Nuno Miguel Carvalho Galego

Estudo da eficiência da comunicação IPv4 versus IPv6 na rede de investigação e ensino Portuguesa RCTS entre Lisboa e Covilhã

Orientador: Prof. Doutor Nuno Manuel Garcia dos Santos

Co-orientador: Dr. Carlos Miguel Queirós Friaças

Universidade Lusófona de Humanidades e Tecnologias
Escola de Comunicação, Arquitetura, Artes e Tecnologias de Informação

Lisboa
2016

Nuno Miguel Carvalho Galego

Estudo da eficiência da comunicação IPv4 versus IPv6 na rede de investigação e ensino Portuguesa RCTS entre Lisboa e Covilhã

Dissertação defendida em provas públicas na Universidade Lusófona de Humanidades e Tecnologias no dia 05/04/2017, perante o júri, nomeado pelo Despacho de Nomeação nº: 494/2016, de 21 de dezembro com a seguinte composição:

Presidente: Prof. Doutor José Luis de Azevedo Quintino Rogado (ULHT)

Arguente: Profª Doutora Teresa Maria Sá Ferreira Vazão Vasques (IST)

Orientador: Prof. Doutor Nuno Manuel Garcia dos Santos (ULHT)

Universidade Lusófona de Humanidades e Tecnologias
Escola de Comunicação, Arquitetura, Artes e Tecnologias de Informação

Lisboa
2016

Epígrafe

"Do pouco se faz muito, do nada, nada se faz…"

Nuno Galego

Dedicatória

Dedico esta dissertação aos meus pais, João, que faleceu há sensivelmente 8 anos, relativamente jovem a quem a vida infelizmente pregou uma rasteira e Conceição que foram as únicas pessoas que sempre me ajudaram em toda a minha vida.

Nuno Miguel Carvalho Galego

Agradecimento

Esta dissertação é fruto de um longo trabalho e dedicação, contudo não seria possível sem conselhos e apoio durante todo o trabalho.

Em primeiro lugar quero agradecer a orientação e disponibilidade do professor Nuno Garcia em todas as fases da dissertação, pois sem o seu sábio conhecimento e orientação tudo teria sido mais difícil.

Quero também agradecer a colaboração do Dr. Carlos Friaças como co-orientador que sempre esteve disponível para me ajudar de modo a levar a dissertação a bom porto.

Aos meus orientadores, o meu sentido obrigado pela ajuda e interesse demonstrado no projecto.

Um agradecimento especial à minha família, à minha filha Maria e à minha namorada Ana por todo o apoio, companheirismo e paciência ao longo de todo o curso.

Ao Marco Cassapo que passou horas a fio comigo a fazer várias experiências e ao Dr. João Ildefonso pela disponibilidade e ajuda nos testes finais na Universidade Lusófona.

Gostaria de deixar uma palavra de apreço aos meus colegas de Mestrado Telmo Paixão e Ricardo Henriques, pois tiveram um papel fundamental ao longo do curso, agradecendo todo o apoio que sempre me disponibilizaram.

Por último, quero agradecer a todos os colegas da Sumol+Compal que me apoiaram nesta etapa da minha vida.

A todos, muito obrigado.

Resumo

Com a entrada num paradigma de escassez da distribuição dos endereços IPv4 a transição para IPv6 é a única solução para o crescimento contínuo da *Internet*. Contudo o IPv4 não é totalmente compatível com o IPv6 mas, uma vez que o IPv4 é o protocolo dominante, é necessário usar métodos de transição para que os protocolos funcionem em simultâneo até que surja uma possibilidade real de realizar uma transição total para o protocolo IPv6. A transição terá de ser feita desta forma, de modo a que cada aplicação que necessite de recursos de rede consiga comunicar tanto com redes em IPv4 como IPv6.

É importante perceber que esta mudança não irá acontecer da noite para o dia e vai ser um processo que irá demorar algum tempo e que será necessário avaliar diversas métricas antes da sua transição completa, tais como o desempenho.

Esta tese visa avaliar o desempenho com recurso a métricas de avaliação de qualidade de serviço (QoS) dos protocolos IPv4 e IPv6 no interior da rede de investigação e ensino Portuguesa (RCTS) através da injecção de tráfego na rede com recurso ao *software* de geração e medição de tráfego D-ITG. Para tal foram realizados dois testes experimentais, onde a injecção de tráfego ocorreu em dois momentos distintos (em horário laboral e horário pós-laboral) e simulados quatro cenários em simultâneo sendo eles: transferência de pacotes UDP e TCP, VoIP e *streaming* de áudio e vídeo. Os parâmetros de avaliação escolhidos foram a quantidade de pacotes transferidos, atraso, variação do atraso e perda de pacotes.

São também referidas algumas vantagens do protocolo IPv6 em relação ao IPv4.

Palavras-chave: IPv4, IPv6, RCTS, D-ITG, variação do atraso, atraso, perda de pacotes, TCP, UDP, VoIP, streaming, Qualidade de serviço.

Abstract

With the entry into a paradigm of distribution scarcity of IPv4 addresses the transition to IPv6 is the only solution for the continued growth of the Internet. However IPv4 is not compatible with IPv6 but, still there are many IPv4 networks that use that protocol so, it is necessary to use transition methods for both protocols to work simultaneously until a real possibility of making a full transition to IPv6 protocol. The transition will have to be done in this way, so that each application requiring network resources can communicate with both IPv4 and IPv6 networks.

It is important to realize that this change will not happen overnight and it will be a process that will take some time and it will be necessary to evaluate several metrics before full transition, such as performance.

This thesis aims to evaluate the performance using the metrics for the evaluation of quality of service (QoS) of IPv4 and IPv6 protocols within the Portuguese Research and Education Network (RCTS) through traffic injection on the network using the software of generation and measurement of traffic D-ITG. For this there were two experimental tests, where the traffic injection occurred at two different times (during working hours and after work hours) and simulated four scenarios simultaneously: transfer of UDP and TCP packets, VoIP and streaming audio and video. The evaluation parameters chosen were the amount of transferred packets, delay, jitter and packet loss.

Some advantages of the IPv6 protocol in relation to IPv4 are also mentioned.

Keywords: IPv4, IPv6, RCTS, D-ITG, Jitter, Delay, Packet Loss, TCP, UDP, VoIP, Streaming, Quality of Service.

Siglas e Acrónimos

6RD - IPv6 rapid deployment

APNIC - Asia Pacific Network Information Centre

ARPANET - Advanced Research And Projects Agency Network

ASICs - Application Specific Integrated Circuits

CPU - Central Processing Unit

DCCP - Datagram Congestion Control Protocol

DLPI - Data Link Provider Interface

DNS - Domain Name System

DS - Differentiated Services

FCCN - Fundação para a Computação Científica Nacional

FCT - Fundação para a Ciência e a Tecnologia

GRE - Generic Routing Encapsulation

HTTP - Hypertext Transfer Protocol

IANA - Internet Assigned Numbers Authority

ICMP - Internet Control Message Protocol

ICMPv4 - Internet Control Message Protocol Version 4

ICMPv6 - Internet Control Message Protocol Version 6

IETF - Internet Engineering Task Force

IoT - Internet of Things

IPSec - IP Security Protocol

IPv4 - Internet Protocol Version 4

IPv6 - Internet Protocol Version 6

ISATAP - Intra-Site Automatic Tunnel Addressing Protocol

ITU - International Telecommunication Union

LAN - Local Area Network

MTU - Maximum Transmission Unit

NAT – Network Address Translation

NAT-PT - Network Address Translation with Protocol Translation

NNTP - Network News Transfer Protocol

NREN - National Research and Education Network

NTP - Network Time Protocol

OSI - Open Systems Interconnection

OWD - One-Way Delay

PPS - Packets Per Second

QoS - Quality of Service

RCTS - Rede Ciência, Tecnologia e Sociedade

RFC - Request for Comments

RIPE/NCC - Réseaux IP Européens / Network Coordination Centre

RTP - Real-time Transport Protocol

RTSP - Real Time Streaming Protocol

RTT - Round-Trip Time

SCTP - Stream Control Transmission Protocol

SIP - Session Initiation Protoco

TCP - Transmission Control Protocol

ToS - Type of Services

TTL - Time to Live

UBI - Universidade da Beira Interior

UDP - User Datagram Protocol

ULHT - Universidade Lusófona de Humanidades e Tecnocologias

VAD - Voice activity detection

VLC - Video LAN Client

VLSM - Variable-length Subnet Mask

VoIP - Voice over Internet Protocol

Índice

Índice de figuras

Índice de tabelas

Índice de gráficos

1. Introdução

1.1 Enquadramento

Antes de iniciar este trabalho sobre o estudo da eficiência da comunicação IPv4 (*Internet Protocol Version* 4) versus IPv6 (*Internet Protocol Version* 6) na rede de investigação e ensino Portuguesa (RCTS) entre a Universidade Lusófona de Humanidades e Tecnologias em Lisboa e a Universidade da Beira Interior na Covilhã é necessário relembrar alguns pontos sobre o funcionamento das redes e, em especial, da *Internet*.

Uma rede pode ser definida como um conjunto de computadores e outros equipamentos interligados e capazes de comunicar entre si utilizando um conjunto de regras, ou protocolos.

O IP (*Internet Protocol)* é um protocolo que foi projectado para criar ligações entre diferentes redes, possibilitando a comunicação entre dispositivos. O protocolo IP teve origem no ano de 1970 pela ARPANET *(Advanced Research Projects Agency Network*), esta rede, de origem militar, foi sendo expandida e interligada a outras, formando em 1980 um vasto conjunto que passou a ser conhecido por *Internet*.

O protocolo IP fornece um serviço que é usado por outros protocolos de nível superior (camada 4 do modelo OSI), tais como o TCP *(Transmission Control Protocol)* e o UDP *(User Datagram Protocol).*

Actualmente a maior parte dos computadores utilizam apenas o protocolo IPv4, mas devido ao rápido crescimento da *Internet* os endereços que fazem parte deste protocolo estão a ficar esgotados e essa escassez de endereços IPv4 irá implicar a mudança generalizada para um novo protocolo (Sharma & Chauhan, 2014).

Esse rápido crescimento deu-se nos anos 90, com a disseminação maciça dos dispositivos móveis que a partir do ano 2000 deram origem a uma nova era em que o elemento mais importante deixou de ser a máquina e passou a ser o utilizador, ou seja a pessoa. Nesta nova era, as pessoas estão cada vez mais ligadas a redes sociais, serviços de *home banking* ou *E-commerce* em qualquer lugar a qualquer hora através de vários dispositivos, quer sejam eles fixos ou móveis (o que inclui *smartphones*, *tablets* e afins). Cada um desses dispositivos está ligado à *Internet* e possui um endereço IP único, que serve para o identificar univocamente na *Internet* (Kumar & Kumar, 2016).

A próxima era será aquela em que qualquer dispositivo poderá estar ligado à *Internet* para os mais diversos fins. O crescimento da *Internet* prevê que dispositivos como frigoríficos, micro-ondas, veículos e muitos outros no futuro irão necessitar de acesso à Internet para o seu funcionamento. Esta era é a chamada *Internet* das coisas (IoT – *Internet of Things*), contudo este avanço só será viável quando o IPv6 estiver implementado de

forma generalizada, pois afinal irão ser necessários mais endereços do que os 4.3 mil milhões possíveis no IPv4, além de outros requisitos como a segurança, e a mobilidade (Brito, 2013).

Para endereçar esta questão nos anos 90 foi criado o IPv6, que veio resolver vários problemas do IPv4, entre eles a falta de endereços, a falta de segurança, já que a segurança não era requisito obrigatório no IPv4. No IPv6 o tema segurança foi um critério relevante, tanto que o protocolo IPSec (Kent & Seo, 2005) foi criado para o IPv6 e só depois foi aproveitado para o IPv4.

Desde Junho de 2012 (World IPv6 Launch, 2016), graças a uma forte dinamização da ISOC – Internet Society - o IPv6 passou a ser considerado o novo protocolo padrão da *Internet* em substituição do IPv4, onde a partir dessa data, todos os novos equipamentos de rede fabricados no Mundo devem possuir suporte para IPv6. A expectativa é que o IPv6 substitua gradualmente o IPv4, de tal forma que as duas versões possam coexistir durante um longo período de transição. As organizações que não fizerem esta mudança atempadamente, no futuro poderão incorrer em mais custos, pois não haverá tempo para prepararem um plano de transição equilibrado (Almes, Mundrane, Polichar, & Anderson, 2013).

O IPv6 foi projectado para constituir um passo evolutivo na melhoria da *Internet* onde hoje em dia uma das principais preocupações dos utilizadores é a ligação à rede e o seu desempenho, quer seja para aceder a uma rede social, consumir conteúdos através de *streaming* ou jogar jogos *online.* Por estes motivos é necessário prestar atenção ao desempenho das redes para que possam ser estudados e eliminados eventuais problemas.

Por todos os motivos apresentados, nos próximos anos, os profissionais preparados para lidar com este novo protocolo, serão recursos humanos cada vez mais valorizados e procurados pelo mercado.

1.2 Motivação

A Internet que conhecemos hoje em dia está a ser inundada por vários tipos de tráfego (s*treaming* de áudio e vídeo, VoIP, transferência de ficheiros, etc..) existindo cada vez mais investigadores que procuram provar que o IPv6 é o único caminho para o crescimento da Internet (Babatunde & Al-Debagy, 2014; Shiranzaei & Khan, 2015). É imperativo optimizar e melhorar o desempenho das redes em várias métricas estatísticas, como a taxa de transferência, atraso, variação do atraso ou perda de pacotes.

Por esse motivo, o presente trabalho tem como proposta apresentar o desempenho dos protocolos IPv4 e IPv6 entre dois nós da rede de investigação e ensino Portuguesa (RCTS) localizados em Lisboa e na Covilhã, em momentos distintos, de forma a realizar

uma análise comparativa de ambos os protocolos. A RCTS à data deste documento fornece serviços a cerca de uma centena de instituições, sedeadas no continente e regiões autónomas.

1.3 Questão e hipótese

Numa fase inicial um dos passos mais importantes é a definição da questão de investigação que eventualmente será a solução para a resolução do problema. Com base nas metodologias de investigação apropriadas é possível encontrar a resposta a essa mesma questão.

A questão principal é: Que desempenho terá a utilização do IPv6 no interior da rede de investigação e ensino Portuguesa (RCTS)? Terá melhor desempenho que o IPv4?

A hipótese para dar resposta a esta questão poderá ser:

- Analisar o desempenho verificado em comunicações através de IPv6 como de IPv4 entre os pontos.

Como forma de testar a hipótese a solução poderá passar por realizar uma análise de desempenho em ambiente real sobre a rede RCTS entre dois extremos localizados em Lisboa e na Covilhã, das seguintes formas:

- IPv4 para IPv4 e IPv6 para IPv6;
- Realizar testes de *streaming,* VoIP e tráfego de ficheiros com os protocolos TCP e UDP sobre ambas as versões do protocolo IP;
- Realizar os testes em momentos distintos.

1.4 Objectivos

A resposta à questão é transformada em objectivos desta investigação, que passam por realizar uma análise comparativa de desempenho de transferência de ficheiros, VoIP e *streaming* de áudio e vídeo com os protocolos de rede IPv4 e IPv6 para concluir qual das versões do protocolo oferece melhor qualidade de serviço (QoS).

Desta forma são enumerados os seguintes objectivos para este trabalho:

- Identificar as vantagens e desvantagens da utilização dos protocolos IPv4 e IPv6;
- Examinar o número de pacotes tal como o tamanho dos pacotes durante um determinado período de tempo, o endereço IP de origem, endereço IP de destino e que tipo de protocolo de transporte foi utilizado;
- Medir e avaliar a quantidade de tráfego gerado em cada uma das versões do protocolo ao nível do atraso, variação do atraso e pacotes perdidos;

- Apresentar e justificar com detalhe qual dos protocolos apresenta um melhor desempenho com base na análise realizada.

1.5 Metodologia

O método quantitativo foi adoptado para este tema de investigação de análise de desempenho comparativo em redes IPv4 e IPv6. Os métodos quantitativos são focados na recolha de factos e estudam a relação entre eles. Realizam medições com a ajuda de técnicas científicas e analisam dados que conduzem a conclusões quantitativas.

Por outro lado, o método qualitativo tem como objectivo obter um resultado e a descoberta ou constatação de algo, o que também se aplica nesta investigação.

Os resultados desta pesquisa são os resultados de uma comparação do desempenho de redes mistas onde após essa comparação irá ser usada uma abordagem qualitativa para analisar os dados recolhidos. Serão medidos os prós e contras, chegando-se idealmente a uma conclusão de qual será a melhor versão do protocolo IP a ser aplicado, tendo em conta a realidade.

Esta investigação vai focar-se no estilo experimental, visto que os resultados estão dependentes de resultados experimentais e com o método de testes de hipóteses onde irão ser testadas todas as hipóteses de modo a chegar a uma conclusão.

A investigação usa por isso uma abordagem mista, na qual usará procedimentos simultâneos, convergindo dados quantitativos e qualitativos, com o fim de fornecer uma análise abrangente do problema em pesquisa (Creswell, 2014).

1.6 Organização da dissertação

O presente trabalho está estruturado em cinco capítulos, contendo ainda dois anexos relativos ao trabalho desenvolvido.

Este primeiro capítulo contextualiza o conteúdo a ser apresentado bem como a motivação, os objectivos e a metodologia utilizada. Os restantes capítulos apresentam os seguintes temas:

- o Capitulo 2: aborda o estado da arte, onde é efectuada uma pequena análise dos protocolos IPv4 e IPv6, bem como o estado do IPv6 em Portugal e no mundo. São apresentados trabalhos relacionados com o tema, incluindo ferramentas de geração e medição de tráfego de rede, explicando o seu funcionamento e também uma abordagem sobre os mecanismos de transição do IPv4 para o IPv6;
- o Capítulo 3 descreve a arquitectura utilizada na experiência, apresentando com detalhe as metodologias utilizadas para a realização da experiência, evidenciando a

ferramenta seleccionada. É ainda descrito o ambiente em que os testes foram desenvolvidos;

- o Capítulo 4 apresenta os resultados obtidos, representados através de tabelas e gráficos, bem como algumas conclusões;

- o Capítulo 5: Conclui esta dissertação apresentando as conclusões finais da experiência, assim como algumas sugestões para trabalhos futuros, relacionados com o tema.

2. Estudo do Estado da arte

2.1 Introdução

Este capítulo apresenta uma revisão do estado da arte, consistindo em duas componentes. Inicialmente irão ser apresentados alguns conceitos sobre os protocolos IPv4 e IPv6, sobre o estado do IPv6 em Portugal e no mundo, e como analisar os mecanismos de transição existentes para melhor compreender como eles podem facilitar a transição para o IPv6. É também objectivo desta revisão do estado da arte apresentar alguns parâmetros de qualidade de serviço que são importantes para a descrição do trabalho de investigação, sendo também fornecido um pequeno resumo para cada um dos parâmetros.

No final deste capítulo, irão ser apresentados os trabalhos mais significativos e relacionados com o tema em estudo, que terão como objectivo demonstrar conclusões de investigação nesta área.

2.2 IPv4

O IPv4 foi criado por Jon Postel e publicado pela primeira vez em 1980 com a RFC 760 (Postel, 1980) e substituído em 1981 pela RFC 791 (Postel, 1981), sendo mais tarde em 1982 adoptado como o protocolo oficial da ARPANET (*Advanced Research And Projects Agency*) (Kleinrock, 1969). Este protocolo funciona na camada 3 do modelo OSI (*Open Systems Interconnection*) (ISO, 1984) também conhecida por camada de rede (*Network*) e utiliza endereços de 32 *bits*, o que limita o espaço de endereçamento a 2^{32} endereços. Os endereços são escritos em forma de quatro octetos em notação decimal separados por pontos, por exemplo: 203.0.113.3.

O espaço de endereçamento do IPv4 não é pequeno, visto que existem mais de 4 biliões de endereços (4 294 967 296), no entanto, alguns blocos de endereços são reservados para fins especiais, tais como redes privadas e endereços de *multicast*. Isso reduz o número de endereços que podem ser usados para encaminhamento na *Internet*.

Os endereços privados estão distribuídos em 3 classes de endereços privados (Rekhter, Moskowitz, Karrenberg, de Groot, & Lear, 1996), sendo eles:

Classe A - 10.0.0.0 - 10.255.255.255 (prefixo 10/8);

Classe B - 172.16.0.0 - 172.31.255.255 (prefixo 172.16/12);

Classe C - 192.168.0.0 - 192.168.255.255 (prefixo 192.168/16);

Os endereços IPv4 foram divididos em 3 classes, de A até à C. A Classe A consigna o octeto mais significativo para os endereços de rede e os restantes 3 octetos para os endereços de terminais, a Classe B consigna os dois octetos mais à esquerda para os

endereços de rede e os restantes para os endereços de terminal, a Classe C consigna os três primeiros octetos para os endereços de rede e o último para endereços de terminais.

O problema surgiu quando muitas redes começaram a necessitar de blocos de endereços maiores do que uma classe C, e portanto, eles passaram a receber um bloco de endereços de classe B, que era muito maior do que o necessário. Com o rápido crescimento da Internet, o espaço de endereços de classe B rapidamente tornou-se insuficiente.

Em 1985, foi planeado um método para subdividir redes IP que se tem revelado flexível, e que usa uma máscara de sub-rede de comprimento variável (VLSM - *variable-length subnet mask*) (Mogul & Postel, 1985).

2.3 IPv6

No final dos anos 90 foi criado o IPv6 com a RFC 2460 (Deering & Hinden, 1998) com a intenção de resolver vários problemas do IPv4, entre eles a falta de endereços públicos. O IPv6 é constituído por 128 bits em vez dos 32 do IPv4 e destaca-se entre muitos outros aspectos pela dispensa da utilização do NAT e a introdução do protocolo de segurança IPSec como obrigatório, o que no IPv4 era opcional. A quantidade de endereços disponíveis pode chegar a 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços o que equivale a aproximadamente 665.570.793.348.866.943.898.599 endereços por metro quadrado da superfície do nosso planeta.

Outra das alterações significativas do protocolo IPv6 é o facto de deixarem de existir os endereços *broadcast*, sendo a sua função substituída pelos endereços *multicast.* Os modos de comunicação são então caracterizados do seguinte modo (Hinden & Deering, 1998):

- *Unicast* - identifica apenas uma única interface de rede. Um pacote enviado para um endereço *unicast* é entregue apenas à interface identificada por esse endereço;
- *Multicast* - identifica um conjunto de interfaces, que tipicamente pertencem a diferentes nós. Um pacote enviado para um endereço *multicast* é entregue a todas as interfaces identificadas por esse endereço;
- *Anycast* - tal como um endereço *multicast*, identifica um conjunto de interfaces, embora neste caso um pacote enviado para este tipo de endereço é entregue à interface ”mais próxima” identificada por esse endereço, de acordo com o protocolo de encaminhamento.

Os endereços passam a ser representados por números hexadecimais de 16 *bits,* separados por “:”, sendo indiferente representar as letras com maiúsculas ou minúsculas, e algumas abreviações são possíveis, como a omissão de zeros à esquerda e a

representação de um conjunto contínuo de zeros por "::" apenas uma vez em cada endereço.

Os endereços IPv6 são escritos em oito grupos de quatro dígitos hexadecimais (exemplo: 2001:0db8:85b3:1319:8c2e::0370:7344).

A expectativa tem sido que o IPv6 substitua gradualmente o IPv4, verificando-se que as duas versões coexistam durante o longo período de transição (Domingos , 2011).

2.3.1 IPv6 em Portugal e no mundo

Em Portugal a adopção do IPv6 ainda está um pouco aquém dos países mais desenvolvidos do mundo. Apesar de ter ainda um baixo valor a tendência será de aumentar nos próximos anos assim como no resto do mundo, porque o IPv6 vai ser o futuro da *Internet*.

Todas as redes da Tabela 1 dispõem de prefixos IPv6, onde a quantidade está expressa em múltiplos de prefixos /32, onde por exemplo a RCTS (Fundação para a Ciência e a Tecnologia, I.P.) usa o seu espaço para fornecer prefixos /48 a cada Universidade/Politécnico/Laboratório ligada/o à sua rede. Empresas como o caso das principais operadoras MEO, NOS e Vodafone podem utilizar os seus prefixos para fornecer acesso IPv6 aos seus clientes. Para fazer isso apenas terão de ser criadas sub-redes a partir dos prefixos de que dispõem. A Tabela 1 mostra as empresas Portuguesas com endereços IPv6 em Portugal em Outubro de 2016.

Tabela 1 – Organizações em Portugal com prefixos IPv6 (RIR, 2016).

NOME	Número de endereços IPv6 /32
MEO - SERVICOS DE COMUNICACOES E MULTIMEDIA S.A.	32
100 LIMITE - SERVICOS DE INTERNET ONLINE Lda	8
APDL - Administração dos Portos do Douro, Leixões e Viana do Castelo, S.A.	8
Associação DNS.PT	8
Associação Porto Digital	8
EDP - Energias de Portugal, S.A.	8
Entidade de Serviços Partilhados da Administração Publica, I.P.	8
Estoril Sol Digital, Online Gaming Products And Services, S.A.	8
European Maritime Safety Agency	8
Eurotux Informática S.A.	8

Fundação para a Ciência e a Tecnologia, I.P.	8
INESC - Instituto de Engenharia de Sistemas e Computadores PCUP	8
João Carlos de Almeida Silveira trading as Bitcanal	8
MIGUEL GONCALVES UNIPESSOAL Lda	8
Novabase IMS-Infrastructures & Managed Services S.A.	8
Nuno Caria, Unipessoal Lda	8
Nuno Felgueiras	8
RSIL, Lda	8
SAMPLING LINE-SERVICOS E INTERNET, Lda	8
STV - SOCIEDADE DE TELECOMUNICACOES DO VALE DO SOUSA, S.A.	8
Vodafone Telecel, Comunicações Pessoais, S.A.	8
Widespace, Lda	8
Claranet Portugal Telecomunicacoes S.A.	4
NOS COMUNICACOES, S.A.	3
AllTele Lda	1
ALMOUROLTEC SERVICOS DE INFORMATICA E INTERNET Lda	1
AR TELECOM - Acessos e Redes de Telecomunicacoes, S.A.	1
BLU, S.A.	1
Cabovisão, televisão por cabo, S.A.	1
CiberConceito Informatica e Servicos Unipessoal, Lda	1
Digital Absolut Business - Servidor, Virtualizacao, Cluster, Datacenters e Telecomunicacoes, Lda	1
Dotsi, Unipessoal Lda	1
IP TELECOM, SERVICOS DE TELECOMUNICACOES S.A.	1
Lazer Telecomunicacoes, unipessoal, Lda	1
Make It Simple Consultoria Informática Lda	1
Nanium S.A.	1
NOS Madeira Comunicações, S.A.	1
ONITELECOM - INFOCOMUNICAÇÕES, S.A.	1
Ricardo Rodrigues Charneca	1
Robot Telecomunicações Projectos e Servicos, Lda	1
Verizon Portugal - Sociedade Unipessoal, Lda	1

WebSP - Comercio e Prestação de Serviços Informáticos, Lda	1
WebTuga, Lda	1

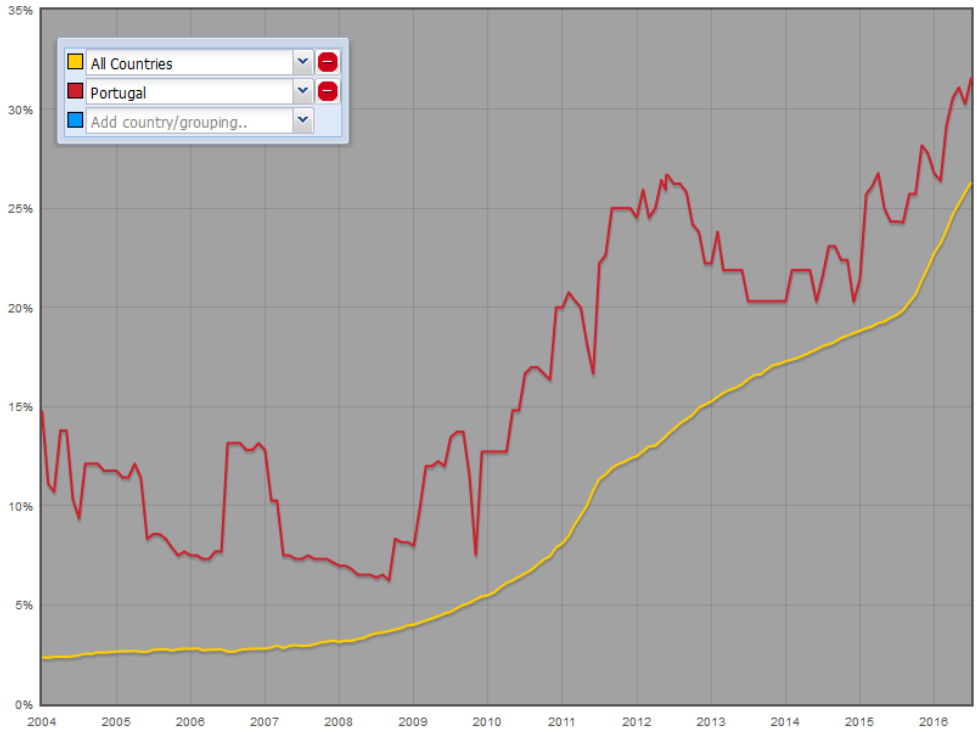


Gráfico 1 – Evolução dos prefixos IPv6 em Portugal *(RIPE, 2016)*.

O Gráfico 1 mostra a evolução das redes IPv6 em Portugal em comparação com o panorama mundial. Tivemos algum recuo em 2013 e 2014, mas actualmente a tendência é de crescimento, uma vez que os endereços IPv4 estão praticamente esgotados e o IPv6 é o único caminho possível para fazer endereçamento público no futuro.

É importante perceber que esta mudança não irá acontecer da noite para o dia e vai ser um processo que irá demorar algum tempo. A expectativa é que o IPv6 substitua gradualmente o IPv4, de tal forma que as duas versões possam coexistir durante o período de transição. No entanto, a implementação do IPv6 a nível mundial está muito aquém do que tinha sido planeado, quando era expectável que antes do esgotamento dos endereços IPv4 a migração avançasse.

2.3.2 Qualidade de serviço (QoS)

Os parâmetros de qualidade de serviço são usados para avaliar não só a qualidade da sessão, mas também o desempenho da rede. Para comunicação em tempo real, o parâmetro mais importante é o atraso (*delay*) porque o seu aumento pode reduzir os níveis de interactividade entre as aplicações do cliente e do servidor. No entanto, a variação do atraso (*jitter*) é também importante, porque um *jitter* elevado, assim como uma perda de

pacotes elevada afecta significativamente a qualidade de experiência do utilizador final, sendo particularmente crítico nas comunicações em tempo real.

2.3.2.1 Atraso (delay)

O atraso define-se como a quantidade de tempo que demora a transmissão de pacotes de um emissor a um receptor, em que a recepção seja bem-sucedida. O atraso deve também considerar o tempo que leva a transmitir o pacote pela rede com recurso à medição da diferença (tempo) entre a transmissão de um pacote pela rede e a recepção, do pacote por um outro *host.*

O atraso pode ser medido em transmissões unidireccionais e bidireccionais. Essa medição poderá ser útil para aplicações de vídeo e voz, ou outras aplicações que utilizem o protocolo UDP, pois uma grande variação do atraso pode causar uma degradação de transmissões de imagem e áudio podendo causar no pior cenário a perda dos pacotes no caso do UDP ou abortar a transmissão por *timeout* no caso de aplicações com o protocolo TCP. O atraso pode ter valores diferentes em cada uma das direcções e que devem ser consideradas. Para medir o atraso é necessário garantir a sincronização do tempo entre o emissor e o receptor.

Uma medição do atraso pode ser efectuada pacote a pacote ou pode ser medido o atraso médio relativo a um conjunto de pacotes.

2.3.2.2 Variação do atraso (jitter)

A variação do atraso é definida como o desvio padrão dos tempos entre pacotes, isto é, se o atraso for constante de pacote para pacote o *jitter* será zero, caso contrário, se os pacotes sofrem atrasos muito variáveis, o *jitter* será positivo. O atraso pode ser algo expectável numa rede, mas a variação do atraso é um indicador de que a rede está com comportamentos instáveis, por exemplo ao nível do reencaminhamento de pacotes, ou por sobrecargas momentâneas dos equipamentos intermédios.

A variação do atraso é uma métrica importante de qualidade de serviço (QoS) para aplicações de voz e vídeo em tempo real, já que grandes variações podem inviabilizar uma comunicação fluída.

2.3.2.3 Perda de pacotes (packet loss)

Quando a rede está sobrecarregada ou não tem capacidade de receber mais pacotes poderá ocorrer a perda de pacotes. Os pacotes são descartados nos *routers*, ou *firewalls* com funções de *router* quando os recursos de transmissão estão congestionados,

ou quando os pacotes atingem o número máximo de transmissões entre *routers* a que podem ser sujeitos.

A perda de pacotes só é detectável a partir da camada 4 do modelo OSI, em particular, com o protocolo Transmission Control Protocol - TCP (Duke, Braden, Eddy, Blanton, & Zimmermann, 2015), ou com protocolos de camada de aplicação (camada 7).

Para detectar a perda de pacotes, o TCP insere um número de sequência no segmento enviado pelo remetente, e desta forma é possível detectar quando um pacote foi perdido ou não entregue com a confirmação por parte do receptor com outro número de sequência. Caso essa confirmação seja um número não sequencial quer dizer que houve perda de pacotes e terão de ser reenviados no caso de uma ligação com recurso ao protocolo TCP.

A perda de pacotes poderá não ser detectada, já que ela decorre de factores que são independentes dos protocolos utilizados. A perda indetectada de pacotes tem impacto especialmente em transmissões de *streaming* de vídeo e voz em tempo real, pois nesses casos a ligação é feita com recurso ao protocolo UDP (Fenner & Flick, 2005) ou RTP (Schulzrinne, Casner, Frederick, & Jacobson, 2003) (ou outros protocolos de camada 4) onde os pacotes perdidos não serão reenviados já que estes protocolos não têm mecanismos para detectar as perdas.

