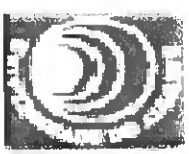
MESTRADO DE ENGENHARIA DE SISTEMAS E COMPUTAÇÃO

Protocolos de Acesso ao Meio em Redes Locais Não Cabladas

Autora:
Cidália Maria Leal Paço



Faculdade de Ciências e Tecnologias
UNIVERSIDADE DO ALGARVE
FARO – PORTUGAL
2001

MESTRADO DE ENGENHARIA DE SISTEMAS E COMPUTAÇÃO

Protocolos de Acesso ao Meio em Redes Locais Não Cabladas

Autora:
Cidália Maria Leal Paço

Faculdade de Ciências e Tecnologias
UNIVERSIDADE DO ALGARVE
FARO – PORTUGAL
2001

Cidália Maria Leal Paço

Protocolos de Acesso ao Meio em Redes Locais Não Cabladas

Dissertação realizada sob a orientação da Profª Doutora Maria do Carmo de Medeiros, para obtenção do grau de Mestre em Engenharia de Sistemas e Computação.

Faculdade de Ciências e Tecnologias
UNIVERSIDADE DO ALGARVE
FARO – PORTUGAL
2001

2794 T.

DECLARAÇÃO DE ORIGINALIDADE

Em cumprimento do disposto na alínea b) do nº 2 do artigo 5º do Decreto-Lei nº216/92 de 13 de Outubro, Cidália Maria Leal Paço declara que todo o trabalho desenvolvido na presente dissertação é da sua autoria.

Mestrando

Cidália Maria Leal Paço

(Cidália Maria Leal Paço)

Orientador

Maria do Carmo Raposo de Medeiros

(Profª Doutora Maria do Carmo Raposo de Medeiros)

Aos meus pais e, de modo especial, ao João Maria

MENÇÃO DE APOIO

Este trabalho foi apoiado financeiramente pela Estrutura de Apoio Técnico PRODEP III, Medida 5 – Acção 5.2, Concurso Público nº2/PRODEP/98 do Ministério da Educação.

AGRADECIMENTOS

A realização desta dissertação não teria sido possível sem o apoio de um conjunto de pessoas e Entidades às quais quero manifestar os meus sinceros agradecimentos. Começo por referir a Profª Maria do Carmo de Medeiros pela orientação, motivação para a área e empenho que manifestou durante a realização deste trabalho. Aos meus colegas do Núcleo da ESGHT que me apoiaram e compreenderam a minha ausência. Aos elementos do Conselho Directivo da ESGHT pelo apoio manifestado. Aos meus amigos pelo carinho das horas difíceis. Um obrigado muito especial aos meus pais, eles saberão porquê.

Agradeço ainda à Escola Superior de Gestão Hotelaria e Turismo da Universidade do Algarve pelo facto de ter apostado em mim.

RESUMO

A comunicação é uma das maiores necessidades da sociedade humana desde os primórdios da sua existência. Os avanços das comunicações nos últimos anos, tornaram possível o aparecimento de várias tecnologias que, desde então, tentam responder ás necessidades dos utilizadores com a melhor qualidade possível. Actualmente, as empresas e particulares estão a apostar numa das mais recentes e revolucionárias tendências da tecnologia: a comunicação sem fios (*wireless*).

A tecnologia de redes de área local sem fios, WLANs (*Wireless* LANs) tornou-se, rapidamente, numa componente crucial das redes de computadores e a sua utilização cresceu exponencialmente. Graças à finalização do standard para redes de área local sem fios, IEEE 802.11 e às suas actualizações mais recentes IEEE 802. 11a e IEEE 802.11b, a tecnologia sem fios emergiu do mundo de implementações proprietárias para se tornar uma solução aberta para o fornecimento de mobilidade, bem como os serviços de rede essenciais onde as instalações de cabos se manifestaram impraticáveis.

O presente trabalho enquadra-se no domínio científico das redes de comunicação de área local sem fios. Esta dissertação baseia-se no standard IEEE 802.11, complementado pela recente actualização IEEE 802.11b, para analisar, planear e implementar redes móveis locais, com ênfase especial para o protocolo de acesso ao meio.

Introdutoriamente é apresentada a evolução dos sistemas de comunicação, os diferentes tipos de rede de área local sem fios e é feita uma comparação entre as duas tecnologias de suporte (rádio frequência e infravermelhos). São também mencionados os principais organismos que desenvolvem actividades de normalização para este tipo de redes.

O protocolo de acesso ao meio é uma das funcionalidades implementadas pela camada MAC. São descritos os principais protocolos de acesso ao meio para redes de comunicação de área locais sem fios bem como as funções associadas. Em último lugar é estudado o comportamento de uma rede de área local sem fios em termos de escalabilidade e na presença de erros, implementada segundo a norma IEEE 802.11b, onde a camada MAC usa o protocolo CSMA/CA (*Carrier Sense Multiple Access / Collision Avoidance*) e a função DCF (*Distribute Coordination Function*) com tramas ACK e camada física usa modulação DSSS (*Direct Sequence Spread Spectrum*) a 11 Mbps.

PALAVRAS CHAVE: redes de comunicação de área local sem fios, protocolo de acesso ao meio, camada MAC, Norma IEEE 802.11, Norma IEEE 802.11b.

ABSTRACT

The communication is one of the greatest needs of human society since its origin. The communication advances over the last years are behind the new technologies responsable to respond to users needs with the best quality as possible. Nowadays the enterprises and individuals are reliyng on one of the most recent and challenging technology: the wireless communication.

The wireless network technology of local scope (WLAN, *Wireless Local Area Network*) has quickly become a crucial element of modern computer networks and its expansion has increased almost exponentially. Thanks to modern versions of the IEEE 802.11 standard for wireless local area networks – IEEE 802.11*a* and IEEE 802.11*b* – the wireless technology has emerged from the world of proprietary software to become the opened solution for better mobility and for essential network services where the use of cables is not feasible.

The present work fits on the scientific domain of wireless local area networks. This dissertation is based on the IEEE 802.11 standard, mainly on its recent version IEEE 802.11*b* to analyse, plan and implement local mobile networks with a special focus on the medium access protocol.

Initially it presents the communication systems evolution and the different types of wireless local area networks. Then it compares the two main support technologies (radio-frequency and infrareds). It also mentions the principal institutions that develop the normalisation process of this kind of networks.

The medium access protocol is one of the functions that is implemented on the MAC layer. It then describes the main medium access protocols for wireless local area networks and their functions.

At last, it studies the behaviour of a wireless local area network on the subject of its scalability and related errors, using standards IEEE 802.11 and IEEE 802.11*b* for its implementation, where the MAC layer uses the CSMA/CA protocol (*Carrier Sense Multiple Access width Collision Avoidance*) and the a DCF function (*Distribute Coordination Function*) with the ACK frames and where the physical layer uses DSSS modulation (*Direct Sequence Spread Spectrum*) at 11 Mbps throughput.

KEYWORDS: Wireless Local Area Networks (WLANs); Medium Access Protocol; MAC Layer; IEEE 802.11 and IEEE 802.11*b* Standards.

INDICE

INDICE DE ILUSTRAÇÕES

ACRÓNIMOS E ABREVIATURAS

ACK	Acknowledgment Frame
AP	Access Point
BER	Basic Error Ratio
BPSK	Binary Phase Shift Keying
BSS	Basic Service Set
BSSID	Basic Service Identifier
CDMA	Code Division Multiple Access
CF	Contention Free
CF-End	Contention-free End
CFP	Contention-free Period
CF-Poll	Contention-free Poll
CP	Contention Period
CRC	Cyclic Redundancy Check
CS	Carrier Sense
CSMA	Carrier Sense Multiple Access
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CTS	Clear To Send
CW	Contention Window
DA	Destination Address
dB	Decibels
DBPSK	Differential Binary Phase Shift Keying
DCF	Distributed Coordination Function
DIFS	Distributed Inter-Frame Space
DPSK	Differential Phase Shift Keying
DQPSK	Differential Quadrature Phase Shift Keying
DS	Distribution System
DSSS	Direct Sequence Spread Spectrum
EIFS	Extended Inter-Frame Space
ESS	Extended Service Set
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FCS	Frame Check Sequence
FHSS	Frequency Hopping Spread Spectrum
GFSK	Gaussian Frequency Shift Keying
HR/DSSS	High Rate Sequence Spread Spectrum
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers

IR	Infrared
ISI	Intersymbol Interference
ISM	Industrial, Scientific and Medical
ISO	International Standards Organization
LAN	Local Area Network
LED	Light Emitting Diode
LLC	Logical Link Control
MAC	Medium Access Control
MAN	Metropolitan Area Network
MIB	Management Information Base
MMPDU	MAC Management Protocol Data Unit
MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit
NAV	Network Allocation Vector
NIC	Network Interface Card
OSA	Open System Authentication
OSI	Open System Interconnection
PC	Point Coordinator
PCF	Point Coordination Function
PCMCIA	Personal Computer Memory Card International Association
PDU	Protocol Data Unit
PHY	Physical, Physical Layer
PIFS	Priority Inter-Frame Space
PLCP	Physical Layer Convergence Procedure
PLME	Physical Layer Management Entity
PMD	Physical Medium Dependent
PN	Pseudo Noise (code sequence)
PPDU	PLCP Protocol Data Unit
PPM	Pulse Position Modulation
PSDU	PLCP Service Data Unit
QPSK	Quadrature Phase Shift Keying
RA	Receiver Address
RF	Radio Frequency
RTS	Request To Send
SA	Source Address
SAP	Service Access Point
SIFS	Short Inter-Frame Space
SNR	Signal to Noise Ratio
SSID	Service Set Identity
STA	Station

TA	Transmitter Address
TCP	Transmission Control Protocol
TIM	Traffic Indication Map
TSF	Timer Synchronization Factor
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless LAN

CAPITULO I
INTRODUÇÃO

Este capítulo apresenta o contexto, objectivo e a organização da dissertação.

I.1. Contexto da dissertação

O progresso e necessidade da computação móvel tem, de algum modo, obrigado as empresas a encararem alternativas para os tradicionais meios de transmissão de dados. A utilização, por exemplo, de rádio para interligar redes locais (LANs) ou regionais (WANs) tem ganho terreno na medida em que a tecnologia tem avançado e oferecido mais recursos, tendo como um dos principais resultados o aparecimento constante de soluções sem fios (*wireless*).

Esta tecnologia tem-se apresentado como a solução ideal para problemas distintos, como a permuta de informação entre redes situadas em edifícios distantes ou redes instaladas na mesma localização; pôr fim à confusão de fios quando se instala uma rede de micro-computadores, ou ainda, auxiliar na necessidade de informação requerida por alguns profissionais que têm que se deslocar do seu posto de trabalho, conquistando a mobilidade oferecida pelo modem portátil sem fios.

Desde a implementação da telefonia celular, que o crescimento das comunicações sem fios tem vindo a aumentar rapidamente. Vários sistemas têm surgido, não apenas de telecomunicações como o telefone móvel, mas também no segmento de redes como forma de interligação de LANs e WANs. A partir da introdução das comunicações sem fios no mercado, em meados de 1990, que a popularidade desta tecnologia de transmissão de dados tem vindo a crescer exponencialmente [1]. O aparecimento e crescimento contínuo das redes sem fios foi motivado pela necessidade de baixar os custos associados às infra-estruturas das redes cabladas e dar suporte a aplicações de redes móveis, as quais oferecem ganhos em termos de eficiência do processo, precisão e custos menores [27].

No que diz respeito aos utilizadores, a mobilidade permite que se desloquem fisicamente enquanto usam uma aplicação por meio de um PC manuseável ou um colector de dados (*data collector*). Exemplos destes são responsáveis por stocks e inventários, trabalhadores de serviços da área de saúde em termos hospitalares, agentes de policia e especialistas em cenários de emergência.

Em termos de aplicações móveis, que requerem ligação sem fios, podemos incluir todas aquelas que dependam do acesso a dados em tempo real, modo geral armazenados em Bases de Dados centralizadas. Assim, se uma aplicação requerer utilizadores móveis, os quais devam ter acesso imediato a alterações efectuadas aos dados ou, se por outro lado a informação disponibilizada no sistema deva ser imediatamente disponibilizada a terceiros, estamos, sem dúvida, na presença de um cenário com necessidade de uma rede sem fios. Podemos, deste modo, afirmar que a interligação ou utilização de redes sem fios aplica-se a todos os sectores, nos quais exista a necessidade de utilização de computação móvel ou quando a instalação física de meios cablados não seja viável.

Actualmente, como cenários onde as redes de área local sem fios são usadas, podemos referir a interligação de edifícios distantes, bancos, hospitais, lojas e até em provas de corridas de automóveis, ou seja desde instalações permanentes a temporárias. Nestes cenários, elas tornaram-se tão comuns quanto os telefones sem fios.

Em termos de vantagens a interligação de dispositivos portáteis, com conectividade sem fios, a uma base de dados comum e aplicações especificas satisfaz, entre outros requisitos, a necessidade de mobilidade, elimina a dependência de papéis, diminui possíveis erros e reduz os custos inerentes ao processo melhorando, deste modo, a eficiência geral do processo. A alternativa a este cenário é a execução manual de tarefas a qual é um processo lento, muito mais susceptível a erros e notoriamente inferior.

Em suma podemos afirmar de modo peremptório, que a globalidade das comunicações sem fios possibilitam o próximo passo na evolução dos ambientes computacionais, nos quais os recursos informáticos poderão ser utilizados com mais flexibilidade, pois os utilizadores deixarão de ter necessidade de estar conectados fisicamente (através de fios) a uma rede.

No domínio das redes locais, objecto desta dissertação, a rápida evolução do equipamento informático portátil e a sua utilização cada vez mais frequente conduziu a necessidades de comunicação que levaram ao desenvolvimento de uma nova geração de redes de área local sem fios. O objectivo primordial desta nova geração de redes é o de satisfazer os requisitos dos utilizadores de equipamento informático caracterizado por portabilidade, computação em movimento e baixo consumo de potência. Assim este tipo de redes permite não só o acesso nómada a redes já existentes, mas também a possibilidade de estabelecimento de grupos Ad Hoc de comunicação entre utilizadores de computadores portáteis durante períodos temporários.

Nas redes de área local sem fios as comunicações processam-se em espaço livre, podendo ser usadas duas tecnologias de transmissão: infravermelhos ou rádio frequência. A utilização de uma ou outra depende, sobretudo, do ambiente do meio de propagação e da aplicação.

Independentemente da tecnologia de transmissão utilizada, uma rede deste tipo deverá satisfazer os seguintes requisitos: assegurar transmissões robustas e seguras mesmo em ambiente ruidosos; ser de fácil instalação e operação não sujeita a licenciamento; interligar equipamento caracterizado por consumos de potência reduzidos; permitir a sobreposição de redes, possibilitando a existência de mais do que uma rede na mesma área geográfica a operar num mesmo canal de transmissão; permitir a utilização do mesmo equipamento em diferentes países e garantir salvaguarda do investimento permitindo evoluções futuras [27].

O cumprimento de alguns destes requisitos e a coexistência dos dois tipos de redes, cablada e sem fios, levanta o problema da compatibilidade e motiva o surgimento de normas para as novas redes. No início da década de 90 surgiram os primeiros trabalhos desenvolvidos com este intuito. Actualmente, as actividades de normalização desenvolvem-se na Europa, Japão e Estados Unidos.

Na Europa o organismo responsável pelas actividades de normalização é o ETSI (*European Telecommunications Standard Institute*) através de um standard denominado HIPERLAN. No Japão o estabelecimento de normas é, principalmente, da responsabilidade dos organismos RCR (*Research and Development Center for Radio Systems*), em parceria com outros. Nos Estados Unidos o organismo IEEE (*Institute of Electric and Electronics Engineers*) desempenha um papel relevante no estabelecimento de normas no domínio das redes de comunicação de área local através de comité IEEE 802. Exemplos são as normas, existentes para redes cabladas, nomeadamente a rede Ethernet (IEEE802.3), a rede Token Bus (IEEE802.4) e a rede Token Ring (IEEE802.5).

No domínio das redes de área local sem fios os primeiros esforços do IEEE foram realizados, em 1987, no interior do grupo IEEE 802.4. Em 1990 foi criado um grupo autónomo para levar a cabo a especificação de uma norma para redes sem fios, denominado IEEE 802.11. A comissão IEEE responsável pelo standard aprovou-o em 26/Jun/1997 e o IEEE publicou-o em 18/Nov/1997 [27]. A norma [35], denominada IEEE 802.11 (*Wireless* LAN), cobre todos os aspectos da camada física e camada MAC. Especialmente por limitações ao nível da velocidade de operação das várias camada físicas (1 e 2 Mbps) a norma foi revista e melhorada, tendo sido aprovadas as alterações denominadas IEEE 802.11a [37] e IEEE 802.11b [36] que foram ratificadas em Setembro de 1999, as quais apenas introduziram alterações ao nível da camada física.

Tanto na Europa como no Japão as normas dão preferência à utilização da tecnologia rádio frequência e apenas a norma IEEE 802.11 contempla uma solução integrada em que uma mesma

camada MAC pode ser utilizada por diversas camadas físicas, implementadas usando rádio frequência ou infravermelhos.

1.2. Objectivo da dissertação

O presente trabalho tem como objectivo o estudo e implementação de protocolos de acesso em redes de área local sem fios. A autora teve como motivação para a realização desta dissertação o facto de considerar esta uma solução extremamente útil e inovadora, face à sua experiência profissional em redes locais, e pelas dificuldades que se lhes foram levantadas na implementação das mesmas em cenários onde, por um lado, a passagem de cabos era extremamente difícil, dispendiosa e morosa e por outro lado a mobilidade era uma exigência. Por outro lado uma vertente de alguma importância diz respeito à interligação de edifícios distantes.

Assim, pretendemos com este trabalho analisar e tecer conclusões sobre o acesso ao meio nas rede locais sem fios em termos de escalabilidade e na presença de erros, que sabemos serem muito frequentes nestes cenários. Foi nosso objectivo efectuar um estudo, que foi feito recorrendo ao uso de um simulador, não tecer demasiada teorização nem modelização matemática do problema mas sim realizar um trabalho de síntese, com base no qual qualquer um com interesse na área possa de forma prática e objectiva inteirar-se daquilo que de mais recente existe em termos de standarização bem como os prós e contras associados ao uso desta tecnologia. Assim, pelas conclusões do nosso estudo pensamos ter realizado um trabalho que pode motivar qualquer interessado na área a tomar uma decisão fundamentada e a enveredar pela utilização de uma solução tendo como base uma WLAN.

1.3. Organização da dissertação

Esta dissertação divide-se em sete capítulos, que abordam a temática das redes de comunicação de área local sem fios.

O Capitulo I apresenta o contexto, objectivo e organização da presente dissertação.

O Capitulo II ilustra a aplicação das tecnologias sem fios na vida quotidiana e sua aplicação a redes de área local sem fios.

O Capitulo III aborda aspectos relativos às tecnologias de transmissão.

O Capitulo IV descreve os protocolos de acesso ao meio para redes de área local sem fios, distinguindo entre acesso com e sem contenção. Por último é feita uma análise qualitativa dos mesmos.

O Capitulo V descreve os principais atributos e especificações da norma IEEE 802.11, enquanto padrão de standarização para redes de área local sem fios.

O Capítulo VI descreve, de modo aprofundado, a camada MAC de rede sem fios IEEE 802.11. Assim são abordadas as funções: protocolo de acesso ao meio, fragmentação e gestão bem como as funções que asseguram o transporte da informação através da rede.

O Capitulo VII, que é um caso de estudo, descreve a simulação de uma rede WLAN IEEE 802.11 aplicada a um cenário em particular recorrendo ao COMNET III. Com base nesta é feita uma análise da performance da rede em termos de erros e escalabilidade. Por último são apresentadas as conclusões do estudo efectuado.

CAPITULO II
FUNDAMENTOS DE COMUNICAÇÕES SEM FIOS

Este capitulo visa ilustrar a aplicação das tecnologias sem fios na vida quotidiana, particularmente quais os serviços disponibilizados por meio deste tipo de conectividade. Posteriormente é analisada a natureza competitiva das ofertas e em último lugar é abordada a aplicação desta tecnologia em redes de comunicação de área local sem fios.

II.1. Abordagem histórica das comunicações sem fios

Desde os tempos das civilizações mais antigas que várias formas de comunicação tiveram lugar sem tirar vantagem da conectividade física, a titulo ilustrativo podemos referir-nos ás tribos primitivas, nas quais os tambores foram o primeiro meio para comunicação sem fios à distância. Na maioria das situações estas apenas conseguiam percorrer distâncias limitadas, e então tornavam-se necessários vários pontos de retransmissão. Este era um processo rudimentar mas que, no entanto, funcionava. Poderemos ainda citar, como exemplo, as tribos nativas americanas que usavam sinais de fumo como forma de comunicação a curtas distâncias. Esta debatia-se com vários problemas de natureza técnica, se assim lhe poder-mos chamar, como as limitações de distância, o facto de serem baseadas na linha dc visão, terem um alfabeto limitado e introdução de erros causados pela dissipação do fumo.

No entanto o início da grande revolução das telecomunicações deveu-se a Guglielmo Marconi que, em 1894, demonstrou a telegrafia sem fios ou seja rádio. Até 1910 as ondas rádio foram usadas essencialmente para a transmissão de sinais telegráficos. Porém com a invenção em 1907, por De Forest, da válvula termoionica, tornou-se possível a geração e modulação de portadoras eléctricas e a rádio telefonia começou a dar os primeiros passos. Surgiam assim os sistemas baseados em rádio. Progressos tecnológicos nesta área permitiram estabelecer, em 1914, um serviço transatlântico de telegrafia sem fios e realizar, em 1926, a primeira ligação entre os Estados Unidos e a Inglaterra.

Deveu-se a Sir William Herschel a descoberta da luz infravermelha, em 1800, quando separou a luz solar nas suas componentes cromáticas com o auxilio de um prisma [27]. Este observou que a maior parte do calor, presente no feixe, caia numa região do espectro onde não existia luz visível, justamente além do vermelho. No Sec XIX, feixes de luz eram usados em comunicações de curta distância, particularmente em contexto militar. Assim, mensagens verdadeiramente detalhadas, podiam ser transmitidas através de uma sequência codificada (Código Morse) de

cortes de luz do emissor para o receptor. Mais uma vez, esta forma de comunicação é efectivamente limitada pela distância e recepção não autorizada de informação.

Em termos evolutivos, podemos apontar a disponibilização de díodos laser de baixa potência, como o factor que abriu inúmeras possibilidades de produção de *links* de comunicação por luz infravermelha de custo aceitável para curtas distâncias, os quais foram de encontro às necessidades de transporte de voz, dados, vídeo e mais recentemente o trafego de redes de comunicação de área local. Os sistemas baseados em luz tornaram-se, deste modo, um outro sistema de transmissão sem fios, fiável e pouco dispendioso, mas apesar disso menos popular que os sistemas de rádio frequência.

A primeira ideia de redes sem fios foi desenvolvida na Universidade do Hawai, onde existia um sistema telefónico que não supria as necessidades [20]. Como as ilhas do arquipélago ficavam relativamente distantes os investigadores resolveram desenvolver um sistema de transmissão que não necessita-se de cabos, surgindo então as redes sem fios. Este sistema permitiu que computadores localizados em sete campos, espalhados por quatro ilhas, comunicassem com o computador central, em Oahu, sem utilizar as linhas telefónicas existentes pouco fiáveis e dispendiosas. Esta rede oferecia comunicações bidireccionais, segundo uma topologia em estrela, entre o computador central e cada uma das estações remotas.

A utilização comercial de redes sem fios ocorreu em 1985, quando a FCC (*Federal Communications Commission*) procedeu ao desenvolvimento comercial de componentes rádio para redes de área local, o qual foi possível devida à autorização de uso público das bandas ISM (*Industrial, Scientific and Medical*), da qual falaremos em mais detalhe posteriormente nesta dissertação. A banda ISM foi, e continua a sê-lo até ao presente, bastante atractiva para os fabricantes de produtos para redes sem fios, porque fornece uma parcela do espectro na qual podem basear os seus produtos e os utilizadores finais não tiveram que requer licenças de operação à FCC. A sua alocação teve um efeito avassalador na industria, promovendo o desenvolvimento de componentes para redes de área local sem fios. A não existência, contudo, de uma norma standard levou a que os fabricantes enveredassem por placas rádio e pontos de acesso proprietários.

Com o intuito de suprir esta lacuna no final dos anos 80, o grupo de trabalho IEEE 802, responsável pelo desenvolvimento de standards para redes de área local como Ethernet e Token Ring, iniciou o desenvolvimento da norma standard para redes de área local sem fios [27]. Sob a presidência de Vic Hayes, um engenheiro da NCR, o grupo de trabalho IEEE 802.11 desenvolveu as especificações da Camada MAC e da Camada Física para redes sem fios. A sua

finalização, em 1997, incentivou os fabricantes a criarem placas rádio e pontos de acesso compatíveis com a norma IEEE 802.11 [35].

II.1.1. Aplicabilidade das comunicações sem fios a redes locais

Com alguma frequência as empresas deparam-se com dificuldades técnicas ao tentarem instalar redes de comunicação de dados através de uma solução que use cabos. É o caso, por exemplo, de instalações nas quais exista uma rua que separe edifícios ou que estes sejam distantes. Neste cenário a empresa é obrigada a alugar uma linha telefónica, dedicada ou outra, ou a realizar um grande investimento em fios e cabos.

Um rede local sem utilização de cabos, conhecida internacionalmente como *Wireless* LAN (WLAN), é um sistema de transmissão de dados sem fios flexível que pode ser usado como alternativas ás redes cabladas recorrendo à tecnologia rádio frequência e/ou infravermelhos. São inúmeros os cenários onde este tipo de conectividade pode ser usada desde instalações de caracter temporário até instalações permanentes.

De entre as vantagens genéricas de uma rede sem fios, podemos enumerar as seguintes: capacidade para transpor porções de água como lagos ou rios, nas quais os cabos poderiam requerer tratamento especial para prevenir infiltrações no cobre condutor; capacidade para ultrapassar obstáculos de transmissão causados por montanhas e vales profundos, nos quais os custos de cablagem constituiriam uma limitação para a sua instalação, acrescidos de uma manutenção difícil; capacidade para transpor as conexões básicas das Companhias Telefónicas Locais. Para além das vantagens, já mencionadas, os sistemas que utilizam infravermelhos, apresentam: imunidade às interferências das frequências rádio (RFI) ou electromagnéticas (EMI); tecnologia mais segura do que a baseada em rádio; não exigem licenciamento e têm a capacidade de atravessar caminhos idênticos sem que isso cause interferência [33].

Actualmente, a maioria dos utilizadores estão familiarizados com técnicas de transmissão sem fios, embora possam não a utilizar. Temos, provavelmente, usado durante anos dispositivos de sinalização infravermelha como, por exemplo, controles remotos de TV, vídeos, rádios, luzes e outras aplicações. Nestes, quando premimos um botão, um código correspondente é modulado num sinal de luz infravermelha o qual é transmitido para o dispositivo que executará a função nele aplicada. Estes controladores de baixa potência têm aplicações bastante limitadas mas possuem todas as propriedades das transmissões por infravermelhos, apenas podendo ser usados para curtas distâncias e são altamente direccionados (ponto a ponto).

Se pretendermos comparar as duas técnicas, a luz infravermelha está, modo geral, sujeita a limitações mais especificas do que a tecnologia rádio frequência, das quais podemos referir: distâncias de transmissão inferiores a 2 quilómetros; limitações de linha de visão; larguras de banda restritas; predisposição para distúrbios no ambiente; perturbações causadas por nevoeiro, poeiras e obstáculos na trajectória [33]. Facto é que nenhuma tecnologia sem fios consegue ser 100 % efectiva, cada uma tendo as suas limitações e restrições próprias. Apesar das limitações técnicas e de largura de banda, existem vantagens inerentes ao custo e considerações sobre a facilidade de utilização, as quais posicionam os sistemas baseados em luz numa escala alta de aceitação por parte dos utilizadores para uma variedade especifica de aplicações.

II.2. Estado da arte

A constante mudança associada a cada serviço facilita um número infinito de opções. É certo, por isso, ser da incumbência dos profissionais de telecomunicações, gestores, designers e outros analisar todas as soluções possíveis antes de se eleger uma. Acresce, também, a habilidade de combinar e multiplicar serviços e tecnologias. Nenhum serviço pode afastar qualquer outro totalmente, podendo sim, os sistemas coexistir de forma harmoniosa num ambiente de demanda constante e flexibilidade crescente.

A utilização de soluções sem fios pode preencher um nicho e, até certo ponto, ser usada como uma simples tecnologia de substituição. Os responsáveis pelo fabrico e venda destes sistemas e tecnologias são, um tanto ou quanto, guiados pela necessidade e desejo de comercializar os serviços que oferecem. Como tal, acreditam que a sua é a única solução para um dado problema, enquanto que as pessoas sem experiência tendem a deixar-se conduzir por eles. Muitas empresas enveredaram por um caminho errado e opções limitadas devido sobretudo à falta de conhecimento do estado da arte. Outras, por seu lado foram apanhadas pela atitude de o último ser o melhor, postura que pode conduzir a visões menos coerentes.

Pretendemos com esta explanação não apenas tecer uma critica à industria, mas lançar um alerta para que todas as opções devam ser completamente pesquisadas. Muitos dos sistemas que preenchem um dado nicho são de facto os standard criados pelos pioneiros dos sistemas. Enquanto a industria encara de uma forma séria a standartização e a interoperacionalidade, persiste o risco de que a solução hoje escolhida possa ser um motivo de estrangulamento no futuro. Devemos estar conscientes que, existem algumas soluções conducentes estritamente a dadas aplicações, e muitas formas de colocar as comunicações sem fios a funcionar numa organização. Assim que os sistemas se tornem conhecidos, ou seja consigamos perceber o seu

funcionamento, podem deixar de existir problemas que não possam ser resolvidos no futuro. Logo, a combinação de aplicações e serviços deve conduzir o processo de tomada de decisão.

Financeiramente, a necessidade de justificar o sistema pode ser sempre uma restrição. Por conseguinte, devemos ter em mente que os sistemas novos são mais dispendiosos inicialmente, do que após a sua proliferação. Exemplo disto é o que tem vindo a acontecer no mundo das comunicações pessoais. Ponto de ordem é que a questão dos custos não deve de forma alguma ser passada em claro. Contudo, facilmente se conclui que o pioneiro vai ser o inovador e cobaia até que os *bugs* deixem de existir num qualquer serviço em fase de lançamento. Depois as massas adoptam uma oferta standard a preços bem mais acessíveis [26].

As discussões futuristas sobre serviços e tecnologias sem fios não devem levar o utilizador a avançar para uma aplicação não provada, ou mesmo tornar-se pioneiro, mas sim tomar uma atitude *esperar para ver*. Continua a ser ditado pela comunidade vendedora e organismos de standarização a determinação da direcção que o mercado seguirá. Ninguém pode saber ao certo quais as oportunidades ou standards de futuro que podem estar nos sistemas sem fios, porque por cada novo serviço um concorrente usando uma tecnologia cablada, irá possivelmente ser criado. Contudo somos deparados com conclusões pragmáticas e motivadoras como, os sistemas sem fios representam o próximo passo lógico na evolução dos sistemas computacionais e na sua relação com o utilizador [39].

Sem aludirmos de modo exaustivo à evolução dos sistemas, situemo-nos na mais valia introduzida pelas redes locais / LANs. Este tipo de ambiente possui recursos dedicados ao utilizador sob a forma de estações de trabalho e recursos partilhados, tais como servidores, impressoras, e outros, espalhados numa área relativamente grande. Na sua forma actual os utilizadores partilham uma imagem simples do sistema, tornando possível, a um utilizador, usar qualquer estação de trabalho e aceder ao seu ambiente dedicado.

Vista como uma vertente da evolução da informática, os sistemas sem fios representam o próximo passo lógico na libertação do utilizador dos ambientes fortemente cablados. Este pode aceder aos recursos dos sistema (serviços, servidores, impressoras, etc) de modo permanente e continuo, bastando para tal estar dentro dos limites de uma infra-estrutura de comunicação sem fios.

Podemos sumariar as possíveis mais valias e aplicações como forma para justificar um serviço sem fios pioneiro ou em larga escala. Esta abordagem não é a única, mas existem alguns critérios gerais para o processo de avaliação e justificação de dada opção que deverão ser devidamente fundamentados. Estes critérios devem ser substituídos ou complementados por questões

especificas das organizações nas quais o sistema possa ser instalado, ou que se julgarem convenientes.

A tabela (Tabela 1) resume questões e conceitos envolvidos na análise das novas tecnologias, onde pode ser atribuída uma dada pontuação a cada resposta e a decisão ser tomada com base na qualificação obtida [26].

QUESTÃO	RESPOSTA	PONTUAÇÃO
1. Esta tecnologia é capaz de ser conjugada com os serviços existentes, como os sistemas cablados?	☐ S ☐ N	
2. Esta tecnologia é nova na organização?	☐ S ☐ N	
3. Existem outras opções que possam ser pesquisadas?	☐ S ☐ N	
4. Existem outras empresas a usar este serviço?	☐ S ☐ N	
5. Em caso afirmativo, são a favor da sua instalação e utilização?	☐ S ☐ N	
6. Existem standards na industria para esta oferta?	☐ S ☐ N	
7. Em caso negativo, existem outras opções ou standards de facto comercializados por outros?	☐ S ☐ N	
8. Existe alguma questão legal disponível sobre a implementação desta tecnologia ou a aplicação esta a ser alvo de consideração?	☐ S ☐ N	
9. Pode esta solução técnica ser comparada favoravelmente com outras disponíveis?	☐ S ☐ N	
10. O serviço pode ser assegurado doutra forma? Se sim, esta é a preferida?	☐ S ☐ N	
11. São claros os requisitos físicos e eléctricos deste sistema?	☐ S ☐ N	
12. O fornecedor mostra um entendimento completo da tecnologia a ser instalada?	☐ S ☐ N	
13. Esta é a única solução disponível para responder ás necessidades?	☐ S ☐ N	
14. Se sim, é mais dispendiosa de instalar e operar, que o sistema em utilização?	☐ S ☐ N	

Tabela 1 - Tabela para obtenção de qualificação

II.3. Redes de área locais (LANs, Local Area Networks)

Considera-se como rede local o conjunto de recursos informáticos (computadores e periféricos a eles conectados) ligados entre si através de um meio que permita troca de informação entre eles. Uma rede local de computadores (LAN, *Local Area Network*) é um sistema no qual as distâncias entre módulos processadores se enquadram na faixa de poucos metros a poucos quilómetros. Pode caracterizar-se, uma rede local, pelo facto de permitir a interligação de equipamentos de comunicação de dados numa pequena região, diremos distâncias de 100 metros a 25 quilómetros, embora as limitações associadas às técnicas utilizadas não imponham limites a essas distâncias. Outras características típicas encontradas e, modo geral, associadas a estas redes são alta taxa de transmissão (de 1 a 100 Mbps), baixas taxas de erro (de 10^{-8} a 10^{-11}) e, regra geral, são de propriedade privada [24].

Numa rede local, a sub-rede de comunicação consiste num meio de transmissão e num conjunto de interfaces para ligação dos utilizadores. O meio de transmissão pode ser cablado (cabo coaxial, fibra óptica) ou não cablado (ar). A sub-rede de comunicação é normalmente estruturada segundo uma dada topologia. Para que a troca de informação entre os vários componentes, de uma rede local, se efectue de uma forma ordenada e / ou eficaz, estabelecem-se protocolos que definem as regras a serem usadas na comunicação entre os componentes.

Cada interface na sub-rede é geralmente responsável pela implementação do **protocolo de acesso ao meio** que controla as transmissões no meio; **protocolo de ligação** que regula a comunicação entre interfaces e **protocolo de acesso à rede** que especifica e gere as interacções entre um interface e o seu utilizador. Estes são denominados **protocolos de baixo nível.**

Uma das funções básicas das redes locais é a partilha de recursos dispendiosos e especializados (equipamentos, programas, bases de dados ou meios de comunicação), isto é, serviços entre os vários utilizadores da rede. Foram desenvolvidas para fornecer o suporte necessário a aplicações tais como: transmissão de dados e/ou voz e/ou vídeo, comunicação entre terminais e computadores, comunicação entre computadores, entre outras.

Independentemente da aplicação, vários factores devem ser tidos em conta como dispersão geográfica, ambiente de operação, número máximo de nós, separação máxima e mínima entre nós, tempo de resposta, tipo de informação transmitida, tipo de interacção entre dispositivos, taxa máxima de informação transmitida, fiabilidade requerida, tipo de tráfego (regular ou rajada), entre outros.

A exigência de tempo de resposta limitado a um valor máximo, bem como o tipo de tráfego requerido serão de importância fundamental na escolha do protocolo de acesso. Para, por

exemplo, aplicações de controle de processos e outras igualmente de tempo real, a garantia do tempo de resposta limitada é uma característica desejável. Infelizmente, em qualquer aplicação existe sempre a possibilidade de ocorrer erros na transmissão, que causará uma limitação ao tempo de resposta. Em muitas aplicações contudo, é importante que este problema não seja causado pelo protocolo utilizado.

Relativamente ao tráfego, em geral, varia de rajadas de poucos dados a grandes quantidades de dados transmitidas continuamente. Quanto ao tipo de informação transmitida esta pode ser dados, vídeo e voz, que vão diferir em termos de frequência, quantidade de informação, natureza analógica ou digital, requisitos de tempo real e ausência de erros. Por exemplo, a transmissão de dados entre dispositivos não deve conter erros, requerendo retransmissão quando os erros são detectados. Por seu lado, a transmissão de voz e vídeo deve ser efectiva, sem interrupções, em tempo real e tem uma certa tolerância a erros. Em suma, o tipo de informação transmitida será um factor determinante na escolha do meio de transmissão e do protocolo de acesso, podendo exigir circuitos dedicados para comunicação ponto a ponto.

II.3.1. Topologia e arquitectura de uma rede local

A topologia de uma rede de comunicação refere-se à forma como as ligações e os nós de comunicação estão organizados, determinando os caminhos físicos existentes e possíveis de utilizar entre quaisquer pares de estações da rede [24]. Assim, é uma das questões vitais na construção de qualquer sistema de comunicação que caracteriza, muitas vezes, o tipo, eficiência e velocidade da rede.

As linhas de comunicação, entre estações, podem ser utilizadas de várias formas, fazendo com que as ligações possam ser de dois tipos: ponto a ponto ou multiponto. Ligações ponto a ponto são caracterizadas pela presença de apenas dois pontos de comunicação, um em cada extremidade. Nas ligações multiponto observa-se a presença de vários dispositivos de comunicação com possibilidade de utilização da mesma ligação.

A comunicação na ligação diz respeito à utilização do meio físico e pode ser do tipo:

Simplex, *Half-Duplex* e *Full-Duplex*.

A arquitectura de uma rede é formada por níveis (camadas), interfaces e protocolos. Cada nível oferece um conjunto de serviços ao nível superior, usando as funções realizadas no próprio nível e serviços disponíveis nos níveis superiores. Um protocolo de dado nível, por exemplo N, é um conjunto de regras e formatos (semântica e sintaxe), através dos quais informações ou dados do nível N são trocados com as entidades do nível N, localizadas em sistemas distintos, com o

objectivo de realizar as funções que os serviços do nível N implementam. Num dado nível, um ou mais protocolos podem ser definidos.

Esta filosofia, de protocolos em níveis, é a forma mais eficiente para estruturar uma rede. Uma vez definido, claramente, o interface entre os diversos níveis, uma alteração na implementação de um nível pode ser levada a cabo sem que isso cause impacto na estrutura global. O número, nome, conjunto de funções e serviços bem como o protocolo de cada camada varia consoante a arquitectura de rede.

Inicialmente cada fabricante desenvolveu a sua própria arquitectura. Rapidamente, os utilizadores se aperceberam que estas arquitecturas de rede, denominadas proprietárias, não eram uma boa aposta. Com o intuito de permitir o intercâmbio de informação entre as máquinas de diferentes fabricantes tornou-se necessário definir uma arquitectura única. Foi com esse objectivo que a ISO (*International Standards Organization*) definiu o modelo OSI (*Open Standards Arquitecture*), que não iremos abordar. Outra iniciativa do género, foi por parte do IEEE, referimo-nos à recomendação IEEE 802, que define padrões para os níveis físicos e de ligação de redes locais de computadores.

II.4. Redes de área local sem fios (WLANs, Wireless LANs)

Numa rede de área local sem fios, o canal de comunicação é o ar e a transmissão é feita através de rádio frequência ou infravermelhos. O principio de funcionamento destas redes baseia-se na transmissão de dados através da camada atmosférica, utilizando a propagação de ondas electromagnéticas num percurso entre o emissor e o receptor.

Embora o conceito de rede local sem fios não esteja perfeitamente definido, trata-se de um conjunto de recursos informáticos espacialmente confinados ligados entre si, sem fios, através de rádio frequência ou infravermelhos [33]. Operam com placas de rede que possuem um adaptador para antena (por exemplo), através da qual recebem os dados na forma de sinais rádio. As placas com antenas são instaladas nos PCs em vez das placas de rede tradicionais. Uma rede local sem fios pode, ou não, estar ligada a outra rede local, com ou sem fios e tipicamente está limitada a uma ou várias salas de um edifício.

Estas redes fornecem uma nova era de flexibilidade e serviços para ambientes e utilizadores, os quais não podem ser servidos de modo eficiente pelas redes cabladas tradicionais [20]. À medida, que cada vez mais utilizadores sintam necessidade de grande mobilidade dentro dos seus ambientes de trabalho interiores, as redes sem fios podem ser a forma mais efectiva de ligar o utilizador móvel à sua informação bem como serviços de comunicação. As redes de área local

sem fios podem ser usadas em quase todos os ambientes de edifícios. Podemos referir a sua instalação em edifícios históricos, nos quais a passagem de cabos seria extremamente dispendiosa ou impedida por razões de estética; empresas com condições precárias as quais podem não suportar estruturas cabladas; situações de emergência, nas quais não há tempo para passar cabos ou instalar redes estáveis, são exemplos de situações que poderão ser suportadas pela instalação e implementação imediata destes sistemas. Em suma, as redes de área local sem fios fornecem os serviços do mundo LAN e acessos de interligação para numerosas situações e condições incomparáveis.

Os requisitos impostos pelos utilizadores de uma rede sem fios são essencialmente os mesmos que para as redes com fios. No entanto, devido a limitações físicas e largura de banda disponível, a taxa de transmissão das redes de área local sem fios situa-se entre 1 a 25 Mbps [36].

O conceito chave, subjacente a estas redes é a capacidade para partilhar, sem fios, um grupo de dispositivos e dados num ambiente em que a conectividade seja simples e flexível. Uma das implicações deste cenário é uma largura de banda relativamente simétrica entre o nó sem fios e a rede, tentando alcançar a maior possível para que a velocidade da rede seja próxima das atingidas nas arquitecturas tradicionais cabladas (*Ethernet, Token Ring*).

As redes de área local sem fios apresentam várias implementações. Podem ser usadas para ligar um único utilizador a periféricos locais e / ou a máquinas fixas, podem ligar entre si pequenos PDAs (*Personal Digital Assistants*) ou podem também suportar diversos utilizadores nómadas numa área local circunscrita. Embora normalmente consideradas como serviços de distância limitada, com a tecnologia apropriada, a rede de área local sem fios pode transmitir sinais a 50 quilómetros com velocidades razoáveis (1 - 2 Mbps), as quais competem com uma linha tipo T1 cablada, mas a custos muito menores.

Os benefícios das redes sem fios são, certamente, frutíferos para as empresas e organizações. Devemos, no entanto, estar cientes das preocupações que ensombram a sua implementação e uso como por exemplo, interferência do sinal radio, gestão de potência, interoperacionalidade dos sistemas, segurança da rede, problemas relativos à conexão e instalação e riscos para a saúde.

A titulo conclusivo podemos afirmar que as redes de área local sem fios representam um leque de capacidades que suportam cobertura limitada a distância local, cobertura moderada a distância metropolitana e cobertura a longa distância. Dependendo de factores como potência do emissor e sensibilidade do receptor, as redes de área local sem fios podem tornar-se a primeira forma verdadeiramente universal de LAN virtuais (VLAN) [36]. Pela ligação de redes de área local sem fios com outras formas de comunicação sem fios, como por exemplo as comunicações celulares ou satélite a conectividade do utilizador pode ser quase ilimitada.

II.4.1. Redes sem fios (WLANs versus redes cabladas (LANs)

Esta é uma questão pertinente para qualquer gestor, pelo que tentámos de modo sumário equacionar um conjunto de tópicos de auxilio para que o processo de tomada de decisão possa ser fundamentado.

Para iniciar este processo, podemos começar por colocar uma questão pertinente relativamente a esta temática:

Quando deve um utilizador considerar a utilização de uma rede de área local sem fios ?

Obviamente, esta é uma questão à qual cada um deve responder individualmente, com base no cenário em análise, antes de passar a uma fase posterior.

Até à não muito tempo atrás, as redes cabladas eram a única opção disponível para fornecer a conectividade necessária entre utilizadores num ambiente dinâmico. A ligação, por vezes, demasiado dispendiosa dos sistemas cablados criou desinteresse e em casos extremos a opção foi mesmo abandonada. Muitos dos cabos existentes nos edifícios foram usados para a conexão de dispositivos, sem atender à necessidade de precisão conseguida através da qualidade dos mesmos. Devidas a alterações físicas operadas no ambiente, por exemplo a sua remodelação, e que se prendem com a necessidade de ser flexível e eficiente, o sistema de cabos teve que voltar ao ponto de partida.

A opção por uma rede sem fios pode ser um meio de activar um utilizador durante um curto período de tempo, pressuposto que pode não ser fisicamente possível pelo uso de um sistema cablado. Acrescem, também, restrições de ordem legal e social, tais como a estética ou os requisitos legais para certo tipo de cabos, as quais podem ditar o uso de uma plataforma sem fios.

Em termos económicos, os serviços sem fios podem não ser a solução menos dispendiosa, contudo devemos ter em conta a sua mais valia para que esta questão possa, de alguma forma, ser contornada. Na tabela (Tabela 2) apresentamos uma lista de possíveis opções conducentes à utilização de um sistema sem fios. Esta representa uma análise continua e não uma comparação ponto a ponto entre as duas opções. Na primeira coluna são enumerados os factores que levam a decidir por um sistema cablado e na segunda os que conduzem a decisão por um sistema sem fios.

SISTEMA CABLADO (WIRED)	SISTEMA SEM FIOS (WIRELESS)
Dinheiro é um factor decisivo e os custos de instalação de cabos são relativamente baixos.	Dinheiro não é um factor decisivo e as novas tecnologias são sempre alvo de consideração.
A localização é fixa, os utilizadores nunca se movem.	A localização é apenas temporária, ou os utilizadores estão em constante movimento, aumentando ou diminuindo.
Os condutores são ocos e o cabo é facilmente extraído.	Condutores são sólidos. De modo a fornecer conexão LAN, novas ligações poderão ser requeridas ou as existentes podem ter que ser desligadas. Contudo, se tal for feito, o risco de disfunção ou de arrancar cabos errados é elevado.
Não existem requisitos ou limitações de ordem legal na instalação dos cabos.	Espaços cheios requerem cabos especiais ou ligações, as quais são bastante dispendiosas de instalar ou não podem ser feitas por falta de espaço. A existência de amianto no tecto ou espaços apertados, podem requerer tratamentos especiais antes que o cabo possa ser passado pela área.
O acesso por soalhos, chão e armários é rapidamente disponibilizado.	Os soalhos necessitarão de ser escavados. Este é um processo dispendioso, pode não ser facilmente autorizado e produzir risco de incêndios. Tudo isto faz com que o acesso ao sistema não seja rapidamente disponibilizado.
A estética não é importante. Paredes e postes de tensão podem ser colocados sem que isso traga qualquer problema.	Esteticamente, não é permitida a passagem de calha, ligações ou qualquer outro ponto ao longo do percurso. O ambiente pode não se adaptar.

Tabela 2 - Factores de opção por uma WLAN

Podemos, de igual modo, referir os pontos fortes e fracos das redes sem fios, mais uma vez a titulo comparativo conforme ilustrado na tabela (Tabela 3).

PONTOS FORTES	PONTOS FRACOS
Criar uma maior mobilidade para os utilizadores de PC e LAN.	Obtenção de performance inferior ás dos sistemas cablados, devido ás limitações da largura de banda.
Evitar os altos custos de movimentação, alteração ou adição de utilizadores e constante redefinição.	Pode estar sujeito a interferências ou limitações de distância, dependendo da técnica usada.
Pode diminuir os custos de manutenção da LAN, desde que não existam cabos que requeiram reconfiguração.	Requerer hardware proprietário e mais dispendioso, dependendo do sistema usado.

Tabela 3 - Pontes fortes e fracos das WLANs

Outra solução atractiva é que as redes sem fios permitem ampliar um arranjo cablado existente, disponibilizando conectividade e mobilidade incomparáveis para o futuro. Contudo, os críticos desde logo argumentaram que esta solução é demasiado dispendiosa e lenta, quando comparada com as soluções cabladas. Embora possamos considerar este facto verdadeiro, até certo ponto, as ideias têm vindo a mudar rapidamente desde que os fabricantes desta tecnologia procederam à redução gradual dos custos dos seus equipamentos e melhoram a velocidade e performance do sistema.

II.4.2. Arquitectura física de uma rede sem fios

A arquitectura física de uma rede sem fios refere-se aos seus componentes. Estes implementam as funções das camadas: Física (*Physical*), Ligação (*Data Link*) e Rede (*Network*), tendo como base o modelo de referência OSI. Satisfazem, ainda, a funcionalidade necessária em áreas locais, metropolitanas e alargadas e são, basicamente, os referidos nas secções seguintes.

II.4.2.1. Ferramentas do utilizador final

À semelhança do que acontece em qualquer sistema, será necessário existirem dispositivos através dos quais utilizadores interactuem com aplicações e serviços. Assim, uma ferramenta de utilizador final (*end-user appliance*) é um interface entre o utilizador e a rede.

Nas redes sem fios como dispositivos mais adequados podemos enumerar: *Desktop Workstations*, computadores *Laptop*, computadores *Palmtop*, PCs *Handheld*, computadores *Pen-Based*, PDA (*Personal Digital Assistant*), *Scanners*, colectores de dados (*Data Collectors*) e impressoras.

Actualmente o PC *handheld*, introduzido pela Microsoft, é a principal plataforma de hardware para Windows CE [27]. O objectivo principal foi desenvolver um PC manuseável que inclua bateria de longa duração, preço aceitável, seja compacto e leve, possua interfaces standard, seja de fácil conexão e inclua um teclado efectivo. Este tipo de dispositivos, independentemente do fabricante, possuem como características comuns: teclado QWERTY, teclas alfanuméricas, pontuação standard, teclas CTRL e ALT bem como teclas opcionais; écrans sensitivos com resolução de 480x240 e 640x240 pixels e quatro escalas de cinza; dispositivo com funções análogas às do rato; tomadas para carregar a bateria e conectar ao nosso PC; slot para placa PCMCIA, conector série e porta para infravermelhos (IrDA) e memórias de, pelo menos, RAM (2 MB) e ROM (4 MB).

II.4.2.2. Software de rede

Uma rede sem fios possuí *software* que reside nas diferentes partes da rede. Exemplo disso é o sistema operativo de rede (NOS, *Network Operating System*) caso, por exemplo, do Windows NT Server residente num servidor, bem como serviços de aplicação e impressão.

A maioria dos sistemas operativos são orientados à existência de servidores, segundo a filosofia Cliente / Servidor [27], nos quais reside o *software* aplicacional e as bases de dados. Nesta filosofia, as ferramentas do utilizador farão o interface, via por exemplo TCP/IP, com o software aplicacional ou bases de dados executadas no sistema operativo da rede. Assim o software cliente, residente nas ferramentas do utilizador final, encaminha os comandos executados pelos utilizadores para o software local ou conduzem-nos para fora através da rede sem fios.

O *software* residente nas ferramentas das redes sem fios é muito semelhante ao existente nas de uma rede cablada. A diferença principal reside no facto de ser importante desenvolvê-lo de modo a optimizar a utilização das redes sem fios face à relativamente pouca porção de largura de banda com que estas se deparam. O *software* que executa funções de aplicação pode correr num servidor (*host*), na ferramenta do utilizador final ou numa combinação de ambos. Em alguns casos, como por exemplo o de aplicações que são executadas em computadores *mainframe*, como IBM, IBM AS/400 ou outros baseados no sistema operativo Unix, poderá existir a necessidade de correr *software* de emulação de terminal. Isto faz com que a ferramenta actue como um terminal não inteligente, apenas servindo como interface à aplicação que é executada no servidor, pelo uso de teclado, écran e impressora.

Por outro lado, nos sistemas Cliente / Servidor, o *software* da ferramenta do utilizador final pode executar parte, ou mesmo todas as funcionalidades das aplicações, e unicamente fazer o interface

com bases de dados localizadas no servidor, caso do Windows NT. Em alguns casos, poderá ser necessária a existência de um *gateway* que execute *middleware*. O objectivo é fornecer um interface entre a ferramenta e o *software* aplicacional executado no servidor. A ferramenta comunicará com o servidor / *host* através do *gateway* o qual actuará como *proxy* para várias aplicações.

II.4.2.3. Interface de uma rede sem fios

Como é do conhecimento geral, os computadores processam informação no formato digital, representando os dados com zeros e uns. Estes sinais são adequados para transmissões internas, contudo o mesmo não acontece com o transporte de dados através de meios cablados ou sem fios.

Um interface de rede sem fios liga o sinal digital da ferramenta do utilizador final ao meio sem fios, isto é o ar, de modo a permitir uma transferência de dados efectiva entre o emissor e o receptor. Este processo envolve duas técnicas denominadas modulação e amplificação do sinal digital para uma forma adequada à propagação em causa.

A modulação é o processo que permite modificar o sinal digital em banda base, usado na ferramenta, para um formato analógico adequado para transmissão através do ar. Este processo é muito idêntico ao executado nos modems telefónicos comuns, os quais convertem dados digitais de um computador para um formato analógico dentro da limitação do circuito no qual operam, 4 KHz. O modulador sem fios modifica o sinal digital para uma frequência cuja propagação seja adequada através da atmosfera. Claro é que as redes sem fios empregam modulação por meio do uso de ondas rádio e luz infravermelha, das quais faremos alusão posteriormente nesta dissertação (CAPITULO III).

O interface de redes sem fios, normalmente, apresenta-se sob a forma de uma placa NIC (*Network Interface Card*) sem fios ou um modem externo que facilita o modulador e protocolos de comunicação. Estes componentes fazem o interface com a ferramenta do utilizador via um BUS de computador, à semelhança de uma placa standard ISA (*Industry Standard Architecture*) ou PCMCIA (*Personal Computer Memory Card International Association*). Muitos computadores portáteis possuem slots de expansão PCMCIA que aceitam placas NIC do tamanho de um cartão de crédito. Alguns fabricantes produzem componentes para redes sem fios que são ligados ao computador via porta série RS-232.

O interface entre a ferramenta utilizada e a NIC inclui, também, um driver de software, o qual liga as aplicações cliente ou o sistema operativo da rede à placa. Exemplos de driver standard

são: NDIS (*Network Driver Interface Specification*) usado com o sistema operativo da Microsoft; ODI (*Open Datalink Interface*) usado com o sistema operativo da Novell entre outros [27].

As placas rádio, de um modo geral, apresentam uma configuração com uma versão de duas componentes (*two-piece*), que são: placa PCMCIA inserida na ferramenta do utilizador e uma caixa externa, denominada *transceiver* . Esta arquitectura poderá ser prática para alguns tipos de aplicações, contudo o mesmo não se verifica para outras tais como ferramentas de mão. Outros fabricantes, especialmente dos modelos mais recentes de placas rádio, oferecem unidades únicas possuidoras de rádio e *transceiver* integrados que se encaixam no formato da placa PCMCIA.

II.4.2.4. Antena

No caso de transmissão por ondas rádio, uma antena radia o sinal modulado através do ar e, deste modo, o receptor pode recebê-lo. As antenas apresentam-se sob várias formas e tamanhos e possuem as seguinte características eléctricas específicas: padrão de propagação (radiação); ganho; potência transmitida e largura de banda.

O padrão de radiação de uma antena define a sua cobertura. Uma antena omnidireccional é aquela que transmite a sua potência em todas as direcções, enquanto uma antena direccional concentra a maior parte da sua radiação numa dada direcção [27].

Relativamente ao ganho, podemos afirmar que este depende da direcionalidade da antena. A antena direccional tem maior ganho (grau de amplificação) que o tipo omnidireccional, e permite a propagação do sinal modulado a maior distância porque foca a potência numa única direcção. Assim, uma antena direccional será mais adequada para a interligação de edifícios em áreas metropolitanas atendendo à sua cobertura superior e necessidade de minimização de interferências com outros sistemas. Uma antena omnidirecional tem um ganho igual a um, isto é, ela não foca a sua potência numa dada direcção em particular. Este tipo de antenas é o mais adequado para redes sem fios interiores devido aos seus requisitos relativos a curta distância e menor susceptibilidade a interferência externa.

A potência de transmissão combinada com o ganho da antena definem a distância percorrida pelo sinal. Transmissões a grandes distâncias requererão potência elevada e padrão de radiação directos, enquanto transmissões a curta distância podem ser alcançadas com antenas de potência e ganho menores. Nas redes sem fios, a potência de transmissão é relativamente baixa, modo geral, um Watt ou inferior.

Numa antena a largura de banda é a parte efectiva do espectro de frequência propagada pelo sinal. O sistema telefónico comum, por exemplo, opera numa largura de banda, aproximadamente de 0 a 4 KHz, a qual é suficiente para alojar a maioria dos componentes de frequência presentes na voz. Por outro lado, os sistemas de ondas rádio, possuem quantidades de largura de banda superiores localizados, em termos do espectro, também em frequências muito superiores. A taxa de dados e a largura de banda são directamente proporcionais, quanto maiores as taxas de dados mais largura de banda será necessária.

II.4.2.5. O canal de comunicação

Todos os sistemas informação usam um canal de comunicação, ao longo do qual esta circula da origem para o destino. As redes Ethernet, por exemplo, utilizam o par de cobre ou o cabo coaxial. As redes sem fios usam o meio ar, como já anteriormente aludido. Este também é, por vezes, referido como meio de transmissão.

Nenhum meio de transmissão é capaz de transmitir informação sem que ocorram perdas de energia durante o processo, ou sejam reduções na amplitude dos sinais componentes [24]. Se todos os sinais componentes fossem reduzidos de igual modo, o sinal resultante seria todo reduzido, por exemplo em amplitude, mas não distorcido. Contudo, as características do meio de transmissão provocam perdas, nos sinais componentes em proporções diferentes, causando distorção no sinal resultante a ser transmitido. Podemos dizer que, desta forma, o meio de transmissão actua como um filtro sobre o sinal.

Outro efeito negativo provocado pelo meio de transmissão acontece porque na superfície da terra, onde a maioria das redes sem fios operam, o ar puro contem gazes, tais como azoto e oxigénio. Esta atmosfera fornece um meio efectivo para a propagação das ondas rádio ou luz infravermelha. Já outros factores presentes na atmosfera, como por exemplo chuva, nevoeiro e neve, podem aumentar a quantidade de moléculas de água presentes no ar e causar um efeito de atenuação significativo na propagação de sinais sem fios modulados. Sendo a atenuação um fenómeno que conduz ao decrescimento da amplitude do sinal, esta limita o seu intervalo de operação. Poderão utilizar-se meios para combater a atenuação, como por exemplo, aumento da potência transmitida pelos dispositivos sem fios, a qual na maioria dos casos é limitada pela FCC (*Federal Communications Commission*); incorporação de amplificadores especiais, denominados repetidores, os quais recebem sinais atenuados, reconstroem-nos e transmitem-nos para a estação final ou para o próximo repetidor.

Em suma os factores que afectam qualquer transmissão são distorção, atenuação e ruído.

II.4.3. Arquitectura lógica de uma rede sem fios

A arquitectura lógica diz respeito aos protocolos da rede, que asseguram uma gestão adequada bem como meios de comunicação efectivos, aos quais faremos alusão posteriormente nesta dissertação. Os dispositivos de rede activos, como por exemplo PCs, servidores, *routers* e outros, devem estar em conformidade com regras precisas de modo a facilitar uma coordenação adequada e transferência da informação de modo fiável.

Uma arquitectura lógica standard e bastante popular é o modelo se sete camadas, desenvolvido pela ISO (*International Standards Organization*), denominado OSI (*Open System Interconnect*), o qual especifica um conjunto completo de funções de rede organizadas em camadas. Uma questão pertinente, que pode ser colocada, é se uma rede sem fios poderá oferecer todas as funções do modelo OSI à qual a resposta é não, no sentido teórico. Como exibido na figura (Ilustração 1), as redes sem fios operam apenas ao nível das três camadas inferiores (Física, Ligação e Rede) embora, apenas as WANs (*Wide Area Networks*) sem fios executam funções da camada de rede.

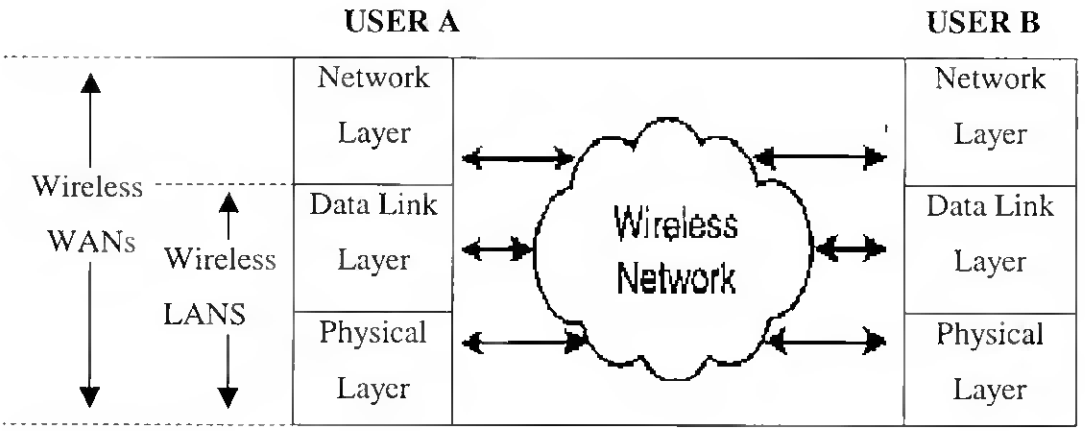


Ilustração 1 - Níveis de operação das redes sem fios

Adicionalmente às funções das redes sem fios, uma arquitectura de rede completa necessita de incluir funções como estabelecimento de conexões fim-a-fim e serviços aplicacionais para que as mesmas se tornem úteis.

II.4.4. Topologia de uma rede de área local sem fios

A topologia diz respeito à configuração da rede em particular, ou seja à forma como os diversos componentes estão agrupados. Podem existir vários tipos de componentes que permitam a interligação, mas os mais importantes são: placas NIC sem fios e *Bridge* local sem fios, referida, muitas vezes, como Ponto de Acesso (AP, *Access Point*). As placas NIC fazem o interface entre a ferramenta usada e a rede sem fios e o AP faz o interface entre a rede sem fios e a rede cablada. A maioria das placas, NICs sem fios, fazem o interface com a rede sem fios pela implementação de protocolos de acesso do tipo *Carrier Sense* e pela modulação do sinal de dados com uma sequência de espalhamento (*Spreading Sequence*) recorrendo a técnicas de *Spread Spectrum* a que faremos alusão posteriormente (III.2.3.).

As implementações de redes de área local sem fios podem ser as mais variadas, entre elas a complementação aos cabos tradicionais, como o par entrelaçado, cabo coaxial e fibra óptica, utilizados nas redes cabladas passando, deste modo, a ser uma solução bastante interessante. Desta forma os pontos que necessitam de mobilidade são conectados à rede através do meio sem fios e as estações fixas são ligadas à rede via cabo.

Tanto as características do canal como a mobilidade de um nó, podem alterar as conexões entre os vários nós e consequentemente a topologia da rede. Acresce o facto de estas alterações poderem ser bastante dinâmicas, ocorrendo em dezenas de milisegundos. Assim, os protocolos de rede devem ser capazes de negociar as questões de mobilidade de modo a fornecer serviços continuamente (sem interrupções). Além das características referidas, é ainda desejável que o intervalo de transmissão seja curto para que, deste modo, os nós móveis possam reservar potência de bateria, extremamente valiosa, e assim a totalidade da rede pode adoptar o conceito de reutilização de frequência visando a eficiência do espectro.

Outro conceito, de extrema importância, consiste no facto de que a unidade básica de uma rede de área local sem fios é a célula, que corresponde à área geográfica na qual um conjunto de estações se movimentam livremente. Nas células as comunicações entre estações processam-se em espaço livre. Por outro lado, as estações podem ser portáteis ou móveis. Uma estação diz-se portátil quando é facilmente deslocada, mas opera apenas a partir de uma posição fixa. Uma estação e diz-se móvel quando tem a capacidade para operar em movimento. Cada estação pode comunicar com estações da mesma célula e, eventualmente com estações de outras células, desde que as células estejam ligadas através de uma infra-estrutura física.

As redes sem fios apresentam, normalmente, dois tipos de configuração ou topologia, podendo ser denominadas como: Redes Ad-hoc (b) constituídas por uma única célula isolada e Redes

Infra-estruturadas (controlada pela estação (a)) constituídas por várias células interligadas através de uma infra-estrutura física [23]. Estas configurações são exibidas na figura (Ilustração 2).

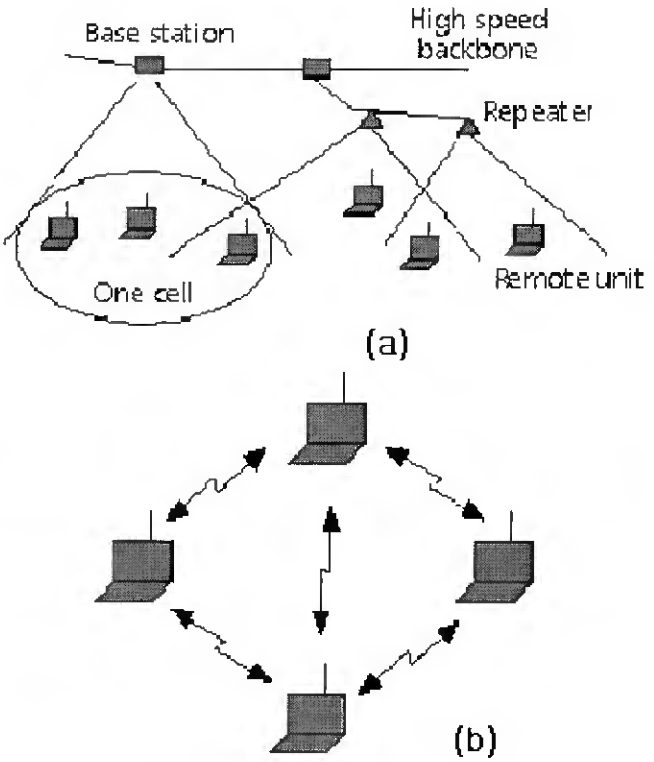


Ilustração 2 - Toplogia de redes [23]

II.4.4.1. Redes Ad Hoc

Nesta configuração os nós móveis, por exemplo computadores *notebook*, podem estar juntos numa pequena área (por exemplo sala de conferências) e estabelecer entre eles comunicações ponto-a-ponto, sem necessidade de recorrer a qualquer infra-estrutura, como por exemplo um *backbone* cablado / não cablado. Neste tipo de comunicação o meio é partilhado, sem que se verifiquem interferências com qualquer outro no seu raio de alcance.

Estudos de caracterização de canais interiores, indicam que uma pequena área de cobertura pode não significar garantia de comunicação [23/3]. Em geral, a interligação por meio de redes Ad Hoc pode não presumir uma topologia de rede completamente conectada, como a da figura (Ilustração 3).

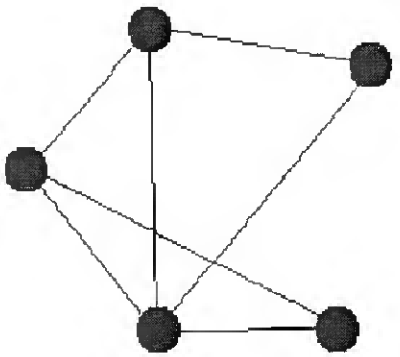


Ilustração 3 - Topologia típica da rede Ad Hoc [23]

Numa rede de comunicação do tipo *ad hoc* a transmissão da informação é feita por difusão. Assim, qualquer nó com pacote(s) disponíveis transmite-os deste modo, que consiste no envio da mesma informação para vários utilizadores, simultaneamente, baseado em algum tipo de protocolo de acesso múltiplo como, por exemplo ALOHA, Slotted ALHOA ou o mais sofisticado CSMA (*Carrier Sense Multiple Access*). Quando outro nó recebe um pacote verifica a sua identificação e, caso não seja o destinatário, retransmite-o.

Com este modo de transmissão a utilização do canal é baixa, embora a sua implementação seja simples e fácil. Por outro lado, a difusão pode não garantir conexão a todos os nós móveis e os utilizadores podem necessitar de encontrar uma localização correcta para, deste modo, conseguirem uma recepção fiável. Os nós podem definir uma infra-estrutura temporária, a qual é usualmente um esquema hierárquico de passagem de pacotes. Esta conjectura normalmente recorre a algoritmos adicionais que conduzem a uma sobrecarga e consequente redução da eficiência do canal.

As redes Ad-Hoc caracterizam-se por uma instalação rápida, dado não exigirem planeamento e são independentes de qualquer infra-estrutura que possa existir. Em termos práticos, são adequadas às necessidades de utilizadores que ocupem uma pequena área, como por exemplo um andar ou ala de um hospital. Apresentam, porém, limitações que se traduzem quer no tipo de serviços que podem fornecer, quer na área de cobertura da própria rede. Por outro lado, não podem ser expandidas em termos geográficos, pelo simples facto de não terem associadas a entidade que permite essa funcionalidade, que é o AP. Será com base nesta topologia que iremos implementar a rede do nosso caso de estudo (CAPITULO VII).

II.4.4.2. Redes infraestruturadas

São redes que obrigam à existência de uma estrutura cablada. Justificam-se porque apesar da possibilidade de interligação A*d Hoc*, a maioria das aplicações requerem comunicação com serviços situados numa infra-estrutura pré existente, a qual é normalmente uma rede *backbone* cablada, ou não, de alta velocidade.

Podemos diferenciar o trafego típico desta rede em duas direcções: Trafego *Downlink* (do backbone) e Trafego *Uplink* (para o backbone). O ponto de contacto do *backbone* com o meio sem fios é denominado ponto de acesso (AP, *Access Point*). Estes podem ser uma de duas opções, ou estações base ou repetidores para ampliar a área de cobertura da comunicação.

Trafego Downlink

Chama-se trafego *downlink* ao que decorre do *backbone* para o meio sem fios. Devida à limitada largura de banda, das redes de área local sem fios, normalmente é usado um canal de comunicação comum entre um ponto de acesso e nós móveis, ou mesmo um canal comum para todos os pontos de acesso e nós móveis. A comunicação *downlink* é efectuada por difusão neste canal comum. De modo mais preciso, o(s) ponto(s) de acesso transmite(m) pacotes para todos os nós móveis mesmo se existir apenas um destinatário.

O conceito de difusão (*broadcasting*) introduz duas considerações importantes na implementação de uma rede de área local sem fios:

***Multicasting* (Lançamento múltiplo):** Embora possa ser uma função desnecessária, esta não deve ser proibida pelo meio físico de transmissão. Contudo, poder-se-à tornar um problema que traduziremos com o seguinte exemplo. Suponha-mos que existem 200 nós sob a cobertura de uma estação base, que cada pacote tem a dimensão de 1 Kbit e que a taxa de erro de bit é de 10^{-5} para cada para pacote emitido/recebido. A taxa de erro de pacote resultante é 10^{-2} e a probabilidade de que pelo menos um nó receba incorrectamente o pacote lançado é de aproximadamente 0.8666. Se o pacote for reenviado para corrigir o erro, um nó que anteriormente o recebeu correctamente pode agora recebe-lo com erro. Em média são efectuadas 7.46 (1/81-0.866) transmissões, para todos os nós de modo a receberem correctamente o *multicast*.

O problema anteriormente descrito pode ser ultrapassado pelos seguintes métodos:

Difusão múltipla para cada multicast: a estação base difunde o pacote *multicast* diversas vezes com um elevado número de sequências de cada vez, atendendo a que um nó móvel necessita de o receber correctamente apenas uma vez. A taxa de erro de pacote resultante, para 200 nós com

uma taxa de erro individual de 10^{-2}, é de 0.02 e a média de tempo de transmissão de pacote é 1.02, significativamente menor que os 7.46 do esquema anterior;

Sem reconhecimento (acknowledgement) para multicast: outra forma de resolver o problema é simplesmente abolir o reconhecimento. Sob o pressuposto que os nós móveis devem ser capazes de escutar a estação base e que a taxa de erro de pacote é usualmente pequena, esta abordagem funciona de modo razoável. Contudo é de referir, que a entrega fiável de pacotes não é garantida.

A questão final e de grande importância, sobre o trafego do *downlink*, é que os nós das redes locais actuais, frequentemente, operam no modo cliente / servidor. Neste caso, um pedido para transferência de ficheiros efectuado no *uplink* pode ter como resultado uma grande transferência de ficheiros no *downlink*. Consequentemente, a actividade do *downlink* pode constituir até 75% ou 80 % do trafego total das numa rede de área local sem fios.

Trafego Uplink

Este é o tráfego que decorre do meio sem fios para o *backbone*, e geralmente necessita de um protocolo de acesso múltiplo de modo a organizar a informação proveniente dos nós móveis. Existem diversas razões pelas quais o acesso múltiplo é mais difícil de implementar para redes de área local sem fios do que para redes cabladas. Podemos referir, por exemplo, as características da dinâmica física dos canais. Estas redes habitualmente operam em canais de multi-caminho sob atenuação verdadeiramente forte, os quais podem alterar as suas características num intervalo de tempo ou distância verdadeiramente curtos, e os quais podem não ser recíprocos. Estes canais onde exista tal atenuação podem tornar a comunicação não fiável e resultar em captura, que conduz a um acesso falso.

Medições práticas mostram que, de acordo com as dimensões do canal e o modelo do ambiente de operação primário das redes sem fios de alta performance - propagação rádio interior, as características do canal podem alterar-se significativamente num intervalo de tempo de 10 a 20 ms ou qualquer movimento de aproximadamente 30 centímetros de distância [23].

Em suma, o meio sem fios é completamente diferente do cabo e da fibra óptica. Deste modo, muitas das funções que seriam de implementação trivial nos meios cablados não podem facilmente ser aplicadas nos meios sem fios. Por exemplo, a percepção da portadora nos cabos é fácil, mas a mesma operação na tecnologia rádio leva pelo menos 30 a 50 μs, já por si uma porção não trivial no tempo de transmissão de um pacote.

Outra questão importante, diz respeito a reconhecer e registar novos nós móveis que se juntem à rede a qualquer momento e local, e uma espécie de protocolo de acesso aleatório é, sem dúvida, necessário. Contudo, uma vez que a conexão *uplink* tenha sido definida o acesso aleatório pode

não ser necessário, se o canal for estático podemos considerar esta situação como equivalente a uma rede cablada. Lamentavelmente o pressuposto de canais estáticos é, sem duvida, uma política não razoável. Por este motivo, na área das comunicações sem fios, foram propostas técnicas de reserva para preservar os serviços, especialmente para os de tempo limitado tais como voz e vídeo. Consequentemente, o protocolo do *uplink* é a tarefa central na concepção MAC (*Medium Access Control* / Acesso ao Meio) de redes de área local sem fios, bem como na concepção do acesso ao meio de qualquer rede de dados sem fios de modo a suportar computação móvel.

II.4.5. Comunicação entre as estações de uma rede sem fios

A comunicação entre as estações duma rede, por exemplo dentro de um escritório, pode ser efectuada por meio de um *hub*[1] central instalado no tecto do ambiente, o qual envia e recebe sinais das antenas instaladas nos micro-computadores pertencentes à rede. Neste caso, o barramento da rede local, passa a ser o sinal emitido (pode ser numa frequência rádio na faixa de 900 MHz a 6 GHz ou infravermelho na faixa de frequências dos 100 THz) e o alcance ou cobertura varia de 30 a 100 metros, dependendo do tipo de sistema utilizado.

A comunicação entre as estações de uma rede sem fios pode introduzir um comportamento de domínio espacial (*spatial domain behavior*) devida à estrutura por múltiplas células [23].

Uma das razões primárias para a adopção de uma estrutura celular é para aumentar a largura de banda total efectiva, devida à utilização de diferentes frequências em diferentes células. Por outro lado, a mobilidade do utilizador obriga a que as células devam estar, entre si, com uma sobreposição adequada. Este conceito traduz-se em que a sobreposição deve ser larga o suficiente para garantir que não existam falhas no serviço e, por outro lado, deve ser pequena o suficiente para não reduzir muito a eficiência do espectro, sempre dependendo do protocolo utilizado. Uma implicação adicional é a necessidade de coordenação adequada entre pontos de acesso, de modo a fornecer serviço ininterrupto aos nós móveis.

O conceito anteriormente referido, que permite aumentar a largura de banda efectiva, conhecido como reutilização de frequência, é ilustrado na figura (Ilustração 4).

