Norma IEEE 802.11

Esta norma define as funções e os serviços necessários para um cliente 802.11, de maneira a este operar no modo ad-hoc ou no modo infra-estrutura. Define ainda os aspectos da mobilidade das estações dentro de cada modo de funcionamento. Abrange igualmente os procedimentos e técnicas do nível MAC e nível Físico que permitem a coexistência de redes *wireless* 802.11 no mesmo local, mas onde o cliente esteja associado apenas a uma rede específica e não interfira com os membros de outras redes presentes no local. Descreve ainda os requerimentos e procedimentos necessários para manter a privacidade sobre a informação que circula no meio *wireless* e a autenticação correcta dos clientes.

Arquitectura IEEE 802.11

Antes de se definir as topologias de rede possíveis nas *LAN*'s *wireless,* há que introduzir certos conceitos como o de ***Basic Service Set (BSS),*** que consiste em dois ou mais clientes *wireless* que se reconhecem e estabelecem uma comunicação entre si, e a ***Basic Service Area (BSA)*** que representa uma área conceptual onde membros do BSS podem comunicar.

Existem duas topologias de rede possíveis na norma IEEE 802.11. As mais simples consistem nas redes Ad-Hoc, que são compostas somente por estações que comunicam entre si, via *wireless* (ver figura 1). Uma rede desde tipo é criada duma forma espontânea. A sua principal característica é a limitação a nível temporal e espacial. Estas limitações permitem que a criação e dissolução de uma rede Ad-Hoc sejam realizadas de uma forma simples, que podem ser feitas por alguém que não tenha conhecimentos técnicos. Requerem também pouco ou mesmo nenhum investimento, visto que, apenas, é necessária uma estação para poder participar numa rede Ad-Hoc. O termo Ad-Hoc pode ser substituído por ***IBSS (Independent Basic Service Set).***

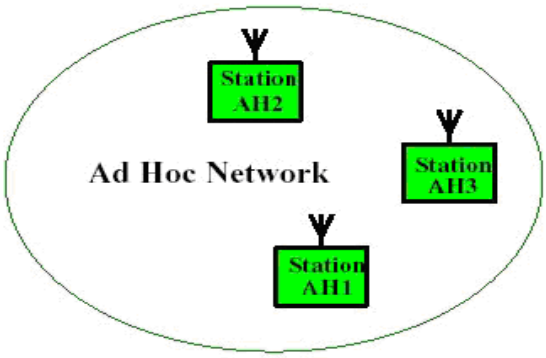

Figura 1 – Rede Ad-Hoc

A outra topologia possível para as redes *wireless* é a de modo infra-estrutura. (ver figura 2) Nesta topologia na BSS existe um AP (*Access point*). A função principal de um AP é o de formar uma *bridge* entre as redes *wireless* e as redes com fios. Ao contrário do modo Ad-Hoc, as estações não comunicam entre si.

Todas as comunicações entre as estações móveis, ou entre uma estação e um cliente da rede com fios são feitas através do AP. Os AP's não são móveis e fazem parte da infra-estrutura da rede com fios.

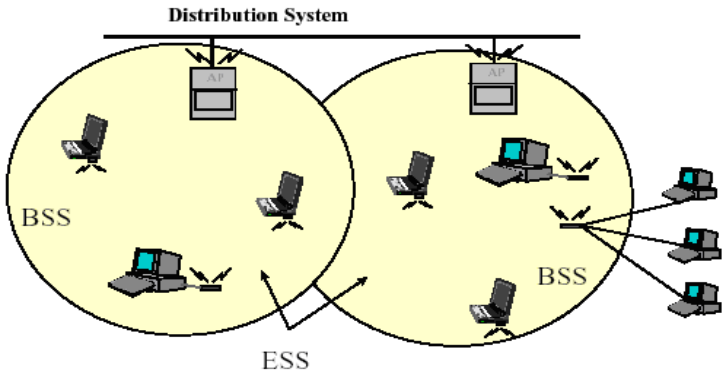

Figura 2 – Redes no modo Infra-estrutura. ESS.

O que se encontra na figura acima apresentada é uma ***ESS (Extended Service Set)*** que consiste numa série de BSS's. Cada BSS contém um AP, e os diferentes AP's encontram-se ligados, entre si, por meio de um Sistema Distribuído. De um modo geral este Sistema Distribuído é uma *LAN Ethernet*, apesar de poder ser qualquer outro tipo de rede. Estações móveis podem fazer *Roaming* entre as várias BSS, associando-se ao AP da BSS para onde se acabaram de mover

Uma característica das redes 802.11 é a de que cada ESS possui um ESSID (ESS *Identification*). Este identificador deve estar presente nos AP's e nas estações móveis. Para as estações se poderem associar à ESS, o ESSID deve ser o mesmo que se

encontra nos AP's. Com isto, consegue-se ter diferentes ESS na mesma área mas uma vez que os seus ESSID são diferentes, as estações só se irão associar à ESS correspondente ao seu ESSID.

Acesso ao meio

Como todos os protocolos 802.x, o 802.11 engloba a camada MAC e Física. Para além das suas funções normais, o 802.11 MAC efectua funções que são típicas de camadas superiores como a fragmentação, retransmissão e confirmação de pacotes.

