3
Redes Locais sem fio IEEE 802.11

3.1.
Padrões das redes sem fio IEEE 802.11

Uma rede sem fio *(Wireless)* é tipicamente uma extensão de uma rede local *(Local Area Network - LAN)* convencional com fio, criando-se o conceito de rede local sem fio *(Wireless Local Area Network - WLAN)*. Uma WLAN converte pacotes de dados em onda de rádio ou infravermelho e os envia para outros dispositivos sem fio ou para um ponto de acesso que serve como uma conexão para uma LAN com fio.

"Uma rede sem fio é um sistema que interliga vários equipamentos fixos ou móveis utilizando o ar como meio de transmissão".

A Figura 4 ilustra uma rede sem fio conectada por um ponto de acesso (AP) a uma rede convencional com fio.

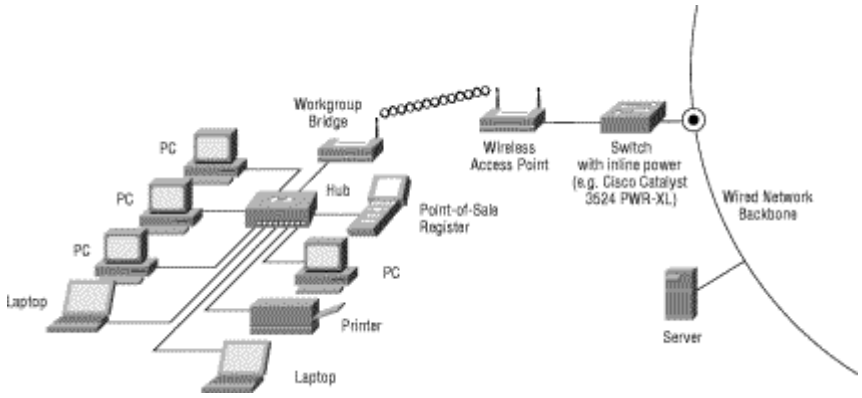


Figura 4 Conexão de uma rede sem fio com uma convencional com fio

O IEEE constituiu um grupo chamado de WLAN – SWG (*Wireless Local-Area Networks Standard Working Group),* com a finalidade de criar padrões para redes sem fio, definindo um nível físico para redes onde, as transmissões são realizadas na freqüência de rádio ou infravermelho, e um protocolo de controle de acesso ao meio, o DFWMAC (*Distributed Foundation Wireless MAC*).

Esse padrão é denominado de Projeto IEEE 802.11 e tem, entre outras, as seguintes premissas: Suportar diversos canais; sobrepor diversas redes na mesma área de canal; apresentar robustez com relação à interferência; possuir mecanismos para evitar *nós* escondidos; oferecer privacidade e controle de acesso ao meio.

A Figura 5 ilustra o padrão IEEE 802.11, comparando com o modelo padrão de redes de computadores, o RM-OSI da ISO (*Reference Model – Open Systems Interconnection of the International Standardization Organization*).

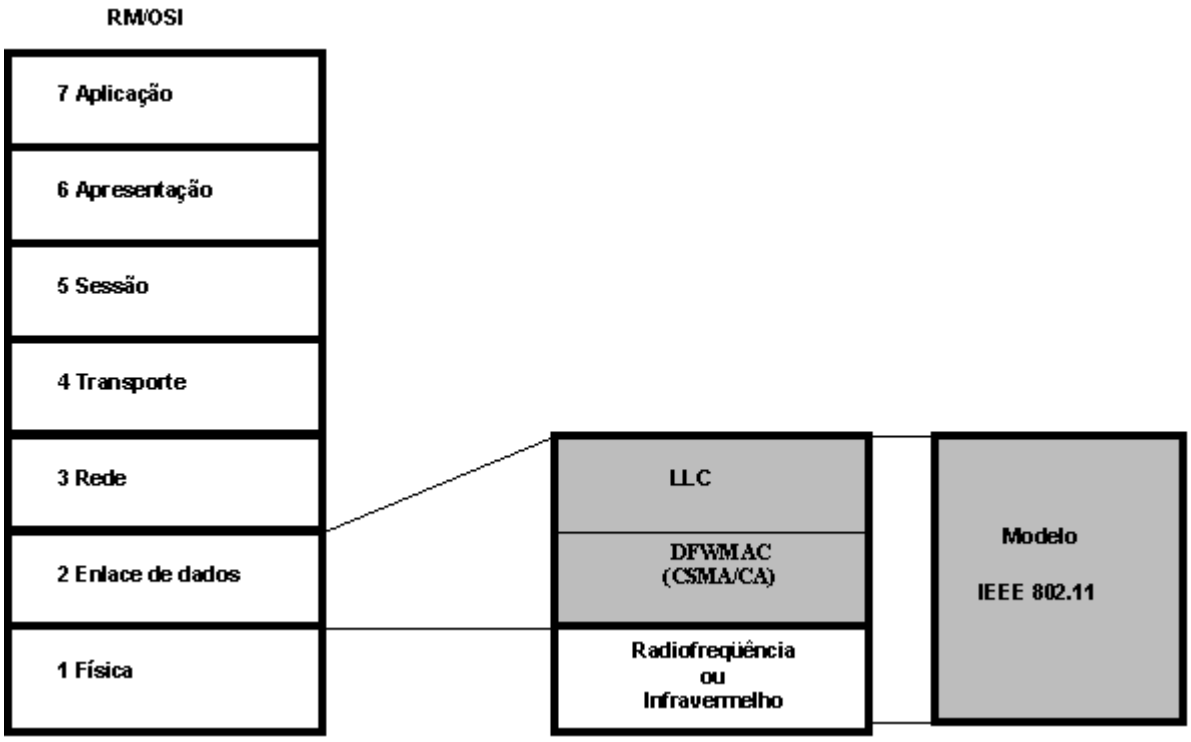


Figura 5 - Comparação do padrão 802.11 com o RM-OSI

A maioria das redes sem fio é baseada nos padrões IEEE 802.11 e 802.11b (sendo este último evolução do primeiro), para comunicação sem fio entre um dispositivo e uma rede LAN. Esses padrões permitem transmissão de dados de 1 a 2Mbps, para o padrão IEEE 802.11, e de 5 a 11Mbps, para o padrão IEEE 802.11b, e especificam uma arquitetura comum, métodos de transmissão, e outros aspectos de transferência de dados sem fio, permitindo a interoperabilidade entre os produtos.

Duas razões contribuíram bastante para que a tecnologia sem fio avançasse: a aprovação do padrão IEEE 802.11, em 1997, o que ajudou a tornar as WLAN uma realidade; e o barateamento dos equipamentos para WLAN, que fizeram com que as redes sem fio ficassem mais acessíveis para algumas empresas, aumentando consideravelmente a comercialização de produtos para computadores móveis, como o cartão PCMCIA para Notebook e o cartão PCI / USB para PCs.

3.1.1. Pilha de Protocolos

Semelhante ao que ocorre quando se utiliza a rede local com fio (LAN) , por exemplo : Ethernet, os padrões de Redes locais sem fio (WLAN) especificam as camadas 1 e 2 do modelo OSI :

a) Camada 1 (camada física) => suporta o serviço de transmissão radio . Define o sinal transmitido (Banda de frequencia, largura de banda do canal, modulação, filtragem) em relação à codificação do canal necessária para assegurar uma maior robustez da transmissão radio.

b) Camada 2 (Camada de Enlace de dados) => esta camada está dividida em duas subcamadas:

- **Subcamada MAC (Controle de acesso ao meio) =>** Suporta o serviço de acesso ao meio para transmissão dos frames (quadros). Dependendo do padrão, este tipo de acesso pode ser suportado com esquemas baseado em contenção ou contenção livre.

- **Subcamada LC (Controle de enlace) =>** é responsável pela condução às conexões lógicas e interface com as camadas superiores. Dependendo do padrão, a subcamada de controle de enlace deve suportar : esquemas de retransmissão e detecção de erros usando algoritmos ARQ (Automatic Repeat Request) ; Controle de admissão; Gerenciamento de conexões; Controle de recursos rádio; Uso em dependência de subcamada LLC existente especificada no padrão IEEE 802.2

Então, a camada 2 suporta um serviço de transporte para unidades de dados entregues pelas camadas mais altas, camada 3 (Camada rede-OSI) e tecnologias WLAN que são comumente usadas na entrega de datagramas IP sobre o enlace rádio. Entretanto, no sentido de simplificar implementações, produtos atuais oferecem o transporte radio para frames ethernet.

Desta forma, podemos entregar um serviço totalmente equivalente para camadas mais altas : a pilha de protocolos terminal (pilhas TCP/IP num PC) usa a mesma forma de interface interna (driver) , qualquer que seja a mídia (LAN tradicional ou WLAN).

3.2. Arquitetura de uma rede sem fio IEEE 802.11

O padrão IEEE 802.11 define uma arquitetura para as redes sem fio, baseada na divisão da área coberta pela rede em células. Essas células são denominadas de **BSA *(Basic Service Area)***. O tamanho da BSA (célula) depende das características do ambiente e da potência dos transmissores / receptores usados nas estações.

