2
Padrão IEEE 802.11

O IEEE *(Institute of Electrical and Electronics Engineers)* em 1997 apresentou um modelo de referência para redes sem fio denominado IEEE 802.11. Este modelo define especificações que abrangem as camadas física e de enlace (segundo o modelo de referência OSI).

a) ***Camada Física***: define como as informações são trocadas no meio através de transmissão por radiofreqüência ou por infravermelho;

b) ***Camada de Enlace***: define o método de acesso ao meio. O Padrão IEEE 802.11 utiliza um método denominado CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*), semelhante ao das redes locais *ethernet,* CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*).

A taxa de transmissão nominal deste Padrão era de 1 a 2Mbps.

Atendendo a uma exigência de mercado, em 1999 surgiu uma nova especificação, a IEEE 802.11b, que proporcionava maior velocidade de transmissão. O IEEE alterou as características da camada física para que fosse possível atingir maior velocidade nominal, neste caso, de até 11Mbps.

A seguir é apresentada as principais características da família 802.11:

802.11a: Operação em 5GHz, 54Mbps, modulação OFDM

802.11b: Operação em 2,4GHz, 11Mbps, DSSS/FHSS

802.11d: *Wold Mode* (Europa 20dB, EUA/BRA 36dB)

802.11e: Suporte para aplicações que necessitam de Qualidade de Serviço (QoS)

802.11f: Recomendação para redes ponto a ponto sob protocolo IAP (*Inter Access Point*)

802.11g: Operação em 2,4GHz, 54Mbps, modulação OFDM, compatibilidade com o 802.11b

802.11h: Gerenciamento do espectro

802.11i: Avanços em segurança

Neste trabalho será utilizada a recomendação IEEE 802.11b.

2.1
Topologia

O padrão IEEE 802.11 define uma arquitetura para as redes sem fio, baseada na divisão da área coberta pela rede em células (denominadas BSA - *Basic Service Área).* As dimensões da BSA dependem das características do ambiente e da potência dos transmissores/receptores utilizados nas EM (estações móveis).

Outros conceitos que fazem parte da arquitetura de rede sem fio:

a) BSS *(Basic Service Set):* representa um grupo de EM se comunicando por uma BSA;

b) AP (*Access Point*): tem como função interligar as EM à rede fixa. O AP funciona como uma interface entre as redes com e sem fio;

c) DS (*Distribution System*): representa uma infra-estrutura de comunicação que interliga as várias BSA para permitir a construção de redes multi-células;

d) ESA *(Extended Service Área):* representa a interligação de várias BSA pelo sistema de distribuição através dos AP;

e) ESS *(Extended Service Set):* representa um conjunto de EM formado pela união de vários BSS conectados por um DS. Esta configuração foi criada para os casos onde os requisitos de serviços excedam as limitações de um BSS. É utilizada para cobrir áreas extensas em tamanho e complexidade.

A figura a seguir ilustra a união de dois BSS conectados por um sistema de distribuição, formando um ESS.

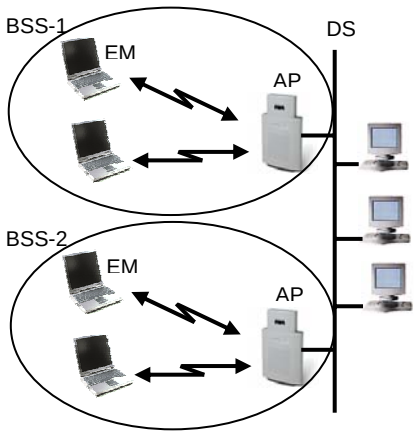


Figura 1: Sistema ESS

Existem três arquiteturas para redes sem fio que são empregadas segundo a infra-estrutura do local ou necessidade do usuário.

a) Redes com Infra-estrutura: nesta situação tem-se como principal característica a presença de um AP.

b) Redes sem Infra-estrutura: neste tipo de configuração, também conhecida como *ad-hoc* ou IBSS (*Independent Basic Service Set*), a EM não necessita de um controle centralizado e nem de um equipamento específico que a interligue a um *backbone*;

c) Enlace entre Redes: esta configuração é uma solução para interligar duas LAN instaladas em locais distintos, onde a melhor opção de comunicação não é por infra-estrutura de rede cabeada.

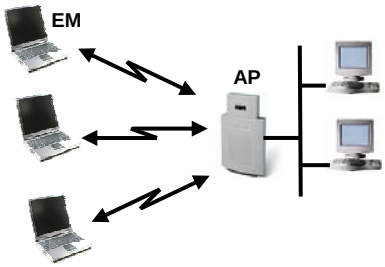


Figura 2: Arquitetura com um AP

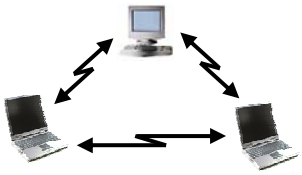


Figura 3: Arquitetura sem AP

2.2
Estrutura das Camadas do Padrão IEEE 802.11

A figura a seguir ilustra as camadas do padrão IEEE 802.11, comparando com o modelo RM-OSI da ISO (*Reference Model - Open System Interconnecttion of the International Satandardization Organization*).

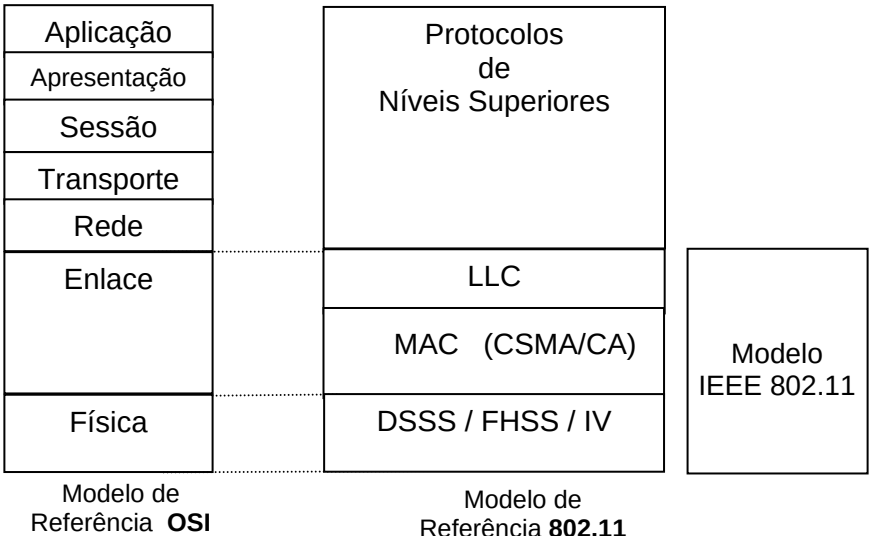


Figura 4: Estrutura das camadas do padrão IEEE 802.11

2.3
Camada Física

A camada física especificada no padrão IEEE 802.11 é responsável pela transmissão dos bits através do canal de comunicação, definindo as especificações elétricas e mecânicas.