2.4 Mecanismos de transição

Apesar dos protocolos IPv4 e IPv6 não serem conceptualmente diferentes, eles não são compatíveis entre si, e assim, para a transição ser bem sucedida deve ser garantida a possibilidade de comunicação entre máquinas que usem diferentes versões do protocolo. A grande questão que se coloca ao novo protocolo está relacionada com a forma como se irá processar a integração de serviços IPv6 em redes IPv4, as quais podem incluir terminais exclusivamente com acesso IPv6 que necessitam de interagir com serviços apenas disponibilizados em IPv4. Pode dar-se o caso de algumas empresas ou organizações que não tenham iniciado a transição e é necessário comunicar também com estas. Se por um lado os utilizadores irão beneficiar das novas potencialidades introduzidas pelo IPv6, por outro lado é importante que tenham a percepção que os serviços suportados pelo novo protocolo não são piores nem melhores que os serviços suportados pelo seu antecessor. Como foi dito anteriormente, o futuro do IPv6 estará fortemente dependente da capacidade de o integrar com serviços disponíveis nas redes IPv4 existentes sem que existam situações significativas que provoquem qualquer inoperabilidade.

Por esta razão a IETF (Internet Engineering Task Force) (Arkko & Baker, 2011) tem trabalhado em mecanismos específicos para permitir uma transição suave entre o protocolo IPv4 e IPv6. A transição deve ser transparente para os utilizadores finais.

Para que os protocolos IPv4 e IPv6 funcionem em simultâneo existem vários mecanismos, entre os quais:

- Pilha dupla ou camada de IP dupla (*Dual Stack*);
- Túneis IPv6 sobre IPv4 (*Tunneling*);
- Tradução (*Translation*).

Prevê-se que ambos os protocolos funcionem lado a lado ainda durante bastante tempo, mas no futuro o IPv6 substituirá o IPv4 por completo.

2.4.1 Pilha dupla (Dual stack)

Uma configuração em pilha dupla (Nordmark & Gilligan, RFC 4213, 2005), tal como o nome indica, implica a presença das duas pilhas protocolares, uma para cada versão do protocolo IP, na mesma interface de rede executando os protocolos IPv4 e o IPv6 em simultâneo. Quando implementado em *hosts* e *routers* na rede, estes também devem executar ambos os protocolos para que possa existir comunicação.

Um dos pilares fundamentais deste mecanismo é a utilização do serviço DNS. Ao receber endereços IPv4 e IPv6 como resposta a uma *query* DNS, um sistema cliente estará a receber um registo A associado a um endereço IPv4 e um registo AAAA associado a um endereço IPv6 (Thomson, Huitema, Ksinant, & Souissi, 2003).

Muitos sistemas operativos já funcionam em pilha dupla, como por exemplo, Microsoft Windows XP e seguintes e o Windows Server 2003 e seguintes já têm disponível o IPv6.

Esta técnica tem alguns inconvenientes como o facto de manter os dois protocolos em funcionamento em simultâneo, pois poderá trazer alguma complexidade à gestão da rede, afinal passam a existir duas redes em que cada uma tem o seu plano de endereçamento, tabelas de roteamento distintas e regras de *firewall* diferentes.

Esta é a forma mais simples e mais desejável para o IPv4 e o IPv6 coexistirem e é mais provável que venha a ser o próximo passo na evolução das redes em geral, antes de uma transição maior para uma Internet IPv6 que apenas poderá ser alcançada em todo o mundo a longo prazo.

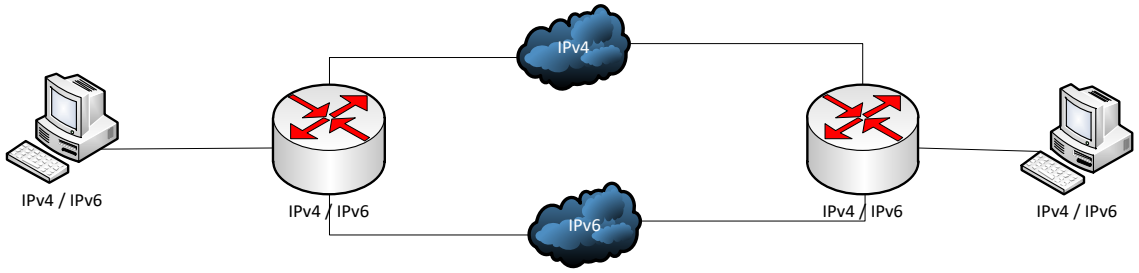


Figura 1 – Mecanismo de Pilha Dupla.

2.4.2 Túneis (Tunneling)

A técnica dos túneis é muitas vezes usada para sobrepor um novo protocolo como o IPv6 sobre uma rede em IPv4, sem necessidade de realizar qualquer mudança nos *routers*, encapsulando o conteúdo do pacote IPv6 num pacote IPv4. Esta técnica também pode ser usada para encapsular pacotes IPv4 em IPv6, sendo que este tipo de túneis irá ser usado numa fase mais avançada da transição quando o protocolo IPv6 estiver implementado na maior parte das redes (Durand, Droms, Woodyatt, & Lee, 2011).

Independentemente do ponto de entrada e de saída dos túneis, ambos os pontos têm de ter um endereço IPv4 e um endereço IPv6. Assim, em qualquer caso, o ponto de entrada e de saída dos túneis têm de ter suporte IPv4 e IPv6.

Os mecanismos de *tunneling* funcionam da seguinte forma:

- Encapsulam os pacotes IPv6 em pacotes IPv4 e vice-versa, o que significa que também podem ser usados para ligações IPv4 sobre redes nativas IPv6, embora ainda existam muito poucas;
- A extremidade de um túnel pede a retransmissão dos pacotes fragmentados, encaminha os pacotes para uma rede IPv6 e o campo *Hop Limit* (correspondente ao campo TTL em IPv4) é reduzido para 1, ou seja, o túnel é “transparente” para o IPv6;
- Os nós que executam o encapsulamento e o desencapsulamento têm de ser nós com pilha dupla, com capacidade de fragmentar e remontar o pacote.

Um processo de encapsulamento poderá provocar fragmentação de pacotes, que ocorre quando é enviado um pacote IPv4 com IPv6 embutido, maior que a Unidade Máxima de Transmissão (MTU - *Maximum Transmission Unit*) (McCann, Deering, & Mogul, 1996) para o destino. A fragmentação consiste num pacote dividido em pedaços com o tamanho suficiente para ser transmitido. O processo de fragmentação marca os fragmentos do pacote original para que a camada IP do destinatário possa reagrupar os pacotes recebidos, reconstituindo o pacote original.

No IPv6 o MTU encapsulado é menor e a fragmentação de pacotes não acontece nos *routers*, mas sim na origem do tráfego. Quando um *router* determina que determinado pacote ultrapassa o MTU, ele retorna uma mensagem para a origem para que os pacotes sejam fragmentados.

Todo esse processo de fragmentação e reagrupamento (desfragmentação) é realizado de modo automático e transparente sem impacto para os utilizadores (António, 2013).

Os túneis podem ser criados manualmente ou de forma automática, em que os que sejam criados de forma manual requerem intervenção nos dois extremos e portanto um total conhecimento sobre a rede em questão. Os túneis manuais são uma boa solução do ponto de vista de gestão em que se sabe o que está no outro extremo.

Os túneis automáticos não precisam de grandes configurações manuais e podem variar entre os mecanismos 6TO4 (Kuarsingh, Lee, & Vautrin, 2012), ISATAP (Templin, Gleeson, Talwar, & Thaler, 2005), Teredo (Huitema, 2006) e 6RD (Despres, 2010).

A utilização de túneis automáticos é fortemente desaconselhado em cenários que não sejam completamente controlados, pois levantam inúmeros problemas de segurança, tais como ataques onde são enviados pacotes encapsulados falsos enviados por atacantes em redes IPv4.

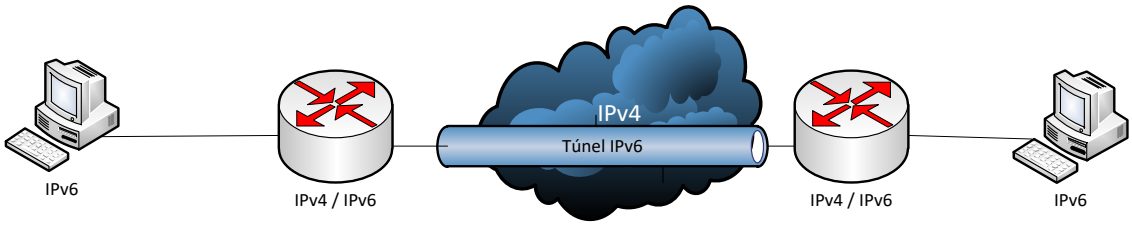


Figura 2 – Mecanismo de Túnel.

2.4.3 Tradução (Translation)

Mecanismos de pilha dupla exigem um investimento enorme para actualizar o equipamento actual ou investir em novos equipamentos, o que para organizações que não tenham essa possibilidade torna a tradução na única solução viável (Baker, 2009).

Os mecanismos de tradução permitem que equipamentos que usem IPv4 consigam comunicar com outros que usam IPv6, e vice-versa por meio da conversão dos pacotes.

São normalmente utilizados para permitir que redes que utilizam o protocolo IPv4 e que não possuam suporte para o protocolo IPv6 consigam comunicar entre si com recurso a um mecanismo complexo de tradução que irá realizar traduções de IPv6 para IPv4 e vice-versa.

São exemplos de métodos de tradução o NAT64 (Bagnulo, Matthews, & Van Beijnum, RFC 6146, 2011) / DNS64 (Bagnulo, Sullivan, Matthews, & Van Beijnum, 2011), NAT-PT (Tsirtsis & Srisuresh, 2000) e SIIT (Nordmark, RFC 2765, 2000).

Figura 3 – Mecanismo de Tradução.

2.4.4 Análise das vantagens e desvantagens dos principais métodos de transição

Tanto os métodos de transição de pilha dupla, túneis e tradução, são boas formas de fazer a transição, mas é importante ter a noção que cada caso é um caso.

À primeira vista o método de pilha dupla seria a melhor opção isto porque funciona com os dois protocolos em simultâneo, mas tem algumas desvantagens como por exemplo o investimento para actualizar os equipamentos e adquirir novos caso seja necessário, onde na aquisição de um novo equipamento o IPv6 deve ser um requisito mandatório.

Para empresas ou organizações que não possuam nenhum endereço IPv4 público e apenas possuam um endereço IPv6 (como é o caso da região da Ásia/Pacífico, servida pelo APNIC, onde já não existem endereços IPv4 públicos para distribuir (Silva R. , 2011)) as técnicas de tradução e túneis são as únicas soluções para comunicar. Estas duas técnicas têm uma clara desvantagem em relação à técnica de pilha dupla que é o atraso provocado na rede pelo encapsulamento dos pacotes e pela tradução.

Com base nas informações a partir da revisão de literatura, testes e pesquisa, foi apresentada uma visão geral de alguns métodos de transição. Cada técnica possui atributos individuais e desempenha um papel importante no processo de transição.

Abaixo está apresentada a tabela que contem as vantagens e desvantagens para os três principais métodos de transição (Nguyen & Nguyen , 2012).

Tabela 2 - Vantagens e desvantagens dos principais métodos de transição.

	Vantagens	Desvantagens
Pilha Dupla	- Fácil de implementar; - Redes podem comunicar com redes IPv4 e IPv6 directamente; - Mais rápido que os métodos	- Duas tabelas de roteamento, o que irá consumir mais memória nos *routers* e computadores; - Pode requerer algum investimento caso os

	de transição de tradução e túneis, pois os pacotes são transferidos directamente;	equipamentos existentes não suportem o IPv6; - A resposta aos pedidos do DNS (A ou AAAA), podem afectar o desempenho da rede; - Políticas de segurança e de *firewall* têm de ser duplicadas para os protocolos IPv4 e IPv6;
Túneis	- Basta configurar os *endpoints*; - Não necessita de gestão adicional;	- Os pacotes são encapsulados, o que irá causar lentidão e atrasos na entrega, para além de baixar o MTU; - Maior utilização do CPU, pois o processo de encapsulamento gera mais esforço no CPU; - Os túneis automáticos levantam sérias questões de segurança, difíceis de mitigar como ataques de spoofing, ataques distribuídos, etc…
Tradução	- Permite que redes em IPv4 comuniquem com redes IPv6 e vice-versa sem *update* dos equipamentos; - Resolve facilmente o problema da incompatibilidade dos protocolos;	- Os pacotes precisam de ser traduzidos, o que causará lentidão e atrasos na entrega; - Escalabilidade, de um ou mais sistemas destinados a realizar as traduções, que normalmente têm uma complexidade elevada.

2.5 Ferramentas de geração e medição de tráfego de rede

Foi realizado um estudo sobre as diversas ferramentas de geração e medição de tráfego de rede em redes IP, visando identificar quais as mais utilizadas e as suas funcionalidades.

Depois de uma pesquisa sobre estas ferramentas no portal IEEE Explore (IEEE, 2016) foi reunida uma lista dos geradores de tráfego ao nível da popularidade que é apresentada no gráfico 4. Nesta lista de geradores de tráfego de rede destacam-se o Iperf (Tirumala, Qin, Dugan, Ferguson, & Gibbs, 2003), Netperf (Jones, Rick - Hewlett-Packard,

1996), MGEN (NRL - Naval Research Laboratory, 2015), D-ITG (Avallone, Pescapè, & Ventre, 2003) e Ostinato (Srivats, 2010).

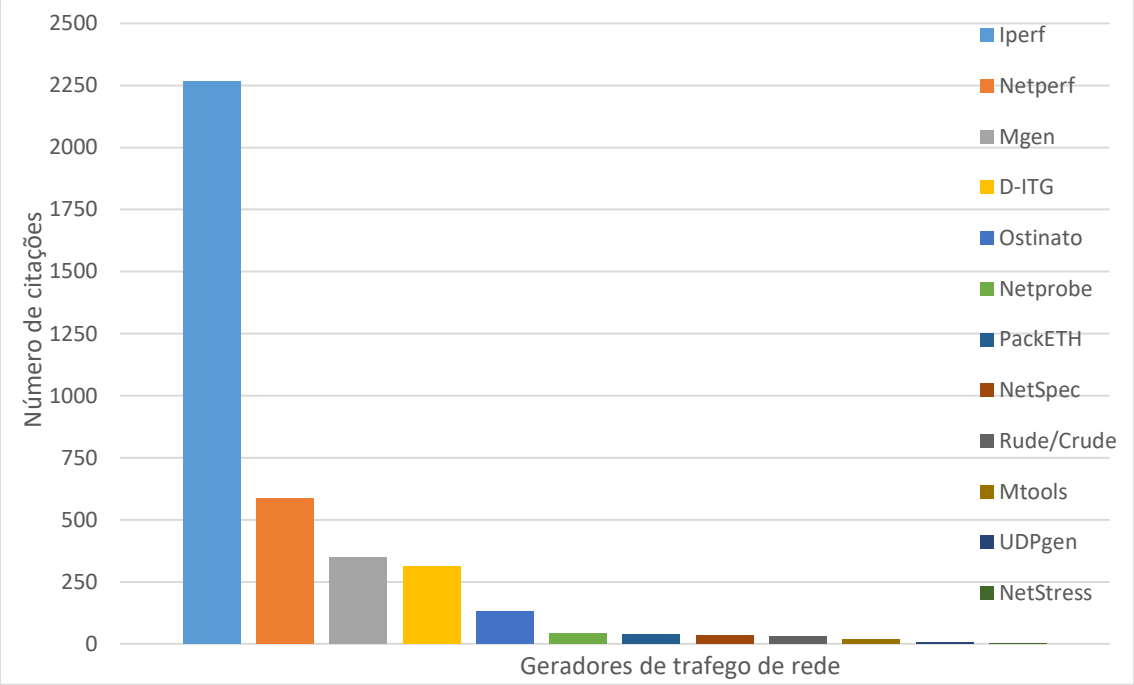


Gráfico 2 – Geradores de tráfego com maior número de citações *(IEEE, 2016)*.

As ferramentas de geração e medição de rede são importantes para a análise de desempenho da rede. A escolha da ferramenta ideal varia de acordo com o que é pretendido medir e da forma como queremos apresentar os dados. Nesta secção irão ser discutidos os cinco geradores de tráfego de rede com melhor cotação na pesquisa efectuada.

2.5.1 Iperf

O Iperf (Tirumala, Qin, Dugan, Ferguson, & Gibbs, 2003) é uma ferramenta *open-source*, desenvolvida pela *Distributed Applications Support Team* (DAST) no laboratório nacional de investigação de rede aplicada (NLANR) da universidade de Illinois e está disponível para os sistemas operativos Windows (Gates & Allen, 1985), Linux (Torvalds, 1991), Mac OSX (Apple, 2001), FreeBSD (FreeBSD-Project, 1993), Android (Google, 2008) e iOS (Apple, 2007).

Esta ferramenta é utilizada para a avaliação de desempenho de tráfego TCP, UDP e SCTP, onde é possível realizar várias medições estatísticas como largura de banda (*bandwidth*), variação do atraso (*jitter*) e perda de pacotes (*packet loss*), gera também um relatório da quantidade de dados transferidos. Embora o Iperf seja uma ferramenta de

geração de pacotes e análise de desempenho que funciona em linha de comandos, existe também uma versão gráfica do Iperf, chamada Jperf (Lattner, Cook, & Gibbs, 2003), desenvolvida em Java.

O Iperf permite ao utilizador ajustar vários parâmetros TCP/UDP que podem ser usados para o teste na rede, além disso, o Iperf é capaz de lidar com múltiplas transferências paralelas e segue o modelo cliente-servidor. Esta ferramenta está projectada para funcionar com IPv4 e IPv6 (Silva & Júnior, 2014) sendo a sua versão mais recente o Iperf3, lançado a 1 de Fevereiro de 2016.

2.5.2 Netperf

O Netperf (Jones, Rick - Hewlett-Packard, 1996). É uma ferramenta *open-source* que pode medir vários aspectos do desempenho da rede. É possível fazer testes de taxa de transferência (*throughput)* e medir a latência onde é verificado o tempo de resposta, utilização do CPU assim como medir o desempenho de transferência de dados analisando os pacotes perdidos, sendo também capaz de apresentar o número de pacotes perdidos (*packet loss*) no caso de o tráfego ser UDP. Contudo esta ferramenta tem uma lacuna que é o facto de não ser possível utilizar o campo ToS para especificar o tipo de tráfego que está a ser gerado.

Esta ferramenta usa os protocolos TCP, UDP, SCTP (Stewart, et al., 2000) e DLPI (Open-Group, 2000), para os protocolos de rede IPv4 e IPv6 e suporta os sistemas operativos Linux e Windows.

Esta ferramenta funciona em modo cliente-servidor composto pelos programas Netperf (cliente) e Netserver (servidor) e pode funcionar tanto em modo gráfico como linha de comandos. A última versão deste *software* é o Netperf 2.7.0 e foi lançada a 1 de Julho de 2015.

2.5.3 MGEN

O Multi-Generator (MGEN) (NRL - Naval Research Laboratory, 2015) é um *software open-source* capaz de gerar tráfego ao nível da camada de rede IPv4 e IPv6, e tráfego TCP e UDP na camada de transporte. O MGEN segue o modelo cliente-servidor, gera tráfego em *unicast*, *multicast* e *broadcast* e permite a alteração do tipo de serviço (ToS) (Nichols, Blake, Baker, & Black, RFC - 2474 - Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, 1998). É possível medir a taxa de transmissão de pacotes por segundo, tamanho dos pacotes, número de pacotes e o tempo da geração de tráfego. O tráfego gerado pode ser recebido e registado para análises utilizando a ferramenta TRPR (NRL - Naval Research Laboratory, 2014). Ao analisar o ficheiro de *log* com o TRPR é

possível analisar as estatísticas de desempenho da taxa de transferência (*throughput*), atraso (*delay*), variação do atraso (*jitter*) e pacotes perdidos (*packet loss*). Nessa análise é exibida a origem e o destino do fluxo, o número de pacotes recebidos tal como a taxa média, máxima e mínima de atraso (*delay*).

Podem ser gerados vários fluxos de tráfego (constante, periódico, *Poisson*, *Burst* e incremental).

Actualmente o MGEN é suportado pelos sistemas operativos Linux, Mac OSX, Windows e FreeBSD e a sua última versão foi lançada a 16 de Abril de 2015 com o nome MGEN 5.0.

2.5.4 D-ITG

O *Distributed Internet Traffic Generator* (D-ITG) (Avallone, Pescapè, & Ventre, 2003) é um gerador de tráfego *open-source* desenvolvido pela Universidade Frederico II em Nápoles. Actualmente disponível nas plataformas Windows, Mac OSX, FreeBSD e Linux com linha de comando e interface gráfica (Semken, 2004).

O D-ITG produz vários tipos de tráfego de acordo com várias distribuições de probabilidade (constante, exponencial, uniforme, *Pareto*, *Cauchy*, normal, *Poisson* e *Gamma*) para as variáveis *packet per second* e *packet size*, onde é possível alterar o tamanho do pacote e o número de pacotes a gerar para os protocolos IPv4 e IPv6 (Botta, Donato, Dainotti, Avallone, & Pescapè, 2013).

Suporta os protocolos de transporte TCP, UDP, SCTP, DCCP (Kohler, Handley, & Floyd, 2006) e replica tráfego ICMP (Postel, 1981), DNS (Mockapetris, 1983), Telnet (Postel & Reynolds, 1983) e VoIP (Uzelac & Lee, 2011) com *Voice Activity Detection* (VAD) (Ramirez, Górriz, & Segura, 2007) e *Compressed* RTP (Casner & Jacobson, 1999) fornecendo resultados próximos de uma experiência real. O tamanho dos *codecs de VoIP* é fixo e não pode ser alterado, contudo é possível gerar vários fluxos de tráfego VoIP em simultâneo tal como de outros tipos de tráfego. A Tabela 4 descreve os tipos de *codecs* suportados e as suas características.

O D-ITG realiza medições numa direcção (*one-way-delay*) e tempo de ida e volta (*round trip time*), onde é possível medir a variação do atraso (*jitter*), atraso (*delay*) onde é possível calcular três tipos de atraso (mínimo, médio e máximo), perda de pacotes (*packet loss*), tempo de transmissão e número de pacotes transferidos. Para realizar uma medição de tráfego numa direcção (*one-way-delay*) e tempo de ida e volta (*round trip time*) é necessária a sincronização do tempo usando o protocolo NTP entre o cliente e o servidor.

Permite também a definição dos campos de tipo de serviço (ToS/DS) e o número de saltos entre máquinas (TTL) (Agarwal & Akyol, 2003).

É possível reproduzir condições de rede complexas sob diferentes cargas e configurações de tráfego com a possibilidade de armazenar a informação tanto da origem como destino num ficheiro de *log*. (Botta, Donato, Dainotti, Avallone, & Pescapè, 2013)

Esta ferramenta consiste em cinco componentes: ITGSend, ITGRecv, ITGLog, ITGDec e ITGManager. A Figura 4 mostra uma visão geral da relação entre os componentes.

Tabela 3 – *Codecs* VoIP suportados pelo D-ITG e suas especificações (Alessio, Alberto, & Antonio, 2009).

CODECs	Amostras	Tamanho do pacote (Bytes)	Pacotes por segundo
G.711.1	1	80	100
G.711.2	2	80	50
G.723.1	1	30	26
G.729.2	2	10	50
G.729.3	3	10	33

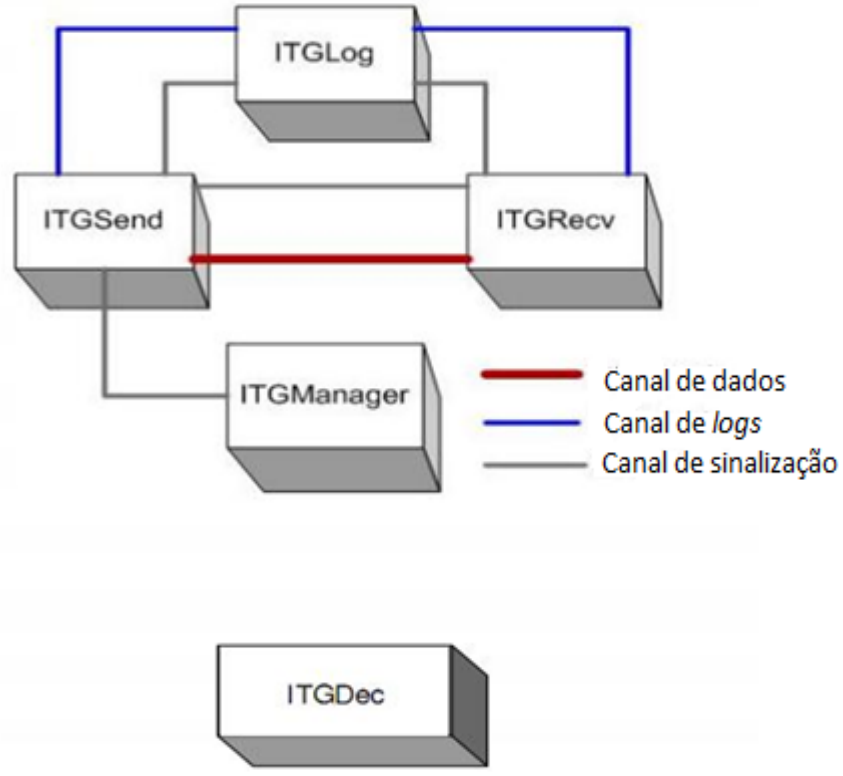


Figura 4 – Arquitectura do *software* D-ITG (Adaptado de (Pescapè, Avallone, Guadagno, & Emma, 2004)).

Esta ferramenta segue o modelo cliente-servidor, onde o ITGSend é o emissor (cliente) que pode gerar um único fluxo de tráfego ou múltiplos fluxos, tendo a possibilidade de ser remotamente controlado pelo componente ITGManager. O ITGRecv actua como servidor para receber os dados. Ambos geram ficheiros de *log*, onde a informação é armazenada localmente ou remotamente usando o ITGLog que é um servidor de *logs*. Finalmente, com o uso do ITGDec é possível analisar os resultados a partir dos arquivos de *log* gerados pela origem (ITGSend) e pelo destino (ITGRecv). É o ITGDec quem calcula os valores médios da taxa de transmissão, atraso e variação do atraso e perda de pacotes de toda a transmissão. A última versão do D-ITG é a 2.8.2-r2717, lançada no dia 21 de Março de 2016.

2.5.5 Ostinato

Ostinato (Srivats, 2010) é uma ferramenta *open-source* de geração e medição de tráfego com interface gráfica. Está disponível para os sistemas operativos Linux, Mac OSX, FreeBSD e Windows. Os protocolos suportados pelo Ostinato são IPv4, IPv6, TCP, UDP, ICMPv4, ICMPv6, e outros protocolos, como HTTP, RTSP, SIP, NNTP. Suporta também os Túneis (6over4, 4over6, 4over4, 6over6). Funciona com a arquitectura cliente-servidor e pode criar e configurar fluxos sequenciais e intercalados de diferentes protocolos em taxas diferentes. Possui flexibilidade para adicionar qualquer protocolo ainda não implementado. A última versão desta ferramenta é o Ostinato 0.7.1 lançado no dia 16 de Junho de 2015.

2.6 Trabalhos relacionados

Depois de realizada uma pesquisa sobre o tema a abordar, nos motores de busca *Google Scholar* e *IEEE Xplore* é possível concluir que a análise de desempenho das redes ainda está por explorar em alguns campos.

Não foram encontrados trabalhos que respondam na totalidade ao problema colocado neste trabalho, no entanto foram encontrados outros estudos que, devido ao seu conteúdo, estão relacionados com o problema colocado.

O objectivo desta secção é apresentar trabalhos relacionados ao tema a abordar. Serão descritas pesquisas cujo foco corresponda à análise de desempenho utilizando o protocolo IPv4 ou IPv6.

2.6.1 Evaluation and Comparations of Migration Techniques From IPv4 to IPv6 Using GNS3 Simulator (Al-Gadi, Mustafa, & Hamied, 2014)

Este artigo discute as técnicas de migração de IPv4 para IPv6, com recurso ao simulador GNS3 para simular as três técnicas usadas na transição para IPv6 (Pilha dupla, túneis e tradução). Os autores neste trabalho mostram as bases do protocolo IPv6, a migração da rede com o *software* GNS3 para simular os três métodos de transição em 3 redes distintas sendo que nesta simulação para a transição com a técnica de túnel foi utilizada a técnica GRE e para o método de tradução foi utilizado o NAT-PT. O *software Solarwinds* foi utilizado para efectuar a análise do tráfego de pacotes entre os múltiplos nós e para medir o desempenho da rede em cada um dos métodos de transição de acordo com os três parâmetros (latência, perda de pacotes e tempo de resposta).

Os autores com o programa *Solarwinds* concluíram que o tempo de resposta é diferente em todas as redes montadas. Nesta análise o tempo de resposta na rede com a passagem com o túnel foi de 36ms, pilha dupla 283ms e tradução de 800ms. Este resultado mostra que o elevado tempo de resposta resulta numa maior latência (atraso médio), onde a tradução obteve a latência mais elevada e com bastantes perdas de pacotes muito por culpa do seu sistema de tradução, seguido da pilha dupla e com o valor mais baixo o túnel onde não foi registada perda de pacotes.

Como conclusão final os autores concluíram que nesta simulação com as três técnicas ainda que em ambiente virtual e talvez os resultados tenham sido influenciados pelo ambiente de virtualização, o método de transição com recurso a túneis apresenta melhores resultados tanto em latência, perda de pacotes e tempo de resposta.

2.6.2 Network Performance Evaluation of 6to4 Tunneling (Bahaman, Erman, & Prabuwono, 2012)

Este artigo centra-se na avaliação de desempenho do mecanismo de transição de túnel 6to4. Os autores fizeram testes no sentido de realizar uma comparação das taxas de transferência de dados em TCP e UDP, medir o tempo de ida e volta (RTT - *round trip time*) também no protocolo de transmissão TCP e UDP e medir a sobrecarga no túnel.

Para esta experiência os autores criaram três cenários, onde foi criado um túnel 6to4 e duas redes nativas em IPv4 e IPv6 de forma a serem feitas análises de desempenho dos protocolos TCP e UDP. Para fazer a avaliação nesta comparação foram utilizados os *softwares D-ITG* para gerar tráfego TCP e UDP e o *WireShark* 1.2.6 para visualizar os pacotes na rede.

Após a execução dos testes por várias vezes de forma a assegurar a precisão dos dados, os autores concluíram que a comparação das métricas definidas entre o mecanismo de túnel e as redes IPv4 e IPv6, mostrou que o túnel tem um aumento de sobrecarga, taxas de transferência baixas e de tempo de ida e volta alto em comparação com os outros dois cenários, foi também constatado que quando o tamanho dos pacotes aumenta, a taxa de transferência diminui para metade no protocolo TCP. Já no protocolo UDP a transmissão de dados no túnel não afecta o desempenho, sendo os resultados semelhantes ao dos dois protocolos.

Como conclusão o desempenho do mecanismo de túnel é mais baixo em cerca de 50% do que nos dois cenários de ambientes nativos IPv4 e IPv6 no protocolo de transmissão TCP. Isto acontece porque os pacotes com o protocolo TCP geram maior volume de tráfego. Com os resultados obtidos os autores concluíram que o método de transição 6to4 não é um método adequado, onde ficou demonstrado que a capacidade de transmissão de dados com TCP é reduzida, este resultado pode ter sido influenciado pelo facto dos *routers relay* utilizados terem pouca capacidade ou encontrarem-se sobrecarregados na altura da experiência. No entanto o mecanismo 6to4 é uma boa hipótese para uma implementação na fase inicial da transição de IPv4 para IPv6.

2.6.3 *Performance Analysis of IPv4 v/s IPv6 in Virtual Environment Using UBUNTU* (Shiwani, Purohit, & Hemrajani, 2011)

Este artigo foca a análise de desempenho em redes IPv4 e IPv6 no sistema operativo Ubuntu 10.0.1 numa infra-estrutura virtual com o *sotfware* VMWare, onde o Ubuntu foi configurado com as duas versões do IP de forma a verificar as diferenças de desempenho. As métricas de desempenho avaliadas foram a taxa de transferência (*throuhgput*) e a variação do atraso (*jitter*) para três diferentes tamanhos de largura de banda (*Kbyte/s*, *Mbyte/s* e *Gbit/s*). Para esta expêriencia os autores utilizaram a ferramenta Iperf 2.0.4 e o Jperf 2.0.2 para geração e medição de tráfego em TCP e UDP.

Foram realizadass três experiências em simultâneo de 30 segundos cada uma para cada um dos protocolos, com diferentes larguras de banda (*Bandwidth*).

Os resultados apurados pelos autores estão representados na tabela 4 e 5, onde de acordo com a tabela 4 que representa a experiência com o protocolo TCP é verificado que as taxas médias de transferência em IPv6 aumentam quando a largura de banda é definida em *Kbytes* e *Mbytes* comparando com as do IPv4, enquanto as taxas de transferência em *GBits* são semelhantes em ambos os protocolos.

Tabela 4 – Largura de banda com o protocolo TCP (Shiwani, Purohit, & Hemrajani, 2011).

Taxa de transferência em TCP	Máximo	Mínimo	Média
IPv4	1200 Kbytes 1.70 Mbytes 0.02 GBits	500 Kbytes 0.40 Mbytes 0.01 Gbits	734.00 Kytes 0.85 Mbytes 0.01 Gbits
IPv6	4000 Kbytes 2.00 Mbytes 0.02 Gbits	525 Kbytes 0.50 Mbytes 0.01 Gbits	1220.00 Kbytes 0.96 Kbytes 0.01 Gbits

Nos resultados da experiência em UDP representados na tabela 5 os autores verificam que os resultados das taxas de transferência são muito semelhantes em ambos os protocolos, sendo que apenas a taxa média de transferência em *Kbytes* foi um pouco superior em IPv6.

