Bruno Marques Amaral
brunoma@cbpf.br
Marita Maestrelli
marita@cbpf.br

Segurança em Redes Wireless 802.11

Resumo

Esta nota técnica aborda as principais características da segurança em redes *wireless* do padrão IEEE 802.11. Serão apontadas as principais fragilidades, assim como os métodos de segurança e tipos de ataques. Além disso, serão tratadas alternativas conhecidas que garantem segurança a estas redes.

Índice

1 Introdução

O avanço da tecnologia nos últimos anos tem permitido o rápido crescimento do seguimento das comunicações. A necessidade de velocidade nas transmissões vem sendo fator primordial na disputa dos mercados pela informação. Neste contexto inóspito de intensas transformações, surge a possibilidade da concretização das redes *wireless* (sem fio), um projeto que por algum tempo não pôde ser efetivado, por causa da tecnologia que somente nos dias atuais tem possibilitado a difusão deste tipo de sistema. Neste tipo de rede, um usuário, portando um *notebook*, poderá se mover dentro do ambiente de trabalho sem perder a conexão.

As principais vantagens deste sistema são: a mobilidade que supera indiscutivelmente à das redes a cabo; o rápido retorno financeiro devido ao baixo custo de instalação (já que dispensa os cabos); além da facilidade de adaptação de uma rede *wireless* a uma rede a cabo já existente. Por essas razões, alguns centros de pesquisa já apontam um crescimento anual de pelo menos 42% até 2007.

Contrariamente ao processo de comercialização de novas tecnologias, o crescimento das redes *wireless* tem demonstrado uma grande vontade de consumo no mercado de usuários domésticos, que normalmente procuram um amadurecimento da nova tecnologia para depois usufruí-la. Certamente, este mercado não tem tantas preocupações quanto às implicações associadas à segurança deste tipo de rede. Por outro lado, empresas de grande e médio porte ainda estão bastante preocupadas com o fato de transmitir dados confidenciais pelo ar.

Os riscos são inerentes a qualquer tecnologia *wireless*, porém alguns destes riscos são semelhantes aos das redes a cabo, outros são mais significativos em redes *wireless* e outros são novos. Neste caso, alguns ataques podem ser feitos, por exemplo, lançando um vírus na rede, paralisando a rede ou até mesmo visualizando dados confidenciais.

2 IEEE 802.11: O Padrão de Redes *Wireless*

WLANs (*Wireless Local Area Network*) são baseadas no padrão IEEE 802.11, que começou a ser desenvolvido em 1997. Este padrão foi projetado para suprir aplicações com altas taxas de transmissão de dados, como as redes *Ethernet*.

802.11 é o padrão original das WLANs, projetado para transmitir de 1Mbps a 2Mbps de largura de banda sem fio. Este padrão foi seguido em 1999 pelo IEEE 802.11a, que estabelecia uma transmissão de alta velocidade, na faixa de 5GHz e que chega a 54 Mbps. Ainda em 1999, o padrão IEEE 802.11b foi criado, porém este operando na faixa de 2,4 - 2,48GHz e que suporta 11Mbps. Atualmente, este padrão é

o mais utilizado por atender as aplicações em geral. Outro padrão criado depois e que vem se popularizando é o IEEE 802.11g que corrige e melhora algumas limitações do 802.11b, e por operar na mesma faixa de freqüência, é inteiramente compatível com este padrão. Ou seja, na prática uma WLAN implementada com padrão 802.11b não é perdida caso queira-se introduzir o 802.11g nesta rede.

Outros dois padrões importantes para WLAN são o IEEE 802.1X e o IEEE 802.11i. O primeiro, é um protocolo de controle de acesso (autenticação), o segundo é um protocolo específico para as funções de segurança e que opera com o 802.1X. As características do IEEE 802.11i serão discutidas em uma seção posterior.

2.1 A Arquitetura 802.11

Esta seção será dedicada a uma breve explicação das características gerais das redes *wireless*. Na tabela abaixo, verificamos algumas destas características.

Característica	Descrição
Camada Física	*Direct Sequence Spread Spectrum*(DSSS), *Frequency Hopping Spread Spectrum*(FHSS) e infravermelho (IR).
Faixa de Freqüência	2,4GHz (11b, 11g) e 5GHz (11a)
Largura de Banda	1Mbps, 2Mbps, 5.5Mbps, 11Mbps (11b), 54Mbps (11a, 11g)
Segurança de informação	Autenticação, confidencialidade e integridade baseada no algoritmo de encriptação RC4, porém com gerenciamento da chave limitado.
Distância de Operação	Aproximadamente 50m (ambientes fechados) e 400m (ambientes abertos).
Throughput	Aproximadamente 5.5Mbps (11Mbps) e 25 - 30Mbps (54Mbps).
Aspectos Positivos	Velocidade de rede *Ethernet*, porém sem cabo, muitos produtos diferentes de empresas diferentes. *Access Points* e *Wireless Client Cards* estão diminuindo de preço.
Aspectos Negativos	Segurança baixa na configuração padrão, o *throughput* cai muito com a distância e a carga.

Tabela 2.1-1: Características do Padrão 802.11

O padrão 802.11b permite que dispositivos estabeleçam uma ligação ponto-a-ponto (P2P) ou redes baseadas em pontos de acesso (*access points* - AP) fixos no qual aparelhos móveis podem se comunicar. Este padrão estabelece duas topologias básicas de rede: a rede estruturada e a rede *ad hoc*.

A rede estruturada permite estender a área de comunicação de uma rede cabeada com uma célula *wireless*. Um *laptop* ou outro dispositivo móvel de comunicação precisa passar de célula para célula (de AP para AP) para manter a

conexão com a rede. Uma célula é a área coberta por um AP e é chamado de BSS (*basic service set*). A união de vários BSSs que formam a infraestrutura de uma rede é chamada de ESS (*extended service set*). Esta topologia é útil para prover acesso em uma região como um prédio ou o campus de uma universidade.

Um ambiente WLAN possui estações clientes que usam *modems* de comunicação via rádio. As estações clientes geralmente utilizam NIC (*network interface card*) que consiste em um modem *wireless* com lógica para interagir com a máquina cliente e o *software*. Um AP é um dispositivo que consiste essencialmente em um *hub* do lado *wireless* e uma *bridge* do lado cabeado. Logo, todas as comunicações entre estações clientes e redes cabeadas passam pelo AP. A topologia básica de uma rede *wireless* é mostrada abaixo.

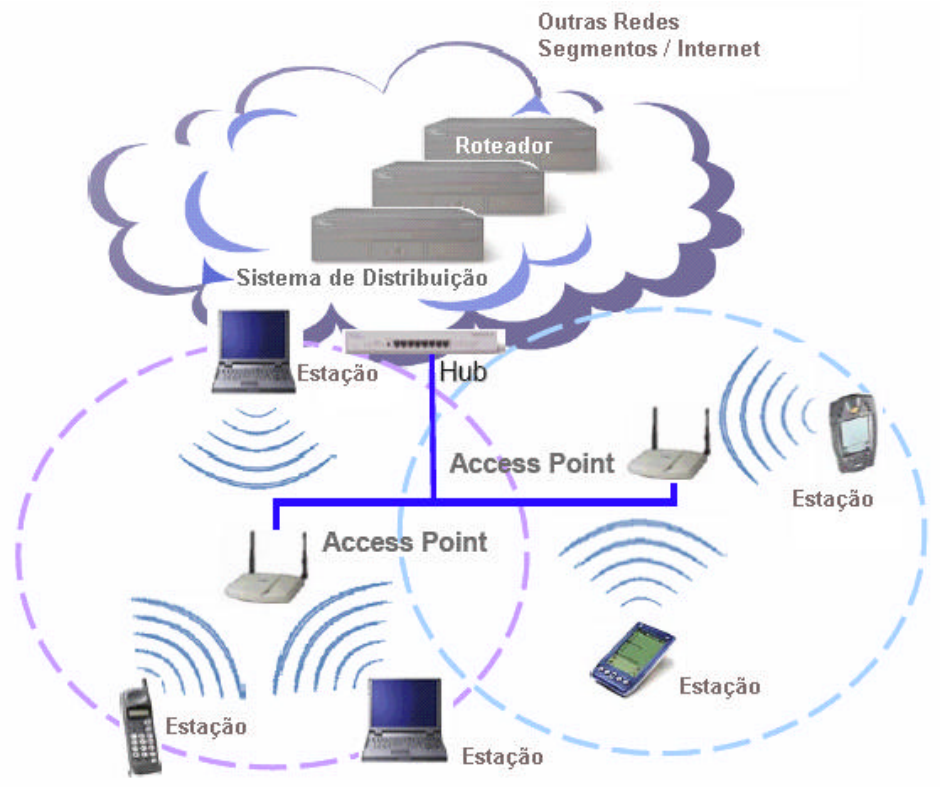

Figura 2.1-1: Topologia Fundamental de uma LAN *Wireless*

Apesar da maioria das WLANs operarem no modo de rede estruturada, como descrito anteriormente, uma outra topologia também pode ser utilizada. Este segundo tipo de topologia, conhecida como redes *ad hoc*, permite interconectar facilmente dispositivos que estiverem na mesma área. Nesta arquitetura, estações clientes são agrupadas dentro de uma única área geográfica para que possam se comunicar, porém estas não terão acesso a LAN cabeada. Os dispositivos interconectados no

modo *ad hoc* funcionam como um IBSS (*independent basic service set*). Um esquema da topologia *ad hoc* pode ser visto na figura abaixo.

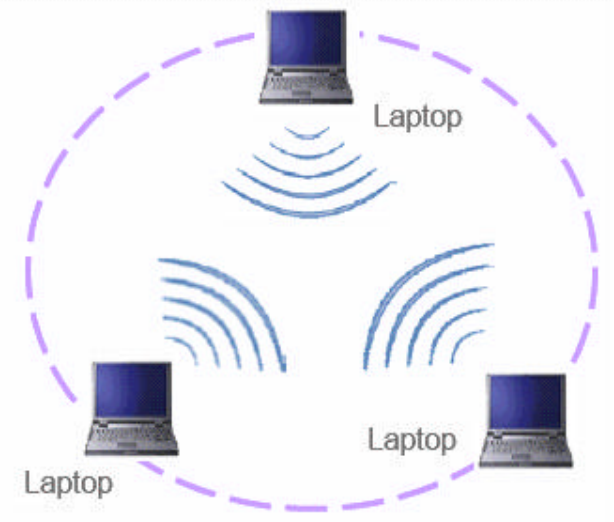

Figura 2.1-2: Topologia Fundamental de uma LAN *Ad hoc*

A configuração *ad hoc* é similar a uma rede ponto-a-ponto, na qual nenhum ponto funciona como servidor. Em uma rede *ad hoc*, cada ponto (*laptops*, *desktops* e outros dispositivos) pode compartilhar arquivos sem a necessidade de um AP.

2.2 Componentes

Uma WLAN compreende de dois tipos de equipamentos: uma estação cliente e um ponto de acesso (AP). Uma estação cliente é normalmente um *laptop*, *notebook* ou um PC (computador pessoal) com um NIC *wireless* ou placa de rede *wireless*. O NIC é normalmente inserido em uma porta PCMCIA (*Personal Computer Memory Card International Association*) ou em uma porta USB (*Universal Serial Bus*). Um AP funciona como uma estação base para a rede *wireless*, podendo agregar várias estações *wireless* a rede cabeada.

2.3 Área de Cobertura

A área de cobertura para redes *wireless* baseadas no padrão 802.11b depende de vários fatores como a taxa de dados necessária, a capacidade, as fontes de interferências de RF (rádio-freqüência) e a área física, além das características de potência, conectividade e o tipo de antena. Teoricamente, a área é compreendida dentro de um círculo de raio igual a 29m (vinte e nove metros) a 11Mbps em áreas fechadas e 400m (quatrocentos metros) a 1Mbps em áreas abertas. Contudo, na prática verifica-se que para áreas fechadas consegue-se conectividade a 50m (cinqüenta metros) de distância do AP mais próximo. Já para áreas abertas, com a

utilização de antenas de alto ganho pode-se conseguir conectividade a 1000m (mil metros) de distância.

