

Faculdade de Engenharia da Universidade do Porto



**Análise e comparação das tecnologias Wi-Fi e
Homeplug para a transmissão de *streams* de vídeo**

Nuno Filipe da Costa Santos

Dissertação realizada no âmbito do
Mestrado Integrado em Engenharia Electrotécnica e de Computadores
Major Telecomunicações

Orientador: Prof. Dr. José Ruela
Co-orientador: Eng. Carlos Pinho

30/07/2010

© Nuno Filipe da Costa Santos, 2010

A Dissertação intitulada

**“ANÁLISE E COMPARAÇÃO DAS TECNOLOGIAS WI-FI E HOMEPLUG PARA
TRANSMISSÃO DE STREAMS DE VÍDEO”**

foi aprovada em provas realizadas em 21/Julho/2010

o júri



Presidente Professor Doutor Luís António Pereira de Meneses Corte-Real
Professor Associado do Departamento de Engenharia Electrotécnica e de
Computadores da Faculdade de Engenharia da Universidade do Porto



Professora Doutora Paula Maria Marques Moura Gomes Viana
Professora Coordenadora S/Agregação do Departamento de Engenharia
Electrotécnica do Instituto Superior de Engenharia do Porto

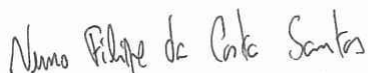


Professor Doutor José António Ruela Simões Fernandes
Professor Associado do Departamento de Engenharia Electrotécnica e de
Computadores da Faculdade de Engenharia da Universidade do Porto (Orientador).



Mestre Carlos Pinho
Investigador do INESC-Porto (Co-Orientador).

O autor declara que a presente dissertação (ou relatório de projecto) é da sua exclusiva autoria e foi escrita sem qualquer apoio externo não explicitamente autorizado. Os resultados, ideias, parágrafos, ou outros extractos tomados de ou inspirados em trabalhos de outros autores, e demais referências bibliográficas usadas, são correctamente citados.



Autor - Nuno Filipe da Costa Santos

Faculdade de Engenharia da Universidade do Porto

Resumo

Com o aparecimento de diferentes tecnologias acessíveis e capazes de oferecer serviços de alta qualidade a elevados débitos para contextos de utilização comum (e.g., escritórios, habitações, etc.), torna-se importante compreender melhor o funcionamento de cada uma delas, as suas vantagens e desvantagens. Também devido à constante evolução tecnológica, é necessário estudar essas tecnologias e adaptá-las a cenários novos que permitam uma evolução contínua e melhor exploração das mesmas. No contexto deste trabalho, as tecnologias Wi-Fi e HomePlug serão analisadas para serem adaptadas para diversos cenários. Estas tecnologias, que oferecem débitos relativamente elevados, conseguem adaptar-se a diversos cenários e contextos de comunicação, como por exemplo, novos sistemas de carregamento de veículos eléctricos onde o carro comunica com o sistema de gestão de carregamentos, em dispositivos móveis que pretendam comunicar com uma central e trocar informação, entre outros. Hoje em dia com estas tecnologias já é possível transmitir som e imagem em alta definição o que pode trazer benefícios consideráveis a aplicações com estes requisitos, como é o caso da transmissão de vídeo na Internet. Para saber que tecnologia melhor se adapta a cada situação é fundamental conhecer em profundidade as principais características de cada tecnologia. A escolha da melhor tecnologia, ou combinação delas, é fundamental para produzir arquitecturas mais funcionais e eficientes.

Este trabalho tem como objectivo principal fazer uma análise comparativa das tecnologias Wi-Fi e HomePlug para a transmissão de *streams* de vídeo em “tempo-real”, em particular em cenários de utilização conjunta das duas tecnologias. De facto, as duas tecnologias estão essencialmente posicionadas (embora não limitadas a) para aplicações distintas. Ao passo que o Wi-Fi está mais orientado para a rede de acesso, o HomePlug está mais orientado à comunicação ponto-a-ponto (na medida em que cada estação tem de usar uma frequência própria para comunicar com qualquer outra estação na mesma rede).

Para a realização deste trabalho foi efectuado um estudo destas tecnologias e respectivas normas mais recentes que servem de base à comparação teórica presente no capítulo do estado da arte. Foi ainda feito um levantamento dos diferentes tipos de codificação de vídeo em “tempo-real” que se presume que sejam adequados no domínio da videovigilância, que é o contexto de aplicação do estudo deste trabalho, e são ainda apresentados alguns protocolos de comunicação.

Assim, foram realizados diversos cenários de teste onde se utilizaram estas duas tecnologias. Primeiramente, testaram-se as duas tecnologias separadamente, para perceber o

seu funcionamento e no caso do *Wireless* saber qual a melhor norma a utilizar entre a 802.11a, 802.11g e 802.11n. Depois analisaram-se cenários híbridos em que se testou o emissor a funcionar com *Wireless* e o receptor com HomePlug e vice-versa, e tanto o receptor como o emissor a funcionar com *Wireless*, mas com os *routers* ligados por HomePlug. Os últimos dois cenários serviram para perceber o funcionamento do QoS das duas tecnologias em situações onde o canal está cheio.

Nos testes realizados percebeu-se que a norma n é a melhor do IEEE 802.11 para aplicações de *streaming*. Outra conclusão a retirar é a maneira diferente como um sistema destes responde com a presença de tráfego adicional UDP e TCP, onde o primeiro apresenta mais dificuldades ao sistema. Verificou-se que o QoS é fundamental para este tipo de aplicações para se obter reprodução de vídeo com boa qualidade e sem perdas. Sobre o HomePlug foi possível verificar que é uma tecnologia onde é necessário um estudo da parte eléctrica do local a implementar para esta trabalhar na sua máxima capacidade.

Este trabalho traz assim um conjunto de contribuições inovadoras na medida em que tanto quanto é do conhecimento do autor não existem testes deste género na literatura. Assim, este trabalho é mais um contributo para a investigação ao nível das comunicações nomeadamente no que respeita às tecnologias *Wireless* e HomePlug, pois foram testadas as suas normas mais recentes. Esta dissertação pode assim ser um bom início de caminho para se perceber qual a melhor tecnologia a adoptar em sistemas móveis dotados de câmaras.

Abstract

With the appearance of different accessible technologies capable of offering high quality services with high throughput for the common use context (for example offices, housing, etc), it becomes important to understand how they work, as well as they're advantages and disadvantages. Also with the constant technological evolution, it is necessary to study those technologies and adapt them to new scenarios that will give us a continuous evolution and a better exploration of them. In the context of this work, the Wi-Fi and HomePlug technologies will be analyzed so they can be adapted to different scenarios. These technologies, that offer relatively high throughput, can adapt to different communication scenarios and contexts like, for example, new electric vehicles charging systems where the car communicates with the charging management system, in mobile devices that want to communicate with an agency and exchange information, among others. Today, with these technologies it is possible to transmit high definition sounds and images which can bring considerable benefits to applications that require these things, like internet video transmissions. To know which technology best adapts to each situation it is fundamental to know in depth the main characteristics of each technology. The choice of the best technology, or the combination of the best, is fundamental to produce more functional and efficient architectures.

This paper has the objective of making a comparative analysis of the Wi-Fi and HomePlug technologies to the transmission of "real-time" video *streams*, in particular in scenarios addressing the combined utilization of these two technologies. In fact, the two technologies are essentially positioned (although not limited to) to distinct applications. While Wi-Fi is more oriented to access network, HomePlug is more oriented to point-to-point communication (as each station has to use an individual frequency to communicate with another station in the same network).

For the conclusion of this paper a study was made about these technologies and respective recent standards that can be used as a theoretical term of comparison in the state of the art chapter. A survey of the different types of "real-time" video codification that are presumed to be adequate in the video surveillance domain was also made, that is the context of the study of this paper, and there are also presented some communication protocols.

Therefore, different testing scenarios where these two technologies were used were made. Firstly, both technologies were tested separately, to better understand how they work and in case of *Wireless* to know which is the best standard to use between 802.11a, 802.11g and 802.11n. Then there were analyzed hybrid scenarios in which it was tested the *Wireless*

receiver and the HomePlug receptor and vice-versa, and both the receptor and the receiver working with *Wireless*, but with the routers connected by HomePlug. The last two scenarios served to understand how the QoS of the two technologies work in situations where the channel is full.

The performed tests led to the conclusion that the n standard is the best of the IEEE 802.11 for *streaming* applications. Another conclusion that can be perceived is the different way that a system such as this responds with the presence of additional UDP and TCP traffic, where the first presents more difficulties to the system. We can verify that the QoS is fundamental for this type of application so to obtain videos in good conditions and without losses. About the HomePlug it was possible to verify that it is a technology where a study about the electrical part of the implementation place is necessary for this system to work in its maximum capacity.

So this paper brings a set of innovative contributions as far as the author knows there are no tests of this kind in the literature. Therefore, this paper is another contribution to the investigation in communications, namely in what concerns the *Wireless* and HomePlug technologies, in particular the most recent versions of the standards that have been tested. In conclusion, this thesis may be a good starting point to understand what is the best technology to adopt in mobile systems with cameras.

Agradecimentos

Gostava de agradecer a todos que me ajudaram a completar esta dissertação com êxito. Para começar, muito obrigado ao Prof. Dr. José Ruela e Eng. Carlos Pinho por toda a disponibilidade e ajuda mostrada durante o semestre. Foram uns verdadeiros orientadores. Queria também agradecer ao Hugo e ao Bruno por toda a ajuda e pela companhia diária que foram durante estes meses.

À minha namorada, Rosinha, e aos meus Pais por toda a força transmitida mesmo nos momentos de maior cansaço e exaustão.

Aos meus amigos do Gaia United, porque este último mês não compareci a nenhum treino e sempre me apoiaram e ajudaram no que foi preciso.

A todos os outros meus amigos e pessoas que me deram força, porque uma parte desta tese também é deles.

Índice

Resumo	v
Abstract.....	vii
Agradecimentos	ix
Índice.....	xi
Lista de figuras	xiii
Lista de tabelas	xvii
Abreviaturas e Símbolos	xxi
Capítulo 1	1
Introdução.....	1
1.1 - Objectivos.....	2
1.2 - Contexto e motivação.....	3
Capítulo 2	5
Estado da arte	5
2.1 - Introdução.....	5
2.2 - Tecnologias	5
2.2.1 - HomePlug.....	5
2.2.1.1 - Aparecimento e utilização actual.....	5
2.2.1.2 - Caracterização do HomePlug 1.0	7
2.2.1.3 - Caracterização do HomePlug AV	9
2.2.1.4 - Melhorias e outros aspectos.....	12
2.2.2 - IEEE 802.11.....	13
2.2.2.1 - Aparecimento e utilização actual.....	13
2.2.2.2 - <i>Standard</i> 802.11.....	14
2.2.2.3 - IEEE 802.11a	16
2.2.2.4 - IEEE 802.11b	17
2.2.2.5 - IEEE 802.11g	18
2.2.2.6 - IEEE 802.11n	19
2.2.2.7 - IEEE 802.11p	20
2.2.3 - Comparação das tecnologias.....	21

2.2.3.1 - IEEE 802.11a, IEEE 802.11b, IEEE 802.11g e IEEE 802.11n.....	21
2.2.3.2 - HomePlug AV e HomePlug 1.0.....	22
2.2.3.3 - IEEE 802.11b e HomePlug 1.0.....	22
2.3 - Vídeo em “tempo-real”.....	23
2.3.1 - Principais codificações.....	23
2.3.2 - Caracterização das codificações mais relevantes.....	24
2.3.3 - Requisitos de vídeo.....	31
2.3.4 - Mapeamento teórico dos requisitos de vídeo sobre as tecnologias anteriores.....	31
2.4 - Streaming.....	32
2.4.1 - Protocolos.....	32
Capítulo 3	37
Tecnologias	37
3.1 - Hardware utilizado	37
3.2 - Software e configurações	39
3.2.1 - Servidor de <i>streaming</i>	39
3.2.2 - Medição de parâmetros de rede	43
3.2.3 - Gerador de tráfego adicional.....	45
3.2.4 - Configuração de QoS	47
Capítulo 4	49
Cenários de teste	49
4.1 - Cenário 1	50
4.2 - Cenário 2	56
4.3 - Cenário 3	58
4.4 - Cenário 4.....	60
4.5 - Cenário 5.....	61
4.6 - Cenário 6.....	62
4.7 - Cenário 7.....	63
Capítulo 5	67
Análise dos resultados	67
5.1 - Cenário 1	68
5.2 - Cenário 2.....	69
5.3 - Cenário 3, 4 e 5.....	71
5.4 - Cenário 6.....	72
5.5 - Cenário 7.....	73
5.6 - Análise Geral	74
Capítulo 6	77
Conclusão	77
Referências	79
Anexo A - Tabelas dos resultados	83
Anexo B - Comportamento CPU	110

Lista de figuras

Figura 2.1 - Serviços e aplicações suportados por HomePlug [2].	6
Figura 2.2 - Trama longa e curta do HomePlug 1.0 [10].	8
Figura 2.3 - Esquema do “Priority Resolution” e mecanismo de “Backoff” [10].	8
Figura 2.4 - Arquitectura HomePlug AV [13].	9
Figura 2.5 - Transmissor e Receptor OFDM do HPAV [13].	10
Figura 2.6 - Testes do débito do HomePlug 1.0 com 2 nós [12].	13
Figura 2.7 - IEEE 802.11 no modelo OSI [21].	14
Figura 2.8 - Modos do standard 802.11 [21].	14
Figura 2.9 - Estrutura da trama do <i>standard</i> 802.11.	16
Figura 2.10 - Funcionamento do sistema MIMO [20].	19
Figura 2.11 - Gráficos dos resultados dos testes de comparação entre a norma 802.11b e 802.11g [25].	21
Figura 2.12 - Resultados do teste de comparação entre a norma HomePlug 1.0 e a norma 802.11b [24].	22
Figura 2.13 - Codificador/Descodificador geral de vídeo [27].	24
Figura 2.14 - Estrutura dos dados relativos a uma sequência de vídeo [27].	25
Figura 2.15 - Desempenho comparativo de codificação [27].	26
Figura 2.16 - Arquitectura simplificada da representação audiovisual MPEG-4 [27].	28
Figura 2.17 - Ganhos médios em débito para aplicações de <i>streaming</i> [27].	28
Figura 2.18 - Resultado dos testes subjectivos realizados pela Blu-Ray Association [27].	30
Figura 2.19 - Desempenho comparativo para sessões de <i>streaming</i> [27].	30
Figura 2.20 - TCP, UDP e RTP na pilha TCP/IP.	33

Figura 2.21 - Funcionamento dente de serra [49].....	34
Figura 3.1 - Janela principal VLC.	40
Figura 3.2 - Janela “Emissão” do VLC.....	40
Figura 3.3 - Janela com opções de <i>streaming</i> do VLC.....	41
Figura 3.4 - Janela com opções de <i>streaming</i> do VLC com protocolo escolhido.....	41
Figura 3.5 - Janela de transcodificação do VLC.	42
Figura 3.6 - Janela “Abrir Emissão de Rede” do VLC.	43
Figura 3.7 - Janela Wireshark.....	44
Figura 3.8 - Janela “Stream Analysis...” do Wreshark.	44
Figura 3.9 - Janela do Network Traffic Generator.	45
Figura 3.10 - Extracto Wireshark com tráfego TCP.	46
Figura 3.11 - Extracto Wireshark com tráfego UDP.	46
Figura 3.12 - Janelas configuração QoS.....	47
Figura 4.1 - Diagrama genérico dos cenários de teste.	49
Figura 4.2 - Representação do Cenário 1.....	50
Figura 4.3 - Planta da sala de testes com testes representados.	51
Figura 4.4 - Gráfico do <i>streaming</i> do teste nº1.....	52
Figura 4.5 - Ping ente PC1 e PC3 do teste nº1.....	53
Figura 4.6 - Gráfico do <i>streaming</i> do teste nº2.....	54
Figura 4.7 - Ping ente PC1 e PC3 do teste nº2.....	54
Figura 4.8 - Gráfico do <i>streaming</i> do teste nº3.....	55
Figura 4.9 - Ping ente PC1 e PC3 do teste nº2.....	55
Figura 4.10 - Esquema do cenário 2 sem QoS.	57
Figura 4.11 - Esquema do cenário 2 com QoS.....	57
Figura 4.12 - Esquema do cenário 3 sem QoS.	59
Figura 4.13 - Esquema do cenário 3 com QoS.	59
Figura 4.14 - Esquema do cenário 4 sem QoS.	60
Figura 4.15 - Esquema do cenário 4 com QoS.....	60
Figura 4.16 - Esquema do cenário 5 sem QoS.	61
Figura 4.17 - Esquema do cenário 5 com QoS.....	62

Figura 4.18 - Esquema do cenário 6.	63
Figura 4.19 - Esquema do cenário 7 sem QoS.....	64
Figura 4.20 - Esquema do cenário 7 com QoS.....	64
Figura 5.1 - Resultados cenário 1 /1 cliente /porta 1234.	68
Figura 5.2 - Média dos 3 clientes no cenário 1.....	68
Figura 5.3 - Comparação da norma 802.11a, 802.11g e 802.11n no cenário 2 com 1 cliente.....	69
Figura 5.4 - Comparação da norma 802.11a, 802.11g e 802.11n no cenário 2 com 3 cliente.....	70
Figura 5.5 - Comparação do cenário 3, cenário 4 e cenário 5 com 1 cliente.....	71
Figura 5.6 - Comparação do cenário 3, cenário 4 e cenário 5 com 3 clientes.	72
Figura 5.7 - Comparação do cenário 6 entre 1 e 3 clientes na presença de tráfego UDP adicional.	73
Figura 5.8 - Comparação do cenário 7 com tráfego UDP adicional com e sem QoS na porta 1234.	74
Figura B.1 - Desempenho CPU com 3 <i>streams</i> de vídeo.....	110

Lista de tabelas

Tabela 2.1 - Valores comparativos entre a norma 802.11a, 802.11b, 802.11g e 802.11n.	22
Tabela 3.1 - Características do Computador 1.	37
Tabela 3.2 - Características do Computador 2.	38
Tabela 3.3 - Características do Computador 3.	38
Tabela 3.4 - Modelos <i>Wireless</i> e HomePlug escolhidos.....	38
Tabela 3.5 - Especificação do router WRT610N	39
Tabela 3.6 - Especificação dos dispositivos HomePlug PLK300	39
Tabela 3.7 - Especificações do adaptador USB WUSB600N	39
Tabela 4.1 - Características do vídeo utilizado.	50
Tabela 4.2 - Resultados do débito da transferência no teste nº1.	52
Tabela 4.3 - Resultados do <i>streaming</i> do teste nº1.....	52
Tabela 4.4 - Resultados do débito da transferência no teste nº2.	53
Tabela 4.5 - Resultados do <i>streaming</i> do teste nº2.....	53
Tabela 4.6 - Resultados do débito da transferência no teste nº3.	54
Tabela 4.7 - Resultados do <i>streaming</i> do teste nº3.....	55
Tabela 4.8 - Resultados do débito da transferência para a norma 802.11a.	57
Tabela 4.9 - Resultados do débito da transferência para a norma 802.11g.	58
Tabela 4.10 - Resultados do débito da transferência para a norma 802.11n.	58
Tabela 4.11 - Resultados do débito da transferência para o cenário 3.	60
Tabela 4.12 - Resultados do débito da transferência para o cenário 4.	61
Tabela 4.13 - Resultados do débito da transferência para o cenário 5.	62
Tabela 4.14 - Resultados do débito da transferência para o cenário 6.	63

Tabela 4.15 - Resultados do débito da transferência para o cenário 7.	64
Tabela A.1 - Resultados cenário 1 /1 cliente /porta 1234.	83
Tabela A.2 - Resultados cenário 1 /3 clientes /porta 1234.	83
Tabela A.3 - Resultados cenário 1 /3 clientes /porta 2500.	83
Tabela A.4 - Resultados cenário 1 /3 clientes /porta 5004.	84
Tabela A.5 - Média dos 3 clientes no cenário 1.	84
Tabela A.6 - Resultados cenário 2 /norma a /1 cliente /porta 1234.	84
Tabela A.7 - Resultados cenário 2 /norma a /3 clientes /porta 1234.	85
Tabela A.8 - Resultados cenário 2 /norma a /3 clientes /porta 2500.	86
Tabela A.9 - Resultados cenário 2 /norma a /3 clientes /porta 5004.	86
Tabela A.10 - Média dos 3 clientes no cenário 2/ norma a.	87
Tabela A.11 - Resultados cenário 2 /norma g /1 cliente /porta 1234.	88
Tabela A.12 - Resultados cenário 2 /norma g /3 clientes /porta 1234.	89
Tabela A.13 - Resultados cenário 2 /norma g /3 clientes /porta 2500.	89
Tabela A.14 - Resultados cenário 2 /norma g /3 clientes /porta 5400.	90
Tabela A.15 - Média dos 3 clientes no cenário 2/ norma g.	91
Tabela A.16 - Resultados cenário 2 /norma n /1 cliente /porta 1234.	91
Tabela A.17 - Resultados cenário 2 /norma n /3 clientes /porta 1234.	92
Tabela A.18 - Resultados cenário 2 /norma n /3 clientes /porta 2500.	93
Tabela A.19 - Resultados cenário 2 /norma n /3 clientes /porta 5004.	93
Tabela A.20 - Média dos 3 clientes no cenário 2/ norma n.	94
Tabela A.21 - Resultados cenário 3 /1 cliente /porta 1234.	95
Tabela A.22 - Resultados cenário 3 /3 clientes /porta 1234.	95
Tabela A.23 - Resultados cenário 3 /3 clientes /porta 2500.	96
Tabela A.24 - Resultados cenário 3 /3 clientes /porta 5400.	97
Tabela A.25 - Média dos 3 clientes no cenário 3.	97
Tabela A.26 - Resultados cenário 4 /1 clientes /porta 1234.	98
Tabela A.27 - Resultados cenário 4 /3 clientes /porta 1234.	99
Tabela A.28 - Resultados cenário 4 /3 clientes /porta 2500.	99
Tabela A.29 - Resultados cenário 4 /3 clientes /porta 5004.	100

Tabela A.30 - Média dos 3 clientes no cenário 4.	101
Tabela A.31 - Resultados cenário 5 /1 cliente /porta 1234.	101
Tabela A.32 - Resultados cenário 5 /3 clientes /porta 1234.	102
Tabela A.33 - Resultados cenário 5 /3 clientes /porta 2500.	103
Tabela A.34 - Resultados cenário 5 /3 clientes /porta 5004.	103
Tabela A.35 - Média dos 3 clientes no cenário 5.	104
Tabela A.36 - Resultados cenário 6 /1 cliente /porta 1234.	105
Tabela A.37 - Resultados cenário 6 /3 clientes /porta 1234.	105
Tabela A.38 - Resultados cenário 6 /3 clientes /porta 2500.	105
Tabela A.39 - Resultados cenário 6 /3 clientes /porta 5004.	106
Tabela A.40 - Resultados cenário 7 /1 cliente /porta 1234.	106
Tabela A.41 - Resultados cenário 7 /3 clientes /porta 1234.	107
Tabela A.42 - Resultados cenário 7 /3 clientes /porta 2500.	108
Tabela A.43 - Resultados cenário 7 /3 clientes /porta 5004.	108

Abreviaturas e Símbolos

Lista de abreviaturas (ordenadas por ordem alfabética)

3GPP	3rd Generation Partnership Project
ACC	Advances Audio Coding
ACK	Acknowledgment
ACS	Auto Connect Service
AES	Advances Encryption Standard
AFE	Analog Front End
AGC	Automatic Gain Controller
AP	Access Point
ARQ	Automatic Repeat Request
ATS	Arrival Time Stamp
AVC	Advanced Video Coding
AVLN	AV Logical Network
BCH	Bose, Chaudhuri and Hocquengham
BPL	Broadband over Powerline
BPSK	Binary Phase Shift Keying
BSS	Basic Service Set
BSSID	Basic Service Set Identification
CCH	Canal de Controlo
CCK	Complementary Code Keying
CCo	Central Coordinator
CCTV	Closed Circuit Television
CD	Compact Disc
CF	Contention Free
CID	Connection ID
CIF	Common Intermediate Format
CL	Convergence Layer

CM	Connection Manager
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access/ Collision Avoidance
CSPEC	Connection Specification
CTS	Clear to Send
CW	Contention Window
DBC	Decreasing BER-constrained
DBPSK	Differential Binary Phase Shift Keying
DCT	Transformada Discreta de Co-seno
DEK	Default Encryption Keys
DES	Data Encryption Standard
DMIF	Delivery Multimedia Integration Framework
DNL	Discovered Networks Lists
DQPSK	Differential Quadrature Phase Shift Keying
DS	Distribution Service
DSL	Discovered Station List
DSM-CC	Digital Storage Media - Command and Control
DSRC	Dedicated Short Range Communications
DSSS	Direct Sequence Spread Spectrum
DVB	Digital Vídeo Broadcasting
DVD	Digital Versatile Disk
EAP	Extensible Authentication Protocol
EKS	Encryption Key Select
ERP	Extended Rate Physicals
ESS	Extended Service Set
FCC	Federal Communications Commision
FCS	Frame Check Sequence
FEC	Forward Error Correction
FEUP	Faculdade de Engenharia da Universidade do Porto
FHSS	Frequency Hopping Spread Spectrum
GOP	Group of Pictures
HDTV	High Definition Television
HLE	Higher Layer Entities
HPAV	HomePlug AV
HTTP	HyperText Transfer Protocol
IBSS	Independent BSS
IEC	International Electrotechnical Commission
IEEE	Institute os Electrical and Electronics Engineers Inc.
INESC	Instituto de Engenharia de Sistemas e Computadores
INL	Interfering Network List

IPMC	Intellectual Property Management and Protection
IPTV	Internet Protocol Television
IR	Infravermelhos
ISO	International Standards Organization
ITS	Sistema Inteligente de Transporte
ITU	International Telecommunication Union
LLC	Logical Link Control
MAC	Media Access Control
MB	MacroBlock
MGEN	Multi Generator
MIC	Message Integrity Check
MIMO	Multiple Input Multiple Output
MoCA	Multimedia over Coax Alliance
MPEG	Moving Picture Experts Group
MSDU	MAC Service Data Unit
NAL	Network Abstraction Layer
NEK	Network Encryption Key
NIC	Network Interface Card
NMK	Network Membership Key
NNs	Neighboring Networks
OFDM	Orthogonal Frequency Division Multiplexing
PB	PHY Block
PBCC	Packet Binary Convolutional Coding
PCF	Persistent Contention Free
PCF	Point Coordination Function
PCo	Proxy Coordinator
PCS	Physical Carrier Sense
PLC	Power Line Communications
PLCP	Physical Layer Convergence Protocol
PRS	Priority Resolution Slots
PSNR	Peak Signal to Noise Ratio
QAM	Quadrature Amplitude Modulation
QCIF	Quarter CIF
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RC4 PRGN	Ron's Code or Rivest's Cipher Pseudo Random Number Generator
RDIS	Rede Digital com Integração de Serviços
ROBO	ROundaBOunt
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol

RTS	Request to Send
SACK	Selective Acknowledge
SAP	Service Access Point
SCH	Canais de Serviço
SDM	Spacial Division Multiplexing
SDTV	Standard Definition Television
SIF	Source Input Format
SNR	Signal-to-noise Ratio
SQCIF	Sub-QCIF
TCC	Turbo Convolutional Code
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
VCD	Video CD
VCEG	Vídeo Coding Experts Group
VCL	Vídeo Coding Layer
VCS	Virtual Carrier Sense
VHS	Video Home System
VoIP	Voice over Internet Protocol
WBSS	Wave BSS
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access

Capítulo 1

Introdução

Nos dias que correm a evolução da tecnologia determina a evolução do próprio Homem. Com o objectivo de melhorar o seu estilo de vida, o Homem procura através da tecnologia atingir esse objectivo. As novas normas IEEE 802.11 e o HomePlug AV surgiram para satisfazer necessidades actuais tanto no contexto sem fios como cablado, respectivamente. Estas tecnologias permitem, devido aos seus altos débitos fornecer novos serviços, como a televisão, em alta definição.

A norma IEEE 802.11 (também conhecida como Wi-Fi) [1] encontra-se amplamente difundida, podendo ser encontrada em milhões de casas e nos mais diversos locais públicos, sendo actualmente a forma mais popular de acesso à Internet através de um ponto de acesso. Mais recentemente o HomePlug [2] surgiu numa perspectiva de aproveitar a rede eléctrica já instalada para a transmissão do mesmo tipo de serviços, na perspectiva ponto-a-ponto. A principal vantagem desta tecnologia é o facto de não necessitar da instalação de novos cabos e suportar débitos na ordem das centenas de Mbit/s.

Cada uma destas tecnologias apresenta as suas vantagens e desvantagens tendo em conta o seu contexto de aplicação natural, por exemplo, ao passo que o Wi-Fi está mais orientado para a rede de acesso sem fios facilitando assim a mobilidade dos utilizadores, o Homeplug não requer a instalação de novos cabos, suportando a comunicação entre locais afastados/“isolados” (e.g., diferentes andares de um edifício).

Quer o Wi-Fi quer o HomePlug têm influência na área da vídeo vigilância, que tradicionalmente é realizada através de câmaras fixas que enviam imagens a preto e branco e mais recentemente através da tecnologia CCTV (“Closed Circuit Television”), de tal forma que esta possa evoluir de modo a aparecerem novos mecanismos que tirem partido do protocolo Internet (IP) sobre Wi-Fi e/ou HomePlug em simultâneo. Contudo, para garantir a melhor forma de suportar este tipo de aplicações sobre as referidas tecnologias é necessário realizar um estudo sobre cada uma delas, cenários de aplicação e testes de casos de utilização onde os resultados sejam analisados de forma a retirar as devidas conclusões. A pesquisa realizada na literatura existente não devolveu nenhum estudo de relevo que comparasse estas tecnologias no contexto aqui apresentado.

Existem actualmente diversas tecnologias de comunicação, com características próprias, que as tornam mais ou menos adequadas em diferentes contextos de utilização. A norma IEEE 802.11 (e respectivas variantes) é uma tecnologia *wireless* que suporta débitos até 600

2 Introdução

Mbit/s (802.11n). Pelo facto de ser *wireless*, apresenta vantagens e desvantagens, nomeadamente ao nível da instalação e mobilidade dos equipamentos terminais quer ao nível das características do canal/ meio de transmissão partilhado, entre outros. Por outro lado, algumas tecnologias cabladas como o HomePlug (e em particular a versão “HomePlug AV”), foram desenvolvidas de raiz de forma a ser possível transmitir/disseminar “High Definition Television” (HDTV) e “Voice over Internet Protocol” (VoIP) dentro de edifícios (por exemplo, habitações), para além de suportarem outras aplicações ou serviços tradicionais tais como Internet, consolas de jogos e outros aparelhos electrónicos.

1.1 - Objectivos

Esta dissertação está inserida num projecto do Instituto de Engenharia de Sistemas e Computadores do Porto (INESC Porto), que pretende estudar e desenvolver uma estrutura optimizada para a transmissão de *streams* de vídeo em “tempo-real” a partir de elementos móveis dotados de câmaras. Foram definidos vários objectivos para este trabalho, que funcionaram como metas a cumprir para uma conclusão satisfatória desta dissertação. O objectivo principal é a comparação das tecnologias Wi-Fi (em particular 802.11a, g, n) com a tecnologia HomePlug AV para a transmissão de vídeo em “tempo-real”. Como objectivos paralelos ao anterior, apresentam-se a identificação dos parâmetros adequados para a comparação, a identificação de cenários de teste e a realização dos testes para explorar estas tecnologias de forma isolada ou híbrida, tirando conclusões sobre o seu funcionamento e desempenho. A comparação das tecnologias pode incidir sobre o número de *streams* simultâneos suportados em cada uma delas, o débito máximo, o *jitter*, o *skew* e a perda de pacotes que pode ocorrer numa dada transmissão. Contudo, nesta comparação não se mede o atraso, *jitter*, *skew* e as outras grandezas introduzidos por cada tecnologia no percurso dos *streams*. Os objectivos anteriores têm como meta atingir o melhor desempenho do sistema, ou seja, encontrar a tecnologia ou a combinação delas que faça com que o sistema seja o mais rápido, fiável, seguro e robusto possível. Depois de descobertas as grandezas a comparar são descritos vários cenários de teste. Estes cenários dão a possibilidade de estudar o funcionamento das diferentes tecnologias, de forma separada ou híbrida. É importante referir que não é realizada a comparação das tecnologias em cenários idênticos, isto é, não foi considerada a utilização do Wi-Fi em modo *ad-hoc* para comparação do seu desempenho com o HomePlug para transporte de dados ponto-a-ponto nem se tem o HomePlug a funcionar como rede de acesso para uma comparação com o Wi-Fi. Foram criados sete cenários de teste, e cada um foi testado com/sem qualidade de serviço e com/sem geração de tráfego TCP ou UDP, exceptuando os cenários que apenas se utilizou a tecnologia HomePlug em que apenas foi testada com o QoS implementado de origem. Os resultados foram transportados para tabelas que mostram valores médios para cada parâmetro de medição. Depois de apresentados os resultados são apresentadas as conclusões a retirar dos mesmos.

O documento encontra-se organizado em 8 capítulos. No primeiro capítulo é dado o contexto e a motivação do trabalho dando-se uma visão mais detalhada sobre o mesmo e são descritos os objectivos que se pretendem atingir. São também apresentados os tópicos de pesquisa da bibliografia e uma breve explicação sobre o estado actual da área de vigilância e videovigilância.

No capítulo dois é apresentado o estado da arte no que diz respeito às tecnologias HomePlug e às diferentes normas do IEEE 802.11. Para ambas as tecnologias é explicado o

aparecimento e a sua utilização actual. Depois de abordadas as tecnologias, é feita uma comparação teórica entre elas na perspectiva de melhor perceber o seu funcionamento e vantagens. No final do capítulo é ainda abordada a problemática da transmissão de vídeo em “tempo-real” identificando e descrevendo os diferentes tipos de codificação e requisitos adequados ao contexto deste trabalho.

No terceiro capítulo é apresentada uma visão geral do que é um *streaming* e da sua importância nos dias de hoje, sendo também apresentada uma breve descrição sobre os protocolos de comunicação utilizados neste trabalho.

No quarto capítulo são descritos o *hardware*, *software* e configurações que foram necessárias para a elaboração desta dissertação.

No capítulo cinco são dados a conhecer todos os cenários de teste que foram idealizados para este trabalho, contemplando cenários onde apenas se utiliza uma tecnologia ou onde duas tecnologias funcionam ao mesmo tempo.

No sexto capítulo são apresentadas algumas conclusões possíveis de tirar dos resultados obtidos, dizendo qual foi a melhor e a pior norma, assim como resultados inesperados que aconteçam ou outros aspectos que foram relevantes no trabalho.

A conclusão corresponde ao capítulo sete, e capítulo final, fazendo um sumário de tudo o que está para trás e enumera as principais conclusões dos resultados obtidos, assim como a contribuição que este trabalho poderá ter para o futuro.

1.2 - Contexto e motivação

O trabalho apresentado faz uma análise e uma comparação das tecnologias IEEE 802.11 (e suas normas) com o HomePlug. Este trabalho centra-se em dispositivos ou equipamentos móveis que estão dotados de câmaras e que fazem *streaming* de vídeo em “tempo-real”. Este estudo é especialmente orientado para a área da vigilância, i.e., em *robots* de segurança. Actualmente, existem já vários projectos de *robots* de segurança que têm o objectivo de monitorizar e registar eventos quer em edifícios quer ao ar livre (cenário não abordado neste estudo). Apesar de estes *robots* serem autónomos, ainda possuem limitações naturais do ambiente onde estão inseridos, tais como necessitarem da intervenção humana para reparações ou revisões. O projecto do *robot* da Hitachi [3] é capaz de mapear locais utilizando sensores de infra-vermelhos e câmaras detectando a falta de objectos ou a presença de intrusos; porém, tem limitações como a curta duração da bateria e a incapacidade de detectar objectos com dimensões inferiores ao de uma lata de refrigerante. Outro exemplo equivalente é o da Sohgo Security Services Co [4], que também está a desenvolver um *robot* com estas capacidades e com percursos pré-programados.