Já na variação do atraso os valores são superiores em IPv6, sendo apenas superiores em IPv4 quando a largura de banda foi definida em *Kbytes*.

Tabela 5 – Largura de banda e variação do atraso com o protocolo UDP (Shiwani, Purohit, & Hemrajani, 2011).

Taxa de transferência em UDP	Média de Bytes por segundo	Média de Variação do atraso
IPv4	117 Kbytes 0.12 Mbytes 0.01 GBits	1.48ms 0.60ms 0.15ms
IPv6	121 Kbytes 0.12 Mbytes 0.01 Gbits	0.73ms 1.84ms 0.16s

Como conclusão os autores puderam apurar que as diferenças de desempenho entre os protocolos IPv4 e IPv6 são em média de 486 *Kbytes* e 0.11*Mbytes*, sendo que na escala de *GBits* os tempos são semelhantes em ambos os protocolos. Estes resultados podem ter sido influenciados pelo facto de os testes terem ocorrido em ambiente de virtualização.

Foi também possível concluir que quando a largura de banda é pequena existe uma maior discrepância nos valores e à medida que vai aumentando os valores vão se tornando semelhantes.

De salientar também que as unidades de medida utilizadas no artigo são pouco ortodoxas, uma vez que normalmente em redes utiliza-se Kb/s, Mb/s e Gb/s.

2.6.4 Performance Monitoring of VoIP with Multiple Codecs Using IPv4 and IPv6to4 Tunneling Mechanism on Windows and Linux (Sathu & Shah, 2012)

Neste artigo é analisado o desempenho do protocolo VoIP nos seus cinco diferentes *codecs*, em duas redes distintas, uma com o protocolo IPv4 e outra com o protocolo IPv6 num túnel 6to4, para enviar pacotes IPv6 sobre a rede IPv4 para outra rede IPv6, nos sistemas operativos Windows 7 e Linux Ubuntu 9, onde os autores pretendem medir o atraso (*delay*), variação do atraso (*jitter*) e a taxa de transferência (*throughput*).

Os *CODECs* utilizados nesta experiência foram: G.711.1, G.711.2, G.723.1, G.729.2 e G.729.3.

A ferramenta seleccionada pelos autores para gerar e medir o tráfego foi o D-ITG. Esta ferramenta foi escolhida porque consegue gerar tráfego IPv4 e IPv6, funciona tanto em Windows como Linux e gera tráfego VoIP com os *CODECs* seleccionados para o estudo.

Nos resultados obtidos nesta experiência os autores concluíram que em termos de atraso, o Windows teve sempre o maior tempo de atraso em modo de túnel tendo atingido o seu valor mais alto com o *CODEC* G.711.1 (0.78 ms) seguido do *CODEC* G.711.2 (0.77 ms). Já o Ubuntu registou valores mais baixos, tendo o *CODEC* G.723.1 obtido o valor mais baixo com o protocolo IPv4 com o valor de 0.44 ms.

Em termos de variação do atraso, o sistema operativo Windows teve um melhor desempenho nos *CODECs* e protocolos testados com o *CODEC* G.729.3 a obter os melhores valores em relação à variação do atraso com aproximadamente 0.07 ms em modo de túnel e 0.065 ms em IPv4, a excepção deu-se no caso do *CODEC* G.711.1, onde o túnel 6to4 teve uma variação do atraso (0.2 ms).

Nos resultados relativos às taxas de transferência, o Windows foi melhor em todos os *CODECs* no protocolo IPv4, com o *CODEC* G.711.1 a obter o valor mais alto (687.59 kbps) e o Linux obteve melhores taxas de transferência no túnel 6to4 tendo sido registado também o valor mais alto com o *CODEC* G.711.1 (692.99 kbps).

Considerando que este estudo se destina principalmente a avaliar o desempenho do protocolo VoIP, o atraso e a variação do atraso são os parâmetros mais significativos.

Com base nos resultados verificam-se valores um pouco altos em termos de atraso concluindo-se que a utilização do túnel 6to4 aumentou o atraso em comparação com a rede em IPv4. Este elevado atraso foi provocado devido à necessidade de encapsular os pacotes no emissor e desencapsular do lado do receptor. No entanto os valores de atraso registados estão dentro dos valores razoáveis para que a comunicação em tempo real seja efectiva.

3 Dados da experiência e descrição dos testes

3.1 Rede de investigação e Ensino Portuguesa

A Rede Ciência, Tecnologia e Sociedade (RCTS) "caracteriza-se pelo facto de ser uma rede de alto desempenho para as instituições com maiores requisitos de comunicações, nomeadamente, Universidades, Laboratórios de Estado, Institutos Politécnicos, constituindo-se igualmente como uma plataforma de experimentação para aplicações e serviços avançados de comunicações. Através da RCTS é disponibilizada uma gama alargada de serviços de conectividade e infra-estrutura, suportando diversas aplicações e serviços cobrindo as áreas da colaboração, do conhecimento e da segurança. Esta rede fornece à comunidade de investigadores, professores e alunos portugueses uma plataforma de comunicação avançada, com características específicas para fazer face às exigentes necessidades destes utilizadores" (FCCN, 2016).

A Unidade *FCCN* da Fundação para a Ciência e a Tecnologia I.P. (FCT) que tem como principal actividade o planeamento, gestão e operação da RCTS tem promovido a adopção do protocolo IPv6 há vários anos e dessa forma desde há muitos anos compatibilizou por completo o *backbone* da Rede nacional de investigação e ensino (National Research and Education Network, NREN). Esta organização tem também vindo a procurar constituir-se como um membro de referência na disseminação das potencialidades do protocolo IPv6, através do apoio que tem prestado a vários projectos na temática do IPv6 (Friaças, Domingues, Massano, & Veiga, 2008).

Actualmente a RCTS tem 77 membros, entre eles 24 Universidades, 15 Institutos Politécnicos e 38 são instituições de outro tipo, onde apenas 33 dos membros tem ligação IPv6 (cerca de 43%), funcionado em pilha dupla (Friaças, O Estado do IPv6 na RCTS, 2016).

3.1.1 Características da rede

A FCCN dispõe de diverso endereçamento IPv4 atribuído pelo RIPE/NCC ao longo dos anos (Réseaux IP Européens, s.d.) e um bloco de endereçamento IPv6 com o prefixo 2001:690::/29 (em que um dos prefixos /32 é utilizado pela RCTS) que abrange um total de 2^99 endereços. Por questões de boa prática optou-se por hierarquizar o endereçamento tal como mostra a figura 5, fazendo a atribuição de blocos de endereços /48 a cada membro da RCTS e aconselhando fortemente a utilização de prefixos /64 nas redes locais (LAN).

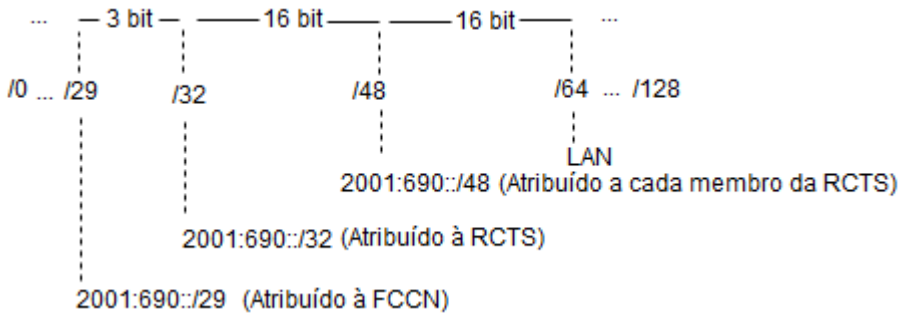


Figura 5 – Divisão do endereçamento da rede da FCCN.

Em termos de ligações, o diagrama da rede RCTS está representado na figura 6 que é composto por dois nós principais, um em Lisboa, e outro no Porto, os quais ligam às restantes instituições do país, com ligações redundantes entre várias capitais de distrito. É possível verificar na figura que existem predominantemente dois tipos de ligação na rede: as ligações em fibra óptica que ligam os principais nós geridos directamente pela FCCN e as ligações baseadas em serviços de comunicações contratados no mercado. A tendência será alargar a cobertura da rede de fibra óptica gerida pela FCCN, uma vez que este tipo de solução confere uma maior capacidade e flexibilidade (FCCN, 2016).

O tráfego em tempo real em IPv4 e IPv6 gerado na rede no dia 08/06/2016 está representado nas figuras 7 e 8. De notar que a altura em que existe mais tráfego é entre as 12h e as 18h, onde o tráfego total de saída da RCTS em IPv4 chega a atingir os 12.26 GB e o IPv6 apenas atinge os 1.05 GB no seu maior pico diário.

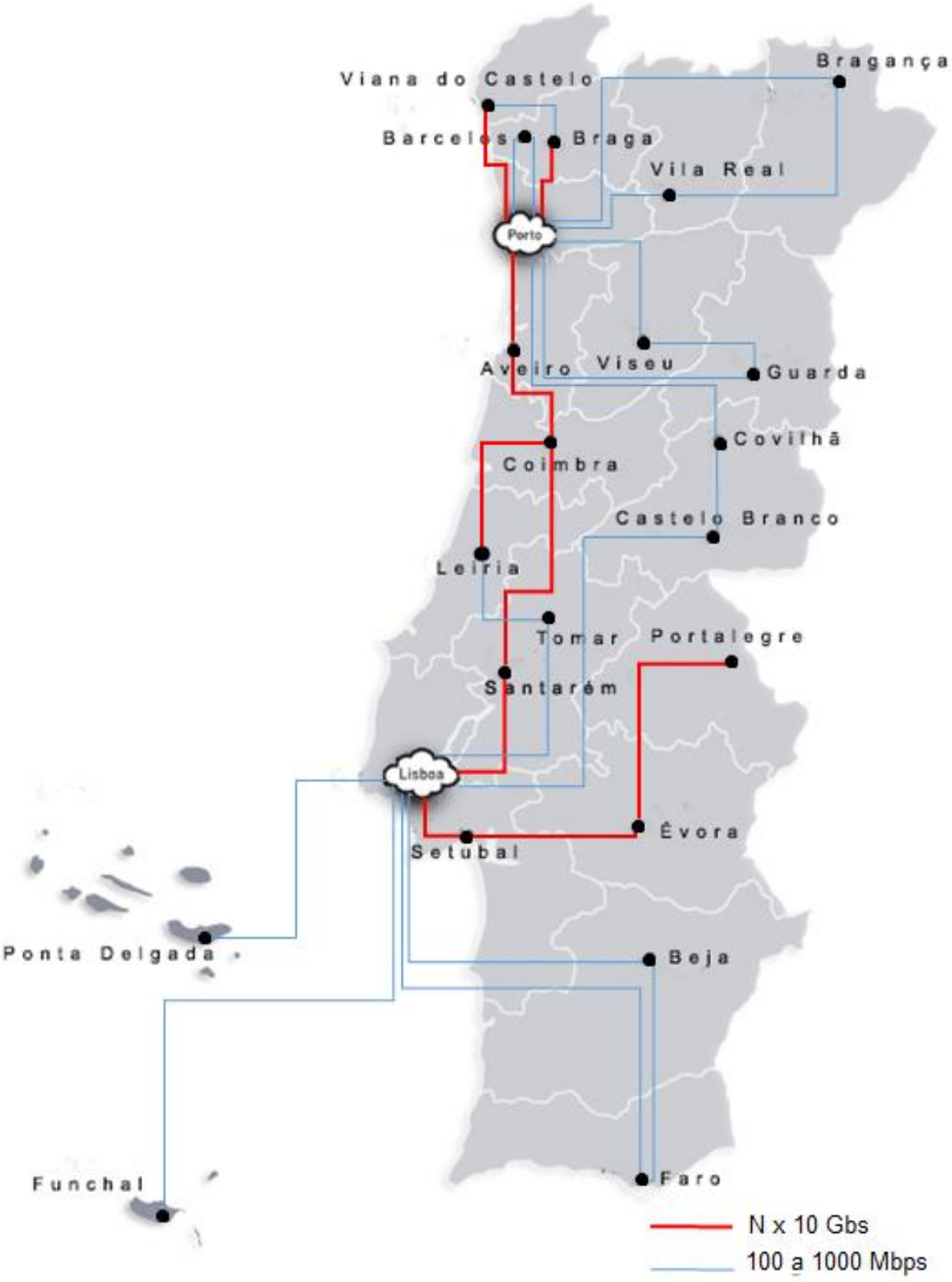


Figura 6 – Diagrama da rede da RCTS em Julho de 2016.

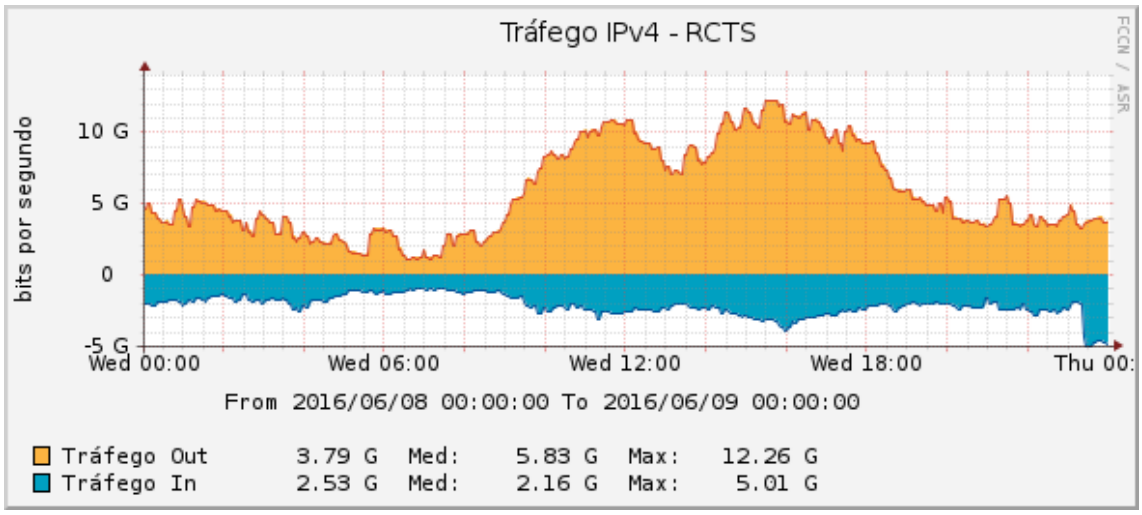


Figura 7 – Tráfego IPv4 (usado com permissão do autor (Friaças, O Estado do IPv6 na RCTS, 2016)).

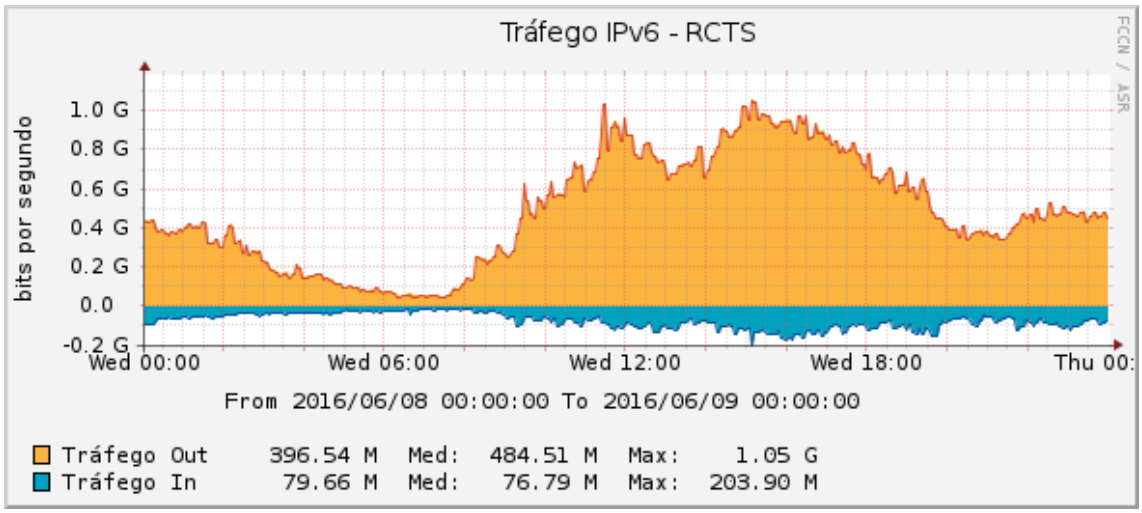


Figura 8 – Tráfego IPv6 (usado com permissão do autor (Friaças, O Estado do IPv6 na RCTS, 2016)).

3.2 Metodologia da experiência

Uma rede é composta por um conjunto de ligações, que pode ser simples ou complexa, usando diferentes tecnologias e protocolos e suportando um ou vários serviços (dados, vídeo, áudio).

Independentemente da arquitectura da rede, para que possa haver comunicação têm de existir protocolos de comunicação tal como os da pilha protocolar TCP/IP (ARPANET, 1983), um conjunto de protocolos compartimentados em camadas, onde cada camada é responsável por um grupo de tarefas. A camada de aplicação é a mais alta desta hierarquia, e lida com dados mais abstractos, estando logicamente mais próxima do

utilizador (Garcia, Taludker, & Jayateertha, 2013). Seguem-se em ordem descendente a camada de transporte, de rede e a camada de acesso à rede.

Figura 9 – Modelo TCP/IP (Cisco Systems, 2013).

Ao utilizar um *software* de injecção de tráfego para realizar medições de qualidade de serviço (QoS) na rede, são activados os protocolos da pilha TCP/IP, com o objectivo de o tráfego injectado na rede ser semelhante ao tráfego gerado por uma aplicação real, como por exemplo uma comunicação *VoIP*.

O *software* D-ITG foi o programa escolhido para a realização desta experiência, visto que permite simular tráfego nas camadas de rede, transporte e aplicação do modelo TCP/IP, nomeadamente tráfego da camada de aplicação *VoIP* entre outros, tráfego da camada de transporte UDP e TCP nos protocolos de rede IPv4 e IPv6 que são pretendidos para a realização desta medição. Este programa pode ser usado para testar as propriedades estatísticas do tráfego com foco na taxa de perda de pacotes, variação do atraso (*Jitter*), taxa de transferência e medição do atraso de ida e volta (RTT). Outro facto que influenciou esta escolha em detrimento de todos os outros *softwares* analisados anteriormente foi o facto de este *software* permitir a alteração do tamanho e número de pacotes de forma a atender aos requisitos dos testes.

Contudo este *software* não tem disponível a simulação de tráfego de s*treaming* (Ozer, 2011), tendo por isso sido necessário recorrer a outras ferramentas para a simulação e análise deste tipo de tráfego.

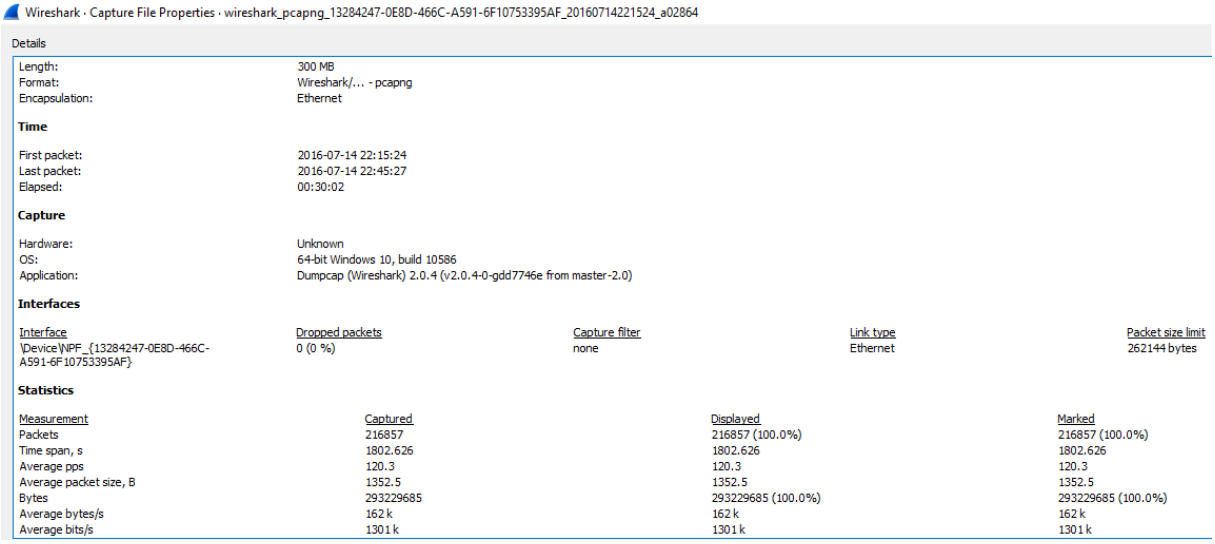
```
Flow number: 1
From 2001:690:2300:2:8fa9:7b5c:f303:ed5:34830
To    2001:690:810:36::2:10001
---------------------------------------------------------
Total time                =   1800.000596 s
Total packets             =         214070
Minimum delay             =       0.000028 s
Maximum delay             =       1.008395 s
Average delay             =       0.018643 s
Average jitter            =       0.017083 s
Delay standard deviation  =       0.107508 s
Bytes received            =      289422640
Average bitrate           =   1286.322419 Kbit/s
Average packet rate       =    118.927738 pkt/s
Packets dropped           =          2470 (1.14 %)
Average loss-burst size   =       1.075784 pkt
---------------------------------------------------------
```

Figura 10 – Exemplo de ficheiro de registo (log) do programa D-ITG.

A metodologia utilizada para medição dos parâmetros necessários para a simulação de tráfego de *streaming*, consistiu em 3 etapas. Para a realização da primeira etapa foi necessário emitir um fluxo de *streaming* com recurso a um ficheiro de vídeo pela rede com o *software Video LAN Client* (VLC) (VideoLAN, 2001), que permite a reprodução de um vídeo em tempo real através das portas HTTP (Berners-Lee, et al., 1999), UDP e RTP, funcionando numa arquitectura cliente-servidor. Esta ferramenta suporta os sistemas operativos Windows, Linux e Mac tal como os protocolos IPv4 e IPv6. Nesta primeira etapa foi gerado um fluxo de s*treaming* entre o *host* emissor e o *host* receptor em IPv4, com o protocolo UDP.

A segunda etapa consistiu em monitorizar o tráfego gerado e rever os resultados. Para esse efeito foi utilizada uma ferramenta de captura de pacotes chamada Wireshark (Combs, 1998), que funciona nos sistemas operativos Windows, OSX, Solaris e Linux. No âmbito desta dissertação, os dados analisados têm como objectivo conhecer os níveis estatísticos da transmissão e o comportamento do tráfego gerado pelo VLC de forma a aplicá-los no D-ITG.

Estes resultados contêm dados que determinam o comportamento estatístico da aplicação, tal como o número de pacotes, tamanho médio dos pacotes, média de pacotes por segundo, número de bytes transferidos, média de bytes por segundo e média de bits por segundo.



Wireshark · Capture File Properties · wireshark_pcapng_13284247-0E8D-466C-A591-6F10753395AF_20160714221524_a02864

Details

Length:	300 MB
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet
Time	
First packet:	2016-07-14 22:15:24
Last packet:	2016-07-14 22:45:27
Elapsed:	00:30:02
Capture	
Hardware:	Unknown
OS:	64-bit Windows 10, build 10586
Application:	Dumpcap (Wireshark) 2.0.4 (v2.0.4-0-gdd7746e from master-2.0)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
\Device\NPF_{13284247-0E8D-466C-A591-6F10753395AF}	0 (0 %)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	216857	216857 (100.0%)	216857 (100.0%)
Time span, s	1802.626	1802.626	1802.626
Average pps	120.3	120.3	120.3
Average packet size, B	1352.5	1352.5	1352.5
Bytes	293229685	293229685 (100.0%)	293229685 (100.0%)
Average bytes/s	162 k	162 k	162 k
Average bits/s	1301 k	1301 k	1301 k

Figura 11 – Exemplo de um ecrã mostrando a captura do tráfego de s*treaming* efectuada pela ferramenta Wireshark.

A etapa final, consistiu em simular a transmissão de dados com o D-ITG, utilizando os parâmetros pacotes por segundo (*Average pps*), tamanho médio dos pacotes (*Average packet size*), a duração da experiência, o protocolo UDP e a opção ToS/DS (*Type of Services* (Almquist, 1992)/ *DiffServ* (Nichols, Blake, Baker, & Black, RFC 2474, 1998)) disponível no D-ITG que é de 136 bits (Babiazrz, Chan, & Baker, 2006) para uma compressão com o protocolo padrão H.323 (ITU-T, 1998). O padrão *(standard)* utilizado nesta simulação foi definido pela ITU-T (*International Telecommunication Union Standardization Sector*) como o protocolo para transmissão em tempo real de áudio, vídeo e dados com base em redes IP.

3.2.1 Definição de métricas da experiência

Os métodos comuns para a medição do atraso dos pacotes são a medição de tempos de ida e volta (RTT - *Round Trip Time*) e a medição de atraso unidireccional (OWD - *One Way Delay*). Usar o método RTT permite a medição do atraso de propagação total, ou seja, o tempo necessário que demora um sinal ser enviado e o tempo que demora a confirmação da recepção do mesmo sinal. Já uma medição do atraso unidireccional fornece um valor que ilustra o tempo necessário para propagar um sinal entre dois pontos numa rede (emissor e receptor). Nesta experiência o parâmetro utilizado para medir o atraso foi o RTT. Esta opção poderá ter o aspecto negativo de não ser 100% fiável em relação ao comportamento da rede, se o dispositivo que recebe a 1ª comunicação e gera a comunicação de retorno adicionar algum atraso significativo, mas numa transmissão de

dados de volume estatisticamente significativo, tem a vantagem de se aproximar mais de uma transmissão bidireccional de dados reais.

Para a realização dos testes foi definido que as simulações de tráfego teriam a duração de 30 minutos, sendo executadas todas em simultâneo em dois momentos distintos, sendo o primeiro em horário laboral (15.30h - 16h) e o segundo em horário pós-laboral (22h – 22.30h) com o objectivo de obter as seguintes métricas de qualidade de serviço:

- Atraso (atraso de ida e volta);
- Variação do atraso;
- Pacotes perdidos;
- Número de pacotes transmitidos;
- Fluxo médio de transferência de bits (*Bitrate*).

Tabela 6 – Características dos tipos de tráfego da experiência.

	Média de pacotes por segundo (pps)	Média de tamanho dos pacotes (*bytes*)
UDP	256	512
TCP	256	512
Streaming H.323	120.3	1352.5
VoIP *codec* G.711.1	100	80

3.3 Especificação dos componentes da experiência

Esta subsecção procura descrever o desenho experimental do ambiente de simulação para este estudo, abrangendo os detalhes de *software* e *hardware*, bem como a topologia da rede utilizada na experiência.

3.3.1 Especificações de *hardware*

Para produzir uma medição de desempenho de rede consistente e precisa foram utilizados dois computadores exactamente iguais com as mesmas caracteristicas bem como os mesmos *drivers*, *i.e.*, mesma marca, modelo e sistema operativo configurado exactamente da mesma maneira. Os detalhes do *hardware* estão representados na tabela 8.

Devido à limitação de recursos de *hardware*, cada computador não pode ter duas placas de rede, sendo necessário no caso da Universidade *Lusófona* de Humanidades e Tecnologias (ULHT) fazer a ligação do cabo IPv6 na placa de rede e o IPv4 com recurso a um adaptador de USB para RJ45 (Anker USB 3.0 to RJ45 Gigabit Ethernet Adapter

Supporting 10/100/1000 bit Ethernet) de forma a minimizar o impacto na largura de banda de rede. Do lado da *Universidade da Beira Interior* (*UBI*) os endereços IPv4 e IPv6 foram configurados no mesmo adaptador de rede (a funcionar em pilha dupla). De referir que esta configuração na ULHT deriva de a conectividade IPv6 ser ainda fisicamente separada da conectividade IPv4. As Figuras 12 e 13 mostram imagens dos dois portáteis, o primeiro instalado na sala de servidores da ULHT (Lisboa) e o segundo instalado na sala de servidores da UBI (Covilhã).

Tabela 7 – Especificações de *hardware*

Hardware	**Detalhe**
CPU	Intel® Core™ i5-3210M CPU @ 2.50GHz × 4
Memoria	4 Gb DDR3 SDRAM
Placa gráfica	Nvidia GeForce GT 610M
Placa de rede	Realtek RTL8111/8168/8411 PCI Express Gigabit Ethernet Controller
Disco rígido	Western Digital Scorpio Blue 1TB, SATA 3.0Gbp/s, 5400RPM
Portas USB	USB 3.0 ports

Figura 12 – Portátil na sala de servidores da ULHT.

Figura 13 – Portátil na sala de servidores da UBI.

3.3.2 Especificações de *software*

Nesta experiência estiveram envolvidos um sistema operativo, dois geradores de tráfego de rede, um emulador de terminais e um analisador de tráfego de rede a fim de

medir o desempenho da rede em alturas distintas. A tabela 8 descreve os detalhes dos componentes de *software* utilizados.

Tabela 8 – Detalhes do Software usado.

Software	**Detalhe / Descrição**
Ubuntu 16.04 64 bits	Sistema operativo
Wireshark 1.12.5	*Sniffer* de tráfego de rede
VLC Media Player 2.2.3	Transmissor de *Streaming*
D-ITG 2.8.2-r2717	Gerador e medidor de tráfego de rede
PuTTY beta 0.67	Emulador de terminais

3.3.3 Topologia da rede utilizada na experiência

A experiência envolveu 2 computadores ligados às redes locais da UBI e ULHT, por sua vez ligadas à RCTS, com cabo de rede CAT6 e duas placas de rede a 1000Mbps. Ambos os equipamentos tinham o sistema operativo Ubuntu 16.04. Nesta topologia a rede da ULHT está ligada a um dos *routers* de Lisboa do backbone da RCTS e a rede da UBI a um dos *routers* do Porto. Tanto o *router* que liga à UBI como o que liga à ULHT não têm ligação directa entre si, existindo vários *routers* entre eles.

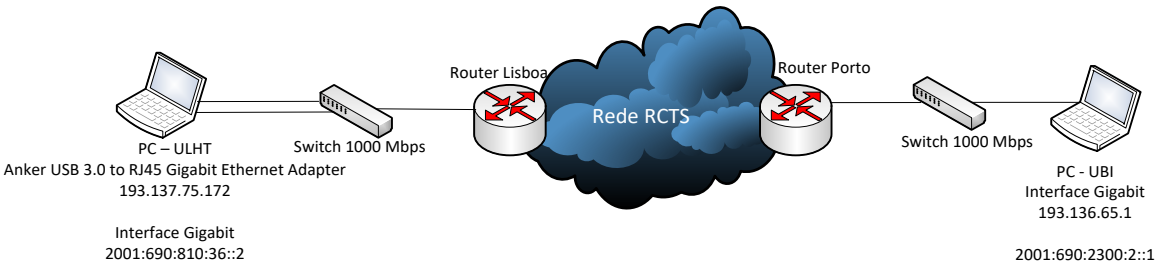


Figura 14 – Topologia utilizada para a experiência.

Na Figura 14 está representada a topologia utilizada, onde em cada ligação existem routers que não são propriedade da RCTS, á excepção da ligação IPv6 da ULHT que está ligado directamente ao router da RCTS.

A rede 2001:690:810:36::/64 tem por objectivo servir de "fronteira" entre o *backbone* da RCTS e a ULHT. Por analogia com a UBI, essa /64 é a rede 2001:690:810:24::/64.

4 Resultados

Este capítulo mostra os resultados da experiência em ambientes distintos, representados através de gráficos e tabelas onde foi possível analisar a performance da rede usando as duas versões do protocolo IP. Esta análise de um troço da rede RCTS com recurso ao *software* D-ITG visou analisar em cada uma das experiências o tráfego de ficheiros com o protocolo UDP, TCP, simulação de tráfego de *streaming* e tráfego de VoIP, sendo que em cada um dos fluxos foi avaliado o atraso (*delay*), variação do atraso (*jitter*) e perda de pacotes (*packet loss*).

Além dos parâmetros anteriores, em cada uma das experiências também foi possível medir:

- Quantidade de pacotes transferidos;
- Atraso médio;
- Variação média do atraso;
- Bytes recebidos;
- Taxa de transferência média;
- Média de pacotes transferidos por segundo;
- Número de pacotes descartados.

4.1 Experiência em horário laboral

A primeira experiência decorreu no dia 21/07/2016 das 15.30h às 16h, onde durante 30 minutos foram executados em simultâneo todos os fluxos de tráfego. Os resultados estão representados através de tabelas com os resumos da transmissão e através de gráficos, onde é possível ver detalhadamente o desempenho dos protocolos.

4.1.1 Tráfego UDP

Nesta experiência com o protocolo UDP foi gerado um fluxo de transferência de 256 pacotes por segundo (pps) onde cada um desses pacotes tem 512 bytes.

Os resultados obtidos na tabela 9 e representados nos gráficos 3 e 4, mostram que o atraso e a variação do atraso foram superiores no protocolo IPv4 onde segundo a tabela 9 o atraso médio em IPv4 foi superior em cerca de 1.675 milissegundos e a variação média do atraso foi superior em 0.669 milissegundos também no protocolo IPv4.

Em contrapartida houve mais pacotes descartados em IPv6 (0.09%), de acordo com a tabela 9 e como se mostra no gráfico 5.

De salientar também que em função das perdas de pacotes por parte do protocolo IPv6 foram transferidos mais 288 pacotes em IPv4, recebidos mais 147456 *bytes* e uma

média de 0.160051 pacotes transmitidos por segundo em IPv4, sendo que a taxa de transferência foi de acordo com a tabela 9 ligeiramente inferior em IPv6, sendo de 1048.2553 Kbit/s em IPv4 e 1047.5998 Kbit/s em IPv6.