[1] Hub :dispositivo electrónico usado para interligação de múltiplos computadores

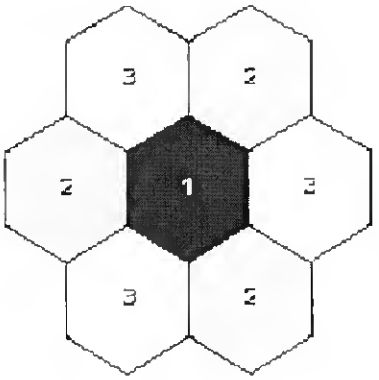


Ilustração 4 - Reutilização de frequências [23]

Neste exemplo, de uma estrutura de sete células, suponhamos que é necessária uma largura de banda total de 3-B, para servir os utilizadores nesta área. Assim, com reutilização de frequências, apenas três bandas diferentes podem dar cobertura a esta região. Se, pelo contrário, esta técnica não for utilizada e uma única banda servir todos os utilizadores na mesma região, uma largura de banda total de 7-B será necessária para assegurar o mesmo nível de qualidade do serviço. Como resultado da reutilização de frequências, a totalidade da largura de banda disponível para comunicação de todos os utilizadores é muito maior. Acresce o facto de que a reutilização de frequências não só preserva o espectro mas também reduz a potência de transmissão pela redução do tamanho da célula. Outra função inerente à comunicação nas redes sem fios é o denominado *handoff* ou *handover* , que permite que um nó móvel comunique com um ponto de acesso numa célula e depois, ao mover-se, mude para o ponto de acesso de outra célula. O objectivo deste mecanismo é manter o serviço continuamente, isto é sem interrupções, aos nós móveis através da cobertura de diferentes células. Esta é uma característica especial que permite gerir a questão da mobilidade nas redes sem fios.

O *handoff* pode, basicamente, ser implementado de modo centralizado, controlado por uma central ou descentralizado controlado por meio de nós móveis. Existem diversas técnicas e algoritmos para a gestão desta permuta, contudo por irem além do âmbito do nosso estudo não iremos abordá-las. Vamos apenas referir que o *handoff* é uma função que pode afectar a concepção de protocolos em diversas camadas. Uma abordagem comum é associá-lo ao controle de potência e coordenação dos pontos de acesso via gestão da rede.

CAPITULO III
ASPECTOS ESPECÍFICOS DE REDES DE ÁREA LOCAL SEM FIOS

Este capítulo aborda aspectos das redes sem fios no que diz respeito às tecnologias de transmissão rádio: DSSS (Direct Sequence Spread Spectrum) e FHSS (Frequency Hopping Spread Spectrum) e por infravermelhos (IR). Concluímos com uma análise comparativa das mesmas.

III.1. Técnicas para transmissão sem fios

Nas comunicações em espaço livre, o canal de comunicação é o ar e a transmissão é feita através de ondas rádio frequência ou ondas de luz infravermelha.

A tecnologia rádio frequência é amplamente utilizada no domínio das telecomunicações, sobretudo nas tão em voga comunicações telefónicas celulares. A sua aplicação a redes de área local sem fios é bastante atractiva, como podemos verificar numa análise feita aos produtos disponibilizados pelos vários fabricantes, existindo inúmeras redes que fazem uso dela. A maioria destas operam sobre frequências não licenciadas a velocidades próximas da rede *Ethernet* (10 Mbps), usando protocolos de *Carrier Sense* de modo a partilhar o meio das ondas rádio.

Uma alternativa à utilização da tecnologia de rádio frequência, principalmente em espaços interiores, é a tecnologia de infravermelhos. A sua aplicação a redes de área local sem fios foi inicialmente sugerida por Gfeller [40]. O seu contributo foi importante para fomentar o interesse pela mesma e desplotar a exploração das diversas vantagens que apresenta face à tecnologia rádio.

Independentemente da abordagem tecnológica escolhida, existem algumas regras básicas que devem ser tidas em consideração, antes que qualquer decisão possa ser efectiva. Assim, deverão ser analisados os seguintes pontos cruciais, mesmos antes do utilizador considerar a hipótese de recorrer a uma rede de área local sem fios : facilidade de instalação, segurança da conectividade e eficiência em termos de custos.

III.2. Transmissão rádio frequência em redes de área local sem fios

Em qualquer transmissão rádio e como tal nas redes locais, desde que o sinal seja transmitido em espaço livre, os factores enumerados na tabela (Tabela - 4) deverão ser tidos em conta

relativamente ao tipo de sistema de transmissão rádio a utilizar. Esta lista não inclui todos os factores limitantes, mas sim aqueles que são genéricos para a maioria dos sistemas rádio.

1- Decisão a ser tomada sobre o uso de linha de visão, ponto a ponto ou transferência via difusão.
2- O ruído será sempre um factor que, desde que esteja presente, degrada o sinal.
3- A potência de saída afecta directamente a distância percorrida pelo sinal.
4- Perdas ou atenuações do sinal serão sempre factores a ter em conta. Assim, o sinal rádio diminuirá ao passar por certos materiais isolantes, sofrerá ganhos ao passar através de condutores e pode ainda ser reflectido por outros objectos.
5- A presença de chuva intensa ou neve absorvem parte do sinal transmitido em certas bandas de frequência (Ex.: Microondas e Satélite).

Tabela - 4 Factores que afectam a transmissão rádio [27]

Nestas redes uma vantagem das ondas rádio, sobre outras formas de conectividade sem fios, é que estas podem interligar utilizadores sem que exista linha de visão e podem propagar-se através de obstáculos, tais como paredes e portas, com atenuação muito pequena. Assim, embora possam existir, por exemplo, diversas paredes a separar o utilizador da *bridge* sem fios, este consegue manter conexão à rede suportando mobilidade real.

Uma desvantagem da utilização dos sistemas rádio é que, normalmente, um circuito que utilize como modo de transmissão a onda rádio é mais sofisticado do que outro que utilize infravermelhos, devida à probabilidade de existência de interferências ser maior. Por outro lado, a sua implementação deverá ter em consideração outras propagações electromagnéticas existentes no local. A título de exemplo podemos referir que equipamento médico e componentes industriais, provavelmente utilizam as mesmas frequências rádio que as redes locais podendo, deste modo, causar interferência. Estas deverão, dentro do possível, ser tidas em consideração e determinadas à priori. Existe, também, a possibilidade de interferências de outras transmissões referentes à própria rede, que operem na mesma frequência. Isto poderá acontecer numa localização onde existam várias estações móveis (EM) a transmitir, conforme ilustra a figura (Ilustração 5).

Para resolver este problema, são criadas várias sub-bandas de transmissão em que as suas camadas adjacentes usam frequências diferentes.

Outra desvantagem diz respeito à potência do sinal recebido, que não depende apenas da

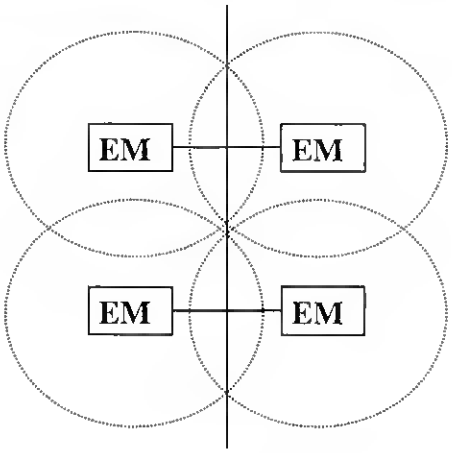


Ilustração 5 - Interferência de transmissão

potência do sinal emitido mas também da distância entre o emissor e o receptor. A perda do sinal transmitido é ainda, como anteriormente referido, devida à presença de objectos, como por exemplo móveis e pessoas, e à interferência que estes causam ao reflectir o sinal rádio. A combinação de ambos provoca a quebra da potência no sinal recebido. Por outro lado, a segurança deverá ser um problema a equacionar devido ao facto das ondas rádio poderem passar através de paredes e assim pessoas não autorizadas, que se encontrem fora das áreas sob controle, conseguirem receber informação confidencial.

III.2.1. O espectro de frequências rádio

A utilização de ondas rádio em espaço aberto requer a conversão de qualquer forma de informação seja ela voz, dados ou outra, da sua forma original para o seu equivalente eléctrico. Os componentes dos equipamentos usados para realizar esta conversão operam de modo idêntico, em quase todos os sistemas rádio, podendo contudo apresentar nomes distintos.

Podemos sumariar os intervalos de frequência para os sistemas rádio associando-os a uma dada banda, a qual é classificada como se mostra na tabela (Tabela 5).

FREQUÊNCIA	BANDA
< 30 KHz	**VLF** (Very Low Frequency)
30 – 300 KHz	**LF** (Low Frequency)
300 KHz – 3 MHz	**MF** (Medium Frequency)
3 MHz – 30 MHz	**HF** (High Frequency)
30 MHz – 300 MHz	**VHF** (Very High Frequency)
300 MHz – 3 GHz	**UHF** (Ultra High Frequency)
3 GHz – 30 GHz	**SHF** (Super High Frequency)
> 30 GHz	**EHF** (Extremely High Frequency)

Tabela 5 - Bandas de Frequência Rádio

Para a tecnologia rádio, quando aplicada a WLAN, existem dois cenários possíveis, quanto à utilização do espectro de frequências: intervalo licenciado de frequência rádio microondas (18 - 23 GHz) e intervalo não licenciado de frequência rádio (902 - 928 MHz ; 2.4 e 5.7 GHz).

As redes de comunicação de área local sem fios, começaram por utilizar as bandas baixas do espectro de frequência (LF / 30 – 300 MHz ; HF / 3 MHz – 30 MHz) como solução para transmissão de sentido único e numa única frequência. Esta filosofia, regra geral, obriga a que uma parte escute enquanto a outra fala. Neste caso é usada transmissão *push-to-talk*, na qual se ambas as partes tentarem enviar ao mesmo tempo é causado o efeito de compressão que tornará a comunicação inútil. Por outro lado, são necessários protocolos de transmissão bastante específicos, para que a tecnologia rádio, segundo este modo, possa ser usada eficazmente. Para evitar este efeito não desejado, de um modo geral, são necessárias duas frequências separadas facto pelo qual as bandas baixas foram abandonadas.

Pelo exposto, nas redes de área local que usem a tecnologia rádio frequência, as comunicações processam-se nas bandas altas não licenciadas. A banda ISM (*Industrial, Scientific and Medical*) não requer licenciamento e foi originalmente regulamentada nos Estados Unidos pela FCC (*Federal Communications Commission*), nas bandas 902-928 MHz, 2400-2483.5 MHz e 5725-5850 MHz, ou seja entre os 902 MHz e 5.85 GHz, imediatamente acima das frequências de operação dos telefones celulares [27].

Em 1985, numa tentativa de estimular a produção e utilização de produtos para redes sem fios, a FCC modificou a Parte 15 da regulamentação do espectro rádio, a qual rege o uso de dispositivos que não estão sujeitos a licenciamento. Esta modificação autorizou os produtos das redes sem fios a operar nas bandas ISM (*Industrial, Scientific and Medical*), as quais são exibidas na figura (Ilustração 6).

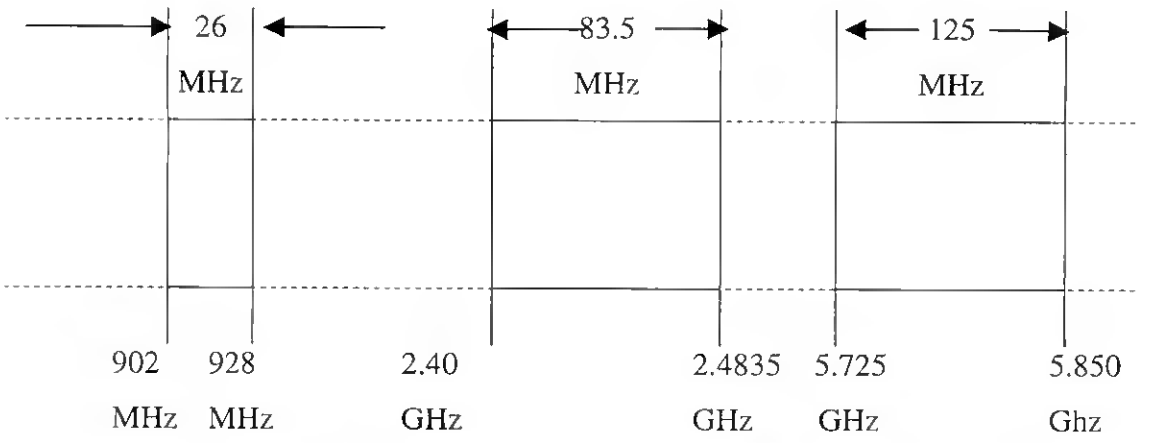


Ilustração 6 - Banda ISM

Em termos práticos a FCC permitiu que os utilizadores operassem produtos para redes sem fios sem obtenção de licenças, por parte deste Organismo, se os mesmos cumprirem certos requisitos. Esta medida eliminou a necessidade de planear frequências, processo moroso e dispendioso. É também uma vantagem caso se pretenda mudar, frequentemente, o equipamento de local, evitando a burocracia de um novo licenciamento.

A maior quantidade de largura de banda está disponível nas bandas de frequências superiores (5.725 GHz a 5.850 GHz), as quais suportarão taxas de dados elevadas. No entanto, a maioria das redes de comunicação de área local sem fios, utilizadas nos Estados Unidos, operam a 902 MHz, contudo esta frequência não está disponível para o mundo todo [27].

A banda de 2.4 GHz é a única, banda não licenciada, disponível no mundo inteiro, incluindo claro o caso de Portugal. Esta banda foi aprovada na América do Norte e Sul em meados dos anos 80 e foi aceite na Europa e Ásia em 1995 [27]. Actualmente, a grande maioria dos fabricantes enquadram os seus produtos na banda de 2.4 GHz. Nestes sistemas o alcance atingido é de cerca de 1 Km em espaço livre e 50 a 100 metros em ambientes interiores, dependendo dos obstáculos a transpor [41].

Apresentamos uma tabela (Tabela 6) que descreve os pontos fortes e fracos das frequências de operação 902 MHz e 2.4 GHz, indicando que a última é, claramente, a melhor escolha para redes de área local sem fios.

Banda 902 MHz	Banda 2.4 GHz
Baixo custo	Custo elevado
Grande intervalo	Pequeno intervalo
Largura de banda limitada (26 MHz)	Largura de banda ampla (83.5 MHz)
Não compatível IEEE 802.11	Compatível IEEE 802.11
Disponível principalmente nos USA	Disponível no mundo inteiro
A maioria das instalações são na América do Norte	A maioria das instalações são na América do Norte e também no estrangeiro

Tabela 6 - Comparação da banda 902 MHz com 2.4 GHz

Um futuro promissor, que já foi alvo das recentes alterações à norma base IEEE 802.11 [36] será, sem dúvida, a utilização da banda de 5.7 GHz que oferece maior largura que qualquer uma das anteriores, permitindo taxas de dados acima de 10 Mbps. Por outro lado, um sistema que opere a 5.7 GHz será também menos susceptível a interferência. Questões como menor intervalo de cobertura, elevada propagação multi-caminho são ainda um factor que limita a sua utilização.

III.2.2. Modulação da portadora rádio

Uma vez determinada a frequência à qual a informação vai ser transmitida esta tem que ser modulada, recorrendo a técnicas de modulação específicas. Nas redes sem fios a modulação, função da camada física (*Physical Layer*), é o processo pelo qual o emissor rádio prepara o sinal de informação digital presente no interior da placa NIC para transmissões através de ondas aéreas.

Em redes WLAN, utilizam-se normalmente sistemas baseados em modulação de fase, com amplitudes de portadora constante tal como a técnica QPSK (*Quadrature Phase Shift Keying*) ou uma das suas variantes. Apesar disso, face às elevadas taxas de transmissão utilizadas, os efeitos de dispersão e multi-caminho, na propagação, acontecem com frequência, pelo que existe um alto nível de interferência, entre bits adjacentes, obrigando à utilização de circuitos de igualização sofisticados.

A modulação de múltiplas sub-portadoras refere-se a primeiro dividir o elevado *bit rate* do sinal binário a ser transmitido, num número de sequências binárias de baixo débito binário. Cada uma dessas sequências será utilizada para modular uma sub-portadora separada, tal como num esquema de portadora simples. Contudo, neste caso, como o nível de interferência (ISI, *InterSymbol Interference*) é mais reduzido, torna-se desnecessária a utilização de equalizadores. Ainda pode ocorrer atenuação (*fading*) de frequência selectiva, sendo provável que apenas uma

(ou um pequeno número) de sub-portadortas seja afectado. Na prática, as sub-portadoras utilizadas são múltiplos inteiros da primeira sub-portadora: f1, 2f1, 3f1,e assim por diante. Por tal facto, o esquema é conhecido como OFDM (*Orthogonal Frequency Division Multiplexing*).

III.2.3. Técnicas de transmissão com espalhamento espectral / Spread Spectrum

Além da utilização da banda ISM, a FCC autoriza a utilização de três técnicas de transmissão com espectro espalhado: FHSS (*Frequency Hopping Spread Spectrum*), DSSS (*Direct Sequence Spread Spectrum*) e um híbrido das anteriores, às quais iremos aludir em seguida.

A técnica de espectro espalhado (*Spread Spectrum*), ilustrada na figura (Ilustração 7), distribuí a potência do sinal numa ampla banda de frequências, sacrificando largura de banda para ganhar em termos da performance sinal / ruído, referido como ganho do processo [27].

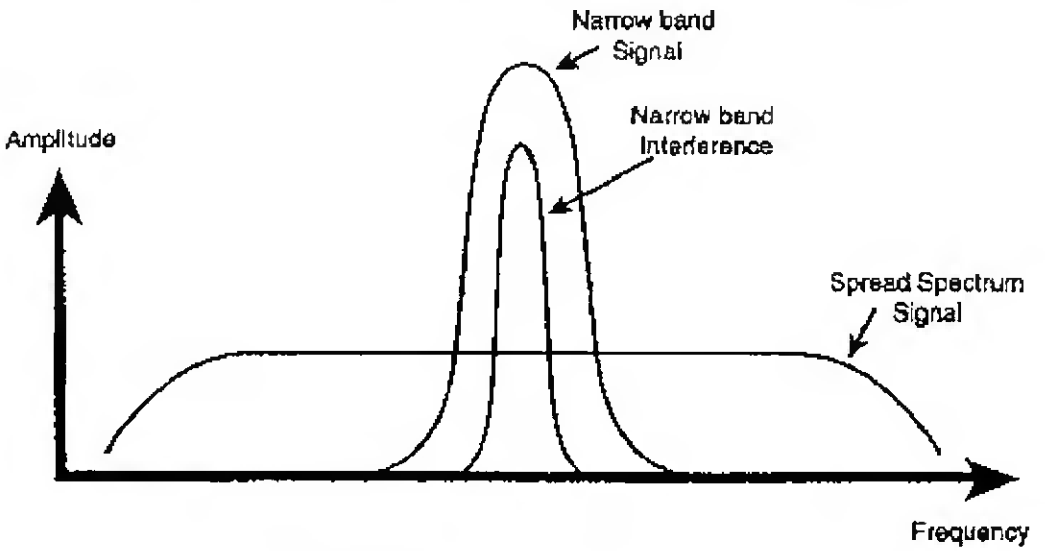


Ilustração 7 - Técnica *Spread Spectrum* [27]

Esta atitude contradiz o desejo de preservar largura de banda, em termos de frequência, mas o processo (espalhamento espectral) torna o sinal de dados mais resistente ao ruído eléctrico quando comparado com as técnicas de modulação rádio convencionais. Assim, o efeito de outras transmissões bem como o ruído eléctrico, modo geral estreito em largura de banda, interferirão apenas com uma pequena porção do sinal espalhado, tendo como resultado menor interferência e menor quantidade de erros aquando da recepção.

A técnica de espalhamento espectral nos dias de hoje, não é vista apenas como uma forma de tornar as comunicações mais seguras relativamente a interferências, mas também como uma maneira de melhorar a qualidade e fiabilidade da ligação. Embora esta técnica tenha surgido

essencialmente de utilizações militares, as suas vantagens têm despertado o interesse de investigadores em inúmeras áreas e a cada dia que passa é maior a sua utilização. O facto de cada transmissão ocupar uma faixa larga do espectro de frequências é compensado pela capacidade, inerente ao sistema, de reduzir a interferência entre sinais que utilizem códigos diferentes, permitindo assim que vários utilizadores comuniquem na mesma banda de frequência.

Existem alguns pontos críticos no desenvolvimento de sistemas de espectro espalhado (*Spread Spectrum*), dos quais podemos citar [9]:

Velocidade de processamento: à medida que são desenvolvidos códigos mais eficientes, os processadores precisam de ser mais rápidos de modo a que a correlação de sequências longas possa ser realizada em tempo real;

Sincronismo entre emissor e receptor: que passa pelas fases de aquisição (início da transmissão) e teste (durante a comunicação), necessita de ser estabelecido no mais curto intervalo de tempo possível.

Deverá ser encontrado um ponto de equilíbrio entre o comprimento da sequência de espalhamento e o tempo de sincronismo, em conformidade com a utilização do sistema. Esta atitude justifica-se dado que sequências maiores são desejáveis mas, por outro lado, acarretam maior tempo na obtenção do sincronismo inicial do sistema.

Em termos práticos, um dispositivo rádio usa uma conexão RS-232 como interface de dados série e pode transmitir assincronamente a velocidades até 38.4 Kbps. Este recebe e transmite dados numa faixa de frequência de 902 - 928 MHz a velocidades de 128 Kbps. Ao comunicar à velocidade aérea de 128 Kbps permite simular comunicação *full duplex* (transmissão bidireccional, na qual os dispositivos enviam os dados simultaneamente).

O sistema pode, também, ser configurado para comunicações ponto a ponto ou multi-ponto [3]. Por outro lado, contem um módulo controlador de pacotes com um protocolo de comunicação proprietário que prevê *handshaking* (aperto de mão / negociação), detecção de erros, sequência de pacotes, controle de fluxo e pode suportar até três repetidores para alargar a distância de comunicação.

III.2.3.1. Sequência directa no espectro espalhado (DSSS / Direct Sequence Spread Spectrum)

A técnica DSSS combina o sinal de dados, na estação emissora, com uma sequência de bits de elevada taxa de dados. Esta sequência pseudo-aletória é também referida como sequência de

espalhamento (*spreading sequence*), cada bit na sequência como um *chip* ou *chipping code*, o bit rate resultante como *chipping rate* e o número de bits na sequência é o factor de espalhamento (*spreading factor*).

O factor de espalhamento (*spreading factor*) determina a performance do sistema, normalmente é expresso em decibeis (dB) e é, também, conhecido como ganho do processo. Assim, o ganho do processo é o logaritmo do factor de espalhamento. A titulo de exemplo, um sistema de espectro espalhado com um factor de espalhamento de 10:1, tem um ganho de processo de 10 dB, um de 100:1 de 20 dB e assim sucessivamente. Um ganho de processo elevado aumenta a resistência do sinal à interferência.

Em termos da relação Sinal - Ruído o ganho do processo efectivo é subtraído do anterior. Se um sistema que não utilize espalhamento do espectro requerer uma relação sinal / ruído de, por exemplo, 10 dB (a potência do sinal é 10 vezes a potência do ruído), então com um sistema de espalhamento de espectro com ganho de processo de 10 dB, o sistema operaria de modo satisfatório, mesmo quando a potência do sinal for igual à potência do ruído.

As redes de comunicação de área local sem fios podem, como opção, usar a técnica DSSS também conhecida como pseudo - ruído (*pseudonoise*) [14]. Como tal os emissores enviam o sinal adicionando-lhe bits de dados redundantes, denominados *chips* , ou seja um falso ruído, garantindo assim resistência a interferências.

Segundo normas da FCC cada sinal deve ter dez ou mais *chips*, isto é, o ganho de processo linear mínimo permitido é 10 [27]. Isso limita a velocidade máxima dos emissores desta técnica a 2 Mbps na banda de 902 MHz e 8 Mbps na banda de 2.4 GHz. O número de *chips* está, como já se disse, directamente relacionado com a imunidade do sinal a interferências, assim numa área com muita interferência rádio, e não outros tipos de erros, é necessário diminuir a velocidade (aumentar os *chips*) para evitar a corrupção de dados. Por outro lado, o standard IEEE 802.11, ao qual faremos alusão em secção apropriada nesta dissertação (CAPITULO V), determinou que o número de *chips* para DSSS fosse de onze isto é, definiu o seu ganho de processo mínimo a 11.

Em termos gerais o funcionamento da técnica DSSS é o seguinte, uma portadora é modulada em fase por um sinal digital, também referido como sequência binária pseudo-aleatória (valores representados são discretos). O sinal resultante é modulado, uma segunda vez, para uma portadora de rádio frequência.

A figura (Ilustração 8) exibe um exemplo da operação de DSSS. Um *chipping code* é designado para representar os bits de dados lógicos, 0 e 1. Como a trama de dados a ser enviada é " 101 ", o código correspondente é efectivamente enviado.

Chipping Code:	0 = 11101100011 1 = 00010011100
Data Stream :	101
Transmitted Sequence :	

00010011100	11101100011	00010011100
1	0	1

Ilustração 8 - Exemplo da operação DSSS para " 101 "

Os utilizadores da mesma rede sem fios conhecem a sequência binária pseudo-aleatória que está a ser utilizada. Nesta, todos os dados transmitidos são precedidos de uma sequência (*preamble*) seguindo-se uma delimitação de início de trama (*start-of-frame*). Este processo é ilustrado na figura (Ilustração 9).

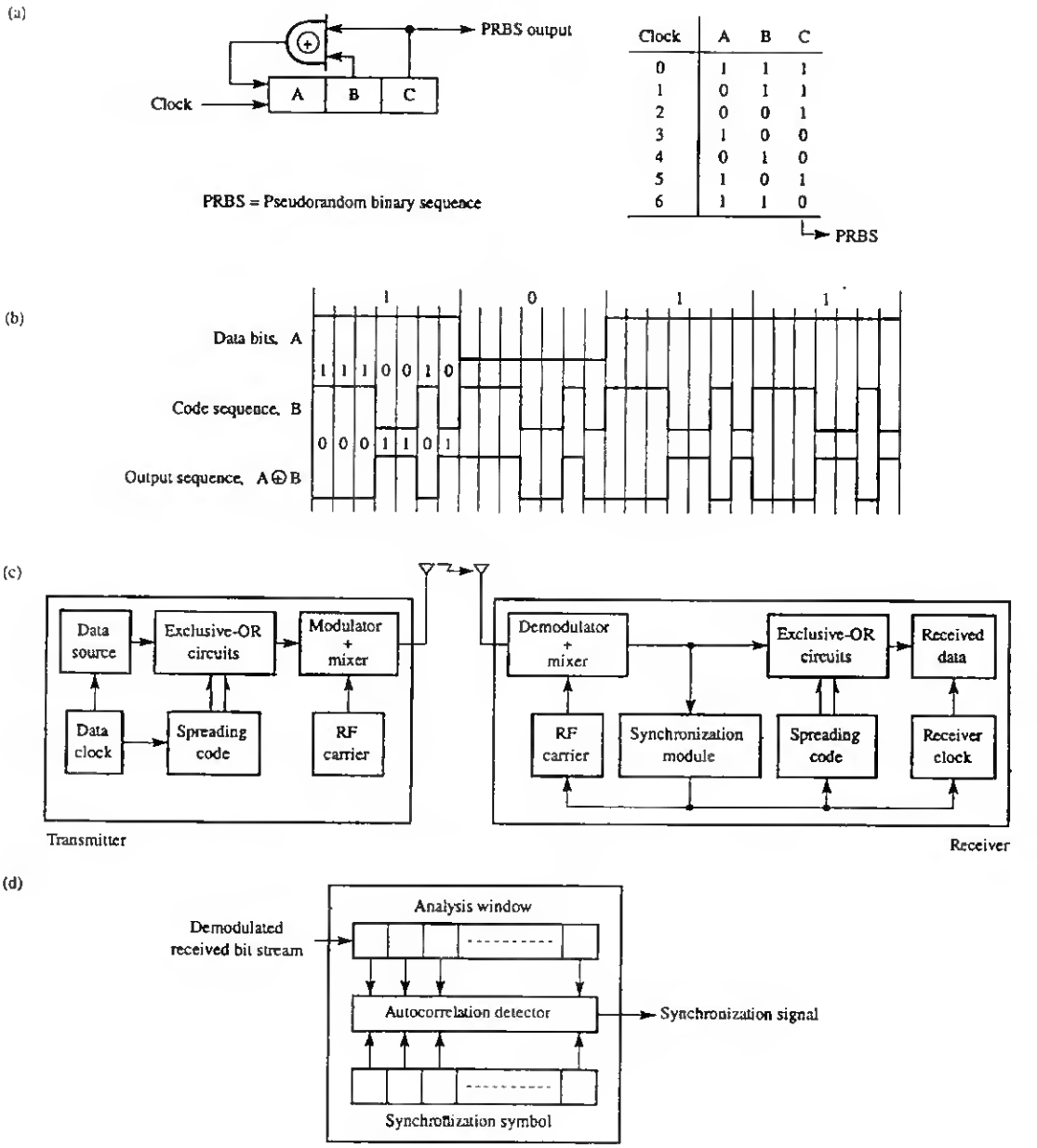


Ilustração 9 - Operação DSSS [22]

Os receptores depois de desmodularem o sinal transmitido procuram a sequência (*preamble*), que normalmente é a *string* de todos os bits definidos a 1, até que a mesma seja localizada e estes se preparem para interpretar o sinal recebido. Aguardam, então, a recepção do delimitador de início de trama (*start-of-frame*) e começam a receber o conteúdo da trama (*frame contents*). O receptor deve estar, por esta razão, em sincronismo com o sinal recebido, o que é conseguido pela transmissão de uma sequência binária padrão (preambulo como por exemplo sequência de 1s), no início de cada trama transmitida. Obtém-se a sincronização se ao receber este preambulo espalhado, ele for passado através de um *n-bit shift register*, onde n é o número de bits na

sequência espalhada, for comparado numa base chip-a-chip, com a sequência espalhada conhecida, correspondente ao bit fonte 1 (do preambulo). Se 2 bits numa determinada posição do *chip* são iguais, diz-se que há um acordo (A), se forem diferentes haverá um desacordo (D). A medida da diferença entre dois símbolos, é determinada pela diferença do número de Ds do número de As. Por outro lado, um receptor de DS necessita de conhecer o código de difusão, de um dado emissor, para poder decifrar os dados correctamente. Uma vez que capte todos os sinais de dados usa um correlator, baseado no código de difusão, para remover os *chips* e devolver o sinal ao tamanho original. É este, também, que permite que diversos sistemas, que usem esta tecnologia, operem na mesma área sem interferir com outros.

Devido a considerações de ordem prática e principalmente pela dificuldade de obtenção de sincronismo no receptor, com precisão superior a alguns nanosegundos, os sistemas *Spread Spectrum* actuais que usem *Direct Sequence*, operam tipicamente com geradores de código cuja taxa é menor ou igual a 100 Mbps, implicando uma banda de espalhamento de frequências limitada a algumas dezenas de MHz.

Pode parecer que todos os utilizadores ao operarem na mesma rede sem fios utilizando a mesma banda de frequências e o mesmo código pseudo-aleatório as suas transmissões irão interferir umas com as outras. Contudo, tal não acontece porque é resolvido pelos protocolos da camada MAC, os quais serão abordados em secção própria nesta dissertação (CAPITULO IV), que asseguram que apenas uma transmissão tenha lugar de cada vez. Os requisitos de sincronismo entre o emissor e o receptor são superiores nesta técnica quando comparada com outras. A técnica DSSS é também utilizada como meio de combate à dispersão multi-caminho, embora necessite de maiores larguras de banda.

Implementação de DSSS segundo a norma IEEE802.11

A primeira versão do standard IEEE 802.11, ao qual fazemos alusão em secção própria (CAPITULO V), especifica, relativamente às taxas de dados, o mesmo valor para ambas DSSS e FHSS embora, versões posteriores, IEEE 802.11b, suportem taxas de dados superiores para DSSS [21], [36]. Por outro lado, se as características desta técnica, em vez de desvantagens, tiverem peso superior relativamente à utilização de FHSS e IR, então a opção da camada física deverá ser DSSS.

A operação da subcamada PMD / DSSS converte a representação binária de PPDUs num sinal rádio adequado a transmissão. A camada física DSSS executa este processo pela multiplicação de uma portadora RF por um sinal digital ortogonal (*Pseudo*-Noise). A ideia geral, tal como

anteriormente referido, é a de primeiro espalhar digitalmente a trama de dados em banda base, isto é a PPDU, e depois modular os dados espalhados para uma frequência em particular. A figura (Ilustração 10) ilustra os componentes típicos de um emissor DSSS.

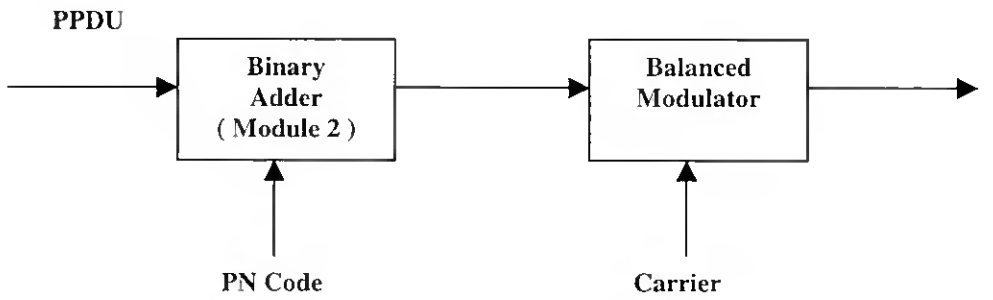


Ilustração 10 - Transmissor DSSS

A segunda modulação imposta ao sinal, efectuada pelo modulador (*Balanced Modulator*), comuta o sinal em banda base para a frequência de transmissão à qual opera o canal escolhido. Esta é denominada função modulação na frequência e funciona do seguinte modo. A subcamada PMD DSSS transmite o PPDU inicial a 1, 2 ou 11 Mbps, usando diferentes tipos de modulação, dependendo de qual a taxa de dados escolhida.

III.2.3.2. Salto na frequência no espectro espalhado (FHSS / Frequency Hopping Spread Spectrum)

Os sistemas FHSS operam em conformidade com o conceito implícito ao próprio nome. Assim, o sinal de dados original é modulado para uma portadora, cuja frequência salta em função do tempo, numa ampla banda de frequências. O salto na frequência dos sinais rádio, por exemplo, mudará a sua frequência da portadora na banda de 2.4 GHz, entre 2.4 e 2.483 GHz.

Na modulação FHSS a banda disponível é dividida num conjunto de canais de igual largura de banda. A FCC especifica a largura de banda de cada canal e o número mínimo de canais utilizados em cada banda ISM. Assim, na banda dos 915 MHz os canais estão limitados a 0.5 MHz e devem ser utilizados 50 dos 52 disponíveis. Nas bandas dos 2.4 e 5.8 GHz os canais estão limitados a 1.0 MHz e o número de canais disponíveis é, respectivamente 83 e 125, dos quais 75 devem ser utilizados [41]. Por outro lado, a FCC requer que os fabricantes usem no mínimo 75 frequências por canal de transmissão com um tempo máximo de pausa (*dwell time* – tempo gasto numa dada frequência, em particular, durante um único salto) de 400 ms [27].

Quanto ao seu funcionamento, no emissor um código de salto (*hopping code*) determinará as frequências nas quais o dispositivo rádio transmitirá e em que ordem. O receptor, para que o

sinal possa ser recebido de modo adequado, deve conhecer o código de salto bem como escutar o sinal enviado no momento exacto e na frequência correcta. Se o emissor rádio se deparar com interferência numa dada frequência, este irá retransmitir o sinal, no salto subsequente, numa frequência diferente.

Atendendo à natureza desta técnica de modulação, poderão ser alcançadas taxas de dados até 2 Mbps, dado que valores superiores seriam susceptíveis de um grande número de erros [27]. Por outro lado, reduz interferências porque um sinal que as cause, proveniente de um sistema de banda estreita, afectará o sinal espalhado no espectro apenas se ambos forem transmitidos na mesma frequência e em simultâneo. Por tal facto, a interferência agregada será bastante reduzida, resultando em poucos ou mesmo nenhuns erros de bits.

Nestes sistemas, como anteriormente referido, tanto o emissor como o receptor têm que estar sincronizados permanecendo num canal por um determinado período de tempo, denominado *chip*, após o qual transitam para outro canal. A transição de um canal para outro é denominada por salto (*hop*). A razão entre a velocidade com que mudam de canal (*chipping rate*) e a velocidade de transmissão faz a diferença entre dois tipos de sistemas: *fast*-FHSS e *slow*-FHSS, conforme ilustrado na figura (Ilustração 11). Em ambos os casos uma frequência portadora é utilizada no centro de cada canal.

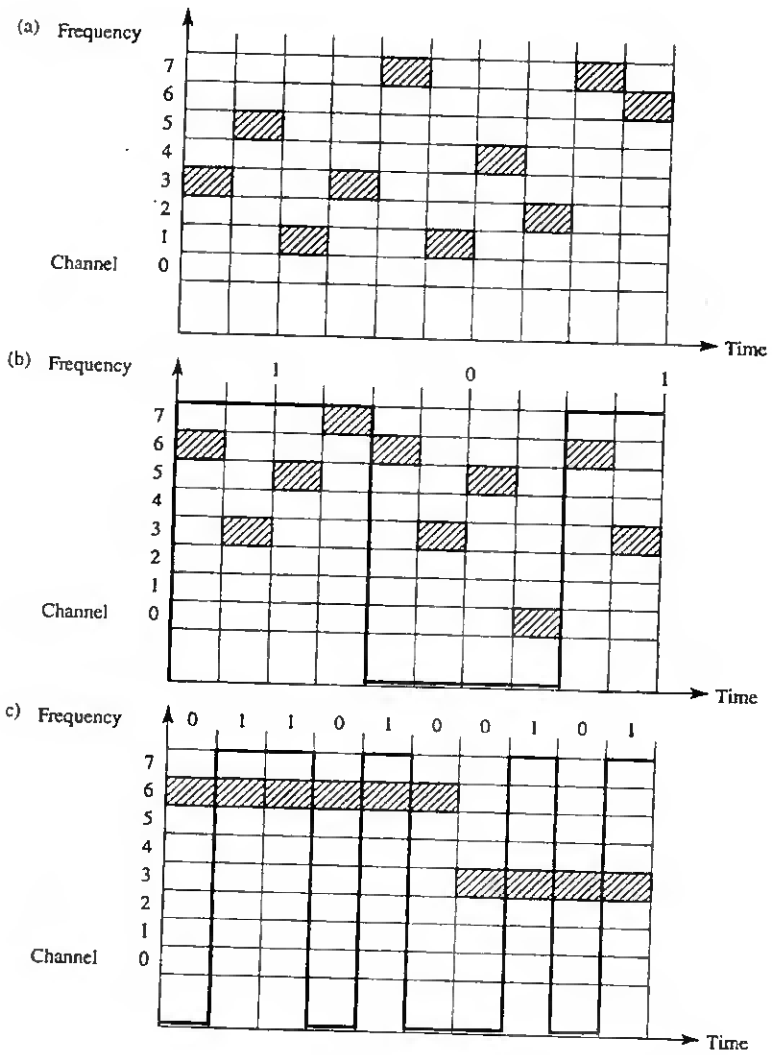


Ilustração 11 - Fast / Slow FHSS [22]

Pode dizer-se que o sistema realiza um salto na frequência rápida (FFH, *Fast Frequency Hopping*), quando o mesmo executa vários saltos durante um bit de informação e um salto na frequência lenta (SHF, *Slow Frequency Hopping*) quando são transmitidos vários bits de informação em cada salto. A tecnologia actual permite saltos nas bandas de frequências da ordem de vários GHz, valor este bem maior do que os possíveis de obter para as bandas de *Spread* por *Direct Sequence*. Relativamente à taxa de salto, já se encontram hoje sistemas capazes de realizar centenas de Ksalto/Seg e outros, em desenvolvimento, já realizam testes de saltos superiores a 1 Msalto/Seg.

No sistema *fast*-FHSS a velocidade de comutação de canal é superior à velocidade de transmissão, ao passo que no segundo acontece o contrário. Assim, os sistemas f*ast*-FHSS são menos susceptíveis a interferências porque cada bit é transmitido em vários canais, em oposição aos sistemas *slow*-FHSS, nos quais em cada *chip* é transmitido, pelo menos, um pacote. Contudo, para velocidades de transmissão elevadas os sistemas *fast*-FHSS apresentam custos e

consumo de potência muito elevados [41]. Tais factores condicionam a utilização desta técnica em redes de área local, sendo favorecida a sua oponente.

Nesta técnica um emissor envia o sinal sobre uma série, aparentemente aleatória, de frequências rádio [14]. Um receptor, em sintonia, capta o sinal saltando entre essas frequências. A mensagem é totalmente recebida apenas se a série de frequências for conhecida ou seja, apenas o receptor conhecedor das frequências nas quais o emissor saltará o sinal, poderá receber com sucesso os dados (o receptor contém o mesmo algarismo do emissor).

A sequência pseudo-aleatória (código de dispersão), alimenta o sintetizador de frequências que gera o sinal portador (onda rádio modulada com informação de algum tipo, segundo um método especifico) a ser transmitido, fazendo com que este varie aleatoriamente dentro da banda de dispersão. Em cada instante a portadora assume um dos 2k valores possíveis de frequências, onde k é o tamanho da sequência de código utilizada. O código de espalhamento neste caso, não modula directamente a portadora (f_0) que contém a informação, sendo utilizado na determinação das frequências que serão geradas pelo sintetizador [9].

Em contrate com o sistema *Direct Sequence*, que descrevemos anteriormente, onde a sequência de espalhamento é utilizada sequencialmente (um bit de cada vez), aqui ela é utilizada em paralelo (k bits de cada vez), fornecendo ao sintetizador, a cada instante, um número pseudo aleatório de 0 a 2k-1 correspondente à frequência que será gerada. Deste modo, o sinal a ser transmitido consiste na frequência da portadora f_0 modulada inicialmente pelos dados a serem transmitidos e alterada para a frequência $f_0 + f_N$ (através de uma modulação GFSK (*Gaussian Frequency Shift Key*), que é a mais utilizada), onde f_N é a frequência gerada pelo sintetizador a cada salto. Num dado salto, a faixa de frequência ocupada pelo sinal é idêntica à de um sinal GFSK convencional, que é tipicamente muito menor que a banda de espalhamento. Finalmente, numa média realizada ao longo de muitos saltos, o espectro do sinal resultante ocupará toda a banda de espalhamento (*Spread*).

Outra característica a ser tida em consideração é facto de ser possível ter vários dispositivos rádio a operar, usando FHSS, na mesma banda de frequência sem que isso cause interferência entre eles. Para tal assume-se que cada um deles usa um padrão de salto (*hopping pattern*) diferente, enquanto um está a transmitir numa frequência em particular o outro estará a usar uma frequência diferente. Um conjunto de códigos de salto (*hopping codes*) que nunca usem as mesmas frequências simultaneamente é considerado ortogonal.

Os requisitos da FCC, para o número de frequências de transmissão diferentes, permite que os utilizadores desta técnica possuam muitos canais de não interferência.

Implementação de FHSS segundo a norma IEEE 802.11

A subcamada PMD FHSS transmite os dados binários a taxas de 1 ou 2 Mbps usando um tipo de modulação específico para cada, dependendo da taxa de dados escolhida.

É usada modulação GFSK (*Gaussian Frequency Shift Key*) de dois níveis, para a transmissão de tramas de dados a 1 Mbps. É usada modulação GFSK (*Gaussian Frequency Shift Key*) de quatro níveis, para a transmissão de tramas de dados a 2 Mbps. As estações que implementem esta versão deverão, também, ser capazes de operar a 1 Mbps para a totalidade da MSDU. Na operação a 2 Mbps, a entrada do modulador são combinações de 2 bits (00, 01, 10 ou 11) provenientes da subcamada PLCP. Cada um destes símbolos, de 2 bits, é enviado a 1 Mbps, significando que cada bit é enviado a 2 Mbps. Deste modo, esta técnica de modulação, de 4 níveis, duplica a taxa de dados mantendo a mesma *baud rate* do sinal de 1 Mbps.

III.2.3.3. Comparação das técnica

Quando se optar pela camada física DSSS, devemos ter em conta os seguintes factores, comparativamente a FHSS: custo superior; consumo de potência elevado; taxas de dados potencialmente elevadas das camadas físicas individuais; capacidade agregada inferior a FHSS quando se usam múltiplas camadas físicas; menor número de células rádio geograficamente separadas, devido ao limitado número de canais e maior área de cobertura que qualquer uma das outras técnicas FHSS e IR [27].

Uma vantagem da camada física FHSS em relação à técnica de sequência directa, é a sua capacidade para evitar a utilização de canais seleccionados, numa banda de frequência alocada, por todos. Nesta técnica, se há uma fonte a transmitir e a interferir com o nosso sistema, é possível eliminar a utilização dessa frequência na nossa sequência de salto. É particularmente útil nas transmissões com salto lento de frequência já que com salto rápido de frequência, múltiplos saltos por bit de dados são utilizados e consequentemente apenas um simples *chip* será afectado.

Em termos de velocidade, se comparar-mos DSSS com FHSS, a primeira pode atingir taxas de dados muito mais elevadas que 2 Mbps. No entanto, na maioria dos casos, FHSS é o tipo mais efectivo para redes de área local sem fios, se as necessidades em termos de largura de banda da rede forem 2 Mbps ou inferior. Por seu lado, DSSS possui potencialidade para taxas de dados superiores, a qual será mais adequada para aplicações que requeiram grande largura de banda.

Em termos de custos, se comparar-mos as duas técnicas, *slow*-FHSS e DSSS, apesar de ambas apresentarem custos de implementação relativamente baixos, os da técnica DSSS são inferiores. Tal deve-se ao facto dos transceptores da primeira técnica necessitarem de filtros fortemente selectivos e de circuitos detectores de frequência de grande estabilidade. Relativamente à velocidade de transmissão esta é superior para os sistemas *slow*-FHSS, para a mesma largura de banda disponível [41].

Em termos regulamentares, a FCC exige um factor de espalhamento de pelo menos 10 para os sistemas DSSS, o que significa que a velocidade de transmissão de um sistema cuja largura de banda é W não excede W/10 [41]. Nos sistemas *slow*-FHSS a velocidade de transmissão não depende da disposição geográfica das estações e, demonstra-se que para uma largura de banda disponível W, no pior dos casos é W/4. Na banda ISM os sistemas *slow*-FHSS são também menos susceptíveis a interferência provocada por sistemas a operar na mesma banda, sendo esta resultado da flexibilidade com que é gerida a sua largura de banda (maior número de canais na largura de banda disponível).

Finalmente iremos abordar a coexistência de múltiplas redes na mesma área geográfica. Nos sistemas DSSS isso apenas é possível se este utilizar uma única fracção da largura de banda total disponível. Em tais situações podem sobrepor-se algumas redes, na mesma área geográfica, desde que cada uma delas use um canal diferente. Nos sistemas *slow*-FHSS a sobreposição de redes é possível dado que cada rede utiliza o seu próprio padrão de saltos na frequência. Os canais podem eventualmente sobrepor-se, porque é possível definir conjuntos de padrões de saltos em qualquer subconjunto, de um dado conjunto, que interfere, quanto muito, numa única frequência com qualquer outro retirado do mesmo conjunto [41].

A decisão sobre qual o método a utilizar depende da performance desejada, assim se for necessária alta velocidade e não existirem problemas de interferências, pode ser usada sequência directa (*Direct Sequence*) de forma pacifica. Por outro lado, se não houver necessidade de velocidade superior a 2 Mbps, salto na frequência (*Frequency Hopping*) oferece uma solução menos dispendiosa e de igual fiabilidade. Qualquer que seja o método de espalhamento espectral utilizado, o resultado final é um sistema extremamente fiável relativamente a intrusão, não interferindo com outros serviços e ainda com uma largura de banda razoável para o transporte de dados.

III.3. Transmissão por infravermelhos em redes de área local

A luz infravermelha há muito que tem sido usada como técnica de transmissão para comunicações locais de curta distância, como é o caso das redes locais. De entre as vantagens desta utilização, em particular, são de fácil e rápida instalação e não requerem licenças caras ou morosas. Como principais desvantagens dos sistemas infravermelhos, aplicados a redes locais, podemos apontar: distâncias limitadas; larguras de banda limitadas e transmissões sujeitas a atenuação e ruído.

A operação dos controles remotos por infravermelhos, anteriormente descrita, é extremamente simples, mas as redes de comunicação de área local sem fios por infravermelhos não são muito mais complexas. A principal diferença reside no facto destas utilizarem luz infravermelha a níveis de potência ligeiramente superiores e protocolos de comunicação para transportar os dados. A luz infravermelha é, sem dúvida, uma alternativa ao uso de ondas rádio para conectividade em redes de comunicação de área local sem fios. O seu comprimento de onda é maior (baixo em frequência) dos que nas cores espectrais, mas muito menor (superior em frequência) do que as ondas rádio, como tal, sob a maior parte das condições de iluminação a luz infravermelha é invisível a olho nu.

Os produtos para redes de área local sem fios com tecnologia por infravermelhos operam com comprimentos de onda por volta de 820 nm, porque o ar oferece a menor atenuação nesse ponto do espectro infravermelho [27]; actuam no espectro de frequência infravermelho (100 terahertz (THz)) e são não licenciadas. Por outro lado, a maioria dos fornecedores recomendam distâncias inferiores a aproximadamente um quilómetro para que possa ser mantida a fiabilidade e integridade da transmissão infravermelha. Comparativamente, a frequência das ondas de infravermelhos é muito superior à das ondas rádio, sendo os dispositivos que as transmitem classificados de acordo com o tamanho do comprimento da onda que é emitida e que é recebida.

Como vantagens e desvantagens podemos referir que, os infravermelhos possuem propriedades idênticas ás da transmissão da luz, por isso são reflectidos por superfícies brilhantes, atravessam o vidro, mas não passam através de paredes ou objectos opacos, oferecendo elevado grau de segurança. Comparativamente às ondas rádio, tornam-se vantajosos, eliminado as possibilidades de interferências com redes próximas. De igual modo, também as fontes de ruído comum, como por exemplo fornos microondas e transmissores rádio, não interferem com o sinal de luz.

Em termos de performance, a luz infravermelha faz uma melhor gestão da largura de banda, tornando possível a operação a taxas de dados verdadeiramente elevadas que podem atingir

valores de 2 Mbps. A luz infravermelha, contudo, não é tão adequada, como as ondas rádio, para aplicações móveis porque é limitada em termos de área de cobertura.

Devemos sublinhar que, quando se opera na gama dos infravermelhos, temos que ter particular atenção ás interferências da luz ambiente. A luz solar, bem como a luz proveniente de lâmpadas eléctricas, possuem quantidades significativas de infravermelhos que irão ser recebidos pelo receptor. Poderemos resolver este problema por meio da utilização de filtros que eliminam as radiações não pertencentes ao sinal de transmissão.

III.3.1. Requisitos de licenciamento

Sempre que a tecnologia infravermelha se integre no espectro de luz invisível, as questões de licenças não são alvo de negociação. Não existem linhas regulamentares para a utilização do sistema neste espectro de frequência. Como resultado, torna-se muito mais fácil analisar apenas as questões inerentes à tecnologia *per si* e, deste modo, o utilizador pode colocar um sistema a funcionar rapidamente.

Contrariamente à tecnologia rádio, na qual a maior parte do espectro de frequências requer licenças e espaço livre por parte dos organismos reguladores, a utilização de luz, teoricamente, não causa interferências entre sistemas. Deste modo, qualquer utilização deste espectro é permitida com escassos, ou mesmo sem quaisquer, esforços de coordenação.

Outra características atractiva desta tecnologia, é o facto de dois sistemas poderem ser instalados lado a lado, ou mesmo atravessar cada um dos respectivos caminhos, desde que o angulo receptor de aceitação não coexista no mesmo eixo. Contudo, não nos devemos esquecer da limitação da distância. Como consideração adicional devemos referir que, os fabricantes desta tecnologia devem considerar as limitações da radiação e estar alertados para o facto de que o contacto directo com o feixe de saída deve ser evitado, devido aos riscos provenientes da exposição directa. Pelo exposto é obrigatório que passem por um processo de certificação.

O IrDA (*Infrared Data Association*), que é um grupo constituído por mais de 80 empresas de computadores, telecomunicações que inclui, por exemplo, a HP; AMP; Apple Computer; AST; IBM, Intel; Novell entre muitas outras, adoptou um standard que cobre três níveis da arquitectura de redes: IrDASIR, *Serial Infrared Physical Layer Link* (Nível 1); IrLAP, *Ir Link Access Protocol* (Nível 2) e IrLMP, *Ir Link Management and Transport Protocols*. Estes standards especificam transmissões, ponto a ponto, por infravermelhos a 115.2 Kbps entre dispositivos. Outros standards de velocidade superior, como por exemplo 1.15 Mbps e 4 Mbps,

os quais serão mais adequados para *backup* e armazenamento *offline*, estão actualmente a ser estudados pelo IrDA [27].

III.3.2. Modulação IR

Nestes sistemas, o sinal de infravermelhos emitido é focado para o receptor, que o converte no sinal eléctrico equivalente. Este modo de operar é conhecido como modulação de intensidade com detecção directa (IMDD). Existem, basicamente, dois tipos de emissores de infravermelhos (componentes optoelectrónicos), os díodos LASER e os emissores de luz, mais conhecidos como *LEDs* (*Light Emitting Diodes*). Como receptores utilizam-se fotodetectores PIN ou APDs.

O emissor do tipo LASER é utilizado para transmitir em sistemas de fibra óptica os quais, atendendo ás suas características peculiares, permitem obter uma densidade de potência distribuída muito forte. Nas redes sem fios como a propagação é feita em espaço aberto, não por cabos de fibra óptica, a emissão de laser tem que ser bastante mais forte, cuidada e difusa de modo a não causar, por exemplo, graves danos à vista humana.

O emissor do tipo *LED* possui uma banda de frequências com comprimento de onda entre os 25 e 100 nm e com uma potência emitida muito menor tornando-se, por isso, muito mais seguro. A velocidade de transmissão pode ir até 10 Mbps. Se pretender-mos obter uma velocidade superior será necessário utilizar o LASER, que permite centenas de MHz de largura de banda. Atendendo ao seu baixo custo, normalmente, utilizam-se *LEDs* desde que se consideram razoáveis taxas de bits até 10 Mbps. Por outro lado apresentam circuitos de *driver* menos complexos e menores problemas de segurança. Os *LEDs* introduzem, todavia, algumas limitações resultantes da reduzida eficiência de conversão optoelectrónica e da reduzida largura de banda, as quais se reflectem, sobretudo, no alcance e na velocidade de transmissão.

Nos receptores utilizam-se normalmente fotodetectores PIN porque têm baixo custo e consumo reduzido. A área de detecção destes determina, em parte, a sensibilidade do receptor e áreas maiores possibilitam a recolha de mais potência óptica. Contudo, estas implicam também maiores capacidades, as quais limitam a largura de banda. A potência do receptor depende, também, da sua posição e orientação em virtude da elevada gama óptica do canal.

Quando comparados, com os receptores de rádio frequência, os receptores de infravermelhos são mais simples resultado de apenas terem que detectar a intensidade dos sinais ópticos e não a sua frequência ou fase.

Em termos de implementação física, uma rede local com tecnologia infravermelha, tem dois componentes principais: Placa adaptadora ou unidade, que é ligada ao PC ou impressora via um

slot de expansão tipo ISA ou PCMCIA (ou conexão por meio de porta paralela) e *Transducer* este dispositivo, idêntico às antenas das redes sem fios baseadas em rádio, é colocado numa parede ou outra qualquer localização do ambiente. As placas adaptadoras manusciam os protocolos necessários para operar num ambiente onde o meio é partilhado e os *transducers* emitem e recebem os sinais de luz.

Como modos de propagação do sinal num canal de infravermelhos, poderemos decidir por uma de duas opções conducentes a dois tipos de redes sem fios com tecnologia por infravermelhos: Ponto a ponto e Difusão (*diffused*).

No modo de propagação ponto a ponto o emissor aponta directamente para o receptor, ou seja em linha de vista e alinhados um pelo outro. Este modo de propagação conduz a sistemas bastante rígidos em termos de tolerância a movimentos das estações, face à limitação imposta pela largura do feixe. Os emissores deverão ter uma grande potência, o mesmo não sendo necessário para os receptores. Para uma mesma potência transmitida quanto mais estreito o feixe maior será o seu alcance, podendo chegar até às dezenas de quilómetros. Este método é o aconselhado para a comunicação entre dois equipamentos, por exemplo para a transferência de ficheiros entre um *LapTop* e um computador, sendo extremamente sensível a obstáculos que se introduzam no meio de ambos.

Nas aplicações de redes de locais sem fios, normalmente, são necessárias operações de um para vários (*broadcast*) pelo que o modo de transmissão mais usado é a difusão do sinal de infravermelhos. Essencialmente são usados os seguintes modos de difusão do sinal, técnica que usa protocolos *Carrier Sense* para partilhar o acesso ao meio:

Modo básico: Existe um emissor infravermelho e um detector associado em cada computador. O sinal infravermelho depois de emitido é captado pelo receptor, após múltiplas reflexões nas paredes do ambiente ou tecto que actuam como ponto de reflexão.

Antenas direccionadas: Este método consiste na colocação de antenas direccionadas para zonas especificas, para as quais os detectores se encontram direccionados.

Devido à geometria, a luz infravermelha difusa está limitada em termos de distância de separação, normalmente de 90 centímetros a 2 metros. Por outro lado, como depende de pontos de difusão, como o tecto, estas redes não operam em espaços exteriores. As estações podem ser livremente orientadas, já que este modo de propagação se baseia em sucessivas reflexões do sinal emitido. Contudo, esta flexibilidade tem custos que se traduzem nas elevadas quantidades de potência que uma estação terá que emitir. Esta deverá ser tal que por sucessivas reflexões se atinja toda a área de cobertura da célula, podendo assim ser recebida por qualquer estação, independentemente da sua posição e orientação da célula.

A principal vantagem desta tecnologia em ambos os modos, ponto a ponto e difusão, é a sua habilidade para transportar uma grande largura de banda, podendo atingir velocidades até 16 Mbps (maiores que outros sistemas), operando na faixa de 100 THz. Contudo, teremos que referir que os infravermelhos podem ser facilmente obstruídos: a luz não consegue atravessar objectos sólidos e opacos, pode estar sujeira a interferências da luz ambiente e exige linha de visão directa entre dois pontos.

Operação IR segundo a norma IEEE 802.11

A camada física IR 802.11 opera usando transmissão indirecta por difusão, como exibido na figura (Ilustração 12), eliminando a necessidade de operação com linha de vista. Nestes sistemas, o tecto é usado como ponto de reflexão de modo a suportar o protocolos de *carrier sense*. Este tipo de transmissão é, muitas vezes, referido como infravermelhos por difusão (*diffused infrared*).

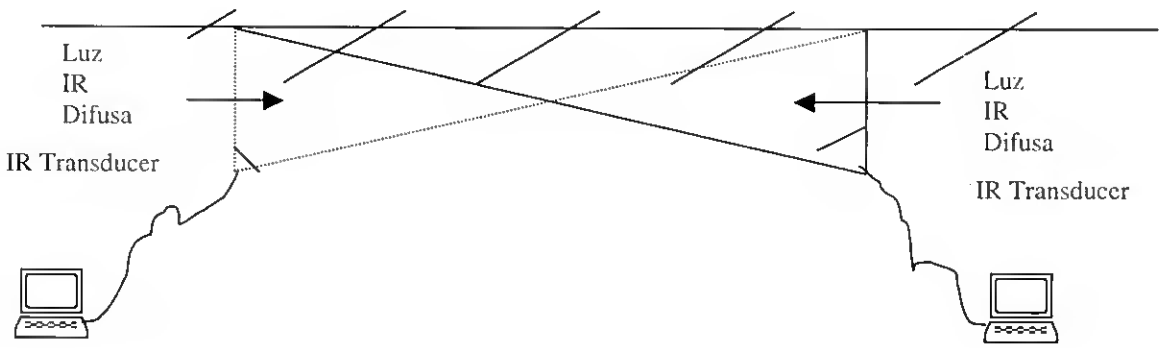


Ilustração 12 - Sistema IR base 802.11

Devida a esta forma de transmissão, a camada física IR é planeada apenas para operações em interior onde exista a presença de um tecto para reflectir os sinais. As janelas podem, de modo significativo, atenuar os sinais infravermelhos, daí serem necessários testes prévios. Devida à utilização do tecto como ponto de reflexão, os dispositivos IR 802.11 são limitados quanto ao espaço de transmissão. Podemos referir distâncias de 10 a 20 metros, dependendo da altura do tecto [27].

A camada física IR transmite os seus sinais próximo do intervalo da luz visível, 850 – 950 nm, ao nível máximo de potência transmitida de 2 watts de pico óptico. Devida à, relativamente, elevada potência de transmissão não existem restrições regulamentares, em termos de

frequência, para os sistemas IR. Na realidade, o único standard que se aplica aos sistema IR compatíveis 802.11 são regras de segurança, denominadas IEC 60825-1 e ANSI Z136.1 [27].

A subcamada PMD IR transmite os dados binários a ambas as taxas, 1 Mbps (Taxa de Acesso Básico) ou 2 Mbps (Taxa de Acesso Melhorado) usando, para cada, um tipo de modulação específico. Para operação a 1 Mbps, a PMD IR usa PPM / 16 (16- *Pulse Position Modulation*) e para operação a 2 Mbps, a PMD IR usa PPM / 4 (4- *Pulse Position Modulation*).

III.4. Considerações adicionais a ambas as técnicas

A escolha da camada física depende dos requisitos da aplicação. Segundo o padrão IEEE 802.11 existem três possibilidades de camadas para o nível físico (Nível Físico do Modelo OSI):

⇒ Rádio na banda de 2.4 GHz com salto de frequência (FHSS);

⇒ Rádio na banda de 2.4 GHz com sequência directa de frequências (DSSS);

⇒ Luz no espectro infravermelho (IR).

Adicionalmente a estes tipos, foram especificadas, inicialmente, as taxas binárias de 1 e 2 Mbps para FHSS, DSSS e IR. Posteriormente foram adicionadas as velocidades de 20 a 25 Mbps para a banda 5 GHz e 5.5 a 11 Mbps para a banda 2.4 GHz (Secção V.4.7.). A existência de vários modelos obriga a que, necessariamente, os utilizadores tenham que especificar o tipo e taxa binária, para que deste modo seja permitida a interoperacionalidade.

De referir que tanto os sinais rádio como os infravermelhos são afectados pelo efeito de multi-caminho, ou seja, o receptor recebe vários sinais provenientes do mesmo emissor, isto acontece, por exemplo, devido ao efeito de reflexão das ondas nos objectos. Uma das soluções para o problema é a diversidade espacial, que consiste em colocar duas antenas separadas entre si por um quarto de comprimento de onda, de forma que o receptor ao receber os sinais os combine num só. Outra solução é utilizar a técnica de igualização, que consiste em determinar os vários caminhos percorridos pela onda, estando o receptor equipado com um igualizador que soma as várias ondas resultantes e diversas no tempo, numa só.

Apresentamos em seguida (Tabela 7) um resumo comparativo das duas tecnologias quando aplicadas a redes da área local sem fios.

	Infravermelhos	Rádio Frequência
Custo	Baixo	Médio
Licenciamento	Não	Sim / Não [2]
Interferência	Luz ambiente	Electromagnética
Área de cobertura	Pequena	Média / Grande
Limites Físicos	Paredes	Atenuada por paredes [3]
Operação em ambientes exteriores	Por feixe dirigido	Sim
Operação em ambientes interiores	Sim	Sim
Coexistência de múltiplas redes [4]	Sim / Limitado [5]	Sim
Segurança	Muita	Fraca
Complexidade	Menor	Maior

Tabela 7 - Comparação entre infravermelhos e rádio frequência

Embora possamos pensar que as tecnologias de rádio frequência e de infravermelhos serão fortes concorrentes, na realidade constata-se que proliferam no mercado paralelamente. A sua coexistência é perfeitamente possível atendendo que algumas características particulares, inerentes a cada uma delas, acabam por fazer com que se complementem, vocacionando-as para aplicações específicas. A opção por uma ou outra tecnologia fica assim apenas condicionada por factores que passam quer pelo ambiente físico quer pelo tipo de utilizadores ou, mais precisamente pelo tipo de tráfego que estes geram.

Em suma, a tecnologia de infravermelhos à mais adequada a uma utilização em ambientes interiores, em aplicações de pequena envergadura e em ambientes electromagnéticos ruidosos. Por seu lado a rádio frequência tanto pode ser usada em ambientes interiores como exteriores e em aplicações de maior alcance, desde que longe de fontes electromagnéticas.

[2] Bandas ISM
[3] Sistemas de baixa potência
[4] No mesmo espaço
[5] Pela capacidade de obtenção de diferentes frequências ópticas

CAPITULO IV
ACESSO AO MEIO EM REDES DE ÁREA LOCAL

Este capitulo descreve os protocolos de acesso ao meio para redes de área local, segundo uma dada classificação: protocolos de acesso ao meio sem e com contenção (acesso aleatório). Será analisada a sua aplicabilidade a redes de área local sem fios e é feita, também, uma análise qualitativa da mesma.

IV.1. Introdução

Numa rede de comunicação as trocas de informação entre as estações são efectuadas através do canal de transmissão partilhado. A forma como cada estação coloca a informação no canal ou acede a esta, tem que obedecer a determinadas regras às quais se dá o nome de protocolo de acesso ao meio, que é uma das funções da camada MAC (*Medium Access Control*), também referido como protocolo de ligação. Assim, este fornece um mecanismo que permite a todas as estações de uma rede, partilhando o mesmo meio, acederem-lhe sem interferir ou então causando interferência mínima com as outras estações. Por outro lado, este mecanismo deverá fazer uma utilização, dentro do possível, eficiente do canal de transmissão garantindo o mínimo atraso na transmissão das mensagens. As mensagens podem, eventualmente, ser de diferentes tipos (dados, controle ou gestão), possuírem prioridades e durações diferentes. Determinadas funções dos protocolos de ligação estão, em certos casos, directamente relacionadas com o tipo de acesso ao meio, são exemplo disso a detecção de erros, sequência e controle de fluxo de dados.

A razão principal para a existência destas regras é porque a maioria das redes de computadores utilizam o mesmo meio físico para troca de informações entre estações, com vista a uma maior economia de recursos (menor custo proveniente de uma utilização mais eficiente da largura de banda oferecida pelo canal). Existe, deste modo, o risco de duas ou mais estações transmitirem simultaneamente, ocasionando perda de dados já que os impulsos electromagnéticos podem chocar tornando a mensagem ilegível. Para evitar que tal aconteça foram estabelecidos estes conjuntos de regras - métodos de acesso - que asseguram que dois sinais não serão transmitidos ao mesmo tempo, controlando a forma como os dispositivos acedem ao canal.

Os primeiros protocolos de acesso ao meio utilizavam técnicas de multiplexagem no tempo ou no domínio da frequência. Estas, embora sejam as que melhor satisfazem os requisitos

exigidos, por exemplo por sinais de voz, demonstraram não ser muito adequadas para tráfego de dados, especialmente do tipo rajada (*bursty*).

Os mecanismos de acesso ao meio existentes para redes com fios não se adaptam a um meio sem fios, entre outras razões, porque o raio de alcance da estação emissora pode não ser suficiente para detectar a existência de outras estações próximas do receptor ou estas poderem estar escondidas por obstáculos, não sendo detectadas e pela acção de sentir a portadora ser feita de modo diferente. Em suma, nas redes sem fios é de extrema importância detectar possíveis interferências na recepção. Nestas, tanto as comunicações por rádio frequência como por infravermelhos usam filosofia de difusão (*broadcast)*, na colocação de dados no meio de transmissão [22]. Como resultado, nas redes sem fios, é necessário utilizar um MAC que permita partilhar os acessos ao meio, tal como nas redes cabladas, para assegurar que apenas um emissor o está a usar.

Outra função dos protocolos MAC é a implementação de mecanismos capazes de assegurarem a transmissão de informação relativamente a erros. Numa rede sem fios existem duas estratégias para a implementação desta função. A primeira delas, consiste em colocar *cheksums* mais sofisticados nos cabeçalhos dos pacotes. Outra estratégia, alternativa, simplesmente retransmite o pacote caso a sua transmissão não seja confirmada após um dado período de espera. Um protocolo de rede eficaz deverá contemplar ambas as abordagens.

O segundo ponto a ser observado nos protocolos de rede sem fios é como aceder ao meio e consequente detecção de colisões resultantes. Poderá ser usado um esquema convencional de detecção de colisões, à semelhança dos protocolos *Ethernet* e *Aloha*, requerendo que o emissor seja capaz de ouvir todos os terminais que estejam a tentar comunicar, ao mesmo tempo. O principal problema, consiste no facto de um terminal, de um lado da célula, poder não conseguir detectar que está em colisão com outro no lado oposto da célula.

IV.2. Tipos de protocolos de acesso ao meio (Métodos de acesso ao meio)

Vários autores classificaram os protocolos segundo tipos e classes, tendo em consideração parâmetros como, por exemplo, a natureza do algoritmo de atribuição do meio (com contenção ou sem contenção; estática ou dinâmica), a natureza centralizada ou distribuída do protocolo e o seu grau de adaptação a variações.

Iremos classificar os protocolos de acesso ao meio tendo por base a classificação realizada por Rom [42]. Este autor considera como factor de diferenciação das classes principais o algoritmo de acesso ou atribuição do meio. Conforme ilustrado na figura (Ilustração 13), os

métodos de acesso ou protocolos de acesso ao meio podem ser divididos em três grandes classes: Protocolos de acesso ao meio sem contenção; Protocolos de acesso ao meio aleatório e Protocolos de acesso híbrido.

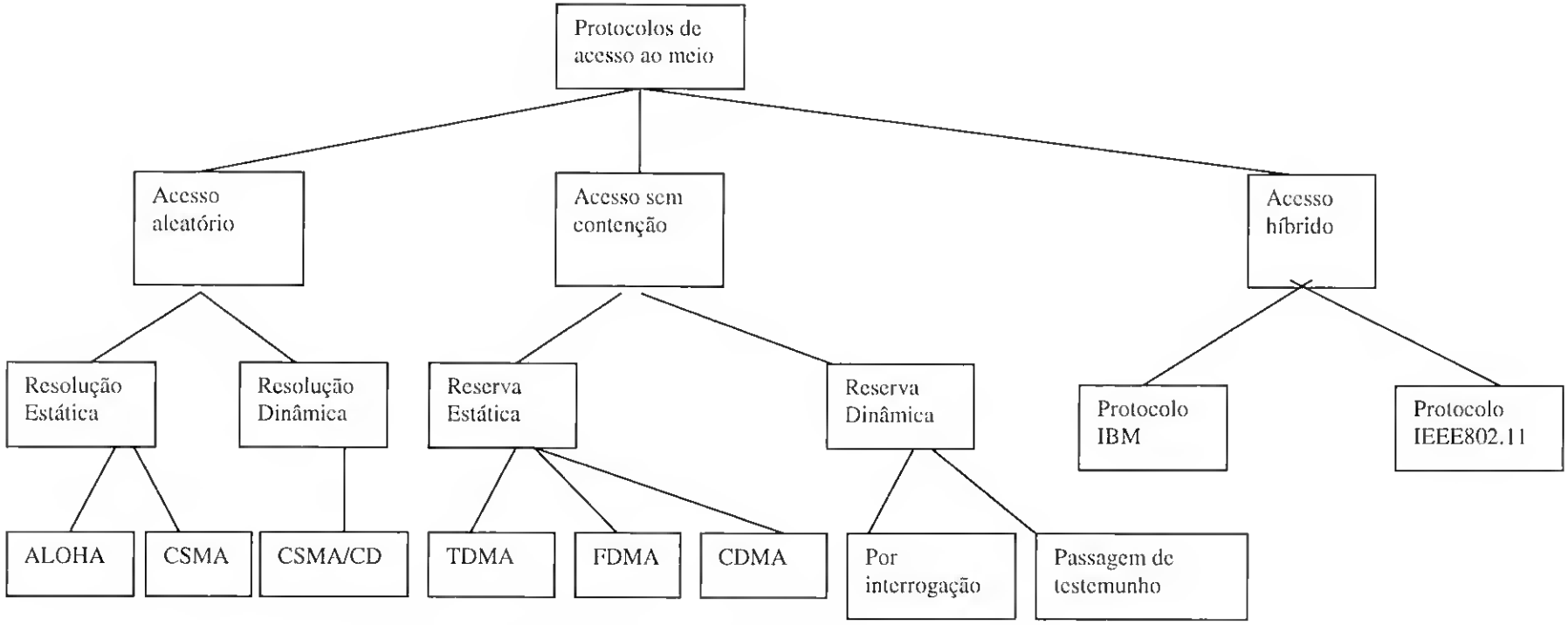


Ilustração 13 - Classificação dos protocolos de acesso ao meio

Os protocolos de acesso ao meio sem contenção são aqueles em que, uma vez atribuído o canal para uma dada transmissão, existe a garantia de que esta se realize sem interferências provocadas por outras transmissões. Nesta classe de protocolos distinguimos duas subclasses, tendo em conta a forma como é atribuído o canal de transmissão: estática ou dinamicamente. Exemplos de protocolos, em que a atribuição do meio é realizada de forma estática, são os que usam multiplexagem no tempo (TDMA, *Time Division Multiple Access*), multiplexagem no domínio da frequência (FDMA, *Frequency Division Multiple Access*) ou em técnicas de multiplexagem de códigos de transmissão (CDMA, *Code Division Multiple Access*). Exemplos de protocolos, em que a atribuição do meio é realizada de forma dinâmica, são os que usam esquemas de interrogação ou passagem de testemunho.

Os protocolos de acesso aleatório (baseados em contenção) são aqueles onde, contrariamente aos anteriormente expostos, não existe a garantia de que as transmissões sejam efectuadas sem interferência, dado que várias estações podem transmitir simultaneamente. O protocolo poderá resolver os conflitos resultantes de transmissões simultâneas de forma estática como, por exemplo, acontece nos protocolos ALOHA ou CSMA (*Carrier Sense Multiple Access*), ou de forma dinâmica como acontece com o protocolo CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*).

Por ultimo iremos referir os protocolos híbridos que integram mecanismos de acesso aleatório e não aleatório. Em suma, existem períodos de tempo nos quais o acesso ao meio se faz sem contenção e outros em que se verifica o inverso. Exemplos deste tipo de protocolos são o proposto pela IBM ao grupo IEEE 802.11 e o próprio protocolo IEEE 802.11.

IV.3. Protocolos de acesso ao meio sem contenção

Esta classe engloba os protocolos segundo os quais as estações não têm que disputar, entre si, o acesso ao canal de transmissão dado que este lhes é atribuído previamente. A sua atribuição pode ser feita de modo estático ou dinâmico.

A atribuição estática do canal de transmissão pode ser realizada de três formas: recorrendo a técnicas de multiplexagem temporal, atribuindo a cada estação toda a largura de banda do canal durante um dado período de tempo; utilizando técnicas de multiplexagem no domínio da frequência, atribuindo a cada estação uma dada largura de banda durante todo o tempo; ou, utilizando técnicas de multiplexagem de códigos de transmissão, atribuindo a todas as estações, simultaneamente, o mesmo canal de transmissão. Quando a concessão do canal de

transmissão é realizada recorrendo a uma das três técnicas anteriormente descritas, as estações apenas lhe podem aceder se este lhes foi previamente atribuído.

A atribuição dinâmica do canal de transmissão, ao contrário do modo anterior, tem em consideração as necessidades de utilização do canal pelas estações. Existem diversos esquemas que preconizam esta filosofia, podendo ser realizada por passagem de testemunho ou utilizando mecanismos de interrogação. Os protocolos baseados em passagem de testemunho utilizam-no fazendo o mesmo circular, sequencialmente, por todas as estações da rede. As estações apenas podem aceder ao canal de transmissão se estiverem na posse do testemunho. Os protocolos baseados em mecanismos de interrogação partem do principio que existe um controlador que sequencialmente interrogará as estações, concedendo-lhes permissão para aceder ao meio. Se uma estação interrogada pelo controlador não tiver informação para transmitir, este passa para a estação seguinte na sequência.

IV.3.1. Protocolos de acesso ao meio sem contenção com atribuição estática do meio

Dentro desta classe existem três tipos de protocolos: TDMA, FDMA, CDMA.

IV.3.1.1. TDMA (Time Division Multiple Access)

Neste método, cada nó tem um determinado intervalo de tempo (*slot*) para transmissão, isto é, toda a largura de banda do meio fica disponível nesse intervalo (Ilustração 14). Por outras palavras a ideia básica, de um protocolo do tipo TDMA, consiste na divisão da utilização do canal em intervalos de tempo, denominados *slot*.

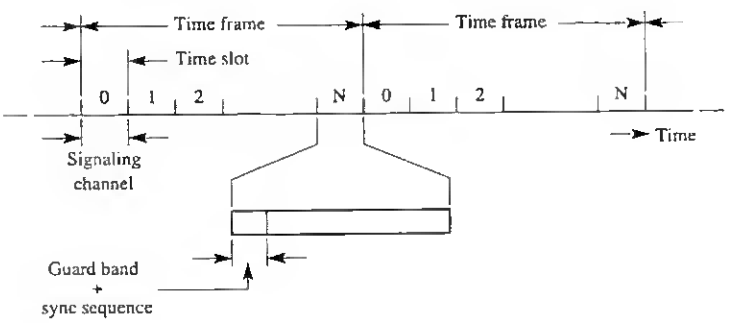


Ilustração 14 – TDMA [22]

A atribuição de *slots* às estações da rede obedece a um determinado padrão que se repete periodicamente, sendo cada período denominado ciclo ou trama. Normalmente a duração de

cada intervalo é pequena, logo a possibilidade de ocorrer um erro também é pequena. O ciclo de transmissão das tramas é determinado pela duração de cada *slot* e o número de slots/transmissões suportadas.