Um produto já em comercialização é o “Ofro” da Robowatch Technologies [5], que foi sugerido para fazer a segurança durante o mundial 2006 na Alemanha. Lançado originalmente em 2003, o preço pode chegar aos 85 mil euros. O “Ofro” é capaz de detectar armas e engenhos explosivos e subir escadas. Através de sensores específicos, que analisam a qualidade do ar, consegue ainda identificar agentes químicos, susceptíveis de serem usados como armas biológicas. Este *robot*, de 50 kg, está equipado com antenas “Universal Mobile Telecommunications System” (UMTS (rede móvel de 3ª geração)), reencaminhando todos os dados que analisa para uma central de segurança. O “Ofro” é capaz de detectar indivíduos, tanto de dia como de noite, através de uma câmara móvel localizada no topo do autómato, podendo desta forma alertar para movimentos suspeitos no recinto. Em 2008, a empresa

4 Introdução

comercializou 12 unidades e em 2009 já contava com 27 encomendas. Este tipo de tecnologia pode ser também importante noutros contextos, tais como para aceder a terrenos difíceis, por exemplo em locais atingidos por sismos, onde já existem projectos de robots que têm como missão encontrar pessoas. [6]

A demonstração desta tendência de introdução de *robots* na área da vigilância leva a crer que, no futuro, a segurança em edifícios e eventos pode passar por este tipo de soluções. De facto, a segurança como existe hoje em dia, apenas com pessoas especializadas pode ter tendência a desaparecer, estando para breve a introdução de *robots* neste ramo de negócio como indica o aumento de número de encomendas existentes nas empresas que produzem este tipo de tecnologia. [5]

Como se pode constatar pelos exemplos de *robots* já existentes, não estará para muito tarde o aparecimento de *robots* vigilantes. Para estes *robots* o *streaming* tem um papel fundamental, pois é através deste processo que estes *robots* enviam as imagens captadas para uma central onde irão estar pessoas a ver os vídeos ou onde os vídeos são gravados. Devido à importância do *streaming* elaborou-se um levantamento dos requisitos necessários para o *streaming* de vídeo em “tempo-real” no contexto da vigilância. Numa breve análise constata-se que este tipo de *streaming* não necessita de alta definição, requerendo antes outro tipo de requisitos que são identificados no decorrer desta tese, como por exemplo vários *streams* simultâneos e tecnologias que permitam suportar um débito relativamente elevado. Devido a já existirem diversas tecnologias de comunicação, é possível elaborar cenários/arquitecturas eficientes para perceber que tecnologia se adapta melhor a cada um destes cenários. No caso desta dissertação o objectivo é comparar as tecnologias Wi-Fi e HomePlug para a transmissão de *streams* de vídeo para perceber o funcionamento de cada uma perante diferentes cenários.

Capítulo 2

Estado da arte

2.1 - Introdução

Este capítulo descreve os aspectos mais relevantes das tecnologias Wi-Fi e HomePlug, em particular as normas IEEE 802.11 a, b, g e n, bem como o HomePlug 1.0 e AV. A apresentação destas tecnologias foca-se sobretudo nas suas vertentes de desempenho e segurança para uma melhor compreensão das mesmas no contexto deste projecto. Com este estudo será possível identificar e comparar os pontos fortes e fracos de cada uma das tecnologias e avaliar a sua potencial adopção individual e conjunta.

Neste capítulo é ainda abordada a problemática do vídeo em “tempo-real”, os principais tipos de codificação e respectivas descrições. Para terminar o capítulo faz-se uma pequena abordagem ao *streaming* e aos protocolos mais utilizados para o fazer, como o UDP e RTP.

No final deste capítulo será possível ter uma ideia mais concreta das tecnologias envolvidas neste projecto bem como os requisitos e desafios colocados para o suporte de *streaming* de vídeo no contexto da vídeo vigilância.

2.2 - Tecnologias

O HomePlug é uma das tecnologias, actualmente disponíveis, mais adequadas para redes domésticas. Outras tecnologias também disponíveis/adequadas para as redes domésticas são o Wi-Fi, a Ethernet [7] e o “Multimedia over Coax Alliance” (MoCA) [8].

2.2.1 - HomePlug

2.2.1.1 - Aparecimento e utilização actual

A tecnologia HomePlug é adoptada em duas normas, HomePlug 1.0 e HomePlug AV (HSPA) que é uma evolução da anterior. Esta tecnologia visa suportar, através da rede eléctrica já existente nos edifícios, um conjunto de serviços e aplicações tipicamente usadas pelos utilizadores em suas casas e demonstrada na figura 2.1.



Figura 2.1 - Serviços e aplicações suportados por HomePlug [2].

Em 2001 foi criado o primeiro sistema de comunicação utilizando a rede eléctrica (PLC) de alta velocidade chamado HomePlug 1.0, sendo vendidos mais de sete milhões de dispositivos [9]. Em 2004 teve lugar um upgrade chamado HomePlug 1.0 Turbo. O processo de criação do HomePlug 1.0 foi um sucesso e por isso foi mantido intacto para o desenvolvimento do HomePlug AV. Por isso, em 2006 surgiu esta nova tecnologia, chamada HomePlug AV. Esta tecnologia é capaz de colocar à disposição do utilizador, em qualquer local da casa, acesso à Internet, TV/"Internet Protocol Television" (IPTV) /vídeo, *streaming* de música, partilha de ficheiros, segurança, entre outros. Os consumidores estão habituados a fazer *streaming* de vídeos da Internet, mas com o HomePlug AV surgiu um novo paradigma que permite a distribuição de dados e de entretenimento *multi-stream* pela casa, incluindo HDTV (televisão em alta-definição) e "Standard Definition Television" (SDTV), e está preparado para co-existir com o HomePlug 1.0. Outros requisitos são uma elevada largura de banda em qualquer local da casa. Para tal o áudio e o vídeo têm de ser entregues em perfeitas condições. O objectivo foi desenvolver uma tecnologia que suporte um elevado número de aplicações simultaneamente. A ideia do HPAV é fazer com que vários tipos de serviços possam ser disponibilizados com recurso à tecnologia HomePlug, ou seja, pode-se ter ligado a Ethernet, o VoIP, a rede *Wireless*, as consolas, a Internet, entre outros, tudo na mesma tecnologia. No futuro serão ainda disponibilizados mais serviços e opções [1].

O HomePlug funciona através da rede eléctrica e como todas as casas (dos países desenvolvidos) estão equipadas com cabos para a rede eléctrica não são necessários novos cabos para a comunicação. Todas estas tecnologias (HomePlug, IEEE 802.11) surgiram com a necessidade de existir em todas as casas redes internas e acesso a redes de banda larga, partilha de recursos e outros serviços. A ideia de não usar novos cabos tem recebido uma atenção especial, porque quando se projecta uma casa esse tipo de infra-estrutura não é contemplada e a sua instalação à posteriori comporta custos substanciais. A norma HomePlug, actualmente na segunda versão, foi desenvolvida pela HomePlug Powerline Alliance [1], em que a principal preocupação é a robustez de transmissão de dados para compensar os efeitos adversos do canal, pois o meio eléctrico é pior que o meio sem fios em termos de atenuação e ruído, sendo este o principal motivo para não ter sido tão usado no passado. Aparelhos eléctricos com sistemas de comutação "on/off" e lâmpadas de halogéneo, por exemplo, podem provocar impulsos de ruído que degradam a qualidade do sinal. Esta norma foi construída com a preocupação de qualidade de serviço (QoS), sendo criados níveis de

prioridade para estas redes terem um bom desempenho e serem o mais fácil de usar possível. Os produtos com certificado HomePlug são considerados seguros, fiáveis e fáceis de instalar.

2.2.1.2 - Caracterização do HomePlug 1.0

Devido aos problemas existentes na rede eléctrica, em particular as interferências, o HomePlug 1.0 utiliza a técnica de transmissão robusta OFDM (“Orthogonal Frequency Division Multiplexing” (OFDM)) combinada com detecção de erros de transmissão “Forward Error Correction” (FEC) e pedidos de reenvio de tramas “Automatic Repeat Request” (ARQ).

A ideia principal do OFDM consiste em dividir o espectro disponível em vários canais de menor largura de banda, com subportadoras de baixo débito [10]. Para obter uma elevada eficiência espectral, as respostas em frequência das subportadoras estão sobrepostas e são ortogonais. O OFDM utilizado no HomePlug é especialmente concebido para comunicações sobre a rede eléctrica. São utilizados 84 subportadoras igualmente espaçadas na banda de frequências entre 4.5MHz e 21 MHz. Para eliminar qualquer necessidade de igualização são usadas as técnicas de “Differential Binary Phase Shift Keying” (DBPSK) e “Differential Quadrature Phase Shift Keying” (DQPSK).

Ao nível do FEC, é usada uma concatenação de “Viterbi” e “Reed-Solomon” [2]. O problema do ruído impulsivo (causado pela comutação “on-off” de equipamentos domésticos, entre outros) é superado pelo FEC e por “data interleaving” que consiste na dispersão de dados por um período de tempo variável para corrigir erros que a técnica “Reed-Solomon” não consegue corrigir. Com “data interleaving” os erros devidos a impulsos localizados (“burst”) são espalhados por diferentes pacotes e assim o FEC tem menos erros para resolver em cada pacote [10].

Uma vez que o canal da rede eléctrica entre dois quaisquer pontos tem diferentes respostas em amplitude e fase, o HomePlug 1.0 utiliza uma aproximação adaptativa. A adaptação do canal é feita através da escolha da “Tone Allocation”, modulação e FEC. “Tone Allocation” consiste no processo de escolha de portadora que sofre menos perturbação, uma portadora fortemente condicionada é “desligada”. Este processo de escolha das melhores portadoras para modulação contribui também para a redução da taxa de erros [10] ao mesmo tempo que garante algum isolamento entre os pares comunicantes e confidencialidade de troca de informação.

A escolha do protocolo MAC conduz a mais desafios. As redes domésticas devem suportar desde a transferência de ficheiros até serviços que exijam um elevado QoS. A camada MAC do HomePlug [2] foi construída para interagir com a camada física e corresponder aos requisitos levantados.

Esta tecnologia utiliza dois formatos de trama que são a “trama longa” e a “trama curta”. As tramas são apresentadas na figura 2.2. Estas tramas usam vários delimitadores e todos partilham a mesma estrutura. Um delimitador consiste num preâmbulo e num campo de informação de controlo da trama¹. Os delimitadores transmitem informação temporal que irá ser usada pelo MAC para determinar a disponibilidade do meio. A sua robustez ajuda os nós a obter uma elevada precisão de sincronização, reduzindo as colisões. Se o pacote não couber numa trama longa usam-se mecanismos de segmentação e reconstrução para o enviar em

¹ O preâmbulo e o campo de informação de controlo da trama são usados para sincronização e controlo.

8 Estado da arte

múltiplas tramas longas. O cabeçalho da trama tem a informação necessária para o receptor reconstruir novamente o pacote.

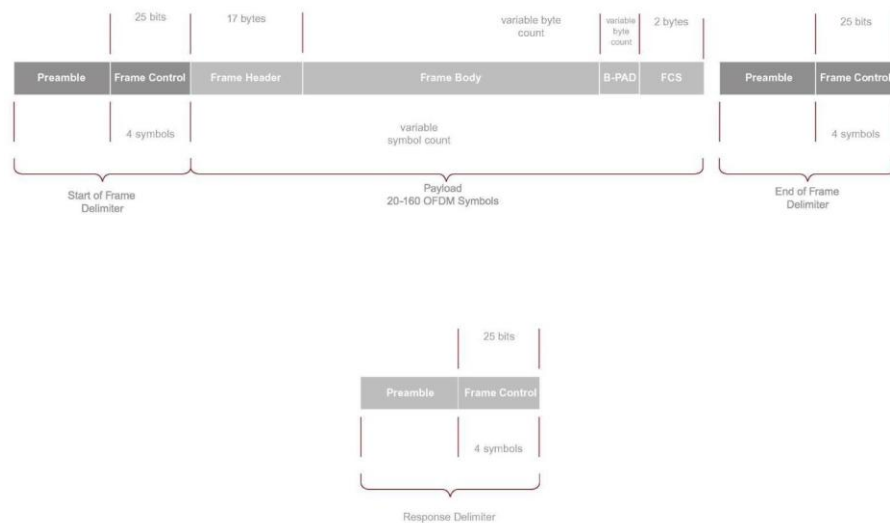


Figura 2.2 - Trama longa e curta do HomePlug 1.0 [10].

O mecanismo de acesso ao canal usado pelo HomePlug MAC é uma variante do protocolo “Carrier Sense Multiple Access/ Collision Avoidance” (CSMA/CA). Tipicamente, um protocolo CSMA/CA requer que os nós monitorizem o estado do meio. Se o meio estiver ocupado os nós não transmitem até este estar livre. Nesse caso, os nós vão esperar um certo período de tempo para evitar colisões. Um nó apenas vai transmitir se não detectar mais nenhum tráfego. O protocolo ainda inclui “carrier sensing mechanism”, “priority resolution” e um algoritmo de “backoff”. O esquema destes dois últimos é mostrado na figura 2.3. O “carrier sense mechanism” ajuda os nós a sincronizarem uns com os outros. Depois do fim de todas as transmissões, dois slots são alocados pela sua prioridade nos PRS. Este mecanismo de gestão das prioridades resulta num elevado nível nos parâmetros do QoS. No que diz respeito ao algoritmo de *backoff* usado pelo MAC foi concebido para disponibilizar uma utilização elevada da rede, mesmo quando existe tráfego na rede. É também estruturado para integrar os níveis de prioridade e as aplicações que esses níveis devem suportar. Como em qualquer algoritmo CSMA/CA, o “*backoff slot*” é escolhido aleatoriamente entre 0 e o tamanho da janela de contenção.



Figura 2.3 - Esquema do “Priority Resolution” e mecanismo de “Backoff” [10].

No que toca a desempenho, os testes realizados indicam que na maioria das casas é suportado um débito de 5Mbit/s na camada MAC [12], embora os débitos variem entre 1Mbit/s a 14Mbit/s. O HomePlug usa a banda de frequência entre 4.5 - 21MHz para transmitir o sinal através da rede eléctrica.

Uma parte importante desta tecnologia é a segurança, pois em todo o tipo de redes é importante garantir a privacidade. A privacidade e segurança do HomePlug são baseadas no

56-bit “Data Encryption Standard” (DES). Cada estação tem uma tabela com a chave de cifragem e a associada “Encryption Key Select” (EKS). Todos os transmissores numa mesma rede são cifrados com um “Network Encryption Key” (NEK) partilhado. Este NEK é único e define uma rede. Um utilizador para entrar numa rede tem o NEK da rede e o EKS associado. Os valores EKS funcionam como identificador para cada chave de cifragem. Para facilitar o processo de escolha de chaves de cifragem, o HomePlug define o uso de palavras-chave ASCII que geram as respectivas chaves. Para obter uma configuração privada é necessário, em cada estação, introduzir e seleccionar uma palavra-chave única para a rede. Cada estação vai ter nas suas tabelas os pares NEK/EKS que vão ser transmitidos através da camada MAC devidamente cifrados pelo “Default Encryption Keys” (DEK). Quando se transmite uma trama, a chave de cifragem codifica o corpo da mensagem e no cabeçalho segue a respectiva EKS. Quando uma estação recebe a trama usa o EKS para seleccionar a chave de cifragem associada da sua tabela de chaves para decifrar o corpo da mensagem.

Outro nível de segurança é o de garantir um único canal entre duas estações. O processo de estimativa do canal entre duas estações resulta num de par de “Tone Maps” com as portadoras, “FEC coding rate” e o método de modulação a ser usado em cada estação para cada sentido da comunicação. Os “Tone Maps” são reavaliados para se adaptarem às mudanças da rede. Uma terceira estação que pretenda comunicar com as duas já existentes tem de pedir o “Tone Map” a cada uma delas e que em princípio será diferente das duas anteriores, pois depende da impedância da ligação entre elas. Os “Tone Maps” de A -> B diferem dos de B -> A.

2.2.1.3 - Caracterização do HomePlug AV

O HomePlug AV representa uma nova geração da tecnologia HomePlug [13]. O seu objectivo é fornecer alta qualidade de som e imagem, multi-*stream* e entretenimento também ela através da rede eléctrica existente numa casa, sendo compatível com o HomePlug 1.0.

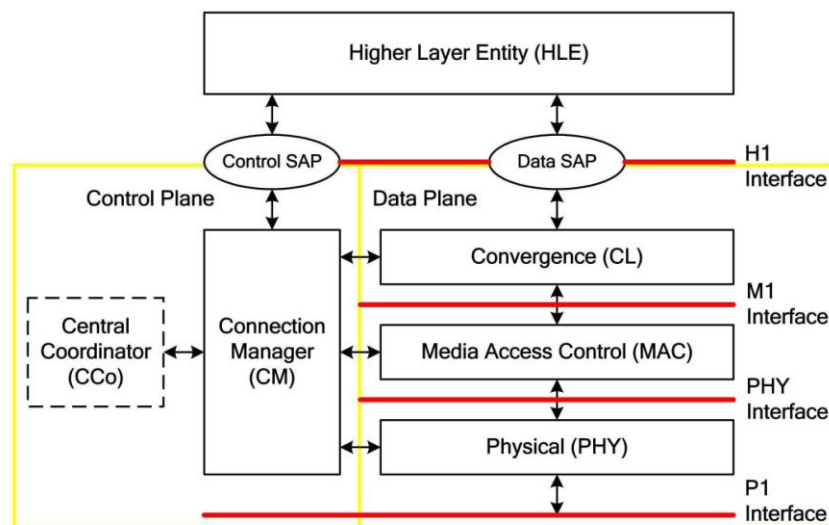


Figura 2.4 - Arquitectura HomePlug AV [13].

A arquitectura desta tecnologia [13], na figura 2.4, é composta pelo “Higher Layer Entities” (HLEs) que está acima da interface H1 (Host). O “Data Service Access Point” (SAP) aceita pacotes com formato Ethernet, logo todos os protocolos sobre IP são facilmente manipulados. Numa rede HPAV, o plano de controlo vai estar presente em todas as estações, mas o “Central Coordinator” (CCo) só vai estar activo numa única estação.

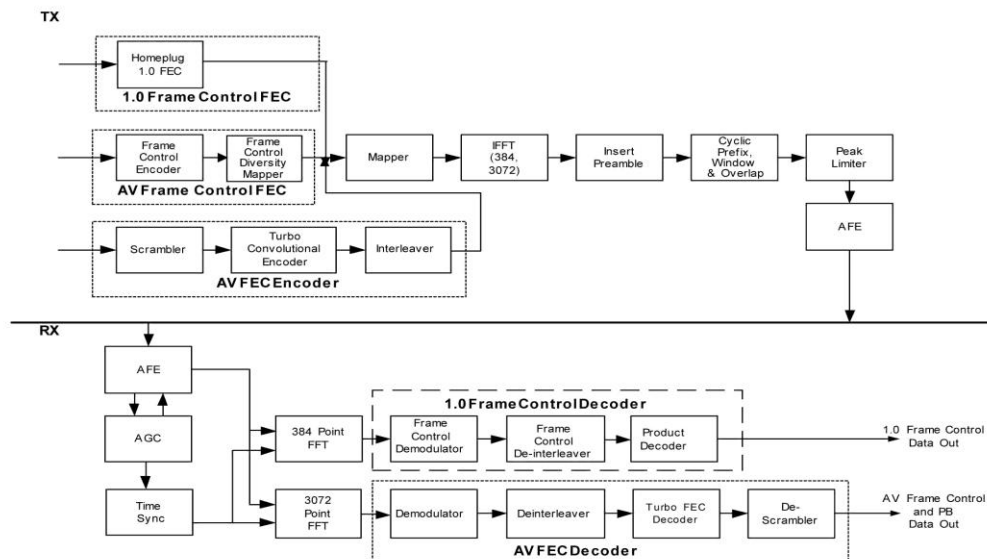


Figura 2.5 - Transmissor e Receptor OFDM do HPAV [13].

A camada PHY [13] [26] opera numa frequência entre os 2 e os 28 MHz e disponibiliza um débito no canal de 200 Mbit/s e um débito de informação de 150 Mbit/s. Utiliza OFDM, que permite um espectro flexível e “Turbo Convolutional Code” (TCC). Os símbolos OFDM longos, com 917 portadoras, são utilizados conjuntamente com um intervalo de guarda flexível. A modulação a ser usada pode ser desde BPSK a 1024 “Quadrature Amplitude Modulation” (QAM) dependendo das características do canal entre o transmissor e o receptor. No lado do transmissor a camada PHY recebe os inputs através da camada MAC, representados na figura 2.5 pelas setas de entrada que vêm da camada MAC. Os inputs dos dados HPAV são separados, existindo um para controlo da informação HPAV e outro para HomePlug 1.0. Depois de tratados os dados no transmissor, o resultado dos três *streams* é conduzido para a estrutura OFDM. No receptor, a informação recebida pelo “Analog Front End” (AFE), que trabalha em conjunto com o “Automatic Gain Controller” (AGC) e com um bloco de sincronização de tempo, separa os dados de informação e os dados de recuperação de circuitos. O HPAV PHY prevê a implementação de um espectro flexível que permite uma melhor adaptação a variações geográficas, de rede e de regulação.

HPAV tem um módulo “Contention Free” (CF) que ajuda ao cumprimento dos requisitos de QoS. Este CF funciona em “Time Division Multiple Access” (TDMA). Existe uma outra funcionalidade que é baseada em CSMA/CA que faz com que apenas os dados com maior prioridade sejam transferidos. Para implementar ambos os serviços existe um gestor central chamado CCo. O CCo fornece um “Beacon Period” que é dividido em três partes, o “Beacon Region”, o “CSMA Region” e o “Contention-Free Region”. A camada MAC disponibiliza CSMA e CF em cada “Beacon Period”. O HLE é responsável pelos requisitos QoS, em que o HLE usa o “Connection Specification” (CSPEC) que especifica os requisitos de QoS (i.e., garantir largura de banda, latência fixa, controlo de *jitter*, etc.). Se o CCo estabelecer uma ligação, este vai

pedir a cada estação para “ouvir” o meio. As estações vão fazer o seu “Tone Map” e a estimativa do canal de maneira a cumprir o QoS para a conexão dentro da região “CCo-managed Persistent Contention Free” (PCF) [13].

Cada CCo controla uma rede AV (AVLN - “AV Logical Network”) que é constituída por algumas estações AV em que todos partilham o mesmo “Network Membership Key” (NMK) para comunicarem de forma segura e privada. Como já foi dito o CCo fornece uma largura de banda para os serviços de gestão. Quando uma estação é ligada, esta ouve o meio. Se reconhecer uma AVLN vai tentar juntar-se a ela. Se por outro lado não reconhecer vai formar a sua própria AVLN e ser o CCo e enviar um beacon em broadcast. Qualquer outra que seja ligada pode agora juntar-se a esta e aumentar a AVLN. O CCo tenta aprender a topologia da AVLN e de outra rede vizinha qualquer. Para o alcançar, cada estação AV envia periodicamente em broadcast o “Discover Beacon” que contém informação sobre a estação e a AVLN a que pertence. O CCo vai receber de cada estação o “Discovered Station List” (DSL) e “Discovered Networks Lists” (DNL) e vai construir um mapa com a topologia da rede [13]. Este mapa é usado para saber se existe na rede alguma estação que pode ser melhor CCo que esta, e se existir as duas estações negociam entre elas as suas novas funções. O CCo pode também seleccionar um CCo-capable para que se torne o CCo principal em caso de falha. Para comunicar com estações escondidas é criado o “Proxy Coordinator” (PCo) que envia repetidamente beacons para as estações escondidas. Quando todas as estações estão desocupadas o CCo pede que a AVLN entre em gestão de energia, havendo apenas uma pequena região CSMA e PCF.

O CL funciona como interface entre os HLEs e o MAC no Data Plane. O uso do formato Ethernet torna mais fácil para as AVLNs interagir com outras LANs. Tanto no receptor como no emissor, o CL fornece ao CM informação suficiente para monitorizar o nível de QoS. O classificador examina cada pacote recebido por H1 e entrega-o, usando as regras de classificação [13]. O ACS é responsável pela manutenção da ligação no mesmo sentido em que o HLE faria. Na estação de destino, o CL trata dos pacotes recebidos e fornece informação para o CM garantir os níveis de QoS. O CM toma medidas, estabelecidas pelo CSPEC, se existir algum problema no QoS.

A respeito da segurança [13], o HPAV tem processos de controlo de admissão que garantem que apenas aparelhos com permissão podem entrar num AVLN. A possibilidade de uma estação manter várias palavras-chave permite-lhe participar em múltiplas AVLNs. A segurança é assegurada através da encriptação 128-bit “Advances Encryption Standard” (AES). A cifragem utiliza o “Network Encryption Key” (NEK) que pode ser automática e dinamicamente alterado. Para entrar num AVLN uma estação tem de obter um “Network Membership Key” (NMK), porém se já o tiver pode entrar na rede automaticamente. Quando uma estação tem o NMK correcto e se junta a uma AVLN, será dado o NEK actual que é usado de facto para cifrar dados durante a segmentação do MAC.

O HPAV incorpora mecanismos que proporcionam coordenação de redes vizinhas através do “Neighboring Networks” (NNs) [13]. Uma vez detectadas redes vizinhas, os CCos conseguem cooperativamente agendar transmissões nas suas próprias redes sem causar interferências nas outras. Cada CCo tem um “Interfering Network List” (INL). O INL identifica todos os CCos vizinhos que consegue ouvir. HPAV requer que o CCo tem de reconhecer todos os INLs que escuta e não interferir com essas redes. Quando um CCo de uma AVLN descobre outro CCo tenta coordenar-se com o novo CCo negociando um “beacon slot”. Quando as negociações estão acabadas ambos os CCos sincronizam os seus relógios. Todos os NNs

partilham a mesma região CSMA. Quando múltiplas AVLNs coexistem cada uma tem uma porção do “Beacon Period”, que por omissão é igual. Se uma AVLN utiliza mais do que a sua porção tem de baixar a sua quota se questionada pelos vizinhos.

A camada PHY [13] [26] do HPAV permite a coexistência e a interoperabilidade com os aparelhos que apenas suportam HomePlug 1.0. Os aparelhos HPAV têm de ser capazes de comunicar com os que apenas suportam a versão 1.0. Os mecanismos de coexistência são apenas colocados activos quando um ou mais aparelhos 1.0 são detectados. HPAV também é compatível com “Broadband over Powerline” (BPL) através de dois métodos: coexistência de serviços ou coexistência de tecnologias.

HPAV é a tecnologia mais rápida e robusta [13] que funciona através das linhas de energia, superando as outras tecnologias especialmente quando é encontrado uma elevada relação sinal/ruído (“Signal-to-noise Ratio” (SNR)) devido a todas as técnicas escolhidas pelo HPAV, desde a modulação, escolha de bandas para comunicação e correcção de erros.

2.2.1.4 - Melhorias e outros aspectos

Ao longo dos tempos, desde o surgimento do HomePlug 1.0, que existem investigadores que tentam melhorar alguns aspectos desta tecnologia. No que diz respeito à primeira versão, o HomePlug 1.0, e para melhorar o desempenho foi desenvolvido um repetidor ao nível do MAC [14], pois é impossível desenvolvê-lo na camada PHY, para facilitar a comunicação entre dispositivos situados em locais distantes um do outro. Outra melhoria foi o desempenho que o OFDM obtém com o “Low Density Parity Check” [15], em vez do proposto ROBO. Um último exemplo diz respeito à melhoria do desempenho do HomePlug através de uma simples modificação no mecanismo de evitar colisões [16], ao nível da subcamada do MAC que o vai tornar mais eficiente, melhorando o débito.

Quanto ao HPAV, já foi estudado qual o melhor algoritmo de bit-loading para maximizar o débito [17]. A escolha da modulação de cada subportadora deve ser feita por este algoritmo, que tem por base um valor estimado de SNR. Os resultados mostraram que quando uma subportadora com um determinado SNR é assumida o melhor algoritmo é o “Decreasing BER-constrained” (DBC), porém se a subportadora for estimada com uma margem para o SNR o desempenho do DBC e do BER “threshold constant” (BTC) é próxima. Outro método que pode melhorar o HPAV é o simples aumento da “Contention Window” (CW) [18] caso a rede esteja muito ocupada e, pelo contrário, a sua diminuição se estiver livre.

A utilização da tecnologia HPAV pode ser feita em conjunto com outra tecnologia. Existe um exemplo de um hospital que utiliza as tecnologias HPAV e IEEE802.16 [19], ou seja uma técnica com fios e outra sem fios. O HPAV foi adoptado para a entrega de dados médicos dentro dos edifícios do hospital para evitar as interferências com outros dispositivos médicos e permitir um débito de aproximadamente 200Mbit/s na camada PHY, enquanto o IEEE802.16 é utilizado para a comunicação entre diferentes edifícios do hospital. É utilizado um “QoS broker” que faz com que os mecanismos QoS em ambas as tecnologias estejam correlacionados e deste modo o desempenho está garantido, mesmo com descargas de ficheiros vídeo ou imagem ao mesmo tempo.

Relativamente a outros aspectos existem testes práticos feitos à tecnologia HomePlug 1.0 [12] que tentam demonstrar o desempenho desta em casos reais. Para esses testes utilizaram-se casas em diferentes localizações geográficas e com diferentes idades e tamanho. Depois de efectuados os testes foi verificado que esta tecnologia é altamente

robusta e disponibiliza um débito maior do que 5Mbit/s na maioria dos casos. Apenas cerca de 15% das ligações atingiu o débito máximo que é aproximadamente de 8.2Mbit/s. Na figura 2.6 são apresentados os resultados dos testes na presença de dois nós.

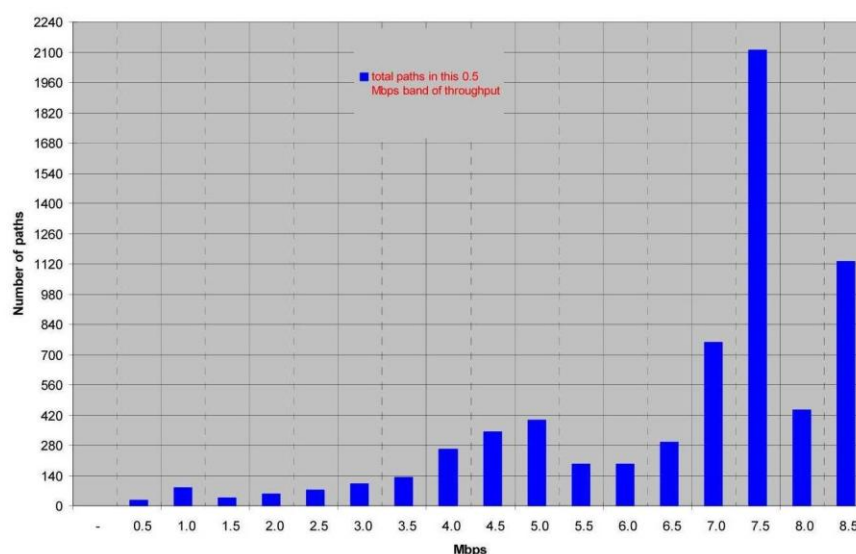


Figura 2.6 - Testes do débito do HomePlug 1.0 com 2 nós [12].

Nesta lógica, existem aparelhos como carregadores de telemóveis antigos e lâmpadas com reactores electrónicos que provocam uma redução na taxa de transmissão. Outra das conclusões foi que em casas muito grandes existe uma degradação do desempenho, embora não seja uma quebra muito significativa. No que diz respeito à idade das casas, o desempenho não é afectado por este aspecto. A tecnologia HomePlug aguenta altos débitos mesmo quando estão muitos nós na rede

2.2.2 - IEEE 802.11

2.2.2.1 - Aparecimento e utilização actual

A norma IEEE 802.11 contempla um grupo de especificações desenvolvidas pelo “Institute of Electrical and Electronics Engineers Inc.” (IEEE) para redes locais sem fios. Estas redes são mundialmente conhecidas por redes Wi-Fi, e por exemplo, em 2007 foram vendidas em todo o mundo cerca de 300 milhões de equipamentos [20]. O crescimento deste tipo de redes deveu-se ao aparecimento das redes de banda larga, sendo possível encontrar estas redes Wi-Fi em escolas, hospitais, centros comerciais, bibliotecas, entre outros. Em escritórios as redes sem fios têm a vantagem de permitirem, a partir de qualquer ponto, a um utilizador aceder à informação que necessita. Uma rede sem fios é um sistema de transmissão de dados concebido para a troca de informação entre dispositivos através de ondas rádio. Normalmente estas redes são usadas como ponto final de uma rede cablada que comunica com um conjunto de computadores, permitindo a estes utilizadores o acesso aos recursos e serviços disponibilizados pela rede.

Em 1989, um órgão americano que distribuía as frequências autorizou o uso de 3 faixas de frequência e um ano depois o IEEE estabeleceu um comité para produzir uma norma de

redes sem fios. Após sete anos de pesquisa, em 1997, foi aprovado o *standard* 802.11. Em 1999, foram aprovadas duas normas, o 802.11a e o 802.11b que funcionam em faixas de frequência diferentes. No ano de 2003 saiu a terceira norma que é o 802.11g. Actualmente, com os primeiros testes em 2006, já está disponível o 802.11n que traz vantagens em relação às versões anteriores. Estima-se que em 2013, 90% dos produtos Wi-Fi já vão ser compatíveis com esta norma [20]. Esta nova tecnologia é vista como um passo em frente, pois vai permitir aos utilizadores ver HDTV, fazer *streaming* de vídeo digital e outras aplicações com altos débitos. Esta nova norma responde a questões actuais importantes como o reforço da segurança, *roaming* e QoS.

2.2.2.2 - Standard 802.11

Esta foi a norma original que levou ao aparecimento das outras normas. O *standard* 802.11 foca-se nos dois níveis mais baixos do modelo do “International Organization for Standardization” (ISO), como é apresentado na figura 2.7: a camada física e a de ligação de dados.

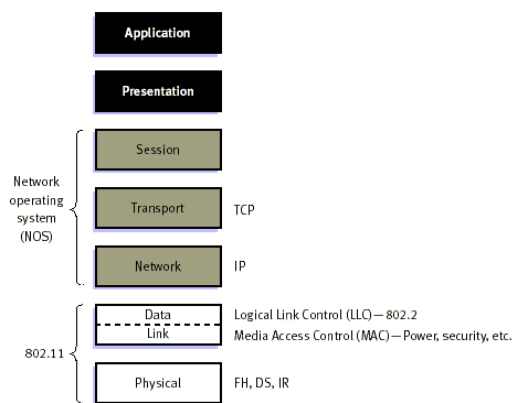


Figura 2.7 - IEEE 802.11 no modelo OSI [21].

Esta norma é composta por dois tipos de equipamentos: uma estação sem fios, normalmente um computador, equipado com um “Network Interface Card” (NIC) e um “Access Point” (AP), que funciona como uma “bridge” entre a rede sem fios e a cablada.

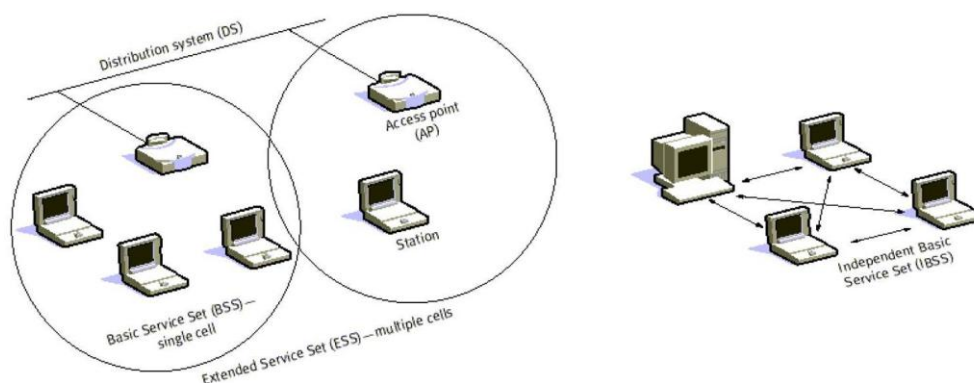


Figura 2.8 - Modos do standard 802.11 [21].

- a) Modo infra-estruturado (com formação de ESS)
- b) Modo ad-hoc.

O *standard* 802.11 define dois modos, o modo infra-estruturado e o modo *ad-hoc* [21], ilustrados na figura 2.8. O primeiro modo consiste em pelo menos um AP conectado à infra-estrutura cablada e um conjunto de estações sem fios. Esta configuração é conhecida por “Basic Service Set” (BSS). Por outro lado, um “Extended Service Set” (ESS) é um conjunto de dois ou mais BSSs que formam uma subrede. O modo *ad-hoc* funciona com várias estações sem fios que comunicam directamente umas com as outras sem recurso a nenhum AP. Este modo é útil em casos onde não existe uma infra-estrutura cablada, como numa sala de reuniões ou um espaço *outdoor*. Originalmente foi definida uma camada física com três modos de operação, duas com técnicas rádio de espalhamento espectral a funcionar a 2.4 GHz e um com especificação de infra-vermelho.

Inicialmente, o IEEE 802.11 possibilitava débitos de 1 ou 2 Mbit/s na camada física, dependendo do modo de operação, devido às técnicas de “Frequency Hopping Spread Spectrum” (FHSS) e “Direct Sequence Spread Spectrum” (DSSS). Destes dois modos de operação o mais utilizado é o que utiliza a técnica de DSSS, porque possibilita maiores débitos (2 Mbit/s). A técnica DSSS divide a banda de 2.4 GHz em 14 canais com largura de 22 MHz sem saltos para outros canais. Para compensar o ruído utiliza-se uma técnica chamada “chipping”, que consiste em que cada bit dos dados é convertido em séries padrão de bits redundantes chamados “chip”. Com esta técnica mesmo que o sinal sofra danos, em muito dos casos é possível recuperar, minimizando a necessidade de retransmissões. Usando a técnica de FHSS a banda de 2.4 GHz é dividida em 75 subcanais de 1 MHz. O transmissor e receptor concordam num padrão de saltos, definidos de modo a que se minimize a hipótese de dois transmissores usarem o mesmo subcanal simultaneamente, e os dados são enviados numa sequência de subcanais. As técnicas FHSS não permitem um débito superior a 2 Mbit/s devido ao “Federal Communications Commission” (FCC) que restringem a banda dos subcanais a 1 MHz. Estas restrições forçam o sistema FHSS a espalhar o espectro pelos 2.4 GHz, o que provoca saltos mais frequentes originando um aumento no *overhead* de salto.