Tabela 9 – Resumo do tráfego UDP em horário laboral.

	IPv4	IPv6
Pacotes transmitidos	460658	460370
Atraso médio	0.017008 s	0.015333 s
Variação média do atraso	0.008778 s	0.008109 s
Bytes recebidos	235856896	235709440
Taxa de transferência média	1048.255370 Kbit/s	1047.599801 Kbit/s
Média de pacotes transmitidos	255.921721 pkt/s	255.761670 pkt/s
Pacotes descartados	142 (0.03 %)	430 (0.09 %)

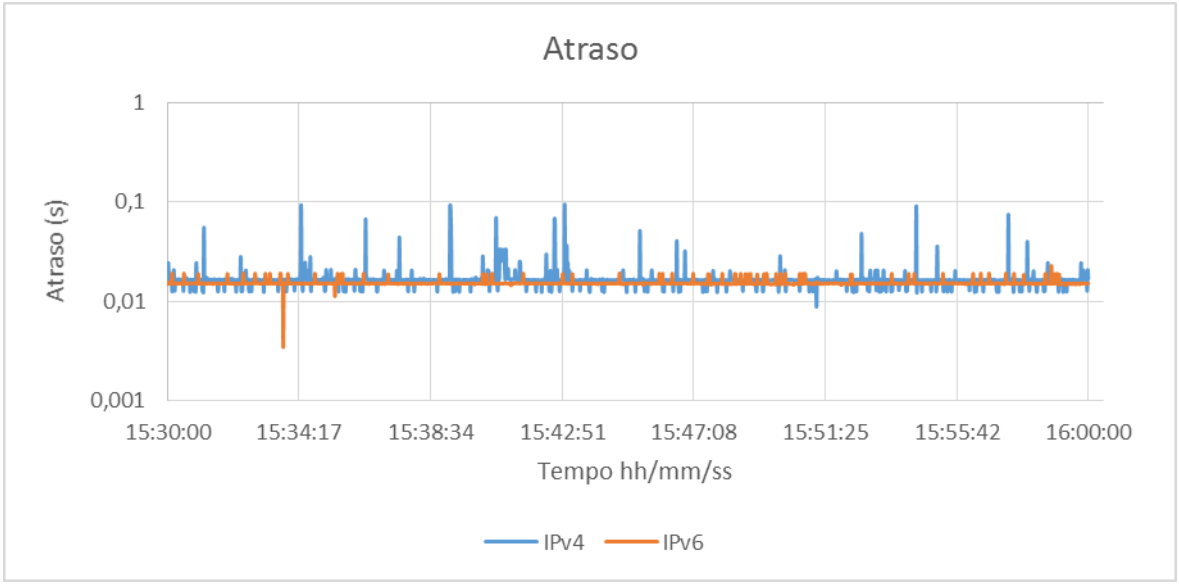


Gráfico 3 – Atraso em segundos do tráfego UDP em horário laboral.

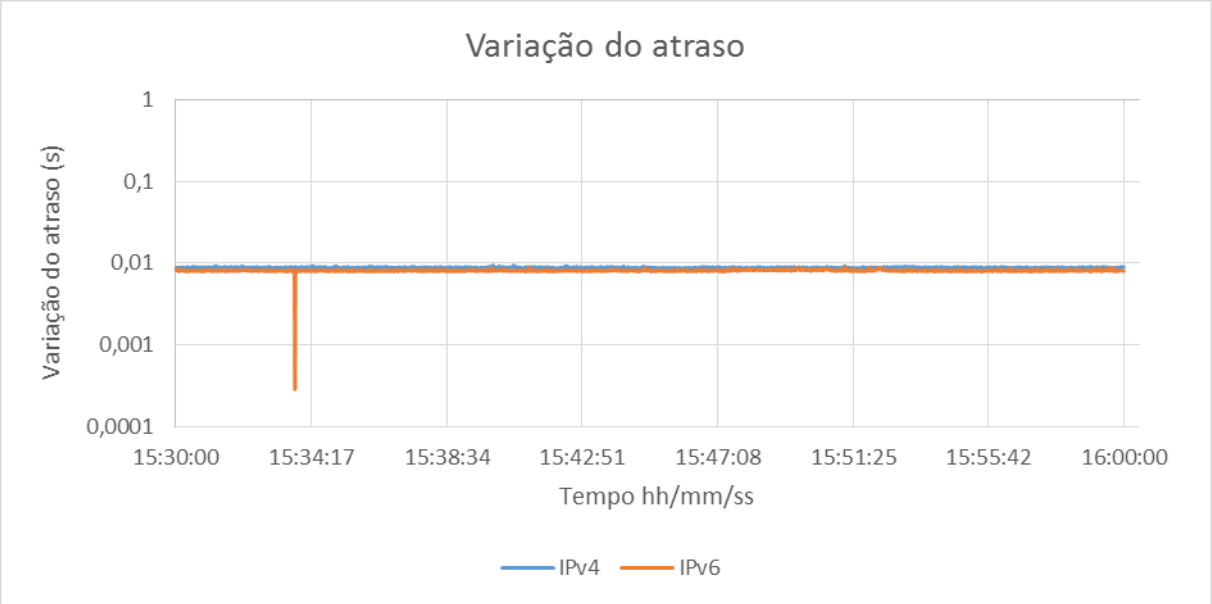


Gráfico 4 – Variação do atraso em segundos do tráfego UDP em horário laboral.

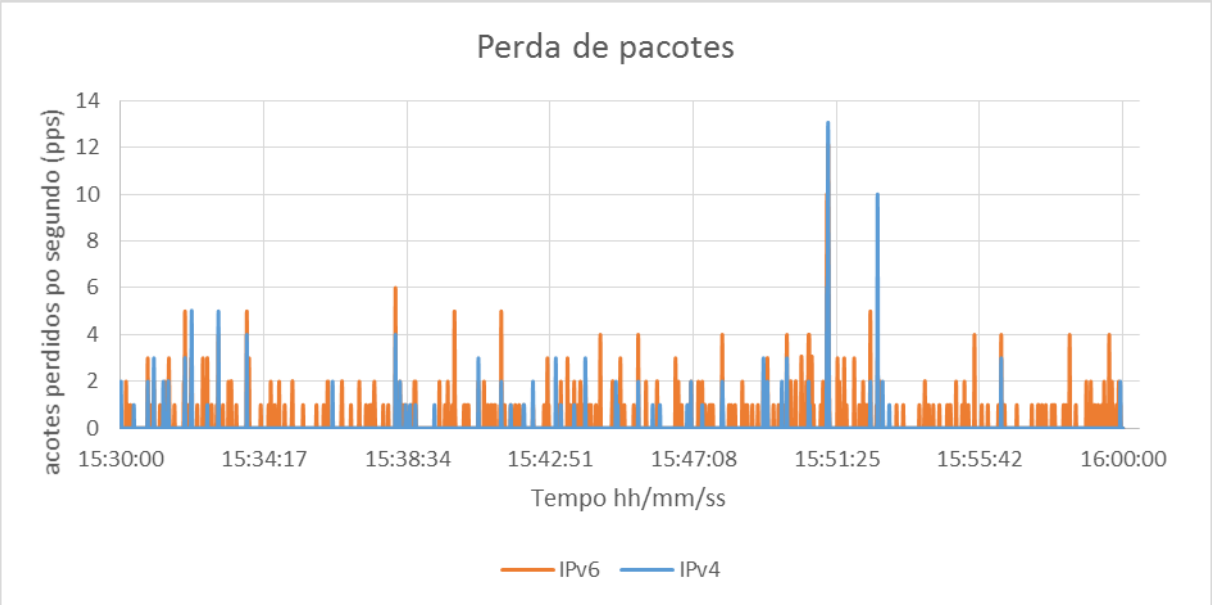


Gráfico 5 – Perda de pacotes por segundo em tráfego UDP em horário laboral.

4.1.2 Tráfego TCP

Nesta experiência com o protocolo TCP, à semelhança da anterior foi gerado um fluxo de transferência de 256 pacotes por segundo (pps) onde cada um desses pacotes tem 512 *bytes.*

Os resultados obtidos nesta experiência, mostram que o atraso foi superior no protocolo IPv4, onde segundo a tabela 10 e o gráfico 6 o atraso médio em IPv4 foi superior

em cerca de 2.049 milissegundos, mas em contrapartida como pode ser verificado no gráfico 7 a variação média do atraso foi ligeiramente superior no protocolo IPv6 em cerca de 1.539 milissegundos segundo a tabela 10.

Não foi registada a perda de pacotes, pois o protocolo TCP garante a entrega de todos os pacotes, com recurso a um "pré-acordo" entre o emissor e o receptor chamado "*Three way handshake*" (SYN, SYN-ACK, ACK), em que todos os pacotes não recebidos pelo receptor sejam reenviados pelo emissor até que sejam recebidos no destino.

De notar também que foram transferidos praticamente o mesmo número de pacotes, onde segundo a tabela 10 foram transferidos mais 3 pacotes em IPv6 e recebidos mais 11536 *bytes* relação ao IPv4. Em relação à média de pacotes transmitidos por segundo a diferença é irrelevante (0.00005 pacotes por segundo) em relação ao IPv4 a uma taxa de transferência média também muito semelhante, apenas 0.206848 bit/s mais rápido em IPv6.

Tabela 10 – Resumo do tráfego TCP em horário laboral.

	IPv4	IPv6
Pacotes transmitidos	460797	460800
Atraso médio	0.021446 s	0.019397 s
Variação média do atraso	0.012229 s	0.013768 s
Bytes recebidos	235928064	235929600
Taxa de transferência média	1048.567781 Kbit/s	1048.567983 Kbit/s
Média de pacotes transmitidos	255.997993 pkt/s	255.998043 pkt/s
Pacotes descartados	0 (0.00 %)	0 (0.00 %)

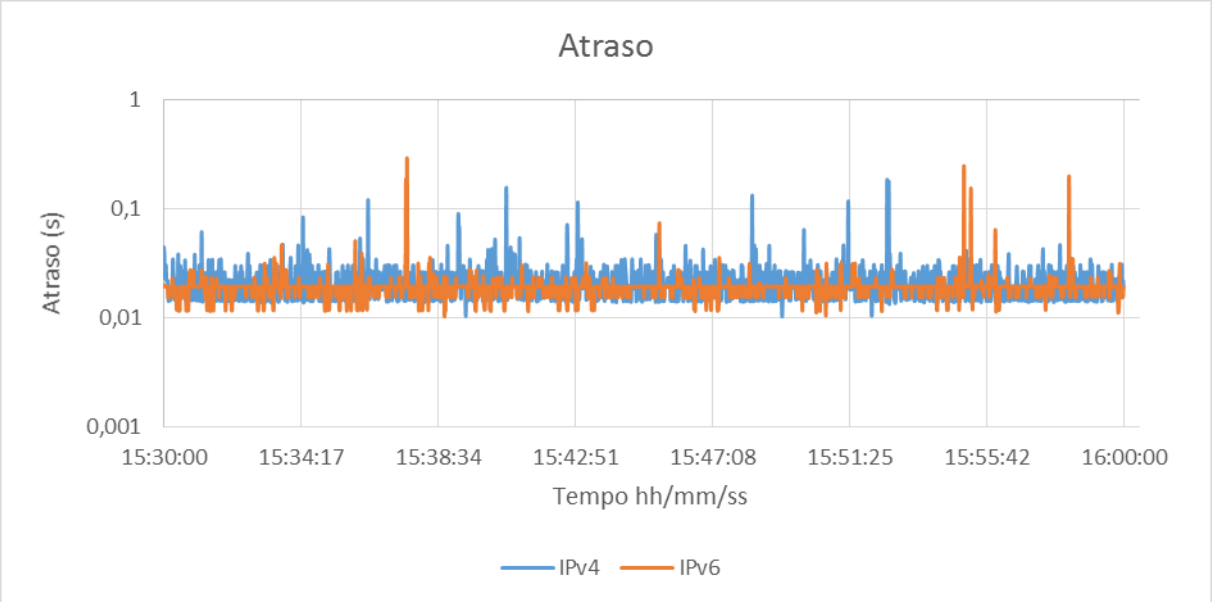


Gráfico 6 – Atraso em segundos do tráfego TCP em horário laboral.

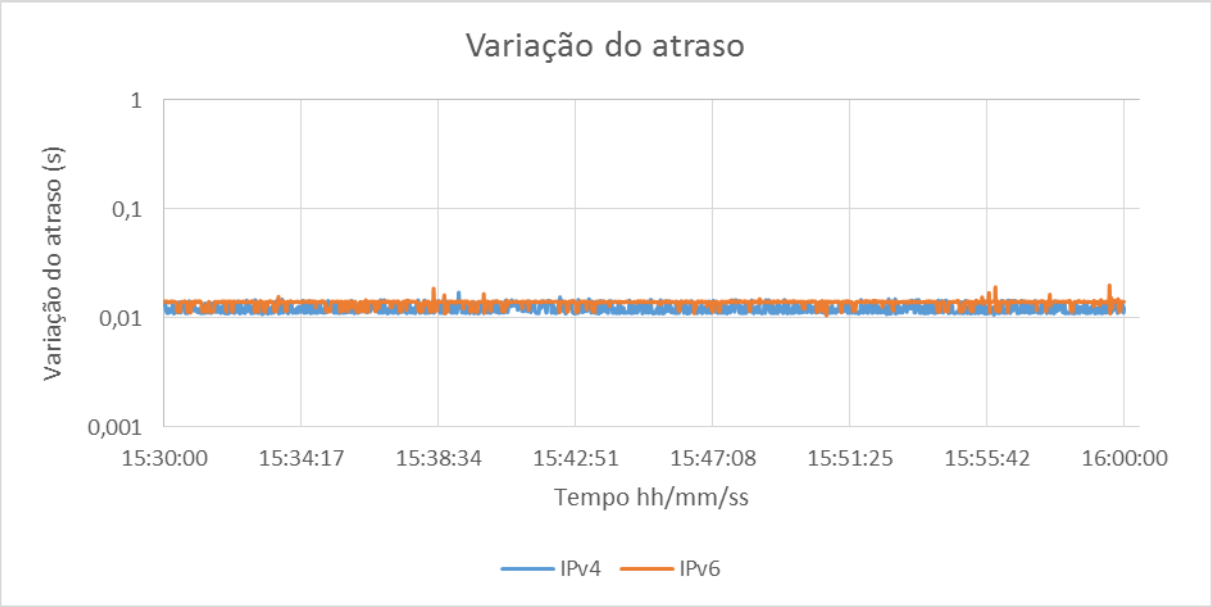


Gráfico 7 – Variação do atraso em segundos do tráfego TCP em horário laboral.

4.1.3 Tráfego de *streaming* com o padrão H.323

Nesta simulação de *streaming* foi gerado um fluxo de transferência de 120.3 pacotes por segundo (pps) com um tamanho médio de 1352.5 *bytes* por pacote.

Os resultados obtidos na tabela 11 e representados nos gráficos 8 e 9 mostram que o atraso e a variação do atraso foram superiores no protocolo IPv4, onde o atraso foi muito inconstante no protocolo IPv4 como está representado no gráfico 8 com um atraso médio superior em 1.449 milissegundos em relação ao IPv6 e com uma variabilidade média em IPv4 de 19.114 milissegundos apesar de muito semelhante à variação média do atraso em IPv6, verifica-se uma diferença de 2.223 milissegundos como representado na tabela 11.

Tabela 11 – Resumo do tráfego de *streaming* em horário laboral.

	IPv4	IPv6
Pacotes transmitidos	216467	216356
Atraso médio	0.017033 s	0.015584 s
Variação média do atraso	0.019114 s	0.016891 s
Bytes recebidos	292663384	292513312
Taxa de transferência média	1300.730760 Kbit/s	1300.065003 Kbit/s
Média de pacotes transmitidos	120.259871 pkt/s	120.198318 pkt/s
Pacotes descartados	73 (0.03 %)	184 (0.08 %)

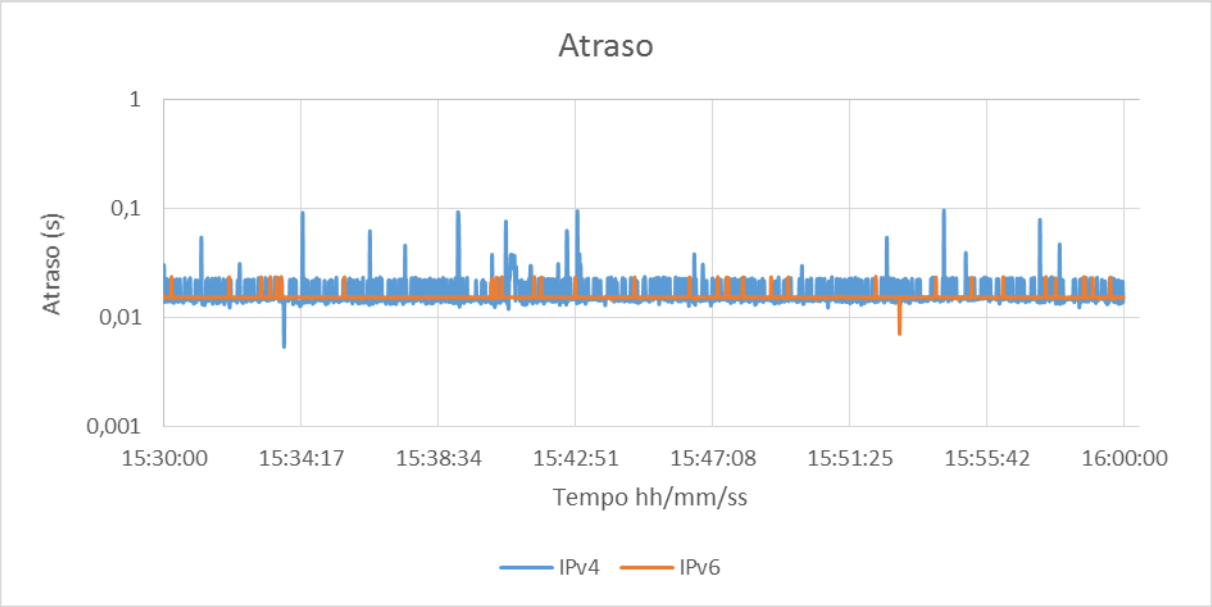


Gráfico 8 – Atraso em segundos do tráfego *streaming* em horário laboral.

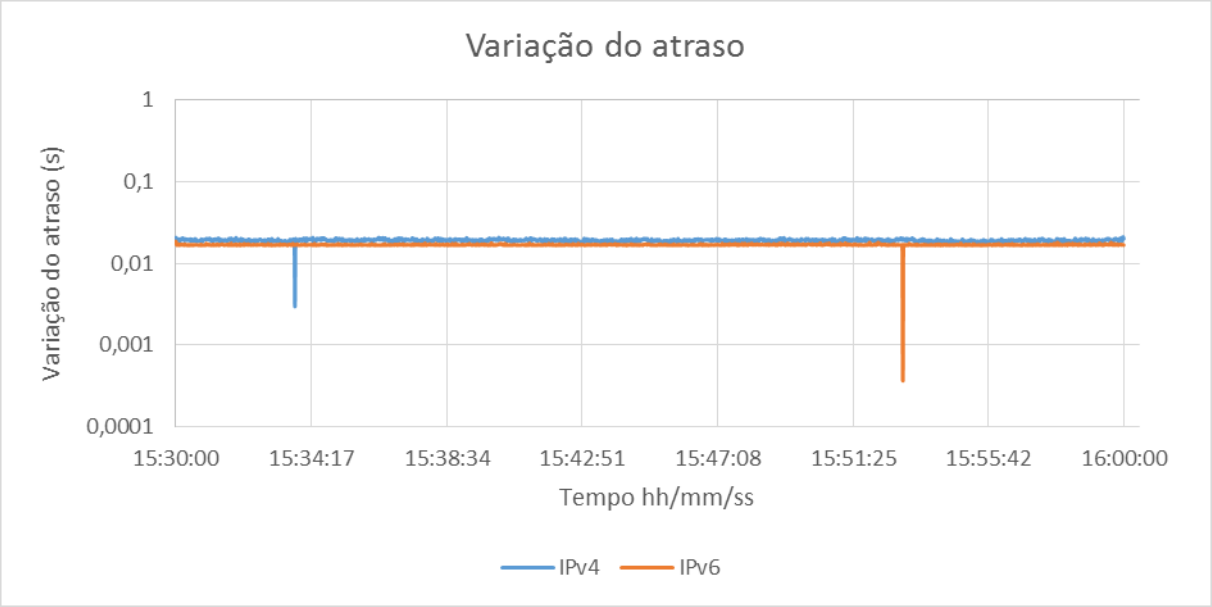


Gráfico 9 – Variação do atraso em segundos do tráfego *streaming* em horário laboral.

Recordando que na indústria o padrão de sucesso são os "*five nines*" (Cisco Systems, 2002), *i.e.*, 99.999%, isso implica uma taxa de perdas aceitável 0.001%, pode afirmar-se que houve um considerável número de pacotes descartados em ambos os protocolos, sendo na sua maioria pacotes IPv6 (0.08%) de acordo com a tabela 11 e o gráfico 10. De referir que em função das perdas de pacotes por parte do protocolo IPv6 foram transferidos mais 111 pacotes em IPv4, recebidos mais 150072 *bytes* e cerca de uma média de 0.531442 pacotes transmitidos por segundo em IPv4 sendo que a taxa de transferência foi muito semelhante com uma ligeira superioridade de 681.735168 bits/s em IPv4.

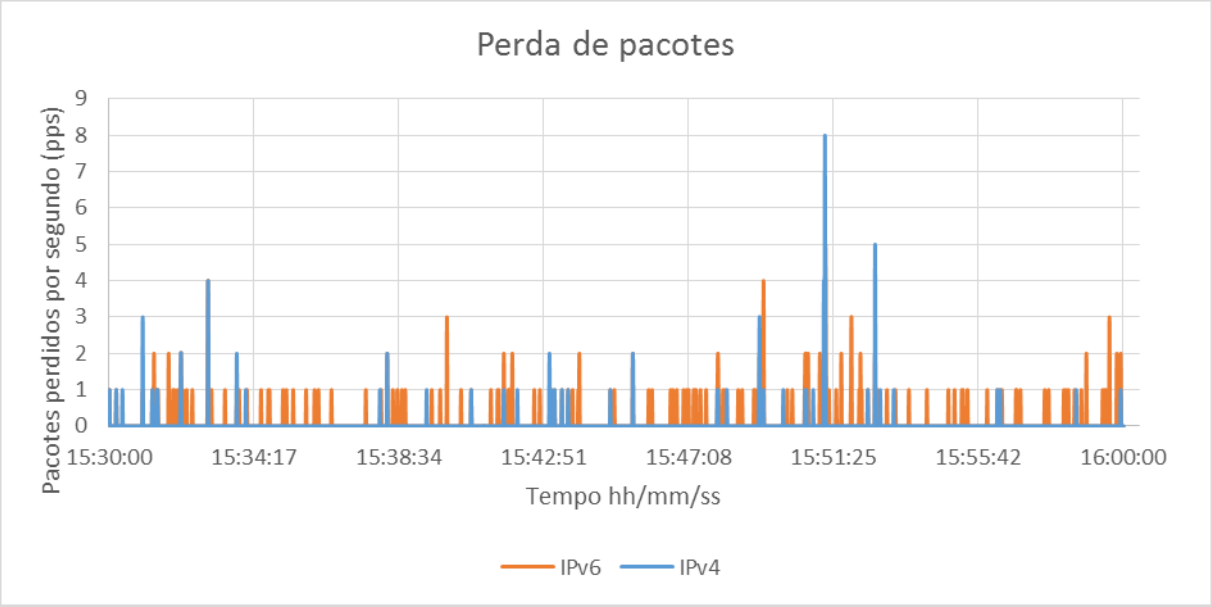


Gráfico 10 – Perda de pacotes por segundo em tráfego *streaming* em horário laboral.

4.1.4 Tráfego de VoIP com o codec G.711.1

Nesta simulação de tráfego VoIP com o *codec* G.711.1 foi gerado um fluxo de transferência de 100 pacotes por segundo (pps), com um tamanho individual de 80 *bytes*.

Os resultados que constam da tabela 12 e representados nos gráficos 11 e 12, mostram que o atraso e a variação do atraso foram superiores no protocolo IPv4 onde segundo a tabela 12 o atraso médio em IPv4 foi superior em cerca de 1.67 milissegundos e a variação média do atraso foi ligeiramente superior com mais 0.677 milissegundos também no protocolo IPv4. Como pode ser observado no gráfico 13 houve maior perda de pacotes por parte do protocolo IPv6 (0.09%), tendo por isso sido transferidos mais 89 pacotes com o protocolo IPv4 e recebidos mais 8188 *bytes* fruto da perda de pacotes superior em IPv6 como representado na tabela 12.

Tabela 12 – Resumo do tráfego de *VoIP* em horário laboral.

	IPv4	IPv6
Pacotes transmitidos	179930	179841
Atraso médio	0.016885 s	0.015215 s
Variação média do atraso	0.020832 s	0.020155 s
Bytes recebidos	16553560	16545372
Taxa de transferência média	73.571815 Kbit/s	73.535396 Kbit/s
Média de pacotes transmitidos	99.961705 pkt/s	99.912223 pkt/s

Pacotes descartados	70 (0.04 %)	159 (0.09 %)

Também segundo a tabela 12 a média de pacotes transmitidos e a taxa de transferência foi muito semelhante em ambos os protocolos com uma superioridade de 0.049482 pacotes por segundo e uma taxa de transferência média de 37.293 bit/s superior para IPv4.

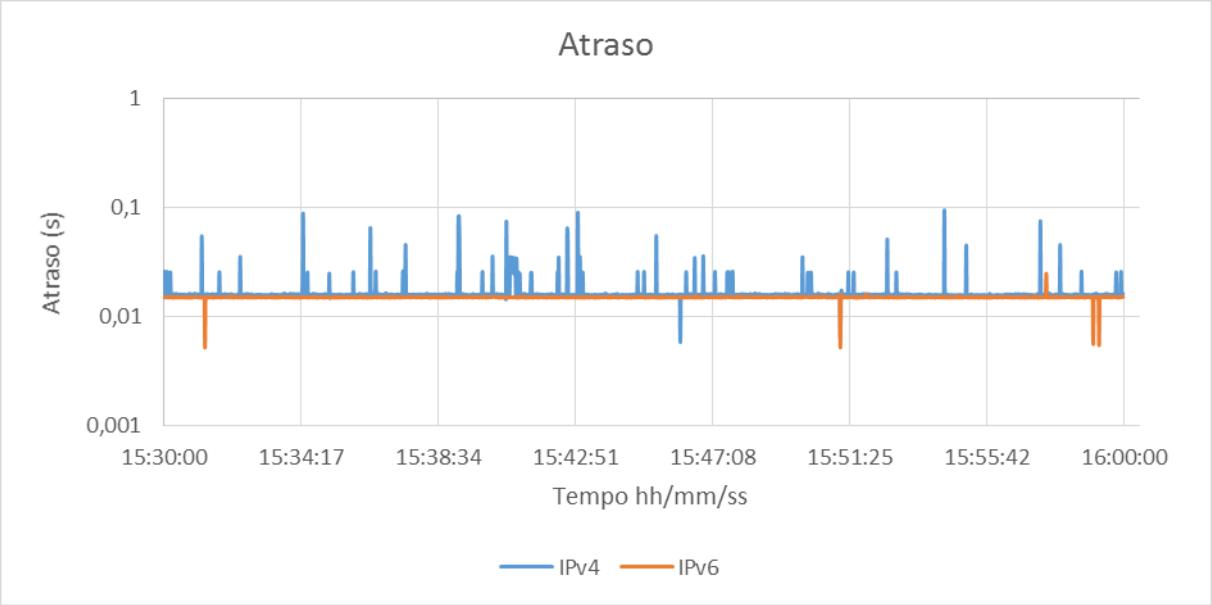


Gráfico 11 – Atraso em segundos do tráfego VoIP em horário laboral.

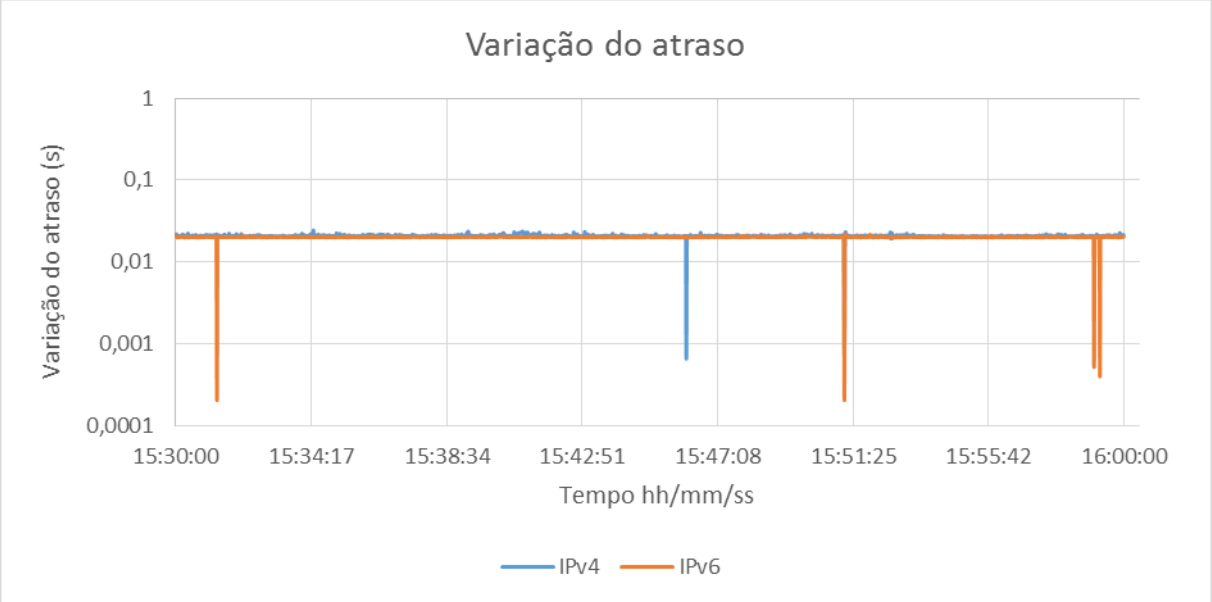


Gráfico 12 – Variação do atraso em segundos do tráfego VoIP em horário laboral.

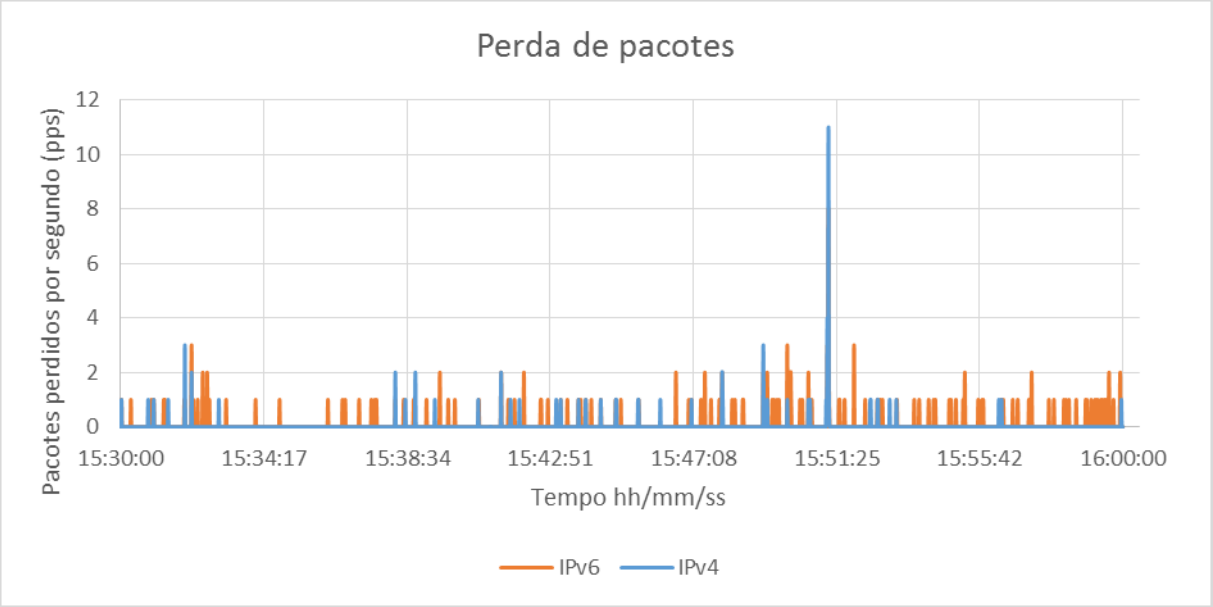


Gráfico 13 – Perda de pacotes por segundo em tráfego VoIP em horário laboral.

4.2 Experiência em horário pós-laboral

A segunda experiência decorreu no dia 21/07/2016 entre as 22h e as 22.30h, onde durante 30 minutos foram executados em simultâneo todos os fluxos de tráfego propostos. Os resultados estão representados através de tabelas com os resumos da transmissão e através de gráficos, onde é possível ver detalhadamente o desempenho dos protocolos.

4.2.1 Tráfego UDP

Nesta experiência com o protocolo UDP foi gerado um fluxo de transferência de 256 pacotes por segundo (pps) onde cada um desses pacotes tem 512 *bytes.*

Os resultados obtidos na tabela 13 e representados nos gráficos 14 e 15, mostram que o atraso e a variação do atraso foram ligeiramente superiores no protocolo IPv4 onde segundo a tabela 13 o atraso médio em IPv4 foi superior em cerca de 0.925 milissegundos e uma variação média do atraso superior em 1.06 milissegundos também no protocolo IPv4.