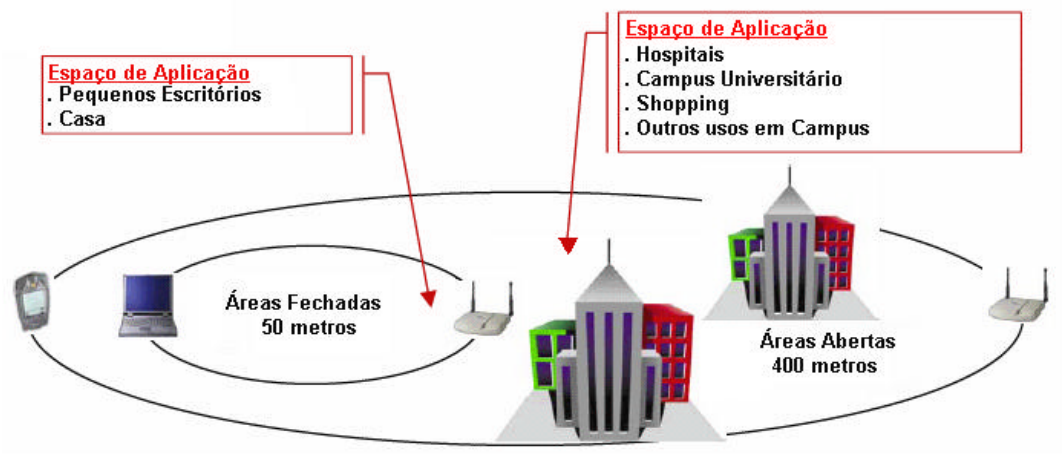

Figura 2.3-1: Área de Cobertura Típica de LAN *Wireless*

2.4 Benefícios

O método de comunicação móvel que as WLANs possibilitam, fazem dela um recurso muito atrativo nos dias atuais, que podem diminuir custos e aumentar a eficiência paralelamente.

WLANs oferecem quatro principais benefícios aos usuários:

- **Mobilidade ao usuário –** Usuários podem acessar arquivos, recursos da rede e a Internet sem estarem fisicamente conectados através de cabos. Além disso, usuários podem ser móveis e ter alta velocidade de transmissão com acesso instantâneo a rede.
- **Rápida Instalação –** O tempo necessário para a instalação é reduzido porque conexões podem ser feitas sem mover ou adicionar cabos, tendo que passá-los por paredes ou tetos.
- **Flexibilidade –** Testes com diversos cenários podem ser executados, trocando de lugar as áreas de acesso conforme a necessidade.
- **Escalabilidade –** Redes do tipo WLAN, podem ser configuradas para serem usadas em pequenas redes como ponto-a-ponto ou em grandes redes de teste, que sofrem constantes alterações.

Por causa destas facilidades, WLANs estão se tornando soluções viáveis se comparadas às redes cabeadas, com isso, hospitais, aeroportos, hotéis e lojas especializadas estão oferecendo acesso por WLAN à Internet.

3 WEP: O Padrão de Segurança de WLANs 802.11

Esta seção ajudará o leitor a compreender as características relativas a segurança em ambientes providos de redes baseadas no padrão 802.11b. A especificação do IEEE 802.11b aborda vários serviços para levar segurança ao ambiente operacional. A maior parte da segurança é colocada no protocolo WEP (*wired equivalent privacy*) para proteger a camada de enlace de dados durante a transmissão de um cliente com os APs. Ou seja, o WEP só controla a parte sem fio da rede, logo a parte cabeada terá sua segurança feita por outros meios, como na figura a seguir.

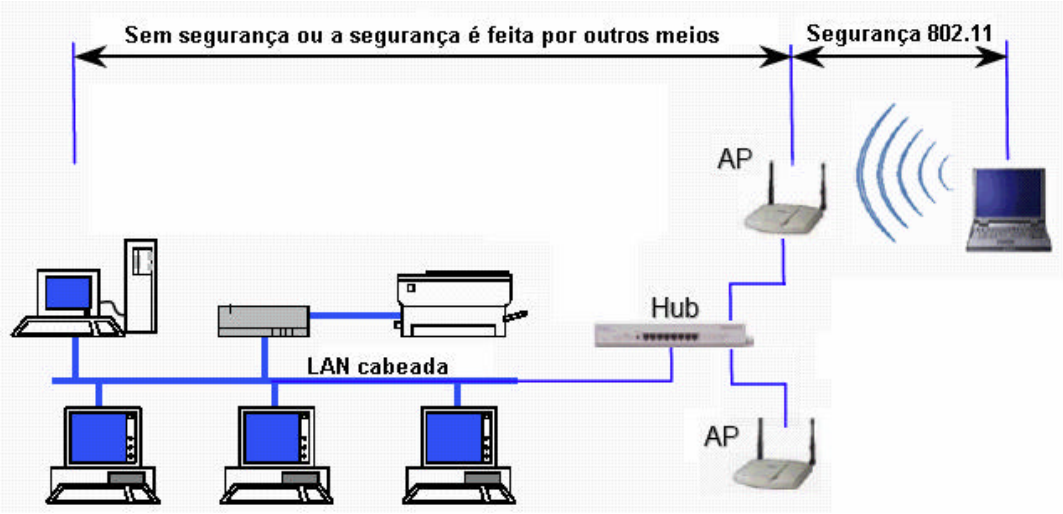

Figura 3-1: Segurança de uma WLAN 802.11b em uma Rede Típica

Os três serviços básicos de segurança para redes *wireless* são os seguintes:

- **Autenticação –** Esta primeira característica tenta assegurar que somente clientes pertencentes a rede poderão acessar a própria. Ou seja, ela verifica a identidade do cliente e avalia se esta estação cliente poderá ou não acessar a rede.
- **Privacidade –** Este serviço pretende assegurar a privacidade dos dados disponíveis na rede. Isto é, ele avalia se os dados poderão ser vistos por clientes que tiverem autorização.
- **Integridade –** Um outro quesito presente no protocolo WEP, promete garantir que os dados que sejam transmitidos não sejam modificados no caminho de ida e volta entre os clientes e os APs.

É importante notar que o protocolo WEP dispõe somente dos três serviços acima descritos, os quais serão explicados com maiores detalhes.

3.1 Autenticação

O IEEE 802.11b define duas maneiras para validar um cliente *wireless* que queira obter acesso a rede. Uma maneira envolve a utilização de criptografia e a outra não. Para o acesso de clientes sem o uso de criptografia, existem essencialmente duas maneiras de verificar se um cliente *wireless* deseja acessar a rede. As duas maneiras são chamadas de Sistema Fechado de Autenticação e Sistema Aberto de Autenticação. A estrutura de autenticação está descrita no esquema abaixo.

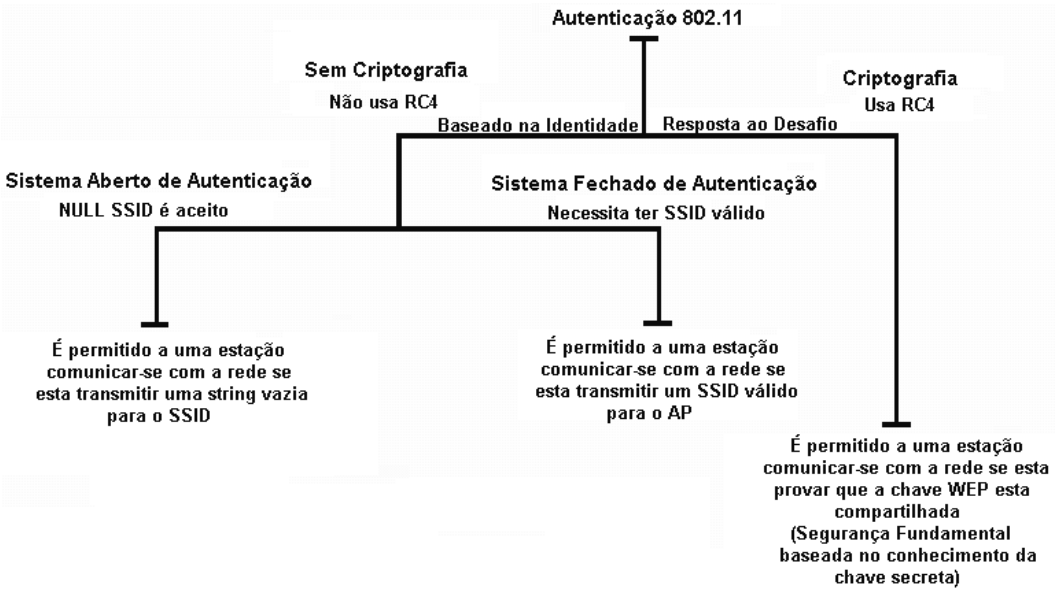

Figura 3.1-1: Técnicas de Autenticação do 802.11b

Uma estação que faz uma requisição de acesso a rede, simplesmente responde com um SSID (*service set identifier*). No sistema aberto, um cliente é autenticado mesmo se ele simplesmente responder com uma *string* vazia para o SSID, esta autenticação é conhecida como *NULL Authentication*. Com o segundo método, Sistema Fechado de Autenticação, clientes *wireless* precisam responder obrigatoriamente com o SSID atual da rede *wireless*. O que significa que a cada cliente é permitido o acesso se ele responder com a *string* correta de 0 a 32 bytes, identificando o BSS da rede *wireless*.

Na prática, nenhum deste dois métodos garante uma segurança eficiente contra acessos não autorizados. Novamente, tanto o Sistema Aberto quanto o Sistema Fechado de Autenticação são extremamente vulneráveis a ataques, e se não aprimorados, praticamente convidam ataques à rede.

A autenticação por chave compartilhada (*shared key*) é uma técnica que envolve a criptografia para a autenticação. Nela, um simples “desafio” é travado entre a estação cliente e o dispositivo (como um AP), na qual o cliente deve conhecer o

segredo compartilhado (*shared secret*). Primeiro, o AP gera um desafio aleatório que é enviado a estação cliente. O cliente usando uma chave criptográfica (chave WEP) que é compartilhada com o AP, criptografa o desafio e retorna o resultado para o AP. O AP descriptografa o resultado computado pelo cliente e só permitirá o acesso à rede caso o valor encontrado seja o mesmo que foi enviado inicialmente pelo AP. O algoritmo usado para fazer a criptografia é o código RC4, criado por Ron Rivest do MIT. É importante notar que a técnica de criptografia descrita acima é rudimentar e não provê autenticação mútua. Logo, o cliente não autentica o AP e então não há segurança se a estação cliente estará se comunicando com um AP legitimo da rede. É também conhecido que a autenticação feita por somente uma das partes é considerada um método fraco e que sofre constantes ataques.