No *standard* 802.11 é impossível detectar colisões devido ao problema de “near/far”, ou seja, para detectar uma colisão, uma estação tem de estar preparada para transmitir e ouvir o meio ao mesmo tempo, o que no meio de ondas rádio tipicamente não acontece. Devido a este problema foi adoptado o protocolo CSMA/CA. CSMA/CA evita colisões utilizando o pacote “acknowledgment” (ACK). Este processo introduz sempre um certo *overhead* às redes 802.11, embora lide bem com interferências.

Outro problema da subcamada MAC é a questão do nó escondido em que duas estações de lados opostos de um AP podem “ouvir” actividade de um AP, mas não entre si devido à distância ou obstruções. Para resolver este problema, 802.11 especifica um protocolo opcional “Request to Send/Clear to Send” (RTS/CTS) na subcamada MAC. Quando está em uso, o transmissor envia um RTS e espera que o AP responda com um CTS. Desde que todas as estações da rede “ouçam” o AP, o CTS faz com que elas não transmitam durante o envio dos dados de uma outra estação que já enviou o pedido. Como este processo também provoca *overhead* é apenas utilizado em pacotes de grandes dimensões, onde a retransmissão pode ser prejudicial em termos de largura de banda.

A subcamada MAC tem mecanismos que aumentam a robustez, tais como, o “Cyclic Redundancy Check” (CRC) checksum e a fragmentação do pacote. Cada pacote tem um CRC calculado e anexado para assegurar que os dados não foram corrompidos durante a transmissão. A fragmentação do pacote permite que pacotes maiores sejam divididos em pacotes mais pequenos quando são enviados, o que é útil quando o meio está congestionado e

com interferências, pois com este processo é menor a hipótese de serem corrompidos. Esta técnica reduz as retransmissões em muitos casos e melhora o desempenho geral da rede. O MAC é responsável por voltar a unir os pacotes sendo este processo transparente para protocolos de níveis mais altos. A camada MAC é responsável pela maneira como o cliente se associa a um AP. Quando um cliente está no meio de uma ou mais APs ele associa-se em função da força do sinal e dos pacotes perdidos. Depois de se associar a um AP, o cliente é periodicamente questionado com o objectivo de verificar se está conectado ao melhor AP disponível. Caso exista algum com melhores características, o cliente desassocia-se do AP antigo e associa-se ao novo. Estas mudanças de AP podem acontecer porque o utilizador muda de local (ou alteraram-se as condições de propagação no local), o AP está com demasiado tráfego ou então com o objectivo de espalhar os clientes por toda a infraestrutura.

Dados com requisitos temporais (“time-bounded”), como voz e vídeo, são suportados pela subcamada MAC através do “Point Coordination Function” (PCF), onde apenas um AP controla o acesso ao meio para garantir o QoS do sistema. Ao nível da segurança o *standard* IEEE 802.11 utiliza o protocolo “Wired Equivalent Privacy” (WEP) que disponibiliza controlo de acessos e mecanismos de encriptação. Para controlo de acesso, a rede sem fios é programada em cada AP para controlar cada utilizador que se queira associar. Só se podem associar utilizadores que o respectivo “MAC address” seja reconhecido pelo AP. Na encriptação é utilizada uma chave partilhada com 40 bits do algoritmo RC4 PRNG (“Ron’s Code or Rivest’s Cipher Pseudo Random Number Generator”) [21]. Todos os dados enviados e recebidos podem ser encriptados com esta chave. Quando este mecanismo de encriptação está activo, o AP envia um desafio para todas as estações que elas têm de resolver usando a sua chave para se autenticarem e garantirem acesso à rede.



Figura 2.9 - Estrutura da trama do *standard* 802.11.

No *standard* 802.11 são definidos três tipos de tramas que são das tramas de dados, controlo e gestão. Como se apresenta na figura 2.9, representados por address 1, 2, 3 e 4. Existe assim espaço para quatro tipos de endereços, ou seja, o endereço de destino, o endereço de origem, o endereço da estação base de destino e o endereço da estação base de origem.

2.2.2.3 - IEEE 802.11a

A norma IEEE 802.11a [31], que apareceu em 1999, utiliza uma faixa de frequência de 5 GHz que é diferente da faixa utilizada pelas outras normas 802.11 (na casa dos 2.4 GHz). O objectivo do aparecimento desta norma era proporcionar débitos superiores aos 11 Mbit/s oferecidos pela norma 802.11b. A faixa utilizada por esta norma está mais imune a

interferências, por exemplo de microondas ou aparelhos Bluetooth. O facto de não sofrer estas interferências, que podem afectar as taxas de transferência, é um ponto positivo desta norma. Um ponto negativo em utilizar frequências mais altas é o facto de reduzir o alcance e de ser mais difícil manter a qualidade do sinal na presença de obstáculos (e.g., paredes).

A norma IEEE 802.11a consegue atingir débitos máximos de 54 Mbit/s, utilizando 52 subportadoras, que dividem cada um dos 8 canais disponíveis a 20 MHz cada e utilizam o OFDM como esquema de transmissão. A informação é então modulada e codificada em cada uma das subportadoras que posteriormente a envia paralelamente por multiplexação. A técnica de modulação aplicada a cada subportadora pode ser BPSK, QPSK, 16-QAM ou 64-QAM. A técnica de acesso ao meio utilizada é igual nas normas 802.11a e 802.11b, o CSMA/CA. Apesar das semelhanças entre estas duas normas a nível da camada MAC, estas duas normas são incompatíveis devido às diferenças na camada física. A camada física do 802.11a está dividida em duas partes: o PLCP e o “Physical Medium Dependent” (PMD) que é adaptado à camada física através de uma função convergente [2]. Quando esta norma apareceu era mais cara do que a 802.11b, o que provocou que a aderência a esta norma fosse maior em empresas do que por utilizadores particulares [32]. Actualmente, esta norma continua a não ser muito popular para uso doméstico, e com o aparecimento da norma 802.11n que oferece maiores débitos, poderá continuar a ser sobretudo adoptada a nível empresarial.

2.2.2.4 - IEEE 802.11b

O aparecimento da norma IEEE 802.11b deveu-se ao facto de o *standard* IEEE 802.11 ser demasiado lento e estar a atrasar a evolução deste tipo de redes, pois os débitos de 2 Mbit/s eram insuficientes. O IEEE 802.11b permite débitos até 11 Mbit/s. As diferenças entre esta norma e o *standard* 802.11 são diferenças na camada física que proporcionam maiores débitos, que passaram de 2 Mbit/s para 11 Mbit/s, e melhor conectividade.

A contribuição desta nova norma foi obter na camada física duas opções com novas velocidades, 5,5 Mbit/s e 11 Mbit/s [21]. Para tal, o sistema 802.11b trabalha com o sistema DSSS do *standard* 802.11 com débitos de 1 e 2 Mbit/s, mas não com o sistema FHSS do *standard* 802.11. O DSSS aplicado no *standard* 802.11 utiliza para a transmissão de dados, entretanto transformados em símbolos, a técnica de BPSK para débitos de 1 Mbit/s e QPSK para débitos de 2 Mbit/s. O IEEE 802.11b utiliza uma técnica chamada “Complementary Code Keying” (CCK) que consiste num conjunto de 64 palavras código com 8-bit [21]. Como conjunto, estas palavras código têm apenas propriedades matemáticas, o que torna fácil a distinção pelo receptor mesmo na presença de ruído e interferências. O débito de 5,5 Mbit/s utiliza CCK para codificar 4 bits por portadora, enquanto o débito de 11 Mbit/s codifica 8 bits. Ambos os débitos utilizam QPSK como técnica de modulação. Para trabalhar em ambientes com muito ruído as redes 802.11b utilizam a técnica “dynamic rate shifting”, permitindo que os débitos de dados se ajustem automaticamente para compensar as alterações que acontecem no canal rádio. Esta técnica é transparente para o utilizador e para as camadas superiores da pilha de protocolos.

2.2.2.5 - IEEE 802.11g

A publicação da norma IEEE 802.11g [22] surge da convergência entre a norma IEEE 802.11a, utilizando o mesmo débito, e IEEE 802.11b, pois trabalha na mesma frequência (os 2,4GHz). Este facto vem promover a interoperabilidade com os equipamentos da norma b já instalados.

Na norma IEEE 802.11g utiliza-se DSSS, OFDM ou ambas a 2.4 GHz para se obter débitos de 54 Mbit/s. O facto de existirem, pela primeira vez, quatro modos diferentes de operação na camada física possibilita o uso de DSSS e OFDM em simultâneo.

O *overhead* de um pacote da camada física incorpora duas componentes: o preâmbulo, para a sincronização, e o cabeçalho, que guarda a informação sobre a camada física que formam o “Physical Layer Convergence Protocol” (PLCP). Para diminuir o *overhead* existente nas antigas normas devido ao longo tamanho do preâmbulo foi decidido torná-lo mais pequeno.

Tal como no IEEE 802.11b, o IEEE 802.11g adoptou os mesmos valores de tempo de slot (20 μ s) e de “minimum contention window” (31 slots). Os valores ideais de tempo de slot e de “minimum contention window” seriam idênticos aos adoptados pela norma IEEE 802.11a que são 9 μ s e 15 slots, respectivamente. Por esta razão o IEEE 802.11g utiliza um ajuste dinâmico destes valores definindo um atributo nas redes ERP em que as estações têm conhecimento através da trama do *beacon* que contem informações sobre a rede.

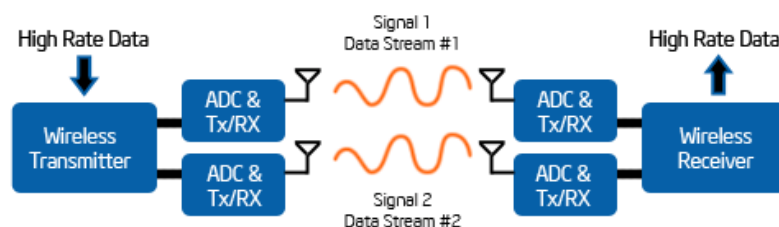
Numa rede IEEE 802.11g, uma estação pode escolher entre 14 débitos diferentes. Isto faz com que os problemas de interoperabilidade aumentem. Existem 3 tipos de estações nas redes desta norma: estações ERP (estas estações suportam ERP-OFDM), estações que não são ERP mas que permitem a utilização de preâmbulo curto (última geração do IEEE 802.11b) e estações que não são ERP nem suportam preâmbulo curto (versões mais antigas do IEEE 802.11b). Quanto ao problema de interoperabilidade se existir uma rede com estações ERP e estações não ERP, as estações ERP comunicam entre si através de pacotes ERP-OFDM que não são detectados pelas estações não ERP. Por isso se uma estação ERP transmitir um pacote o meio parece vazio para as estações não ERP e qualquer tentativa delas em transmitir vai resultar numa colisão. A primeira solução do IEEE 802.11g é o uso da camada física DSSS-OFDM, onde todas as estações são capazes de detectar transmissões [22], evitando assim que estações enviem pacotes ao mesmo tempo de forma a evitar colisões. A segunda solução é enviar pedidos de “request to send/clear to send” (RTS/CTS). Todos os RTS e CTS devem ser enviados através da camada ERP-DSSS. Se existirem apenas estações ERP não há necessidade de enviar RTS/CTS. Além destes mecanismos é ainda proposto o “CTS-to-self mechanism” [22], que é semelhante ao anterior mas reduz o *overhead* da rede embora não resolva de forma tão eficiente o problema do terminal escondido. Este mecanismo deve ser apenas usado quando todas as estações conseguem detectar a transmissão de cada uma delas.

Concluindo, estes melhoramentos fazem com que esta norma seja mais completa do que as anteriores. A maior novidade do IEEE 802.11g é o facto de suportar quatro opções de funcionamento na camada física que combinam os débitos do IEEE 802.11a com as especificações do IEEE 802.11b. Esta nova norma é compatível com o *standard* IEEE 802.11. Testes realizados [22] comprovam que a nova camada física melhora a capacidade do canal principalmente quando todas as estações têm interface IEEE 802.11g.

2.2.2.6 - IEEE 802.11n

Esta norma [20] trouxe uma solução para o aumento de débito e da gama de potência. Enquanto as normas anteriores suportam aplicações com débitos mais reduzidos, esta nova norma está sobretudo orientada para aplicações que necessitam de débitos elevados, tais como muitas aplicações dos dias de hoje. Para melhorar os débitos, o desafio foi alterar as camadas MAC e PHY para se obter um débito mínimo de 100 Mbit/s no MAC SAP (“Service Access Point”), o que quadruplica os valores apresentados nas normas b e g. Com o apoio da configuração de múltiplas antenas e maior largura de banda os débitos binários podem chegar aos 600Mbit/s. A evolução para esta norma prevê-se ser suave, na medida em que estes dispositivos são compatíveis com qualquer dos padrões anteriores. No que respeita à segurança este processo é totalmente compatível com 802.11i [44] (protecção dos dados), 802.11r [45] (segurança na mudança de ponto de acesso) e 802.11w [46] (segurança no transporte de pacotes na camada física).

Para aumentar a velocidade de transferência é usado um sistema de múltiplas antenas para o transmissor e receptor. Este mecanismo é conhecido por “Multiple Input Multiple Output” (MIMO) [20]. O mecanismo MIMO, representado na figura 2.10, tem um papel decisivo no comportamento da norma 802.11n, explorando o uso de múltiplos sinais transmitidos para o meio sem fios e recebidos do meio. Com várias antenas a funcionar no mesmo canal, mas a transmitir com características diferentes, o MIMO utiliza o espectro de forma mais eficiente. Cada receptor capta os sinais de todos os transmissores possibilitando fazer multi-caminhos para atingir os objectivos. A tecnologia MIMO fornece também “Spatial Division Multiplexing” (SDM) [47]. O SDM multiplexa no espaço diversos fluxos de dados independentes, transferidos simultaneamente dentro dum canal com uma largura de banda, o que permite aumentar o débito dos dados à medida que aumentar o número de fluxos de dados espaciais resolvidos. O MIMO requer diferentes frequências de rádio e um conversor analógico-digital para cada antena MIMO. Outro instrumento importante para aumentar a taxa de transferência é o aumento da largura de banda dos canais. Usando uma maior largura juntamente com OFDM oferece vantagens quando se pretende maximizar o desempenho. Esta técnica permite a utilização de mais do dobro da banda de canal do que o usado com outros modos. A abordagem MIMO diz que apenas os canais que usam 20MHz exigem mais custos de implementação.



How a Smart Antenna (MIMO) System Works

Figura 2.10 - Funcionamento do sistema MIMO [20].

Um dos maiores problemas para redes sem fios é a segurança. Devido a esta preocupação a equipa IEEE começou a trabalhar no 802.11i para proteger a integridade dos dados através de cifragem por 128-bits AES e de autenticação (EAP - “Extensible Authentication Protocol”).

O primeiro sistema de segurança implementado foi o Wi-Fi Protected Access (WPA) [20], que veio resolver algumas das vulnerabilidades do WEP com o uso de chaves de cifragem de 128-bits e o uso do “Temporal Key Integrity Protocol” (TKIP). A “Message Integrity Check” (MIC) impede os atacantes de capturar e alterar os dados de um pacote. Actualmente existe o WPA2 que fornece uma chave de cifragem por 128-bits AES, confidencialidade de dados, autenticação, integridade e protecção contra a reprodução².

2.2.2.7 - IEEE 802.11p

Esta norma tem uma filosofia diferente das anteriores e é vocacionada para utilização em veículos. Embora não seja testada na parte prática deste trabalho, até porque embora o grupo do IEEE 802.11p já tenha terminado o seu trabalho espera-se que esta norma seja publicada a 15 de Julho de 2010, esta evolução na norma 802.11 deve ser registada no âmbito deste trabalho, pois pode proporcionar interacção entre dispositivos móveis e permitir uma gestão de mobilidade e troca de dados em contextos de vigilância. A norma IEEE 802.11p [23] é um projecto que surgiu para a alteração do *standard* IEEE 802.11 para permitir o acesso sem fios em ambientes veiculares (WAVE). Esta nova norma implementa melhorias com o objectivo de suportar aplicações de Sistema Inteligente de Transporte (ITS). Isto inclui a troca de informação entre veículos de alta velocidade e com as infra-estruturas rodoviárias. O 802.11p baseia-se numa norma de uma camada superior que é o IEEE 1609. A comunicação entre veículos impõe o aparecimento de um novo paradigma na comunicação sem fios. O facto de os veículos se moverem e da própria natureza de uma estrada, por exemplo, apresenta-se como um desafio para a camada física. Nos Estados Unidos da América, esta norma utiliza uma banda de frequência para uso exclusivo das comunicações veículo/veículo e infra-estrutura/veículo através do “Dedicated Short Range Communications” (DSRC). O espectro do DSRC é estruturado em sete canais com 10 MHz de largura. Existe um canal de controlo (CCH) para comunicações seguras, os dois últimos reservados para casos especiais e o resto são canais de serviço (SCH) para comunicações seguras ou inseguras.

Ao nível da camada MAC o principal objectivo é o de simplificar as operações de “Basic Service Set” (BSS) de modo a ter uma comunicação *ad-hoc* pura. Os mecanismos BSS controlam o acesso a um AP. Nesta norma o problema é o reduzido período de tempo que existe para a troca de informação. Para resolver esta questão o IEEE 802.11p diz que cada estação em modo WAVE pode receber ou transmitir dados, com o “Basic Service Set Identification” (BSSID) mas sem ter de pertencer a nenhum BSS. Mesmo para comunicações não seguras o *overhead* existente em BSS é um problema, pois com o veículo em movimento o espaço em que vai ter cobertura de rede é curto. Para tal, foi criado o WBSS (“Wave BSS”) que permite que uma estação pode decidir se se conecta apenas com a recepção de um “WAVE advertisement” em vez de um processo mais complicado com troca de informações dos dois lados que demora mais tempo. Com este mecanismo o *overhead* baixa, porque não há processos de autenticação e associação. As camadas superiores serão responsáveis por tornar este processo seguro. Uma estação em modo WAVE pode receber e enviar tramas de

² Um ataque por reprodução consiste na interceptação de pacotes, que depois são usados ou para sobrecarregar a rede ou para entrar nela sem autorização.

dados com o BSSID com os campos “to distribution service (DS)” e “from DS” a 0. Uma estação não deve pertencer a mais do que um WBSS ao mesmo tempo.

Na camada PHY, o objectivo é modificar o menos possível em relação ao *standard* 802.11. A comunicação é possível pois esta norma vai utilizar frequências semelhantes às usadas na IEEE 802.11a que é 5 GHz. Sendo assim, existem apenas três modificações. A primeira, e visto que esta norma funciona com OFDM PHY, é alterar a largura dos canais passando de 20 MHz, usado em 802.11a, para 10 MHz duplicando todos os valores temporais usados no OFDM. Outra modificação deve-se ao problema de interferências entre os canais e por último foram definidas quatro máscaras espectrais para as diferentes operações existentes.

2.2.3 - Comparação das tecnologias

Nesta parte do capítulo iremos estabelecer algumas comparações entre as diferentes tecnologias com base em estudos feitos e apresentados na literatura.

2.2.3.1 - IEEE 802.11a, IEEE 802.11b, IEEE 802.11g e IEEE 802.11n

A vantagem da norma IEEE 802.11b [21] é o facto de ser uma tecnologia madura, pois já é “antiga” o que faz também com que os preços dos seus aparelhos sejam reduzidos. Esta norma possui um bom alcance. No entanto, é a norma que tem menor débito e apenas três canais de rede. No que respeita ao 802.11g volta a usar a banda de frequências do 802.11b. Como ponto forte, a norma 802.11g apresenta o facto de ser compatível com as normas anteriores, mas com um débito maior. A norma apresenta a mesma desvantagem de limitação de canal em relação ao IEEE 802.11b [25].

Segundo um estudo [25], onde foi realizada uma comparação entre a norma 802.11b e 802.11g, esta última obteve melhores resultados. Para os testes foi criado um ambiente semelhante ao de uma casa ou escritório, O objectivo destes testes são medir o débito de cada uma das normas e o seu comportamento à medida que se afastam do AP. A tarefa era fazer um *upload* de um ficheiro de 5 MB.

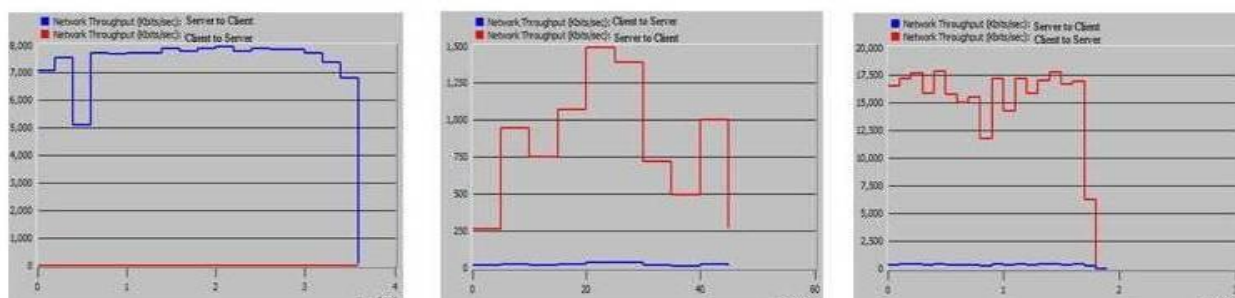


Figura 2.11 - Gráficos dos resultados dos testes de comparação entre a norma 802.11b e 802.11g [25].

Na figura 2.11, no primeiro gráfico vê-se os resultados da norma 802.11b. O gráfico mostra que o débito da norma foi constante entre os 7 e os 8 Mbit/s. No gráfico do meio está o resultado do *upload* do ficheiro pela norma 802.11g quando se encontra afastada da AP. Pode-se constatar que o débito binário foi bastante irregular variando dos 250 kbit/s até aos 1,5 Mbit/s. No último gráfico a norma 802.11g fez o *upload* nas mesmas condições da norma 802.11b. Comparando as duas normas constata-se que a norma 802.11g atingiu maiores débitos, cerca de 17,5 Mbit/s constantes, e que por isso o tempo de *upload* do ficheiro foi menor.

Tabela 2.1 - Valores comparativos entre a norma 802.11a, 802.11b, 802.11g e 802.11n.

	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n
débito máximo over-the-air	54 Mbit/s	11 Mbit/s	54 Mbit/s	600 Mbit/s
banda de frequência	5 GHz	2.4 GHz	2.4 GHz	2.4 GHz & 5 GHz
Cobertura <i>indoor</i>	50 m	100 m	100 m	150 m
canais sem sobreposição	13	3	3	3(2.4 GHz) e 23(5 GHz)

Na tabela 2.1 estão resumidos os principais aspectos de cada tecnologia. Pode-se concluir que a norma IEEE 802.11n é a que tem maior débito e a que apresenta maior cobertura. Como é a que possui um maior débito é a indicada para serviços de voz e imagem de alta definição. Contudo, as outras normas são mais antigas, o que as torna mais maduras e faz com que os seus aparelhos sejam mais baratos. A norma 802.11a é um caso particular que surgiu no início da tecnologia Wi-Fi juntamente com a norma b, mas funciona numa banda de frequência diferente da norma b e g. A norma 802.11a apresenta o mesmo débito que 802.11g, tem mais canais sem sobreposição, mas tem menos cobertura.

2.2.3.2 - HomePlug AV e HomePlug 1.0

A norma HomePlug AV também já foi testada em casas e apresenta débitos que podem ser 10 vezes superiores ao da norma anterior [26]. Esta melhoria fica-se a dever ao facto da norma HPAV ter maior largura de banda, mais potência, transmissão coerente, maior ordem de modulação, melhores técnicas de concatenação e escolha de canal e uma sinalização eficiente. Esta comparação não está muito elaborada, mas ainda não existe literatura que permita uma comparação num cenário real.

2.2.3.3 - IEEE 802.11b e HomePlug 1.0

Segundo um teste de desempenho [24], onde ambas tinham exactamente as mesmas condições e o objectivo era a transferência de um ficheiro em vários locais da casa, pode-se concluir que o HomePlug 1.0 foi sempre melhor do que a rede sem fios atingindo débitos mais elevados. Durante a realização dos testes não havia mais tráfego na rede.

Transmitter Location	Receiver Location	Tx to Rx Distance	802.11b T'put (Mbps)		Powerline T'put (Mbps)	
			WSFTP	TTCP	WSFTP	TTCP
Laptop-1	Laptop-2	2 ft	3.2	4.9	4.2	5.2
Study Room	Dinning Room	23	3.6	4.7	4.5	5.3
Home Office	Kitchen	~35	2.5	4.1	4.0	4.5
Kitchen	Home Office	~35	2.4	1.6	3.1	3.1
Bedroom C	Home Office	~70	No Conn.	No Conn.	1.9	1.8
Home Office	Bedroom C	~70	No Conn.	No Conn.	4.1	3.9
Pool Area	Home Office	~60	No Conn.	No Conn.	2.0	1.6
Home Office	Pool Area	~60	No Conn.	No Conn.	2.4	2.8

Figura 2.12 - Resultados do teste de comparação entre a norma HomePlug 1.0 e a norma 802.11b [24].

Uma vantagem do HomePlug, como se pode ver na figura 2.12, é o facto de ter conectividade em todos os locais onde foram realizados os testes. Durante a transferência do ficheiro constatou-se que os débitos do HomePlug são mais constantes do que da norma IEEE 802.11b. Longas distâncias entre o transmissor e o receptor prejudicaram o comportamento de ambas as tecnologias, mas a existência de uma parede entre o transmissor e o receptor criou uma quebra no débito da rede sem fios.

2.3 - Vídeo em “tempo-real”

Nos últimos anos, a utilização de vídeo digital no formato comprimido sofreu uma enorme expansão, sobretudo devido à massificação do uso da Internet e à distribuição de filmes e canais de televisão no formato digital. O aparecimento destas normas foi promovido pela “International Telecommunication Union” (ITU-T) e da “International Standards Organization/International Electrotechnical Commission” (ISO/IEC) em colaboração com empresas de electrónica, telecomunicações e universidades.

2.3.1 - Principais codificações

A necessidade de comprimir o vídeo digital surgiu devido ao elevado débito que resulta da sua representação digital não comprimida. Uma codificação consiste na representação da informação à saída da fonte por um menor número de símbolos a transmitir, com o principal objectivo de reduzir a largura de banda, sendo a descodificação o processo inverso. Estes processos de codificação/descodificação podem ser apresentados como compressão/descompressão. As características mais importantes de um codificador/descodificador são a taxa de compressão, a complexidade e o atraso introduzido no sinal. A codificação de vídeo é feita a partir de uma análise temporal e/ou espacial das imagens primitivas, com o objectivo de retirar a informação redundante ou pouco importante. Existem codificadores clássicos que retiram esta informação redundante das imagens, por exemplo, a compensação de movimento [29] e a transformada discreta de Coseno (DCT) [29].

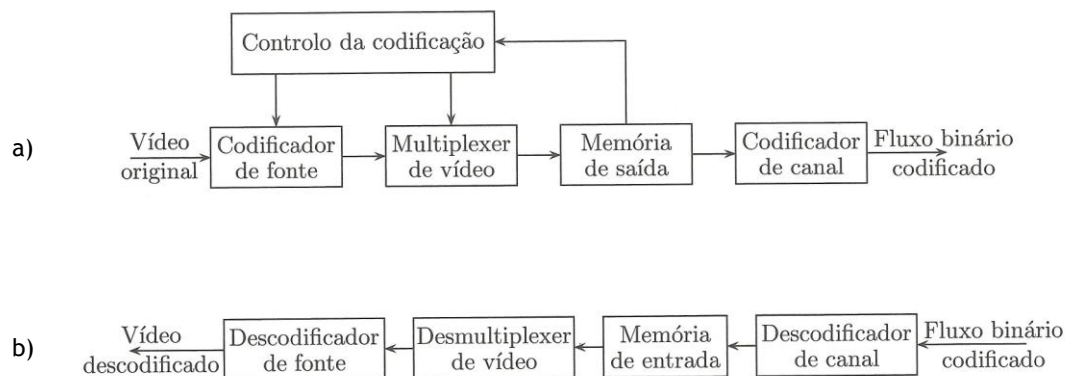


Figura 2.13 - Codificador/Decodificador geral de vídeo [27].

a)Diagrama de blocos geral de um codificador de vídeo.

b)Diagrama de blocos de um decodificador de vídeo.

Na figura 2.13 é apresentada a estrutura de um codificador e decodificador de vídeo com as suas principais tarefas. Nesta fase do trabalho vão ser apresentadas as normas H.261, H.263, MPEG-1, MPEG-2, H.263, MPEG-4 e H.264/AVC. Em relação ao seu surgimento apenas uma alteração cronológica com a passagem da norma H.263 para depois da H.261 quando apenas surgiu depois da norma MPEG-2. Esta alteração permite um melhor entendimento em relação às inovações que surgiram em cada norma.

2.3.2 - Caracterização das codificações mais relevantes

Em 1990, a actual ITU-T, estabeleceu uma recomendação para adaptar a transmissão de vídeo à tecnologia de Rede Digital com Integração de Serviços (RDIS). O H.261 a norma mais utilizada actualmente para a realização de videoconferências a $p \times 64\text{ kbit/s}$ (p é um inteiro de 1 a 30). Usam-se as técnicas de compressão que são utilizadas em todos os algoritmos de vídeo, onde o nível de qualidade inferior, 64 kbit/s necessita de uma elevada taxa de compressão, funcionando perfeitamente em terminais com visores mais reduzidos. Na capacidade máxima ($30 \times 64\text{ kbit/s} = 1,92\text{ Mbit/s}$) a qualidade é semelhante à de um “Video Home System” (VHS). Esta foi a primeira norma a aplicar um algoritmo de compressão híbrido [28] para aplicações em vídeo-conferência. A norma H.261 foi a primeira que se impôs como standard de compressão de vídeo, sendo progressivamente ultrapassada pela norma H.263.

O desenvolvimento do MPEG-1 decorreu entre 1988 e 1993, com o objectivo de codificar vídeo e áudio para armazenamento digital em dispositivos como o “Compact Disc” (CD), com qualidade VHS, requerendo que áudio e vídeo tenham um débito binário até cerca de $1,5\text{ Mbit/s}$. Esta primeira norma MPEG surgiu como resposta às necessidades da indústria em disponibilizar um modo de armazenamento de informação digital audiovisual mais eficiente do que a gravação em cassetes sem prejudicar a qualidade. A qualidade do vídeo decodificado deve ser pelo menos semelhante à obtida pelos sistemas analógicos de gravação de vídeo VHS.

A norma especifica a sintaxe e as funções disponíveis para a codificação, mas não define o codificador. A norma MPEG-1 (ISO/IEC 11172) foi publicada em cinco partes: Sistemas, Vídeo, Áudio, Compliance Testing e Software Simulation.

A norma MPEG-1 Vídeo não especifica o processo de codificação, somente o processo de decodificação e a sintaxe e semântica do fluxo binário, de modo a assegurar que qualquer fluxo possa ser decodificado por qualquer dispositivo que esteja de acordo com as normas. A norma MPEG-1 suporta sequências de vídeo em formato progressivo e com uma resolução espacial e temporal designada por “Source Input Format” (SIF). A informação vídeo na parte MPEG-1 Vídeo está organizada numa estrutura hierárquica, que consiste em seis níveis: sequência (Sequence), grupo de imagens (“Group of Images” (GOP)), imagem (Picture), grupo de macroblocos (Slice), macrobloco (MacroBlock (MB)) e bloco (Block). Essa estrutura hierárquica pode ser melhor analisada na figura 2.14.

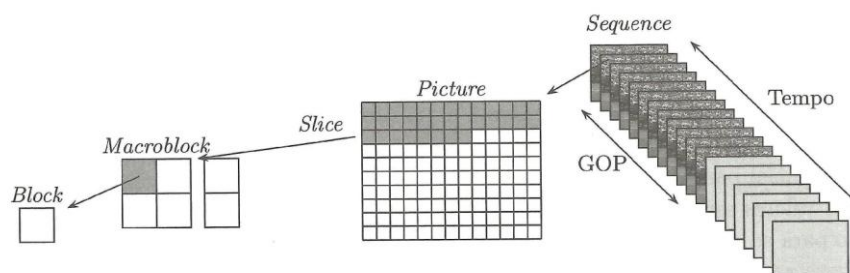


Figura 2.14 - Estrutura dos dados relativos a uma sequência de vídeo [27].

As aplicações para a norma MPEG-1 podem ser classificadas do tipo simétrico ou assimétrico [29]. Uma característica que distingue o MPEG-1 para o H.261 consiste no facto do H.261 se destinar essencialmente a serviços em tempo real, enquanto que o MPEG-1 se destina a aplicações para gravação de vídeo digital comprimido. Como o MPEG-1 inclui também uma norma para a codificação de áudio, é a norma utilizada para a codificação de vídeos de boa qualidade e para o *streaming* de vídeo através da Internet. Esta norma é utilizada pelo “Video CD” (VCD) que suporta a resolução espacial de 352 x 288 pixels e tem a possibilidade de introdução de legendas ou playback, som estéreo com débitos entre 128 e os 284 kbit/s. Esta versão do VCD tornou-se particularmente popular em leitores de karaoke.

A ITU-T desenvolveu um upgrade da antiga H.261 de forma a aumentar a sua eficiência, expandindo a aplicação destas técnicas a velocidades de transmissão mais baixas para que os primeiros modems que operavam a velocidades inferiores a 64Kbit/s a pudessem adoptar. Para tal, em 1995, surgiu esta norma H.263 que se baseou na anterior, o que provocou a manutenção da estrutura básica da norma H.261 em que ambas apresentam um codificador híbrido, bem como um conjunto adicional de funcionalidades, quase todas opcionais.

As inovações trazidas por esta nova norma são o facto da estrutura da imagem permitir novos formatos com uma resolução espacial reduzida (“4CIF”, “16CIF” e “Sub-QCIF” (SQCIF) e com uma frequência de imagens por segundo também mais reduzida.

A eficiência do H.263 é superior à do H.261 em ~1,5 a 2 vezes e o débito binário não comprimido varia entre os 4.4 Mbit/s para SQCIF e os 584 Mbit/s para 16CIF.

Esta norma teve duas evoluções que melhoraram as suas características que foram a norma H.263+, que surgiu em 1998, com novos modos de codificação e ferramentas adicionais, para melhorar a qualidade do vídeo. Em 2001 apareceu a norma H.263++ oferecendo ainda mais ferramentas e capacidades, tais como, o aumento da eficiência da

codificação para aplicações com pouco atraso, maior robustez a erros para transmissões de vídeo em tecnologia sem fios e suporte para vídeo entrelaçado.

A gama de aplicações para esta recomendação é muito vasta e alguns exemplos são a videoconferência por computador ou com equipamento dedicado, a transmissão de vídeo na Internet ou por telemóvel e sistemas de monitorização e vigilância.

Débito binário (kbit/s)	Frequência de trama	Formato	Norma	H.261 Y SNR (dB)	MPEG-1 Vídeo Y SNR (dB)	H.263 (Perfil 3) Y SNR (dB)
1152	30	CIF	MPEG-1 Vídeo		33.53 ($M = 1$)	
			H.261 ($p = 18$)	32.85	33.67 ($M = 2$)	37.87
			H.263 Nível 40		33.58 ($M = 3$)	
384	30	CIF	H.263 Nível 30		29.07 ($M = 1$)	
			H.261 ($p = 6$)	28.81	28.89 ($M = 2$)	33.83
					28.27 ($M = 3$)	
64	15	QCIF	H.263 Nível 10 H.261 ($p = 1$)	25.11	Não disponível	31.96
32	7.5	QCIF	H.263 Nível 10	23.37	Não disponível	28.96

Figura 2.15 - Desempenho comparativo de codificação [27].

Na figura 2.15 apresentam-se os resultados da comparação do desempenho da norma H.261 com a norma MPEG-1 Vídeo e a norma H.263 utilizando o perfil 3. Os resultados indicam que existe um ganho de 4 a 5 dB da norma H.263 em relação à norma MPEG-1 que apresenta melhores resultados do que H.261. Este ganho deve-se às técnicas de compressão mais eficientes [27] [29].