Em contrapartida como representado no gráfico 16 houve mais pacotes descartados em IPv6 (cerca de 20 o que em percentagem foi aproximadamente 0.0043%), transferidos mais 18 pacotes em IPv4, sendo que a taxa média de pacotes transmitidos foi superior em 0.010091 pacotes por segundo e mais 9216 *bytes* recebidos em IPv4 segundo a tabela 13. De salientar que a taxa de transferência média foi semelhante em ambos os protocolos com uma diferença de 42.323968 bit/s entre eles.

Tabela 13 – Resumo do tráfego UDP em horário pós-laboral.

	IPv4	IPv6
Pacotes transmitidos	460798	460780
Atraso médio	0.016211 s	0.015286 s
Variação média do atraso	0.008992 s	0.007932 s
Bytes recebidos	235928576	235919360
Taxa de transferência média	1048.574031 Kbit/s	1048.532699 Kbit/s
Média de pacotes transmitidos	255.999519 pkt/s	255.989428 pkt/s
Pacotes descartados	2 (0.00 %)	20 (0.00 %)

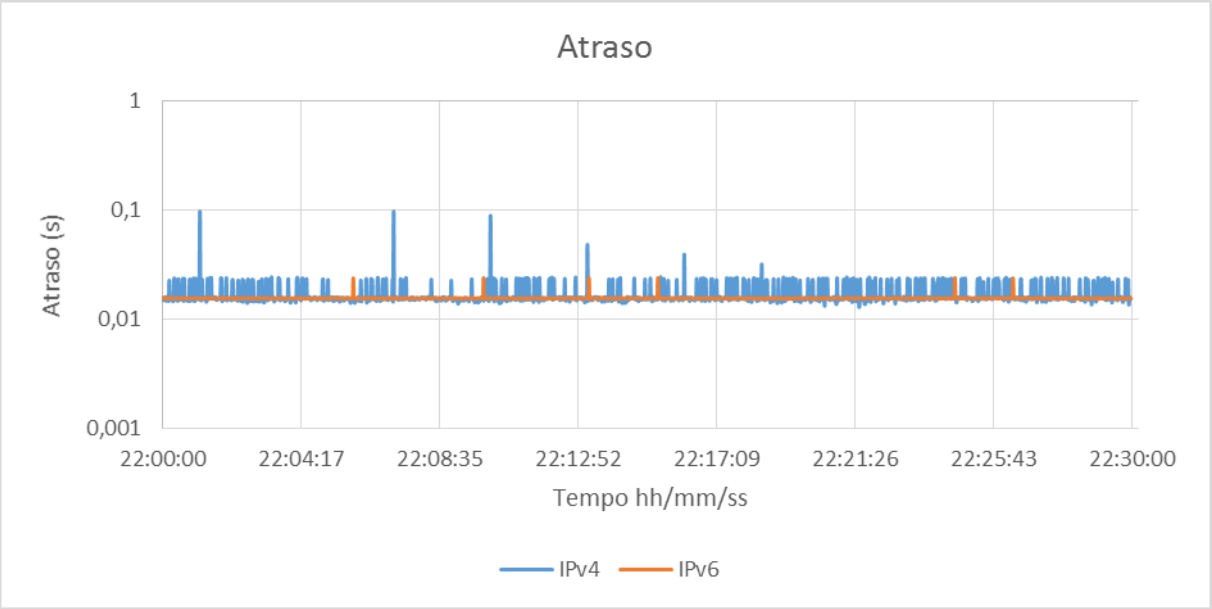


Gráfico 14 – Atraso em segundos do tráfego UDP em horário pós-laboral.

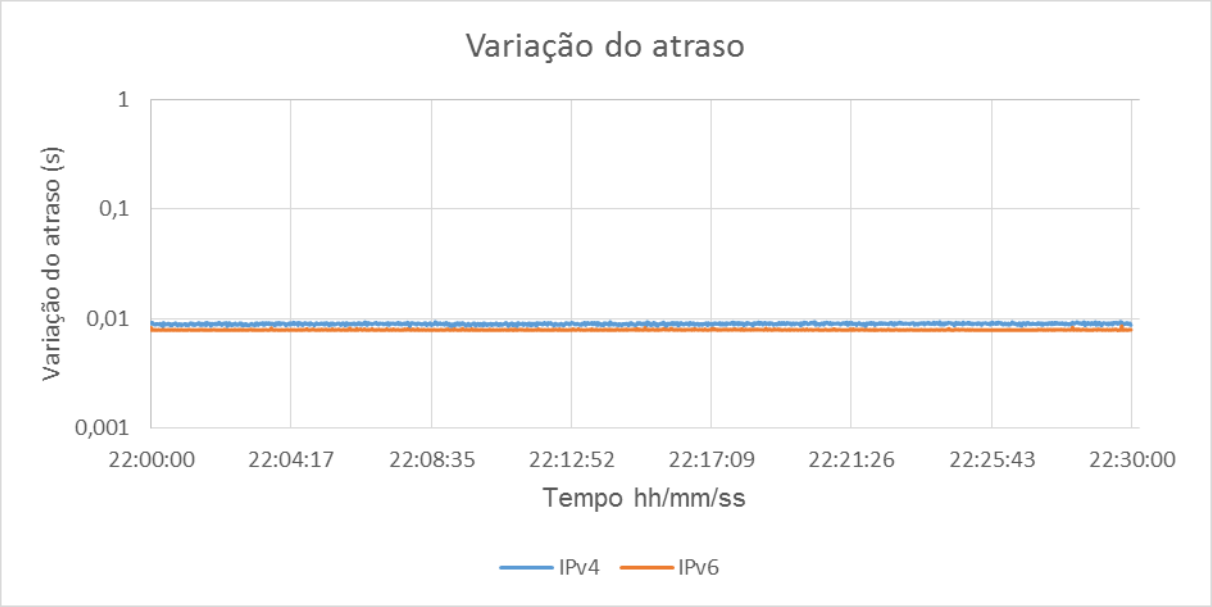


Gráfico 15 – Variação do atraso em segundos do tráfego UDP em horário pós-laboral.

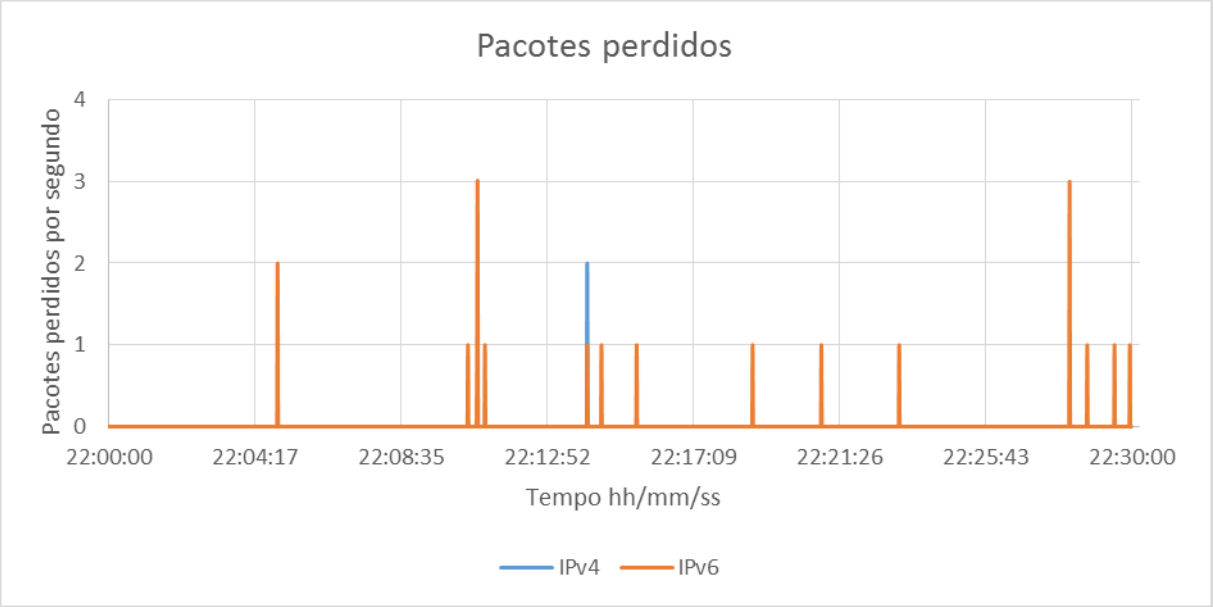


Gráfico 16 – Perda de pacotes por segundo em tráfego UDP em horário pós-laboral.

4.2.2 Tráfego TCP

Nesta experiência em horário pós-laboral com o protocolo TCP, à semelhança da anterior foi também gerado um fluxo de transferência de 256 pacotes por segundo (pps) onde cada um desses pacotes tem 512 *bytes.*

Os resultados obtidos nesta experiência, mostram que o atraso foi superior no protocolo IPv4, onde segundo a tabela 14 e o gráfico 17 o atraso médio em IPv4 foi superior em cerca de 1.932 milissegundos, mas em contrapartida como pode ser verificado no gráfico 18 a variação média do atraso foi ligeiramente superior no protocolo IPv6 em cerca de 1.159 milissegundos segundo a tabela 14. Pelos mesmos motivos que na experiência anterior não foram registadas perdas de pacotes, como já tinha sido registado na experiência anterior em horário laboral.

Tabela 14 – Resumo do tráfego TCP em horário pós-laboral.

	IPv4	IPv6
Pacotes transmitidos	460798	460797
Atraso médio	0.020510 s	0.018578 s
Variação média do atraso	0.012608 s	0.013767 s
Bytes recebidos	235928576	235928064
Taxa de transferência média	1048.569255 Kbit/s	1048.568938 Kbit/s
Média de pacotes transmitidos	255.998353 pkt/s	255.998276 pkt/s
Pacotes descartados	0 (0.00 %)	0 (0.00 %)

Verificou-se uma transferência de pacotes praticamente igual, com apenas 1 pacote IPv4 a mais a ser transmitido, onde foram recebidos mais 512 bytes em IPv4 a uma média de pacotes transmitidos também muito idêntica com cerca de 0.000077 pacotes por segundo como registado na tabela 14. A taxa de transferência média também foi muito idêntica com um ligeiro incremento de 0.324608 bit/s no protocolo IPv4.

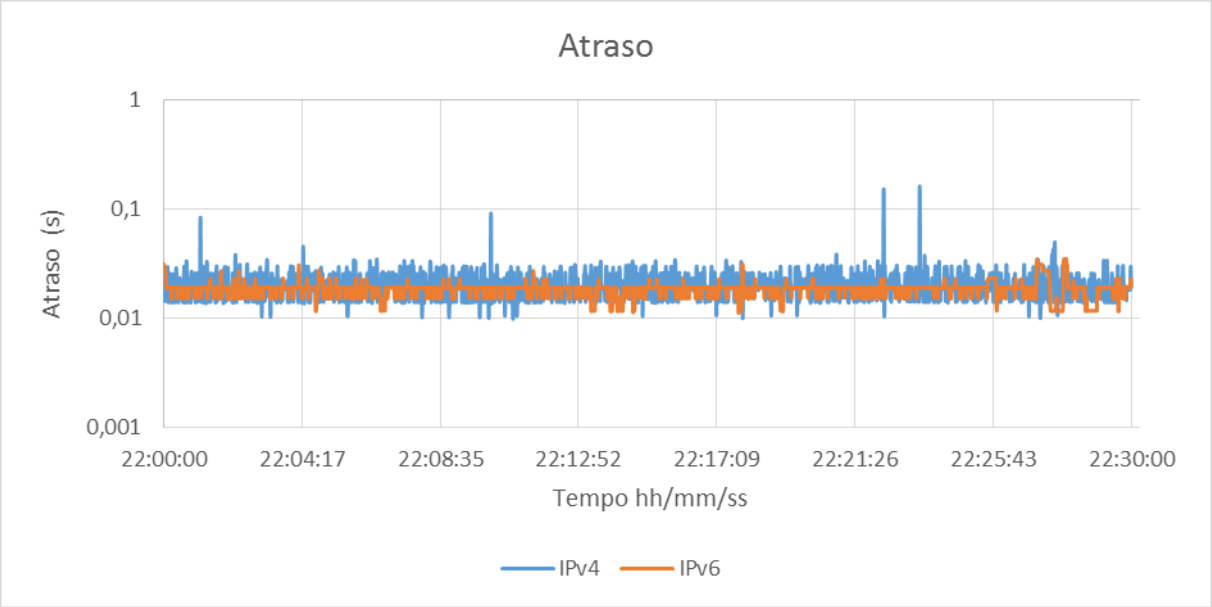


Gráfico 17 – Atraso em segundos do tráfego TCP em horário pós-laboral.

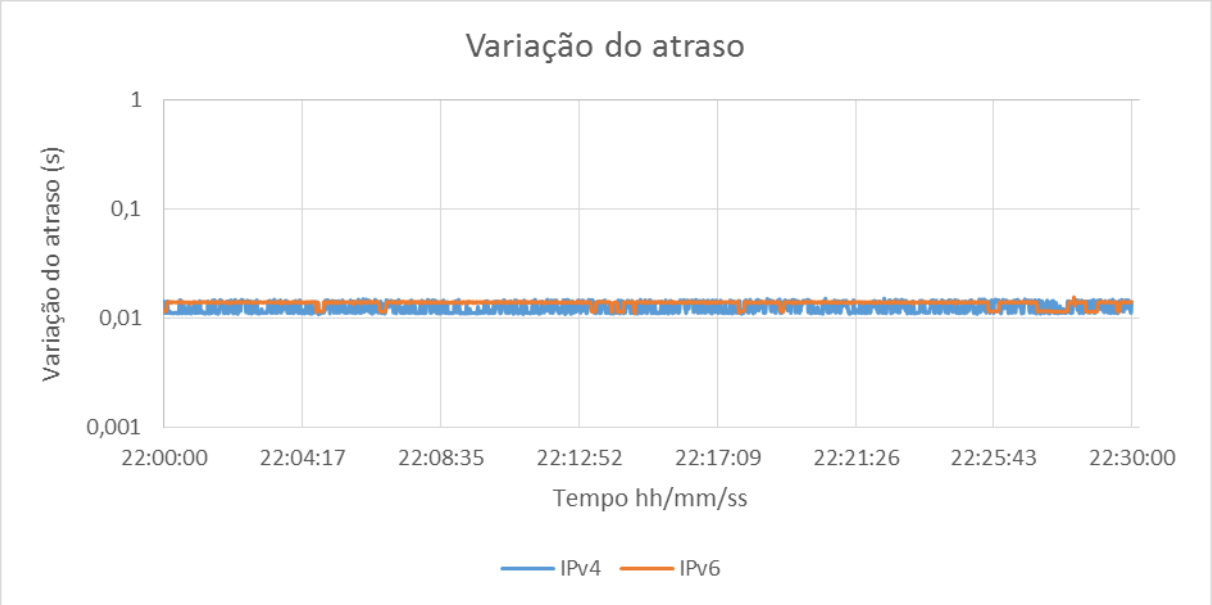


Gráfico 18 – Variação do atraso em segundos do tráfego TCP em horário pós-laboral.

4.2.3 Tráfego de *streaming* com o padrão H.323

Nesta simulação foi gerado um fluxo de transferência de 120.3 pacotes por segundo (pps) onde cada pacote tem um tamanho médio de 1352.5 *bytes.*

Os resultados obtidos na tabela 15 e representados nos gráficos 19 e 20 mostram que o atraso e a variação do atraso foram superiores no protocolo IPv4, onde os resultados com o protocolo IPv6 revelam-se bastante estáveis como está representado no gráfico 19.

Como representado na tabela 15 apesar de ligeiro, o IPv4 obteve um atraso médio superior em 0.952 milissegundos em relação ao IPv6 e com uma variabilidade média de 18,083 milissegundos em IPv4, onde se verifica uma diferença de 1.334 milissegundos em relação ao IPv6 como representado na tabela 15.

Apesar de não haver registo de muitos pacotes perdidos como representado no gráfico 21, houve 7 pacotes descartados em IPv6 face aos 2 descartados em IPv4 o que resultou na transmissão de mais 5 pacotes em IPv4 do que em IPv6 e mais 6760 *bytes* recebidos pelo IPv4. Ao nível da média de pacotes transmitidos, os resultados foram muito idênticos com ligeira vantagem para o IPv4 com mais 0.002846 pacotes por segundo, no sentido contrario a taxa de transferência foi ligeiramente superior em IPv6 em 131.009536 bit/s como representado na tabela 15.

Tabela 15 – Resumo do tráfego de *streaming* em horário pós-laboral.

	IPv4	IPv6
Pacotes transmitidos	216538	216533
Atraso médio	0.016475 s	0.015523 s
Variação média do atraso	0.018083 s	0.016749 s
Bytes recebidos	292759376	292752616
Taxa de transferência média	1301.159531 Kbit/s	1301.28747 Kbit/s
Média de pacotes transmitidos	120.299513 pkt/s	120.296667 pkt/s
Pacotes descartados	2 (0.00 %)	7 (0.00 %)

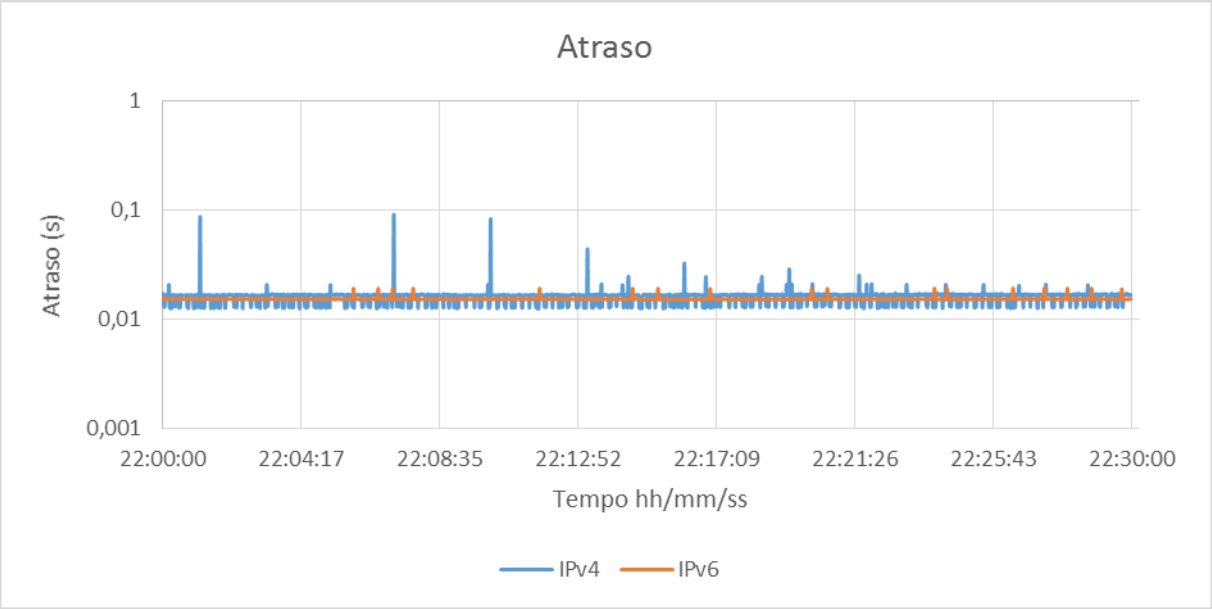


Gráfico 19 – Atraso em segundos do tráfego *streaming* em horário pós-laboral.

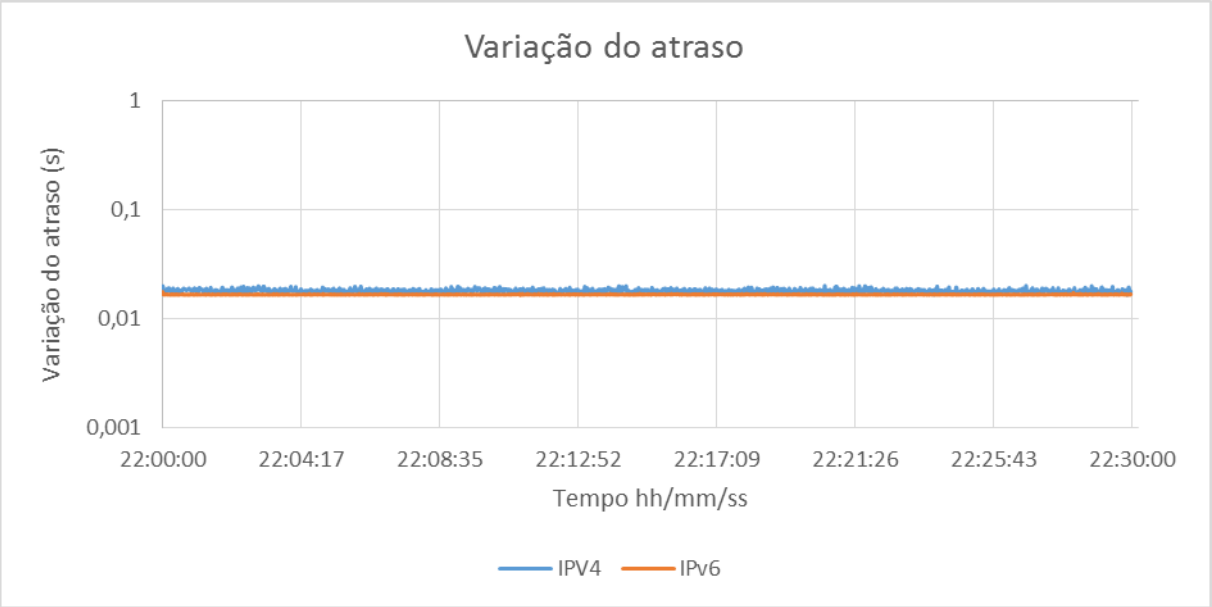


Gráfico 20 – Variação do atraso em segundos do tráfego streaming *em horário pós-laboral.*

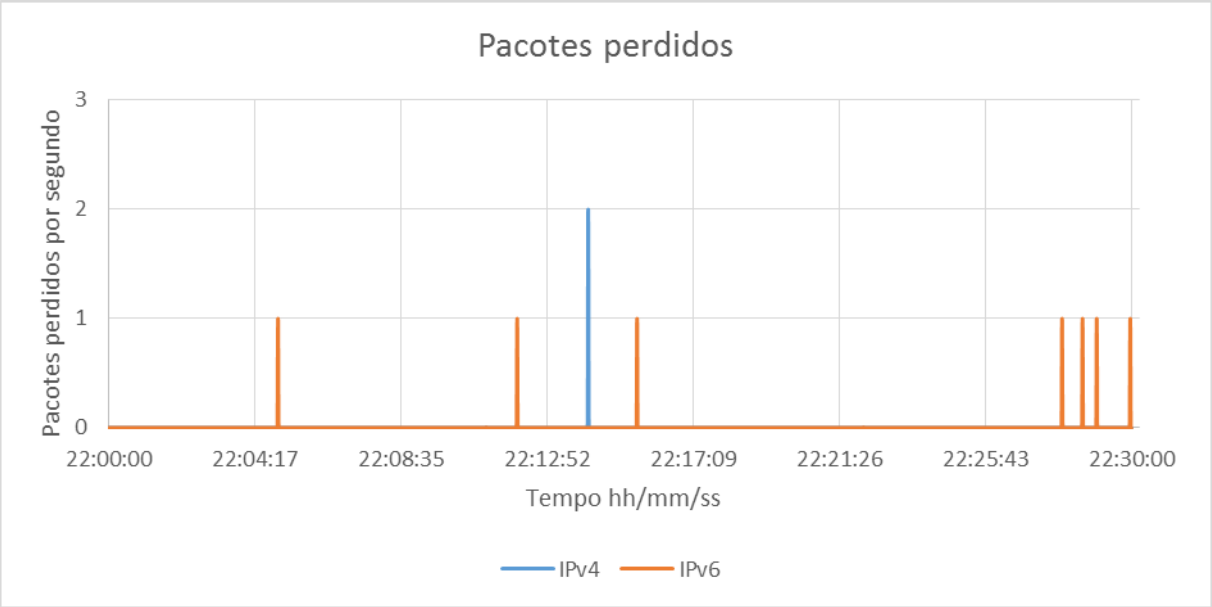


Gráfico 21 – Perda de pacotes por segundo em tráfego *streaming* em horário pós-laboral.

4.2.4 Tráfego de VoIP com o codec G.711.1

Nesta simulação de tráfego de VoIP com o *codec* G.711.1 foi gerado um fluxo de transferência de 100 pacotes por segundo (pps) onde cada um desses pacotes tem 80 *bytes*.

Os resultados obtidos na tabela 16 e representados nos gráficos 22 e 23, mostram que o atraso e a variação do atraso foram superiores no protocolo IPv4 onde ao nível do atraso no protocolo IPv4 houve alguns picos no decorrer da experiência, enquanto o protocolo IPv6 revelou-se estável como é visível no gráfico 22.

Segundo a tabela 16 o atraso médio em IPv4 foi superior em cerca de 0.88 milissegundos e a variação média do atraso foi ligeiramente superior com mais 0.412 milissegundos também no protocolo IPv4.

Segundo o gráfico 24, houve maior perda de pacotes por parte do protocolo IPv6 (10 pacotes o que representa 0.01%), embora num número pouco significativo, tendo por isso sido transferidos mais 7 pacotes com o protocolo IPv4 e recebidos mais 644 *bytes* fruto da perda de pacotes superior em IPv6 como representado na tabela 16. Também segundo a tabela 16 a média de pacotes transmitidos foi superior em IPv4 com 0.003973 pacotes por segundo e a taxa de transferência média também superior com 2.994176 bit/s sendo os resultados foram muito idênticos, entre IPv4 e IPv6.

Tabela 16 – Resumo do tráfego de VoIP em horário pós-laboral.

	IPv4	IPv6
Pacotes transmitidos	179997	179990
Atraso médio	0.016046 s	0.015166 s
Variação média do atraso	0.020519 s	0.020107 s
Bytes recebidos	16559724	16559080
Taxa de transferência média	73.599243 Kbit/s	73.596319 Kbit/s
Média de pacotes transmitidos	99.998972 pkt/s	99.994999 pkt/s
Pacotes descartados	3 (0.00 %)	10 (0.01 %)

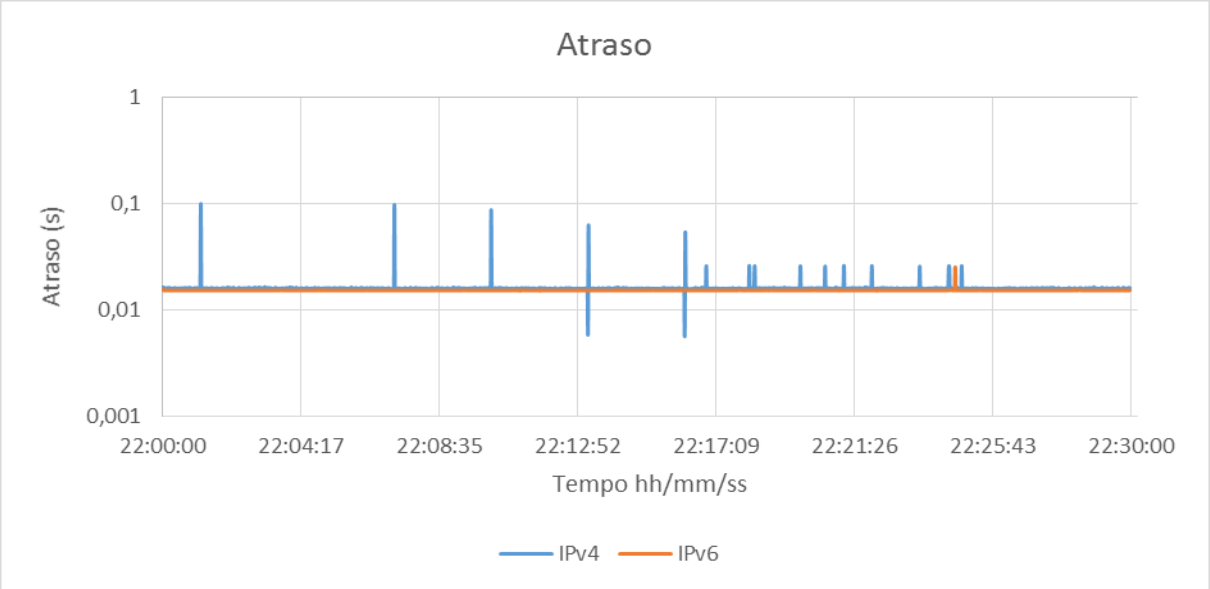


Gráfico 22 – Atraso em segundos do tráfego VoIP em horário pós-laboral.

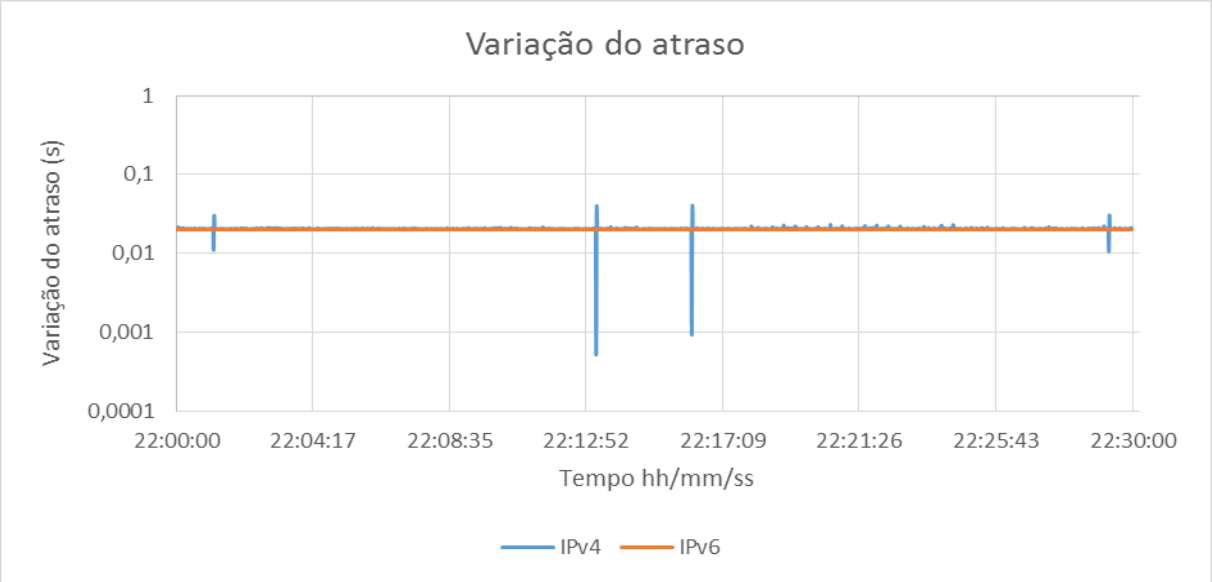


Gráfico 23 – Variação do atraso em segundos do tráfego VoIP em horário pós-laboral.

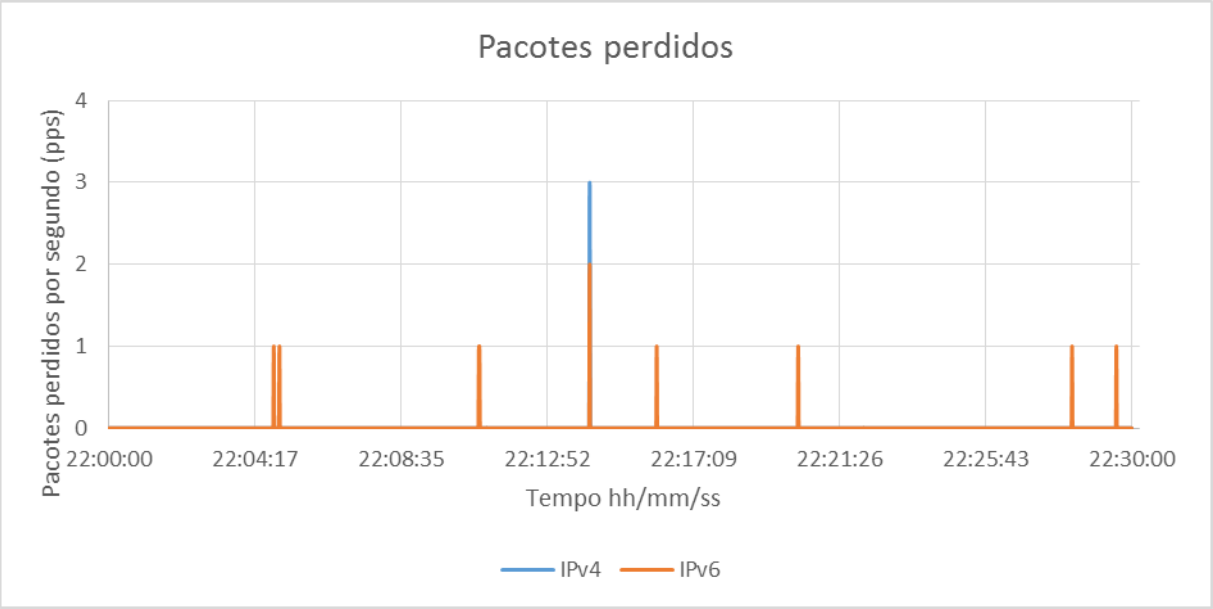


Gráfico 24 – Perda de pacotes por segundo em tráfego VoIP em horário pós-laboral.

4.3 Comparação de resultados com o protocolo IPv4 e IPv6 em horário laboral e pós-laboral

As sub-secções seguintes apresentam uma comparação de medidas feitas entre os horários laboral e pós-laboral, nas várias classes de tráfego.

4.3.1 Tráfego UDP em IPv4 em horário laboral e pós-laboral

Como se pode ver na tabela 17, foram transmitidos mais 140 pacotes em horário pós-laboral e o rácio de pacotes UDP descartados em horário pós-laboral é praticamente nulo, enquanto que em horário laboral verificou-se um rácio ainda expressivo. Do mesmo modo, o atraso médio desceu cerca de 0.797 milissegundos, tendo-se mantido a variação do atraso sensivelmente nos mesmos valores. Em horário pós-laboral também foram recebidos mais *Bytes* a uma taxa de transferência média superior. Estes resultados representados nos Gráficos 25, 26 e 27, eram esperados uma vez que a rede tem mais recursos disponíveis e portanto entra menos vezes em cenários de contenção.

