

# 1 Introdução

Enquanto as redes cabeadas possuem hoje capacidade de transmissão de dados da ordem de gigabit/segundo, redes WLAN ainda operam no limite de 54 Mbps. Ainda assim, redes WLAN são cada vez mais adotadas. Isso se deve ao fato de redes WLAN apresentarem inúmeras vantagens em relação às redes cabeadas.

Redes WLAN permitem uma maior *mobilidade* ao usuário, uma vez que ele pode se conectar às redes e se locomover livremente por toda a área de alcance da estação-base, maior *flexibilidade*, uma vez que adicionar um novo usuário exige apenas a configuração do computador do usuário, sem necessidade de nenhuma nova estrutura de cabeamento, maior *facilidade*, já que uma rede wireless não exige a instalação de cabeamentos para interconectar prédios afastados, como em travessias de rios ou rodovias, maior *rapidez* porque o tempo que uma rede cabeada fica parada, devido a problemas que afetam o cabeamento é muito maior que em redes wireless, maior *praticidade*, já que a rede está pronta para uso imediatamente após a configuração do sistema e, por fim, maior *economia*, uma vez que o uso de WLAN para interligar dois prédios apresenta custo de instalação da ordem de quatro a cinco mil reais sem custos mensais para alguma operadora.

## 2 Redes Sem Fio 802.11

Antes do padrão 802.11 ser criado, as redes sem fio eram baseadas em tecnologia proprietária. Por isso, além da incompatibilidade entre os equipamentos, havia um alto custo para a implantação dessas redes e, conseqüentemente, elas estavam ao alcance apenas de grandes empresas ou instituições. Com este cenário de crescente desordem, sentiu-se a necessidade de criar um padrão.

### 2.1 Wi-Fi

O Wi-Fi uma marca registrada pertencente à WECA (Wireless Ethernet Compatibility Alliance). A WECA é uma organização sem fins lucrativos formada em 1999. Ela tem como missão certificar a interoperabilidade entre produtos que utilizam o padrão 802.11. Isto é feito através de diversos testes e os produtos que atendem ao padrão de interoperabilidade recebem o logotipo Wi-Fi.

## 3 Padrões de redes sem fio

### 3.1 O padrão 802.11

Para solucionar o problema da padronização anteriormente exposto, a Sociedade de Computação do IEEE (Institute of Electrical and Electronics Engineers) instaurou

um comitê para definir um padrão para a conectividade sem fio. Após sete anos de pesquisa e desenvolvimento, em 1997, aprovou-se o padrão IEEE 802.11.

O padrão 802.11 especifica os detalhes da camada física e da subcamada MAC da camada de enlace. Para a camada física foram definidos os mecanismos para efetuar a troca de dados entre os dispositivos. Para transferência de dados nas redes sem fio, o espectro de rádio frequência é dividido em faixas, que normalmente são intervalos reservados para um determinado tipo de serviço. Estes intervalos são definidos por agências reguladoras e/ou convenções internacionais. Uma faixa é, em geral, subdividida em frequências menores, conhecidas por canais.

Seguindo-se convenções internacionais, há pelo menos três segmentos de rádio frequência que podem ser usados sem a necessidade de obter licença da agência reguladora governamental. Esses segmentos foram reservados a uso industrial, científico e médico. Desta forma, as frequências disponíveis em cada uma das três faixas são:

- 902 - 928 MHz;
- 2,4 - 2,485 GHz (2,4 a 2,5 no Brasil);
- 5,150 - 5,725 GHz.

A frequência de 2,4 GHz é utilizada por uma vasta quantidade de equipamentos e serviços. Por exemplo: babás eletrônicas, forno microondas, telefones sem fio, etc. Isto é um problema, pois o risco de interferência se torna elevado. Em contrapartida a frequência de 5 GHz tem poucos concorrentes. Porém, seu alcance é menor em relação à frequência de 2.4 GHz.

Para a subcamada MAC foram determinadas outras características importantes de uma comunicação. Por exemplo: a verificação de erros.