A principal função da camada física é a modulação, preparando a informação para ser transmitida no meio, em forma de onda eletromagnética. Além da modulação, utiliza-se uma técnica de espalhamento do sinal denominada "*Spread Spectrum*" que tem a função de proteger o sinal contra interferência co-canal.

O padrão prevê que o nível físico empregará três formas de transmissão: duas de rádio-freqüência baseadas em *spread spectrum*, conhecidas como ***Frequency Hopping Spread Spectrum*** **(FHSS)** e ***Direct Sequence Spread Spectrum*** **(DSSS)**, além da transmissão infravermelha difusa.

Podemos dividir a camada física em duas subcamadas, conforme mostra a figura a seguir.

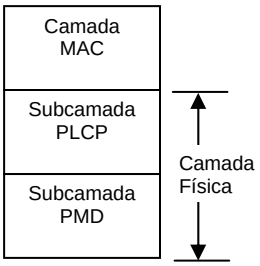


Figura 5: Estrutura da Camada Física

a) PMD (*Physical Medium Dependent*): esta subcamada trata das diferentes técnicas de transmissão, cuidando da modulação e codificação do sinal, e sendo responsável pelo envio e recebimento de pacotes no meio. Esta função é executada modulando os pacotes provenientes da camada superior (PPDU-*PLCP Protocols Data Unit*) e demodulando os pacotes recebidos de outra estação;

b) PLCP (*Physical Layer Convergence Procedure*): esta subcamada provê os pontos de acesso de serviços comuns ao nível físico, sendo a interface entre a camada de enlace e a camada física. Sua principal função é entregar as informações recebidas da PMD, na forma de PPDU, à subcamada MAC, e preparar as informações provenientes da própria subcamada MAC para serem enviadas à PMD.

A troca de informações entre a camada física e a subcamada MAC é realizada através de quadros denominados MPDU (*MAC Protocols Data Unit*).

O MPDU contém campos de informações alocadas pela PLCP necessários à comunicação das camadas.

As subcamadas PLCP e PMD comunicam-se através de premissas.

2.3.1
Operações da Camada Física

As operações da camada física são similares, independente da técnica de modulação utilizada. O Padrão definiu três estados possíveis, conforme descritos abaixo:

a) Detecção de Portadora: estado que permite a camada MAC "*escutar*" o meio;

b) Transmissão: modo de transmissão dos dados;

c) Recepção: modo de recebimento dos dados.

2.3.1.1
Detecção de Portadora

A camada física executa esta operação consultando a PMD periodicamente para saber se o meio está ocioso ou não. A PLCP implementa as seguintes operações, no caso de nenhuma transmissão ou recepção:

a) Detecção de sinais de entrada: a PLCP verifica, periodicamente, o meio para detectar a chegada de alguma mensagem. Quando algum quadro MPDU é detectado, seu cabeçalho é lido de forma a se identificar o destino daquela informação;

b) Determinação de canal ocioso: esta operação verifica, periodicamente, se o canal está ocioso ou não (através de premissas).

2.3.1.2
Transmissão

A PLCP envia uma mensagem para a PMD alterar seu estado de detecção de portadora para transmissão, assim que recebe um pedido de requisição de transmissão da subcamada MAC.

A PMD responde à solicitação garantindo que o serviço está disponível e envia um preâmbulo.

O cabeçalho da mensagem será posteriormente adicionado ao preâmbulo, completando as informações do início do quadro que será transmitido a uma taxa nominal de 1Mbps. Após o envio do cabeçalho e do preâmbulo, a PLCP altera a taxa de transmissão para a mesma que foi informada ao receptor, e então termina de enviar o pacote. Quando o envio do pacote é concluído, o transmissor é desligado e o modo de operação da PMD é alterado para modo de detecção de portadora.

2.3.1.3
Recepção

O modo recepção tem início sempre que a PMD se encontra no modo de detecção de portadora e um pacote é detectado.

O sinal do pacote para ser detectado deverá possuir uma intensidade de potência mínima de 85dBm e seu preâmbulo ser considerado válido, para então o processo de verificação de cabeçalho ser iniciado. Caso o cabeçalho não contenha erro, ele será anexado a uma premissa que é enviada à subcamada MAC pela PLCP para indicar a chegada de um pacote.

A PLCP também é responsável por detectar o fim do pacote e informar à camada MAC quando isso ocorrer. A verificação do tamanho do pacote é executada através de um contador de bytes que é comparado a um campo deste pacote, o qual contém a informação do seu tamanho. Assim, a PLCP pode notificar a subcamada MAC do fim do pacote, e o processo de recebimento é concluído. Então, a PLCP envia uma ordem para PMD voltar ao modo de detecção de portadora.

2.3.2
Frequency Hopping Spread Spectrum (FHSS)

A técnica de transmissão FHSS consiste em dividir a banda do canal em subcanais, nos quais a transmissão ocorrerá em tempos curtos. O transmissor envia seus dados ciclicamente em diversos subcanais conforme uma seqüência pré-definida. O receptor para recuperar os dados corretamente deve percorrer os subcanais na mesma ordem pré-definida.

A largura de banda de 83,5MHz da faixa 2,4GHz foi dividida em 83 subcanais de 1MHz, devendo ser utilizados, no mínimo, 75 desses subcanais.

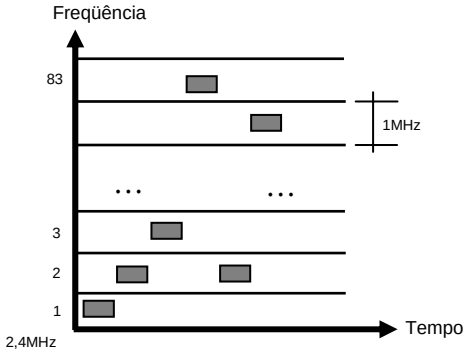


Figura 6: Transmissão FHSS

A fim de minimizar interferências, a seqüência de saltos deve observar alguns critérios:

a) Assegurar a distância mínima de salto para evitar a propagação de multipercurso;

b) Minimizar saltos simultâneos de seqüências diferentes para o mesmo canal ou canais adjacentes;

c) Minimizar saltos consecutivos para um mesmo canal de sistemas FHSS diferentes.

O *frame* gerado pela PLCP (*PPDU – PLCP Packet Data Unit*), cuja função é a de informar parâmetros do pacote que será transmitido, está ilustrado a seguir.

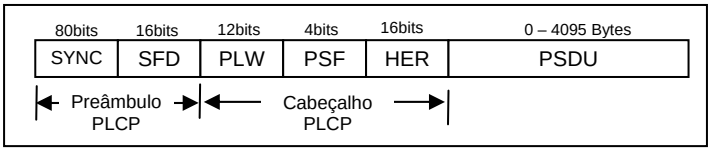


Figura 7: Formato do pacote PLCP para o FHSS

a) SYNC: seqüência de sincronismo;

b) SFD (*Start Frame Delimiter*): sincronização de símbolo para indicar o início do pacote;

c) PLW (*PSDU Length Word*): informa o tamanho do pacote em bytes;

d) PSF (*PLCP Signaling Field*): indica em que taxa de transmissão a PSDU será transmitida. O cabeçalho será sempre a 1Mbps. A taxa para o restante do pacote será informada pelo PSF;

e) HER (*Header Error Check*): contém informações relativas a código corretor de erro (CRC-16). A camada física não determina se há erros na PSDU, pois esta função pertence à subcamada MAC, que faz a verificação através do FCS;

f) PSDU (*PLCP Service Data Unit*): campo que contém os dados da subcamada MAC.