O método básico de acesso para o 802.11 é ***Distributed Coordination Function (DCF)*** que usa o ***Carrier Sense Multiple Access / Collision Avoidance (CSMA / CA)***. O CSMA funciona da seguinte maneira:

> uma estação que queira transmitir tem de ouvir os outros utilizadores. Se o canal estiver livre, então a estação pode transmitir, mas se estiver ocupado cada estação espera que a transmissão acabe e espera um tempo aleatório antes de começar a transmitir. Isto evita que várias estações tentem aceder ao meio assim que uma transmissão termine. Este protocolo é muito eficaz quando o meio não se encontra muito pesado.

Contudo, se o meio estiver a ser usado por muitas estações, existe a hipótese de duas estações acederem ao meio simultaneamente e assim ocorrer uma colisão. A colisão acontece quando duas estações ouvem o canal livre e decidem transmitir ao mesmo tempo. Tais situações têm de ser identificadas para que a camada MAC possa retransmitir os pacotes.

No caso da *Ethernet* (802.3), as colisões são detectadas e as estações entram numa fase de retransmissão usando o algoritmo ***exponential random backoff***, mas este método não é viável num ambiente *wireless*, pois a implementação do mecanismo de detecção de pacotes implica a existência de um canal *Full Duplex*, o que iria fazer os custos aumentarem consideravelmente.

No meio *wireless* não se pode assumir que todas as estações se podem ouvir umas às outras. Esta é a base dos algoritmos de detecção de colisões. O facto de o meio se encontrar livre nas imediações da estação emissora, não significa que esteja livre nas imediações da estação receptora.

Para solucionar este problema usa-se o algoritmo CA *(Collision Avoidance)* com um sistema de ACK (ver figura 3). Uma estação que queira transmitir, escuta o canal, se este tiver ocupado, a estação fica em silêncio e não transmite. Se estiver livre durante um tempo específico chamado DIFS *(Distributed Inter Trama Space)*, então a estação está livre para transmitir. A estação receptora irá verificar o CRC (*Cyclic Redundancy Check*) e envia um ACK após um período de contenção entre a transmissão do

pacote e o envio da *trama* de ACK. Este período tem o nome SIFS *(Short Inter Frame Space)*. A recepção de um ACK indica ao transmissor que não existiram colisões. Se o transmissor não receber um ACK irá então, retransmitir o pacote em questão, até ter um ACK desse pacote ou até um determinado número de reenvios.

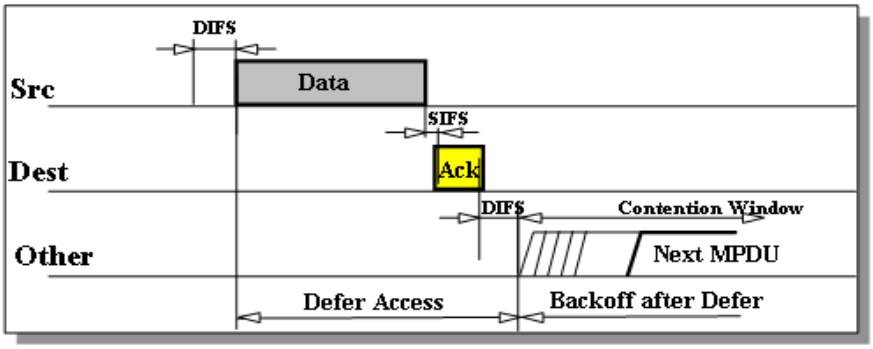

Figura 3 – *Collision Avoidance* com *Acknowledge*

O método descrito depende da escuta do meio físico. Assume-se que todas as estações podem ouvir-se umas às outras. Esta suposição nem sempre é válida, como se pode ver na figura 4. Como as duas estações estão relativamente longe uma da outra, e a comunicação é feita entre as estações e o AP, a estação B não irá detectar transmissões da estação A, sendo então a probabilidade de colisão bastante alta. Este problema é conhecido como a **estação escondida**.

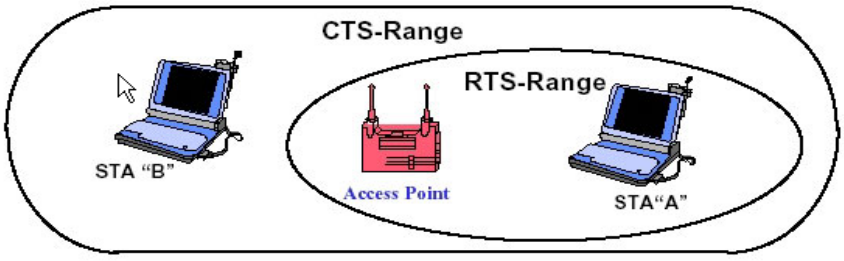

Figura 4 – Problema da estação escondida

Para a resolução deste problema foi criado um mecanismo, ***Virtual Carrier Sense*** representado na figura 5. A estação A que pretende transmitir, irá primeiro transmitir um curto pacote de controlo, RTS **(*Request To Send)***, que inclui a identificação do transmissor e do destinatário e a duração da transmissão (pacote a enviar e o respectivo ACK). A estação B, de destino, irá responder, se o canal estiver livre, com um pacote de controlo do tipo CTS **(*Clear To Send),*** que também incluirá a duração da transmissão. Todas as estações que recebam um RTS e/ou um CTS irão actualizar o indicador, NAV **(*Network Allocation Vector)*** com o tempo de transmissão que se irá suceder e usam essa informação para saber quando escutar o canal.