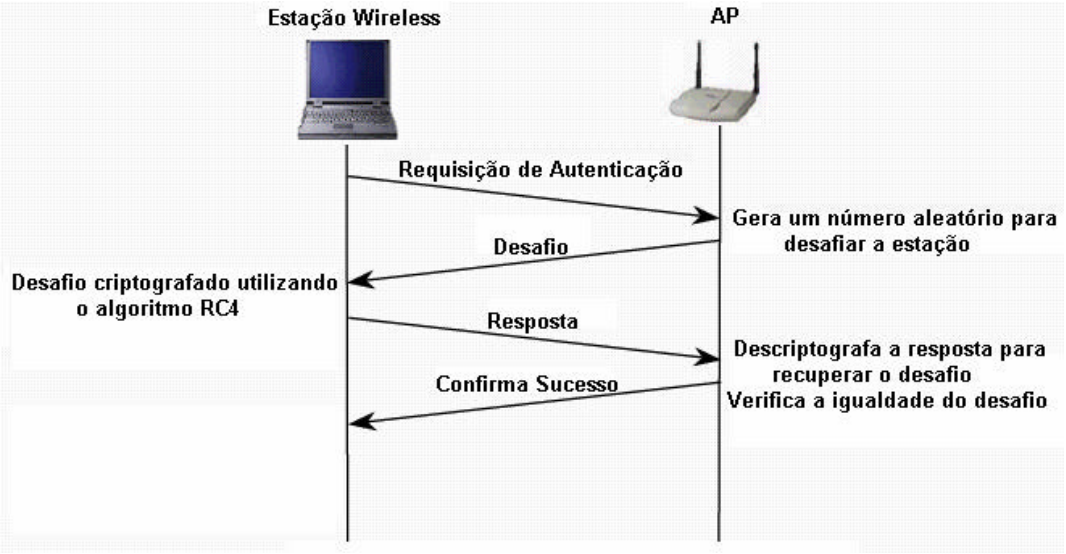

Figura 3.1-2: Processo de Autenticação por Chave Compartilhada

3.2 Privacidade

O padrão 802.11b também suporta o serviço de privacidade através do uso de técnicas de criptografia para a interface *wireless*. Esta técnica de criptografia WEP para privacidade também utiliza o algoritmo RC4 para gerar uma pseudo-seqüência de dados aleatória. Através desta técnica, o WEP pode impedir a descoberta dos dados durante a transmissão pela rede *wireless*. O WEP é aplicado em todo o tráfego da rede para proteger o TCP/IP (*Transmission Control Protocol / Internet Protocol*), IPX (*Internet Packet Exchange*), HTTP (*Hyper Text Transfer Protocol*).

O WEP suporta chaves criptográficas de 40 bits a 104 bits. A chave WEP de 104 bits, por exemplo, com 24 bits para o vetor de inicialização (IV) torna-se uma chave RC4 de 128 bits. Em geral, o aumento do tamanho da chave criptográfica, aumenta o nível de segurança. Algumas pesquisas têm mostrado que chaves com

tamanho maior que 80 bits, faz com que a quebra do código torne-se praticamente impossível. No entanto, a maioria das WLAN conta com chaves criptográficas de até 40 bits. Uma ilustração esquemática a seguir mostra como é feito o serviço de privacidade.

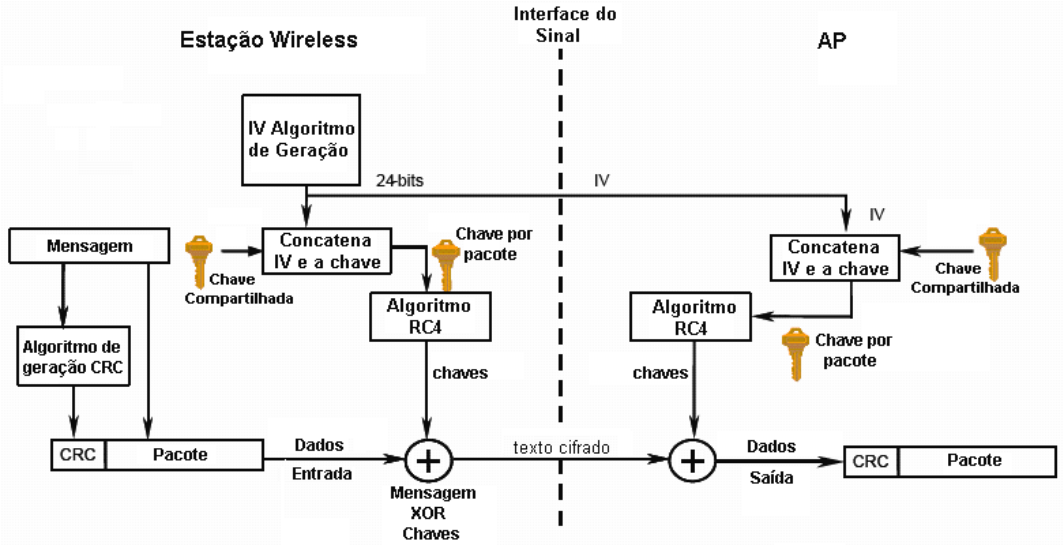

Figura 3.2-1: Privacidade WEP Utilizando Algoritmo RC4

3.3 Integridade

O padrão IEEE 802.11b também especifica uma maneira de garantir integridade dos dados transmitidos entre clientes e APs. Este serviço de segurança foi criado para rejeitar qualquer mensagem que tenha sido alterada durante a transmissão. Esta técnica utiliza um simples CRC (*Cyclic Redundancy Check*). Como descrito na ilustração anterior, o CRC, ou seqüência de checagem de quadro, é calculado em cada pacote a ser transmitido. A integridade do pacote é então criptografada utilizando uma chave RC4 para gerar o texto cifrado da mensagem. No receptor, é feita a descriptografia e o CRC é então recalculado na mensagem recebida. Depois, o CRC calculado é comparado com o CRC da mensagem original. Caso, os CRCs calculados sejam diferentes, indicará que a mensagem teve sua integridade violada e o receptor irá descartá-la. Infelizmente, como no serviço de privacidade, a integridade é vulnerável a certos ataques, sem levar em consideração o tamanho da chave.

Um aspecto importante que não é, muitas vezes, levado em consideração refere-se quanto ao gerenciamento das chaves de criptografia, ou seja, por quanto tempo deve-se utilizar a mesma chave criptográfica em uma WLAN. O resultado da falta de preocupação com gerenciamento da chave criptográfica pode trazer inúmeras vulnerabilidades às WLANs. Estas vulnerabilidades incluem as chaves WEP que

quase nunca são trocadas ou são mantidas com o valor padrão ou são chaves fracas (só zeros, só uns, baseados em senhas fracas ou outro padrão trivial similar). Outro problema é a dificuldade de se trocar esta chave WEP constantemente, em um amplo ambiente WLAN. Em um ambiente grande que pode ter 15.000 APs, trocar as chaves WEP torna-se um desafio.

3.4 Problemas com o Padrão de Segurança do IEEE 802.11b

Nesta seção serão abordados vários problemas encontrados em redes wireless IEEE 802.11b. Entre fatores causadores de problemas na segurança encontram-se: ataques passivos, para decodificar o tráfego na rede baseada em análises estatísticas; ataques ativos para inserir novos tráfegos a partir de estações móveis desautorizadas, entre outros.

Com isso, várias falhas podem ser encontradas no WEP, como descrito abaixo:

- **O Uso de Chaves WEP estáticas –** Vários usuários *wireless* utilizando uma chave idêntica, durante muito tempo, é um fator de risco. Se um computador, como um *laptop*, fosse roubado, a chave poderia tornar-se comprometida deixando todos os computadores que compartilham a mesma chave também comprometidos.
- **O IV (*initialization vector*) –** do WEP tem o campo com 24 bits na parte vazia da mensagem enviada. Esse campo de 24 bits, utilizado para iniciar a geração da chave pelo algoritmo RC4 é considerado pequeno para a criptografia. A reutilização do mesmo IV produz uma chave idêntica para a proteção dos dados e o tamanho pequeno, garante que ele repetirá com uma freqüência relativamente alta em uma rede ocupada. Mais ainda, o padrão 802.11 não especifica como os IVs são ajustados ou trocados, então dispositivos wireless de mesma marca podem gerar todos a mesma seqüência do IV e outros podem ter um IV constante. Como resultado, invasores podem gravar o tráfego da rede, determinar a chave e usá-la para decodificar os dados.
- **O Conhecimento Prévio –** O fato de um curioso saber que o IV de cada chave possui 24 bits, combinada com a fraqueza da chave RC4, leva a um ataque que recupera a chave após interceptar e analisar uma pequena quantidade de pacotes do tráfego.
- **A Integridade Não Criptografada –** O WEP não provê proteção de integridade criptografada. No entanto, o protocolo 802.11 MAC usa uma CRC não-criptografada para checar a integridade dos pacotes com a

correta soma de verificação (checksum). Essa combinação é considerada perigosa e freqüentemente leva a ataques não intencionais de “side channel”. Existe ainda um ataque ativo que permite ao atacante decodificar qualquer pacote por uma modificação sistemática dos pacotes e seus CRCs enviados para o AP. Esses tipos de ataques normalmente são súbitos e considera-se arriscado projetar protocolos de criptografia que não incluam proteção de integridade criptografada, por causa da possibilidade de interação com outros níveis de protocolo que podem deixar vazar informações sobre o texto cifrado.

Note que somente um dos problemas apontados acima depende da fraqueza do algoritmo de criptografia. Então, os outros problemas não seriam resolvidos, utilizando-se um método mais forte. O terceiro problema listado é, em parte, uma conseqüência da fraqueza do RC4, mas que só é exposta quando utilizado um protocolo com um projeto pobre.

Vulnerabilidades	Características
1. As características de segurança normalmente não são utilizadas.	Normalmente, as configurações de segurança não são postas em prática. Porém segurança fraca ainda é melhor que não ter segurança.
2. IVs são pequenas ou estáticas.	IVs de 24 bits permitem que a geração de chaves possa se repetir com uma certa freqüência. Esta repetição facilitará o trabalho de um invasor mais sofisticado.
3. As chaves de criptografia são pequenas.	Chaves de 40 bits são inadequadas para qualquer sistema. Normalmente, só é considerado aceitável chaves maiores que 80 bits.
4. As chaves de criptografia são compartilhadas.	Chaves que são compartilhadas podem comprometer o sistema. Um fator fundamental de segurança através de criptografia especifica que o segredo das chaves criptográficas é um ponto primordial para a segurança da rede.
5. As chaves de criptografia não podem ser atualizadas automaticamente.	As chaves de criptografia devem ser substituídas freqüentemente para evitar ataques do tipo força bruta.
6. RC4 tem uma chave fraca e é utilizado inapropriadamente no WEP.	A combinação de revelar a chave de 24 bits no IV e a fraqueza nos primeiros bytes da codificação RC4 pode levar a um ataque eficiente que recupera a chave.
7. A integridade do pacote é fraca.	CRC ou outro código linear de verificação de integridade são inadequados. A modificação da mensagem é possível, logo a criptografia dos dados é indicada.
8. Não ocorre autenticação do usuário.	Somente o dispositivo é autenticado. Então um dispositivo roubado poderá acessar a rede.

9. A Autenticação não é habilitada, somente uma verificação de SSID é feita.	Segurança através da identificação do SSID são altamente vulneráveis principalmente em sistemas *wireless*.
10. A autenticação do dispositivo é muito simples.	Resposta ao desafio em uma só direção para autenticação é vulnerável a ataques do tipo "*man-in-the-middle*". Autenticação mútua é mais indicada para verificar que o usuário e a rede são legítimos.

Tabela 3.4-1: Principais Problemas Existentes na Segurança do 802.11

3.5 Por que o WEP foi escolhido e implementado no padrão 802.11?

No momento em que o padrão 802.11 foi aprovado e finalizado, as indústrias de equipamentos para WLANs logo colocaram seus produtos no mercado. O padrão 802.11 especificava que fossem atendidos os seguintes critérios para segurança:

- Exportável;
- Razoavelmente forte;
- Auto sincronizável;
- Computacionalmente eficiente;
- Opcional.

O WEP responde a estes quesitos. Então, quando o WEP foi implementado, cabia a este assegurar algumas características de privacidade, controle de acesso, e integridade dos dados. Ou seja, não seria o WEP um responsável muito confiável para prover segurança efetiva a WLANs. Felizmente para as indústrias de equipamentos de WLAN, o método de comunicação *wireless* ganhou imensa popularidade, o que obrigou estas mesmas indústrias a procurarem soluções mais confiáveis para a segurança.