Existem outros elementos fazendo parte do conceito da arquitetura de rede sem fio, que serão descritos abaixo :

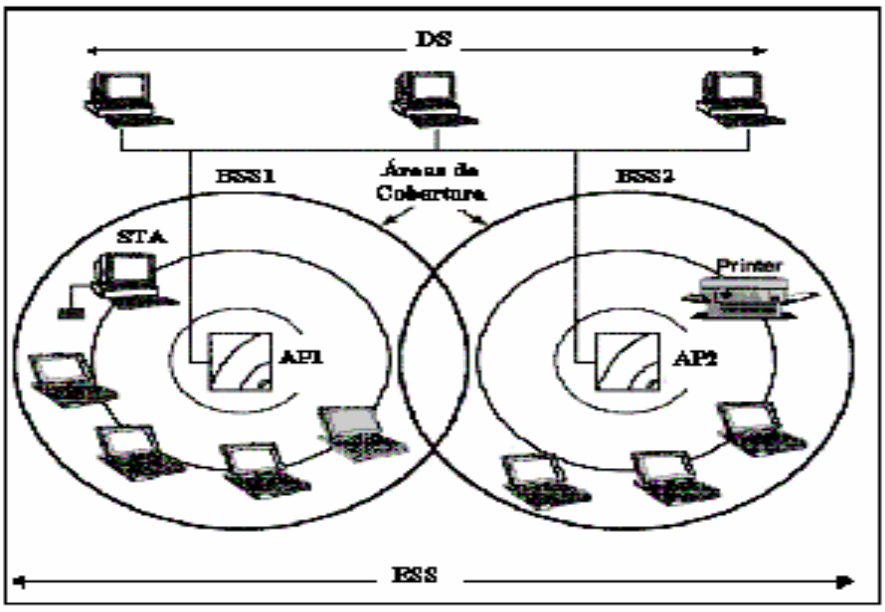


Figura 6 Arquitetura de uma rede sem fio

a) Conjunto de serviço básico *(Basic Service Set - BSS)* => representa um grupo de estações comunicando-se por radiodifusão ou infravermelho em uma BSA.

b) Estações de Trabalho (**Wireless LAN Station – STA**) => Estão representando as estações (clientes) da rede

c) Ponto de acesso *(Access Point – AP)* – são estações especiais responsáveis pela captura das transmissões realizadas pelas estações (STA) de sua BSA, destinadas a estações localizadas em outras BSAs, retransmitindo-as, usando um sistema de distribuição.

d) Sistema de distribuição (Distribution System - DS) => representa uma infra-estrutura de comunicação (backbone) que interliga múltiplas BSAs para permitir a construção de redes cobrindo áreas maiores que uma célula.

e) Area de serviço extendida *(Extend Service Area - ESA)* => representa a interligação de vários BSAs pelo sistema de distribuição através dos APs.

f) Conjunto de serviço extendido *(Extend Service Set - ESS)* => representa um conjunto de estações formado pela união de vários BSSs cujos APs estão conectados a uma mesma rede convencional por um sistema de distribuição. Nestas condições uma STA pode se movimentar de uma célula BSS para outra permanecendo conectada à rede. Este processo é denominado de Roaming.

A Figura abaixo, apresenta a união de duas BSSs conectadas por um sistema de distribuição.

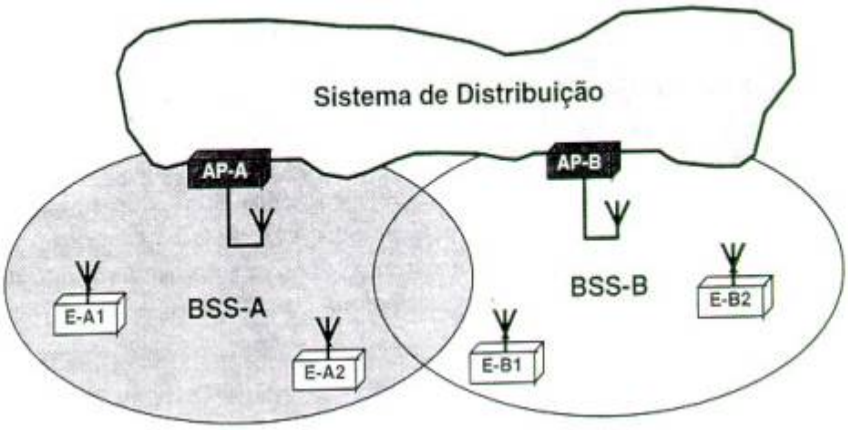


Figura 7 – União de duas BSS formando uma ESS

A identificação da rede ocorre da seguinte maneira: cada um dos ESSs recebe uma identificação chamada de ESS-ID; dentro de cada um desses ESSs, cada BSS recebe uma identificação chamada de BSS-ID. Então, o conjunto formado por esses dois identificadores (o ESS-ID e o BSS-ID), forma o *Network-ID* de uma rede sem fio padrão 802.11.

Apesar dos elementos que fazem parte da arquitetura sem fio possibilitar a construção de uma rede abrangendo áreas maiores do que um ambiente local, o projeto do IEEE 802.11 limita o padrão IEEE 802.11 às redes locais, com ou sem infra-estrutura.

Numa rede WLAN sem infra-estrutura (conhecidas por redes *Ad Hoc*), as estações se comunicam numa mesma célula, sem a necessidade de estações especiais, ou seja, sem necessidade dos APs para estabelecer as comunicações. Numa rede local com infra-estrutura, é necessária a interconexão de múltiplos BBSs, formando um ESS. Nesse caso, a infra-estrutura é representada pelos APs, e pelo sistema de distribuição que interliga esses APs. O sistema de distribuição, além de interligar os vários pontos de acesso, pode fornecer os recursos necessários para interligar a rede sem fio a outras redes, e ele, o sistema de distribuição, geralmente é representado por um sistema de comunicação com fio (cobre ou fibra).

Um elemento fundamental na arquitetura de rede local sem fio com infra-estrutura é o ponto de acesso, que desempenha as seguintes funções:

a) ***autenticação, associação e reassociação***: permite que uma estação móvel mesmo saindo de sua célula de origem continue conectada à infra-estrutura e não perca a comunicação.

A função que permite manter a continuidade da comunicação quando um usuário passa de uma célula para outra, é conhecida como *handoff* .

b) ***gerenciamento de potência****:* permite que as estações operem economizando energia, através de um modo chamado de *power save*.

c) ***Sincronização****:* garante que as estações associadas a um AP estejam sincronizadas por um relógio comum

3.3. Protocolo MAC do padrão IEEE 802.11

Além de definir um mecanismo para transmissão física usando radiofreqüência ou infravermelho, o IEEE definiu um protocolo de acesso ao meio (subcamada MAC do nível de enlace de dados), denominado de DFWMAC (*Distributed Foundation Wireless Medium Access Control*), que suporta dois métodos de acesso: um método distribuído básico, que é obrigatório, e um método centralizado, que é opcional, podendo esses dois métodos coexistir, o protocolo de acesso ao meio das redes 802.11 também tratam de problemas relacionados com estações que se deslocam para outras células (*roaming*) e com estações perdidas (*hidden node*).

O método de acesso distribuído forma à base sobre a qual é construído o método centralizado. Os dois métodos, que também podem ser chamados de funções de coordenação *(Coordination Functions)*, são usados para dar suporte à transmissão de tráfego assíncrono ou tráfego com retardo limitado (*time bounded*).

Uma *função de coordenação* é usada para decidir quando uma estação tem permissão para transmitir. Na função de coordenação distribuída *(Distributed Coordination Functions - DCF)*, essa decisão é realizada individualmente pelos *pontos* da rede*,* podendo, dessa forma, ocorrer colisões. Na função de coordenação centralizada, também chamada de função pontual *(Point Coordination Function - PCF)*, a decisão de quando transmitir é centralizada em um ponto especial, que determina qual estação deve transmitir em que momento, evitando teoricamente a ocorrência de colisões . Seguem detalhes do funcionamento dessas duas funções:

3.3.1. Função de Coordenação Distribuída (DFC)

Representa o método de acesso básico do protocolo DFWMAC. É uma função conhecida como CSMA/CA *(Carrier Sense Multiple Access / Collision Avoidance)* com reconhecimento. A DFC trabalha semelhantemente a função CSMA/CD da tecnologia de rede local cabeada (Padrão Ethernet 802.3), apenas com uma diferença: o protocolo CSMA/CD do Ethernet controla as colisões quando elas ocorrem, enquanto que o protocolo CSMA/CA do padrão sem fio apenas tenta evitar as colisões. A utilização dessa função distribuída é obrigatória para todas as estações e pontos de acesso (APs), nas configurações *Ad Hoc* e com *infra-estrutura*, e ela, a DFC, trabalha da seguinte maneira, quando uma estação deseja transmitir :

a) a estação sente o meio para determinar se outra estação já está transmitindo.

b) se o meio estiver livre, a estação transmite seu quadro, caso contrário, ela aguarda o final da transmissão.

c) após cada transmissão com ou sem colisão, a rede fica em um modo onde às estações só podem começar a transmitir em intervalos de tempo a elas pré-alocados.

d) ao findar uma transmissão, as estações alocadas ao primeiro intervalo têm o direito de transmitir. Se não o fazem, o direito passa as estações alocadas ao segundo intervalo, e assim sucessivamente até que ocorra uma transmissão, quando todo o processo reinicia.

e) se todos os intervalos não são utilizados, a rede entra então no estado onde o CSMA comum é usado para acesso, podendo dessa forma ocorrer colisões.

