento na largura de banda para que os serviços elástico e *stream* não degradem. Os administradores de rede definem o aumento conforme os tipos de serviços prestados.

Além de comparar os resultados experimentais e simulados, a dissertação teve como contribuições gerais:

- Estudos dos impactos do protocolo IPv6 e pilha dupla, em vazão, latência, *jitter* e perda de pacotes.
- Estratégias para convivência dos protocolos, sendo apresentada a técnica de transição 6to4.
- Analise de rede com a ferramenta Iperf.
- Simulações de seis serviços de rede (videoconferência, *Vídeo on Demand*, VoIP, *Vídeo Clips*, câmera IP e *data files*), utilizando dados extraídos de redes reais.

Acerca do experimento/simulação proposto nesta dissertação, foi utilizado um cenário particular para avaliar o impacto da mudança IPv4/IPv6. Na aplicação da metodologia em uma rede real torna-se importante na atribuição de dados reais, tais como as distribuições dos tamanhos dos fluxos e dos tempos de chegadas (neste caso, somente para os *Data Files*, porém, no caso real há outros serviços elásticos), as distribuições dos diversos serviços *stream* e seus respectivos *codecs*.

Aspira-se em trabalhos futuros a realização de medições/simulações em outros cenários e em variados volumes de tráfego com maior número de serviços do tipo *stream* e elástico gerado. Podem ser efetuadas em redes de longas distâncias, bem como através de comunicação *wireless*.

REFERÊNCIAS BIBLIOGRÁFICAS

[CGI] Disponível em <www.cgi.br/regulamentaco/resolucao2012-007.htm>. Acesso em 09/2012.

[Chang, Y. et al., 2004] Chang, Y. et.el. **Performance Investigation of IPv4/IPv6 Transition Mechanisms**. Department of Electrical Engineering National Dong Hwa University, Taiwan, 2004. Disponível em: <http://dormv6.niu.edu.tw/~hccftp.pdf>. Acesso em 11/2011.

[Christian O'Flaherty (et. al.), 2009] Christian O'Flaherty, et.al. **IPv6 para Todos**. Buenos Aires: Association Civil Argentinos em Internet, 2009. Pág. 15.

[Carissimi, 2009] CARISSIMI, A. **Redes de Computadores.** Instituto de Informática UFRGS. Editora Bookman, 2009.

[Comer, 2004] COMER, DOUGLAS E. **Computer and Networks Internet with Internet Applications**, São Paulo: Tradução Artmed Editora ,2007. Pág. 239.

[Dietz, 1992] Dietz, M. **Outline of a sucessful simulation projects. Industrial Engineering**, Industrial Engineering, 1992. Disponível em <www.accessmylibrary.com/article-1G1-13038825/outline-successful-simulation-project.html>. Acesso em 05/2013.

[Filippetti, 2008] Filippetti, Marco A. **CCNA 4.1 – Guia Completo de Estudo**. Florianópolis: Visual Books, 2008. Pág. 174.

[Fiorentino, 2012] Fiorentino, Adilson A. **IPv6 na Pratica**, São Paulo: Linux New Media do Brasil Editora Ltda, 2012. Pág. 19.

[Forouzan, 2006] FOROUZAN, A. **Comunicação de Dados e Redes de Computadores**. Porto Alegre: Tradução Bookman, 2006. Pág. 39.

[Freitas, 2008] FREITAS FILHO, P. J. **Introdução à Modelagem e Simulação de Sistemas com Aplicações em Arena.** Florianópolis: Visual Books, 2008.

[Gilligan & Nordmark, 1996] Gilligan, R.; Nordmark, E. Network Working Group: RFC 1933. Disponível em: <http://tools.ietf.org/html/rfc1933>. Acesso em 08/2012.

[Hagen, 2002] HAGEN, SILVIA. **IPv6 Essentials.** Editora O'Reilly, 2002. Pág. 06, 170.

[Ioan & Zeadally, 2003] Ioan, R.; Zeadally, S. **Evaluating IPv4 to IPv6 Transition Mechanisms.** Purdue University, USA, 2003. Disponível em: < http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1191589&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D1191589 >. Acesso em 12/2011.