4 Tratamento da Segurança e Tipos de Ataques

A figura abaixo mostra um esquema de distribuição dos possíveis ataques a uma rede *wireless*.

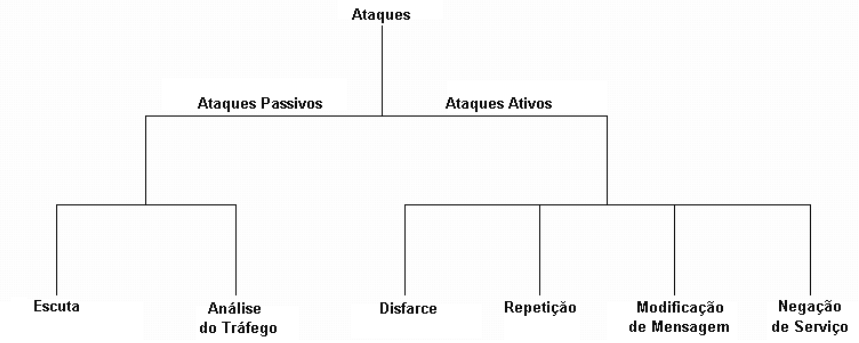

Figura 4-1: Tipos de Ataques

Como a figura mostra, os ataques são classificados em ataques passivos e ataques ativos. Esses dois grandes grupos são divididos em vários tipos de ataques. Todos definidos abaixo.

- **Ataque Passivo –** É um ataque no qual uma pessoa desautorizada obtém acesso a uma rede, mas não altera o conteúdo dos dados. Ataque passivo pode ser apenas a análise do tráfego da rede. Os dois tipos de ataques passivos são descritos abaixo.
  - **Escuta:** o atacante simplesmente monitora a transmissão para obter o conteúdo do que está sendo transmitido.
  - **Análise do Tráfego:** o atacante monitora a transmissão para entender os padrões de comunicação.
- **Ataque Ativo –** É um ataque no qual uma pessoa desautorizada obtém acesso a rede e modifica o conteúdo da mensagem que está sendo transmitida. Ataques ativos podem ser detectados, mas nem sempre impedidos. Um ataque deste tipo necessita que o atacante utilize algum dos recursos (ou a combinação deles) como: disfarce, repetição, modificação da mensagem ou negação de serviço.
  - **Disfarce:** o atacante personifica um usuário e com isso obtém alguns recursos desautorizados da rede.
  - **Repetição:** o atacante intercepta a transmissão e envia como se fosse o usuário legítimo.
  - **Modificação de Mensagem:** o atacante altera uma mensagem legítima, apagando, adicionando, editando ou reordenando a própria mensagem.
  - **Negação de Serviço:** o atacante dificulta o uso normal ou o gerenciamento dos dispositivos da rede.

Todos os riscos contra as WLAN 802.11 são resultados destes tipos de ataques. As conseqüências destes ataques incluem: perdas de informações proprietárias e perda dos serviços da rede, principalmente.

4.1 Perda de Privacidade

Privacidade é propriamente aquele tipo de informação da qual não se deseja que pessoas ou entidades desautorizadas tenham acesso ao conteúdo. Isto é, em geral, o fundamento básico de segurança requerido pelas organizações. Por causa da natureza dos sistemas *wireless*, privacidade é tipicamente um fator de dificuldade, por

que neste caso não é possível saber com precisão os limites da área em que a transmissão ocorre.

Logo, um adversário pode estar ouvindo o tráfego e com isso, obter informações sensíveis à rede como informações proprietárias, IDs da rede, senhas e configurações. Este risco está presente, pois o sinal do 802.11b pode alcançar espaços além do perímetro do prédio, facilitando o invasor. Portanto, intrusos podem potencialmente detectar transmissões estando no estacionamento ou em locais próximos. Esse tipo de ataque, com a utilização de analisadores de redes *wireless* que é popularmente conhecido como *sniffer*, é particularmente fácil por duas razões: 1) freqüentemente, características confidenciais de dispositivos utilizados na rede não estão bem guardadas e 2) conhecendo as inúmeras vulnerabilidades do 802.11b, o adversário conseguirá comprometer o sistema.

Analisadores de rede *wireless* (*sniffers*) como *AirSnort* e *WEPcrack*, são facilmente encontradas na Internet. O *AirSnort* foi uma das primeiras ferramentas criadas para automatizar o processo de análise das redes. Infelizmente, ela também é utilizada com o intuito de prejudicar as redes. O *AirSnort* pode tirar vantagem das falhas na marcação das chaves do algoritmo RC4, que é parte do padrão WEP. Para completar, esta ferramenta requer apenas um computador com o *Linux* instalado e uma placa de rede *wireless*. O programa monitora passivamente as informações transmitidas e calcula o valor da chave com pelo menos 100MB de pacotes colhidos na rede. Em uma rede bastante saturada, coletar esta quantidade de informação pode levar apenas 3 a 4 horas, já se o volume de informações for baixo, esta coleta deverá levar alguns dias. Depois dos pacotes serem colhidos, o programa demora aproximadamente um segundo para calcular o valor da chave fundamental. Uma vez que o invasor conheça a chave do administrador da rede, ele poderá ter acesso a qualquer pacote que esteja trafegando na rede. Pela facilidade com que se pode conseguir estes programas e utilizá-los, as implementações de segurança devem ser levadas bastante a sério.

Uma outra maneira na qual se pode perder privacidade será quando o invasor estiver monitorando a rede com um *laptop* e o AP ao invés de estar conectado a um *switch* estiver conectado a um *hub*. *Hubs*, normalmente, enviam todos os pacotes que chegam a ele por todas as suas portas (este processo é conhecido como *broadcast*), deixando o tráfego vulnerável a monitoramento desautorizado. Por exemplo, se um AP estiver conectado a um *hub* alguém poderia pegar informações endereçadas aos clientes *wireless*. Conseqüentemente, é viável imaginar que será mais seguro utilizar APs conectados a *switches*.

WLANs também estão expostas a ataques ativos através da perda de privacidade. Os programas citados anteriormente podem coletar dados como: nomes de usuários e senhas, com isso, o atacante poderá se fingir de usuário legítimo e ter acesso a dados da rede cabeada a partir da rede *wireless*.

Por último, um usuário malicioso poderia fisicamente inserir um AP qualquer dentro de um armário ou em baixo de uma mesa de conferência, por exemplo, e obter acesso à rede. Colocando este AP próximo ao usuário, ele poderia interceptar o tráfego entre o AP legítimo e o cliente, apenas colocando o sinal de seu AP mais forte que do AP legítimo. Ele também poderia ganhar acesso através do AP em redes que não necessitam de autorização de APs para se conectar a rede.

4.2 Perda de Integridade

As questões relacionadas a integridade dos dados em redes *wireless* são similares às de redes cabeadas. Freqüentemente, organizações implementam comunicações sem fio e com fio sem a proteção criptográfica adequada dos dados. Um invasor, por exemplo, pode comprometer a integridade dos dados, apagando ou modificando o conteúdo de um email em um sistema *wireless*. Dependendo da importância do e-mail e como esse e-mail será distribuído, o impacto pode ser bastante danoso a organização.

As características de segurança existentes no 802.11 não asseguram um controle rigoroso sobre a integridade dos dados. Como abordado anteriormente, a base do mecanismo de integridade do WEP é simplesmente um CRC linear. Ataques que modificam as informações transmitidas são possíveis sem o uso de mecanismos de verificação criptográfica.

4.3 Perda da Capacidade da Rede

A perda de capacidade da rede envolve normalmente uma forma de ataque conhecida como DoS (*Denial of Service*) ou *Jamming*. Este tipo de ataque ocorre quando um usuário malicioso envia um sinal deliberadamente a partir de um dispositivo *wireless* no intuito de sobrecarregar sinais legítimos. Isto resulta na quebra de conexão, por que os sinais legítimos estarão impedidos de se comunicar com a rede. Às vezes, usuários não maliciosos podem causar este tipo de ataque. Suponha que, por um instante, um usuário monopolize o sinal fazendo *download* de grandes arquivos, então ele estará efetivamente impedindo outros usuários de acessar a rede.

4.4 Outros Riscos

Com o aumento das redes *wireless*, usuários estão podendo se conectar a suas organizações através dessas redes. É comum ter em centros de conferências serviços de acesso a Internet através de WLANs. Desta forma, torna-se possível um usuário também se conectar a sua organização. Aeroportos também estão começando a oferecer este tipo de serviço. Porém, esta comodidade tem três riscos básicos: 1) por serem redes públicas, qualquer um pode ter acesso, até mesmo usuários maliciosos; 2) estas redes funcionam como *bridge* para uma rede do próprio usuário, assim, estas WLANs, potencialmente, permitem a qualquer um na rede pública ganhar acesso ou atacar a rede do próprio usuário e 3) elas utilizam altas potências de transmissão na faixa de RF (Radiofreqüência) para que todos possam alcançar o sinal. Todavia, isto também favorece que usuários maliciosos invadam a rede com mais facilidade.

Quando um usuário conecta-se a sua própria rede através de uma rede não confiável, esse pode gerar vulnerabilidades a rede de sua própria companhia. A não ser que esta companhia crie maneiras de proteger o usuário e a ela mesma. Como o usuário freqüentemente necessita acessar dados públicos ou privados de suas organizações é aconselhável que se utilize protocolos de proteção da camada de aplicação como o TLS (*Transport Layer Security*) e o SSL (*Secure Sockets Layer*). Para recursos privados a utilização de VPNs (*Virtual Private Network*) é mais adequada.

5 IEEE 802.11i: Um Novo Modelo de Segurança

Por causa das diversas falhas já apontadas sobre o WEP, um grupo foi formado para a elaboração do IEEE 802.11i, na tentativa de estabelecer uma solução mais efetiva para o problema de segurança em WLANs. Este grupo criou um padrão chamado de RSN (*Robust Security Network*). Este padrão inclui duas partes: o AES (*Advanced Encryption Standard*) para criptografia do tráfego nas WLANs; e o IEEE 802.1X (Padrão de Autenticação baseado em Portas na Rede) para autenticação de usuário e gerenciamento da chave criptográfica.

Este mesmo grupo, também recomendou uma série de mudanças para o WEP com o intuito de compatibilizar produtos 802.11b que não suportam as atualizações do AES pela suas limitações de projeto. Estas modificações constituem o TKIP (*Temporal Key Integrity Protocol*).