No método CSMA/CA pode ocorrer colisões e esse método não garante a entrega correta dos dados. Com isso, uma estação após transmitir um quadro, necessita de um aviso de recebimento que deve ser enviado pela estação destino. Para isso, a estação que enviou o quadro aguarda um tempo *(timeout)* pelo aviso de recebimento do quadro por parte da estação destino. Caso esse aviso não chegue no tempo considerado, a estação origem realiza novamente a transmissão do quadro.

Para melhorar a transmissão de dados, o protocolo DFWMAC acrescenta ao método CSMA/CA com reconhecimento, um mecanismo opcional que envolve a troca de quadros de controle RTS *(Request To Send)* e CTS *(Clear To Send)* antes da transmissão de quadros de dados. Esse mecanismo funciona da seguinte forma:

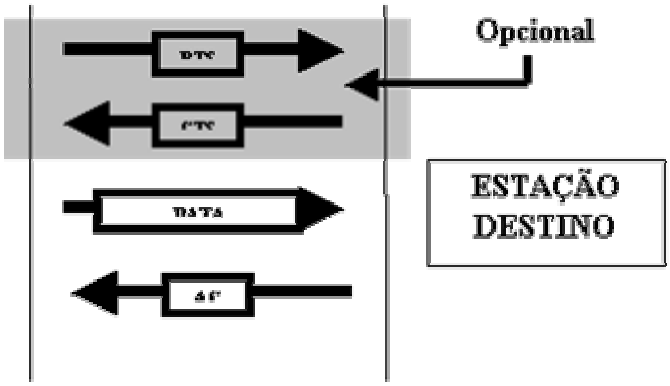
a) uma estação antes de efetivamente transmitir o quadro de dados, transmite um quadro de controle RTS, que carrega uma estimativa da duração no tempo da futura transmissão do quadro de dados.

b) A estação de destino em reposta ao quadro de controle RTS envia um quadro de controle CTS avisando que está pronta para receber o quadro de dados. Só então, a estação transmissora envia o quadro de dados, que deve ser respondido com um reconhecimento *(ack)* enviado pela estação receptora.

O quadro RTS basicamente possui as funcionalidades de reservar o meio para a transmissão do quadro de dados, e de verificar se a estação de destino está pronta para receber o quadro de dados, sendo esta última funcionalidade devido à possibilidade da estação de destino estar operando no modo de economia de energia (modo *power save)*.

A figura abaixo, apresenta a troca de dados para a transmissão de informações, usando o mecanismo opcional com RTS e CTS.

ESTAÇÃO FONTE



ESTAÇÃO DESTINO

Figura 8 – Troca de dados para transmissão de informações

O mecanismo básico do controle de acesso DFWMAC é ilustrado na Figura 9, nela podemos observar que uma estação, com quadros para transmitir, deve sentir o meio livre por um período de silêncio mínimo, *IFS* (*Inter Frame Space*), antes de utilizá-lo. Utilizando valores diferentes para esse período.

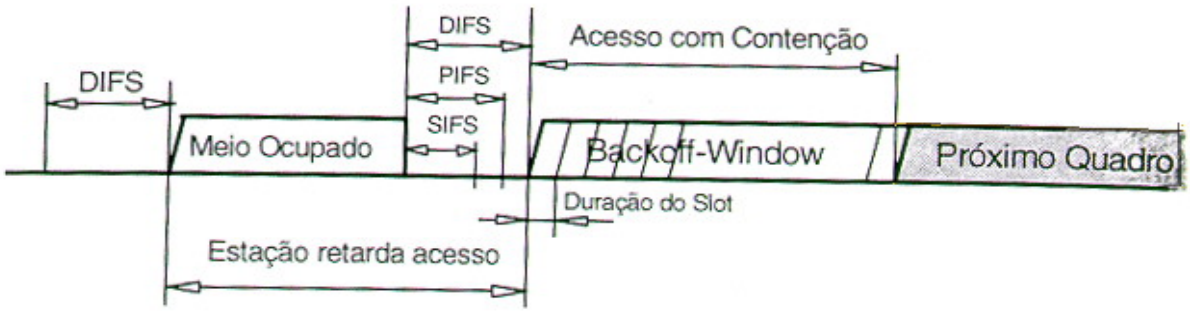


Figura 9 - Método de acesso CSMA/CA

O DFWMAC define três prioridades de acesso ao meio :

a) Distributed Inter Frame Space (*DIFS*) – espaço entre quadros da DFC (*Função de Coordenação Distribuída*), este parâmetro indica o maior tempo de espera, ele monitora o meio, aguardando no mínimo um intervalo de silêncio para transmitir os dados.

b) Priority Inter Frame Space (*PIFS*) – espaço entre quadros da PFC (*Função de Coordenação Pontual*), um tempo de espera entre o DIFS e o SIFS (prioridade média) envia quadros de contenção de superquadros, é usado para o serviço de acesso com retardo.

c) Short Inter Frame Space (*SIFS*) – é usado para transmissão de quadros carregando respostas imediatas (curtas), como ACK.

3.3.2. Função de Coordenação Pontual (PCF)

Trata-se de uma função opcional que pode ser inserida no protocolo DFWMAC, sendo construída sobre uma função de coordenação distribuída (DCF) para transmissões de quadros assíncronos, e é implementada através de um mecanismo de acesso ordenado ao meio, que suporta a transmissão de *tráfego com retardo limitado* ou *tráfego assíncrono*.

Para a integração dessas duas funções – pontual e distribuída – é utilizado o conceito de superquadro, fazendo com que o protocolo possa trabalhar de uma forma em que a função pontual assuma o controle da transmissão, para evitar a ocorrência de colisões. Para isso, o protocolo DFWMAC divide o tempo em períodos denominados superquadros, que consiste em dois intervalos de tempo consecutivos, que são usados da seguinte maneira :

a) no primeiro tempo, controlado pela PCF, o acesso é ordenado, o que evita a ocorrência de colisões;

b) no segundo tempo, controlado pela DCF, o acesso baseia-se na disputa pela posse do meio, podendo ocorrer colisões.

3.4. Roaming

O roaming é uma importante característica de comunicação sem fio. Permite que estações mudem de célula e continuem enviando e recebendo informações. Sistemas de roaming empregam arquiteturas de microcélulas que usam pontos de acesso estrategicamente localizados. O handoff entre pontos de acesso é totalmente transparente para o usuário.

Redes sem fio típicas dentro de prédios requerem mais que apenas um AP para cobrir todos os ambientes. Dependendo do material de que é feita a parede dos prédios, um AP tem um raio transmissão que varia de 10 a 20 metros, se a transmissão for de boa qualidade. Se um usuário passeia com uma estação (aparelho sem fio), a estação tem que se mover de uma célula para outra. A função do *roaming* funciona da seguinte forma :

a) Uma estação móvel, ao entrar em uma nova célula, e não estando em conversação, registra-se automaticamente pelo AP que controla a célula destino.

b) Na célula visitada, o AP desta, irá verificar se a estação móvel visitante não havia se registrado anteriormente. Caso esse procedimento não tenha sido efetuado, o referido AP irá informar ao AP da célula origem sobre a nova posição.

c) Com isso, o AP da célula origem fica sabendo da nova posição da estação móvel, e envia a informação a ela destinada, como se a referida estação estivesse em sua própria célula.

3.5. Estações Perdidas (Hidden Node)

Um dos grandes problemas em redes sem fio ocorre quando uma estação fica incomunicável por um período de tempo com o AP. São vários os motivos porque isto ocorre.

O desligamento da estação móvel, a saída da estação móvel da área de atuação do AP, entrada da estação móvel em uma área, onde as ondas de rádio proveniente de outro lugar não se propagam ou locais com grande degradação de sinal, que pode ser por motivos geográficos ou ambientais (área de sombra).

A Figura abaixo ilustra uma perda de conexão do AP com a estação móvel por razões geográficas.

Figura 10 - Perda de conexão com a estação móvel por razão geográfica

O protocolo MAC analisa o problema de estações perdidas da seguinte forma:

a) Ao tentar comunicar-se com a estação móvel inúmeras vezes sem obter resposta, o AP envia um *request* para todas as outras estações móveis sob sua área de cobertura. Cada uma destas envia um *request communication* para a estação perdida, esta por sua vez, envia um *response request* para todos avisando que está ativo.

b) As estações que ouvirem esta comunicação enviam um *bridge request*, diretamente para o AP, podendo que assim encontrar a melhor opção de comunicação entre o AP e a estação perdida.

A Figura 11 ilustra o AP escolhendo uma estação móvel para usar como ponte para comunicar-se com a estação perdida.

Figura 11 - AP escolhe uma estação móvel mas próxima da estação perdida para usar como ponte.

A comunicação do AP com a estação perdida, será via “ponte”. O AP deve enviar dados para a ponte, como diretamente para a estação perdida. Assim se esta receber a comunicação, não há mais a necessidade da ponte.

Se o AP perder a comunicação com a ponte ou a ponte perde a comunicação com a estação perdida, o AP escolhe outra ponte entre as estações que respondera inicialmente.

Com este método o AP tem a chance de recuperar uma estação que por algum motivo tornou-se incomunicável com a rede.

3.6. Transmissão em redes locais sem fio IEEE 802.11

3.6.1. O Padrão IEEE 802.11b

É o padrão principal ainda muito utilizado nas redes locais sem fio e que tem maior poder de penetração e maior disponibilidade de equipamentos e soluções de desempenho de redes.