Este método reduz a probabilidade de colisão na área da estação receptora causada por uma estação escondida do transmissor, porque a estação irá ouvir um CTS e saberá que o meio irá estar ocupado até ao fim daquela transmissão. De salientar o facto de RTS e CTS serem tramas curtas, o que reduz o número de colisões, visto que estas podem ser reconhecidas, mais rapidamente, do que um pacote normal. Este algoritmo é conhecido como MACAW.

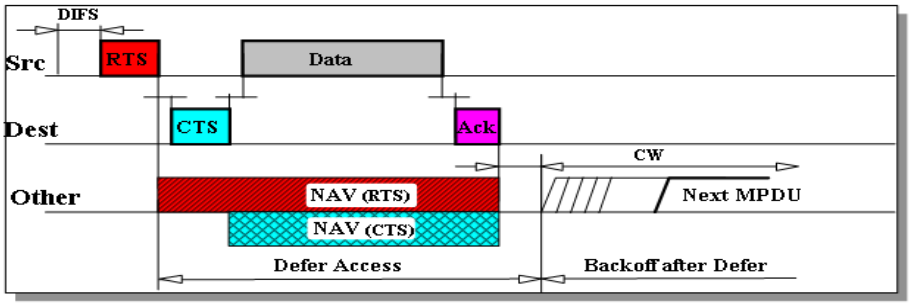

Figura 5 – Virtual Carrier Sense

Associação a uma célula (BSS) existente

Quando uma estação pretende aceder a uma BSS, seja porque foi ligada naquele momento, se encontrava em hibernação, ou porque tinha acabado de entrar na zona da BSS, esta necessita de sincronizar informação com o AP ou com outras estações, se estiver a funcionar em modo Ad-Hoc.

Existem dois métodos possíveis para a sincronização de informação, o passivo e activo. O primeiro consiste em a estação esperar até receber uma trama do tipo *Beacon* enviada pelo AP. Esta trama é enviada periodicamente pelo AP com informação de sincronização. O outro método resulta duma situação em que a estação tenta encontrar um AP que esteja a transmitir uma trama do tipo *Probe Request* e espera por um *Probe Response* do AP. Tanto um método como o outro são válidos e dependem do nível de energia da estação móvel.

Uma vez encontrado o *Access Point*, o passo seguinte é o processo de autenticação. Este consiste na troca de informação entre o AP e a estação, onde cada parte fornece a sua *palavra-chave* para ser identificada pela outra parte. Este processo deve terminar com as duas entidades a terem certeza que estão a comunicar com quem realmente pensam estar a comunicar, independentemente do processo usado para esse efeito.

Após a estação se encontrar devidamente autenticada, inicia-se o processo de associação, onde se troca informação sobre as capacidades das estações e capacidades da BSS, o que permitirá ao Sistema Distribuído saber a posição exacta de cada estação. Só após este processo terminado, é possível a transmissão e recepção de pacotes.

Uma estação móvel que se encontre em deslocamento, a certa altura irá chegar à zona limite de cobertura da BSS, onde o sinal do AP já se encontra fraco. A estação usa a função de *scanning* para tentar encontrar outro AP do mesmo Sistema Distribuído ou então usa informação de *scannings* anteriores. Uma vez encontrado um novo AP, o pedido de associação é feito ao novo AP. Caso o AP aceite o pedido de associação, este irá informar, através do Sistema Distribuído, a nova localização da estação ao AP antigo. Este processo é conhecido como *Roaming* e permite às estações moverem-se entre BSS (do mesmo Sistema Distribuído)

sem perderem conectividade. É um processo similar ao efectuado no *handover* das redes celulares de telefones. De salientar ainda que o processo de *Roaming* não implica uma nova autenticação da estação, visto que esta foi reconhecida pelo sistema, da primeira vez que se juntou a uma das BSS's.

Sincronização e Gestão de energia

As estações móveis têm a necessidade de estarem sincronizadas com o AP (modo infra-estrutura) ou umas com as outras (modo Ad-Hoc) para as diversas funções.

No modo infra-estrutura, os relógios de todas as estações devem estar sincronizados com o relógio do AP. Para tal o AP transmite tramas periódicas (tipo *Beacon*), que contêm o valor do relógio do AP, no momento exacto da transmissão. As estações receptoras verificam o valor do relógio no momento de recepção e corrigem o seu, de maneira a manter a sincronização com o relógio do AP. No valor do relógio do AP, já está incluído o tempo de propagação da trama para se manter uma sincronização exacta entre o AP e a estação. A sincronização evita oscilações nos relógios o que poderia causar a perda de sincronismo após algum tempo de funcionamento.

A gestão de energia está sempre relacionado com aplicações móveis onde a energia da bateria acaba sempre por ser um recurso escasso, daí a norma 802.11 aborda este aspecto e define mecanismos que permitem às estações entrarem em períodos de hibernação sem perder informação e assim poupar energia da bateria. A principal ideia na gestão da bateria é a de permitir ao AP manter um registo actualizado das estações a trabalhar em modo de hibernação e assim fazer um *buffer* dos pacotes que lhes são destinados. Quando estas "acordarem" para um modo operacional, os pacotes do *buffer* serão enviados ou então a estação faz um pedido específico para que lhe sejam enviados os pacotes, isto é um *polling request.* Os AP's transmitem também informação para as estações que estão em modo de hibernação notificando-as que necessitam de voltar ao modo operacional para receberem uma trama do tipo *Beacon*. Se aí houver uma indicação de que existe informação armazenada a estação deverá manter-se em modo operacional e enviar um *polling request* para receber os pacotes que estão no AP. Caso contrário a estação volta ao modo de hibernação.