No método TDMA básico, o número de slots em cada trama corresponde ao número de estações. Cada slot está exclusivamente reservado para uma dada estação, a qual tem disponível, durante esse período, toda a largura de banda do canal de transmissão. Por outro lado, deverá existir a sincronização de estações de modo a garantir que estas apenas acedam ao meio nos respectivos slots. O método TDMA, modo geral, é utilizado em transmissões de voz e em comunicações síncronas. Nas transmissões de dados assíncronas, este método não se mostra eficiente. Isto é devido às características típicas deste tipo de tráfego que conduzem a um subaproveitamento da largura de banda disponível (tempos mortos), visto que nem todas as estações necessitam de usar os seus *slots*.

Na prática verifica-se que as estações apresentam requisitos diferentes em termos de utilização do canal de transmissão ao longo do tempo. As estações que tenham necessidade de aceder com mais frequência ao canal de transmissão, durante certos períodos de tempo, sujeitar-se-ão a atrasos entre pacotes sucessivos que poderão ser inaceitáveis. Este facto torna-se mais crítico se o número de estações for elevado, o que é facilmente perceptível, podendo ser contornado através da atribuição a cada estação de *slots* de tempo de transmissão de acordo as suas necessidades. Surge assim uma versão modificada do protocolo TDMA básico. Nesta versão continuam a existir tempos mortos, embora menores, sempre que uma estação não transmita no slot que lhe foi atribuído. O desempenho do protocolo continua, de igual modo que na versão base, condicionado pela variação dos requisitos de utilização do canal de transmissão ao longo do tempo.

Nas redes sem fios, TDMA é normalmente utilizado quando existe uma estação base que controle todas as transmissões, por exemplo um PC (*Point Coordinator*), sendo ele que estabelece a estrutura dos *slots* para cada receptor. Em suma, neste método existe uma mesma portadora partilhada por todas as estações móveis que é utilizada por cada estação, para transmitir apenas no *slot* de tempo que lhe está reservado [19]. Deste modo, conseguem-se multiplexar muitos utilizadores na mesma portadora, quase, eliminando a interferência entre eles, facto que é incrementado se for utilizada uma banda de guarda entre os *slots* dos diferentes utilizadores.

IV.3.1.2. FDMA (Frequency Division Multiple Access)

Este método tal como o TDMA, anteriormente descrito, utiliza técnicas de multiplexagem mas no domínio da frequência. A largura de banda disponível é dividida em sub-bandas de frequência que são atribuídas às estações. A largura de banda atribuída a cada estação é factor do número de estações existentes na rede, o que poderá constituir um problema se este for elevado. Neste método de acesso verifica-se, de igual modo que no anterior, um subaproveitamento da largura de banda, em parte pela eventual não utilização das bandas de frequência pelas estações e, por outro lado resultante da necessidade de isolamento que tem que existir entre bandas de frequência contíguas.

Se prendermos comparar o método FDMA com o TDMA, anteriormente descrito, podemos dizer que o presente é mais fácil de implementar dado que dispensa a utilização de mecanismos de sincronização das estações. Por outro lado, o atraso de transmissão de pacotes no método TDMA é menor. A diferença resulta do facto da transmissão de um pacote, utilizando o método TDMA, ter a duração de um *slot* e utilizando o método FDMA demorar o tempo equivalente a uma trama inteira. Outra desvantagem do método FDMA é a inflexibilidade na acomodação de novas portadoras de frequência. Esta implica alterações no equipamento terminal das estações, como por exemplo, inclusão de filtros. Tanto o método ora descrito, FDMA, como o método TDMA não permitem a sobreposição de transmissões, respectivamente, no domínio da frequência e no domínio do tempo. Como veremos posteriormente, isto pode ser alcançado com outros métodos.

Nas redes de comunicação de área local sem fios, o principio de funcionamento do método FDMA é idêntico ao TDMA, existido a necessidade de uma estação base (PC) para controlar as operações [29] (Ilustração 15).

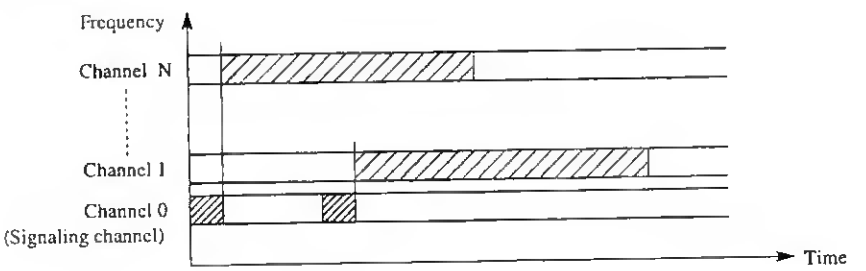


Ilustração 15 – FDMA [22]

A frequência total da banda disponível, é dividida num número de sub-bandas de frequências ou canais, de modo similar, em principio, ao espalhamento do espectro da técnica de salto de

frequência. No entanto, no método FDMA depois de um canal ser atribuído é utilizado enquanto durar a transmissão da trama. Normalmente os canais são atribuídos a pedido, sendo utilizados canais de transmissão separados. Comparativamente, a estação base num sistema FDMA é mais complexa do que num sistema TDMA sendo este último mais difundido. Poderão ser utilizados esquemas híbridos, os quais utilizam FDMA para subdividir a largura de banda em múltiplas frequências, cada uma das quais é então utilizada segundo o método TDMA.

Em suma, este método de acesso consiste na atribuição de um canal (frequência) a cada estação que queira transmitir, o qual se mantém reservado enquanto a comunicação durar [19]. Mais uma vez, de modo a minimizar a interferência entre diferentes comunicações, deve ser utilizada uma banda de guarda entre duas frequências consecutivas.

IV.3.1.3. CDMA (Code Division Multiple Access)

Este método de acesso permite sobreposição tanto no domínio da frequência como do tempo, conforme mostrado na figura (Ilustração 16).

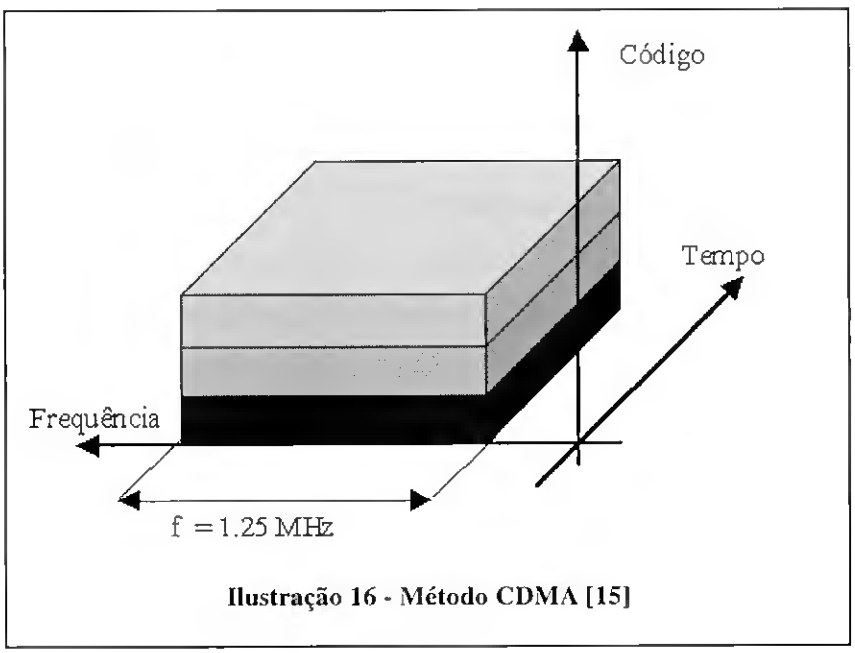


Ilustração 16 - Método CDMA [15]

Se pretender-mos reportar-nos à sua origem, CDMA foi desenvolvido nos EUA pelo segmento militar, sendo a sua primeira utilização para comunicação entre aviões caça e controle rádio de mísseis teleguiados [15]. Neste método as EMs transmitem na mesma portadora e ao mesmo tempo, mas cada comunicação individual é provida de um código

particular, facto que garante alta privacidade na comunicação. Por analogia, podemos imaginar uma sala cheia de pares que comunicam entre si, só que cada um fala um idioma diferente que só eles entendem. Quanto mais diferentes forem os idiomas utilizados na sala, menor a probabilidade de confusão na comunicação (interferência entre códigos). Por exemplo, o português e o espanhol são idiomas bastante parecidos, já o português e o alemão são bastante diferentes.

O método CDMA utiliza uma largura de banda muito superior aquela que seria necessária para transmitir o sinal, por exemplo pela técnica FDMA [19]. Todas as estações que estejam a transmitir operam na mesma gama de frequências e utilizam toda a largura de banda disponível. A não existência de interferência entre os utilizadores é garantida pela atribuição de um código de transmissão, diferente, a cada um deles. Estes códigos ortogonais, entre si, conseguem manter vários terminais em comunicação, simultaneamente, sem que ocorra interferência nas transmissões, porque cada estação utiliza uma forma de codificar as suas mensagens, de modo independente da das restantes estações. Assim, a partir do momento em que lhe é atribuído um código, cada terminal pode começar a transmitir sem necessidade de esperar por qualquer autorização.

Por seu lado o receptor, que terá que conhecer o código no qual a mensagem lhe foi enviada, utilizará técnicas de detecção baseadas em correlação, caso contrário apenas conseguirá receber ruído. Por esta razão, este sistema apresenta como grande vantagem a segurança das comunicações que, como referido, apenas poderão ser descodificadas por um receptor na posse do código que foi usado para a transmissão.

A implementação prática desta técnica baseia-se no seguinte: as ligações simultâneas são diferenciadas por códigos distintos de baixa correlação. Assim, sequências digitais do tipo pseudo-noise (PN) são geradas por códigos pseudo aleatórios (PN *codes*) e ortogonais, com alta taxa de transmissão por *Direct Sequence*, técnica à qual aludimos anteriormente. Deste modo, obtém-se um sinal de faixa larga por espalhamento espectral (*Spread Spectrum*), pelo facto do mesmo ser transmitido a uma taxa maior que a taxa de informação. A razão entre a faixa do sinal espalhada e a sua faixa original é conhecida como ganho de processamento.

O processo de transmissão e recuperação da informação usado pelo método CDMA é o exibido na figura (Ilustração 17).

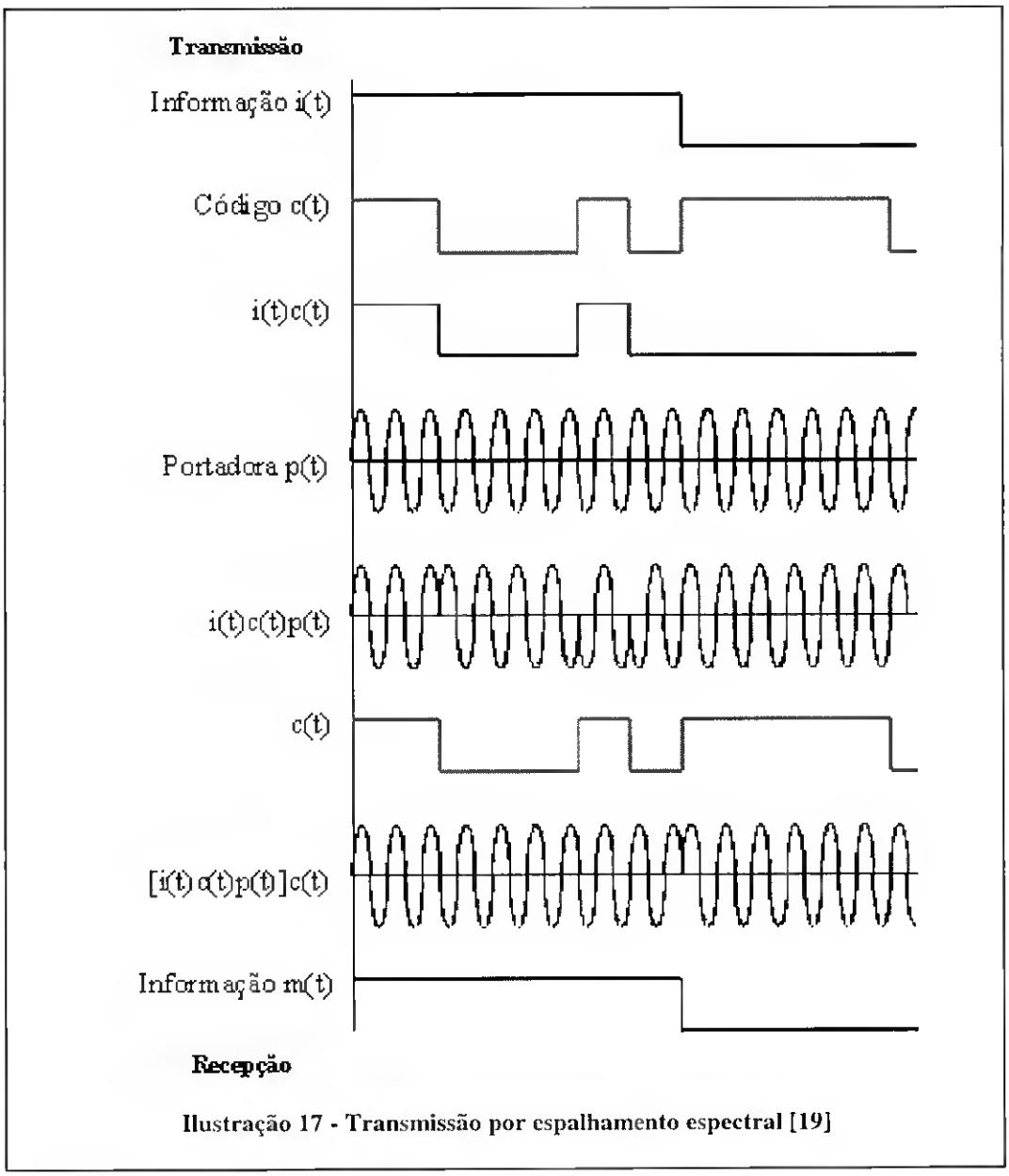


Ilustração 17 - Transmissão por espalhamento espectral [19]

Em aplicações de redes de comunicação sem fios, a tecnologia de transmissão CDMA é utilizada devido ao facto de ser pouco sensível a interferências. Esta associada à transmissão com tecnologia de espectro espalhado (*Spread Spectrum*), anteriormente referida, atravessa obstáculos com mais facilidade que os sistemas que utilizam microondas, devido ao facto de utilizar frequências menores [19].

Nas redes de comunicação de área local sem fios, este método é utilizado com os sistemas rádio por espalhamento do espectro. Ambos, sequência directa e salto na frequência, utilizam uma única sequência aleatória (de salto ou de espalhamento) como base para o seu modo de operação [22]. Em tais operações é definido um código de sequência aleatória diferente para cada um dos nós que conhecem, também, o conjunto dos códigos de todos os outros. Quando

um nó quer comunicar com outro, muda o seu código para o mesmo do receptor e segundo esta filosofia diferentes pares de nós podem estar a comunicar ao mesmo tempo.

Na prática isto apenas é possível com o salto de frequência, pois com sequência directa poderá acontecer um fenómeno conhecido como efeito do próximo - afastado (*near-far effect*), exibido na figura (Ilustração 18), que ocorre quando um nó ao tentar comunicar se encontre junto a outro.

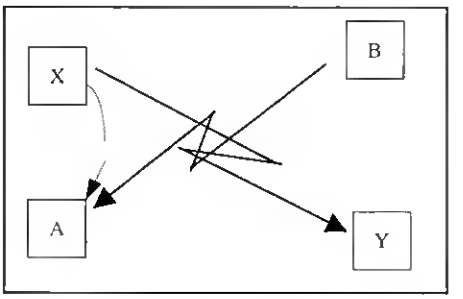


Ilustração 18 - Efeito de Próximo / Afastado

Assim, o nó A sofrerá inevitavelmente interferência, quando está a receber do nó B, pelo efeito de proximidade induzido quando o nó X tenta transmitir. Este fenómeno é também conhecido pelo efeito de terminal escondido (*Hidden Terminal Effect).* Pelo contrário, operando com salto na frequência, como os nós emissores estão constantemente a mudar de frequência, a probabilidade de dois utilizarem a mesma e ao mesmo tempo é muito baixa. Isto pode ser melhorado se efectuarmos um prévio e cuidadoso plano de sequência de saltos na frequência. A desvantagem de ambas as técnicas, é a necessidade de todos os nós conhecerem as sequências pseudo-aleatórias de todos os outros nós o que em redes sem fios é difícil de gerir.

IV.3.2. Protocolos de acesso ao meio sem contenção com atribuição dinâmica do meio

Os protocolos de acesso ao meio descritos anteriormente fazem um subaproveitamento do canal de transmissão ou, para que este efeito seja minimizado, apresentam uma implementação demasiado complexa, caso do protocolo CDMA. Os protocolos de acesso com atribuição dinâmica do meio, ao contrário, minimizam ou chegam mesmo a eliminar esse efeito. Exemplos de protocolos deste tipo são os baseados em interrogação e em passagem de testemunho, os quais iremos descrever em seguida.

IV.3.2.1. Protocolos de acesso ao meio baseados em interrogação

Este tipo de protocolos actuam de modo centralizado, existindo um controlador que é responsável pela atribuição da largura de banda às estações que fazem parte da rede. O seu princípio de funcionamento base, consiste no seguinte: o controlador mantém uma lista, ordenada sequencialmente, das estações e percorre-a interrogando cada estação. Se uma dada estação ao ser interrogada tiver dados para transmitir acede ao canal e transmite-os, caso contrário responde de modo negativo ou simplesmente não responde à interrogação. O controlador sempre que uma estação interrogada não utilize o meio passa para a estação seguinte da lista.

O desempenho deste tipo de protocolos depende, essencialmente, do atraso de propagação de ida e volta (*round-trip propagation delay*) e da sobrecarga (*overhead*) introduzida pela troca de mensagens de controle entre o controlador e as estações da rede. Existem técnicas para minimizar a sobrecarga que, no entanto, não iremos aqui abordar. Estas permitem ao controlador, por exemplo, determinar previamente quais as estações que têm informação para transmitir e apenas interrogar essas. A percentagem de tráfego gerado do tipo rajada (*burst*) é outro factor que, de igual modo, condiciona o desempenho deste tipo de protocolo, com consequência no atraso de transmissão dos pacotes. Este efeito é agravado com o aumento do número de estações na rede.

IV.3.2.2. Protocolos de acesso ao meio por passagem de testemunho

Este tipo de protocolos utilizam uma trama especial denominada testemunho (*Token*) para efectuar o controle do acesso ao meio de transmissão. Uma rede que utilize um protocolo deste tipo estabelece um anel lógico no qual o testemunho circula, de estação em estação. A posse do testemunho dá à estação o direito de transmitir. Excepcionalmente, as estações podem transmitir tramas de confirmação positiva não sendo detentoras do testemunho, quando solicitadas pela estação que o possui. A estação que recebe o testemunho controlará o meio por um período de tempo específico, durante o qual a estação pode transmitir uma ou mais tramas. Quando esse tempo terminar ou quando a estação terminar as suas transmissões passa o testemunho para a estação seguinte no anel lógico.

Este tipo de protocolo é frequentemente encontrado em meios físicos cablados, sobretudo nas topologias em anel ou outras. Existem duas normas IEEE para protocolos de acesso ao meio por passagem testemunho: IEEE 802.5 (*Token Ring*) e IEEE 802.4 (*Token Bus*). Face à

sua não aplicabilidade em redes de comunicação de área local sem fios não iremos tecer mais considerações sobre este método de acesso.

IV.4. Protocolos de acesso aleatórios (com contenção)

Nos protocolos de acesso aleatório o acesso ao meio processa-se com contenção. Caracterizam-se pela atribuição dinâmica do meio de transmissão e por um desempenho que é fortemente condicionado pela relação entre o atraso de propagação e o tempo médio de transmissão do pacote [43]. Numa rede baseada em contenção não existe uma ordem de acesso e nada impede que dois ou mais nós transmitam em simultâneo gerando situações de conflito, denominadas colisões o que resultará, regra geral, na perda de mensagens.

O primeiro protocolo que surgiu, deste tipo, foi o protocolo ALOHA, do qual falaremos em seguida. Posteriormente, como resultado da evolução da ideia desenvolvida pelo ALOHA, outros protocolos surgiram, sempre com o intuito de melhorar a eficiência do original. Assim, em 1975, Kleinrock e Tobagi [44] propuseram um novo método de acesso, denominado CSMA (Carrier Sense Multiple Access), o qual desde então sofreu várias alterações.

Neste tipo de protocolos o sucesso da transmissão não é garantido à partida devido a colisões, anteriormente referidas. A resolução de colisões pode ser estática ou dinâmica, sendo a primeira usada pelos protocolos ALOHA e CSMA e a segunda pelo protocolo CSMA/CD.

O controle de acesso ao meio (MAC) o qual é função da camada de ligação (Data Link Layer) numa rede de comunicação de área local sem fios com tecnologia rádio, permite que múltiplas ferramentas partilhem um meio de transmissão comum via um protocolo *Carrier Sense* tipo protocolo *Ethernet*. Este protocolo permite que um grupo de computadores sem fios partilhem a mesma frequência e consequentemente o mesmo espaço.

Podemos, por analogia, imaginar uma sala cheia de pessoas envolvidas numa única conversação na qual cada uma delas pode ouvir se alguém falar. Em termos de redes de comunicação, isto corresponderia a uma topologia tipo Bus completamente conectada (na qual todos falam usando a mesma frequência) usada nas redes cabladas tipo *Ethernet* e pelas redes de área local sem fios.

Neste cenário, para evitar que duas pessoas falem ao mesmo tempo, deverão esperar até que a outra pessoa acabe de falar. De igual modo, ninguém deve falar se não existir silêncio na sala. Este conjunto de regras, as quais podemos designar por protocolo simples, garantem

que apenas uma pessoa fale de cada vez e oferecem um uso partilhado do meio de comunicação. Os sistemas de comunicação sem fios operam de modo idêntico, excepto que as comunicações são feitas sob a forma de sinais rádio.

Na figura é ilustrado o funcionamento de um protocolo do tipo *Carrier Sense* (Ilustração 19).

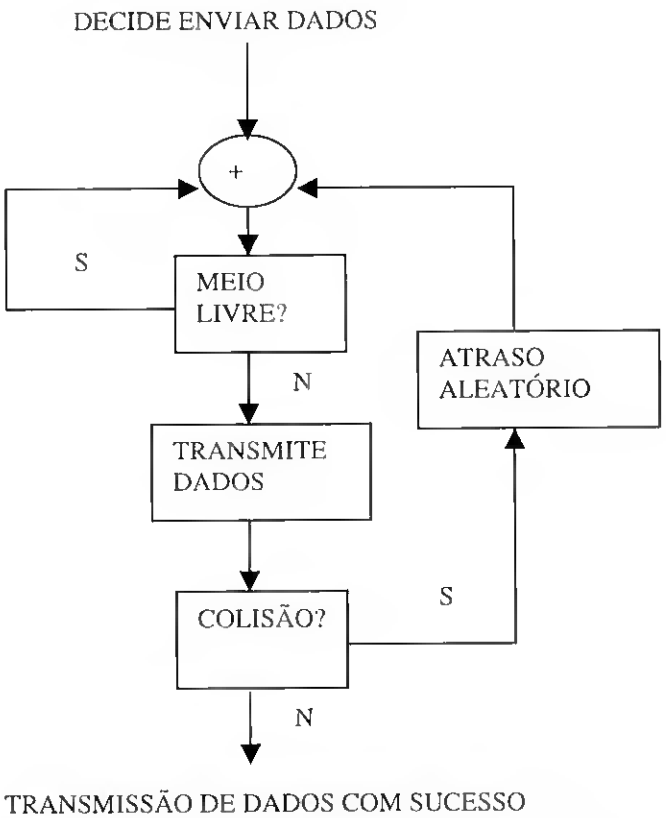


Ilustração 19 - Operação de um protocolo Carrier Sense

Outro aspecto importante refere-se ao controle de erros. Nas redes sem fios este é conseguido pela execução de testes em cada estação, aos dados que chegam, para verificar se existem bits alterados. Assim, continuando a analogia, anteriormente referida, imaginemos que duas pessoas estão a dialogar e ocorre uma disfunção, por exemplo a passagem de um avião, tornando o diálogo imperceptível. Como resultado, a pessoa que está a ouvir pede a quem está a falar para repetir uma frase ou duas.

IV.4.1. Protocolos com resolução estática

IV.4.1.1. ALOHA

Este protocolo foi desenvolvido na Universidade do Hawai no início da década de 70 por Abramson [45], para a rede ALOHA que lhe emprestou o nome, que era uma rede de

radiodifusão via satélite, que começou a operar por volta de 1970 [12]. Embora esta não possa ser considerada uma rede local, o seu estudo é importante uma vez que do seu protocolo resultaram grande parte dos protocolos baseados em contenção. Possuindo dois canais de frequência rádio, um deles alocado para difusão de mensagens do computador para um terminal, e o outro para difusão de mensagens de um terminal para o computador. No primeiro caso não existe problema, dado que a comunicação é única, enquanto no segundo podemos encontrar problemas de comunicação, dado que todos os terminais podem usar esse canal para transmitir. Este é o cenário encontrado nas redes de comunicação de área local sem fios.

O método de acesso utilizado na rede ALOHA é muito simples. Cada terminal só pode ouvir o canal de transmissão do computador para si não tendo, dessa forma, condições de saber se o outro canal está a ser utilizado por outro terminal ou não. Quando um terminal tem uma trama para transmitir envia-a, independentemente de o canal estar, ou não, a ser utilizado. A recepção sem erros dos pacotes é notificada à estação emissora, pela estação receptora, através da transmissão de um pacote de confirmação positiva (ACK). Assim, como as transmissões são iniciadas sem atender ao estado do canal, eventualmente, podem ocorrer colisões. A técnica usada para a detecção de colisões é realizada pelo disparar de um relógio de sincronismo. Se após um intervalo de tempo pré-definido o pacote não for confirmado a estação emissora pode concluir que este foi destruído, resultado de uma colisão, e terá que o retransmitir. Para evitar que ocorram novas colisões a estação antes de efectuar nova retransmissão espera um intervalo de tempo de duração aleatória.

Este método básico pode ser melhorado de um modo simples, restringindo o tempo em que um terminal pode começar a transmitir, de modo a reduzir o tempo total gasto por informações inúteis presentes no canal, provenientes de tramas que colidiram. A técnica utilizada, denominada Slotted-Aloha e proposta por Roberts em 1972 [46], divide o tempo em intervalos de tempo discretos (*slots*) de duração igual à duração de transmissão de um pacote, operação esta que é executada pelo sistema central. Cada terminal apenas pode começar a transmitir no início de cada intervalo. Assim, quando dois dispositivos decidem transmitir ao mesmo tempo eles transmitem toda a trama, mas de modo sincronizado, deste modo o tempo desperdiçado é reduzido. Por outro lado, este método impõe, normalmente, um atraso no início da transmissão, pois antes de transmitir uma trama, a estação tem que esperar o início do próximo *slot* de tempo, mesmo que o canal esteja disponível (Ilustração 20).

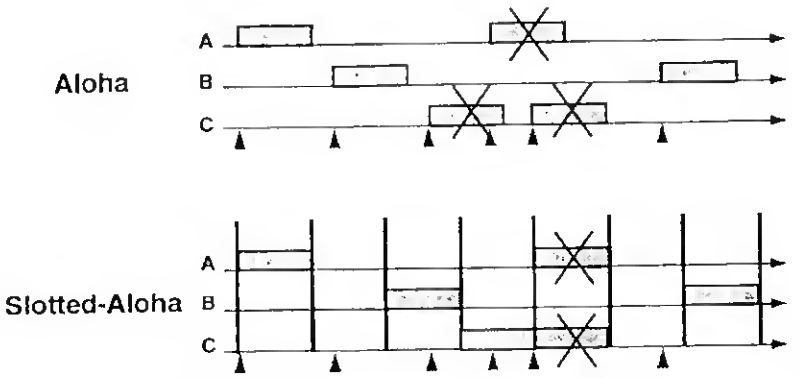


Ilustração 20 - ALOHA / Slotted ALOHA [24]

Como desvantagem de ambas as técnicas, podemos apontar que as redes com grande volume de trafego podem tornar-se instáveis, dado que o trafego resultante de retransmissão e colisão podem tornar a rede inoperante. Por outro lado, este método não garante um atraso de transferência máximo (limitado a dado valor).

Como principal vantagem, podemos referir a sua simplicidade, o que se reflecte no seu baixo custo, sendo adequado para aplicações onde o trafego na rede é pequeno e nas quais a prioridade e tempo de resposta limitado não são importantes.

Em suma, embora a família de protocolos ALOHA faça uma utilização pouco eficiente do canal de transmissão, apresenta um desempenho superior ao obtido com protocolos de acesso ao meio sem contenção, quando o tráfego no canal é preferencialmente do tipo rajada. O mesmo não acontece para tráfego do tipo síncrono em que os atrasos de transmissão de pacotes introduzidos pelos protocolos de acesso aleatório podem comprometer drasticamente o desempenho na rede [43].

IV.4.1.2. Protocolo CSMA (Carrier Sense Multiple Access)

No protocolo CSMA o acesso ao meio é controlado por detecção de actividade no canal de transmissão. Contrariamente ao que se verifica no protocolo ALHOA, antes de iniciar qualquer transmissão as estações verificam se o canal está disponível, atitude que se chama *escutar / sentir* o meio.

Se pretender transmitir e ao escutar o meio a estação detectar que este está ocupado, a transmissão é adiada evitando assim uma situação de colisão. Se o meio estiver livre a estação transmite de imediato. Esta prática não significa que uma colisão não possa ocorrer caso, por exemplo, de duas ou mais estações que ao verificarem que o meio está livre iniciem

uma transmissão em simultâneo. A forma como as estações reagem a uma situação destas permite distingir diferentes tipos de acesso CSMA: CSMA não persistente, CSMA p-persistente e CSMA 1-persistente [44].

No método CSMA não persistente a estação ao escutar o meio, se este estiver livre transmite de imediato, senão adia a transmissão por um dado intervalo de tempo de duração aleatória. Este é de duração aleatória de modo a evitar a ocorrência de transmissões simultâneas e consequentemente de situações de colisão após o adiamento de dada transmissão. Após esse intervalo de tempo a estação volta a escutar o meio e repete todo o processo.

No método CSMA p-persistente, a sua implementação exige a partição do eixo temporal em *slots* de duração igual ao atraso de propagação máximo. Estes *slots* são também, por vezes, designados *mini-slots* para distinção da definição usada no protocolo *slotted* ALOHA, onde a duração corresponde ao tempo de transmissão de um pacote. No método ora descrito as estações estão sincronizadas e apenas transmitem no início de cada *slot*. Se o canal de transmissão estiver livre, quando a estação pretender transmitir ela fá-lo com a probabilidade ***p***. Se o meio estiver ocupado aguarda até que este fique livre, após o que transmite com a probabilidade ***p*** ou atrasa a sua transmissão com a probabilidade ***(1-p)*** durante o *slot*. Ao fim desse *slot* se o meio continuar ocupado a estação repete o processo. O valor para o parâmetro ***p*** é escolhido de modo a reduzir o nível de interferência, mantendo o valor do tempo livre do canal entre transmissões consecutivas o menor possível.

O método CSMA 1-persistente é um caso particular do anteriormente descrito. Este tenta rentabilizar a ocupação do canal de transmissão fazendo uso dele sempre que existam transmissões para efectuar. Assim, uma estação que adopte esta filosofia, ao pretender transmitir, se o canal estiver livre, transmite com probabilidade ***1***. Caso contrário, se o canal estiver ocupado a estação aguarda que o mesmo fique livre e logo que tal aconteça transmite com probabilidade ***1***. Por outras palavras, persiste em transmitir com probabilidade ***1*** e dai advém a sua designação.

O desempenho desta família de protocolos é fortemente condicionado pela relação entre o atraso de propagação e o tempo de transmissão de um pacote [42]. Quanto maior o atraso de propagação maior é o tempo em que o pacote é vulnerável. Quanto maior o período de vulnerabilidade maior a probabilidade que ocorra colisão, ou seja maior é o desperdício de largura de banda, o que significa que menor é a capacidade do canal de transmissão.

IV.4.2. Protocolos com resolução dinâmica

IV.4.2.1. Protocolo CSMA / CD (Carrier-Sense Multiple Access / Collision Detection)

Este método é amplamente utilizado nas redes com fios como um método MAC, exemplo disso é a norma IEEE 802.3, vulgarmente designada *Ethernet*, utilizada em redes de área local com topologia em barramento [24].

O protocolo CSMA/CD pertence à família dos protocolos CSMA, baseando o seu funcionamento na detecção da actividade do meio e em detecção de colisões, mas apresentando um mecanismo de resolução dinâmica de situações de colisão. Tal como no método CSMA anterior, esta técnica vai também sincronizar as tramas em colisão fazendo com que se sobreponham desde o início, mas não utiliza a divisão do tempo em intervalos. Além disso, e principalmente, este vai tentar ao máximo evitar colisões e, em algumas das suas variantes, detectar tramas em colisão durante o tempo de transmissão abortando-as, fazendo com que estas colidam durante o menor tempo possível. Deste modo é aumentada a eficiência em termos da utilização da capacidade do canal.

De acordo com as regras do protocolo CSMA/CD uma estação só transmite se não detectar actividade no canal de transmissão. Assim, quando uma estação deseja transmitir escuta, primeiro, o meio para saber se existe alguma transmissão em progresso. Se ninguém controlar o meio, então a estação pode transmitir. Caso contrário, a estação espera durante um período de tempo e tenta novamente, usando algoritmos para o efeito. Uma colisão só pode ocorrer se dois nós tentarem transmitir, aproximadamente, no mesmo instante de tempo, dado que se um nó iniciar uma transmissão e o seu sinal tiver tempo de se propagar até ao outro nó este, ao ouvir o sinal, aguardará pelo final da transmissão para depois ganhar o acesso.

Neste método existem pelo menos três mecanismos para detecção de colisão: detecção por medição da potência do meio, dado que ao existir mais que uma estação a transmitir aumenta a potência existe no canal; detecção por violação do código no qual os dados estão a ser codificados (exemplo disso é a codificação *Manchester*); ou, detecção por comparação do sinal emitido com o recebido, assumindo-se que ocorreu uma colisão sempre que existirem diferenças. Podemos referir como exemplo de funcionamento a norma IEEE 802.3, redes com fios, onde sempre que ocorre uma colisão as estações envolvidas, ao detectarem a colisão, reforçam o sinal no canal de transmissão, transmitindo um sinal denominado JAM.

O intuito deste reforço das colisões é o de garantir que todas as estações da rede, incluindo as envolvidas na colisão, tomem conhecimento de que esta ocorreu. Por outro lado será activado o algoritmo de resolução de colisões, também denominado algoritmo de recuo. Este será responsável pela redução da probabilidade de ocorrência de novas colisões, pelo que antes de tentar a retransmissão a estação aguarda um período de tempo aleatório.

A detecção de colisões resulta numa melhoria do desempenho do protocolo CSMA/CD quando comparado com os outros da família CSMA, anteriormente abordados [24]. Embora continue a existir uma afectação no desempenho pela relação entre o atraso de propagação no canal e o tempo médio de transmissão de um pacote, este depende, também, do tempo necessário para que a colisão seja detectada. Assim quanto menor for o tempo necessário para detectar uma colisão maior será a capacidade do canal [43].

Nas redes sem fios, o protocolo CSMA permite, também, que um nó em espera possa ceder a vez a outro que já se encontra em transmissão. Contudo, nas comunicações que usem tecnologia rádio frequência e infravermelhos, atendendo à limitação de que não é possível transmitir e receber simultaneamente, o mecanismo de detecção de colisões, na sua forma básica, não pode ser utilizado. Assim, para a resolução deste problema utiliza-se uma variante do mecanismo de detecção, conhecido como *Collision Detection* (Comb). Com este esquema, quando um nó tem uma trama para transmitir, gera primeiro uma pequena sequência binária aleatória (conhecida como *Comb*) que junta imediatamente antes do preambulo da trama. O nó escuta, então, o meio e se não existir transmissão assume que o mesmo está livre, começando a transmitir a sequência *Comb*. Para uma sequência Comb binária 1, o nó transmite um pequeno sinal em curto espaço de tempo. Se a sequência Comb é binário 0, o nó muda o modo de transmissão para recepção. Se um nó detecta transmissão de um sinal, durante o tempo em que está no modo de recepção, desiste da competição de acesso ao meio e cede a vez, até que outro (ou outros) nó tenha transmitido a trama.

A eficiência deste esquema traduz-se no número de bits da sequência aleatória e na sua geração, uma vez que se dois nós geram duas sequências iguais irá ocorrer colisão. Na prática o número de nós em contenção, em qualquer altura, é provavelmente baixo e assim o comprimento de *Comb*, poderá também ser curto.

O método CSMA/CD não exige o reconhecimento de mensagens para retransmissão, podendo-se deixar para níveis superiores de protocolo a garantia de entrega de mensagens [24]. Dado que esta garantia apenas é exigida em alguns tipos de aplicações, várias redes optam assim por fazê-lo, oferecendo a este nível apenas uma grande probabilidade de entrega das tramas.

IV.4.2.2. CSMA / CA (Carrier-Sense Multiple Access / Collision Avoidance)

O protocolo CSMA/CA, pertence à família dos protocolos de acesso aleatório do tipo CSMA, baseia de igual modo o seu funcionamento na detecção da actividade no canal de transmissão e no evitar de colisões. Quando um nó pretende transmitir escuta o meio durante um curto período de tempo aleatório, se não houver comunicação então transmite. De igual modo, se outros nós estiverem à escuta, ganha acesso ao meio aquele que tiver o menor intervalo de tempo de escuta.

A eficiência deste método é função do número de incrementos do tempo - número de bits na sequência pseudo-aleatória - no máximo período de tempo em que é evitada a colisão (*collision avoidance*). Por ser o protocolo usado pela norma IEEE 802.11 iremos abordá-lo em mais detalhe posteriormente nesta dissertação.

IV.5. Aplicabilidade dos protocolos a redes sem fios

Numa rede de área local sem fios as características do canal de transmissão podem, variar de modo dinâmico, no tempo e no espaço. Esta condicionante manifesta-se em fenómenos, já anteriormente referidos, tais como o efeito de terminal oculto (*hidden station*) ou o efeito de próximo-afastado (*near far effect*). O efeito de terminal oculto / estação escondida frequente em redes sem fios ocorre quando uma estação, por qualquer razão, não tem capacidade para escutar outras estações que pertençam à mesma célula ou rede. Este efeito apresenta várias causas como, por exemplo, enfraquecimento do sinal ou obstrução física do canal de transmissão. Por seu lado, o efeito do próximo-afastado resulta do facto da potência recebida por uma estação ser função da sua distância relativamente ao emissor. Este efeito pode comprometer a equidade no acesso ao meio. Nestas redes verifica-se, também, a presença de zonas de sobreposição entre células adjacentes. Corresponde a zonas onde uma estação, ai localizada, se pode fazer ouvir em uma ou mais células adjacentes. Por tal facto será propícia para a ocorrência de interferência que, se possível, deverá ser minimizada já que, atendendo ao protocolo de acesso, poderá causar redução da capacidade da rede.

Face ao anteriormente exposto, o protocolo a ser utilizado em redes de área local sem fios deverá ter em linha de conta os efeitos anteriores e simultaneamente satisfazer requisitos tais como: utilização eficiente do canal de transmissão; garantir a equidade no acesso ao meio de

transmissão; permitir a localização de várias estações em cada célula; suportar a sobreposição de células vizinhas com segurança e privacidade adequadas; permitir mecanismos de conservação de potência; suportar tráfego síncrono e assíncrono; suportar tráfego com prioridades diferentes, entre outros, aos quais aludiremos posteriormente nesta dissertação.

Dos protocolos anteriormente descritos, nem todos obedecem aos requisitos especificados, o que inadequa a sua aplicabilidade a redes de comunicação de área local sem fios. Assim, por exemplo técnicas FDMA [41], são pouco flexível e não eficientes para serem utilizadas em tráfego de dados. Embora se utilizadas conduzam a implementações complexas e, modo geral, com ganhos insuficientes para se justifique a sua utilização em redes rádio sem fios nas bandas licenciadas. Por outro lado, o protocolo CDMA [47] é afectado pelo efeito do próximo-afastado se não se implementarem mecanismos de controle da potência transmitida.

O protocolo baseado em interrogação, descrito anteriormente, é pouco eficiente devido ao *overhead* introduzido pelas mensagens de controle. Por seu lado, os protocolos por passagem de testemunho também não são de utilização adequada em redes sem fios, principalmente, devido a situações como perda de testemunho ou quebra do anel lógico. A primeira situação ocorre devido ao esvaecimento do sinal no meio e ao ruído presente no canal de transmissão, a segunda tem como implicação a não mobilidade das estações. As condicionantes atrás expostas teriam como principal consequência uma afectação do desempenho da rede devido ás necessidades frequentes de gerar novo testemunho e restabelecer o anel lógico.

Dos restantes protocolos de acesso ao meio, anteriormente descritos, os do tipo CSMA e TDMA [41] são os que melhor se adaptam às características das redes sem fios e à diversidade de padrões de tráfego por elas suportados. Um protocolo do tipo CSMA é mais adequado para transmissões de dados do tipo rajada (transmissões assíncronas), mas a sua eficiência é baixa quando o tráfego for tipo síncrono. O suporte a tráfego com diferentes prioridades é difícil, tal como o suporte de mecanismos de conservação de potência. Um protocolo do tipo TDMA, face ás suas características, é mais adequado para transmissões do tipo síncrono e suporta mecanismos de prioridade e conservação de potência. De salientar, contudo, o facto de não ser completamente eficaz, principalmente devido ao efeito de enfraquecimento do sinal, da mobilidade necessária para as estações e estrutura multicélula requerida numa rede sem fios.

Face ao anteriormente exposto, podemos concluir que o ideal seria a integração dos dois métodos num protocolo híbrido, permitindo suportar de modo eficaz tráfego simultâneo dos tipos assíncrono e síncrono. Esta é precisamente a ideia conducente para aplicação a redes de

área local sem fios, conforme os dois principais protocolos submetidos ao grupo de normalização IEEE 802.11 durante a fase de desenvolvimento e especificação da norma [48] e [49]. Ambos os protocolos se baseiam na divisão do eixo temporal em intervalos ou tramas. Cada trama, por sua vez, encontra-se dividida em períodos de acordo com o tipo de acesso, com ou sem contenção.

CAPITULO V
A NORMA IEEE 802.11

Este capítulo descreve os principais atributos e especificações da norma IEEE 802.11 enquanto padrão de standarização para redes de comunicação de área local sem fios.

V.1. Historial da norma IEEE 802.11

A padronização garante interoperacionalidade entre os diversos fornecedores da tecnologia, ou seja, se todos os equipamentos de uma rede sem fios forem padronizados segundo uma determinada norma, independentemente da marca ou modelo, eles necessariamente serão compatíveis [17].

O aparecimento da tecnologia para redes de comunicação de área local sem fios veio preencher uma lacuna no mercado, fornecendo a possibilidade de instalação de redes em ambientes nos quais os cabos seriam impraticáveis atendendo a razões de várias ordens, anteriormente discutidas. Diversos fabricantes têm lançado os seus produtos, e a necessidade de interoperacionalidade entre os mesmo é um factor crescente. Assim os principais Organismos Reguladores criaram padrões específicos para o efeito, como a norma IEEE 802.11 do IEEE (*Institute of Electrical and Electronics Engineers*), o HIPERLAN proposto pelo ETSI (*European Telecommunications Standards Institute*) e o IP móvel. Contudo, observámos que a maioria dos fabricantes de produtos para redes locais não cabladas, actualmente disponibilizam produtos compatíveis com a norma IEEE 802.11 e alterações posteriormente aprovadas, permitindo aos interessados conceber aplicações para redes sem fios baseados em sistemas abertos. A mudança para este tipo de componentes é motivada por preços baixos e pela interoperacionalidade entre redes de área local sem fios de fabricantes distintos. Isto tornou, sem dúvida, a implementação de redes sem fios mais viável do que antes, criando grandes oportunidades de negócio na área. Como reverso deste cenário, acresce o facto de que a maioria das empresas que comercializam esta tecnologia possuem poucos conhecimentos de como implementar e desenvolver um sistema de rede sem fios. Na maioria dos casos existe, ainda, alguma confusão sobre as capacidades e efectividade do standard IEEE 802.11.

A implementação de redes sem fios é muito diferente da das tradicionais redes cabladas. A titulo de exemplo podemos referir que em contraste com a rede Ethernet, por exemplo, uma rede de comunicação de área local sem fios possui um vasto número de parâmetros de

instalação de definição extremamente sensível, os quais afectarão a performance e operacionalidade da rede se a sua configuração não for a mais adequada.

Importante na definição de padrões para redes locais de computadores é o IEEE, que submete as suas propostas através da ANSI (*American National Standards Institute*), e é um dos órgãos mais importantes no estudo de redes [10]. O IEEE, através do seu projecto IEEE 802, desempenha um papel relevante no estabelecimento de normas internacionais para redes de área local. Este comité foi formado em Fevereiro de 1980 [27], produzindo a série de standards conhecidos como IEEE 802.X, inicialmente destinados a redes de área local cabladas, IEEE 802.3 (Rede Ethernet), IEEE 802.4 (Rede Token Ring) e IEEE 802.5 (Rede Token Bus).

De acordo com o projecto IEEE 802 foi formado um grupo de trabalho, IEEE 802.11 *Wireless* LANs, com o objectivo de estabelecer um standard internacional de recomendações para este tipo de redes, as quais suportarão comunicação de dados sem fios de grande largura de banda. Em 1987 alguns esforços no domínio das redes de rádio sem fios foram realizados no interior do grupo IEEE 802.4, mas foi em 1990 que se formou um grupo especializado em redes sem fios, o grupo IEEE 802.11 [50]. O standard 802.11 denominado " *Wireless Access Method and Physical Layer Specifications* " envolve uma variedade de meios físicos, incluindo rádio, FHSS e DSSS bem como luz infravermelha para taxas de dados até 2 Mbps e tem por objectivo definir a camada física para comunicação de dados sem fios, transmissões na camada física (PHY) por meio de rádio ou infravermelhos e ainda protocolos de acesso ao meio (MAC) compatíveis com os standard existentes para as camadas superiores. Em suma concentra-se na definição de protocolos para as duas camadas inferiores do modelo OSI.

O grupo de trabalho decidiu, em Julho de 1992, concentrar os seus estudos de rádio frequência e esforços de standartização na banda ISM *Spread Spectrum* de 2.4 GHz para ambas as camadas físicas FHSS e DSSS [27]. Desde 1994 foram apresentadas várias versões sucessivas da norma, a primeira, [51], ocorreu em Dezembro de 1994 e a segunda, [52], em Julho de 1995 e outras sucederam-se até à versão do standard utilizada nos nossos dias [35].

Apesar das modificações introduzidas, a ideia base da norma IEEE 802.11 no respeitante à camada MAC teve origem no protocolo denominado DFWMAC (*Distributed Foundation Wireless Medium Access Protocol*) [49], resultante da fusão entre os protocolos referenciados pelas siglas WMAC (*Wireless Medium Access Control*) e WHAT (*Wireless Hybrid Asynchrnous Time-Bounded*), propostos, respectivamente, pela NCR e Symbol e pela Xircom.

Várias propostas foram submetidas ao grupo IEEE 802.11 até 1994, como contributos para o estabelecimento de uma norma standard para redes de área local sem fios. Esta organização desenvolveu o padrão IEEE 802.11 para a industria das redes de comunicação de área local sem fios, proporcionando uma plataforma estável [5].

V.2. Introdução à norma 802.11

A norma IEEE 802.11 define e especifica a arquitectura da rede, a camada física e a camada MAC. Para nos centrar-mos no propósito da norma, é importante referirmos o seguinte, inicialmente estabelecido no standard, "... o objectivo do standard proposto [wireless LAN] é o de desenvolver uma especificação para conectividade sem fios para estações fixas, portáteis ou em movimento dentro duma área local.". Posteriormente foi referido " ...o propósito do standard é o de fornecer conectividade sem fios a equipamento e maquinaria automática ou estações que requeiram rápida disponibilização, os quais possam ser portáteis, manuseáveis (*handheld*) ou possam ser instalados em veículos que se movam dentro de uma área local" [27].

O standard resultante, o qual é oficialmente designado por ***IEEE Standard for Wireless LAN Medium Access (MAC) and Physical Layer (PHY) Specifications***, define protocolos, através do ar, (*over-the-air*) necessários para suportar trabalho em rede numa área local. O seu objectivo, à semelhança dos outros standard base IEEE 802 como por exemplo 802.3 e 802.5, é simultaneamente o serviço primário do standard 802.11 e consiste em entregar MSDUs (MAC *Service Data Units*) entre LLCs pares. Este é conseguido porque fornece funcionalidade MAC e PHY para conectividade sem fios de estações fixas, portáteis e estações móveis, que se desloquem a velocidades de peões ou veículos, dentro duma área local.

Como características específicas do standard, podemos referir: suporte a serviços assíncronos e de entrega em tempo limitado; continuidade do serviço em áreas extensas via sistema de distribuição (DS, *Distribution System*), como por exemplo Ethernet; capacidade para taxas de transmissão de 1, 2, 5.5 e 11 Mbps; suporte à maioria das aplicações do mercado; serviços de *multicast* (incluindo *broadcast*); serviços de gestão da rede; serviços de registo e autenticação. Relativamente a ambientes propícios para a utilização do standard são os anteriormente referidos para as redes de área local sem fios, por exemplo: interior de edifícios, tais como escritórios, bancos, lojas, centros comerciais, hospitais, fábricas e

residências; áreas exteriores, tais como estacionamentos, campus, complexos de edifícios e fábricas es espaço livre.

São também, preocupação do standard IEEE 802.11 as diferenças significativas entre redes de área local cabladas e sem fios, que passam pela tomada de posição relativas a vários aspectos.

A gestão de potência é um aspecto importante atendendo a que a maioria das placas NIC (*Network Interface Card*) sem fios estão disponíveis no formato PCMCIA Tipo II, isto permite-nos adaptá-las a computadores portáteis e móveis provendo-os de conectividade sem fios. O problema, contudo, é que este tipo de equipamentos são suportados por baterias que fornecem energia aos seus componentes electrónicos. A adição de uma placa sem fios a um computador portátil pode gastar a sua bateria rapidamente. O grupo de trabalho 802.11 esforçou-se para encontrar soluções para reduzir a potência consumida, encontrando técnicas que permitam que as placas mudem, periodicamente, para o modo de baixo consumo (*standby*) quando não transmitem, reduzindo o consumo de bateria. Estas funções de gestão de potência são implementadas ao nível da camada MAC, à qual nos referiremos posteriormente nesta dissertação.

Relativamente à largura de banda, a banda ISM, anteriormente referida, não oferece uma grande quantidade, mantendo as taxas de dados mais baixas do que aquilo que seria desejável para algumas aplicações. O standard IEEE 802.11 define um conjunto de canais, igualmente espaçados, na banda ISM de 2.4 GHz. Para a maior parte da Europa são 79 o número de canais e no Japão são 23. Estes canais são espalhados pelas bandas de frequência dependendo da localização geográfica. Por exemplo, as estações compatíveis 802.11, na América do Norte e grande parte da Europa, operam de na banda de 2.402 GHz a 2.480 Ghz. No Japão operam de 2.473 a 2.495 GHz. Por outro lado, cada canal tem a largura de banda de 1 MHz; por isso, a frequência central de operação para o canal 2 (o 1° canal) nos Estados Unidos é 2.402 GHz, para o canal 3 (2° canal) é 2.403 e assim por diante. O grupo de trabalho 802.11, contudo, desenvolveu técnicas para compressão de dados, fazendo o melhor uso possível da largura de banda disponível. Por outro lado, foram também desenvolvidos esforços para aumentar as taxas de dados inicialmente suportadas, de 1 ou 2 Mbps, de modo a dar resposta à crescente necessidade de troca de ficheiros cada vez maiores a que aludiremos posteriormente (Secção V.4.7.).

No aspecto da segurança, as redes de comunicação de área local sem fios transmitem sinais sobre áreas muito maiores do que as que usam os tradicionais meios cablados. Em termos de privacidade têm, por isso, uma área muito maior a proteger. De modo a garantir segurança, o

grupo de trabalho 802.11 coordenou os seus esforços com o Comité IEEE 802.10, responsável pelo desenvolvimento de mecanismos de segurança para todas as séries LANs 802.

Questões inerente ao endereçamento colocam-se porque a topologia de uma rede de área local sem fios é dinâmica, por isso, o endereço do destinatário pode nem sempre corresponder à sua localização. Isto origina um problema quando se encaminham pacotes através da rede para um destino pretendido. Assim, podemos ter necessidade de usar um protocolo baseado em TCP/IP, por exemplo IP Móvel, para alojar estações móveis.

A titulo conclusivo é de referir que, para que exista interoperacionalidade, o standard IEEE 802.11 é compatível com os outros da família 802, por exemplo IEEE 802 – Requisitos Funcionais; IEEE 802.2 – Definição de serviço MAC entre outros.

V.3. Relação entre IEEE 802.11 e IEEE 802.2 (LLC)

As camadas MAC e PHY do standard 802 estão organizadas em conjuntos separados, de standards, da camada LLC devida à interdependência entre controle de acesso ao meio, meio e topologia. Exemplos são as normas: IEEE 802.3 (Ethernet), IEEE 802.4 (Token Bus) e IEEE 802.5 (Token Ring) destinadas a redes com fios. De ênfase especial é o standard 802.2, *Logical Link Control* (LLC), o qual define sincronismo e controle de erros de Nível 2 para todos os tipos de LANs, inclusive 802.11. A família de standards IEEE 802 cai no espaço dos níveis 1 e 2 do modelo de referência OSI.

No standard o protocolo LLC (*Logical Link Control*) especifica os mecanismos de endereçamento das estações através do meio e troca de dados entre duas estações; a Camada MAC (*Medium Access Control*) fornece o acesso ao meio e a Camada PHY (*Physical*) fornece as funções de transmissão.

A camada LLC é a mais alta do modelo de referência IEEE 802 e fornece funções idênticas às do tradicional protocolo Data Link Control: HDLC (*High-Level Data Link Control*), como ilustrado na figura (Ilustração 21), ou seja a troca de dados entre utilizadores finais numa LAN usando uma ligação de controle MAC base 802. Isto é conseguido através de endereçamento e controle do link de dados e, é independente da topologia, do meio de transmissão e da técnica de acesso ao meio escolhida. A camada LLC juntamente com a camada MAC, da norma IEEE 802 têm funções correspondentes ao nível 2 do modelo de referência OSI.

IEEE 802.2 LLC Logical Link Control				Nível 2/OSI (Ligação)
IEEE 802.3 Carrier Sense	**IEEE 802.4** Token Bus	**IEEE 802.5** Token Ring	**IEEE 802.11** Wireless	**MAC**
				PHY **Nível 1/OSI** (Físico)

Ilustração 21 - Normas IEEE 802.X

As camadas superiores, como por exemplo TCP/IP, entregam os dados do utilizador à camada LLC (inferior). Por seu lado, a camada LLC acrescenta-lhes um cabeçalho de controle (*control header*) criando um PDU (*Protocol Data Unit*) de nível LLC. Posteriormente a PDU / LLC é encaminhada para a camada MAC (abaixo) através do MAC *Service Acesss Point* (SA), acrescentando informação de controle no início e fim do pacote, formando uma trama MAC, necessária para a operação do protocolo MAC.

O formato do PDU consiste em quatro campos como ilustrado na figura (Ilustração 22).

8 bits	8 bits	8 bits	variável
SAP Destino **(DSAP)**	Serviço SAP **(SSAP)**	Controlo	Dados

Ilustração 22 Formato do PDU / LLC

Os campos DSAP e SSAP, cada um dos quais contem um endereço de 7 bits, especificam as estações destino e origem, respectivamente. Um dos bit no campo DSAP, indica se a PDU é destinada a uma única estação ou grupo de estações. Um dos bit do campo SSAP, indica se se trata de um comando ou, pelo contrário, um PDU resposta.

O campo de controlo, cujo formato é idêntico ao do campo HDLC, usa sequência de números alargada (7 bits). Estes bits indicam se a trama é de um dos tipos seguinte: Informação (*Information*), usada para transportar dados do utilizador; Supervisão (*Supervisory*), usada para controle de erro e de fluxo; Não Numerada (*Unnumbere*), indica que vários protocolos controlam as PDUs.

O campo de dados, contem a informação, proveniente dos protocolos das camadas superiores.

V.3.1. Primitivas de serviço da camada LLC / MAC

As camadas da arquitectura IEEE 802 comunicam umas com as outras via primitivas de serviço (*service primitives*), podendo estas ser de um dos seguintes tipos: Pedido (*Request*): uma camada usa esta primitiva para solicitar, a outra camada que execute um serviço específico; Confirmação (*Confirm*): uma camada usa esta primitiva para transmitir os resultados de uma primitiva de serviço, *request*, prévia; Indicação (*Indication*): uma camada usa esta primitiva para indicar a outra camada que ocorreu um evento significativo, esta primitiva pode resultar de um *request* ou de algum evento gerado internamente ; Resposta (*Response*): uma camada usa esta primitiva para completar um procedimento iniciado por uma primitiva *indication*.

Cada camada do modelo 802 usa primitivas específicas. No caso da comunicação entre a camada LLC e as camadas MACs, a ela associadas, as primitivas de serviço utilizadas são as seguintes:

MA-UNITDATA.request: A camada LLC envia esta primitiva para a camada MAC para solicitar a transferência de tramas de dados da entidade LLC local, para uma entidade LLC igual, específica ou grupos de entidades iguais em estações diferentes. A trama de dados pode ser uma trama de informação contendo dados de uma camada superior ou, pelo contrário, uma trama de controle gerada, internamente, pela LLC para comunicar com LLCs parceiras;

MA-UNITDATA.indication: A camada MAC envia esta primitiva para a camada LLC para transferir uma trama de dados para a camada LLC. Isto apenas ocorre se a camada MAC verificar que a trama que recebeu da camada física (PHY) é válida, não contem erros e que o endereço destino indica o endereço MAC , correcto, da estação;

MA-UNITDATA-STATUS.indication: A camada MAC envia esta primitiva para a camada LLC para fornecer informação de status acerca do serviço fornecido por uma primitiva MA-UNITDATA.request prévia.

V.3.2. Serviços fornecidos da camada LLC para a camada de rede

A camada LLC utiliza informação de controle na operação do seu protocolo, como exibido na figura (Ilustração 23).

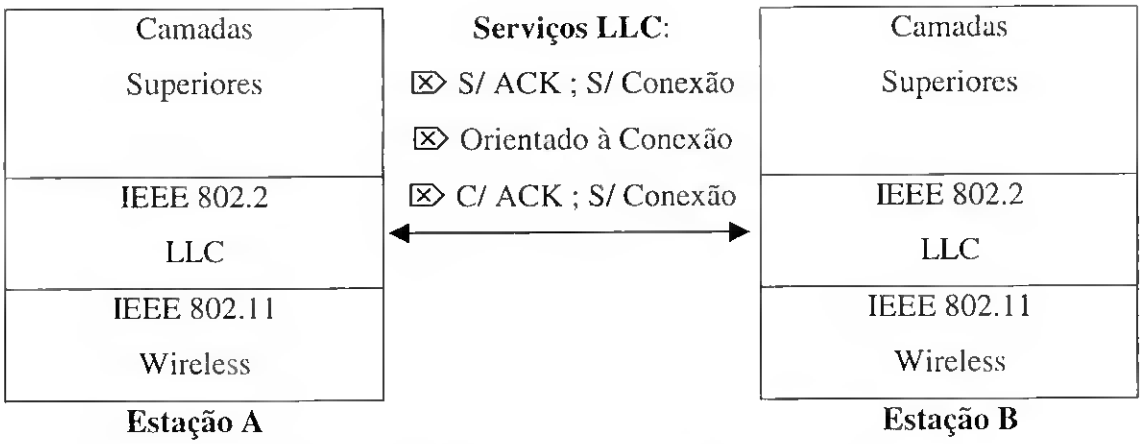


Ilustração 23 - A LLC fornece controle do link fim-a-fim sobre uma LAN IEEE 802.11

A camada LLC fornece os três possíveis tipos de serviços, seguintes, à camada de rede (*Network Layer*): sem reconhecimento e não orientado à conexão; orientado à conexão e com reconhecimento e não orientado à conexão. Estes serviços aplicam-se às comunicações entre camadas LLC iguais (pares), isto é, uma localizada na estação origem e a outra na estação destino. Todos os serviços LLC utilizam o mesmo formato de PDU, anteriormente descrito.

Os fabricantes de componentes para redes sem fios fornecerão estes serviços como opção [27].

V.3.2.1. Serviço sem reconhecimento / Sem conexão

Este serviço é do tipo datagrama, o qual não envolve quaisquer mecanismos de controle de erro ou controle de fluxo. Por outro lado, não implica o estabelecimento de uma conexão ao nível da camada de ligação de dados (*Data Link Layer*), isto é, uma conexão entre LLCs pares e suporta endereçamento individual, *multicast* e *broadcast*.

O serviço apenas envia e recebe PDUs de nível LLC (LLC PDUs) sem qualquer reconhecimento de entrega. Devido ao facto da entrega de dados não ser garantida, a camada superior, por exemplo TCP/IP, deverá gerir as questões inerentes à fiabilidade da transmissão.

Podemos enumerar as seguintes vantagens deste tipo de serviço, se as camadas superiores, da pilha de protocolos, garantirem o fornecimento dos mecanismos necessários para fiabilidade e controle de fluxo seria redundante duplicá-los ao nível LLC. Neste caso o serviço será adequado. São exemplo desta situação os protocolos de transporte ISO e TCP. Por outro lado, nem sempre se manifesta necessário o fornecimento de *feedback* relativo à entrega, com sucesso, da informação. O *overhead* associado ao estabelecimento e manutenção da conexão pode tornar a rede menos eficiente. A implementação prática deste tipo de rede

poderá ser, por exemplo, aplicações que envolvam a amostragem periódica de dados, como sensores para monitorização de temperatura.

V.3.2.2. Serviço orientado à conexão

Este tipo de serviço estabelece uma conexão lógica, a qual fornece controle de fluxo e controle de erros, entre duas estações que necessitem de trocar dados. A sua implementação envolve o estabelecimento de uma conexão entre LLCs pares pela execução das seguintes funções: estabelecimento da conexão, transferência de dados e encerramento da conexão. Por outro lado, apenas pode conectar duas estações por isso, não suportara os modos quer de *multicast* quer de *broadcast*.

As suas vantagens são, principalmente, se as camadas superiores da pilha de protocolos não fornecerem a fiabilidade necessária e mecanismos de controle de fluxo, o que normalmente é o caso dos controladores de terminal. O controle de fluxo é uma característica de protocolo, a qual assegura que uma estação emissora não "entupa" de dados uma estação receptora. Com esta propriedade cada estação alocará uma quantidade finita de recursos de memória e *buffer* para armazenar PDUs enviadas e recebidas.

Para protecção à ocorrência de erros de transmissão, tanto o serviço ora descrito quanto o serviço seguinte, usam mecanismos de controle de erros, os quais detectam e corrigem erros que ocorram aquando da transmissão de PDUs. A titulo meramente informativo podemos referir que estes mecanismos se denominam LLC ARQ (*Automatic Repeat-Request*), do qual podem ser usadas duas abordagens: *Continuos ARQ e Stop-and-Wait ARQ*. Não iremos aborda-las em detalhe por ir além do âmbito da presente dissertação. O controle de erros é justificado porque as redes, especialmente sem fios, padecem do chamado ruído induzido nos links entre as suas estações podendo causar erros de transmissão. Se este for grande o suficiente em amplitude, causará erros na transmissão digital sob a forma de bits alterados. Tal facto poderá conduzir à inexactidão dos dados transmitidos e o receptor pode interpretar de modo incorrecto o significado da informação.

O ruído que causa a maioria dos problemas nas redes é, normalmente de dois tipo Gaussiano e de impulso. Teoricamente, a amplitude do ruído Gaussiano é uniforme ao longo do espectro de frequência, normalmente provocando erros aleatórios e independentes num único bit. O ruído de impulso, mais desastroso, é caracterizado por estar longos períodos de tempo inactivo, seguidos de rajadas de amplitude elevada. Este tipo de ruído resulta de raios ou

relâmpagos e mudanças passageiras, o qual é responsável pela maioria dos erros nos sistemas de comunicação digitais e, geralmente, faz com que os mesmos ocorram em rajadas.

V.3.2.3. Serviço com reconhecimento / Não orientado à conexão

Tal como no primeiro serviço descrito, este não envolve o estabelecimento de uma conexão lógica com a estação remota, contudo, a estação receptora com a versão ACK, deve confirmar a entrega com sucesso de datagramas. O controle de erros e fluxo é manuseado através do método *ARQ Stop-and-Wait*. Este tipo de serviço é útil para diversas aplicações.
O serviço orientado à conexão, anteriormente descrito, exige a manutenção de uma tabela para cada conexão activa, de modo a fazer um traçado inerente ao seu estado. Se a aplicação exigir garantia de entrega, mas existir um grande número de destinatários que necessitem de receber dados, o serviço orientado à conexão pode tornar-se impraticável, entendo ao grande número de tabelas requeridas. Podemos referir, por exemplo, um cenário de fábrica automatizada que requeira que um ponto central comunique com muitos processadores e muitos outros sistemas de tempo real. Todos eles têm em comum o facto da estação emissora necessitar de um ACK para assegurar a entrega de dados com sucesso, contudo, a urgência da transmissão não pode esperar pelo estabelecimento duma conexão.

V.4. O Standard IEEE802.11

A norma IEEE 802.11 define e especifica a arquitectura da rede (distinguindo entre arquitectura física e lógica), a camada física e a camada MAC.

V.4.1. Arquitectura física da rede IEEE 802.11

A arquitectura física de uma rede refere-se à sua topologia e aos blocos básicos que a constituem [24]. A topologia da rede IEEE 802.11 é formada por componentes físicos, os quais interagem para fornecer uma rede de área local sem fios que habilite as estações de uma mobilidade transparente para os protocolos das camadas superiores, como por exemplo a camada LLC.
Um dos componentes fundamentais é a estação, definida como um dispositivo que seja detentor das funcionalidades descritas pela norma 802.11, isto é camada MAC, camada PHY e interface para o meio sem fios. As funções do standard 802.11, anteriormente referidas,

residem fisicamente, na placa rádio NIC, no software de interface que coordena a placa e no ponto de acesso, AP (*Access Point*).

Por seu lado, o bloco básico de uma rede sem fios é a célula ou, como denominado segundo a terminologia IEEE 802.11, área básica de serviço (BSA, *Basic Service Area*) [27]. Ao conjunto das estações que partilham uma mesma BSA dá-se o nome de conjunto básico de serviço (BSS, *Basic Service Set*). Uma BSS é identificado pelo respectivo BSS-Id.

A dimensão de uma BSA depende do ambiente de propagação e também das características dos transceptores. Poderemos aumentar a área de cobertura da rede associando várias BSAs interligadas através de um sistema de distribuição (DS, *Distribution System*), utilizando entidades denominadas pontos de acesso (AP, *Access Points*), como ilustrado na figura (Ilustração 24).

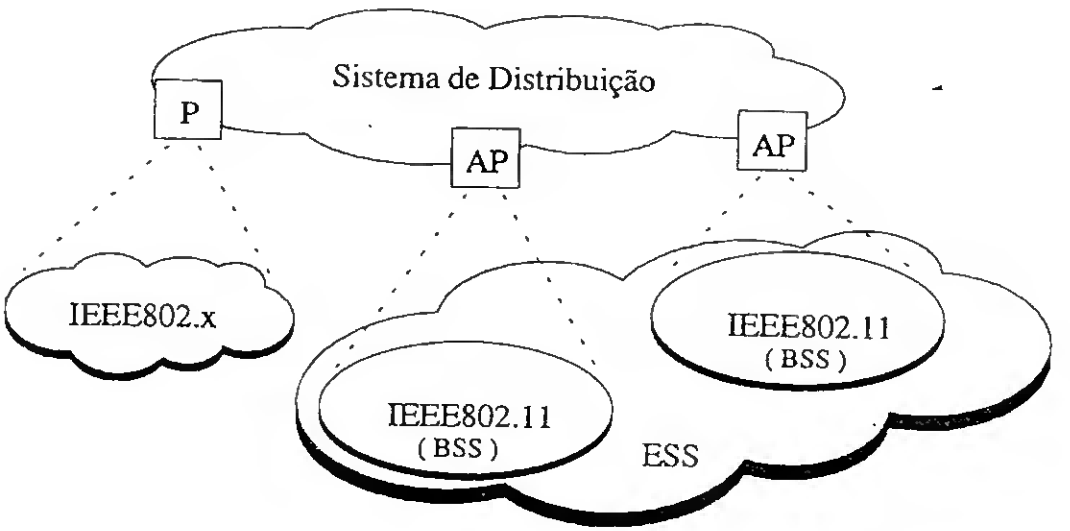


Ilustração 24 – BSA [32]

O sistema de distribuição, DS , pode ter como suporte físico tanto um meio cablado, como sem fios. Assim, numa rede IEEE 802.11 distingem-se dois canais de transmissão : o canal BSA, ou seja o meio onde, normalmente, se movimentam as estações móveis que partilhem a mesma BSA, e o canal DS. Se ocorrer associação de diversas células, BSAs, através de um sistema de distribuição (DS), a esta dá-se o nome de área de serviço estendida (ESA, *Extended Service Area*). Ao conjunto de estações que são abrangidas por uma dada ESA dá-se o nome de conjunto de serviço estendido (ESS, *Extended Service Set*). Um ESS é identificado pelo respectivo ESS-Id. Os elementos funcionais que ligam BSSs, dentro de uma ESS, são os APs (*Acess Points*).

Outra característica importante da arquitectura IEEE 802.11 é a sua flexibilidade para permitir a ligação de redes de área local com fios ao DS utilizando um dispositivo

denominado Portal, P, conforme figura (Ilustração 24). Quando o DS é construído recorrendo a componentes do tipo IEEE 802.X, como por exemplo 802.3 (*Ethernet*) ou 802.5 (*Token Ring*), o Portal e o AP são o mesmo e único componente.

Dependendo da sua arquitectura, as redes IEEE 802.11 podem classificar-se, segundo a sua topologia, em dois tipos : rede Ad-Hoc ou IBSS (*Independent Basic Service Set*) e rede infraestruturada ou ESS (*Extended Service Set*), as quais descreveremos em seguida. De referir que ambas as topologias de rede, IBSS (Ad Hoc) e ESS (infraestruturadas) são transparentes para a camada LLC.

V.4.1.1. Rede Ad Hoc / IBSS

Uma rede Ah Hoc é composta por uma única BSS (célula única) e não necessita de qualquer infra-estrutura para a suportar, nomeadamente um DS. Por outras palavras, é uma BSS *stand-alone* que não tem infra-estrutura de backbone e é composta por, pelo menos, duas estações sem fios. Uma referência mais pormenorizada foi feita no Capitulo III.

V.4.1.2. Rede infraestruturada / ESS

Numa rede infraestruturada a cada BSS está associado um AP, podendo ser constituída por várias BSSs integradas numa única rede IEEE 802.11, através do sistema de distribuição, DS, conforme ilustrado na figura (Ilustração 25).

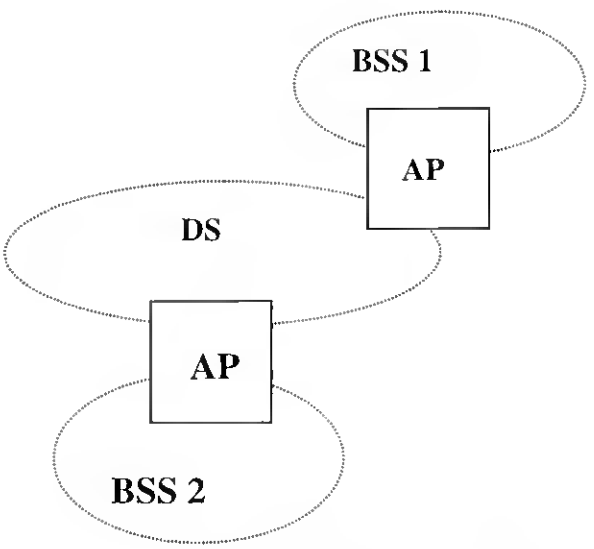


Ilustração 25 Ilustração de uma ESS

Os APs (*Access Points*) suportam diferentes tipos de mobilidades, que referiremos posteriormente, fornecendo os serviços lógicos necessários para manusear o mapeamento endereço - destinatário e a integração ininterrupta de múltiplas BSSs. Outra consideração de extrema importância, reside no facto do standard não limitar o tipo de DS, como tal este pode ser compatível IEE 802 ou qualquer rede não standard. Se as tramas de dados necessitarem de ser transmitidas de e para uma rede local que não seja do tipo IEEE 802.11 estas tramas, como definido pelo standard, entram e saem através do *Portal*. Por outro lado, o AP (Access Point) é uma estação endereçável, servindo de interface com o sistema de distribuição e as estações localizadas dentro das várias BSSs. A cobertura de cada célula é, portanto, garantida pelo AP.

Estas redes caracterizam-se, então por múltiplas células interconectadas por AP e DS e por uma mobilidade livre das estações através das diferentes BSAs. Isto significa que as estações movem-se entre as diferentes BSSs de forma transparente e sem nunca perderem a conectividade com a rede. O fornecimento de serviços que assegurem esta mobilidade das estações é uma função do AP. O standard 802.11 reconhece os seguintes tipos de mobilidade, suportando de modo eficiente as duas primeiras funcionalidades, contudo não garantindo que uma conexão seja mantida quando se mudar de ESS [27]:

Sem transição (***No-transition***): Este tipo de mobilidade refere-se a estações ou que não se movimentam ou que se movem, apenas, dentro de uma BSS local;

Transição BSS (BSS-*transition*): Este tipo de mobilidade refere-se a estações que se movem de uma BSS para outra BSS, dentro da mesma ESS;

Transição ESS (***ESS-transition***): Este tipo de mobilidade refere-se a estações que se movam de uma BSS, situada numa ESS, para outra BSS situada numa ESS diferente.

Na topologia ESS, o standard 802.11 permite as seguintes configurações físicas para as BSSs:

BSS parcialmente sobreposta (***BSSs that partially overlap***): Este tipo de configuração fornece cobertura continua dentro de uma área pré definida, sendo preferencial quando a aplicação não tolerar interrupções no serviço da rede;

BSS fisicamente separadas (***BSSs that are physically disjointed***): Este tipo de configuração não fornece cobertura continua. O standard 802.11 não especifica o limite para a distância entre BSSs;

BSS fisicamente agrupadas (***BSSs that are physically collocated***): Este tipo de configuração garante cobertura continua e pode ser necessário para fornecer uma rede redundante ou de performance bastante elevada.

Estas redes são adequadas às necessidades de utilizadores que excedam as limitações de espaço de uma BSS independente, satisfazendo a necessidade de rede de grande cobertura com tamanho e complexidade arbitrários. A cobertura de cada célula é gerida por um ponto de acesso, AP o qual é geralmente uma estação base ou um repetidor. A rede deve agrupar as células vizinhas de modo apropriado, isto é, a região de sobreposição é planeada para ser mínima de modo a incrementar a capacidade do sistema, mas também para garantir a continuidade do serviço.

A região de junção entre células introduz problemas adicionais, que passaremos a referir:

Interferência própria: existe a possibilidade de que dois APs (ou dois repetidores) tentem transmitir, simultaneamente, um pacote para um nó que se encontre na região de junção. Isto causa interferência e, possivelmente, o pacote é perdido (Ilustração 26(a));

Colisão própria: possível de ocorrer quando um nó na região de sobreposição transmita um pacote, o qual é recebido por mais do que um AP, causando uma possível colisão ou ocupando largura de banda inútil (Ilustração 26 (b));

Colisão cima / baixo: Este é um problema que pode ocorrer nas redes multicélula. O nó A, numa célula, esta a transmitir de baixo para cima (*uplink*) enquanto o nó B, noutra célula, esta a receber (*downlink*) sendo possível que o nó B seja capaz de receber a transmissão do nó A e tal situação resulte em colisão (Ilustração 26 (c)). De referir que esta situação, similar ao problema do terminal oculto, acontece com uma probabilidade muito pequena se as células estiverem correctamente separadas.

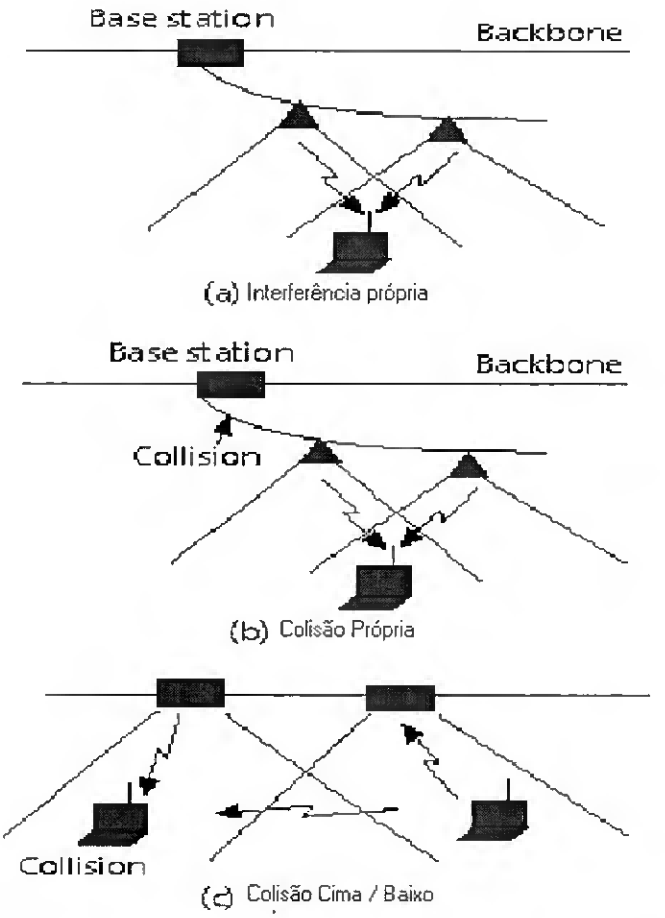


Ilustração 26 - Interferência e colisão [23]

Numa implementação prática, os dois primeiros problemas podem ser eliminados mediante coordenação cuidadosa entre pontos de acesso. Por seu lado, a colisão cima / baixo pode, apenas, ser suavizada mas dificilmente removida. Existirá sempre uma possível janela de colisão, embora possa ser mantida ao mínimo se a coordenação entre pontos de acesso e *uplink / downlink* for adequada.