As WLANs baseadas em radiofreqüência usam as faixas de freqüência ISM *(Industrial - Scientific - Medical)*, que assumem freqüências de 900MHz, 2.4GHz e 5GHz. Quanto maior a freqüência maior é a quantidade de informação que um dispositivo pode enviar num canal. As primeiras WLANs operavam na freqüência de 900MHz, atingindo uma taxa de 256Kbps. O padrão IEEE 802.11 aumentou a taxa de transmissão para 1Mbps, usando a técnica FHSS, e posteriormente para 2Mbps, usando a técnica DSSS, trabalhando na freqüência de 2.4GHz.

a) Técnicas de transmissão DSSS (Direct Sequence Spread Spectrum) e FHSS (Frequency Hopping Spread Spectrum

O Padrão IEEE 802.11b trata da tecnologia sem fio enfocando as redes locais sem fio (WLAN) que trabalham na faixa livre de 2.4 GHz com sua primeira e significativa evolução. Essas redes basicamente utilizam sinais de radiofreqüência para a transmissão de dados, através de duas técnicas conhecidas como **DSSS *(Direct Sequence Spread Spectrum)* e FHSS *(Frequency Hopping Spread Spectrum)*,** codificando dados e modulando sinais de modos diferentes para equilibrar velocidade, distância e capacidade de transmissão. A escolha da técnica DSSS ou FHSS dependerá de vários fatores relacionados com a aplicação dos usuários e o ambiente onde a rede operará.

A tecnologia do Espectro entendido (Spread Spectrum) é uma técnica de modulação que estende transmissões de dados através de bandas inteiras de frequência disponíveis num esquema pré-determinado. Este tipo de modulação torna o sinal menos vulnerável a presença de ruído, interferências e intrusos. Ela também permite muitos usuários compartilhando a faixa de frequência com um mínimo de interferência de outros usuários e de outros dispositivos que trabalhem com radio frequência, como, por exemplo, quando utilizamos fornos de microondas.

Outras formas de transmissão também podem ser usadas em redes locais sem fio, como a transmissão em infravermelho, por exemplo. Mas transmissões com infravermelho não atravessam certos tipos de materiais, apesar de poder enviar mais dados do que a transmissão com radiofreqüência. Com isso, a transmissão através de radiofreqüência acaba sendo o padrão adotado nas transmissões WLAN.

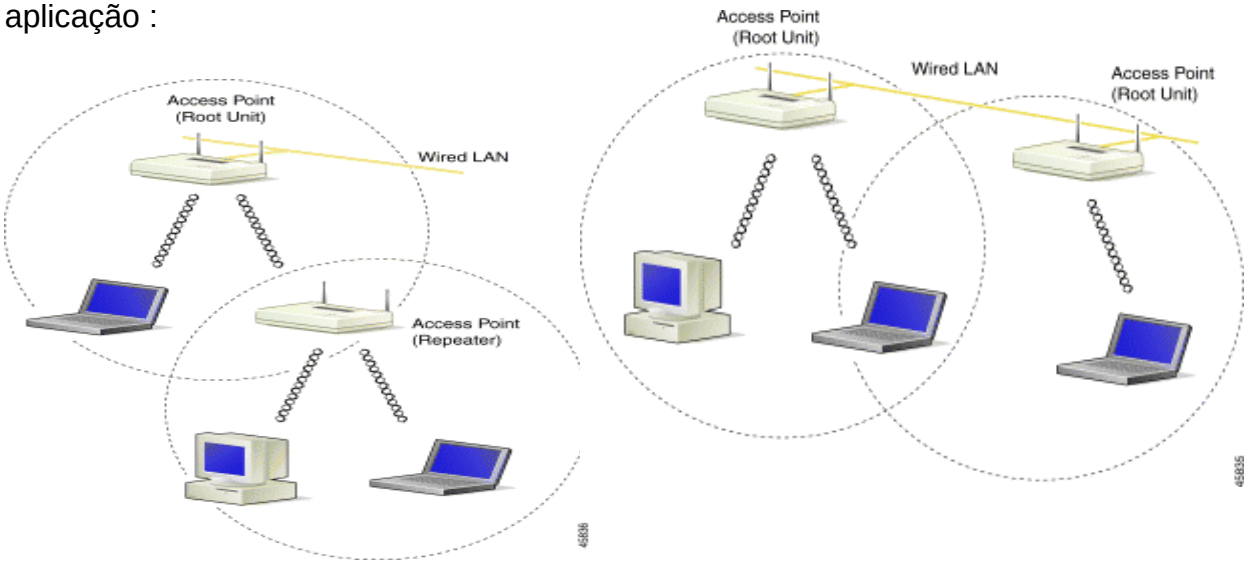
A seguir farei uma comparação entre as técnicas de transmissão :

FHSS => Com esta técnica, uma estação transmissora e outra receptora são sincronizadas para saltar de canal para canal numa sequência pseudo-aleatoria pré-determinada. Uma sequência de salto pré-arranjada é conhecida somente pelas estações transmissora e receptora. O IEEE 802.11 especificou 79 canais de 1Mhz cada um e 78 seqüências diferentes de saltos. Se um canal está sofrendo interferência ou muito ruidoso , os dados são simplesmente retransmitidos quando o transmissor saltar para um canal limpo. Por causa desta limitação, as redes que utilizam esta técnica, ficaram limitadas a taxas de transmissão de 1 a 2 Mbps.

DHSS => Nesta técnica , cada bit a ser transmitido e codificado com um padrão redundante chamado um CHIP , e os bits codificados são estendidos através da banda inteira de frequencia disponível . O código **Chipping** usado na transmissão é conhecido somente nas estações transmissoras e receptoras, tornando difícil para um intruso interceptar e decifrar os dados codificados no sistema sem fio, desta maneira. O padrão redundante também torna possível recuperar os dados sem retransmissão, isto se um u mais bits são danificados ou perdidos durante a transmissão. Por este motivo, está tecnologia atualmente é a mais usada nas redes que utilizam o padrão IEEE 802.11b.

A técnica DSSS distribui o sinal em cima de uma gama extensiva da faixa de freqüência e reorganiza os pacotes no receptor. A técnica FHSS envia segmentos curtos de dados que são transmitidos através de freqüências específicas, controlando o fluxo com o receptor, que negocia velocidades menores comparadas às velocidades oferecidas pela técnica DSSS, mas menos suscetíveis a interferências.

Na figura abaixo mostramos exemplo comparativo das técnicas de transmissão e seus modos de aplicação :



Ponto a ponto Compartilhada

Figura 12 – Comparação entre as técnicas de transmissão : ponto a ponto e compartilhada

O padrão 802.11 usa as duas técnicas, enquanto que outras tecnologias, como o *HomeRF* e *Bluetooth,* usam apenas a técnica FHSS, que é mais eficiente para ambientes que possuem outros tráficos de rádio, como áreas públicas abertas, por exemplo.

b) Projeto de canais e localização dos Pontos de acesso

Para a transmissão em radiofreqüência são usadas as técnicas DSSS e FHSS. Essas técnicas transmitem os quadros de dados enviando-os por vários canais disponíveis dentro de uma freqüência, ao invés de usar um único canal, possibilitando, dessa forma, a transmissão simultânea de vários quadros.

A banda de 2.4 Ghz contém uma faixa de 80 MHz do espectro de frequências. Cada canal DSSS tipicamente utiliza 14 canais de 22 MHz com 5 MHz de espaçamento (existe uma separação entre os canais adjacentes), para minimizar a interferência entre eles. Então, nos 80 MHz disponíveis podem acomodar de 1 a 3 canais equivalentes sem ser necessária a sobreposição entre eles. Isto permite que tenhamos até 3 Pontos de acesso, cada um programado com 1 dos 3 canais não interferentes para ser localizado na area de cobertura com sobreposição.

A figura abaixo mostra este tipo de arquitetura.

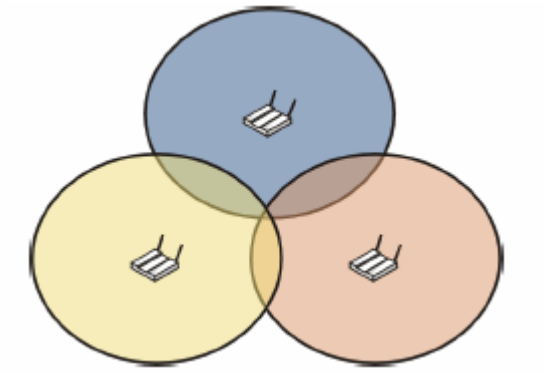


Figura 13 – Rede com 3 AP (Pontos de acesso) com cobertura sobreposta.

c) Largura de banda e Capacidade de escalabilidade

De acordo com a figura abaixo, podemos ver como a largura de banda agregada numa area de cobertura localizada pode ter escalabilidade numa variação de taxas de transmissão de 11 até 33 Mbps, para um serviço com uma maior densidade populacional de clientes wireless ou para um crescimento da largura de banda disponível para cada cliente na sua área de cobertura.

Mostramos na figura que um “Ponto de acesso” prove taxas de transmissão de até 11 Mbps de largura de banda , que é compartilhada por todos os clientes wireless na sua área de cobertura. Na outra figura, 2 ou mais “pontos de acesso” podem ser instalados próximos ao Ponto original. Cada um provém uma taxa adicional de 11 Mbps para a mesma área de cobertura, conseguindo uma largura de banda agregada de até 33 Mbps. Esta solução pode aumentar a largura de banda para uma população existente de clientes wireless, porque muito poucos clientes compartilham a taxa de 11 Mbps de cada Ponto de acesso, ou pode prover capacidade adicional para suportar uma maior densidade populacional.

