UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDE

NADIA AL-BDYWOUI MENDES

# ANÁLISE DE DESEMPENHO DE REDES SEM FIO BASEADA EM MECANISMOS DE CRIPTOGRAFIA

MONOGRAFIA

CURITIBA
2011

NADIA AL-BDYWOUI MENDES

# ANÁLISE DE DESEMPENHO DE REDES SEM FIO BASEADA EM MECANISMOS DE CRIPTOGRAFIA

Monografia apresentada como requisito parcial para obtenção do grau de Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Rede, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Me. Fabiano Scriptore de Carvalho

CURITIBA

2011

## RESUMO

MENDES, Nadia Al-Bdywoui. **Análise de Desempenho de Redes Sem Fio Baseada em Mecanismos de Criptografia.** 2011. 48 f. Monografia de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Rede, Universidade Tecnológica Federal do Paraná, 2011.

Este projeto tem como tema a análise da redução de desempenho nas redes sem fio com a utilização de algoritmos de criptografia. O foco será em equipamentos utilizados em residências e pequenos escritórios e empresas. Serão realizados testes com equipamentos do padrão 802.11g e 802.11n trabalhando no padrão 802.11g. Após a realização dos testes, serão analisados os resultados com o objetivo de verificar se há redução de desempenho com a rede sem nenhuma chave criptográfica configurada e com chaves WEP, WPA e WPA2. Com isso, este projeto poderá ser uma fonte de pesquisa para usuários e profissionais da área de redes de computadores que precisem implementar redes sem fio com equipamentos iguais ou similares aos utilizados nos testes práticos. Assim será possível avaliar qual é o tipo ideal de algoritmo criptográfico para uma implementação em específico, já que para muitos pode ser muito importante o alto desempenho de tráfego de dados em uma rede, enquanto para outros a segurança pode ser fundamental. Com base em testes já realizados fica mais fácil para os interessados analisarem qual é a redução efetiva no desempenho utilizando-se os principais algoritmos criptográficos disponíveis nos equipamentos.



**Palavras-chave**: Redes sem fio. Redes *wireless.* Criptografia. Desempenho. 802.11.

## LISTA DE FIGURAS

## LISTA DE GRÁFICOS

**SUMÁRIO**

# 1 INTRODUÇÃO

Este capítulo de introdução vai apresentar os seguintes itens relacionados ao projeto: tema, delimitação da pesquisa, problema e premissas, objetivos geral e específicos, justificativa, procedimentos metodológicos e estrutura.

## 1.1 TEMA

A tecnologia faz parte do dia a dia das pessoas e atualmente é difícil identificar alguém que não a utilize de alguma forma, seja para estudos, entretenimento e principalmente na profissão, para melhoria dos processos. As redes de computadores incorporam diversas tecnologias existentes no mercado, melhorando a qualidade dos serviços prestados.

É inegável a importância das redes de computadores na vida das pessoas, seja para uso doméstico ou empresarial. Cada vez mais busca-se acesso a informações com o uso da Internet, compartilhamento de informações e recursos como impressoras, etc. Os preços dos computadores reduziram muito no Brasil nos últimos anos e, com isso, cada vez mais pessoas têm acesso a computadores e principalmente a *notebooks*, equipamentos que há alguns anos eram inacessíveis para a maioria da população brasileira. É importante salientar também o avanço das redes de banda larga via rede telefônica (ADSL) e via operadoras de TV a cabo (*cable modem*) entre a população. Estas tecnologias estão abrangendo cada vez mais áreas no país e muitas pessoas passaram a ter acesso a Internet de alta velocidade em suas casas nos últimos anos.

Hoje em dia é muito comum que as pessoas tenham *notebooks* para uso empresarial e também doméstico. Com isso, tem-se mais mobilidade e torna-se muito mais interessante o uso de redes sem fio ou redes *wireless* como também são conhecidas. É muito comum encontrar locais públicos e privados que oferecem acesso a Internet via redes *wireless*. Além disso, atualmente é muito fácil ligar um

ponto de acesso *wireless* na rede cabeada (como ADSL ou *cable modem*) e disponibilizar sinal de rede sem fio em um ambiente, inclusive em residências.