A subcamada PMD tem a função de transmitir e receber os pacotes, sob coordenação da subcamada PLCP, utilizando técnicas de modulação e demodulação.

2.3.3
Direct Sequence Spread Spectrum (DSSS)

Na técnica de transmissão DSSS (*Direct Sequence Spread Spectrum*), cada tempo de bit é dividido em *n* subintervalos denominados *chips*. Para transmitir 1 bit, uma estação deve enviar uma seqüência de *chips*. Ou seja, representa-se cada bit por uma seqüência pseudo-aleatória de símbolos binários. Para enviar o bit 0, utiliza-se o complemento desta seqüência. Para uma transmissão de 1 Mbps tem-se o envio de *n* Mchip/s.

Segundo o padrão IEEE 802.11, todas as estações adotam a seqüência de *Barker*. Esta seqüência, composta por 11 símbolos, é definida como: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1, sinalizando uma taxa de *chip* de 11 M*chip*/s quando se transmite a 1 Mbps.

Para aumentar a taxa de transferência, a especificação IEEE 802.11b mudou a técnica de codificação de *Barker Sequence* para uma denominada *Complementary Code Keying* (CCK). Esta nova codificação consiste de um conjunto de 64 palavras de 8 bits. Esse conjunto de palavras tem propriedades matemáticas únicas, as quais permitem que haja uma distinção entre elas, mesmo com a presença de ruído.

Para suportar ambientes onde o ruído pode ser elevado em determinados momentos, a especificação IEEE 802.11b determina a troca da taxa de transmissão, dinamicamente, dependendo das condições do sinal, sendo essa troca transparente às camadas superiores do protocolo. As velocidades possíveis são: 11Mbps, 5,5 Mbps, 2 Mbps e 1Mbps.

Taxa de Transmissão Nominal	Tamanho do Código	Modulação	Taxa de Símbolos	Bits / s
1 Mbps	11 (*Backer*)	BPSK	1MSps	1
2 Mbps	11 (*Backer*)	QPSK	1MSps	2
5,5 Mbps	8 (CCK)	QPSK	1,375MSps	4
11 Mbps	8 (CCK)	QPSK	1,375MSps	8

Tabela 1: Velocidade do DSSS

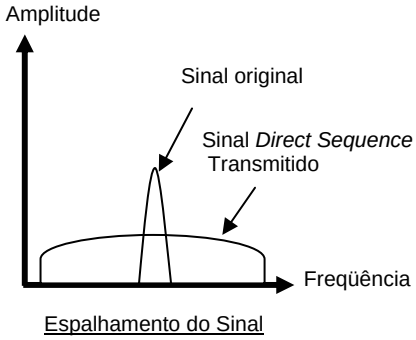


Figura 8: Espectro de freqüência do DSSS

A figura a seguir ilustra o *frame* DSSS PLCP, denominado PPDU. O preâmbulo tem a função de sincronizar os sinais de entrada antes da chegada do conteúdo do pacote. O cabeçalho contém as informações do pacote, enquanto o campo PSDU é o MPDU enviado pela subcamada MAC.

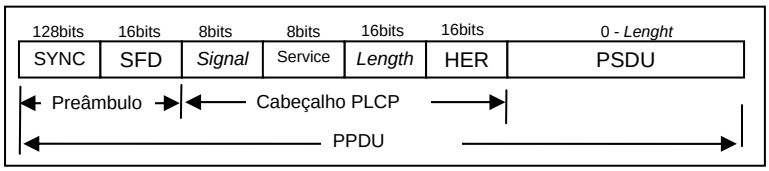


Figura 9: Formato do Pacote PLCP para o DSSS

a) SYNC: 128 bits embaralhados. Utilizado para sincronismo do receptor. Cada bit é representado pela seqüência de *Barker* (seqüência embaralhada);

b) SFD (*Start Frame Delimiter*): provê a sincronização de quadro e de bytes para o receptor;

c) *Signal:* indica qual o tipo de modulação o receptor deve utilizar para receber o sinal e, conseqüentemente, ajusta a taxa de transmissão do quadro MPDU;

d) *Service*: reservado para uso futuro;

e) *Length*: indica o tamanho da PSDU;

f) *HER*: similar ao FHSS;

g) *PPDU*: como no FHSS, este é o pacote enviado pela subcamada MAC (MPDU), e pode ser transmitido com taxas distintas definidas no cabeçalho. Seu tamanho é variável e dependente do valor informado no campo *Lenght*.

2.4
Camada de Enlace

A camada de enlace é divida em duas subcamadas:

a) **Controle Lógico do Link (*LLC – Logical Link Control*)**;

b) **Controle de Acesso ao Meio (*MAC – Media Access Control*)**.

A subcamada LLC é idêntica à da especificação IEEE 802.2. Esta subcamada dá suporte à subcamada MAC para serviços de endereçamento, reconhecimento de quadros e detecção de erros.

2.4.1
Controle de Acesso ao Meio – MAC

Esta subcamada está localizada imediatamente acima da camada física, tendo como principal função a alocação do meio físico para cada estação, de forma que a transmissão não sofra interferência das outras estações que também disputam o meio.

Outras funções da subcamada MAC: prover garantia de acesso justo e atribuição de prioridades.

O meio sem fio apresenta diversas características peculiares que o difere bastante dos meios confinados mais conhecidos (par trançado, cabo coaxial e fibra ótica). Estas características devem ser analisadas para um bom funcionamento da tecnologia e o protocolo da camada de enlace deve ser robusto o suficiente para lidar com todos os novos problemas.

Estas novas características são:

a) Características físicas dinâmicas do canal: o canal pode mudar suas características em períodos de tempo e espaço muito pequenos (desvanecimento de *Rayleigh*), tornando a comunicação inviável ou a utilização injusta do canal. Um usuário em melhores condições de recepção e transmissão pode prejudicar os demais por "*tomar conta"* do canal;

b) Mobilidade e topologia de rede dinâmica: tanto as características do canal quanto a mobilidade das estações podem alterar as conexões entre os nós e assim mudar a topologia da rede. Os protocolos devem ser capazes de manter a operação normalizada enquanto a topologia da rede muda com o tempo;

c) Vazão: desde que o espectro é um recurso escasso, a vazão (*throughput*) é definitivamente a consideração mais crítica dos protocolos de múltiplo acesso;

d) *Retardo:* características de retardo são importantes para todos os tipos de aplicações, mas, especialmente, para aquelas limitadas no tempo e aplicações multimídia, tais como; voz e vídeo;

e) Justiça no acesso: o sinal recebido de uma determinada estação mais afastada pode estar bem mais fraco do que de outras estações. O acesso de uma EM ao AP não pode ser prejudicado se o se sinal está mais fraco que de outras EM mais próximas. O protocolo MAC deve estar apto a resolver este problema garantindo um acesso justo a todas as estações;

f) Consumo de energia: devido ao fato de os terminais serem móveis, tipicamente alimentados por baterias, a subcamada MAC deve fazer considerações no que diz respeito à utilização eficiente da potência de transmissão e recepção.