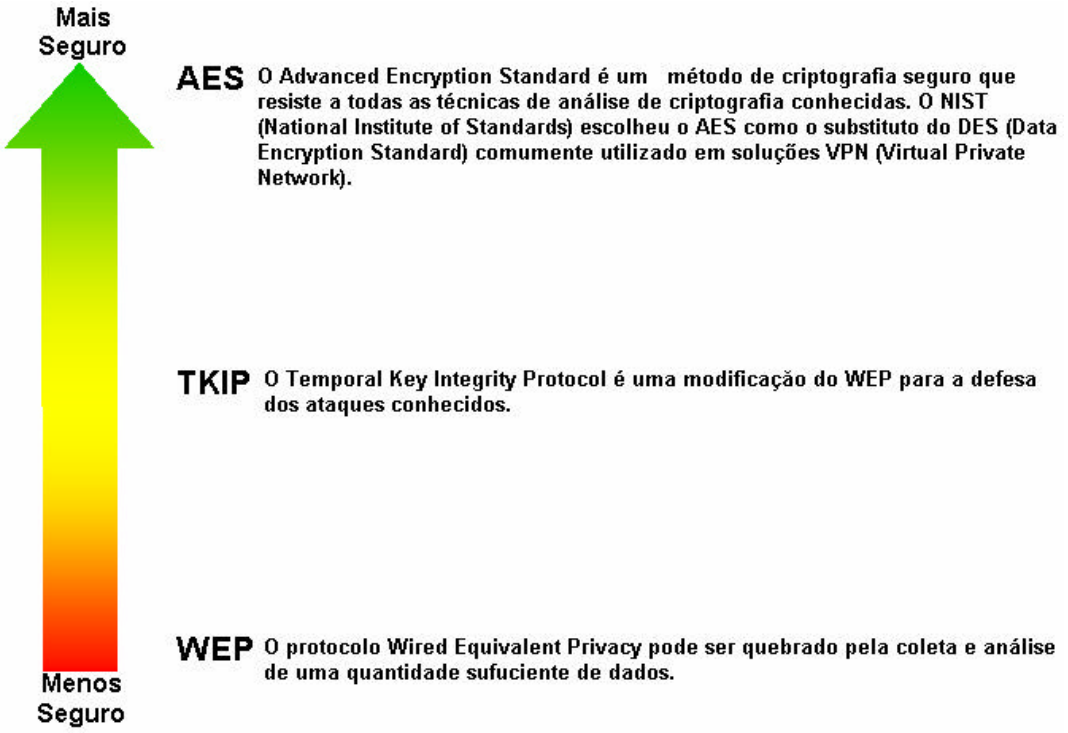

Figura 5-1: Os Diferentes Tipos de Criptografia

É importante citar, que para acomodar uma mistura de vários métodos de criptografia na mesma WLAN, a especificação 802.11i requer que dispositivos avisem aos APs e estações associadas a WLAN sobre suas capacidades de criptografia. Os APs e as estações então escolherão a criptografia apropriada com base na capacidade mútua entre eles.

5.1 Criptografia AES

A comunidade internacional de criptografia participou intensamente nas pesquisas do IEEE 802.11i para a elaboração de um algoritmo de criptografia e selecionou o AES, pois ele resiste a todas as técnicas conhecidas de análises criptográficas. De fato, o AES é considerado por profissionais de criptografia como o substituto do DES (*Data Encryption Standard*) que é comumente utilizado em VPN, soluções de bancos e uma variedade de outras aplicações sensíveis à segurança. Este padrão pode ter chaves dos seguintes tamanhos:

- 128 bits;
- 192 bits;
- 256 bits.

5.2 Criptografia TKIP

Como apresentado anteriormente, o grupo de elaboração do IEEE 802.11i sugeriu várias modificações para as deficiências do WEP para que ele pudesse suportar os produtos já existentes com padrão 802.11b. Uma consideração importante para a maioria dos produtos 802.11b é que eles normalmente utilizam processamento de baixa velocidade e limitações para grandes processamentos computacionais de segurança. Trabalhando dentro destas condições, o grupo formulou o TKIP como uma solução de criptografia que oferece um razoável compromisso entre a adição de segurança e as limitações de processamento dos produtos 802.11b.

O TKIP conserta quatro partes do algoritmo WEP:

- Uma Mensagem de Checagem de Integridade (MIC) referida em especificações como “Michael”;
- Uma contagem que apaga a autenticação existente e a chave de criptografia quando um ataque é detectado;
- Uma função de mistura de chave por pacote;
- Proteção de Revisão.

É importante notar que o TKIP não provê o mesmo nível de segurança do AES. Mesmo assim, a especificação do 802.11i coloca claramente: “Por causa da fraqueza, o IEEE 802.11 recomenda a não utilização do TKIP exceto como uma atualização para o equipamento pré-RSN”.

5.3 Autenticação 802.1X

Para complementar o AES do RSN na criptografia dos dados, o grupo do IEEE 802.11i especificou o 802.1X para autenticação do usuário. O 802.1X é um padrão aberto para autenticação de estações *wireless* com o Servidor de Autenticação na rede cabeada por meio de um AP. O Servidor de Autenticação é geralmente o mesmo utilizado por corporações para autenticar usuários remotos, ou seja, o RADIUS (*Remote Authentication Dial-In User Service*).

O 802.1X é baseado no EAPoL (*Extensible Authentication Protocol over LAN*) do IETF (*Internet Engineering Task Force*) e há um número grande de algoritmos de autenticação do EAPoL que podem ser utilizados. Os tipos mais comuns de autenticação implementadas incluem o EAP-MD5, EAP-TLS, EAP-TTLS, LEAP e PEAP.

Tipo de Autenticação EAP	Comentário
EAP-MD5 (Message Digest 5)	EAP-MD5 é um método de autenticação baseado em senha, que é raramente utilizado, pois não garante um mecanismo eficaz para a troca de chaves novas.
EAP-TLS (Transport Layer Security)	EAP-TLS pode ser um pouco complicado de se configurar, mas não tem tantas fraquezas em sua segurança. Ele requer o uso de um servidor RADIUS e certificado digital tanto na estação quanto no servidor.
LEAP (EAP Cisco Wireless)	LEAP fornece uma boa maneira para assegurar redes *wireless* enquanto ainda utiliza dispositivos do WEP. Ele consiste em uma autenticação mútua baseada em senha com um servidor RADIUS e constantemente modifica as chaves WEP para impedir invasores de descobrirem a chave. No entanto, apesar de muitas estações suportarem o LEAP, o AP necessita ser da *Cisco Systems*.
EAP-TTLS (*Tunneled* TLS)	EAP-TTLS e PEAP são similares ao tipo de autenticação EAP e são suportados por várias marcas de produtos WLAN. Estes protocolos utilizam certificados digitais assim como o EAP-TLS, porém requerem autenticação apenas no servidor RADIUS. A estação autentica o servidor RADIUS e um túnel seguro é então estabelecido entre a estação e o servidor através do qual o servidor RADIUS poderá autenticar a estação.
PEAP (*Protected* EAP)	

Tabela 5.3-1: Os Vários Tipos de Algoritmos de Criptografia EAP

Quando uma estação tenta se conectar a uma WLAN com 802.1X, o AP autoriza a estação a se conectar, porém força a estação a um estado não autorizado no qual somente o tráfego do EAP é passado pelo servidor RADIUS. Utilizando mensagens EAP ou mesmo senhas ou chaves públicas/privadas de criptografia, o servidor RADIUS autentica a estação. O servidor RADIUS então envia ao AP uma chave inicial de criptografia, que veio da estação através do processo de autenticação. O AP gera então uma segunda chave para o uso na comunicação com a estação, faz a criptografia da segunda chave com a chave inicial advinda do servidor RADIUS e envia de volta a estação. Em seguida, o AP envia novas chaves a estação com intervalos de tempo pré-definidos para assegurar que a segurança não foi quebrada.

Pré-supondo que não se conhecem técnicas para quebrar a criptografia AES, não se sabe quando será necessário atualizar as sessões de chaves AES em bases regulares. No entanto, a geração automática das sessões de chaves não elimina a necessidade de configurar manualmente cada estação com uma chave e não elimina a necessidade de se ter certeza de que cada AP tem uma lista atualizada das chaves individuais de cada usuário.

5.4 Alternativas a Utilização do 802.11i

Por causa dos interesses conflitantes no mercado de WLANs, ocorreu um atraso para a finalização do IEEE 802.11i. Como resultado, muitas empresas se adiantaram para elaborar sistemas de proteção mais eficientes que o WEP. As duas alternativas mais promissoras foram da *Cisco Systems* e da *Wi-Fi Alliance* (formalmente conhecido como *Wireless Ethernet CompatibilityAlliance* ou WECA).

5.4.1 LEAP – EAP Cisco *Wireless*

Em dezembro de 2000, a *Cisco Systems* introduziu o LEAP para compensar os problemas de segurança do WEP. O LEAP ainda confia na criptografia do WEP, porém adiciona a autenticação do usuário e a funcionalidade da atualização das chaves. Com este modelo, o usuário será autenticado através de um servidor RADIUS da *Cisco* e as chaves serão atualizadas com bases regulares.

Por causa da grande pressão sobre as falhas do WEP e a confiabilidade no nome *Cisco*, o LEAP teve um grande sucesso no mercado de WLANs. No entanto, o protocolo LEAP é compatível somente com APs da própria *Cisco*. Outra característica importante refere-se ao fato de com o LEAP, as estações necessitam de senhas para serem autenticadas. Isto recai em possíveis ataques de dicionário, em que o invasor tenta descobrir a chave WEP gravando uma série de quadros e então com um programa ele tenta descobrir senhas através de tentativas. Esta possibilidade obriga que se tenham senhas muito grandes e complexas para diminuir o risco.

5.4.2 WPA – *Wi-Fi Protected Access*

A *Wi-Fi Alliance* tem elaborado um novo padrão chamado de *Wi-Fi Protected Access* (WPA). Este novo padrão é sugerido para equipamentos pré-802.11i, porém não é requerido como parte do padrão 802.11i. Os produtos que implementaram o WPA têm suporte para WEP, TKIP e autenticação de usuários 802.1X.

No caso de usuários domésticos que não possuem um servidor de autenticação RADIUS, o WPA oferece um mecanismo de *Pré-Shared Key* (PSK). Para utilizar o PSK, é colocada uma “expressão de passe” tanto no AP, quanto na estação. Esta expressão é usada para autenticar qualquer estação que tente se conectar. Em seguida, a estação recebe do AP uma chave para aquela sessão. Esta chave é atualizada em intervalos regulares.

Diferentemente do WEP, o WPA utiliza um vetor de inicialização (IV) de 48bits, além de regras de seqüência.

No entanto, algumas características devem ser observadas, como: o suporte para o WPA em estações e APs 802.11b requer uma atualização por *software*. Porém,

estas atualizações são evitadas por serem difíceis e pelo risco que há de estragar o aparelho.

Finalmente, a capacidade de negociação cifrada do WPA permite que clientes baseados no WEP possam operar em uma rede misturada WEP/ WPA.

6 Filtros: Aumentando a Segurança em WLANs

A utilização de filtros pode ser utilizada como adição a segurança com o WEP e/ou AES. Filtrar significa manter de fora quem não for autorizado e permitir quem for autorizado, através do método de filtragem. Existem três tipos básicos de filtros:

- Filtro de SSID;
- Filtro de Endereço MAC;
- Filtro de Protocolos.

As próximas seções farão a explicação de cada um dos métodos de filtragem listados.

6.1 Filtro de SSID

Filtro do SSID é um método rudimentar de filtragem, e que somente deverá ser utilizado como método básico de controle de acesso. O SSID é apenas um termo que caracteriza o nome da rede. Logo, um dispositivo que deseja se comunicar com uma determinada rede deverá conhecer o nome da rede para ter acesso. Porém, com a utilização de um *sniffer* é muito fácil descobrir o SSID de uma rede, visto que os APs enviam de tempos em tempos este SSID para que seus clientes possam se comunicar. Por isso, este método é considerado fraco quando se deseja manter usuários não-autorizados fora da rede.

Em determinados casos, é possível fazer com que os APs não enviem o SSID, contudo os clientes deverão ter os SSIDs configurados manualmente.

6.2 Filtro de Endereço MAC

WLANs podem filtrar estações clientes baseadas no endereço MAC destas estações. Neste caso, quando uma estação cliente tentar se conectar a rede, seu endereço MAC será verificado na lista dos endereços permitidos pelo AP e se coincidir com alguma das entradas, será permitido o acesso, por outro lado se não houver coincidência, esta estação estará impedida de se comunicar com a rede.

Obviamente, a inserção dos endereços MAC que poderão acessar a rede terá que ser feita manualmente em cada AP, desta forma este método é impraticável

quando tratamos de grandes redes ou redes na qual não temos certeza sobre quais serão os usuários.

Filtro de endereço MAC também tem seus defeitos. Suponha que um funcionário de uma empresa que possua um *laptop* e que tenha acesso a WLAN da empresa fosse roubado. Se este *laptop* for utilizado por um invasor, ele terá acesso a rede da empresa. Portanto, será necessário que os funcionários avisem quando houver a perda de um componente da rede. Outro problema acontecerá se um invasor forjar um endereço MAC válido para a rede, depois de utilizar um *sniffer*.