Segundo Stallings (2005a, p. 406), há alguns anos as redes sem fio eram pouco utilizadas. Entre as razões para isso estavam o alto custo para implementação e baixas taxas de transmissão de dados. Porém, segundo o mesmo autor, as redes sem fio vêm ocupando um nicho significativo no mercado de redes locais. Cada vez mais as organizações estão descobrindo que as redes sem fio são um complemento indispensável às tradicionais redes locais para satisfazer requisitos de mobilidade, realocação e cobertura de locais difíceis de passar cabos.

Mas com este aumento nos acessos a redes sem fio surge um problema. Muitas pessoas que utilizam equipamentos de redes sem fio em suas casas, escritórios e pequenas empresas não possuem conhecimento suficiente para protegerem as suas redes. Como o meio utilizado para a transmissão é o ar, torna-se muito fácil acessar redes vizinhas e o risco de alguém acessar sua rede e suas informações é latente. Com isso, torna-se essencial a utilização de mecanismos de segurança que protejam a rede e seus dados.

Supõe-se que quanto mais segura for uma rede, menor será o seu desempenho. Suzin, Priesnitz Filho e Camargo (2007, p. 1) destacam que técnicas de segurança acabam por interferir, e muitas vezes degradar o desempenho da rede, uma vez que tais procedimentos requerem maior poder de processamento das máquinas, maior largura de banda, entre outros.

Procurando dados acerca do assunto, pode-se verificar que existem poucos estudos sobre qual é a redução efetiva de desempenho em uma rede quando se utiliza um nível de criptografia mais robusto. Este é o propósito deste projeto, ou seja, a partir de testes com equipamentos disponíveis no mercado realizar um levantamento sobre a redução de desempenho em função da utilização de diferentes níveis de criptografia através dos algoritmos disponíveis.

## 1.2 DELIMITAÇÃO DA PESQUISA

Neste projeto os testes serão realizados com a utilização de equipamentos *home office* que são recomendados para uso em residências, escritórios e pequenas

empresas com poucos usuários. Não serão utilizados equipamentos corporativos, recomendados para uso em grandes empresas e instituições.

O projeto focará o padrão 802.11g. Serão utilizados equipamentos *wireless* dos padrões 802.11g e 802.11n (trabalhando no padrão 802.11g), pois eles são compatíveis. Algumas placas receptoras de sinal utilizadas nos testes são do padrão 802.11n pois não foi possível encontrar no mercado placas novas do padrão 802.11g para os testes. Apesar disso, o padrão 802.11g foi escolhido porque, embora os equipamentos do padrão 802.11n estejam presentes e disponíveis no mercado, este padrão é relativamente novo e mais caro, e os seus pontos de acesso e placas receptoras de sinal ainda não estão tão disseminados quanto os equipamentos do padrão 802.11g. Como um dos objetivos deste projeto é servir como fonte de dados para profissionais e usuários que necessitam aprimorar suas redes, escolheu-se utilizar o padrão 802.11g que ainda é o mais utilizado e já está consolidado.

Existem alguns mecanismos de criptografia disponíveis atualmente, e estes são utilizados pelos diferentes fabricantes de equipamentos de rede sem fio do mercado. Os testes serão realizados primeiramente sem uso de criptografia. Depois serão utilizadas criptografias WEP, WPA e WPA2.

Serão utilizados três pontos de acesso *wireless*, o *software* de análise de desempenho de redes “iperf”, dois computadores sendo um deles o servidor iperf e o outro o cliente com placas de rede sem fio PCI conectadas. Cada ponto de acesso será utilizado por um tempo com cada placa de rede sem fio e com cada tipo de chave criptográfica. Serão analisados os resultados obtidos no tráfego de dados.