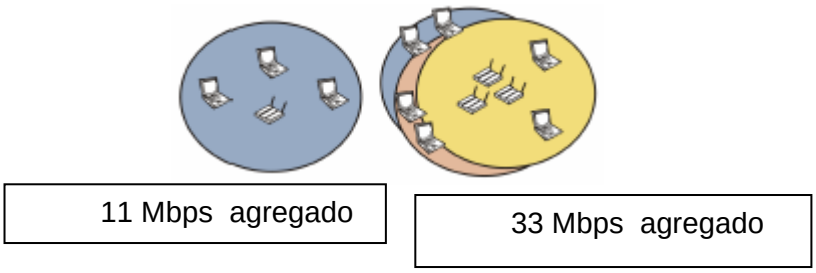


Figura 14 – Escala de largura de banda agregada de 11 a 33 Mbps numa área localizada pela colocação de 3 Pontos de acesso

Capacidade e largura de banda podem também ser escaláveis pela redução do tamanho das áreas de cobertura.

d) Seleção de canais

Dentro da faixa de frequência de 2.4 GHz , vimos que o padrão 802.11 define 14 canais de frequência central, cuja figura abaixo mostra o arranjo de canais , usando o canal 1 (2.412 GHz) , canal 6 (2.437 GHz) e canal 11 (2.462 GHz). Estes canais são geralmente usados para minimizar a complexidade de configuração e gerenciamento dos canais. Estes 3 canais, quando planejados corretamente, podem acomodar diversas instalações com muitos Pontos de acesso (AP) e clientes.

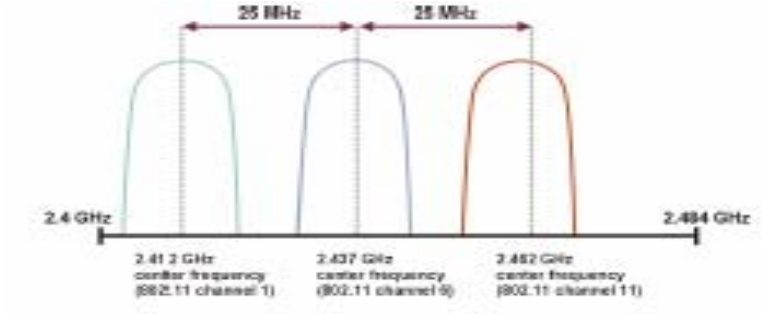


Figura 15 – Canais 802.11b sem sobreposição

A figura abaixo mostra um exemplo de um prédio com 3 andares servidos por 9 APs configurados com os canais 1, 6 e 11. Este modelo mostra a interferência minimizada entre APs localizados no mesmo andar, bem como os APs entre andares. Isto também elimina a contenção de largura de banda que ocorre quando 2 APs com cobertura sobreposta são configurados no mesmo canal.

Quando isto acontece, o mecanismo Ethernet Wireless 802.11 CSMA/CA (carrier sense multiple Access /collision avoidance) assegura que os usuários em ambas áreas de cobertura possam acessar a rede. Entretanto, ao invés de prover 2 canais de 11 Mbps separados e 1 de 22Mbps agregado, os 2 APs provem somente 1 canal de 11 Mbps.

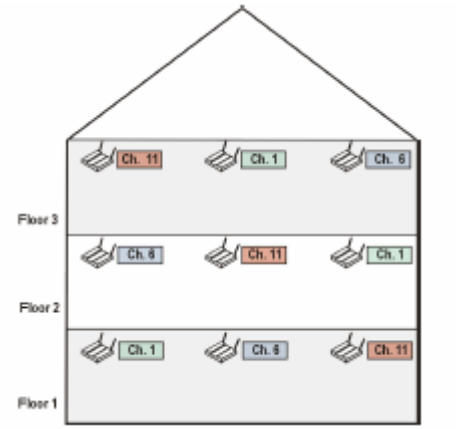


Figura 16 – topologia em frequência baseado nos canais 1, 6 e 11

e) Potência de Transmissão do AP

A potência de transmissão da maioria dos APs pode variar de 1 mW até níveis de 100 mW. Esta potência irá afetar diretamente a faixa efetiva do sinal rádio. Os transmissores de potência mais alta conseguem faixas mais distantes do sinal (área de cobertura mais abrangente). Estes transmissores são mais apropriados em muitas instalações empresariais que trabalhem com muito espaço disponível para cobertura.

Para os transmissores de menor potência são mais apropriados em ambientes menores, tais como: laboratórios de testes ou pequenos escritórios onde uma cobertura maior não seja necessária. A grande vantagem destes ambientes de mais baixa potência estaria no fato de que devido à faixa reduzida do AP, esta rede poderia prover um acesso agregado com taxas mais altas de processamento. Neste caso, uma quantidade maior de Aps poderia ser instalada para atender a uma área em particular, serviço que não poderia ser obtido com os sistemas de alta potência.

A area de cobertura servida por 3 Aps de 100 mW e provendo uma largura de banda agregada de 33 Mbps poderia então ser servida por mais Aps transmitindo em baixas potências e provendo maior largura de banda agregada. Esta aproximação deveria ser apropriada numa área com um alto número de clientes wireless. Entretanto, o crescimento de largura de banda deve ser pesado contra o custo de Aps adicionais.

3.7. Topologias para Redes Locais sem fio IEEE 802.11

O modelo do padrão 802.11b, que tem se tornado o padrão atual para as WLANs. Esse novo padrão especifica a técnica básica de transmissão na camada física usando a técnica DSSS, passando a taxa de transmissão real de 2Mbps para 5Mbps (com a possibilidade de se chegar a 11Mbps), tornando as redes locais sem fio mais atrativas.

Esse novo padrão define os protocolos que cada estação tem que observar de forma que cada uma dessas estações tenha acesso justo ao meio de transmissão. Para isso, um método de controle é implementado de maneira que seja assegurada a possibilidade de uma estação transmitir num dado tempo.

O padrão IEEE 802.11b também define o protocolo para dois tipos de topologias de redes: redes ***Ad Hoc*** e redes ***Cliente/Servidor*** com infra-estrutura.

a) uma rede **Ad Hoc** é um sistema onde as comunicações são estabelecidas entre várias estações de uma mesma área (célula), sem o uso de um ponto de acesso ou servidor e sem a necessidade de infra-estrutura .

b) uma rede **Cliente/Servidor** é sistema com infra-estrutura onde várias células fazem parte da arquitetura, e estações se comunicam com estações de outras células através de pontos de acesso usando um sistema de distribuição.

As Figuras 17 e 18 apresentam exemplos, respectivamente, dos modelos *Ad Hoc* e *infra-estrutura.*

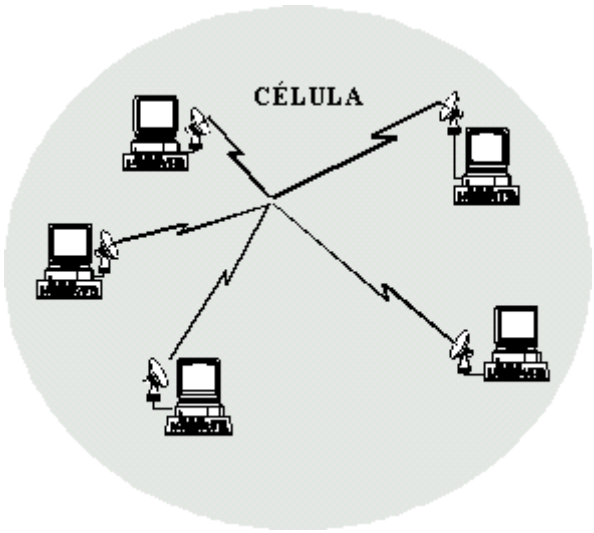


Figura 17 Rede local sem fio *Ad Hoc*

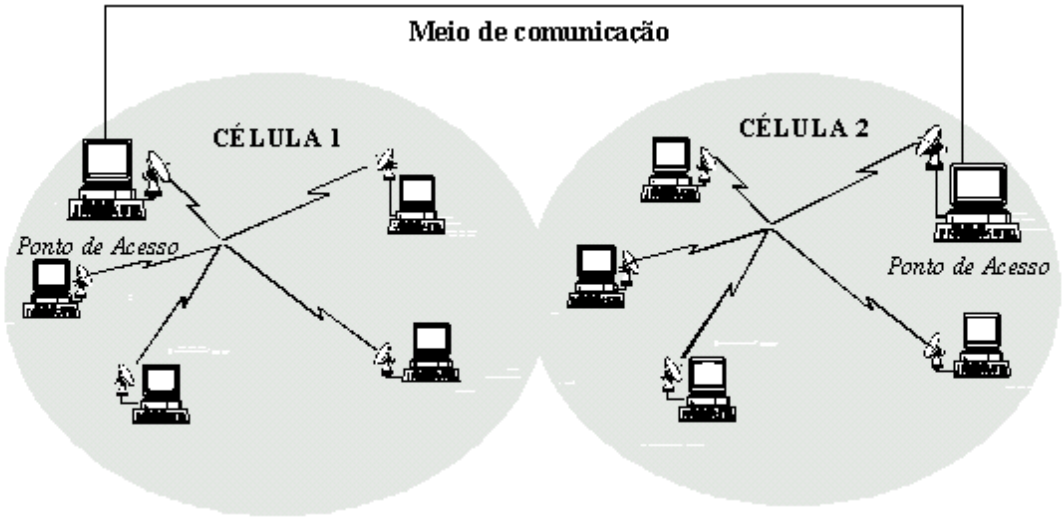


Figura 18 Rede local sem fio com infra-estrutura

3.8.
Características de implementação das redes locais sem fio

O propósito de uma rede sem fio não é a de substituir as redes com fio, e sim, estendê-las. Hoje podemos ter num escritório uma WLAN operando aproximadamente a 5Mbps com uma distância máxima entre as estações de 25 metros. Numa comparação com uma LAN padrão com fio (uma rede Ethernet com cobre, por exemplo), essa taxa pode chegar até 100Mbps e a distância entre as estações até 100 metros. Isso prova que as redes sem fio ainda não substituirão com total eficiência às redes com fio. Além disso, a taxa de 11 Mbps das WLANs ainda não é praticada, sendo atingida apenas de 4 a 6Mbps, por várias razões, entre elas:

a) o padrão 802.11b só é 85% eficiente no que diz respeito à camada física, devido à codificação, sincronização, e protocolos de transmissão acrescentarem cargas em cima do pacote de dados no nível de enlace;

b) a subcamada de controle de acesso ao meio (MAC) trabalha com contenção, tendo que encontrar o melhor momento para transmitir, o que diminui a eficiência.

c) Por outro lado, as redes sem fio permitem maior mobilidade e flexibilidade na transmissão de dados. Elas são fácies de montar, precisando apenas da colocação de cartões PCMCIA ou adaptadores PCI nas estações, e da instalação de pontos de acesso *(Access Points – APs)*, que servem como intermediários entre uma rede local com fio e uma WLAN.

Segurança é a principal preocupação a cerca das redes sem fio, pois dados irão trafegar pelo ar e poderão ser interceptados por pessoas com equipamentos apropriados. Para essa questão de segurança, o padrão IEEE 802.11 definiu um mecanismo de segurança opcional e privativo, que provoca uma sobrecarga *(overhead)* na rede, mas que oferece segurança às redes sem fio tanto quanto às com fio. Para impedir que usuários não autorizados acessem sua rede sem fio, um valor de identificação chamado de ESS-ID, é programado em cada AP para identificar a subrede de comunicação de dados e funciona como ponto de autenticação das estações da rede. Se uma estação não puder identificar esse valor, não poderá se comunicar com o AP respectivo. Outros fabricantes duplicam a tabela de controle de endereços MAC sobre o AP,

permitindo, dessa forma, que apenas estações com o endereço MAC reconhecido possam acessar a WLAN.

A existência de diversas tecnologias sem fio, como o *HomeRF*, *Bluetooth*, e HiperLAN2 (Europa), podem causar confusão para os consumidores e apresentar problemas de interoperabilidade, sem contar ainda que essas tecnologias podem apresentar interferências entre si, quando implantadas num mesmo ambiente, tendo em vista que esses padrões utilizam a mesma freqüência de 2.4GHz, e apesar de usarem técnicas de transmissão diferentes, pacotes aerotransportados podem facilmente colidir. Atualmente a probabilidade de isso acontecer é muito remota, mas de acordo com o crescimento dos usuários sem fio, essa probabilidade pode aumentar e esse problema pode se tornar uma realidade a ser considerada.

Embora ainda hajam muitas questões sendo analisadas a respeitos das redes sem fio, a comunidade científica tem investido de forma significativa no melhoramento dos padrões, tentando oferecer uma velocidade que possa chegar até 50Mbps, e um alcance maior de transmissão que possa se aproximar à distância do padrão Ethernet (100 metros), de maneira que são esperados produtos com essas tecnologias ainda para este ano.

a) Componentes para configuração de uma rede local sem fio

Os componentes essenciais de LANs sem fio são os mesmos ou similares aos das LANs convencionais (cabeadas). A mudança maior está na substituição de cartões de interface de redes Ethernet e Token Ring pelos seus similares nas LANs sem fio, e a ausência de conectores de cabo, e do próprio cabo, evidentemente.

Versatilidade é a palavra mais importante para definir este tipo de tecnologia, pois em algumas situações poderemos até substituir a alimentação local dos equipamentos, utilizando a mesma pela LAN onde eles estiverem conectados. Esta situação é bem proveitosa em alguns locais de difícil acesso onde não tenham uma rede elétrica bem constituída.

A seguir descrevemos os principais componentes de uma rede WLAN :

Cartões de interface de rede NICs (*Network Interface Cards*).

São idênticos aqueles utilizados numa rede local convencional. A grande diferença ocorre no fato que estes cartões em alguns casos terão uma antena acoplada (interna ou externa) para melhor o ganho do sinal e ajustar melhor seu desempenho. Podem ser externos (PCMCIA) ou internos (PCI)

Figura 19 e 20 – cartões PCI e PCMCIA , respectivamente

Antenas

Num sistema wireless LAN utilizamos diversos tipos diferentes de antenas: Omnidirecional (cobertura em todas as direções) ou diretivas (cobertura num local específico), que serão utilizadas conforme as características de cada aplicação, topologia, potência solicitada, etc.

Figura 21 – tipos de antenas WLAN

Pontos de acesso (AP) ou módulos de controle.

Estes equipamentos com uma porta Ethernet e um slot PCMCIA para placa de rede sem fio, funcionam como bridge (ponte) entre a rede Ethernet tradicional e a rede sem fio. Cada ponto de acesso pode atender até 200 estações, sendo recomendável um número médio de até 50 estações por AP (para manter um nível satisfatório de utilização da rede). Usando-se uma pequena antena opcional pode-se aumentar o alcance do sinal. Cria uma célula com raio de até 300 m de alcance em ambiente aberto e 60 m de alcance em ambiente semi-aberto.

Figura 22 – AP(ponto de acesso)

3.9. Evoluções Tecnológicas do padrão IEEE 802.11

A Tecnologia de conexões com redes sem fio está se configurando numa tendência dominante nos ambientes de rede. Como a demanda por aplicações está crescendo na direção de aplicações sem fio (principalmente voz e vídeo), a infra-estrutura deve responder para prover soluções adequadas a cada caso. Segurança, apoio de latência, aplicações sensíveis ao Jitter, potência de radiação, baterias de alta capacidade, são fatores que necessitam considerável atenção. O IEEE tem respondido com o estabelecimento de vários comitês para prover padrão de apoio para o desenvolvimento da tecnologia 802.11.

Verificou-se que diversos novos padrões estão sendo desenvolvidos com determinadas características a fim de suportar uma gama infinita de serviços. A seguir farei a descrição destes novos padrões.

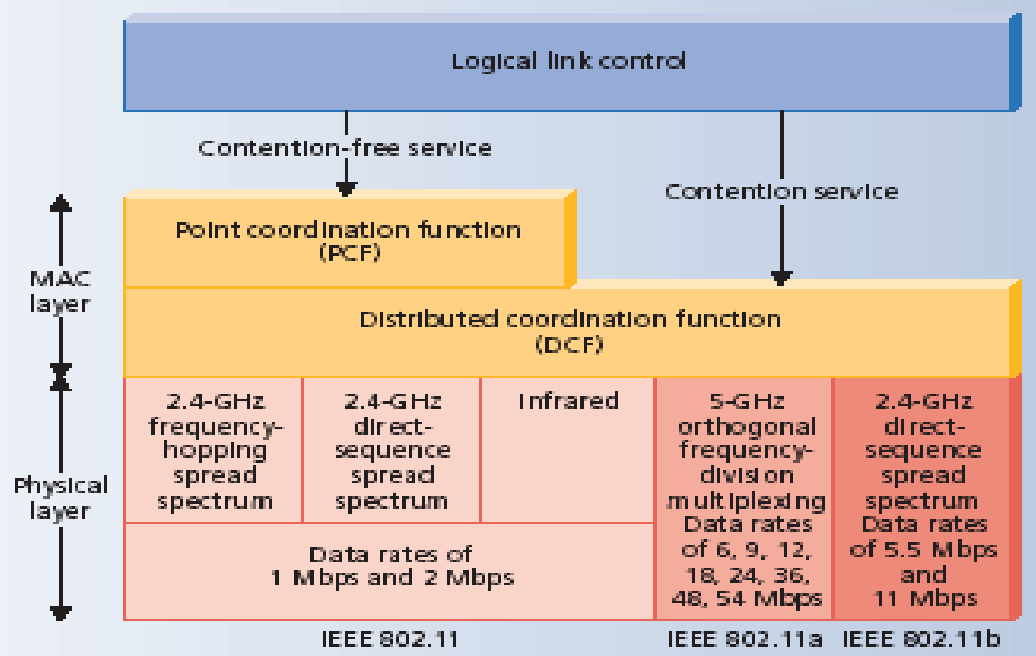


Figura 23 – Comparação entre os padrões IEEE.802.11

3.9.1. Novos padrões IEEE 802.11 desenvolvidos para melhorar o desempenho das redes

a) Padrão IEEE 802.11a

Este padrão foi recentemente ratificado, estabelecendo uma nova banda de frequência não licenciadas para redes sem fio e fez crescer a velocidade de transmissão para até 54 Mbps. Este crescimento foi possível com o uso de uma nova técnica de modulação baseada na divisão de frequência de modo ortogonal, sendo assim denominada OFDM (Orthogonal Frequency Division Modulation).