Em termos organizacionais, o padrão 802.11 define dois modos distintos de operação: Ad-Hoc e infra-estrutura. No modo infra-estrutura existe um equipamento para concentrar todo tráfego da rede. Este equipamento é conhecido por AP (Access Point). Este modo possui alguns aspectos positivos. Por exemplo: a convergência das configurações.

No modo Ad-Hoc não existe um concentrador, ou seja, os equipamentos se conectam diretamente uns aos outros.

### **3.2 802.11a**

O surgimento de equipamentos de rede que obedecem ao padrão 802.11a ocorreu em meados de 1999. O padrão 802.11a tem as seguintes características:

- Utiliza três partes da banda de 5 GHz distribuindo algumas centenas de MHz não contíguos no geral.

- Tem 12 canais não sobrepostos (8 disponíveis para utilização interna e 4 para conexões ponto a ponto) que permitem que mais pontos de acesso cubram o mesmo local físico sem interferências de um sobre outro, com mais canais no caminho.
- Executa a uma taxa de transmissão nominal de 54 Mbps ou aproximadamente 25 Mbps real.
- Funciona somente em distâncias mais curtas, mas tem melhores protocolos que o 802.11b para distinguir a reflexão interna de sinais.

As principais vantagens do 802.11a originam-se dessas quatro diferenças: a banda de 5 GHz ainda não é utilizada por muitos outros dispositivos sem fio e os 8 canais internos distintos permitem um número substancialmente mais alto de usuários em largura de banda completa no mesmo espaço físico. Isso torna o 802.11a uma escolha provável para utilização de alta densidade em escritórios ou salas de servidor. Outros candidatos a equipamentos 802.11a incluem locais com grande quantidade de interferência da 2,4 GHz, como fábricas, hospitais e outras instituições utilizam dispositivos industriais, científicos ou médicos que ocupam a banda de 2,4 GHz.

Devido à utilização da banda de 5 GHz, o 802.11a não é compatível com as dezenas de milhões de dispositivos 802.11b atualmente em utilização. Devido há uma adoção dos grandes fabricantes pelo padrão 802.11b, o modelo 802.11a ficou apenas para equipamentos de entretenimento pessoal como uma possibilidade de emitir sinais digitais de alta definição entre dispositivos eletrônicos de consumo doméstico.

### 3.3 802.11b

O **802.11b** foi o primeiro padrão wireless usado em grande escala. Ele marcou a popularização da tecnologia. Naturalmente existiram vários padrões anteriores mas a maioria proprietários e incompatíveis entre si. O 802.11b permitiu que placas de diferentes fabricantes se tornassem compatíveis e os custos caíssem, graças ao aumento na demanda e à concorrência.

O 802.11b utiliza o espalhamento espectral por sequência direta para transmitir e receber dados em 11 Mbps. A taxa real de throughput (transferência de arquivo) é cerca de 7 Mbps para conexões UDP e de 4 a 5 para conexões TCP. Essa taxa de transmissão depende muito dos Hardwares utilizados e do ambiente onde a comunicação é feita.

O padrão 802.11b usa a técnica de modulação DSSS (Direct-Sequence Spread Spectrum), o qual determina a configuração ponto-multiponto, onde um ponto de acesso se comunica via antena omni-direcional (recebe sinais em todas as direções). As redes com padrão b tem um alcance de 30 metros e podem chegar a 90 metros a 1Mbit/s.

O 802.11b suporta cinco taxas de transmissão, iniciando na mais rápida e caindo para velocidades mais lentas se interferência ou um sinal fraco impedir que os dados

passem. As cinco velocidades são 11 Mbps, 5,5 Mbps, 2 Mbps, 1 Mbps e 512 Kbps (Kilobits por segundo).

Como o 802.11b utiliza a sequência direta, cada ponto de acesso dele pode ser configurado como um dos vários canais para evitar conflitos com outros dispositivos sem fio na mesma vizinhança. O 802.11b utiliza a banda de 2,4 GHz não licenciada, que varia entre 2,4000 GHz e 2,4835 GHz.

