Notas de Aula de Arquitetura e Organização de Computadores

Wi-Fi

Tecnologia Wi-Fi (IEEE 802.11)

Introdução

Por muito tempo, só foi possível interconectar computadores através de cabos. Atualmente, é possível evitar esses e outros problemas com o uso da tecnologia **Wi-Fi** (ou simplesmente WiFi), que permite a interconexão de computadores através de redes sem fio (*wireless*). A implementação desse tipo de rede está se tornando cada vez mais comum, não só nos ambientes domésticos e empresariais, mas também em locais públicos (bares, lanchonetes, shoppings, livrarias, aeroportos, etc) e em instituições acadêmicas.

O que é Wi-Fi

Wi-Fi é um conjunto de especificações para redes locais sem fio (WLAN - Wireless Local Area Network) baseada no padrão IEEE 802.11. O nome Wi-Fi é tido como uma abreviatura do termo inglês Wireless Fidelity, embora a Wi-Fi Alliance, entidade responsável principalmente pelo licenciamento de produtos baseados na tecnologia, nunca tenha afirmado tal conclusão.

Com a tecnologia Wi-Fi, é possível implementar redes que conectam computadores e outros dispositivos compatíveis (telefones celulares, consoles de videogame, impressoras, etc) que estejam próximos geograficamente.

A flexibilidade do Wi-Fi é tão grande, que se tornou viável a implementação de redes que fazem uso dessa tecnologia nos mais variados lugares, principalmente pelo fato das vantagens de não ser necessário intervenções físicas nas instalações prediais. Assim sendo, é comum encontrar redes Wi-Fi disponíveis em hotéis, aeroportos, rodoviárias, bares, restaurantes, shoppings, escolas, universidades, escritórios, hospitais, etc, que oferecem acesso à internet, muitas vezes de maneira gratuita. Para utilizar essas redes, basta ao usuário ter algum laptop, smartphone ou qualquer dispositivo compatível com Wi-Fi.

Um pouco da história do Wi-Fi

Algumas empresas, como 3Com,Nokia, Lucent Technologies (atualmente Alcatel-Lucent) e Symbol Technologies (adquirida pela Motorola), se uniram para criar um grupo para lidar com essa questão e, assim, nasceu em 1999 a Wireless Ethernet Compatibility Alliance (WECA), que passou a se chamar Wi-Fi Alliance, em 2003. Assim como acontece com outros consórcios de padronização de tecnologias, o número de empresas que se associam à Wi-Fi Alliance aumenta constantemente. No momento em que esse artigo era escrito, o grupo contava com a participação de mais de 300 empresas e entidades.

A WECA passou a trabalhar com as especificações IEEE 802.11 que, na verdade, não é muito diferente das especificações IEEE 802.3. Esta última é conhecida pelo nome *Ethernet* e simplesmente consiste na grande maioria das tradicionais redes cabeadas. Além disso, é possível ter redes que utilizam ambos os padrões.

Com um caminho a seguir, a WECA ainda precisava lidar com outra questão: um nome apropriado à tecnologia, que fosse de fácil pronúncia e que permitisse rápida associação à sua proposta, isto é, às redes sem fio. Para isso, a WECA contratou uma empresa especializada em marcas, a Interbrand, que acabou criando não só a denominação Wi-Fi (provavelmente com base no tal termo *Wileress Fidelity*), como também o logotipo da tecnologia. A idéia deu tão certo que a WECA decidiu por mudar o seu nome em 2003 para **Wi-Fi Alliance**, conforme já informado.

Funcionamento do Wi-Fi

Para que um produto receba um selo dessa marca, é necessário que ele seja avaliado e certificado pela Wi-Fi Alliance. É a forma de garantir ao usuário que todos os produtos com o selo Wi-Fi Certified seguem normas de funcionalidade garantindo a interoperabilidade entre si.

O padrão 802.11 estabelece normas para a criação e para o uso de redes sem fio. A transmissão dessa rede é feita por sinais de radiofrequência, que se propagam pelo ar e podem cobrir áreas na casa das centenas de metros. Como existem inúmeros serviços que podem utilizar sinais de rádio, é necessário que cada um opere de acordo com as exigências estabelecidas pelo governo de cada país. Essa é uma maneira de evitar problemas, especialmente interferências.