Todos os pacotes *Multicast* e *Broadcast* são armazenados no AP e só são transmitidos num tempo pré-determinado. Todas as estações que desejam receber estas informações devem estar em modo operacional.

Aspectos associados a planeamento e instalação

Existem alguns aspectos que se devem ter em consideração quando se instala uma *wireless LAN*:

- **Cobertura e distância**. Uma vez que as redes *wireless* são uma tecnologia baseada em rádio, a conectividade entre equipamentos diminui à medida que a distância aumenta. Existe ainda o facto de obstruções como paredes e mobílias causarem reflexões. Este fenómeno, que tem o nome de desvanecimento multipercurso, está na origem de zonas sem cobertura.

- **Ligação rápida VS Ligação estável**. A tecnologia *wireless* foi concebida de maneira a manter a ligação entre dois equipamentos o mais estável e consistente possível. Visto que a velocidade da transmissão se altera com o alcance e qualidade do sinal, os equipamentos irão sacrificar intencionalmente a velocidade da transmissão de dados em troca de manter a ligação estável. Mais vale uma ligação lenta mas estável. Ou seja, equipamentos que necessitam de uma performance elevada têm estar próximos uns dos outros.

- **Interferências**. A norma IEEE 802.11 actua numa gama de rádio frequências onde não é necessário uma licença (com excepção dos Estado Unidos). Isto quer dizer que existe disponibilidade comercial para outros equipamentos, que nada tem a ver com as redes *wireless*, poderem utilizar esta gama de frequências. Consequentemente, estes aparelhos de rádio ao coexistirem com os aparelhos da rede *wireless* irão causar interferências. As interferências provêm de telefones sem fios (DECT, DCS) e aparelhos a operar no comprimento de onda das microondas.

- **Segurança**. A segurança das redes *wireless* é um tema que já fez correr muita tinta na imprensa dedicada às telecomunicações e informática. De facto não se pode negar que as *LAN*'s *wireless* têm falhas de segurança. O algoritmo de segurança WEP (*Wired Equivalent Privacy encryption*) já foi quebrado várias vezes, e de diversas maneiras. Basta apenas uma pequena pesquisa na *Internet* para saber como se obter as chaves de encriptação usadas na rede *wireless* e assim quebrar o respectivo algoritmo. Apesar de tudo existem formas de tornar as redes mais seguras. Pode-se optar por não transmitir o SSID da rede nas tramas de tipo *beacon* e fazer uma filtragem de MAC's (*Media Access Control*) nos AP's. Estes procedimentos combinados com WEP tornam as redes *wireless* mais robustas e seguras.

Arquitectura lógica do 802.11

A arquitectura lógica que se aplica a cada estação consiste conforme é exemplificado na figura a seguir apresentada num nível MAC e múltiplos níveis físicos.

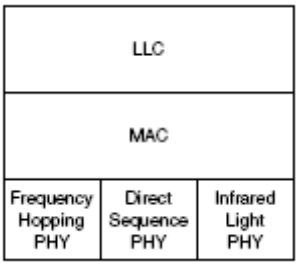

Figura 6 – Arquitectura lógica do 802.11

A finalidade do nível MAC consiste em proporcionar as funções de controlo do nível físico para suporte do LLC (Logical Link Control). Assim operações de endereçamento, coordenação de acessos, geração e verificação de tramas e delimitação de PDU's provenientes do LLC fazem parte das operações executadas pelo MAC.

Nesta norma embora sejam especificados diversos níveis físicos, a estrutura do nível Mac é comum a todas as variantes dentro da família de normas 802.11.

Os serviços definidos fornecem as funções necessárias para o LLC enviar MAC service Data Units (MSDU's) entre duas entidades de rede. Os serviços fornecidos pelo nível MAC encontram-se divididos em duas categorias:

- Serviços de estação ou station services
- Serviços distribuídos

Na primeira categoria englobam-se os serviços comuns a todas as estações presentes na rede. Entenda-se como estação qualquer dispositivo wireless, podendo este ser um posto de trabalho, uma impressora ou outro periférico.
Para realizar estes serviços, as estações necessitam de enviar e receber MSDU's e implementar níveis adequados de segurança.
Dentro das funções realizadas destacam-se:

- Acesso ao meio
- Adesão a uma rede
- Autenticação
- Desautenticação

- Privacidade

Tramas na norma 802.11

Para implementação das funções atribuídas ao MAC, é utilizado um conjunto de tramas cuja a finalidade e estruturas são a seguir apresentadas.

Existem vários tipos de tramas no 802.11. Existem tramas de dados usadas para transmitir dados, tramas de controlo usadas para controlar o acesso ao meio (RTS, CTS e ACK) e tramas de gestão (Management) que são transmitidas da mesma maneira que as tramas de dados mas com a função de fazer a gestão da rede, mas não seguem para camadas mais altas do que o nível MAC.

Todas as tramas obedecem à estrutura representada na figura t-1.