Tabela 17 – Resumo do tráfego de UDP com o protocolo IPv4 em horário laboral e pós-laboral.

	IPv4 Laboral	IPv4 Pós-laboral
Pacotes transmitidos	460658	460798
Atraso médio	0.017008 s	0.016211 s
Variação média do atraso	0.008778 s	0.008992 s
Bytes recebidos	235856896	235928576
Taxa de transferência média	1048.255370 Kbit/s	1048.574031 Kbit/s
Média de pacotes transmitidos	255.921721 pkt/s	255.999519 pkt/s
Pacotes descartados	142 (0.03 %)	2 (0.00 %)

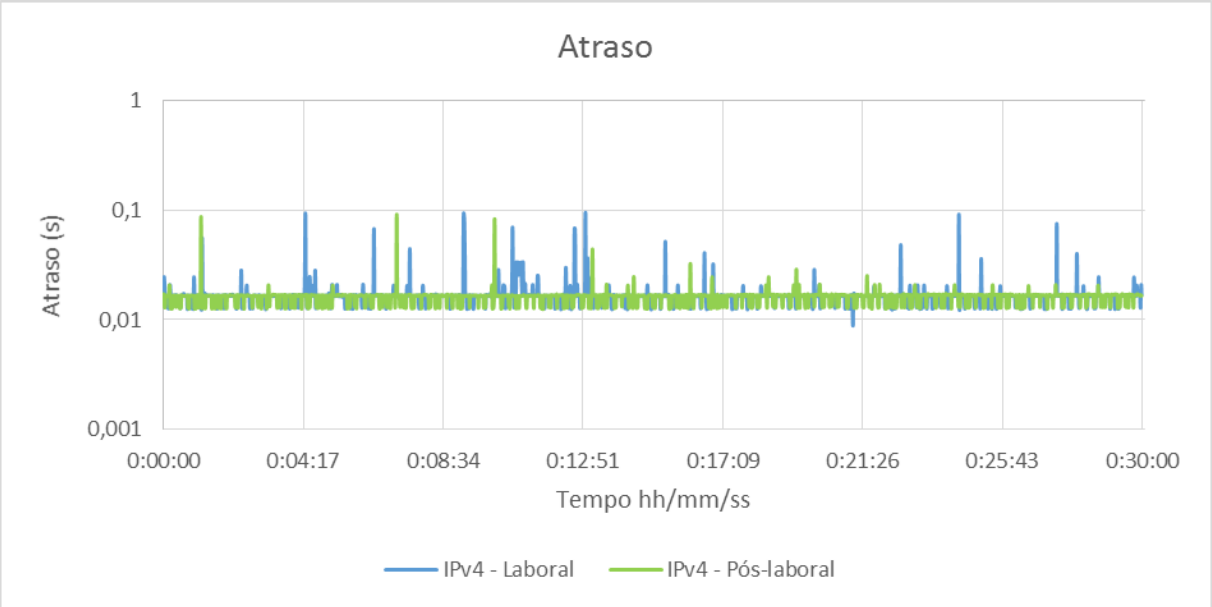


Gráfico 25 – Atraso por segundo em tráfego UDP com o protocolo IPv4 em horário laboral e pós-laboral.

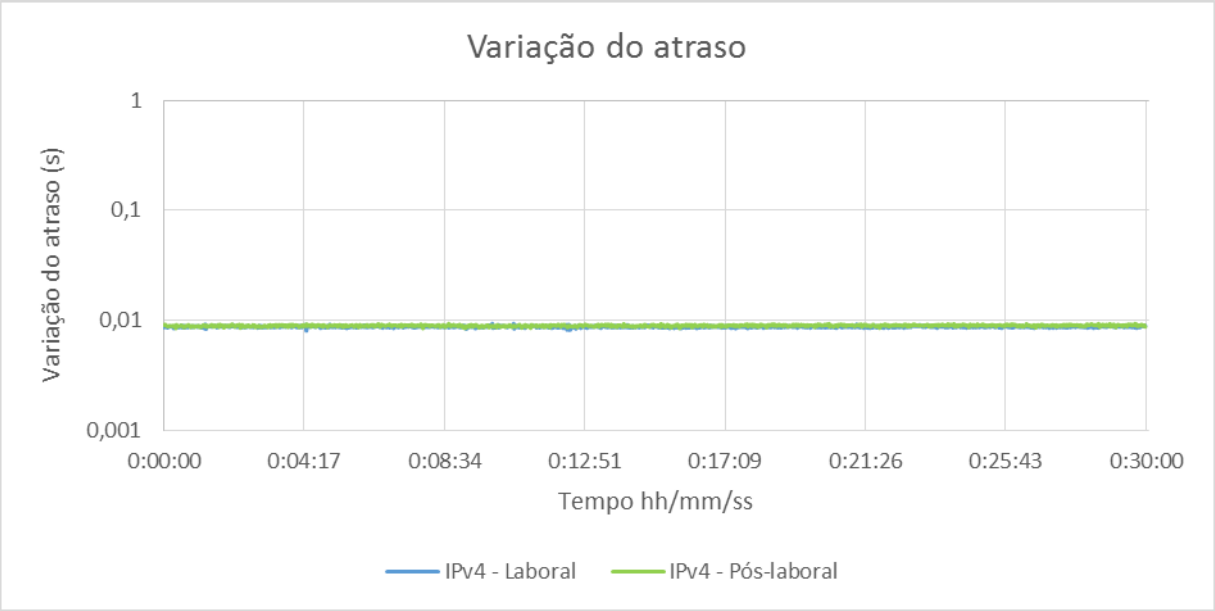


Gráfico 26 – Variação do atraso por segundo em tráfego UDP com o protocolo IPv4 em horário laboral e pós-laboral.

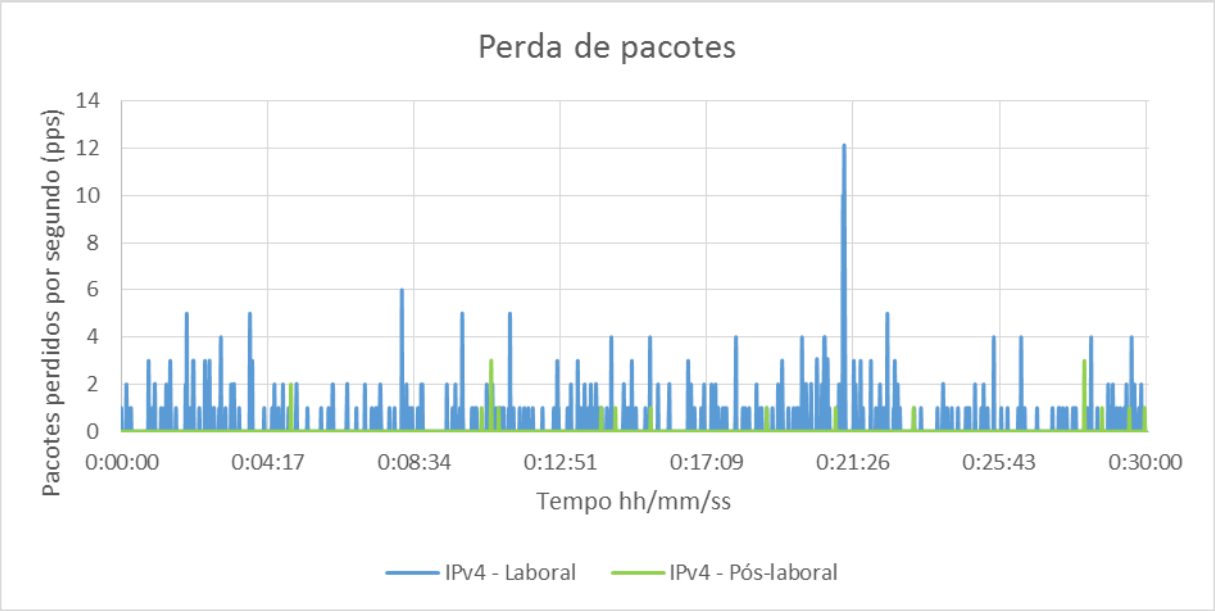


Gráfico 27 – Pacotes perdidos por segundo em tráfego UDP com o protocolo IPv4 em horário laboral e pós-laboral.

4.3.2 Tráfego TCP em IPv4 em horário laboral e pós-laboral

De acordo com os resultados que constam da tabela 18 é possível verificar que foram transmitidos praticamente o mesmo número de pacotes a uma taxa de transferência média e uma média de pacotes transmitidos também muito semelhante embora com uma ligeira superioridade da experiência em horário pós-laboral. Não houve perda de pacotes

pelas razoes descritas acima. Os gráficos 28 e 29 apresentam um atraso médio maior em horário laboral e uma variação média muito semelhante.

Tabela 18 – Resumo do tráfego de TCP com o protocolo IPv4 em horário laboral e pós-laboral.

	IPv4 Laboral	IPv4 Pós-laboral
Pacotes transmitidos	460797	460798
Atraso médio	0.021446 s	0.020510 s
Variação média do atraso	0.012229 s	0.012608 s
Bytes recebidos	235928064	235928576
Taxa de transferência média	1048.567781 Kbit/s	1048.569255 Kbit/s
Média de pacotes transmitidos	255.997993 pkt/s	255.998353 pkt/s
Pacotes descartados	0 (0.00 %)	0 (0.00 %)

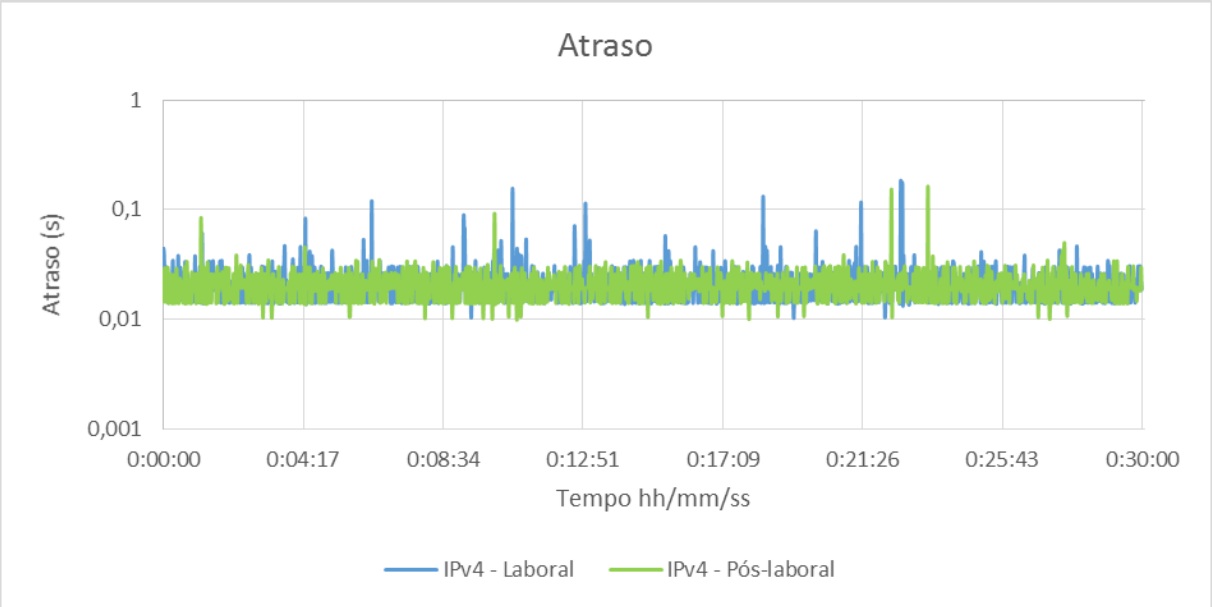


Gráfico 28 – Atraso por segundo em tráfego TCP com o protocolo IPv4 em horário laboral e pós-laboral.

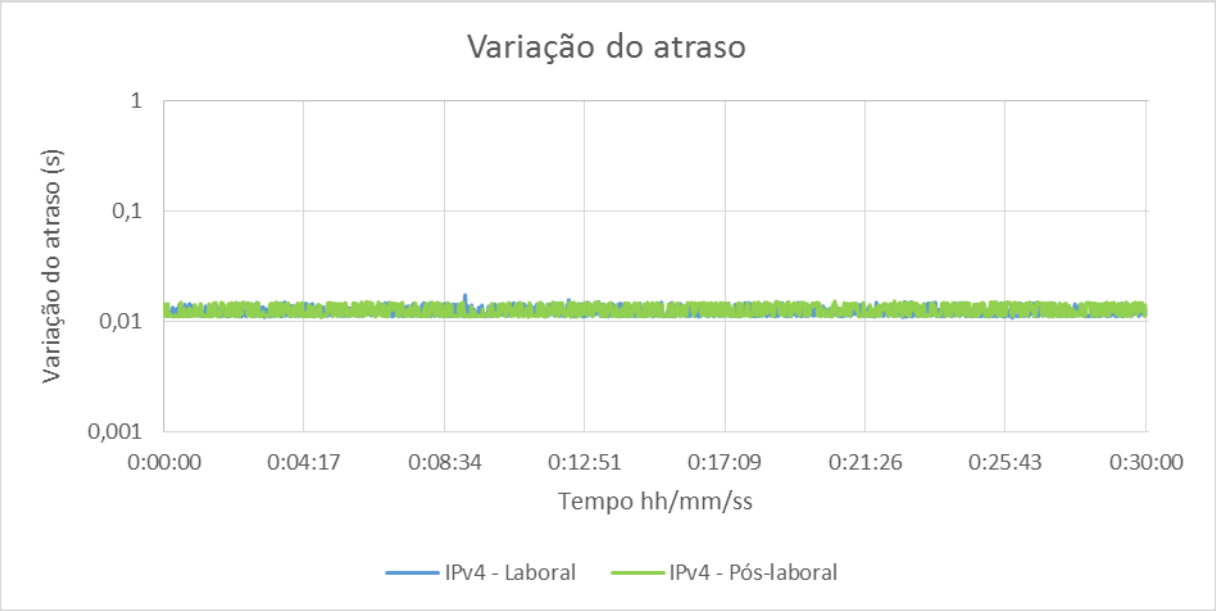


Gráfico 29 – Variação do atraso por segundo em tráfego TCP com o protocolo IPv4 em horário laboral e pós-laboral.

4.3.3 Tráfego s*treaming* em IPv4 em horário laboral e pós-laboral

Os resultados obtidos na tabela 19 mostram que foram transmitidos mais 71 pacotes em horário pós-laboral e descartados 0.03% dos pacotes em horário laboral que representam 73 pacotes tal como representado no gráfico 32. Está representado nos gráficos 30, 31 e na tabela 19 que o atraso médio foi inferior 0.558 milissegundos e horário pós-laboral tal com a variação do atraso que foi inferior em 1.031 milissegundos. De acordo com a tabela 19 também é possível verificar que a taxa de transferência média, a média de pacotes transmitidos e o número de bytes recebidos foi superior na experiência em horário pós-laboral.

Tabela 19 – Resumo do tráfego de *streaming* com o protocolo IPv4 em horário laboral e pós-laboral.

	IPv4 Laboral	IPv4 Pós-laboral
Pacotes transmitidos	216467	216538
Atraso médio	0.017033 s	0.016475 s
Variação média do atraso	0.019114 s	0.018083 s
Bytes recebidos	292663384	292759376
Taxa de transferência média	1300.730760 Kbit/s	1301.159531 Kbit/s
Média de pacotes transmitidos	120.259871 pkt/s	120.299513 pkt/s
Pacotes descartados	73 (0.03 %)	2 (0.00 %)

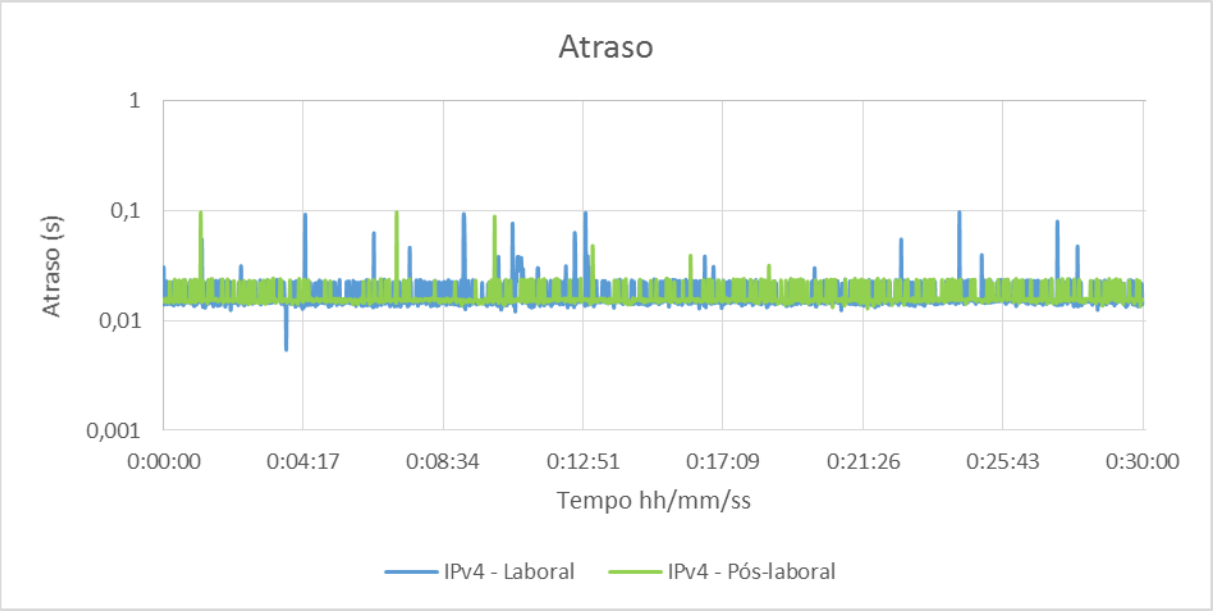


Gráfico 30 – Atraso por segundo em tráfego *streaming* com o protocolo IPv4 em horário laboral e pós-laboral.

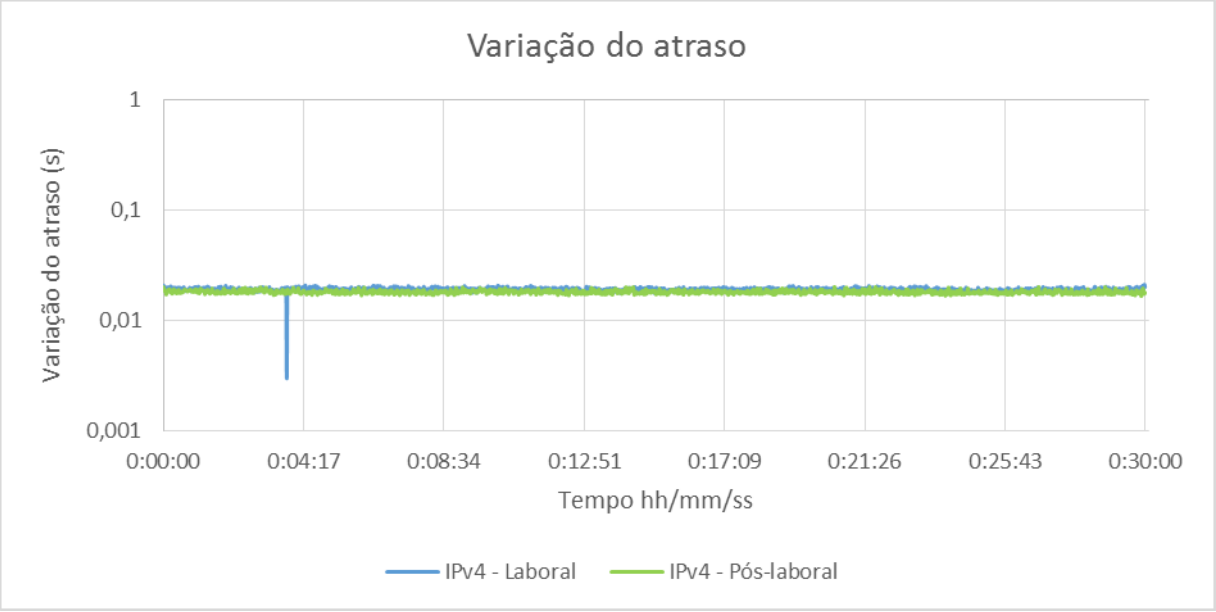


Gráfico 31 – Variação do atraso por segundo em tráfego *streaming* com o protocolo IPv4 em horário laboral e pós-laboral.

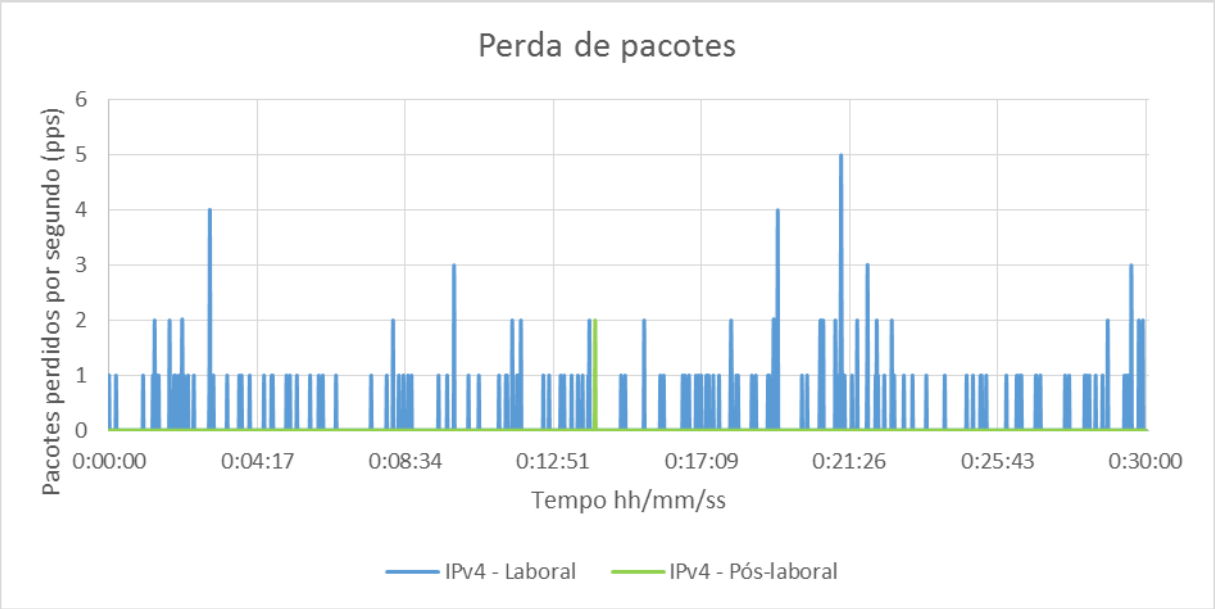


Gráfico 32 – Pacotes perdidos por segundo em tráfego *streaming* com o protocolo IPv4 em horário laboral e pós-laboral.

4.3.4 Tráfego VoIP em IPv4 em horário laboral e pós-laboral

Os resultados que constam da tabela 20 e representados nos gráficos 33 e 34, mostram que o atraso e a variação do atraso foram ligeiramente superiores na experiencia em horário laboral onde segundo a tabela 20 o atraso médio em foi superior em cerca de 0.839 milissegundos e a variação média do atraso foi ligeiramente superior com mais 0.313 milissegundos. Como representado no gráfico 35 foram descartados mais 67 pacotes em horário laboral que de acordo com a tabela 20 representa 0.04%.

De acordo com a tabela 20 os resultados na experiência pós-laboral foram melhores em todos os sentidos.

Tabela 20 – Resumo do tráfego de VoIP com o protocolo IPv4 em horário laboral e pós-laboral.

	IPv4 Laboral	IPv4 Pós-laboral
Pacotes transmitidos	179930	179997
Atraso médio	0.016885 s	0.016046 s
Variação média do atraso	0.020832 s	0.020519 s
Bytes recebidos	16553560	16559724
Taxa de transferência média	73.571815 Kbit/s	73.599243 Kbit/s
Média de pacotes transmitidos	99.961705 pkt/s	99.998972 pkt/s
Pacotes descartados	70 (0.04 %)	3 (0.00 %)

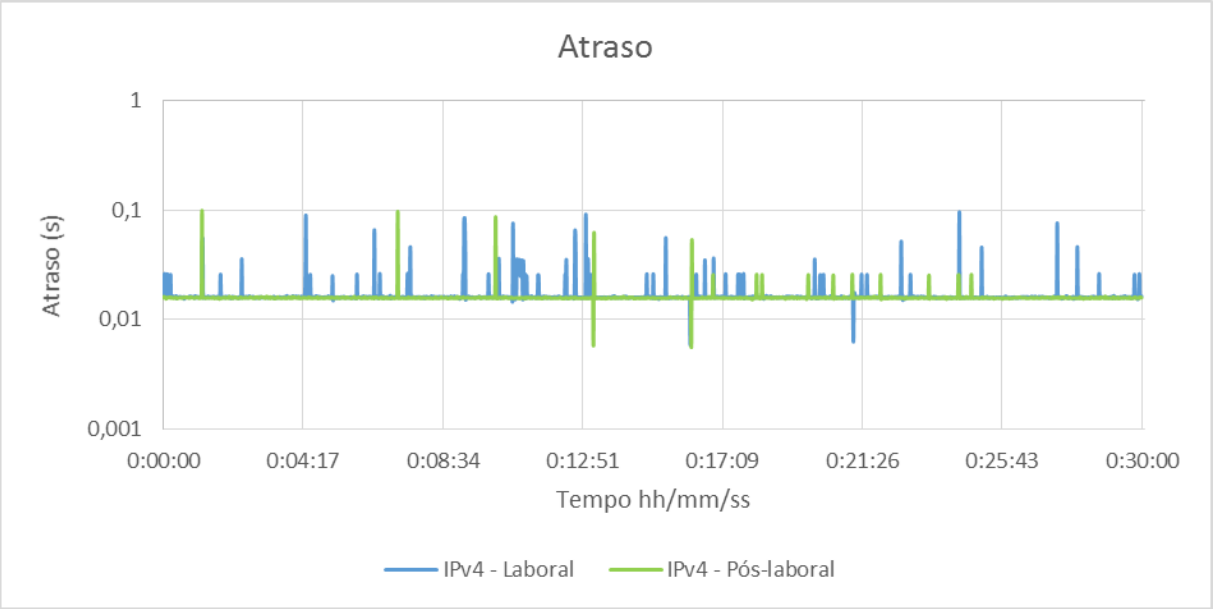


Gráfico 33 – Atraso por segundo em tráfego VoIP com o protocolo IPv4 em horário laboral e pós-laboral.

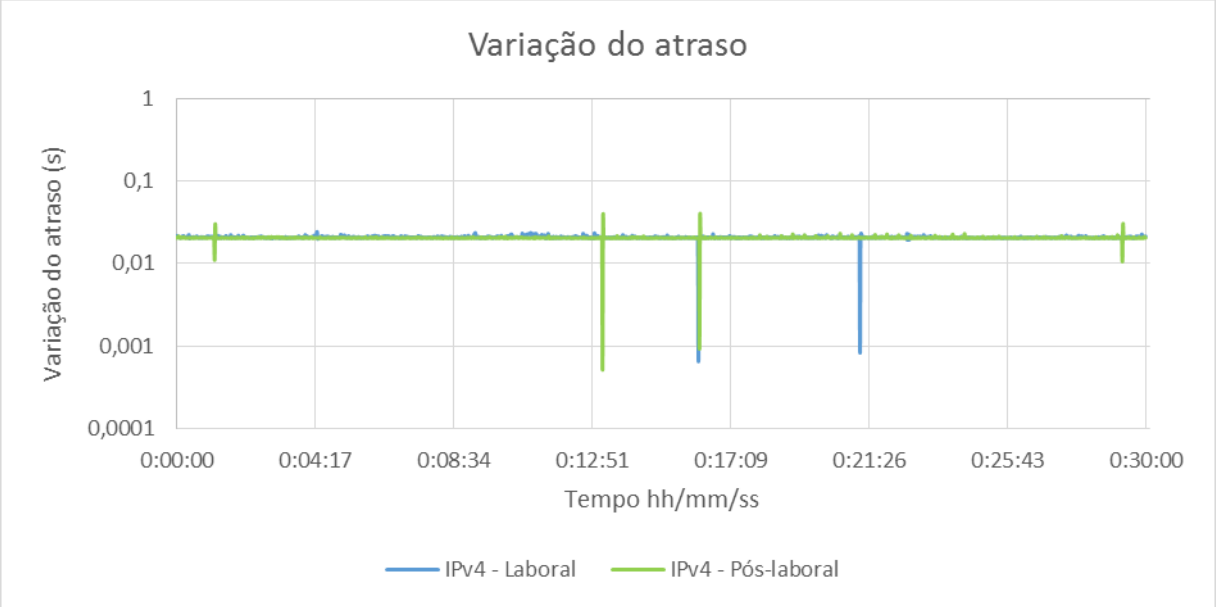


Gráfico 34 – Variação do atraso por segundo em tráfego VoIP com o protocolo IPv4 em horário laboral e pós-laboral.

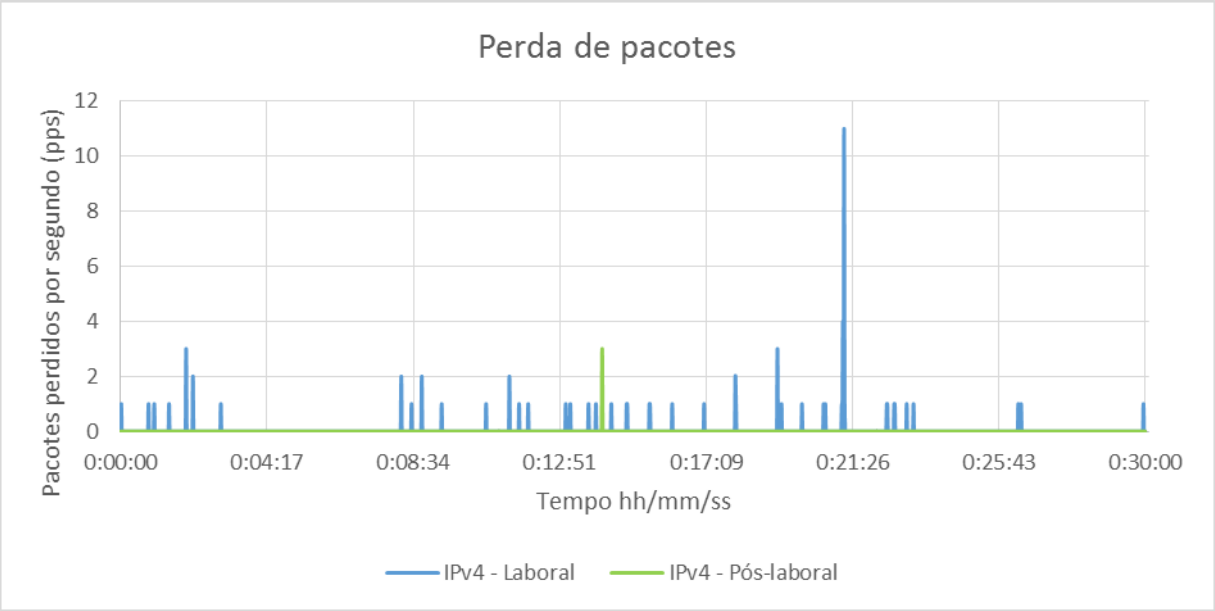


Gráfico 35 – Pacotes perdidos por segundo em tráfego VoIP com o protocolo IPv4 em horário laboral e pós-laboral.

4.3.5 Tráfego UDP em IPv6 em horário laboral e pós-laboral

Como se pode ver na tabela 21, foram transmitidos mais 410 pacotes em horário pós-laboral e descartados 430 pacotes em horário laboral que representa 0.09% dos pacotes conforme representado no gráfico 38. Os gráficos 36 e 37 representam um atraso médio muito semelhante e uma variação média maior em horário laboral.

Foram recebidos mais 209920 *bytes* em horário pós-laboral a uma taxa de transferência média superior e com uma média de pacotes transmitidos também superior em horário pós-laboral.

Tabela 21 – Resumo do tráfego de UDP com o protocolo IPv6 em horário laboral e pós-laboral.

	IPv6 Laboral	IPv6 Pós-laboral
Pacotes transmitidos	460370	460780
Atraso médio	0.015333 s	0.015286 s
Variação média do atraso	0.008109 s	0.007932 s
Bytes recebidos	235709440	235919360
Taxa de transferência média	1047.599801 Kbit/s	1048.532699 Kbit/s
Média de pacotes transmitidos	255.761670 pkt/s	255.989428 pkt/s
Pacotes descartados	430 (0.09 %)	20 (0.00 %)

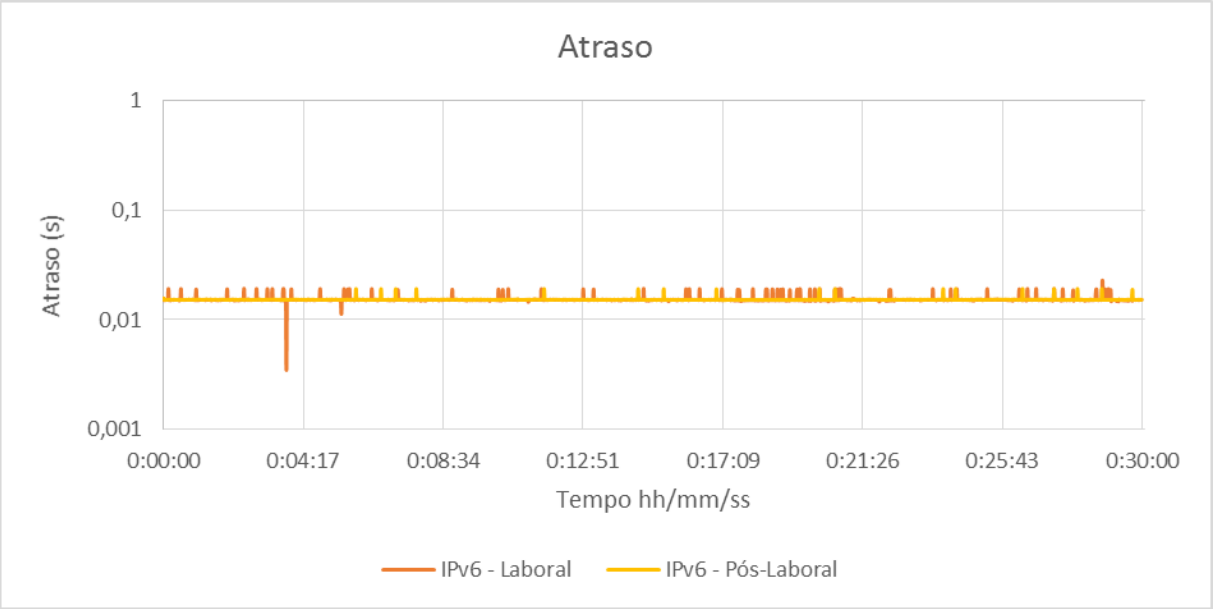


Gráfico 36 – Atraso por segundo em tráfego UDP com o protocolo IPv6 em horário laboral e pós-laboral.