Este padrão utiliza uma banda de frequência que trabalham com uma infra-estrutura de informação nacional não licenciada (UNII). Aplicações em redes sem fio estão apenas começando a empregar esta banda, que trabalha divida em três segmentos não contínuos:

UNII–1 => operação na faixa de 5.2 Ghz => Seu uso está preferencialmente ligado às comunicações Indoor

UNII–2 => operação na faixa de 5.7 Ghz => Uso tanto indoor, quanto outdoor, dependendo da aplicação e emprego de antenas fixas ou móveis.

UNII–3 => trabalhando na faixa de 5.8 Ghz => Esta faixa é dedicada para sistemas de roteamento outdoor e seu uso é largamente empregado sem restrições de uma forma mais abrangente que as outras faixas.

Uma grande vantagem deste padrão foi conseguir uma significativa largura de banda, chegando a taxas teóricas de 54 Mbps. Por trabalhar numa faixa de freqüências mais desobstruída (5 Ghz) , foi conseguido um melhor desempenho no processamento. Cada banda UNII prove 4 canais sem sobreposição de um total de 12, através do espectro de freqüências alocado.

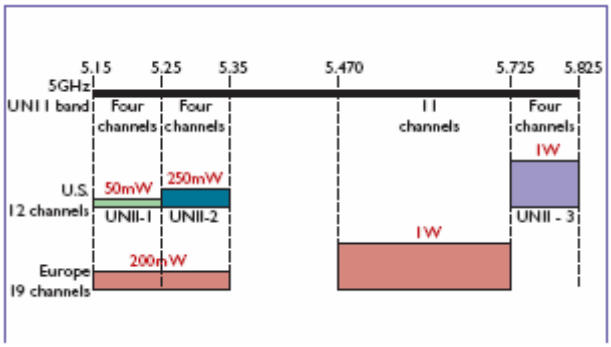


Figura 24 – Alocação de freqüência no modelo UNII

O grande diferencial nas melhoras de processamento na comunicação no padrão 802.11a, vem da aplicação da OFDM, para aplicações em comunicações sem fio. OFDM é uma tecnologia comprovada e provê uma alta eficiência espectral, proteção contra interferência de RF e redução das distorções por multipercurso, encontrados dentro do ambiente empregado.

O OFDM, às vezes é chamada de modulação multiportadora ou DMT (Discrete MultiTone) , onde se trabalham com múltiplas portadoras de baixa potência , por esta razão foi à técnica escolhida para implementação em diversos paises para instalação dos sistemas de TV Digital e também numa base principal largamente empregada nos sistemas de transmissão de dados que utilizam a tecnologia ADSL (Asymmetric Digital Subscriber Line).

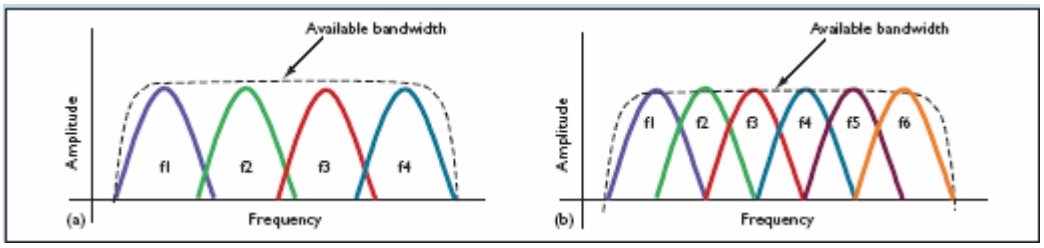


Figura 25 - Comparação entre as técnicas (a) FDM e (b) OFDM

Obs : a segunda tem uma melhor eficiência espectral pela ausência de banda de guarda.

b) Padrão IEEE 802.11e

O comitê que estuda este padrão está trabalhando para estabelecer características de qualidade de serviço (QoS) Ethernet de acordo com o padrão 802.11. Observamos que o esforço para aplicar todas as implementações do padrão 802.11 (b, a e g) tem sido muito freqüente.

Deste padrão se espera um enlace com da rede de QoS ethernet cabeada (802.1p) e o mundo sem fio. Ele não é tão diferente de que tem sido implementado em vários chaveamentos em forma de pilha no mercado (Chaveamento da camada de serviço 3 na camada 2) , mas o ambiente de compartilhamento de banda deve requerer uma baixa latência em técnicas de fila para assegurar interoperabilidade.

c) Padrão IEEE 802.11g

O padrão 802.11g é também conhecido como uma extensão do padrão 802.11b, procurando incrementar uma velocidade de dados na banda de frequências do ISM (2.4 Ghz). Já esta começando a substituir em grande parte as aplicações e equipamentos, o padrão IEEE 802.11b, devido a sua melhor segurança em relação à proteção do sistema contra invasões com mecanismos precisos de codificação para acesso a rede WPA e 802.11x e principalmente uma melhoria em relação à largura de banda, chegando em algumas aplicações a taxa de 54 Mbps.

Vários fabricantes estão estudando um modelo que possa ser compatível com a técnica OFDM, mas estão utilizando a codificação de convolução binárias dos pacotes (PBCC) como uma alternativa para ser uso com maior precisão nas redes que trabalham com DSSS.

d) Padrão IEEE 802.11h

Neste padrão este o crescimento da rede através de duas características muito importantes: um melhor controle efetivo para escolha das frequências que serão utilizadas na rede e um melhor sistema de Transmissão de potência para rede de acesso radio. A Melhor escolha está sendo feita para estudos de tempo de vida de baterias e níveis de potência EIRP de acordo com aqueles de determinados países.

e) Padrões IEEE 802.11i e IEEE 802.11x

Originalmente focado em sistemas que utilizam o padrão 802.11b, este modelo está sendo desenvolvido para protocolos que utilizam dados de segurança para uso nestes sistemas. O Padrão original inclui um protocolo equivalente de sistemas com fio (WEP) com duas chaves estruturadas com tamanho de 40 e 128 bits. O WEP é essencialmente uma técnica de encriptação que não incorpora nenhuma das técnicas de segurança mais conhecidas na indústria. Ele Usa um algoritmo de encriptação chamado RC4 e foi crackeado há algum tempo.

Por causa deste problema está sendo resolvido com o desenvolvimento do novo padrão 802.11x, que estabelece uma versão mais leve do protocolo de autenticação estendido (EAP) do padrão 802.11, que trabalha com chaves de criptografia associadas de 128 bits.

3.10.
Regulamentação das redes IEEE 802.11 no Brasil

Cada país tem sua regulamentação própria em relação a cada tipo de serviço que designa a aplicação de determinada tecnologia.

O organismo regulador de normas de telecomunicações no Brasil se chama ANATEL (Agência Nacional de Telecomunicações) que através da resolução nº 305, de 26 de Julho de 2002, regulamentou os equipamentos de radiocomunicação de radiação restrita, no qual o padrão de Redes Wireless LAN (802.11) estava enquadrado através da seção IX que designa os equipamentos que utilizam a tecnologia de espalhamento espectral.

A aplicação desta norma abrange as 3 faixas de frequência disponíveis para operação do sistema WLAN :

900 MHz (902.0 - 907.5 / 915.0 – 928.0 MHz) => 18.5 Mhz

2.4 GHz ou 2400 MHz (2400 – 2483.5 MHz) => 83.5 MHz

5.8 GHz ou 5800 MHz (5725 – 5850 MHz) => 125 Mhz

Para todas as faixas de aplicação os equipamentos podem operar tanto em ponto-ponto ou ponto-multiponto no serviço fixo ou serviço móvel.

Determinadas características descritas a seguir fazem a diferenciação do tipo de tecnologia usada.

a) Sistemas de salto em frequência (FHSS) => As frequências portadoras dos canais de salto devem estar separadas por no mínimo 25 KHz ou largura de faixa do canal de salto de 20 dB, sempre considerando o maior valor. Este sistema deverá seguir sempre uma sequência pseudo-aleatoria com cada transmissor usando igualmente cada uma das frequências. Na recepção, os equipamentos devem ter largura de faixa compatível com a largura do canal de salto do transmissor e mudar de frequências, sempre de forma sincronizada.

Para a largura de faixa de **900 MHz**, deveremos seguir os seguintes parâmetros:

- Potência máxima de pico na saída do transmissor não superior a 1W para sistemas com 50 canais de salto e 0.25 W para sistemas com menos de 50 canais de salto.

- Quando a largura do canal de salto de 20 dB for < 250 KHz usar no mínimo 50 frequências de salto com tempo médio de ocupação de qualquer frequência < 0.4 seg. num intervalo de 20 seg.

- Quando a largura do canal de salto de 20 dB for >= 250 KHz usar no mínimo 25 frequências de salto com tempo médio de ocupação de qualquer frequência =< 0.4 seg. num intervalo de 10 seg.

- A máxima largura de faixa ocupada do canal de salto a 20 dB deve ser no máximo de 500 KHz.

Para a largura de faixa de **2400 MHz e 5800 MHz**, deveremos seguir os seguintes parâmetros:

- Potência máxima de pico do transmissor = 1W;

- No mínimo 75 frequências de salto.

