João Paulo Malheiro de Barcelos
jpmb@cbpf.br
Raphael Guimarães Gonçalves
raphagg@cbpf.br
Nilton Alves Jr.
naj@cbpf.br
http://mesonpi.cat.cbpf.br/naj

O Padrão 802.11

Resumo

Esta nota técnica apresenta as características do padrão "IEEE 802.11 – Wireless". Este padrão é um conceito revolucionário que permite maior mobilidade aos usuários, por dispensar o uso de cabos. Serão abordados os principais temas relevantes a esta tecnologia, como: equipamentos, segurança e conceitos pertencentes à camada física (FHSS e DSSS) e à camada de enlace.

Índice

1. Introdução

Ao longo dos últimos anos, ocorreu um grande aumento na utilização das redes sem fio em empresas, locais públicos e usuários doméstico. Esta crescente popularização das WLANs (W*ireless Local Area Network*) trouxe mobilidade e praticidade para seus usuários.

Uma rede sem fio consiste em dispositivos que se comunicam através de tecnologia de rádio freqüência, que possuem extrema facilidade de instalação e uso. A maioria dos dispositivos que fornecem conectividade a uma rede sem fio são *plug-n-play*, ou seja, basta conectá-los a rede cabeada para que os serviços sem fio sejam disponibilizados.

Conforme estudos realizados em julho de 2002, o número de redes wireless duplicou nos Estados Unidos em apenas um ano. Há estimativas que mostram que em 2005 existirão aproximadamente 150 milhões de usuários de redes sem fio. Estas estatísticas levam a crer que esta tecnologia tende a tomar uma fatia significativa do mercado de LANs.

2. WLAN, WWAN, WPAN

Existem várias categorias de redes que variam de acordo com número de clientes conectados, alcance e largura de banda.

2.1. WLAN – *Wireless Local Area Network*

Numa WLAN, um dispositivo chamado *Access Point* (AP), conecta todos os outros dispositivos à rede. APs estão se tornando comuns como acesso à rede em escritórios e centros de conferência. WLANs tem alcance de até 100 metros e atingem velocidades de até 54 Mbps e são baseadas em padrões como 802.11.

Figura 1: WPAN

2.2. WPAN – *Wireless Personal Area Network*

Redes pessoais que interconectam, por exemplo, um PC a um PDA (Palms e *handhelds*), sua impressora e sua câmera digital. É baseado no padrão *Bluetooth*, com alcance de até 50 metros, atingindo taxas de 1 Mbps. Os celulares mais modernos, assim como os PDAs, já estão vindo com *Bluetooth* instalados. No futuro, é prevista a interconexão de vários aparelhos domésticos ao computador.

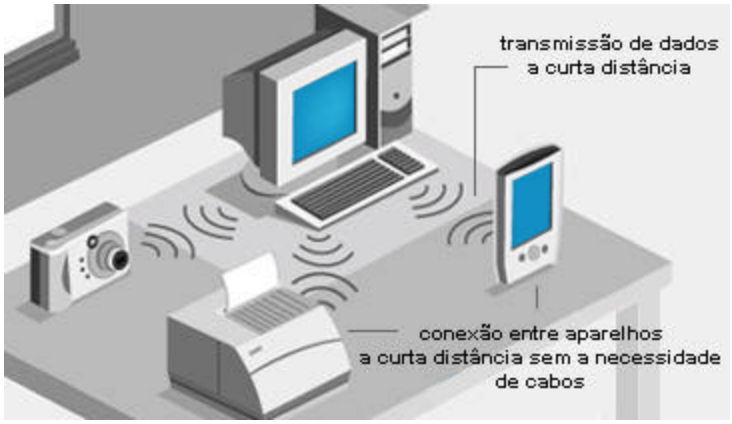

Figura 2: WPAN

2.3. WWAN – *Wireless Wide Area Network*

Transmissão de dados utilizando sinais de telefonia celular, que podem atingir 56kbps e distâncias de até 30km.

Figura 3: WWAN

3. Tecnologia *Spread Spectrum*

O *spread spectrum* é uma técnica de comunicação caracterizada por larga *bandwidth* (largura de banda) e baixa potência. Ele utiliza várias técnicas de modulação

numa WLAN e possui muitas vantagens sobre o outro método de comunicação, banda estreita, utilizada por grande parte das tecnologias que estamos acostumados, como TVs e rádios. Dentre estas esta a característica de ser semelhante a ruído, ou seja, difíceis de serem detectadas, e mais difíceis ainda de serem demoduladas e interceptadas sem equipamentos dedicados. Interferência e tentativas nocivas de *jamming* (travamento) também são menos suscetíveis a acontecer no *Spread Spectrum*.

Para aprender melhor esta técnica é importante explicarmos rapidamente como funciona a técnica de banda estreita.

3.1. Banda Estreita

Nesta tecnologia, é utilizada uma banda bem estreita, suficiente somente para a quantidade de dados que precisa ser transmitidos. É utilizada com alta potência, tendo assim um alcance muito grande. Porém, cada faixa de freqüência precisa ser liberada para apenas uma estação. Isso garante que não haverá interferência, já que esta estação é a única que faz *broadcasts* utilizando esta freqüência.

A tecnologia de *spread spectrum* veio para possibilitar a transmissão de dados a uma certa freqüência por várias pessoas, à baixa potência, evitando assim interferência. Os dados são transmitidos numa fatia muito mais larga do espectro de freqüência, como mostra a figura abaixo.

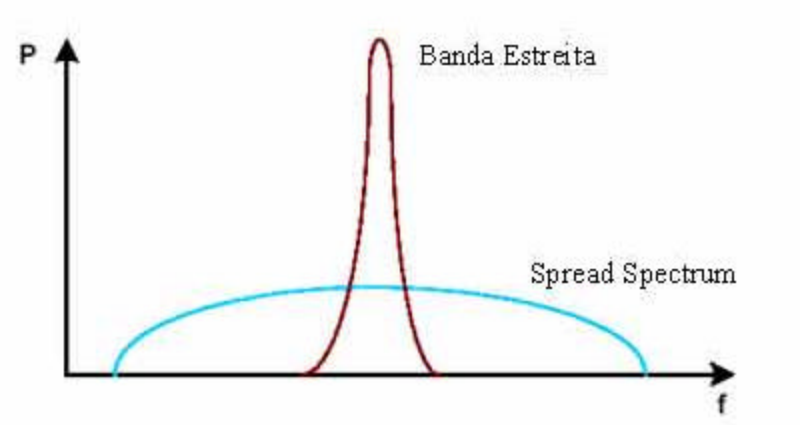

Figura 4: Comparação do *Spread Spectrum* com Banda Estreita

Uma grande vantagem do *Spread Spectrum* sobre a banda estreita é a proteção contra interferência. Normalmente as interferências ocorrem numa determinada faixa. Se a banda for muito estreita, uma interferência pode anular totalmente uma transmissão. Isso já não ocorre no *spread spectrum* já que há uma grande faixa de freqüências para serem utilizadas.

3.2. Spread Spectrum

Ela nos possibilita pegar os dados que vão ser transmitidos e espalhá-los numa faixa muito grande utilizando uma potência muito menor. Por exemplo, quando

normalmente ocorreria uma transmissão a 1 Mhz de 10 Watts, podemos usar 20 Mhz e transmitir a 100mW. Uma interferência que naquela faixa de 1 Mhz destruiria por completo a transmissão, só destruiria assim somente uma pequena parte. Por isso a taxa de erro é muito baixa.

Em redes *wireless*, utilizam-se 2 padrões de *Spread Spectrum*: FHSS e DSSS, que passaremos a descrevê-los a seguir:

Frequency Hopping Spread Spectrum (FHSS)

O primeiro tipo desenvolvido foi o FHSS. De maneira bem simplificada, se resume no processo de pular rapidamente de uma freqüência para outra. Os dados são quebrados em pedaços, e cada um é transmitido em uma freqüência diferente, numa seqüência pré-determinada, conhecida pelo receptor e pelo transmissor. O transmissor irá permanecer numa determinada freqüência durante um período de tempo (*dwell time*) e depois utilizará um curto tempo para pular para próxima freqüência (*hop time*).

No exemplo abaixo, temos uma seqüência de *hops* numa faixa de freqüência de 20Mhz. A seqüência utilizada é: 1. 2,450Ghz; 2. 2,454Ghz; 3. 2,458Ghz; 4. 2,462Ghz; 2,466Ghz; 5. 2,470Ghz. Vemos que após o fim da seqüência, ela é reiniciada.

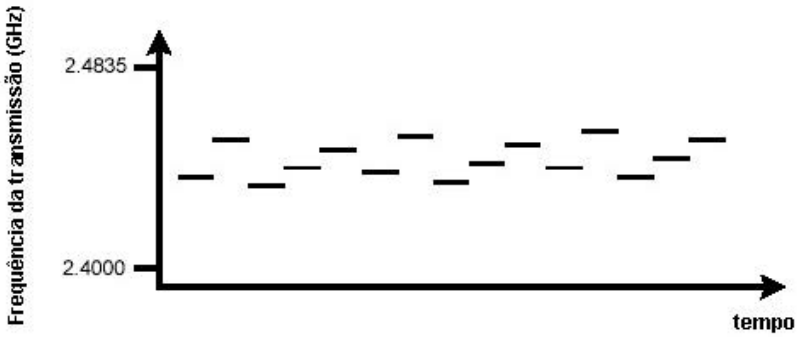

Figura 5: Processo de *Frequency Hopping*

Devido ao tempo perdido no *hop time*, o FHSS cria uma perda de transmissão de dados.Quanto maior for a relação entre o *dwell time* e o *hop time*, maior a transmissão de dados. Em sistemas como o *bluetooth*, em que o *dwell time* é de apenas 500-600us, um *hop time* de 100us gera uma grande perda de taxa de transmissão.