Quando saiu o MPEG-1 os resultados foram tão satisfatórios que se antecipou logo a possibilidade de fazer uma norma para TV e HDTV, que veio a ser o MPEG-2. O MPEG-2 conduziu também a perda de interesse no MPEG-1. O MPEG-2 surgiu devido ao crescimento das tecnologias vídeo e das próprias redes de transmissão que passaram a possibilitar diversos tipos de acesso e velocidades de transmissão mais rápidas. O desenvolvimento deste codificador deu-se em paralelo com o H.262 para TV digital, acomodando todos os formatos desde a baixa definição até HDTV. Os requisitos a satisfazer pela norma tiveram em conta um vasto universo de aplicações e por isso na elaboração do MPEG-2 participaram empresas de telecomunicações, fabricantes de electrónica de consumo e fornecedores de serviços de transmissão, entre outros.

A norma MPEG-2 foi desenvolvida com uma estrutura complexa e flexível apresentando um maior número de partes do que MPEG-1 (dez ao todo).

Tal como em MPEG-1 Vídeo, a norma MPEG-2 Vídeo não especifica a codificação do sinal de vídeo, mas apenas a sintaxe e a semântica do fluxo de dados e o processo de descodificação. O MPEG-2 Vídeo é compatível com o MPEG-1 Vídeo, na medida em que é capaz de descodificar o fluxo de dados gerados por um codificador de vídeo MPEG-1. A estrutura de fluxo de dados é também ela muito semelhante à estrutura do MPEG-1.

As diferenças fundamentais entre o MPEG-1 Vídeo e o MPEG-2 Vídeo estão relacionadas com o aparecimento, nesta última, da codificação de vídeo no formato entrelaçado e a codificação escalável. O MPEG-1 Vídeo só aceita formatos não entrelaçados, ou seja, progressivos e a codificação é sempre não escalável [29].

Inicialmente, o objectivo em termos de qualidade do MPEG-2 era obter vídeo entrelaçado de qualidade de televisão difundida actualmente a débitos entre 4 a 9 Mbit/s. Para alta definição tinha-se estabelecido o MPEG-3, mas como o MPEG-2 provou ser capaz de codificar imagens HDTV, os requisitos do MPEG-3 foram incluídos na norma MPEG-2. Foram adicionadas mais algumas ferramentas ao MPEG-2 Vídeo para se oferecerem mais funcionalidades e qualidade, nomeadamente novos modos de predição para suportar a codificação de vídeo entrelaçado e extensões para codificar vídeo escalável.

A qualidade percebida nesta norma é considerada boa conseguindo-se compressões em vídeo de aproximadamente 100/1. Todas as mudanças introduzidas no MPEG-2 possibilitaram o suporte de novas tecnologias ou funcionalidades como o “Digital Versatile Disk” (DVD), transmissão digital de televisão nos formatos PAL, SECAM ou NTSC, com débitos binários até 100Mbit/s e diferentes resoluções espaço-temporais.

A norma MPEG-2 Vídeo tem como principais aplicações a difusão de televisão digital e o armazenamento em DVD, onde é possível a visualização de vídeos comprimidos com alta qualidade. Recentemente apareceu a tecnologia “Blu-Ray” que também pode utilizar esta norma. A norma MPEG-2 é uma das normas com mais sucesso e contribui de forma significativa para a entrada na designada “era digital”.

Em 1994 e depois de uma análise pormenorizada das grandes tendências no panorama das aplicações, produtos e expectativas na área audiovisual, decidiu-se que a norma MPEG-4 deveria ter como objectivo principal oferecer novas maneiras de comunicar, aceder e manipular informação audiovisual digital, baseadas nomeadamente no próprio conteúdo ao contrário do que acontecia até então, onde o conteúdo propriamente dito não desempenhava um papel na representação do mesmo, ou seja, era representado como uma matriz de *pixels*, independentemente do que nele se passava. Nesta fase os objectivos já são a compressão para cinema, estúdio, redes sem fios, entre outros. A actividade de normalização do MPEG-4, que surgiu em 1999, iniciou-se para a transmissão de TV em redes sem fios. Com os novos algoritmos que permitem suportar codificações a débitos baixos, foi possível atingir uma qualidade superior à apresentada em MPEG-2. Os principais objectivos do MPEG-4 são a interactividade ao nível dos conteúdos, a eficiência na compressão e o acesso universal. A interactividade ao nível dos conteúdos permite o acesso e a gestão eficiente, a manipulação e a edição eficiente, a codificação e a composição bem como a manipulação eficiente de conteúdos, sempre com possibilidade de acesso aleatório ao conteúdo da informação audiovisual. Esta interactividade encontra-se exemplificada na figura 2.16 onde, cada imagem é composta por vários objectos e estes podem ser codificados e decodificados independentemente uns dos outros.

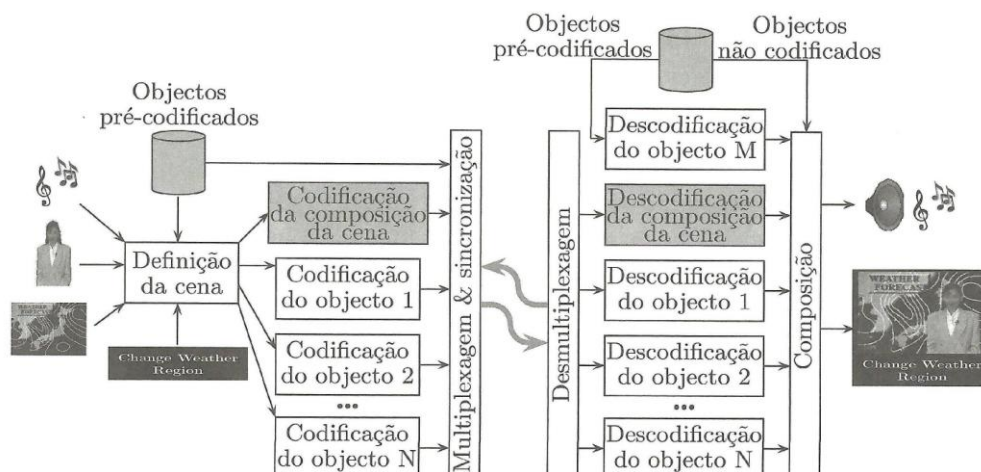


Figura 2.16 - Arquitectura simplificada da representação audiovisual MPEG-4 [27].

Apenas com o MPEG-4 é possível diferenciar os vários elementos que constituem uma cena quer no espaço quer no tempo. De facto, nas normas MPEG anteriores a cena era sempre vista como um todo.

Tal como nas normas anteriores, a norma MPEG-4 especifica o funcionamento dos descodificadores associados aos vários tipos de dados e a sintaxe e semântica dos fluxos binários, mas não a codificação.

A estrutura do MPEG-4 é dividida em 10 partes [28]. Esta norma apresenta múltiplas ferramentas em todas as partes. Ao contrário das normas MPEG-1 e MPEG-2 onde a parte da norma que especifica a codificação de informação visual se chama Vídeo, no MPEG-4 essa parte é chamada de Visual para expressar de maneira clara que especifica ferramentas de codificação não apenas para conteúdo visual natural mas também sintético. Um pormenor importante do MPEG-4, presente na parte 6 (“Delivery Multimedia Integration Framework” (DMIF)), é ter uma subcamada responsável por fornecer o transporte adequado à QoS definida para a sessão de vídeo. A parte 6 tem como principais tarefas o suporte de todo o tipo de redes, o controlo do QoS que pode ser de três tipos: controlo contínuo, controlo a pedido ou controlo de violação de QoS.

Testes realizados pela ISO revelaram desempenho superior às outras técnicas até então existentes no que diz respeito a resposta a erros, adaptação de escalabilidade e qualidade de imagem em baixos ou médios débitos. Como se vê na figura 2.23, com testes efectuados com aplicações de *streaming*, a norma MPEG-4 apresenta ganhos muito superiores às outras normas.

Codec	Decréscimo relativo do débito binário em relação a:		
	MPEG-4 ASP	H.263 HLP	MPEG-2 Vídeo Main
H.264/AVC Main	37.44 %	47.58 %	63.57 %
MPEG-4 ASP	—	16.65 %	42.95 %
H.263 HLP	—	—	30.61 %

Figura 2.17 - Ganhos médios em débito para aplicações de *streaming* [27].

São inúmeras as aplicações que podem beneficiar do MPEG-4 e em vários domínios de aplicação, desde baixos débitos e baixas qualidades até altos débitos e altas qualidades. Um dos casos relevantes de sucesso foi o programa DivX que permitia, por exemplo, converter

filmes em DVD (MPEG-2 Vídeo) para filmes em CD (MPEG-4 Simple), e que veio a trazer para a área do vídeo o problema da pirataria.

A norma H.264 é a mais recente norma, e utilizada neste trabalho, para a codificação de vídeo, que surgiu em 2003, desenvolvida em conjunto pelos grupos MPEG da ISO/IEC e “Video Coding Experts Group” (VCEG). É uma evolução da norma MPEG-4, nomeadamente da sua parte 10, intitulada “Advanced Video Coding” (AVC), que permite melhorar o desempenho do MPEG-4 principalmente nos casos em que é possível tirar proveito das capacidades das máquinas com boas características técnicas de *hardware*.

O objectivo para esta norma era necessitar de cerca de 50 por cento do débito binário das melhores soluções (MPEG-2 Vídeo, H.263 ou MPEG-4 Visual) para alcançar a mesma qualidade. A aplicação principal desta forma era a transmissão de vídeo em qualidade DVD com menos recursos. Além disso, pedia-se especial atenção ao desempenho para canais com erros, nomeadamente canais móveis e Internet. Enquanto o MPEG-4 tinha como objectivo cobrir os utilizadores com baixos débitos, a norma H.264 pretende ir mais longe e cobrir tanto os recursos mais baixos como os maiores.

Como acontecia para todos os outros casos, o H.264 não define explicitamente um codificador mas apenas o decodificador e o fluxo binário são especificados. A implementação é muito semelhante aos seus antecessores, ou seja, predição, compensação de movimento, quantificação, redução de redundância, entre outros. O H.264 pretende ser totalmente transparente em relação à rede de transporte para que tanto possa ser implementada em ambientes IP ou em qualquer tipo de redes privadas.

Relativamente ao MPEG-4, esta norma apresenta as seguintes vantagens [27]:

- Compensação de movimento com tamanhos variáveis de “MacroBlocks”: desde o típico 16 x 16 até o mínimo de 4 x 4;
- Menor complexidade na implementação do processo de precisão dos movimentos até $\frac{1}{4}$ de pixel;
- A DCT é aplicada a blocos 4 x 4 e não 8 x 8 para uma codificação mais precisa. No entanto, são concedidos graus de liberdade para que possa ir até 16 x 16 na croma-luminância ou 8 x 8 na luminância se tal for vantajoso;
- Transformada mais simples. Requer apenas processamento com aritmética de 16 bits, enquanto as outras necessitavam de 32 bits.

Concluindo, as grandes alterações na norma H.264 são ao nível da compressão, com um aumento da complexidade de codificação e decodificação. Os ganhos em termos de eficiência de compressão para a norma H.264 são objectivamente medidos através de ganhos de débito para um dado “Peak Signal to Noise Ratio” (PSNR), em relação a outra norma de codificação de vídeo. Esta norma foi adoptada por diversos organismos e instituições como é exemplo a “3rd Generation Partnership Project” (3GPP), a “Blu-Ray Disc Association” e a “Digital Video Broadcasting” (DVB). Esta norma afigura-se como a norma de codificação de vídeo que deverá dominar o panorama mundial no futuro próximo através do conjunto dos seus perfis que propõe soluções adequadas para um vasto leque de aplicações.

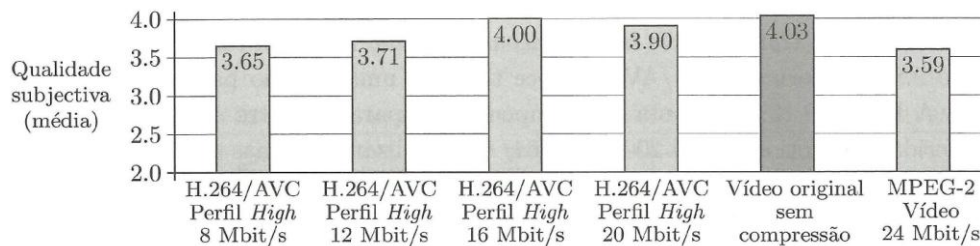


Figura 2.18 - Resultado dos testes subjectivos realizados pela Blu-Ray Association [27].

Na figura 2.18 consegue-se comparar a qualidade com o débito binário gasto pelas normas. Com um débito três vezes inferior, o H.264 no perfil High consegue ter melhor qualidade do que a norma MPEG-2. Esta comparação foi feita com o MPEG-2 uma vez que, é essa a norma utilizada nos DVDs.

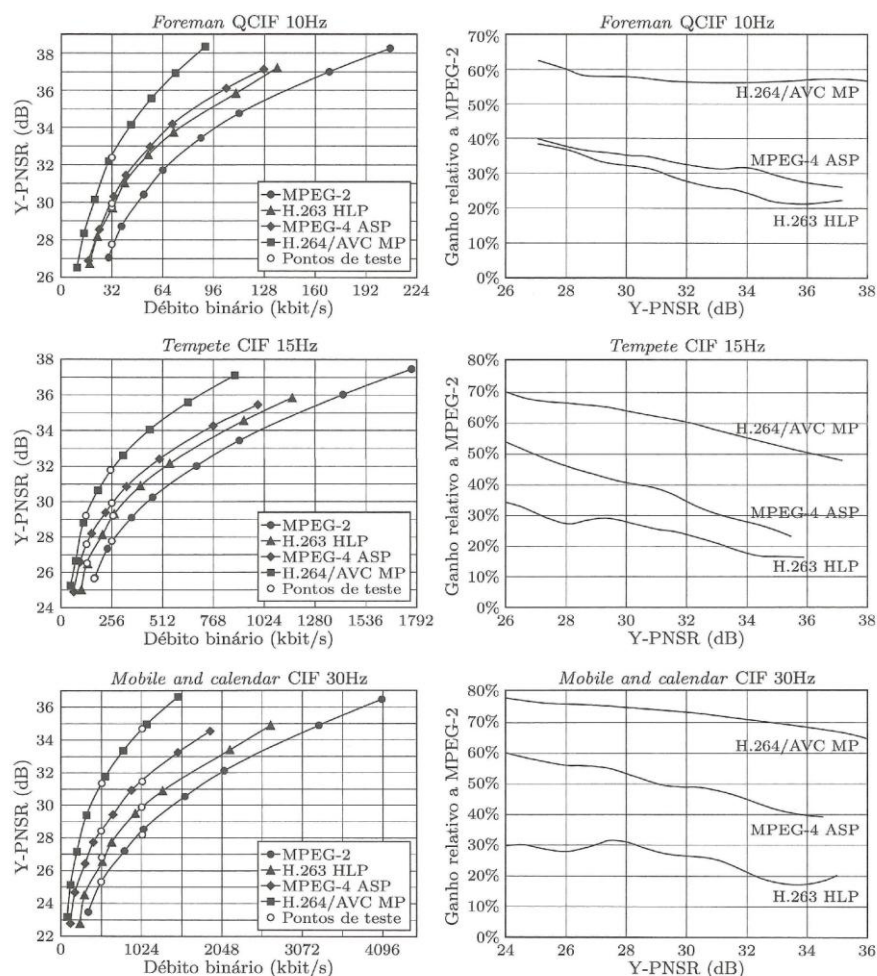


Figura 2.19 - Desempenho comparativo para sessões de *streaming* [27].

Nos gráficos da figura 2.19, consegue-se ver os desempenhos das várias normas através do PSNR. O PSNR compara o ruído introduzido na imagem depois da compressão em relação à imagem original. Todos os gráficos mostram que a norma H.264 obtém melhores resultados, ou seja, consegue atingir níveis de PSNR mais elevados com um débito mais baixo do que as outras tecnologias.

2.3.3 - Requisitos de vídeo

Para o *streaming* de vídeo, particularmente o *streaming* em “tempo-real”, existem requisitos que têm de ser cumpridos de modo a garantir que o vídeo seja transmitido sem falhas. Admitindo que a codificação é seleccionada à partida, os parâmetros a analisar estão englobados no que se chama QoS da rede. Existe um vasto conjunto de indicadores que podem ser importantes para o estudo de *streaming* em tempo real, entre os quais se salienta [27] [30]:

- débito binário: consoante as características de uma aplicação, um codificador pode produzir um fluxo de dados a ritmo constante ou a ritmo variável. Esse fluxo é geralmente caracterizado pelo ritmo médio e pela sua variação. O ritmo médio pode, por exemplo, ser controlado através do passo de quantificação usado no codificador. Existe uma relação estreita entre o ritmo a que o sinal é codificado e a sua qualidade; reduzir o ritmo pode ter consequências indesejadas ao nível da qualidade;
- degradação do sinal: numa comunicação audiovisual, um sinal que apresente grandes variações de qualidade ao longo da sua duração temporal não é, geralmente, bem aceite pelos utilizadores. É necessário ter em atenção que em muitos casos será devida à existência de erros de transmissão. É pois importante conhecer as características de erro dos meios de transmissão para conceber estratégias que tornem os sinais codificados adequadamente resistentes ao tipo de erros esperados no ambiente de operação visado;
- atraso: em *streaming* de vídeo, o atraso de codificação assume um papel relevante. No âmbito deste trabalho é mais importante garantir um atraso limitado e sem grandes variações do que uma qualidade mais elevada;
- *jitter*: tem de ser dada a garantia que a informação importante vai ser processada num intervalo de tempo definido, que é o caso do *streaming* em tempo real. O *jitter* pode ser entendido como a variação do tempo de atraso devido aos atrasos não constantes introduzidos por diferentes elementos existentes no sistema;
- perdas: correspondem à perda de pacotes. O objectivo do QoS é garantir limites para que estas perdas não influenciem negativamente o comportamento do *streaming* e a qualidade percebida.

Estes indicadores de QoS variam de rede para rede e dependem também das tecnologias utilizadas. Para que um serviço apresente um “bom comportamento”, deve existir um bom emparelhamento entre o que é requerido pela aplicação e as capacidades da rede. Neste sentido, salientam-se os dispositivos dos codificadores responsáveis pelo controlo de ritmo, que têm como objectivo adaptar a “produção” de bits à capacidade de escoamento disponibilizada pela rede de comunicação, bem como a necessidade de lidar com os erros introduzidos na transmissão.

2.3.4 - Mapeamento teórico dos requisitos de vídeo sobre as tecnologias anteriores

Para as normas H.263, MPEG-4 e H.264, utilizada neste trabalho, os débitos são sempre dependentes dos níveis e perfis utilizados. Para um bom funcionamento e para o *streaming* ser entregue em perfeitas condições depois de codificado pode-se assumir para todas as normas um atraso sempre menor a 200 ms e um *jitter* menor do que 50 ms. Segundo alguns

dados [30] a duração de um erro tem de ser menor ou igual a 16 ms para as normas MPEG-2, MPEG-4 e H.264. Se se pretender um *streaming* de alta qualidade apenas se pode dar um erro na entrega de pacotes a cada quatro horas. Ao invés, se apenas for necessário um serviço com qualidade normal (SDTV) essa perda de pacotes pode-se dar uma a cada hora. Se esses valores para o atraso, *jitter* e perda forem atingidos, o sistema comporta-se de segundo os parâmetros de QoS que permitem um *streaming* de vídeo com boa qualidade.

2.4 - Streaming

Streaming é uma tecnologia que permite a compressão de dados que permite distribuir informação através de uma rede de dados local (LAN) ou de longa distância (WAN) através de pacotes num fluxo contínuo. A forma mais comum de utilização é o envio de informação multimédia pela Internet. Num caso de *streaming* existe um servidor e pelo menos um cliente, ou seja, a informação pode ser difundida em unicast, multicast ou broadcast. Uma das vantagens do *streaming* é que o cliente não precisa de encher o disco com a informação que está a receber, pois esta é reproduzida automaticamente à medida que vai chegando, ou seja, não necessita de esperar por um *download* para ver o seu ficheiro multimédia. O cliente apenas precisa de largura de banda suficiente que suporte o serviço.

O aparecimento do *streaming* veio proporcionar um novo conjunto de serviços e funcionalidades. Hoje em dia é possível, utilizar o vídeo on-demand, assistir a vídeos nos telemóveis e computadores, e estando em qualquer parte do mundo, através da Internet, pode-se assistir aos programas de televisão favoritos ou ouvir rádio. O *streaming*, que não é uma tecnologia nova, era bastante usada no meio de entretenimento para a transmissão de rádio e TV. Os grandes portais de Internet exploraram a tecnologia para enriquecer o seu conteúdo jornalístico com áudio e vídeo. O *streaming* também está a popularizar-se na transmissão de congressos, palestras, seminários, debates, que são transmitidos ao vivo na Internet, aumentando a produtividade dos profissionais e reduzindo custos operacionais das empresas [33]. Uma pesquisa recente da Instat/MDR aponta que o mercado de *streaming* movimentou 2 bilhões de dólares em 2006 [33].

O *streaming* apenas é possível devido a plataformas que comunicam entre si em diversos níveis. De um lado temos o servidor que distribui os conteúdos através de um protocolo estabelecido. Do outro há os clientes, que com a sua aplicação vêm os conteúdos transmitidos pelo servidor. Os protocolos mais comuns para o *streaming* são o UDP, RTP, RTSP e HTTP. Como neste caso se pretende que o *streaming* seja feito em “tempo real” escolhemos o protocolo RTP, que utiliza UDP como protocolo de transporte, e que como tal tem a mesma desvantagem no que respeita à perda de pacotes. Isto já não acontece no HTTP, porque se detectar a perda de algum pacote, tenta enviar repetidamente aquele pacote até ser recebido com sucesso, pois faz parte da camada aplicação da pilha TCP/IP.

2.4.1 - Protocolos

Nesta parte do capítulo vamos abordar os protocolos utilizados neste trabalho. Além do RTP, que foi o protocolo utilizado para enviar os *streamings*, vamos analisar o protocolo UDP e TCP. Estes dois protocolos foram os gerados com um programa de geração de tráfego com o objectivo de compreender o comportamento dos pacotes RTP com a presença de pacotes TCP ou UDP na mesma rede.

Camada	Protocolo
Aplicação	HTTP, SMTP, FTP, SSH, RTP, Telnet, SIP, RDP, IRC, SNMP, NNTP, POP3, IMAP, BitTorrent, DNS, Ping, ...
Transporte	TCP, UDP, SCTP, DCCP, ...
Rede	IP (IPv4, IPv6), ARP, RARP, ICMP, IPSec, ...
Ligação de dados	Ethernet, 802.11, IEEE 802.1Q, HDLC, Token ring, FDDI, PPP, Switch, Frame Relay, ...
Física	Modem, RDIS, RS-232, EIA-422, RS-449, Bluetooth, USB, ...

Figura 2.20 - TCP, UDP e RTP na pilha TCP/IP.

O TCP [36] é um dos protocolos que suporta o núcleo da Internet devido à sua robustez e versatilidade. O TCP, tal como o UDP, pertence à camada de transporte da pilha TCP/IP, como se vê na figura 2.20, e sobre ele funcionam a maioria das aplicações da internet, tal como SSH, FTP e HTTP. O TCP é orientado à conexão, enviando um pedido para a estabelecer e depois utiliza esse canal seguro para enviar os dados, sendo esta ligação feita entre dois pontos. Uma das maiores vantagens do TCP é a fiabilidade, pois proporciona uma entrega fiável dos pacotes de dados, permitindo a recuperação de pacotes perdidos, a eliminação de pacotes duplicados, a recuperação de dados corrompidos e pode mesmo recuperar a ligação em casos de problemas na rede ou no sistema. A transferência de dados é possível nas duas direcções (cliente-servidor), funcionando em *full duplex*. Para garantir a segurança da transmissão de dados e de estabelecimento da conexão, o TCP utiliza o mecanismo de *handshake* que permite a autenticação e a finalização de uma sessão, garantindo no final desta a recepção de todos os pacotes correctamente. Para controlar o fluxo, o receptor à medida que recebe os dados envia mensagens ACK, confirmando a recepção de um segmento.

O protocolo TCP especifica três etapas durante uma ligação: estabelecimento da ligação, transferência de dados e fim da ligação. Numa ligação TCP existe de um lado um servidor, que abre um socket e espera por ligações, e do outro o cliente. O cliente TCP inicia a ligação enviando um pacote TCP com a flag SYN activa e espera a resposta do servidor, que no caso de aceitar a ligação envia um pacote SYN+ACK. Se durante um determinado espaço de tempo este pacote não for enviado ocorre um timeout e o pacote SYN é reenviado. O estabelecimento da ligação dá-se quando o cliente envia um pacote ACK, que confirma a recepção do pacote enviado pelo servidor. Durante estas trocas, cliente e servidor trocam números de sequência iniciais que vão mais tarde identificar o tráfego no fluxo. No final na fase de estabelecimento da ligação, o servidor inscreve, numa tabela própria que tem um limite de conexões, o cliente. No caso desta tabela estar cheia, todos os pacotes SYN enviados pelo cliente são ignorados pelo servidor. Na fase de transferência de dados, o TCP tem mecanismos que garantem a chegada dos dados tais como foram enviados, com números

de sequência, código detector de erros, confirmação de recepção e temporizadores que controlam o envio em caso de perdas ou atrasos. Na fase final da ligação, cada um se responsabiliza pelo seu fim da ligação. Quando um deles pretende terminar uma ligação envia um pacote com a flag FIN activa, ao qual deverá receber uma resposta ACK. Depois de receber este pacote vai receber outro com a flag FIN activa para o outro lado da ligação também ser terminada. Nem sempre são desligados os dois lados, formando-se uma ligação semi-aberta, em que o lado que não encerrou poderá continuar a enviar informação, mas o outro lado não.

Este protocolo é complexo e ao longo dos anos tem sofrido melhorias embora mantendo sempre as suas funções básicas intactas desde que este protocolo foi disponibilizado no RFC675. Nos últimos dez anos, a preocupação com o congestionamento do canal fez com que fossem propostos vários algoritmos. O primeiro a ser conhecido foi o TCP Tahoe, mas depois já surgiram o TCP Reno, TCP Vegas, FAST TCP, TCP New Reno e TCP Hybla.

Para o controlo do congestionamento no TCP cada fonte avalia a sua capacidade de geração de tráfego. No TCP em casos que o congestionamento da rede diminui aumenta a janela de congestão e se o congestionamento da rede aumentar essa janela vai diminuir. Com janelas maiores existem mais pacotes retransmitidos e descartados e com janelas menores o débito é também menor. As fontes sabem se a rede está congestionada através dos *timeouts*. O TCP funciona em “dente de serra”, porque a subida da janela é aditiva, pois aumenta linearmente, e a descida multiplicativa, pois em caso de perda de pacote divide-se a janela por 2 sendo o resultado o que se verifica na figura 2.21.

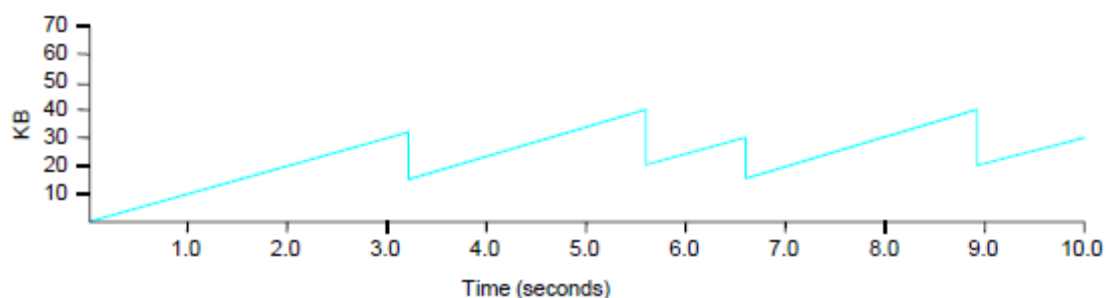


Figura 2.21 - Funcionamento dente de serra [49].

O TCP apresenta também algumas desvantagens, principalmente em redes *wireless* com elevados débitos, porque introduz *overhead* adicional tanto na estação base para cada pacote transmitido como na troca de bases (*hand-off*) feita por unidades móveis, e.g. portáteis.

O UDP permite que a aplicação encapsule os datagramas em pacotes IPv4 ou IPv6 que serão posteriormente enviados para o destino, não havendo garantias que o pacote chegue ao destino ou não. Este facto torna o protocolo UDP não confiável e utilizado para transmitir dados pouco sensíveis, como fluxos de áudio ou vídeo. Caso seja necessário existirem garantias de que o pacote foi entregue é necessário implementar estruturas de controlo, como timeouts, retransmissões ou *acknowledgments*. O UDP é um serviço sem conexão, pois não há necessidade de manter um relacionamento longo entre clientes e servidor. Assim, um cliente UDP pode criar um *socket* e enviar um datagrama para um servidor e logo de seguida com o mesmo *socket* enviar outro datagrama para um servidor diferente. Do mesmo modo, um servidor pode receber datagramas de diferentes clientes através do mesmo *socket*. Este protocolo utiliza portas de origem e destino de 16 bits.

A diferença básica entre o UDP e o TCP é o facto de o TCP ser um protocolo orientado à conexão, e portanto, inclui vários mecanismos para iniciar, manter e encerrar a comunicação, negociar tamanhos de pacotes, detectar e corrigir erros, evitar o congestionamento do fluxo e permitir a retransmissão de pacotes perdidos.

O protocolo RTP [34] é utilizado em aplicações de tempo real, como por exemplo, na entrega de áudio ou vídeo ponto-a-ponto ou em VoIP. O RTP define como deve ser feita a fragmentação do fluxo de dados, adicionando a cada fragmento informação do número de sequência e de tempo de entrega, ainda que a rede altere a ordem dos pacotes. O controlo é realizado por RTCP que é responsável pela monitorização da qualidade de serviço e pelo envio de informação sobre os participantes numa sessão. O método utilizado pelo RTCP baseia-se no envio periódico de pacotes de controlo a todos os participantes. O RTP/RTCP situam-se ao nível da aplicação e utilizam UDP como protocolo de transporte, servindo-se das suas capacidades de multiplexagem e *checksum*.

O RTP é executado extremo a extremo, transportando dados com características de tempo real. Este protocolo não inclui mecanismos que providenciem entrega fiável e com garantias de QoS ou que permitam reservas de recurso. Os dados fornecidos por este protocolo são o *timestamping*, para compensação do *jitter* em pacotes do mesmo *stream*, a numeração sequencial, para detecção de perdas e reordenação e a identificação do tipo de *payload* e da fonte.

O RTCP fornece informações adicionais aos participantes da sessão, como por exemplo, *feedback* sobre a qualidade de serviço em que cada receptor informa sobre o *jitter*, pacotes perdidos e atraso do emissor. O RTCP faz a sincronização entre meios (pacotes de áudio e vídeo transportados em diferentes *streams*), a identificação dos participantes da sessão e o controlo dessa mesma sessão.

Capítulo 3

Tecnologias

Neste capítulo vão ser descritos os equipamentos e tecnologias utilizadas para o desenvolvimento deste projecto. O capítulo está dividido em duas subsecções: *hardware* e *software* e configurações.

3.1 - Hardware utilizado

Para conseguir suportar três *streamings* simultâneos e um gerador de tráfego adicional, sem que o CPU atingisse 100% da sua capacidade, foram necessários três computadores. As características dos três computadores estão descritas nas tabela abaixo.

Tabela 3.1 - Características do Computador 1.

Computador 1	
Modelo	HP Compaq dc7700p small form factor
Processador	Intel(R) Core(TM)2 CPU 6400@2,13 GHz
Memória RAM	2,0 GB
Sistema operativo	Windows 7
Tipo de sistema	32 bits

Tabela 3.2 - Características do Computador 2.

Computador 2	
Modelo	Apple MacBook
Processador	Intel(R) Core(TM)2 Duo CPU T8300@2,4 GHz
Memória RAM	2,0 GB
Sistema operativo	Windows 7
Tipo de sistema	32 bits

Tabela 3.3 - Características do Computador 3.

Computador 3	
Modelo	Toshiba Satellite L40 - 18 L
Processador	Intel(R) Pentium(R) Dual CPU T2330@1,6 GHz
Memória RAM	2,0 GB
Sistema operativo	Windows 7
Tipo de sistema	32 bits

Para além destes três computadores foram utilizados dois *routers wireless* e dois dispositivos *HomePlug*, que permitiu a realização dos diferentes cenários. Todos os dispositivos são da marca Linksys. Devido a ter sido testada a norma a, g e n do 802.11 foi necessário recorrer a adaptadores USB *wireless*. Esta necessidade deveu-se a que nenhum computador suportava a norma 802.11a e nem todos a norma 802.11n. Tanto os *routers wireless* como os adaptadores *wireless* por USB tinham a capacidade de funcionar em duas bandas ao mesmo tempo. Para atingir esse objectivo, o router, criava duas redes. Por exemplo, no caso testado foram criadas a rede “linksys1”, que consegue trabalhar nas normas b, g e n, e a rede “linksys_media1” que trabalha apenas nas normas a e n. Na tabela 3.4 estão descritos os modelos utilizados neste trabalho.

Tabela 3.4 - Modelos *Wireless* e *HomePlug* escolhidos.

Modelo	
Router <i>Wireless</i>	WRT610N
Dispositivos <i>HomePlug</i>	PLK300
Adaptadores USB <i>Wireless</i>	WUSB600N

Tabela 3.5 - Especificação do router WRT610N

WRT610N	Especificações do produto
Normas	802.11a, b, g e n; 802.3; 802.3u; 802.3ab
Portas	Power, Ethernet, USB e Internet
Antenas	3 antenas internas que funcionam a 2.4 GHz e 5 GHz

Tabela 3.6 - Especificação dos dispositivos HomePlug PLK300

PLK300	Especificações do produto
Normas	HomePlug AV, 802.3, 802.3u
Portas	Power, Ethernet

Tabela 3.7 - Especificações do adaptador USB WUSB600N

WUSB600N	Especificações do produto
Normas	802.11a, b, g e n
Antenas	2 antenas internas que funcionam a 2.4 GHz e 5 GHz

Para mais informações sobre cada um dos modelos basta consultar a página do fabricante [37].

3.2 - Software e configurações

Depois de ter sido descrito o hardware utilizado, esta subsecção aborda os programas e respectivas configurações necessárias à realização dos testes.

3.2.1 - Servidor de *streaming*

De forma a realizar o *streaming* e realizar os testes comparativos necessários aos objectivos do trabalho, foi necessário recorrer a programas próprios. O programa escolhido para reproduzir o *streaming* de vídeo foi o “VideoLAN Client” (VLC) [38]. Esta foi uma escolha feita depois de uma comparação com o Quicktime *Streaming* Server. Embora a interface com o utilizador do Quicktime seja mais amigável para o utilizador do que a do VLC, esse não é um aspecto muito relevante na decisão. O VLC é um programa em *opensource* e um dos mais versáteis leitores de vídeo que se pode encontrar. É compatível com os formatos mais populares de vídeos, com integração fácil de legendas e a possibilidade de criar playlists. A principal razão que levou a escolher o VLC é a sua capacidade de trabalhar com quase todos os codecs existentes. No que está relacionado com a parte de *streaming*, o VLC permite efectuar transcodificações, escolher a taxa de bits, a taxa de *frames* e a resolução a que se deseja o vídeo. O VLC suporta vários protocolos de *streaming*, como o UDP e RTP, podendo ser utilizado como servidor de vídeo numa rede de alta velocidade, possuindo suporte a

transmissão em unicast e multicast. Além disso, o VLC opera nas redes IPv4 e IPv6. Em todos os cenários, de um lado está o VLC Servidor e do outro o VLC Cliente. As imagens em baixo mostram todos os passos necessários para a reprodução se um *streaming* do lado do servidor.

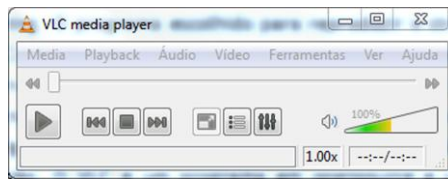


Figura 3.1 - Janela principal VLC.

A figura 3.1 mostra o painel principal do VLC. Para realizar o *streaming* selecciona-se o menu “Media” e de seguida a opção “Emissão...”. Ao carregar-se nesta opção vai surgir a seguinte janela:

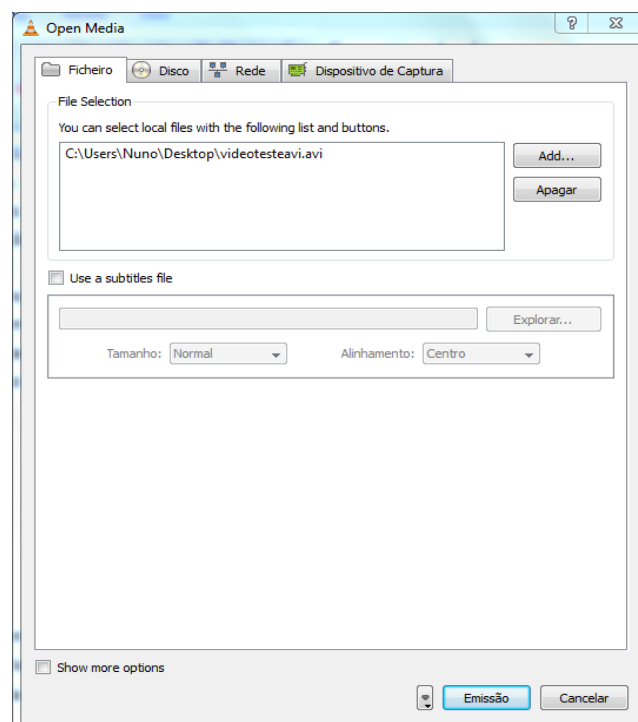


Figura 3.2 - Janela “Emissão” do VLC.