O padrão b até pouco tempo atrás era o mais popular de todos por ter maior alcance do sinal e por ser adotado por mais fabricantes de equipamentos. Porém o padrão 802.11g atualmente se enquadra como o mais popular.

### **3.4 802.11g**

Em 2002 e 2003, a WLAN criou um novo padrão chamado de 802.11g. Este sistema suporta uma largura de banda de 54 Mbps, similar ao protocolo 802.11a, e trabalha na frequência de 2.4 Ghz, similar ao protocolo 802.11b. É tido como o sucessor natural da versão 802.11b, uma vez que é compatível com este. Isso significa que um dispositivo que opera com 802.11g pode "conversar" com outro que trabalha com 802.11b sem qualquer problema, exceto pelo fato de que a taxa de transmissão de dados é, naturalmente, limitada ao máximo suportado pelo 802.11b. A técnica de transmissão utilizada nessa versão é híbrida. Utiliza-se modulação CCK para os cabeçalhos ou preâmbulo e OFDM para o dados, quando se opera entre dois dispositivos 802.11g, todavia, quando a comunicação é entre um dispositivo 802.11b e outro 802.11g, a comunicação é feita totalmente através da modulação CCK (havendo diminuição na taxa de transmissão).

Prós:

- Alta taxa de transmissão de dados.
- A faixa de frequência do sinal é compatível com a maioria e não é tão custosa.
- Compatibilidade com os dispositivos 802.11b.
- Usa autenticação WEP estática já aceitando outros tipos de autenticação como WPA (Wireless Protect Access) com criptografia dinâmica (método de criptografia TKIP e AES).

Contras:

- Custa mais que o 802.11b.
- Menor alcance da rede em relação ao 802.11b.

- Difícil de configurar, como Home Gateway devido à sua frequência de rádio e outros sinais que podem interferir na transmissão da rede sem fio.

### 3.5 802.11n

É o mais novo padrão IEEE na categoria Wi-Fi. Este sistema está sendo desenvolvido para oferecer melhor suporte em relação ao 802.11g. A característica marcante é pelo fato de que o mesmo utiliza a tecnologia MIMO\*, esta tecnologia faz uso de múltiplos sinais e antenas wireless em vez de apenas um. É esperado que as conexões suportem faixas de transmissão que vão além dos 100 Mbps.

Assim sendo, é possível, por exemplo, usar dois, três ou quatro emissores e receptores para o funcionamento da rede. Uma das configurações mais comuns neste caso é o uso de APs que utilizam três antenas (três vias de transmissão) e STAs com a mesma quantidade de receptores. Somando essa característica de combinação com o aperfeiçoamento de suas especificações, o padrão 802.11n é capaz de fazer transmissões de altíssimo nível.

O 802.11n promete ser o padrão wireless para distribuição de mídia, pois oferecerá taxas mais altas de transmissão (até 300 Mbps), maior eficiência na propagação do sinal (com uma área de cobertura de até 400 metros indoor) e ampla compatibilidade reversa com demais protocolos. O 802.11n atende tanto as necessidades de transmissão sem fio para o padrão HDTV, como de um ambiente altamente compartilhado, empresarial ou não.

Sua técnica de transmissão padrão é o OFDM, mas com determinadas alterações, devido ao uso do esquema MIMO, sendo, por isso, muitas vezes chamado de MIMO-OFDM. Alguns estudos apontam que sua área de cobertura pode passar de 400 metros.

\*O MIMO (Multiple Input, Multiple Output) permite que o 802.11n e tecnologias similares possam coordenar múltiplos sinais de rádio simultâneos. Graças ao uso do MIMO, os pontos de acesso 802.11n podem utilizar dois ou quatro fluxos simultâneos podendo dobrar ou até quadruplicar a taxa de transmissão.