Apesar disso, o FHSS tem uma grande vantagem: a faixa de freqüência do padrão FHSS é maior que a do padrão DSSS, fazendo com que seja menos suscetível a interferência.

Padrão *Direct Sequence Spread Spectrum* (DSSS)

É atualmente o método mais utilizado em WLANs. O transmissor consegue espalhar os dados adicionando bits de dados redundantes chamados *chips* aos mesmos. O padrão DSSS adiciona pelo menos 10 *chips* para cada bit para proteger o receptor das perdas. Em outras palavras, o transmissor envia os dados colados a vários *chips* para fornecer redundância. O número fixo de *chips* é chamado de *chipping sequence* ou

Barker sequence. Normalmente muito poucos *chips* serão semelhantes aos outros chips trafegando na freqüência, gerando assim quase que nenhuma interferência com outros usuários DSSS.

Em uma WLAN DSSS, 11 canais podem ser utilizados. Os canais são faixas de freqüências em que os dados são transmitidos. Cada canal tem uma largura de 22Mhz, e todos juntos compõem a largura de banda total da faixa de freqüência de 2,4GHz utilizada em redes *wireless*. Quando existem 2 canais se sobrepondo, é necessária a distância de 5 faixas de freqüência de 22MHz. Assim, o canal 1 só poderia se sobrepor com o canal 6, o 2 com o canal 7 e assim por diante.

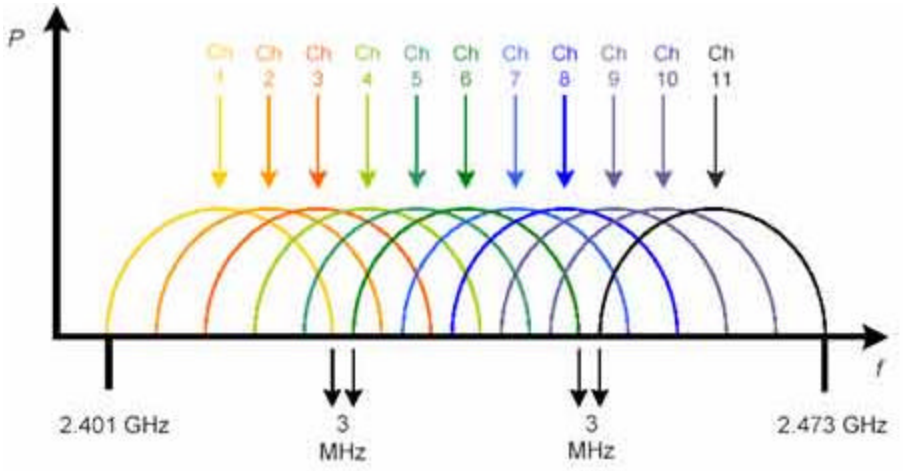

Figura 6: Canais do padrão DSSS

Os sistemas DSSS são hoje em dia muito mais utilizados do que os sistemas FHSS já que eles fornecem uma taxa de transferência muito superior, chegando a até 54Mbps, enquanto o FHSS não ultrapassa 2 Mbps. Por isso, os padrões lançados recentemente utilizam somente o DSSS.

3.3. FHSS versus DSSS

O FHSS fornece uma maior precisão contra interferência, ao custo de velocidade de transmissão. Além disso, os custos de uma rede DSSS são menores do que uma rede FHSS, parcialmente devido a maior presença de produtos DSSS no mercado atualmente.

É tudo uma questão de necessidades. Se interferência não for problema, o uso do sistema DSSS é melhor devido ao preço e velocidade, mas em áreas em que a interferência impossibilita o uso do DSSS, o FHSS é a única solução.

4. O Padrão 802.11

O padrão 802.11 foi criado em 1997 por um grupo de trabalho do IEEE para definir o conceito de WLAN (*Wireless* Local *Area Network*). No momento, há 4

especificações: 802.11; 802.11b; 802.11a; 802.11g e está previsto para o fim do ano o novo padrão 802.11i.

O padrão 802.11, como os outros padrões 802.x, cobre as especificações técnicas das camadas MAC e PHY, de acordo com a figura abaixo:

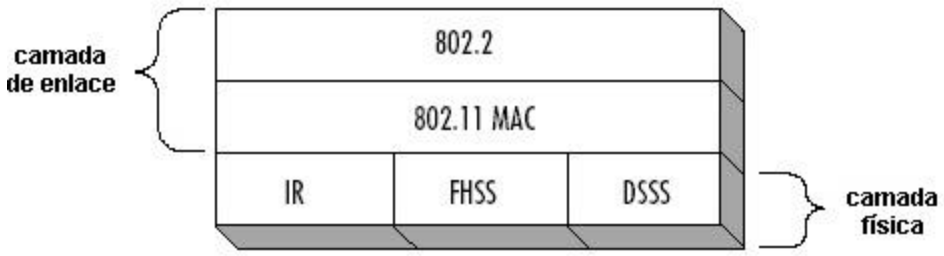

Figura 7: Camadas do 802.11

As três possíveis opções de camada 1 são FHSS e DSSS (ambas utilizando a tecnologia de *Spread Spectrum*) e o Infra Vermelho. Devido ao fato das limitações de linha de visão e distância, o Infra Vermelho foi pouco desenvolvido. Os padrões FHSS e DSSS operam a freqüência de 2,4Mhz, e a grande maioria das implementações utiliza o DSSS. Todas as três trabalham com taxas de 1 e 2 Mbps.

4.1. Topologias 802.11

Uma topologia 802.11 consiste de *sets*, dispositivos que permitem mobilidade transparente para os clientes. Existem três topologias:

Basic Service Set (BSS) – É a topologia mais básica. Consiste em um AP conectado a rede cabeada e um conjunto de clientes. O *access point* fornece a conexão ao mundo, assim como a interconexão entre os clientes da WLAN.

Extended Service Set (ESS) – Consiste de vários BSSs se sobrepondo, conectados uns aos outros por uma rede cabeada, geralmente *ethernet*. Os clientes podem se mover entre os vários APs, através da técnica de *roaming*. Isso permite uma cobertura transparente através da topologia ESS.

Independent Service Set (ISS) – Também conhecidas como topologias Ad-Hoc, são muito similares a redes internas *peer*-2-*peer*, onde um computador é responsável por ser o servidor. Todos os clientes se comunicam entre si, sem a necessidade de um *Access Point*.

A grande vantagem desse padrão é a capacidade de mobilidade sem se preocupar com a mudança de redes ou APs. Para a rede cabeada, tudo é totalmente transparente, não estando ciente da mobilidade dos clientes e nem do fato de estar ligado a uma rede sem fio. A rede cabeada vê os endereços MAC como se fossem diretamente conectados através de um *hub*.

4.2. Serviços 802.11

A arquitetura 802.11 se baseia em nove tipos de serviço, sendo 4 nos serviços de estação e o restante são serviços de distribuição. Os quatro serviços de estação

(*authentication, de-authentication, data delivery, e privacy*) fornecem funcionalidade equivalente à *ethernet*.

Authentication e de-authentication - O primeiro passo para se conectar a um sistema WLAN é a autenticação. Este é o processo em que o cliente tem sua identidade avaliada pela rede a que ele deseja se conectar. O AP basicamente tenta checar se o cliente realmente é quem ele diz que é.

O cliente primeiro manda uma requisição de autenticação para o AP, que em seguida responde a requisição, habilitando ou negando o acesso.

O processo de de-autenticação é usado para deletar uma identidade já existente. A partir do momento em que o processo de de-autenticação for iniciado, o cliente não pode mais acessar o AP.

Delivery - Como nas redes cabeadas, o 802.11 fornece um método de garantia que os dados serão transferidos de um MAC para o outro.

Privacy - Usado para proteger os dados quando atravessam a WLAN. Fornece um nível de segurança semelhante às redes cabeadas, logo o nome *Wire Equivalent Privacy* – WEP. (privacidade equivalente a redes cabeadas).

Entre as subcamadas LLC e MAC, cinco serviços de distribuição decidem para onde os quadros irão. Os cinco são *association, re-association, disassociation, integration,* e *distribution*.

Association – Uma vez autenticado, o cliente então se associa ao AP. O estado de associado é aquele em que o cliente está liberado para trafegar dados através do AP. O processo de associação é semelhante ao de autenticação, em que o cliente primeiro manda uma requisição para depois o AP responder positivamente ou negativamente. Um cliente pode estar autenticado em mais de um AP, mas só pode estar associado a um.

Re-association – Por questões de energia ou *roaming*, um cliente pode não ficar associado continuamente a um AP. Para isso é usado o serviço de re-associação, para que não sejam perdidas as informações de conexão. Isso pode servir, por exemplo, para que um AP entre em contato com outro, de onde o cliente esta saindo, para saber se existem alguns pacotes para serem transmitidos.

Disassociation – Usado para destruir a associação entre um cliente e seu AP. Utilizando quando o AP está sendo desligado ou quando o cliente está fazendo um *roaming* para fora deste BSS.

Distribuition – usado para que os APs saibam determinar para onde mandar o quadro, seja para um outro AP, seja para um cliente ou para rede cabeada.

4.3. CSMA/CA

O mecanismo de acesso básico para o 802.11 é o CSMA/CA, com *backoff* exponencial binário. Muito semelhante ao CSMA/CD, utilizado em redes *ethernet*, mas com algumas modificações.

Como a radio freqüência é um meio compartilhado, as redes *wireless* têm que lidar com a possibilidade de colisões tanto quanto uma rede cabeada tradicional. Contudo, não há como determinar se houve uma colisão. Por isso é utilizado um protocolo que evita colisões, em vez de detectá-las.

A diferença entre esse protocolo e o utilizado por redes *ethernet* (CSMA/CD) é o uso de ACKs. Uma estação manda o pacote, e a estação receptora envia um ACK confirmando a recepção do pacote. Se o ACK não for recebido, a estação que enviou já sabe que houve uma colisão e retransmite o pacote.