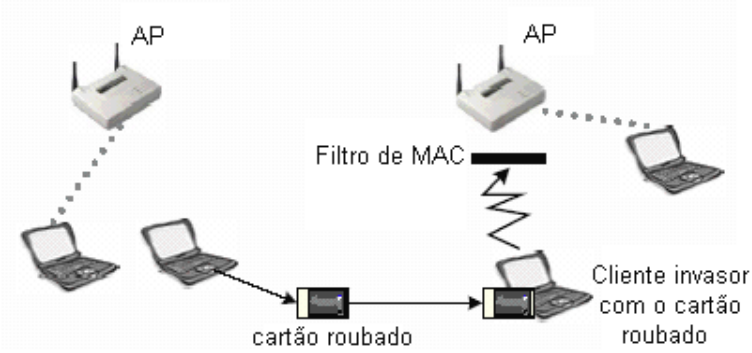

Figura 6.2-1: Funcionamento do Filtro MAC

6.3 Filtro de Protocolos

WLANs podem filtrar pacotes que atravessam a rede com base no protocolo. Suponha uma rede que tenha com função única fornecer acesso a internet para seus usuários. Logo, filtrar os pacote e deixar que somente os protocolos SMTP, POP3, HTTP, HTTPS, FTP possam ser utilizados será a solução mais eficaz para proteger os servidores internos da empresa, por exemplo.

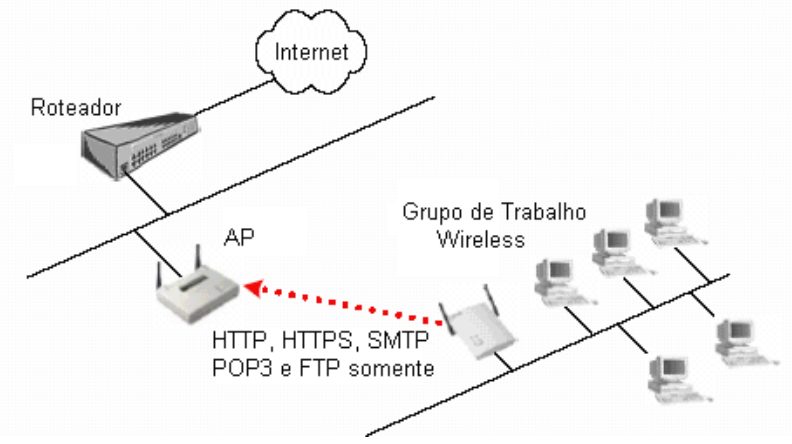

Figura 6.3-1: Funcionamento do Filtro de Protocolos

7 VPN: Aplicando Túneis a WLANs

A VPN (*virtual private network*) é uma tecnologia que vem crescendo rapidamente para garantir a segurança dos dados transmitidos através de redes públicas. Atualmente, as VPNs tem sido utilizada em três diferentes cenários: para acesso de usuário remoto, para conectividade de LAN com LAN e para as chamadas *extranets*. VPNs empregam a técnica de criptografia para proteger as informações do IP enquanto ele passa de uma rede para outra. A informação que está dentro do túnel VPN (o encapsulamento de um protocolo dentro de outro) é criptografada e isolada de outro tráfego da rede.

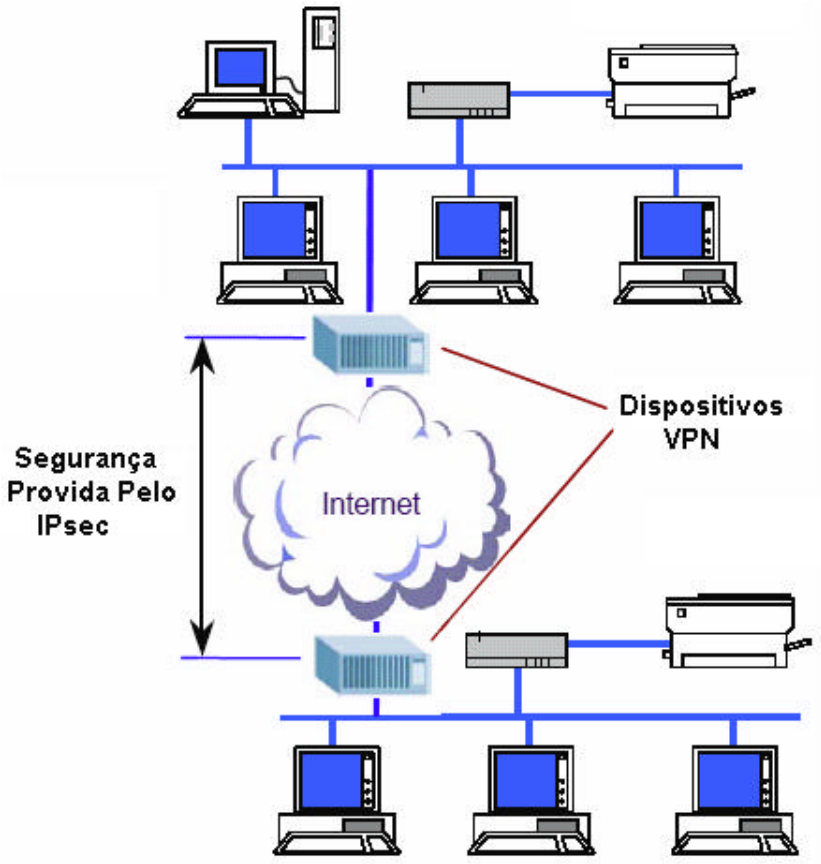

Figura 7-1: Uso Típico de VPN para Segurança da Comunicação via Internet

A maioria das VPNs utilizam o protocolo IPsec (*Internet Protocol Security*). Este protocolo, desenvolvido pelo IETF, provê os seguintes tipos de proteção:

- Privacidade;
- Integridade sem conexão;
- Autenticação da informação de origem;
- Proteção de revisão;

- Proteção pela análise do tráfego.

Privacidade assegura que outros não possam ler as informações contidas nas mensagens enviadas. A integridade sem conexão garante que a mensagem recebida não foi alterada em relação a mensagem original. Autenticação da informação de origem garante que a mensagem recebida foi realmente enviada pelo remetente de origem e não por alguém que tenha personificado o remetente de origem. A proteção de revisão provê a certeza de que a mensagem não tenha sido enviada várias vezes e que não esteja fora de ordem ao chegar ao destino. A proteção pela análise do tráfego assegura que um atacante utilizando a técnica de escuta não possa determinar quem está se comunicando ou a freqüência ou o volume das comunicações.

O IPsec complementa ainda a tarefa de roteamento das mensagens através de um túnel criptografado por dois cabeçalhos IPsec inseridos imediatamente depois do cabeçalho IP de cada mensagem. O cabeçalho do ESP (*Encapsulating Security Protocol*) garante privacidade e proteção contra modificações maliciosas. O protocolo IKE (*Internet Key Exchange*) é um mecanismo que permite que chaves secretas e outros parâmetros de proteção sejam trocados previamente a comunicação sem a intervenção do usuário.

A utilização do IPsec em WLANs é mostrada na figura a seguir.

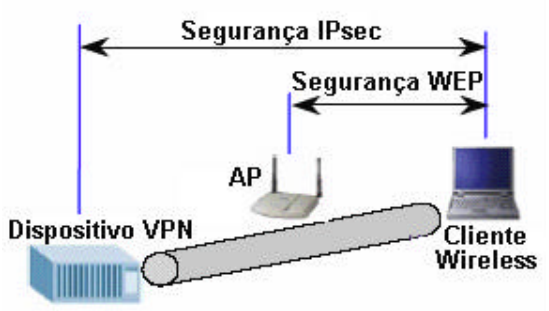

Figura 7-2: Segurança VPN em Adição ao WEP

O túnel IPsec é formado pelo cliente *wireless* através do AP para um dispositivo VPN da rede. Com o IPsec, os serviços de segurança passam a ser feitos na camada de rede. Isto significa que todos os protocolos de camada superior passarão a ser protegidos pelo IPsec. Porém, o serviço de segurança da camada de enlace, o WEP, será independente do IPsec. Portanto, será possível a utilização conjunta do WEP com o IPsec.

A próxima figura ilustra um outro exemplo de uma rede *wireless* com a utilização de VPN. Como mostrado, com a utilização de dispositivos *wireless* e VPNs, clientes podem se conectar a rede de forma segura através de um *gateway* VPN em adição ou substituição ao WEP. Note que o cliente *wireless* não necessita de nenhum

hardware especial, ele só precisa do *software* cliente IPsec/VPN. O *gateway* VPN pode utilizar chaves de criptografia pré-compartilhada ou certificados digitais para a autenticação do usuário *wireless*. Adicionalmente, a autenticação do cliente *wireless* pode ser feita através de um servidor RADIUS.

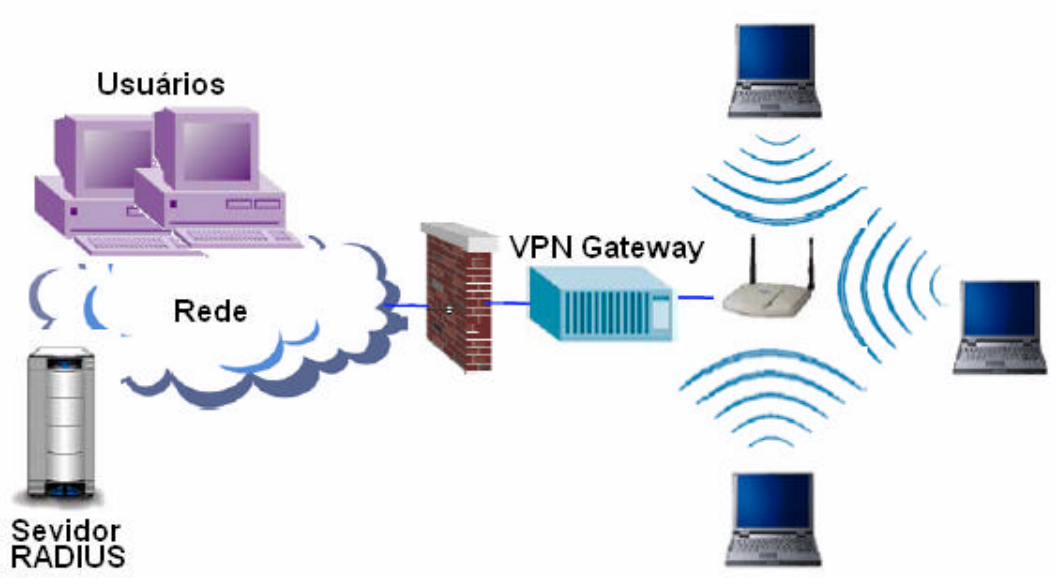

Figura 7-3: Diagrama Simplificado de uma VPN em uma WLAN

É importante notar que apesar das VPNs representarem uma significante melhoria quanto à segurança na parte *wireless* da rede, ela não pode ser considerada solução única, capaz de resolver todos os problemas relativos à segurança.

8 Conclusão

A crescente necessidade de mobilidade tem possibilitado o aumento na procura por dispositivos de comunicação sem fio. Por conta disto, aumenta-se também a preocupação com a segurança do conteúdo que é transmitido pelo ar. Conseqüentemente, muitas empresas e institutos de pesquisas vêm procurando aperfeiçoar os métodos de transmissão e recepção tanto para torná-los mais eficientes quanto mais seguros.

O IEEE, principal responsável pela padronização do sistema de comunicação, é quem estabelece as características para a compatibilidade e segurança da comunicação entre dispositivos. Contudo, o aspecto relativo à segurança sempre causou dúvidas quanto a sua eficácia neste tipo de comunicação. Sabe-se atualmente que o WEP, primeiro padrão de segurança criado para este tipo de rede, não provê uma garantia real de que os dados transmitidos não possam ser descobertos, o que gera dúvidas quanto a sua utilização.