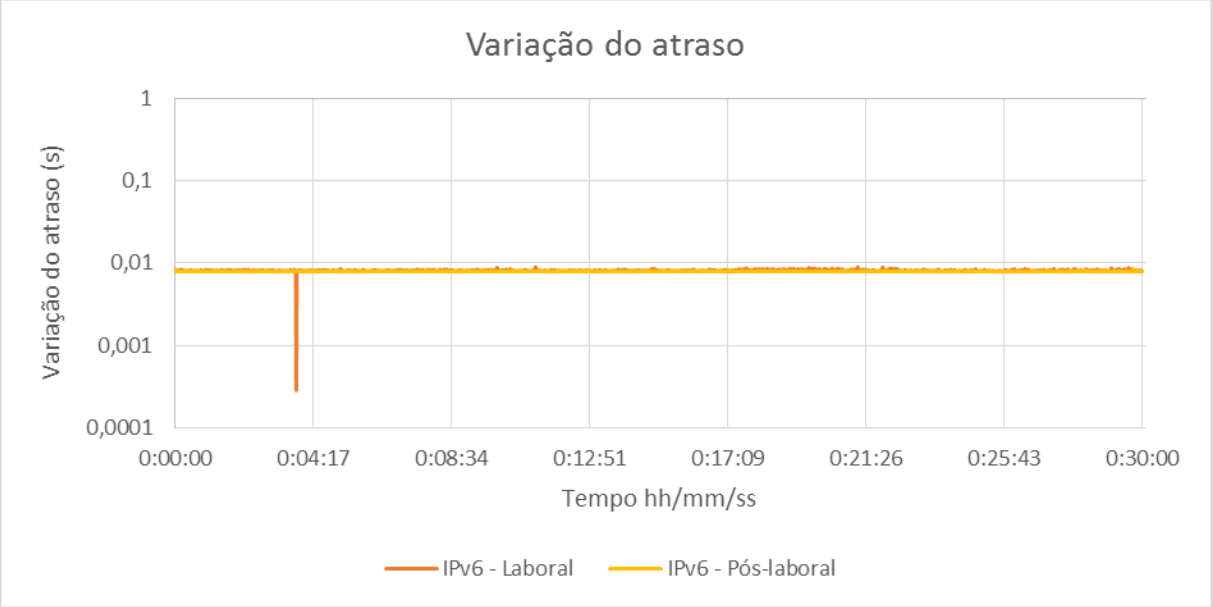


Gráfico 37 – Variação do atraso por segundo em tráfego UDP com o protocolo IPv6 em horário laboral e pós-laboral.

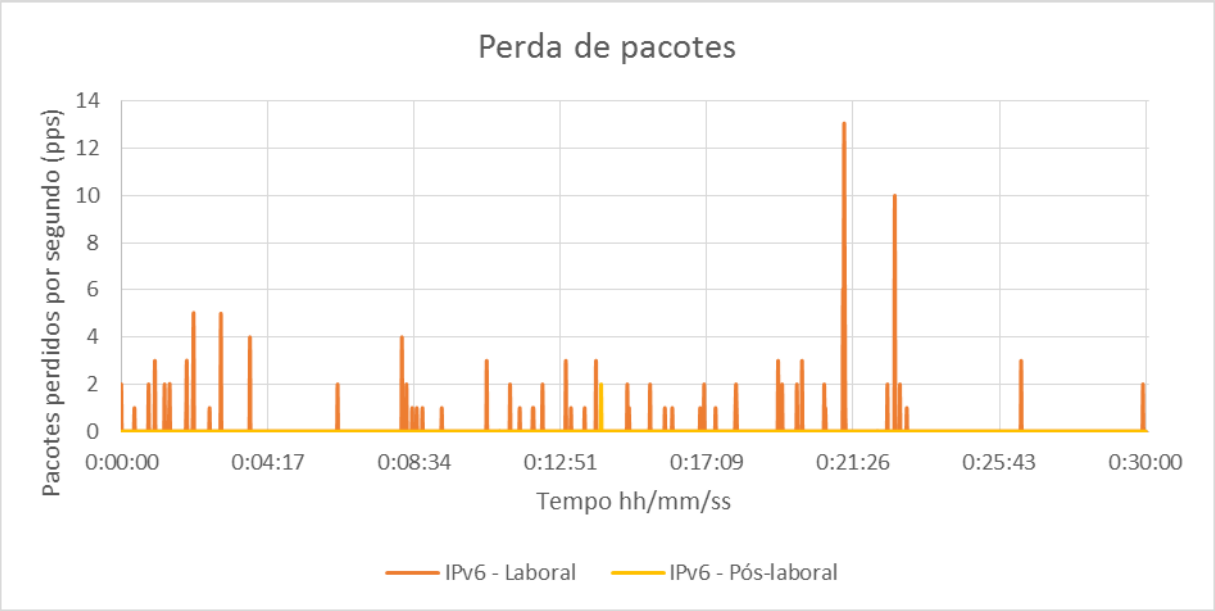


Gráfico 38 – Pacotes perdidos por segundo em tráfego UDP com o protocolo IPv6 em horário laboral e pós-laboral.

4.3.6 Tráfego TCP em IPv6 em horário laboral e pós-laboral

Os resultados obtidos nestas experiências, foram muito semelhantes, onde de acordo com a tabela 22 foram transmitidos mais 3 pacotes em horário laboral e recebidos mais 1536 *bytes*. A variação do atraso também foi muito semelhante em ambas as experiências como representado no gráfico 40. O atraso médio foi superior em 0.819 milissegundos na experiência laboral como representado no gráfico 39.

Tabela 22 – Resumo do tráfego de TCP com o protocolo IPv6 em horário laboral e pós-laboral.

	IPv6 Laboral	IPv6 Pós-laboral
Pacotes transmitidos	460800	460797
Atraso médio	0.019397 s	0.018578 s
Variação média do atraso	0.013768 s	0.013767 s
Bytes recebidos	235929600	235928064
Taxa de transferência média	1048.567983 Kbit/s	1048.568938 Kbit/s
Média de pacotes transmitidos	255.998043 pkt/s	255.998276 pkt/s
Pacotes descartados	0 (0.00 %)	0 (0.00 %)

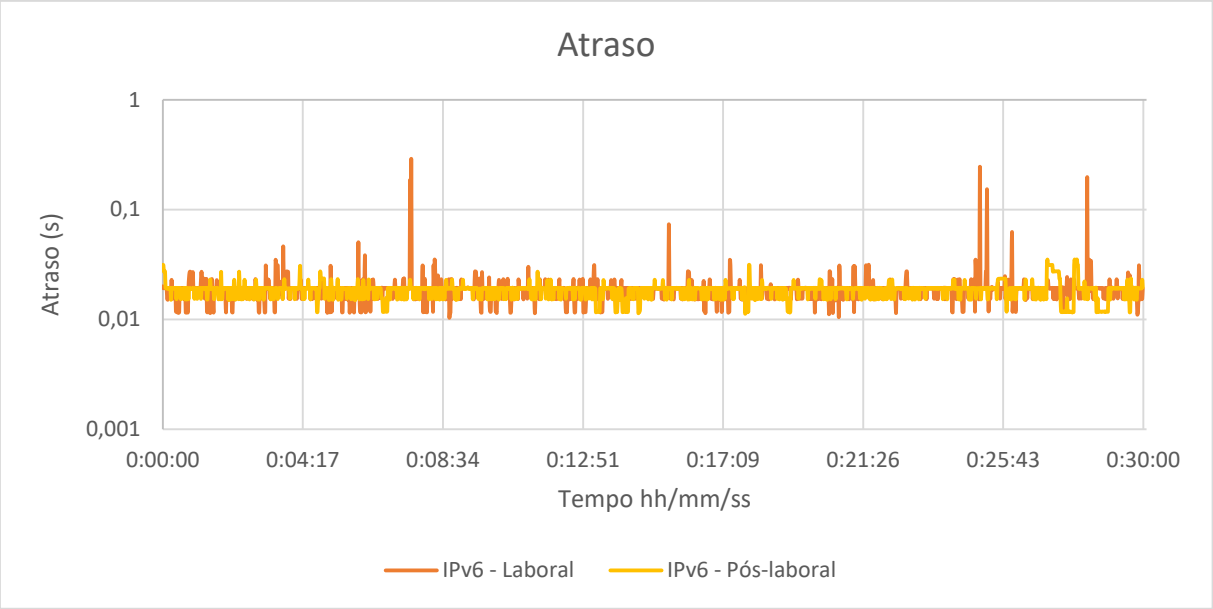


Gráfico 39 – Atraso por segundo em tráfego TCP com o protocolo IPv6 em horário laboral e pós-laboral.

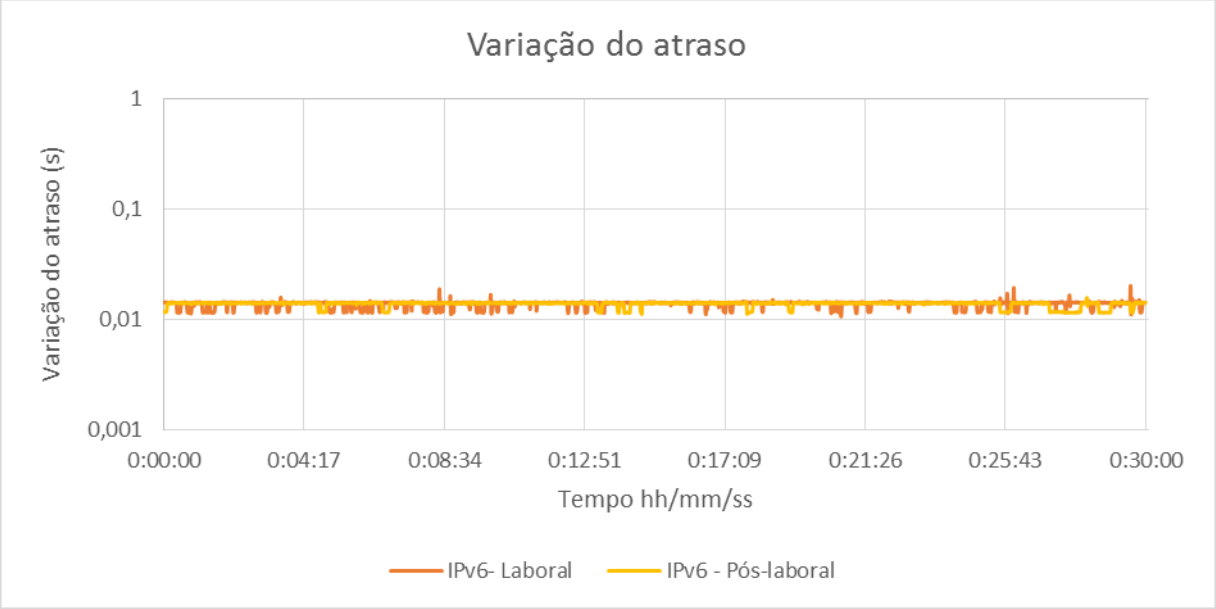


Gráfico 40 – Variação do atraso por segundo em tráfego TCP com o protocolo IPv6 em horário laboral e pós-laboral.

4.3.7 Tráfego *streaming* em IPv6 em horário laboral e pós-laboral

Os resultados que constam da tabela 23 e representados nos gráficos 41 e 42, mostram que o atraso e a variação do atraso foram ligeiramente superiores na experiência em horário laboral onde segundo a tabela 23 o atraso médio foi superior em cerca de 0.061 milissegundos e a variação média do atraso foi também ligeiramente superior com mais 0.142 milissegundos. Como pode ser observado no gráfico 43 houve maior perda de pacotes em horário laboral, onde foram descartados 0.08%, o que representa 184 pacotes

ao que em horário pós-laboral apenas foram descartados 7. Foram transferidos mais 177 pacotes em horário pós-laboral e recebidos mais 239304 *bytes* fruto da perda de pacotes superior na experiência em horário laboral como representado na tabela 23.

Tabela 23 – Resumo do tráfego de *streaming* com o protocolo IPv6 em horário laboral e pós-laboral.

	IPv6 Laboral	IPv6 Pós-laboral
Pacotes transmitidos	216356	216533
Atraso médio	0.015584 s	0.015523 s
Variação média do atraso	0.016891 s	0.016749 s
Bytes recebidos	292513312	292752616
Taxa de transferência média	1300.065003 Kbit/s	1301.28747 Kbit/s
Média de pacotes transmitidos	120.198318 pkt/s	120.296667 pkt/s
Pacotes descartados	184 (0.08 %)	7 (0.00 %)

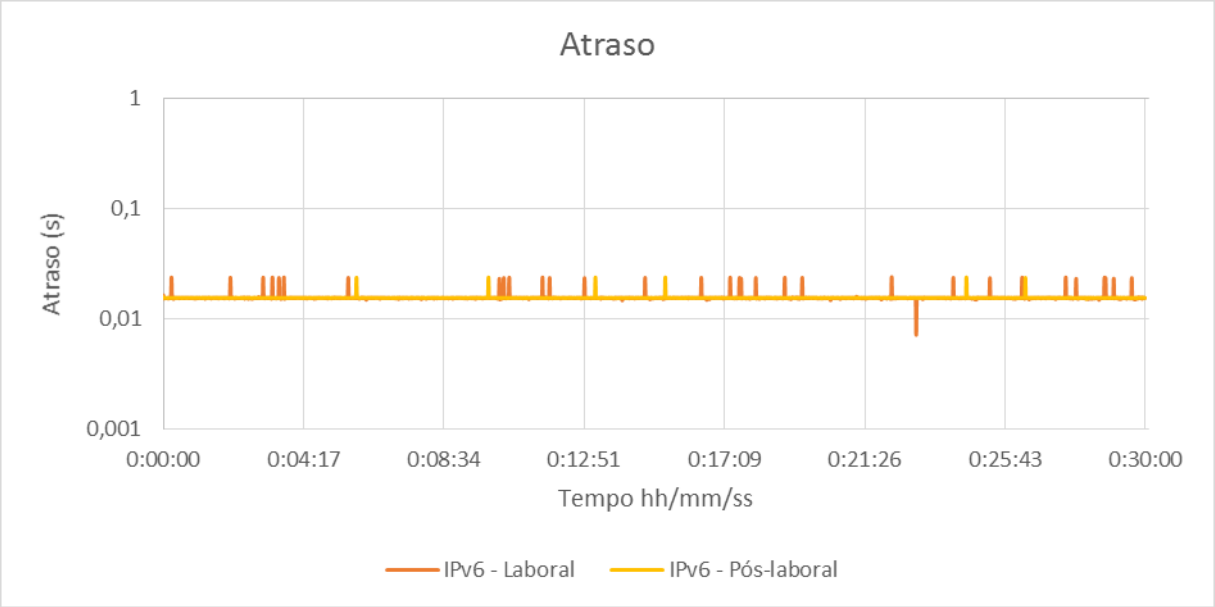


Gráfico 41 – Atraso por segundo em tráfego *streaming* com o protocolo IPv6 em horário laboral e pós-laboral.

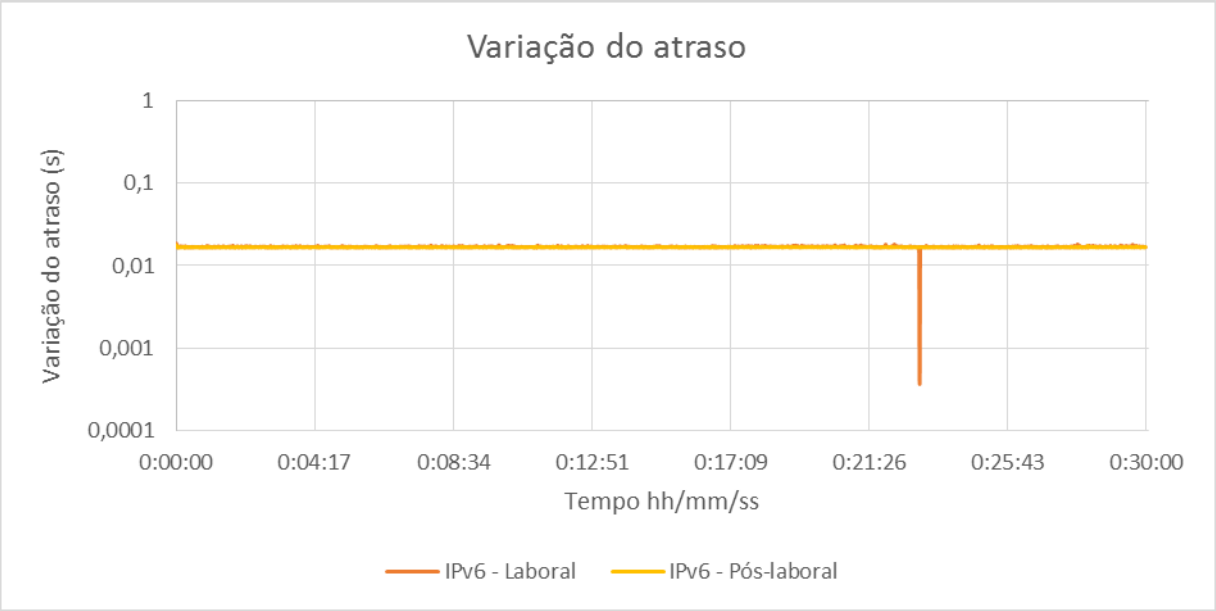


Gráfico 42 – Variação do atraso por segundo em tráfego *streaming* com o protocolo IPv6 em horário laboral e pós-laboral.

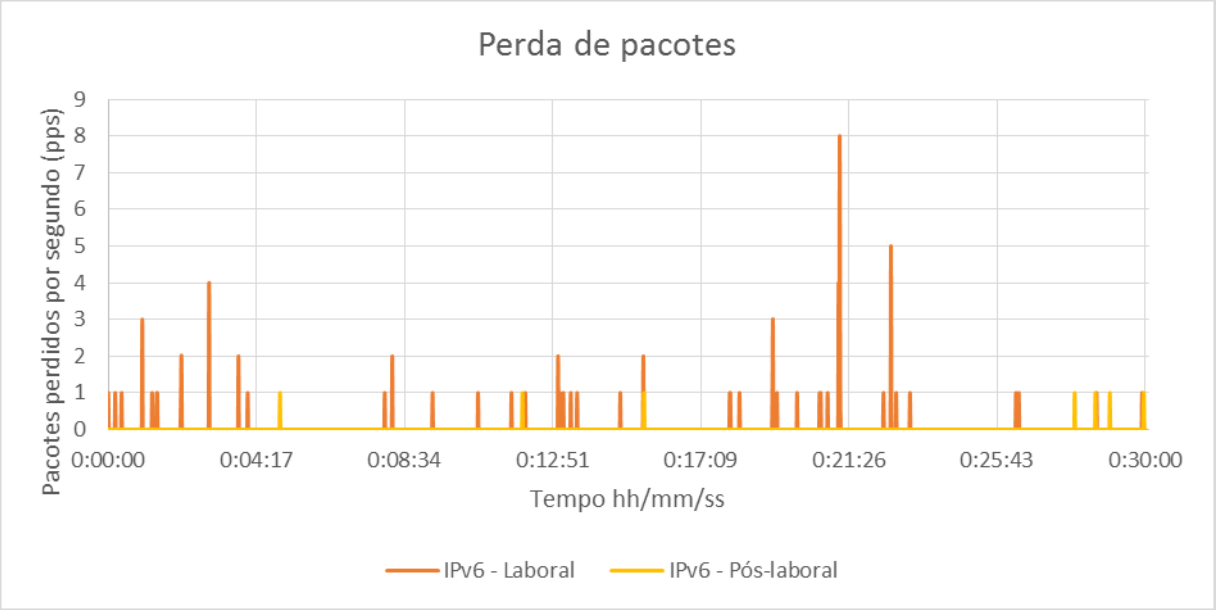


Gráfico 43 – Pacotes perdidos por segundo em tráfego *streaming* com o protocolo IPv6 em horário laboral e pós-laboral.

4.3.8 Tráfego VoIP em IPv6 em horário laboral e pós-laboral

De acordo com os resultados que constam da tabela 24 é possível verificar que foram transmitidos praticamente o mesmo número de pacotes a uma taxa de transferência média e uma média de pacotes transmitidos também muito semelhante embora com uma ligeira superioridade da experiência em horário pós-laboral. Os gráficos 44 e 45 representam

um atraso médio e uma variação do atraso ligeiramente superior em horário laboral, embora pouco expressiva. No gráfico 46 é possível verificar que o numero de pacotes descartados foi muito superior na experiência em horário laboral atingindo os 0.09%.

Tabela 24 – Resumo do tráfego de VoIP com o protocolo IPv6 em horário laboral e pós-laboral.

	IPv6 Laboral	IPv6 Pós-laboral
Pacotes transmitidos	179841	179990
Atraso médio	0.015215 s	0.015166 s
Variação média do atraso	0.020155 s	0.020107 s
Bytes recebidos	16545372	16559080
Taxa de transferência média	73.535396 Kbit/s	73.596319 Kbit/s
Média de pacotes transmitidos	99.912223 pkt/s	99.994999 pkt/s
Pacotes descartados	159 (0.09 %)	10 (0.01 %)

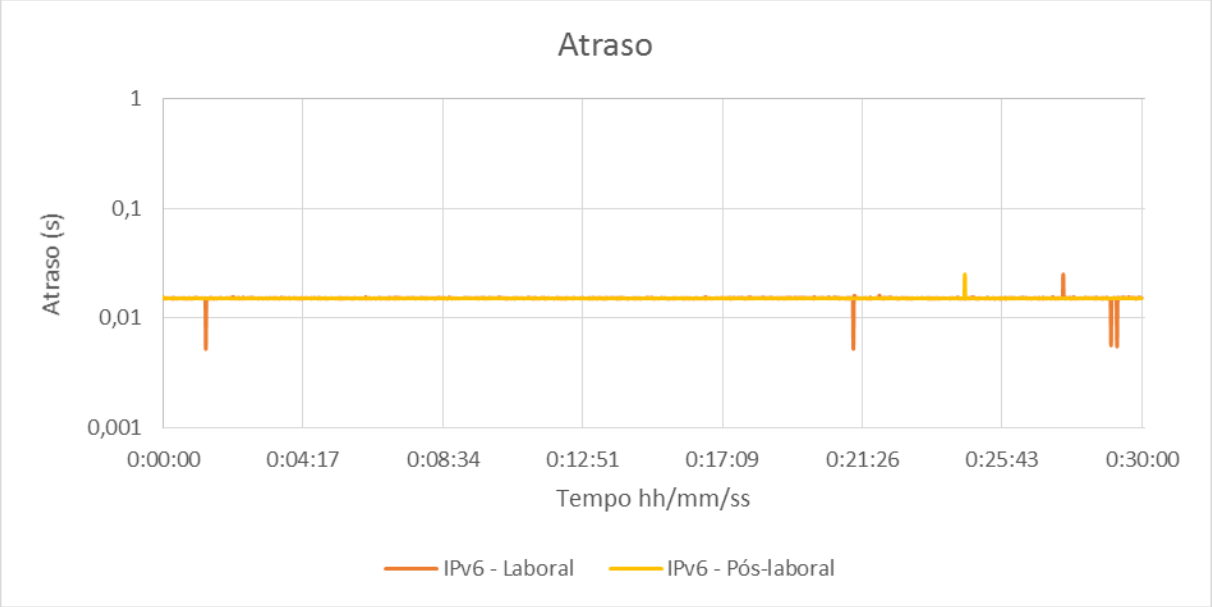


Gráfico 44 – Atraso por segundo em tráfego VoIP com o protocolo IPv6 em horário laboral e pós-laboral.

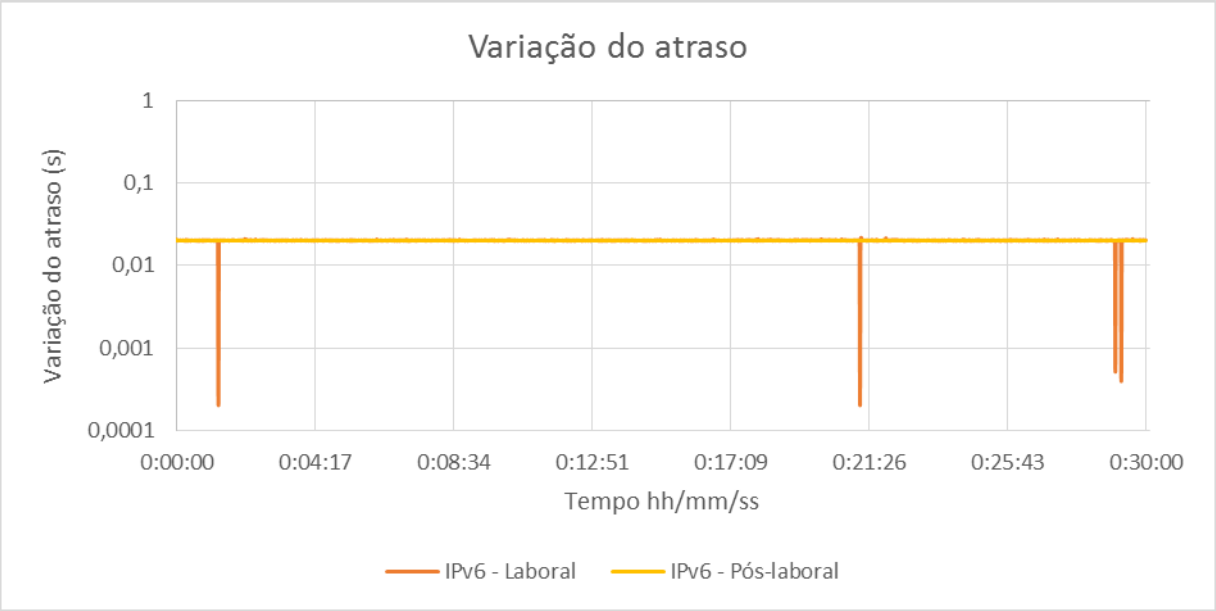


Gráfico 45 – Variação do atraso por segundo em tráfego VoIP com o protocolo IPv6 em horário laboral e pós-laboral.

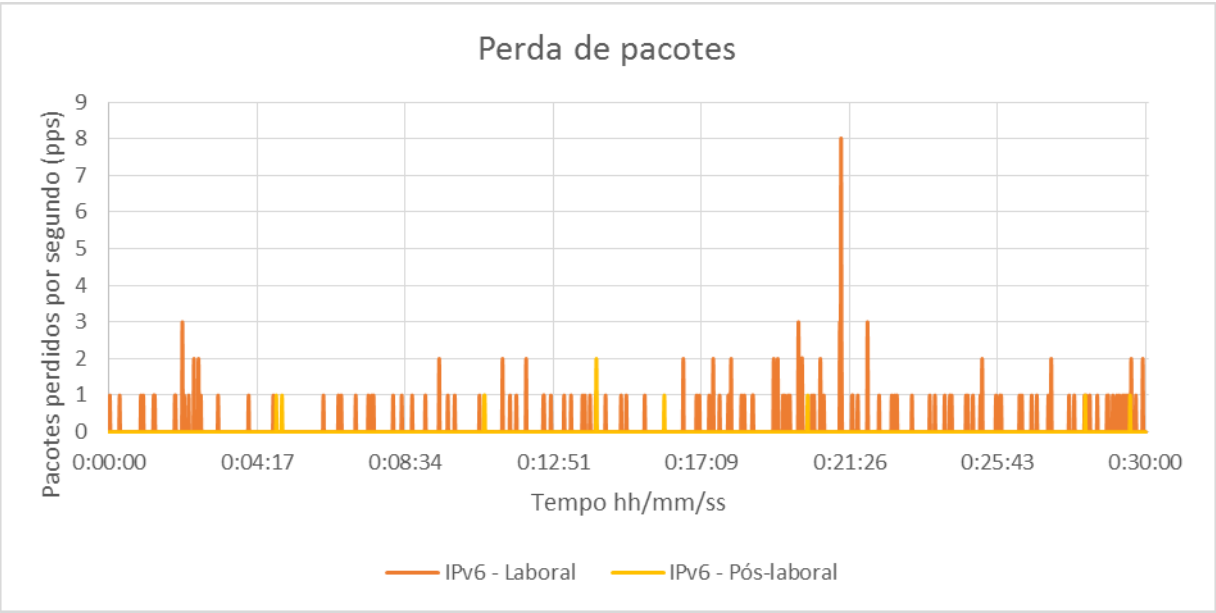


Gráfico 46 – Pacotes perdidos por segundo em tráfego VoIP com o protocolo IPv6 em horário laboral e pós-laboral.

5 Conclusão

Com a actual escassez de disponibilidade de endereços IPv4 (NRO, 2016) é imperativo fazer uma transição (co-existência) das redes existentes para o protocolo IPv6, e para esse mesmo efeito existe um vasto conjunto de ferramentas de transição disponíveis em que cada uma delas tem as suas vantagens e desvantagens mas, não existe uma única melhor solução, sendo que o plano de transição deve ser específico em cada contexto.

Antes de partir para uma transição para o protocolo IPv6, é necessário verificar a qualidade de serviço (QoS), que nos dias de hoje é cada vez mais importante visto que com o desenvolvimento de equipamentos mais sofisticados e de novas tecnologias as redes estão a tornar-se cada vez mais complexas. Desta forma é mais complicado assegurar qualidade de serviço para aplicações e serviços (nomeadamente aqueles com características de tempo-real).

Esta análise, efectuada entre dois nós da rede de investigação e ensino Portuguesa (RCTS) com recurso ao *software* D-ITG visou analisar em momentos distintos 4 tipos de tráfego, onde se verificou um bom desempenho por parte do *software* seleccionado, sendo que as conclusões sobre o desempenho do protocolo IPv4 e IPv6 na rede foram as seguintes:

- como era de esperar, sendo o volume de tráfego em horário laboral superior ao horário pós-laboral, verificou-se de forma geral que o atraso, variação do atraso e a perda de pacotes foi menor no 2º horário;
- em todos os cenários da experiência foram descartados muitos pacotes (0.04% em horário laboral e 0.0016% em horário pós-laboral) tendo em especial atenção os pacotes do protocolo IPv6, sendo que a razão para essa ocorrência possa estar relacionada com a sobrecarga nos *routers* em máquinas intermédias que não são controladas pela RCTS como por exemplo o router UBI.IPv6.fccn.pt (2001:690:810:24::2) que teve um incremento de 15.572ms em relação ao router do Porto da FCCN sendo possível que algumas das maquinas intermédias por onde o pacote passe sejam antigas e/ou o IPv6 não seja suportado na totalidade, pois os fabricantes de dispositivos mais antigos projectados para rotear pacotes IPv4 sofreram actualizações de software para suportar IPv6, mas os ASICs (Einspruch & Hilbert, 2012), podem não ter sido actualizados, o que faz com que o tráfego IPv6 sofra uma degradação de desempenho (Safruti & Kuperman, 2011);
- verificou-se também que em todos os cenários da experiência o atraso e a variação do atraso é menor com o protocolo IPv6, à excepção do protocolo TCP, onde a variação do atraso é ligeiramente superior (13.768 milissegundos

em horário laboral e 13.767 milissegundos em horário pós-laboral), mas mesmo assim este facto é bastante positivo, pois significa que os equipamentos respondem melhor aos pedidos IPv6 do que aos pedidos IPv4. Mesmo com a excepção da variação do atraso no protocolo IPv6, em que a explicação se deve ao facto de que nas outras experiências o valor dos pacotes descartados no protocolo IPv6 ser superior e no protocolo TCP haja a existência de retransmissões que aumentam a variação do atraso;

- Na experiência de VoIP, a ITU-T (ITU-T, Recommendation ITU-T G.711.1, 2012) recomenda que para uma ligação razoável a perda de pacotes não seja superior a 1% e o atraso seja menor que 300 ms (Cox, Neto, Lamblin, & Sherif, 2009), condições que se verificaram em ambos os cenários;
- Na experiência de *streaming*, para que ocorra uma boa interacção entre o emissor e o receptor numa transmissão de *streaming* com o *codec* H.323, a ITU-T (ITU-T, H.323 - Packet-based multimedia communications, 2009) tal como para o tipo de transmissão anterior, recomenda que o atraso para um bom desempenho numa interacção seja mantido abaixo dos 250 ms (Janevski, 2003), pelo que nesta experiência os valores ficaram dentro dos valores aceitáveis em ambos os ambientes. Segundo vários autores (*e.g.* Calyam, Sridharan, Mandrawa, & Schopis) os níveis de perda de pacotes superiores a 1% afectam a qualidade do audiovisual, embora não existam limites de perda de pacotes definidos. Nesta experiência verificou-se uma perda mínima de pacotes em ambos os ambientes.