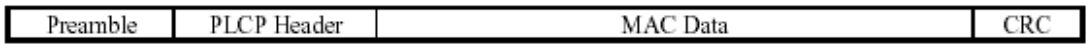

Figura t-1 – Trama genérica 802.11

Na estrutura da trama destacam-se os seguintes elementos:

- ***Preamble*.** Este campo é dependente do meio físico e inclui um campo de sincronização, que consiste numa sequência de 80 bits de zeros e uns que são usados pelo circuito físico para escolher a antena apropriada, para correcções de *offset* da frequência e sincronização com o tempo do pacote

recebido. Inclui também um indicador de início da trama que é usado para definir o timming da trama.

- ***PLCP Header*.** Este campo é sempre transmitido a 1 Mbit/s e contém informação lógica que será usada pelo nível físico para descodificar a trama.

- **Mac *Data*.** Como o nome indica, este campo é usado para transmitir os dados. A figura abaixo mostra como é preenchido este campo.

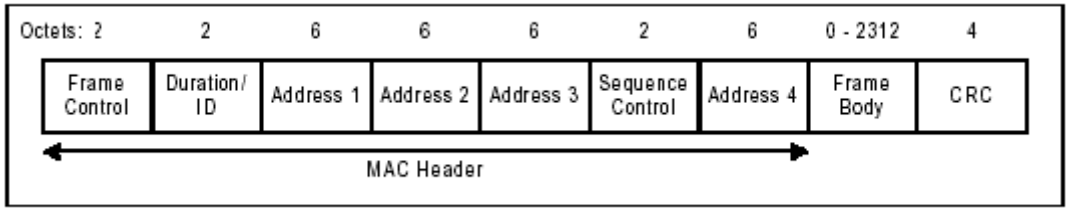

Figura t-2 – Campo Mac Data

O campo frame control, encontra-se por sua vez dividido nos seguintes elementos:

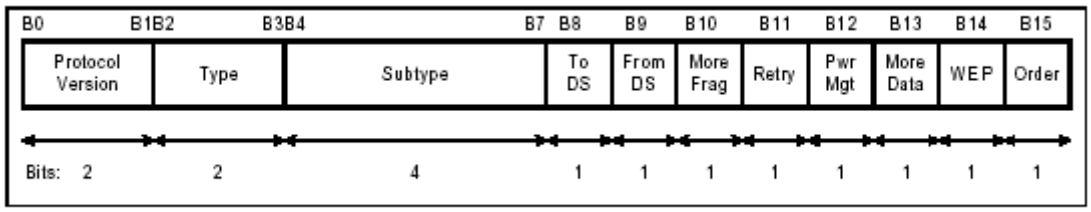

Figura t-3 – Campo Frame Control

O campo da versão do protocolo tem dois bits e serve para identificar que versão da norma 802.11 se está a usar.

Enquanto que as tramas de dados e de Gestão da rede têm o formato exposto anteriormente na figura t-2, as tramas de Controlo são mais específicas. Alguns campos são eliminados, fazendo assim as tramas mais curtas, embora o campo frame control seja o mesmo que se encontra representado na figura t-3.

As tramas de Controlo podem ser de três tipos RTS, CTS e ACK.

O formato de uma trama RTS é o seguinte:

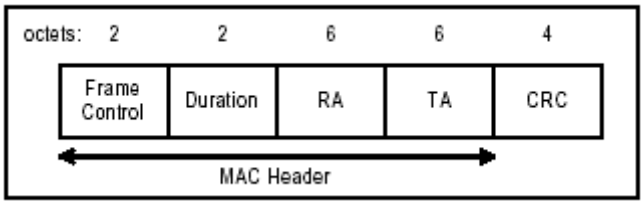

Figura t-4 – Trama RTS

O campo subtype do frame control tem o valor 1101 correspondente ao subtipo RTS.

O campo RA é a morada da estação a que se destina a próxima trama de dados ou trama de gestão (Management). O campo TA é a morada de quem transmite a trama RTS. O campo *Duration* é o tempo (micro segundos) necessário para transmitir a próxima trama de dados ou de gestão, uma trama CTS, uma trama ACK e mais três SIFS.

A trama CTS tem um formato semelhante à do RTS:

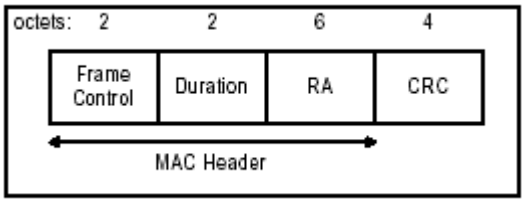

Figura t-5 – Trama CTS

Esta trama é caracterizada pelo valor 0011 do campo subtype do campo Frame control.

O campo RA é a morada a quem se destina a CTS (resposta a RTS). Este é obtido copiando o campo TA da trama RTS correspondente. O campo *Duration* é o valor que veio na trama RTS menos o tempo de transmissão do CTS e um intervalo SIFS.

A trama ACK, representada na figura t-6, tem um formato igual a trama CTS visto que ambas são tramas de resposta. No entanto o subtype agora vale 1011.