- Largura de faixa ocupada do canal de salto a 20 dB de no máximo 1 MHz com tempo médio de ocupação de frequências de 0.4 seg. num intervalo de 30 seg.

b) Sistemas de Sequência Direta (DSSS)

A largura de faixa a 6 dB deve ser no mínimo de 500 KHz com potência de pico máxima do transmissor de 1W.

O pico da densidade de potência em qualquer faixa de 3 KHz durante qualquer intervalo de transmissão contínua deve ser =< 8 dBm.

Em relação ao ganho de processamento de pelo menos 10 dB , determinado a partir da relação Sinal/ruído em dB , tanto com o código de espalhamento ligado, quanto desligado, sempre medido na saída do demodulador do receptor.

c) Sistemas Híbridos (DSSS e FHSS)

Este tipo de sistema irá fazer uma combinação das características do DSSS e do FHSS, que em relação ao ganho de processamento conseguirá no mínimo chegar a 17 dB. A operação FHSS e DSSS off ,terá um tempo médio de ocupação de =< 0.4 seg com período de tempo que será fator de FHSS x 0.4 , devendo obedecer aos critérios de densidade de potência citados no item anterior.

Quando o sistema utiliza antenas de transmissão com ganho direcional de 6 dBi, sua potência de pico máxima do transmissor será reduzida em relação à quantidade de dB que o ganho adicional da antena exceder a 6 dBi, exceto nas seguintes circunstâncias :

- Sistemas na faixa de 2400 MHz em aplicações ponto-ponto do serviço fixo, terão redução de potência de 1dB para cada 3 dB que exceder a 6 dBi.

- Sistemas na faixa de 5800 MHz em aplicações ponto-ponto do serviço fixo, não terão redução de potência. Somente a mesma ocorrerá em aplicações ponto-multiponto, omnidirecionais e múltiplos equipamentos numa mesma instalação transmitindo a mesma informação.

A potência de radiofreqüência produzida em qualquer largura de faixa de 100 KHz fora de operação , deverá estar no mínimo, 20 dB abaixo da potencia máxima produzida dentro da faixa de operação

3.11. Padrões de segurança em redes WLAN

Conforme a evolução desta tecnologia ao longo dos últimos anos, observou-se um grande aumento no número de redes sem fio utilizadas por usuários domésticos, instituições, universidades e empresas.

Esta grande popularidade e crescente uso das redes WLANs, acabaram trazendo uma maior mobilidade e praticidade para seus usuários, mas também gerou uma preocupação maior com a segurança destas redes. É por esta razão visando principalmente este fator primordial nos sistemas de propagação abertos, que vem fazendo com que os protocolos de segurança sejam criados, desenvolvidos e atualizados com uma velocidade cada vez maior e com certa constancia.

a) Protocolo WEP - primeiro protocolo de segurança

O primeiro protocolo de segurança adotado, que conferia no nível do enlace uma certa segurança para as redes sem fio semelhante a segurança das redes com fio foi o WEP (Wired Equivalent Privacy).

Este protocolo, muito usado ainda hoje, utiliza o algoritmo RC4 para criptografar os pacotes que serão trocados numa rede sem fio a fim de tentar garantir confidenciabilidade aos dados de cada usuário. Além disso, utiliza-se também a CRC-32 que é uma função detectora de erros que ao fazer o "checksum" de uma mensagem enviada gera um ICV (Integrity Check Value) que deve ser conferido pelo receptor da mensagem, no intuito de verificar se a mensagem recebida foi corrompida e / ou alterada no meio do caminho.

No entanto, após vários estudos e testes realizados com este protocolo, foram achadas algumas vulnerabilidades e falhas que fizeram com que o WEP perdesse quase toda a sua credibilidade.

No WEP, os dois parâmetros que servem de entrada para o algoritmo RC4 são a chave secreta k de 40 bits ou 104 bits e um vetor de inicialização de 24 bits. A partir desses dois parâmetros, o algoritmo gera uma seqüência criptografada RC4 (k,v)..

Porém, como no WEP a chave secreta k é a mesma utilizada por todos os usuários de uma mesma rede, devemos ter um vetor de inicialização diferente para cada pacote a fim de evitar a repetição de uma mesma seqüência RC4. Essa repetição de seqüência é extremamente indesejável pois dá margem a ataques bem sucedidos e conseqüente descoberta de pacotes por eventuais intrusos.

Além disso, há também uma forte recomendação para que seja feita a troca das chaves secretas periodicamente aumentando-se com isso a segurança da rede. Porém, essa troca quando é feita, é realizada manualmente de maneira pouco prática e por vezes inviável, quando se trata de redes com um número muito alto de usuários.

E ainda uma falha do WEP constatada e provada através de ataques bem sucedidos é a natureza de sua função detectora de erros. A CRC-32 é uma função linear e que não possui chave. Essas duas características tornam o protocolo suscetível a dois tipos de ataques prejudiciais e indesejáveis: é possível fazer uma modificação de mensagens que eventualmente tenham sido capturadas no meio do caminho sem que isso seja descoberto pelo receptor final devido à linearidade da função detectora de erros, e além disso, pelo fato da função não possuir uma chave, é também possível descobrir uma seqüência secreta RC4 e de posse desta ser autenticado na rede e introduzir mensagens clandestinas nesta.
Tendo-se em vista todas essas fraquezas do protocolo, algumas possíveis soluções foram propostas a fim de contornar e por que não acabar com tais fraquezas.

Uma das soluções que foi cogitada foi à substituição da CRC-32 por uma função de hash MD5 ou SHA-1 por exemplo. No entanto, esta seria uma solução muito cara além do que, tornaria a execução do protocolo pelos atuais processadores muito lenta.

Uma outra solução discutida foi descartar os primeiros 256 bytes da saída do gerador de números pseudo-aleatórios utilizado na criação dos vetores de inicialização. Isso seria feito devido à alta correlação dos primeiros bits exalados pelo RC4 com a chave. Porém, essa solução mostrou-se também muito cara e para muitas aplicações, inviável de ser implementada.

Então, no final do ano de 2001, o pessoal dos laboratórios RSA sugeriu que para contornar as fraquezas do WEP fosse usada uma função de hash mais leve, que usasse uma chave temporária para criar chaves diferentes para cada pacote.

Na proposta, mostra-se que essa função de hash mais simples seria composta de duas fases distintas : TK e TA.

Na primeira fase teríamos como entrada a chave temporária TK e o endereço do transmissor TA. Ter o endereço de quem está transmitindo como parâmetro é muito vantajoso para evitar que seqüências RC4 sejam repetidas. Imagine por exemplo uma estação que só se comunica com o AP. A informação trocada entre eles utiliza a mesma chave temporária TK e isso aumenta as chances da seqüência se repetir, bastaria que o mesmo vetor de inicialização fosse utilizado para isso ocorrer.
No entanto agora, juntamente com a chave temporária a estação utilizará seu endereço para gerar suas seqüências RC4 e da mesma forma, o AP utilizará seu próprio endereço para gerar suas seqüências. Dessa forma, evita-se a repetição de seqüências dificultando dessa forma alguns ataques.

Na segunda fase proposta, a entrada seria a saída da primeira fase, e o vetor de inicialização. A saída dessa segunda fase seria então o que chamaram de PPK, ou seja uma chave de 128 bits, diferente para cada pacote.
Apesar desta não ter sido a solução "final", embora a solução final não exista, pois sempre há atualizações para serem feitas, e novos conceitos para serem implementados, os conceitos de chave temporária e chave por pacote foram importantes e serviram de base para a criação de um protocolo intermediário; que chega a ser um "protocolo paliativo" criado especialmente para aqueles que usam redes sem fio e prezam tanto a segurança que não podem esperar pelo WPA2 que chegará ao mercado provavelmente no final de 2004.

b) WPA – 2ª Geração de protocolos de segurança

Também chamado de WEP2, ou TKIP (Temporal Key Integrity Protocol), essa primeira versão do WPA (Wi-Fi Protected Access) surgiu de um esforço conjunto de membros da Wi-Fi Aliança e de membros do IEEE, empenhados em aumentar o nível de segurança das redes sem fio ainda no ano de 2003, combatendo algumas das vulnerabilidades do WEP.

A partir desse esforço, pretende-se colocar no mercado brevemente produtos que utilizam WPA, que apesar de não ser um padrão IEEE 802.11 ainda, é baseado neste padrão e tem algumas características que fazem dele uma ótima opção para quem precisa de segurança rapidamente:

Pode-se utilizar o protocolo WPA numa rede híbrida que já tenha o protocolo WEP instalado.

Para migração ao protocolo WPA, somente é necessária a atualização do software

O Padrão WPA já foi desenvolvido para ser compatível com o padrão de IEEE 802.1i

Com a substituição do WEP pelo WPA, temos como vantagem melhorar a criptografia dos dados ao utilizar um protocolo de chave temporária (TKIP) que possibilita a criação de chaves por pacotes, além de possuir função detetora de erros chamada Michael, um vetor de inicialização de 48 bits, ao invés de 24 como no WEP e um mecanismo de distribuição de chaves.

Além disso, uma outra vantagem é a melhoria no processo de autenticação de usuários. Essa autenticação utiliza o 802.11x e o EAP (Extensible Authentication Protocol), que através de um servidor de autenticação central faz a autenticação de cada usuário antes deste ter acesso à rede.