Antes de transmitir o pacote com a informação, a subcamada MAC deve garantir o acesso ao meio. Para que este serviço seja executado foram propostos dois métodos de acesso, diferenciados entre si pelas atribuições de prioridades às estações.

Estes métodos são:

a) **CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*):** método de acesso ao meio, sem prioridade, baseado no modo DCF (*Distributed Coordination Function*);

b) **Acesso Baseado em Prioridade**: método utilizado em uma rede que contém um coordenador, denominado PC (*Point Coordinator*), e ele decide quem tem acesso ao meio, segundo uma tabela de prioridades. Este método é conhecido como PCF (*Point Coordination Function*).

Para garantir cada uma das funções descritas pelos métodos, as subcamadas MAC das EM envolvidas trocam pacotes, a fim de resolver os problemas de quando acessar o meio.

2.4.2
DCF (*Distributed Coordination Function*)

Este é o mecanismo empregado nas atuais redes instaladas que utilizam o padrão IEEE 802.11. Ele provê acesso múltiplo assíncrono, com contenção, detecção de portadora e prevenção de colisão. Estas funções são executadas pelo mecanismo CSMA/CA.

O DCF trabalha de forma semelhante ao método de detecção de portadora CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*) das redes IEEE 802.3, apenas com uma diferença: o protocolo CSMA/CD do IEEE 802.3 controla as colisões quando elas ocorrem, enquanto que o protocolo CSMA/CA apenas tenta evitar as colisões. Ou seja, a diferença entre os mecanismos empregados nas redes com e sem fio é que, no CSMA/CA, a colisão de pacotes no meio pode ser evitada, diferentemente do CSMA/CD, que só pode ser detectada.

No pacote existe um campo que contém duração prevista para sua transmissão. Esta função é conhecida como *Detecção Virtual da Portadora*, e o campo que carrega esta informação é conhecido como "*Duration Field*". O valor extraído deste campo é então registrado num contador decrescente conhecido como NAV *(Network Allocation Vector)*. Este contador opera como um cronômetro regressivo que enquanto não for igual a zero significa meio ocupado, e quando é igual a zero, meio livre.

Após o NAV atingir o valor zero, um tempo aleatório deve ser aguardado antes da EM transmitir. Este tempo aleatório é conhecido como *backoff time*. Ele foi criado porque a probabilidade de duas EM transmitirem simultaneamente após

o contador NAV atingir zero é bastante considerável, e colisões não seriam evitadas.

A probabilidade de colisão reduz a valores muito próximos de zero com a implementação do *backoff time*.

2.4.3
PCF (*Point Coordination Function*)

Opcionalmente, suportado pelo DCF, pode ser oferecido um mecanismo com serviços livres de contenção, denominado de *Point Coordination Function* (PCF), como mostrado na figura a seguir.

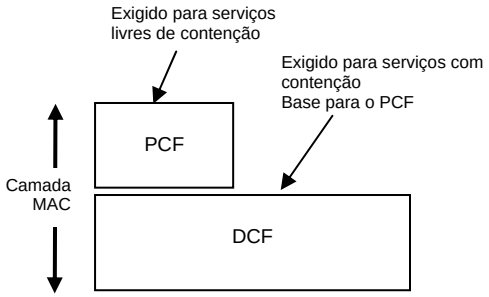


Figura 10: Estrutura da Subcamada MAC

O PCF controla os quadros durante o período livre de contenção CFP (*Contention Free Period)*, que é seguido por um período de contenção controlado pelo mecanismo DCF, anteriormente descrito.

O coordenador PC (*Point Coordination*) obtém o controle de CFP e tenta manter este controle por todo o período, já que uma estação no modo PCF aguarda um tempo menor para transmitir seus pacotes do que estação utilizando DCF. Este intervalo de tempo, pouco menor que DIFS, porém maior que SIFS, é denominado de PIFS (*PCF Inter Frame Space*).

No início de cada CFP o PC informa, após esperar um tempo PIFS, qual o tempo total de CFP e quando ocorrerá novamente, através de um pacote denominado *beacon frame*.

Todas as estações devem colocar, como valor de NAV, a duração total de CFP, a fim de evitar que alguma estação tome o controle do meio durante este período. Após um intervalo de tempo SIFS, o PC pode enviar dados, requisitar que estações enviem dados, confirmar dados que recebeu ou acabar com o CFP.

Durante CFP somente estações que estiverem na lista de *polling* do PC podem transmitir, mas todas as estações podem receber dados. O PC pode terminar CFP a qualquer momento, mesmo que o tempo de duração informado no quadro *beacon* não tenha se esgotado, baseado no tráfego disponível e no tamanho de sua lista de *polling*.

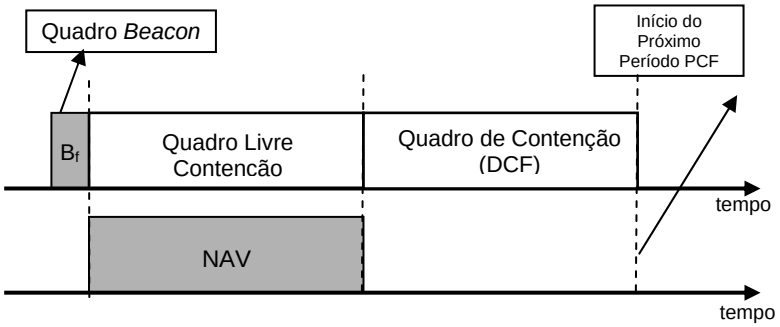


Figura 11: Períodos de acesso com e sem contenção

Todas as estações que estão na lista de *polling* e que, portanto, respondem a pedido de transmissão do PC, ignoram o mecanismo de *Detecção Virtual de Portadora* (temporizador NAV), verificando apenas se o meio está livre após um intervalo SIFS. Estações fora da lista que recebem quadros de dados devem confirmá-los segundo as regras do procedimento DCF. Caso uma estação inserida na lista de *polling* não envie dados, ou uma estação de fora da lista de *polling* não confirme dados recebidos, o PC assume o controle do meio após intervalo PIFS, como pode ser visto na figura a seguir. Caso uma estação na lista de *polling* não possua dados a serem enviados, deve retornar um pacote nulo (*null frame*) para o PC ter garantia de que não houve problemas de transmissão (como interferência causada pela sobreposição de pacotes de transmissão).