V.4.2. Arquitectura Lógica IEEE802.11

A topologia, a que referimos anteriormente, é o meio para justificar a necessidade dos componentes físicos numa rede, enquanto a arquitectura lógica define a operação da rede. Como ilustrado na figura (Ilustração 27) a arquitectura lógica do standard 802.11, que se aplica a cada estação, consiste numa única camada MAC e uma ou múltiplas camadas físicas. No caso particular, são suportadas três camadas físicas separadas; FHSS (*Frequency Hopping Spread Spectrum*), DSSS (*Direct Sequence Spread Spectrum*) e IR (*Infra Read*).

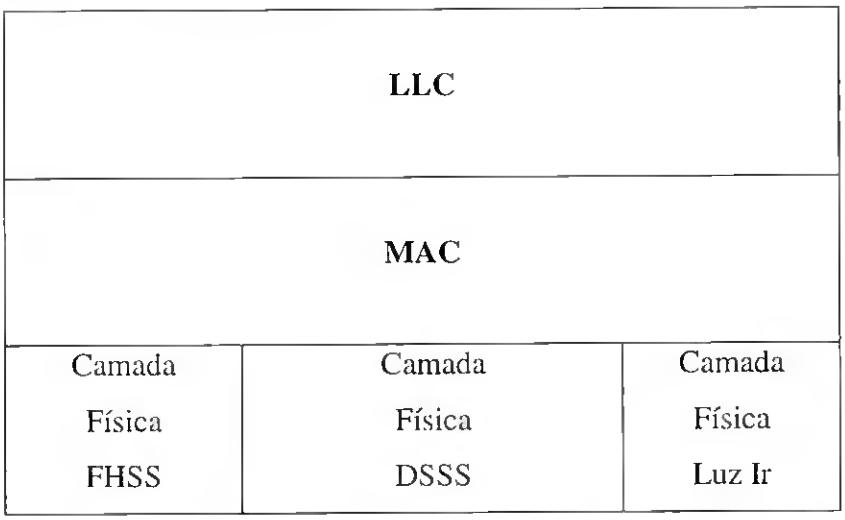


Ilustração 27 -Arquitectura Lógica 802.11

O objectivo da camada MAC é o fornecimento de funções de controle de acesso, tais como endereçamento, coordenação de acesso, geração de sequências de tramas de teste e delimitação de LLC PDU, a um meio físico partilhado como suporte à camada LLC. A camada MAC fornece endereçamento e reconhecimento de tramas no suporte à camada LLC. Por outro lado, o standard IEEE 802.11 implementa ao nível da camada MAC o protocolo de acesso ao meio CSMA/CA (*Carrier Sense Multiple Access / Collision Avoidance*), anteriormente referido. Por ser o tema fulcral desta dissertação iremos abordá-la em capitulo posterior e de modo detalhado (CAPITULO VI).

V.4.3. Camadas físicas IEEE802.11

A camada física admite três possíveis implementações. Quer tanto para DSSS como para FHSS, o standard especifica a banda ISM (*Industrial, Scientific and Medical*) de *Spread Spectrum* de 2.4 GHz porque a mesma está disponível, sem qualquer licenciamento, no mundo inteiro sendo o único factor a ter em consideração a potência radiada. Nos Estados Unidos a FCC Part 15, rege a potência RF radiada na banda ISM, limitando esta norma o ganho de antena ao máximo de 6 dBi e a potência radiada a 1 watt. Os grupos reguladores Europeus e Japoneses limitam a potência radiada a 10 milliwatts per 1 MHz.

A camada física baseada na técnica de modulação DSSS permitia, inicialmente, duas taxas de dados: 2 Mbps usando DQPSK (*Differential Quaternary Phase Shift Keying*) e 1 Mbps usando DBPSK (*Differential Binary Phase Shift Keying*) posteriormente alterada. O standard define sete canais para esta técnica, estando um canal, exclusivamente, definido para o Japão e três pares de canais para os Estados Unidos e Europa. Os canais de um mesmo par podem transmitir sem interferência e todos os canais dos três pares podem ser usados

simultaneamente para efeitos ou de redundância ou de elevada performance, mediante um plano de frequências que evite conflitos de sinal.

O standard IEEE 802.11 especifica a operação com DSSS até 14 canais de frequências diferentes, conforme tabela (Tabela 8). Devemos, também, escolher frequências separadas de pelo menos 30MHz de modo a evitar interferências entre canais.

Nº do Canal	Frequência (GHz)	USA Canadá	Europa	Espanha	França	Japão
1	2.412	X	X			
2	2.417	X	X			
3	2.422	X	X			
4	2.427	X	X			
5	2.432	X	X			
6	2.437	X	X			
7	2.442	X	X			
8	2.447	X	X			
9	2.452	X	X			
10	2.457	X	X	X	X	
11	2.462	X	X	X	X	
12	2.467		X		X	
13	2.472		X		X	
14	2.484					X

Tabela 8 - Canais DSSS específicos para o mundo

Em termos de implementação prática, os fabricantes de produtos para redes de área local sem fios possuem antenas que fornecem uma ampla variedade de padrões de radiação. A norma IEEE 802.11 diz que os níveis de potência transmitida para DSSS deverão estar limitados a dados valores como, por exemplo, na Europa 100 milliwatts (ETS 300-328). A potência efectiva será elevada, embora recorra ao uso de antenas com elevada direccionalidade. De igual modo as PMDs devem suportar, pelo menos, 10 milliwatts de potência de transmissão.

A maioria dos APs e placas rádio permitem-nos seleccionar o seu valor nos parâmetros de inicialização. O standard apela para que os dispositivos rádio possuam controladores de nível de potência, para os casos em que possam transmitir acima de 100 milliwatts.

Em suma, redes de área local sem fios de tecnologia DSSS são capazes de operar a taxas de dados relativamente elevadas, suportando aplicações que requeiram maior área de cobertura e largura de banda dentro de uma única célula. Os produtos DSSS, contudo, são mais caros do que os das outras tecnologias sem fios, podendo fazer com que o preço total do sistema seja superior.

A camada física baseada na técnica de modulação FHSS, permite a taxa de dados de 1 Mbps usando dois níveis de GFSK (*Gaussian Frequency Shift Keying*), podendo, também, utilizar FSK (*Frequency Shift Key*) a 1 ou 2 Mbps. Esta especifica frequências centrais de 79 canais para os Estados Unidos, para os quais existem definidos três conjuntos de 22 sequências de salto. Este sistema é tendencialmente menos dispendiosos na implementação e não consume tanta potência como a sua contrapartida por DSSS, tornado-os mais apropriados para aplicações portáteis. Contudo, FHSS é muito menos tolerante ao efeito de caminho múltiplo ou outras fontes de interferência.

O standard IEEE802.11 define sequências de salto especificando, por exemplo, 78 para a América do Norte e grande parte da Europa e 12 para o Japão. A escolha destas sequências tem por função evitar interferência prolongada o que permitirá, aquando da concepção da arquitectura da rede, colocar múltiplas PMDs de modo a melhorar a performance. Para além das sequências a norma IEEE 802.11 define conjuntos de saltos. Assim, são definidos três conjuntos de saltos, denominados: Set 1, Set 2 e Set 3. Estes contêm uma variedade de sequências de salto concebidas de modo a causarem interferência mínima com cada uma das outras dentro de cada conjunto.

Em termos de implementação prática se optar-mos por uma rede formada por uma única BSS, a escolha destes dois parâmetros é arbitrária. Para este caso, podemos apenas usar as opções por defeito dos fabricantes dos dispositivos. Se, pelo contrário, optar-mos por implementar uma rede formada por várias BSSs integradas na mesma área, devemos assegurar que escolhemos um uma sequência de salto diferente para cada AP, pertencentes a um conjunto comum, de modo a minimizar interferências entre BSSs.

Após seleccionar o conjunto de salto, necessitamos de escolher uma sequência de salto válida para o conjunto escolhido. Os fabricantes usam um número, definido pelo standard 802.11, para representar sequências de salto específicas; e assim, é necessário especificar esse número para cada AP e correspondente BSS. A taxa de salto é configuravel, mas a subcamada PMD deve efectuar salto à taxa mínima especificada pelos Organismos Reguladores do país em particular. A titulo de exemplo podemos referir que FHSS deve

operar à taxa de salto mínima de 2.5 saltos / segundo e, na Europa, a distância mínima de salto em frequência é 6 MHz [27].

Relativamente à potência de transmissão total de rádio FHSS, a mesma deve obedecer ao standard IEEE C95.1 de 1991 [27]. Esta especificação também limita a quantidade máxima de potência de saída de um emissor ao valor de 100 milliwatts de potência irradiada isotropicamente. Este limite permite aos produtos rádio compatíveis coma norma 802.11, obedecer aos valores de potência de transmissão na Europa. A potência efectiva será elevada, embora recorra ao uso de antenas que ofereçam elevada direcionalidade, ou seja ganho. A norma IEEE 802.11 diz, também, que as PMDs devem suportar, pelo menos, 10 milliwatts de potência de transmissão. A maioria dos APs e placas rádio permitem-nos seleccionar o seu valor nos parâmetros de inicialização.

A camada física baseada em técnicas de luz infravermelha, descreve um tipo de modulação que opera na banda de 850 nm para pequenos equipamentos e aplicações de baixa velocidade e utiliza modulação directa. Conforme referimos no Capitulo III, a taxa de dados base é de 1 Mbps usando 16-PPM (Pulse Position Modulation) e permite uma taxa melhorada de 2 Mbps usando 4-PPM. O pico de potência dos dispositivos de infravermelhos está limitado ao valor de 2 watts.

Uma rede de área local sem fios IR oferece excelente imunidade ao ruído e maior segurança do que as implementações rádio DSSS; embora, a pouca disponibilização de produtos força à utilização de dispositivos proprietários.

V.4.3.1. Arquitectura da camada física IEEE802.11

A camada física é dividida em duas subcamadas: PLCP (*Physical Layer Convergence Procedure*) e PMD (*Physical Medium Dependent*), conforme se ilustrado na figura (Ilustração 28).

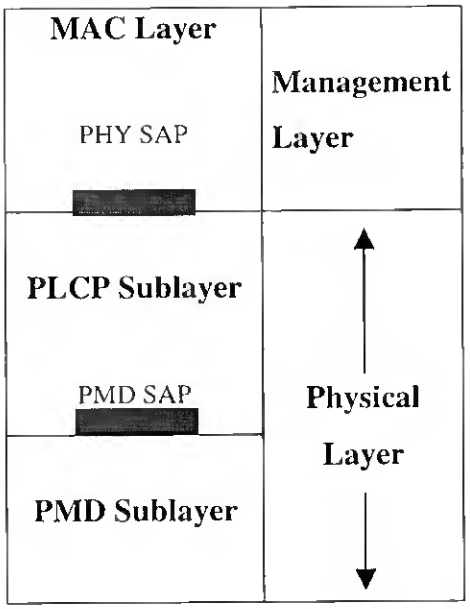


Ilustração 28 - Arquitectura da camada física (PHY Layer)

Em termos de implementação prática esta arquitectura, adoptada pela comunidade IEEE 802.11, permite que uma única camada MAC possa trocar dados com diferentes camadas físicas, de um modo transparente, através do Interface MAC-PHY apropriado em cada estação, conforme figura (Ilustração 29).

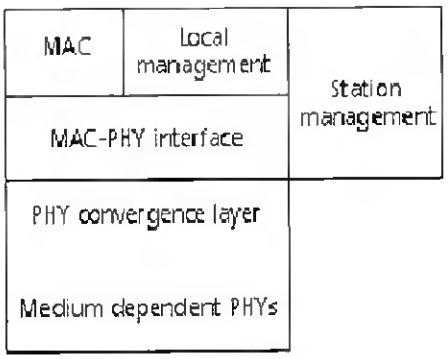


Ilustração 29 - Arquitectura de uma LAN wireless [23]

PLCP (*Physical Layer Convergence Procedure*): A camada MAC comunica com esta subcamada, por meio de primitivas através do PHY SAP (*Physical Layer Service Access Point*). Quando a camada MAC fornece instruções, a PLCP prepara MPDUs para transmissão ou, por outro lado, entrega tramas proveniente do meio sem fios que sejam destinadas à camada MAC. A subcamada PLCP, adiciona campos às MPDUs, os quais contêm informação necessária para os emissores e receptores da camada física.

O standard IEEE 802.11 refere-se a esta trama composta como um PPDU (PLCP *Protocol Data Unit*). A estrutura de trama PPDU permite transferência assíncrona de MPDUs entre estações, como tal a camada física das estações receptoras deve sincronizar os seus circuitos, em particular, para cada trama chegada.

PMD (*Physical Medium Dependent*): A subcamada PMD, actuando sob controle da PLCP, gere a emissão e recepção entre entidades da camada física de duas estações através do meio sem fios. De modo a garantir este serviço, a PMD tem interface directo com o meio e fornece modulação e demodulação das tramas transmitidas. A PLCP e a PMD comunicam entre si por meio de primitivas para gerir a emissão e a recepção.

Gestão da Camada Física: funciona conjuntamente com a gestão da camada MAC, executando funções de gestão para si própria, com o objectivo de minimizar a dependência da camada MAC, da subcamada PMD. A função gestão da camada física que funciona conjuntamente com a gestão da camada MAC, não irá ser aprofundada nesta dissertação.

V.4.3.2. Operações da camada física IEEE 802.11

A operação geral de cada camada física, seja qual for o seu tipo, é muito idêntica. A comunicação com a camada MAC é executada através de primitivas de serviço, as quais são referidas em APÊNDICE B.

As funções, exclusivamente, da responsabilidade da camada física de relevo especial, são executadas ao nível da subcamada PLCP. Para executar estas funções, o standard IEEE 802.11 especifica a utilização de máquinas de estado (*state machines*), cada uma delas com as seguintes atribuições:

1. **Função sentir o meio (*Carrier Sense*)**: esta função determina o estado do meio. A camada física implementa a função de sentir a portadora direccionando a subcamada PMD (*Physical Medium Dependent*) de modo a testar se o meio se encontra livre ou ocupado que, por sua vez, passa esta informação à subcamada PLCP.

Por sua vez, para sentir o meio a subcamada PLCP executa as seguintes operações, caso a estação não esteja a enviar ou receber tramas:

Detecção de sinais: a subcamada PLCP de uma estação sente o meio continuamente. Quando este fica ocupado lê o cabeçalho e preâmbulo PLCP da trama de modo a tentar sincronizar o receptor para a taxa de dados do sinal;

Avaliação do estado do canal: esta operação determina se o meio sem fios está livre ou ocupado. Se o meio estiver livre, a subcamada PLCP envia uma primitiva PHY –

CCA.indication (com o seu campo de status indicando livre) para a camada MAC. Se, pelo contrário, o meio estiver ocupado, a subcamada PLCP envia uma primitiva PHY – CCA.indication (com o seu campo de status indicando ocupado) para a camada MAC. A camada MAC pode então tomar a decisão se deve, ou não, enviar a trama.

2. **Função transmissão (*Transmit*)**: Esta função envia os octetos individuais de cada trama de dados. A subcamada PLCP muda o estado da subcamada PMD para o modo de transmissão após receber, da camada MAC, a primitiva de serviço PHY – TXSTART.request. Juntamente com este pedido são enviados o número de octetos (0 – 4 095) e a instrução da taxa de dados. A subcamada PMD responde enviando o preâmbulo da trama para a antena, no espaço de 20 microsegundos.

O emissor envia o cabeçalho e o preâmbulo da trama a 1 Mbps, esta visa fornecer uma taxa de dados específica e comum a receptores para que todos possam escutar. Após enviar o cabeçalho, o emissor altera a taxa de dados da transmissão para aquela que o cabeçalho especificar. Após efectuada a transmissão, a subcamada PLCP envia uma primitiva PHY – TXSTEND.confirm para a camada MAC, encerra o emissor e muda o estado do circuito da subcamada PMD para o modo de recepção.

3. **Função recepção (*Receive*)**: esta função recebe os octetos individuais de cada trama de dados. A subcamada PMD dará indicação de um meio ocupado enquanto sentir a presença de um sinal de nível de potência de, pelo menos, 85 dBm [35]. Se a operação de avaliação do estado do canal detectar um meio ocupado e a chegada de uma trama com um preâmbulo válido, a subcamada PLCP analisa o cabeçalho respectivo. Se determinar que o cabeçalho não contem erros, enviará para a camada MAC uma primitiva *PHY - RXSTART.indicate* para a notificar da chegada de uma trama. Nesta primitiva enviará, também, a informação que encontrar no cabeçalho da trama (como por exemplo o número de octetos, RSSI e taxa de dados).

Outra função da subcamada PLCP consiste em definir um contador de octetos com base no valor do campo PSDU *Length Word*, do cabeçalho da trama. Este contador registará o número de tramas recebidas, permitindo saber quando ocorre o fim de uma trama. Após receber o octeto final a subcamada PLCP envia, para a camada MAC, a primitiva PHY – RXEND.indicate indicando o final da trama. Do mesmo modo que recebe dados, a subcamada PLCP envia octetos do PSDU para a camada MAC através de primitivas PHY – DATA.indicate.

Em termos de implementação prática, a função recepção pode operar uma única antena ou com múltiplas, factor referido como diversidade[6]. Podemos seleccionar o nível de diversidade, isto é o número de antenas, através do AP e parâmetros da placa rádio.

V.4.3. Tipos de camadas físicas IEEE802.11

V.4.3.1. A camada física FHSS (Frequency Hopping Spread Spectrum)

A subcamada PLCP / FHSS possui tramas próprias, à semelhança das outras subcamadas. A figura (Ilustração 30) ilustra o formato de uma FHSS / PPDU, também denominada trama PCLP.

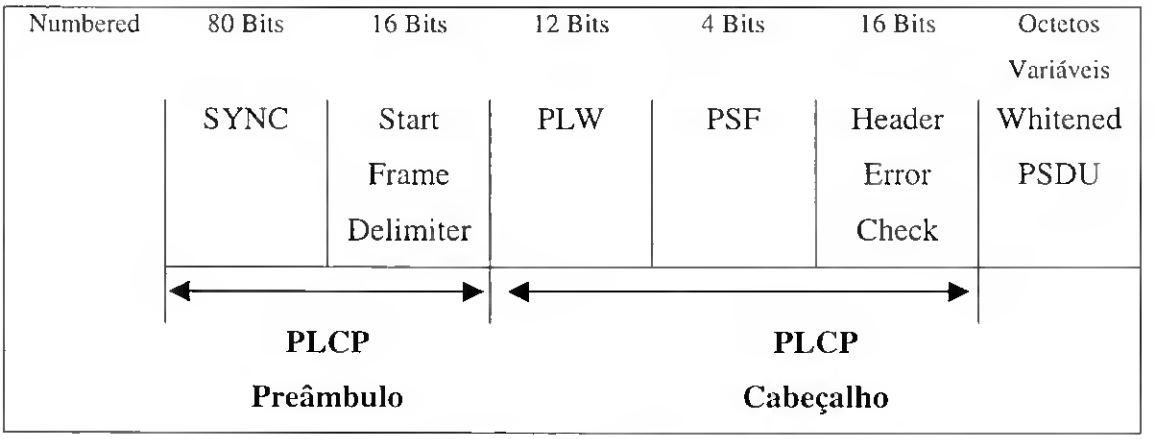


Ilustração 30 - Trama FHSS PLCP

Esta trama é formada por um preâmbulo PLCP, um cabeçalho PLCP e um campo PSDU (PLCP Service Data Unit). De um modo geral, o campo preâmbulo permite ao receptor implementar funções de temporização e diversidade de antena antes da chegada das tramas de dados, o campo cabeçalho fornece informação sobre a trama e o campo PSDU é o MPDU que a estação está a enviar. Os campos específicos da trama PLCP / FHSS são apresentados em APÊNDICE A.

A subcamada PMD / FHSS executa o envio e a recepção de tramas PPDUs sob controle da subcamada PLCP. Para fornecer estes serviços possui um interface directo com o meio ar e permite modulação e demodulação FHSS, da transmissão de tramas. Os serviços são implementados por meio de primitivas, as quais referimos em APÊNDICE B. Estas permitem, entre outras funções, que a subcamada PLCD dirija a subcamada PMD quando a mesma transmite e / ou recebe dados e faz a comutação de canais.

[6] A diversidade (*diversity*) é um método que permite melhorar a recepção do sinal. Assim, o sinal proveniente de várias antenas é analisado e será processado o de maior valor.

A subcamada PMD, baseada em FHSS, transmite PPDUs saltando de canal para canal de acordo com uma sequência de salto pseudo-aleatório, em particular. Esta operação distribui o sinal de modo uniforme através da banda de frequência utilizada. Após ser definida a sequência de salto no AP as estações sincronizam-se, automaticamente, na sequência correcta.

V.4.3.2. A camada física DSSS (Direct Sequence Spread Spectrum)

A subcamada PLCP / DSS possui tramas próprias, à semelhança das outras subcamadas. A figura (Ilustração 31) ilustra o formato de uma trama FHSS / PCLP, que a especificação 802.11 refere como PPDU (PLCP *Protocol Data Unit*).

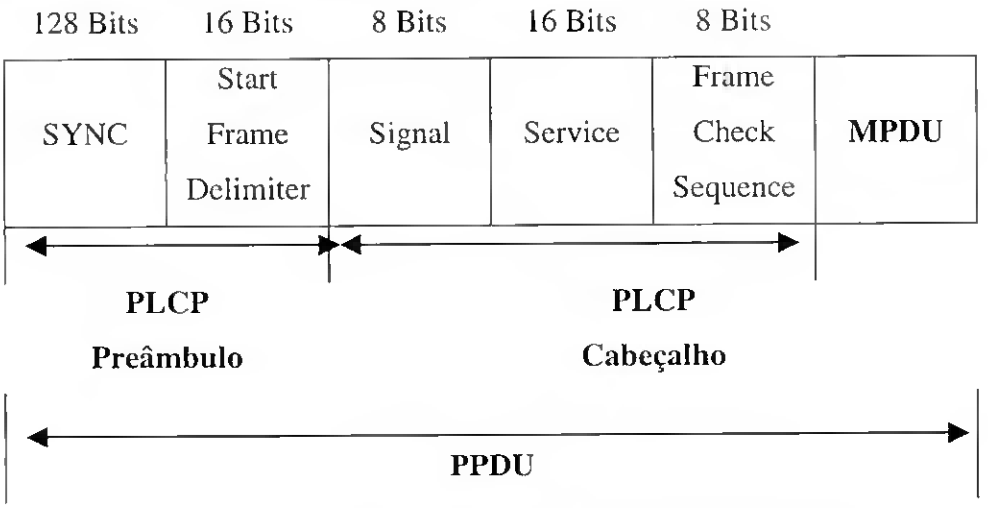


Ilustração 31 - Trama DSSS PCLP / PPDU

Esta trama é formada por um preâmbulo PLCP, um cabeçalho PLCP e um campo MPDU. De um modo geral, o campo preâmbulo permite ao receptor sincronizar-se, de modo adequado, ao sinal chegado antes da chegada da trama de dados, o campo cabeçalho fornece informação sobre a trama e o campo PSDU (PLCP service data unit) é o MPDU que a estação está a enviar. Os campo específicos da trama PLCP / DSSS são apresentados em APÊNDICE A.

A camada MAC, conforme anteriormente referido, efectua uma avaliação da disponibilidade do canal. Com a técnica DSSS, este função varia podendo ser efectuada por um de três modos, os quais passamos a descrever. No modo 1 a subcamada PMD mede a energia presente no meio se esta exceder um nível específico, o qual é o limiar denominado ED (*Energy Detection*);

No modo 2 a subcamada PMD detecta se esta presente no meio um sinal DSSS. Quando tal acontecer, a PMD envia uma primitiva PMD_CS (*Carrier Sense*) para a subcamada PLCP;

No modo 3 a subcamada PMD detecta se esta presente no meio um sinal DSSS que exceda o limiar ED. Quando tal acontecer a PMD envia as primitivas PMD_ED e PMD_CS para a subcamada PLCP. Após acontecer qualquer uma das situações anteriormente referidas, a subcamada PMD envia uma primitiva PMD_ED para a subcamada PLCP. Por sua vez esta subcamada indicará, então, a detecção de canal disponível à camada MAC.

A subcamada PMD / DSS, tal como nas outras camadas físicas, executa o envio e recepção de tramas PPDUs sob controle da subcamada PLCP. Para fornecer este serviço terá um interface directo com o meio ar e permite modulação e demodulação DSSS, da transmissão de tramas. Os serviços a ela inerentes são executado por meio de primitivas, as quais referimos em APÊNDICE B.

V.4.3.3. A camada física IR (Luz Infravermelha)

A figura (Ilustração 32) ilustra o formato de uma trama IR / PCLP a que a especificação 802.11 refere como PPDU (PLCP *Protocol Data Unit*).

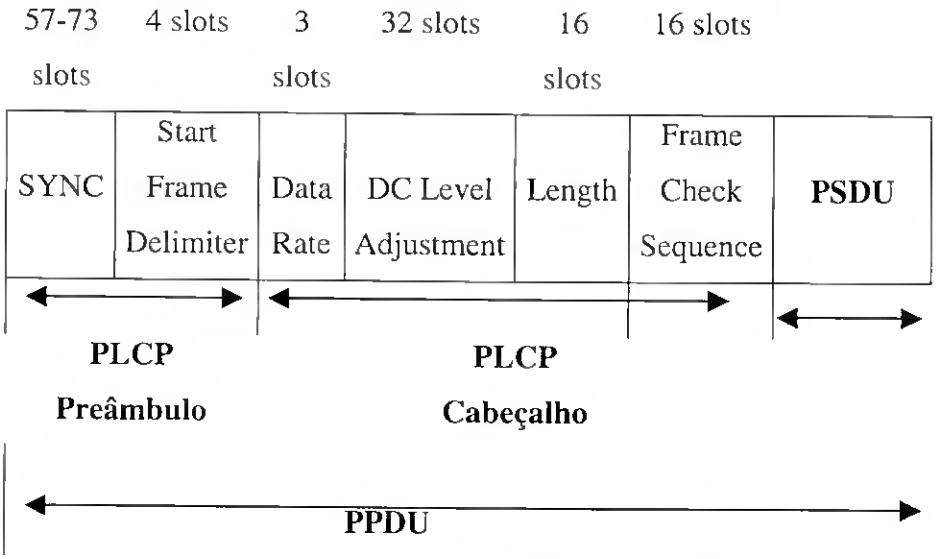


Ilustração 32 - Trama PLCP IR

Esta trama é formada por um preâmbulo PLCP, um cabeçalho PLCP e um campo MPDU. De um modo geral, o campo preâmbulo permite ao receptor sincronizar-se, de modo adequado, ao sinal chegado antes da chegada da trama de dados. O campo cabeçalho fornece informação sobre a trama e o campo PSDU (PLCP service data unit) é o MPDU que a estação está a enviar. Os campos específicos da trama PLCP / IR são apresentados em APÊNDICE A.

A operação da subcamada PMD / IR transforma a representação binária de PPDUs em sinal de luz infravermelha, adequada para transmissão. A camada física IR 802.11 opera usando modulação directa.

V.4.4. Implicações do Standard IEEE 802.11

À semelhança de qualquer outra tecnologia ou standard devemos estar cientes das implicações inerentes à implementação de redes de área local sem fios baseadas no mesmo. Assim, para além de todas as que temos vindo a referir ao longo desta dissertação, vamos em seguida referir as implicações especificamente relacionadas com o standard IEEE 802.11 segundo a sua versão original.

Começamos pelas taxas de dados relativamente baixas, inicialmente 802.11 suportava taxas de dados até 2 Mbps [27]. Alguns fabricantes e utilizadores reclamavam que esta taxa era reduzida. Exemplo disso são transmissões de vídeo, por exemplo, as quais podem requerer elevadas taxas de dados se as aplicações necessitarem de taxas de tramas, profundidade de pixel e resoluções que requeiram elevadas quantidades de largura de banda. O mesmo se passa com transmissões de grandes blocos de dados. No outro extremo as aplicações tipo código de barras; como por exemplo recepção, inventário e marcação de preços trabalham de modo adequado sob a limitação do standard a 2 Mbps. Com as versões actuais do standard, a que faremos alusão posteriormente, esta limitação foi ultrapassada.

Outro factor limitativo diz respeito à falta de *roaming* standard entre os APs de fabricantes distintos. O standard IEEE 802.11 não define o protocolo necessário para mover as suas tramas dentro do DS, o qual sai do âmbito do tipo de LANs 802, sendo a definição de protocolos do DS deixado para as camadas superiores (Rede e Transporte). Como resultado o standard não define comunicações entre APs. Na conjectura actual é deixado aos fabricantes de APs a definição de protocolos necessários para o suporte ao *roaming* de um AP para outro. Como medida preventiva devemos considerar a aquisição de APs de um único fabricante, embora o mesmo não aconteça com as placas rádio.

Relativamente às questões inerentes à compatibilidade com o standard IEEE 802.11, podemos afirmar que nenhuma standartização valerá a pena, a menos que os fabricantes e utilizadores criem produtos compatíveis. Verificou-se que a maioria dos fabricantes de dispositivos para redes sem fios, iniciaram em 1998 e 1999 o lançamento de placas rádio e APs compatíveis com o standard oficial 802.11 e têm ido acompanhando as suas mais recentes actualizações. O standard refere que o fabricante deve cumprir um proforma

denominado PICS (*Protocol Implementation Conformance Statement*). A sua estrutura inclui, principalmente, uma lista de questões fixas às quais o fabricante responderá com sim / não. Assim, de modo a garantir compatibilidade, os fabricantes testam os seus produtos no InterOperability Laboratory da Universidade de New Hamphire [27]. Fundado em 1988, efectua trabalhos de pesquisa e desenvolvimento para verificar a interoperacionalidade e conformidade de produtos destinados a comunicações, não apenas para redes sem fios como também para redes cabladas.

Deve existir compatibilidade por parte do utilizador final tendo-se assistido a este fenómeno durante o ano de 1999 e seguintes. Uma questão pertinente é se como utilizadores finais teremos a necessidade de utilizar produtos compatíveis. Claro que a resposta é não, mas devemos considerar, cuidadosamente, as vantagens e desvantagens da instalação de redes compatíveis. O mais provável é que a compatibilidade, com o standard, seja favorecida em detrimento de implementações proprietárias.

A compatibilidade electromagnética internacional é abordada pelo standard. Como anteriormente referido, este especifica operação na banda de 2.4 GHz; contudo, os requisitos relativos ao comportamento electromagnético variam de país para país. Assim, podemos salientar que as frequências de operação, os níveis de potência e níveis de *spurious* diferem. Os organismos reguladores em cada país, individualmente certificam o equipamento sem fios. O standard IEEE 802.11, contudo, identifica os requisitos técnicos mínimos par garantir interoperacionalidade e compatibilidade baseados nas normas estabelecidas para a Europa, Japão e Estados Unidos.

No caso da Europa os requisitos são estabelecidos pelos seguintes Organismos e Documentos, embora possam existir regras próprias para alguns países, em particular: Aprovação: ETSI (*European Telecommunications Standards Institute*); Documentos: ETS 300-328, ETS 300-339; Autorização: *National Type Approval Authorities* [27].

V.4.5. As versões actuais do standard IEEE 802.11

Questões, sem duvida, pertinentes são, por exemplo, qual será o futuro do standard IEEE 802.11; poderão os utilizadores finais possuir completa compatibilidade com a norma; poderá o grupo de trabalho resolver questões que limitam o standard. A estas e outras questões apenas o tempo poderá responder. É dado adquirido que os principais fabricantes de redes de área local sem fios estão a disponibilizar, sobretudo deste 1998, produtos compatíveis e a facilitar a actualização dos sistemas instalados. Se combinarmos este feito

com a vantagem de normalização devemos assistir à proliferação de redes compatíveis IEEE 802.11.

V.4.5.1. As normas IEEE802.11a e IEEE802.11b

Como anteriormente referido o IEEE homologou a norma original, 802.11, em Junho de 1997, após sete anos de trabalho, como o standard para WLANs, a qual suportava taxas de dados de 1 e 2 Mbps. A questão mais crítica relativa à exigência destas redes foi o seu limitado *throughput*. Assim, verificou-se que as taxas de dados suportadas pelo standard inicial se tornaram demasiado lentas para suportar os requisitos das aplicações mais recentes. Tendo o Comité 802.11 sentido esta necessidade concentrou esforços para produzir um standard para WLANs de alta velocidade (*high speeed WLAN*), surgindo assim dois grupos de trabalho TGa e TGb (*Task Group*) [21]. O TGa desenvolveu uma camada física, de alta velocidade, na banda ISM de 5 GHz, a qual é completamente compatível com a camada MAC 802.11 existente e é adequada não apenas para o transporte de dados, mas também de voz e imagem. Esta banda permite velocidades de 20 a 25 Mbps. Por outro lado, o TGb desenvolveu uma camada física, de alta velocidade, na banda ISM de 2.4 GHz com velocidades de 5.5 e 11 Mbps, também completamente compatível com a camada MAC 802.11.

Em Setembro de 1999 foram ratificadas as normas IEEE 802.11a [37] e IEEE 802.11b [36], as quais introduziram alterações apenas ao nível da camada física, conforme ilustrado na figura (Ilustração 33).

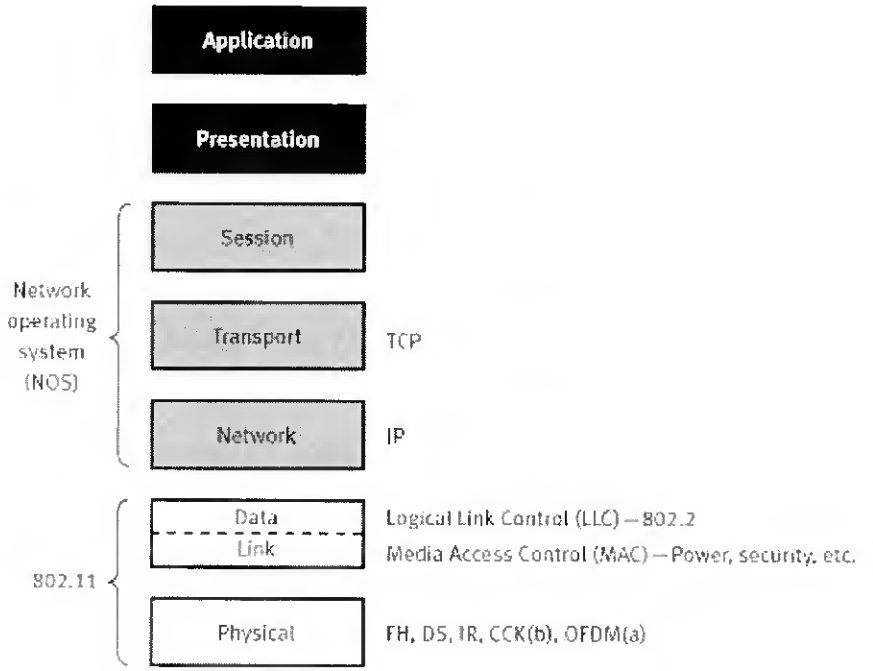


Ilustração 33 - Camada Física IEEE 802.1a e IEEE 802.11b [21]

A camada MAC 802.11, que não sofreu alterações, permite múltiplas taxas de dados dentro da mesma área bem como a sua computação por estações que possam não as suportar. Isto significa que, na teoria, as estações podem suportar taxas de dados superiores e continuar compatíveis com os produtos existentes.

Com estas alterações a família de standards 802.11 é actualmente a ilustrada na tabela (Tabela 9).

	IEEE 802.11	**IEEE802.11a**	**IEEE802.11b**
Aplicação	Wireless Ethernet (LAN)	Wireless ATM	Wireless Ethernet (LAN)
Intervalo de Frequências	2.4 GHz	5 GHz	2.4 GHz
Taxa de Dados	1 - 2 Mbps	20 – 25 Mbps	5.5 – 11 Mbps

Tabela 9 - Família de Standards IEEE 802.11

Após estas reformulações o standard 802.11 passou a especificar cinco camadas físicas: FHSS, DSSS, IR, *High Rate* DSSS (HR/DSSS) e *Orthogonal Frequency Division Multiplexing* (OFDM). As duas últimas são usadas nas WLANs de alta velocidade do seguinte modo, IEEE 802.11a usa OFDM e IEEE 802.11b usa HR/DSSS.

Relativamente às técnicas de modulação, até à aprovação destas novas versões, BPSK e QPSK eram usadas pelas várias camadas físicas, as quais eram suficientes para velocidades de 1 e 2 Mbps mas não acompanharam as exigências dos esquemas de transmissão de taxas

de dados a velocidades superiores. Assim, tiveram que ser equacionadas técnicas de modulação diferentes. As possíveis técnicas consideradas pelo comité 802.11 foram, entre outras: *M-ary Orthogonal Keying* (MOK), *Complementary Code Keing* (CCK), *Shift Keying (CCSK), Pulse-Position Modulation* (PPM) e *Orthogonal Frequency Division Multiplexing* (OFDM).

Para a banda de 5 GHz o comité IEEE 802.111 ratificou a especificação sugerida pelo grupo de trabalho 802.11a. Esta é baseada na técnica de modulação OFDM e opera nas bandas 5.15-5.25; 5.25-5.35 e 5.725-5.825 GHz. Estes sistemas fornecem taxas de dados de 6 a 54 Mbps [25].

Para a banda de 2.4 GHz o comité IEEE 802.111 ratificou a especificação sugerida pelo grupo de trabalho 802.11b. Esta é baseada ns técnica de modulação CCK, suporta ambas as taxas de dados de 5.5 e 11 Mbps e continua, no entanto, compatível com os esquemas de 1 e 2 Mbps. Este foi, sem dúvida, um factor que contribuiu para a sua maior aceitação por parte dos diversos fabricantes das tecnologias sem fios.

O standard original definiu três camadas físicas duas *Spread Spectrum* e uma por Infravermelhos. De notar que FHSS e DSSS são fundamentalmente mecanismos de sinalização diferentes e não inter-operam um com o outro, conforme referimos anteriormente. De ênfase especial é o facto da FCC restringir, na técnica FHSS, a largura dos subcanais a 1 MHz, o que faz com que estes sistemas tenham que espalhar a sua utilização pela totalidade da largura de banda disponível. Esta limitação faz com tenham que saltar, de frequência em frequência, muitas vezes o que conduz a um grande *overhead* proveniente dos saltos e por outro lado não pode suportar velocidades superiores sem violar as regras actuais da FCC.

A principal melhoria introduzida ao nível da camada física foi a de tornar standard a sua utilização às velocidades de 5.5 e 11 Mbps. Para conseguir este desempenho foi seleccionada a técnica de modulação DSSS atendendo a que a sua utilização não viola qualquer norma da FCC, como acontece com FHSS. Por outro lado, os novos sistemas 802.11 DSSS são completamente compatíveis com os anteriores a 1 e 2 Mbps, mas não com os FHSS a 1 e 2 Mbps.

Os Organismos Reguladores bem como os fabricantes apoiaram estas novas versões baseados na mais valia de que as WLANs serão capazes de alcançar *performance* sem fios bem como *throughput* comparáveis à sua contrapartida cablada Ethernet. De referir a criação, pelas empresas lideres deste mercado, de uma aliança denominada WECA (*Wireless Ethernet Compability Alliance*), cuja missão é a de certificar interoperacionalidade entre os

produtos dos vários fabricantes bem como entre os produtos para redes sem fios 802.11b e fomentar a utilização do standard nos mais diversos cenários.

Em suma podemos afirmar que com estas alterações a arquitectura base, características e serviços da norma 802.11b são os mesmos que os definidos pelo standard 802.11. A nova especificação apenas afecta a Camada Física (PHY *Layer*) adicionando-lhe taxas de dados superiores e conectividade mais robusta. Por outro lado, a técnica, apresenta como principal benefício a resistência a interferência por múltiplos caminhos, o que faz com os dispositivos baseados na mesma sejam menos susceptíveis a este efeito e consequentemente apresentem performance superior.

Para além da compatibilidade e demais vantagens anteriormente referidas, outro factor de extrema importância consiste no facto de que, para suportar ambientes muito ruidosos bem com grandes distâncias, as WLANs 802.11b usam uma técnica denominada *Dynamic Rate Shifting*, a qual permite que as taxas de dados sejam automaticamente ajustadas. Esta tem por objectivo compensar a natureza inconstante dos canais rádio. Em condições ideais os utilizadores estão conectados à taxa total e permanente de 11 Mbps, contudo quando estes se afastam do intervalo de operação óptimo ou a interferência seja significativa os dispositivos irão transmitir a velocidades inferiores descendo para 5.5, 2 e 1 Mbps. Da mesma forma se o dispositivo voltar para o espaço de transmissão de alta velocidade a conexão automaticamente retomará a taxa original. O mecanismo anteriormente descrito, da camada física, é transparente tanto para o utilizador como para as pilhas de protocolos das camadas superiores.

Relativamente à mobilidade nas redes infraestruturadas, 802.11b define a forma como uma estação se associa com os APs, mas continua a não definir, porém, como estes mantêm um traçado dos utilizadores à medida que estes se movem, em primeiro lugar entre a camada 2 de dois APs da mesma rede ou em segundo lugar na camada 3 quando os utilizadores passam a barreira de um *router* entre duas redes. Para resolver estas questões, normalmente é feito um manuseamento através de protocolos específicos dos diversos fabricantes os quais variam em termos de performance.

Relativamente à gestão de potência os produtos finais compatíveis com a norma 802.11b incorporam um mecanismo denominado *Power Saving Protocol*, que permite maximizar a duração da bateria. Relativamente à segurança dos dados, a norma 802.11b possui encritptação WEP de 40-bit, a qual deve ser suficiente para a maioria das aplicações. Esta pode ser complementada com outras técnicas de controle de acesso disponíveis.

Como conclusão podemos referir que a versão actual do standard IEEE 802.11 possui, com certeza, benefícios que qualquer potencial utilizador deve considerar ao seleccionar componentes que forneçam mobilidade numa rede de área local. Por outro lado, quando concebemos uma rede de área local sem fios devemos analisar a utilização de produtos compatíveis com o standard, mas certificar-nos que a taxa de dados permitida suportará as nossas aplicações e que os componentes escolhidos suportam a necessária mobilidade entre APs.

CAPITULO VI
A CAMADA MAC IEEE 802.11

Este capítulo descreve, de modo aprofundado, a camada MAC da rede sem fios IEEE 802.11. Assim, vamos abordar as suas funções que são o protocolo de acesso ao meio, a função de fragmentação, as funções de gestão e as funções que asseguram o transporte de informação através da rede.

VI.1. Introdução

O modelo de referência elaborado pelo IEEE (*Institute of Electric and Electronics Engineers*) definiu, como anteriormente referido, uma arquitectura de três camadas, cujas funções de comunicação, essenciais de uma rede local sem fios, correspondem aos níveis 1 e 2 do modelo OSI. Destas funções compete, como vimos, à camada LLC fornecer um ou mais pontos de acesso aos utilizadores. As restantes, tratadas numa camada separada denominada MAC, são: na emissão, converter os dados a serem transmitidas em tramas com campos de endereço e detecção de erros; na recepção, desmontar as tramas efectuando o reconhecimento do endereço bem como detecção de erros e gerir a comunicação. O objectivo primordial desta filosofia é permitir a definição de várias opções para a camada MAC, que podem ser optimizados segundo as necessidades. A sua arquitectura, anteriormente descrita, prevê o acesso das estações ao sistema de distribuição (DS / backbone) via pontos de acesso (AP) no que diz respeito ás redes infraestruturadas e um outro modelo no qual um conjunto de estações comunicam na rede de forma interactiva (Ad Hoc). Assim, a camada MAC de uma rede IEEE 802.11, para além da execução do protocolo da acesso ao meio, é também responsável pela execução da função de fragmentação, das funções gestão e de um conjunto de funções que asseguram o transporte da informação através da rede.

Relativamente ao protocolo de acesso ao meio, a norma IEEE 802.11 define um acesso do tipo híbrido que integra duas funções de coordenação do mesmo, uma distribuída e outra centralizada.

A função de fragmentação é utilizada pela estação emissora sempre que esta necessite de subdividir o MSDU (MAC *Service Data Unit*) entregue à camada MAC, caso por exemplo de quando o canal de transmissão é afectado por interferências externas. Na recepção a função inversa é denominada reconstrução.

As funções de gestão têm por base mecanismos que implementam a função de sincronização temporal, a função de associação e reassociação e a função de conservação de potência consumida.

As funções que asseguram o transporte da informação através da rede podem ser divididas em dois tipos de serviços : serviços da estação e serviços do sistema de distribuição.

Cada estação e ponto de acesso numa rede de área local sem fios 802.11 implementam o serviço da camada MAC que fornece a capacidade para entidades LCC, parceiras, trocarem MSDUs entre SAPs (*Service Access Points*). Estes transportam tramas LLC, as quais facilitam as funções da camada LLC. Em suma a camada MAC, de uma estação, fornece principalmente três funções: acesso ao meios sem fios, integração na rede e fornecimento de autenticação e privacidade.

As características esperadas de protocolos da camada MAC são as seguintes. Devemos ter em consideração que, o grupo de trabalho da norma IEEE 802.11 determinou requisitos a que um protocolo MAC (*Medium Access Control*) deve obedecer de modo a ser consistente. Estes, que iremos descrever em seguida, podem genericamente ser considerados como características esperadas em qualquer rede de comunicação de área local sem fios e não apenas de uma rede IEEE 802.11 [27].

1. **Desempenho (*Throughput*)**: Este requisito é também referido como capacidade e é o escoamento máximo que o método de acesso pode tirar do meio relativamente à percentagem de banda passante disponível. Algumas das variáveis que afectam a capacidade são a taxa de transmissão, comprimento da rede, tamanho do cabeçalho e o atraso em cada estação (filas de espera provocadas por deferimentos e retransmissão). É uma das considerações mais criticas na concepção de um protocolo MAC, desde que o espectro seja um recurso escasso. Podemos referir como exemplo de análise de desempenho, os protocolos de acesso aleatório do tipo ALOHA, os quais padecem de problemas de estabilidade isto é, o pico de *throughput* é acompanhado de grandes atraso. Por outro lado, o protocolo Ethernet com transmissão física a 10 Mbps e acima de 80 % de throughput para CSMA/CD pode alcançar, em principio, uma performance acima de 8 Mbps. Na realidade, medições práticas mostram que apenas é conseguida performance de 3 a 3.5 Mbps.

2. **Atraso**: As características relativas a este requisito têm uma importância que é directamente dependente da aplicação em particular. Afectam, de modo especial, os serviços de tempo limitado e aplicações multimédia tais como voz e vídeo. Este atributo corresponde ao somatório dos atrasos de acesso e de transmissão. O atraso na transferência é na maioria

dos casos, senão em todos, uma variável aleatória, no entanto em alguns protocolos o maior valor que este pode assumir é limitado.

3. **Estabilidade:** É uma característica importante em aplicações nas quais exista uma sobrecarga da rede. Os protocolos de acesso que alocam intervalos separados para cada nó são, normalmente, bastante estáveis e não apresentam grandes variações relativamente ao atraso. Por outro lado, os esquemas baseados em contenção têm uma estabilidade bastante dependente da realização, exigindo mecanismos sofisticados para o tratamento de conflitos e assim tornar o protocolo mais estável.

4. **Transparência das diferentes camadas físicas (PHY Layers)**: Um dos requisitos especiais da camada MAC, para as redes em causa, é a transparência relativa ás diferentes camadas de transmissão físicas seja qual for o seu tipo. Estas apresentam, com vimos anteriormente, diferenças na concepção do sistema e nas características de propagação devendo um MAC manusear todas elas.

5. **Capacidade para servir voz, dados e vídeo**: Este requisito da camada MAC visa dar resposta à popularidade das aplicações multimédia. Assim, será desejável que as redes de comunicação de área local sem fios sejam capazes de fornecer alguns serviços de tempo limitado tais como voz e vídeo, adicionalmente aos serviços de dados obrigatórios.

6. **Justiça no acesso (*Fairness*)**: é um atributo desejável na maioria das redes de modo a permitir ás estações o acesso a recursos partilhados. Justiça não significa a não existência de prioridade de acesso, mas simplesmente que a estação deverá ser tratada de modo igual dentro da sua classe de prioridade. Este requisito prende-se com as características de atenuação inerentes aos canais interiores (*indoor)* onde estas redes tipicamente operam. Esta situação pode resultar num acesso injusto à rede isto é, um nó móvel pode ter recebido muito menos potência da estação base que outro.

Quando o protocolo MAC estiver a operar no modo de contenção, ao qual faremos referência posteriormente (necessário para o registo inicial e frequentemente usado para trafego *uplink*), o nó móvel em desvantagem pode não ter possibilidade de aceder, por enquanto, ao canal. Por tal facto o MAC deve estar habilitado para resolver esta situação, desde que seja possível que a captura possa ocorrer com diferenças de potência tão pequenas, na ordem 6 a 9 dB, enquanto a gama dinâmica de atenuação pode ser grande, na ordem de várias dezenas de dB.

7. **Consumo de bateria**: Este requisito é outra consideração importante para um protocolo MAC, tendo em vista a utilização eficiente das potências emitida e recebida. Muitos dos protocolos de alto nível propostos, requerem a existência de nós móveis para constante monitorização dos pontos de acesso ou *handshake* com a estação base com

propósitos de sincronismo, controle de potência ou troca de informações de estado. Assim, deve ser utilizada potência limitada para a transferência de pacotes bem como ser possível implementar o modo *sleep* no lado receptor. Podemos referir, a titulo de exemplo, que o modo de recepção permanentemente activo pode consumir mais potência de bateria do que a operação de transmissão.

8. **Número máximo de nós**: Este requisito, também referido como escalabilidade do protocolo, diz que o MAC não deve limitar o número máximo de nós de modo a manter uma performance aceitável. Esta consideração prende-se com estudos de mercado que mostram que uma rede de comunicação de área local sem fios pode ter necessidade de suportar centenas de nós.

9. **Robustez em redes agrupadas**: Um dos grandes desafios que se coloca na concepção de um MAC para uma rede de comunicação de área local sem fios é o facto deste funcionar com sucesso no caso de redes agrupadas. Este conceito baseia-se na realidade de ser possível, com elevada probabilidade, que duas ou mais redes operem na mesma região, ou em regiões onde exista interferência entre redes diferentes e com o facto de alguns protocolos não conseguirem funcionar normalmente em situações análogas.

10. **Capacidade para suportar *handoff* / *roaming* entre áreas de serviço**: Um protocolo MAC deve suportar a função de *handoff* para servir nós que se movam de uma célula para outra. Esta questão da mobilidade é uma característica especial das redes de comunicação de área local sem fios nas quais, devido ao ambiente interior (*indoo*) e à rápida atenuação, o *handoff* não é um problema objectivo.

Nos serviços de tempo limitado a capacidade do protocolo MAC para suportar o *handoff* em tempo real não é tarefa fácil, especialmente se tivermos em consideração o consumo de potência. Por outro lado, o *handoff* das redes de comunicação de área local sem fios, modo geral, é distribuído isto é, não existe uma estação central com esta tarefa adstrita o que o torna mais difícil.

11. **Estabelecimento de conectividade ponto-a-ponto sem conhecimento à priori**: O MAC de uma rede de comunicação de área local sem fios deve suportar interligação ad hoc (redes ad hoc). Assim, não deverá ser requerida à priori informação sobre a topologia da rede (se existir comunicação por todos os nós).

12. **Impacto no *throughput* dos acessos não autorizados**: Um MAC conjuntamente com um esquema de segurança da rede, ambos de sucesso, deverão rejeitar este tipo de acessos e minimizar o seu impacto, se for o caso. Este último deve ser tido em conta porque, uma vez que não se consiga identificar qualquer acesso não autorizado à rede antes deste

ocorrer, ele inevitavelmente terá impacto no desempenho da mesma bem como consequente atraso.

13. **Capacidade para suportar transmissões por difusão (*broadcast / multicast*)**: O MAC deve também suportar *multicast*, embora a forma de comunicação nativa de uma rede de comunicação de área local sem fios seja por difusão (*broadcasting*).

14. **Atrasos críticos limitam áreas de cobertura grandes**: As redes de comunicação de área local sem fios deverão operar, possivelmente, a mais do que 10 a 20 chips por segundo (c/s) para DSSS e mais do que 1 M símbolos por segundo para outras camadas físicas (PHYs) [100]. Um atraso no intervalo de 500 a 1000 ns pode causar grandes problemas para alguns MACs. Como tal devemos ter em conta que, atendendo a que a sua área de cobertura típica pode ser de 150 metros quadrados a 300 metros quadrados, introduz aproximadamente 500 a 1000 ns de atraso de propagação. Por exemplo, se o MAC tiver que operar com precisão síncrona entre cada par de nós de comunicação, o atraso de propagação pode destruir a qualidade do sinal e assim limitar a área de cobertura.

15. **Insensibilidade para o efeito de captura**: De um MAC é esperado manter a sensibilidade do receptor para melhorar a transmissão física e evitar qualquer potencial problema proveniente da captura. Embora o efeito de captura possa aumentar o *throughput*, pode também ser proibitivo de justiça no acesso sendo uma solução forçar a insensibilidade do receptor para o mesmo.

16. **Suporte a trafego prioritário**: De um MAC é esperado o suporte a trafego com diferentes prioridades, adicionalmente aos serviços de tempo limitado anteriormente referidos. O acesso com base em mecanismos de prioridade é desejável por várias aplicações, principalmente aquelas que envolvam necessidades de tempo real.

17. **Capacidade de suporte a trafego não reciproco**: Um MAC concebido de modo adequado deve suportar este tipo de trafego. Esta é uma característica especial das redes de comunicação de área local sem fios, onde o trafego do *downlink* (backbone / rede) é, frequentemente, muito maior que o trafego do *uplink*.

18. **Preservação da ordem dos pacotes**: Esta característica MAC é importante, principalmente para os serviços multimédia incluindo voz, áudio e vídeo.

19. **Capacidade para funcionar num sistema de espaço amplo**: Este requisito obriga a que o MAC deva ser robusto à dimensão geográfica e ao número de nós na rede. Esta característica deriva do facto das as redes de comunicação de área local sem fios poderem dar cobertura a várias áreas e servir um amplo conjunto de nós.

20. **Limitar a complexidade física (PHY)**: Atendendo a que a concepção de uma rede de comunicação de área local sem fios é um problema integrado, desde a camada física até à gestão da rede, a concepção de um MAC que induza dificuldades nas outras partes / camadas não é, de modo algum, desejável. Assim, uma preocupação importante e critica é a preservação ao mínimo da complexidade da camada física (*Medium Dependent Layer*, PHY *Convergence Layer* e MAC-PHY interface).

21. **Capacidade para negociar e complexidade**: O passo final para o sucesso de uma rede de comunicação de área local sem fios consiste em proporcionar ao utilizador produtos de alta qualidade e atempadamente. Normalmente isto traduz-se na expressão que a simplicidade é bela.

VI.2. Arquitectura da camada MAC IEEE 802.11

A arquitectura da camada MAC do standard IEEE 80211 é formada por blocos conforme se mostra na figura (Ilustração 34).

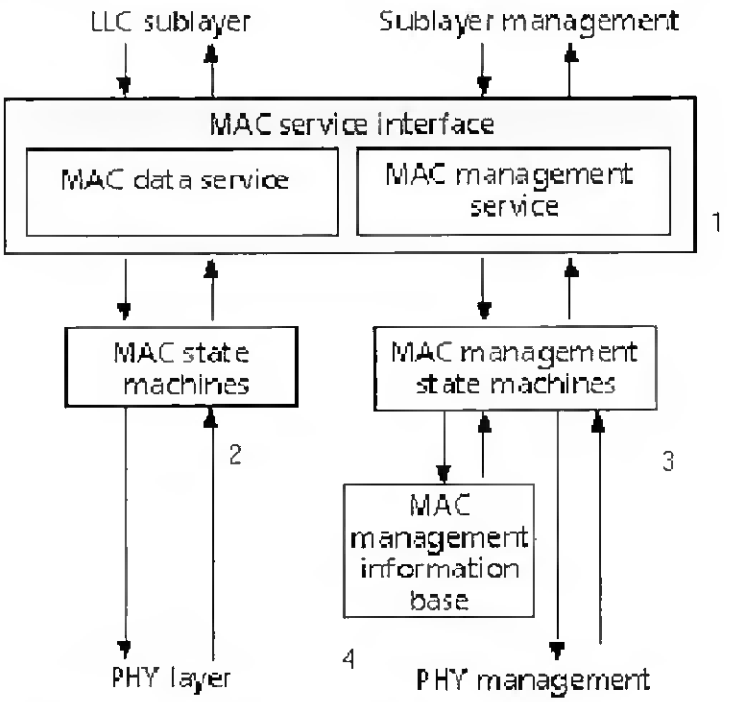


Ilustração 34 - Diagrama de blocos da arquitectura MAC IEEE 802.11 [23]

Os blocos funcionais que actuam num esquema de interligação são:

Bloco 1- MAC-LLC *service interface*

Bloco 2- MAC *state machine*

Bloco 3- MAC *managemente state machine*

Bloco 4- MAC *managemente information base* (MIB)

O bloco 1 aceita os pedidos de serviços provenientes das camadas superiores e distribui-os para um dos seus sub-blocos: MAC *data service* ou MAC *management service*. O bloco 2 fornece a sequência para os vários serviços suportados pelas redes de comunicação de área local sem fios. O bloco 3 fornece a sequência de protocolo para associação e reassociação, acesso ao bloco 4, sincronização, gestão de potência e autenticação. Por ultimo, o bloco 4 disponibiliza armazenamento e acesso a toda a informação de modo a possibilitar uma gestão adequada da camada MAC.

VI.3. Funcionalidades da camada MAC no acesso ao meio

VI.3.1. Funcionamento da camada MAC

Os protocolos de acesso ao meio, especificamente, sistematizam as fases de estabelecimento, controle, gestão de tráfego e encerramento relativas às ligações para troca de informações, desempenhando funções de endereçamento e controle de erros [10]. No âmbito das redes sem fios, torna-se necessário acrescentar funções adicionais ao protocolo MAC, incluindo entre elas fragmentação, controlo de fluxo para gerir o envio de fragmentos de tramas para o meio físico e manipulação de múltiplas taxas de transmissão, o que permite fazer face ás diferentes hipóteses de operar em meios físicos diferentes.

Uma questão importante é a taxa de transmissão que é determinado pela qualidade do serviço do nível físico (Modelo OSI). A sua operacionalidade é especificada ao nível MAC através de um parâmetro associado com as primitivas de serviço da camada física isto é, se chegam muitas tramas corrompidas, selecciona-se bit rate mais baixo, caso contrário aumenta-se o bit rate. Naturalmente que o emissor e receptor deverão trabalhar com o mesmo bit rate usando, também, o mesmo método de modulação, operações supervisionadas pela troca, entre eles, de parâmetros de controlo adicionais presentes nas tramas RTS e CTS (APÊNDICE A). Estas trocas são feitas a menor bit rate, e apenas se o receptor der respostas positivas é o que emissor sobe o bit rate. Normalmente o bit rate operacional, utilizado em diferentes destinos, é guardado numa tabela para evitar a renegociação antes de cada transmissão.

O sucesso das técnicas CSMA no acesso ao meio em redes cabladas levou à proposta da sua aplicação a redes sem fios. No entanto a aplicabilidade de CSMA a redes sem fios é dificultada porque a operação de sentir a portadora (*carrier sense*) ou transmissão continua a ser um problema, principalmente, devido ao problema do terminal oculto [23], [16], [18].

Esta operação é, também, extremamente difícil de ser conseguida de modo fiável ou seguro, devido à existência de uma atenuação severa do canal em ambientes interiores e pela utilização de antenas direccionais. Outra preocupação, relativa ao protocolo CSMA, é a sua instabilidade. Como demostrado por vários trabalhos de pesquisa, os protocolos ALOHA e CSMA não são estáveis [23], [15]. Este problema é fundamentado pela observação das curvas de atraso, onde se pode observar que o mesmo aumenta, de modo brusco, proporcionalmente à carga oferecida.

Outra consideração importante prende-se com factores do domínio espacial (*Spatial Domain Factors*). As redes de comunicação de área local sem fios infraestruturadas têm, como vimos, uma estrutura celular. Nestas redes, cada estação base (ponto de acesso) recebe carga de uma célula e tem que ter sobreposição adequada, relativamente ás células vizinhas, de modo a que seja assegurado serviço continuo aos nós móveis que se movam entre células. Esta topologia pode fazer com que interferências provenientes de outras células (normalmente as células vizinhas) influenciem a operação do protocolo MAC e, deste modo, introduzir efeitos do domínio espacial, conduzindo a degradação de acordo com os vários graus de sobreposição. Estudos efectuados mostram que a possibilidade de que esta situação ocorra não é pequena para um canal com características de atenuação severa e imprevisível, como é o caso dos canais rádio interiores, podendo a probabilidade ser estimada pela concepção do sistema e estatísticas de atenuação. Isto é o que acontece rigorosamente com o protocolo *slotted* ALHOA.

Em termos de comparação, podemos basear-nos estudos efectuados para afirmar que o protocolo CSMA, apesar das suas limitações, é melhor que o protocolo ALOHA [23]. Para simplificar esta análise adoptamos uma estrutura de duas células conforme a figura (Ilustração 35).

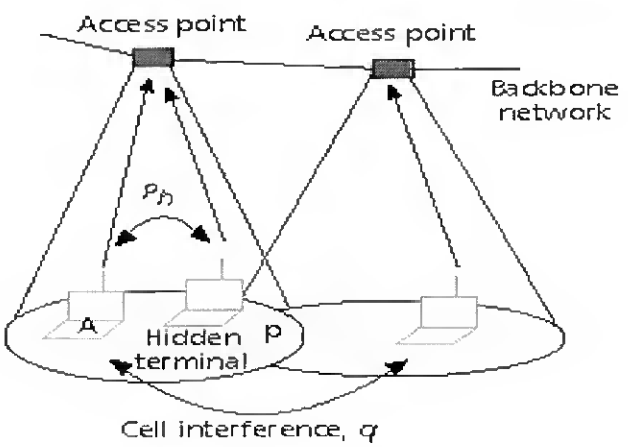


Ilustração 35 - Modelo de interferência de duas células [23]

A primeira situação que vamos a bordar é a *interferência* causada pela sobreposição de células, modelada segundo uma abordagem estocástica, na qual as probabilidades de interferência podem ser calculadas [23], [22]. Assim, assumimos que cada nó móvel tem a probabilidade p de escutar duas estações base (*Access Point*) quando estiver numa região de sobreposição e que cada nó móvel numa dada célula, tem a probabilidade q de sentir a portadora (transmissão) que ocorre noutra célula. Esta situação acontece, na prática, desde que a potência do sinal recebido não seja simplesmente uma função da distância geográfica, especialmente nos canais de atenuação interiores, introduzindo uma outra consideração que se prende com a atenuação e propagação da onda. Assim, nós móveis em células diferentes podem sentir cada uma das outras portadoras.

Abordamos agora o efeito de terminais ocultos. Este é modelado estocásticamente, justificada por melhor representar a mobilidade e dinâmica do canal, pela probabilidade P_h de que um nó se torne um terminal oculto de outro. Os resultados analíticos, baseados no modelo paramétrico anterior, produzem os resultados numéricos da figura (Ilustração 36).

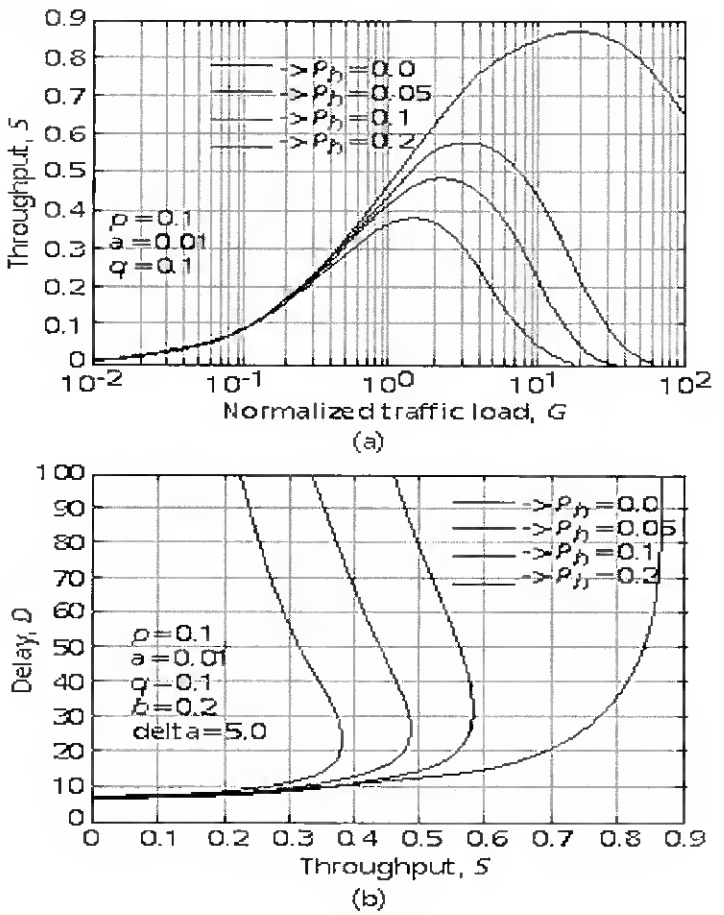


Ilustração 36 - Resultados de CSMA não persistente [23]

Face ao anteriormente exposto, podemos concluir que existe instabilidade, acrescida do facto de que na prática nestas redes a interferência poder provir de diversas células e não apenas de duas. Atendendo a esta instabilidade CSMA pode não ser atractivo para redes sem fios.
Com o intuito de suavizar o problema do terminal oculto e simultaneamente aumentar a confiança por parte dos utilizadores, surgiu uma versão melhorada do protocolo CSMA denominada CSMA/CA (*Carrier Sense Multiple Access with Colission Avoidance*), que apresenta como grande melhoria o facto de que antes de transmitir uma trama a coordenação MAC deve primeiro ganhar o acesso ao meio.

VI.3.2. Função de coordenação de acesso ao meio

Numa rede implementada segundo o protocolo IEEE 802.11, conforme referimos anteriormente, podem coexistir duas funções de coordenação acesso: Distribuída (DCF, *Distribute Coordination Function*) ou Centralizada (PCF, *Point Coordination Function*). A implementação da primeira função, DCF, é obrigatória e utiliza como método de acesso CSMA/CA (*Carrier Sense Multiple Access with Colission Avoidance*), também denominado método de acesso básico do protocolo IEEE 802.11. A implementação da segunda função, PCF, é opcional e, em termos de arquitectura ou topologia, reside sobre DCF. A função de coordenação, CF, utiliza um controlador, função desempenhada normalmente pelo AP associado à BSS. A sua implementação exige, contudo, a não sobreposição de BSSs adjacentes, que estejam a implementar a PCF, no mesmo canal de transmissão, na medida em que o protocolo não tem capacidade para resolver situações de contenção no acesso ao meio quando se verifica esta condição.
A existência de duas funções de coordenação, conforme ilustrado na figura (Ilustração 37), permite o suporte de dois tipos de trafego: síncrono e assíncrono.

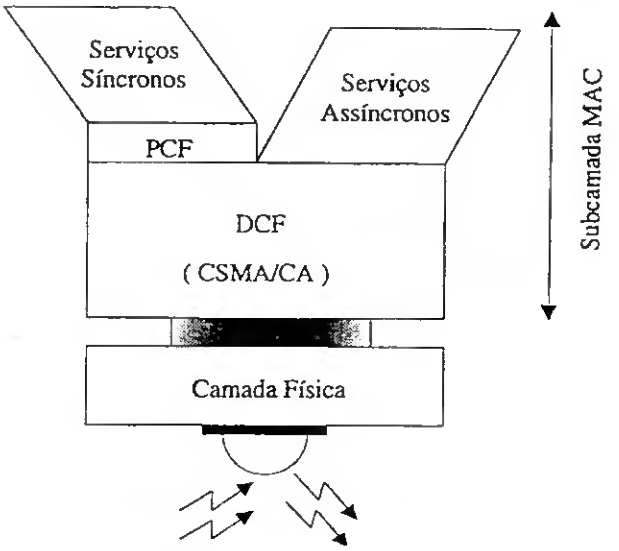


Ilustração 37 - PCF e DCF [32]

Os serviços síncronos e assíncronos são integrados através de uma supertrama, como ilustrado na figura (Ilustração 38).

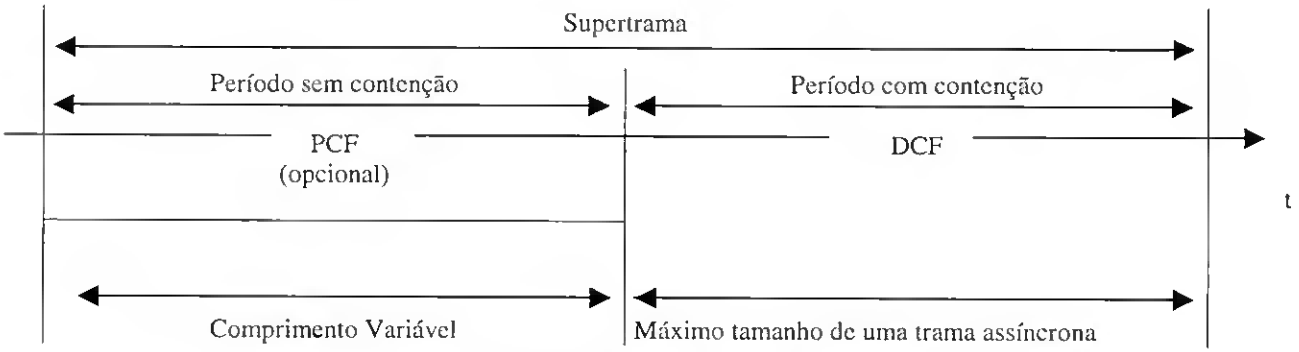


Ilustração 38 - Formato de uma supertrama

Esta supertrama é dividida em dois subintervalos: um no qual não existe contenção no acesso ao meio e onde domina o método de acesso centralizado, e outro no qual o acesso ao meio se faz com contenção e no qual reina o método de acesso básico. Em suma, deverá ser adoptada uma estrutura de supertrama com partes sem contenção e partes com contenção, como exibida na figura (Ilustração 39).

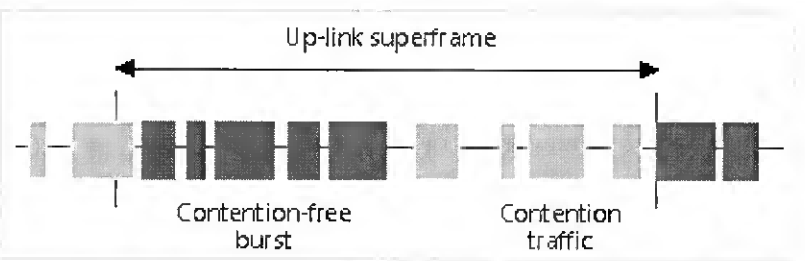


Ilustração 39 Estrutura de supertrama IEEE 802.11 (uplink) [23]

Existe uma referência temporal fixa que marca o início de cada supertrama. Contudo, a mesma poderá não ter início nesse exacto instante se, nessa altura, o meio se encontrar ocupado com alguma transmissão restante do período de contenção da supertrama precedente. Numa situação destas o começo da supertrama será atrasado, iniciando-se logo que o meio fique livre. Como tal, podemos afirmar que a duração das supertramas é variável, assim como a duração dos seu dois subintervalos.

Em suma, por defeito todos as estações compatíveis 802.11 usam DCF, que é um mecanismo de acesso básico pelo sentir da portadora (*carrier sense*) [27]. Opcionalmente podemos inicializar as estações para implementarem, também, o acesso prioritário baseado em PCF. Na maioria dos casos o DCF será suficiente; contudo, é de considerar a activação de PCF se for necessário dar suporte a serviços de transmissão de tempo limitado, tais como áudio e vídeo.

VI.3.2.1. DCF – Função de coordenação de acesso ao meio distribuída

Os mecanismos utilizado pelo método de acesso básico, que se baseia no protocolo CSMA/CA, diferem em relação aos, anteriormente descritos, nos aspectos seguintes: mecanismos de detecção de actividade, mecanismos de procedimento de transação de dados entre duas estações, o mecanismos de recuperação de erros, mecanismos de prioridades e algoritmo de recuo aos quais faremos alusão em seguida.

VI.3.2.1.1. Mecanismo de detecção de actividade

A detecção de actividade é efectuada por meio de dois mecanismos para sentir o meio, um físico e outro virtual, cuja combinação permite à coordenação MAC determinar se o meio esta livre ou ocupado. No protocolo CSMA/CA a detecção de actividade, que é efectuada pela camada física através do sinal CS (*Carrier Sense*), é complementada com um mecanismo de detecção de actividade virtual, conforme figura (Ilustração 40).

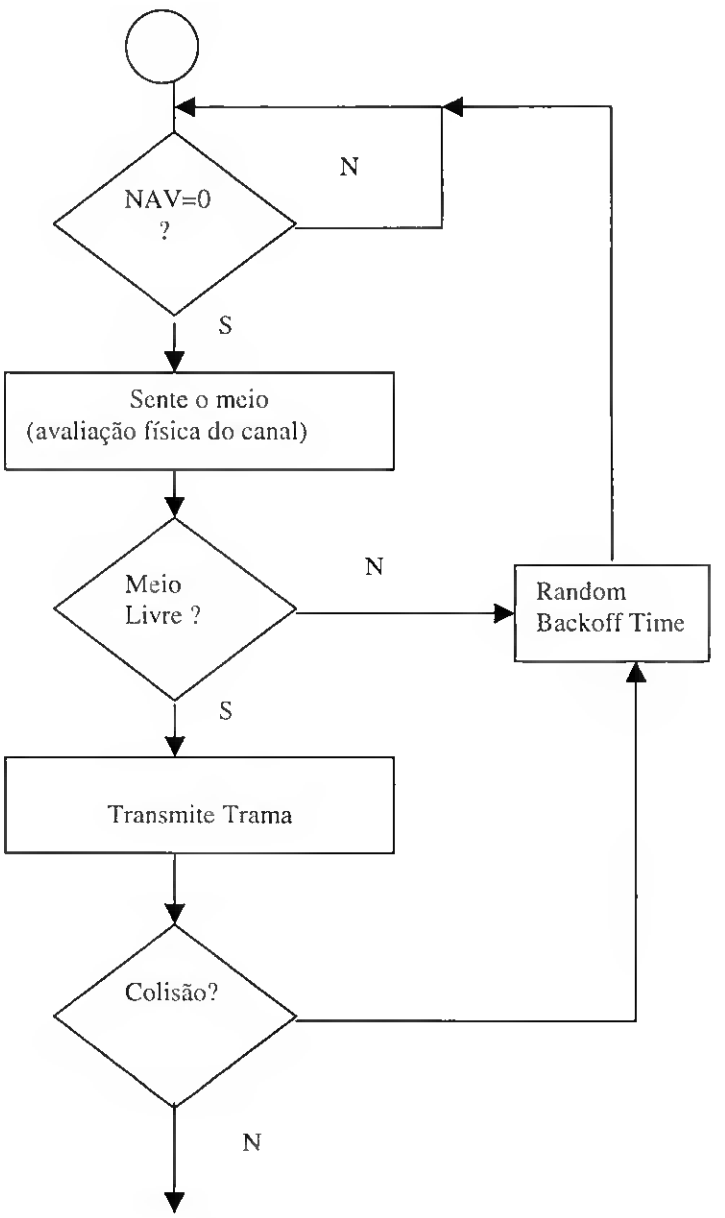


Ilustração 40 - Operação MAC / DCF

Cada uma das camadas físicas fornece um meio físico de sentir o canal, normalmente baseado na detecção de energia. Os resultados desta avaliação do canal são enviados, da coordenação PHY para a coordenação MAC, como parte da informação factorizada sobre a decisão do estado do canal. A coordenação MAC continua o processo com o protocolo de *carrier sense* virtual, com base na informação de reserva encontrada no campo *Duration* de

todas as tramas. Esta informação anuncia, a todas as outras estações, que dada estação irá usar o meio.

Cada estação, por seu lado, mantém uma estrutura denominada NAV (*Network Allocation Vector*) que funciona como um temporizador, indicando em cada momento o tempo restante para completar a uma dada transacção, que é denominado como reserva do canal. A forma como este vector é mantido tem como base a informação de duração, a qual é transportada por tramas especiais trocadas entre a estação emissora e receptora antes da transmissão da trama de dados. Uma forma de o fazer é através do uso de tramas especiais denominadas RTS (*Request To Send*) e CTS (*Clear To Send*), que é opcional e controlada individualmente pelas estações, dependendo do tamanho da trama de dados a transmitir e apenas podem ser usadas para tramas digitais. O NAV opera, como um temporizador, sendo inicializado com um valor igual ao do campo duração da ultima trama transmitida no meio e decrescendo até atingir zero. Após o NAV atingir este valor (NAV=0), a estação pode transmitir se a coordenação PHY indicar um canal livre.