Nesta janela aparece o campo para colocar o vídeo que se irá fazer *streaming*. Depois de adicionado o vídeo carrega-se no botão “Emissão”. De seguida aparece uma janela que volta a confirmar o vídeo e que basta carregar no botão “Seguinte”. Depois deste processo surge a janela principal do *streaming* que se pode ver em baixo.

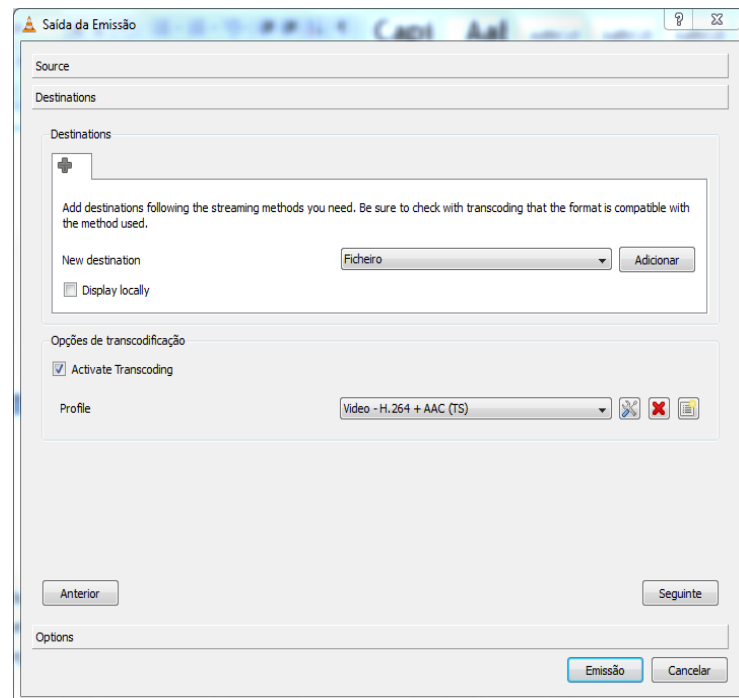


Figura 3.3 - Janela com opções de *streaming* do VLC.

Na janela anterior existem duas coisas a fazer. A primeira é escolher o protocolo para fazer o *streaming*. Nos cenários de teste o protocolo escolhido foi o RTP, porque é o protocolo utilizado para *streaming* em “tempo-real” e principalmente porque o Wireshark permite saber as grandezas a medir através de um fluxo RTP. A segunda coisa é escolher a transcodificação que se quer fazer ao vídeo. Para escolher manualmente todas as definições basta carregar no botão com as ferramentas, que é o botão que está marcado com um círculo na figura 3.4.

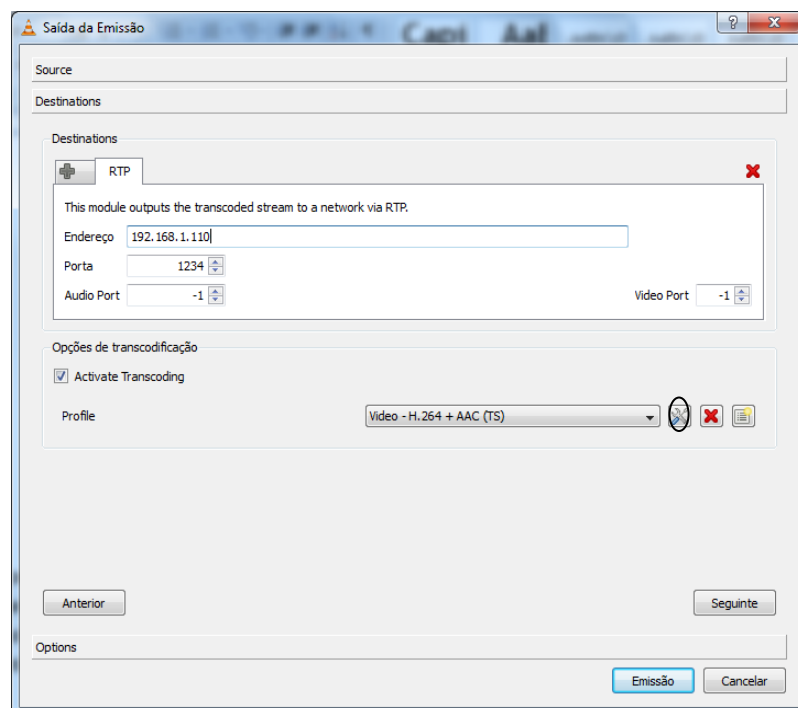


Figura 3.4 - Janela com opções de *streaming* do VLC com protocolo escolhido.

A figura em cima mostra que depois de seleccionado o protocolo é necessário introduzir o endereço IP e a porta. Este endereço IP é o do computador que vai receber o *streaming*.

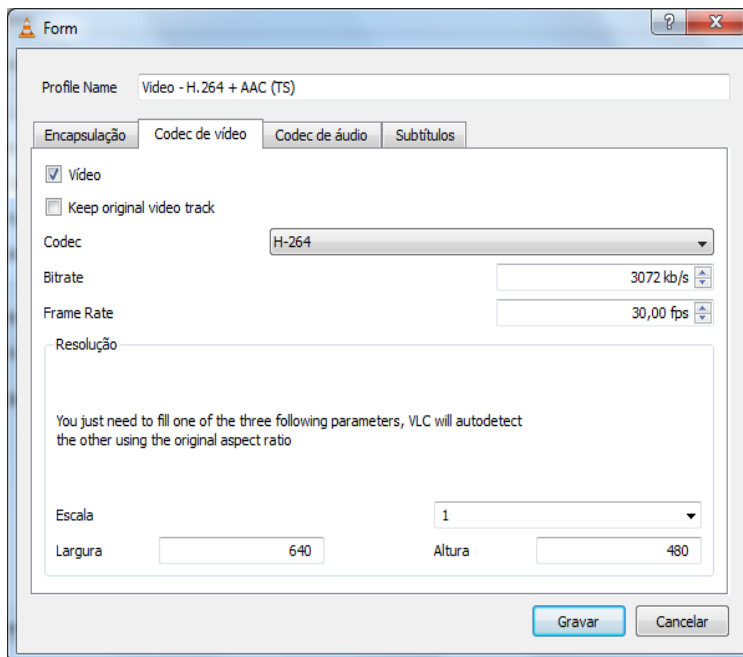


Figura 3.5 - Janela de transcodificação do VLC.

A figura 3.5 é a janela principal da transcodificação e é exemplificativa relativamente às definições utilizadas no trabalho. Nesta janela existe a opção de escolher o codec, o *bitrate*, o *frame rate* e a resolução do vídeo. Para os testes realizados, o *bitrate* é 3072 Kbit/s, o *frame rate* é de 30 frames por segundo, com um tamanho de 640x480. O codec utilizado é o H.264.

Depois de definidos os parâmetros mencionados, basta carregar no botão “Gravar” e voltando à interface anterior (figura 3.4) basta carregar no botão “Emissão” para que o *streaming* se inicie.

Para um cliente visualizar o *streaming* os passos necessários são ainda mais fáceis. Basta na janela principal do programa seleccionar o menu “Media” e de seguida a opção “Abrir Emissão de Rede...”. Ao seleccionar esta opção abre-se a seguinte janela:

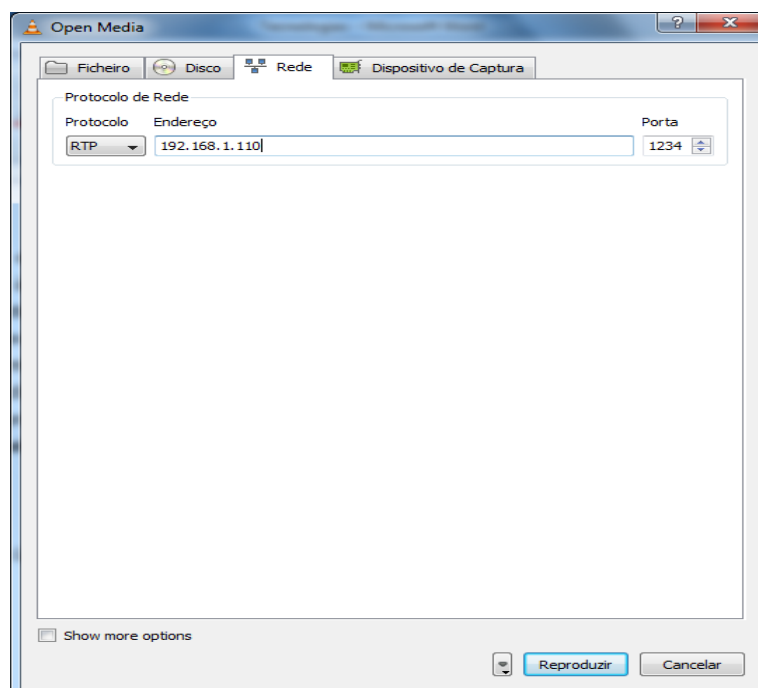


Figura 3.6 - Janela “Abrir Emissão de Rede” do VLC.

Nesta janela tem de se seleccionar o mesmo protocolo, IP e porta anteriormente escolhidos no servidor. Depois de todas estas tarefas realizadas basta carregar no botão “Reproduzir” e o *streaming* iniciar-se-á.

3.2.2 - Medição de parâmetros de rede

Outro programa fundamental para a realização desta dissertação foi o Wireshark [39], que permitiu fazer a medição dos parâmetros da rede. O Wireshark, que veio substituir o Ethereal, é um programa que analisa o tráfego de uma rede e o organiza por protocolos. Esta aplicação permite capturar todo o tráfego que entra e sai do computador, em diferentes protocolos. No contexto do trabalho, esta aplicação vai ser importante porque permite analisar o tráfego da rede e calcular o débito, o *skew*, o *jitter*, o delta e as perdas de pacotes (estas variáveis estarão explicadas no capítulo 4 na secção 4.1).

O outro programa existente capaz de medir os parâmetros de uma rede é o TCPDump. A principal vantagem do Wireshark é o facto de ter uma interface com o utilizador que o torna mais fácil de utilizar. Outro factor que levou a escolher este programa é o facto de o autor ter experiência de trabalho com esta aplicação.

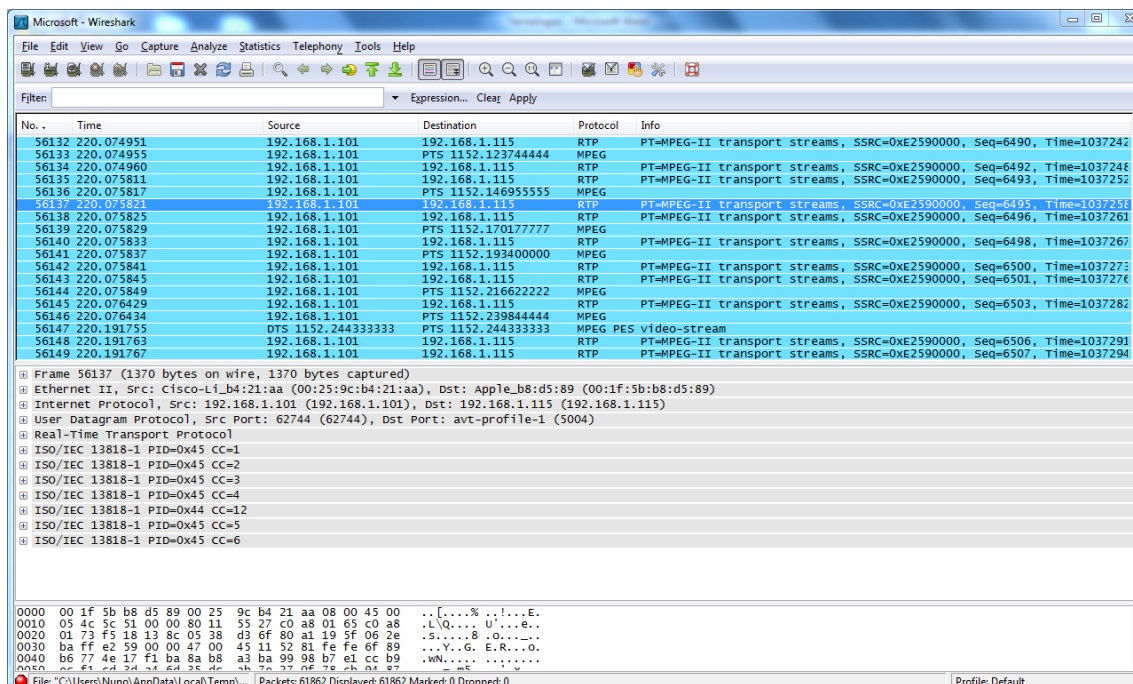


Figura 3.7 - Janela Wireshark.

A figura 3.7 mostra a janela do wireshark após a transmissão de um *streaming* em RTP. Para obter este fluxo basta seleccionar o menu “Capture” e depois seleccionar a interface correcta. Na figura é possível ver os IPs dos dois computadores que trocam fluxos de dados, o protocolo escolhido, o tamanho dos pacotes e a porta utilizada, que neste caso foi a 5004. Depois de capturado o tráfego pretendido, o Wireshark é capaz de dar as informações que se precisa para analisar um fluxo RTP. Para tal, basta seleccionar o menu “Telephony”, escolhendo a opção “RTP” e de seguida “Stream Analysis...”. Nesse momento o Wireshark analisa os pacotes e mostra uma tabela como a que se mostra em baixo.

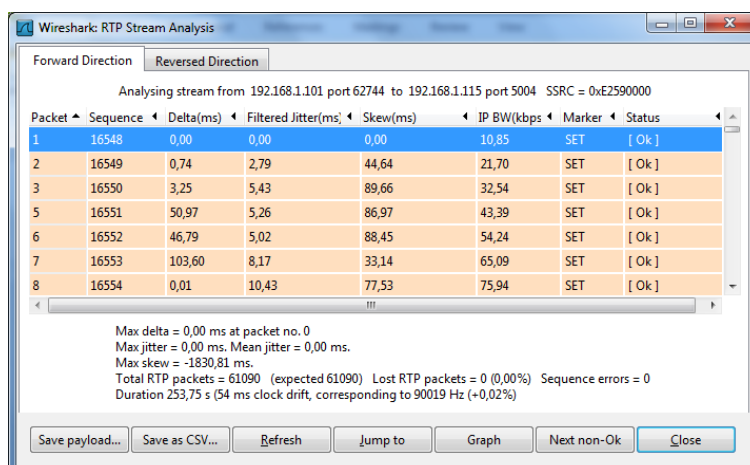


Figura 3.8 - Janela “Stream Analysis...” do Wreshark.

A tabela, na figura 3.8, permite visualizar de forma resumida a informação sobre os pacotes RTP trocados durante o *streaming*. Para se proceder a análises posteriores deste tipo de informação, existe ainda a possibilidade de guardar esta tabela como CVS, o que permite, por exemplo, que seja aberta em folhas cálculo Microsoft Office Excel ou Open Office.

3.2.3 - Gerador de tráfego adicional

Para gerador de tráfego adicional foi escolhido um programa *opensource*, o Network Traffic Generator [40] para os primeiros cinco cenários e para gerar tráfego TCP nos cenários 6 e 7. Como o nome da aplicação indica é um gerador de tráfego de rede. Existem outras aplicações para este objectivo, mas esta foi a escolhida porque gera tráfego UDP e TCP e tem uma interface gráfica que torna mais fácil o seu manuseamento. Esta aplicação tem dois executáveis: um para o cliente e outro para o servidor. O executável do servidor apenas pode correr num computador, mas o do cliente pode correr no número de terminais que se desejar. A aplicação servidor, onde se escolhe o tipo de tráfego a simular e a porta por onde será recebido, corre no computador que está a fazer o *streaming* e a aplicação cliente nos computadores que estão a receber o vídeo. Na aplicação cliente existem três domínios de escolha: o *payload*, o cliente e o protocolo. No *payload* existe a opção de escolher o débito mínimo e máximo, a duração e o incremento. Uma opção que apenas existe no payload é escolher se desejamos tráfego aleatório, fixo ou crescente. No caso de se escolher tráfego fixo apenas se pode alterar o campo do débito máximo. Na aplicação cliente permite escolher o número de clientes que se deseja para a simulação. Para o protocolo define-se o protocolo de tráfego a gerar e a porta, que são os mesmos da aplicação servidor. Nos testes foi gerado tanto tráfego UDP e TCP e foram escolhidas as portas 1234, 2500 e 5004 para receber o tráfego. Existe também um campo para colocar o IP do computador onde está a correr a aplicação servidor. A figura 3.9 mostra as interfaces do servidor e do cliente.

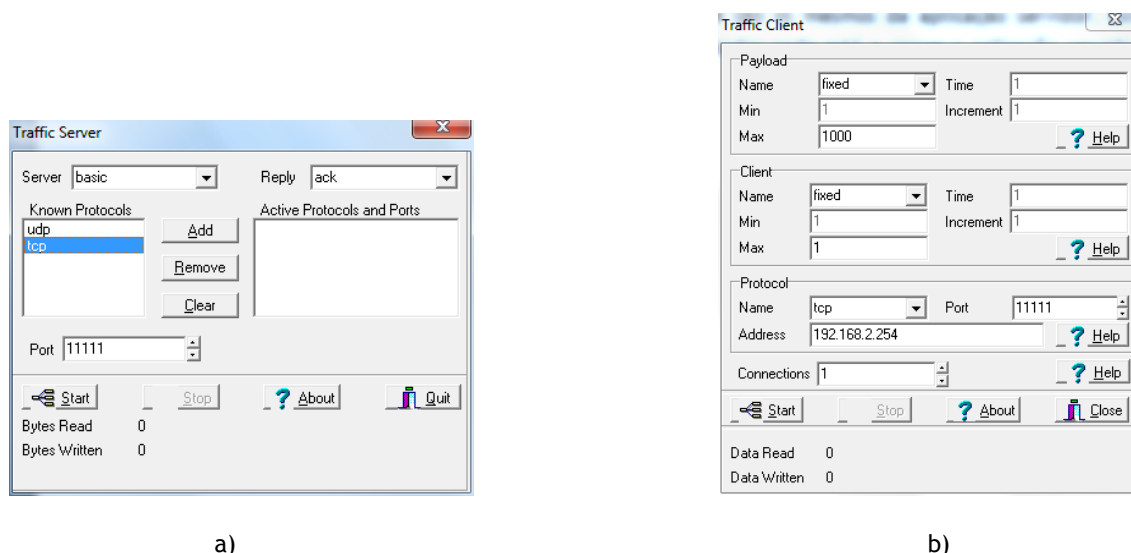


Figura 3.9 - Janela do Network Traffic Generator.

a) Janela do Traffic Server.

b) Janela do traffic Client.

No. -	Time	Source	Destination	Protocol	Info
15770	16.880770	192.168.1.102	192.168.1.100	TCP	vce > 50078 [ACK] Seq=7089 Ack=13739386 win=17408 Len=0
15771	16.880871	192.168.1.100	192.168.1.102	TCP	50078 > vce [ACK] Seq=13752526 Ack=7089 win=16288 Len=1460
15772	16.880891	192.168.1.100	192.168.1.102	TCP	50078 > vce [ACK] Seq=13753986 Ack=7089 win=16288 Len=1460
15773	16.881609	192.168.1.102	192.168.1.100	TCP	vce > 50078 [ACK] Seq=7089 Ack=13742306 win=17408 Len=0
15774	16.881659	192.168.1.100	192.168.1.102	TCP	50078 > vce [ACK] Seq=13755446 Ack=7089 win=16288 Len=199
15775	16.881673	192.168.1.100	192.168.1.102	TCP	vce > 50078 [ACK] Seq=7089 Ack=13756906 win=16288 Len=0
15776	16.881767	192.168.1.102	192.168.1.100	TCP	vce > 50078 [ACK] Seq=7089 Ack=13745226 win=17408 Len=0
15777	16.881866	192.168.1.102	192.168.1.100	TCP	vce > 50078 [ACK] Seq=7089 Ack=13748146 win=17408 Len=0
15778	16.884131	192.168.1.102	192.168.1.100	TCP	vce > 50078 [ACK] Seq=7089 Ack=13751066 win=17408 Len=0
15779	16.885757	192.168.1.102	192.168.1.100	TCP	vce > 50078 [ACK] Seq=7089 Ack=13753986 win=17408 Len=0
15780	16.889101	192.168.1.102	192.168.1.100	TCP	vce > 50078 [ACK] Seq=7089 Ack=13756906 win=17408 Len=0
15781	16.889174	192.168.1.102	192.168.1.100	TCP	vce > 50078 [PSH, ACK] Seq=7089 Ack=13757105 win=17152 Len=8
15782	16.889410	192.168.1.100	192.168.1.102	TCP	50078 > vce [ACK] Seq=13757105 Ack=7097 win=16280 Len=1460
15783	16.889432	192.168.1.100	192.168.1.102	TCP	50078 > vce [ACK] Seq=13758565 Ack=7097 win=16280 Len=1460
15784	16.889448	192.168.1.100	192.168.1.102	TCP	50078 > vce [ACK] Seq=13760025 Ack=7097 win=16280 Len=1460
15785	16.889466	192.168.1.100	192.168.1.102	TCP	50078 > vce [ACK] Seq=13761485 Ack=7097 win=16280 Len=1460
15786	16.889479	192.168.1.100	192.168.1.102	TCP	50078 > vce [ACK] Seq=13762945 Ack=7097 win=16280 Len=1460
15787	16.889490	192.168.1.100	192.168.1.102	TCP	50078 > vce [PSH, ACK] Seq=13764405 Ack=7097 win=16280 Len=671
15788	16.898075	192.168.1.102	192.168.1.100	TCP	vce > 50078 [ACK] Seq=7097 Ack=13760025 win=17408 Len=0
15789	16.898813	192.168.1.102	192.168.1.100	TCP	vce > 50078 [ACK] Seq=7097 Ack=13762945 win=17408 Len=0
15790	16.899390	192.168.1.102	192.168.1.100	TCP	vce > 50078 [ACK] Seq=7097 Ack=13765076 win=17408 Len=0
15791	16.899855	192.168.1.102	192.168.1.100	TCP	vce > 50078 [PSH, ACK] Seq=7097 Ack=13765076 win=17408 Len=8
15792	16.900051	192.168.1.100	192.168.1.102	TCP	50078 > vce [ACK] Seq=13765076 Ack=7105 win=16272 Len=1460
15793	16.900074	192.168.1.100	192.168.1.102	TCP	50078 > vce [ACK] Seq=13766536 Ack=7105 win=16272 Len=1460
15794	16.900087	192.168.1.100	192.168.1.102	TCP	50078 > vce [ACK] Seq=13767996 Ack=7105 win=16272 Len=1460
15795	16.900116	192.168.1.100	192.168.1.102	TCP	50078 > vce [ACK] Seq=13769456 Ack=7105 win=16272 Len=1460
15796	16.900127	192.168.1.100	192.168.1.102	TCP	50078 > vce [ACK] Seq=13770916 Ack=7105 win=16272 Len=1460

[Frame 15774 (1514 bytes on wire, 1514 bytes captured)]
 [Ethernet II, Src: Apple_b8:d5:89 (00:1f:5b:b8:d5:89), Dst: Lite-onT_aa:e6:4c (00:16:44:aa:e6:4c)]
 [Internet Protocol, Src: 192.168.1.100 (192.168.1.100), Dst: 192.168.1.102 (192.168.1.102)]
 [Transmission Control Protocol, Src Port: 50078 (50078), Dst Port: vce (11111), Seq: 13755446, Ack: 7089, Len: 1460]
 [Data (1460 bytes)]

Figura 3.10 - Extracto Wireshark com tráfego TCP.

No. -	Time	Source	Destination	Protocol	Info
7893	6.945047	192.168.1.102	192.168.1.100	UDP	Source port: vce Destination port: 60765
7896	6.945253	192.168.1.100	192.168.1.102	UDP	Source port: 60765 Destination port: vce
7897	6.947022	192.168.1.102	192.168.1.100	UDP	Source port: vce Destination port: 60765
7898	6.947228	192.168.1.100	192.168.1.102	UDP	Source port: 60765 Destination port: vce
7899	6.948836	192.168.1.102	192.168.1.100	UDP	Source port: vce Destination port: 60765
7900	6.949330	192.168.1.100	192.168.1.102	UDP	Source port: 60765 Destination port: vce
7901	6.951127	192.168.1.102	192.168.1.100	UDP	Source port: vce Destination port: 60765
7902	6.951332	192.168.1.100	192.168.1.102	UDP	Source port: 60765 Destination port: vce
7903	6.953309	192.168.1.102	192.168.1.100	UDP	Source port: vce Destination port: 60765
7904	6.953516	192.168.1.100	192.168.1.102	UDP	Source port: 60765 Destination port: vce
7905	6.956073	192.168.1.102	192.168.1.100	UDP	Source port: vce Destination port: 60765
7906	6.956228	192.168.1.100	192.168.1.102	UDP	Source port: 60765 Destination port: vce
7907	6.957879	192.168.1.102	192.168.1.100	UDP	Source port: vce Destination port: 60765
7908	6.958096	192.168.1.100	192.168.1.102	UDP	Source port: 60765 Destination port: vce
7909	6.959649	192.168.1.102	192.168.1.100	UDP	Source port: vce Destination port: 60765
7910	6.959821	192.168.1.100	192.168.1.102	UDP	Source port: 60765 Destination port: vce
7911	6.961621	192.168.1.102	192.168.1.100	UDP	Source port: vce Destination port: 60765
7912	6.961828	192.168.1.100	192.168.1.102	UDP	Source port: 60765 Destination port: vce
7913	6.963461	192.168.1.102	192.168.1.100	UDP	Source port: vce Destination port: 60765
7914	6.963668	192.168.1.100	192.168.1.102	UDP	Source port: 60765 Destination port: vce
7915	6.965380	192.168.1.102	192.168.1.100	UDP	Source port: vce Destination port: 60765
7916	6.965586	192.168.1.100	192.168.1.102	UDP	Source port: 60765 Destination port: vce
7917	6.968079	192.168.1.102	192.168.1.100	UDP	Source port: vce Destination port: 60765
7918	6.968240	192.168.1.100	192.168.1.102	UDP	Source port: 60765 Destination port: vce
7919	6.970507	192.168.1.102	192.168.1.100	UDP	Source port: vce Destination port: 60765
7920	6.970643	192.168.1.100	192.168.1.102	UDP	Source port: 60765 Destination port: vce
7921	6.972141	192.168.1.102	192.168.1.100	UDP	Source port: vce Destination port: 60765

[Frame 7902 (503 bytes on wire, 503 bytes captured)]
 [Ethernet II, Src: Apple_b8:d5:89 (00:1f:5b:b8:d5:89), Dst: Lite-onT_aa:e6:4c (00:16:44:aa:e6:4c)]
 [Internet Protocol, Src: 192.168.1.100 (192.168.1.100), Dst: 192.168.1.102 (192.168.1.102)]
 [User Datagram Protocol, Src Port: 60765 (60765), Dst Port: vce (11111)]
 [Data (461 bytes)]

Figura 3.11 - Extracto Wireshark com tráfego UDP.

As figuras 3.10 e 3.11 mostram exemplos de geração de tráfego. Na primeira é possível ver que o tráfego gerado é TCP e na segunda é UDP. Era este o tráfego que era introduzido juntamente com os *streams* de vídeo.

Para os últimos dois cenários foi escolhida uma outra aplicação para gerar tráfego UDP chamada “Multi Generator” (MGEN) [50]. O Multi-Generator (MGEN) Network Test Tool [1] permite a realização de testes e medições de desempenho em redes IP recorrendo à injeção de tráfego UDP. Através da criação de scripts, em formato .mgn, permite recriar padrões de tráfego na rede a fim de testar as redes com cargas variadas.

O tráfego gerado pode ser visualizado em tempo real ou armazenado em ficheiro. Esta aplicação foi essencial para a realização do cenário 6 e 7, onde é necessário saturar o canal com tráfego UDP. Com o gerador anterior não foi possível gerar débitos elevados de tráfego UDP sem ele encravar depois de alguns segundos de funcionamento. A grande vantagem deste gerador UDP é o facto de não gastar muita capacidade de processamento em relação ao Network Traffic Generator.

O script utilizado para saturar o canal no cenário 6 foi o seguinte:

- 0.0 ON 1 UDP SRC 5005 DST 192.168.0.11/5555 PERIODIC [350 6144]

Este script significa que vai começar a gerar tráfego UDP constante desde o momento em que se abre a aplicação. O tráfego sai da porta 5005 que corre o executável do programa e tem como destino a porta 5555 da máquina com o endereço IP acima indicado com uma regularidade de 350 mensagens por segundo com 6144 bytes. Para qualquer simulação é possível alterar o momento em que o tráfego se inicia e a largura de banda que se quer ocupar com tráfego UDP. Para correr esta aplicação, que funciona em *Windows*, basta abrir a linha de comandos, aceder à pasta onde está instalada a aplicação e escrever na consola o seguinte comando: `mgen input nomedascript.mgn`. Este gerador tem a vantagem de ser muito menos pesado para o CPU do que o Network Traffic Generator, porém é apenas capaz de gerar tráfego UDP.

3.2.4 - Configuração de QoS

No caso da tecnologia *wireless* a gestão do QoS [41] vai ser feita pelo router. Se se aceder à página de configuração do router, no caso `http://192.168.1.1`, na zona de Applications and Gaming, é possível escolher trabalhar com ou sem QoS. Se se escolher a opção de trabalhar com QoS existem quatro categorias disponíveis: aplicações, jogos on-line, endereço MAC ou porta Ethernet e dispositivos de voz. Para todas as categorias podemos escolher o tipo de prioridade: alta, média, normal ou baixa, sendo portanto um QoS relativo. Estas prioridades é que vão seleccionar a quantidade de largura de banda disponível para cada categoria. Este QoS é atribuído para *wireless* e/ou Ethernet, dependendo da forma como o router está ligado ao computador.

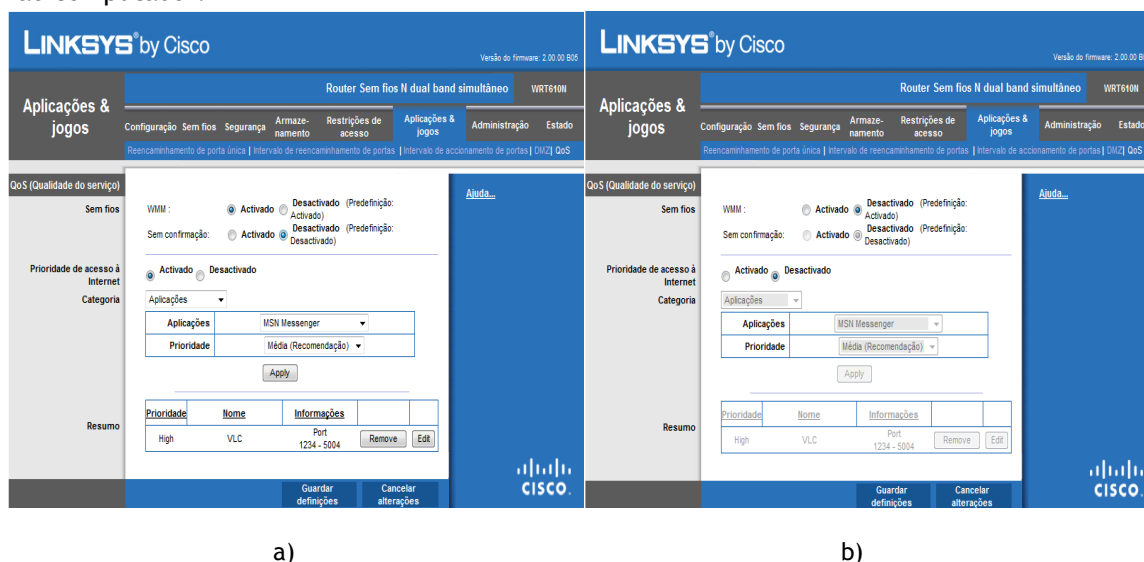


Figura 3.12 - Janelas configuração QoS.

a) Definições com QoS.

b) Definições sem QoS.

A figura 3.12a) mostra a opção em que se seleccionou QoS e a figura 3.12b) a que se optou por trabalhar sem QoS. Na figura da esquerda foi seleccionada a opção de dar

prioridade à aplicação VLC com tráfego UDP das portas 1234 a 5004, pois as portas que se escolheu para o *streaming* estavam neste intervalo.

No que respeita ao HomePlug, o QoS já vem definido de origem [42] e até ao momento ainda não há nenhuma aplicação para o dispositivo PLK300, existindo uma para o seu antecessor [43] mas que não é compatível. Portanto as definições de QoS nunca foram alteradas no HomePlug, permanecendo sempre as de origem que segundo o manual têm a capacidade de acesso livre contenção, acesso de contenção baseado em prioridades de quatro níveis e intermitência de vários segmentos.

Para não existirem interferências com as redes já existentes no local onde se testaram os vários cenários foi escolhido um canal para os routers trabalharem diferente do das redes existentes. Todas as redes trabalhavam no canal 6, por isso foi escolhido para um router o canal 1 e para outro o canal 11.

Capítulo 4

Cenários de teste

Este capítulo descreve os cenários de teste que foram definidos para mesma avaliação das várias tecnologias. Todos os cenários, sete no seu todo, têm uma estrutura semelhante à apresentada nos blocos da figura 4.1. De um lado existe uma câmara ligada a um computador que comunica com outro computador utilizando a tecnologia HomePlug, *Wireless* ou uma solução híbrida em que são combinadas estas duas tecnologias. O cenário 1 apresenta apenas HomePlug, o cenário 2 apresenta somente a tecnologia *Wireless* e os cenários 3, 4 e 5 apresentam soluções híbridas. O cenário 6 utiliza apenas HomePlug e o 7 HomePlug e Wi-Fi, tendo sido considerados para perceber o funcionamento com QoS, em situações de sobrecarga da rede. Todos os cenários foram testados com 1 e 3 clientes, onde se tem um ou três servidores e um ou três clientes. Quer isto dizer que do lado do servidor se tem dois computadores e no lado do cliente um computador. No lado do servidor um dos computadores terá no máximo duas aplicações VLC a correr o servidor de *streaming* e o outro computador terá a aplicação de geração de tráfego e se necessário o terceiro servidor. Do lado do cliente apenas se tem um computador que receberá o(s) *stream(s)* e o tráfego gerado.

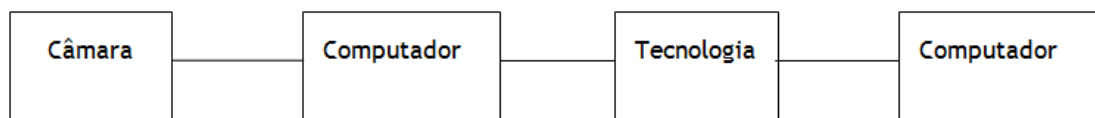


Figura 4.1 - Diagrama genérico dos cenários de teste.

Em todos os cenários foi utilizado o mesmo *stream* de vídeo, cujas características são apresentadas na tabela 4.1 em baixo.

Tabela 4.1 - Características do vídeo utilizado.

Características do vídeo	
Encapsulação	MPEG-TS
Codec	H.264
Tamanho	VGA(640x480)
Bitrate	3072 Kbit/s
Frame rate	30 rames/s

Estas características do vídeo foram definidas depois de uma análise sobre as câmaras que actualmente se utilizam na área da vigilância. A Axis recentemente montou nos autocarros de Madrid, com o objectivo de melhorar a segurança, várias das suas novas câmaras que possuem estas mesmas características [53]. O codec H.264 é o que, hoje em dia, as novas câmaras trazem e que tem o melhor desempenho. Qualquer dos valores presentes nas tabelas é configurável.

4.1 - Cenário 1

Este cenário serve de base ao teste do sistema utilizando unicamente a tecnologia HomePlug de forma a analisar o seu comportamento perante os *streams* de vídeo.

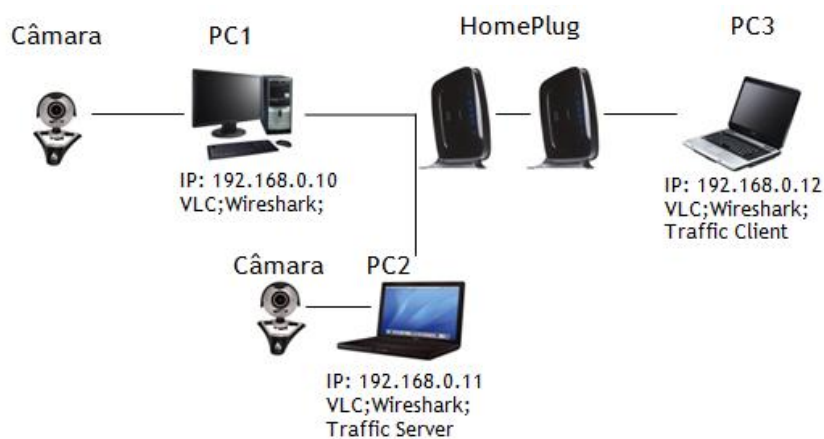


Figura 4.2 - Representação do Cenário 1.