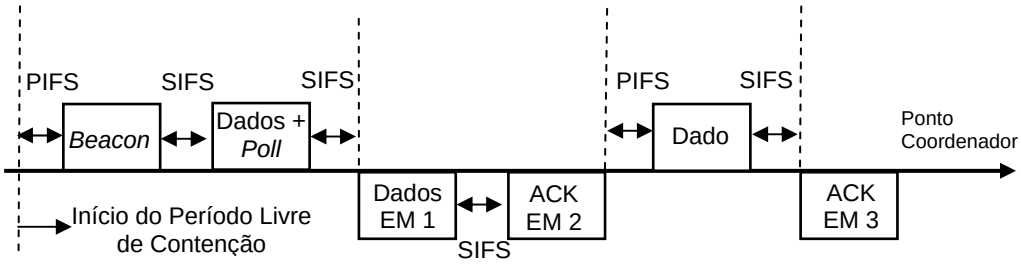


Figura 12: Exemplo de funcionamento do CFP

Uma estação define para a rede sem fio, no início de suas atividades, se deseja ou não estar na lista de *polling*, podendo mudar seu estado em relação à lista, posteriormente. O PC também interfere na constituição da lista, integrando ou descartando a estação da lista, pela observação de seu tráfego nos períodos com e sem contenção.

Por fim, observa-se que nem todas as estações reconhecem o modo de operação PCF. Neste caso, jamais integrarão a lista, e, se receberem dados, deverão confirmá-los como no regime DCF. Supõe-se que jamais obterão o controle do canal, pois, em nenhum momento, o canal deverá ficar livre por um tempo igual ou maior do que DIFS (o tempo máximo em que o canal ficará livre deve ser igual à PIFS).

As soluções adotadas para serviços com e sem contenção visam a atender, principalmente, requisitos de economia de energia e prioridade. De fato, o mecanismo de *Detecção Virtual da Portadora* possibilita que se desliguem os circuitos de transmissão e recepção até o contador NAV atingir zero, pois uma estação não pode transmitir, e nem receberá nenhum quadro durante este intervalo de tempo.

Porém, existe um problema inerente a estas duas modelagens, conhecido como estação escondida (*hidden node*).

O problema da estação escondida ocorre quando três estações A, B e C, com suas respectivas áreas de cobertura, necessitam de comunicação, conforme ilustrado na figura abaixo.

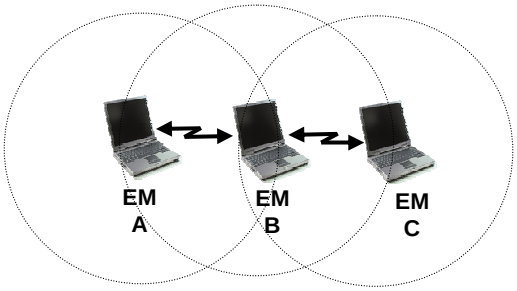


Figura 13: Problema da estação escondida

Esta situação acontece quando a estação A, querendo comunicar-se com B, envia um pacote seguindo as regras do modo DCF, e ao mesmo tempo C também quer enviar uma mensagem para B. O problema é que A e C não têm

áreas de cobertura completamente sobrepostas. Logo, pacotes de A podem não chegar a C e vice-versa.

A estação A recebe sinal de B, mas não de C. A estação C recebe sinal de B, mas não de A. Então, A e C não podem saber se B está em silêncio ou não.

Assim, as informações de tempo de transmissão nunca chegam e o contador NAV nunca é atualizado, o que provoca uma falsa informação de meio ocioso. As duas estações transmitem seus pacotes e, neste momento, ocorre a colisão.

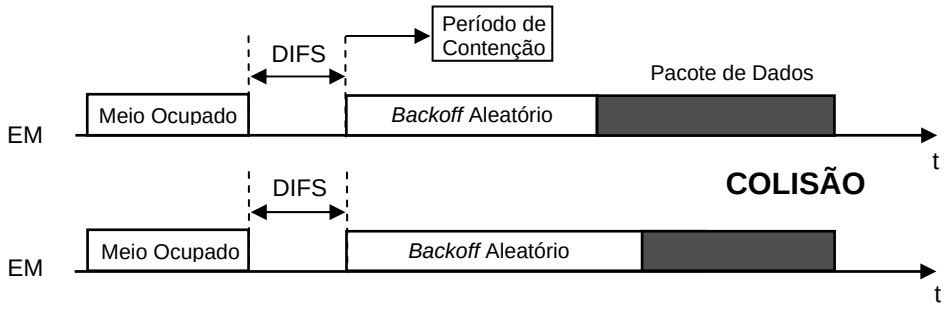


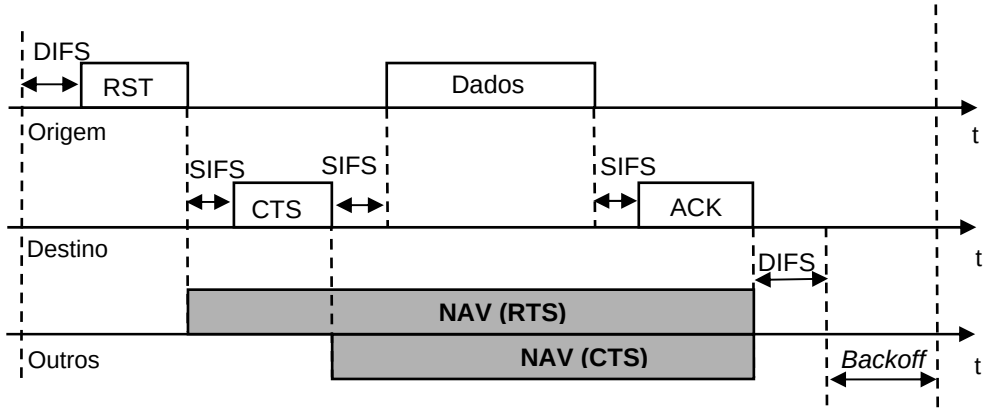
Figura 14: Problema de colisão (*hidden node*)

O problema de colisão não foi resolvido e, portanto, um novo método teve que ser adotado para então garantir que os pacotes pudessem ser transmitidos com sucesso.

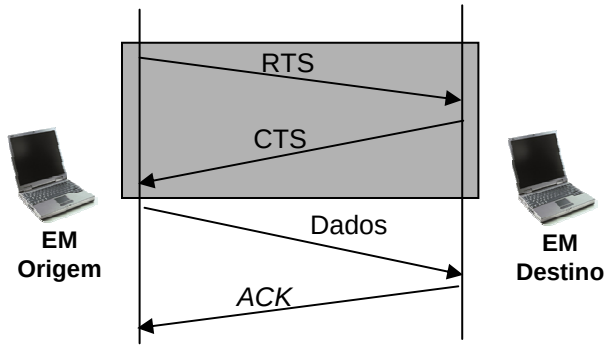
A solução consiste no transmissor e receptor, antes de entrar em operação, trocarem pequenos quadros de controle denominados RTS (*Request to Send*) e CTS (*Clear to Send*).