Estações (STAs) e Access Point (AP) Wi-Fi

Há, no entanto, alguns segmentos de frequência que podem ser usados sem necessidade de aprovação direta de entidades apropriadas de cada governo: as faixas ISM (Industrial, Scientific and Medical), que podem operar, entre outros, com os seguintes intervalos: 902 a 928 MHz; 2,4 a 2,485 GHz e 5,15 a 5,825 GHz (dependendo do país, esses limites podem sofrer variações). Como você verá a seguir, são justamente essas duas últimas faixas que o Wi-Fi utiliza, no entanto, tal característica pode variar conforme a versão do padrão 802.11.

Sendo assim, vamos conhecer as versões mais importantes do 802.11, mas antes, para facilitar a compreensão, é conveniente saber que, para uma rede desse tipo ser estabelecida, é necessário que os dispositivos (também chamados de STA - de *station*) se conectem a aparelhos que fornecem o acesso. Estes são genericamente denominados Access Point (AP). Quando um ou mais STAs se conectam a um AP, tem-se, portanto, uma rede, que é denominada Basic Service Set (BSS). Por questões de segurança e pela possibilidade de haver mais de um BBS em um determinado local (por exemplo, duas redes sem fio criadas por empresas diferentes em uma área de eventos), é importante que cada um receba uma identificação denominada Service Set Identifier (SSID), um conjunto de caracteres que, após definido, é inserido no cabeçalho de cada pacote de dados da rede. O SSID nada mais é do que o nome dado a cada rede sem fio.

802.11 (original)

A primeira versão do padrão **802.11** foi lançada em 1997, após 7 anos de estudos, aproximadamente. Com o surgimento de novas versões, a versão original passou a ser conhecida como 802.11-1997 ou, ainda, como 802.11 legacy. Por se tratar de uma tecnologia de transmissão por radiofrequência, o IEEE (Institute of Electrical and Electronic Engineers) determinou que o

padrão operasse no intervalo de frequências entre 2,4 GHz e 2,4835 GHz, uma das já citadas faixas ISM. Sua taxa de transmissão de dados é de 1 Mbps ou 2 Mbps e é possível usar as técnicas de transmissão Direct Sequence Spread Spectrum (DSSS) e Frequency Hopping Spread Spectrum (FHSS). Ambas as técnicas permitem transmissões utilizando vários canais dentro de uma frequência, O DSSS acaba sendo mais rápido, mas tem maiores chances de sofrer interferência, pois usa todos os canais ao mesmo tempo.

802.11b

Em 1999, foi lançada uma atualização sob nome **802.11b**. Como característica a versão é a pode estabelecer conexões em: 1 Mbps, 2 Mbps, 5,5 Mbps e 11 Mbps. O intervalo de frequências é o mesmo utilizado pelo 802.11 original (entre 2,4 GHz e 2,4835 GHz), mas a técnica de transmissão se limita ao DSSS, uma vez que o FHSS acaba não atendendo às normas estabelecidas pela Federal Communications Commission (FCC) quando opera em transmissões com taxas superiores a 2 Mbps. Para trabalhar de maneira efetiva com as velocidades de 5.5 Mbps e 11 Mbps, o 802.11b também utiliza uma técnica chamada Complementary Code Keying (CCK).

A cobertura do padrão 802.11b pode chegar, teoricamente, a 400 metros em ambientes abertos e pode atingir até 50 metros em lugares fechados (locais como escritórios e residências). Para manter a transmissão o mais funcional possível, o padrão 802.11b (e os padrões sucessores) pode fazer com que a taxa de transmissão de dados diminua até chegar ao seu limite (1 Mbps) à medida que uma estação fica mais longe do ponto de acesso.

802.11a

O padrão **802.11a** foi disponibilizado no final do ano de 1999, quase que na mesma época que a versão 802.11b. Sua principal característica é a possibilidade de operar com taxas de transmissão de dados nos seguintes valores: 6, 9, 12, 18, 24, 36, 48 e 54 Mbps. O alcance geográfico de sua transmissão é de cerca de 50 metros. No entanto, a sua frequência de operação é diferente do padrão 802.11 original: 5 GHz. Por um lado, o uso dessa frequência é conveniente por apresentar menos possibilidades de interferência, afinal, essa valor é pouco usado. Por outro, pode trazer determinados problemas, já que muitos países não possuem regulamento para essa frequência. Além disso, essa característica pode fazer com que haja dificuldades de comunicação com dispositivos que operam nos padrões 802.11 original e 802.11b.