## 1.3 PROBLEMA E PREMISSAS

Muitas pessoas instalam redes sem fio em suas casas, escritórios e pequenas empresas e tem o desempenho abaixo do esperado sem saber que o mecanismo de criptografia utilizado pode estar interferindo. Outros fatores como interferências de outros equipamentos e obstáculos físicos podem influenciar muito o desempenho de uma rede sem fio, mas pouco se sabe sobre quanto a segurança interfere nisso.

Conforme mecanismos de criptografia mais eficientes são utilizados na instalação e configuração do ponto de acesso que vai prover acesso a rede sem fio, menor pode ser a taxa de transferência de tráfego de dados nesta rede.

Com a redução de desempenho, pode ser necessário utilizar mais equipamentos com a função de repetir o sinal e aumentar o alcance da rede. Isso representa aumento de custo. Portanto, dependendo da situação pode ser mais interessante a utilização de um mecanismo de criptografia mais simples, evitando a degradação do desempenho e conseqüentemente reduzindo a quantidade de equipamentos utilizados. Neste contexto:

Qual é a redução média de desempenho em uma rede sem fio com o aumento do nível de segurança?

É difícil mensurar exatamente qual é essa redução, mas com este projeto busca-se estabelecer uma média de redução para equipamentos comumente encontrados.

Este estudo pode servir como base para pessoas que pretendem implementar redes sem fio em suas casas e pequenos escritórios e empresas. Com isso será possível ter uma noção de qual mecanismo de criptografia é o ideal para aquele ambiente de acordo com a necessidade de desempenho daqueles usuários. Para alguns a velocidade de transmissão pode ser essencial, enquanto para outros o tráfego de dados pode não ser tão grande e importante, mas a segurança pode ser fundamental.

## 1.4 OBJETIVOS

### 1.4.1 Objetivo Geral

O objetivo deste projeto é levantar se e quanto se reduz o desempenho de uma rede sem fio na medida em que se aumenta a segurança.

### 1.4.2 Objetivos Específicos

- Levantar o desempenho de pontos de acesso *wireless*, padrão *home office*, com os diferentes mecanismos de criptografia disponíveis;
- Comparar o desempenho de cada roteador com cada diferente configuração de segurança e identificar as reduções de velocidade;
- Analisar equipamentos de diferentes fabricantes;
- Identificar os *chipsets* de rádio utilizados pelos equipamentos analisados, possibilitando a comparação com equipamentos não utilizados neste projeto.

## 1.5 JUSTIFICATIVA

As redes sem fio são cada vez mais utilizadas na medida em que ocorrem evoluções nas tecnologias e os preços dos equipamentos ficam mais reduzidos. Cada vez mais as pessoas se interessam por instalar um ponto de acesso *wireless* nas suas redes cabeadas para ganhar mobilidade e evitar passagem de cabos pelo local. Enquanto as redes sem fio ficam mais presentes, torna-se necessário realizar estudos acerca dos temas relacionados às suas tecnologias.

É importante que sempre existam estudos como este pois trata-se de uma área muito dinâmica. Este tipo de análise deve ser renovada conforme as tecnologias vão evoluindo e os perfis dos usuários e serviços vão se alterando.

## 1.6 PROCEDIMENTOS METODOLÓGICOS

Com relação aos procedimentos metodológicos, pode-se classificar o tipo de pesquisa realizado neste projeto da seguinte forma: com relação à natureza é científica aplicada; quanto aos propósitos é explicativa; quanto ao objeto de estudo e técnicas de apreensão é bibliográfica e experimental.

Serão realizados testes práticos utilizando equipamentos de redes e *software* para análise de tráfego. Para o embasamento teórico e ajuda na definição dos critérios para realização dos testes e principalmente da análise dos resultados, serão analisados materiais existentes de autores de livros e artigos relacionados ao tema.

## 1.7 ESTRUTURA

Este projeto será dividido em cinco partes. O capítulo 1 apresentará a introdução, que é composta pelo tema, delimitação da pesquisa, apresentação do problema e premissas, objetivos geral e específicos, justificativa, procedimentos metodológicos e descrição da estrutura.