A estação que deseja transmitir envia um pacote RTS para a estação de destino. Se a estação de destino estiver livre, ela responde com um pacote CTS para a estação transmissora. Sendo assim, todas as estações ligadas ao AP ouvem este pacote e não fazem transmissões por um determinado período de tempo, permitindo assim que a estação transmissora envie seus dados e receba o pacote de reconhecimento (ACK) sem chance de colisões.

Assim, após a espera da liberação do meio, é enviado um pacote de requisição de transmissão chamado de RTS (*Request to Send*) e espera-se a confirmação deste pedido, CTS (*Clear to Send*), para então enviar os pacotes de dados.



Figuras 15: Transmissão com quadros RTS e CTS



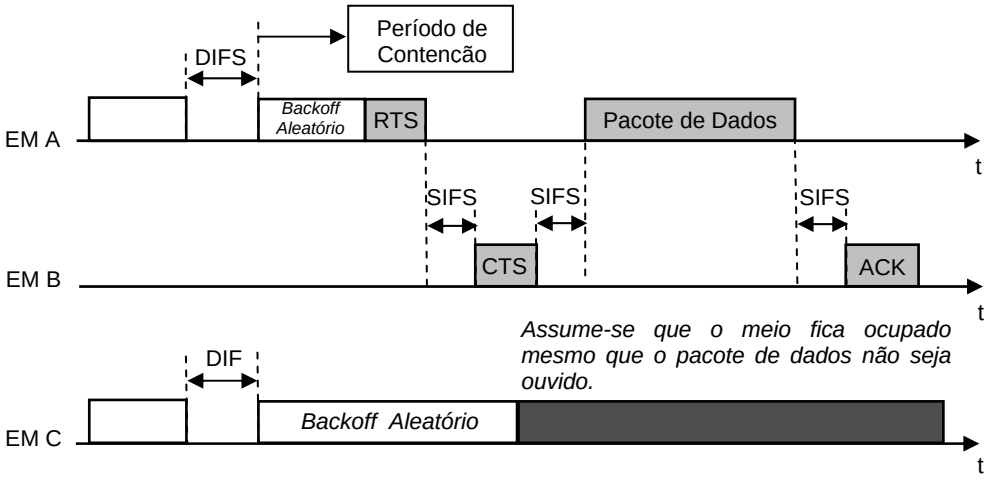
Figuras 16: Transmissão com quadros RTS e CTS (*Four-Way Handshake*)

Os pacotes RST e CTS têm um campo denominado *Duration/ID* que determina o tempo de acesso ao meio de que as estações necessitam para transmitir o pacote de dados, incluindo também o ACK.

As demais estações, ligadas ao AP, utilizam as informações de tempo do RTS/CTS para atualizar o contador NAV, e este determina a ocupação da rede.

Quando as estações desejam transmitir, elas verificam, em sua tabela se o meio está livre.

Os pacotes RTS e CTS contêm a informação do tempo previsto de duração de transmissão do pacote de dados. Estes pacotes informarão a todas estações pertencentes às áreas de cobertura das estações A e B, que o meio está ocupado durante o tempo indicado. Assim, a possibilidade de colisão no meio será mínima.



Figuras 17: Transmissão entre as estações A e B com reserva de recursos

A diminuição da probabilidade de colisão é obtida à custa de um grande *overhead* envolvendo as trocas dos quadros CTS e RTS, o que pode ser significativo para pacotes de dados pequenos.

A seguir é apresentado um resumo dos intervalos entre pacotes:

a) SIFS (*Short Inter Frame Space*): definido com o menor intervalo de tempo entre pacotes. Tempo aguardado pelos pacotes de maior prioridade, tais como um pacote de resposta de transmissão ACK, ou um pacote de resposta CTS (Clear to Send);

b) PIFS (*PCF Inter Frame Space*): intervalo em que a estação, trabalhando no modo PCF, deve aguardar para enviar o seu pacote;

c) DIFS (*DCF Inter Frame Space*): intervalo de tempo em que, uma estação no modo DCF, deve aguardar para transmitir seus pacotes. Este tempo é maior que o PIFS, o que significa que as estações que trabalham no modo PCF têm prioridade de transmissão sobre as que trabalham no modo DCF;

d) EIFS (*Extended Inter Frame Space*): período de tempo em que toda estação que trabalha no modo DCF deve aguardar quando um pacote com problemas é recebido e seus erros foram detectados pelo FCS. Este intervalo de tempo permite à estação receptora corrigir o pacote e transmitir o ACK, pois é iniciado logo após o DIFS.

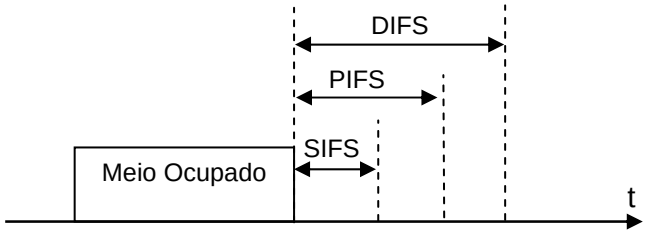


Figura 18: Intervalos de tempo que diferentes pacotes devem aguardar

2.4.4
Pacotes da Camada MAC

2.4.4.1
Quadro MAC

O *frame* MPDU (*MAC Protocol Data Unit*) da subcamada MAC é composto dos seguintes componentes básicos:

a) Cabeçalho MAC: contém informações de controle do *frame*, duração, endereços e informações de controle de seqüência;

b) Corpo do *frame* com tamanho variável: contém informações específicas do tipo do *frame*;

c) Informação de redundância FCS (*Frame Check Sequence*).

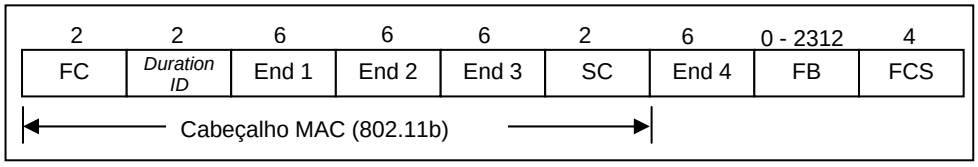


Figura 19: Formato do quadro MAC

O conteúdo de cada campo é mostrado a seguir:

a) FC (*Frame Control*): contém as informações de controle enviadas da estação transmissora para a estação receptora. Ele é subdividido em outros campos, cada um com uma respectiva função: versão e tipo de protocolo, informações de fragmentação e gerenciamento de energia, e encriptação (WEP), como será visto adiante;

b) *Duration ID*: este campo tem significados diferentes, dependendo do contexto, os quais podem ser:

⇨ Em pacotes de controle do subtipo PS *(Power Save)*, o campo *Duration/ID* tem, em seus dois bits mais significativos, valores 1 e 1, e no restante dos 14 bits, a identificação da associação AID *(Association Identity*) da EM que transmitiu o pacote. O valor do AID varia de 1 a 2007;