Um detalhe importante, é que ao invés de utilizar DSSS ou FHSS, o padrão 802.11a faz uso de uma técnica conhecida como Orthogonal Frequency Division Multiplexing (OFDM). Nela, a informação a ser transmitida é dividida em vários pequenos conjuntos de dados que são transmitidos simultaneamente em diferentes frequências. Essas frequências são utilizadas de uma forma que impede que uma interfira na outra, fazendo com que a técnica OFDM funcione de maneira bastante satisfatória. Apesar de oferecer taxas de transmissão maiores, o padrão 802.11a não chegou a ser tão popular quanto o padrão 802.11b.

802.11g

O padrão **802.11g** foi disponibilizado em 2003 e é tido como o sucessor natural da versão 802.11b, uma vez que é totalmente 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 o fato de que a taxa de transmissão de dados é, naturalmente, limitava ao máximo suportado por este último.

O principal atrativo do padrão 802.11g é poder operar com taxas de transmissão de até 54 Mbps, assim como acontece com o padrão 802.11a. O 802.11g opera com frequências na faixa de 2,4 GHz e possui praticamente o mesmo poder de cobertura do seu antecessor, o padrão 802.11b. A técnica de transmissão utilizada nessa versão também é o OFDM, todavia, quando é feita comunicação com um dispositivo 802.11b, a técnica de transmissão passa a ser o DSSS.

Roteador wireless da 3Com: suporte aos padrões: 802.11b,g, e a conexões Ethernet

802.11n

O **802.11n** tem como principal característica o uso de um esquema chamado *Multiple-Input Multiple-Output* (MIMO), capaz de aumentar consideravelmente as taxas de transferência de dados através da combinação de várias vias de transmissão. 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 aprimoramento de suas especificações, o padrão 802.11n é capaz de fazer transmissões na faixa de 300 Mbps e, teoricamente, pode atingir taxas de até 600 Mbps.

Em relação à sua frequência, o padrão 802.11n pode trabalhar com as faixas de 2,4 GHz e 5 GHz, o que o torna compatível com os padrões anteriores, inclusive com o 802.11a (pelo menos, teoricamente). 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.

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 ou Quality of Service das transmissões. Isso torna esse padrão interessante para aplicações que são severamente prejudicadas por ruídos (interferências), tais como as comunicações por VoIP.

Há também o padrão **802.11f**, que trabalha com um esquema conhecido como *handoff*. Esse esquema faz com que um determinado dispositivo se desconecte de um AP (Access Point) 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 (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 (802.11a) ser aplicada em diversos sistemas na Europa.

Há vários outras especificações, mas a não ser por motivos específicos, é conveniente trabalhar com as versões mais populares, preferencialmente com a mais recente.

Segurança: WEP, WPA e WPA2

Se *você* tem uma rede Ethernet com dez pontos de acesso onde todos estão em uso, não será possível adicionar outro computador, a não ser que mais um cabo seja disponibilizado. Nas redes Wi-Fi, isso já não acontece, pois basta a qualquer dispositivo ter compatibilidade com a tecnologia para se conectar a rede. Mas, e se uma pessoa não autorizada conectar um computador à rede de maneira oculta para aproveitar todos os seus recursos, inclusive o acesso à internet? É

para evitar que esses e outros problemas que as redes sem fio devem contar com esquemas de segurança. Um deles é o Wired Equivalent Privacy (WEP).

O WEP existe desde o padrão 802.11 original e consiste em um mecanismo de autenticação que funciona, basicamente, de forma aberta ou restrita por uso de chaves. Na forma aberta, a rede aceita qualquer dispositivo que solicite conexão, portanto, há apenas uma autorização. Na forma restrita, é necessário que cada dispositivo solicitante forneça uma chave (combinação de caracteres, como uma senha) pré-estabelecida. Essa mesma chave é utilizada para cifrar os dados trafegados pela rede. O WEP pode trabalhar com chaves de 64 bits e de 128 bits. Naturalmente, esta última é mais segura. Há alguns equipamentos que permitem chaves de 256 bits, mas isso se deve a alterações implementadas por determinados fabricantes, portanto, o seu uso pode gerar incompatibilidade com dispositivos de outras marcas.

O uso do WEP, no entanto, não é recomendado por causa de suas potenciais falhas de segurança (embora seja melhor utilizá-lo do que deixar a rede sem proteção alguma). Acontece que o WEP utiliza vetores de inicialização que, com uso de algumas técnicas, fazem com que a chave seja facilmente quebrada. Uma rede WEP de 64 bits, por exemplo, tem 24 bits como vetor de inicialização. Os 40 bits restantes formam uma chave muito fácil de ser quebrada. Mesmo com o uso de uma combinação de 128 bits, é relativamente fácil quebrar todo o esquema de segurança.