No capítulo 2 serão abordados de forma aprofundada os conceitos relacionados aos temas abordados no projeto, como conceitos de redes sem fio, os padrões 802.11, tipos de equipamentos utilizados em redes sem fio, conceitos de criptografia, segurança em redes sem fio e os algoritmos de criptografia WEP, WPA e WPA2.

O capítulo 3 irá descrever o ambiente dos testes práticos a serem realizados, com a especificação dos equipamentos e softwares utilizados.

No capítulo 4 serão apresentados os resultados dos testes e análise destes resultados.

O capítulo seguinte será dedicado as considerações finais e propostas para projetos futuros.

# 2 REFERENCIAL TEÓRICO

As redes de computadores têm crescido explosivamente. Há duas décadas, poucas pessoas tinham acesso a uma rede. Agora, a comunicação via computador transformou-se em uma parte essencial da infra-estrutura de todos (COMER, 2007, p. 33).

Cada vez mais as pessoas utilizam as redes de computadores para acessar a Internet, compartilhar dados, pesquisar, estudar e trabalhar. Com o avanço das tecnologias é cada vez mais comum as pessoas utilizarem *notebooks, tablets*, celulares para se conectarem, e com o aumento do uso destes equipamentos móveis, tornou-se mais importante e popular o uso das redes sem fio. De acordo com Kurose e Ross (2006, p. 22), acompanhando a revolução atual da Internet, a revolução sem fio também está causando um profundo impacto sobre o modo de vida e de trabalho das pessoas. Atualmente, as LANs (*Local Area Network*) sem fio, baseadas em tecnologia 802.11 (também conhecida como Ethernet sem fio), estão se desenvolvendo rapidamente em departamentos universitários, escritórios comerciais, cafés e residências.

Segundo Kurose e Ross (2006, p. 22), hoje há duas categorias amplas de acesso sem fio a Internet. Nas LANs sem fio, os usuários sem fio transmitem/recebem pacotes de/para uma estação-base (também conhecida como ponto de acesso sem fio) dentro de um raio de algumas dezenas de metros. A estação-base normalmente está ligada por fio a Internet, portanto, serve para conectar usuários sem fio a uma rede ligada por fio. Nas redes sem fio de acesso de longa distância, a estação-base é gerenciada por um provedor de telecomunicações e atende usuários dentro de um raio de dezenas de quilômetros. Este trabalho se refere às LANs sem fio.

Quadros em uma rede 802.11 devem ser convertidos para outro tipo de quadro para entrega ao resto do mundo. Pontos de acesso realizam a função de ponte de rede *wireless* para rede com cabos (GAST, 2005, p. 15).

Abaixo, na figura 1 pode-se ver uma típica topologia de LAN sem fio. Porém, na maioria dos casos atualmente, o próprio modem tem a função de roteador (modem roteador) ou ainda o ponto de acesso tem essa função (roteador wireless),

ou seja, normalmente tem-se apenas o modem e o ponto de acesso ou roteador wireless.