Na figura 4.2 em cima é apresentado o esquema do cenário e todos os programas que corriam em cada PC. Este é um cenário em que apenas se utiliza a tecnologia HomePlug. Para estes testes foram usados três computadores. Dois deles estão ligados a um dispositivo de HomePlug e o PC3 está ligado ao outro dispositivo HomePlug. A função do PC1 é apenas de enviar um *stream* de vídeo para o PC3. O PC2 além de enviar um *stream* no caso de existirem 3 utilizadores é responsável pelo servidor que vai gerar o tráfego adicional para se efectuarem testes na presença de tráfego adicional na rede. O PC3 tem a função de receber

os *streams* e tem também instalada o executável cliente do gerador de tráfego que lhe permite receber o tráfego que esteja a ser gerado pelo PC2.

Para realizar este teste, é necessário caracterizar o meio eléctrico do local onde se realizaram os testes. O laboratório tem diversas tomadas eléctricas, e por essa razão foram elaborados 3 testes para obter uma resposta mais concreta quanto às variações do meio físico do mesmo. O objectivo seria analisar as variações das características dos canais, quaisquer que fossem as tomadas do laboratório onde se ligassem os dispositivos. Na figura em baixo é apresentada a planta do laboratório onde foram realizados os testes e explicados os locais dos três testes efectuados ao meio.

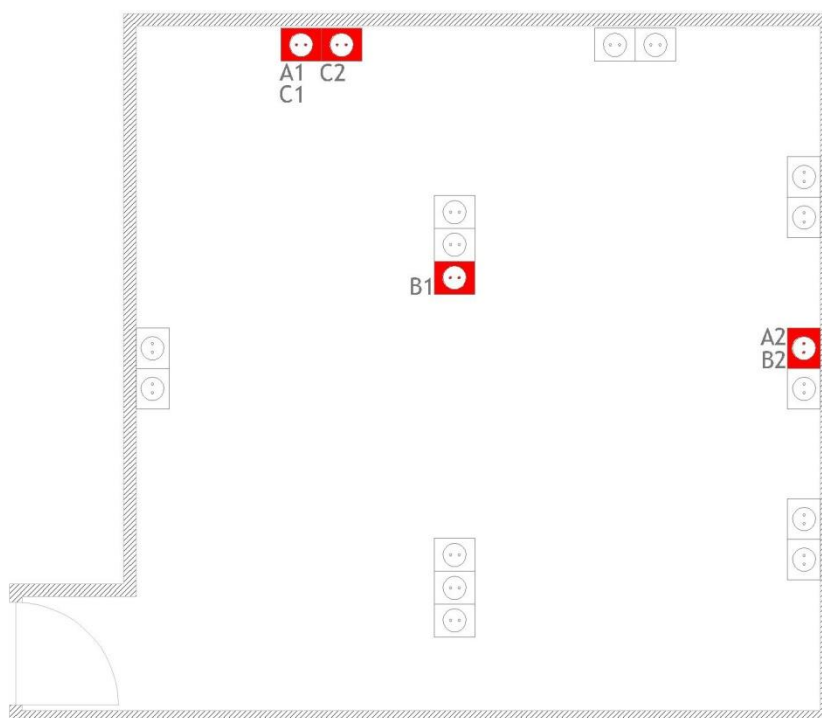


Figura 4.3 - Planta da sala de testes com testes representados.

As letras apresentadas na figura representam as diferentes tomadas onde foram efectuados testes, ou seja, no caso do primeiro teste uma tomada do dispositivo HomePlug foi ligada no local A1 da planta apresentada na figura 5.3 e o outro equipamento HomePlug ligado no local A2 e assim de forma idêntica para os testes 2 (tomadas B) e 3 (tomadas C).

A realização da análise do canal consistiu na utilização de um PC a transferir um ficheiro suficientemente grande (neste caso 700MB) para outro PC pertencente à mesma rede. A transferência do ficheiro foi realizada 5 vezes, a horas distintas (10 horas, 11 horas, 12 horas, 15 horas, 16 horas) para se verificar se existiam variações, bem como a respectiva dependência com a hora do dia - uma vez que diferentes equipamentos eléctricos ligados provocam interferências distintas. Com este teste, em que o ponto de estrangulamento é o canal HomePlug, pretende-se analisar a largura de banda do canal e o tempo médio de transferência.

Para o teste utilizando as tomadas A1 e A2, os resultados do débito da transferência do ficheiro são apresentados na tabela 4.2.

Tabela 4.2 - Resultados do débito da transferência no teste nº1.

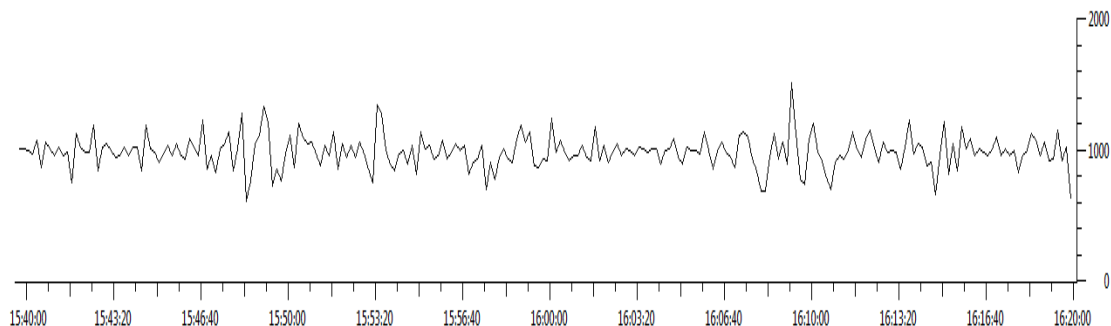
	Débito médio (Mbit/s)
Transferência nº1	58,954
Transferência nº2	61,069
Transferência nº3	61,307
Transferência nº4	62,487
Transferência nº5	59,766
Média	60,717

Ainda para uma melhor compreensão do comportamento do meio, foi efectuado o *streaming* do vídeo transferido. Embora com débitos mais baixos do que vídeos de alta definição, este teste serviu para verificar se o débito médio nos três testes realizados seria muito diferente. Os valores obtidos para este teste foram os que se apresentam na tabela 4.3.

Tabela 4.3 - Resultados do *streaming* do teste nº1.

	Valores
Pacotes	516 784
Tempo (s)	5293,71
Média pacotes/s	97,62
Média tamanho dos pacotes (Bytes)	1354,71
Bytes	700 092 500
Média Bytes/s	132 250,30
Média Mbit/s	1,058

Para este processo de *streaming* foi criado um gráfico onde no eixo dos XX está representado o tempo (s) e no eixo dos YY o débito (kbit/s) dos pacotes por cada intervalo de tempo. O intervalo de tempo escolhido para a apresentação em gráfico do *streaming* foi de 40 minutos e o aspecto do gráfico produzido no teste é o apresentado na figura 4.4.

Figura 4.4 - Gráfico do *streaming* do teste nº1.

O valor máximo de transferência obtido (e apresentado no gráfico) é 1,512 Mbit/s, o valor mínimo é 0,631 Mbit/s e o valor médio é 1,058 Mbit/s.

Para finalizar este teste nº1 foi realizado um ping, que é uma transferência simétrica, durando cerca de 30 minutos, de um computador para o outro com os valores apresentados na figura abaixo.

```
--- 192.168.0.11 ping statistics ---
1813 packets transmitted, 1813 packets received, 0% packet loss
round-trip min/avg/max/stddev = 3.618/4.016/8.307/0.365 ms
```

Figura 4.5 - Ping ente PC1 e PC3 do teste nº1.

Apresentam-se de seguida os resultados dos testes nas tomadas B1 e B2 e C1 e C2 em que todos os passos seguidos foram os mesmos. Os resultados para os testes de transferência de ficheiros e *streaming* nas tomadas B1 e B2 estão apresentados na Tabela 4.4 e Tabela 4.5, respectivamente.

Tabela 4.4 - Resultados do débito da transferência no teste nº2.

	Débito médio (Mbit/s)
Transferência nº1	54,123
Transferência nº2	55,450
Transferência nº3	55,187
Transferência nº4	55,312
Transferência nº5	55,179
Média	55,050

Tabela 4.5 - Resultados do *streaming* do teste nº2.

	Valores
Pacotes	516 669
Tempo (s)	5271,08
Média pacotes/s	98,02
Média tamanho dos pacotes (Bytes)	1355,06
Bytes	699 977 700
Média Bytes/s	132 822,83
Média Mbit/s	1,063

O gráfico correspondente à Tabela 4.5 está representado a seguir. O valor máximo do gráfico é 1,423 Mbit/s, o valor mínimo é 0,638 Mbit/s e a média é 1,063 Mbit/s.

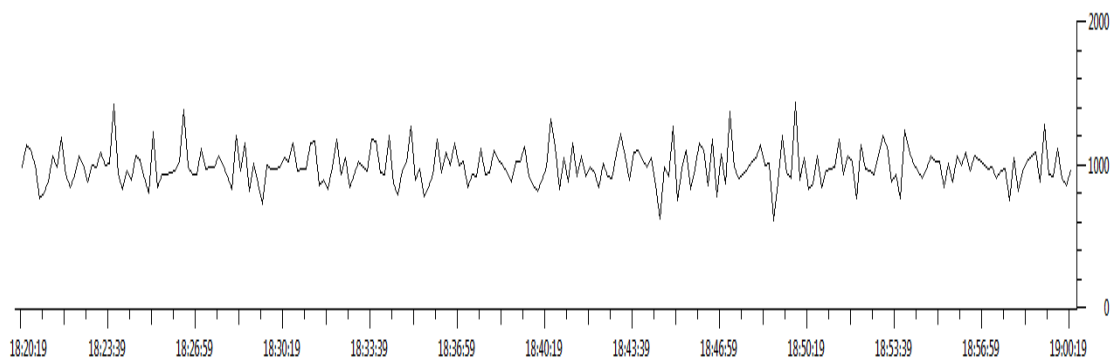


Figura 4.6 - Gráfico do *streaming* do teste nº2.

Finalmente, no teste nas tomadas B1 e B2 o resultado do ping efectuado do PC1 para o PC3 foi o representado na figura.

```
--- 192.168.0.11 ping statistics ---
1803 packets transmitted, 1803 packets received, 0% packet loss
round-trip min/avg/max/stddev = 3.611/4.562/10.048/0.701 ms
```

Figura 4.7 - Ping ente PC1 e PC3 do teste nº2.

Por fim, apresentam-se os resultados do teste das tomadas C1 e C2. Em baixo, estão representadas as tabelas com os resultados da transferência de ficheiros e do *streaming* do mesmo ficheiro.

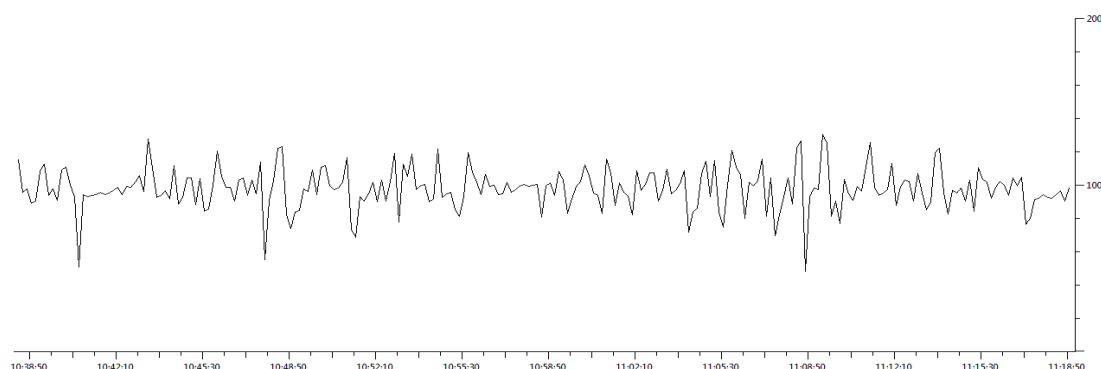
Tabela 4.6 - Resultados do débito da transferência no teste nº3.

	Débito médio (Mbit/s)
Transferência nº1	86,783
Transferência nº2	87,633
Transferência nº3	86,187
Transferência nº4	86,249
Transferência nº5	86,709
Média	86,712

Tabela 4.7 - Resultados do *streaming* do teste nº3.

	Valores
Pacotes	516 563
Tempo (s)	5289,40
Média pacotes/s	97,66
Média tamanho dos pacotes (Bytes)	1356,24
Bytes	700 189 580
Média Bytes/s	132 454,68
Média Mbit/s	1,060

Tal como nos testes anteriores, apresenta-se de seguida o gráfico do processo de *streaming*. Neste caso o valor máximo é 1,230 Mbit/s, o valor mínimo 0,511 Mbit/s e a média 1,060 Mbit/s.

Figura 4.8 - Gráfico do *streaming* do teste nº3.

O resultado do ping entre o PC1 e o PC3 nestas circunstâncias é apresentado na figura 4.9 abaixo.

```
--- 192.168.0.11 ping statistics ---
1809 packets transmitted, 1809 packets received, 0% packet loss
round-trip min/avg/max/stddev = 3.616/3.975/8.364/0.208 ms
```

Figura 4.9 - Ping ente PC1 e PC3 do teste nº2.

Com base nos testes efectuados ao meio, pode-se concluir que o teste nº3 é o que apresenta melhores resultados, mas no geral existem variações significativas conforme o local onde estejam ligados os dispositivos HomePlug. Quanto ao *streaming* do vídeo, que não ocupa toda a largura de banda disponível, o valor médio é semelhante em todos os casos. O teste nº3 permitia em teoria ter simultaneamente cerca de 80 vídeos iguais aos testados no *streaming*. Nos outros casos a largura de banda permite em teoria ter cerca de 60 vídeos. Esta diferença deve-se provavelmente aos caminhos que a rede eléctrica faz entre as duas tomadas e as respectivas interferências sofridas em cada caso.

Para a realização dos testes seguintes usaram-se as tomadas A1 e A2 para ligação dos equipamentos HomePlug porque, não corresponde aos casos que apresentam nem o maior nem o menor débito sendo a que melhor poderá representar o cenário de laboratório.

Convém ainda salientar que numa situação real, dificilmente os dois dispositivos estariam ligados em tomadas eléctricas tão próximas uma da outra.

Para os testes seguintes é importante identificar os casos em que existe QoS, sendo que este já vem implementado de base nos dispositivos HomePlug. Para retirar ou alterar as definições de QoS seria necessário já estar disponibilizado um *utility*, que existe mas apenas para o PLK200 e que não é compatível para este novo modelo (PLK300).

Outra vertente em análise é o comportamento do *streaming* na presença de tráfego adicional TCP ou UDP. Os testes com tráfego TCP foram realizados com o gerador Network Traffic Generator [40], com tráfego aleatório entre 1000 e 30000 kbit/s. A escolha deste tráfego tem o objectivo de mostrar que o tráfego RTP do *streaming*, mesmo com menores débitos vai conseguir um bom funcionamento, uma vez que quando estão os dois fluxos distintos em disputa pelo canal, o TCP devido ao seu mecanismo de controlo de congestionamento reduz o débito, o que não acontece no UDP. As simulações de tráfego UDP também são aleatórias entre 5000 e 6000 kbit/s. A escolha desta quantidade de tráfego serviu para mostrar o comportamento do tráfego UDP junto com o RTP. Analisaram-se situações em que existe mais tráfego gerado do que tráfego de *streaming* e vice-versa. Quando existe apenas um cliente o débito é apenas de 3072 kbit/s contra os cerca de 5500 kbit/s de tráfego UDP gerado. Mas na presença de 3 clientes em que o débito total do *streaming* é de aproximadamente 9000 kbit/s o tráfego adicionado pelo gerador já vai ser menor.

Os valores a serem monitorizados serão os mesmos para todos os cenários, ou seja, o *delta*, o *skew*, o *jitter*, a perda de pacotes e o débito. Relativamente a estes parâmetros, o *delta* representa a diferença entre o tempo de chegada do pacote actual e o tempo de chegada do pacote anterior. O *skew* é a medida de atraso ou avanço de um pacote em relação a um instante de chegada de referência, atendo em conta a taxa de geração de pacotes, por exemplo, se a taxa de pacotes for igual a 50 pacotes por segundo, e o milésimo pacote chegar 20,03 segundos depois do primeiro, então o *skew* do pacote é 30 ms. O *jitter* é definido segundo o RFC3550 [52], sendo esta definição adoptada no Wireshark [51]. A perda de pacotes simboliza os pacotes RTP, que é o protocolo escolhido para fazer *streaming*, que são perdidos durante o *streaming* e o débito é a largura de banda ocupada pelo vídeo. As portas utilizadas para os testes foram a 1234, 2500 e 5004. A escolha destas portas deveu-se primeiramente ao facto de a porta 5004 ser a destinada a fluxos de *streaming* RTP. No que respeita às outras duas portas, são portas que estão livres e preparadas para o tráfego UDP do *streaming*, segundo o site da IANA [54].

4.2 - Cenário 2

Neste teste (número 2) vão ser testadas as normas a, g e n. Pretende-se concluir qual é a melhor norma (em termos de largura de banda visto ser fundamental para os cenários de videovigilância), e a partir deste cenário sempre que se utilizar a tecnologia Wi-Fi vai ser utilizada essa mesma norma, ou seja, a que apresentar melhor desempenho neste teste. Os esquemas representados na figura 4.10 são para o caso com e sem QoS. Em ambos os casos existem dois computadores ligados ao router e um ligado ao outro router. O funcionamento de quem envia *streams* e outros fluxos de dados e os recebe é igual ao cenário 1.

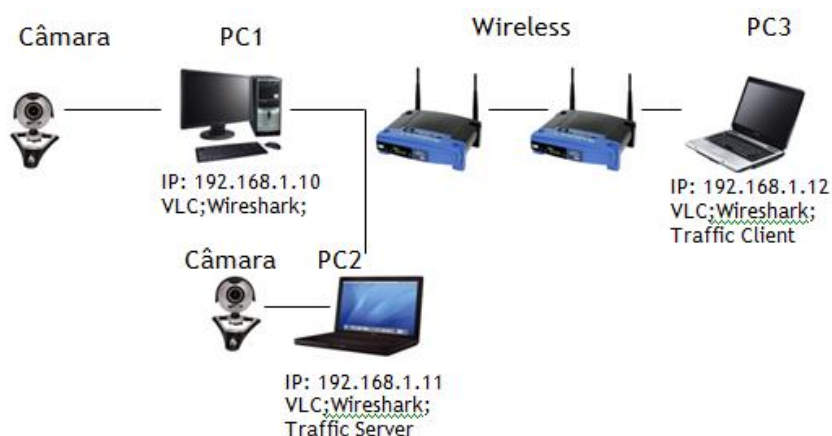


Figura 4.10 - Esquema do cenário 2 sem QoS.

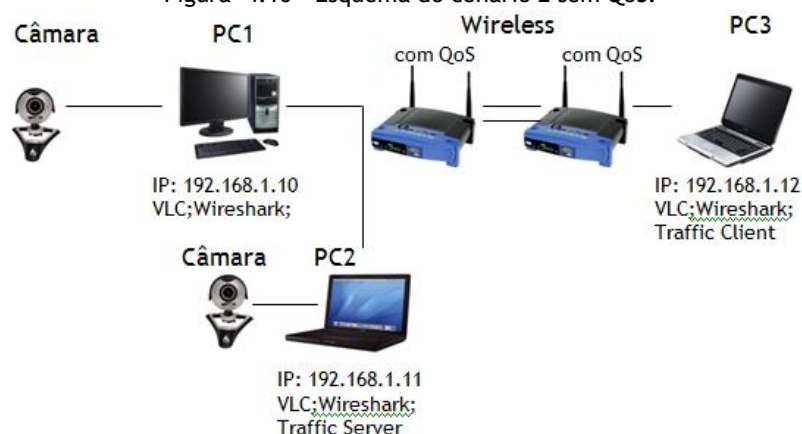


Figura 4.11 - Esquema do cenário 2 com QoS.

Neste cenário os *routers* estão ligados por cabo Ethernet, mas os computadores estão ligados aos *routers* por *Wireless*. Um dos *routers* é configurado para obter o endereço IP automaticamente por DHCP, enquanto que o endereço do outro *router* é introduzido manualmente pertencendo à mesma rede do anterior. Tal como no cenário anterior, o meio foi analisado pela transferência do mesmo ficheiro. A transferência foi realizada utilizando as normas 802.11a, 802.11g e 802.11n de forma a todas serem testadas. Este processo, de transferência de ficheiro, foi repetido em todos os cenários.

Tabela 4.8 - Resultados do débito da transferência para a norma 802.11a.

	Débito médio (Mbit/s)
Transferência nº1	31,896
Transferência nº2	31,681
Transferência nº3	30,599
Transferência nº4	32,077
Transferência nº5	31.250
Média	31,501

Tabela 4.9 - Resultados do débito da transferência para a norma 802.11g.

	Débito médio (Mbit/s)
Transferência nº1	23,150
Transferência nº2	22,552
Transferência nº3	22,942
Transferência nº4	23,198
Transferência nº5	22,925
Média	22,953

Tabela 4.10 - Resultados do débito da transferência para a norma 802.11n.

	Débito médio (Mbit/s)
Transferência nº1	62,728
Transferência nº2	65,929
Transferência nº3	59,593
Transferência nº4	60,039
Transferência nº5	63,751
Média	62,408

As tabelas em cima mostram, como seria de esperar, que é a norma 802.11n que apresenta maior largura de banda.

4.3 - Cenário 3

Neste cenário testa-se uma solução híbrida com e sem QoS, tal como representado nas figuras abaixo. O QoS vai ser tratado no *router* do mesmo modo que foi tratado no cenário 2 e descrito no capítulo 3 na secção 3.2.4.

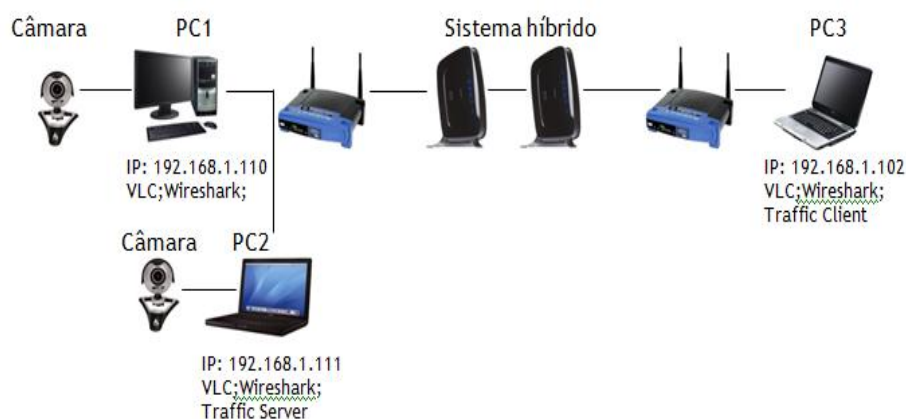


Figura 4.12 - Esquema do cenário 3 sem QoS.

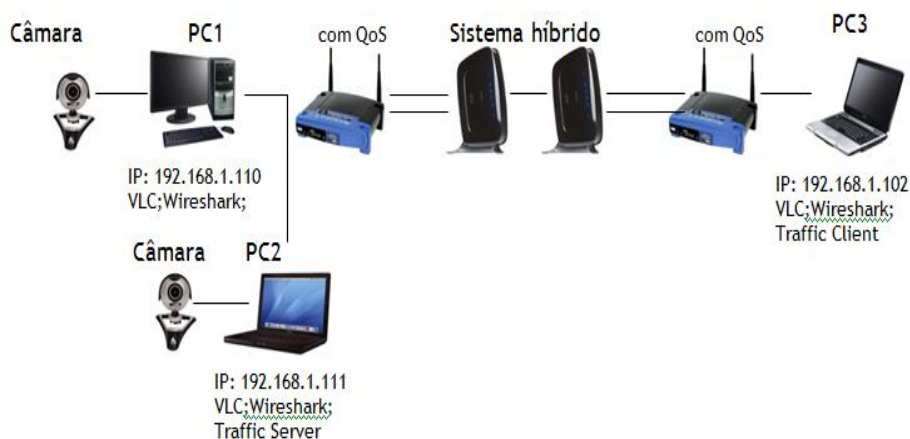


Figura 4.13 - Esquema do cenário 3 com QoS.

Tanto os emissores como o receptor vão estar ligados apenas aos *routers*. As tomadas eléctricas em que os dispositivos HomePlug estão ligados são as mesmas do cenário 1. Como referido anteriormente, a norma IEEE 802.11 aplicada neste caso é a que apresentou melhor desempenho no cenário 2. Neste cenário e nos dois que se seguem, o objectivo é estudar o comportamento das tecnologias *Wireless* e HomePlug quando trabalham em conjunto. Para isso compara-se o funcionamento com acesso *wireless* no emissor e receptor (cenário 3), apenas *wireless* no receptor (cenário 4) e depois apenas *wireless* no emissor (cenário 5). As tabelas a preencher serão as mesmas dos cenários anteriores. Para comparar este cenário híbrido com os cenários anteriores foi analisado o canal através da transferência do mesmo ficheiro dos testes anteriores. Os resultados estão presentes na tabela abaixo.

Tabela 4.11 - Resultados do débito da transferência para o cenário 3.

	Débito médio (Mbit/s)
Transferência nº1	47,006
Transferência nº2	45,840
Transferência nº3	45,774
Transferência nº4	49,796
Transferência nº5	44,030
Média	46,489

Este cenário apresenta uma largura de banda inferior às das duas tecnologias que estão a funcionar, sendo mesmo assim o cenário híbrido que atingiu maior débito.

4.4 - Cenário 4

Neste cenário é testada outra solução híbrida em que os emissores estão ligados a um dispositivo HomePlug e o receptor é ligado por *wireless*. Os dispositivos HomePlug permanecem ligados nas mesmas tomadas eléctricas A1 e A2 do cenário 1 e 3 e a norma 802.11 adoptada é a que melhor desempenho apresentou no cenário 2 (802.11n, como irá ser demonstrado no capítulo da análise de resultados).

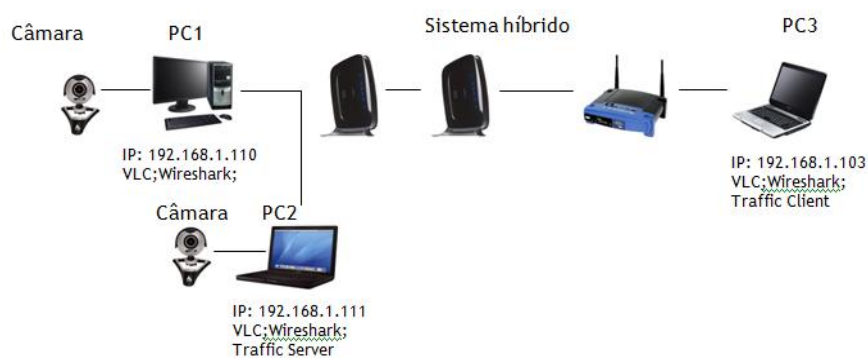


Figura 4.14 - Esquema do cenário 4 sem QoS.

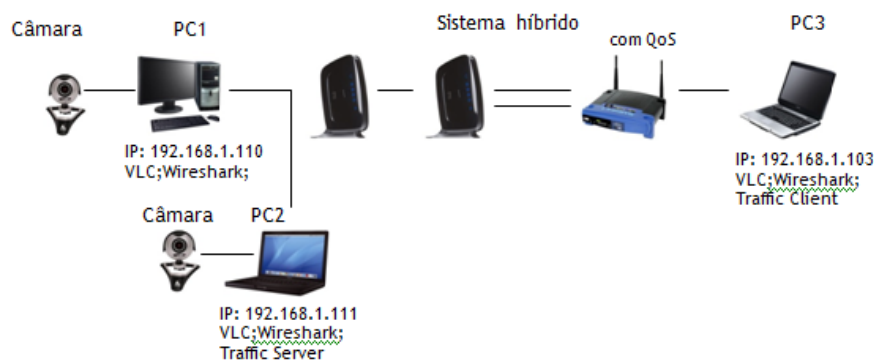


Figura 4.15 - Esquema do cenário 4 com QoS.

Neste caso o QoS é implementado no *router* e do mesmo modo dos casos anteriores com prioridade máxima para as portas que vão receber o *streaming*. Os procedimentos a tomar serão os mesmos dos casos anteriores, ou seja, as tabelas a preencher serão as mesmas do que nos dois cenários anteriores e a análise da largura do canal através da transferência de um ficheiro é apresentada na tabela 4.12.

Tabela 4.12 - Resultados do débito da transferência para o cenário 4.

	Débito médio (Mbit/s)
Transferência nº1	40,846
Transferência nº2	40,876
Transferência nº3	40,160
Transferência nº4	40,090
Transferência nº5	42,474
Média	40,909

Este cenário apresenta menor largura de banda do que o cenário anterior, embora também se apresentando na casa dos 40 Mbit/s.

4.5 - Cenário 5

Idêntico ao cenário 4 mas agora com o *router* do lado do emissor. Este cenário será testado também com e sem QoS. As tabelas e processos também são semelhantes aos anteriores.

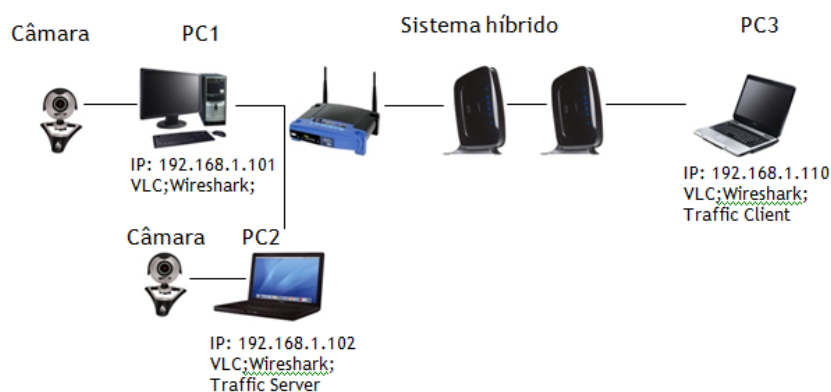


Figura 4.16 - Esquema do cenário 5 sem QoS.

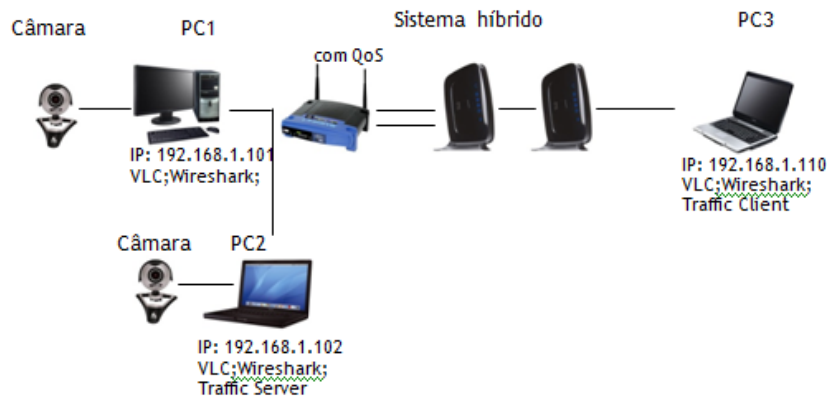


Figura 4.17 - Esquema do cenário 5 com QoS.

Todos os procedimentos destes testes são semelhantes e neste caso o método de configuração de QoS é igual aos cenários anteriores.

Novamente, a tabela dos resultados da transferência de um ficheiro, que foi sempre o mesmo, é apresentada em baixo e mostra a largura do canal utilizado.

Tabela 4.13 - Resultados do débito da transferência para o cenário 5.

	Débito médio (Mbit/s)
Transferência nº1	41,953
Transferência nº2	45,329
Transferência nº3	43,770
Transferência nº4	42,510
Transferência nº5	43,669
Média	43,446

Este foi o cenário híbrido que apresentou o segundo melhor resultado médio nestas transferências de ficheiro. A diferença de se ter o *router* no emissor ou no receptor representa, segundo este teste, uma diferença de aproximadamente 2,5 Mbit/s. Depois de analisados estes três cenários híbridos, o cenário mais favorável no capítulo da largura de banda é quando temos o emissor e receptor ligados por *Wireless* aos *routers*, estando estes ligados por HomePlug. Reparou-se que o cenário menos favorável foi quando o emissor estava ligado por HomePlug, provavelmente devido ao facto de ser o HomePlug o ponto de estrangulamento do canal.

4.6 - Cenário 6

Como se pode ver na figura 4.18, este cenário é idêntico ao cenário nº1, mas foi realizado com um objectivo diferente. O objectivo deste teste é fazer com que os dispositivos HomePlug constituam o ponto de estrangulamento do sistema.

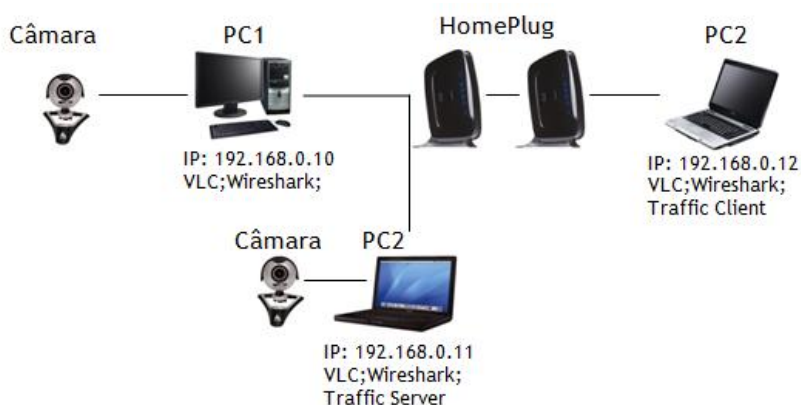


Figura 4.18 - Esquema do cenário 6.

Como nos testes anteriores o canal HomePlug nunca esteve totalmente cheio, também nunca se soube exactamente o modo como o HomePlug iria funcionar numa situação desse género. Para encontrar esta situação de estrangulamento distanciaram-se os dois dispositivos HomePlug de modo a que o débito baixasse consideravelmente, para cerca de 15 Mbit/s. Ao baixar o débito foi mais fácil encher o canal com o tráfego adicional gerado, quer TCP quer UDP.

Tabela 4.14 - Resultados do débito da transferência para o cenário 6.

	Débito médio (Mbit/s)
Transferência nº1	14,279
Transferência nº2	14,720
Transferência nº3	15,047
Transferência nº4	14,429
Transferência nº5	14,623
Média	14,620

Como se vê na tabela 4.14, a largura de banda deste canal baixou consideravelmente, o que fez com que o objectivo deste cenário fosse mais fácil de atingir. Para o saturar utilizou-se o programa MGEN para UDP e o Network Traffic Generator para TCP. Agora com o canal cheio é possível estudar com mais detalhe o comportamento desta tecnologia e do QoS que tem implementado, embora aqui o QoS seja apenas o que já vem de origem não havendo possibilidade de o alterar.

4.7 - Cenário 7

Como se pode ver na figura 4.19 em baixo este cenário tem uma configuração igual ao cenário 4. A diferença está no objectivo da realização do teste. Neste caso o objectivo é

estudar o papel do *router Wireless* na gestão do QoS. Neste cenário é possível verificar que com o canal saturado (o estrangulamento ocorre na ligação HomePlug) e com as devidas prioridades estabelecidas no *router*, os erros vão ser bastantes menores do que não utilizando QoS.

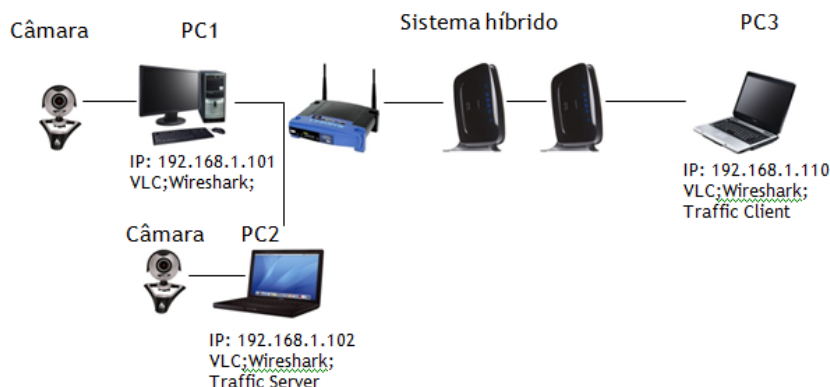


Figura 4.19 - Esquema do cenário 7 sem QoS

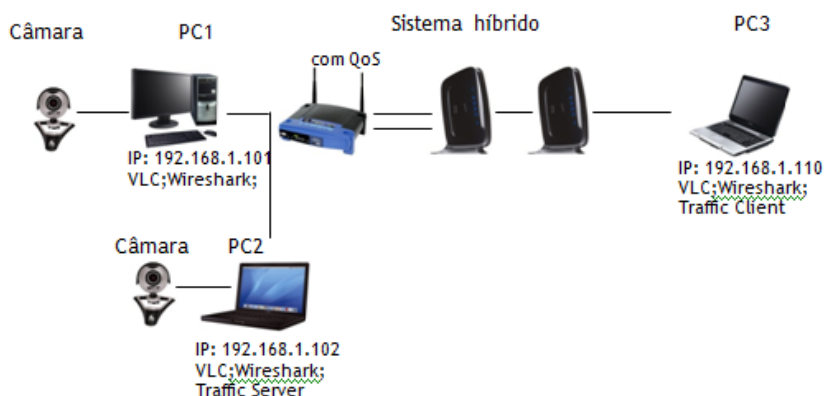


Figura 4.20 - Esquema do cenário 7 com QoS.