Além disso, o CSMA/CA toma muito cuidado para que não haja colisões. Antes de transmitir um pacote, a estação fica ouvindo para tentar detectar se há alguém falando. Se o meio estiver ocupado, o protocolo gera um tempo randômico de segundos para esperar até ouvir se o meio já está livre.

Este processo gera um *overhead* muito grande, de aproximadamente 50% em WLANs. Adicionado a protocolos como RTS/CTS, a largura de banda de uma rede 802.11b de 11Mbps opera em torno de 5Mbps. O CSMA/CD gera um *overhead* em torno de 30%, que atinge 70% quando o meio estiver congestionado. O CSMA/CA mantém os 50%, independente do nível de utilização.

RTS/CTS

Para minimizar o risco de uma estação transmitir ao mesmo tempo que outra, foram desenvolvidas duas funções, DCF e PCF, que empregam um mecanismo conhecido como Request To Send / Clear To Send (RTS/CTS).

Distributed Coordination Protocol (DCF) é usado por qualquer topologia para determinar quando uma estação pode transmitir em tempos de congestionamento. Se um canal estiver sendo usado, então um período de espera é inicializado. *Point Coordination Protocol* (PCF) utiliza um ponto centralizado na rede (como um AP) para agir como coordenador, avisando a todas as estações quando elas podem e quando não podem transmitir.

Quando uma estação deseja enviar dados para o AP, ela envia um RTS dizendo que deseja utilizar o meio por um determinado tempo (calculado a partir do tamanho do pacote que deseja transmitir). O AP iria então devolver um CTS dizendo que estaria livre e que não aceitaria nenhum outro tráfego de dados até que a transmissão estivesse terminada. As outras estações ouviriam essa conversa, e saberiam o tempo necessário de espera para que o AP começasse a receber dados de novo.

4.4. Economia de Energia 802.11

Devido à vantagem da WLAN ser a mobilidade, a questão de economia de energia passa a ser de primeira importância. Foi então incluído um serviço de economia de energia para permitir que clientes entrem em modo de espera (*sleep*) para economizar energia sem perder conectividade.

Clientes *wireless* funcionam em dois modos de energia definidos pelo padrão 802.11: O modo ativo, ou *Continuos Aware Mode* (CAM) e o modo de economia, *Power Save Polling* (PSP).

Continuous Aware Mode (CAM)

Este modo utiliza potência total, não entra em modo de *sleep*, e se mantém em constante comunicação com o AP. Qualquer cliente que fique permanentemente conectado a rede elétrica deve utilizar o CAM. Nessas circunstâncias, não há necessidade de economia de energia.

Power *Save* Polling (PSP)

Este modo permite que o cliente entre em modo de *sleep*. Quando isso acontece, o cliente se desliga completamente por um curto período de tempo, possivelmente alguma fração de segundos. Esse tempo é suficiente para economizar uma quantia significante de energia no cliente. Quando funcionam em PSP, os clientes se comportam de maneira diferente do que normalmente fariam. O processo de operação PSP ocorre varias vezes por segundo, e adiciona um considerável *overhead*, já que várias mensagens são trocadas entre AP e *host*.

Para entrar em PSP, a estação primeiro manda um quadro para o AP para avisar que vai entrar no modo de *sleep*. O AP então grava em sua memória as estações que estão dormindo. O tráfego para estas estações continua chegando, e esses pacotes são guardados num *buffer* para que possam ser enviados quando o cliente sai do *sleep*.

Todas as estações sabem quando o AP vai enviar o pacote *beacon* (as estações e o AP são sincronizados), e a estação acorda todas vez que sabe que vai recebê-lo. Todo *beacon* contém um *Traffic Indication Map* (TIM), que lista todos os clientes em modo de *sleep* que possuem pacotes dentro do *buffer*. Se a estação estiver listada no TIM, ela envia um quadro para o AP notificando que acordou e que pode receber os pacotes. Após a recepção desses pacotes, ela envia outro quadro avisando ao AP que vai voltar a dormir.

4.5. *Roaming* 802.11

Um grande benefício de uma WLAN é a possibilidade de se mover entre células sem a necessidade de modificação dos seus serviços de rede. *Roaming* entre os APs de sua topologia ESS é uma porção essencial do padrão 802.11. Baseia-se na capacidade de um cliente determinar a qualidade do sinal de qualquer AP em sua área, e se conectar ao que tiver melhor sinal.

Roaming é o processo em que um cliente se move entre células (BSS) sem perder conectividade. Os APs distribuem os clientes de uma maneira transparente, disponibilizando uma conexão contínua. *Roaming* entre APs dentro de um ESS é uma

característica muito importante de redes 802.11, e é baseado na capacidade de um cliente *wireless* determinar a qualidade dos sinais que ele está recebendo, e escolher um AP com melhor sinal.

Para determinar esse sinal os clientes utilizam o *Signal to Noise Ratio* (SNR), que nada mais é do que a relação entre a potência do sinal transmitido e o ruído. O AP envia *beacons* esporadicamente, e através desses *beacons* o sinal é medido. É bom lembrar que uma estação não sai de um BSS (entrar em *roaming*) a não ser que o sinal atual atinja uma marca pré-definida.

O padrão 802.11 não define exatamente como o processo tem que ser feito, mas define alguns passos básicos, como *scanning* ativo e passivo e *reassociation*. Quando a estação wireless recebe os *beacons* mandados pelos vários APs, ela escolhe o que possui melhor sinal. Se o seu sinal atual estiver abaixo do pré-determinado para *roaming*, ela faz a dissociação deste AP e se reassocia ao outro (*handoff*).

Nesta troca de APs, os dois envolvidos trocam informações sobre o cliente, para que, por exemplo, um pacote que ainda não terminou de ser enviado seja reendereçado para o outro AP para que o cliente possa terminar de recebê-lo. Esta troca de informações é o que difere os processos de associação e reassociação.

Fronteiras de Camada 3

Quando os vários APs são divididos em sub-redes, não é mais possível o *handoff* de sessões, já que os roteadores trocarão o endereço IP dos clientes. Quando o cliente se reconecta a rede, o antigo AP não sabe mais para onde enviar os pacotes, e todas as aplicações que dependem de *login* são perdidas e o usuário forçado a se logar de novo.

4.6. Localização de uma WLAN 802.11

Após ser instalado e configurado, o cliente irá automaticamente começar a 'ouvir' para ver se existe alguma WLAN a seu alcance, e caso positivo, tentará descobrir se é possível se associar a mesma. Esse processo é chamado de *scanning*, e ocorre antes de qualquer outro processo, já que esta é a maneira que o cliente acha a rede.

Há dois modos de *scanning*: passivo e ativo. Para o cliente achar a rede, ele segue uma trilha deixada pelo AP. Essa trilha é composta por *Service Set Identifiers* e *beacons*. Eles servem como ferramentas para que os clientes descubram os APs.

Service Set Identifier (SSID) – é um valor alfanumérico, podendo ter entre 2 e 32 caracteres, que define o nome da WLAN. É utilizado para segmentar redes e no processo de requisição de entrada para rede. O cliente precisa estar configurado com o SSID correto para se unir à rede.

Beacon – Os beacons são pacotes curtos que são enviados do AP para os clientes com a finalidade de sincronizar a comunicação sem fio numa WLAN.

Passive Scanning

É o processo de ficar ouvindo beacons por um determinado tempo após a inicialização da estação. O cliente fica ouvindo até achar um *beacon* que tenha o SSID da rede a qual ele deseja se conectar. No caso de múltiplos APs, todos irão anunciar em seus beacons o mesmo SSID. Nesse caso, o cliente se conectará ao AP que tenha o melhor sinal.

O processo de *scanning* é mantido mesmo após o cliente se associar a um AP. Isto ocorre para que o cliente mantenha sempre atualizada uma tabela com os sinais de cada AP em sua região, para caso seja necessário entrar em *roaming* já será conhecido o novo AP a que ele vai se conectar.

Active Scanning

Consiste do envio de um pacote *probe request* a partir do cliente. Este pacote é enviado sempre que o cliente deseja se conectar a uma rede. Neste pacote é inserido o SSID. Somente os APs que possuírem esse SSID responderão. Assim que o AP desejado for encontrado, é iniciado o processo de autenticação e associação.

4.7. O Padrão 802.11b

Em setembro de 1999, o IEEE ratificou uma revisão do padrão 802.11, chamada de 802.11 *High Rate* (HR/DSSS), ou 802.11b, que fornece taxa de transferência de dados muito superior, mantendo o padrão inicial. A arquitetura básica, assim como características e serviços definidos no padrão original foram totalmente mantidos, já que a nova especificação afetou somente a camada física. As modificações no modo em que os chips são codificados e um novo método de modulação chamado de QPSK possibilitaram esse aumento nas taxas de transferências.

Sua principal inovação é o suporte para duas novas velocidades: 5,5 e 11Mbps. Para isso, o DSSS foi escolhido como único modo de transmissão, já que o FHSS não suporta tráfego a tais velocidades. A idéia é que este novo padrão tenha interoperabilidade com sistemas 802.11 DSSS, mas não com FHSS. A transição 802.11/802.11b é semelhante à transição *ethernet/fastethernet*. A máquinas *fastethernet* podem diminuir suas velocidades para conversar com portas *ethernet*, mas jamais ao contrário.

As WLANs utilizam *Dynamic Rate Shifting*, permitindo que as taxas de transmissão sejam automaticamente modificadas dependendo da qualidade do sinal recebido pelo cliente. Este ajuste de velocidade acontece em função da qualidade do sinal recebido pelo cliente. A tecnologias de *Spread Spectrum* mais recentes são criadas para pular de forma transparente entre velocidades como 1, 2, 5.5 e 11Mbps. Quando uma estação se afasta de seu AP, o sinal diminui de potência e as taxas máximas não podem ser mais atingidas. A estação irá então automaticamente deixar cair à velocidade da conexão.