Por causa disso, muitas empresas se anteciparam em criar métodos mais seguros e assim surgiu o WPA, um padrão que vem sendo a solução para muitos casos enquanto produtos com suporte completo ao padrão IEEE 802.11i não são comercializados.

Portanto, é importante notar que o futuro deste tipo de rede está relacionado diretamente à necessidade e à confiança das pessoas em se comunicarem aonde quer que elas estejam, de forma instantânea e com a segurança de que seus dados estarão protegidos de pessoas maliciosas.

Anexo A – Configurações de Segurança

Este anexo tem o intuito de aplicar os conceitos descritos e explicar de que forma pode-se implementar a teoria apresentada na prática.

Inicialmente, dividiremos o processo em duas partes: a primeira relativa às configurações de segurança em estações clientes que possuam acesso a rede *wireless*; a segunda fará referência às configurações gerais em um AP.

A.1 Configurações de Segurança em Estações Clientes

Normalmente, as configurações relativas à segurança em estações são coordenadas pelo *software* de instalação da placa de rede *wireless*. As configurações podem variar dependendo da marca do fabricante ou modelo da placa. A figura A.1-1 mostra a tela do *software* de configuração de uma placa PCI *wireless* da SMC, modelo SMC2802W.

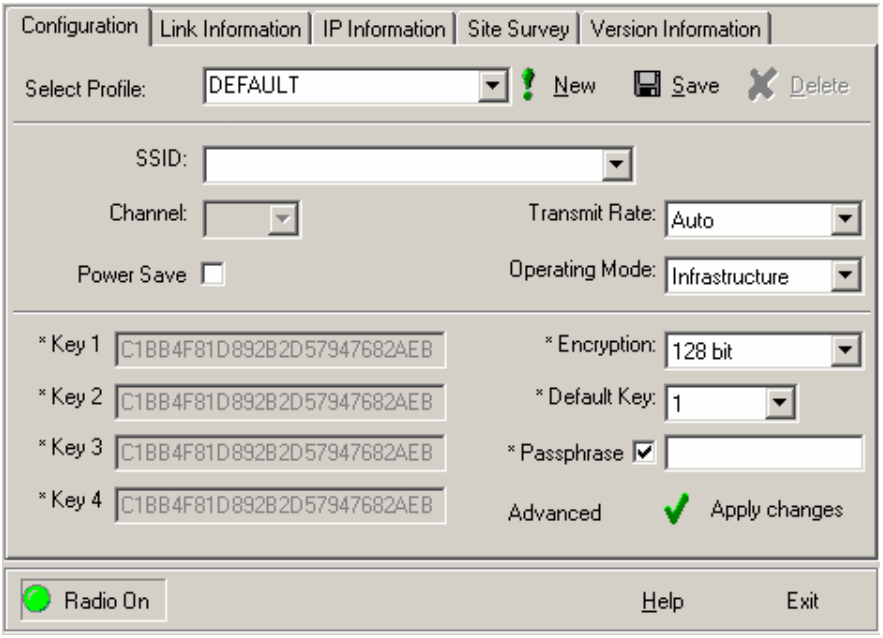

Figura A.1-1: Configuração de Estação Cliente

No campo SSID, deve-se colocar o SSID atual da rede, ou seja, o mesmo nome que estiver configurado no AP.

O campo *Channel* especifica qual o canal de comunicação que deverá estar ativo para a comunicação da estação com o AP.

O campo *Transmit Rate* mostra a taxa de transmissão escolhida. *Auto* significa que a estação e o AP estabelecerão automaticamente qual será a taxa de transmissão.

Operating Mode permite duas opções: Infra-estrutura ou *Ad-hoc*.

Encryption refere-se ao nível de encriptação do WEP.

O campo *Passphrase* permite que se crie chaves (Key 1, Key 2, Key 3, Key 4) a partir de uma palavra e que pode conter também números e símbolos. Também é possível se inserir manualmente as chaves.

A.2 Configurações de Segurança em *Access Point*

As configurações de segurança em um AP podem variar dependendo do modelo ou marca do dispositivo. Sendo assim, alguns modelos possuem opções de configuração que outros não possuem. Porém, algumas características poderão ser apontadas, pois são consideradas básicas para segurança em qualquer AP de qualquer marca.

As figuras que virão a seguir foram capturadas a partir das telas de configuração de um AP da marca SMC, modelo SMC2804WBR. Através delas será possível mostrar com mais clareza as configurações de segurança em um AP.

A configuração do SSID, por exemplo, é pré-requisito para o funcionamento adequado de qualquer rede *wireless*.

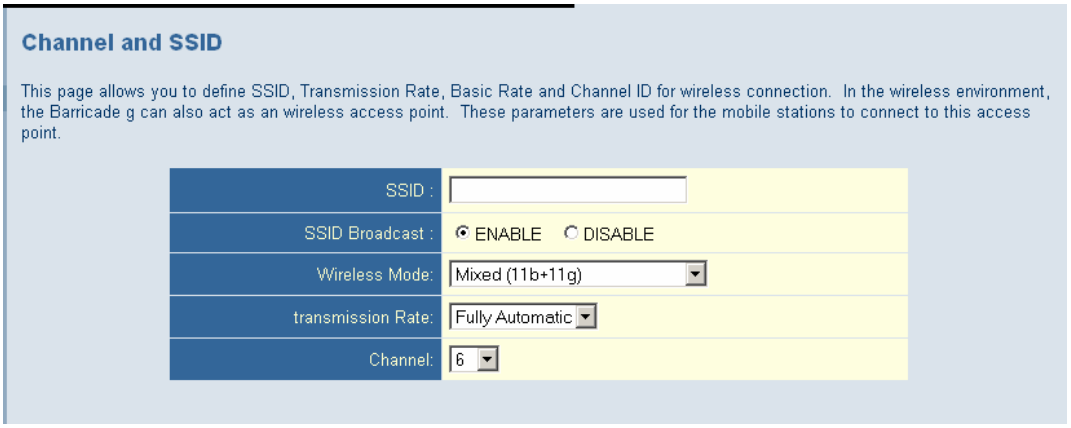

Figura A.2-1: Canal e SSID

O primeiro campo da figura A.2-1, especifica o SSID (um “nome” para a rede), o campo logo abaixo se refere a opção do possível *broadcast* do SSID para os clientes da rede *wireless*. Esta opção deve ser avaliada com cautela antes de se optar por deixá-la habilitada conforme o padrão. Caso, a rede *wireless* tenha clientes (estações) fixos e previamente conhecidos, será interessante desabilitar a opção e configurar todos os clientes manualmente, pois o conhecimento do SSID, apesar de não ser um fator primordial para uma invasão, é um primeiro passo para se invadir este tipo de rede. Contudo, existem situações em que será indicado habilitar esta função, como em redes públicas em geral. Neste caso, como não se conhece o cliente que estará acessando a rede, o envio automático do SSID facilitará o gerenciamento da rede.

O campo *Wireless Mode* indica que este AP está preparado para se associar a estações que sejam do padrão 802.11b ou 802.11g. Dentro desta opção pode-se ainda escolher por apenas um dos padrões.

O campo *Transmission Rate* determina que a taxa de transmissão está configurada para ser automática, então o AP e a estação conectada estabelecerão a que taxa irão transmitir. Opção bastante razoável, visto que este AP pode associar-se com os padrões 802.11b (taxa máxima 11Mbps) e 802.11g (taxa máxima 54Mbps) ao mesmo tempo.

O campo *Channel* especifica qual será o canal de freqüência para transmissão. É importante lembrar que o mesmo canal que estiver configurado o AP terá que estar configurada as estações. Atualmente existem *softwares* que buscam automaticamente os canais disponíveis para as estações se conectarem. Contudo, se existirem redes que estejam disponíveis em canais diferentes, terá que ser feita a escolha de um canal para àquela interface de rede.

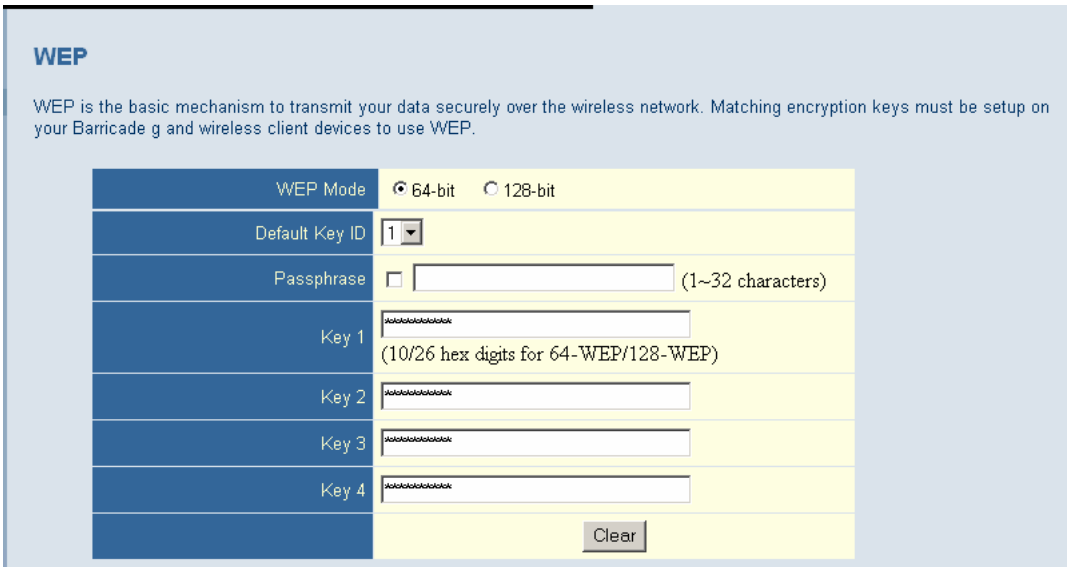

Figura A.2-2: WEP

O primeiro campo da figura A.2-2 especifica o nível de criptografia se o WEP for ativado. Recomenda-se o uso de 128 bits, pois dificultará um ataque passivo de escuta. Deve-se lembrar que as estações terão que estar configuradas com o mesmo nível de criptografia dos APs, caso contrário, as estações não conseguirão se associar aos APs.

O campo *passphrase* é responsável por gerar as chaves: Key 1, Key 2, Key 3 e Key 4 através de uma palavra que é colocada no próprio campo. A inserção das

chaves também poderá ser manual. Novamente, com o WEP ativado, as chaves terão que ser idênticas no AP e nas estações.

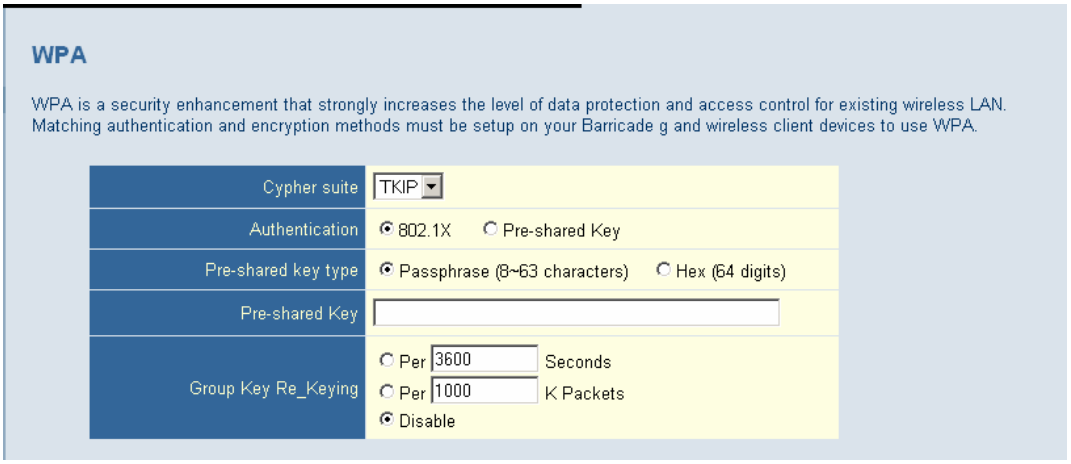

Figura A.2-3: WPA

Quando se deseja aumentar o nível de segurança, o WPA é uma boa opção. O campo *Cypher suite* da figura A.2-3 especifica o TKIP como opção de segurança, que é certamente mais indicado do que WEP.