[IPv6.br] Referencias disponíveis em <http://ipv6.br/>.

[Junior, L. et al., 2005] Junior, L. et.al. **Análise da Segurança em Redes Puramente IPv6.** Centro Universitário Luterano de Palmas, 2005. Disponível em: < http://lucaszc.homelinux.org/fic-pos/IPV6/IPv6.pdf>. Acesso em 12/2011.

[Kurose, 2006] KUROSE, JAMES F. **Redes de Computadores e a Internet: Uma abordagem top-down**. – São Paulo: Editora Pearson Addison Wesley, 3ª edição, 2006. Pág. 29.

[Martinez, 2011] Tutorial disponível <www.bitabit.eng.br/2011/02/03/conectividade-IPv6-em-casa---parte-1/>. Acesso 08/2012.

[Mogul, 1990] MOGUL, JEFFREY C. Efficient Use of Workstation for Passive Monitoring of Local Area Networks. [on-line], Califórnia, 1990. Disponível em: < http://dl.acm.org/citation.cfm?id=99562 >. Acesso em 02/2012.

[Mun & Lee, 2005] MUN, Y. e LEE, K. **Understanding IPv6.** United States of America: Editora Spriger Science, 2005. Pág. 121.

[Oliver, 2001] P. Olivier e N. Benameur, **"Flow Level IP Traffic Characterization"**, Elsevier Science, ITC 17 – 17th International Teletraffic Congress , 2001.

[Pinotti, F., 2011] Pinotti, Fernando L. **Simulação e Emulação de Tráfego Multimídia em Redes IP**. Faculdade Estadual de Campinas, 2011. Pág. 07.

[RFC 791] Disponível em <http://www.ietf.org/rfc/rfc791.txt>. Acesso em 10/2012.

[RFC 2460] Disponível em <http://ipv6.net/RFC/rfc-2460-internet-protocol-version-6-ipv6-specification.html>. Acesso em 10/2012.

[RFC 2461] Disponível em <http://datatracker.ietf.org/doc/rfc2461/>. Acesso em 10/2012.

[RFC 2983] Disponível em <https://tools.ietf.org/rfc/rfc2983.txt>. Acesso em 10/2012.

[RFC 3035] Disponível em <http://datatracker.ietf.org/doc/rfc3035/>. Acesso em 10/2012.

[RFC 3214] Disponível em <http://tools.ietf.org/html/rfc3214>. Acesso em 10/2012.

[RFC 4213] Disponível em <http://datatracker.ietf.org/doc/rfc4213/>. Acesso em 10/2012.

[RFC 4338] Disponível em <http://datatracker.ietf.org/doc/rfc4338/>. Acesso em 10/2012.

[RFC 4380] Disponível em <http://www.ietf.org/rfc/rfc4380.txt>. Acesso em 10/2012.

[RFC 4443] Disponível em <http://rfc-ref.org/RFC-TEXTS/4443/index.html>. Acesso em 10/2012.

[Tanenbaum, 1997] TANENBAUM, ANDREW S. **Redes de Computadores**. Editora Campus, 4ª edição, 1997. Pág. 357.

[Tatipamula & Grossetete, 2004] Tatipamula, M.; Grossetete, P. **Coexistence Strategies for Next-Generation Networks**. University of Tokyo, 2004. Disponível em: < http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1262167&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D1262167>. Acesso em 11/2011.

[Teleco] Figura disponível em < www.teleco.com.br>, Acesso em 08/2012.

TOME, Sandra M. Campanholi; Ursini, E. L.; Mincov N. **Dimensionamento de Rede IP Integrada Corporativa/Operativa de Subestação de Energia**, Fortaleza. Em: Congresso Tecnológico Infobrasil 2008, 2008.

[Torres, 2001] Torres, G. **Redes de Computadores**. Rio de Janeiro: Editora Axcel Books, 2001. Pág. 64.

[Tsirtsis, 2000] Tsirtsis, G. Network Working Group: RFC 2766. Disponíve em: <www.ietf.org/rfc/rfc2766.txt>. Acesso em 07/2012.

[V6ops] IETF IPv6 Operations. Disponível em: < http://datatracker.ietf.org/wg/v6ops/ >. Acesso em 08/2012.