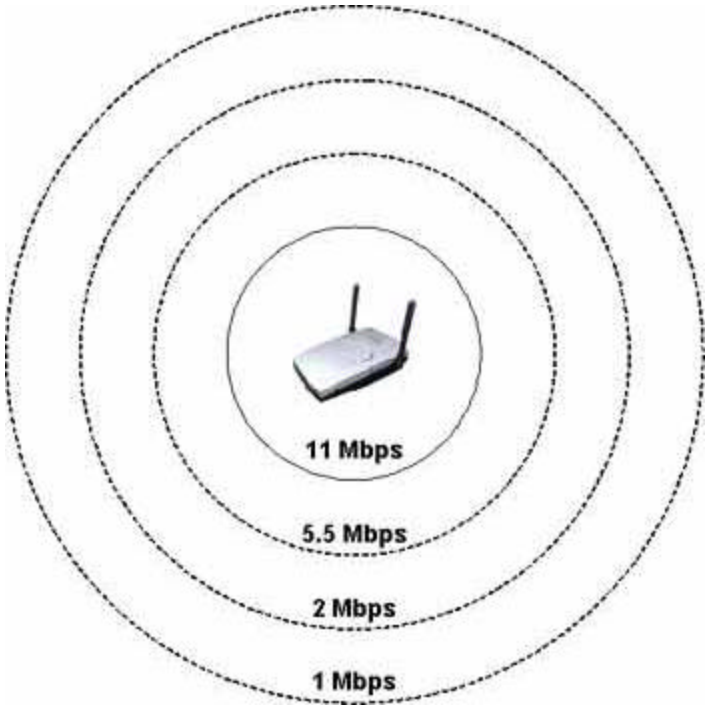

Figura 8: ***Dynamic Rate Shifting***

4.8. O Padrão 802.11a

O padrão 802.11a é mais uma extensão da camada física do 802.11. O *Spread Spectrum* já não é mais utilizado, em vez disso é utilizada uma técnica de codificação chamada de *Orthogonal Frequency Division Multiplexing* (OFDM), muito semelhante à utilizada no padrão *HiperLAN* europeu.

Os equipamentos 802.11a operam a freqüência de 5Ghz e atingem taxas de transferência de até 54mbps. Em termos de potência, esse padrão é dividido em três domínios: o primeiro, que opera a uma potência máxima de 50mW, o segundo opera até 250mW e o terceiro pode atingir 1W. Cada domínio tem seu respectivo espectro de freqüência na faixa dos 5GHz.

Devido a modo de operação completamente diferente na camada um, as redes 802.11a, não possuem interoperabilidade com redes 802.11b nem 802.11. Ou você opta por maior interoperabilidade e mais baixa transmissão, ou por maior transmissão e baixa interoperabilidade. Porém, como os padrões funcionam em faixas de freqüências distintas, elas podem coexistir sem o menor problema de interferência.

Como o padrão 802.11a utiliza o mesmo MAC que o padrão 802.11b, ele possui as mesmas deficiências. O MAC 802.11b é aproximadamente 70% eficiente. Isso significa que as taxas máximas de transferências não são atingidas. Logo, uma rede 802.11a de 54 Mbps opera entre 30 e 35Mbps.

4.9. O Padrão 802.11g

Este padrão fornece velocidades semelhantes ao 802.11a, adicionado com interoperabilidade com dispositivos 802.11b. Esta interoperabilidade facilita eventuais melhorias na sua WLAN, já que os dispositivos mais antigos poderão funcionar com os mais novos. Este padrão ainda não foi ratificado pelo IEEE, e produtos já estão sendo lançados baseados no *draft* 802.11g do IEEE.

Dispositivos 802.11g operam na faixa de freqüência de 2.4GHz e utilizam a tecnologia de modulação usada no 802.11a, chamada de OFDM. São capazes de automaticamente comutar sua modulação para operar na QPSK (Q*uadrature Phase Shift Keying*) para se comunicar com dispositivos 802.11b.

4.10. Outros padrões 802.11

802.11d – se concentra no desenvolvimento de equipamentos 802.11 que possam operar em países não servidos pelo padrão atual. O padrão 802.11 atual só opera em alguns países.

802.11e – visa promover melhorias como QoS e segurança para o padrão enquanto possuir interoperabilidade com o 802.11b e a.

802.11f – desenvolve um protocolo entre APs, devido a algumas limitações inerentes a marcas diferentes. Esse protocolo irá permitir *roaming* entre APs de qualquer empresa.

802.11h – desenvolve economia de energia e controle de espectro para que o padrão 802.11a possa ser usado na Europa.

802.11i – desenvolve melhorias nas questões relevantes à segurança. Promove a criação do WEPv2, que utiliza nova criptografia e corrige as falhas do modelo atual.

5. Equipamentos

5.1. *Access Point* (AP)

Um AP é um radio *wireless*. São os pontos centrais de uma rede *wireless*, ou a conexão entre o mundo cabeado e o sem fio. São dispositivos *half-duplex* equivalente a *switches* inteligentes. Podem funcionar em três modos: *Root*, Repetidor e *Bridge*.

Modo *Root*

O AP é conectado ao *backbone* cabeado através de uma interface (geralmente *ethernet*). Neste modo, ele serve como conexão entre o mundo cabeado e o mundo sem

fio, onde todos os clientes *wireless* se comunicam através dele. Quando há mais de um AP, eles podem trocar informações para permitir *roaming* transparente para o cliente.

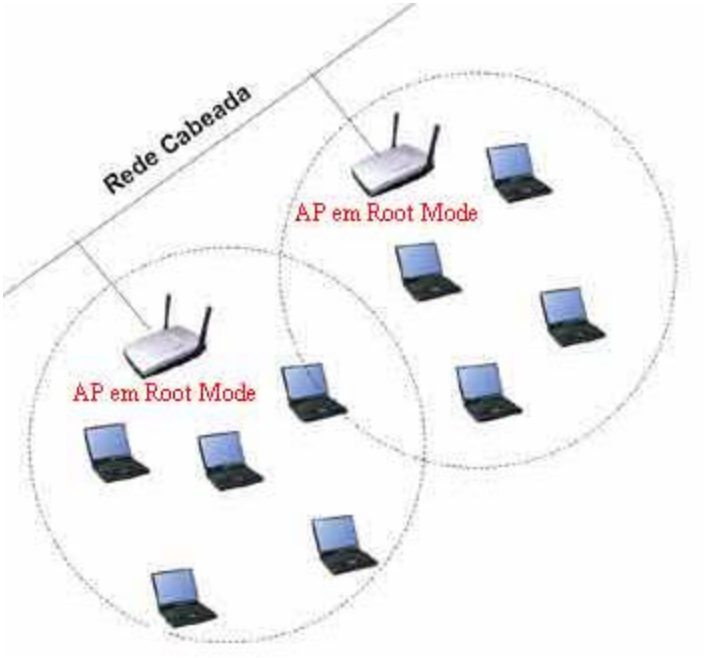

Figura 9: Modo *Root*

Modo Repetidor

Funciona de modo a levar a rede *wireless* até onde não chegaria com apenas um AP. Ou seja, repete o sinal *wireless* das estações conectadas a ele para atingir um outro AP que está funcionando no modo *root*. O AP repetidor compartilhará a conexão com outros clientes que estarão usando o AP *root*. Usuários conectados ao AP repetido provavelmente sofrerão com conexões ruins, com muitas falhas e baixas taxas de transferência.

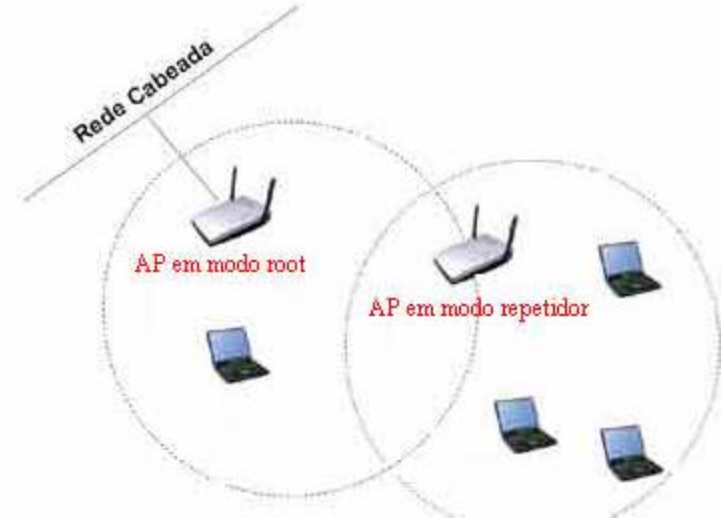

Figura 10: Modo Repetidor

Modo *Bridge*

No modo *bridge*, os APs funcionam como se fossem *bridges wireless*. São usadas para conectar duas redes cabeadas através de um link *wireless*. Normalmente não possuem clientes *wireless* diretos, e toda largura de banda é usada para a interconexão das redes cabeadas.