A avaliação física do canal conjuntamente com os conteúdos do NAV fornecem informação suficiente para a camada MAC decidir o estado do canal. Por exemplo, a camada PHY pode determinar que não estão a ter lugar quaisquer transmissões no meio, mas o NAV pode indicar que a transmissão de uma trama prévia, teve um valor no campo *Duration* que impossibilita transmissões durante um período de tempo específico. Neste caso, a camada MAC deve suspender a transmissão de tramas enquanto o período de tempo (*duration*) não expirar.

VI.3.2.1.2. Mecanismo de transacção de dados entre duas estações com reserva do canal

O protocolo que corresponde ao foco de interesse do comité IEEE 80211 pode usar opcionalmente, como anteriormente referido, CSMA/CA com quatro modos de *handshake* conforme figura (Ilustração 41), essencialmente para combater a atenuação inerente aos canais interiores [23].

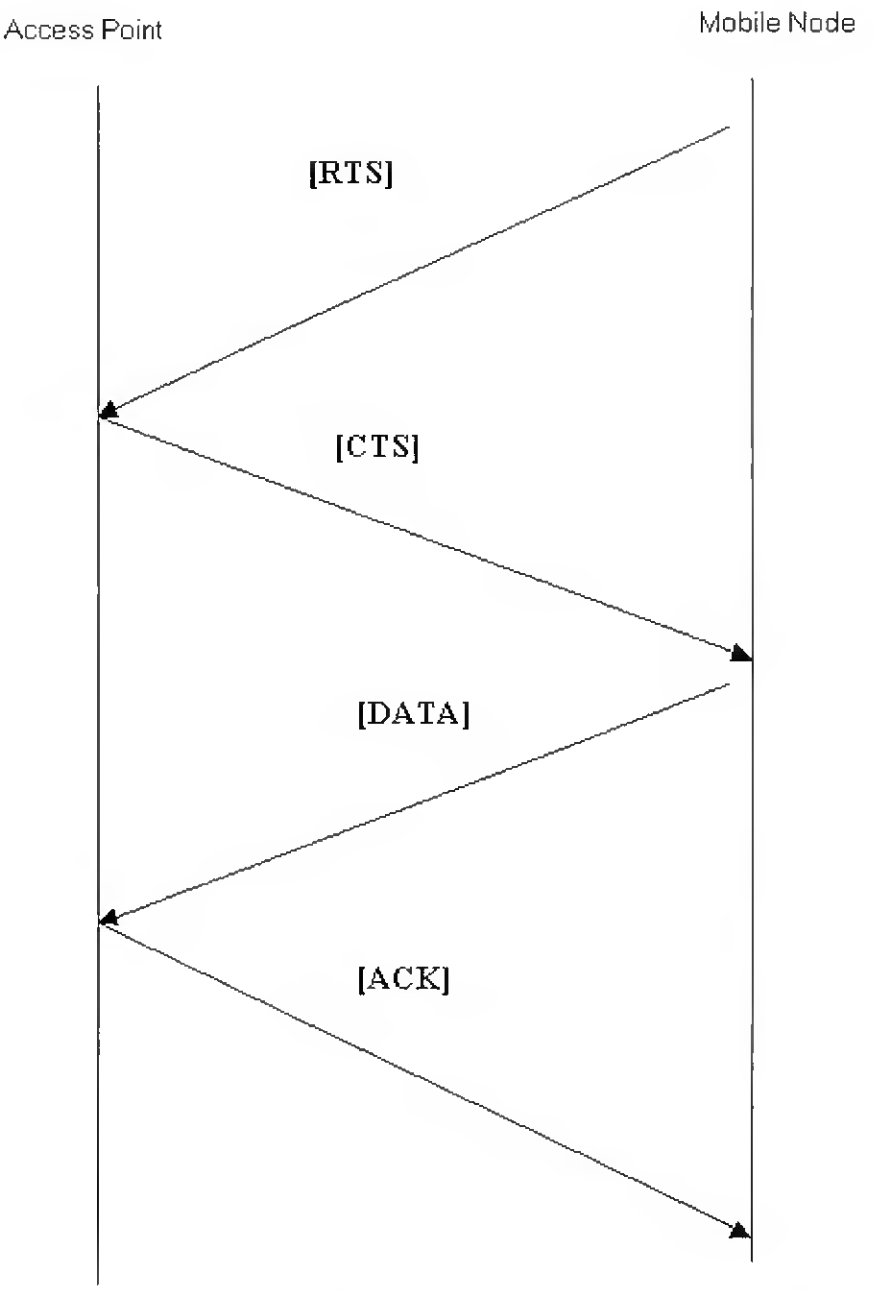


Ilustração 41 CSMA / CA com quatro handshaking

Numa rede infraestruturada, o seu funcionamento é o seguinte, cada utilizador ou estação móvel (*Mobile Node*) ao pretender transmitir envia uma trama RTS (*Request-To-Transmite*) ao ponto de acesso (*Access Point*) usando o protocolo CSMA/CA. Quando o ponto de acesso recebe a trama RTS de um utilizador, elege-o enviando-lhe uma trama CTS (*Clear-To-Send*). Este envia então os seus pacotes de dados (DATA) para o ponto de acesso. Após ter recebido um pacote correctamente, o ponto de acesso envia um reconhecimento positivo (ACK, *Acknowledgement*) ao utilizador. Numa rede Ad Hoc, o processo é idêntico, mas esta troca de tramas é efectuada entre as várias estações que fazem parte da rede.

Podemos sumariar que numa transação de dados que se processe durante o período com contenção, existem basicamente quatro tramas diferentes: RTS, CTS, DATA e ACK. As duas primeiras, conjuntamente, permitem fazer a reserva do canal de transmissão, a trama DATA corresponde aos dados propriamente ditos e a trama ACK é utilizada pela estação receptora para fazer a confirmação positiva da recepção da trama de dados. Ao conjunto das quatro tramas dá-se o nome de MPDU (MAC *Protocol Data Unit*).

A vantagem da troca das tramas RTS e CTS entre duas estações ou entre uma estação e AP, como anteriormente referido, é permitir efectuar uma reserva do meio para que estes possam comunicar minimizando a ocorrência de colisões durante o processo de transmissão da trama de dados. Ambas as tramas, RTS e CTS, contêm a duração de todo o processo do MPDU, com vista a minimizar os efeitos de estação escondida (terminal oculto). Isto traduz-se, conf orme figura (Ilustração 42), no facto de que uma estação mesmo que não escute a trama RTS poderá actualizar o seu NAV se escutar a trama CTS.

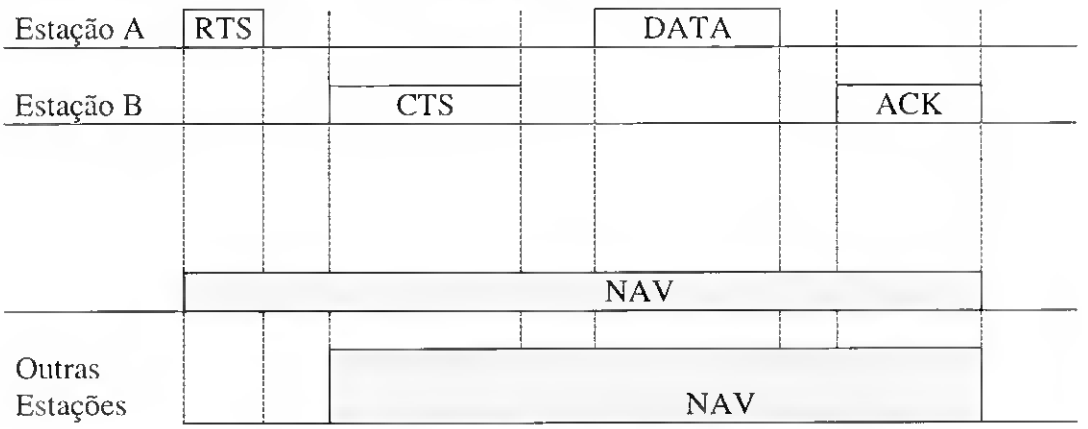


Ilustração 42 - Actualização do NAV

A troca de destas tramas, embora reduzindo a probabilidade de ocorrência de colisão durante a transmissão de tramas de dados, contribui para o aumento do *overhead* na rede. A utilização das tramas RTS e CTS é, por isso, opcional e como tal um MPDU poderá ser simplesmente composto pelas tramas DATA e ACK, ou unicamente pela trama DATA, no caso de transmissões de difusão ou de grupo. Como tal, as estações podem ser configuradas para incluírem, ou não, as tramas RTS e CTS nos MPDUs, decisão que depende de diversos factores entre os quais o número de estações da rede e a probabilidade destas poderem ficar escondidas, a velocidade de transmissão e o volume médio de trafego na rede. Como parâmetro de referência, para este processo de decisão, utiliza-se o tamanho da trama de dados, incluindo-se as tramas RTS e CTS no MPDU sempre que esta tenha uma dimensão superior a um dado valor, que depende dos factores supra referidos.

Baseados no modelo analítico anteriormente usado para CSMA, podemos avaliar a performance do protocolo CSMA/CA com quatro formas de *handshake* [23]. Assumimos que o ciclo de transmissão das tramas [RTS] / [CTS] ocupe um tempo normalizado (para transmissão de pacote), que denominamos por ***b*** e que a eleição (*polling*) é perfeitamente fiável e não consome tempo adicional (*overhead*). Na transmissão da trama [RTS] é adoptado CSMA não persistente, enquanto o tempo aleatório de resposta (*backoff*), para evitar colisões, é negligenciado para alcançar o limite superior em rendimento. Portanto, as colisões de tramas [RTS] são a única perda possível do protocolo.

Atendendo à possibilidade de conectividade parcial da rede, os protocolos para rede de área local sem fios devem ter em conta a existência de potenciais estações ocultas, podendo este efeito ser evitado, como referimos, activando o modo RTS / CTS. Este modo de operação fornece uma melhor performance sobre o acesso básico, quando existir uma possibilidade elevada de existirem estações ocultas. Adicionalmente, a performance degrada-se muito mais lentamente, do que no acesso básico, quando a utilização da rede aumenta. O uso desta técnica contudo, resultará num *throughput* relativamente menor quando a probabilidade de estações ocultas for baixa [27].

Podemos exemplificar o efeito de terminal oculto, numa rede infraestruturada, com a implementação prática ilustrada na figura (Ilustração 43), onde ambas as estações podem comunicar directamente com o AP. Contudo a barreira, que representa a falta de conectividade, impede as estações A e B de comunicarem directamente uma com a outra, causando colisões de acesso quando a estação A tenta aceder ao meio mas a estação B está a transmitir uma trama para o AP. Isto acontece porque a estação A não é capaz de detectar que a estação B já está a transmitir.

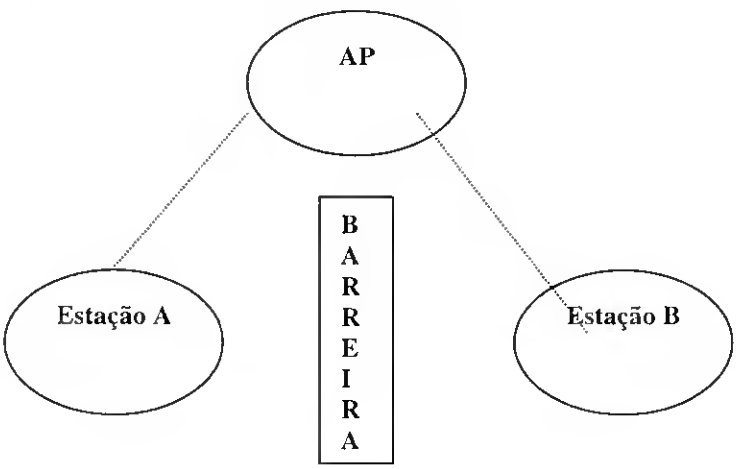


Ilustração 43 - Rede com barreira

Para evitar este tipo de colisões, baseadas na existência de estações ocultas, a estação B pode enviar uma trama RTS para o AP requerendo serviço durante um certo período de tempo. Se o AP autorizar difundirá uma trama CTS, anunciando a ocupação do meio durante este período, a todas as estações que escutem a transmissão da trama. Como resultado todas as estações, incluindo a estação A, não tentarão aceder ao meio durante esse período. Por outro lado a troca de tramas RTS / CTS executa, também, teste de rápida detecção de interferência por colisão e teste ao percurso da transmissão. Estes são executados caso a estação que enviou a trama RTS não receba a correspondente resposta CTS. Esta pode repetir o processo (após observar as outras regras do meio) mais rapidamente do que se uma grande trama de dador for enviada e a sua trama ACK não for detectada.

VI.3.2.1.3. Mecanismo de recuperação de erros

A existência de bits errados que podem quebrar a sequência de tramas, acontece devido à degradação da transmissão (enfraquecimento) que tem como causas, por exemplo, interferências e colisões. Assim, retomando o exemplo da figura (Ilustração 43), a estação A pode enviar uma trama RTS e nunca receber a correspondente CTS, ou a estação A pode enviar uma trama *data* e nunca receber um ACK. Devido a estes problemas a coordenação MAC executa mecanismos de recuperação de erros. As estações que iniciam a troca de tramas têm a responsabilidade de recuperação de erros. Este processo, modo geral, envolve a retransmissão de tramas após um período de tempo, caso não seja ouvida qualquer resposta da parte da estação destino. Este processo, normalmente referido como ARQ (*Automatic Repeat-Request*), tem em conta que erros de bits podem, também, tornar a trama ACK irreconhecível.

A coordenação MAC faz a distinção entre tramas curtas e longas, de modo a controlar o número de retransmissões. Para tramas curtas (tramas cujo comprimento é menor que um atributo MIB[7] – *aRTSThreshold*), as retransmissões prosseguem até que o número de tentativas atinja o valor MIB *aShortRetryLimit*. Para tramas longas, a coordenação da camada MAC retransmite tramas do mesmo modo mas baseado no valor MIB *aLongRetryLimit*. Após exceder o limite de novas tentativas a trama é descartada.

[7] MIB (Management Information Base)
A camada MAC inclui uma base de dados que armazena parâmetros do protocolo MAC, necessários à sua operação.

VI.3.2.1.4. Mecanismo de prioridade no acesso ao meio

A norma IEEE 802.11 define diversos intervalos de espaçamento standard (definidos na MIB), os quais adiam o acesso das estações ao meio e fornecem vários níveis de prioridade. Cada intervalo define o tempo desde o fim do último símbolo, da trama prévia, ao início do primeiro símbolo da próxima trama.

Quando uma estação pretende transmitir, só o poderá fazer após decorrer um intervalo de tempo mínimo, denominado intervalo-entre-tramas (IFS, *InterFrame Space*), durante o qual o meio não registou actividade. Conforme ilustrado na figura (Ilustração 44), prevêem-se quatro valores para o referido intervalo: SIFS (*Short Interframe Space*), PIFS (*Point coordination function IntreFrame Space*), DIFS (*Distributed InterFrame Space*) e EIFS (Extended IFS). Estes valores permitem atribuir prioridades no acesso ao meio, dado que uma estação que use um intervalo entre tramas menor terá prioridade em relação a outra que utilize um valor superior.

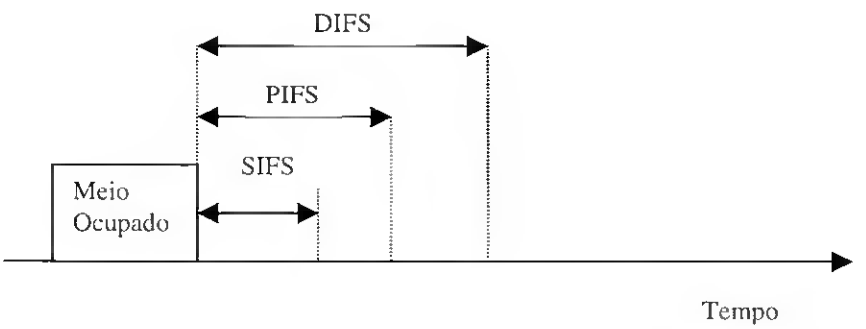


Ilustração 44 - Intervalos IFS

Podem, então, ser definidos quatro tipos de intervalos (prioridades) distintos:

1) **SIFS (Short IFS)**: é o menor valor que o intervalo entre tramas pode tomar e é utilizado em respostas imediatas. Fornece o nível de prioridade mais elevado ao permitir que certas tramas acedam ao meio antes de outras. As tramas que usam este intervalos são: CTS, ACK e o segundo ou subsequente MSDU numa rajada de fragmentos, as quais requerem acesso vantajoso ao meio de modo a minimizar a retransmissão. É também utilizado, como veremos na secção apropriada, na função de coordenação de acesso ao meio centralizada (PCF);

2) **PIFS (PCF IFS)**: é utilizado pelo ponto de acesso, AP, também durante o período da supertrama reservado para acesso ao meio sem contenção (PCF). Este é, de igual modo, o intervalo que as estações, operando no modo PCF, usam para ganhar acesso ao meio, fornecendo-lhes prioridade sob as tramas enviadas no modo DCF. Estas estações podem

transmitir, tráfego sem contenção, se sentirem que o meio está livre. Este intervalo dota uma estação, baseada em PCF, de uma prioridade de acesso mais alta que as estações baseadas em DCF para a transmissão de tramas;

3) **DIFS (DCF IFS)**: é o maior valor que o intervalo entre tramas pode tomar e é utilizado pelo método de acesso básico para transmitir tramas, de modo assíncrono, no período da supertrama reservado a tráfego sem contenção. Por outras palavras, todas as estações que operem no modo DCF usam o intervalo DIFS para transmitir tramas de dados e tramas de gestão. Este espaço torna a transmissão destas tramas de prioridade mais baixa do que as transmissões baseadas em PCF;

4) **EIFS (Extended IFS)**: todas as estações baseadas em DCF usam estes intervalos, as quais vão além do tempo do intervalo DIFS, como um período de espera. Esta situação ocorre quando a transmissão de uma trama resultar na sua má recepção devido a um valor incorrecto de FCS. Este intervalo irá fornecer tempo suficiente para a estação receptora enviar uma trama ACK.

VI.3.2.1.5. Algoritmo de recuo (*Backoff Algoritm*)

A tentativa de transmissão de uma trama de dados, por parte de uma estação, pode não ter sucesso caso o meio se encontre ocupado no momento em que esta pretende iniciar a transmissão ou caso ocorra uma colisão durante a transação do MPDU. Em ambas as situações são necessárias transmissões posteriores, as quais são resolvidas executando, previamente, um algoritmo denominado de recuo.

O período de tempo imediatamente a seguir a um meio ocupado será aquele onde existe maior probabilidade de que ocorram colisões, especialmente em cenários de grande utilização. A razão para que tal aconteça, é que muitas estações podem estar à espera que o meio fique livre e tentam transmitir ao mesmo tempo. Assim, quando o meio ficar livre um tempo de espera (*random backoff time*) adia a transmissão de uma trama, minimizando a hipótese de colisão. Este processo funciona de modo que, conforme ilustrado na figura (Ilustração 45), a estação atrasa a transmissão sempre que ao iniciar uma transação o meio se encontre ocupado.

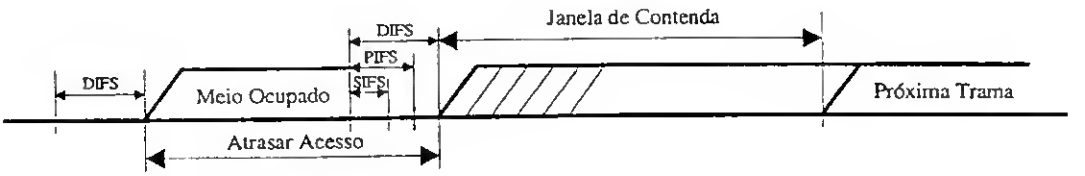


Ilustração 45 – Acesso Básico [32]

Quando o meio fica livre, a estação executa o algoritmo de recuo e disputa o canal de transmissão durante um intervalo de tempo denominado janela de contenção. As estações consideram que ocorreu uma colisão quando não recebem resposta à sua trama ou recebem mas com erros. Neste caso, a estação emissora executa sempre o algoritmo de recuo antes de tentar nova transmissão.

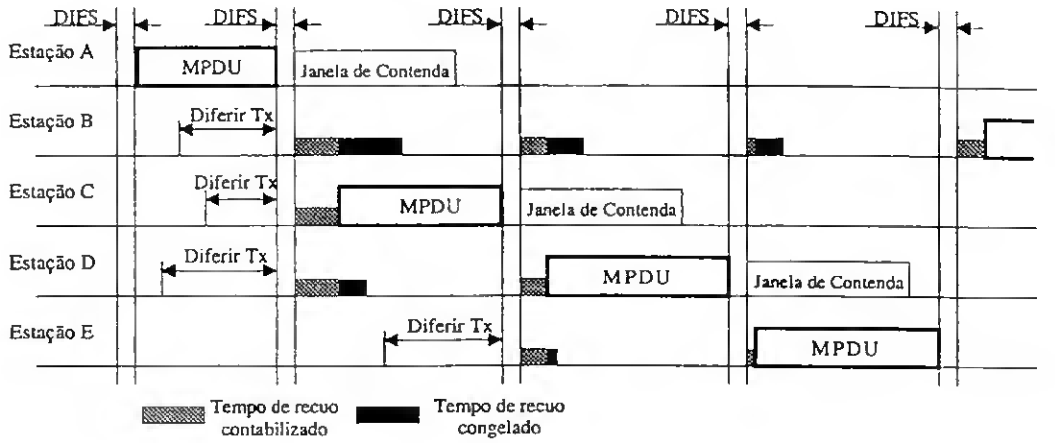


Ilustração 46 - Algoritmo de recuo [32]

A figura (Ilustração 46), ilustra a execução do algoritmo de recuo, que consiste basicamente no seguinte: a estação gera um valor aleatório, o qual corresponderá ao intervalo de tempo que esta terá que esperar antes de aceder ao meio. Este tempo é dado pela expressão:

Backoff_Time= INT (CW * Random ( )) * Slot_Time

onde, CW corresponde à duração da janela de contenção, Random () é uma função que gera aleatoriamente um valor entre 0 e 1 e Slot_Time corresponde à duração de um slot, dependente da camada física. A duração de um slot corresponde ao somatório dos tempos relativos ao tempo de reacção do emissor, ao atraso de propagação no canal de transmissão e ao tempo de detecção de meio ocupado.

Na execução do algoritmo de recuo, quando o meio fica livre a estação inicia a contagem do tempo de recuo, o qual só é contabilizado enquanto o meio se mantiver livre. Esta contagem irá terminar quando o tempo de recuo se esgotar e a estação poder tentar, novamente, aceder ao meio. Contudo, se o meio for ocupado antes de finalizada a contagem do tempo de recuo,

o relógio que o contabiliza é imediatamente e temporariamente desactivado. A sua reactivação ocorrerá, apenas, quando o meio ficar novamente livre, por um período superior a DIFS. O tempo de recuo restante diminui à medida que o processo evolui. Em termos práticos tal significa que as estações que estão a executar o algoritmo há mais tempo terão maior probabilidade de aceder ao meio do que as que estejam à menos tempo. Este processo termina quando se esgote o tempo de recuo e a estação possa tentar novamente aceder ao meio.

Se ao aceder ao meio este estiver ocupado, a estação contabiliza uma tentativa de transmissão falhada. Se ainda não tiver esgotado o número máximo de tentativas a estação inicia uma nova retransmissão executando previamente o algoritmo de recuo. Caso contrário, a transmissão da trama é abortada.

O algoritmo de recuo é ainda utilizado, após a transmissão com sucesso de um MPDU, com o objectivo de garantir a equidade no acesso ao meio. Se a utilização da rede for baixa, as estações não serão forçadas a esperar muito antes de transmitirem as suas tramas. Na primeira ou segunda tentativa, a estação efectuará uma transmissão de sucesso num curto espaço de tempo. Se, pelo contrário, a utilização da rede for alta, o protocolo restringe estações durante períodos de tempo mais longos para evitar a possibilidade de múltiplas estações a transmitir em simultâneo. Por outro lado, sob as mesmas condições, o valor de CW aumenta para valores relativamente altos após transmissões sucessivas. Assim, fornece espaço de transmissão considerável entre estações que necessitem de transmitir.

Podemos concluir, que este mecanismo tem uma boa prestação como técnica para evitar de colisões, contudo, estações ou redes de elevada utilização poderão experimentar atrasos substanciais enquanto aguardam para transmitir as suas tramas [27].

VI.3.2.2. PCF – Função de coordenação de acesso ao meio centralizado

O protocolo IEEE 802.11, com referimos anteriormente, suporta opcionalmente um método de acesso centralizado (PCF, *Point Coordination Function*), o qual se baseia no método de acesso distribuído, anteriormente descrito, com recurso a um esquema de prioridades. A prioridade opcional, baseada em PCF, fornece transferência de tramas sem contenção (*contention free*) que pode ser utilizada tanto em trafego síncrono como assíncrono.

A função PCF é o método de acesso que impera durante o período de supertrama destinado a tráfego sem contenção. A implementação desta função obriga à existência de um controlador (PC, *Point Coordinator*) localizado no ponto de acesso, AP, para gerir e coordenar o acesso

ao meio e controlar a transmissão de tramas das estações, daí que apenas possa ser usado em redes infraestruturadas. Todas as estações obedecem ao PC, definindo o seu valor NAV no início de cada período sem contenção, mas podem, de qualquer modo, como opção responder a uma votação sem contenção (CF-Poll frame).

No início do período sem contenção, o PC tem a oportunidade de ganhar o controle do meio. Este segue o intervalo PIFS como a base para aceder ao meio podendo, por isso, ser capaz de manter o seu controlo durante o período sem contenção e tendo que esperar pouco tempo entre transmissões de estações que operem no modo DCF. Em termos práticos este método de acesso é implementado tendo em conta que o período sem contenção é de duração variável e o PC (AP) sente o meio no início de cada um. Se o meio estiver livre, após o intervalo PIFS, o PC (AP) inicia a transmissão com uma trama denominada *BEACON* (sinalização), a qual inclui o elemento CF *Parameter Set*. Quando as estações recebem este sinal, actualizam o seu NAV com o valor CPF *MaxDuration* que faz parte do elemento anterior. Este valor comunica a duração do período sem contenção a todas as estações, impedindo-as de terem o controle do meio até ao seu terminus.

Após enviar uma trama *Beacon*, o PC (AP) transmite uma das seguintes tramas, depois de ter esperado pelo menos um intervalo SIFS:

Trama de dados: o PC envia esta trama para uma dada estação em particular. Se não receber a correspondente trama ACK do receptor, o PC pode retransmitir a trama não reconhecida durante o período sem contenção, após o intervalo PIFS. Um PC pode enviar tramas individuais, *broadcast* e *multicast* para todas as estações, incluindo as que estão no modo de consumo reduzido;

Trama CF Poll: o PC envia esta trama para uma estação, em particular, concedendo-lhe permissão para transmitir uma única trama para qualquer destino. Caso esta não tenha tramas para enviar deverá responder com uma trama NULL. Se a estação emissora não receber qualquer uma das tramas ACK, como resposta a uma transmissão, não pode retransmitir a trama, a não ser que o PC a elega novamente. Se, por outro lado, a estação receptora da transmissão sem contenção, não for CF (*Contention Free*) elegível, reconhecerá a recepção da trama usando regras DCF;

Trama Data+CF Poll: pelo seu uso o PC envia uma trama de dados para uma estação e simultaneamente elege, essa mesma estação para enviar uma trama sem contenção. Isto é uma técnica que reduz a sobrecarga na rede;

Trama CF End: Esta trama é enviada para assinalar o fim do período sem contenção, o qual ocorrerá quando se verificar qualquer uma das seguintes situações: quando expirar o tempo

CPF *DurRemaining*; quando o PC não tiver tramas para transmitir nem estações para eleger. Este período, sem contenção, é terminando com a transmissão, também pelo AP, de uma trama denominada END. Ester processo é ilustrado na figura (Ilustração 47).

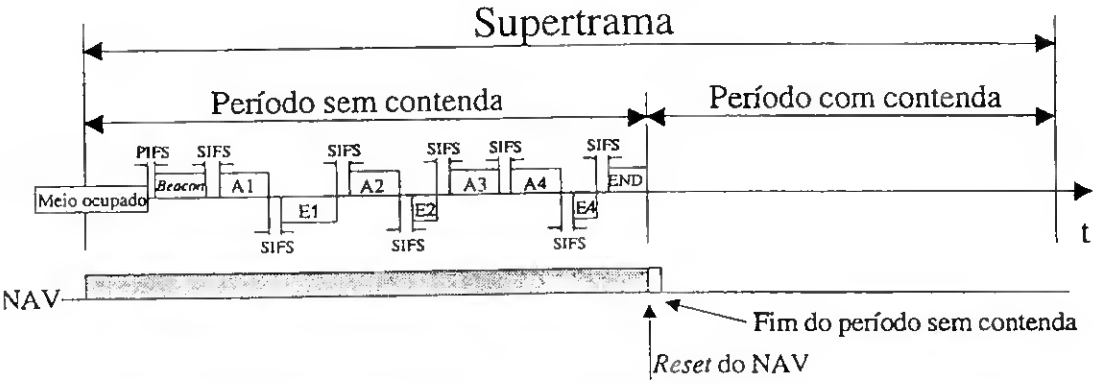


Ilustração 47 - Método PCF [32]

Neste processo, PCF, são de relevância especial, em primeiro lugar a trama BEACON que contém um campo com a duração do período sem contenção e destina-se a sinalizar todas as estações da rede, para que estas possam actualizar o seu NAV e a trama END que se destina a sinalizar as estações, que aguardam pelo período de contenção, para que estas possam iniciar a disputa do meio. Assim, no início de uma supertrama se o meio estiver livre o AP fica com o seu controle durante o período de tempo reservado ao acesso sem contenção. Durante este período de tempo as estações estão impedidas de iniciar transações, transmitindo apenas com a permissão do AP. Se, pelo contrário, o meio estiver ocupado no início da supertrama o AP é obrigado a atrasar a aquisição do controlo do meio, adquirindo-o, com prioridade PIFS, logo que detecte que este ficou livre.

Podemos afirmar que o método de acesso centralizado (PCF) se baseia num esquema de interrogação, onde o AP mantém uma lista, denominada lista de interrogação, com a identificação das estações. Durante o período sem contenção o AP vai interrogar todas as estações dessa lista. Se o intervalo sem contenção da supertrama não tiver duração suficiente que permita interrogar todas as estações. O AP retomará este processo na supertrama seguinte exactamente no ponto da lista onde tinha ficado. Este processo é implementado por meio de um mecanismo em que todas as tramas oriundas do AP contêm, no seu cabeçalho, um *bit* denominado *poll* (interrogação), através do qual se faz a interrogação das estações para que estas enviem dados caso os tenham para transmitir. As estações reagirão à interrogação imediatamente, com prioridade SIFS, caso tenham uma trama de dados a aguardar transmissão ou se pretenderem confirmar a recepção da trama anterior. Se, por qualquer motivo, uma estação não reagir em tempo devido à interrogação, ou seja após um

intervalo SIFS, o AP retomará o controle do meio e interrogará a próxima estação na fila de espera. Desta forma o AP garante o controlo permanente do acesso ao meio. De modo idêntico, recorrendo ao bit *poll*, anteriormente referido, o AP pode simultaneamente interrogar uma estação e transmitir uma trama de dados (DATA+CF_POLL) ou mesmo interrogar, transmitir e confirmar a recepção de uma trama anterior (DATA+CF_POLL+CF_ACK).

As estações possuem uma opção para ser elegíveis. Assim uma estação pode indicar o seu desejo para *polling* usando o sub-campo CF-Pollable, dentro do campo Capability Information, de uma trama Association Request. O PC manterá, como já se disse, uma lista de *pooling*, das estações elegíveis, que podem ser escolhidas durante o período sem contenção.

No método de acesso centralizado a confirmação positiva de uma trama (CF_ACK) pode também ser feita através de um *bit* (APF, *Ack_Previous_Frame*) presente em todas as tramas, no respectivo cabeçalho. Este bit é utilizado, tanto pelas estações como pelo AP, para confirmar a recepção duma trama precedente. Conforme ilustrado na figura (Ilustração 47), no caso da trama A1, transmitida pelo AP, requerer confirmação de recepção esta é efectuada colocando o bit APF a um na trama seguinte transmitida pela estação, neste caso particular na trama de dados E1 (DATA +CF_ACK).

O período destinado a trafego sem contenção pode terminar, pelas razões anteriormente descritas e antes do fim da janela de tempo prevista para este tipo de trafego, caso o AP determine que tal seja necessário com base no trafego disponível e na lista de interrogação. O AP transmitirá, então, uma trama END que terá como objectivo sinalizar o fim desse período e, eventualmente, confirmar a recepção da ultima trama recebida (END + CF_ACK). A recepção desta trama pelas estações, conforme ilustrado na figura (Ilustração 47), fará com que elas realizem o *reset* do seu NAV. Esta operação é plenamente justificada e de extrema importância de modo a garantir que todas as estações possam aceder aleatoriamente ao meio imediatamente após o fim do período reservado a trafego sem contenção em curso.

A titulo final é de referir que o modo PCF não opera rotineiramente usando o período de *backoff* do modo DCF por isso, existirá risco de colisões quando PCs sobrepostos estiverem presentes no mesmo canal físico. Isto poderá tornar-se uma realidade quando múltiplos APs formam uma rede infraestruturada. De modo a minimizar estas colisões, o PC usa um período de *backoff* aleatório (*random backoff time*), caso encontre um meio ocupado quando espera para transmitir a trama *BEACON* inicial.

VI.4. Função de Fragmentação e Reconstrução

Os serviços MAC fornecem fragmentação e consequente desfragmentação. A função de fragmentação consiste na divisão do MSDU (MAC *Service Data Unit*), entregue à camada MAC, em fragmentos de tamanho inferior destinados a transmissão. Esta tem como objectivo aumentar a probabilidade de sucesso da transmissão do MPDU, devido ao pequeno tamanho das tramas, face ás interferências externas existentes no canal de transmissão. Como anteriormente referido, estas podem ter as mais variadas origens.

Nas redes sem fios a fragmentação é uma função necessária porque terão que ser usadas tramas pequenas, devido ao alto BER existente nas comunicações por rádio e infravermelhos (valores típicos da ordem 10^{-3} a 10^{-5}), enquanto nas suas congéneres cabladas podem utilizar-se tramas grande face ao baixíssimo BER existente (valores típicos da ordem de 10^{-9} a 10^{-11}).

As tramas fragmentadas da camada MAC (*unicast*) têm, apenas, um único endereço receptor, nunca sendo fragmentadas tramas de *broadcast* ou *multicast* porque tal resultaria numa sobrecarga excessiva para a rede [27]. Se o tamanho do MSDU, que necessite de ser transmitido exceder o parâmetro *aFragmentationThreshold*, localizado na MIB (MAC Managment Information Base), o protocolo MAC fragmentará o MSDU. Após divisão do MSDU em fragmentos, se o meio estiver livre, a estação emissora inicia a transmissão dos mesmos, que devem ser transmitidos em rajada com prioridade SIFS. A estação receptora deverá fazer a confirmação positiva imediata de cada fragmento, conforme ilustrado na figura (Ilustração 48). No caso da estação emissora não receber a trama ACK correspondente a um dado fragmento executará o algoritmo de recuo, após o qual inicia a transmissão a partir do primeiro fragmento não confirmado.

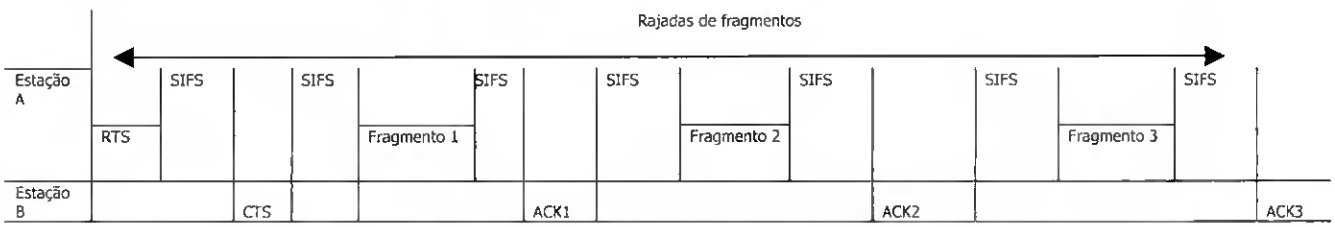


Ilustração 48 - Rajadas de fragmentos

Cada fragmento e respectivo ACK contêm um campo com a duração da transação do próximo fragmento. Esta informação permite às estações fazer reserva do canal para a transmissão do fragmento seguinte e tem como objectivo minimizar as interferências provocadas por estações escondidas. O canal de transmissão pode também ser reservado para a transação do primeiro fragmento através da troca de tramas RTS e CTS. Por outro lado, o cabeçalho de cada fragmento, para além do tipo de trama e endereços de origem e destino,

contém informação que permite a sua reconstrução pela estação receptora, como é o caso do campo de controle de sequência e um campo indicador do último fragmento. O campo de controle de sequência contém o número da sequência e o número do fragmento, permitindo à estação receptora reagrupar e ordenar os fragmentos correspondentes ao mesmo MSDU. O campo indicador é colocado no último fragmento, sinalizando a estação receptora que a transmissão do MSDU está concluída. Na reconstrução a estação receptora poderá assim eliminar qualquer fragmento duplicado, baseada no número de fragmento.

No caso de estações que implementem WEP, após ter lugar a desencriptação, a estação destino combinará todos os fragmentos com o mesmo número de sequência, na ordem correcta, de modo a reconstruir o correspondente MSDU.

Em redes de elevada utilização e caso exista significativa interferência ou colisões, deverá tentar definir-se o tamanho do fragmento, de modo a envia-los menores. Tal opção, permitirá a retransmissão de pequenas tramas com muito maior rapidez. Por outro lado, é mais eficiente definir um tamanho de fragmento grande se a interferência for pequena, ou nenhuma, porque alivia a sobrecarga criada pela transmissão de múltiplas tramas. O valor para o tamanho de fragmento deve ser definido entre 256 e 2048 bytes [27].

VI.5. Funções de Gestão em Redes IEEE 802.11

VI.5.1. Sincronismo temporal

As estações da rede devem estar sincronizadas porque só assim é possível a implementação de algumas funções da camada MAC, como o suporte de serviços síncronos ou de mecanismo de conservação de potência.

O mecanismo de sincronismo proposto pela norma IEEE 802.11 consiste em manter as estações pertencentes à mesma BSS sincronizadas segundo um relógio comum. Esta técnica de sincronização temporal é denominado TSF (*Timing Synchronisation Function*) e a sua implementação difere entre redes Ad-Hoc e redes infraestruturadas, conforme descrito posteriormente. É, no entanto, comum ás duas implementações o uso de tramas de controle denominadas BEACON. Estas tramas são utilizadas para manter sincronizadas as estações da BSS e também na implementação de mecanismos de conservação de potência, para além de conterem informação sobre a camada física que está a ser usada.

Os campos utilizados, exclusivamente, para manter o sincronismo são, o campo *Time_Stamp* e o campo *Beacon_Interval*. O campo *Time_Stamp* corresponde ao valor do relógio quando o

primeiro *bit* é transmitido para a camada física. O campo *Beacon_Interval* representa a periodicidade relativa de transmissão de tramas BEACONS. Em cada *Beacon_Interval* é sempre transmitida uma trama BEACON, embora a sua transmissão possa ser atrasada porque o meio se encontra ocupado.

VI.5.1.1. Sincronismo em redes Ad-Hoc

Numa rede Ad-Hoc a técnica TSF (*Timing Synchronisation Function*) é executada por meio de um algoritmo distribuído, assim todas as estações da BSS participam na transmissão de tramas BEACONS. Quando transmite uma trama BEACON, a estação preenche o campo *Time_Stamp* com o valor do seu relógio local. Quando recebe uma trama BEACON, a estação actualiza o seu relógio com o valor do *Time_*Stamp, se este for superior ao valor do seu relógio. A estação, antes de actualizar o seu próprio relógio, compensa o valor do *Time_Stamp*, tendo em consideração o atraso com que este é recebido, adicionando-lhe um valor fixo definido pela norma. Os relógios de todas as estações sincronizadas na BSS convergirão para o mesmo valor após um período de tempo.

Em cada Beacon_Interval apenas uma estação da BSS transmite uma trama BEACON, sendo isso garantido do seguinte modo. Para evitar que em cada Beacon_Interval várias estações transmitam tramas BEACONS simultaneamente, todas as estações da BSS esperam um período de tempo de duração aleatória (RD, *Random Delay*). Após esse período transmitem uma trama BEACON se e só se, entretanto, não receberem nenhuma proveniente doutra estação.

VI.5.1.2. Sincronismo em redes Infraestruturadas

Numa rede infraestruturada a execução da função TSF (*Timing Synchronisation Function*) é centralizada no AP. Assim, é da sua responsabilidade a transmissão periódica de tramas BEACONS com o seu valor de relógio. Todas as estações que pertencem à BSS, servida pelo AP, actualizam os seus relógios de acordo com o Time_Stamp contido nas BEACONS, isto é, com o valor do relógio do AP. O AP transmite a trama BEACON no início de cada Beacon_Interval, excepto quando o meio está ocupado. Nesta situação a trama é transmitida logo que o meio fique livre.

VI.5.1.3. Aquisição de sincronismo

A aquisição de sincronismo pode ser realizada por pesquisa passiva (*Passive Scanning*) ou por pesquisa activa (*Active Scanning*). O algoritmo de aquisição de sincronismo por pesquisa passiva consiste, simplesmente, na escuta de tramas BEACONS durante dado intervalo de tempo. Este procedimento permite à estação conhecer a identificação da BSS e o valor do relógio comum a todas as estações a ela sincronizadas. Este método só é prático se a periodicidade das tramas em causa for pequena e, caso a camada física suporte vários canais de transmissão simultâneos, se o seu número for pequeno.

O algoritmo de aquisição de sincronismo por pesquisa activa é um mecanismo que permite a uma estação a obtenção da informação que necessita de forma mais rápida que o anterior. Este procedimento consiste na transmissão, pela estação, de uma trama denominada PROBE. Esta trama sinaliza as restantes estações da rede solicitando-lhes informação de sincronismo. A responsabilidade de dar resposta a tramas PROBES é atribuída, numa rede Ad-Hoc, à estação que transmitiu a última trama BEACON e, numa rede infraestruturada, ao AP. As tramas de resposta a tramas PROBES contêm identificação da BSS (BSS-Id) e o valor do seu relógio.

Numa rede infraestruturada pode, conforme anteriormente referido, existir sobreposição de BSAs adjacentes, o que quer dizer que uma estação localizada numa dessas zonas poderá escutar mais do que um AP. Essa estação, eventualmente, obterá mais que uma resposta à sua trama PROBE. Face a uma situação destas a estação deverá sincronizar-se com o melhor AP, tendo, para tal, em consideração a qualidade das respostas obtidas. Por outro lado, pode acontecer que uma dada estação ao pretender sincronizar-se, não detecte nenhuma rede com o qual o possa fazer. Neste caso, a estação deverá tomar a iniciativa de inicializar uma rede Ad Hoc. Este processo consiste em estabelecer a referência inicial, em termos temporais, da rede e a partir desse momento a estação passa a constituir uma rede transmitindo periodicamente as suas tramas BEACONS.

VI.5.2. Associação e Reassociação (Junção à Rede)

Após uma estação ser activada é necessário determinar, em primeiro lugar, se outra estação ou AP está presente para junção, antes do processo de autenticação e associação com um deles. A estação efectua esta fase de descoberta operando num modo de busca (*scanning*), que poderá ser activo ou passivo, tal como o utilizado na aquisição de sincronismo. Após

juntar-se a uma BSS ou ESS, a estação receberá do AP os seguintes parâmetros: SSID (*Service Set Identifier*), TSF (*Timing Synchronization Function*), valor de relógio (*timer value*) e parâmetros de inicialização da camada física (PHY).

Se este processo for passivo, a estação escuta cada canal durante um período de tempo específico, definido no parâmetro *ChannelTime*, e apenas espera transmissões de tramas *Beacon*, detentoras do SSID, provenientes das estações que desejem juntar-se a ela. Após a estação detectar este sinal, poderá negociar uma conexão avançando com os processos de autenticação e associação. Por outro lado, se o processo for activo, envolve a transmissão, pela estação, de tramas *Probe* indicando o SSID da rede à qual esta se deseja juntar. A estação que envia esta sonda aguardará por uma trama *Probe Response* que assinala a presença da rede desejada. Uma estação pode, também, enviar tramas *Probe* usando transmissão por difusão de SSIDs que fará com que todas as redes na área respondam.

No caso de redes infraestruturadas um AP responderá a todos os pedidos de sonda que escutar e as funções de associação e reassociação irão permitir associar-lhe uma dada estação. Para tal, as estações transmitem uma trama denominada *ASSOCIATION REQUEST* dirigida ao AP. Este, por seu lado, responde com uma trama *ASSOCIATION RESPONSE*, a qual contém o endereço atribuído à estação. A estação deverá fazer a confirmação positiva, imediata, transmitindo uma trama ACK. A partir do momento em que o AP recebe o ACK com sucesso a estação considera-se associada à BSS. Quando as estações não recebem resposta ao seu pedido de *ASSOCIATION REQUEST* ou a recebem sem sucesso devem pesquisar outro AP para se associar.

Nas redes ad-hoc a estação que gerou a última trama *Beacon* responderá a todos os pedidos. A trama *Probe Response* indica a presença das redes desejadas, e a estação pode completar o seu processo de conexão iniciando os processos de autenticação e associação.

O procedimento de reassociação processa-se de igual modo, fazendo uso das tramas RE*ASSOCIATION REQUEST* e RE*ASSOCIATION RESPONSE.*

Em termos práticos, alguns fabricantes permitem ao utilizador instalar cada placa rádio de modo a associá-la com um AP da sua preferência, mesmo que o seu sinal, em particular, seja inferior ao de outros APs [27]. Este cenário, pode ser útil se existir a necessidade de regular o fluxo de trafego através de um AP, em particular. Na maioria dos casos, contudo, a estação reassocia-se a outro AP, se não receber sinais do AP preferido.

VI.5.3. Gestão do consumo de potência

Como referimos anteriormente o consumo de potência é, por inúmeras razões, um factor de extrema importância no projecto de qualquer rede sem fios. As estações deverão ter, quanto possível, um consumo reduzido para que a sua autonomia seja a máxima.

Uma estação consome potência tanto ao transmitir como ao receber. Na transmissão apenas existe consumo de potência quando o emissor está activo, ou seja a emitir, o que significa que não é possível o uso de qualquer mecanismo para reduzir o consumo total de potência da estação. Tal facto, contudo, não se verifica na recepção, onde caso não se implemente qualquer mecanismo de conservação de potência a estação consome-a mesmo quando não está efectivamente a receber. Ao ser implementado, este deverá activar o receptor apenas quando é estritamente necessário permitindo reduzir o consumo total das estações, sem contudo deixar de garantir que as tramas a elas destinadas lhes sejam entregues.

Uma estação poderá estar num de três estados, conforme figura (Ilustração 49), a transmitir, quando o emissor está activo (Tx_Activ); acordada, quando o receptor esta activo (Rx_Activ) e adormecida, quando está a operar num modo de conservação de potência (Tx_Rx_Off).

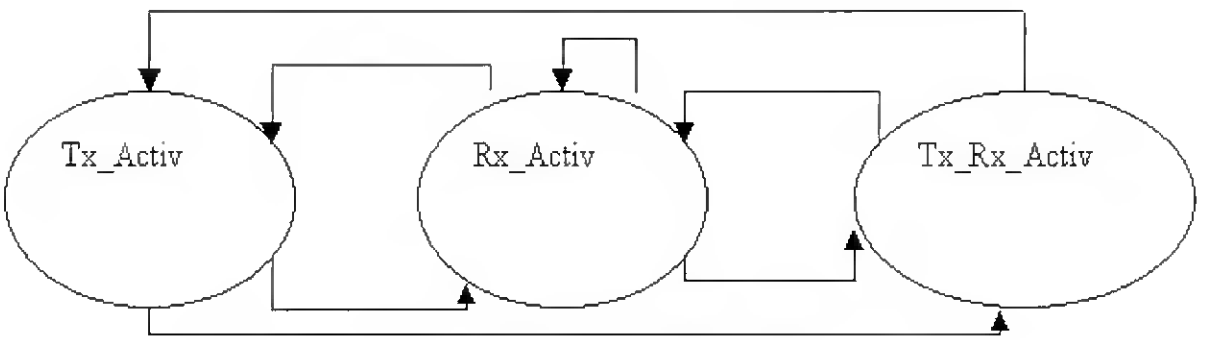


Ilustração 49 - Estados Possíveis

Neste último estado embora alguns circuitos estejam activos, como por exemplo os relógios, o circuito receptor está desactivado. As estações que não implementem mecanismos de conservação de potência transitam entre os dois estados Tx_Activ e Rx_Activ. Por outro lado, aquelas que implementem um desses mecanismos transitam entre ao três estados, permanecendo grande parte do seu tempo no estado de consumo reduzido (adormecidas) transitando apenas para os outros estados quando tal se manifeste necessário. Existe, em geral, uma relação inversa entre a potência consumida e o desempenho, pelo que qualquer mecanismo que implemente redução do consumo de potência deverá ter em conta esse facto.

Em termos da norma IEEE 802.11 uma estação poderá funcionar e comutar entre um de dois modos possíveis, modo AM (*Active Mode*) e modo PSP (*Power Save Polling*). O modo AM opera sem redução no consumo de potência. O modo PSP opera com redução de consumo de potência e apenas pode ser implementado em redes infraestruturadas. Sempre que se pretenda alterar o modo de funcionamento as estações devem informar o AP, utilizando para isso dois *bits* (PM) do campo de controlo das tramas transmitidas, que será descrito em pormenor quando nos referirmos ao formato das tramas.

VI.5.3.1. Modo de funcionamento IEEE 802.11 - AM (*Active Mode*)

As estações que funcionam no modo AM têm os seus emissores e receptores continuamente activos. Numa rede infraestruturada sempre que o AP tenha alguma trama para transmitir para uma estação, a operar no modo AM, transmite-a de imediato sem necessidade de armazenamento. Deste modo as tramas são recebidas pela estação sem qualquer atraso provocado pelo seu armazenamento. No período sem contenção (PCF), caso a estação se encontre na lista de interrogação do AP deverá permanecer no modo AM durante esse intervalo de tempo. Numa rede Ad-Hoc a estação que transmitiu a última trama BEACON deverá permanecer no modo AM até que finalize o *Beacon_Interval*, já que é da sua responsabilidade responder a possíveis tramas PROBES.

VI.5.3.2. Modo de funcionamento IEEE 802.11 - PSP (*Power Save Polling*)

Neste modo de funcionamento, o AP é a entidade à qual é atribuído o controle de gestão do consumo de potência e as estações apenas são activadas em momentos específicos, nos quais determinam se podem regressar ao estado adormecido ou se têm que continuar activas. Por outro lado, cabe ao AP armazenar temporariamente as tramas destinadas a estações que estejam a operar neste modo, transmitindo-as apenas quando as estações estão acordadas e, simultaneamente, construir uma tabela denominada TIM (*Traffic Indication* MAP), que contém a identificação das tramas armazenadas.

A forma como o AP dá conhecimento às estações das tramas armazenadas e respectivos destinos é pela inclusão do TIM nas tramas BEACONS. Estas são geradas, com certa periodicidade, pelo AP e as estações podem individualmente determinar com que frequência as escutarão, dependendo da relação consumo de potência / desempenho que se pretende. O seu período de escuta deve ser sincronizado de forma a garantir que a trama BEACON

inicial é recebida imediatamente após o receptor ter sido activado, ou seja após a estação ter transitado do estado adormecida para o estado acordado. Por análise do TIM contido nas tramas BEACONS, as estações podem determinar se o AP tem armazenadas tramas que lhes sejam destinadas e, deste modo, tomarem as atitudes necessárias para que as mesmas lhes sejam entregues.

As atitudes a tomar pela estação diferem de acordo com o facto de se estar no período com contenção (DCF) ou sem contenção (PCF). Durante o período com contenção se existirem no AP tramas armazenadas para uma dada estação esta transmite uma pequena trama, denominada PS-POLL (*Power Save-Pol*), para as solicitar. O AP por seu lado, ao receber a PS-POLL transmite uma das tramas destinada à estação. Uma estação enviará tantas tramas PS-POLL quantas as tramas armazenadas no AP que lhe sejam destinadas, valor do qual terá conhecimento analisando, no campo de controle das tramas que chegam do AP, o *bit* denominado *More*. Durante o período sem contenção as estações devem escutar a trama BEACON inicial. Todas as estações que tenham tramas armazenadas no AP deverão permanecer activas durante esse período para as receber. Se a recepção de todas as tramas, por uma estação, ficar concluída antes do final deste período a estação pode regressar ao estado adormecida. Caso contrário, se o período sem contenção terminar e a estação ainda não tiver recebido todas as tramas armazenadas, então esta envia ao AP uma trama PS-POLL requerendo a transmissão das restantes tramas armazenadas.

As tramas BEACONS podem também incluir, para além do TIM, um subconjunto das entradas na tabela TIM, denominado DTIM (*Delivery* TIM), que contem a identificação das tramas de difusão e de grupo armazenadas no AP, as quais são transmitidas imediatamente após cada BEACON com DTIM. A periodicidade com que os DTIMs são incluídos nos BEACONS é configuravel.

Em suma, esta função da rede IEEE 802.11 permite que as estações vão para um modo *sleep*, de modo a conservar potência, durante longos períodos de tempo sem perda de informação. Esta função é suportada pelo uso de APs por isso, não está disponível quando se implementa uma rede ad-hoc. Devemos equacionar a implementação desta função se a conservação de potência da bateria das placas rádio e das ferramentas for uma preocupação. Na implementação prática de redes de área local sem fios IEEE 802.11 define-se, em primeiro lugar, os APs e placas rádio para operam neste modo via rotinas de inicialização e parâmetros do fabricante. Como parte desta rotina de gestão da potência consumida, os APs manterão um registo das estações que estão, em dado momento, a funcionar em conformidade. Isto é conseguido, entre outras, pela monitorização do subcampo de bit único,

power-management, pertencente ao campo *Frame Control* da cabeçalho das tramas MAC enviadas na rede.

VI.6. Serviços IEEE 802.11 / Funções de transporte

O standard 802.11 define serviços que fornecem as funções que a camada LLC necessita para enviar MSDUs (MAC Service Data Units) ente duas entidades na rede. Estes serviços, implementados pela camada MAC, dividem-se em duas categorias: Serviços da Estação e Serviços do Sistema de Distribuição e asseguram o transporte de informação através da rede.

VI.6.1. Serviços da estação

Os serviços da estação asseguram o transporte de informação entre estações pertencentes a uma mesma BSS. Estes são autenticação, desautenticação e privacidade, os quais fornecem funcionalidade entre estações para entrega de MSDUs, que podem ser qualquer dispositivo da rede sem fios. Adicionalmente, todos os APs implementam serviços de estação.

O serviço de autenticação permite dar conhecimento da identidade duma estação às restantes ou cancelar uma autenticação existente, garantindo a confidencialidade. Tem como principal função prevenir acessos não autorizados equivalente ao nível do de uma rede cablada e justifica-se devido ao facto das redes de área local sem fios possuírem segurança física limitada. Todas as estações IEEE 802.11 que fazem parte de uma rede, ad hoc ou infraestruturada, deverão usar este serviço antes de estabelecer uma ligação, referida nos termos da norma como associação, com outra estação com a qual irão comunicar. Este processo é implementado com o envio de uma trama *unicast* para a estação correspondente. O standard IEEE 802.11 define dois tipos de serviços de autenticação: o primeiro denominado *Open System Authentication*, é o método usado por defeito pela norma e é implementado em dois passos. Em primeiro lugar, uma estação que pretenda autenticação com outra envia uma trama (*authentication management frame*) que contem a sua identificação. Após isso, a estação receptora devolverá outra trama (*alerting*) caso reconheça a identidade da estação emissora. O segundo denominado *Shared Key Authentication*, assume que cada estação recebeu uma chave secreta, a qual foi partilhada através de um canal independente da rede 802.11. O uso desta técnica requer a implementação do algoritmo WEP (*Wireless Equivalent Protocol*).

O serviço de desautenticação é usado quando uma estação pretende dessassociar-se de outra, não podendo ser recusado porque se trata de uma notificação. As estações executam-no enviando uma trama (*authentication management frame*) para advertir o fim da conexão.
O serviço de privacidade inibe a possibilidade de leitura de mensagens por parte de entidades não pertencentes à rede, fornecendo condições que elevam a segurança da rede ao nível do da rede cablada. Esta questão faz sentido porque numa rede de área local sem fios todas as estações, ou outros dispositivos, podem ouvir o tráfego que tem lugar no seu espaço o que pode ter um impacto sério ao nível da segurança do link. O standard IEEE 802.11 contornou este problema oferecendo este serviço, aplicado a todas as tramas de dados e a algumas tramas de gestão, baseado no algoritmo 802.11 WEP (*Wired Equivalent Privacy*) que executa a encriptação de mensagens reduzindo significativamente os riscos de escuta ilícita na rede.

OSA - Open System Authentication

Este serviço de autenticação, tal como outros, é justificado pela natureza da operação por difusão aberta, na qual operam as redes de área local sem fios, obrigando a implementar níveis de segurança adequados. Este é o mecanismo implementado por defeito, apenas anunciando o desejo de associação com outra estação ou AP, como tal deve ser usado quando não seja necessário validar positivamente a identidade da estação emissora.
Uma estação pode autenticar-se com qualquer outra ou AP usando este processo, como ilustrado na figura (Ilustração 50). Para tal a estação receptora tem que o permitir, indicando OSA no parâmetro MIB, *aAuthenticationType*. O código de *status* localizado no corpo da segunda trama de autenticação indica ou sucesso, ou não, do processo.

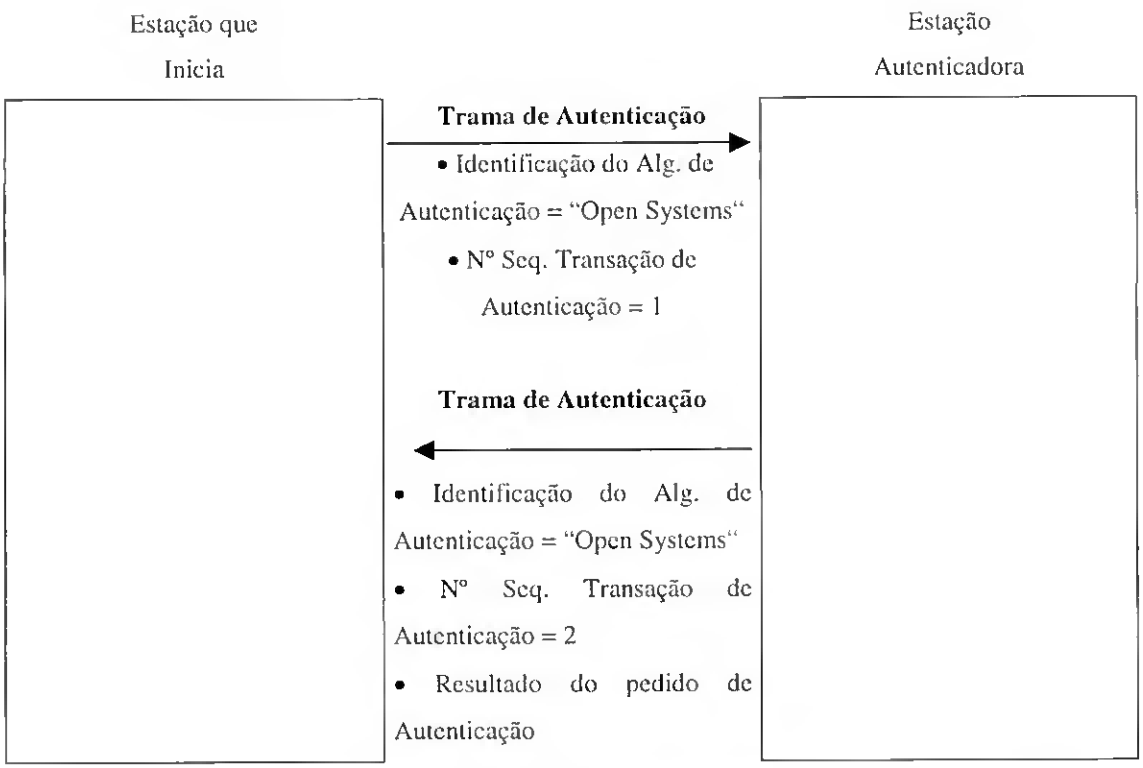


Ilustração 50- Processo de autenticação usando OSA

Shared Key Authentication

Este processo envolve uma troca de tramas mais rigorosa assegurando a autenticidade da estação requisitante fornecendo, por isso, um grau de segurança muito mais elevado do que o anterior. Para que uma estação possa usar este tipo de autenticação terá que, obrigatoriamente, implementar WEP (*Wired Equivalent Privacy*). Neste algoritmo a chave secreta partilhada reside na MIB de cada estação num formato *write-only* de modo a torná-la disponível, apenas, à coordenação da camada MAC. O standard IEEE 802.11, contudo, não especifica o processo de instalação das chaves nas respectivas estações.

Este processo de autenticação funciona da seguinte forma:

1. Uma estação requisitante envia uma trama de autenticação para outra estação;
2. Quando uma estação recebe uma trama de autenticação inicial, responderá com outra trama do mesmo tipo contendo 128 bits de texto, do tipo *challenge*, gerado pelos serviços WEP;
3. A estação requisitante copiará, então, este texto para uma trama de autenticação, encriptando-o com uma chave partilhada e envia a trama para a estação destino (*responding*);
4. A estação receptora desencriptará o texto usando a mesma chave partilhada e compara-o com o texto enviado anteriormente. Se existir uma correspondência, esta

(*responding*) responderá com uma trama de autenticação indicando o sucesso da operação. Se, pelo contrário, tal não se verificar será enviada uma autenticação negativa.

Em suma, o algoritmo WEP gera chaves de encriptação privadas que ambas as estações, origem e destino, podem usar para alterar bits numa trama de modo a prevenir, eventuais, escutas ilegais. Este processo é também conhecido como *symmetric encryption*. Por outro lado, a transmissão de tramas privadas (WEP) permite oferecer um nível de privacidade idêntico ao das redes cabladas, sendo definida como opção pela especificação IEEE 802.11. As estações podem usar WEP por si só, sem serviços de autenticação, mas é aconselhável implementar ambos. Assim, a utilização conjunta de WEP e autenticação evitará que a rede seja vulnerável a ameaças à sua segurança.

Não iremos descrever o funcionamento deste algoritmo por ir além do âmbito do estudo.

VI.6.2. Serviços do sistema de distribuição

Os serviços do sistema de distribuição, DS, apenas são suportados por redes infraestruturadas e asseguram o transporte de informação através dele. Os serviços do sistema de distribuição são associação, desassociação, reassociação, distribuição e integração. Estes serviços, como descritos na norma, fornecem a funcionalidade necessária para que o mesmo permita transferência adequada de MSDUs.

O serviço de associação é aquele que cada estação deve, inicialmente, invocar com um AP antes que possa enviar informação através do DS. Este irá mapear a estação no DS através de um AP. Cada estação apenas pode estar associada a um AP, mas um AP pode ter associadas múltiplas estações. A associação é, ainda, o primeiro passo para dotar uma estação de capacidade para se mover entre BSSs.

O serviço de desassociação é invocado, por uma estação ou AP, para terminar uma associação existente, constituindo uma notificação e como tal nenhuma das partes o pode recusar. As estações deverão desassociar-se quando deixam a rede, um AP pode desassociar-se quando, por exemplo, é removido para manutenção.

O serviço de reassociação assegura a passagem das estações de uma BSS para outra sem perda de conectividade, pela possibilidade de uma estação alterar o seu estado actual de associação. Exemplo disso é a capacidade para suportar a mobilidade necessária à transição entre BSSs, permitindo a uma estação transmitir a sua associação de um AP para outro. Esta atitude manterá o DS informado do mapeamento actual entre o AP e a estação ao mesmo tempo que a estação se move de BSS para BSS, dentro de uma ESS. Por outro lado permite,

também, a alteração dos atributos de associação, relativos a uma associação já estabelecida, enquanto a estação permanecer associada ao mesmo AP. Este serviço é de activação obrigatória para uma estação móvel.

O serviço de distribuição é usado por uma estação sempre que esta envie tramas MAC através do DS. Embora o standard 802.11 não especifique o modo como o DS entrega os dados, este serviço capacita-o apenas de informação suficiente para determinar a BSS destino apropriada.

O serviço de integração possibilita a transferência de informação entre o DS e uma rede não IEEE 802.11. Isto é conseguido pela entrega de tramas MAC através de um *portal* existente entre o DS e uma rede de área local de outro tipo. Esta função executa todos os passos requeridos para a translação do espaço de endereços e as suas especificidades, que dependem da implementação do DS, e vão além do âmbito do standard 802.11.

A titulo de conclusão devemos referir que o standard IEEE 802.11, através dos vários serviços, permite ao utilizador mover-se ente múltiplos APs, os quais poderão operar no mesmo ou em canais separados [27]. De modo a suportar esta função de mobilidade (*roaming*) cada AP geralmente transmite um sinal (*beacon*) a cada 100 ms, que as estações em *roaming* usarão para medir a potência da conexão existe com o AP. Se sentirem a existência de um sinal fraco podem recorrer ao serviço de reassociação para se ligar a um AP que emita um sinal de potência superior. De referir, também, é o estado existente entre uma estação origem e destino. Como ilustrado na figura (Ilustração 51), este é definido de acordo com os tipos de tramas IEEE 802.11 que as duas podem trocar.

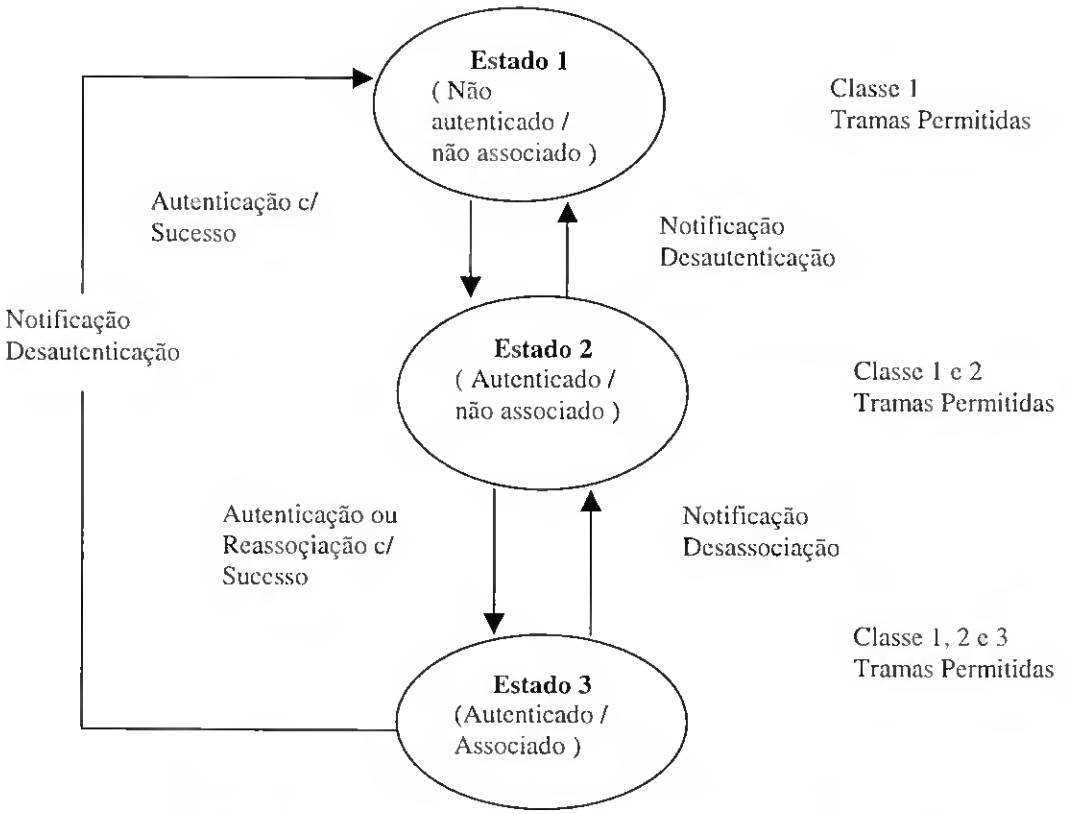


Ilustração 51 A operação de uma estação depende so seu estado

Os tipos de funções estão de acordo com uma classificação das tramas segundo classes, as quais são referidas em Apêndice. Para manter um traçado do estado da estação, cada uma poderá estar num dos dois estado seguintes, que são variáveis: Estado de Autenticação: com valores de autenticado ou não autenticado e Estado de Associação: com valores de associado ou não associado.

VI.7. Formato das tramas IEEE 802.11

O formato genérico de uma trama da camada MAC IEEE 802.11 é o apresentado na figura (Ilustração 52).

2 octetos	2 octetos	6 octetos	6 octetos	6 octetos	2 octetos	6 octetos	0-2312 octetos	4 octetos
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

MAC Header

Ilustração 52 - Formato da trama MAC

A trama divide-se em três partes:

CABEÇALHO: que incluí informação de controlo, duração, endereçamento e controlo de sequência;

CORPO DA TRAMA: que contém informação especifica relativa a cada tipo de trama e é de comprimento variável (0 –2312);

CRC: que consiste num *Cyclic Redundancy Check* de 32 bits, calculado sobre a trama. Este campo pode, também, apresentar a designação FCS (*Frame Check Sequence*).

No APÊNDICE A é apresentada uma descrição pormenorizada de cada uma destas bem como os formatos de cada uma das tramas suportadas pela norma IEEE 802.11.

VI.8. Tipos de tramas da camada MAC

A camada MAC usa uma variedade de tramas, cada uma com o seu propósito particular, para transportar e garantir a entrega de MSDUs entre LLCs pares.

O standard IEEE 802.11 divide as tramas MAC em três categorias que fornecem funções de gestão, controle e troca de dados entre estações e APs. Uma descrição aprofundada dos vários tipos de tramas é apresentada em APÊNDICE A.

VI.8.1. Tramas de gestão

O objectivo das tramas de gestão é estabelecer comunicações iniciais entre estações e APs. Deste modo estas tramas fornecem serviços anteriormente referidos, como por exemplo, associação e autenticação.

VI.8.2. Tramas de controle

O objectivo das tramas de controle é fornecer a funcionalidade que assiste à entrega de tramas de dados, após estabelecida uma associação e autenticação entre estações e APs.

O fluxo, comum, de tramas de controle é o exibido na figura (Ilustração 53).

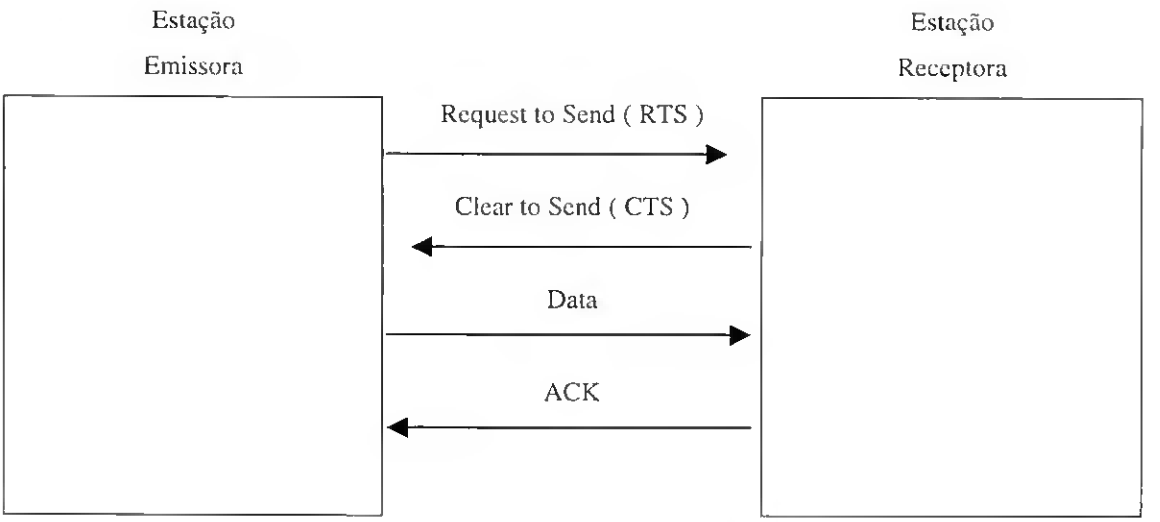


Ilustração 53 - Sincronismo com tramas de controle

VI.8.3. Tramas de dados

O objectivo principal das tramas de dados é transportar informação, tal como MSDUs, para a estação destino para *handoff* da sua camada LLC, se aplicável.

CAPITULO VII
UM CASO DE ESTUDO

Este capítulo descreve a simulação de uma rede WLAN IEEE802.11 aplicada a um cenário em particular recorrendo ao simulador COMNET III. Em seguida é feita uma análise da performance da rede em termos de escalabilidade e na presença de erros. Por último apresentamos as conclusão do estudo efectuado.

VII.1. Cenário da aplicação

Uma dada organização pretende instalar uma rede sem fios para fazer face ás necessidades de um departamento que, por razões próprias e inadiáveis, teve que se deslocar temporariamente para novas instalações, onde apenas existe uma infraestrutura de corrente eléctrica e uma linha telefónica. Pelo facto de ser temporário não pretende ter custos adicionais inerentes à instalação de uma infraestrutura cablada de rede local. Por outro lado, tem que existir a garantia que a rede seja instalada o mais rapidamente possível dada a pertinência dos serviços suportados pela mesma e as implicações que o seu não funcionamento acarreta para a organização. A rede suportará um determinado número de utilizadores móveis que pode variar de acordo com as necessidades. Deve, também, ser considerada a existência de um servidor de correio electrónico interno (*e-mail*), para a troca de mensagens entre os utilizadores da própria rede, e de um servidor de ficheiros (*file server*) para o departamento, ambos móveis. Por outro lado, para além desta utilização existe a necessidade de uma ligação ao exterior que será garantida por uma linha dedicada T1, ligação esta que é feita recorrendo a um *router*. Esta visa facultar o acesso a serviços WWW e a consulta a correio electrónico proveniente do exterior.

Atendendo ao número variável de utilizadores da rede, uma das preocupações da organização, à qual a nossa simulação pretende responder, é a adição de estações móveis a esta rede e se a mesma pode ou não ser capaz de os suportar. Esta preocupação advêm do facto de não existir um meio que permita medir a utilização da rede ou atraso. Assim pretende-se estimar os níveis actuais de atraso antes de avançar com o processo, tendo em conta estimativas do tráfego típico da rede.

Para simular o tráfego da rede, baseamo-nos em estudos efectuados em redes locais, o qual é maioritariamente proveniente de *e-mail*, transferência de ficheiros entre as várias aplicações

e pedidos http [30]. O método de estudo, anteriormente referido, baseou-se em entrevistas realizadas aos utilizadores dessas redes bem como estimativas do tamanho comum das mensagens enviadas, o que permitiu descrever as características do tráfego estatisticamente.
Assim separamos o tráfego da rede nas seguintes categorias:

Tráfego inerente a *e-mail*: este tipo de tráfego apresenta um tempo médio entre chegadas de mensagens (*average interarrival rate*) que pode ser descrito por meio de uma Distribuição Exponencial com média de 900 segundos e o tamanho das mensagens pode ser descrito através de uma Distribuição Uniforme no intervalo de 500 a 2000 bytes [30].

Por outro lado todas as mensagens são enviadas pelos servidores destinados ao efeito, onde as mensagens são guardadas na conta de cada utilizador, interno caso se trate de mensagens enviadas entre os utilizadores da rede sem fios ou externo caso a origem destas não seja um utilizador da própria rede. Assim, para ler o seu correio cada utilizador deverá enviar um pedido ao respectivo servidor que, após o receber, irá proceder à leitura dos ficheiros e efectuar o *downloading* das mensagens para os respectivos dispositivos pessoais. O tempo necessário para esta operação pode ser descrito através de uma Distribuição Uniforme compreendida entre 3 a 5 segundos [30].

O tempo entre pedidos (*interarrival time*) para acesso a contas pode ser descrito por meio de uma Distribuição de Poisson com média em 800 segundos e cada pedido apresenta um tamanho de mensagem fixo definido em 60 bytes. Por outro lado o tamanho das mensagens de *e-mail* transmitidas pelo respectivo servidor pode ser descrito por meio de uma Distribuição Normal com média de 40 000 bytes e desvio padrão de 10 000 bytes [30].

Tráfego inerente a pedidos de ficheiros:

Este tráfego será gerado pelas solicitações de ficheiros, por parte dos utilizadores móveis, ao respectivo servidor. Estudos de caracterização, mostram que o mesmo pode ser descrito por meio de uma Distribuição Exponencial com média em 900 segundos. O tamanho das mensagens correspondente a cada pedido, variam de acordo com uma Distribuição Uniforme entre 10 e 20 Bytes [30].

Todas as solicitações de ficheiros são exclusivamente enviadas para o servidor destinado ao efeito. Após receber um pedido, o servidor lê o ficheiro correspondente e envia-o para o utilizador móvel que o solicitou, processo no qual existe um atraso pequeno.

O tamanho dos ficheiros a serem transferidos pode ser descrito por meio de uma Distribuição Normal com média em 100 000 Bytes e desvio padrão em 25 000 Bytes.