⇨ Para os demais tipos de pacotes, o campo *Duration/ID* indica o tempo de duração de transmissão necessário para as EM atualizarem o temporizador NAV;

c) Endereço 1, 2, 3 e 4: este campo carrega diferentes tipos de endereço, dependendo do tipo de pacote que está sendo enviado. Os endereços podem ser:

⇨ DA (*Destination Address*): endereço do destino final do pacote;

⇨ SA (*Source Address*): endereço de origem do pacote, ou seja, da primeira estação a transmiti-lo;

⇨ RA (*Receiver Address*): endereço que determina o destino imediato do pacote, como, por exemplo, o endereço do AP, se a estação estiver utilizando um BSS;

⇨ TA (*Transmitter Address*): endereço que determina a estação que transmitiu o *frame*. Esta estação pode ser um ponto intermediário da comunicação, como, por exemplo, um AP;

⇨ BSSID (*Basic Service Set Identification*): identificação da BSS em que se encontram as EM. Utilizado também para limitar o alcance de *broadcast*;

d) SC (*Sequence Control*): este campo é responsável pelo controle de seqüência de pacotes que são fragmentados. O SC tem duas funções: identificar em quantos pacotes a mensagem será fragmentada e informar qual porção do pacote fragmentado está sendo transmitido no momento;

e) FB (*Frame Body*): neste campo são inseridas as informações provenientes das camadas superiores, inclusive da camada LLC (MSDU), se for o caso. O seu tamanho varia entre 0 e 2312 bytes;

f) FCS (*Frame Check Sequence*): a subcamada MAC da estação transmissora calcula uma seqüência de 32 bits, que é o resultado da operação efetuada pelo código CRC sobre o cabeçalho e o campo FB do pacote, e a insere

neste campo. Sua função é permitir que o pacote possa ser recuperado caso ocorram erros durante sua transmissão.

2.4.4.2
Campo FC - *Frame Control*

Este campo está presente em todos os pacotes transmitidos e tem o seguinte formato:

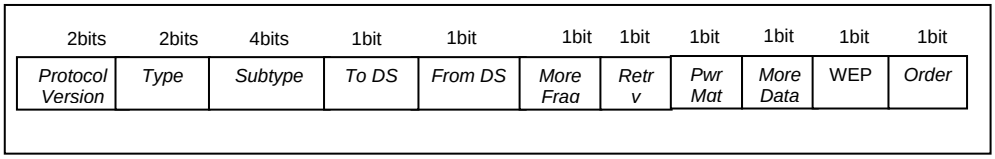


Figura 20: Formato do campo FC

a) *Protocol Version*: indica a versão do protocolo;

b) Type: indica o tipo do *frame* transmitido. Os tipos podem ser:

- ⇨ 00: *Management*
- ⇨ 01: *Control*
- ⇨ 10: *Data*
- ⇨ 11: Reservado

c) *Subtype:* indica o subtipo do *frame*, e em combinação com o campo *Type*, define a função do *frame*. A combinação do tipo e subtipo pode resultar em *frames* de: associação, reassociação, autenticação, RTS, CTS, dentre outros;

d) *ToDS*: indica se o destino do *frame* é um DS;

e) *FromDS*: indica se a origem do *frame* é um DS;

To DS	From DS	End 1	End 2	End 3	End 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	AS	DA	N/A
1	1	RA	TA	DA	SA

Tabela 2: Possíveis combinações de *ToDS/FromDS*

f) *More Fragments:* indica se há mais fragmentos pertencentes ao mesmo *frame*;

g) *Retry:* indica se o pacote está sendo retransmitido. A estação receptora do pacote utiliza este valor para controlar a eliminação de pacotes duplicados, em casos onde a estação transmissora não tenha recebido o quadro ACK;

h) *Power Management:* indica o modo de gerenciamento de energia que a estação usará após o sucesso na seqüência de troca de quadros;

i) *More Data:* indica se há mais quadros a serem transmitidos do AP para a EM. Este campo é utilizado em conjunto com o *Power Management*, para que a EM não entre no modo econômico pelo fato de existirem mais dados para ela. Ou caso a EM esteja no modo econômico, ela decida entrar no modo ativo para a recepção de vários quadros;

j) *WEP:* indica se o corpo do *frame* está sendo transmitido criptografado. O valor 1 indica que há criptografia;

k) *Order:* indica se o *frame* está sendo transmitido utilizando uma classe de serviço *StrictOrder*, utilizado, principalmente, quando há fragmentação.

2.4.4.3
Pacotes de Controle

Request To Send (RTS): este pacote é enviado para uma estação solicitar permissão de transmitir seu pacote.

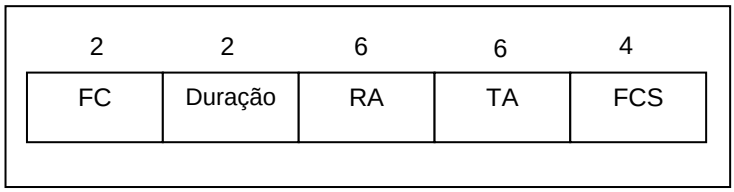


Figura 21: Formato do pacote RTS

Clear To Send (CTS): depois de receber um pacote RTS, a estação envia um pacote CTS para informar à estação transmissora que o pacote de informações pode ser enviado.

Este pacote é semelhante ao pacote RTS, mas sem o endereço de origem, pois ele só é enviado para a estação que enviou o RTS anteriormente.

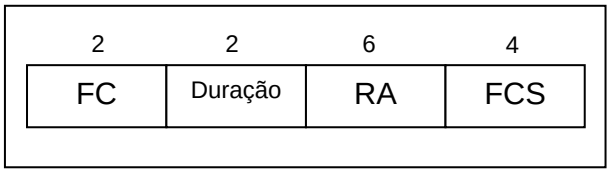


Figura 22: Formato do pacote CTS

Acknowledgement (*ACK*): toda estação que recebe um pacote de dados com sucesso deve retornar um pacote ACK à estação transmissora, informando o seu recebimento sem problemas.

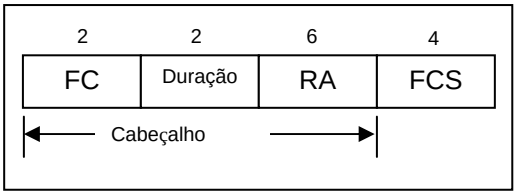


Figura 23: Formato do Pacote ACK

Power-Save Poll (PS-Poll): pacote enviado para atualizar o campo NAV de todas as estações da área de cobertura em comunicação.

Os novos campos que aparecem são AID (*Association Identifier*), que identifica a qual AP a estação deverá se associar, e o BSSID (*Basic Service Set Identification*), com a identificação da BSS atual.

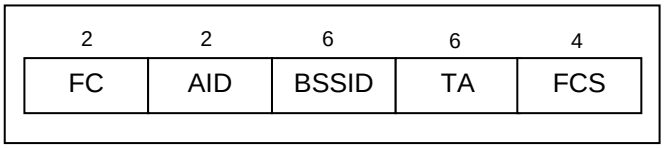


Figura 24: Formato do Pacote *PS-Poll*

CF End (Contention-Free End): Este pacote informa o fim do período de contenção no modo PCF.