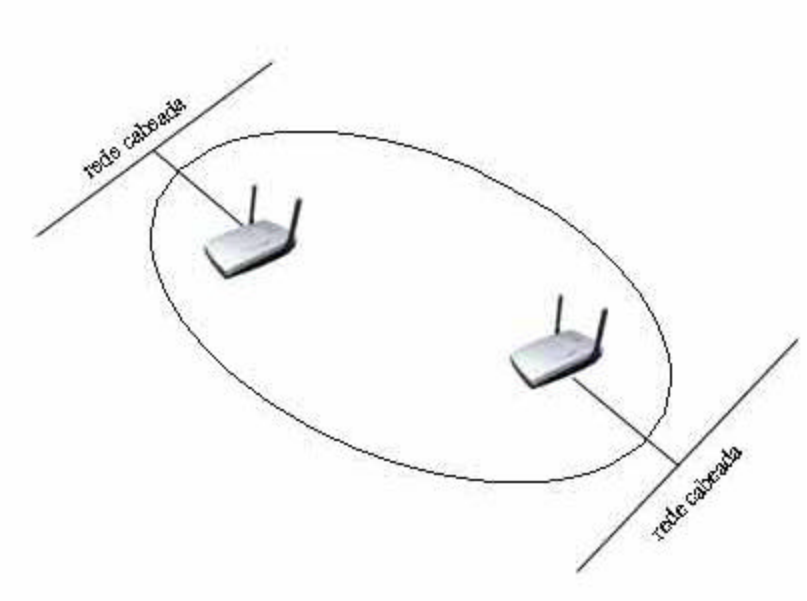

Figura 11: Modo *Bridge*

5.2. Cartão *Wireless*

Network interface cards (NIC) são placas de rede que possuem rádios para se comunicar com redes *wireless*. São instaladas em clientes como PCs e *laptops* para fornecer acesso à rede através de conexão sem fio. Eles podem vir de duas maneiras: PCMCIA e CF. Todas as outras variações desses dois são maneiras dos fabricantes facilitarem a instalação em interfaces diferentes, como USB e PCI.

PCMCIA e *Compact Flash*

O componente mais comum numa rede *wireless* são as placas PCMCIA. Esses dispositivos podem ser usados em *laptops* ou PDAs. As antenas presentes em cada placa PCMCIA variam de acordo com o fabricante. É possível ver vários modelos diferentes, alguns com antenas longas e finas, outras chatas e curtas.

Cartões *Compact Flash*, mais conhecidos como cartões CF, tem a mesma funcionalidade dos PCMCIA, mas são menores e normalmente usados em PDAs. Eles

têm como vantagem usar muito pouca energia e são aproximadamente do tamanho de uma caixa de fósforos.

Abaixo vemos alguns exemplos de PCMCIAs e CFs.

Figura 12: PCMCIA

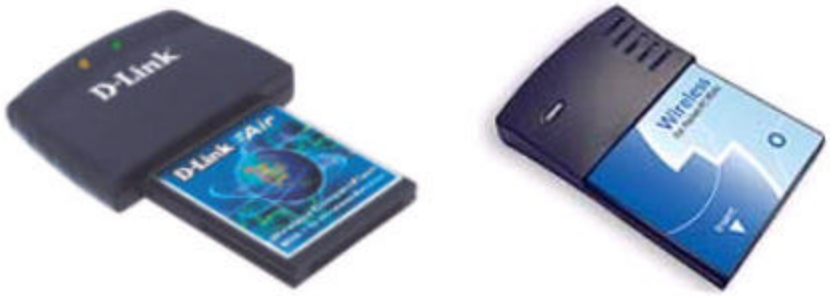

Figura 13: *Compact Flash*

Além destes dois modelos, há outras opções de placas de rede *wireless*, como adaptadores USB e PCI.

Adaptadores USB

Conectores USB estão se tornando muito populares devido a sua simples conectividade. Eles são *plug-n-play*, e não requerem nenhuma energia além da que é fornecida pelo conector USB. Basta conectar a placa a entrada USB do seu PC e você já estará conectado.

Figura 14: Adaptadores USB

Adaptadores PCI

São placas PCMCIA com adaptadores para serem conectados em portas PCI. A maioria é *plug-n-play*, então basta iniciar o PC para estar conectado à rede.

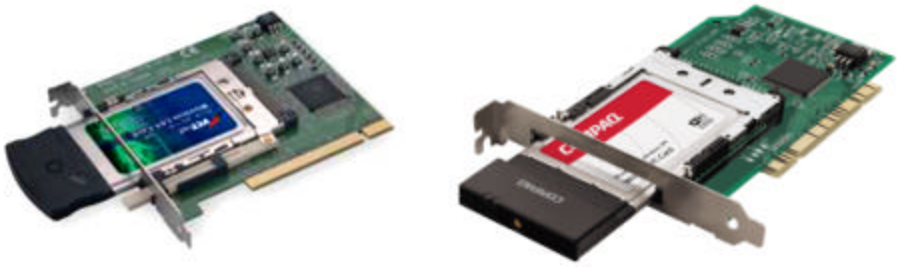

Figura 15: Adaptadores PCI

5.3. *W-Router*

Um AP fornece conectividade a clientes *wireless*, se conectando a uma rede *ethernet*. Ele pode fazer NAT, mas não possui outras características de roteamento. Quando estiver funcionando, o AP só irá rotear entre a rede que se conecta na interface *ethernet* e a rede NAT sem fio.

Um roteador *wireless* possui várias interfaces, como *fastethernet*, e pode rotear entre todas elas. Possui maior poder de processamento e outras características, como QoS e *multicast*. A diferença entre um roteador normal e um *w-router* é a presença de uma interface *wireless* que fornece conectividade a clientes *wireless* da mesma forma que um AP.

Figura 16: *W-Routers*

5.4. Antenas

Antenas são os elementos básicos para a comunicação entre todos os dispositivos de uma rede *wireless*. Elas podem ser usadas para aumentar o alcance de um sinal, ou para concentrar o sinal em alguma direção. As antenas se encaixam em três classificações gerais: omni-direcionais, semi-direcionais e altamente-direcionais.

Omni-direcionais

Também conhecidas como antenas dipolares, é o formato mais comum em redes sem fio. Ela irradia o sinal RF (radio freqüência) em todas as direções, ao redor do seu eixo. Elas são geralmente muito pequenas, já que o tamanho de uma antena é proporcional ao comprimento de onda do sinal. A figura abaixo mostra a forma que esta antena distribui sua energia. Quanto maior for o ganho desta antena, mais achatado é o eixo z, se aproximando do formato de uma panqueca, como acontece em antenas de alto ganho.

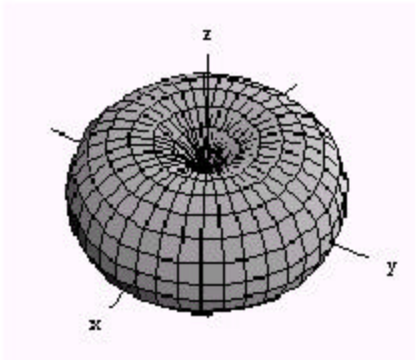

Figura 17: Distribuição do sinal em uma antena omni-direcional

As antenas omni-direcionais são usadas quando uma cobertura em todas as direções e necessária, como no caso de um ponto central fornecendo sinal para vários

clientes ao redor. É utilizada em topologias *Point-to-multipoint*, assim como topologias SOHO (*Small Office Home Office*).

Semi-direcionais

As antenas semi-direcionais existem em inúmeras maneiras, tamanhos e formatos. As mais utilizadas são *Yagi*, *Patch* e *Pannel*. Elas geralmente são achatadas para serem instaladas em paredes, e cada uma tem características de cobertura. Elas tendem a transmitir muito mais em uma direção do que nas outras, de forma cilíndrica, como mostrado na figura abaixo.

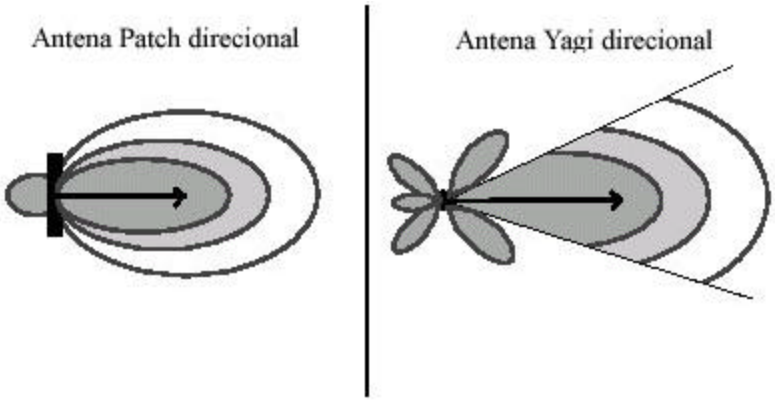

Figura 18: Padrão de irradiação de antenas semidirecionais

Antenas semi-direcionais são usadas no modo *bridge* de curto e médio alcance. Por exemplo, dois prédios a uma determinada distância um do outro podem se comunicar por enlaces sem fio usando antenas semi-direcionais.

Altamente-direcionais

Antenas altamente-direcionais emitem o sinal num feixe muito fino, de alto alcance e alto ganho. São ideais para enlaces *point-to-point* a longas distâncias.

Figura 19: Antena altamente-direcional

Alguns modelos são as parabólicas e as antenas *grid*:

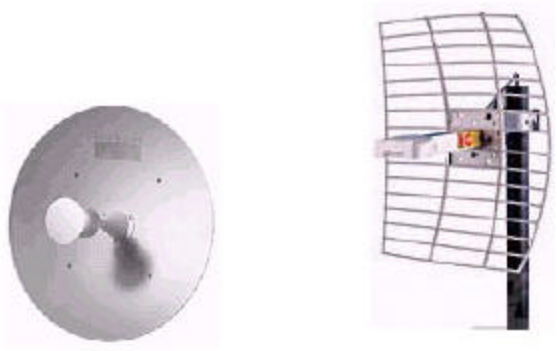

Figura 20: Antenas parabólica e grid

5.5. PoE

Considere uma área aberta em que o AP é colocado na parede de um prédio. Não há nenhuma tomada próxima ao ponto onde o AP possa ser conectado. Levar a rede elétrica de maneira eficiente seria caro e complexo. Para isso a energia pode ser transmitida em forma de uma tensão DC através do mesmo cabo *ethernet* que irá ligar o AP a rede interna. Do mesmo modo que o cabo CAT-5 pode transmitir dados a 100 metros, a PoE só é viável até 100m de distância.

Na maioria das vezes o melhor ponto para instalação do AP será num local sem acesso a rede elétrica. Nesses caso o PoE pode ter grande importância. É bom lembrar que o AP precisa ser compatível com PoE, assim como o *switch*/*hub* a quem o AP irá se conectar.