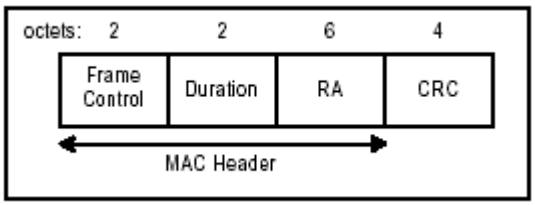

Figura t-6 – Trama ACK

O campo RA é copiado do campo *Address* 2 da *trama* recebida imediatamente antes. O Campo *Duration* é o campo *Duration* da

trama anterior menos o tempo de transmitir do ACK e o respectivo SIFS.

As tramas de gestão podem ser de diferentes tipos, embora tenham uma estrutura genérica comum. Nestas tramas destacam-se os seguintes tipos:

- *Beacon*. Estas tramas têm informação sobre o relógio do AP (para efeitos de sincronização), o intervalo de transmissão das *beacon* tramas, as capacidades da rede, o ESSID, a largura de banda suportada e parâmetros.

- *Probe*. Associado às capacidades da rede, largura de banda suportada e ESSID.

- *Probe Response*. Informação sobre o relógio do AP, o intervalo de transmissão das tramas do tipo *beacon*, as capacidades da rede, o ESSID, a largura de banda suportada e parâmetros.

- *Association Request*. Associadas às capacidades da estação, intervalo de escuta, ESSID e largura de Banda.

- *Association Response*. Relativas à capacidade da rede, Código de estado, ID da estação e largura de banda.

- Desassociação. Transmite o motivo pelo qual se vai desassociar.

Segurança 802.11

Foram desenvolvidos dois métodos de segurança: Autenticação e um algoritmo de encriptação desenvolvido pelo IEEE 802.11 chamado ***Wired Equivalent Privacy*** (WEP). Com estes dois métodos pretende-se evitar o acesso aos recursos da rede e à capacidade de capturar o tráfico *wireless*.

A autenticação é um procedimento no qual se verifica se uma estação tem autorização para se juntar a uma rede, usar os seus recursos e comunicar com as outras estações. No modo infra-estrutura, a autenticação é feita entre o AP e cada estação. Existem dois métodos de funcionamento para autenticar uma estação: um **Sistema Aberto** ou um **Sistema de Partilha de Chaves**. Num Sistema Aberto qualquer estação pode pedir autenticação. O AP que recebe o pedido pode conceder autorização a qualquer estação ou somente a estações que se encontrem numa lista predefinida de utilizadores. Num Sistema de Partilha de Chaves só estações que tenham na sua posse uma chave de encriptação poderão ser autenticadas. A autenticação por partilha de chaves só está disponível em sistemas que tenham a capacidade de encriptação como opção.

O acesso ao tráfico *wireless* é evitado usando o algoritmo WEP. O WEP baseia-se num gerador de números aleatórios iniciado por uma chave partilhada, mas secreta e que recorre ao algoritmo RSA's RC4 (este algoritmo devido a falhas na sua concepção é facilmente quebrado, logo não garante um nível de segurança adequado).
Na saída do gerador é obtido um número de bits aleatórios com o comprimento igual ao maior pacote possível. Esta sequência de bits é combinada com o pacote a transmitir pelo meio *wireless*.

Devido a falhas inerentes ao algoritmo, actualmente as protecções das redes *wireless* utilizam métodos de segurança, definidos em 802.x.

Frequências e potências na norma 802.11

A utilização das gamas de frequência é algo que tem de se encontrar legislado pelas autoridades de cada país. Na maioria dos casos as gamas de frequência na zona dos 2.4 GHz são consideradas livres (banda ISM), embora hajam restrições distintas nos diversos continentes.
A norma 802.11a permite uma taxa de transmissão de 54 Mbps e usa frequências na ordem dos 5 GHz. Esta apresenta uma grande

vantagem em relação a norma 802.11b que opera na gama dos 2.4 GHz e apresenta uma taxa máxima de apenas 11 Mbps.
A norma 802.11a pode transmitir a 54, 48, 36, 24, 18, 12 e 6 Mbps enquanto que o 802.11b só pode transmitir a 11, 5.5, 2 ou 1 Mbps. Logo o 802.11a apresenta-se mais eficiente do que 802.11b. As taxas de transmissão acima apresentadas não são na verdade as taxas de transmissão efectivas. Parte da largura de banda está reservada para tramas de controlo e gestão da rede. Logo o 802.11a a 54 Mbps apresenta uma taxa efectiva de 28.3 Mbps enquanto o 802.11b a 11 Mbps apresenta apenas 5.2 Mbps.

A banda de frequências de 2.4 GHz é uma banda que o 802.11b tem de partilhar com muitos outros equipamentos como microondas, equipamentos *Bluetooth*, entre outros. Já a banda de 5.2 GHz usada pela 802.11a não sofre do problema de interferências externas, pois apenas alguns radares utilizam esta frequência, ou seja encontra-se relativamente vazia.
Contudo, o 802.11a só pode ser utilizado no continente Americano e nas regiões asiáticas e do pacífico, devido ao facto da gama de frequências de 5GHz não estar licenciada na comunidade europeia.