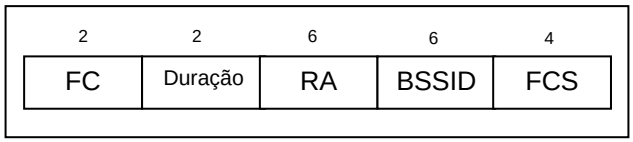


Figura 25: Formato do Pacote *CF End*

2.4.4.4
Pacote de Dados

O quadro de dados segue o seguinte formato:

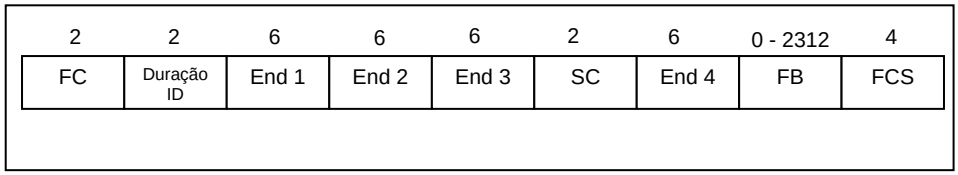


Figura 26: Formato do Pacote de Dados

O campo *Endereço* pode assumir diferentes valores dependendo dos valores dos campos *ToDS/FromDS*.

2.5
Serviços em Redes IEEE 802.11

O padrão IEEE 802.11 define os serviços que as subcamadas MAC e LLC necessitam para o envio de pacotes entre duas estações. Estes serviços podem ser classificados em duas categorias:

a) Serviços de Estação (*SS - Station Service*), presentes em todas as EM;

b) Serviços de Sistema de Distribuição (*DSS - Distribution System Service*), fornecidos pelo sistema distribuído.

2.5.1
Tipos de Mensagens

Existem três tipos de mensagens que podem ser trocadas entre as estações:

a) Mensagem de Gerência: tem por finalidade dar suporte aos serviços do IEEE 802.11;

b) Mensagem de Controle: tem por finalidade dar suporte à entrega das mensagens de dados e gerência;

c) Mensagem de Dados.

2.5.2
Serviços de Estação

Esta categoria define os serviços que são necessários para troca de informações entre duas estações. Para desempenhá-los, a estação deve enviar e receber pacotes denominados MSDU (*MAC Service Data Units*) e implementar níveis de segurança.

Os serviços de estação são importantes e necessários para que uma rede sem fio possua funcionalidade equivalente a uma rede com fio.

a) ***Autenticação***: procedimento efetuado por toda estação para se conectar à rede sem fio. Ele é necessário para garantir que apenas estações autorizadas se conectem à rede, garantindo, assim, a segurança. O processo se dá quando uma estação envia um quadro de gerenciamento de autenticação, que é a solicitação de entrada na rede. De acordo com a política de cada modo de autenticação, um procedimento é iniciado para verificação dos dados contidos no quadro, tais como: endereço, chave de segurança e demais dados da estação. Sem autenticação, não existe associação. Existem dois modos de autenticação definidos e que serão explorados com mais detalhes no capítulo 3.

⇨ Autenticação por Sistema Aberto;

⇨ Autenticação por Chave Compartilhada.

b) ***Privacidade (Criptografia)***: a necessidade de privacidade das informações em redes sem fio é muito importante, pois os dados numa área de cobertura estão disponíveis para todas as estações. Mas nem sempre estes dados podem ser disponibilizados a todos os usuários. Surge assim a necessidade de cifragem dos dados, que tem como objetivo codificá-los para que apenas usuários autorizados tenham acesso às informações. O mecanismo desenvolvido para executar esta função é denominado WEP (*Wired Equivalent Privacy*), a ser estudado em detalhes no capítulo 3.

c) ***Desautenticação***: Procedimento utilizado por uma estação quando não existe mais a necessidade de comunicação. Este procedimento não pode ser negado e também se dá através de um quadro de gerenciamento de autenticação.

2.5.3
Serviços de Sistema de Distribuição

Quando é utilizada uma estrutura de rede do tipo ESS, é responsabilidade do sistema de distribuição localizar e rotear as mensagens.

Para isto são necessários alguns serviços, nos quais todos os AP interligados ao sistema de distribuição devem implementar:

a) ***Associação***: toda estação que deseja enviar uma informação deve iniciar um serviço de associação, no caso de já estar autenticada na rede. Este serviço mapeia as estações que podem estar associadas a um AP. Uma estação somente pode estar associada a um único AP de cada vez. O AP, por sua vez, pode se associar a várias estações em determinado momento;

b) ***Desassociação***: uma EM inicia um serviço de desassociação para finalizar uma associação existente, devido a uma migração ou desligamento. Pode ser requisitado pela estação ou AP;

c) ***Integração***: este serviço garante que quadros MAC podem ser trocados e compreendidos por estações utilizando IEEE 802.11b e estações utilizando outras tecnologias;

d) ***Reassociação***: através deste serviço, uma estação pode alterar seu estado de associação atual podendo ser no mesmo AP ou com um AP distinto. O processo de reassociação é sempre iniciado por uma estação.

e) ***Distribuição***: responsável pela distribuição dos quadros, equivalente ao roteamento em uma rede convencional. É de responsabilidade do serviço de distribuição localizar a estação de destino do quadro;

A figura seguir ilustra o relacionamento dos estados de uma conexão entre dispositivos sem fio.

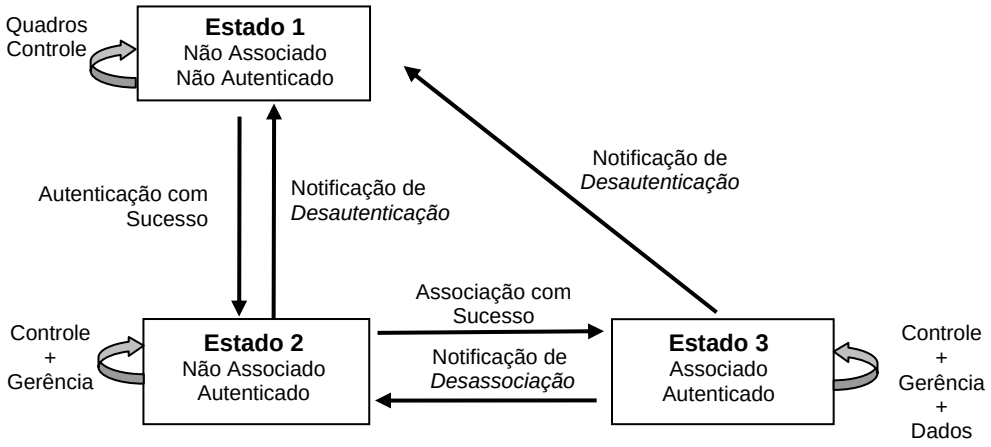


Figura 27: Diagrama de Estados - Autenticação e Associação