6. Segurança

Apesar de os usuários só levarem em conta o lado positivo, existem aspectos de segurança para serem levados em conta no que diz respeito à redes *wireless*. Neste tópico alguns destes aspectos serão abordados.

6.1. O protocolo WEP

O protocolo WEP (*Wire Equivalency Privacy*) foi o primeiro protocolo a ser utilizado para criptografia em redes *wireless*. Este protocolo trabalha na camada *Data-Link* e só fornece uma criptografia entre o cliente e o *Access Point*.

Este protocolo utiliza um algoritmo RC4 da RSA *Security* para criptografar os pacotes que serão trocados dentro de uma rede *wireless*, este algoritmo usa um vetor de inicialização (IV) de 24 bits e uma chave secreta compartilhada k de 40 ou 104 bits. A partir desses dois parâmetros, o algoritmo gera uma seqüência criptografada RC4 (k,v) de 64 ou 128 bits. Além disso, o protocolo WEP utiliza a CRC-32 para calcular o *checksum*

da mensagem, que é incluso no pacote. Para garantir integridade dos dados ele envia uma mensagem ICV (*Integrity Check Value*) logo após do *checksum* ser feito.

Vulnerabilidades do protocolo WEP

Como este protocolo foi o primeiro a ser utilizado, depois de algum tempo foram achadas algumas vulnerabilidades e falhas que fizeram com que o protocolo WEP perdesse quase toda sua credibilidade.

Como neste protocolo a chave secreta k gerada pelo RC4 é a mesma utilizada por todos usuários de uma mesma rede, devemos ter um vetor de inicialização diferente para cada pacote para evitar a repetição de uma mesma seqüência RC4. Essa repetição é extremamente indesejável, pois facilitará ataques e invasões. É recomendado que seja feita a troca da chave secreta periodicamente para que se possa dificultar possíveis ataques, só que isto se torna muito trabalhoso, pois esta troca será feita de forma manual. Se imaginarmos uma rede com um número alto de usuários isto se torna impraticável.

Outra falha existente no protocolo WEP diz respeito a sua função detectora de erros. A CRC-32 é uma função linear que não possui chave, e estas duas características fazem com que o protocolo seja susceptível a ataques. Um dos ataques seria fazer uma modificação das mensagens que sejam capturadas no meio do caminho sem que o receptor final perceba (isso pode ser feito devido à linearidade da função detectora de erros). Como o protocolo não possui uma chave temporária, torna-se mais fácil a descoberta da seqüência RC4. Com a posse da mesma, é possível conseguir autenticação na rede, e com isto conseguir introduzir mensagens clandestinas.

Soluções para o protocolo WEP

Algumas soluções foram propostas a fim de contornar ou acabar com as fraquezas deste protocolo. Uma das soluções que foi cogitada foi substituir a CRC-32 por uma função de hash MD5 ou SHA-1, só que esta solução se tornou muito cara e tornaria a execução do protocolo muito lenta pelos processadores atuais. Outras soluções foram discutidas, até que a RSA sugeriu que se usasse uma função hash mais leve, que usasse uma chave temporária conseguindo com isso a criação de uma chave diferente para cada pacote. Esta função de hash seria composta de duas fases distintas. Na primeira fase teríamos como entrada uma 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, a entrada seria a saída da primeira fase, além do 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. É válido lembrar que esta não foi a solução final, pois sempre serão feitas atualizações e sempre existirão novos conceitos para serem implementados.

6.2. O padrão WPA

O padrão WPA (*Wi-fi Protected* Access) foi criado para substituir temporariamente o WEP, conseguindo com isso combater as vulnerabilidades que este protocolo apresentava. Este padrão também é chamado de TKIP (*Temporal Key Integrity Protocol*) por usar conceitos de chave temporária, conceitos estes que foram de suma importância para a elaboração deste protocolo que usa além da chave temporária, chave por pacote.

Este protocolo ainda não se tornou um padrão IEEE 802.11, mas há um grande esforço no mercado para colocar à disposição produtos que utilizem o padrão WPA. Este padrão tem algumas características que fazem dele uma ótima opção para quem precisa de segurança rapidamente:

- É compatível com o protocolo WEP.
- Migrar para o padrão WPA requer somente atualização de software.
- O padrão WPA é desenvolvido para ser compatível com o próximo padrão IEEE 802.11i.

Vantagens do padrão WPA sobre o protocolo WEP

A principal vantagem da migração do protocolo WEP para o padrão WPA é a utilização de um protocolo de chave temporária (TKIP) que possibilita a criação de chave por pacotes, além de sua função detectora de erros, chamada *Michael*, possuir um vetor de inicialização (IV) de 48 bits (superando os 24 do protocolo WEP) e um mecanismo de distribuição de chaves.

Outra melhoria foi no processo de autenticação de usuários. Agora para fazer esta autenticação o protocolo utiliza o padrão 802.1x e o protocolo EAP (*Extensible Authentication Protocol*), que através de um servidor central faz a autenticação de cada usuário antes de fornecer acesso à rede.

6.2. IEEE 802.1x e protocolo EAP

Como forma de melhoramento substancial no que diz respeito à segurança de uma rede foi criado o padrão IEEE 802.1x. Este padrão define um novo tipo de segurança de acesso, que requisita a todos usuários uma prévia autenticação antes da disponibilidade dos recursos e serviços da rede. O método do 802.11x é totalmente baseado na identificação do usuário, utilizando serviços de autenticação para executar esta identificação. Para isto é comum a utilização de servidores RADIUS.

O padrão 802.1x tem sido incorporado em muitas *wireless* LAN e tem se tornado um padrão praticado entre muitos fabricantes. Este padrão, quando é combinado com o *Extensible Authentication Protocol* (EAP), pode prover um ambiente muito seguro e flexível baseado em vários esquemas de autenticação que estão em uso hoje em dia.

O protocolo EAP, que foi primeiro definido para o *Point-to-Point Protocol* (PPP), é um protocolo para negociar autenticações. EAP é definido pela RFC 2284 e define as características do método de autenticação incluindo as requeridas credenciais de usuários (*passwords*, certificações, etc.). O protocolo pode suportar múltiplos métodos de autenticação (*smart cards, transport layer security*, TLS, Kerberos Microsoft, etc.). Há várias versões do protocolo EAP no mercado, pois nenhuma industria nem o IEEE concordaram com algum tipo simples ou mesmo com um padrão para o protocolo.

Terminologia

Antes de começar a explicar como funciona o padrão 802.1x é necessário que se entenda algumas terminologias que serão utilizadas:
- *Authentication Server*: Agente responsável pelo processo de recebimento e resposta de solicitações para autenticação de acesso à rede. Normalmente este agente é um Servidor RADIUS.
- *Authenticator*: É um dispositivo de rede (switch, roteador, AP) que disponibiliza o acesso aos usuários da rede. Ele é responsável pela autenticação de acesso à rede.
- *Supplicant*: Dispositivo de rede que necessita ser autenticado na rede. Na maioria das vezes são estações de trabalho, mas podem ser *switches* que devem autenticar-se em outros *Authenticators*.

Processo de autenticação

Quando o 802.1x é usado na rede, é necessário que um *supplicant* autentique-se no agente *authenticator* que fornece acesso à LAN. O agente *authenticator* mantém um controle do status da porta para cada *supplicant* que ele está enxergando, e no caso do *supplicant* conseguir ser autenticado ele passará aquela porta para o status de autorizado, a partir daí o *supplicant* pode enviar dados para a LAN através do *Network Access Server* (NAS), que no caso de WLANs pode ser um AP. Se o *supplicant* não conseguir ser autenticado o agente *authenticator* deixa o status da porta como não autorizado, e o *supplicant* não consegue mandar tráfego através do NAS.

Quando NAS detecta uma atividade na porta, ele envia uma mensagem EAP-*Request* ID para obter a identificação do usuário do dispositivo. Quando o dispositivo recebe esta requisição (é necessário possuir um cliente 802.1x instalado) ele responde com sua identificação para o *authenticator*, que por sua vez encaminha a mesma para um servidor de autenticação. Neste caso o servidor de autenticação estará trabalhando como um identificador e fornecedor de perfil de acesso, através do qual o usuário pode estar em localidades diferentes acessando o mesmo perfil dentro do mesmo servidor de autenticação.

Como resposta ao *Access Request* o servidor de autenticação envia ao *authenticator* um *Access Challenge*, e o NAS neste momento encaminha uma mensagem EAP-*Request* para o dispositivo que por sua vez responde com uma mensagem EAP-*Response* com a identificação do usuário. Então o NAS encaminha esta identificação do usuário para o servidor de autenticação, que determina se o mesmo possui acesso ou não à rede, baseado na sua identificação. Quando o usuário é identificado, é enviado uma

mensagem Radius-Accept para o NAS, que por sua vez encaminha uma mensagem EAP-*Success* para o dispositivo, autorizando o tráfego de dados na respectiva porta do usuário.

Toda vez que houver uma mudança no estado da porta *up/down*, todas as configurações realizadas serão perdidas, acarretando assim que o processo seja todo repetido.

A figura a seguir representa como é feito o processo de autenticação.