A norma 802.11g beneficia das vantagens do 802.11a e do 802.11b. A taxa de transmissão máxima é de 54 Mbps a 2.4GHz, o mesmo que 802.11a. Os clientes 802.11b serão suportados pelos

pontos de acesso 802.11g e os clientes 802.11g poderão conectar-se a pontos de acesso 802.11b. Claro que esta possibilidade de *roaming* entre as diferentes tecnologias tem as suas limitações: um cliente 802.11b, apesar de estar ligado a um AP 802.11g nunca poderá ultrapassar os 11 Mbps (limitado pela tecnologia cliente 802.11b) e um cliente 802.11g conectado a um AP 802.11b também só terá 11 Mbps (limitado pelo AP 802.11b). Apresenta ainda um melhor alcance que o 802.11a visto que trabalha a uma frequência mais baixa.

Tipicamente a potência de emissão situa-se entre os 50 e 100 mW.

Continente	Canais	Frequências (GHz)	Potência (mw)
América (EUA, Canada)	1 a 11	2.412-2.462	50 a 200
Europa	1 a 13	2.412-2.472	idem
França	10 a 13	2.457-2.462	idem
Espanha	10 e 11	2.457-2.462	idem
Japão	14	2.484	idem

Tabela T-1- Potências e gamas de frequências para 802.11b

O nível físico na norma 802.11b é conhecido como HR/DS ou HR/DSSS. Embora a modulação e codificação seja distinta da usada no nível físico do tipo DS, a gama de frequências e canais operacionais é o mesmo que utiliza o DS, conforme apresentado na tabela T-1.

O ritmo usado é de 11 Mchips por segundo, baseado em palavras de 11 bits pertencentes a uma sequência de Backer. Note-se que o espalhamento quer em DS quer em HR/DS é realizado com recurso a sequências de Backer. A diferença principal, relativamente ao nível físico do DS, reside no processo de codificação. Assim no DS cada palavra é codificada num ou dois bits, dependendo do tipo de modulação utilizada. No caso da DBPSK ter-se-à um ritmo de 1 Mbps e na DQPSK um ritmo de 2 Mbps.

No HR/DS é usado um código complementar que divide a sequência de chips numa sequência de símbolos com 8 bits, transmitidos a um ritmo fixo de 1.375 M Simb/seg. Os ritmos de 5.5 e 11 Mbps atingem-se por intermédio da utilização de um codificador CCK que na sua saída cada símbolo de 8 bits pode estar a codificar 4 bits ou 8 bits da sequência de Backer obtida por espalhamento. Para ritmos de 1 Mbps ou 2 Mbps não é usado o código CCK.

O nível físico encontra-se dividido em dois sub níveis, à semelhança dos restantes níveis físicos definidos nas normas da

família 802.11. O PLCP (Physical Layer Convergence Procedure) é responsável pela adaptação do nível físico ao MAC, isto é, recebe tramas do MAC para transmissão via interface ar ou entrega tramas ao MAC. O PMD (Physical Medium Dependent) trata do envio e recepção dos dados ou pacotes gerados no PLCP através da interface ar propriamente dita.

PLCP

Existem duas opções relativas aos formatos das tramas associadas a este sub-nível e directamente relacionadas com os ritmos de transmissão pretendidos. A diferença entre os dois formatos reside no tamanho do cabeçalho utilizado em cada um dos tipos.

O formato longo, associado a ritmos de 1, 2, 5.5 e 11 Mbps e o formato curto associado aos ritmos mais elevados de 5.5 e 11 Mbps.

Saliente-se que pode existir equipamento que suporte unicamente um forma to de trama. No entanto estações utilizando cabeçalhos longos podem responder neste formato a uma AP configurada no formato curto, dada a capacidade destas reconhecerem os dois formatos.

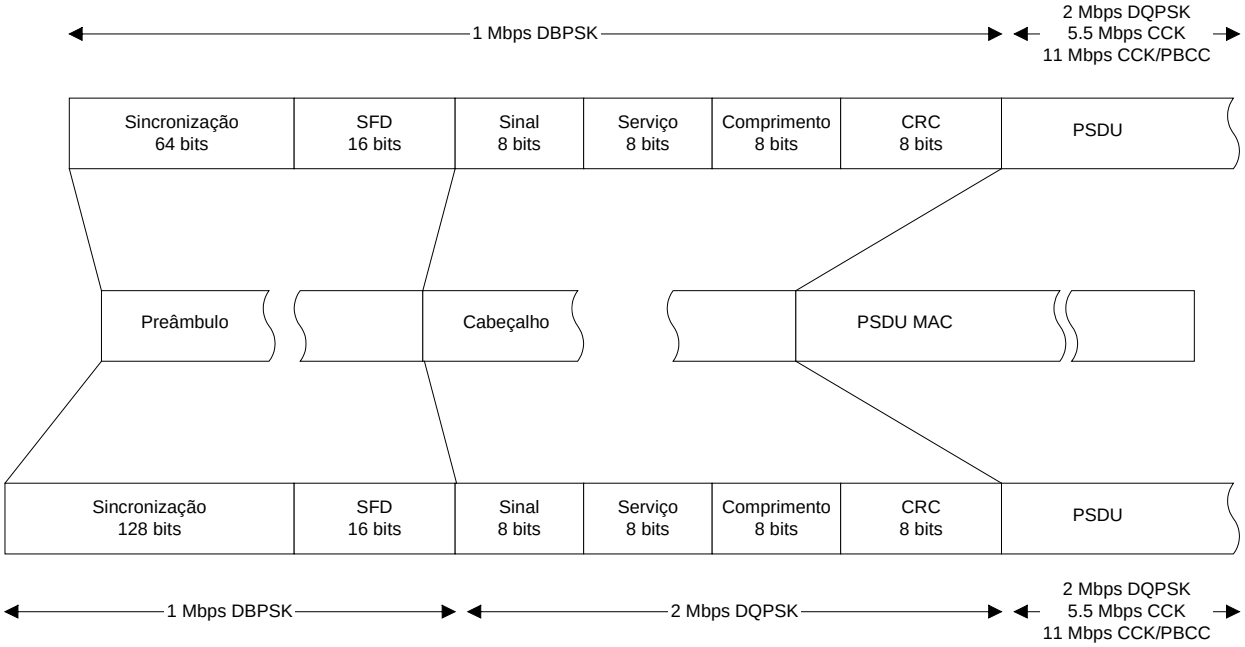

Figura t-8 Estrutura da trama PLCP nos formatos longo e curto.