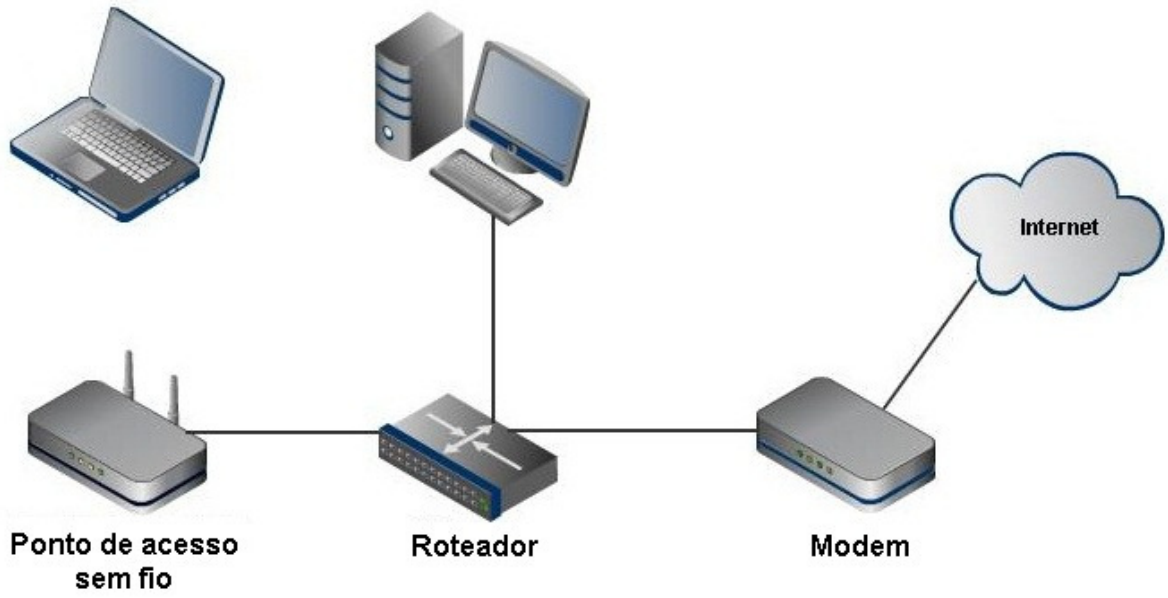



**Figura 1 – Um diagrama esquemático de uma rede residencial típica**
**Fonte: Adaptado de Kurose e Ross (2006, p. 23)**

As redes sem fio trazem grandes benefícios a quem as utiliza, sendo o principal deles a mobilidade. Porém, a sua utilização também traz algumas dificuldades. Heusse et allii (2003, apud MENDES, 2008, p. 14) mencionam que os problemas das redes sem fio estão relacionados com a degradação do nível de sinal, interferência no local onde a rede se encontra, mobilidade das estações, características do método de acesso ao meio, além da quantidade simultânea de usuários utilizando a rede.

Além das dificuldades apresentadas acima, deve-se considerar também os problemas relacionados à segurança ao se utilizar uma rede sem fio. Na medida em que muitas pessoas têm acesso a estas redes, com algum equipamento como um *notebook*, por exemplo, é possível acessar as redes vizinhas e conseqüentemente acessar informações alheias. Por isso é muito importante a utilização de mecanismos de segurança para proteger uma rede sem fio contra acessos indevidos.

As redes sem fio utilizam canais de rádio para a propagação dos sinais. Segundo Kurose e Ross (2006, p. 25), canais de rádio carregam sinais dentro do

espectro eletromagnético. São um meio atraente porque sua instalação não requer cabos físicos, podem atravessar paredes e dão conectividade ao usuário móvel. As LANs sem fio utilizam canais de rádio de pequeno alcance, que funcionam em locais próximos, normalmente abrangendo de dez a algumas centenas de metros.

Segundo Gast (2005, p. 227), no modelo de transmissão clássico, evitar interferências é uma questão de lei e não física. Com saídas de alta potência em bandas estreitas, uma autoridade legal deve impor regras sobre como o espectro de radiofreqüência é usado. Nos Estados Unidos, a *Federal Communications Comission* (FCC) é responsável for regular o uso do espectro de radiofreqüência. Muitas regras da FCC são adotadas por outros países das Américas. Uma instituição deve ter uma licença para transmitir em uma dada freqüência. Licenças podem restringir as freqüências e a potência usada nas transmissões, assim como a área sobre a qual os sinais de rádio podem ser transmitidos. Licenciar garante o uso exclusivo de um conjunto particular de freqüências.