Tráfego inerente a pedidos http:

Os dados relativos ao servidor bem como o tamanho dos ficheiros correspondentes às *home pages* mais solicitadas forma obtidos com base numa estatística que resultou de uma observação efectuada durante 120 dias por hora (das 0H às 24H) [30]. Neste estudo a modelização dos pedidos http, teve que ser convertida para uma forma que representa-se os tempos entre chegadas (*interarrival times*), partindo do pressuposto que os mesmos ocorriam de modo uniforme no período de tempo total, dado que não existia informação disponível relativa à sua natureza por rajadas. Foi calculado o tempo médio entre pedidos e efectuada a representação gráfica da distribuição correspondente. Com base nisso foi definido que o tempo médio entre pedidos podia ser representado por uma Distribuição Normal com média de 31.8 segundos e desvio padrão de 3.8 segundos. Na hipótese de um aumento de 60% no número de pedidos os valores anteriores seriam escalados por um factor de 60%, passando a média de tempo entre chegadas a ser representada por uma Distribuição Normal com média de 19.4 segundos e desvio padrão em 3.8 segundos [30]. Relativamente ao tamanho dos pedidos http, os dados que permitiram a sua descrição não foram recolhidos mas sim estimados com base no número de caracteres de um pedido típico a um servidor Web. Deste estudo resultou uma Distribuição Uniforme com mínimo em 10 Bytes e máximo em 100 Bytes.

A modelização do processo que se passa no servidor Internet, após receber um pedido http, traduz-se em primeiro na leitura de um ficheiro e em seguida na criação de uma mensagem para devolver ao nó móvel que solicitou, com base no tamanho do ficheiro lido. O problema que se coloca é de como estimar a número de bytes a ler para cada pedido. Estudos efectuados apresentam as estatísticas relativas a pedidos de ficheiros, as quais contêm informação relativa ao número de pedidos das *home pages* mais frequentemente acedidas e disponibilizam uma lista das páginas frequentemente activadas com o respectivo tamanho e probabilidade associada [30]. Esta informação irá ser usada, no estudo a que nos propomos, para criar uma tabela de distribuição (WEB_READ) que permita estimar o número de bytes a ler após receber um pedido http.

VII.2. Implementação prática da rede

VII.2.1. Arquitectura do sistema

Relativamente à topologia e face às características do exemplo em estudo, atendendo à natureza da implementação a qual pretende suprir necessidades temporárias e responder à

disponibilização imediata deste tipo de conectividade sem fios, optámos por uma topologia ad hoc, ponto a ponto (IBSS; *Independent Basic Service Set*) que julgámos ser a mais adequada a um cenário com as exigências do apresentado. Esta consiste simplesmente num conjunto de estações sem fios, autónomas, que comunicam directamente umas com as outras sem recorrer ao uso de um AP ou qualquer outra ligação com uma rede cablada, comforme exibido na figura (Ilustração 54).

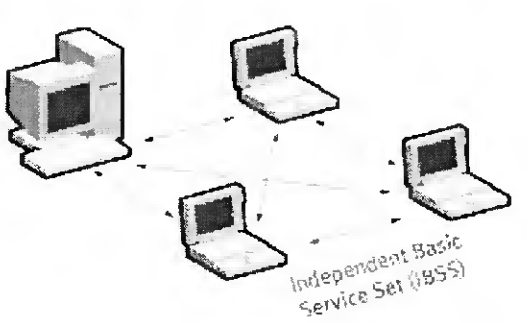


Ilustração 54 - Configuração da rede ad-hoc [25]

A rede que pretendemos modelizar apresenta como estrutura global uma única célula com várias estações móveis que comunicam com os vários serviços (*e-mail*, http e pedidos de ficheiros). O tamanho da célula é escolhido de modo que todas as estações móveis, dentro da célula, consigam comunicar umas com as outras, o que se traduz no pressuposto de considerar-mos que não existirão estações ocultas. Por outro lado, pressupõe-se que as estações se movem lentamente no ambiente puramente interno e numa área limitada. Em termos de mobilidade consideramos que as estações são livres de se moverem na célula aleatoriamente, mudando assim a topologia da rede de um modo dinâmico.

VII.2.2. Ferramenta usada na simulação / COMNET III

Na simulação usámos como ferramenta o COMNET III desenvolvido pela CACI Product Company, a qual é adequada para as nossas intenções porque permite fazer a análise de performance para redes de computadores. Assim, com base na descrição de uma rede, nos algoritmos de controle e no tráfego da rede esta ferramenta irá simular a sua operação e fornecer indicadores de performance, permitindo a sua análise e premonição.

O COMNET III é uma aplicação comercial, onde não é exigida nenhuma programação, que apresenta um interface gráfico e permite a simulação desde simples LANs até sistemas mais complexos. A abordagem de construção é baseada em blocos, os quais representam objectos

que nos são familiares do mundo real. A estes estão associadas algoritmos que, de modo aproximado, modelizam cada uma das partes da rede real e podem corresponder a um ou mais items. A cada objecto está, também, associado um conjunto de parâmetros facilmente ajustáveis e permitem, desta forma, simular uma série de cenários baseados no pressuposto " E se?". Esta concepção orientada a objectos dota o COMNET III de uma capacidade que permite abstrair partes do modelo da rede e tratá-las como componentes modulares, cada uma das quais associadas a algoritmos, que podem ser facilmente mudadas de acordo com o que se pretenda.

Relativamente à metodologia é utilizada a simulação de eventos discretos, a qual é usada como alternativa à matemática tradicional baseada em métodos analíticos os quais podem não ter em conta os efeitos de variação aleatória, que fornece resultados reais e com grande grau de precisão [31]. Esta é justificada porque a variedade de situações reais não são descritas por eventos que ocorrem em intervalos de tempo uniformemente separados e a uma taxa média conhecida à priori.

O COMNET III foi escrito numa linguagem de programação de alto nível e orientada a objectos, MODSIM II, tendo sido concebido para estimar, de modo preciso, as características em termos de performance de redes de computação e comunicação. Estimar significa que a rede em estudo é descrita através de dados e o programa executará então uma simulação dinâmica da rede, a qual corresponde a uma representação computacional da mesma e o trafego simulado é encaminhado através dela [31].

As aplicações típicas do simulador incluem o estudo de picos de carga (*Peak Loading*); dimensionamento de uma rede no estado de concepção; planeamento de recuperação rápida em caso de falha; introdução de novos utilizadores e/ou aplicações; avaliação de performance e opções de melhorias; avaliação do grau de satisfação de serviços contratados; entre outras. Em suma a especificidade desta ferramenta é a predição de performance através de simulação [31]. Esta metodologia pretende não apenas testar a implementação de um novo cenário como no caso em estudo, mas também efectuar melhorias a um já existente, podendo ser uma ferramenta de grande valor dado que fornece um modo de modelizar uma rede e determinar o seu desempenho.

Optámos por usar a simulação, porque é uma técnica bastante utilizada, nos mais variados cenários, e pretende dar reposta à, crescente e cada vez maior, dependência das organizações das suas redes seja qual for o seu tipo. Assim, à medida que as redes suportam cada vez mais as operações vitais de uma organização mais repercussões terão eventuais riscos de falha causada por uma performance de rede inadequada, pelo que as ferramentas de suporte que

auxiliem na tomada de decisão, face a um dado cenário ou concepção, são cada vez mais de extrema importância. Os decisores irão usar os resultados obtidos para seguir por um dado caminho.

Em suma o objectivo da simulação da rede sem fios é a partir da representação da topologia da rede e das funções inerentes a cada um dos blocos obter medidas de performance da mesma.

VII.2.3. Construção do modelo da rede

Na construção do modelo é descrita a topologia da rede usando os vários Nós, Computadores e Servidores disponíveis; o tráfego e trabalho da rede, onde o primeiro se refere às mensagens a serem enviadas entre os nós na topologia da rede e o segundo refere-se à actividade interna dos nós processadores. A frequência e tamanho das diferentes tarefas pode ser descrita estatisticamente. Em último os protocolos que correspondem ao conjunto de regras para escalonamento das aplicações e encaminhamento do tráfego.

Um dos conceitos base que deve tido em consideração na modelização de uma rede usando o COMNET III é que a maioria das características de qualquer um dos objectos (nós, fontes de trafego ou aplicações) podem ser descritas ou através de constantes ou por meio de distribuições estatísticas. Se optarmos pela última, a forma como a aplicação selecciona os valores de uma distribuição, enquanto a simulação é executada, é baseada na geração de números aleatórios com base numa filosofia multiplicativa e congruêncial. Além das que já vêm definidas no COMNET este permite também a criação distribuições definidas pelo utilizador. Para dados que não possam ser descritos do modo anterior é possível, também, definir tabelas de probabilidades, as quais poderão ser discretas ou contínuas, onde os valores de probabilidade introduzidos devem ser na forma de distribuição cumulativa.

Após construído o modelo é então verificado de acordo com a sua exactidão ou seja, é executado um teste lógico ao modelo construído e, caso não tenham sido detectados erros, pode ser executada a simulação. O COMNET usa muitas vezes o planeamento no tempo, onde os nós começarão a enviar mensagens, de um determinado tipo, em intervalos aleatórios definidos no campo *Interarrival*. Este termo refere-se à simulação de um evento discreto.

Iremos construir o modelo proposto para a nossa rede usando o COMNET III, o qual irá ser feito por etapas que passamos a especificar em seguida.

TOPOLOGIA DA REDE

Começamos em primeiro lugar pela construção da topologia da rede que diz respeito a todos os computadores, *routers*, *switchs* e *links* através dos quais as mensagens são criadas e transportadas.

A. Modelização dos Computadores Pessoais

Na nossa rede vamos criar um conjunto de computadores, cujo número será um dos parâmetros variáveis na execução as simulação, representado por um nó do tipo *Computer Group* denominado PC.

Este objecto tem as mesmas funcionalidades que um único nó com excepção que possuí um campo quantitativo, o qual permite especificar quantas cópias idênticas deverão ser incluídas quando a simulação for executada, mas que contudo não aparecerão no interface do utilizador. Justificamos a sua utilização porque na modelização da nossa rede existem vários nós com os mesmos parâmetros e padrões de geração de tráfego, e quando formos executar a simulação cada computador definido no grupo será criado como um caso desse nó. Por outro lado, qualquer aplicação ou objecto ligado ao nó será modelizada como estando disponível para qualquer um dos computadores e as mensagens destinadas ao grupo serão uniformemente analisadas por todos.

Os parâmetros que definimos para este objecto são os apresentados (Ilustração 55), onde o *number in group* será variável.

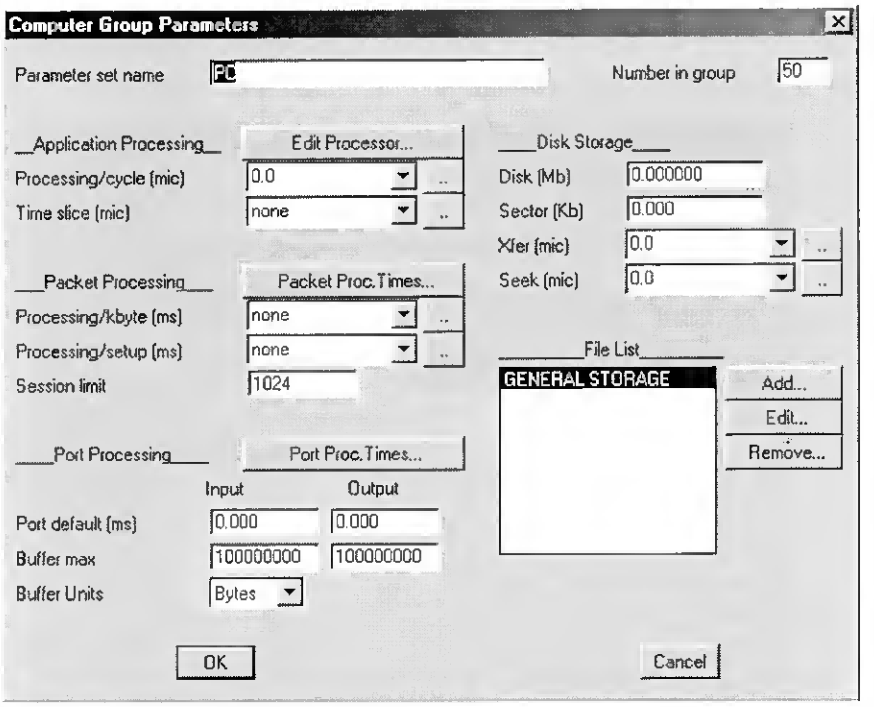


Ilustração 55 - Parâmetros do nó PCs

B. Modelização dos servidores de *e-mail* e ficheiros.

Estes irão ser representados por nós do tipo Processing Node denominados E_MAIL SERVER e FILE SERVER respectivamente. Os parâmetros que definimos, comuns para estes objectos, são os apresentados na figura (Ilustração 56).

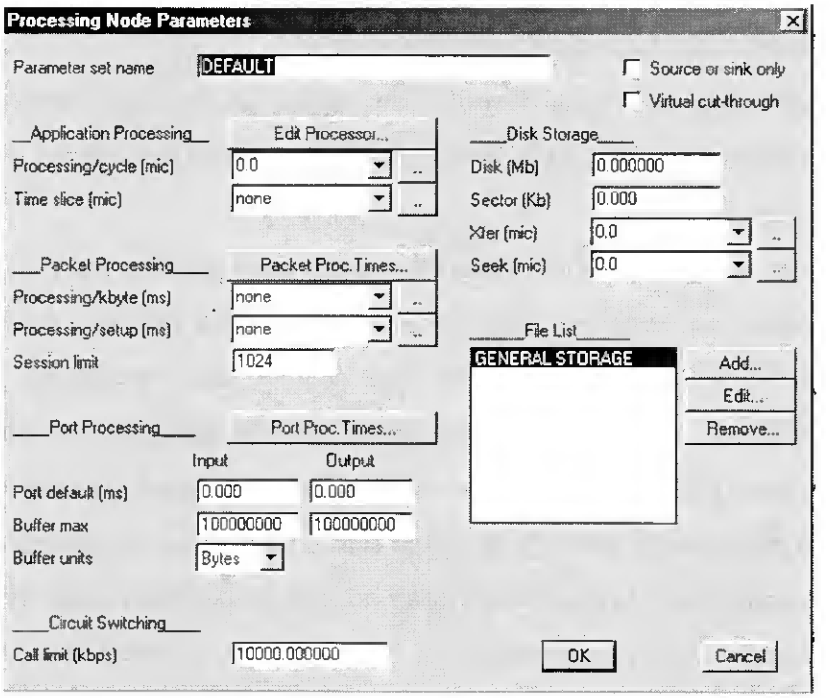


Ilustração 56 - Parâmetros de E_MAIL SERVER e FILE SERVER

C. Modelização do servidor Internet.

Este irá ser representado por um nó do tipo *Processing Node* denominado INTERNET. Os parâmetros que definimos são os apresentados na figura (Ilustração 57).

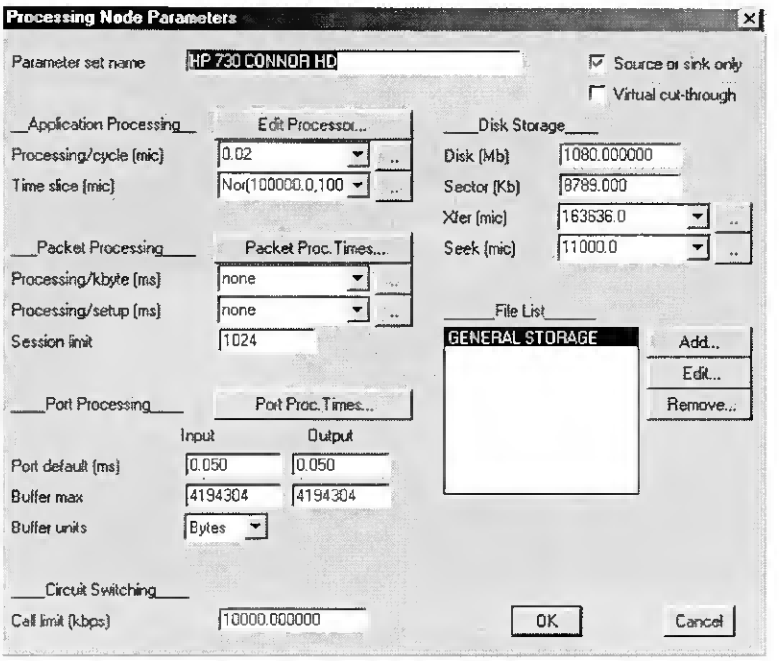


Ilustração 57 - INTERNET

A parametrização deste *processing node* teve em consideração os seguintes dados relativos às características da rede que nos propomos simular. O campo *Time slice* foi definido com base no tempo médio entre pedidos http processados no servidor, que pode ser descrito por uma Distribuição Normal com Média em 100 000 microsegundos e Desvio Padrão de 10 000 ms, o campo *Packet Proc. Times* foi alterado para que seja modelizado o atraso do protocolo IP em 0.01 milisegundos e o campo *Port Proc. Times* foi alterado para modelizar um atraso nas portas de I/O de 0.05 milisegundos e capacidade máxima de buffer I/O de 4194304 bytes, para representar uma disponibilidade de 4 MB para cada.

D. Modelização dos *routers*

Estes elementos permitirão fazer a segmentação das redes, tanto interna como externa. Estes irão ser representados por nós do tipo *Router* denominados ROUTER e ROUTER_OUT respectivamente. Os parâmetros que definimos, são comuns para estes elementos e são os apresentados na figura (Ilustração 58).

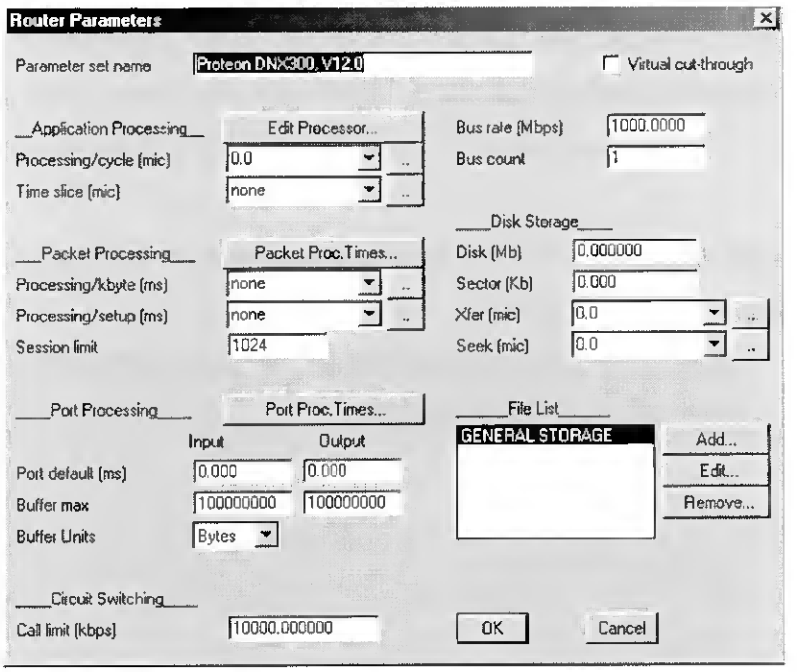


Ilustração 58 - Parâmetros de ROUTER e ROUTER_OUT

E. Criação dos *links*

Estes permitirão em primeiro lugar, simular o tráfego (tipo de tramas) na rede sem fios, a ligação ao exterior e tráfego da rede externa e em segundo lugar modelizar o meio físico através do qual as mensagens irão ser transportadas. Estes serão representados pelos nós denominados WLAN 802.11, T1 e ETHERNET respectivamente.

Os parâmetros que definimos variam de acordo com o objecto e são os apresentados nas figuras (Ilustração 59 / Ilustração 60 / Ilustração 61).

De referir que os parâmetros, no caso do link WLAN 802.11 são meramente ilustrativos dado que irão ser alvo de definição em secção apropriada (VII.2.4.). O link IEEE 802.11 *Wireless* LAN é do tipo acesso múltiplo baseado em contenção, usa o protocolo CSMA/CA, e permite a especificação de um intervalo (*Retry Interval*) destinado a retransmissão caso ocorra uma colisão. A retransmissão poderá ser feita com base numa distribuição de probabilidade ou num intervalo de *backoff*. A lógica, quando é executada uma simulação, aplicada a este link é a geral (*transmission delay / propagation delay*) descrita a seguir com excepção de que, como se disse, poderão ocorrer colisões quando dois ou mais nós, pertencentes ao link, transmitirem ao mesmo tempo. Os nós, com tramas prontas para transmissão, irão testar o estado do *link* determinando à priori se está ocupado. Se sim, a transmissão do pacote é adiada até que o mesmo fique disponível.

O link T1 do tipo ponto-a-ponto é usado para modelizar a ligação da rede 802.11 com fontes exteriores. Justificamos a sua utilização atendendo que o mesmo pode ser usado para modelizar o caso particular de linhas telefónicas para transmissões com dispositivos terminais do tipo Modem e com capacidade full-duplex. As tramas serão multiplexadas para o link pela ordem em que aparecem no seu *buffer*, o qual é definido pelo arco a que esta ligado.

O link 802.3 ETHERNET 10BASE5 pertence à rede externa e como tal vamos considerar os valores típicos para este tipo de rede.

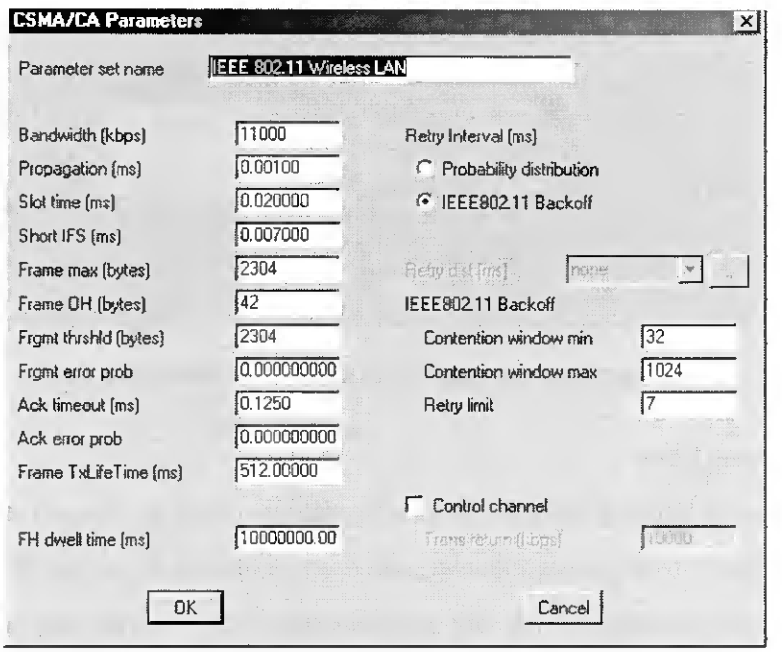


Ilustração 59 - Link WLAN 802.11

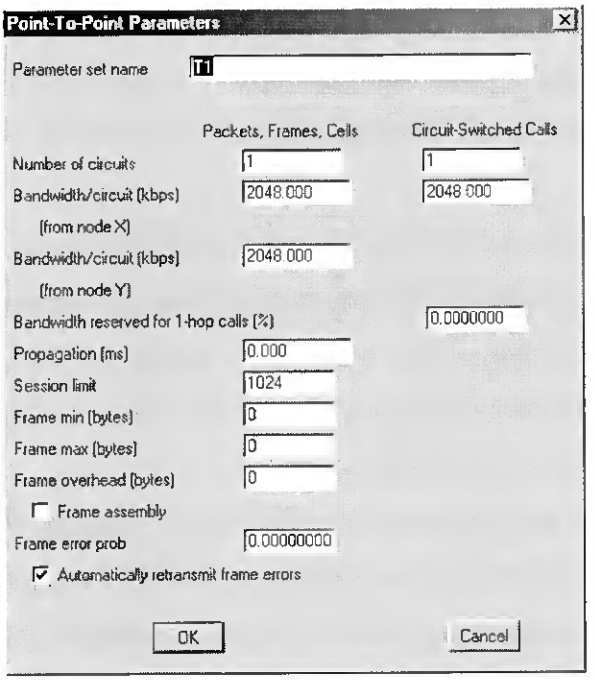


Ilustração 60 - Link T1

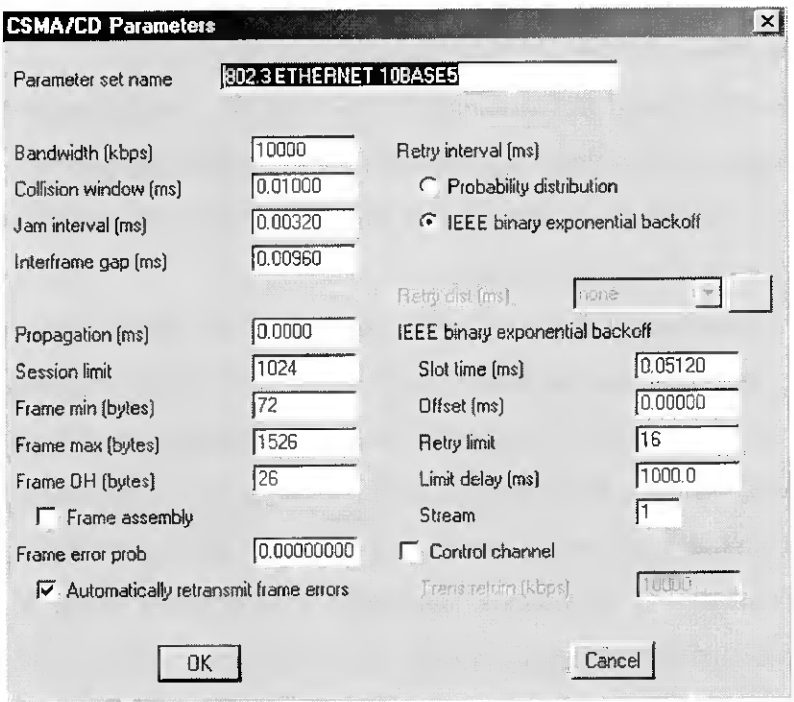


Ilustração 61 - Link ETHERNET

A lógica de operação aplicada a qualquer tipo de link, que permite a modelização de tráfego nos mesmos, é a seguinte: quando um nó tem um pacote, pertencente a uma mensagem pronto para ser transmitido este, eventualmente, ganhará o acesso ao meio (link). Os pacotes são então divididos em tramas de acordo com o conjunto de características definidas para o link. O modelo calculará então, o tempo de transmissão da trama (*transmission delay*) através do link com base no seu tamanho e na taxas de transmissão (*transmission rate*) à qual

o link está a operar. Se tiver sido definida probabilidade de erro de trama (*Frame Error Probability*) irá ser calculado um valor aleatório com base na distribuição, definida para o link e usada para descrever este erro, de modo a determinar se a trama chegou com erro e exige retransmissão.

Após este processo o link será considerado como ocupado durante o tempo calculado para a transmissão da trama (*transmission delay*) mais o tempo de propagação (*propagation delay*) que tiver sido definido para o link. Após uma trama ter sido sujeita a estes atrasos é considerada como tendo chegado ao seu destinatário, caso este pertença à mesma rede ou, caso contrário, ao próximo nó ao longo da sua rota.

Todas as características anteriormente referidas podem ser parametrizadas para cada link em particular, vamos dar especial atenção, no entanto, a dois campos. Começamos pelo tempo de propagação (*propagation delay* (ms)), que é comum a todos os links e permite modelizar o tempo necessário para que um pacote se mova entre dois nós num link, com base na distância que os separa. O segundo, largura de banda (B*andwidth*) associada a cada link é usada para especificar a sua taxa de transmissão (*transmission rate*).

De igual modo, as tramas apresentam uma variedade de características e são usadas para modelizar os protocolos do Nível de Ligação na rede, não detalhada sob um ponto de vista de funções comuns a este nível, mas apenas em parâmetros como tamanho da trama (*Frame Payload Capacity*) e *Overhead* associado.

F. Criação dos arcos ou linhas (*Ports*) que são usados para conectar ao vários nós aos vários tipos de *links*. Se for estabelecida uma conexão lógica é criada uma porta, caso contrário isso não acontecerá. Em termos físicos estes podem ser vistos como a modelização da parte relativa às placas de rede (NICs) em todos os tipos de nós e apresentam como principais características o facto de terem capacidade de armazenamento (*buffer*), poderem ser usados para modelizar os atrasos nas portas e recolha de estatísticas do tráfego. Os parâmetros que definimos variam de acordo com o objecto e são os apresentados na figura (Ilustração 62).

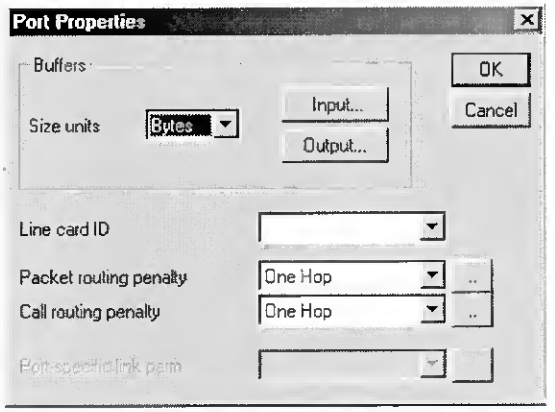


Ilustração 62 - Parâmetros dos arcos

DEFINIÇÃO DAS FONTES DE TRÁFEGO: E-MAIL / FILE SERVER / HTTP

Estes objectos irão gerar a carga na rede e serão criados recorrendo a *Message Sources*.

A. E-Mail / E-Mail_Out

Estes objectos são usados para modelizar o transporte de mensagens de e-mail dos nós da rede para o E-MAIL SERVER da rede interna e o E-MAIL SERVER_OUT da rede externa. A sua parametrização é idêntica, com excepção do tempo entre chegadas, e é a exibida nas figuras (Ilustração 63 / Ilustração - 64).

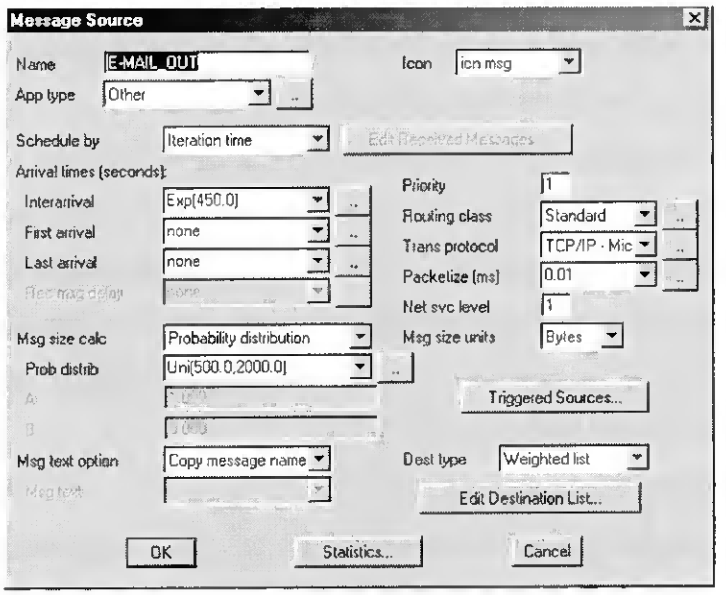


Ilustração 63 - E-MAIL_OUT

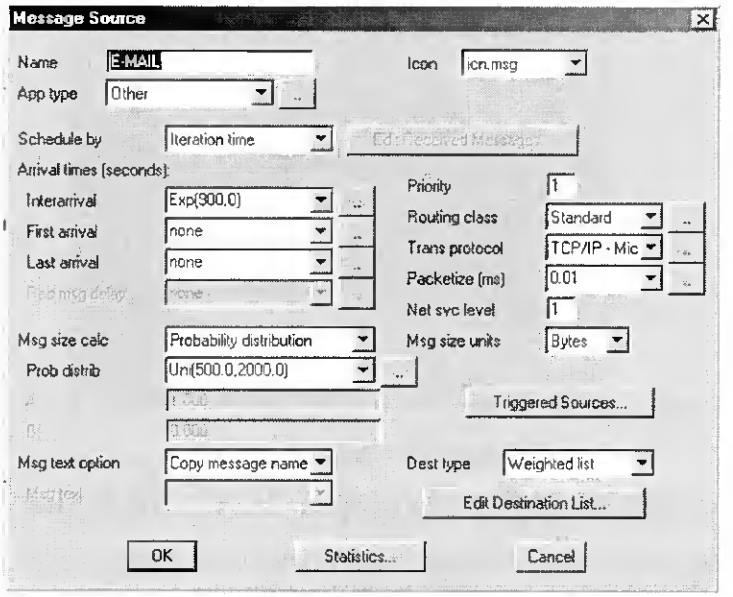


Ilustração - 64 E-MAIL

A parametrização desta *message source* teve em consideração os seguintes dados relativos às características da rede que nos propomos simular. O campo *Interarrival* foi definido de acordo com o facto de o envio de uma mensagem de e-mail ocorrer com um tempo médio entre chegadas que pode ser descrito por uma Distribuição Exponencial com média em 900 segundos (450 segundos para o externo) e o *stream value* pode ser definido como qualquer valor inteiro entre 0 e 99, pressuposto que vamos assumir para todos os items do tipo. Relativamente ao tamanho das mensagens (*Msg size calc*) este é descrito por uma Distribuição de Probabilidades com base numa Distribuição Uniforme cuja dimensão é dispersa de modo regular no intervalo de 500 a 2000 bytes. O protocolo de transporte usado é TCP/IP com um atraso de empacotamento de 0.01 ms. O destinatário desta mensagens (*Dest type / Weighted list*) varia de acordo com o facto ser correio interno ou externo (E-MAIL SERVER / E-MAIL SERVER_OUT).

B. E-Mail Check / E-Mail Check_Out

Estes objectos são usados para modelizar os testes que são efectuados, periodicamente, pelos utilizadores da rede ao E-MAIL SERVER da rede interna e ao E-MAIL SERVER_OUT da rede externa, de modo a fazerem o *dowload* do seu correio. A sua parametrização é idêntica, com excepção do tempo entre chegadas, e é a exibida nas figuras (Ilustração 65 / Ilustração 66).

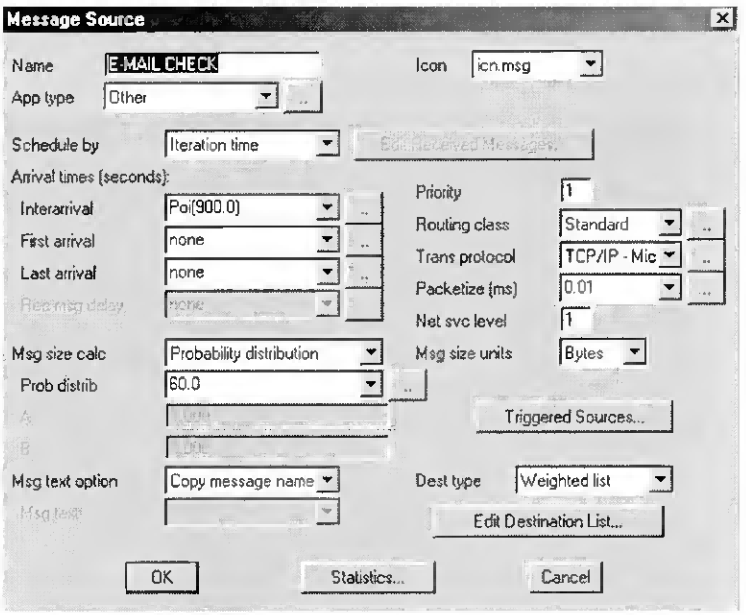


Ilustração 65 - E-MAIL CHECK

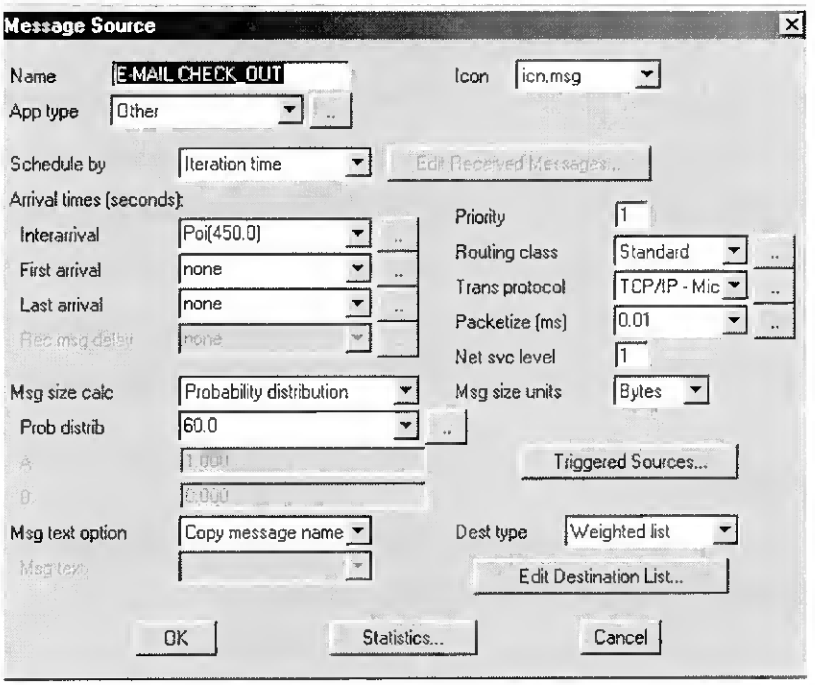


Ilustração 66 - E-MAIL CKECK_OUT

A parametrização desta *message source* teve em consideração os seguintes dados relativos às características da rede que nos propomos simular. O campo *Interarrival* para simular o tempo entre pedidos para acesso a contas é descrito por uma Distribuição Poisson com média em 900 segundos. Por outro lado cada pedido tem um tamanho de mensagem definido como constante (60 bytes).

C. **File Req**

Estes objecto é usado para modelizar os pedidos ao servidor de ficheiros para o *dowload* dos mesmos. A sua parametrização é a exibida na figura (Ilustração 67).

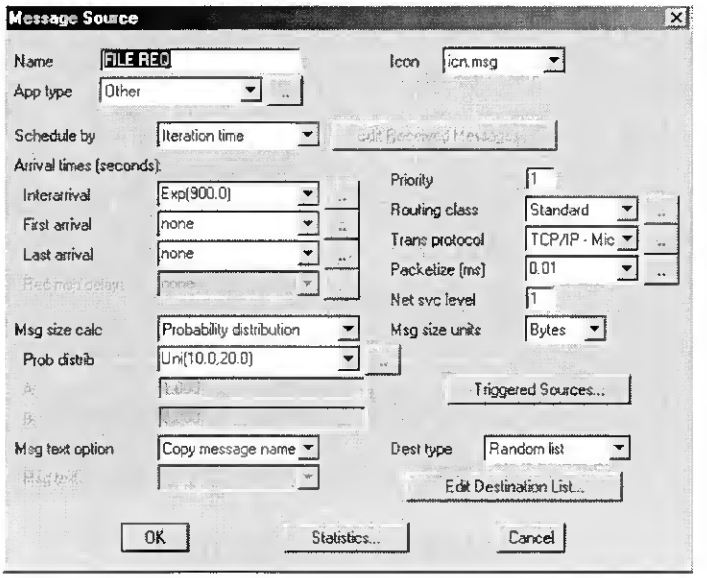


Ilustração 67 - FILE REQ

A parametrização desta *message source* teve em consideração os seguintes dados relativos às características da rede que nos propomos simular. O campo *Interarrival* que corresponde ao pedido de ficheiros é descrito por uma Distribuição Exponencial com Média em 900 segundos. Por outro lado cada pedido tem um tamanho de mensagem (*Msg size calc*) definido de acordo com uma Distribuição Uniforme com tamanho entre 10 e 20 bytes e todas as solicitações de ficheiros (*Dest type / Random list*) são enviadas, exclusivamente, ao FILE SERVER.

D. **Web Request**

Estes objecto é usado para modelizar os pedidos http para a visualização de páginas WEB. A sua parametrização é a exibida na figura (Ilustração 68).

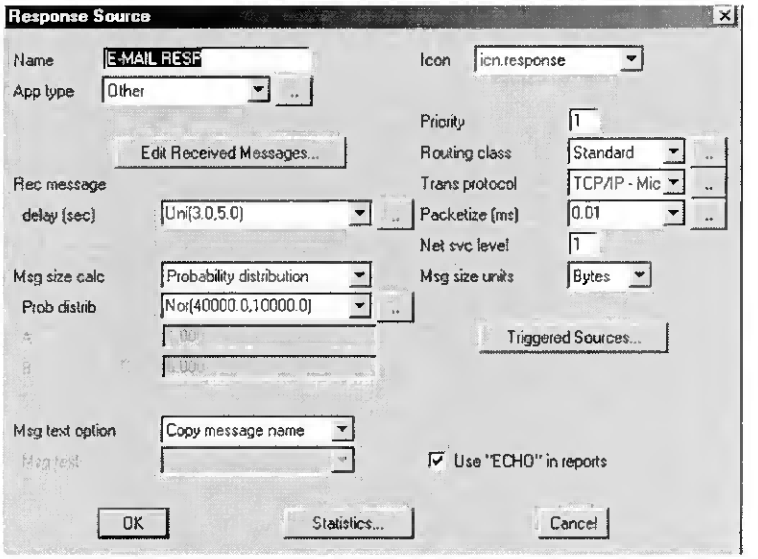


Ilustração 69 - E-MAIL RESP

A parametrização desta *response source* teve em consideração os seguintes dados relativos às características da rede que nos propomos simular. No campo *Edit Received Messages* foi criada uma lista de modo que a recepção de uma mensagem "E-MAIL CHECK" activará a fonte. Por outro lado, após receber um pedido para download, o servidor de e-mail irá ler os ficheiros correspondentes ao utilizador e enviar as mensagens para o seu computador. O tempo necessário para esta operação (*delay* (sec)) pode ser descrita através de uma Distribuição Uniforme compreendida entre 3 a 5 segundos. Relativamente ao tamanho das mensagens de mail (*Msg size calc*) transmitidas pelo servidor, pode ser descrito através de uma Distribuição Normal com média em 40 000 bytes e desvio padrão de 10 000 bytes.

B. File Resp

Este objecto é usados para modelizar o envio de ficheiros, provenientes do FILE SERVER, através da rede após receber uma solicitação para os mesmos. A sua parametrização é a exibida na figura (Ilustração 70).

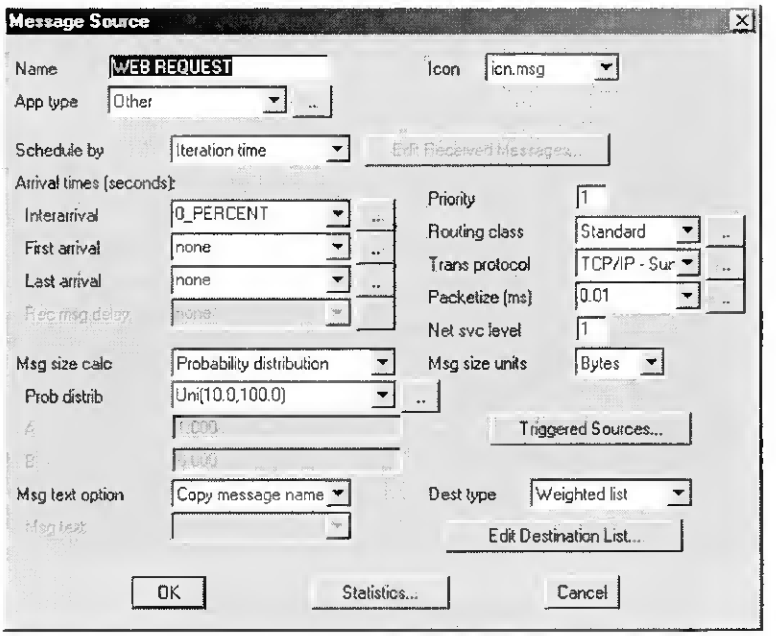


Ilustração 68 - WEB REQUEST

Antes da sua criação tivemos que definir a distribuição que permite modelizar o tempo entre chegadas dos pedidos http. Para tal adicionamos uma nova distribuição (*User Distributions*) denominada: O_PERCENT com base numa Distribuição Normal com Média em 31.8 segundos e Desvio Padrão em 3.8 segundos.

A parametrização desta *message source* teve em consideração os seguintes dados relativos às características da rede que nos propomos simular. No campo *Interarrival* foi indicada a distribuição à qual os pedidos obedecem (O_PERCENT), o tamanho das mensagens correspondentes aos pedidos (*Msg size calc*) foram definidos de acordo com uma Distribuição Uniforme com Mínimo em 10 bytes e Máximo em 100 bytes e, por fim, o destinatário das mensagens foi definido (*Dest type/Weighted list*) como sendo exclusivamente o servidor INTERNET.

DEFINIÇÃO DAS FONTES DE RESPOSTA E-MAIL / FILE REQ

Estes objectos irão gerar respostas e respectiva carga associada na rede e irão ser criados recorrendo a *Response Sources*.

A. E-Mail Resp / E-Mail Resp_Out

Estes objectos são usados para modelizar o *download* e transporte de tráfego de e-mail proveniente dos nós E-MAIL SERVER da rede interna e o E-MAIL SERVER_OUT da rede externa. A sua parametrização é idêntica e é a exibida na figura (Ilustração 69).

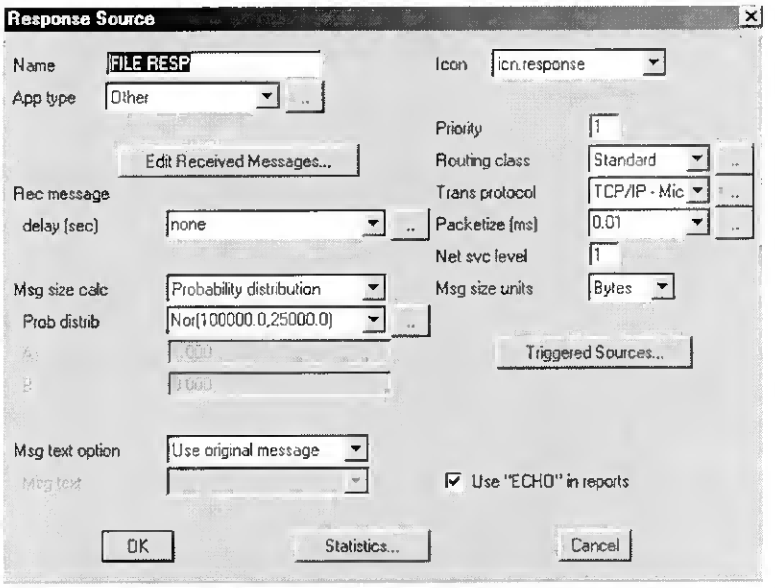


Ilustração 70 - FILE RESP

A parametrização desta *response source* teve em consideração os seguintes dados relativos às características da rede que nos propomos simular. No campo *Edit Received Messages* foi criada uma lista de modo que a recepção de uma mensagem "FILE REQ" activará a fonte. Por outro lado, o tamanho dos ficheiros a serem transferidos pode ser descrito por uma Distribuição Normal com média em 100 000 bytes e desvio padrão em 25 000 bytes.

DEFINIÇÃO DA RESPOSTA WEB RESPONSE

Este objecto irá gerar respostas a pedidos http e respectiva carga associada na rede e irá ser criados recorrendo a *Application Source*.

A. Criação da tabela WEB_READ

Em primeiro lugar tivemos que criar a tabela de distribuição (WEB_READ), usada pelo comando Read, para modelizar o número de bytes lidos após receber uma mensagem de WEB REQUEST. A sua representação gráfica é a exibida na figura (Ilustração 71).

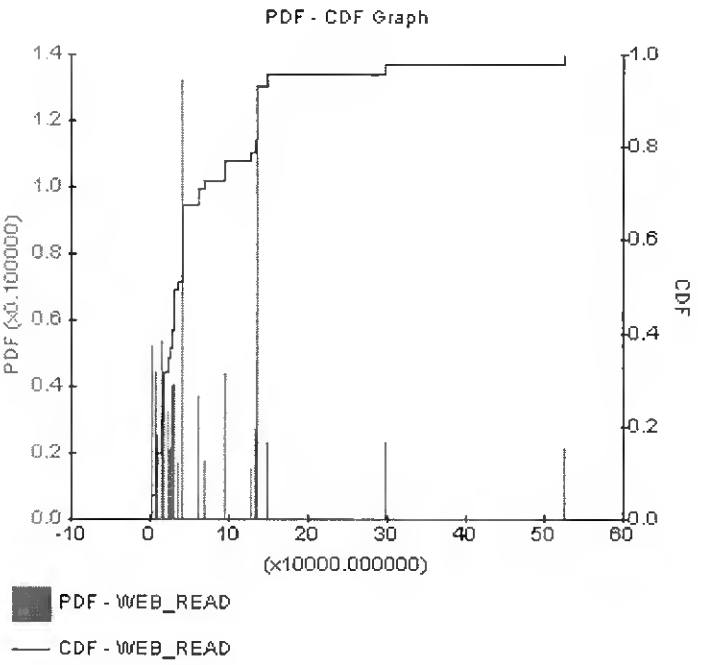


Ilustração 71 - Distribuição de probabilidades do nº de bytes lidos

B. Criação da aplicação Read Command

Este comando será usado na WEB_RESPONSE para executar a leitura do disco local no nó INTERNET. Para tal vamos alterar os comandos executados pelo servidor de acordo com o exibido na figura (Ilustração 72). De referir que este comando é baseado na distribuição de probabilidades anteriormente definida (WEB_READ).

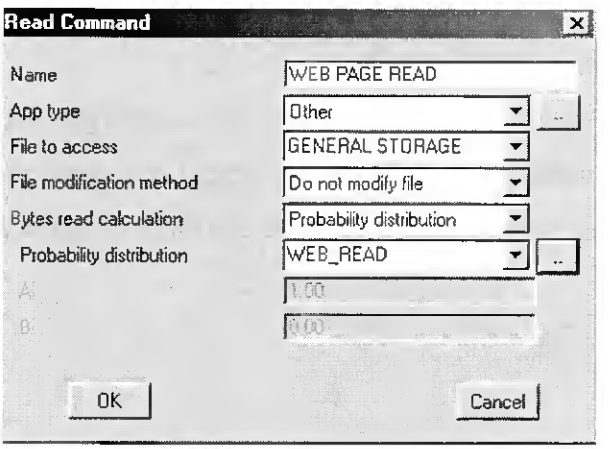


Ilustração 72 - Comando READ

C. Criação da aplicação Answer Command

Este comando será usado na aplicação para modelizar a geração de mensagens que serão enviadas com base no ficheiro lido quando é usado o comando WEB PAGE READ. Para tal vamos criá-lo como comando global de acordo com o exibido na figura (Ilustração 73).

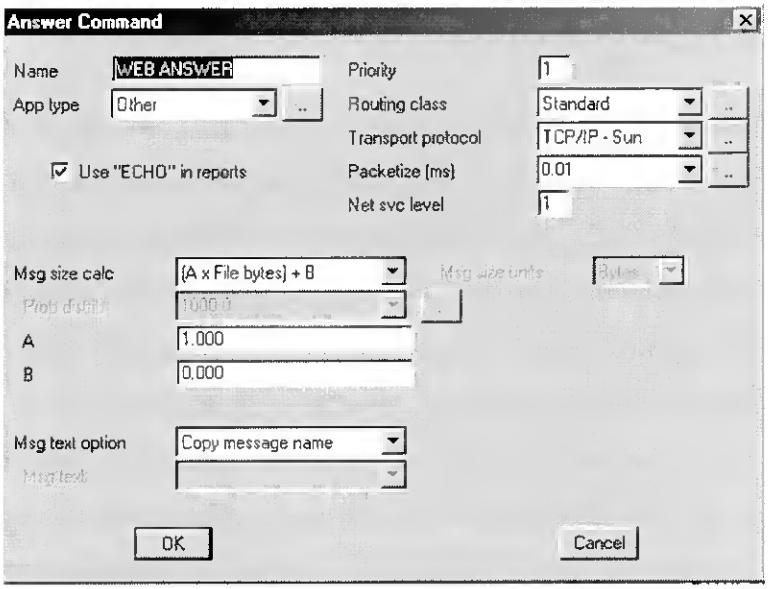


Ilustração 73 - Answer Command

D. Criação da aplicação WEB RESPOSTE

Esta *application source* usará os comandos previamente criados para modelizar o processo que tem lugar no servidor INTERNET após receber um pedido http. Para tal foi parametrizada de acordo com o exibido na figura (Ilustração 74).

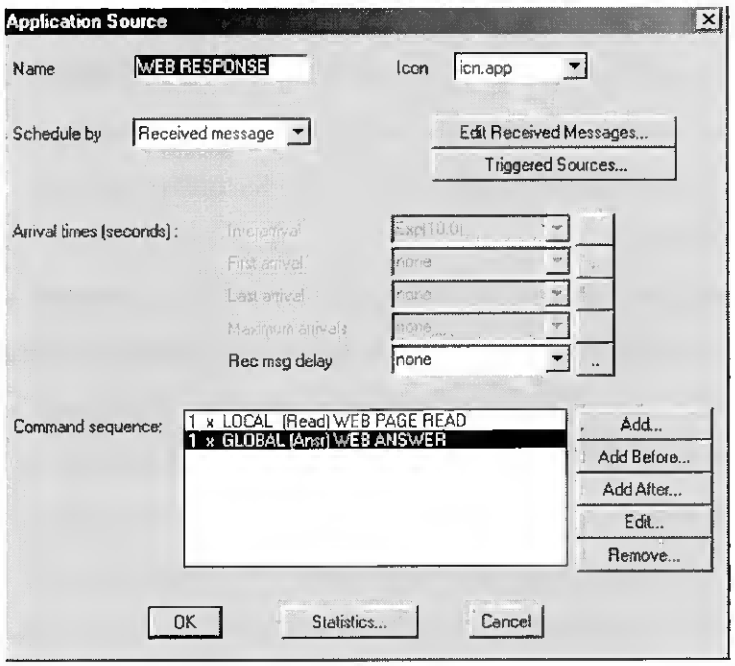


Ilustração 74 - WEB RESPONSE

Foram adicionados os comando que permitem ler a página WEB e responder ao solicitado. Esta fonte é desencadeada pela recepção de uma mensagem WEB REQUEST.

VII.2.4. Modelização do link IEEE 802.11

A rede que é objecto do nosso estudo foi modelizada usando um link do tipo CSMA/CA que é um mecanismo de acesso a um meio partilhado, que determina quando é que uma estação pode transmitir, decisão que cabe individualmente às estações podendo resultar em várias transmissões simultaneamente. Ou seja é usado *shared medium access mechanism* baseado na função DCF (*Distributed Coordination Function*) da norma IEEE 802.11 WLAN [35].

No cenário da rede em estudo foi assumido o pressuposto de que o controle de acesso ao meio apenas se irá basear nesta função implementada segundo o método de acesso básico (tramas ACK). Assim, não será usado o mecanismo adicional, que visa combater o efeito do terminal oculto, conhecido como RTS/CTS, porque assumimos um cenário de rede completamente conectada, ou seja todas as estações conseguirão comunicar entre si. O procedimento base para aceder ao meio partilhado será descrito posteriormente.

Em secção apropriada desta dissertação justificámos a utilização do protocolo CSMA/CA como método de acesso ao meio nas WLANs. Esta pretende-se sobretudo com a incapacidade de uma estação para escutar e enviar ao mesmo tempo, dado que a antena destinada a emitir e receber é única, e daí que a detecção de colisões, técnica frequentemente usada nas redes cabladas, se tornasse impraticável. Assim, CSMA/CA foi concebido com o intuito de reduzir, em vez de eliminar a probabilidade de ocorrência de colisões entre múltiplas estações que estejam a aceder ao meio, a um ponto onde estas deverão mais provavelmente ter lugar.

De relevo relativamente à performance da rede, a qual nos propomos estudar, é o facto de numa WLAN a camada MAC ser especifica, contrariamente às outras camadas que são idênticas às de outras redes IEEE 802, podendo apenas existir termos comuns com camada MAC da rede Ethernet (802.3) pelo facto desta suportar múltiplos utilizadores num meio partilhado, tendo o emissor que sentir o meio antes de aceder ao mesmo. Contudo, atendendo ao modo como esta função é implementada num meio sem fios poderá acrescentar algum *overhead* à rede 802.11, o que não acontece na rede 802.3, e assim uma WLAN 802.11 terá sempre performance inferior à da sua equivalente Ethernet [29].

Em termos gerais o funcionamento do protocolo CSMA/CA consiste em cada estação, que pretenda transmitir, primeiro irá sentir o meio através dos mecanismos, físicos e virtuais para o efeito, de modo a determinar se este está livre ou a ser usado por outra estação. Se o resultado desta análise for um meio livre a transmissão pode ter início. Por outro lado, o *distributed algorithm* da norma 802.11, determina que terá que existir um intervalo de

duração mínima especificada (DIFS, *Distributed Inter Frame Space*) entre a transmissão de tramas contíguas. Assim a estação emissora garante que o meio fica livre durante DIFS antes de tentar transmitir. Se, pelo contrário, o meio for detectado como ocupado a estação difere a transmissão até à finalização da que está a decorrer. Após este adiamento, ou antes de tentar transmitir novamente após uma transmissão de sucesso, a estação selecciona um intervalo de duração aleatória (*random backoff interval*) e diminui o contador (*backoff interval counter*) durante o tempo em que o meio estiver livre. Quando este contador atingir o valor zero a estação prossegue com a transmissão dos seus dados.

Na rede em estudo a modelização do link WLAN 802.11 foi efectuada de acordo com o mecanismo de acesso ao meio partilhado (*Shared Medium Access Mechanism*) baseado na função DCF (*Distributed Coordination Function*) definida segundo as normas IEEE Std 802.11, 1999 Edition [35], revisão do IEEE Std 802.11-1997 e IEEE Std 802.11b-1999 Part 11: Higher-Speed Physical Layer aprovada em 16 de Setembro de 1999 [36]. Esta norma dita que as comunicações sejam feitas na banda ISM de 2.4 GHz, com velocidade de transmissão de até 11 Mbps e usem modulação DSSS.

A parametrização do link será feita por meio da atribuição de valores ou estabelecidos pela norma, dependentes de características estáticas da camada física DSSS fornecidos pelas primitivas de serviço PLME-CHARACTERISTICS e das características especificas da camada MAC ou outros, os quais serão o alvo da nossa simulação. Os parâmetros simulados foram seleccionados de acordo com a sua sensibilidade relativamente ao *throughput* da rede em relação ao objectivo do nosso estudo. Assim definimos:

BANDWIDTH: Este parâmetro define a taxa de dados (*bit rate*) suportada pela camada física em particular. A norma IEEE 802.11b define este **valor como 11 Mbps, embora suporte as velocidades de transmissão adicionais de 5.5, 2 e 1 Mbps**. Este é o caso de uma camada física que possuí capacidade para transferência de dados a múltiplas taxas, permitindo que as implementações executem comutação dinâmica com o objectivo de melhorar a performance. O algoritmo para efectuar a mudança vai para além do âmbito da norma 802.11.

PROPAGATION: Este parâmetro, que é fixo para a camada física em particular, especifica o tempo de propagação, através do ar, que o sinal transmitido demora a ir da estação origem para a estação destino. Para a camada física DSSS *High Speed* (IEEE 802.11b) **este valor é de 1 microsegundo** [36].

SLOT TIME: Este valor, que é fixo para cada camada física em particular, é definido genericamente como o tempo nominal, em microsegundos, que as camadas MAC e física

exigem para receber o último símbolo de uma trama, processar a trama e responder enviando, o mais cedo possível, o primeiro símbolo da trama resposta. Para a camada física DSSS *High Speed* (IEEE 802.11b) **este valor é de 20 microsegundos** [pag 29]. Para além disso irá, também, ser usado para definir os intervalos SIFS, DIFS e para actualizar o *backoff interval* no algoritmo de acesso ao meio partilhado. A fórmula de cálculo é especificada na norma [36].

O caso particular do método de acesso que vamos implementar, DCF, por razões inerentes à sua eficiência usa uma escala de tempo discreto (*discrete time backoff*), pelo que o tempo imediatamente após um intervalo DIFS desocupado é dividido em slots e apenas é permitido a uma estação transmitir no início de cada slot time. Assim, o slot time é definido como o tempo necessário para que qualquer estação consiga detectar a transmissão de um pacote por qualquer outra.

O slot time é tido em conta no calculo do *propagation delay*, do tempo necessário para uma estação mudar do estado de recepção para o de emissão (Rx-Tx-SwitchTime) e do tempo necessário para a camada MAC assinalar o estado do canal.

De referir que, no COMNET, este valor pode ser definido de acordo com as especificações dos fabricantes dos diversos produtos que se pretendam modelizar.

SIFS: Genericamente IFS é definido como o intervalo de tempo entre tramas que permite associar diferentes prioridades no acesso ao meio sem fios. Os vários IFS deverão ser definidos como intervalos de tempo no meio e fixos para cada camada física, mesmo para as que permitam múltiplas taxas, que é o caso da camada física DSSS *Higher Speed* que vamos simular.

No caso particular do intervalo SIFS é definido como o tempo, em microsegundos, que decorrerá desde o fim do último símbolo da trama prévia até ao início do primeiro símbolo do preâmbulo da trama seguinte que ocorrer no meio e é usado para fornecer um mecanismo eficiente de entrega de MSDUs. SIFS corresponde ao menor dos intervalos entre tramas definidos pela norma 802.11, fixo para cada camada física em particular, e no caso de DSSS *High Speed* é **10 microsegundos** [36]. A fórmula de cálculo é especificada na norma [pag 85], depende do *slot time* e o seu valor entra no cálculo dos outros intervalos entre tramas de acordo com: **PIFS=SIFS + SlotTime e DIFS=SIFS + 2*SlotTime**.

Em termos práticos, este intervalo deve ser usado quando uma estação ganhou o acesso ao meio e necessita de o conservar durante a sequência de troca da trama em curso. Uma vez que o meio seja capturado, a estação retira este valor da duração da troca de tramas que estiver a efectuar devendo ser usado, no modelo em estudo DCF, pelas tramas ACK e pelo

segundo MPDU ou pelos seguinte de uma rajada de fragmentos se simular-mos a existência de fragmentação. Em suma o intervalo SIFS é usado pelas trama ACK e entre fragmentos de um MSDU (fragmentos pertencente à mesma trama) e as respectivas tramas ACK. Esta utilização é justificada pelo facto prevenir que outras estações, às quais foi pedido que aguardem que o meio fique livre durante um intervalo superior (DIFS), tentem usar o meio dando, deste modo, prioridade à finalização da transmissão da trama em curso.

Por outro lado, o valor de SIFS é também usado para calcular o intervalo DIFS, como anteriormente referido, usado pelo protocolo CSMA/CA para competir pelo acesso ao canal na transmissão inicial de tramas. Este intervalo deve ser usado pelas estações a operar no modo DCF para transmitirem as tramas de dados (MPDUs) e as tramas de gestão (MMPDUs). No método que será alvo da nossa simulação, DCF implementado segundo o método de acesso básico, é permitido a uma estação transmitir caso se detecte que o meio fica livre durante, pelo menos, um intervalo DIFS e o seu *backoff time* tenha expirado. Assim, uma estação com pacotes para transmitir irá monitorar a actividade no canal e se detectar o meio estiver livre durante um período de tempo igual a DIFS então ela transmite. Se o meio estiver ocupado (imediatamente após ou durante DIFS), a estação continuará a monitorar o canal até que este seja detectado como livre durante um intervalo DIFS. Nessa altura a estação gera um *random backoff interval* antes de transmitir (característica *Colission Avoidance* do protocolo) de modo a minimizar a probabilidade de colisão com tramas que tenham, entretanto, sido começados a enviar por outra estação. Adicionalmente, para evitar o efeito de captura do canal, a estação deverá esperar um *random backoff time* entre duas transmissões consecutivas de tramas diferentes, mesmo que o meio tenha sido sentido como livre durante um intervalo DIFS. Como excepção desta regra e unicamente no caso de fragmentação, técnica a que aludiremos posteriormente, os diferentes fragmentos de uma mesma trama são transmitidos sequencialmente com um intervalo SIFS entre eles e assim apenas o primeiro irá competir pelo acesso ao canal.

Outra importante consideração, que se prende com a definição de um intervalo SIFS, baseia-se no facto de que CSMA/CA não confiar na capacidade de uma estação para detectar uma colisão ao escutar a sua própria transmissão [28]. Assim uma trama ACK é transmitida após um intervalo SIFS, imediatamente depois do fim da trama, pela estação receptora para notificar a recepção com sucesso. Dado que este intervalo acrescido do tempo de propagação da trama ACK é menor que DIFS, nenhuma outra estação será capaz de detectar o canal livre durante um intervalo DIFS até ao fim da transmissão do ACK. Se por outro lado a estação emissora não receber a trama ACK durante um dado período (ACK *Timeout*) irá escalonar a

retransmissão do pacote de acordo com as regras de *backoff* definidas e que referiremos posteriormente.

De referir que no COMNET, este valor pode ser definido de acordo com as especificações dos fabricantes dos diversos produtos.

FRAME MAX: Este parâmetro é usado para especificar o tamanho máximo da trama (MSDU) que será aceite para transmissão. De referir que um MSDU, segundo a norma, é definido como a informação unitária que é trocada entre MAC *Service Access Points* (SAPs) para comunicação com as camadas superiores . Por outro lado, para o IEEE 802.11 o **tamanho do MSDU deve ser menor ou igual a 2304 bytes** [36].

Para operação em ambientes com elevados níveis de interferência, a qual limita o comprimento máximo das tramas transmitidas com sucesso, o protocolo fornece um mecanismo de fragmentação que permite à camada MAC dividir um MSDU (MAC Service Data Unit), pacote que lhe é entregue pelas camadas superiores, em vários MPDUs (MAC Protocol Data Unit), pacote entregue pela camada MAC à camada física, caso o seu tamanho exceda o valor máximo permitido para o MPDU, do qual falaremos posteriormente na parametrização de *Frgmt Thrshld*. Em suma, este processo cria MPDUs menores que a trama MSDU e a sua aplicação visa aumentar a fiabilidade, pelo aumento da probabilidade de transmissão com sucesso da trama MSDU, especialmente no caso em que as características do canal limitem a fiabilidade da transmissão de tramas longas.

FRAME OH: Este parâmetro corresponde ao *overhead* associado à transmissão de uma trama, que é composto pelo cabeçalho MAC 802.11, um FCS de 32 bits e uma chave partilhada para autenticação de 8 bits. No caso de fragmentação esta é também a sobrecarga associada à transmissão de um fragmento.

Para definir este valor tomemos como exemplo a trama de dados da camada MAC (MPDU) cujo formato é independente do subtipo. Assim esta apresenta, como ovherhead, um cabeçalho de 30 bytes, um FCS de 4 bytes e a norma diz que o corpo da trama são, no máximo, 2312 bytes dos quais 2304 correspondem ao tamanho máximo permitido para o MSDU e os restantes (8) correspondem a campos WEP [36]. Assim consideraremos **um *overhead*, associado à transmissão de uma trama, de 42 bytes** (30+4+8).

FRGMT THRSHLD: Este parâmetro especifica o tamanho máximo, em octetos, do MPDU que será entregue à camada física caso tenha sido usada fragmentação. O valor por defeito é definido igual ao tamanho máximo da trama (MSDU / 2304) e nesse caso não existirá fragmentação. Caso contrário, quando for recebida uma trama MSDU com tamanho superior ao especificado neste parâmetros esta será fragmentada. Este visa simular a característica

adaptativa da fragmentação para permir a escolha do tamanho do fragmento de acordo com as condições do canal de transmissão em particula.

A fragmentação definida como o processo de divisão de um MSDU (MAC *Service Data Unit*), trama recebida da camada LLC, ou MMPDU (MAC *Mangement Protocol Data Unit*), trama recebida da camada MAC / MLME, em tramas de nível MAC denominadas MPDUs (MAC *Protocol Data Unit*), criando MPDUs menores que o MSDU original. A sua finalidade é aumentar a fiabilidade, através do aumento da probabilidade de transmissão com sucesso de um MSDU ou MMPDU, nos casos onde as características do canal limitem a fiabilidade de recepção de tramas grandes [35], por outro lado a camada MAC pode directamente fragmentar e reconstruir MSDUs e MMPDUs. Cada fragmento resultante é uma trama de tamanho menor ou igual ao valor indicado para este parâmetro, *fragmentation thershold*, que define o número de octetos de um fragmento, mas nunca superior a menos que o MPDU use WEP. Todos os fragmentos MPDU devem ser iguais, ter o mesmo número par de octetos, excepto o último que poderá ser menor e ser par ou ímpar.

Os MPDUs resultantes da fragmentação são enviados como transmissões independentes, cada uma com uma das quais com ACK separado, o que permite que as retransmissões, caso se justifiquem, ocorram por fragmento em vez de por MSDU ou MMPDU. A menos que por interrupções devidas a limitações, para cada camada física em particular, de ocupação do meio os fragmentos de um MSDU serão enviados em rajada durante o período com contenção, usando uma única invocação do método de acesso ao meio DCF com base no protocolo CSMA/CA. Em suma, uma vez que uma estação tenha competido pelo acesso ao canal continuará a enviar fragmentos (usando SIFS em vez de DIFS) até que a totalidade do MSDU tenha sido enviado ou então não tenha sido recebida uma trama ACK directa devido a uma possível colisão ou outro erro de transmissão. Se por qualquer uma destas razões, ou outras não consideradas, o envio de fragmentos tiver que ser interrompido estes entrarão num período de retransmissão denominado *retransmission backoff period* e quando surgir a próxima oportunidade a estação retomará o processo enviando os restantes fragmentos da trama. A estação emissora deverá manter um relógio de transmissão (*Transmit MSDU Timer*) para cada MSDU a ser transmitido, processo de que falaremos em mais pormenor no parâmetro *Frame TxLife Time*.

O processo inverso que consiste em recombinar vários MPDUs num único MSDU ou MMPU, denominado desfragmentação, é executado em cada receptor imediatamente após recepção, por meio da informação contida em cada fragmento e que permite reconstruir o MSDU ou MMPDU.

De referir que apenas os MPDUs com um único endereço receptor (*unicast*) deverão ser fragmentados, todas as outras tramas não deverão ser fragmentadas mesmo que o seu tamanho exceda o valor referido neste parâmetro.

Na simulação não vamos considerar existência de fragmentação porque o tráfego não gera tramas longas.

FRGMT ERROR PROB: Este parâmetro especifica a taxa de erro que pode ser associada à transmissão de um fragmento ou trama, caso não exista fragmentação, através do meio físico. O pressuposto de probabilidade de colisão constante e independente de uma trama transmitida por uma estação, conduz a resultados extremamente precisos, praticamente exactos, caso o número de estações na rede seja grande, maior ou igual a 10 [28]. Este será um pressuposto que vamos modelizar através da execução de simulação sem e com probabilidade de erros.

ACK TIMEOUT: Este parâmetro especifica o intervalo de tempo durante o qual o reconhecimento de uma trama enviada (ACK), que o exija, deve ser recebido como resposta e não deverá ser inferior a: **(2 * *Propagation* + *SIFS* + *ACK Transmission Time*)** [30].

Este período é contado a partir do momento em que a estação emissora termina o envio da trama ou fragmento. Assim, na simulação calculamos o tempo de transmissão de uma trama ACK, de 14 bytes a 11 Mbps ($8*14 / 11 * 10^6$), como 0.01 ms **pelo que este parâmetro nunca poderá ser inferior a 0.022 ms** (2*0.001+0.01+0.01). Assim considerámos o valor de **0.023 ms**.

Modo geral, o reconhecimento é apenas exigido após a recepção de trama ou fragmento, caso seja necessário o uso de fragmentação, directo (*unicast* / lançamento único) e assim a estação destino responde com uma trama ACK se a recepção da trama ou fragmento for correcta. A ausência de um ACK esperado indica à estação origem que ocorreu um erro e faz com que esta proceda à retransmissão da trama ou fragmento para o qual não houve reconhecimento, operação que só pode ser tentada um número de vezes pré-definido. A estação origem aguarda pela trama ACK este intervalo de tempo pré-definido. Por outro lado, a recepção de uma trama ACK com erro é, também, motivo para retransmissão.

A transmissão da trama ACK, como anteriormente referido, tem início após o intervalo de mais alta prioridade SIFS sem observar o estado do meio (livre ou ocupado), para garantir que esta seja transmitida sem ter que competir pelo acesso ao canal, sendo este o mecanismo que exige a existência de prioridades no acesso ao meio. A estação emissora deverá aguardar durante o período de tempo especificado neste parâmetro, sem receber um ACK, antes de concluir que a trama falhou.

ACK ERROR PROB: Este parâmetro especifica a taxa de erro de transmissão de uma trama ACK pelo meio físico cujo tamanho, segundo a norma 802.11, são 14 bytes.

Na simulação vamos considerar cenários sem e com existência de erros.

FRAME TXLIFE TIME: Este parâmetro (*Frame Transmission Life Time*) é definido como o tempo que deve decorrer após a transmissão inicial de um MSDU, ao fim do qual tentativas de retransmissão posteriores do mesmo terminarão, ou seja especifica a quantidade máxima de tempo permitido para transmitir um MSDU. Como tal este parâmetro é definido por trama e não por fragmento. Na simulação definimos este parâmetro tendo em conta a norma 802.11 que recomenda que o valor escolhido para este parâmetro seja suficientemente grande de modo a que o MSDU não seja descartado devidos a excessivos *timeouts*, sob condições normais de operação e sugere o valor de **512 ms** [35].

O seu funcionamento recorre a um relógio que é inicializado na tentativa de transmissão do primeiro fragmento do MSDU e é incrementado para cada fragmento posterior. Se, e quando, este exceder o valor definido para o parâmetro então todas as tramas restantes serão descartadas, pela estação emissora, e não será realizada mais nenhuma tentativa para completar a transmissão do MSDU.

FH DWELL TIME: Este parâmetro é específico para a camada física FHSS, que não é o caso do exemplo em estudo.

No modelo CSMA/CA, caso em estudo, este parâmetro é usado para determinar se a estação pode deter o controle do canal durante o processo de transmissão de fragmentos de um MSDU e durante quanto tempo. Uma vez que este seja excedido (*dwell boundary*) a trama terá que entrar, novamente, num período de *backoff* e voltar a competir pelo acesso ao canal. **Na simulação considerou-se um tempo de retenção do canal grande de modo a garantir o envio de toda a trama MSDU, 1 0000000 ms**.

RETRY INTERVAL: O conjunto de opções para a definição do tempo ao fim do qual deve ocorrer uma nova tentativa de transmissão, caso uma estação que pretenda iniciar a transferência de dados encontre um meio ocupado, pode ter por base uma distribuição de probabilidades ou um algoritmo de recuo (*backoff random interval*, *backoff interval*).

Na simulação optámos pela segunda alternativa implementada com base na norma 802.11 e no método básico de acesso ao meio (DCF), o qual permite a sua partilha automática, entre camadas físicas compatíveis, através do uso de CSMA/CA e de um *random backoff time* a seguir a uma condição de meio ocupado. Adicionalmente, todo o tráfego directo usa reconhecimentos positivos imediatos (ACK), não tendo sido considerada a existência de reserva do meio através de tramas RTS/CTS. Justificámos a nossa opção porque, segundo a

norma, esta apenas deve ser usada, por uma estação para tramas directas, quando o tamanho do MPDU for maior que um dado limite, indicado pelo parâmetro RTSThreshold (normalmente 3000 bytes) o que não se verifica na rede que estamos a simular.

O protocolo CSMA/CA pretende reduzir a probabilidade de colisões entre as múltiplas estações da nossa rede ad hoc, que estejam a tentar aceder ao meio, ao ponto onde estas terão mais probabilidade de ocorrer, ou seja exactamente após o meio ter ficado livre depois de um período de ocupação. Isto acontece porque muitas estações poderão ter estado a aguardar que o meio fique livre. Assim, uma estação que pretenda transmitir segue o procedimento de *random backoff*, que resolve os conflitos de contenção pelo meio, executado com base em mecanismos que permitam sentir o meio (*Carrier Sense*) e evitar colisões (*Collision Avoidance*). Se o meio estiver ocupado a estação deve adiar a transmissão até que o mesmo seja determinado como livre por um período, sem interrupções, de duração igual a DIFS ou EIFS após a última trama detectada no meio ter sido correctamente recebida. Após este período livre a estação deverá então gerar um intervalo de tempo aleatório atraso do recuo (*random bachoff period*) para um adiamento adicional antes de transmitir, a menos que o contador *backoff timer* já contenha um valor diferente de zero e neste caso a selecção de um número aleatório já não é executada porque não é necessário. Este processo minimiza colisões durante a contenção, entre múltiplas estações que tenham deferido o mesmo evento e, ao contrário da rede Ethernet, é controlado por detecção de actividade no canal. Uma estação tem um número de tentativas de transmissão restrito e caso tente transmitir e detecte o canal como ocupado defere a transmissão, contabilizando esta tentativa como falhada. Estes deferimentos irão, como veremos, adicionar atrasos è rede afectando a sua performance de modo significativo.

A estação selecciona um *backoff time* com base na seguinte regra:

Backoff Time = Random() * Slot Time onde:

Random(): Número inteiro pseudoaleatório retirado de uma distribuição uniforme no intervalo [0,CW], onde CW (*Contention Window*) é um número inteiro escolhido de entre os valores definidos, de acordo com as características da camada física, para CW_{min} e CW_{max} e $CW_{min} <= CW <= CW_{max}$;

Slot Time: Valor especificado para este parâmetro de acordo com as características da camada física.