O uso de diversos transmissores transmitindo simultaneamente na mesma faixa de frequência geraria interferência, podendo fazer com os sinais se cancelassem mutuamente. Para solucionar o problema a tecnologia tira proveito da reflexão do sinal. Pelo fato de serem transmitidos por antenas diferentes e ainda encontrarem obstáculos, os sinais fazem percursos diferentes até o receptor, fazendo com que não cheguem exatamente ao mesmo tempo. O receptor utiliza um conjunto de algoritmos sofisticados que fazem o tratamento dos sinais recebidos.

**Prós:**

- Altíssima taxa de transmissão.
- Faixa de transmissão que atende aos padrões atuais.
- Mais resistência à interferência de sinais provenientes de fontes externas.
- Grande alcance.

**Contras:**

- O padrão ainda não finalizado.
- Mais custoso que o 802.11g.
- O uso de múltiplos sinais poderia interferir em redes de protocolos anteriores.

**3.6 Outros padrões 802.11**

O padrão IEEE 802.11 teve (e terá) outras versões além das mencionadas anteriormente, que não se tornaram populares por diversos motivos. Um deles é o padrão *802.11d*, que é aplicado apenas em alguns países onde, por algum motivo, não é possível utilizar alguns dos outros padrões estabelecidos. Outro exemplo é o padrão *802.11e*, cujo foco principal é o QoS (*Quality of Service*) das transmissões, isto é, a qualidade do serviço. Isso torna esse padrão interessante para aplicações que são severamente prejudicadas por ruídos, tais como as comunicações por VOIP.

Há também o padrão *802.11f*, que trabalha com um esquema conhecido como *handoff*. Em poucas palavras, esse esquema faz com que um determinado dispositivo se desconecte de um AP (Access Point - ponto de acesso) de sinal fraco e se conecte em outro, de sinal mais forte, dentro da mesma rede. O problema é que alguns fatores podem fazer com que esse procedimento não ocorra da maneira devida, causando transtornos ao usuário. As especificações 802.11f (também conhecido como *Inter-Access Point Protocol*) fazem com que haja melhor interoperabilidade entre os APs para diminuir esses problemas.

Também merece destaque o padrão *802.11h*. Na verdade, este nada mais é do que uma versão do 802.11a que conta com recursos de alteração de frequência e controle do sinal devido ao fato da frequência de 5 GHz (usada pelo 802.11a) ser aplicada em diversos sistemas na Europa.

Há várias outras especificações, porém não iremos abordá-las neste texto.

## 4 Modulação

Para transmitir dados, analogicamente ou digitalmente, em um sistema com ou sem fio, necessita-se inserir os dados úteis em um sinal de rádio frequência. Esse sinal é chamado de onda-portadora, que é justamente o veículo de transporte de um dado, de um ponto à outro. A essa inserção, dá-se o nome de modulação e ela permite o transporte de informações seja embutida nos parâmetros de amplitude, fase ou frequência da onda portadora.

### 4.1 Modulação em Fase

Modulação em fase que dizer, basicamente, modificar a fase da onda portadora.

BPSK ( Binary Phase Shift Keying )

Se nós fizermos com que a onda portadora sofra um alteração de fase de 180 graus, estamos utilizando uma forma particular do PSK, onde, quando não há nenhuma transição, a portadora continua a ser transmitida com a mesma fase.

QPSK ( Quadrature Phase Shift Keying )

Se quisermos transmitir 4 tipos de símbolos possíveis, através de 2 bits, a portadora pode assumir 4 fases diferentes, a saber: 45, 135, 225, 315 graus

DQPSK ( Differential Quadrature Phase Shift Keying )

É uma variação do QPSK, onde, ao invés de modificarmos a fase, cada símbolo representa uma variação na fase, e não a fase em si.

### 4.2 Modulação em Amplitude

QAM ( Quadrature Amplitude Modulation )

Aqui as informações são inseridas nos parâmetros de amplitude e quadratura da onda portadora.