A estrutura da trama é a que se encontra apresentada na figura t-8. Em ambos os tipos de trama destacam-se os seguintes elementos:

- Preambulo – composto pelo campo de sincronização de 56 ou 128 bits a 0 ou 1 consoante o formato considerado e o delimitador de início de trama SFD (Start Frame Delimiter) composto por 16 bits. O preâmbulo é transmitido usando a modulação DBPSK, associada a um ritmo de 1 Mbps. O campo SFD no formato longo corresponde à sequência 1111 0011 1010 0000 que é transmitida a partir do bit menos significativo situado à direita. No formato curto a sequência é simplesmente obtida a partir da anterior por inversão da ordem dos bits, obtendo-se 0000 1010 1100 1111.

- Cabeçalho – Este é transmitido após o preâmbulo. Consoante o formato considerado (longo ou curto), o ritmo de transmissão varia. Assim no formato longo a modulação usada para a sua transmissão consiste na DBPSK com um ritmo de 1 Mbps. No formato curto usa-se a DQPSK associada a um ritmo de 2 Mbps.

  O cabeçalho é formado pelos campos sinal, serviço, comprimento e CRC a seguir descritos:

  - Sinal – Pode ser do tipo longo ou curto e indica a velocidade e método de transmissão da trama MAC. Os valores possíveis são os que constam da tabela T-2. Enquanto que no formato longo o campo sinal pode assumir qualquer um dos cinco valores apresentados na tabela, já no formato curto só são possíveis os três últimos valores, correspondentes aos ritmos de 2, 5.5 e 11 mbps.

Ritmos (Mbps)	valor
1	0000 1010
2	0001 0100
5.5	0011 0111
11	0110 1110

Tabela T2 – Valores do campo sinal/ritmos

- Serviço – Este campo é formado por 8 bits e transmitido a partir do bit menos significativo. O oitavo bit é usado para prolongamento do campo comprimento descrito adiante. O 3º bit está relacionado com os relógios relativos ao ritmo de símbolo e frequência de transmissão. O 4º bit indica o tipo de código usado no pacote a transmitir. Os restantes bits não têm funções específicas atribuídas.

- Comprimento – Este campo tem um formato único e indica o tempo em microssegundos necessário para a transmissão da trama MAC. Convem salientar que a trama MAC está limitada a um comprimento máximo de 4095 octetos.

- CRC - É igual para ambos os formatos. É calculado antes do baralhamento e abrange os campos sinal, serviço e comprimento.

PMD

Resumindo o nível físico recebe as tramas do nível MAC. A estas, o PLCP adiciona um cabeçalho longo ou curto consoante o

formato que está a usar, baralha os seus bits e entrega a trama obtida ao sub-nível PMD para este proceder ao seu envio através da interface ar, com recurso a uma modulação do tipo DQPSK. Note-se que para efeitos de transmissão são usados parelhas de bits transmitidas nas componentes em fase e quadratura.

Para um ritmo de 5.5 Mbps, a trama MAC incluída na trama PLCP é dividida em blocos de 4 bits. Cada um destes blocos por sua vez é dividido em segmentos de 2 bits. O 1º segmento é transmitido usando uma modulação DQPSK, na qual as fases transmitidas não só dependem da parelha anterior bem como da paridade do símbolo a transmitir. A contagem dos símbolos é iniciada a zero no primeiro bloco de 4 bits da trama MAC.
O segundo segmento de 2 bits é usado para seleccionar uma palavra de oito bits dentro de um alfabeto quaternário, apresentado na tabela t-3. Notar que estas palavras são também transmitidas via canal físico com recurso à mesma modulação.

Para um ritmo de 11 Mbps, o processo é análogo ao anterior. Agora a trama MAC é dividida em blocos de 8 bits, dos quais os primeiros 2 bits são codificados com recurso a DQPSK e os restantes 6 bits são agrupados dois a dois para selecção de um ângulo de fase e posterior selecção de uma palavra de oito bits dentro de um alfabeto 64-ário. Agora as fases já não dependem da paridade ou não da ordem do bloco dentro da trama MAC a

transmitir. A correspondência entre fase e bits é a que se apresenta na tabela t-4.

Seq. bits	Palavra
00	i,1,i,-1,i,1,-i,1
01	-i,-1,-i,1,1,1,-i,1
10	-i,1,-i,-1,-i,1,i,1
11	i,-1, i,1,-i,1,i,1

Tabela T-3

Bits	fase
00	0
01	Π/2
10	Π
11	3Π/2

Tabela T-4 - codificação de fase para 11 Mbps