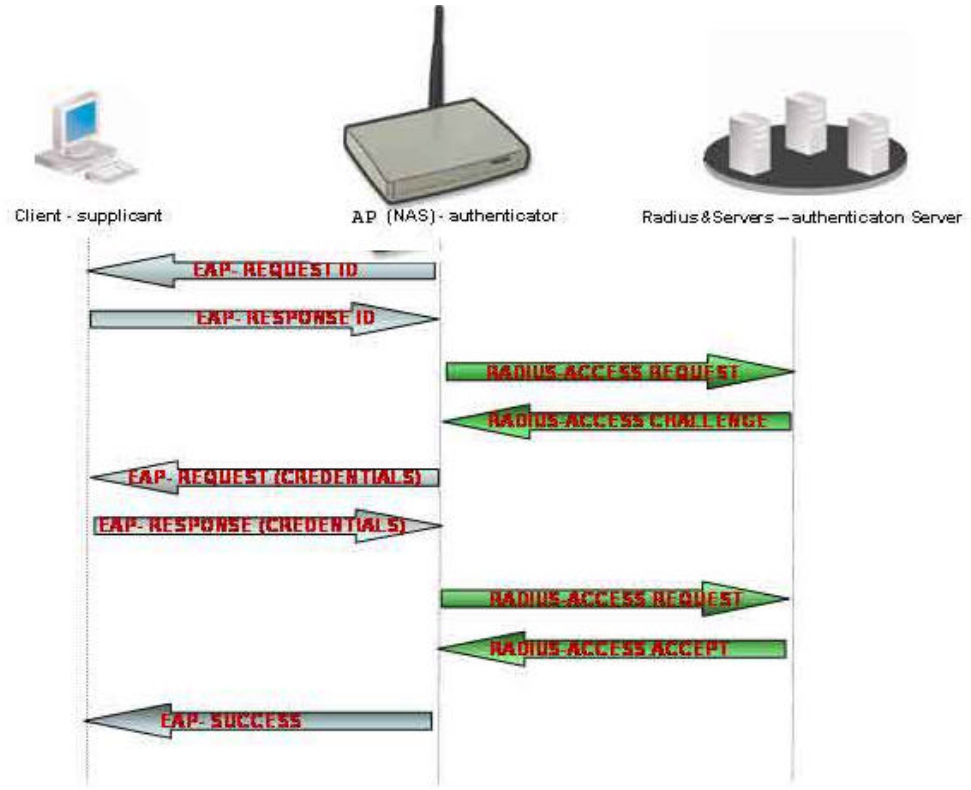

Figura 21: Processo de autenticação

Benefícios do 802.1x

O padrão 802.1x trouxe números benefícios para os administradores de redes. Os *supplicants* permitem que o administrador da rede continue utilizando seus servidores Radius como centralizadores na autenticação de usuários. Os *authenticators* suportam que vários servidores Radius sejam usados simultaneamente suportando ainda uma contingência de servidores (primário e secundário), isto vai garantir que os usuários sempre serão autenticados no NAS.

No que diz respeito a WLANs este padrão supera o protocolo WEP principalmente por conseguir contornar o problema com as chaves estáticas usadas neste protocolo utilizando o protocolo TLS (*Transport Layer Security*). O TLS irá garantir que uma chave será gerada toda vez que uma estação associar-se ao AP.

6.3. O padrão AES

O *Advanced Encryption Standard* (AES) está tendo uma melhor aceitação como método de segurança, pois faz uma substituição apropriada do RC4, algoritmo usado no protocolo WEP. O protocolo do AES usa o algoritmo Rijndale que é especificado para os seguintes tamanhos de chaves:

- 128-bit
- 192-bit
- 256-bit

Este padrão é considerado inquebrável, e o *National Institute of Standards and Technology* (NIST) tem escolhido o padrão AES para a *Federal Information Processing Standard*, ou FIPS. Como parte do esforço para melhorar o padrão 802.11, o grupo de trabalho 802.11i esta considerando o uso do AES no WEPv2.

O padrão AES, se for aprovado pelo grupo de trabalho 802.11i para ser usado no WEPv2, será implementado como *firmware* e software pelos fabricantes. *Firmware* de *access point* e *firmware* de clientes (o cartão de rádio PCMCIA) terão de sofrer um *upgrade* que suporte o padrão AES. *Software* para estações clientes (*drivers* e utilitários para clientes) suportarão configurações AES com chaves secretas.

6.4. Filtros

Filtros são um componente de segurança básico, que pode ser usado juntamente com outro protocolo, por exemplo, WEP ou AES. Eles trabalham semelhantes a uma *access list* de um roteador: definem parâmetros que as estações devem aderir para conseguir acesso à rede. Há três tipos básicos de filtros que podem ser configurados em uma WLAN:

- SSID
- MAC *address*
- Protocolo

SSID

Filtragem SSID é um método rudimentar de segurança, só é usado para um controle básico do acesso ao meio. O SSID (*service set identifier)* é só um outro termo para o *network name*. O SSID de uma estação deve combinar com o SSID do AP (*infrastructure mode*) ou de uma outra estação (*ad hoc mode*) para o cliente autenticar o serviço utilizado. A mensagem SSID é um *broadcast* presente em todo *beacon* que o AP envia, é muito simples achar o SSID de uma rede usando um *sniffer*. Muitos APs têm a característica de tirar o SSID do *beacon*. Quando é usado um AP deste tipo, o cliente deve ter o SSID configurado manualmente no *driver*. Quando um sistema é configurado desta maneira, é dito ser um "sistema fechado". Filtragem SSID não é considerada um método confiável para manter usuários não autorizados fora da rede.

MAC *Address*

WLANs podem ter filtros baseados no endereço MAC de um cliente. Quase todos os APs podem ter filtros baseados no MAC. Esta ferramenta permite que o administrador possa compilar, distribuir, e manter uma lista de endereços MAC permitidos e programá-los dentro de cada AP. Se um PC *card* ou outro cliente com endereço MAC que não está lista do AP tentar ter acesso à rede, o filtro não permitirá que o cliente consiga se associar com o AP. A figura a seguir ilustra este exemplo.

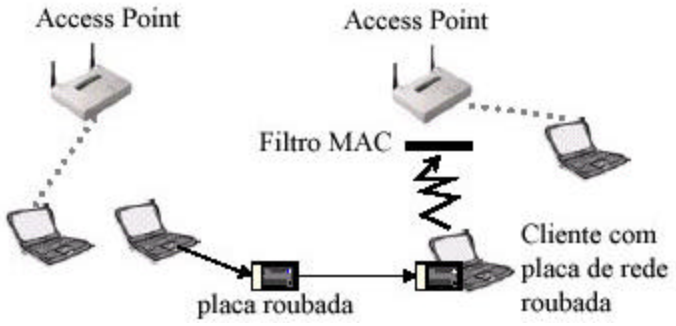

Figura 22: Filtragem por endereço MAC

É claro que colocar todos os endereços MAC de cliente de sua WLAN em um filtro pode ser impraticável se formos pensar em uma rede com um número grande de usuários. Para facilitar a vida do administrador, estes filtros podem ser implementados em algum servidor RADIUS ao invés de serem implementado em cada AP.

Embora pareça que filtros MAC sejam um ótimo método de segurança para uma WLAN isto não é totalmente verdadeiro, pois eles são susceptíveis a alguns tipos de intrusos. Usar o protocolo WEP e filtros MAC em conjunto provê uma boa segurança só quando trata-se de uma rede pequena, pois fica difícil imaginar que algum *hacker* gaste muito tempo tentando quebrar uma chave WEP ou burlando o filtro de uma rede que não possui informações valiosas.

Protocolo

É possível criar filtros para pacotes que passam pela rede baseado em protocolos da camada 2 a 7. Em muitos casos estes filtros são independentemente configurados para os segmentos com fio e o sem fio (*wireless*).

Imagine um cenário onde um AP em modo *bridge* é colocado em um outro prédio, conectado a uma WLAN que se liga a uma rede ethernet. Se este link foi instalado com o propósito de dar acesso a Internet para seus usuários, pode-se filtrar todos protocolos exceto SMTP, POP3, HTTP, HTTPS, FTP, e isto limitará o acesso de usuários a arquivos internos do servidor da empresa, por exemplo. A figura abaixo mostra como funciona o filtro de protocolos em uma WLAN.

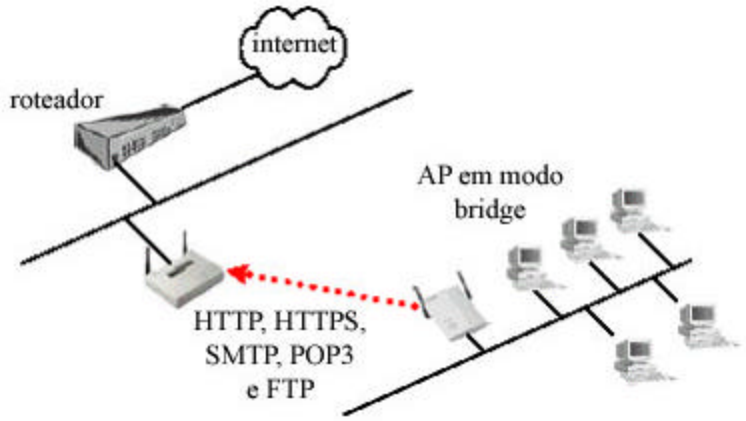

Figura 23: Filtros de Protocolos

6.5. Futuro

A seguir serão listadas algumas das soluções que o grupo de trabalho 802.11i do IEEE indica para ter uma melhoria no que diz respeito ao aspecto de segurança em uma WLAN.

TKIP

Para eliminar as conhecidas falhas do protocolo WEP o grupo de trabalho 802.11i especifica o uso do *Temporal Key Integrity Protocol* (TKIP). Este protocolo, que também é conhecido como WPA supera o WEP principalmente no seu processo de criptografia por usar chaves temporárias, dando assim uma segurança maior à rede.

AES

O uso do padrão AES está em estudo, e pode ser utilizado no WEPv2. Sua principal característica é suportar chaves de até 256 bits.

802.1x

Será usado o *Extensible Authentication Protocol* (EAP) *over* LANs (EAPOL) para conseguir um nível de segurança maior no 802.1x. O EAPOL vai melhorar principalmente a autenticação de usuários de uma WLAN, dificultando com isso a invasão da rede. Sua principal característica é que sua autenticação é feita através de portas como se fosse um *switch*. O padrão 802.1x suporta além do EAP, o RADIUS como método de autenticação.