Para este caso, os símbolos são mapeados em um diagrama de fase e quadratura, onde cada símbolo apresenta uma distância específica da origem do diagrama que representa a sua amplitude, diferentemente da modulação PSK, na qual todos os símbolos estão a igual distância da origem. Isto significa que as informações são inseridas nos parâmetros de amplitude e quadratura da onda portadora.

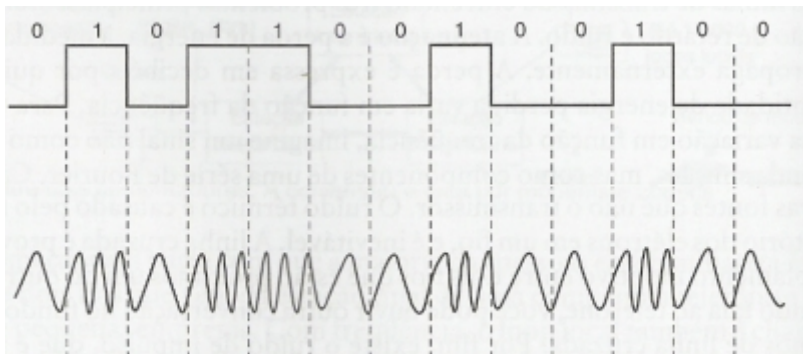
No caso do 16 QAM, temos 16 símbolos, sendo 4 em cada quadrante do diagrama, o que significa que cada símbolo representa 4 bits. Podemos ter também, por exemplo, o modo 64 QAM, onde temos 64 símbolos, cada um deles representando 6 bits.

### 4.3 Modulação em frequência

Modular em frequência quer dizer, basicamente, atribuir frequências diferentes, para a portadora, em função do bit que é transmitido.

FSK ( Frequency Shift Keying )

A modulação FSK ( Frequency Shift Keying ), faz justamente isso. Quando um bit zero é transmitido, a portadora assume o valor para o bit zero, oscilando em uma determinada frequência. Se a mudança de bit ocorre, a frequência da portadora muda.



Pode-se usar, também, quatro frequências de transmissões diferentes, com cada uma, coorespondendo a 2 bits. Esse método é chamado de 4FSK. Isso aumenta a taxa de bits transmitidos, porém aumenta também a banda de frequência de transmissão utilizada.

Essa modulação apresenta o inconveniente de ocupar uma banda de frequência bastante alta e de possibilitar baixas taxas de transmissão.

Gaussian Frequency Shift Keying

A modulação GFSK, é similar à modulação FSK diferenciando-se apenas no fato de que antes de se modular o sinal, ele passa por um filtro Gaussiano, onde se pretende “suavizar” seus contornos.

### 4.4 Espalhamento Espectral

Espalhamento espectral é uma forma de se aumentar a quantidade de bits utilizados para transmitir uma informação, de modo a espalhar o espectro de frequência do sinal. Fazendo-se isso, aumenta-se a banda de frequência na qual o sistema é transmitido. O código de espalhamento, é muito utilizado em transmissões digitais, uma vez que ao espalharem o sinal na frequência, proporcionam uma série de vantagens que melhoram a qualidade da transmissão.



## DSSS - ( Direct Sequency Spread Spectrum )

Basicamente essa técnica multiplica o bit original por uma sequência de 11 bits conhecidos como sequência de Barker (10110111000). Temos então que em um dos modos DSSS, um bit do sinal original, é representado por outros 11 bits no sinal modulado. Se o destinatário possui a sequência inicial, consegue decodificar o sinal.

Após espalhado, o sinal é modulado normalmente pela portadora. Geralmente utiliza-se dois esquemas de modulação para DSSS, a saber, DBPSK ( Differential Binary Phase Shift Keying ) que permite uma taxa de 1Mbps e DQPSK ( Differential Quadrature Phase Shift Keying ) que permite uma taxa de 2Mbps.