Diante desse problema, a Wi-Fi Alliance aprovou e disponibilizou em 2003 outra solução: o Wired Protected Access (WPA). Tal como o WEP, o WPA também se baseia na autenticação e cifragem dos dados da rede, mas o faz de maneira muito mais segura e confiável. Sua base está em um protocolo chamado Temporal Key Integrity Protocol (TKIP), que ficou conhecido também como WEP2. Nele, uma chave de 128 bits é utilizada pelos dispositivos da rede e combinada com o MAC Address (um código hexadecimal existente em cada dispositivo de rede) de cada estação. Como cada MAC Address é diferente do outro, acaba-se tendo uma sequência específica para cada dispositivo. A chave é trocada periodicamente (ao contrário do WEP, que é fixo), e a sequência definida na configuração da rede (o *passphrase*, que pode ser entendido como uma espécie de senha) é usada, basicamente, para o estabelecimento da conexão. Assim sendo, é expressamente recomendável usar WPA, ao invés de WEP.

Apesar do WPA ser mais seguro que o WEP, a intenção da Wi-Fi Alliance foi a de trabalhar com um esquema de segurança ainda mais confiável. É aí que surge o **802.11i**, que ao invés de ser um padrão de redes sem fio, é um conjunto de especificações de segurança, sendo também conhecido como WPA2. Este utilizada um protocolo denominado Advanced Encryption Standard (AES), que é muito seguro e eficiente, mas tem a desvantagem de exigir bastante processamento. O uso é recomendável para quem deseja alto grau de segurança, mas pode prejudicar o desempenho de equipamentos de redes não tão sofisticados (muito utilizado no ambiente doméstico). Deve-se considerar que equipamentos antigos podem não ser compatíveis com o WPA2, portanto, sua utilização deve ser testada antes da implementação definitiva.

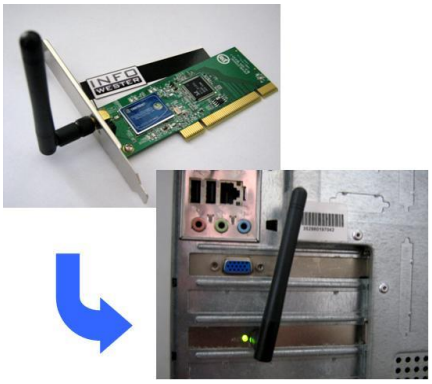
Configuração a encriptação em um roteador wireless 3Com - Note que é possível escolher o tempo de renovação da chave no modo WPA

Alguns equipamentos Wi-Fi

As redes Wi-Fi são tão práticas, que o seu uso não precisa ser feito apenas por PCs. Há até *smartphones* e consoles de videogames capazes de acessar tais redes. Assim, para se ter acesso as redes sem fio de casa de empresa, de escola ou de qualquer lugar com acesso público.

Uma placa Wi-Fi deve ser instalada na placa-mãe do computador. As placas mais comuns utilizam slots PCI ou, ainda, PCI Express. Após a instalação, é necessário ligar o computador e instalar os drivers do dispositivo, caso o sistema operacional não os tenha. Também há placas próprias para o uso em laptops (através de uma interface PC Card, por exemplo).

Por sua vez, os adaptadores USB Wi-Fi utilizam, como o próprio nome indica, qualquer porta USB presente no computador. A vantagem desse tipo de dispositivo está no fato de não ser necessário abrir o computador para instalá-lo e de poder removê-lo facilmente de uma máquina para acoplá-lo em outra. No entanto, como adaptadores USB geralmente são pequenos, sua antena é de tamanho reduzido, o que pode fazer com que o alcance seja menor que o de uma placa Wi-Fi PCI ou PCI Express. Mas, isso não é regra, e tal condição pode depender do fabricante e do modelo do dispositivo.



Placa Wi-Fi PCI posteriormente conectada em um PC

Nos ambientes domésticos e escritórios de porte pequeno, por ex., é comum encontrar 2 tipos de aparelhos: os que são chamados simplesmente de AP e os roteadores wireless. Ambos são dispositivos parecidos, mas o AP apenas propaga dados de uma rede wireless, é muitas vezes usado como uma extensão de uma rede baseada em fios.