Neste cenário as tabelas a preencher serão as mesmas do cenário 2, 3, 4 e 5. Vão ser testadas com e sem QoS as situações de não haver tráfego adicional, a de existir tráfego adicional TCP e a de se gerar tráfego UDP. Os fluxos UDP e TCP gerados serão suficientemente elevados para ocupar completamente o canal.

Tabela 4.15 - Resultados do débito da transferência para o cenário 7.

	Débito médio (Mbit/s)
Transferência nº1	16,363
Transferência nº2	16,434
Transferência nº3	17,143
Transferência nº4	16,826
Transferência nº5	16,419
Média	16,637

O débito neste cenário também teve de ser baixo para se conseguir mais facilmente inundar o canal com tráfego gerado TCP e UDP.

Capítulo 5

Análise dos resultados

Neste capítulo são analisados os resultados obtidos nos testes. Para não tornar esta análise muito densa apenas serão apresentadas algumas tabelas, assim como os valores que se destaquem, sendo possível consultar todas as tabelas em anexo. Os resultados serão analisados em dois conjuntos. O primeiro conjunto corresponde aos primeiros cinco cenários, que estiveram sujeitos às mesmas condições, e o segundo conjunto inclui os cenários 6 e 7. Nesta análise são analisadas as variações dos valores em cada cenário comparativamente com os restantes. Para o cenário 2 é apresentada uma tabela comparativa que vai permitir analisar as diferenças entre as normas 802.11a, 802.11g e 802.11n num determinado cenário. Uma tabela semelhante à do cenário 2 foi utilizada para comparar os cenários 3, 4 e 5. Estes três cenários são os casos onde foram utilizadas as duas tecnologias, ou seja, os cenários híbridos. Nos cenários 6 e 7 são analisados todos os valores mediante a presença ou não de QoS, e a sua influência no débito e nos outros valores.

Para os primeiros cinco cenários, o canal, tanto HomePlug como Wi-Fi, nunca é saturado, por isso os resultados acabam por ser próximos uns dos outros, como seria esperado. Nos dois últimos cenários, 6 e 7, o canal já está completamente saturado e aí compreende-se melhor o funcionamento do QoS (*wireless*, uma vez que HomePlug usa QoS por omissão, mas não configurável). Para relembrar, até ao cenário 5 o canal além de ter os *streams*, ou não tinha tráfego de dados, ou tinha tráfego TCP entre 1 Mbit/s e 30 Mbit/s ou tráfego UDP entre 5 Mbit/s e 6 Mbit/s. Nos dois últimos cenários os canais receberam cerca de 15 Mbit/s de tráfego UDP ou TCP para saturar o canal.

5.1 - Cenário 1

Neste cenário (apresentado na figura 4.2) em que foi testada a tecnologia HomePlug verifica-se que esta pode ser a que oferece maior largura de banda, dependendo das tomadas eléctricas a que estão ligados os dispositivos. É importante disponibilizar a maior largura de banda possível para que tráfego que exista nessa mesma rede não afecte o tráfego do *streaming*, de modo a não existirem perdas nem danos nos pacotes, e para que seja suportado o maior número de *streams* simultâneos.

Quando apenas existe um cliente, um factor a ter em conta é não existirem perdas de pacotes quando está a ser usada apenas uma tecnologia.

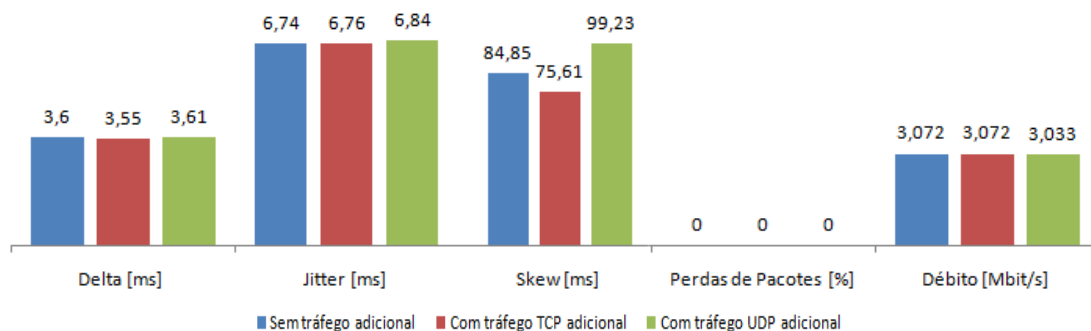


Figura 5.1 - Resultados cenário 1 / 1 cliente / porta 1234.

Este cenário de HomePlug puro é testado apenas com o QoS que vem implementado de origem. Quando existe apenas 1 cliente, e o canal está longe de estar saturado, o cenário apresenta o débito total do vídeo (3,072 Mbit/s) quando não existe tráfego adicional e quando existe tráfego adicional TCP, como se pode ver na figura 5.1. Quando existe tráfego UDP nota-se uma diminuição do débito, como seria de esperar devido à disputa do canal entre o tráfego UDP e o tráfego RTP do *streaming*. Quanto aos valores do delta, *skew* e *jitter* existe apenas uma pequena variação entre os três casos analisados, sendo, no entanto, na presença de tráfego UDP que se registam os maiores delta, *skew* e *jitter*. De referir que para nenhum caso existe perda de pacotes.

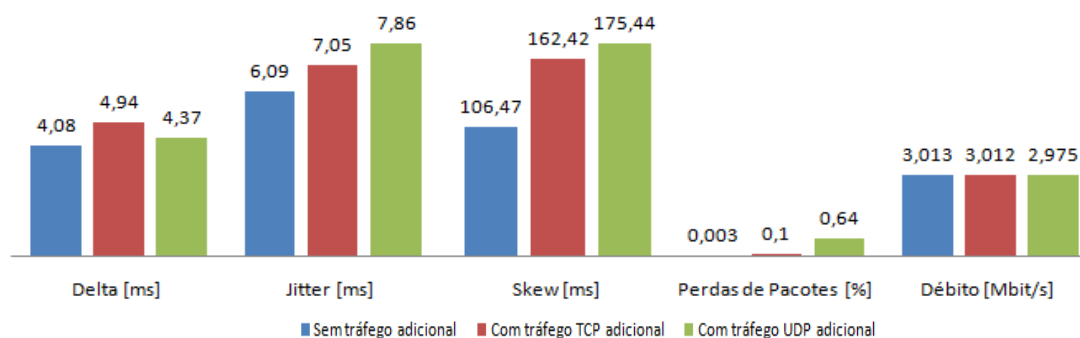


Figura 5.2 - Média dos 3 clientes no cenário 1.

Como mostra a figura 5.2, se se adicionar mais dois clientes as tendências são as mesmas do que foi referido antes, com os piores débitos a serem atingidos na presença de tráfego adicional UDP. Apenas numa porta (porta 1234) o débito é inferior na presença de tráfego TCP do que na presença de tráfego UDP. Isto acontece provavelmente devido ao número

elevado de retransmissões TCP que faz baixar o débito do *stream*. A maior diferença em relação ao caso em que apenas existe um cliente é que aqui já existem perdas de pacotes, principalmente quando existe tráfego adicional. A perda de pacotes é maior quando existe tráfego UDP, sendo uma das razões para que seja neste caso que o débito é menor, não atingindo os 3Mbit/s. O valor de delta apenas difere em menos de 1 ms para todos os casos, mas o *jitter* e o *skew* são menores quando não existe tráfego adicional e maiores na presença de tráfego UDP.

5.2 - Cenário 2

No cenário em causa (apresentado na figura 4.10), em que foram testadas as normas 802.11a, 802.11g e 802.11n, foi possível tirar algumas conclusões sobre o seu funcionamento. Mesmo antes dos testes propriamente ditos, é possível verificar que as três normas têm larguras de banda diferentes. A norma que apresenta uma maior largura de banda, como seria de esperar, é a norma 802.11n. A diferença para a que apresentou o segundo melhor resultado é sensivelmente o dobro, pois a norma 802.11a teve uma largura de banda de 31,5 Mbit/s e a norma 802.11n teve 62,4 Mbit/s. A norma que apresentou o pior resultado foi a norma g, que apenas obteve uma largura de banda cerca de 23 Mbit/s. Teoricamente a norma 802.11g e a norma 802.11a deveriam ter a mesma largura de banda, mas o facto de a norma 802.11a funcionar numa frequência diferente das normas comuns, g e n, beneficia-a porque todas as redes detectadas na sala de testes funcionam segundo a norma g. Porém, para que as redes *Wireless* detectadas na sala de testes não prejudicassem o funcionamento dos testes da norma g, os *routers* foram colocados a trabalhar em canais diferentes, ou seja, as redes detectadas funcionam no canal 6 e os *routers* usados na dissertação estão no canal 1 e/ou 11. Em relação à largura de banda obtida nos outros cenários, embora o 802.11n seja o que apresenta maior largura de banda (como já foi referido), comparando esta tecnologia com o HomePlug, a largura de banda deste último poderá ser mais elevada em alguns cenários que dependem do local de testes e das tomadas onde os dispositivos estão ligados (como foi o caso da sala de testes que foi usada).

Para melhor comparar estes cenários foi escolhido o caso mais ilustrativo de um cenário real e que pode ser mais interessante. Vai-se então analisar o caso em que existe tráfego adicional UDP e o QoS está activo nos emissores. Assim, é possível comparar os valores dos diferentes cenários para este caso específico. Os valores podem ser visualizados nos gráficos das figuras 5.3 e 5.4.

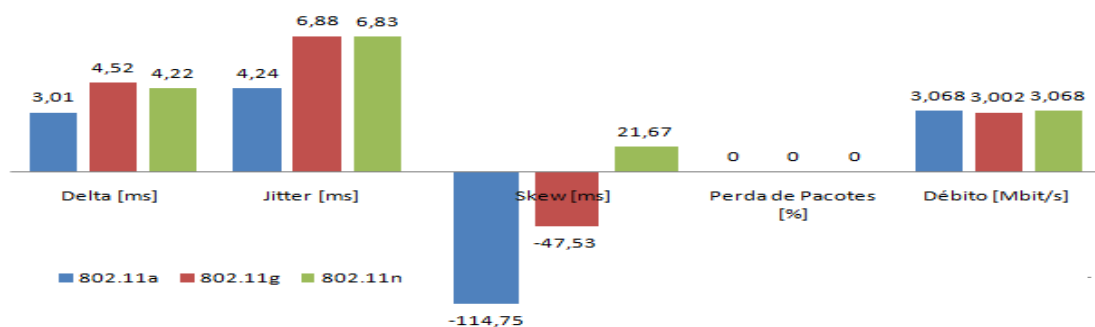


Figura 5.3 - Comparação da norma 802.11a, 802.11g e 802.11n no cenário 2 com 1 cliente.

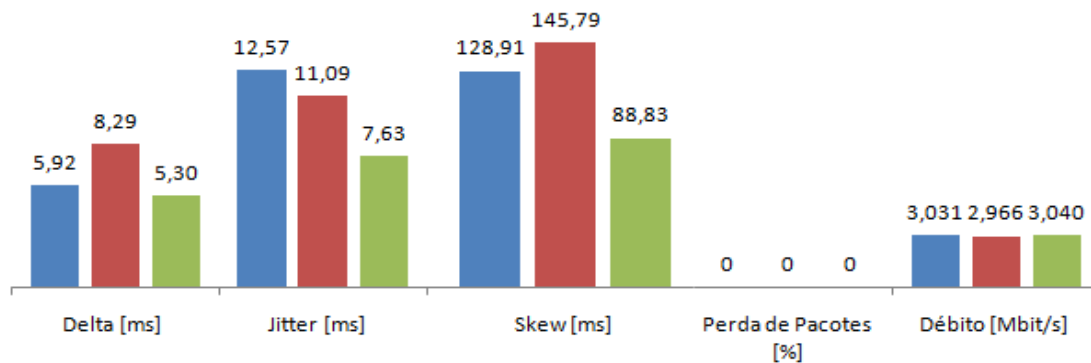


Figura 5.4 - Comparação da norma 802.11a, 802.11g e 802.11n no cenário 2 com 3 cliente.

Analisando primeiro quando existe apenas um cliente é possível verificar que o delta e o *jitter* são menores na norma 802.11a, sendo no entanto o caso que apresenta um maior *skew*. A norma 802.11a apresenta delta e *skew* menores também nos outros casos (sem tráfego adicional e com QoS e com tráfego adicional TCP e com QoS), ou seja, é nesta norma que a média de tempos da recepção de pacotes em relação ao anterior é menor e que os pacotes chegam mais perto do tempo que deviam chegar. O débito, com um cliente, é igual na norma 802.11a e 802.11n e superior ao débito na norma 802.11g. Embora não existam perdas de pacotes para nenhuma das normas, a norma 802.11g é a que apresenta piores valores. A norma 802.11g apresenta os piores valores mesmo se analisarmos os casos sem tráfego adicional ou com tráfego adicional TCP.

Quando passam a existir 3 clientes, as variações de valores já se passam de modo diferente. Neste caso é evidente que a norma 802.11n apresenta, para todos os valores medidos, um melhor desempenho, apresentando um delta, *skew* e *jitter* mais baixo e um débito mais elevado. De referir que com a presença de QoS em nenhuma das normas existem pacotes perdidos. Apenas na norma 802.11g o débito não atingiu os 3Mbit/s e é esta norma que apresenta novamente os piores valores em relação às outras normas.

Analisando a variação do delta para cada norma, quando se passa de um para três clientes verifica-se que esta passa sensivelmente para o dobro, exceptuando a norma n. Tal facto justifica-se porque a norma n apresenta uma largura de banda superior ao que a norma a e g. Olhando agora para o *jitter* pode-se dizer que a norma n, pelos mesmos motivos, continua a ser a que menor variação apresenta quando se passa de um para três clientes. Na norma 802.11a o jitter passa praticamente para o triplo quando se utilizam três clientes. Em todos os casos os débitos médios baixam ligeiramente com a introdução de novos clientes, sensivelmente na mesma proporção relativamente aos seus débitos no caso de um único cliente.

Depois de analisados os resultados a melhor opção é a norma 802.11n. Quando existe apenas um cliente a diferença entre as normas não é substancial, pois o débito de apenas um cliente não é suficiente para causar transtorno à rede. Na presença de três clientes já é possível tirar mais conclusões. A norma 802.11n é a única que não apresentou qualquer pacote perdido, seja com ou sem QoS. Em todos os outros valores medidos, a norma n apresenta melhor desempenho do que as outras normas como é fácil de constatar nas tabelas dos resultados. A norma n apresenta uma média final menor de quase todos os valores, nomeadamente o débito, *jitter* e perdas de pacotes. A norma que apresenta piores resultados é a 802.11g a todos os níveis. Esta é a norma que está mais sujeita a interferências de outras

redes existentes, pois apenas trabalha em 2.4 GHz, tal como as redes mais comuns. Estas interferências podem ter provocado as diferenças existentes entre a norma 802.11a e 802.11g que utilizam os mesmos princípios mas operam em frequências diferentes. Apesar de se ter procedido ao uso de outros canais, desejava-se efectuar testes destes cenários noutros ambientes para que os resultados fossem mais conclusivos, mas não houve tempo para isso. Em particular, a comparação de mais cenários *indoor* com cenários *outdoor* em espaço livre poderiam trazer resultados interessantes.

5.3 - Cenário 3, 4 e 5

No que diz respeito aos casos híbridos, testados no cenário 4 (figura 4.12 e 4.13), no cenário 4 (figura 4.14 e 4.15) e no cenário 5 (figura 4.16 e 4.17), é possível verificar que em nenhum deles é possível atingir a largura de banda que as tecnologias, quando a trabalhar isoladamente, atingem. Este resultado é esperado uma vez que estamos a incluir mais elementos no sistema, aumentando o atraso, inserindo potenciais pontos de estrangulamento, etc. No cenário 4, em que se tem o emissor e o receptor a comunicar através de Wi-Fi (norma 802.11n) obtém-se uma maior largura de banda no que se refere aos cenários híbridos, no entanto cerca de 16 Mbit/s inferior à tecnologia 802.11n. Dentro dos cenários híbridos, o cenário 4 é o caso que apresentou menor largura de banda, a uma distância de cerca de 5,5 Mbit/s em relação ao melhor caso nos testes híbridos verificados no cenário 3. No cenário 5, onde a diferença para o anterior é a troca em que o emissor passa a estar ligado por HomePlug e o receptor por *Wireless*, apresenta uma largura de banda intermédia em relação aos cenários 3 e 4, ou seja é cerca de 3 Mbit/s inferior em relação ao cenário 3 e cerca de 3 Mbit/s superior ao cenário 4.

Para comparar estes três cenários foi construída uma tabela semelhante à realizada para a comparação das três normas do IEEE 802.11. O caso escolhido foi o mesmo, ou seja, presença de tráfego adicional UDP com QoS. Neste cenário, tal como nos anteriores, o canal não estava saturado e por isso os valores são próximos uns dos outros.

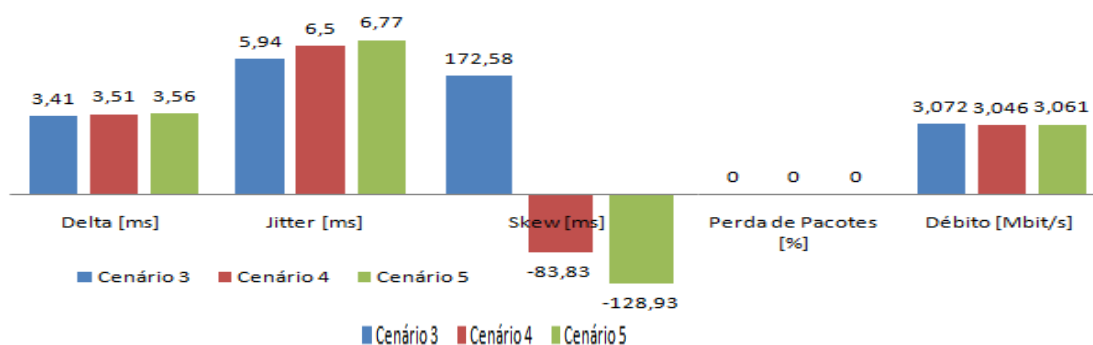


Figura 5.5 - Comparação do cenário 3, cenário 4 e cenário 5 com 1 cliente.

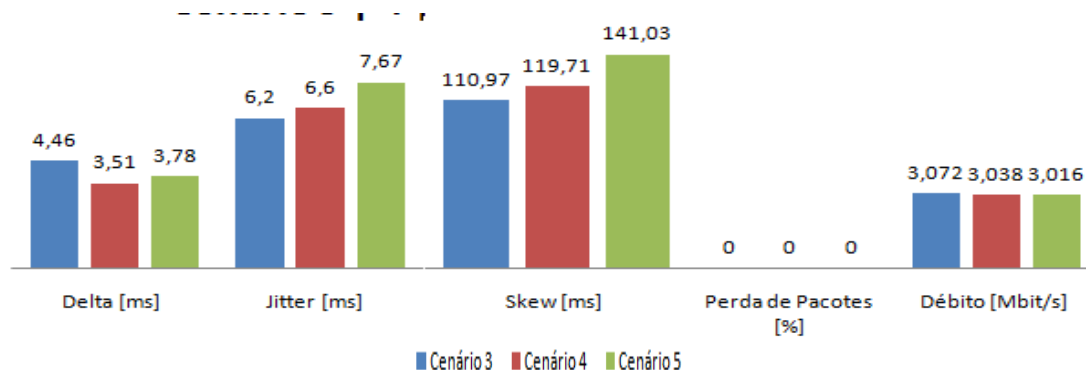


Figura 5.6 - Comparação do cenário 3, cenário 4 e cenário 5 com 3 clientes.

Na presença de 1 cliente é possível verificar que o cenário 3 é o que apresenta o débito igual ao da emissão do *stream*. Para os outros dois cenários o débito é diferente de 3,072 Mbit/s, mas o cenário 5 apresenta um débito superior ao do cenário 4. É no cenário 3 que se obteve o melhor *jitter* e delta, embora o melhor *skew* tenha sido obtido no cenário 4. Como o canal está longe de estar saturado e existe QoS, em nenhum dos cenários existiu perda de pacotes. Quando apenas existe 1 cliente, o cenário 4 foi o único cenários destes 3 em que existiu um caso em que não atingiu um débito de 3 Mbit/s. Isso aconteceu quando existia tráfego UDP adicional mas não havia QoS, o que provocou um número de perdas de 0,28%.

Nestes cenários híbridos é possível verificar que quando se adicionam 2 clientes os valores medidos não sofrem grandes alterações. O delta e *jitter* sofrem variações ligeiras em qualquer dos três cenários. Isto acontece, porque mesmo com mais estes 2 clientes o canal continua a estar longe da saturação. Um aspecto importante a referir é o facto do cenário 3 apresentar uma média de débito de 3,072 Mbit/s, ou seja, nas três portas foi atingido o débito total do *streaming*. Em nenhum dos 3 cenários existiu perda de pacotes, tal como aconteceu para quando apenas existia 1 cliente. O menor débito passou a ser no cenário 5, em troca com o cenário 4 que tinha sido o pior com 1 cliente. Os valores atingidos pelo cenário 4 mostram uma grande estabilidade, pois são muito idênticos quer para 1 cliente como para 3 clientes. Tal como quando existia apenas 1 cliente, agora com 3 clientes foi no cenário 4 que se atingiu o pior cenário quando existia tráfego UDP mas não estava implementado QoS. Neste caso o débito foi de 2,892 Mbit/s devido a perdas de 2,2%. Estes valores mais baixos de débito, que costumam existir onde há mais perdas, tornam o vídeo mais lento e com algumas paragens de imagem.

As diferenças entre os casos sem tráfego adicional, com tráfego adicional TCP e/ou UDP passam-se do mesmo modo que no cenário 2, ou seja, como o canal não está saturado os resultados são piores quando não existe QoS. O facto de não existir QoS é mais prejudicial na presença de tráfego UDP adicional do que TCP.

5.4 - Cenário 6

Este é um cenário (figura 4.18) num contexto totalmente diferente dos cinco anteriores. Aqui pretendia-se encontrar um canal com uma baixa largura de banda para melhor perceber o funcionamento do QoS implementado no caso do HomePlug. Os resultados obtidos mostram que o QoS implementado nos dispositivos HomePlug não é o adequado para este tipo de sistemas em que é necessário receber as imagens com o menor número de perdas possível. Tal como para o modelo anterior destes dispositivos HomePlug, o PLK200, que já permite

configurar QoS, é de acreditar que brevemente esteja disponível para estes dispositivos uma aplicação semelhante.

Quando apenas existe um cliente que utiliza uma porta, como era de esperar, o caso mais crítico ocorreu com a presença de tráfego adicional UDP. Isto deve-se ao facto de as portas que conduzem o tráfego adicional terem a mesma prioridade do que as portas de *streaming*. Como o tráfego UDP, que não é sujeito a qualquer controlo de fluxo, entra sempre em disputa com o tráfego do *stream*, vão existir mais perdas, ao contrário do caso com tráfego TCP, onde este é sujeito a controlo de fluxo e ocupa apenas a largura de banda livre. Estas características já tinham sido demonstradas nos cenários anteriores. Esse caso crítico com tráfego UDP é apresentado na figura em baixo, onde se mostra um débito bem inferior ao esperado que é 3,072 Mbit/s.

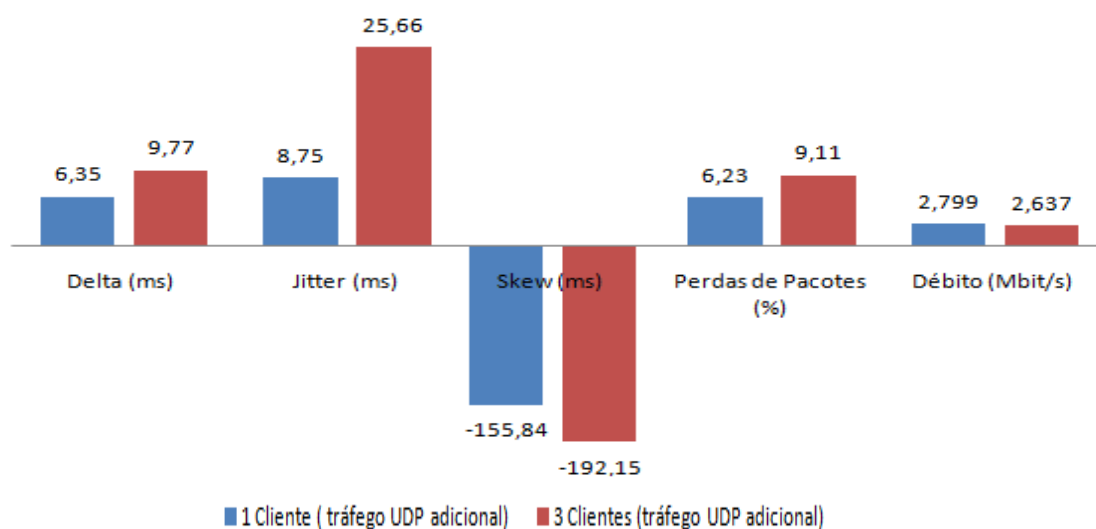


Figura 5.7 - Comparação do cenário 6 entre 1 e 3 clientes na presença de tráfego UDP adicional.

Tal como seria de esperar, pelo canal já estar cheio, ao introduzir no sistema mais 2 clientes, os resultados ainda se degradaram mais. A porta 5004 é a que apresenta um menor débito e mais pacotes perdidos. O gráfico é apresentado na figura 5.6 para facilitar a comparação entre 1 e 3 clientes.

Neste gráfico é possível verificar o esperado, ou seja, uma diminuição no débito e um aumento no número de pacotes perdidos. Se o canal já tinha apresentado perdas com apenas 1 cliente é normal que estes resultados piores com a introdução de ainda mais 2 clientes. É possível verificar uma degradação de resultados com tráfego adicional UDP em relação ao que se passa com TCP. Com tráfego TCP, os resultados são semelhantes ao que se passa quando não existe tráfego adicional, apenas com pequenas perdas e um delta e *jitter* ligeiramente mais altos.

5.5 - Cenário 7

Este cenário (figura 4.19) tem o mesmo objectivo do que o cenário anterior, mas agora usando a tecnologia *Wireless* para perceber a diferença da ligação quando o canal está cheio, com e sem QoS. De referir que o canal apenas fica cheio quando existe tráfego adicional no sistema. Como já foi dito anteriormente, no caso do *Wireless* é possível ligar e desligar o QoS e definir níveis de prioridade.

Os resultados obtidos nos testes estão de acordo com o esperado, ou seja, é bastante visível a diferença entre os resultados com e sem QoS. Na tabela em baixo é apresentada uma comparação na porta 1234 do que se passou com e sem QoS quando estavam a funcionar 3 clientes.

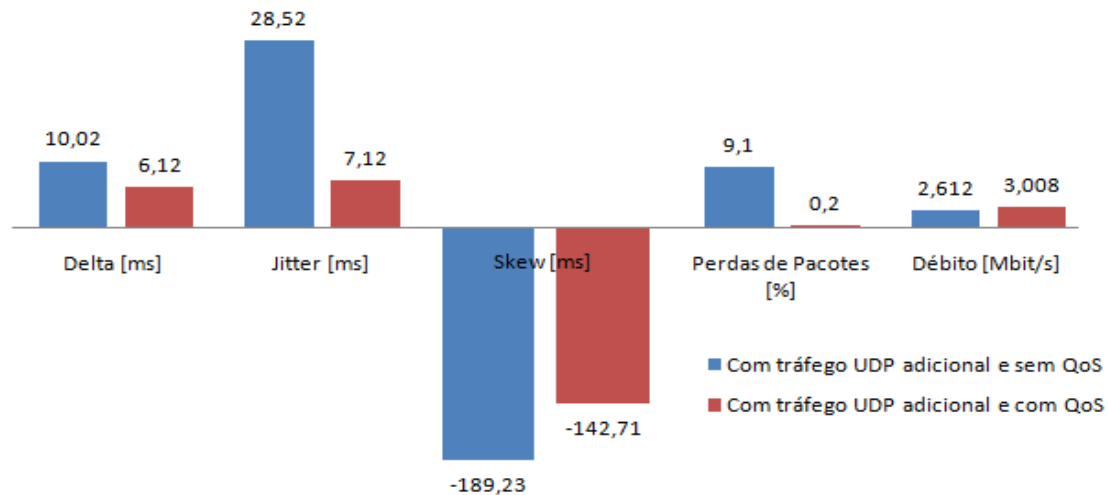


Figura 5.8 - Comparação do cenário 7 com tráfego UDP adicional com e sem QoS na porta 1234.

Como se pode ver na figura, o facto da porta 1234 ter prioridade no QoS beneficia-a bastante em termos de eficiência. Com QoS esta porta tem um menor delta, *skew*, *jitter*, pacotes perdidos e um maior débito. De referir que os resultados sem QoS são semelhantes ao do cenário 6, onde se trabalhou apenas com a tecnologia HomePlug. Estes resultados são semelhantes, pois não é possível desactivar nem mudar o QoS que está implementado nos dispositivos HomePlug. Para os casos em que não existiu tráfego adicional, os resultados são semelhantes entre eles, porque não existiu saturação do canal. Quando se adicionou tráfego TCP houve uma ligeira melhoria quando o QoS esteve activo, mas como com TCP a perda de pacotes sem QoS não é tão notória, onde melhor se vê o efeito do QoS é na presença de tráfego UDP.

5.6 - Análise Geral

A norma que apresentou melhores resultados individuais foi a norma 802.11n, ao passo que a montagem de cenários híbridos é recomendada de forma a aproveitar da melhor forma a capacidade da rede eléctrica, uma vez que embora seja necessário experimentar variadas tomadas eléctricas, o HomePlug pode ser uma tecnologia que pode proporcionar débitos ainda mais elevados do que a norma 802.11n.

Ainda relativamente às normas 802.11, nos testes efectuados detectaram-se casos particulares como na norma 802.11g que, como era esperado, foi a que piores resultados apresentou. Por isso, caso a norma 802.11n não possa ser adquirida por algum motivo, a norma recomendada seria a 802.11a que obteve melhor desempenho do que a norma g. Talvez não fosse esperado que o QoS implementado nos dispositivos HomePlug fosse tão ineficiente, pois apresentou perdas relativamente altas, principalmente na presença de três clientes.

Com os testes verificou-se que a implementação de QoS tem impacto no sistema melhorando todas as grandezas em análise. O QoS é mesmo fundamental para um sistema fiável e sem perdas. O funcionamento do QoS é bem visível no último cenário em que se prova que existem muito mais perdas e o débito é menor quando não existe QoS.

Ao nível da experiência do utilizador a assistir ao *streaming*, este é particularmente sensível com tráfego UDP. Nos primeiros cinco testes efectuados não foram detectadas quebras de imagem e a experiência do utilizador foi boa. Apenas nos dois últimos cenários, quando apenas existia QoS do HomePlug, existiram algumas paragens na imagem e alguns quadrados que tornavam a imagem confusa. No cenário 7, mesmo com o canal saturado, foi possível verificar que com a introdução do *wireless* e o seu sistema de QoS, a imagem melhorou bastante e se deixou de ter os tais quadrados e paragens na imagem. De referir que em todos os casos, os valores apresentados pelo vídeo foram sempre melhores do que os definidos no capítulo 2, na secção 2.3.4, como mínimos para se obter uma boa experiência de utilizador.

Como conclusão final dos testes conclui-se que estas tecnologias individualmente ou em conjunto podem ser aplicadas à videovigilância com os cuidados a ter no que respeita ao local onde vão ser aplicadas, principalmente no caso do HomePlug. O facto do HomePlug, quando actua sozinho, ser necessário um cabo Ethernet é um ponto contra esta tecnologia. É por isso de pensar que esta tecnologia seja melhor a trabalhar juntamente com a norma 802.11.

Capítulo 6

Conclusão

Esta dissertação realizou uma comparação e análise de duas tecnologias diferentes passíveis de serem integradas em cenários de *streaming* de vídeo para videovigilância. Estas duas tecnologias foram o *Wireless* (normas a/b/g/n) e o HomePlug, a primeira sem fios e a segunda cablada. Para fazer esta comparação foram testados vários cenários utilizando estas tecnologias de forma isolada e combinada (cenários híbridos). Relativamente aos testes efectuados, os primeiros cinco cenários de teste visam identificar as diferenças entre utilizar estas tecnologias isoladamente, cenário 1 e 2, e utilizadas em conjunto, cenário 3, 4 e 5. No cenário 2 avaliaram-se três versões diferentes da norma 802.11. Depois dos primeiros 5 cenários, percebeu-se que os resultados não eram totalmente conclusivos, porque o canal não foi testado estando completamente saturado. Para perceber o funcionamento do canal saturado, pensou-se em dois cenários em que se utilizassem as duas tecnologias. Um dos testes efectuados para a tecnologia HomePlug permitiu concluir que para diminuir a largura de banda do canal se pode proceder ao afastamento dos dois dispositivos (HomePlug) e à utilização de fichas triplas. Estas alterações introduzem mais ruído e atenuação e podem mesmo obrigar à escolha de outro tone map provocando uma diminuição acentuada na largura de banda. No que respeita às normas 802.11 concluiu-se que aquela que apresentou melhor desempenho foi a norma n. Quando se utilizam as duas tecnologias (IEEE 802.11 e HomePlug) conseguiu-se perceber que as larguras de banda variam conforme a montagem do cenário.

Os resultados dos testes permitem ainda concluir que estas tecnologias podem ser adoptadas para a videovigilância, em cenários de utilização individual ou híbrida. A arquitectura mista seleccionada é de extrema importância bem como o uso de QoS. Um sistema híbrido pode ser uma boa solução para locais onde os dispositivos HomePlug tenham um bom desempenho. Já o QoS é fundamental para um sistema de videovigilância em que pretende que as imagens recebidas tenham o mínimo de atraso e poucas perdas.

Ao nível dos resultados atingidos, a realização deste trabalho apresentou alguns desafios, que foram superadas com maior ou menor dificuldade. A maior dificuldade surgiu no princípio dos testes onde se verificou que o gerador de tráfego Network Traffic Generator era muito pesado computacionalmente para o processador e que não era possível, na mesma máquina, suportar mais do que uma aplicação de *streaming* de vídeo em simultâneo com a geração de

tráfego - pois facilmente o CPU atingia os 100% de capacidade de processamento. Quando foi decidido que era relevante saturar o canal teve-se que encontrar um outro modo de o fazer. Como no cenário 1 já se sabia que o débito variava mediante o local onde estavam ligados os dispositivos, optou-se por realizar o procedimento descrito acima, que consiste no afastamento dos equipamentos HomePlug e introdução de fichas triplas. Foi ainda necessário encontrar um novo gerador de tráfego UDP, já que o adoptado anteriormente (o Network Traffic Generator) apresentava limitações quando se pretendia gerar uma quantidade significativa de tráfego UDP.

Os objectivos deste trabalho foram totalmente atingidos na medida em que foi possível comparar as tecnologias separadamente e em conjunto, percebendo alguns dos seus pontos fortes e fracos. Este trabalho apresenta também uma série de contribuições inovadoras na medida em que não foi encontrada na literatura nada de semelhante com os testes realizados.

Como trabalho futuro, um aspecto importante é estabelecer critérios de QoS para o HomePlug. O facto de não ter sido possível alterar as definições do QoS do HomePlug foi um factor que não permitiu uma comparação melhor quando se usam as tecnologias separadamente. Poderá ser interessante também novos cenários de teste noutros ambientes, tanto *indoor* como *outdoor* em que se utiliza um “mix” de normas IEEE 802.11. Como num cenário de videovigilância como o mencionado aqui no trabalho, os *robots* são dispositivos móveis, e por isso era interessante realizar testes onde, por exemplo, as fontes se afastassem dos pontos de acesso para ver como reagiria a qualidade do vídeo. Outro cenário interessante de análise e estudo é a gestão da mobilidade dos dispositivos móveis.