É possível concluir que o protocolo IPv6 em termos gerais (e especificamente com os meios utilizados) tem um desempenho ligeiramente superior ao IPv4 segundo os parâmetros definidos, quer seja em ambientes híbridos quer seja com a rede congestionada ou não.

O facto de não existirem grandes disparidades entre ambos os protocolos é visto como muito positivo, pois em termos de taxas de transferência e número de pacotes transmitidos os valores são bastante semelhantes, sendo que em termos de atraso e variação do atraso o IPv6 é inferior e nas perdas de pacotes o IPv6 foi superior pelas razões explicadas anteriormente.

O protocolo IPv6 está bem estruturado e foi construído com base na experiência adquirida com o protocolo IPv4, onde foram adicionadas novas funcionalidades, permitindo novas e melhores formas de comunicação, mas mesmo assim existem ainda barreiras à sua implementação, tais como a falta de conteúdos IPv6 na Internet, a necessidade de actualizar equipamentos no caso dos existentes não serem compatíveis com IPv6, receios com

problemas de segurança que possam vir a existir e muitos outros. No entanto, devido à escassez dos endereços IPv4, o IPv6 será o protocolo predominante no futuro. Este momento pode ainda demorar 5, 10 ou 20 anos, mas isso é algo inevitável.

É esperado que este estudo possa de alguma forma desmistificar algumas preocupações sobre o desempenho do IPv6 e contribuir para tornar mais célere a implementação do protocolo IPv6, para que num futuro próximo seja também implementado no meio empresarial. É também esperado que este estudo possa de alguma forma ajudar outros investigadores, fornecendo elementos úteis para futuras investigações.

5.1 Limitações e trabalho futuro

Este trabalho visou estudar a eficiência da comunicação entre os protocolos IPv4 e IPv6 entre dois nós da rede de investigação e ensino Portuguesa (RCTS), mas existem temas que não foram estudados, ou podem ser mais aprofundados, tais como as ameaças de segurança que possam vir exclusivamente associadas ao uso do IPv6, ficando para trabalho futuro um estudo sobre a segurança no protocolo IPv6 e nomeadamente em relação aos vários mecanismos de transição. Um estudo sobre o IPv6 em redes móveis ou de suporte à mobilidade com o MIPv6 será também uma possibilidade.

Outro possível tema para investigar futuramente seria a realização de um teste com características semelhantes ao apresentado nesta tese, quando a rede for na totalidade a 10 Gb/s sem interferência de outros operadores externos, mas com outros níveis de carga, com outros *codecs* de áudio e *vídeo* e com sistemas operativos diferentes.

Referências bibliográficas

Agarwal, P., & Akyol, B. (Janeiro de 2003). *RFC - 3443 - Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks.* Obtido de https://tools.ietf.org/html/rfc3443

Alessio, B., Alberto, D., & Antonio, P. (2009). *Multi-Protocol and Multi-Platform Traffic Generation and Measurement*. Obtido de http://www.grid.unina.it/software/ITG/

Al-Gadi, G. Y., Mustafa, A. B., & Hamied, M. A. (August de 2014). Evaluation and Comparisons of Migration Techniques From IPv4 To IPv6 Using GNS3 Simulator. *IOSR Journal of Engineering (IOSRJEN)*, PP 51-57.

Almes, G., Mundrane, M., Polichar, V., & Anderson, C. (Outubro de 2013). Transition to IPv6. Education Center for Analysis and Research.

Almquist, P. (Julho de 1992). *RFC 1349.* Obtido de https://tools.ietf.org/html/rfc1349

António, M. G. (2013). *Estudo do impacto do tamanho máximo da carga da trama Ethernet no perfil do tráfego IPv6 na Internet.* Lisboa: Universidade Lusófona de Humanidades e Tecnologias.

Apple. (2001). Obtido de http://www.apple.com/osx/

Apple. (2007). Obtido de http://www.apple.com/ios

Arkko, J., & Baker, F. (Maio de 2011). *RFC 6180.* Obtido de Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment: https://tools.ietf.org/html/rfc6180

ARPANET. (1 de Janeiro de 1983). *TCP/IP - History of Computers*. Obtido de http://www.history-computer.com/Internet/Maturing/TCPIP.html

Avallone, S., Pescapè, A., & Ventre, G. (Novembro de 2003). Distributed Internet Traffic Generator (D-ITG): analysis and experimentation over heterogeneous networks. Obtido de http://traffic.comics.unina.it/software/ITG/D-ITGpublications/29URCININA-ICNP2003poster.pdf

Babatunde, O., & Al-Debagy, O. (2014). A Comparative Review Of Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6). *International Journal of Computer Trends and Technology (IJCTT)*, 10-13.

Babiazrz, J., Chan, K., & Baker, F. (Agosto de 2006). *RFC 4594.* Obtido de http://www.ietf.org/rfc/rfc4594.txt

Bagnulo, M., Matthews, P., & Van Beijnum, I. (Abril de 2011). *RFC 6146.* Obtido de Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers: https://tools.ietf.org/html/rfc6146

Bagnulo, M., Sullivan, A., Matthews, P., & Van Beijnum, I. (Abril de 2011). *RFC 6147.* Obtido de DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers: https://tools.ietf.org/html/rfc6147

Bahaman, N., Erman, H., & Prabuwono, A. S. (2012). Network Performance Evaluation of 6to4 Tunneling. *nternational Conference on Innovation, Management and Technology Research (ICIMTR2012), Malacca, Malaysia.* Malacca: IEEE.

Baker, F. (Fevereiro de 2009). *Internet Society* . Obtido de IPv4/IPv6 Coexistence and Transition: http://www.internetsociety.org/articles/ipv4ipv6-coexistence-and-transition

Berners-Lee, T., Leach, P., Masinter, L., Frystyk, H., Mogul, J., Gettys, J., & Fielding, R. (Junho de 1999). *RFC 2616.* Obtido de https://www.rfc-editor.org/rfc/rfc2616.txt

Botta, A., Donato, W. d., Dainotti, A., Avallone, S., & Pescapè, A. (2013). *D-ITG 2.8.1 Manual.* COMICS (COMputer for Interaction and CommunicationS) Group Department of Electrical Engineering and Information Technologies University of Napoli Federico II.

Brito, S. B. (2013). *IPv6 - O novo protocolo da Internet.* São Paulo - Brasil: Novatec.

Casner, S., & Jacobson, V. (Fevereiro de 1999). *RFC - 2508 - Compressing IP/UDP/RTP Headers for Low-Speed Serial Links.* Obtido de http://www.ietf.org/rfc/rfc2508.txt?number=2508

Cisco Systems. (2002). IP Telephony: The Fine Nines Story. p. 17.

Cisco Systems. (16 de Março de 2013). Comunicação através da Rede. *Cisco Networking Academy*. Santarém.

Combs, G. (Julho de 1998). *Wireshark.* Obtido de www.wireshark.org

Creswell, J. (2014). *Research Design - Quantitative, Quantitative and Mixed Methods Approaches.* California: Sage Publications.

Deering, S., & Hinden, R. (Dezembro de 1998). *RFC 2460.* Obtido de Internet Protocol, Version 6 (IPv6): https://tools.ietf.org/html/rfc2460

Despres, R. (Janeiro de 2010). *RFC 5569.* Obtido de IPv6 Rapid Deployment on IPv4 Infrastructures (6rd): https://tools.ietf.org/html/rfc5569

Domingos , F. D. (2011). TECNICA DE TRANSIÇÃO ENTRE REDES IPV4/IPV6. *Revista de Ciências Exatas e Tecnologia*.

Duke, M., Braden, R., Eddy, W., Blanton, E., & Zimmermann, A. (Fevereiro de 2015). *RFC 7414.* Obtido de A Roadmap for Transmission Control Protocol (TCP): https://tools.ietf.org/html/rfc7414

Durand, A., Droms, R., Woodyatt, J., & Lee, Y. (Agosto de 2011). *RFC 6333.* Obtido de Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion: https://tools.ietf.org/html/rfc6333

Einspruch, N., & Hilbert, J. (2012). *Application Specific Integrated Circuit (ASIC) Technology.* California: Academic Press.

FCCN. (28 de Julho de 2016). *FCT - Fundação para a Ciencia e Tecnologia*. Obtido de FCCN - Computação Cientifica Nacional: https://www.fccn.pt/pt/rede-academica/a-rede-ciencia-tecnologia-e-sociedade-rcts/

Fenner, B., & Flick, J. (Junho de 2005). *RFC 4113.* Obtido de Management Information Base for the User Datagram Protocol (UDP): https://tools.ietf.org/html/rfc768

FreeBSD-Project. (1993). Obtido de www.freebsd.org

Friaças, C. (2016). O Estado do IPv6 na RCTS. *IPv6 em Portugal: Diagnóstico e Perspectiva.* Lisboa.

Friaças, C., Domingues, M., Massano, E., & Veiga, P. (2008). Probing Next Generation Portuguese Academic. (pp. 301-310). Emerald.

Garcia, N. M., Taludker, A. K., & Jayateertha, G. (2013). *Convergence through all IP Networks.* Singapore: Pan Stanford Publishing.

Gates, B., & Allen, P. (1985). Obtido de https://www.microsoft.com/pt-pt/windows

Google. (2008). Obtido de www.android.com

Hinden, R., & Deering, S. (Julho de 1998). *RFC 2373.* Obtido de IP Version 6 Addressing Architecture: https://tools.ietf.org/html/rfc2373

Huitema, C. (Fevereiro de 2006). *RFC 4380.* Obtido de Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs): https://www.ietf.org/rfc/rfc4380.txt

IEEE. (17 de Março de 2016). *IEEE Explore*. Obtido de http://ieeexplore.ieee.org/search/advsearch.jsp

ISO. (1984). *ISO - International Organization for Standardization*. Obtido de www.iso.org

ITU-T. (Fevereiro de 1998). ITU-T Recommendation H.323.

Jones, Rick - Hewlett-Packard. (15 de Fevereiro de 1996). Netperf 2.1. Obtido de http://users.informatik.haw-hamburg.de/~schulz/pub/Rechnernetze/tools/netperf.pdf

Kent, S., & Seo, K. (Dezembro de 2005). *RFC 4301.* Obtido de Security Architecture for the Internet Protocol: https://tools.ietf.org/html/rfc4301

Kleinrock, L. (30 de August de 1969). *ARPANET – The First Internet*. Obtido de http://www.livinginternet.com/i/ii_arpanet.htm

Kohler, E., Handley, M., & Floyd, S. (Março de 2006). *RFC - 4340 - Datagram Congestion Control Protocol (DCCP).* Obtido de https://tools.ietf.org/html/rfc4340

Kuarsingh, V., Lee, Y., & Vautrin, O. (Setembro de 2012). *RFC 6732.* Obtido de 6to4 Provider Managed Tunnels: https://tools.ietf.org/html/rfc6732

Kumar, G. S., & Kumar, N. S. (2016). Internet of Things - A Communication Protocol Perspective. *CSI Communications - Knowledge Digest for IT Community*, 11-13.

Lattner, T., Cook, D., & Gibbs, K. (Outubro de 2003). Jperf 1.0. Obtido de http://web.archive.org/web/20081012104244/http://www.dast.nlanr.net/projects/jperf/

McCann, J., Deering, S., & Mogul, J. (Agosto de 1996). *RFC 1981.* Obtido de Path MTU Discovery for IP version 6: https://tools.ietf.org/html/rfc1981

Mockapetris, P. (Novembro de 1983). *RFC - 882 - DOMAIN NAMES - CONCEPTS and FACILITIES.* Obtido de https://tools.ietf.org/html/rfc882

Mogul, J., & Postel, J. (August de 1985). *RFC950.* Obtido de Internet Standard Subnetting Procedure: https://tools.ietf.org/html/rfc950

Nguyen , Q. A., & Nguyen , P. N. (2012). TRANSITION FROM IPv4 TO IPv6. *Best Transition Method for Large Enterprise Networks*.

Nichols, K., Blake, S., Baker, F., & Black, D. (Dezembro de 1998). *RFC - 2474 - Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.* Obtido de https://tools.ietf.org/html/rfc2474

Nichols, K., Blake, S., Baker, F., & Black, D. (Dezembro de 1998). *RFC 2474.* Obtido de https://tools.ietf.org/html/rfc2474

Nordmark, E. (Fevereiro de 2000). *RFC 2765.* Obtido de Stateless IP/ICMP Translation Algorithm (SIIT): https://tools.ietf.org/html/rfc2765

Nordmark, E., & Gilligan, R. (Outubro de 2005). *RFC 4213.* Obtido de Basic Transition Mechanisms for IPv6 Hosts and Routers: https://tools.ietf.org/html/rfc4213

NRL - Naval Research Laboratory. (Setembro de 2014). TRPR Version 2.1b2. *Tcpdump Rate Plot Real Time Version 2.1b2*. Obtido de http://downloads.pf.itd.nrl.navy.mil/docs/proteantools/trpr.html

NRL - Naval Research Laboratory. (16 de Abril de 2015). Multi-Generator (MGEN) Version 5.0. Obtido de Naval Research Laboratory: http://www.nrl.navy.mil/itd/ncs/products/mgen

NRO. (2016). *Internet Number Resource Status Report - 30 June 2016.* Number Resource Organization .

Open-Group, T. (Janeiro de 2000). Data Link Provider Interface.

Ozer, J. (26 de Fevereiro de 2011). *What is Streaming?* Obtido de Streaming Media: http://www.streamingmedia.com/Articles/ReadArticle.aspx?ArticleID=74052

Péricas, F. A. (2012). *Redes de Computadores - Conceitos e a Arquitetura Internet.* Blumenau: Edição de Autor.

Pescapè, A., Avallone, S., Guadagno, S., & Emma, D. (2004). D-ITG Distributed Internet Traffic Generator. *First International Conference on the Quantitative Evaluation os Systems.*

Ramirez, J., Górriz, M., & Segura, C. (Junho de 2007). Voice Activity Detection. Fundamentals and Speech Recognition System Robustness. Obtido de http://cdn.intechopen.com/pdfs/104/InTech-Voice_activity_detection_fundamentals_and_speech_recognition_system_robustness.pdf

Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., & Lear, E. (Fevereiro de 1996). *RFC 1918.* Obtido de Address Allocation for Private Internets: https://tools.ietf.org/html/rfc1918

Réseaux IP Européens. (s.d.). *RIPE Network Coordination Centre*. Obtido de https://www.ripe.net/

RIPE. (22 de Setembro de 2016). *RIPE NCC*. Obtido de RIPE NETWORK COORDINATION CENTRE: http://v6asns.ripe.net/v/6?s=_ALL;s=PT

RIR. (19 de Setembro de 2016). *Regional Internet Registries Statistics*. Obtido de Portugal (PT) - IPv6 address statistics (in /32 blocks): http://www-public.tem-tsp.eu/~maigron/RIR_Stats/RIPE_Allocations/IPv6/ByNb/PT.html

Safruti, I., & Kuperman, M. (15 de Fevereiro de 2011). *Avoiding the pitfalls when transitioning to IPv6*. Obtido de Techworld: http://www.techworld.com/tutorial/networking/avoiding-the-pitfalls-when-transitioning-to-ipv6-3261102/

Sathu, H., & Shah, M. (2012). Performance Monitoring of VoIP with Multiple Codecs Using IPv4 and IPv6to4 Tunnelling Mechanism on Windows and Linux. *International Journal of Modeling and Optimization*, Vol. 2, No. 3.

Schulzrinne, H., Casner, S., Frederick, R., & Jacobson, V. (Julho de 2003). *RFC 3550.* Obtido de RTP - A Transport Protocol for Real-Time Applications: https://tools.ietf.org/html/rfc3550

Semken, V. (Dezembro de 2004). Graphical User Interface for D-ITG. Obtido de http://www.semken.com/projekte/index.html

Sharma, S., & Chauhan, D. (2014). A Survey on Next Generation Internet Protocol: IPv6. *International Journal of Electronics and Electrical Engineering Vol2, No2.* Engineering and Technology Publishing.

Shiranzaei, A., & Khan, R. Z. (2015). A Comparative Study on IPv4 and IPv6. *International Journal of Advanced Information Science and Technology (IJAIST)*, 9-16.

Shiwani, S., Purohit, G., & Hemrajani, N. (2011). Performance Analysis of IPv4 v/s IPv6 in Virtual Environment Using UBUNTU. *International Journal of Computer Applications (IJCA) - International Conference on Computer Communication and Networks*.

Silva, P. H., & Júnior, N. A. (2014). Ferramenta IPERF: geração e medição de Tráfego TCP e UDP. *CBPF.* Rio de Janeiro - Brasil.

Silva, R. (2011). *Tecnoblog*. Obtido de https://tecnoblog.net/62581/enderecos-ipv4-esgotam-asia/

Srivats, P. (11 de Abril de 2010). Ostinato version 0.1. Obtido de http://ostinato.org/

Stewart, R., Xie, Q., Morneault, K., Sharp, C., Schwarzbauer, H., Taylor, T., . . . Paxson, V. (Outubro de 2000). *RFC - 2960 - Stream Control Transmission Protocol.* Obtido de https://tools.ietf.org/html/rfc2960

Templin, F., Gleeson, T., Talwar, M., & Thaler, D. (Outubro de 2005). *RFC 4214.* Obtido de Intra-Site Automatic Tunnel Addressing Protocol (ISATAP): http://www.rfc-base.org/rfc-4214.html

Thomson, S., Huitema, C., Ksinant, V., & Souissi, M. (Outubro de 2003). *RFC 3596.* Obtido de DNS Extensions to Support IP Version 6: https://www.ietf.org/rfc/rfc3596.txt

Tirumala, A., Qin, F., Dugan, J., Ferguson, J., & Gibbs, K. (13 de Março de 2003). Iperf 1.7.0. Obtido de Distributed Applications Support Team: http://web.archive.org/web/20081012013349/http://dast.nlanr.net/Projects/Iperf/

Torvalds, L. (1991). Obtido de https://www.linux.com

Tsirtsis, G., & Srisuresh, P. (Fevereiro de 2000). *RFC 2766.* Obtido de Network Address Translation - Protocol Translation (NAT-PT): https://www.ietf.org/rfc/rfc2766.txt

Uzelac, A., & Lee, Y. (Novembro de 2011). *RFC 6405 - Voice over IP (VoIP) SIP Peering Use Cases.* Obtido de https://tools.ietf.org/html/rfc6405

VideoLAN. (1 de Fevereiro de 2001). *VideoLAN - Official page for VLC media player*. Obtido de videolan.org/vlc/

World IPv6 Launch. (25 de Agosto de 2016). *World IPv6 Launch*. Obtido de http://www.worldipv6launch.org/

Apêndice I

Abaixo está o script utilizado nas duas experiências contendo os logs com os resultados devolvidos pela aplicação, que foram a base para a representação dos gráficos apresentados no capítulo 4.

Gerador de tráfego – D-ITG

O *software* D-ITG foi utilizado para gerar tráfego nesta experiência. Os seguintes comandos foram utilizados para gerar e receber tráfego.

ITGDec: É o componente responsável pela análise dos arquivos de log para extrair métricas de desempenho relacionadas com os fluxos de tráfego.

ITGRecv: Recebe os fluxos de dados enviados pelo emissor. É por este comando que o receptor abre uma porta e recebe os dados enviados pelo emissor.

ITGSend: Gera fluxos de tráfego. O script seguinte foi utilizado na experiência de modo a gerar 8 fluxos em simultâneo.

Script utilizado nas experiências

-a 2001:690:2300:2::1 -rp 10001 -m rtm -C 256 -c 512 -t 1800000 -T UDP

-a 193.136.65.1 -rp 10002 -m rtm -C 256 -c 512 -t 1800000 -T UDP

-a 2001:690:2300:2::1 -rp 10003 -m rtm -C 256 -c 512 -t 1800000 -T TCP

-a 193.136.65.1 -rp 10004 -m rtm -C 256 -c 512 -t 1800000 -T TCP

-a 2001:690:2300:2::1 -rp 10005 -m rtm -b 136 -C 120.3 -c 1352.5 -t 1800000 -T UDP

-a 193.136.65.1 -rp 10006 -m rtm -b 136 -C 120.3 -c 1352.5 -t 1800000 -T UDP

-a 2001:690:2300:2::1 -rp 10001 -m rtm -t 1800000 VoIP

-a 193.136.65.1 -rp 10002 -m rtm -t 1800000 VoIP

O resultado dos ficheiros de log gerados estão representados abaixo.

Horário laboral

UDP

Flow number: 1

From 2001:690:810:36:8fa9:7b5c:f303:ed5:33941

To 2001:690:2300:2::1:10001

Total time = 1799.996065 s

Total packets = 460370

Minimum delay = 0.000005 s

Maximum delay = 1.003964 s
Average delay = 0.015333 s
Average jitter = 0.008109 s
Delay standard deviation = 0.108303 s
Bytes received = 235709440
Average bitrate = 1047.599801 Kbit/s
Average packet rate = 255.761670 pkt/s
Packets dropped = 430 (0.09 %)
Average loss-burst size = 1.159030 pkt

Flow number: 2
From 193.137.75.172:43889
To 193.136.65.1:10002

Total time = 1799.995709 s
Total packets = 460658
Minimum delay = 0.000006 s
Maximum delay = 1.003970 s
Average delay = 0.017008 s
Average jitter = 0.008778 s
Delay standard deviation = 0.125726 s
Bytes received = 235856896
Average bitrate = 1048.255370 Kbit/s
Average packet rate = 255.921721 pkt/s
Packets dropped = 142 (0.03 %)
Average loss-burst size = 1.256637 pkt

TCP

Flow number: 3
From 2001:690:810:36:8fa9:7b5c:f303:ed5:44348
To 2001:690:2300:2::1:10003

Total time = 1800.013762 s
Total packets = 460800

Minimum delay = 0.000002 s
Maximum delay = 1.252035 s
Average delay = 0.019397 s
Average jitter = 0.013768 s
Delay standard deviation = 0.124679 s
Bytes received = 235929600
Average bitrate = 1048.567983 Kbit/s
Average packet rate = 255.998043 pkt/s
Packets dropped = 0 (0.00 %)
Average loss-burst size = 0.000000 pkt

Flow number: 4
From 193.137.75.172:41418
To 193.136.65.1:10004

Total time = 1800.002390 s
Total packets = 460797
Minimum delay = 0.000001 s
Maximum delay = 1.131051 s
Average delay = 0.021446 s
Average jitter = 0.012229 s
Delay standard deviation = 0.135100 s
Bytes received = 235928064
Average bitrate = 1048.567781 Kbit/s
Average packet rate = 255.997993 pkt/s
Packets dropped = 0 (0.00 %)
Average loss-burst size = 0.000000 pkt

Streaming

Flow number: 5
From 2001:690:810:36:8fa9:7b5c:f303:ed5:60851
To 2001:690:2300:2::1:10005

Total time = 1799.991916 s

Total packets = 216356
Minimum delay = 0.000008 s
Maximum delay = 1.008310 s
Average delay = 0.015584 s
Average jitter = 0.016891 s
Delay standard deviation = 0.091572 s
Bytes received = 292513312
Average bitrate = 1300.065003 Kbit/s
Average packet rate = 120.198318 pkt/s
Packets dropped = 184 (0.08 %)
Average loss-burst size = 1.051429 pkt

Flow number: 6
From 193.137.75.172:48317
To 193.136.65.1:10006

Total time = 1799.993622 s
Total packets = 216467
Minimum delay = 0.000007 s
Maximum delay = 1.008346 s
Average delay = 0.017033 s
Average jitter = 0.019114 s
Delay standard deviation = 0.103590 s
Bytes received = 292663384
Average bitrate = 1300.730760 Kbit/s
Average packet rate = 120.259871 pkt/s
Packets dropped = 73 (0.03 %)
Average loss-burst size = 1.158730 pkt

VoIP

Flow number: 7
From 193.137.75.172:49111
To 193.136.65.1:10008

Total time = 1799.989308 s
Total packets = 179930
Minimum delay = 0.000013 s
Maximum delay = 1.009961 s
Average delay = 0.016885 s
Average jitter = 0.020832 s
Delay standard deviation = 0.103632 s
Bytes received = 16553560
Average bitrate = 73.571815 Kbit/s
Average packet rate = 99.961705 pkt/s
Packets dropped = 70 (0.04 %)
Average loss-burst size = 1.093750 pkt

Flow number: 8
From 2001:690:810:36:8fa9:7b5c:f303:ed5:51216
To 2001:690:2300:2::1:10007

Total time = 1799.989980 s
Total packets = 179841
Minimum delay = 0.000026 s
Maximum delay = 1.008709 s
Average delay = 0.015215 s
Average jitter = 0.020155 s
Delay standard deviation = 0.099461 s
Bytes received = 16545372
Average bitrate = 73.535396 Kbit/s
Average packet rate = 99.912223 pkt/s
Packets dropped = 159 (0.09 %)
Average loss-burst size = 1.067114 pkt

********** TOTAL RESULTS **********

Number of flows = 8
Total time = 1800.082256 s
Total packets = 2635219

Minimum delay = 0.000001 s
Maximum delay = 1.252035 s
Average delay = 0.017237625 s
Average jitter = 0.0149845 s
Delay standard deviation = 0.119334 s
Bytes received = 1561699628
Average bitrate = 6940.57519 Kbit/s
Average packet rate = 1463.95394 pkt/s
Packets dropped = 1058 (0.04 %)
Average loss-burst size = 1.148199 pkt
Corrupted log records = 0

Pós-laboral

UDP

Flow number: 1
From 2001:690:810:36:8fa9:7b5c:f303:ed5:39092
To 2001:690:2300:2::1:10001

Total time = 1799.996206 s
Total packets = 460780
Minimum delay = 0.000006 s
Maximum delay = 1.003924 s
Average delay = 0.015286 s
Average jitter = 0.007932 s
Delay standard deviation = 0.107783 s
Bytes received = 235919360
Average bitrate = 1048.532699 Kbit/s
Average packet rate = 255.989428 pkt/s
Packets dropped = 20 (0.00 %)
Average loss-burst size = 1.250000 pkt

Flow number: 2
From 193.137.75.172:36007
To 193.136.65.1:10002 -

Total time = 1799.995567 s
Total packets = 460798
Minimum delay = 0.000005 s
Maximum delay = 1.003984 s
Average delay = 0.016211 s
Average jitter = 0.008992 s
Delay standard deviation = 0.121898 s
Bytes received = 235928576
Average bitrate = 1048.574031 Kbit/s
Average packet rate = 255.999519 pkt/s
Packets dropped = 2 (0.00 %)
Average loss-burst size = 1.000000 pkt

TCP

Flow number: 3
From 2001:690:810:36:8fa9:7b5c:f303:ed5:44476
To 2001:690:2300:2::1:10003

Total time = 1800.000404 s
Total packets = 460797
Minimum delay = 0.000002 s
Maximum delay = 1.017391 s
Average delay = 0.018578 s
Average jitter = 0.013767 s
Delay standard deviation = 0.121620 s
Bytes received = 235928064
Average bitrate = 1048.568938 Kbit/s
Average packet rate = 255.998276 pkt/s
Packets dropped = 0 (0.00 %)
Average loss-burst size = 0.000000 pkt

Flow number: 4
From 193.137.75.172:41546

To 193.136.65.1:10004

Total time = 1800.003766 s
Total packets = 460798
Minimum delay = 0.000002 s
Maximum delay = 1.026864 s
Average delay = 0.020510 s
Average jitter = 0.012608 s
Delay standard deviation = 0.131221 s
Bytes received = 235928576
Average bitrate = 1048.569255 Kbit/s
Average packet rate = 255.998353 pkt/s
Packets dropped = 0 (0.00 %)
Average loss-burst size = 0.000000 pkt

Streaming

Flow number: 5
From 2001:690:810:36:8fa9:7b5c:f303:ed5:53257
To 2001:690:2300:2::1:10005

Total time = 1799.991687 s
Total packets = 216533
Minimum delay = 0.000008 s
Maximum delay = 1.007950 s
Average delay = 0.015523 s
Average jitter = 0.016749 s
Delay standard deviation = 0.090943 s
Bytes received = 292752616
Average bitrate = 1301.128747 Kbit/s
Average packet rate = 120.296667 pkt/s
Packets dropped = 7 (0.00 %)
Average loss-burst size = 1.000000 pkt

Flow number: 6

From 193.137.75.172:46616

To 193.136.65.1:10006

Total time = 1799.990664 s

Total packets = 216538

Minimum delay = 0.000008 s

Maximum delay = 1.008339 s

Average delay = 0.016475 s

Average jitter = 0.018083 s

Delay standard deviation = 0.097074 s

Bytes received = 292759376

Average bitrate = 1301.159531 Kbit/s

Average packet rate = 120.299513 pkt/s

Packets dropped = 2 (0.00 %)

Average loss-burst size = 2.000000 pkt

VoIP

Flow number: 7

From 2001:690:810:36:8fa9:7b5c:f303:ed5:39898

To 2001:690:2300:2::1:10007

Total time = 1799.990021 s

Total packets = 179990

Minimum delay = 0.000046 s

Maximum delay = 1.009582 s

Average delay = 0.015166 s

Average jitter = 0.020107 s

Delay standard deviation = 0.099526 s

Bytes received = 16559080

Average bitrate = 73.596319 Kbit/s

Average packet rate = 99.994999 pkt/s

Packets dropped = 10 (0.01 %)

Average loss-burst size = 1.111111 pkt

Flow number: 8

From 193.137.75.172:34051

To 193.136.65.1:10008

Total time = 1799.988502 s

Total packets = 179997

Minimum delay = 0.000015 s

Maximum delay = 1.009845 s

Average delay = 0.016046 s

Average jitter = 0.020519 s

Delay standard deviation = 0.100617 s

Bytes received = 16559724

Average bitrate = 73.599243 Kbit/s

Average packet rate = 99.998972 pkt/s

Packets dropped = 3 (0.00 %)

Average loss-burst size = 1.500000 pkt

_____

********** TOTAL RESULTS **********

_____

Number of flows = 8

Total time = 1800.074109 s

Total packets = 2636231

Minimum delay = 0.000002 s

Maximum delay = 1.026864 s

Average delay = 0.016724375 s

Average jitter = 0.01484462 s

Delay standard deviation = 0.116305 s

Bytes received = 1562335372

Average bitrate = 6943.431454 Kbit/s

Average packet rate = 1464.518679 pkt/s

Packets dropped = 41 (0.00 %)

Average loss-burst size = 1.192308 pkt

Corrupted log records = 0

Apêndice II

Abaixo estão representados os *traceroutes* entre os dois nós, em ambas as direcções e em ambas as versões do protocolo.

UBI – ULHT

traceroute 193.137.75.172

traceroute to 193.137.75.172 (193.137.75.172), 64 hops max

1 193.136.65.6 0,500ms 0,398ms 0,390ms

2 193.137.98.102 0,331ms 0,199ms 0,196ms

3 193.137.97.101 0,816ms 0,546ms 0,604ms

4 * * *

5 193.137.4.9 10,777ms 10,673ms 10,370ms

6 193.136.1.1 16,266ms 15,346ms 15,296ms

7 193.137.0.25 15,059ms 14,803ms 15,159ms

8 193.136.1.74 15,507ms 15,094ms 14,874ms

9 193.137.75.172 15,630ms 15,394ms 15,419ms

traceroute6 2001:690:810:36::2

traceroute to 2001:690:810:36::2 (2001:690:810:36::2) from

2001:690:2300:2:8fa9:7b5c:f303:ed5, 30 hops max, 24 byte packets

1 2001:690:2300:2::1 (2001:690:2300:2::1) 1.208 ms 1.146 ms 0.947 ms

2 2001:690:2300:ffff::1 (2001:690:2300:ffff::1) 1.099 ms 1.137 ms 0.983 ms

3 router20.ipv6.fccn.pt (2001:690:810:24::1) 175.546 ms 10.933 ms 10.756 ms

4 router20.ipv6.10ge.porto.fccn.pt (2001:690:880:2::20) 10.802 ms 10.64 ms 10.588 ms

5 router3.10ge.dwdm.ipv6.porto.fccn.pt (2001:690:840:30::3) 15.55 ms * *

6 router9.ipv6.ge.lisboa.fccn.pt (2001:690:800:1::9) 15.232 ms 15.234 ms 15.299 ms

7 2001:690:810:36::2 (2001:690:810:36::2) 15.124 ms 15.168 ms 15.268 ms

ULHT - UBI

traceroute 193.136.65.1

traceroute to 193.136.65.1 (193.136.65.1), 64 hops max

1 193.137.75.129 0,586ms 0,393ms 0,440ms

2 193.136.1.73 0,686ms 0,686ms 0,405ms

3 193.137.0.13 1,516ms 1,090ms 1,262ms

4 193.136.1.2 5,470ms 5,089ms 5,124ms

5 193.137.4.1 5,047ms 5,076ms 5,365ms

6 193.136.4.122 15,363ms 15,400ms 15,405ms

7 193.137.97.102 15,397ms 15,682ms 15,357ms

8 * * *

9 193.136.65.1 16,427ms 15,401ms 15,401ms

traceroute6 2001:690:2300:2::1

traceroute to 2001:690:2300:2::1 (2001:690:2300:2::1) from 2001:690:810:36::2, 30 hops max, 24 byte packets

1 2001:690:810:36::1 (2001:690:810:36::1) 0.787 ms 0.652 ms 0.543 ms

2 2001:690:800:1::13 (2001:690:800:1::13) 1.158 ms 1.046 ms 1.074 ms

3 Router2.10GE.DWDM.IPv6.Porto.fccn.pt (2001:690:840:30::2) 4.922 ms 4.888 ms 4.821 ms

4 ROUTER2.IPv6.GE.Porto.fccn.pt (2001:690:880:2::2) 5.359 ms 5.275 ms 5.1 ms

5 UBI.IPv6.fccn.pt (2001:690:810:24::2) 15.541 ms 15.488 ms 15.572 ms

6 2001:690:2300:2::1 (2001:690:2300:2::1) 15.426 ms * 15.548 ms