O campo *Authentication* mostra duas opções: 802.1X e chave pré-compartilhada. A primeira opção necessita de um servidor de autenticação como o RADIUS, já a segunda não. Assim como no WEP, neste caso, pode-se colocar a chave pré-compartilhada através do *passphrase* ou em dígitos hexadecimais.

O campo *Group Key Re_Keying* especifica o tempo em que será mantida a mesma chave: por segundo, por quantidade de dados (pacotes) ou nunca mudar a chave.

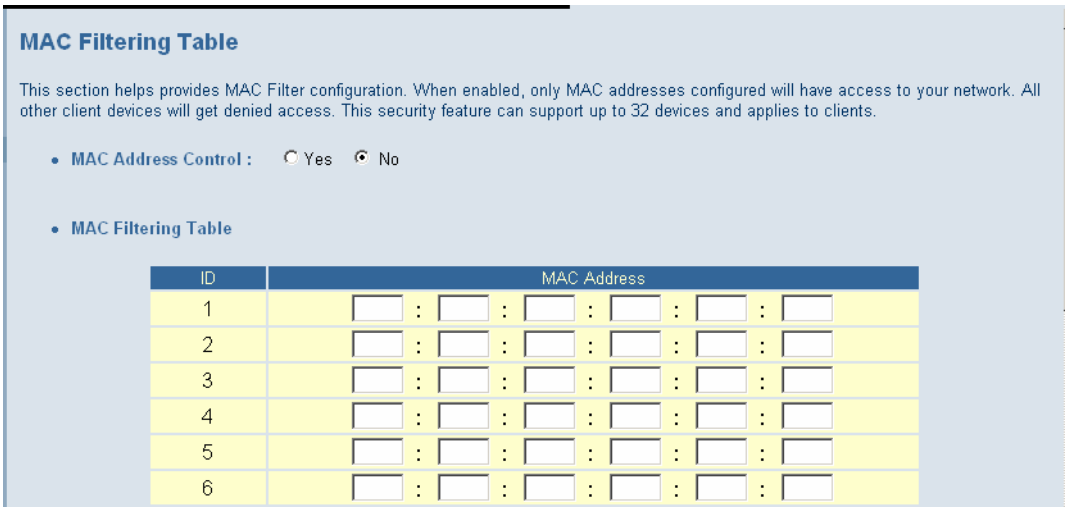

Figura A.2-4: Tabela do Filtro de Endereço MAC

Uma opção importante que também poderá ser utilizada como complemento a segurança é o Filtro de Endereço MAC. Na tabela, mostrada pela figura A.2-4 são colocados os endereços MAC de estações que poderão se conectar a rede, então somente os endereços MAC relacionados na lista poderão associar-se ao AP. O número máximo de estações na lista do filtro de endereço MAC varia dependendo do AP. Assim como no caso do SSID, em uma rede pública, o filtro de endereço MAC dificilmente será uma solução.

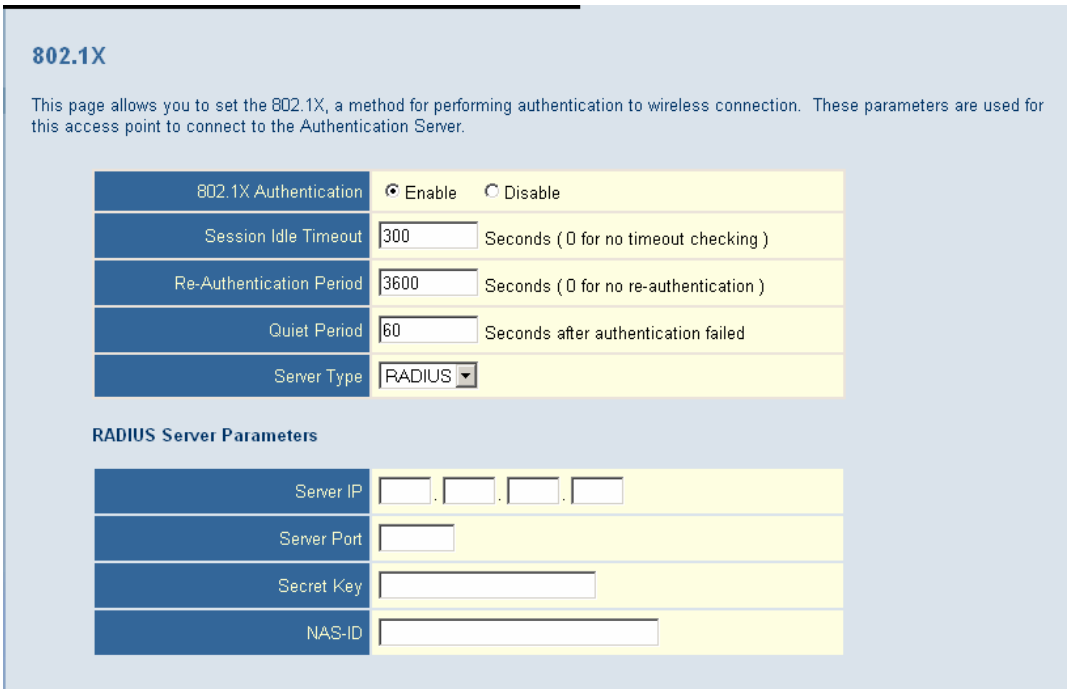

Figura A.2-4: 802.1X

A configuração que assegura a autenticação das estações, ou seja, a que afirma que as estações que estão conectadas possam estar conectadas é tratada pelo 802.1X. Este método é o mais comum para este tipo de autenticação e é feito através de um Servidor RADIUS.

Na figura A.2-4, o campo *Session Idle Timeout* especifica o tempo que uma sessão será colocada como inativa antes de ser terminada.

O campo *Re-Authentication Period* estabelece por quanto tempo uma estação ficará autenticada até que tenha que fazer uma nova autenticação.

O campo *Quiet Period* estabelece o tempo que o AP irá esperar após a falha de uma autenticação até uma nova tentativa.

Os parâmetros do Servidor RADIUS se referem ao IP do servidor e a porta de comunicação do AP com o servidor para a autenticação das estações clientes.

Glossário

AES ***A****dvanced* ***E****ncryption* ***S****tandard*	Algoritmo de criptografia selecionado pelo grupo elaborador do IEEE 802.11i para fornecer uma segurança robusta em redes *wireless*.
AP ***A****ccess* ***P****oint*	Dispositivo que garante um ponto de acesso a rede cabeada para estações da rede *wireless*.
Atacante	Pessoa mal intencionada que lança ataques a uma rede com o intuito de invadi-la ou simplesmente causar a paralisação da própria rede.
Bridge	Dispositivo de rede que filtra os dados que interessam ao segmento de rede em que a *bridge* estiver instalada.
Broadcast	Envio de mensagem para todas as estações de uma rede.
BSS ***B****asic* ***S****ervice* ***S****et*	Topologia mais básica de uma rede *wireless*. Consiste de vários *hosts* com um *access point* interligando-os.
Certificado Digital	Mensagem eletrônica que verifica a identidade do usuário e que pode ser utilizado para codificar dados transmitidos. A mensagem enviada é codificada com uma chave privada, o receptor decodifica a mensagem com a chave pública enviada. A chave de codificação pública/privada é assimétrica, logo o dado codificado com a chave privada só poderá ser decodificado com a chave pública e vice-versa.
Criptografia	Técnica de embaralhar os dados transmitidos no intuito de manter a privacidade.
DES ***D****ata* ***E****ncrytion* ***S****tandard*	Algoritmo de criptografia utilizado para proteger os dados quando transmitido através de redes inseguras.
DoS ***D****enial* ***o****f* ***S****ervice*	Ataque de negação de serviço. O atacante tenta paralisar o funcionamento da rede. Este ataque também é conhecido como *Jamming.*
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*.
EAP ***E****xtensible* ***A****uthentication* ***P****rotocol*	Protocolo geral para autenticação, podendo utilizar inúmeros métodos de autenticação, como servidores RADIUS.
ESP ***E****ncapsulating* ***S****ecurity* ***P****rotocol*	Protocolo de Segurança no Encapsulamento, provê privacidade e proteção contra modificações maliciosas.
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.
Gateway VPN	Porta de comunicação com um dispositivo VPN.
Hub	Dispositivo de rede semelhante a um repetidor, porém com mais de uma porta de saída.
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.
IPsec ***I****nternet* ***P****rotocol* ***Sec****urity*	Protocolo de Segurança da Internet, suporta troca segura de pacotes. Sua utilização é comum em aplicações de VPN.
Jamming	Ver DoS.
MAC ***M****edia* ***A****ccess* ***C****ontrol*	Endereço físico de um dispositivo de rede.
MIT ***M****assachusetts* ***I****nstitute of* ***T****echnology*	Instituto de Tecnologia de Massachusetts.
NIC ***N****etwork* ***I****nterface* ***C****ard*	Placa com circuito impresso ou cartão que é instalada ao computador para fornecer conectividade entre o computador e a rede.
Notebook	Computador compacto e portátil.
NULL Authentication	Autenticação na qual o cliente não precisa conhecer a identidade da rede (SSID) para se conectar.
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 portátil que une características de PC, Internet e rede.
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	Algoritmo de criptografia que utiliza um vetor de inicialização de 28 bits e uma chave secreta compartilhada de 40 ou 104 bits.
Sniffer	*Software* que coleta dados do tráfego da rede para posterior análise.

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.
String	Variável que armazena caracteres.
TKIP ***T****emporal* ***K****ey* ***I****ntegrity* ***P****rotocol*	Tipo de protocolo de segurança que utiliza chaves temporárias de criptografia.
VPN ***V****irtual* ***P****rivate* ***N****etwork*	Rede Privada Virtual. Rede de comunicação privada estabelecida sobre uma rede pública.
WEP ***W****ired* ***E****quivalent* ***P****rivacy*	Protocolo de segurança definido no padrão 802.11 que tem como finalidade fornecer o mesmo nível de segurança presente em redes cabeadas.
Wi-fi ***Wi****reless* ***Fi****delity*	Sigla que faz uma referência genérica a rede *wireless* do padrão 802.11.
WLAN ***W****ireless* ***L****ocal* ***A****rea* ***N****etwork*	Tipo de rede local que utiliza 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 uma atualização de software.

Referências Bibliográficas

[1] Karygiannis, T. e Owens, L. "Wireless Network Security." *802.11, Bluetooth™ and Handheld Devices*, Special Publication 800-48. NIST – National Institute of Standards and Technology.

[2] "CWNA - Certified Wireless Network Administrator™." *Official Study Guide.*

[3] "Building Secure Wireless Networks." *How Atheros Defines Wireless Network*, Security Today And In The Future. Atheros® Communications.

[4] Barcelos, J.P.M. e Gonçalves, R.G. e Alves Jr., N. "O Padrão 802.11." *Nota Técnica CBPF-NT-003/03*.

[5] Klein, M. "Wireless Network Security." *Executive Briefing*. Interlink Networks.

[6] Alves Jr., N. e da Silva, S. L. P. "Introdução às Redes Wireless." *Nota Técnica CBPF-NT-003/02.*

[7] Maxim, M. e Pollino, D. "Wireless Security." *Capítulo 2 – Wireless Threats.* McGraw-Hill Companies.