O roteador wireless, por sua vez, é capaz de direcionar o tráfego da internet, isto é, de distribuir os dados da rede mundial de computadores entre todas as estações. Para que isso seja feito, geralmente liga-se o dispositivo de recepção da internet (por exemplo, um modem ADSL) no roteador, e este faz a função de distribuir o acesso às estações. Se, no entanto, o usuário possui um modem que também faz roteamento, precisa apenas de um AP, pois o próprio modem se encarregará do compartilhamento do acesso à internet.

Antes de comprar o seu equipamento wireless, seja para montar uma rede, seja para fazer com que um dispositivo acesse uma, é importante conhecer as características de cada aparelho para fazer a aquisição certa. Pode ser um desperdício adquirir uma placa Wi-Fi 802.11n e um AP 802.11g. Não é melhor comprar uma placa 802.11g ou logo um roteador 802.11n?

Via de regra, deve-se optar pelos equipamentos que possuem tecnologias mais recentes, mas também deve-se considerar a relação custo-benefício e os recursos oferecidos por cada dispositivo. É muito comum encontrar aparelhos 802.11g que alcançam taxas de até 108 Mbps, sendo que o limite do referido padrão é 54 Mbps. Qual o truque? Simplesmente o fabricante utilizou macetes que aumentam a taxa de transferência, mas se determinados dispositivos da rede não contarem com a mesma funcionalidade, de nada adianta a velocidade adicional.

Dicas de segurança

Ao chegar a este ponto do artigo, você certamente já conhece as vantagens de se ter uma rede Wi-Fi e, de igual forma, sabe que entre as suas desvantagens estão alguns problemas de

segurança. No entanto, medidas preventivas podem fazer com que você nunca enfrente transtornos desse tipo. Eis algumas dicas importantes:

- Habilite a encriptação de sua rede, preferencialmente com WPA ou, se possível, com WPA2. Em ambientes com muitas estações, pode-se utilizar WPA ou WPA2 com um servidor de autenticação RADIUS (Remote Authentication Dial In User Service), um esquema conhecido como WPA-RADIUS;
- Ao habilitar o WPA ou o WPA2, use uma *passphrase* - isto é, uma seqüência que servirá como uma espécie de senha - com pelo menos 20 caracteres. Note que em sua rede Wi-Fi esses itens podem estar com os nomes WPA Pre-Shared Key e WPA2 Pre-Shared Key ou **WPA-PSK** e **WPA2-PSK**;
- Altere o SSID, isto é, o nome da rede, para uma denominação de sua preferência. Se mantiver o nome estabelecido de fábrica, um invasor pode ter a impressão de que o dono da rede não se preocupa com os aspectos de segurança;
- Também é importante desativar o *broadcast* do SSID (um recurso que faz com uma determinada estação detecte a rede pelo seu nome automaticamente), pois isso impede que dispositivos externos enxerguem a rede e tentem utilizá-la (embora existam técnicas avançadas que conseguem enxergar redes ocultas). Ao se fazer isso, deve-se informar o SSID manualmente, se for adicionar uma estação à rede. Há um campo apropriado para isso no aplicativo que faz a conexão;
- Mude a senha padrão do roteador ou do AP. Muitos invasores conhecem as senhas aplicadas pelos fabricantes e, podem, portanto, acessar as propriedades de uma rede cuja senha não foi alterada;
- Sempre que possível, habilite as opções de firewall;
- Diminuir a intensidade do sinal, caso a rede seja a de servir pequena área. Para isso, alguns aparelhos permitem regular a emissão do sinal ou desativar uma antena extra;
- Por fim, leia o manual do aparelho e siga todas as orientações de segurança recomendadas pelo fabricante.

Essas e outras configurações são feitas através de uma interface em HTML fornecida pelo roteador ou por um dispositivo equivalente. Por exemplo, o roteador 3Com apresentado em uma foto acima, tem a sua interface acessada no endereço IP 168.192.1.1 (este é um IP local, não válido na internet). Ao digitar esse endereço no navegador, o roteador mostrará uma página em HTML com campos de *login* (obviamente, o dispositivo já tem que estar em funcionamento para isso). Quando o *login* é efetuado, o usuário pode então acessar e alterar as configurações do aparelho.

Interface em HTML do roteador Wireless - Nesta página é possível, entre outras coisas, configurar o SSID

Fontes de pesquisa:

FutureLooks, TechRadar, PCPlus, bit-tech, TechTudo, TecMundo. Livros Didáticos.