7. Conclusão

Podemos concluir que as redes *wireless* são uma realidade no mundo atual. Isto foi alcançado através da criação de um padrão universal que estabelecesse critérios para fabricação de equipamentos compatíveis entre si, tornando assim as redes sem fio semelhantes às redes cabeadas que hoje em dia dominam o mercado.

Novos subpadrões do 802.11 estão sendo desenvolvidos por grupos de trabalho do IEEE, visando melhorias em relação à falhas existentes no padrão atual. Uma destas falhas se refere à questão da falta de segurança, trabalhada pelo padrão mais recente: 802.11i. Outra melhoria buscada diz respeito às taxas de transmissão, que atualmente estão muito abaixo das outras tecnologias de LAN.

A queda de custo dos equipamentos, maior disponibilidade dos dispositivos wireless e a facilidade de instalação foram responsáveis pela popularização das redes sem fio, tornando muito comum hoje em dia encontrarmos redes *wireless* privadas domésticas.

Num futuro bem próximo, pretende-se que as redes sem fio sejam a tecnologia predominante em LANs. Vale ressaltar que isto só ocorrerá se constantes investimentos forem feitos para o contínuo desenvolvimento deste padrão.

8. Glossário

802.1x Padrão utilizado para autenticar usuários na rede. A grande vantagem deste padrão sobre os outros é basear-se totalmente na identificação e autenticação do usuário.

Access Point Dispositivo central de uma rede *wireless*, é utilizado para interligar a rede sem fio com a cabeada.

Access-list Conjunto de regras configuradas em algum dispositivo de rede, cuja principal função é controlar o trafego que passa pela rede.

Active Scanning Neste processo o cliente envia o pacote para descobrir o AP.

Ad-Hoc Topologia de rede sem fio em que os computadores se comunicam entre si sem a necessidade de um *Access Point*.

AES ***A****dvanced* ***E****ncryption* ***S****tandard*: padrão de segurança que utiliza um algoritmo especificado para chaves de criptografia de 128, 192 e 256 bits.

Antenas Elemento básico de uma rede sem fio, são utilizadas para aumentar o alcance de um sinal ou para concentrá-lo em uma determinada direção.

Banda estreita Tecnologia que para transmissão de dados utiliza uma banda muito estreita e com alta potência, conseguindo assim um longo alcance.

Beacon Pacotes curtos que são trocados entre o AP e os clientes, com finalidade de sincronizar a comunicação em uma WLAN.

Bluetooth Tecnologia sem fio de curto alcance (até 10 metros) para troca de dados entre dispositivos eletrônicos.

BSS ***B****asic* ***S****ervice* ***S****et*: topologia mais básica de uma rede *wireless*. Consiste de vários *hosts* com um *access point* interligando-os.

CAM ***C****ontinuos* ***A****ware* ***M****ode*: oposto ao PSP, neste modo o cliente não entra em modo *sleep*, utilizando a potência total.

CF ***C****ompact* ***F****lash*: cartão de memória não volátil que utiliza memória *flash*, pode ser usado como placa de rede wireless para *PDAs* e *handhelds*.

CSMA-CA ***C****arrier* ***S****ense* ***M****ultiple* ***A****ccess* – ***C****ollision* ***A****voidance*: método de acesso ao meio semelhante ao CSMA-CD nas redes ethernet. Baseia-se no fato que o dispositivo cria algoritmos para evitar as colisões de pacotes.

CTS ***C****lear* ***T****o* ***S****end*: mensagem que o AP envia ao cliente para informá-lo que o trafego está liberado e que só ouvirá o que ele tem a dizer.

DSSS ***D****irect-****S****equence* ***S****pread* ***S****pectrum*: um dos dois tipos de *spread spectrum*, é uma tecnologia de transmissão. O sinal é espalhado pelo espectro, adicionando-se bits de dados redundantes chamados *chips*.

Dynamic Rate Shifting Capacidade da WLAN de automaticamente modificar a taxa de transmissão de acordo com a qualidade do sinal recebido.

EAP ***E****xtensible* ***A****uthentication* ***P****rotocol*: protocolo geral para autenticação, podendo utilizar inúmeros métodos de autenticação, como servidores RADIUS.

ESS ***E****xtended* ***S****ervice* ***S****et*: conjunto de BSSs, que normalmente são interligados por uma rede cabeada.

FHSS ***F****requency-****H****opping* ***S****pread* ***S****pectrum*: um dos dois tipos de *spread spectrum*, é uma tecnologia de transmissão. O sinal é modulado por uma portadora que oscila sua freqüência de forma aleatória mais previsível.

Handheld dispositivo com funções igual aos PDAs.

IEEE ***I****nstitute of* ***E****lectrical and* ***E****lectronics* ***E****ngineers***:** instituto formado em 1884, é composto por engenheiros, estudantes e pesquisadores. Tem como principal função desenvolver padrões nas áreas de engenharia e informática.

ISS ***I****ndependent* ***S****ervice* ***S****et*: conhecidas como topologias *Ad-Hoc*, os clientes se comunicam entre si sem a necessidade de um dispositivos de interconexão.

MAC ***M****edia* ***A****ccess* ***C****ontrol*: endereço físico de um dispositivo de rede.

OFDM ***O****rthogonal* ***F****requency* ***D****ivision* ***M****ultiplexing*: técnica de modulação digital em que o sinal é dividido em inúmeros canais de banda estreita.

Passive Scanning Neste processo o cliente espera receber um *beacon* do AP para descobri-lo.

PCMCIA ***P****ersonal* ***C****omputer* ***M****emory* ***C****ard* ***I****nternational* ***A****ssociation*: associação responsável pela criação de dispositivos pequenos e finos chamados de *PC Cards*, normalmente utilizados em *laptops*.

PDA ***P****ersonal* ***D****igital* ***A****ssistant*: dispositivo de portátil que une características de PC, Internet e rede.

PoE ***P****ower* ***o****ver* ***E****thernet*: solução para fornecimento de energia para dispositivos em que a energia elétrica é transmitida através de um cabo CAT-5.

PSP ***P****ower* ***S****ave* ***P****olling*: neste modo o cliente se desliga completamente por um

pequeno espaço de tempo para economizar energia.

QPSK ***Q****uadrature* ***P****hase* ***S****hift* ***K****eying*: técnica de modulação digital em freqüência

Radius ***R****emote* ***A****ccess* ***D****ial-in* ***U****ser* ***S****ervice*: protocolo utilizado para comunicação entre dispositivo de acesso remoto e um servidor de autenticação. Um servidor rodando autenticação RADIUS é usualmente chamado de Servidor RADIUS.

RC4 é um algoritmo de criptografia que utiliza um vetor de inicialização de 28 bits e uma chave secreta compartilhada de 40 ou 104 bits.

Roaming Em redes sem fio, se refere a capacidade de mobilidade de um cliente entre vários APs sem a perda de conectividade.

RTS ***R****equest* ***T****o* ***S****end*: mensagem que o cliente manda para o AP com o intuito de avisá-lo que quer utilizar o meio por um determinado tempo.

Sniffer Software que coleta dados do trafego da rede para posterior análise.

Spread Spectrum Tecnologia que permite transmitir dados espalhando-os numa faixa de freqüência muito grande utilizando uma potência muito pequena.

SSID ***S****ervice* ***S****et* ***Id****entifier*: identificador de até 32 caracteres presente no cabeçalho de cada pacote transmitido na rede *wireless*, que funciona como senha quando um cliente tenta se conectar a um BSS.

TKIP ***T****emporal* ***K****ey* ***I****ntegrity* ***P****rotocol*: tipo de protocolo de segurança que utiliza chaves temporárias de criptografia.

WEP ***W****ired* ***E****quivalent* ***P****rivacy*: protocolo de segurança definido no padrão 802.11, tem como finalidade fornecer a mesma segurança presente em redes cabeadas.

WLAN ***W****ireless* ***L****ocal* ***A****rea* ***N****etwork*: tipo de LAN que utilize ondas eletromagnéticas de alta freqüência para comunicação entre estações.

WPA ***W****i-Fi* ***P****rotected* ***A****ccess*: padrão desenvolvido pela Wi-Fi Alliance para melhorar a segurança do WEP. Foi criado para funcionar em redes existentes que utilizem o WEP, sendo necessário somente um *upgrade* de software.

WPAN ***W****ireless* ***P****ersonal* ***A****rea* ***N****etwork:* rede pessoal, sem fio, utilizada para intercomunicação de dispositivos a curto alcance.

WWAN ***W****ireless* ***W****ide* ***A****rea* ***N****etwork:* rede mais ampla que faz a transmissão de dados através de sinais celulares.

9. Bibliografia

Certified Wireless Network Administrator – Official Study Guide, Planet3 Wireless

Building Wireless Community Networks - Matthew S. Gast - O´Reilly

Building a Cisco Wireless LAN, Eric Ouellet, Robert Padjen, Arthur Pfund – Syngress

Search Networking.com - www.searchnetworking.com

Institute of Electrical and Electronic Engineers (IEEE) – www.ieee.org

Wireless Ethernet Compatibility Alliance (WECA) – www.wirelessethernet.org

Federal Communications Commission – www.fcc.gov

Wireless LAN Association – www.wlana.org

Módulo Security – www.modulo.com

"A tecnologia de redes Wireless" , RNP News Generation – www.rnp.br/newsgen

"IEEE 802.1", Enterasys Networks – www.enterasys.com

"Introdução às redes Wireless", Nilton Alves Jr. & Sandro P. da Silva, CBPF-NT-003/02

"How Wireless Internetworking Works", How Stuff Works – www.howstuffworks.com

802.11g News – www.80211gnews.com

PaloWireless – The Wireless Resource Center – www.palowireless.com

The Network World Fusion – Wi-Fi - http://www.nwfusion.com/research/wifi.html

Dell – Learn About Wireless -
http://www.dell.com/us/en/bsd/topics/segtopic_how3_2_lma_truemobile.htm

Wi-Fi Alliance – www.wi-fi.com