Na implementação específica do método de acesso básico, DCF, é adoptado um mecanismo de *exponential backoff* [28]. Assim, em cada transmissão de uma trama o *backoff time* é escolhido de modo uniforme no intervalo (0,CW-1) onde CW (*Contention Window*) depende

do número de transmissões que falharam para a trama. Inicialmente o parâmetro CW assume o valor de CW_{min} para cada MSDU em fila transmissão. Posteriormente irá assumir o próximo valor na série, de cada vez que ocorra uma tentativa de transmissão sem sucesso de um MPDU em particular (retransmissão de um MPDU), até atingir o valor definido para CW_{max}. Após cada tentativa de transmissão com sucesso, de um MSDU ou MMPDU, o valor anterior deve ser apagado e CW volta a tomar o valor de CW_{min}. O conjunto de valores para CW deverão, assim, ser inteiros calculados de acordo com a seguinte regra: o valor inicial para CW, que designaremos por CW_1, será igual a CW_{min} e depois cada novo valor será $CW_n=(2*CW_{n-1})+1$, até que seja atingido o valor definido para CW_{max}. Assim, se uma transmissão tiver sucesso o valor de CW retoma o valor inicial antes que o *random backoff interval* seja escolhido, o que permite que as tramas transmitidas por uma estação sejam sempre separadas de, pelo menos, um *backoff interval* e não se verifique o efeito de captura.

Por seu lado, o *backoff time counter* ou *backoff timer* pode sofrer uma de três acções ser decrementado à medida que o canal é sentido como livre, congelado quando é detectada uma transmissão no canal e reactivado quando o canal voltar a ser sentido como livre, mais uma vez por um intervalo DIFS. A estação irá transmitir quando o contador atingir o valor zero. Este actualização ao *backoff timer* é processada do seguinte modo. Todos os períodos de *backoff* ocorrem a seguir a um intervalo DIFS, durante o qual o meio está livre. A estação em *backoff* monitorizará o meio para detectar actividade de portadora durante esses períodos. Se não for detectada actividade durante um determinado slot então o processo de *random backoff* irá decrementar o relógio pelo valor do parâmetro *slot time*. Se, pelo contrário, for detectada actividade em qualquer momento durante o período de *backoff* então o processo é suspenso; isto é, o *timer* não é decrementado pelo valor do slot time permanecendo constante (congelado). Para que o processo de *backoff* possa ser retomado o meio deverá ser sentido como livre, novamente, durante um intervalo DIFS. A transmissão terá início quando o *backoff timer* atingir o valor zero.

O efeito geral deste procedimento é que quando múltiplas estações estejam a adiar as suas transmissões e entrem num *random backoff*, ganhará a competição aquela que escolher o menor *backoff time*, usando a função aleatória. De referir, que uma estação que acabe de transmitir um MSDU e tenha outro pronto para ser enviado executará novamente o procedimento de *backoff* como forma de produzir justiça, entre estações, no acesso ao meio.

CONTENTION WINDOW MIN/MAX: Os valores que estes parâmetros podem tomar são fixos para a camada física em particular e são especificados pela norma 8020.11. **A camada física DSSS High Speed define-os como 31 e 1023 respectivamente** [36].

RETRY LIMIT: Este parâmetro indica o número máximo de retransmissões que podem ser tentadas para um fragmento. Após este limite ter sido atingido as tentativas de retransmissão deverão acabar, o mesmo será descartado e é passada uma condição de falha à camada superior.

A recuperação de erros, de acordo com a norma, é sempre da responsabilidade da estação que iníciou a sequência de troca de tramas e deverá ser implementada por retransmissão da sequência que incorreu em erro. O número de retransmissões, para cada sequência de troca de tramas, é limitada por uma de duas condições aquela que ocorrer primeiro. A primeira é o facto de a transmissão ter sido efectuada com sucesso e a segunda é que o valor definido neste parâmetro seja atingido. De referir que a recuperação de erros é apenas feita para transmissões directas. Assim, não existe recuperação de nível MAC em tramas *multicast* ou *broadcast*, excepto para um tipo específico das redes infraestruturadas que não são objecto da presente simulação, como tal a fiabilidade deste tipo de tráfego é reduzido relativamente à do tráfego directo, devido à probabilidade acrescida de perda de tramas causada por colisões, interferências ou propriedades do canal variáveis no tempo.

A norma 802.11 recomenda que o valor escolhido para este parâmetro seja 7 [35].

O conjunto de parâmetros base usados na presente simulação são os apresentados na tabela (Tabela 10). Sempre que existirem alterações, para dado cenário em particular, iremos referir a que parâmetros.

NOME	CAMADA DA QUAL DEPENDE	VALOR DEFINIDO PELA NORMA
N.° de Estações	Definido pelo user	15
Bandwidth (kbps)	PHY MIB	11 000
Propagation (ms)	PHY MIB	0.001
Slot time (ms)	PHY MIB	0.020
Short IFS (ms)	PHY MIB	0.010
Frame max (bytes)	PHY MIB	2304
Frame OH (bytes)	MAC MIB	42
Frgmt thrshld (bytes)	MAC MIB	2304 / 1023 / 576
Frmt Error Prob	Definido pelo user	0
Ack timeout (ms)	MAC MIB	0.022 (300/1000)
Ack error prob	Definido pelo user	0
Frame TxLife (ms)	MAC MIB	512 (5632)
FH dwell time (ms)	MAC MIB	1 0000000
Contention window min	PHY MIB	31
Contention window max	PHY MIB	1023
Retry limit	MAC MIB	7

Tabela 10 - Parâmetros usados na simulação

VII.2.5. Execução da simulação

A simulação é executada com base em parâmetros seleccionados, os quais irão determinar a forma como a mesma deve ser executada. Os principais são: o tempo (*Replication Length*), em segundos, durante o qual a simulação irá correr, que determina quantos eventos aleatórios são usados para representar o tráfego gerado e deste modo condiciona a precisão da simulação; o tempo de execução, em segundos, a partir do qual a aplicação iniciará a recolha de dados (*Warmup Length*); definição do número de replicações, ou seja quantas vezes é executa a simulação (*Number of Replication*); determinação se o tempo de *warmup* deve ser respeitado em cada réplica (*Warmup Every Replication*); definição se o tráfego de réplicas anteriores será apagado antes do início da próxima (*Reset System Every Replication*); definição se as estatísticas deverão, ou não, ser enviadas para um ficheiro próprio (*Export Stats After Run*) e se os percentis deverão ser incluídos nas estatísticas exportadas (*Include*

Percentils in Export). Na nossa simulação foram usados os valores exibidos na figura (Ilustração 75)

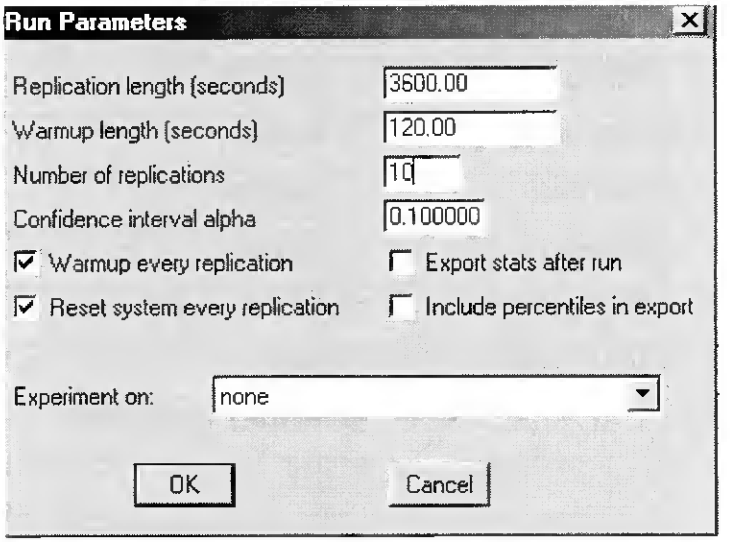


Ilustração 75 - Valores da simulação

Outro conjunto de opções que podemos activar tem a ver com a animação. Assim, se pretendemos visualizar no écran, durante a simulação, o movimento dos pacotes à medida que são passados na rede (*Animate Packet Flow*), podemos fazê-lo. De referir que este processo sobrecarrega de modo considerável a execução podendo ter implicações ao nível da recolha de resultados, motivo pelo qual não o fizemos. Por outro lado, podemos definir a velocidade à qual os pacote atravessarão a topologia da rede de dois modos: lento (10) ou rápido (100).

Como referimos anteriormente, o COMNET usa simulação de eventos discretos quando é executada a simulação do modelo da rede, o que significa que a aplicação observa o primeiro evento que ocorre com base no tráfego, descrito no modelo, e executa-o. Após completar a sua execução passa ao próximo evento da lista. Este processo repete-se até ao tempo total especificado para que a simulação correr.

O protocolo MAC irá desempenhar um papel relevante actuando como moderador no acesso ao meio partilhado de modo a que a limitada largura de banda do meio sem fios possa ser facilmente partilhada e utilizada de modo eficaz bem como o manuseamento do modo de operação *half duplex* da rede ad hoc. A simulação que iremos executar pretende analisar a performance de DCF sob os pressupostos de rede completamente conectada, isto é, sem terminais ocultos; todas as estações da rede operam em condições de saturação, isto é, possuírem sempre uma trama pronta para ser transmitida e número finito de estações.

Relativamente às condições do canal iremos simular o pressuposto de canal ideal, isto é, sem erros de transmissão e numa segunda fase simularemos a sua existência.

Na nossa simulação o tempo de execução foi de 3600 segundos, de modo a representar uma hora de tráfego na rede; a simulação começará a recolher dados após 120 segundos e foram corridas 10 réplicas. Em suma, executámos em cada cenário uma simulação que representa 10 horas de tráfego na rede.

VII.2.6. Análise dos resultados

A análise dos resultados é feita com base em relatórios representativos de estimativas da performance esperada para a rede real, medida nos diferentes elementos do modelo bem como características de rede totais. Estes são produzidos automaticamente no fim da execução de uma simulação ou mesmo quando esta termina por qualquer outra razão. Por defeito o *report* é gravado para um ficheiro ASCII denominado stat1.rpt. De referir que apenas são recolhidas estatísticas para os relatórios que tenham sido seleccionados antes de executada a simulação. O número de relatórios bem como dos objectos que os mesmos incluem irá afectar o tempo de execução. Outra forma adicional de análise são as estatísticas que podem ser activadas para alguns tipos de objectos. Assim, a aplicação permite recolher dados para, por exemplo, links, fontes de tráfego e outros e após executada a simulação estes podem ser exibidos na forma de *plots* que normalmente correspondem a dados, histogramas e percentis.

A precisão dos resultados, que é um factor de extrema importância, depende dos dados que foram introduzidos para descrever a rede. Assim, quanto mais precisos forem os dados consequentemente mais fiáveis as estimativas de performance. Outro factor, o qual determina a precisão, é o tempo de execução da simulação que corresponde ao tempo durante o qual o modelo é executado. Esta meta temporal determina quantos eventos aleatórios são usados para representar o trafego gerado estatisticamente.

Na nossa simulação irá ser avaliada a performance da rede em termos do protocolo de acesso ao meio. Existem diversas métricas quantitativas para o fazer, contudo as que iremos considerar são: utilização da rede, atrasos e erros.

Em primeiro lugar, analisaremos medidas de performance típicas como são o *throughput* e *delay* para mostrar a efectividade do protocolo. Modo geral o *throughput* (S) é definido como a fracção de tempo que o canal é usado para a transmissão com sucesso de uma dada quantidade de informação (Q = Quantidade de informação transmitida no tempo / T= Tempo

que a transmissão demorou ou seja o número de pacotes transmitidos / Tempo). No nosso estudo este valor é dado pela utilização média do canal em termos percentuais (*Link Utlizitation %*). Assim o *tempo de transmissão de uma trama* é calculado dividindo o tamanho da trama pela velocidade à qual o link opera e para cada trama o link é usado durante o tempo de transmissão mais o tempo de propagação (*propagation delay*). Do anterior é calculada a *percentagem de utilização média do link* como o somatório do tempo total em que o link foi usado sobre o tempo de execução da simulação. São ainda considerados factores como o número total de tramas transmitidas bem como pacotes, tamanho médio das tramas e velocidade dos pacotes (pacotes/segundo).

Em segundo lugar e relativamente ao link analisaremos a sua utilização em termos de largura de banda (*bandwidth*) de modo a ver quanto eficiente é o protocolo de acesso nomeadamente em relação aos episódios de colisão verificados, ao número de tramas que colidiram, ao número de retransmissões devidas a erros ou colisões (NBR TRIES TO RESOLVE), ao número de deferimentos de transmissão bem como a quantidade de tramas na fila. O atraso resultante é uma medida importante porque os tempos de resposta não devem ser longos de modo a que a produtividade dos utilizadores fique comprometida. Assim analisaremos o atraso relativa a transmissões (*transmission delay*), definido como o tempo entre o instante em que a trama é criada na entrada do link até que é entregue no final do link tendo em conta a ocorrência de colisões e a necessidade de retransmissão. Este inclui *transmission time*, *contention resolution time* e *propagation time*. Analisaremos, também, o atraso devido ao adiamento de transmissões pelo facto do meio se encontrar ocupado.

Outras medidas interessantes serão: Rácio do nº de bytes das tramas transmitidas / nº de bytes das tramas entregues, para medir a eficiência do protocolo e Rácio da quantidades de bits de dados transmitidos / bits de dados entregues, para mostrar a eficiência do *throughupt* de entrega de dados da rede.

A simulação executada pretende, essencialmente, analisar factores com a escalabilidade da rede, ou seja o que acontece se juntarmos mais utilizadores e o efeito da existência de erros nas transmissões. Para dar cumprimento ao primeiro objectivo executámos a simulação da rede, com a parametrização anteriormente descrita para o link IEEE 802.11, para cenários de 15, 30 e 45 utilizadores os quais designaremos, neste estudo, por **(1)**, **(3)** e **(5)** respectivamente. Posteriormente estudamos os efeitos causados pela introdução de erros.

Para todos os cenários vamos estudar a performance da rede com base nos seguintes tópicos: Utilização do canal e atrasos; Utilização do canal em termos de pacotes e velocidade; Tamanho das tramas e Performance do link IEEE 802.11.

UTILIZAÇÃO DO CANAL E ATRASOS

Fornece as taxas de utilização do link no transporte de mensagens. Com base no *plot* obtido após a execução da simulação (Ilustração 76), relativamente à utilização do canal ao longo do tempo de execução, podemos concluir que os resultados reflectem a forma aleatória de geração do tráfego, feito com base em distribuições, bem como a sua natureza por rajadas. Assim, ao analisar o gráfico verificamos que este exibe intervalos com utilizações de 100% e outros com utilização de 0%.

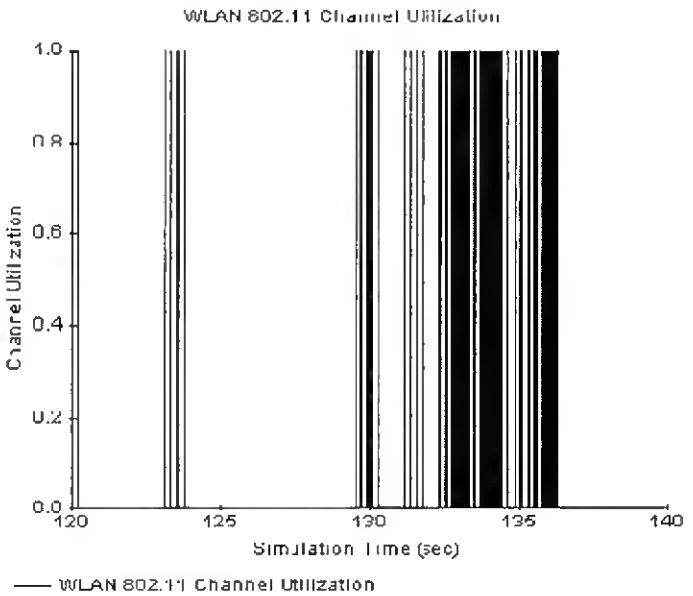


Ilustração 76 - Utlização do canal

Relativamente à utilização do canal em termos de número total de tramas entregues em cada um dos cenários, definimos como sendo o número de tramas de dados movidas do *buffer* de output de um nó emissor para o link e subsequentemente colocadas no *buffer* de input de um nó receptor. De referir que em todo o nosso estudo quando usarmos o termo trama estamos sempre e apenas a referir-nos a tramas do tipo dados, excepto se o contrário for explicitamente indicado. Assim, como seria de esperar, o número total de tramas entregues, que é exibido no gráfico (Gráfico 1), apresenta um crescimento linear com o aumento do número de utilizadores de 15 para 30 e para 45.

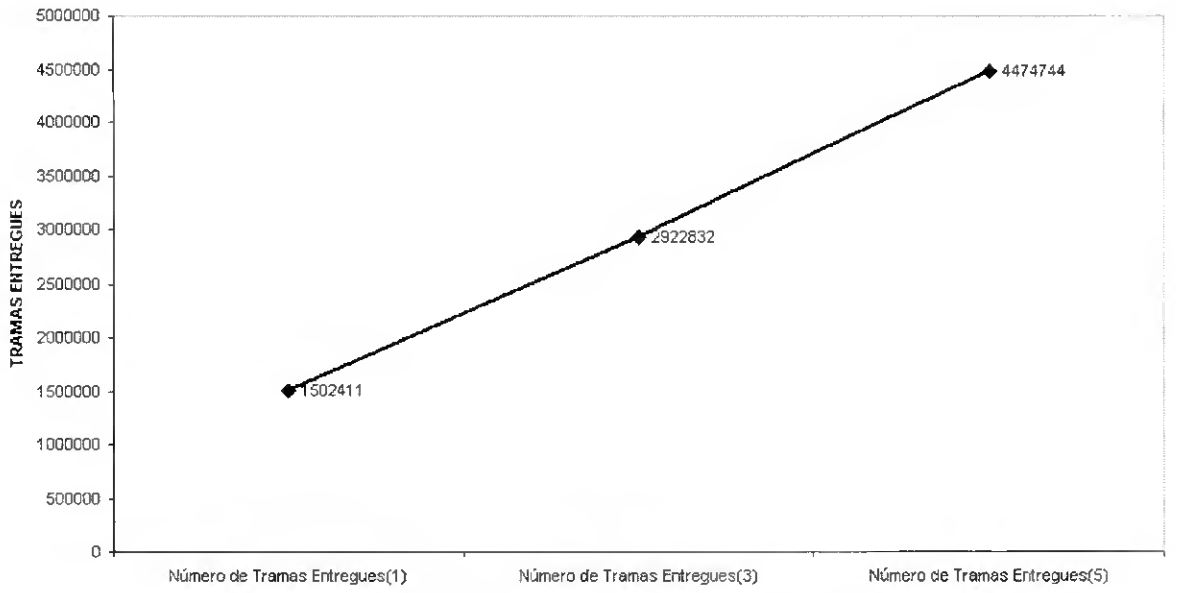


Gráfico 1 - Número de tramas entregues versus número de utilizadores

Relativamente ao número de tramas que atingem o número máximo de tentativas (*Retry Limit*) ou o tempo de vida útil (*Frame TxLife Time*) observamos para todos os cenário o valor zero, pelo que concluímos que estes dois parâmetros estão correctamente definidos porque não têm um impacto adverso na performance da rede.

Relativamente aos atrasos estes são os esperados face à variação que estamos a efectuar e que apenas tem em conta o aumento do número de utilizadores. Assim, será de esperar que o atraso aumente em função do número de utilizadores dado que a carga da rede aumenta. Este apresenta os valores da Tabela 11, relativos ao atraso médio e ao desvio padrão.

	Maior atraso Médio (ms)	**Menor atraso Médio (ms)**	**Média do atraso Médio (ms)**	**Desvio Padrão**
(1)	0.764	0.751	0.759	[54.9% 56.4%]
(3)	0.769	0.759	0.765	[56.6% 58.0%]
(5)	0.779	0.773	0.776	[58.2% 59.3%]

Tabela 11 – Atraso versus número de utilizadores

A representação gráfica (Gráfico 2) permite uma análise mais objectiva dos valores observados, da qual podemos concluir que a variação de 15 para 30 utilizadores não tem um efeito tão acentuado no atraso médio como de 30 para 45 utilizadores. Contudo, os valores apresentam uma tendência que não conduzirá a latência excessiva pelo que podemos concluir que a escalabilidade da rede não é posta em causa pelos atrasos de transmissão.

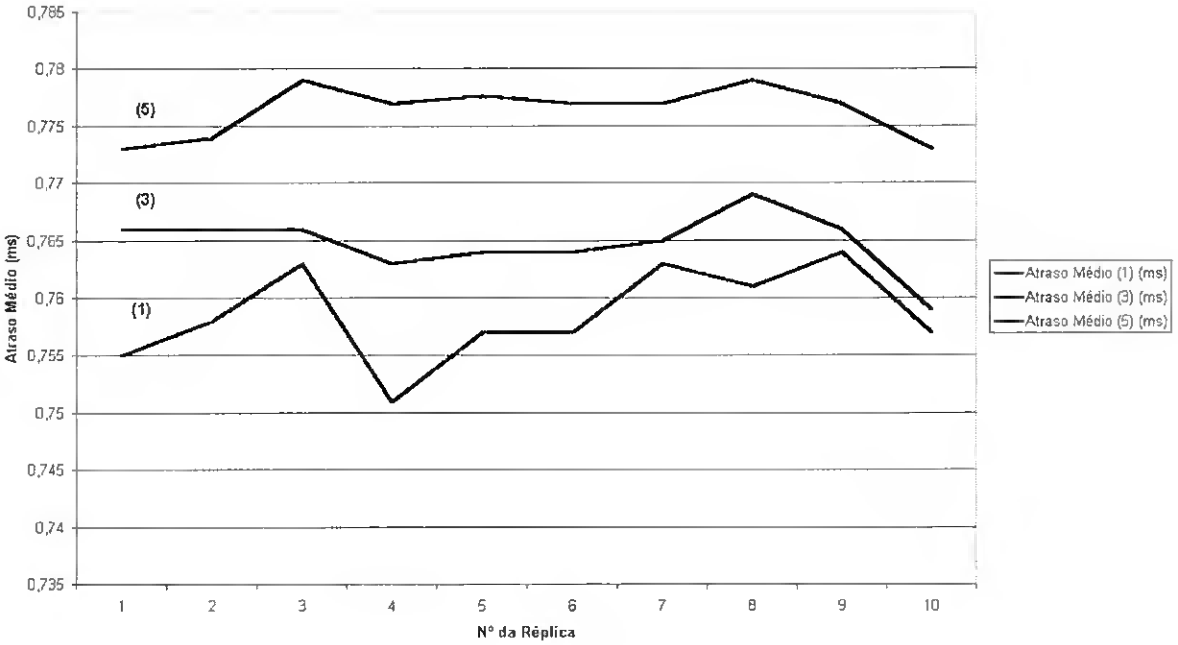


Gráfico 2 – Atraso médio versus número de utilizadores para 10 réplicas

De especial relevo é a variação dos atrasos máximos observados, descritos na Tabela 12, os quais corresponderão aos picos de maior utilização da rede para os vários cenários.

	Maior atraso Máximo (ms)	**Menor atraso Máximo (ms)**
(1)	18.646	7.59
(3)	19.714	11.078
(5)	25.639	12.047

Tabela 12 – Maior e menor atraso máximo versus número de utilizadores

Pela representação gráfica (Gráfico 3) dos mesmos podemos ver que no cenário **(5)** existem muitos mais picos onde a sobrecarga da rede é muito superior à dos outros.

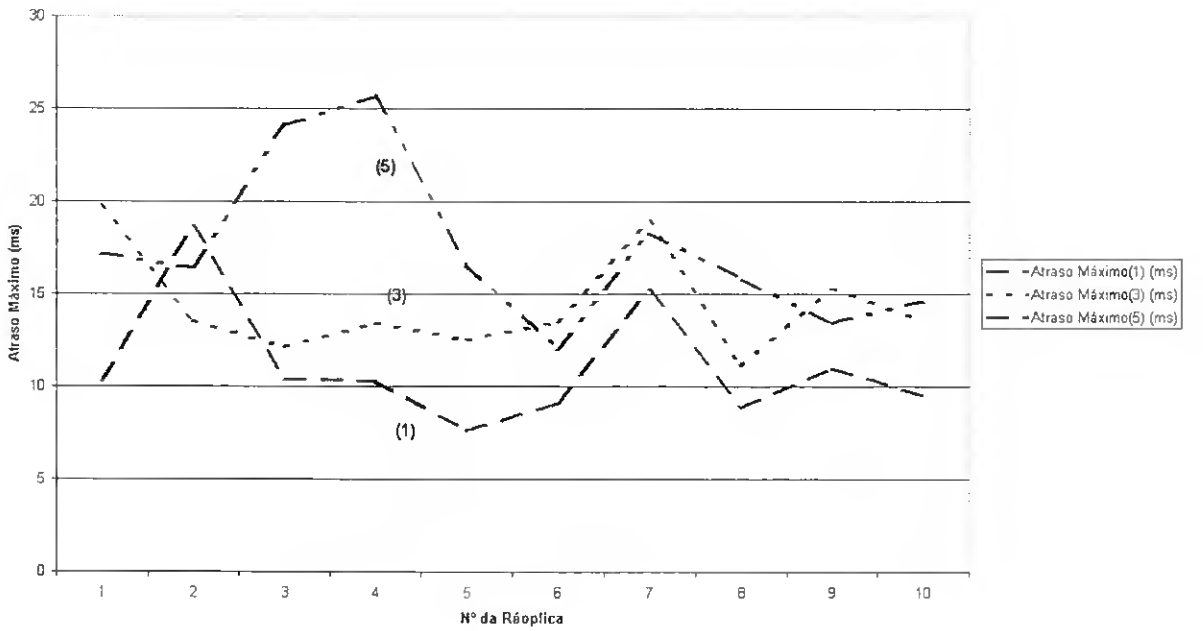


Gráfico 3 – Atraso Máximo versus número de utilizadores para 10 réplicas

Para finalizar o estudo da utilização do canal vamos referir-nos à sua utilização média em termos percentuais. Assim, a rede apresenta a utilização descrita na Tabela 13.

	Maior Utilização Média (%)	Menor Utilização Média (%)	Valor Médio
(1)	2.91%	2.57%	2.81%
(3)	5.55%	5.28%	5.44%
(5)	8.53%	8.10%	8.35%

Tabela 13 – Utlização média versus número de utilizadores

A análise é o exibida no Gráfico 4.

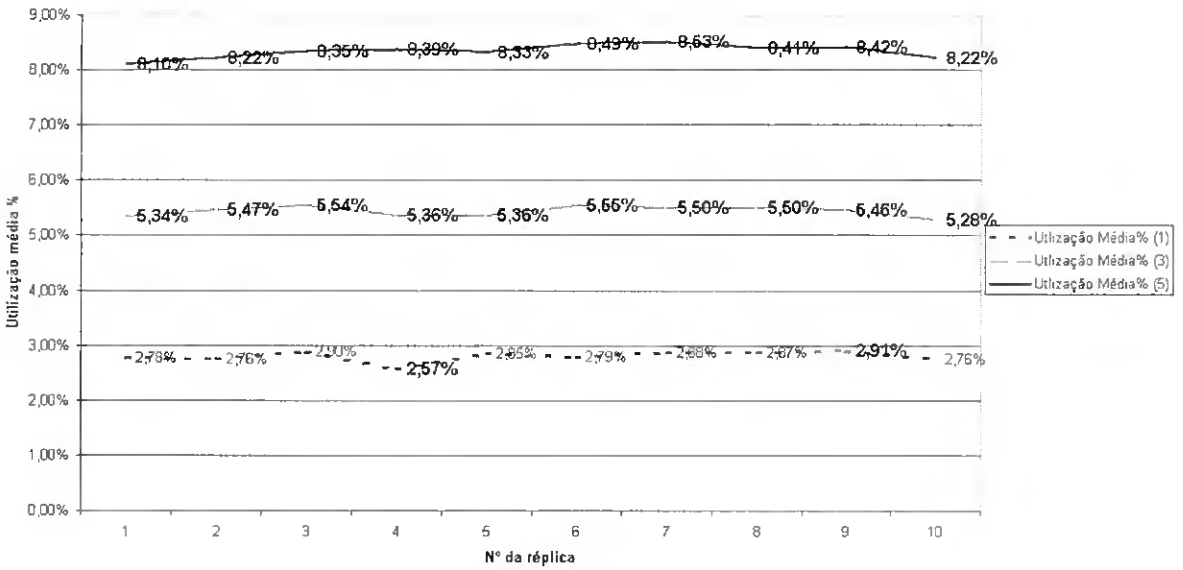


Gráfico 4 – Utlização média versus número de utilizadores para 10 réplicas

Pela sua análise podemos concluir que a largura de banda da rede é suficiente para permitir aumentar o número de utilizadores sem que isso conduza a uma latência excessiva, dado que no cenário de maior sobrecarga a utilização média está abaixo de 9%.

UTILIZAÇÃO DO CANAL EM TERMOS DE PACOTES E VELOCIDADE

Vamos analisar a utilização do canal sob o ponto de vista da aplicação ou seja, o número total pacotes que fluíram no link, a velocidade de entrega (pacotes/segundo) e a percentagem de bytes entregues. Assim, os resultados obtidos são os apresentados na Tabela 14.

	Número Total Pacotes Entregues	**Maior Número de Entrega Média**	**Menor Número de Entrega Média**	**Valor Médio**
(1)	1559629	162305	144437	155963
(3)	3030820	307367	296192	303082
(5)	4631357	471225	452217	463136

Tabela 14 – Pacotes entregues versus número de utilizadores

Pela sua análise concluímos que estes vão de encontro ao resultado observado para o número total de tramas entregues ou seja apresenta um crescimento linear.

Relativamente à velocidade de entrega de pacotes os resultados obtidos são os da Tabela 15.

	Maior Velocidade de Entrega Média (Pacotes/seg)	Menor Velocidade de Entrega Média	Valor Médio
(1)	45.085	40.121	43.32
(3)	85.38	82.27	84.19
(5)	130.89	125.16	128.60

Tabela 15 – Velocidade de entrega dos pacotes versus número de utilizadores

Pela sua análise podemos concluir que a performance da rede é boa, ou seja aumenta a velocidade face ao aumento do tráfego. Isto acontece porque e rede está bem dimensionada em termos de largura de banda contudo, não significa que pela velocidade de entrega ser superior a rede seja mais rápida uma vez que a performance total depende de atrasos provenientes de colisões e deferimentos resultantes da contenda pelo acesso ao meio.

Por último, relativamente à percentagem de bytes entregues verificou-se ser sempre de 100 % para todas as simulações realizadas ou seja, a rede consegue entregar todos os pacotes de dados que lhe chegam, obviamente tendo para tal que incorrer em maiores atrasos.

TAMANHO DAS TRAMAS

Esta análise apresenta valores estatísticos do número e tamanho das tramas transmitidas no link, o primeiro dos quais já foi anteriormente referido. O tamanho médio das tramas é exibido na Tabela 16.

	Maior Tamanho Médio (bytes)	Menor Tamanho Médio (bytes)	Desvio Padrão
(1)	915.403	900.53	[718.404 719.903]
(3)	910.368	901.911	[718.985 719.827]
(5)	911.955	905.208	[718.834 719.525]

Tabela 16 – Tamanho das tramas versus número de utilizadores

Relativamente ao tamanho das tramas podemos concluir que estas apresentam um valor que é directamente dependente do trafego gerado ou seja, o mesmo é praticamente constante para todas as simulações realizadas. Assim, apresenta em todas as simulações um tamanho máximo constante de 1542 bytes e médio com uma variação muito pequena como se pode constatar da análise do Desvio Padrão.

PERFORMANCE DO LINK IEEE 802.11

Vamos analisar a performance do link que usa como protocolo de acesso ao meio CSMA/CA, que foi o alvo principal da nossa simulação. Justifica-se uma vez que o objectivo do presente trabalho é estudar o comportamento da rede de área local sem fios implementada de acordo com as especificações da norma 802.11b.

Estudámos os indicadores a seguir enumerados, bem como aquilo que esperamos relativamente ao comportamento de cada um deles. Comecemos pelo *número de episódios de colisão* (*Collision Episodes*) que relata quantas vezes ocorreu uma colisão no link isto é, quando dois ou mais nós tentam transmitir dentro da mesma janela de colisão (*collision window*). Acresce, também, o *número total de tramas envolvidas em colisões* (*collided frames*). Estas duas métricas são importantes dado que as colisões irão desencadear a retransmissão das tramas nela envolvidas e consequentes atrasos que elas acarretarão para a rede, tornando-a menos efectiva em termos de performance uma vez que isso conduzirá a uma latência superior e os utilizadores poderão ter tempos de espera bastante superiores relativamente às tarefas que pretendem executar.

Outra factor tido em conta foi o *número de retransmissões devidas a erros ou colisões* (*Nbr Of Tries To Resolve*) em termos do valor médio, desvio padrão e valor máximo, dado que quanto maior o número de tentativas para voltar a enviar uma trama colidida maior será a latência da rede em termos de atraso. Assim, quando ocorre uma colisão cada uma das tramas que colidiu tem que voltar a ser transmitida algum tempo depois, a qual pode também voltar a colidir. Do ponto de vista da primeira trama na sequência de retransmissão, é relatado o número médio de retransmissões tentadas antes de uma transmissão de sucesso bem como o Desvio Padrão. Outro factor em análise e que é bastante pertinente corresponde ao numero máximo observado, durante a simulação, de novas tentativas que tiveram que ser feitas até que uma trama inicialmente em colisão fosse transmitida, se este valor for demasiado a latência da rede aumentará de modo significativo traduzido numa grande ocupação da rede mas sempre a tentar transmitir a mesma trama.

Analisamos agora o *número de deferimentos* (*Number of Deferrals*). Cada estação com tramas para transmitir, segundo o protocolo CSMA/CA, escuta o estado do canal, através de mecanismos físicos e virtuais anteriormente descritos, de modo a detectar se o mesmo está livre ou ocupado e com base nesse teste procederá, ou não, ao envio de tramas. Se o resultado, caso um nó tente transmitir uma trama, for um meio ocupado a estação irá adiar a

sua transmissão, segundo os mecanismo anteriormente descritos, até que o meio fique livre mais o intervalo de contenção. Obviamente que quanto maior o número de vezes que isto acontecer maior a latência da rede. A ocupação decorre do facto de outras estações estarem a usar o canal e esta atitude (*Carrier Sense*) é o principio base do protocolo CSMA/CA para evitar colisões com tramas que estejam a ser transmitidas, quer sejam de dados ou de qualquer outro tipo permitido.

Estes adiamentos acrescentam atrasos adicionais à rede que são medidos pelo *atraso do deferimento* (*Deferral Delay* (ms)) em termos da média, desvio padrão e máximo valor observado. Por outro lado, quando o nó tenta aceder ao meio, porque tem tramas para transmitir, e tem que adiar a transmissão por encontrar um meio ocupado ele não descarta as tramas mas sim coloca-as numa fila de espera no seu *buffer* de output. O *número de tramas na fila* pode ser medido (*Deferral Queue Size*) de modo a dar uma ideia da eficiência da rede em termos das tramas que têm que aguardar a sua vez para poderem ser enviadas e consequentemente o tempo de quem está à sua espera terá que aguardar por elas.

Em termos de colisões quando estas ocorrem, na janela de colisão, podem ser entre duas ou mais tramas provenientes dos diferentes nós. O caso mais simples é apenas entre duas tramas, contudo isto pode não acontecer em sistemas muito carregados. Então, o *número de episódios de colisões múltiplas* (*Multiple Collision Episodes*) relata o número de episódios de colisão nos quais estiveram envolvidas mais do que duas tramas, dando-nos uma ideia da sobrecarga da rede porque mais do que duas estações tentaram aceder ao meio simultaneamente e consequentemente será maior o tempo despendido na retransmissão de um número superior de tramas colididas.

Por outro lado, podemos tomar como linha orientadora que um protocolo de acesso ao meio que seja adequado, a hipótese de que os dados sejam perdidos devido a colisões durante os períodos de contenção pelo canal é constante e igual a zero. Na nossa simulação este facto é verificado, como referimos na utilização do canal, em relação ao parâmetro RST/ERR que apresentou o valor zero constante para todas as simulações, embora à custa de maior atraso nas tramas enviadas e recebidas à medida que cada nó espera pela sua vez para usar a largura de banda que tem disponível. Assim, podemos concluir que enquanto o nosso modelo exibe com precisão o número de tramas / pacotes que são transmitidos no link não consegue completamente avaliar a latência da troca de uma trama em particular. Por outro lado, foi uma constante em todas as simulações que a rede em análise conseguiu sempre entregar todas as tramas resultantes do trafego gerado, a % Bytes entregues apresentou o resultado

100% para todas as simulações, claro à custa de maior ou menor atraso, isto é, não foi observada nenhuma réplica em que existissem tramas descartadas.

Relativamente ao link os resultados obtidos, como estatísticas de colisão, foram os apresentados na Tabela 17.

	N.º Total de Episódios de Colisão	**N.º Máximo de Episódios de Colisão**	**N.º Mínimo de Episódios de Colisão**	**Valor Médio**
(1)	141	24	4	14
(3)	537	76	40	54
(5)	1284	149	106	128
	N.º Total de Tramas Envolvidas	**N.º Máximo de Tramas Envolvidas**	**N.º Mínimo de Tramas Envolvidas**	**Valor Médio**
(1)	282	48	8	28
(3)	1075	152	80	108
(5)	2568	298	212	257

Tabela 17 – Episódios de colisão e número total de tramas envolvidas para o diferente número de utilizadores

Da análise concluímos que o número de episódios de colisão, bem como respectivas tramas envolvidas, apresenta um crescimento linear causado pelo facto do tráfego aumentar face ao número de utilizadores.

O número médio de retransmissões da mesma trama é exibido na Tabela 18.

	Maior Nº Médio Tentativas p/ Resolver	Menor Nº Médio Tentativas p/ Resolver	Desvio Padrão
(1)	1.09	1	[0 0.29]
(3)	1.04	1	[0 0.19]
(5)	1.05	1.01	[0.09 0.22]
	Nº Máximo de Tentativas p/ Resolver		
(1)	6 Vezes 1 Tentativa 4 Vezes 2 Tentativas		
(3)	2 vezes 1 Tentativa 8 Vezes 2 Tentativas		
(5)	9 Vezes 2 Tentativas 1 Vez 3 Tentativas		

Tabela 18 – Número médio e máximo de tentativas para resolver colisões para o diferente número de utilizadores

Concluímos que apresenta valores normais ou seja, no caso de maior sobrecarga **(5)** as tramas são transmitidas com sucesso ao fim do número com duas tentativas, sendo no entanto observado também apenas uma tentativa. Do anterior concluímos que os atrasos decorrentes não induzirão latência significativa.

A apresentação gráfica (Gráfico 5) dos valores relativos a colisões confirma o anteriormente referido, ou seja o seu aumento é linear e como tal causado pelo aumento de tráfego na rede.

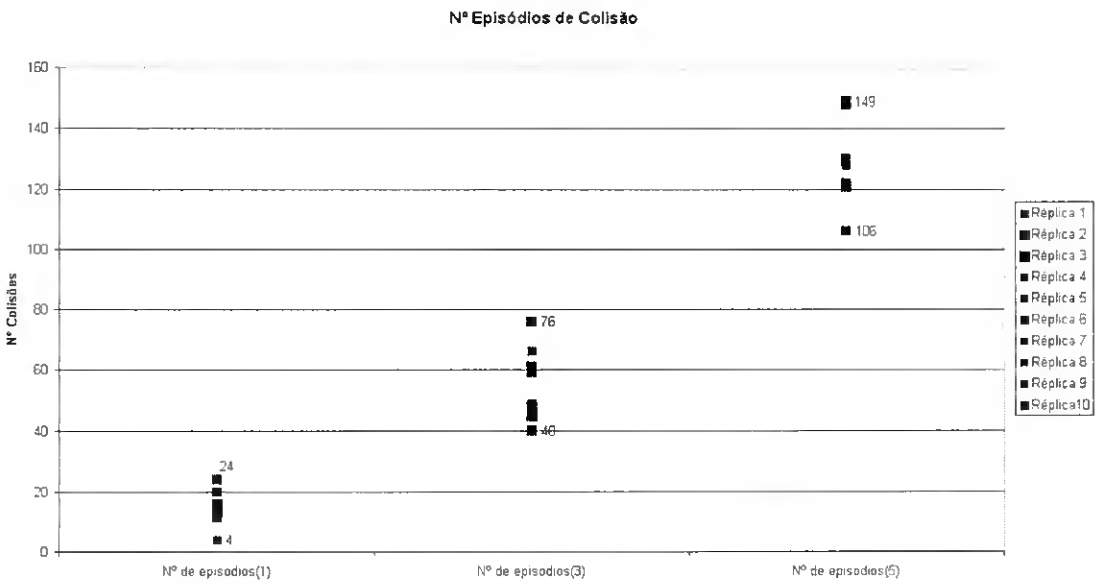


Gráfico 5 – Número de episódios de colisão versus número de utilizadores para as 10 réplicas

Relativamente aos deferimentos, métrica de extrema importância, os valores observados foram os da Tabela 19. As conclusões relativas às colisões podem ser aplicadas a este indicador, ou seja os valores são os esperados face ao aumento do volume de tráfego.

	N.º Total de Deferimentos	**N.º Máximo de Deferimentos**	**N.º Mínimo de Deferimentos**	**Valor Médio**
(1)	72365	8226	6365	7237
(3)	172613	18335	16110	17261
(5)	313907	33079	29391	31391
	Maior Valor do Atraso Máximo (ms)	**Menor Valor do Atraso Máximo (ms)**	**Desvio Padrão**	
(1)	7.98	5.36	[0.41 .54]	
(3)	10.53	6.52	[0.53 .060]	
(5)	10.55	6.97	[0.60 0.64]	
	Nº Máximo de Tramas na Fila de Deferimentos		**Desvio Padrão**	
(1)	5 vezes 2 Tramas 5 Vezes 3 Tramas		[0.03 0.04]	
(3)	10 Vezes 3 Tramas		[0.05 0.06]	
(5)	8 Vezes 3 Tramas 2 vezes 4 Tramas		[0.08 0.08]	

Tabela 19 - Número total, máximo e mínimo de deferimentos; maior e menor atraso máximo e número máximo de tramas na fila de deferimentos

Face à totalidade dos resultados apresentados podemos concluir que:

1) A parametrização do link, referimo-nos aos parâmetros sensíveis à rede, está feita de modo adequado face aos resultados obtidos. Ênfase especial para o parâmetro *Dwell Time* ao qual foi atribuído um valor grande (10000000.0 ms) para garantir a entrega de todas as tramas em detrimento de um atraso que se provou não ser significativo. Normalmente nas redes de comunicação é preferível que seja cumprida uma meta que garanta a entrega de todos os dados mesmo em detrimento de um pouco mais rapidez;

2) Em termos de escalabilidade a rede tem o comportamento desejado face à introdução de maior número de utilizadores, facto que se pode concluir face à tendência de crescimento

linear quer do número de tramas e pacotes entregues e respectiva velocidade sem que os atrasos aumentem de modo comprometedor;

3) Os atrasos provenientes de colisões estão dentro dos padrões normais esperados relativamente ao aumento de trafego que advém do aumento do número de utilizadores. Assim, as colisões aumentam mas o número de retransmissões para as resolver não é demasiado grande que cause atrasos indesejáveis na performance da rede, isto é, os 11 Mbps de largura de banda são suficientes para responder a um aumento de tráfego sem causar atrasos excessivos conducentes a uma espera prolongada, por parte dos utilizadores da rede, por respostas aos seus pedidos seja qual for a sua natureza;

4) Os deferimentos acompanham, igualmente, os aumentos de tráfego não causando atrasos exagerados no acesso ao meio por este se encontrar ocupado. Tal pode concluir-se porque o número de tramas na fila espera, para serem transmitidas, não é grande face aos níveis de tráfego da rede. O maior valor observado mas também o menos frequente, nos diversos cenários, são 4 que quando comparado com o número total de tramas que são transmitidas no link é quase desprezável;

5) Em suma a rede é suficientemente escalável apresentando um comportamento estável face à introdução de mais utilizadores e consequente tráfego gerado porque a utilização média da rede, em termos percentuais, acompanha o volume do trafego gerado e não cria níveis de utilização que possam por em risco o *throughput*, isto é, não existem utilizações médias demasiado grandes conducentes a um hipotético congestionamento.

INTRODUÇÃO DE ERROS

Os erros são frequentes nos cenários WLANs devido a elevados níveis de ruído e outros fenómenos que põem em causa as transmissões. Assim, observamos valores elevados de BER (Bit Error Rate) existente nas comunicações por rádio e infravermelhos (tipicamente da ordem 10^{-3} a 10^{-5}), enquanto nas suas congéneres cabladas o BER existente é baixíssimo (valores típicos da ordem de 10^{-9} a 10^{-11}), no nosso estudo consideramos erros de 10^{-3}. Estes são causados sobretudo por interferência, a qual é devida à necessidade de existência de transmissões simultâneas no mesmo canal, facto que também acontece nas redes de área local sem fios pelo que estas estão, modo geral, sujeitas a tal efeito. No protocolo CSMA, como anteriormente referido, o acesso ao meio é controlado por detecção de actividade e a interferência será causada pelas estações da própria célula que não consigam detectar transmissões em curso no canal provenientes das suas congéneres, fenómeno referido como

terminal oculto. Tal facto não significa que necessariamente a trama não seja recebida. Assim, devido à diferença de potência da recepção, uma trama de potência superior pode ser capturada. Outro causa de erros é o ruído induzido por fontes exteriores à rede a que fizemos alusão anteriormente.

Podem ser aplicadas medidas conducentes à atenuação dos erros de transmissão. Assim, como referimos a norma 802.11b embora opere à velocidade máxima de 11 Mbps possuí um mecanismo, que visa combater os erros de transmissão, para suporte a múltiplas velocidades (5.5, 2 e 1 Mbps) ao nível da camada MAC, o qual minimiza o consumo de potência e permite a adaptação imediata às condições do canal de transmissão que apresenta alterações em constante mudança. Quando a rede detectar níveis de ruído e interferência elevados baixa a velocidade de transmissão para melhorar a qualidade da ligação. A implementação desta técnica depende do facto dos dispositivos dos diversos fabricantes o permitirem ou não, uma vez que ela esta contemplada na norma 802.11b cuja camada física permite o suporte a múltiplas velocidades.

Existe outra técnica da responsabilidade da camada MAC, denominada fragmentação e anteriormente referida, para resolver o problema de ambientes extremamente ruidosos que, por esse facto, põem em causa a transmissão com sucesso de tramas grandes. No nosso estudo não iremos usar essa técnica porque o tamanho de trama máximo (1542 bytes) gerado pelos nossos dados não produz tramas que justifiquem ser fragmentadas.

Uma última técnica, que é usada na rede em estudo, baseia-se no facto da função que estamos a implementar DCF incluir, para além do protocolo CSMA/CA, da reserva de canal e de um esquema de prioridades, um mecanismo de reconhecimentos positivos imediatos (ACK). Esta foi inicialmente proposta por Tobagi [43] e é justificada pelo facto de que a utilização de tramas de confirmação positiva, no acesso a um meio partilhado, possibilita a detecção de erros pelo emissor. Além destas existem ainda técnicas implementadas ao nível físico que visam combater os erros nas redes de área local sem fios das quais não iremos falar por irem para além do âmbito do presente estudo.

Iremos, em seguida, analisar a performance da rede executando simulações com a presença de erros gerados aleatoriamente. Face ao anteriormente exposto, atendendo a que a rede em estudo poderá estar sujeita a erros, simulámos três cenários nos quais induzimos a existência de erros com probabilidade de 1×10^{-3}, anteriormente justificada. Definimos cenários de 15 utilizadores e erros; 30 utilizadores e erros e 45 utilizadores e erros os quais referiremos, neste estudo, como **(2)**, **(4)** e **(6)** respectivamente. Pretendemos, deste modo, analisar o efeito dos erros na performance da rede comparando, para tal, os valores ora obtidos com os que

resultaram da simulação, anteriormente descrita, correspondente à situação normal. O estudo incidiu na indução de erros de igual probabilidade tanto nas tramas de dados como nas tramas ACK de forma a criar cenários o mais reais possíveis.

UTILIZAÇÃO DO CANAL E ATRASOS

Nesta abordagem mantêm-se os pressupostos estabelecidos para a utilização do canal no cenário sem erros, no que diz respeito ao tipo de tráfego. Relativamente à utilização do canal, em termos do número total de tramas entregues, é a exibida na Tabela 20.

	Nº Total de Tramas Entregues	**DIFERENÇA**
(1)	1502411	
(2)	1500186	**-2225**
(3)	2922832	
(4)	2919187	**-3645**
(5)	4474744	
(6)	4445961	**-28783**

Tabela 20 – Tramas entregues versus os diferentes cenários

Da análise dos resultados, concluímos que se verificou um decrescimento no número de tramas entregues com a indução de erros em comparação com o cenário normal, o qual é bastante mais acentuado à medida que o número de tramas em curso na rede aumenta **(6)**.

Relativamente aos atrasos a diferença é sentida em termos do aumento do atraso máximo como podemos concluir da análise gráfica apresentada (Gráfico 6/Gráfico 7/Gráfico 8). Nesta exibimos a comparação entre os resultados da simulação normal para cada cenário e da simulação na presença de erros.

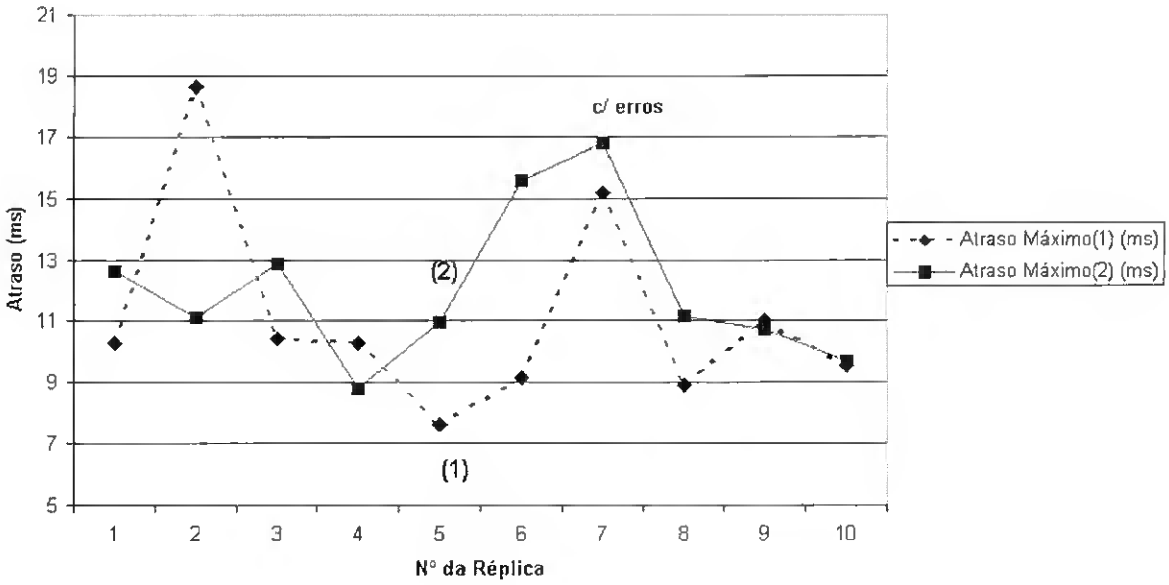


Gráfico 6 – Atraso máximo para os cenários (1) e (2), para 10 réplicas

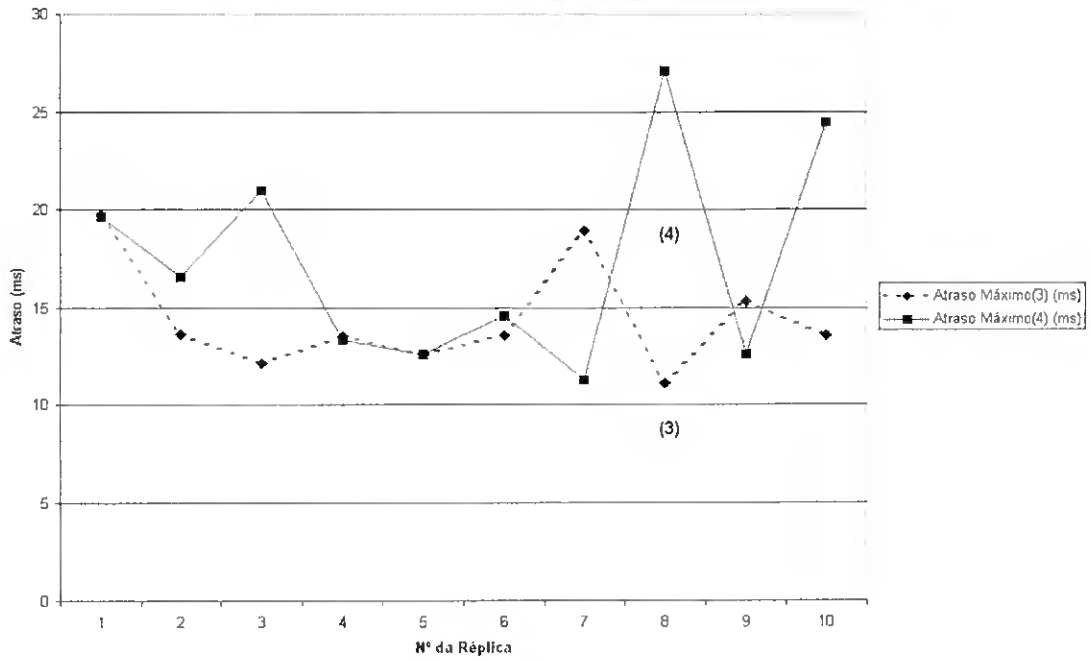


Gráfico 7 - Atraso máximo para os cenários (3) e (4), para 10 réplicas

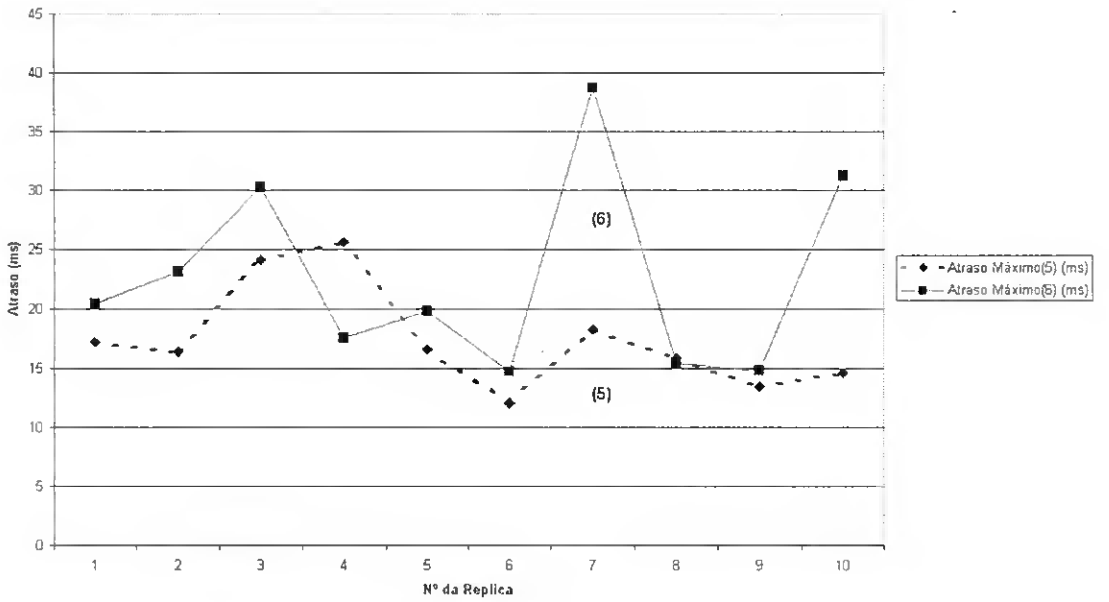


Gráfico 8 - Atraso máximo para os cenários (5) e (6), para 10 réplicas

Um último facto de relevo refere-se à utilização média da rede, em termos percentuais, como exibido na Tabela 21.

	Maior Utilização Média (%)	Menor Utilização Média (%)	Valor Médio
(1)	2.91%	2.57%	2.81%
(2)	2.94%	2.63%	2.81%
(3)	5.55%	5.28%	5.44%
(4)	5.73%	5.27%	5.54%
(5)	8.53%	8.10%	8.35%
(6)	8.49%	8.11%	8.35%

Tabela 21 – Utilização para os diferentes cenários

Conclui-se que a percentagem ou é idêntica à dos cenários sem erros ou então aumenta mas, no entanto, para transmitir um número de tramas inferiores. Este facto revela que a rede passou a estar em média mais tempo ocupada, mas para transmitir menor quantidade de informação logo o seu *throughput* diminui na presença de erros.

UTILIZAÇÃO DO CANAL EM TERMOS DE PACOTES E VELOCIDADE

Em termos de utilização do canal na presença de erros vamos analisá-la sob o mesmo ponto de vista que fizemos anteriormente ou seja, o número total pacotes que fluíram no link, a velocidade de entrega (pacotes/segundo) e a percentagem de bytes entregues. Os resultados obtidos, relativamente aos pacotes entregues, são os exibidos na Tabela 22.

	Número Total Pacotes Entregues	DIFERENÇA
(1)	1559629	
(2)	1557319	-2310
(3)	3030820	
(4)	3026472	-4348
(5)	4631357	
(6)	4601662	-29695

Tabela 22 – Número de pacotes entregues nos diferentes cenários

Da sua análise concluímos que na presença de erros o número de pacotes entregues segue a mesma tendência das tramas, ou seja decrescem sobretudo com o aumento do volume de tráfego.

Relativamente à velocidade de entrega de pacotes os resultados são os da Tabela 23.

	Maior Velocidade de Entrega Média (Pacotes/seg)	Menor Velocidade de Entrega Média	Valor Médio
(1)	45.08	40.12	43.32
(2)	45.08	40.89	43.23
(3)	85.38	82.27	84.19
(4)	87.84	82.55	84.91
(5)	130.89	125.16	128.98
(6)	130.61	125.47	127.82

Tabela 23 – Velocidade de entrega dos pacotes para os diferentes cenários

Assim, após análise concluímos que a velocidade de entrega de cada pacote não difere muito do cenário sem erros embora a tendência para uma ligeira diminuição se prenda com o facto da rede adaptar a velocidade de acordo com as características do canal, baixando-a na

presença de erros. A menor performance da rede não pode, portanto, ser atribuída à velocidade de entrega de pacotes mas sim a atrasos provenientes quer de colisões e consequente retransmissão quer dos deferimentos, dos quais falaremos posteriormente.
Em último, relativamente à percentagem de bytes entregues verificou-se ser sempre de 100 % para todas as simulações realizadas, ou seja a rede, na presença de erros, continua a entregar a totalidade dos pacotes embora em menor número.

TAMANHO DAS TRAMAS

Esta análise apresenta valores estatísticos do número e tamanho das tramas transmitidas no link, o primeiro dos quais já foi anteriormente referido e, tal como se disse, decresceu. O tamanho médio das tramas é exibido na Tabela 24.

	Maior Tamanho Médio (bytes)	Menor Tamanho Médio (bytes)	Desvio Padrão
(1)	915.403	900.53	[718.404 719.903]
(2)	915.53	902.345	[718.384 719.345]
(3)	910.368	901.911	[718.985 719.827]
(4)	913.067	902.786	[718.668 719.757]
(5)	911.955	905.208	[718.834 719.525]
(6)	910.874	905.539	[718.897 719.516]

Tabela 24 – Tamanho das tramas para os diferentes cenários

Relativamente ao tamanho das tramas podemos verificar que estas apresentam um valor directamente dependente do trafego gerado, pelo que são praticamente constantes para todas as simulações realizadas. Assim, apresentam em todas as réplicas um tamanho máximo constante de 1542 bytes e médio com uma variação muito pequena, como se pode constatar da análise do desvio padrão. Podemos concluir que os erros não afectam a rede ao nível do tamanho da trama criada, sendo as alterações verificas meramente produzidas pela natureza aleatória do tráfego.
Como análise geral, do anteriormente exposto, podemos concluir que os erros diminuem o número da tramas que são transmitidas e consequentemente o número de pacotes, provocado pelo aumento dos atrasos máximos ou seja o tempo que demora a transmitir com sucesso uma trama em particular. Em termos de velocidade esta não é ligeiramente afectada. Por

outro lado a utilização da rede aumenta ligeiramente, em alguns casos, mas esse facto não se traduz numa atitude que conduza a um maior número de tramas entregues mas sim o contrário. Analisaremos em seguida o que se passa em termos do link para que possamos fundamentar estes resultados.

PERFORMANCE DO LINK IEEE 802.11

Mantêm-se as considerações genéricas feitas a quando da simulação sem erros, nomeadamente em termos do protocolo de acesso ao meio e dos indicadores a serem estudados.

Pela análise da conjectura do problema em estudo, aliado à nossa percepção proveniente de estudos que analisam este fenómeno [38], pensamos que os erros afectarão o número de episódios de colisão, o número de tramas envolvidas, o número máximo de retransmissões para as resolver, o número de vezes que uma tentativa de transmissão é adiada (deferimentos) por encontrar o meio ocupado e o número máximo de tramas na fila a aguardar transmissão. A conjugação de todos estes factores afectará a performance da rede pelos atrasos a que a mesma fica sujeita, caso os seus valores sejam grandes, não apenas pelo volume de tráfego, como observado na primeira simulação, mas também pela existência de anomalias ou erros e consequente resolução.

Relativamente ao link os resultados obtidos, como estatísticas de colisão, foram os exibidos nas tabelas (Tabela 25 / Tabela 26).

	N.º Total de Episódios de Colisão	**N.º Máximo de Episódios de Colisão**	**N.º Mínimo de Episódios de Colisão**	**Valor Médio**
(1)	141	24	4	14
(2)	150	24	9	15
(3)	537	76	40	54
(4)	607	99	34	61
(5)	1284	149	106	128
(6) a)	1326	159	120	133

a) Forma verificados dois episódios de colisões múltiplas envolvendo 3 tramas em cada um deles.

Tabela 25 – Colisões para os diferentes cenários

	N.º Total de Tramas Envolvidas	N.º Máximo de Tramas Envolvidas	N.º Mínimo de Tramas Envolvidas	Valor Médio
(1)	282	48	8	28
(2)	300	48	18	30
(3)	1075	152	80	108
(4)	1214	198	68	121
(5)	2568	298	212	257
(6)	2653	318	240	265

Tabela 26 – Número de tramas envolvidas

Da análise concluímos que o número de episódios de colisão, bem como as tramas envolvidas, aumentam na presença de erros. Por outro lado, foram registados dois episódios de colisão múltipla, o que pode acontecer em redes onde a sobrecarga é grande, como tal se verificou para 45 utilizadores, mas apenas na presença de erros, podemos concluir que serão consequência directa dos mesmos.

O número médio, menor e máximo de retransmissões da mesma trama é exibido nas tabelas (Tabela 27 / Tabela 28).

	Maior Nº Médio Tentativas p/ Resolver	Menor Nº Médio Tentativas p/ Resolver	Desvio Padrão
(1)	1.09	1	[0 0.29]
(2)	1.01	1	[0 0.11]
(3)	1.04	1	[0 0.19]
(4)	1.01	1	[0.04 0.12]
(5)	1.05	1.01	[0.09 0.22]
(6)	1.02	1.01	[0.09 0.13]

Tabela 27 – Número de retransmissões da mesma trama

	Nº Máximo de Tentativas p/ Resolver (Retransmissões)
(1)	6 Vezes 1 Tentativa 4 Vezes 2 Tentativas
(2)	1 Vez 1 Tentativa 9 Vezes 2 Tentativas
(3)	2 vezes 1 Tentativa 8 Vezes 2 Tentativas
(4)	9 Vezes 2 Tentativas 1 Vez 3 Tentativas
(5)	9 Vezes 2 Tentativas 1 Vez 3 Tentativas
(6)	7 Vezes 2 Tentativas 3 Vezes 3 Tentativas

Tabela 28 – Número de tentativas necessárias para resolver uma colisão

Concluímos que os erros afectaram o número máximo de tentativas para resolver uma colisão, porque uma trama teve que ser retransmitida um número superior de vezes até à recepção com sucesso, facto que agora acontece com muito mais frequência que no cenário normal.

A apresentação gráfica (Gráfico 9) dos resultados relativos a colisões mostra, claramente, que o número de colisões cresce na presença de erros.

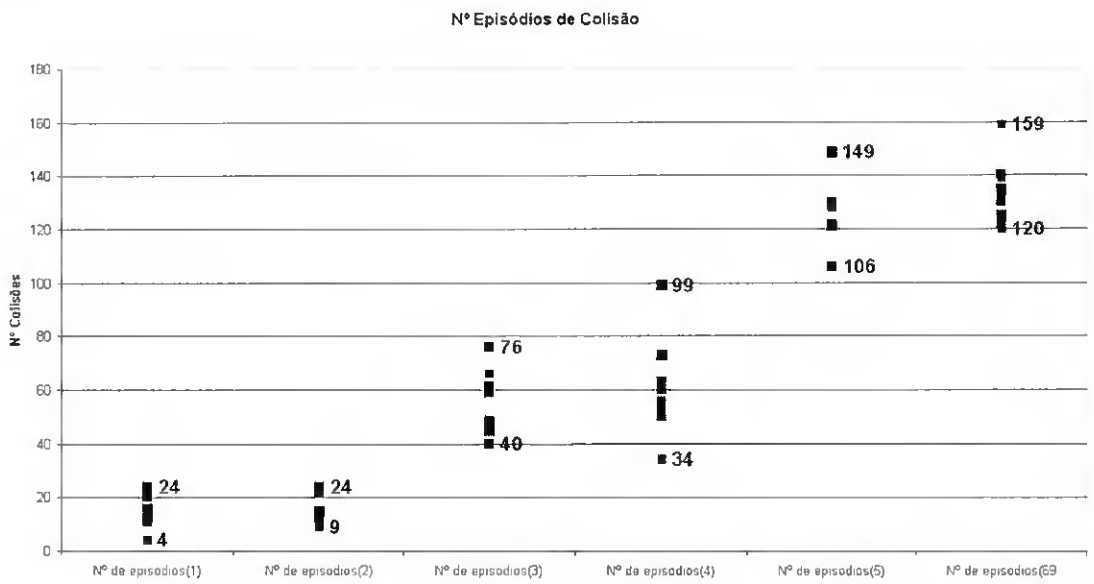


Gráfico 9 – Número de episódios de colisão

Face ao anteriormente concluímos que na presença de erros o número de colisões aumentam e consequentemente o número de tramas envolvidas. Como resultado o número de retransmissões para as resolver irá aumentar e consequentemente a rede sofrerá uma degradação de performance devido aos atrasos provenientes das novas tentativas de envio da mesma trama.

Relativamente aos deferimentos, métrica de extrema importância os valores observados foram os da Tabela 29.

	N.º Total de Deferimentos	N.º Máximo de Deferimentos	N.º Mínimo de Deferimentos	Valor Médio
(1)	72365	8226	6365	7237
(2)	76050	8565	6686	7605
(3)	172613	18335	16110	17261
(4)	175924	18785	16698	17592
(5)	313907	33079	29391	31391
(6)	316264	33237	30101	31626

Tabela 29 – Número de deferimentos

Graficamente obtemos uma comparação para os cenários sem e com erros (Gráfico 10 / Gráfico 11 / Gráfico 12).

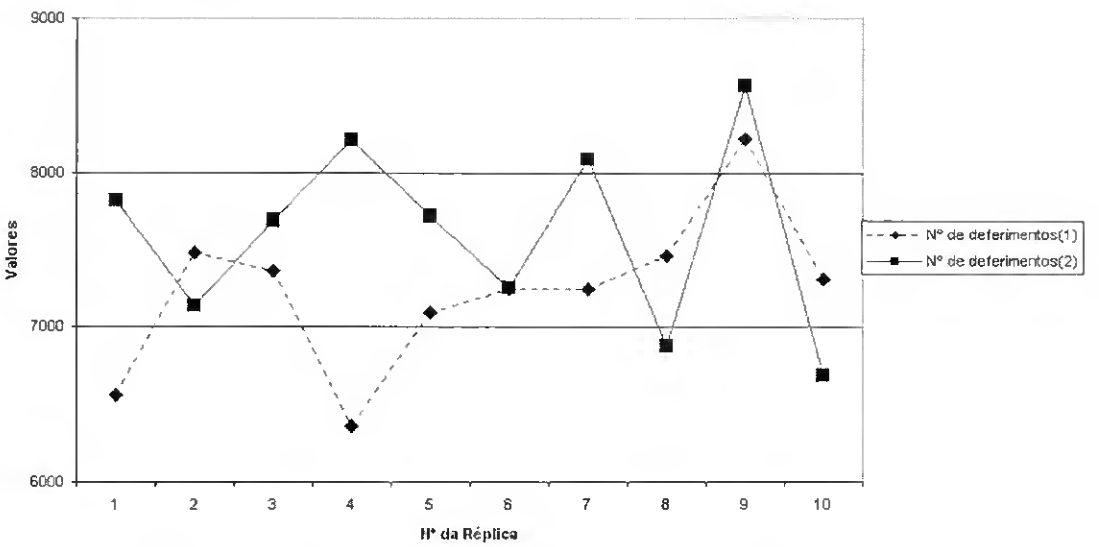


Gráfico 10 – Número de deferimentos versus réplica para os cenários (1) e (2)

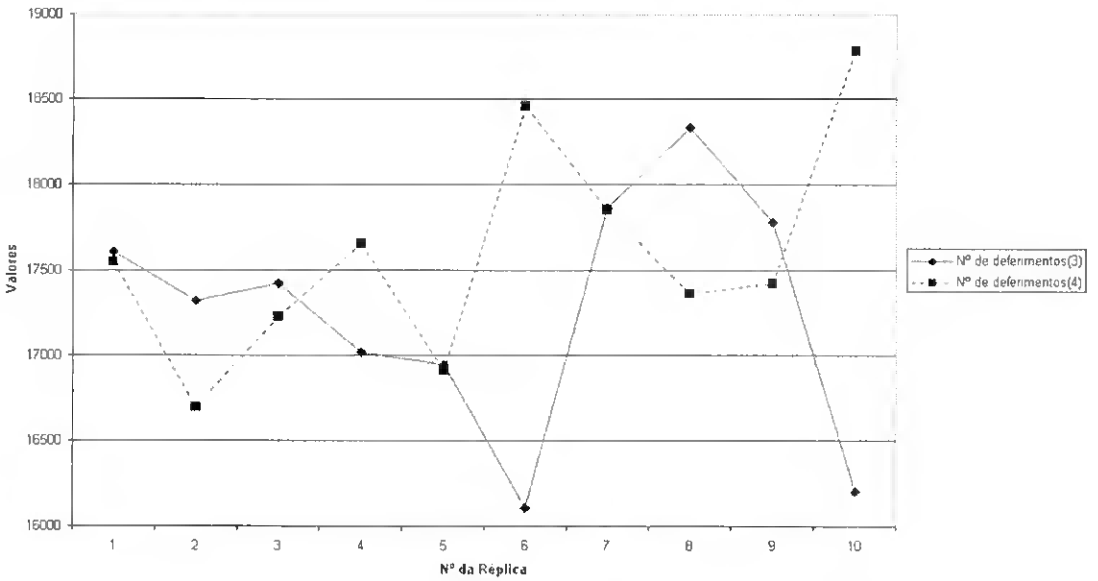


Gráfico 11 - Número de deferimentos versus réplica para os cenários (3) e (4)

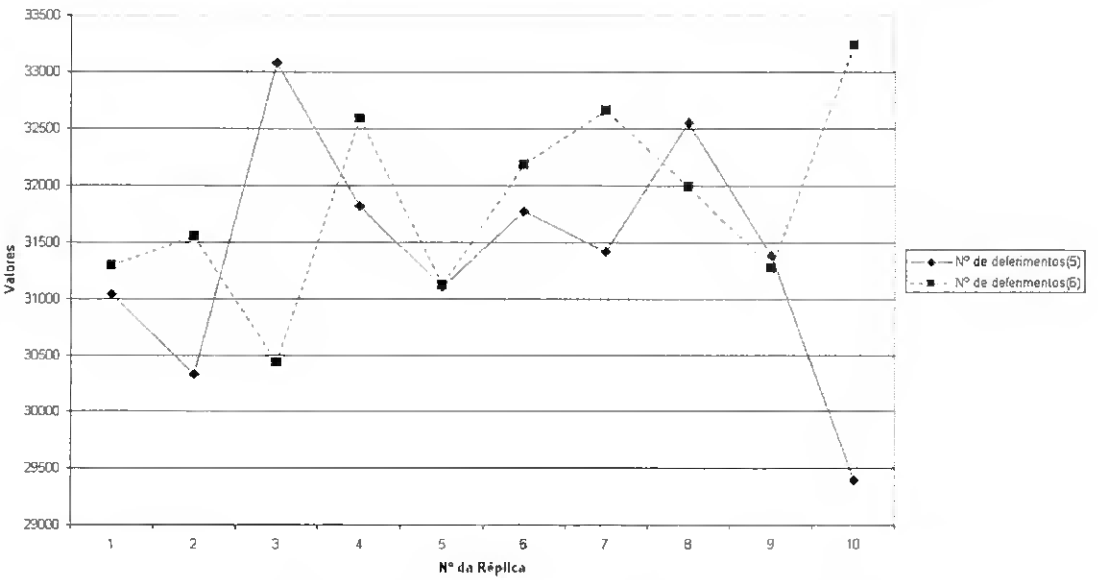


Gráfico 12 - Número de deferimentos versus réplica para os cenários (5) e (6)

A dispersão dos resultados referentes ao atrasos máximos, provenientes de deferimentos, verificados para cada um dos cenários é exibida graficamente (Gráfico 13), onde podemos ver que a tendência é para um crescimento na presença de erros.

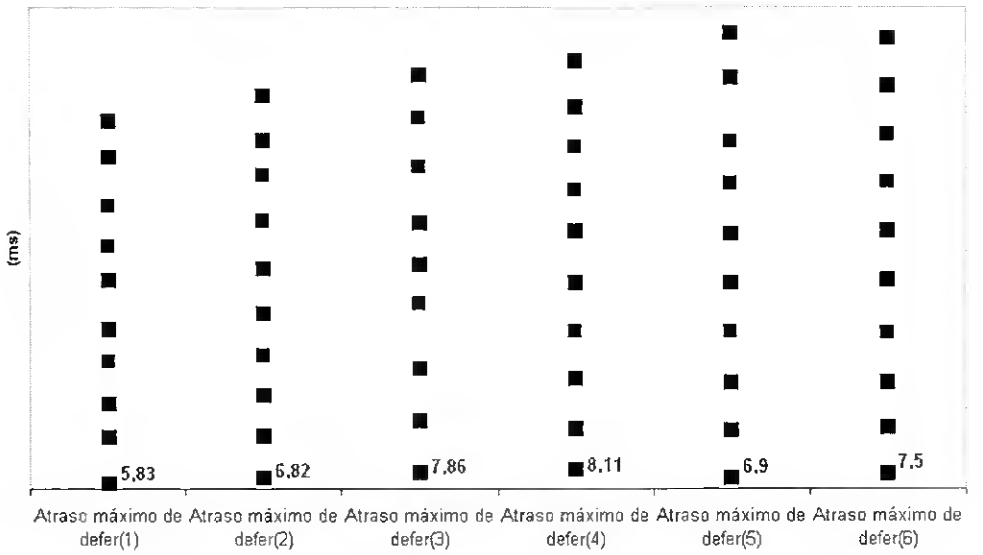


Gráfico 13 – Atraso máximo dos deferimentos para vários cenários

O número de tramas na fila de deferimento é mostrado na Tabela 30.

	Nº Máximo de Tramas na Fila de Um Deferimento	**Desvio Padrão**
(1)	5 vezes 2 Tramas 5 Vezes 3 Tramas	[0.03 0.04]
(2)	4 Vezes 2 Tramas 6 Vezes 3 Tramas	[0.03 0.04]
(3)	10 Vezes 3 Tramas	[0.05 0.06]
(4)	10 Vezes 3 Tramas	[0.05 0.06]
(5)	8 Vezes 3 Tramas 2 vezes 4 Tramas	[0.07 0.08]
(6)	8 Vezes 3 Tramas 2 vezes 4 Tramas	[0.07 0.08]

Tabela 30 – Número de tramas na fila de deferimentos

Face aos resultados obtidos podemos concluir que:

1) Relativamente ao número de episódios de colisão e consequentemente as tramas neles envolvidas observamos que aumentam na presença de erros. Assim, a análise comparativa dos vários cenários é exibida na Tabela 31.

	Nº Episódios de Colisões	Nº Tramas Envolvidas	Nº Episódios de Colisão Múltipla
(1) Versus (2)	+9	+18	0
(3) Versus (4)	+70	+139	0
(5) Versus (6)	+42	+85	2 apenas em (6)

Tabela 31 – Análise comparativa dos vários cenários

2) O número de retransmissões máximo aumenta e também a frequência com que se tem que recorrer a um número de tentativas superior;

3) O número de adiamentos aumenta na presença de erros, ou seja o número de acessos a um meio ocupado cresce na presença de erros, conforme exibido na Tabela 32.

	Nº Deferimentos
(1) Versus (2)	+3685
(3) Versus (4)	+3311
(5) Versus (6)	+2357

Tabela 32 – Deferimentos em função do erro

4) A conjugação de todos estes condicionantes conduz a uma rede de performance inferior pelo aumento verificado nos atrasos que os erros induzem.