Referências

- [1] IEEE 802.11 *Wireless Local Area Networks*, <http://www.ieee802.org/11/>. Acesso em 08/Fevereiro/2010.
- [2] HomePlug Powerline Alliance, <http://www.homeplug.org>. Acesso em 08/Fevereiro/2010.
- [3] Iftk.com.br, <http://www.iftk.com.br/wordpress/robo-seguranca-da-hitachi.html>. Acesso em 08/Fevereiro/2010.
- [4] terra, <http://tecnologia.terra.com.br/interna/0,,OI564801-EI4799,00.html>. Acesso em 08/Fevereiro/2010.
- [5] Ocasionalidades, <http://ocasionalidades.wordpress.com/2006/04/12/alemanha-contrata-robots-para-garantir-seguranca-do-mundial/>. Acesso em 08/Fevereiro/2010.
- [6] Fox News, <http://www.foxnews.com/scitech/2010/01/19/robot-cockroaches-help-haiti-earthquake-victims/>. Acesso em 08/Fevereiro/2010.
- [7] Charles Spurgeon's Ethernet, <http://www.ethermanage.com/Ethernet/Ethernet.html/>. Acesso em 08/Fevereiro/2010.
- [8] MoCA, <http://www.mocalliance.org/>. Acesso em 08/Fevereiro/2010.
- [9] Haniph A. Latchman, Richard Newman, "HomePlug Standards for Worldwide Multimedia In-Home Networking and Broadband Powerline Access", Intellon Corporation
- [10] HomePlug 1.0 Technology White Paper.
- [11] David Williams, "Turbo Product Code Tutorial", Maio de 2000.
- [12] HomePlug Technology Field Test Results - A White Paper.
- [13] HomePlug AV White Paper.
- [14] F. J. González-Castaño, F. J. Gil-Castiñeira, M. Rodelgo-Lacruz, R. Asorey-Cacheda, "Off-the-shelf transparent HomePlug range extension", Departamento de Ingeniería Telemática, Universidad de Vigo.
- [15] Christine Hsu, Neng Wang, Wai-Yip Chan, Praveen Jain, "Improving HomePlug Power Line Communications with LDPC Coded OFDM", Department of Electrical & Computer Engineering, Queen's University, Kingston, Ontario, Canada.
- [16] Miguel Elias M. Campos, Luis Henrique M. K. Costa, Otto Carlos M. B. Duarte, "Improving the Data Transmission Throughput over the Home Electrical Wiring", Grupo de Teleinformática e Automação, Universidade Federal do Rio de Janeiro.
- [17] E. Guerrini, G. Dell' Amico, P. Bisaglia, L. Guerrini, "Bit-Algorithms and SNR estimate for HomePlug AV", STMicroelectronics Group, Aosta, Italy.

- [18] Sung-Guk Yoon, Jeongkyun Yun, Saewoong Bahk, "Adaptative Contention Window Mechanism for Enhancing Throughput in HomePlug AV Networks", School of Electrical Engineering and Computer Science, Seoul, Korea.
- [19] Xufeng Huo, Peng Wang, George Kolev, "eHealth for Hospital Environment: Incorporating IEEE802.16 and HomePlug AV Standards", Department of Communications Systems, University of Lancaster, UK.
- [20] "Intel and 802.11- Helping Define 802.11n and other *Wireless* LAN Standards". Disponível em http://www.intel.com/standards/case/case_802_11.htm. Acedido em 08/Fevereiro/2010.
- [21] "IEEE 801.11b *Wireless* LANs Technical Paper", 3COM - *Wireless* Freedom at Ethernet Speeds.
- [22] Dimitris Vassis, George Kormentzas, Angelos Rouskas, Ilias Maglogiannis, "The IEEE 802.11g Standard for High Data Rate WLANs", University of the Aegean.
- [23] Daniel Jiang, Luca Delgrossi, "IEEE 802.11p: Towards an International Standard for *Wireless* Access in Vehicular Environments", Mercedes-Benz Research & Development North America, Inc.
- [24] M. K. Lee, H. A. Latchman, R. E. Newman, S. Katar, L. Youge, "Field Performance Comparison of IEEE 802.11b and HomePlug 1.0", Intellon Corporation.
- [25] Victor Clincy, Ajay Sitaram, David Odaibo, Garima Sogarwal, "A Real-Time Study of 802.11b and 802.11g", Kennesaw State University.
- [26] Kaywan H. Afkhamie, Srinivas Katar, Larry Uouge, Richard Newman, "An Overview of the upcoming HomePlug AV Standard", Intellon Corporation.
- [27] Fernando Pereira, Aníbal Ferreira, Carlos Salema, Isabel Trancoso, Paulo Correia, Pedro Assunção, Sérgio Faria, "Comunicações Audiovisuais - Tecnologias, Normas e Aplicações", IST Press.
- [28] Artur Pimenta Alves, Teresa Andrade, Apontamentos da cadeira de "Televisão Digital e outros Serviços" disponível em <http://paginas.fe.up.pt/~mandrade/tvd/2006/index-2006.html>; Acesso em 08/Fevereiro/2010.
- [29] Rui Almeida, "Transmissão de video em tempo real na Internet", Dissertação de mestrado, Universidade de Aveiro, 2004.
- [30] Architecture & Transport Working Group, Tim Rahrer, Riccardo Fiandra, Steven Wright, "Triple-play Quality of Experience (QoE) Requirements", Dezembro de 2006.
- [31] Wikipedia, http://en.wikipedia.org/wiki/IEEE_802.11a-1999; Acesso em 10/Junho/2010.
- [32] Vocal Technologies, "802.11a White Paper". Disponível em http://www.vocal.com/white_paper/80211a_wp1pdf.pdf; Acesso em 10/Junho/2010.
- [33] Broadneeds, http://www.broadneeds.com.br/ver_noticia.asp?id=5; Acesso em 10/Junho/2010.
- [34] José Ruela, "Arquitecturas Multimédia" Disponível em http://paginas.fe.up.pt/~jruela/Apontamentos/Arq_IETF.pdf; Acesso em 10/Junho/2010.
- [35] J. Postel, "RFC768 - User Datagram Protocol". Disponível em <http://www.faqs.org/rfcs/rfc768.html>. Acesso em 10/Junho/2010.
- [36] "RFC - Transmission Control Protocol". Disponível em <http://www.faqs.org/rfcs/rfc793.html>; Acesso em 10/Junho/2010.
- [37] Linksys, <http://www.linksys.com/>. Acesso em 15/Junho/2010.
- [38] VLC, <http://www.videolan.org/vlc/>. Acesso em 15/Junho/2010.
- [39] Wireshark, <http://www.wireshark.org/>. Acesso em 15/Junho/2010.

- [40] Network Traffic Generator, <http://sourceforge.net/projects/traffic/>. Acesso em 15/Junho/2010.
- [41] Manual do Router. Disponível em <http://www.linksysbycisco.com/LATAM/pt/products/WRT610N>. Acesso em 15/Junho/2010.
- [42] Manual HomePlug, <http://homesupport.cisco.com/en-us/wireless/lbc/PLK300>. Acesso em 15/Junho/2010.
- [43] Utility. Disponível em <http://homesupport.cisco.com/en-us/wireless/lbc/PLK200>. Acesso em 15/Junho/2010.
- [44] IEEE 802.11i Group. Disponível em http://www.ieee802.org/11/Reports/tgi_update.htm. Acesso em 27/Junho/2010.
- [45] IEEE 802.11r Group. Disponível em http://www.ieee802.org/11/Reports/tgr_update.htm. Acesso em 27/Junho/2010.
- [46] IEEE 802.11w Group. Disponível em http://standards.ieee.org/announcements/2009/pr_802.11w.html. Acesso em 27/Junho/2010.
- [47] IEEE 802.11n Group. Disponível em http://www.ieee802.org/11/Reports/tgn_update.htm. Acesso em 27/Junho/2010.
- [48] RFC 675. Disponível em <http://tools.ietf.org/html/rfc675>. Acesso em 27/Junho/2010.
- [49] Manuel Pereira Ricardo, "TCP". Disponível em http://paginas.fe.up.pt/~mricardo/09_10/pgre/slides/tcp-flow+congestion.pdf. Acesso em 27/Junho/2010.
- [50] Multi-Generator. Disponível em <http://cs.itd.nrl.navy.mil/work/mgen/index.php>. Acesso em 26/Junho/2010.
- [51] Wireshark. Disponível em http://wiki.wireshark.org/RTP_statistics. Acesso em 21/Junho/2010.
- [52] RFC3550. Disponível em <http://tools.ietf.org/rfcmarkup?rfc=3550&draft=&url=#section-6.4.1>. Acesso em 21/Junho/2010.
- [53] Axis. Disponível em <http://www.axis.com/corporate/press/pressrelease.php?pl=NDc5MDI1&f=aHR0cDovL2ZlZWQubmUuY2lzaW9uLmNvbS9jbGllbnQvYXhpcy8vQ29tbWFuZHMvRmlsZS5hc3B4P2lkPTExMDMyMzc=>. Acesso em 21/Junho/2010.
- [54] IANA. Disponível em <http://www.iana.com/assignments/port-numbers>. Acesso em 21/Junho/2010.
- [55] Wikipedia. Disponível em <http://pt.wikipedia.org/wiki/TCP/IP>. Acesso em 28/Junho/2010.

Anexo A - Tabelas dos resultados

Cenário 1

1 Cliente - Porta 1234

Tabela A.1 - Resultados cenário 1 / 1 cliente / porta 1234.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional	3,60	84,85	6,74	0	3,072
Com tráfego TCP adicional	3,55	75,61	6,76	0	3,072
Com tráfego UDP adicional	3,61	99,23	6,84	0	3,033

3 Clientes

Porta 1234

Tabela A.2 - Resultados cenário 1 / 3 clientes / porta 1234.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional	3,28	21,42	6,27	0,01	3,060
Com tráfego TCP adicional	4,7	130,15	8,10	0,22	3,006
Com tráfego UDP adicional	4,5	-161,38	7,65	0,18	3,012

Porta 2500

Tabela A.3 - Resultados cenário 1 / 3 clientes / porta 2500.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional	5,47	-189,75	6,15	0	2,975
Com tráfego TCP	5,78	-181,18	6,25	0	3,010

adicional

Com tráfego UDP adicional	4,30	-175,06	8,50	0,55	2,951
---------------------------	------	---------	------	------	-------

Porta 5004

Tabela A.4 - Resultados cenário 1 /3 clientes /porta 5004.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional	3,49	-108,23	5,84	0	3,004
Com tráfego TCP adicional	4,35	-176,23	6,80	0,08	3,020
Com tráfego UDP adicional	4,3	-189,89	7,43	1,19	2,963

Média dos 3 clientes [porta 1234, 2500 e 5004]

Tabela A.5 - Média dos 3 clientes no cenário 1.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional	4,08	106,47	6,09	0,003	3,013
Com tráfego TCP adicional	4,94	162,42	7,05	0,10	3,012
Com tráfego UDP adicional	4,37	175,44	7,86	0,64	2,975

Cenário 2 - Apenas IEEE 802.11

Norma a

1 Cliente - Porta 1234

Tabela A.6 - Resultados cenário 2 /norma a /1 cliente /porta 1234.

Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
----------------------	------------------	-----------------------	------------------------------	---------------------------

Sem tráfego adicional e sem QoS	3,28	65,33	5,97	0	3,056
Com tráfego TCP adicional e sem QoS	3,92	-54,11	5,02	0	3,018
Com tráfego UDP adicional e sem QoS	5,73	133,31	5,38	0	3,035
Sem tráfego adicional e com QoS	3,22	63,65	5,65	0	3,064
Com tráfego TCP adicional e com QoS	2,72	11,77	3,72	0	3,070
Com tráfego UDP adicional e com QoS	3,01	-114,75	4,24	0	3,068

3 Clientes

Porta 1234

Tabela A.7 - Resultados cenário 2 / norma a / 3 clientes / porta 1234.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	6,58	-134,26	7,66	0	3,057
Com tráfego TCP adicional e sem QoS	6,06	-101,24	10,91	0,17	3,005
Com tráfego UDP adicional e sem QoS	7,55	-165,82	12,97	1,2	3,000
Sem tráfego adicional e com QoS	6,55	122,31	7,55	0	3,068

QoS

Com tráfego TCP adicional e com QoS	7,12	96,22	8,64	0	3,012
-------------------------------------	------	-------	------	---	-------

QoS

Com tráfego UDP adicional e com QoS	5,38	-171,31	12,70	0	3,020
-------------------------------------	------	---------	-------	---	-------

QoS

Porta 2500

Tabela A.8 - Resultados cenário 2 /norma a /3 clientes /porta 2500.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	6,80	151,21	7,89	0	3,018
Com tráfego TCP adicional e sem QoS	4,90	-95,52	11,52	0,25	3,010
Com tráfego UDP adicional e sem QoS	7,93	-115,31	13,54	0	3,027
Sem tráfego adicional e com QoS	6,71	-100,53	7,96	0	3,060
Com tráfego TCP adicional e com QoS	5,32	61,50	6,88	0	3,030
Com tráfego UDP adicional e com QoS	7,26	-126,18	13,12	0	3,012

Porta 5004

Tabela A.9 - Resultados cenário 2 /norma a /3 clientes /porta 5004.

	Delta	Skew [ms]	Jitter	Perdas de	Débito
--	--------------	------------------	---------------	------------------	---------------

	[ms]		[ms]	Pacotes [%]	[Mbit/s]
Sem tráfego adicional e sem QoS	6,27	-143,28	7,56	0	3,061
Com tráfego TCP adicional e sem QoS	6,89	-149,89	7,01	1,11	2,976
Com tráfego UDP adicional e sem QoS	6,85	-142,26	11,78	0,8	3,015
Sem tráfego adicional e com QoS	7,51	136,62	12,98	0	3,053
Com tráfego TCP adicional e com QoS	6,97	112,12	7,74	0	3,016
Com tráfego UDP adicional e com QoS	5,13	-89,24	11,89	0	3,060

Média dos 3 clientes [porta 1234, 2500 e 5004]

Tabela A.10 - Média dos 3 clientes no cenário 2/ norma a.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	6,55	142,92	7,70	0	3,045
Com tráfego TCP adicional e sem QoS	5,95	115,55	9,81	0,51	2,997
Com tráfego UDP adicional e sem QoS	7,44	141,13	12,76	0,67	3,014
Sem tráfego adicional e com QoS	6,93	119,82	9,50	0	3,060

QoS

Com tráfego TCP 6,47 89,95 7,75 0 3,019
adicional e com

QoS

Com tráfego UDP 5,92 128,91 12,57 0 3,031
adicional e com

QoS

Norma g

1 Cliente - Porta 1234

Tabela A.11 - Resultados cenário 2 /norma g /1 cliente /porta 1234.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	3,63	12,01	6,41	0	3,020
Com tráfego TCP adicional e sem QoS	4,85	-105,22	7,08	0	3,007
Com tráfego UDP adicional e sem QoS	6,84	95,67	9,22	0	2,957
Sem tráfego adicional e com QoS	3,58	23,65	6,42	0	3,057
Com tráfego TCP adicional e com QoS	3,09	-167,94	5,27	0	3,069
Com tráfego UDP adicional e com QoS	4,52	-47,53	6,88	0	3,002

3 Clientes

Porta 1234

Tabela A.12 - Resultados cenário 2 /norma g /3 clientes /porta 1234.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	6,61	122,89	7,38	0	2,856
Com tráfego TCP adicional e sem QoS	8,21	-173,12	8,56	0,2	3,021
Com tráfego UDP adicional e sem QoS	9,37	-175,61	10,11	1,5	2,988
Sem tráfego adicional e com QoS	6,92	-171,2	8,22	0	3,011
Com tráfego TCP adicional e com QoS	7,13	-180,47	6,57	0	3,050
Com tráfego UDP adicional e com QoS	8,58	127,87	14,61	0	2,892

Porta 2500

Tabela A.13 - Resultados cenário 2 /norma g /3 clientes /porta 2500.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	6,70	-199,48	7,52	0	3,005
Com tráfego TCP adicional e sem QoS	7,09	-121,28	8,61	1,1	3,015
Com tráfego UDP adicional e sem QoS	12,56	100,26	16,73	1,0	2,998

Sem tráfego adicional e com QoS	6,69	155,51	7,87	0	3,008
Com tráfego TCP adicional e com QoS	8,12	-192,17	7,12	0	3,009
Com tráfego UDP adicional e com QoS	8,61	182,32	9,71	0	3,007

Porta 5004

Tabela A.14 - Resultados cenário 2 /norma g /3 clientes /porta 5400.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	6,67	-148,09	7,56	0	3,017
Com tráfego TCP adicional e sem QoS	6,41	-173,28	7,87	0	3,022
Com tráfego UDP adicional e sem QoS	8,61	179,71	11,30	1,4	2,988
Sem tráfego adicional e com QoS	7,12	-167,76	7,25	0	3,015
Com tráfego TCP adicional e com QoS	6,91	-182,81	7,59	0	3,048
Com tráfego UDP adicional e com QoS	7,67	127,17	8,94	0	3,001

Média dos 3 clientes [porta 1234, 2500 e 5004]

Tabela A.15 - Média dos 3 clientes no cenário 2/ norma g.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	6,66	156,82	7,49	0	2,959
Com tráfego TCP adicional e sem QoS	7,23	155,89	8,35	0,43	3,019
Com tráfego UDP adicional e sem QoS	10,18	151,86	12,71	1,3	2,991
Sem tráfego adicional e com QoS	6,91	164,82	7,78	0	3,011
Com tráfego TCP adicional e com QoS	7,39	185,15	7,09	0	3,036
Com tráfego UDP adicional e com QoS	8,29	145,79	11,09	0	2,966

Norma n

1 Cliente - Porta 1234

Tabela A.16 - Resultados cenário 2 /norma n /1 cliente /porta 1234.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	3,35	16,01	6,10	0	3,057
Com tráfego TCP adicional e sem QoS	3,89	13,42	5,28	0	3,010
Com tráfego UDP adicional e sem QoS	3,18	-33,86	6,11	0	3,070

QoS

Sem tráfego adicional e com QoS	3,35	86,07	5,90	0	3,071
Com tráfego TCP adicional e com QoS	3,05	14,20	5,76	0	3,012
Com tráfego UDP adicional e com QoS	4,22	21,67	6,83	0	3,068

3 Clientes

Porta 1234

Tabela A.17 - Resultados cenário 2 /norma n /3 clientes /porta 1234.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	4,97	64,10	7,00	0	3,010
Com tráfego TCP adicional e sem QoS	5,34	-57,01	5,28	0	3,023
Com tráfego UDP adicional e sem QoS	4,91	62,63	6,83	0	3,070
Sem tráfego adicional e com QoS	4,88	-79,75	7,24	0	3,010
Com tráfego TCP adicional e com QoS	6,59	-61,57	4,19	0	3,069
Com tráfego UDP adicional e com QoS	5,55	-93,21	7,94	0	3,040

Porta 2500

Tabela A.18 - Resultados cenário 2 /norma n /3 clientes /porta 2500.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	4,95	85,36	6,91	0	3,072
Com tráfego TCP adicional e sem QoS	5,35	-72,46	7,13	0	3,059
Com tráfego UDP adicional e sem QoS	6,10	100,45	7,32	0	3,010
Sem tráfego adicional e com QoS	4,95	72,81	6,75	0	3,068
Com tráfego TCP adicional e com QoS	5,04	-66,77	7,53	0	3.060
Com tráfego UDP adicional e com QoS	6,66	-83,92	8,30	0	3,025

Porta 5004

Tabela A.19 - Resultados cenário 2 /norma n /3 clientes /porta 5004.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	3,26	-62,75	5,13	0	3,061
Com tráfego TCP adicional e sem QoS	6,87	-68,05	7,26	0	3,006
Com tráfego UDP	3,76	123,46	5,37	0	3,061

adicional e sem QoS					
Sem tráfego	3,26	-66,54	5,16	0	3,065
adicional e com QoS					
Com tráfego TCP	6,42	-55,37	7,10	0	3,016
adicional e com QoS					
Com tráfego UDP	3,68	-89,36	6,65	0	3,055
adicional e com QoS					

Média dos 3 clientes [porta 1234, 2500 e 5004]

Tabela A.20 - Média dos 3 clientes no cenário 2/ norma n.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego	4,39	70,74	6,35	0	3,048
adicional e sem QoS					
Com tráfego TCP	5,85	65,84	6,56	0	3,029
adicional e sem QoS					
Com tráfego UDP	4,92	95,51	6,51	0	3,047
adicional e sem QoS					
Sem tráfego	4,36	73,03	6,38	0	3,048
adicional e com QoS					
Com tráfego TCP	6,02	61,24	6,27	0	3,048
adicional e com QoS					
Com tráfego UDP	5,30	88,83	7,63	0	3,044
adicional e com QoS					

Cenário 3

1 Cliente - Porta 1234

Tabela A.21 - Resultados cenário 3 / 1 cliente / porta 1234.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	3,47	-132,94	6,12	0	3,072
Com tráfego TCP adicional e sem QoS	3,63	150,67	6,37	0,1	3,046
Com tráfego UDP adicional e sem QoS	3,61	124,04	6,63	0	3,064
Sem tráfego adicional e com QoS	3,41	-47,80	3,65	0	3,072
Com tráfego TCP adicional e com QoS	3,58	-95,93	6,36	0	3,042
Com tráfego UDP adicional e com QoS	3,41	172,58	5,94	0	3,072

3 Clientes

Porta 1234

Tabela A.22 - Resultados cenário 3 / 3 clientes / porta 1234.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	3,37	39,50	6,62	0,37	2,958
Com tráfego TCP adicional e sem QoS	3,41	-3,09	7,92	0	3,005

QoS					
Com tráfego UDP adicional e sem QoS	3,52	76,26	8,04	0	3,030
Sem tráfego adicional e com QoS	3,43	-69,11	6,79	0	3,072
Com tráfego TCP adicional e com QoS	3,35	103,35	9,03	0	3,056
Com tráfego UDP adicional e com QoS	6,28	-180,84	5,79	0	3,072

Porta 2500

Tabela A.23 - Resultados cenário 3 /3 clientes /porta 2500.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	3,53	112,61	5,95	0	3,038
Com tráfego TCP adicional e sem QoS	3,55	-169,13	6,85	1,2	2,983
Com tráfego UDP adicional e sem QoS	3,50	-175,60	6,43	1,5	2,986
Sem tráfego adicional e com QoS	3,52	177,91	5,74	0	3,072
Com tráfego TCP adicional e com QoS	3,42	136,91	7,63	0	3,042
Com tráfego UDP adicional e com QoS	3,56	-132,84	5,62	0	3,072

QoS

Porta 5004

Tabela A.24 - Resultados cenário 3 /3 clientes /porta 5400.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	3,73	107,64	6,56	0	3,037
Com tráfego TCP adicional e sem QoS	3,41	131,11	6,74	0	3,010
Com tráfego UDP adicional e sem QoS	3,54	175,08	6,75	0	3,047
Sem tráfego adicional e com QoS	3,64	-193,06	6,78	0	3,072
Com tráfego TCP adicional e com QoS	3,38	103,80	6,76	0	3,050
Com tráfego UDP adicional e com QoS	3,55	-19,22	7,20	0	3,072

Média dos 3 clientes [porta 1234, 2500 e 5004]

Tabela A.25 - Média dos 3 clientes no cenário 3.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	3,54	86,58	6,38	0,12	3,011
Com tráfego TCP adicional e sem QoS	3,46	101,11	7,17	0,4	2,999

QoS					
Com tráfego UDP adicional e sem QoS	3,52	142,31	7,07	0,5	3,021
Sem tráfego adicional e com QoS	3,53	146,69	6,44	0	3,072
Com tráfego TCP adicional e com QoS	3,38	114,69	7,81	0	3,049
Com tráfego UDP adicional e com QoS	4,46	110,97	6,20	0	3,072

Cenário 4

1 Cliente - Porta 1234

Tabela A.26 - Resultados cenário 4 / 1 clientes / porta 1234.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	3,56	-89,52	4,72	0	3,070
Com tráfego TCP adicional e sem QoS	3,69	96,40	5,20	0	3,071
Com tráfego UDP adicional e sem QoS	3,28	160,80	5,37	0,28	2,940
Sem tráfego adicional e com QoS	4,11	-47,64	5,24	0	3,090
Com tráfego TCP adicional e com QoS	3,52	168,97	6,63	0	3,066
Com tráfego UDP adicional e com QoS	3,51	-83,83	6,50	0	3,046

QoS

3 Clientes

Porta 1234

Tabela A.27 - Resultados cenário 4 /3 clientes /porta 1234.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	3,51	-102,70	6,87	0	3,057
Com tráfego TCP adicional e sem QoS	3,54	157,74	6,48	0	3,069
Com tráfego UDP adicional e sem QoS	3,56	-160,34	7,28	2,2	2,892
Sem tráfego adicional e com QoS	3,48	106,61	6,88	0	3,044
Com tráfego TCP adicional e com QoS	3,33	-154,20	7,19	0	3,010
Com tráfego UDP adicional e com QoS	3,41	-145,28	6,28	0	3,019

Porta 2500

Tabela A.28 - Resultados cenário 4 /3 clientes /porta 2500.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	3,50	133,35	6,11	0	3,023
Com tráfego TCP	3,53	-88,59	6,98	0	3,060

adicional e sem QoS					
Com tráfego UDP adicional e sem QoS	3,43	-114,50	10,29	0,30	3,005
Sem tráfego adicional e com QoS	3,50	109,37	6,29	0	3,052
Com tráfego TCP adicional e com QoS	3,39	-167,21	11,24	0	3,072
Com tráfego UDP adicional e com QoS	3,65	-112,13	6,41	0	3,033

Porta 5004

Tabela A.29 - Resultados cenário 4 /3 clientes /porta 5004.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	3,43	-153,31	6,21	0	3,040
Com tráfego TCP adicional e sem QoS	3,30	-146,96	6,91	0	3,056
Com tráfego UDP adicional e sem QoS	3,44	63,01	7,50	0,02	3,020
Sem tráfego adicional e com QoS	3,56	-110,88	6,65	0	3,072
Com tráfego TCP adicional e com QoS	3,70	127,16	8,26	0	3,072
Com tráfego UDP adicional e com QoS	3,48	-101,72	7,12	0	3,063

QoS

Média dos 3 clientes [porta 1234, 2500 e 5004]

Tabela A.30 - Média dos 3 clientes no cenário 4.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	3,48	129,79	6,40	0	3,040
Com tráfego TCP adicional e sem QoS	3,46	131,10	6,79	0	3,062
Com tráfego UDP adicional e sem QoS	3,48	112,62	8,36	0,84	2,972
Sem tráfego adicional e com QoS	3,51	108,95	6,61	0	3,056
Com tráfego TCP adicional e com QoS	3,47	149,52	8,90	0	3,051
Com tráfego UDP adicional e com QoS	3,51	119,71	6,60	0	3,038

Cenário 5

1 Cliente - Porta 1234

Tabela A.31 - Resultados cenário 5 /1 cliente /porta 1234.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	5,30	-20,42	4,18	0,40	3,012
Com tráfego TCP	4,71	134,57	7,04	0,05	3,049

adicional e sem QoS					
Com tráfego UDP adicional e sem QoS	4,49	48,85	6,87	0	3,070
Sem tráfego adicional e com QoS	3,61	-98,48	4,73	0	3,072
Com tráfego TCP adicional e com QoS	3,44	157,23	6,33	0	3,067
Com tráfego UDP adicional e com QoS	3,56	-128,93	6,77	0	3,061

3 Clientes

Porta 1234

Tabela A.32 - Resultados cenário 5 /3 clientes /porta 1234.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	3,82	83,92	6,72	0	3,066
Com tráfego TCP adicional e sem QoS	3,65	169,07	7,84	0	3,058
Com tráfego UDP adicional e sem QoS	3,57	-165,52	7,09	0,93	2,989
Sem tráfego adicional e com QoS	3,53	71,16	6,19	0	3,072
Com tráfego TCP adicional e com QoS	4,93	13,25	9,41	0	3,026

Com tráfego UDP adicional e com QoS	3,55	-145,46	6,85	0	3,033
-------------------------------------	------	---------	------	---	-------

Porta 2500

Tabela A.33 - Resultados cenário 5 /3 clientes /porta 2500.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	4,57	158,19	5,99	0	3,011
Com tráfego TCP adicional e sem QoS	4,36	145,98	8,27	0,6	2,968
Com tráfego UDP adicional e sem QoS	3,76	120,34	6,42	1,5	2,959
Sem tráfego adicional e com QoS	3,52	85,24	7,06	0	3,059
Com tráfego TCP adicional e com QoS	3,44	-111,21	7,29	0	3,057
Com tráfego UDP adicional e com QoS	4,03	-123,75	8,85	0	2,999

Porta 5004

Tabela A.34 - Resultados cenário 5 /3 clientes /porta 5004.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	4,92	-139,78	7,36	0.04	2,976

Com tráfego TCP adicional e sem QoS	4,17	119,31	7,54	0	3,016
Com tráfego UDP adicional e sem QoS	3,36	-145,36	6,94	0	3,000
Sem tráfego adicional e com QoS	3,51	46,64	6,29	0	3,005
Com tráfego TCP adicional e com QoS	3,36	9,05	7,80	0	3,072
Com tráfego UDP adicional e com QoS	3,75	-153,88	7,31	0	3,015

Média dos 3 clientes [porta 1234, 2500 e 5004]

Tabela A.35 - Média dos 3 clientes no cenário 5.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	4,44	127,30	6,69	0	3,018
Com tráfego TCP adicional e sem QoS	4,06	144,79	7,88	0,2	3,014
Com tráfego UDP adicional e sem QoS	3,56	143,74	6,82	0,81	2,983
Sem tráfego adicional e com QoS	3,52	67,68	6,51	0	3,045
Com tráfego TCP adicional e com QoS	3,91	44,54	8,17	0	3,052

Com tráfego UDP adicional e com QoS	3,78	141,03	7,67	0	3,016
-------------------------------------	------	--------	------	---	-------

Cenário 6

1 cliente - Porta 1234

Tabela A.36 - Resultados cenário 6 / 1 cliente / porta 1234.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional	3,79	-84,69	5,86	0	3,066
Com tráfego TCP adicional	3,96	-98,96	6,14	0,5	3,042
Com tráfego UDP adicional	6,35	-155,84	8,75	6,23	2,799

3 clientes

Porta 1234

Tabela A.37 - Resultados cenário 6 / 3 clientes / porta 1234.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional	3,58	-103,64	6,46	0	3,033
Com tráfego TCP adicional	6,67	-158,52	8,48	1,2	2,962
Com tráfego UDP adicional	8,65	-189,55	22,51	7,12	2,764

Porta 2500

Tabela A.38 - Resultados cenário 6 / 3 clientes / porta 2500.

	Delta	Skew	Jitter	Perdas de	Débito
--	--------------	-------------	---------------	------------------	---------------

	[ms]	[ms]	[ms]	Pacotes [%]	[Mbit/s]
Sem tráfego adicional	3,53	-172,45	7,36	0	3,001
Com tráfego TCP adicional	6,94	-122,55	9,11	0,8	2,985
Com tráfego UDP adicional	10,03	-171,63	23,12	4,10	2,812

Porta 5004

Tabela A.39 - Resultados cenário 6 /3 clientes /porta 5004.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional	3,68	-183,99	6,06	0	3.029
Com tráfego TCP adicional	6,66	-86,57	8,13	0	3,020
Com tráfego UDP adicional	9,77	-192,15	25,66	9,11	2,637

Cenário 7

1 Cliente - Porta 1234

Tabela A.40 - Resultados cenário 7 /1 cliente /porta 1234.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	3,33	-93,12	6,44	0	3,060
Com tráfego TCP adicional e sem QoS	3,58	-95,99	7,01	1,0	3,002
Com tráfego UDP adicional e sem QoS	5,94	-122,82	8,13	5,9	2,869
Sem tráfego	3,48	-89,32	5,98	0	3,061

adicional e com

QoS

Com tráfego TCP	3,71	-102,22	6,56	0	3,044
-----------------	------	---------	------	---	-------

adicional e com

QoS

Com tráfego UDP	3,74	-113,95	6,94	0,28	3,027
-----------------	------	---------	------	------	-------

adicional e com

QoS

3 Clientes

Porta 1234

Tabela A.41 - Resultados cenário 7 /3 clientes /porta 1234.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego	4,11	-112,12	6,99	0,3	3,008
adicional e sem					
QoS					
Com tráfego TCP	6,21	-119,19	8,15	0,9	2,997
adicional e sem					
QoS					
Com tráfego UDP	10,02	-189,23	28,52	9,1	2,612
adicional e sem					
QoS					
Sem tráfego	3,48	-77,18	5,88	0	3,059
adicional e com					
QoS					
Com tráfego TCP	5,88	-122,45	6,91	0	3,050
adicional e com					
QoS					
Com tráfego UDP	6,12	-142,71	7,12	0,2	3,008
adicional e com					
QoS					

Porta 2500

Tabela A.42 - Resultados cenário 7 / 3 clientes / porta 2500.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	3,72	-100,02	6,12	0	3,012
Com tráfego TCP adicional e sem QoS	6,85	-166,73	8,91	1,1	2,986
Com tráfego UDP adicional e sem QoS	9,53	-151,51	25,13	6,6	2,713
Sem tráfego adicional e com QoS	3,67	-102,91	5,91	0	3,057
Com tráfego TCP adicional e com QoS	5,81	-91,72	5,82	0	3,010
Com tráfego UDP adicional e com QoS	5,88	-115,01	6,54	0	3,012

Porta 5004

Tabela A.43 - Resultados cenário 7 / 3 clientes / porta 5004.

	Delta [ms]	Skew [ms]	Jitter [ms]	Perdas de Pacotes [%]	Débito [Mbit/s]
Sem tráfego adicional e sem QoS	3,38	-144,21	7,01	0	3,010
Com tráfego TCP adicional e sem QoS	6,83	-129,12	9,28	1,9	2,918
Com tráfego UDP adicional e sem QoS	9,62	-171,56	31,12	7,2	2,697
Sem tráfego	3,50	-35,92	6,12	0	3,043

adicional e com

QoS

Com tráfego TCP	6,12	-142,45	7,10	0,1	3,005
-----------------	------	---------	------	-----	-------

adicional e com

QoS

Com tráfego UDP	6,45	-33,98	6,99	0,3	3,000
-----------------	------	--------	------	-----	-------

adicional e com

QoS

Anexo B - Comportamento CPU

A figura 8.1 mostra o desempenho do CPU quando estavam 3 *streams* a ser enviados ao mesmo tempo do mesmo computador. Como se vê na imagem, o CPU atinge os 100% de utilização mantendo-se assim, o que prejudicaria os testes. Esta é a razão da utilização de 2 computadores quando foi necessário enviar 3 *streams* de vídeo.

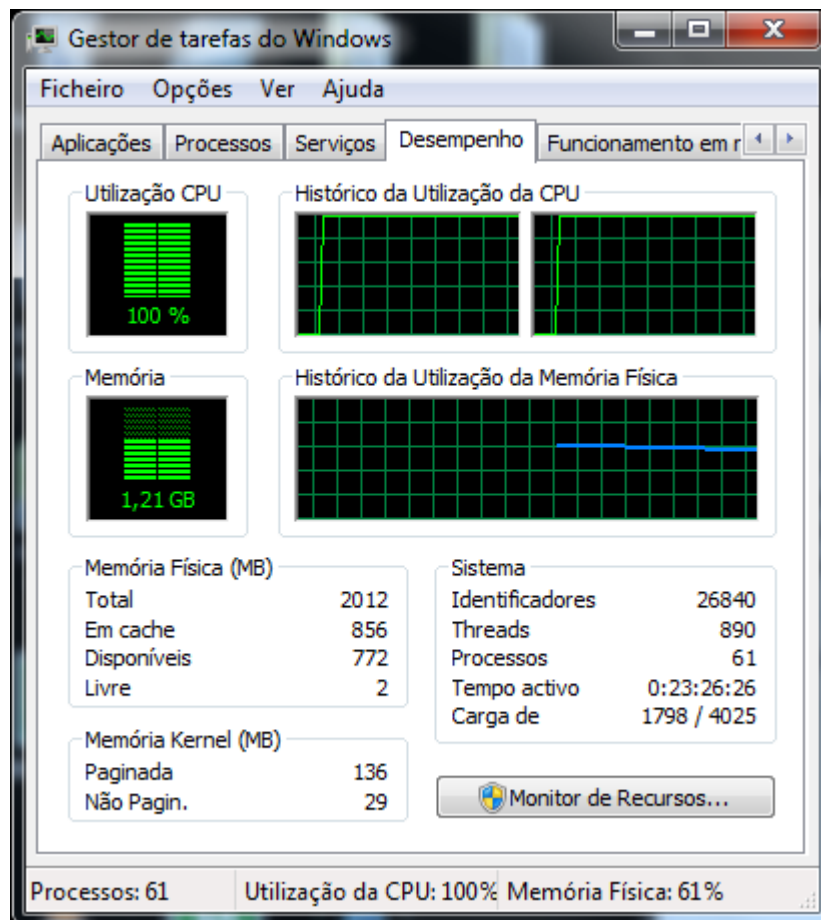


Figura B.1 - Desempenho CPU com 3 *streams* de vídeo.