## FHSS (Frequency Hopping Spread Spectrum )

Como o próprio nome já diz, esse espalhamento baseia-se em saltos na frequência de transmissão do sinal, em um padrão pseudoaleatório, sendo que cada frequência é utilizada para para transmissão durante um curto intervalo de tempo, menor que 400ms, podendo ser ajustado, chamado de dwell time. Os saltos são determinados por um gerador de números pseudoaleatórios, que se encontra nas estações de transmissão e recepção, uma vez que o receptor tem de ter ciência da sequência utilizada para geração do sinal. Portanto, os sistemas precisam estar em sincronia com a mesma sequência pseudoaleatória de frequência. Isso é possível, utilizando-se as mesmas sementes para os geradores.

Com o FH, é possível que dois sistemas diferentes utilizem a mesma banda, uma vez que configurados com sistemas de hopping diferentes, não haverá interferência gerada entre os dois. Para isso, o FH utiliza-se de 79 canais de 1MHz de largura.

A modulação utilizada no FHSS é a GFSK sendo o 2GFSK para a taxa de 1Mbps e 4GFSK para uma taxa de 2Mbps.

Percebe-se também que adicionalmente, o FHSS provê segurança na transmissão, uma vez que precisa-se saber tanto da semente que gerou o código pseudoaleatório quanto do tempo de permanência em cada frequência, para se escutar, inadvertidamente, uma conversa entre duas estações FHSS.

## 4.5 CCK - ( Complementary Code Keying )

Esta técnica baseia-se em procurar em uma tabela previamente construída, (conjunto de 64 palavras de 8 bits) a sequência de espalhamento que corresponde à sequência de bits enviados. Essa técnica funciona somente em conjunto com DSSS e não funciona em conjunto a FHSS.

É utilizada a modulação DQPSK, já que faz o mapeamento de dois bits por símbolo, porém acontece uma diferença no código CCK, que no lugar de mapear um

código para bit como fazia o código de Barker, irá mapear cada palavra do código em 2 ou 6 bits, de acordo com a taxa utilizada, resultando em uma taxa de 4 bits por símbolo para uma taxa de 5,5Mbps e 8 bits por símbolo para 11Mbps.

#### **4.6 OFDM (Orthogonal Frequency Division Multiplex)**

OFDM utiliza várias portadoras ortogonais para transmitir um sinal. Antes de ser modulado, este sinal passa por várias etapas de processamento, a fim de melhorá-lo e performance e outros aspectos. Esses processamentos faz com que esse tipo de modulação ocupe uma banda de frequência bastante larga.

Primeiro, os dados são submetidos a sistemas de proteção de erro que são a inserção de um código corretor de erros como por exemplo o embaralhamento (scrambling), em que os bits de um mesmo byte são todos misturados.

Em seguida, os bits passam por um processo de entrelaçamento ou interleaving, no qual eles são reorganizados de modo que bits subseqüentes passam a ser separados no tempo. Desta forma, a informação torna-se mais imune a erros do tipo rajada (erros de burst), que atingem bits subseqüentes, pois após este processamento, estes erros passam a atingir bits pertencentes a diversos bytes diferentes, que estão muito distantes na informação original. Isto torna mais fácil a recuperação do sinal original no receptor.

No processo de modulação OFDM, diversas portadoras em frequências diferentes são utilizadas para modular o sinal digital, onde cada portadora transporta apenas alguns bits do sinal original após passar pelos processos de interleaving, embaralhamento e incluir códigos de correção de erro. Estas portadoras são ortogonais entre si, para evitar que haja interferência entre elas. Isso significa que o espaçamento entre as portadoras é igual ao inverso da duração de um símbolo.

Estas portadoras podem ser moduladas utilizando, por exemplo, QPSK, 16 QAM ou 64 QAM. Desta forma, cada portadora pode transportar uma taxa relativamente baixa de bits. Além disso, como cada parte do sinal é transportada por uma portadora em uma frequência diferente, isso permite também imunidade ao sinal quanto à interferência em frequências específicas, uma vez que somente uma pequena quantidade de bits serão atingidos, os quais estão bem distantes no sinal original.