Após execução da simulação na presença de erros, comparativamente ao cenário normal, a grande linha chave que podemos extrair é a que a rede apresenta um comportamento extremamente instável. Assim, não podemos definir um comportamento padrão para a maioria dos indicadores, excepto em relação ao número de episódios de colisão e consequente número de tramas envolvidas que levarão a aumento do número máximo de tentativas de transmissão de uma mesma trama. Este resultado não nos é de forma alguma estranho, porque pensamos que este é o cenário observado nas redes reais nas quais os erros não são previsíveis, isto é não apresentam uma cadência constante ao longo da utilização, contrariamente à sua contrapartida cablada Ethernet. Tal facto, justifica-se pelos inúmeros factores que poderão causar erros numa transmissão em espaço livre, frequentemente referida como dinâmica do canal, e a dificuldade quer de os prever quer de os evitar. Assim, a título de exemplo ninguém pode prever quando se abre uma porta que cause, por exemplo, reflexão do sinal transmitido, ou quando passe a estar no meio qualquer fonte que cause interferência no sinal rádio sem que nos apercebamos disso. Por outro lado, se o número de

retransmissões aumentam, consequentemente o número de adiamentos de acesso meio crescerão porque o meio irá estar mais ocupado, cenários todos eles conducentes ao aumento dos atrasos e latência da rede.

Face a todas as considerações que vêm sendo tecidas ao longo deste trabalho recomendamos que na implementação de uma rede sem fios em qualquer cenário, que pelas suas características apresente probabilidade de incutir elevadas taxas de erros, sejam aplicadas as medidas anteriormente referidas para os combater e tornar a performance da rede a melhor possível. Claro que nas WLANs não existem dois locais com as mesmas características pelo que o *site survey* deve ser o mais exacto possível para prevenir eventuais situações anómalas. Como conclusão final desta simulação podemos afirmar que os erros têm impactos negativos na transmissão pelo que deverão, dentro do possível, ser evitados e previstos à prori. Acresce o facto de que um erro que ocorreu hoje poderá estar resolvido amanhã.

INTRODUÇÃO DE ERROS DE 10^{-1}

Queremos com este novo cenário acrescer fundamentação relativa ao efeito adverso dos erros na performance da rede aumentando-os. Assim, executámos duas novas simulações em tudo idênticas às anteriormente realizadas excepto: Erros 10^{-1} e apenas cinco réplicas em cada uma delas. Esta última decisão prendeu-se com o facto de na presença de tão grande número de erros os cálculos serem bastante maiores e muito mais morosos. Assim, os cenários considerados foram uma taxa de erro, igual para todos, de 10^{-1} e fizemos variar o número de utilizadores de 15 para o valor extremo de 45, os quais neste estudo iremos designar como **(A)** e **(B)** respectivamente. Optámos por analisar estas duas situações extremas para podermos comparar dois cenários com níveis de trafego muito distintos.

O nosso pressuposto é o de que com esta taxa de erro a performance da rede se degrade consideravelmente quer no número de tramas transmitidas bem como pacotes; no número de episódios de colisão simples e múltiplas e respectivas tramas colididas; no número de tentativas de retransmissões; no número de tramas na fila de espera e em último o impacto que todas estes irão ter nos atrasos da rede.

UTILIZAÇÃO DO CANAL E ATRASOS

O número de tramas entregues é o exibido na Tabela 33. Verificamos que a tendência, tal como anteriormente, é para decrescimento na presença de erros.

	Nº Total de Tramas Entregues	DIFERENÇA
(1)	743212	
(A)	698661	**-44551**
(5)	2221563	
(B)	2211307	**-10256**

Tabela 33 – Número total de tramas entregues

Relativamente aos atrasos médio e máximo estes são os exibidos nos gráficos (Gráfico 14 / Gráfico 15 / Gráfico 16).

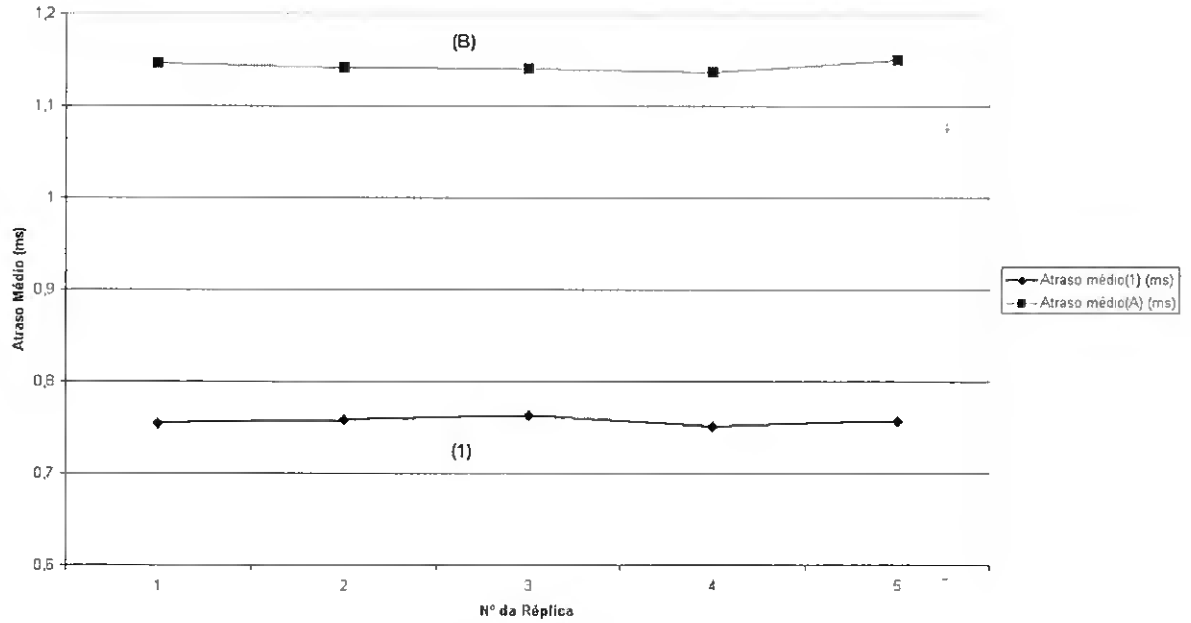


Gráfico 14 – Atraso médio, com e sem erros, para 15 utlizadores e 5 réplicas

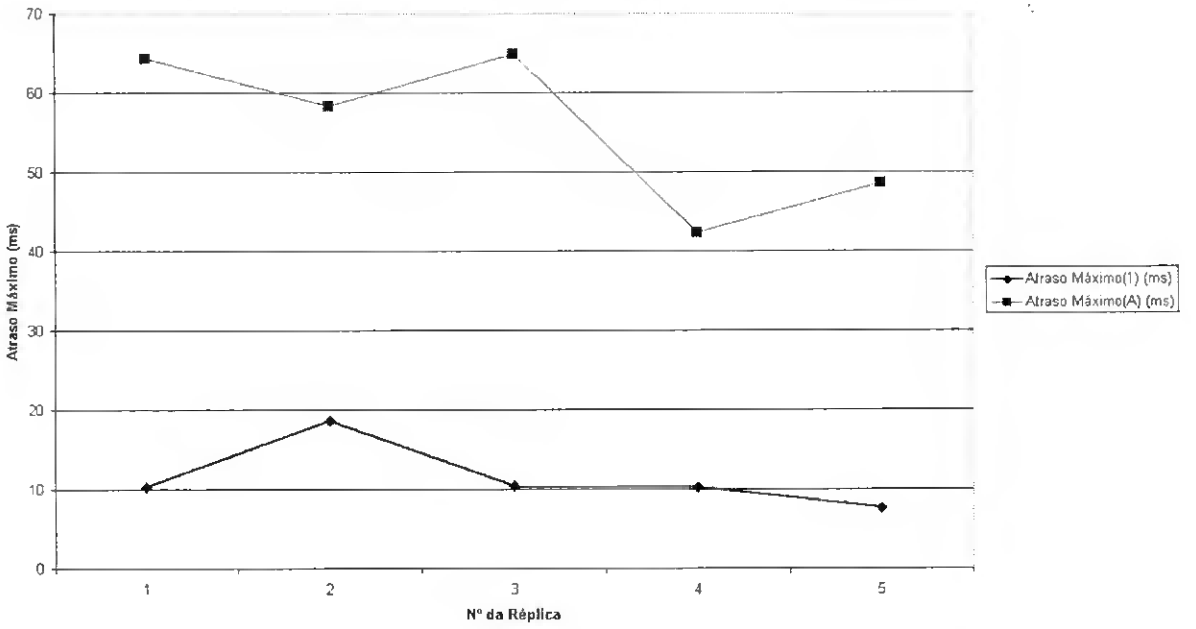


Gráfico 15 - Atraso máximo, com e sem erros, para 15 utlizadores e 5 réplicas

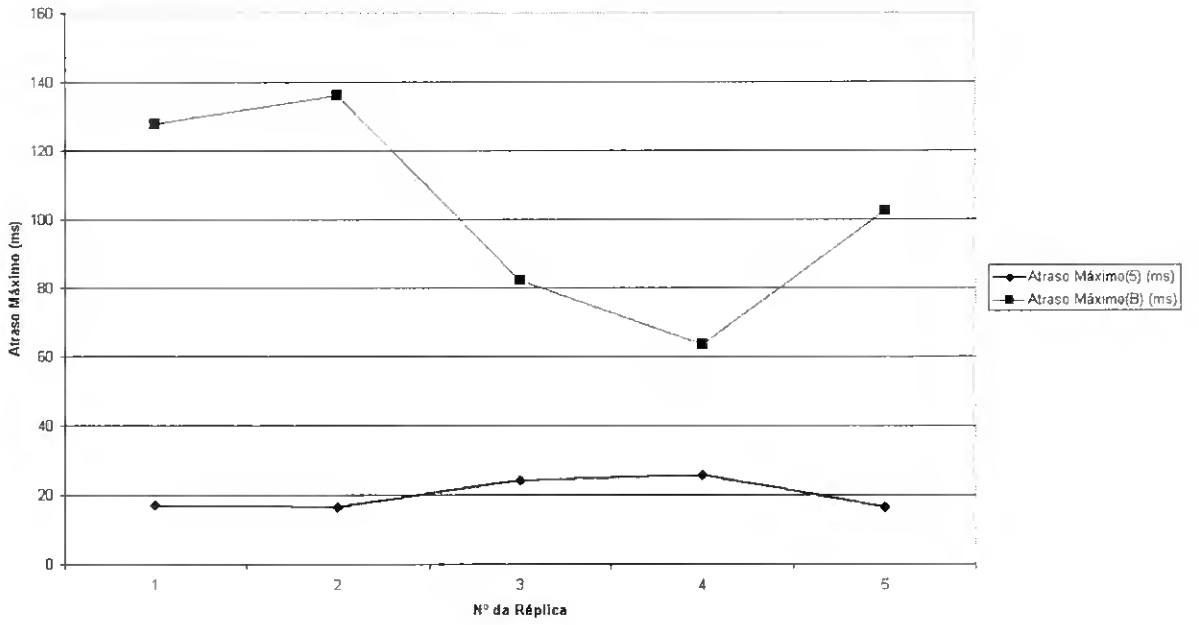


Gráfico 16 - Atraso máximo, com e sem erros, para 45 utlizadores e 5 réplicas

Da representação gráfica podemos concluir que na presença de mais erros os atrasos, médio e máximo, aumentam exponencialmente.

Em termos de percentagem de utilização média da rede obtemos os valores da Tabela 34.

	Maior Utilização Média (%)	Menor Utilização Média (%)	Valor Médio
(1)	2.90%	2.57%	2.77%
(A)	3.02%	2.82%	2.90%
(5)	8.39%	8.10%	8.28%
(B)	9.28%	9.02%	9.14%

Tabela 34 – Maior e menor utilização média nos vários cenários

Concluímos que em todos os cenários de erros a utilização da rede é superior, embora o *throughput* efectivo diminua traduzido num menor número de tramas / pacotes entregues.

UTILIZAÇÃO DO CANAL EM TERMOS DE PACOTES E VELOCIDADE

Da análise dos resultados mantêm-se as conclusões da simulação anterior na presença de erros. Assim, o número de pacotes entregues diminuí proporcionalmente ao número de tramas, a velocidade de entrega é pouco alterada e apesar de erros superiores a rede continua a entregar a totalidade dos pacotes, exibindo percentagem de entrega de 100 % em todos os cenários.

TAMANHO DAS TRAMAS

Mais uma vez os resultados são idênticos aos anteriormente obtidos, ou seja o tamanho da trama depende do trafego gerado e não é afectado pela presença de erros. De referir que não implementámos mecanismos de fragmentação porque o tamanho máximo de trama (1542 bytes) não o justifica.

PERFORMANCE DO LINK IEEE 802.111

Relativamente ao número de colisões, tramas envolvidas e episódios de colisão múltipla são os exibidos na Tabela 35 e Tabela 36.

	Nº Episódios de Colisões	Nº Tramas Envolvidas	Nº Episódios de Colisão Múltipla
(1)	68	136	0
(A)	183	366	0
(A) Versus (1)	**+115**	**+230**	**0**
(5)	643	1286	0
(B)	1547	3098	4
(B) Versus (5)	**+904**	**+1812**	**+4**

Tabela 35 – Diferença entre episódios de colisão e trams envolvidas

	Nº Máximo de Tentativas p/ Resolver (Retransmissões)
(1)	4 Vezes 1 Tentativa 1 Vezes 2 Tentativas
(A)	3 Vez 6 Tentativas 2 Vezes 7 Tentativas
(5)	5 Vezes 2 Tentativas
(B)	5 Vezes 7 Tentativas

Tabela 36 – Número máximo de retransmissões

Concluímos que na presença de maior número de erros o número de colisões aumenta de modo acentuado e consequentemente o número de tramas nelas envolvidas. Também neste cenário as colisões múltiplas tornaram-se uma constante o que se traduz uma realidade de muito mais do que duas estações a acederem ao meio em simultâneo pelo que a performance do protocolo cai.

Outra métrica a referir é o número máximo de tentativas de transmissão que agora aumenta de modo exponencial: Assim, verificamos que com erros elevados o valor do *retry limit* é frequentemente atingido, isto é, o número máximo de tentativas permitido pelo protocolo de acesso ao meio atinge sempre o valor máximo de 7 para o caso de 45 utilizadores. Este denota que a performance desta rede irá ser muito afectada pelos erros e pelos atrasos provenientes de tão elevado número de retransmissões, conforme exibido no Gráfico 17.

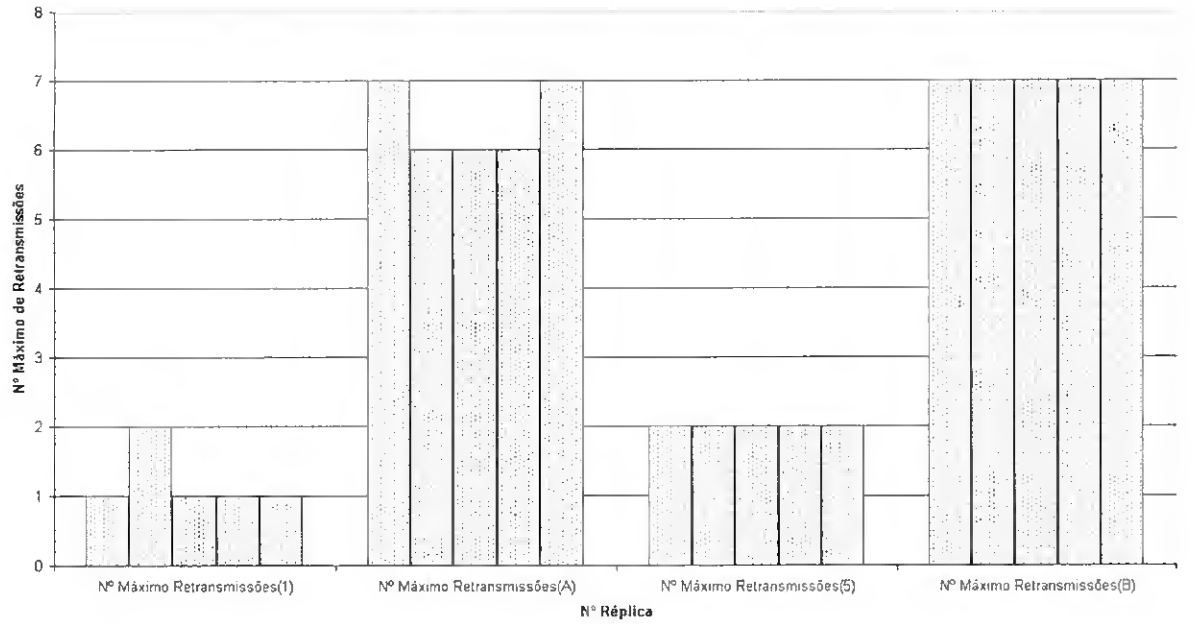


Gráfico 17- Número máximo de retransmissões nas 5 réplicas dos vários cenários

Relativamente aos deferimentos estes apresentam, também, valores muito maiores especialmente para 45 utilizadores, como mostrado na Tabela 37. Assim, o número de tentativas de acesso a um meio ocupado cresce pelo que as estações terão que aguardar mais tempo para poderem transmitir as suas tramas e consequentemente a fila de espera cresce.

	Nº Deferimentos
(1)	34961
(A)	40478
(A) Versus (1)	**+5617**
(5)	157383
(B)	186936
(B) Versus (5)	**+29553**

Tabela 37 – Diferença do número de deferimentos

Graficamente obtemos a seguinte representação do Gráfico 18 e Gráfico 19.

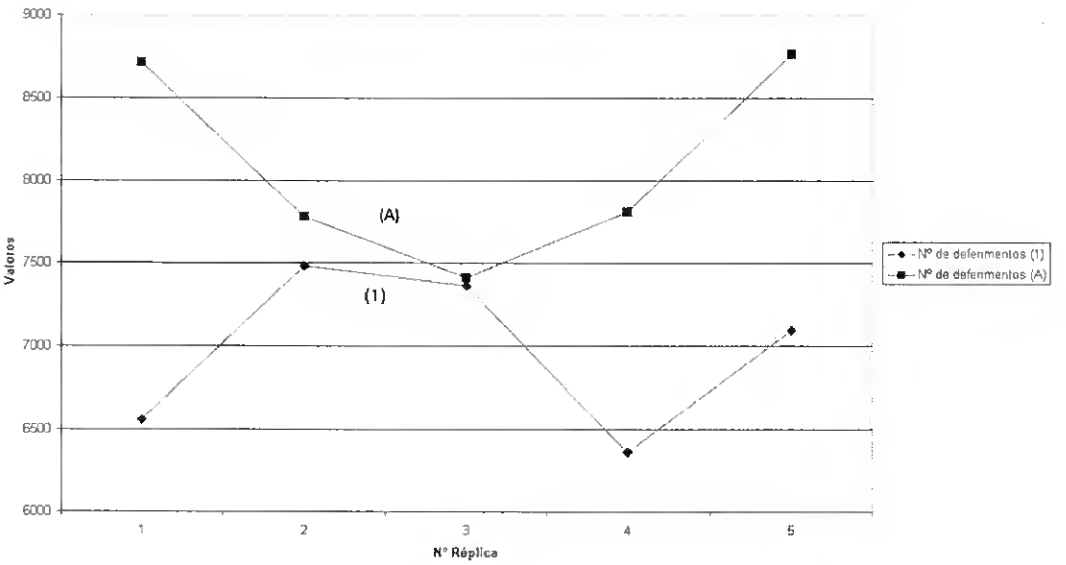


Gráfico 18 – Número de deferimentos (1) versus (A)

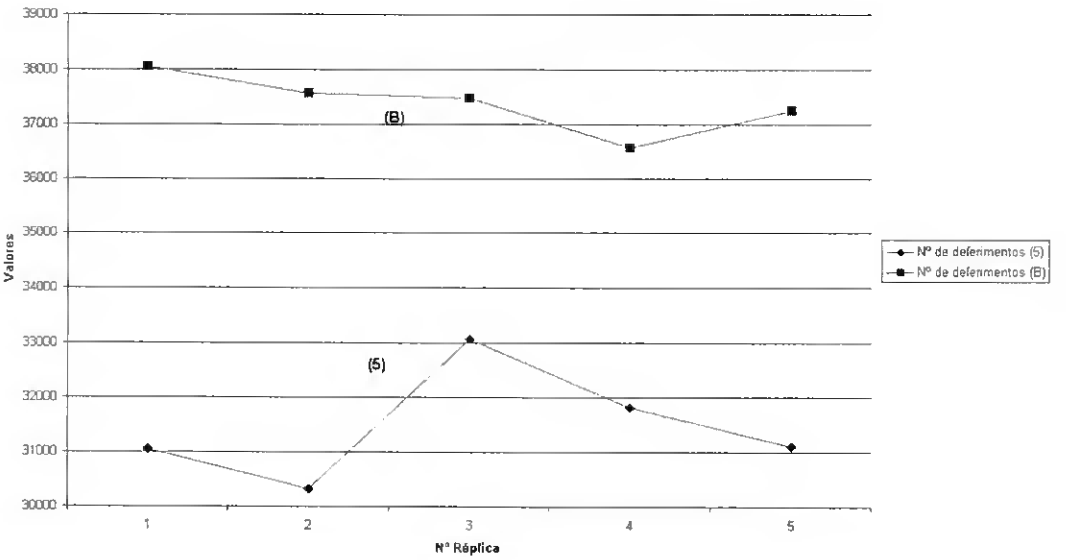


Gráfico 19 – Número de deferimentos (5) versus (B)

CONCLUSÃO

Face à totalidade dos resultados podemos concluir que com maiores erros a rede terá uma performance pior, como seria de esperar. Assim, é notório o aumento dos atrasos totais provocados quer pelo maior número de colisões simples e múltiplas e consequentes retransmissões, quer pelo crescente número de vezes em que tentativas de transmissão, por parte dos utilizadores, têm que ser adiadas.

A implementação do mecanismo de confirmação positiva parece também não produzir os efeitos esperados, na presença de erros, porque a probabilidade de que uma trama ACK seja afectada por erros é igual à de uma trama de dados, contudo a sua retransmissão será mais rápida atendendo ao facto de esta ser uma pequena trama. Pelo que será de questionar se este mecanismo é efectivamente eficaz no combate aos erros das redes de área local sem fios, o que pensamos ser uma questão pertinente para trabalho futuro.

CAPITULO VIII
CONCLUSÃO

Este capítulo apresenta as concluões do estudo efectuado bem como sugestão para trabalho futuro.

VIII.1. Conclusão

Nesta dissertação foram analisadas as redes de comunicação de área local sem fios, designadamente nos aspectos relacionados com o acesso ao meio, as quais se englobam nas redes locais.

A largura de banda é uma das características mais importantes dos vários meios de transmissão, sem excepção do meio ar, a qual influencia de forma directa a velocidade a que, nesse meio, conseguimos transmitir. Num meio com grande largura de banda conseguimos transmitir os nossos dados muito mais rapidamente, contudo uma vez que a mesma tenha que ser partilhada por muitos utilizadores da rede esta pode tornar-se um recurso escasso fazendo diminuir o throughput da rede. Foi nosso objectivo medir a escalabilidade de uma rede de área local sem fios à medida que, à mesma se juntem mais utilizadores.

Outra vertente são os erros, fenómeno que afecta as comunicações em espaço livre e registam, neste meio, taxas muito superiores às das suas contrapartidas cabladas, normalmente de 10^{-5} ou superiores. Com base neste pressuposto e apesar de muito esforço ter sido investido na compreensão do mecanismo de erros bem como na concepção de técnicas com vista à sua resolução concluímos que qualquer bom projecto, como o standard IEEE 802.11, poderá quanto muito aspirar a uma baixa taxa e nunca à sua eliminação. Assim, embora uma taxa de erro de, por exemplo, um por milhão (um bit errado por cada milhão de bits transmitidos) possa parecer diminuta e desprezível, será fácil verificar que à velocidade de operação de 11 Mbps estaremos sujeitos a uma média de 11 erros por segundo. Se para algumas aplicações esta taxa pode ser tolerada já noutras situações isto não acontece. Foi com este intuito que analisamos o comportamento de uma rede de área local sem fios na presença de erros com base em simulações, usando o COMNET, quer de tráfego real quer da presença de erros. Como conclusão geral dos resultados observados podemos referir o comportamento extremamente imprevisível do meio de transmissão das redes de área local sem fios, na presença de erros de transmissão, usando como acesso ao meio o mecanismo DCF, do protocolo CSMA/CA, apenas com tramas ACK.

Por outro lado no nosso estudo usamos uma probabilidade média de erro constante, facto pouco realístico, porque num cenário real isto não se verifica. Assim, acresce dizer que a probabilidade de erro estará directamente ligada ao site onde a rede irá ser instalada e esta directamente dependente da qualidade da ligação que pode passar de muito boa a muito má. Podemos segundo estudos baseados em modelização matemática [38], referir que quando a qualidade da ligação é muito boa (probabilidade de erro próxima de 0), o sucesso de uma transmissão será conseguido logo à primeira tentativa, com grande probabilidade. Pelo contrário, quando a qualidade da ligação é muito má (probabilidade de erro próxima de 1) as sucessivas retransmissões têm todas uma probabilidade muito baixa de sucesso. Contudo, o objectivo do presente trabalho, pela forma como foi conduzido, não é o de tecer conclusões com excessivo rigor cientifico dado que não é feita uma abordagem do problema usando modelos matemáticos, mas sim o de fornecer linhas orientadoras para quem pretenda de um modo rápido conhecer as vantagens e limitações das, tão em voga, WLANs.

A título final concluímos que apesar da existência de erros, de controle difícil num meio com características de transmissão em espaço livre, a rede IEEE 802.11 garante a entrega da totalidade dos dados à custa de uma performance de rede inferior.

VIII.2. Trabalho futuro

De referir o facto do simulador COMNET não incluir, conforme especificado na norma IEEE 802.11, a possibilidade de implementação quer dos mecanismos de RTS/CTS quer da função PCF pelo que não podemos analisar o efeito de tal implementação, que será certamente uma continuação para trabalho futuro.

Como proposta para desenvolvimento de trabalho futuro podemos apontar a utilização dos mecanismos adicionais referidos na norma, nomeadamente DCF com RTS/CTS e a função PCF.

APÊNDICE A

Formato das Tramas IEEE802.11

Cabeçalho da trama

O cabeçalho da trama MAC é formado pelos seguintes campos:

Campo Controle da Trama (*Frame Control*): Este é o primeiro campo do cabeçalho e tem o comprimento de 16 bits que, conforme ilustrado na figura (Ilustração 77), é constituído por vários subcampos. Este campo é enviado de uma estação para outra e carrega informação de controle. Simultaneamente define o tipo de trama como Gestão, Controle e Dados.

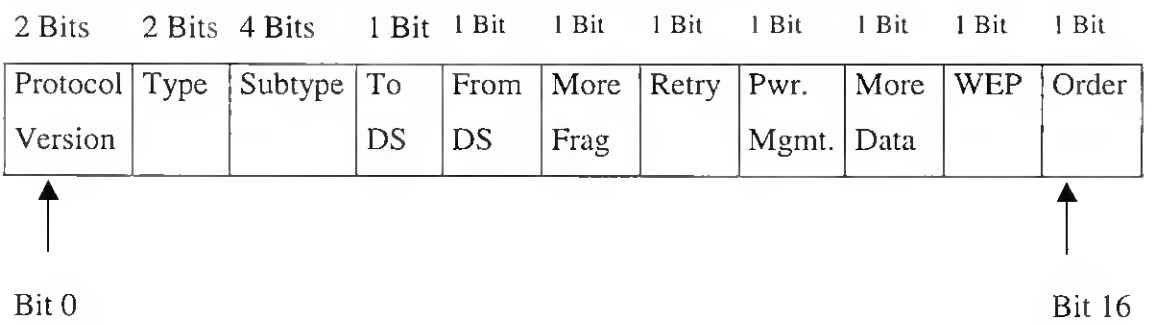


Ilustração 77 Campo Frame Control / Subcampos

Os subcampos do campo de controle da trama são:

Protocol Version: contém a versão do protocolo.

Type e ***Subtype***: conjuntamente identificam o tipo e a função da trama. Existem 32 combinações possíveis;

***To* DS** especifica se a trama se destina ao sistema de distribuição. A coordenação MAC define este campo de bit único a 1 em qualquer trama destinada ao DS e 0 para todas as outras transmissões. Um exemplo onde este bit pode ser definido, será o caso de quando o destinatário da trama estiver numa BSS pertencente a um AP diferente;

***From* DS**: especifica se a trama é proveniente do sistema de distribuição. A coordenação MAC define este campo de bit único a 1 para qualquer trama que deixe o DS e 0 para todas as outras transmissões;

More Fragment: indica se se trata do último fragmento de um MPDU fragmentado, sendo definido a 1 se outro fragmento do mesmo MSDU seguir na trama seguinte;

Retry: indica se se trata ou não de uma trama a ser retransmitida. Se uma trama for uma retransmissão de uma trama prévia, este campo de bit único é definido a 1, sendo 0 para todas as outras transmissões;

PM: (*Power Management*): indica em que modo de gestão de potência a estação emissora ficará a operar após a sequência de troca da trama actual (AM ou PS). A camada MAC colocará neste campo o valor 1, se a estação ficar no modo *sleep* (Power Save, segundo a norma IEEE802.11) e 0 indica que a estação ficará no modo completamente activo (AM). Uma estação receptora pode utilizar esta informação para ajustar transmissões e evitar acordar estações adormecidas. Na maioria dos casos, dispositivos que operam por bateria deverão manter-se no modo de poupança para a conservar;

More Data: este campo alerta a estação receptora para estar pronta para receber tramas adicionais. Se uma estação tem MSDUs adicionais para enviar para outra estação, que está no modo *power-save*, deverá colocar neste campo o valor 1. Este campo é 0 para todas as outras transmissões. Um exemplo da sua utilização é quando uma estação está a enviar um grupo de fragmentos pertencentes a uma única MSDU;

WEP (*Wired Equivalent Privacy*): indica se o corpo da trama foi ou não codificado (encriptação). Se neste campo estiver 1 dirá à estação receptora que o corpo da trama foi processado pelo algoritmo WEP, isto é, os bits de dados foram encriptados usando uma chave secreta. Será 0 para todas as outras transmissões;

Order: Este campo é definido a 1 em qualquer trama que tenha sido enviada usando a classe de serviços *StrictlyOrdered* o que significa, para a estação receptora, que as tramas deverão ser processadas na ordem.

Campo Duration/ID: Este campo, pertencente ao cabeçalho de uma trama IEEE802.11, poderá conter: a duração, em microsegundos, da transação do MPDU contada a partir da trama corrente; a identidade da ligação síncrona, no caso de se tratar de tramas de dados transmitidas sincronamente durante o período sem contenção ou a identificação da estação emissora, caso se trate de tramas do tipo PS-POLL.

Na maioria das tramas este campo contém a duração, a qual depende do tipo de trama enviado. De um modo geral, cada trama contem informação que especifica a duração de transmissão da próxima trama. Por exemplo, numa trama de dados este campo especifica a duração total do próximo fragmento e as estações na rede, ao analisarem-no, descartam transmissões baseadas nessa informação de duração. Apenas nas tramas de controle - *Power Save Poll*, este campo transporta os 14 bits menos significativos da identidade associação da estação emissora, sendo os restantes 2 bits definidos a 1.

Campos de Endereço: O cabeçalho contém quatro campos de endereço (#1, #2, #3 e #4), cujo conteúdo dependendo do tipo de trama a ser enviado. Estes endereços podem incluir: BSSID (*Basic Service Set Identification*), endereço origem, endereço destino, endereço da estação emissora e endereço da estação receptora. A norma IEEE802.11 define a estrutura de endereços onde os seus comprimentos são todos de 48 bits, ou seja, o mesmo endereçamento MAC de 48-bits compatível com a totalidade da família 802. Por outro lado, pode manusear múltiplos meios lógicos e espaços de endereços, o que torna o standard independente da implementação do DS (Distribution System). São definidos os seguintes tipos de endereços:

DA (*Destination Address*): Corresponde ao destino final do MSDU;

SA (*Source Address*): Corresponde ao endereço da entidade MAC que iníciou a transmissão da MSDU;

RA (*Receiver Address*): Corresponde ao endereço do AP que deve ser o próximo a receber a trama;

TA (*Transmitter Address*): Corresponde ao endereço do AP que imediatamente antes enviou a trama.

Os endereços podem ser individuais ou de grupo. Existem dois tipos de endereços de grupo: *multicast*, o qual está associado a um grupo de estações relacionadas de modo lógico e *broadcast*, o qual se refere a todas as estações duma dada rede sem fios, sendo formado por um conjunto de 1s.

Campo de Controle de Sequência: Este campo inclui o número de sequência do MPDU e o número do fragmento, caso a trama de dados tenha sido fragmentada. Os seus 4 bits mais à esquerda formam o subcampo *Fragment Number*, que indica o número de fragmentos de um MSDU, em particular. Este inicia-se em 0 para o primeiro fragmento e depois é incrementado a 1 para cada transmissão sucessiva. Os 12 bits seguintes, formam o subcampo *Sequence Number*, iniciando em 0 e incrementado por 1, para cada transmissão MSDU subsequente. Cada fragmento pertencente a uma MSDU específica terá o mesmo valor neste campo, podendo apenas uma MSDU estar pendente, de cada vez. Na recepção de uma trama, a estação pode filtrar tramas duplicadas pela análise dos números de sequência e fragmento. A estação saberá se uma trama é uma duplicação se os seus números de sequência e fragmento coincidirem com os da trama, imediatamente, anterior, ou se o bit *retry* estiver definido a 1. Esta duplicação de tramas pode ocorrer quando uma estação recebe uma trama sem erros, envia o respectivo ACK para a estação emissora mas este, por qualquer motivo, é destruído. Ao não receber o ACK durante um período de tempo específico, a estação

emissora retransmite a trama , causando a sua duplicação. A estação destino envia um ACK da trama retransmitida, mesmo que esta seja descartada na detecção da sua duplicação.

Corpo da trama

O campo corpo da trama, de dimensão variável, contem informação especifica relativa ao tipo de trama que esta a ser transmitida. A sua dimensão varia desde o número mínimo de 0 *bits* a um máximo de 2312 octetos, dependendo da implementação da camada física. Se a trama não necessitar de transportar informação este campo terá comprimento zero.
Caso se trate de uma trama de dados, este campo contem uma unidade de dados LLC (vulgarmente denominada MSDU). No caso das tramas de gestão e controle, inclui parâmetros específicos pertencentes ao serviço, em particular, implementado pela trama.

Campo de CRC / FCS (Frame Check Sequence)

Este campo permite fazer a detecção de erros nas tramas aquando da sua recepção, pela implementação de um CRC que testa a existência de erros de transmissão.
A camada MAC calcula, na estação emissora, um FCS de 32 bits usando um CRC (Cyclic Redundancy Check) e coloca o seu resultado neste campo. Este valor é calculado, sobre todos os campos do cabeçalho e do corpo da trama, utilizando o seguinte polinómio:

$$G(x)=x^{32}+x^{26}+x^{23}+x^{16}+x^{12}+x^{11}+x^{10}+x^{8}+x^{7}+x^{5}+x^{4}+x^{2}+x+1$$

O resultado de coeficiente de ordem superior é colocado no bit mais à esquerda do campo.

TIPO DAS TRAMAS IEEE802.11

O tipo das tramas apresentadas neste apêndice está de acordo com o formato da versão da norma IEEE802.11.

As tramas, segundo o subcampo *Type* do campo *Frame Control*, definem-se nos seguintes tipos: Gestão, Controle e Dados.
Assim segundo o campo Type (2 bits) :

Bit 3, Bit 2	Tipo
0,0	Trama de Gestão
0,1	Trama de Controle
1,0	Trama de Dados
1,1	Reservado

As tramas, segundo o subcampo *Type* e campo *Subtype* do campo Frame Control, definem-se nas seguintes funções:

Tipo de Trama	Campo Subtype (Bits 7,6,54)	Função
GESTÃO	000	Association Request
(bit3, bit 2) = 00	0001	Association Response
	0010	Reassociation Request
	0011	Reassociation Request
	0100	Probe Request
	0101	Probe Response
	0110-0111	Reserved
	1000	Beacon
	1001	Announcement Traffic Indication Map (ATIM)
	1010	Disassociation
	1011	Authentication
	1100	Deauthentication
	1101-1111	Reserved
CONTROLE	0000-1001	Reserved
(bit3, bit 2) = 01	1010	Power-Save (PS) Poll
	1011	Request to Send (RTS)
	1100	Clear to Send (CTS)
	1101	Acknoledgement (ACK)
	1110	Contention Free (CF) End
	1111	CF End + CF ACK
DADOS	0000	Data

(bit3, bit 2) = 10	0001	Data + CF ACK
	0010	Data + CF Poll
	0011	Data + CF ACK + CF Poll
	0100	Null (no data)
	0101	CF ACK
	0110	CF Poll
	0111	CF ACK + CF Poll
	1000-1111	Reserved
RESERVADO (bit3, bit 2) = 11	000-1111	

TRAMAS DE GESTÃO

O formato genérico das todas as tramas de gestão é o seguinte:

2 Octetos	2 Octetos	6 Octetos	6 Octetos	6 Octetos	2 Octetos	0-2312 Octetos	4 Octetos
Frame Control	Duration	DA	SA	BSSID	Sequence Control	Frame Body	FCS

Sendo, DA (*Destination Address*); SA (*Source Address*) e BSSID (BSS *Identification*).

O campo *Duration* em todas as tramas de gestão, durante o período sem contenção (*contention free*) do modo de operação PCF, é definido com o decimal 32,768 (valor hexadecimal de 8000), capacitando as tramas de gestão de tempo suficiente para estabelecer comunicações, antes que outras estações tenham tempo para aceder ao meio.

Por outro lado, durante o período baseado em contenção do modo de operação DCF (como definido pelo CSMA baseado em DCF), todas as tramas de gestão têm o campo *Duration*, definido do seguinte modo:

0, se o endereço destino (DA) é um endereço de grupo;

Se o bit *More Fragments* = 0 e o endereço destino (DA) for um endereço individual (*unicast*), este campo contem o tempo, em microsegundos, requerido para transmitir um trama ACK e um intervalo SIFS.

Se o bit *More Fragments* = 1 e o endereço destino (DA) for um endereço individual (*unicast*), este campo contem o tempo, em microsegundos, requerido para transmitir o próximo fragmento, duas tramas ACK e três intervalos SIFS.
Uma estação ao receber uma trama de gestão, executa correspondência de endereços para tomar decisões de recepção. Estas são tomadas com base no conteúdo do campo *Address 1* da trama MAC, o qual é o endereço destino (DA). Se o endereço corresponder ao da estação, esta completa a recepção da trama e retira-a da camada LLC. Se isto não se verificar a estação ignora o resto da trama.

TPOS DE TRAMAS DE GESTÃO

O corpo da trama varia consoante o seu tipo. Assim, são definidos os seguintes tipos de tramas de gestão bem como a informação contida em cada uma delas:
Association Request: Uma estação enviará esta trama para um AP, caso se pretenda associar com ele. A estação ficará associada ao AP após este conceder permissão.

Ordem	Informação
1	Capacidade
2	ESS Id
3	Velocidades de tx suportadas

Association Response: Após um AP receber uma trama do tipo anterior, enviará esta trama para indicar se aceitou a associação com a estação emissora.

Ordem	Informação
1	Capacidade
2	Código de estado
3	SID (*Station* ID)
4	Velocidades de tx suportadas

Reassociation Request: Uma estação envia esta trama para um AP caso pretenda reassociar-se com ele. Esta operação pode ocorrer se a estação se mover para fora do intervalo de acção de um AP e para dentro do espaço de outro.

A estação necessitará de se reassociar com o novo AP (em vez de mera associação) e assim, este saberá que necessita de negociar o reencaminhamento de tramas de dados do AP anterior.

Ordem	Informação
1	Capacidade
2	Endereço do AP corrente
3	ESS Id
4	Velocidades de tx suportadas

Reassociation Resposte: Após um AP receber uma trama do tipo anterior, enviará esta trama para indicar se aceita a reassociação com a estação emissora.

Ordem	Informação
1	Capacidade
2	Endereço do AP corrente
3	SID (*Station* Id)
4	Velocidades de tx suportadas

Probe Request: Umas estação envia este tipo de trama para obter informação de uma congénere ou de um AP. Por exemplo, uma estação pode enviar esta trama para determinar se determinado AP está disponível.

Ordem	Informação
1	Capacidade
2	ESS Id
3	Velocidades de tx suportadas

Probe Response: Se uma estação ou AP receber uma trama do tipo anterior, responderá enviando esta trama contendo parâmetros especiais sobre si própria. Como por exemplo, conjuntos de parâmetros para camadas físicas FHSS e DSS.

Ordem	Informação

1	Time_Stamp
2	Beacon_Interval
3	Domínio de regulamentação
4	Capacidade
5	ESS Id
6	Velocidades de tx suportadas
7	Parâmetros FH
	Parâmetros CF

Beacon: Numa rede infraestruturada, um AP envia, periodicamente, uma trama deste tipo (de acordo com o parâmetro da MIB *aBeaconPeriod*) o que fornece sincronização entre estações que utilizem o mesmo camada física (PHY). Esta trama inclui uma mostra do tempo (*timestamp*) que todas as estações usam, para actualizar o seu *timer*. Isto corresponde ao que 802.11 define como TSF (*Timing Synchronization Function*).

Se o AP suportar a função PCF, usará uma trama deste tipo para anunciar o início do período sem contenção (*contention free*). SE a rede for ad-hoc (BSS independente, não tendo AP), todas as estações periodicamente enviam estas tramas, com o objectivo de sincronização.

Ordem	Informação
1	Time_Stamp
2	Beacon_Interval
3	Domínio de regulamentação*
4	Capacidade
5	ESS Id
6	Velocidades de tx suportadas
7	Parâmetros FH
8	Parâmetros CF
9	DTIM
10	TIM

***ATIM* (*Announcement Traffic Indication Function*)**: Uma estação que tenha tramas armazenadas, destinadas a outras estações, envia a cada uma delas uma trama ATIM durante

* 1 EUA, 2 Europa, 3 Japão

a janela ATIM, a qual se segue imediatamente após uma transmissão de trama *Beacom*. A estação transmite, então, estas tramas para o receptor adequado, o que alertará estações no modo sleep para permanecerem acordadas, o tempo suficiente, para receberem as suas respectivas tramas.

Disassociation: Se uma estação ou AP pretenderem terminar uma associação, enviarão esta trama para a estação oposta. Uma única trama deste tipo pode terminar uma associação com mais do que uma estação, através do endereço broadcast com todos os bits definidos a 1s.

Authentication: Uma estação envia esta trama para uma estação ou AP, com o qual se pretenda autenticar. A sequência de autenticação consiste na transmissão de uma os mais tramas deste tipo, dependendo do tipo de autenticação a ser implementada, que poderá ser *Open System* ou *Shared Key*.

Deauthentication: Uma estação envia esta trama para uma estação ou AP, com o qual pretenda terminar o processo de comunicações seguras.

O conteúdo do campo corpo de trama, das tramas de gestão, depende do tipo a ser enviado. A tabela (Tabela 38) ilustra os conteúdos do *Frame Body* de cada subtipo de trama de gestão.

O standard IEEE802.11 descreve os elementos do corpo da trama dos vários subtipos de tramas de gestão. Iremos, em seguida, fazer alusão a estes:

Authentication Algorithm Number: Estes elemento apenas é encontrado em tramas de Autenticação. Este campo especifica o algoritmo de autenticação usado pela estação e pelo AP. O seu valor é 0 para autenticação *Open System* ou 1 para autenticação *Shared* Key.

Authentication Transaction Sequence Numbe: Estes elemento apenas é encontrado em tramas de Autenticação. Este campo indica o estado de progresso do processo de autenticação.

Beacon Interval: Define o número de unidades de tempo entre intervalos de transmissões de tramas Beacon.

Capability Information: Este campo anuncia a informação de capacidade de uma estação em particular. Por exemplo, uma estação pode indicar, neste elemento, se deseja ser *polled*.

Current AP Address: Este campo indica o endereço do AP ao qual a estação está presentemente associada.

Listen Interval: Este valor identifica, em unidades de *Beacon Interval*, o quanto frequentemente acordará, para escutar tramas de gestão Beacon.

Reason Code: Este campo indica o motivo, via um código numerado, pelo qual uma estação gerou uma desassociação ou desautenticação não solicitada.

Exemplos de motivos poderão ser: Autenticações prévias deixam de ser válidas; A estação que requereu a associação não esta autenticada com a estação que respondeu; Desassociação devida a inactividade.

***Association* ID (AID)**: Esta ID, a qual é assignada por um AP durante o processo de associação, é uma identificação de 16 bits da estação, a qual corresponde a essa associação em particular.

Status Code: Este código indica o status de uma operação em particular. Exemplos serão: sucesso, falha não especificada, associação não autorizada porque o AP é incapaz de manusear estações adicionais, autenticação rejeitada devido ao excesso de tempo (timeout) de espera pela próxima trama da sequência.

Timestamp: Este campo contem o valor do timer da estação emissora, quando transmite a trama.

***Service Set Identify* (SSID)**: Este campo contem a identificação da ESS.

Supported Rates: Este campo identifica todas as taxas de dados que uma estação, em particular, pode receber. Este valor representa a taxa de dados em incrementos de 500 Kbps. A coordenação MAC tem capacidade para alterar taxas de dados, de modo a optimizar a performance da transmissão de tramas.

FH *Parameter Set*: Este campo indica o tempo de pausa e o padrão de salto necessários para sincronizar duas estações que usem camada física FHSS.

DS *Parameter Set*: Este campo indica o número de canal que as estações estão a usar com camada física DSSS.

CF *Parameter Set*: Este campo consiste numa série de parâmetros que suportam a função PCF.

TIM: O elemento *traffic indication map* especifica quais as estações que têm MSDUs armazenadas no AP.

IBSS *Parameter Set*: Este campo contem parâmetros que suportam as redes IBSS (ad-hoc).

Challenge Text: Este campo contem o texto alterado de uma sequência de autenticação *shared key*.

Conteúdo do Corpo da trama	Association Request	Association Response	Reassociation Request	Reassociation Response	Probe Response	Probe Request	Beacon	Disassociation	Authentication	Deauthentication
Authentication Algorithm Number									X	
Authentication Transaction Sequence Number									X	
Beacon Interval					X		X			
Current AP Addresss			X							
Listen Interval	X		X							
Reason Code								X		X
Association ID (AID)		X		X						
Status Code		X		X					X	
Timestamp					X		X			

Conteúdo do Corpo da trama	**Association Request**	**Association Response**	**Reassociation Request**	**Reassociation Response**	**Probe Response**	**Probe Request**	**Beacon**	**Disassociation**	**Authentication**	**Deauthentication**
Service Set Identity (SSID)	X		X		X	X	X			
Supported Rates	X	X	X	X	X	X	X			
FH Parameter Set					X		X			
DS Parameter Set					X		X			
CF Parameter Set					X		X			
Capability Information	X	X	X	X	X		X			
Traffic Indication Map (TIM)							X			
IBSS Parameter Set					X		X			
Challenge									X	

Text										

Tabela 38 O conteúdo do corpo da trama de gestão dependo do subtipo de trama em particular

TRAMAS DE CONTROLE

Subtipos de tramas de controle são os apresentados em seguida, bem como a respectiva estrutura.

RTS ***(Request to Sen)***: Uma estação envia uma trama deste tipo, a uma estação receptora em particular, para negociar o envio de uma trama de dados. Através do atributo *aRTSthershold*, armazenado na MIB, podemos configurar uma estação para sempre, nunca ou apenas em tramas maiores que um comprimento específico, iniciar uma sequência de trama RTS.

A figura (Ilustração 78) ilustra o formato de uma trama RTS, onde RA (Receiver Address) e TA (Transmitter Address).

2 Octetos	2 Octetos	6 Octetos	6 Octetos	4 Octetos
Frame Control	Duration	RA	TA	FCS

Ilustração 78 Formato da trama RTS

O valor do campo *duration*, em microsegundos, corresponde à quantidade de tempo que a estação emissora necessita para transmitir, uma trama CTS, uma trama ACK e três intervalos SIFS.

CTS ***(Clear to Send)***: Após receber uma trama RTS, a estação envia uma trama deste tipo para reconhecer à estação emissora o direito de enviar tramas de dados. As estações terão que ter sempre atenção à informação de duração e resposta a uma trama RTS, mesmo se não estiverem definidas para iniciar sequências de tramas RTS.

A figura (Ilustração 79) ilustra o formato de uma trama CTS.

2 Octetos	2 Octetos	6 Octetos	4 Octetos
Frame Control	Duration	RA	FCS

Ilustração 79 Formato da trama CTs

O valor do campo *duration* em microsegundos, define a quantidade de tempo do campo duração da trama RTS prévia menos o tempo requerido para transmitir a trama CTS e seus intervalos SIFS.

ACK ***(Acknowledgment)***: Uma estação que receba uma trama sem erros, pode enviar uma trama ACK para a estação emissora para reconhecer a recepção com sucesso da mesma.
A figura (Ilustração 80) ilustra o formato de uma trama ACK.

2 Octetos	2 Octetos	6 Octetos	4 Octetos
Frame Control	Duration	RA	FCS

Ilustração 80 Formato da trama ACK

O valor do campo *duration* em microsegundos, é igual a zero se o bit More Frag., do campo Frame Control da trama de dados ou gestão precedente for definido a 0. Se, pelo contrário, for definido a 1, o campo duration será a quantidade de tempo do campo duration da trama de dados ou gestão precedente menos o tempo requerido para transmitir a trama ACK e os seus intervalos SIFS.

Power-Save (PS Poll): Se uma estação receber uma trama deste tipo, a estação actualizará o seu NAV (*Network Allocation Vector*), o qual é uma indicação dos períodos de tempo, nos quais uma estação não iniciara uma transmissão. O NAV contem uma previsão do futuro trafego no meio.
A figura (Ilustração 81) ilustra o formato de uma trama PS Poll, onde AID (Association Identifier), BSSID (Basic Service Set Identification)e TA (Transmitter Address).

2 Octetos	2 Octetos	6 Octetos	6 Octetos	4 Octetos
Frame Control	AID	BSSID	TA	FCS

Ilustração 81 Formato da trama PS Poll

Contention-Free End (CF End): Esta trama designa o fim do período com contenção, o qual faz parte do modo se operação PCF.
A figura (Ilustração 82) ilustra o formato de uma trama CF End, onde BSSID (Basic Service Set Identification)e RA (Receiver Address).

2 Octetos	2 Octetos	6 Octetos	6 Octetos	4 Octetos
Frame Control	Duration	Ra	BSSID	FCS

Ilustração 82 Formato das Tramas CF End e CF End + CK ACK

Nesta trama o campo *duration* é sempre definido a zero e o campo RA contem o endereço do grupo de *broadcast*.

CF End + CF ACK: Esta trama confirma o anúncio do fim do período sem contenção de uma trama CF End.

A figura (Ilustração 82) ilustra o formato de uma trama **CF End + CF ACK**, onde BSSID (Basic Service Set Identification)e RA (Receiver Address).

Nesta trama o campo *duration* é sempre definido a zero e o campo RA contem o endereço do grupo de *broadcast*.

TRAMAS DE DADOS

O propósito principal de uma trama de dados é transportar informação, como por exemplo MSDUs, para a estação destino para o *handoff* da camada LLC aplicável. AS tramas de dados podem transportar informação específica, de supervisão ou tramas não numeradas.

O formato das tramas é o exibido na figura (Ilustração 83).

2 Octetos	2 Octetos	6 Octetos	6 Octetos	6 Octetos	2 Octetos	6 Octetos	0-2312 Octetos	4 Octetos
Frame Control	Duratio/ Id	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

Ilustração 83 Formato da trama de dados

To Ds	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	AS	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Ilustração 84 Conteúdos dos campos de endereço

Os subcampos To DS e From DS, do campo Frame Control, definem os conteúdos válidos dos campos de endereço da trama de dados, como exibido na figura (Ilustração 84).

APÊNDICE B

PRIMITIVAS DE SERVIÇO DA CAMADA FÍSICA IEEE802.11

PHY – DATA.request: Transfere um octeto de dados da camada MAC para a camada física. Esta primitiva apenas é possível após a camada física expedir um PHY – TXSTART.confirm.

PHY – DATA.indication: Transfere um octeto de dados, recebidos da camada física, para a camada MAC.

PHY – DATA.confirm: Esta primitiva é enviada da camada física para a camada MAC confirmando a transferência de dados da camada MAC para a camada física.

PHY – TXSTART.request: Esta primitiva é um pedido da camada MAC para a camada física iniciar a transmissão de um MPDU.

PHY – TXSTART.confirm: Esta primitiva é enviada da camada física para a camada MAC e destina-se a confirmar o início da transmissão de uma MPDU.

PHY – TXEND.request: Esta primitiva é um pedido da camada MAC para a camada física, para terminar a transmissão de um MPDU. A camada MAC expede esta primitiva após receber a ultima primitiva *PHY – DATA.confirm* para uma MPDU em particular.

PHY – TXEND.confirm: Esta é uma primitiva enviada da camada física para a camada MAC confirmando o fim da transmissão de uma MPDU, em particular.

PHY – CCARESET.request: Esta primitiva é um pedido da camada MAC para a camada física, para fazer o *reset* à *state machine* avaliação de canal livre (*clear chanel assessement*)

PHY – CCARESET.confirm: Esta é uma primitiva da camada física para a camada MAC confirmando o *reset* pedido pela primitiva anterior.

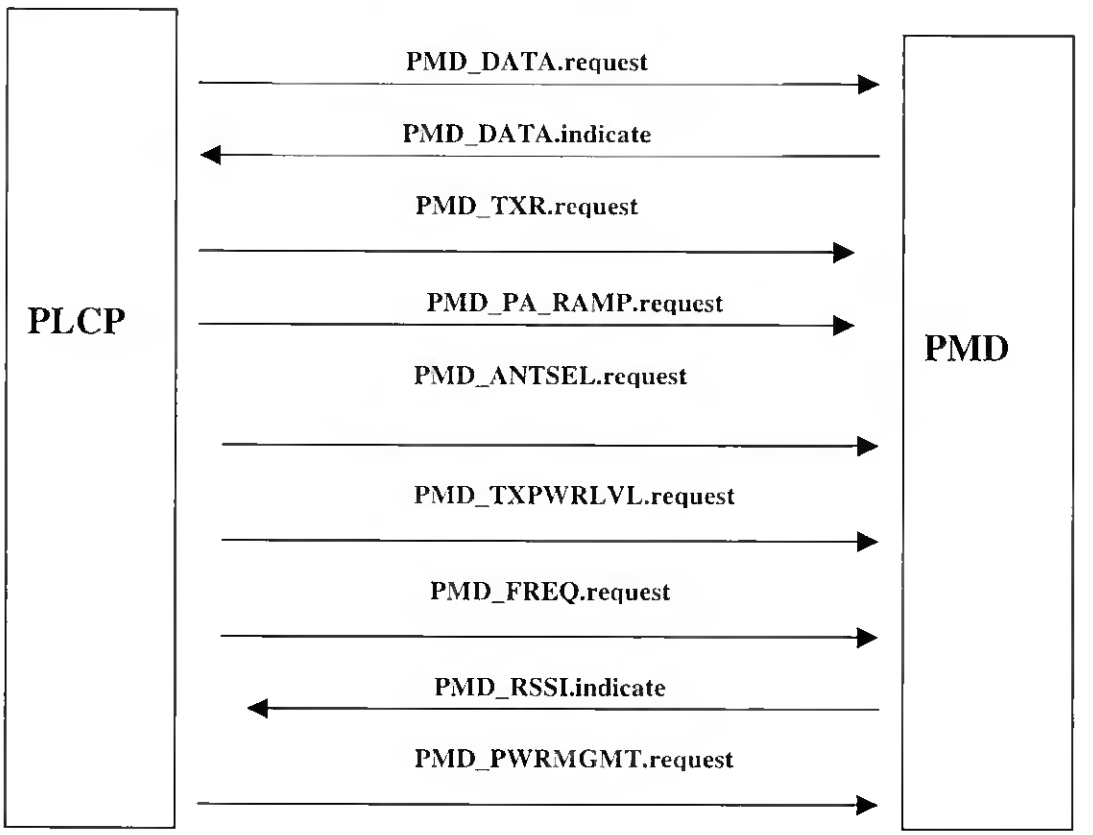
PHY – CCA.indication: Esta é uma primitiva enviada da camada física para a camada MAC para indicar o estado do meio. O estado poderá ser livre (*idle*) ou ocupado (*busy*). A camada física envia esta primitiva de cada vez que o canal mudar de estado.

PHY – RXSTART.indication: Esta é uma primitiva enviada da camada física para a camada MAC para indicar que a PLCP recebeu um delimitador de início de trama válido e respectivo cabeçalho PLCP (baseado no texto de erro CRC contido no cabeçalho).

PHY – RXEND.indication: Esta é uma primitiva enviada da camada física para a camada MAC para indicar que *state machine* receptora completou a recepção de uma MPDU.

PRIMITIVAS DE SERVIÇO DA SUBCAMADA PMD / FHSS

A subcamada PLCP comunica com a camada PMD através das seguintes primitivas, conforme ilustrado na figura seguinte.



PMD_DATA.request: Esta primitiva é um pedido da PLCP dirigido à PMD, para transferir um bit de dados 0 ou 1. Esta acção diz à PMD para modular e enviar o bit de dados através do meio.

PMD_DATA.indicate: A PMD implemente esta primitiva para transferir bits de dados para a PLCP. O valor enviado é 0 ou 1.

PMD_TXR.request: A PLCP usa este pedido para colocar a PMD no modo de emissão ou recepção. O valor enviado é emite ou recebe.

PMD_PA_RAMP.request: Este pedido da PLCP para a PMD inicia a subida ou descida do amplificador de potência do emissor. O valor enviado é ON ou OFF.

PMD_ANTSEL.request: A PLCP envia esta primitiva para seleccionar a antena que a PMD deverá usar. O valor enviado é um número de 1 a N, onde N é o número total de antenas que

o PMP suporta. Para transmitir, este pedido selecciona uma antena. Para receber, o PLCP pode seleccionar múltiplas antenas para implementar a função de diversidade.

PMD_TXPWRLVL.request: Este pedido, da PLCP, define o nível de potência de transmissão da PMD. O valor é Nível 1, Nível 2 e assim por diante, até ao Nível 8 os quais correspondem a os níveis de potência da MIB.

O Nível 1, por exemplo, corresponde ao valor MIB, TxPowerLevel 1.

PMD_FREQ.request: A PLCP envia esta primitiva para a PMD para definir a frequência de transmissão. O valor enviado é a ID do canal.

PMD_RSSI.indicate: A PMD usa esta primitiva para devolver uma indicação continua da potência do sinal recebido do meio PLCP.

A PLCP usa esta primitiva para funções de determinação de canal desocupado. O valor pode variar da potência de sinal 0 (fraco) a 15 (forte).

PMD_PWRMGMT.request: A PLCP envia esta primitiva ao PMD para colocar o rádio no modo *sleep* ou modo *standby* e assim despender menos potência. O valor enviado pode ser ON (modo completamente operacional) ou OFF (modo *standby* ou *sleep*).

PRIMITIVAS DE SERVIÇO PLME (Physical Sublayer Management Entity)

A camada física acede à MIB (Management Information Base) através das seguintes primitivas de serviço PLME:

PLME-GET.request: Pede o valor de um atributo MIB específico.

PLME-GET.confirm: Devolve o valor do atributo MIB aplicável ao pedido anterior.

PLME-SET.request: Pede que a MIB defina um atributo específico para um dado valor em particular.

PLME-SET.confirm: Devolve o *status* do pedido anterior.

PRIMITIVAS DE SERVIÇO DA SUBCAMADA PMD / DSSS

PMD_DATA.request: Esta primitiva é um pedido da PLCP dirigido à PMD, para transferir um símbolo de dados. O valor do símbolo enviado com este pedido é o bit de dados 1 ou 0 se transmitir a 1 Mbps ou qualquer combinação de 2 bits de dados se transmitir a 2 Mbps. Esta primitiva deve ser enviada para a PMD antes de se iniciar a próxima transmissão de dados, com a primitiva PMD_TXSTART.request.

PMD_DATA.indicate: A subcamada PMD implementa esta primitiva para transferir símbolos para a PLCP. Tal como na primitiva anterior, o valor do símbolo enviado com este pedido é o bit de dados 1 ou 0 se transmitir a 1 Mbps ou qualquer combinação de 2 bits de dados se transmitir a 2 Mbps.

PMD_TXSTART.request: A subcamada PLCP envia esta primitiva para a PMD para iniciar a transmissão da próxima PPDU (trama completa).

PMD_TXEND.request: A subcamada PLCP envia esta primitiva para a PMD para terminar a transmissão da PPDU.

PMD_ANTSEL.request: A subcamada PLCP envia esta primitiva para seleccionar a antena que a PMD deve usar. O valor enviado é um número de 1 a N, onde N corresponde ao número total de antenas que a PMD suporta. Para transmitir este pedido selecciona uma antena. Para receber, a subcamada PLCP pode seleccionar múltiplas antenas por diversidade.

PMD_ANTSEL.indicate: Indica qual a antena que a camada física usou para receber a última PPDU.

PMD_TXPWRLVL.request: Este pedido, da PLCP, define o nível de potência de transmissão da PMD. O valor é Nível 1, Nível 2 e assim por diante, até ao Nível 8, os quais correspondem a os níveis de potência da MIB.

O Nível 1, por exemplo, corresponde ao valor MIB, TxPowerLevel 1.

PMD_RATE.request: A subcamada PLCP envia esta primitiva para a PMD para indicar qual a taxa de dados (1 ou 2 Mbps) à qual a parte MPDU, da PPDU, deve ser enviada. Esta taxa de dados aplica-se apenas à taxa de transmissão. A subcamada PMD deve ser sempre capaz de receber a todas as taxas de dados possíveis.

PMD_RATE.indicate: Esta primitiva é enviada da subcamada PMD para PLCP, quando a PMD detecta a presença do campo *signaling*, no preâmbulo PLCP. Este identifica a taxa de dados (1 OU 2 Mbps) da trama recebida.

PMD_RSSI.indicate: A subcamada PMD usa esta primitiva, durante o modo de recepção, para devolver uma indicação continua da potência do sinal recebido (RSSI, *Receiver Signal Strength Indication*) do meio para a PLCP.

A PLCP usa esta primitiva para funções de determinação da disponibilidade do canal. O valor do RSSI é um de 256 níveis, representado por uma 8-bit *data word.*

PMD_SQ.indicate: Esta primitiva, opcional, fornece uma medida da qualidade do sinal (SQ, *Signal Quality*) do código de correlação DSSS Pn. O seu valor +e um de 256 níveis, representado por um 8-bit *data word.*

PMD_CS.indicate: A subcamada PMD envia esta primitiva para indicar que está a decorrer a demodulação do sinal de dados. Isto assinala a recepção de uma PPDU DS 802.11, válida.

PMD_ED.indicate: Esta primitiva, opcional, indica que o valor da energia, representada por uma primitiva PMD_RSSI.indicate em particular, está acima de um limiar pré-definido (armazenado no parâmetro MIB, aED_Threshold). O valor desta primitiva pode ser autorizado, caso o parâmetro da MIB esteja acima do limite ou não autorizado na situação inversa. Esta primitiva fornece um meio de detectar a presença de sinais que não sejam do tipo DS 802.11 ou, pelo menos, os que excedam o valor limiar.

PMD_ED.request: A subcamada PLCP usa esta primitiva para definir o valor da energia na PMD - *energy detect threshold*, o qual corresponde ao mínimo sinal que a PMD consegue detectar. Este valor vai ser definido com base no parâmetro MIB, aED_Threshold.

PMD_CCA.indicate: A subcamada PMD envia esta primitiva para a PLCP para indicar a detecção de energia RF ligada ao algoritmo CCA.

CAMPOS DA TRAMA PLCP / FHSS

⇒ **SYNC**: Este campo é composto por uma alternância de zeros e uns, alertando o receptor da presença de um sinal potencialmente receptível. O receptor iniciará a sua sincronização com o sinal chegado após detectar este campo.

⇒ ***Start Frame Delimiter***: O conteúdo deste campo é sempre o seguinte padrão de bit, definindo o início de uma trama: 0000110010111101.

⇒ **PLW (PSDU *Length Word*)**: Este campo especifica o tamanho do PSDU em octetos. O receptor usará esta informação para determinar o fim da trama.

⇒ **PSF (PLCP *Signaling Field*)**: Este campo identifica a taxa de dados da parte da trama PSDU purificada. O preâmbulo e cabeçalho do PPDU são sempre enviados a 1 Mbps, mas a parte restante pode ser enviada a diferentes taxas de dados, como indicado por este campo. A subcamada PMD, contudo, deve suportar esta taxa de dados.

O bit mais à esquerda do campo PSF, bit 0, é sempre definido a zero. A tabela seguinte identifica a taxa de dados com base nos valores dos bits 1, 2 e 3.

Bit 1-3	**Taxa de dados (Mbps)**
000	1.0
001	1.5
010	2.0
011	2.5
100	3.0
101	3.5
110	4.0
111	4.5

⇒ ***Header Error Check***: O conteúdo deste campo é um resultado CRC de 16 bits baseado no algoritmo de detecção de erro, CCITT CRC-16. O polinómio gerador para este algoritmo é $G(x)=x^{16}+x^{12}+x^5+1$. A camada física não determina se o PSDU contem erros. A camada MAC testará erros baseados em FCS (*Frame Check Sequence*).

A técnica CRC-16 detecta todos os erros de bits únicos e duplos e assegura detecção de 99.998 % de possíveis erros [100]. A maioria dos entendidos acredita que é suficiente para blocos de transmissão de dados até 4 kilobytes.

⇒ ***Whitened* PSDU**: O comprimento do PSDU pode variar de 0 a 4 095 octetos. Antes da transmissão, a camada física faz a purificação da PSDU, acrescentando símbolos especiais (técnica de *stuffing*) em cada quatro octetos para minimizar o *bias* do sinal de dados (desequilibro). Este processo envolve o uso de uma trama de comprimento 127 – *synchronous scrambler*, e de um algoritmo de codificação de 32 / 33 *bias – suppression* para tornar os dados aleatórios.

A figura (Ilustração 85) ilustra este processo.

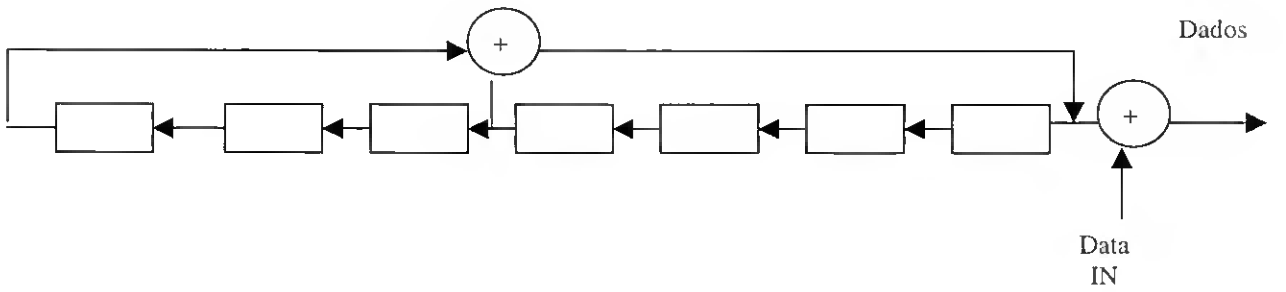


Ilustração 85 Scrambler de dados

Os campos da trama DSSS PLCP

⇒ **SYNC**: Este campo é composto por uma alternância de zeros e uns, alertando o receptor da presença de um sinal potencialmente receptível. O receptor iniciará a sua sincronização com o sinal chegado após detectar este campo.

⇒ ***Start Frame Delimiter***: O conteúdo deste campo é sempre o seguinte padrão de bit, definindo o início de uma trama: 1111001110100000.

⇒ ***Signal***: Este campo indica o tipo de modulação que o receptor deverá usar para demodular o sinal. O valor deste campo é igual ao resultado da expressão:

Taxa de Dados / 100 Kbps

Relativamente à versão do standard IEEE802.11 [100] (Junho / 1997), os dois únicos valores possíveis são 00001010 para DSSS a 1 Mbps e 00010100 para DSSS a 2 Mbps. De notar que o preâmbulo e cabeçalho da trama são sempre enviados a 1 Mbps.

⇒ ***Service***: A especificação 802.11 reserva este campo para utilizações futuras; embora, um valor de 00000000 signifique um dispositivo compatível IEEE802.11.

⇒ ***Length***: O valor deste campo é um inteiro de 16-bit,indicando o número de microsegundos para transmitir a MPDU. O receptor usará esta informação para determinar o fim da trama.

⇒ ***Frame Check Sequence***: Idêntico ao da camada física FHSS, o conteúdo deste campo é um resultado CRC de 16 bits baseado no algoritmo de detecção de erro, CCITT CRC-16.

O polinómio gerador para este algoritmo é $G(x)=x^{16}+x^{12}+x^5+1$. A camada física não determina se o PSDU contem erros. A camada MAC testará erros baseados em FCS (Frame Check Sequence).

A técnica CRC-16 detecta todos os erros de bits únicos e duplos e assegura detecção de 99.998 % de possíveis erros [100]. A maioria dos entendidos acredita que é suficiente para blocos de transmissão de dados até 4 kilobytes.

⇒ **PSDU**: Este trama, que é a MPDU a ser enviada da camada MAC no momento, pode variar de 0 bits ao tamanho máximo definido pelo parâmetro MIB; aMPDUMaxLength.

Os campos da trama IR PLCP

⇒ **SYNC**: Este campo consiste na presença alternada de um pulso em slots de tempo consecutivos.

O standard IEEE802.11 específica que este campo deve ter o comprimento mínimo de 57 slots de tempo e o máximo de 73. O receptor iniciará a sincronização com o sinal chegado após detectar o primeiro Sync.

⇒ ***Start Frame Delimiter***: O conteúdo deste campo define o início de uma trama. O padrão de bit para este campo será sempre o seguinte, o qual é único para PLCPs IR: 1001. Onde 1 representa a presença de pulso e 0 representa a não existência de informação de pulso comunicada.

⇒ ***Data Rate***: Indica a taxa de dados à qual a subcamada PMD deve transmitir a trama. Os dois únicos valores possíveis, com base na versão IEEE802.11 / Junho 1997, são 000 para 1 Mbps e 001 para 2 Mbps. O preâmbulo e cabeçalho PLCP são ambos enviados, sempre, a 1 Mbps.

⇒ **DC *Level Adjustment***: Este campo consiste num padrão de bit, o qual permite que uma estação receptora estabilize o nível DC do sinal. Este padrão de bit, para as duas taxas suportadas, é o seguinte:

1 Mbps = 00000000100000000000000010000000

2 Mbps = 00100010001000100010001100100010

⇒ ***Length***: O valor deste campo é um inteiro de 16-bit não assignado, que indica o tempo, em microsegundos, para transmitir a MPDU (PSDU).O receptor utilizará este valor para determinar o fim da trama.

⇒ ***Frame Check Sequence***: Idêntico ao da camada física FHSS.O conteúdo deste campo é um resultado CRC de 16 bits baseado no algoritmo de detecção de erro, CCITT CRC-16. O polinómio gerador para este algoritmo é $G(x)=x^{16}+x^{12}+x^5+1$. O CRC executa a operação no campo *Length* antes de transmitir a trama. A camada física não determina se o PSDU contem erros. A camada MAC testará erros baseados em FCS (Frame Check Sequence).

A técnica CRC-16 detecta todos os erros de bits únicos e duplos e assegura detecção de 99.998 % de possíveis erros [100]. A maioria dos entendidos acredita que é suficiente para blocos de transmissão de dados até 4 kilobytes

⇒ **PSDU**: Este é o MPDU que está, no momento, a ser enviado pela camada MAC, podendo variar de 0 ao tamanho máximo de 2 500 octetos.

Os seguintes tipos de funções podem ocorrer em cada uma das classes de tramas.

TRAMAS CLASSE 1

Tramas de Controle

- Request to Send (RTS)
- Clear to Send (CTS)
- Acknowledgment (ACK)

Tramas de Gestão

Probe Request / Respone

Beacon

Authentication

Deauthentication

Annoucement traffic indication message (ATIM)

Tramas de Dados

TRAMAS CLASSE 2

Tramas de Gestão

Association request / response

Reassociation request / response

Disassociation

TRAMAS CLASSE 3

Tramas de Dados

Tramas de Gestão

Deauthentication

Tramas de Controle

Power Save Poll

BIBLIOGRAFIA

[1] http://www.tapr.org/tapr/html/ssf.html

[2] http://www.radioconnect.com/

[3] http://www.merconet.com.br/dtr/radioes.htm

[4] http://www.geocities.com/SiliconValley/4915/redes01.htm

[5] http://www.symbionics.co.uk/solutions/WirelessNetworking/IEEE802_11.shtml

[6] http://www.tecview.com.br/wireless.htm

[7] http://penta2.ufrgs.br/Liane/palestras/tecnred/sld003.htm

[8] http://www.tradesys.com.br/wireless.htm

[9] http://www.turma-aguia.com/davi/ss/ss_tec.htm

[10] http://yabae.cptec.inpe.br/%7Eanderson/apost/info/protocolo.htm

[11] http://yabae.cptec.inpe.br/%7Eanderson/apost/info/redes.htm

[12] http://yabae.cptec.inpe.br/%7Eanderson/apost/info/comuni.htm

[13] http://yabae.cptec.inpe.br/%7Eanderson/apost/info/paper_06.htm

[14] http://esin.ucpel.tche.br/bbvirt/pos/ctmr.htm

[15] htttp://www.eee.ufg.br/~lguedes/cm/cm2-7.htm

[16] http://penta.ufrgs.br/redes.94-2/lisianeh/wireless.html

[17] http://www.tecnodatanet.com.br/historia.htm

[18] http://www.gta.ufrj.br/~marcos/COE828/clan.html

[19] http://feldspato.ist.utl.pt/~watm2000/desc.html

[20] http://gta.ufrj.br/grad/98_2/rodrigo/trabalho.html

[21] http://krypton.mnsu.edu/~kawatra/ieee802.11.htm

[22] Carreira, Dario - Comunicação de Dados e Redes – Redes sem Fios (Apontamentos da Cadeira, Universidade Portucalense, Março de 1998)

[23] Chen, Kwang-Cheng – Medium Access Control of Wireless LANs for Mobile Computing (IEEE, Network Magazine September/October 1994, Volume 8, Number 5)

[24] Soares, Luiz; Lemos, Guido e Colcher; Sérgio – Redes de Computadores (Editora Campus, 1995)

[25] Brodsky, Ira – Wireless Computing (ITP, 1997)

[26] Bates, Bud and Ranate, Jay – Wireless Networked Communications (McGraw-Hill, 1995)

[27] Geier, Jim – Wireless LANs Implementing Interoperable Networks (MTP, 1996)

[28] Bianchi, Guiseppe - Performance Analysis of the IEEE 802.11 Distributed Coordination Function (IEEE, Journal on Selected Areas in Communications, vol.18, March 2000)

[29] Weinmiller, J. et al. – Analyzing and Tuning the Distributed Coordination Function in the IEEE 802.11

[30] COMNET III, Tutorial (CACI, 1196)

[31] COMNET III, Planning for Networks Managers Release 1.3 (CACI, 1196)

[32] Couto, Paula - Redes de Área Local Sem Fios Estudo e Desenvolvimento da Subcamada MAC IEEE802.11 (Universidade de Aveiro, 1996)

[33] Wening, Raymond - Wireless LANs (AP, 1996)

[34] Crow, Brian P. ; Widjaja, Indra; Kim, Jeong Geun ; Sakai, Prescott T. – IEEE 802.11 Wireless Local Area Networks (IEEE Communications Magazine, 1997)

[35] Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, ANSI/IEEE Std 802.11, 1999 Edition

[36] Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer, ANSI/IEEE Std 802.11b-1999 Edition

[37] Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer, ANSI/IEEE Std 802.11a-1999 Edition

[38] Valadas, Rui – Redes de Comunicação de Área Local não-Cabladas por Raios Infra Vermelhos (Universidade de Aveiro, 1995)

[39] Katz, R.H. – Adaptation and Mobility in Wireless Information Systems (IEEE Personal Communication Magazine, vol.1, 1994)

[40] Gfeller, F. ; Bapst, U. – Wireless In-House Data Communication via Diffuse Infrared Radiation (Proceedings of the IEEE, vol.67, November 1979)

[41] Batz, D; Bauchot, F. – Wireless LAN Design Alternatives (IEEE Network, Março/Abril 1994)

[42] Rom, R. ; Sidi, M. – Multiple Access Protocols, Performance and Analysis (Springer Verlarg, 1990)

[43] Tobagi, F. – Multiaccess Protocols in Packet Communications Systems (IEEE Transations on Communications, vol.28. Abril 1988)

[44] Tobagi, F. ; Kleinrock, L. – Packet Switching in Radio Channels (IEEE Transactions on Communications, vol.23, Dezembro 1975)

[45] Abramson, N. – The ALOHA System – Another Alternative for Computer Communications (Proceedings of the Fall Joint Computer Conference, 1970)

[46] Roberts, L. – ALOHA Packet System With and Without Slots and Capture (Computer Communication Review, vol.5, Abril 1975)

[47] Rappaport, T. – Wireless Communications Principles and Practice (Prentice Hall, 1996)

[48] Bauchot, F. – Wireless LAN Medium Access Control Protocol (Doc n° IEEE P802.111-93/62, Maio 1993)

[49] Diepstraten, W. ; Belanger, P. ; Ennis, G. – DFWMAC, Distributed Foundation Wireless Medium Access Control (IEEE P802.11-93/190, Novembro 1993)

[50] Hayes, V. – Standardization Efforts for Wireless LANs (IEEE Network Magazine, Novembro 1991)

[51] Project IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, doc n. P802.11/D1 (Draft Standard IEEE 802.11 Dezembro 1994)

[52] Project IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, doc n. P802.11/D2 (Draft Standard IEEE 802.11 Agosto 1995)