Ainda segundo o mesmo autor, o espectro de radiofreqüências é alocado em bandas dedicadas a um propósito particular. Uma banda define as freqüências que uma aplicação pode usar. Isso freqüentemente inclui bandas protegidas, que são porções não utilizadas da alocação global, que evita vazamento de transmissões licenciadas afetando outras bandas alocadas. Muitas bandas foram reservadas para uso não licenciado. Por exemplo, fornos microondas operam a 2.45GHz, mas não teria sentido uma pessoa obter uma licença para utilizar um forno microondas em sua casa. Para permitir ao mercado consumidor desenvolver produtos para uso doméstico, a FCC (e instituições similares em outros países) designou certas bandas para uso de equipamentos industriais, científicos e médicos. Essas bandas de freqüência são comumente referidas como bandas ISM. A banda de 2.4 GHz está disponível para uso não licenciado, assim como o range de 5GHz.

No Brasil, quem regulamenta o uso das bandas de radiofreqüência é a Agência Nacional de Telecomunicações – Anatel (ANATEL, 2011).

Segundo Rufino (2011, p. 20) o espectro de radiofreqüência é dividido em faixas, que são intervalos reservados, normalmente, para determinado tipo de serviço, definido por convenções internacionais e/ou por agências reguladoras. Uma faixa é, em geral, subdividida em freqüências menores, para permitir a transmissão em paralelo de sinais diferentes em cada uma delas. Essas freqüências menores (ou

subfreqüências) são chamadas de canais, que já fazem parte do nosso dia a dia há bastante tempo, como os canais de rádio (AM/FM) e televisão.

Segundo Gast (2005, p. 229), a tecnologia de espectro de propagação é o fundamento utilizado para recuperar as bandas ISM para o uso de dados. Ela trabalha usando funções matemáticas para difundir a potência do sinal sobre uma grande faixa de frequências. A seguir são descritas as três técnicas de espectro de propagação, segundo Gast (2005, p. 232):

- *Frequency hopping* (FH ou FHSS): este sistema pula de uma freqüência para outra em um padrão aleatório, transmitindo uma rajada curta em cada sub-canal.
- *Direct sequence* (DS ou DSSS): este sistema propaga a potência ao longo de uma faixa mais ampla de frequência usando funções matemáticas de codificação.
- *Orthogonal Frequency Division Multiplexing* (OFDM): este sistema divide um canal disponível em vários sub-canais e codifica uma porção do sinal através de cada sub-canal em paralelo. A técnica é similar a utilizada por alguns modens DSL.

## 2.1 MODELOS DE REFERÊNCIA

De acordo com Tanenbaum (1997, p. 19), no projeto das primeiras redes de computadores, o hardware foi colocado como prioridade e o software, em segundo plano. Essa estratégia foi deixada para trás. Atualmente o software da rede está altamente estruturado. Para reduzir a complexidade do projeto, a maioria das redes foi organizada como uma série de camadas ou níveis, que são colocados um em cima do outro. O número, o nome, o conteúdo e a função de cada camada diferem de uma rede para outra. Em todas as redes, no entanto, o objetivo de cada camada é oferecer determinados serviços para as camadas superiores, ocultando detalhes da implementação desses recursos. A camada n de uma máquina se comunica com a camada n da outra máquina. Coletivamente, as regras e convenções usadas nesse diálogo são chamadas de protocolo da camada n. Basicamente, um protocolo

é um conjunto de regras sobre o modo como se dará a comunicação entre as partes envolvidas.

### 2.1.1 Modelo de Referëncia OSI

Segundo Tanembaum (1997, p. 32), o modelo OSI (Open Systems Interconnection) é baseado em uma proposta desenvolvida pela ISO (International Standards Organization) como um primeiro passo na direção da padronização internacional dos protocolos usados nas diversas camadas. O nome do modelo é este pois ele trata da interconexão de sistemas abertos – ou seja, sistemas que estão abertos à comunica;ao com outros sistemas.

Segundo Stallings (2005b, p. 97) as camadas do modelo OSI bem como suas definições são as seguintes:

- Aplicação: proporciona acesso ao ambiente OSI para usuários e também oferece serviços de informação distribuídos.
- Apresentação: oferece independência aos processos da aplicação com relação às diferenças na representação dos dados (sintaxe).
- Sessão: fornece a estrutura de controle para a comunicação entre as aplicações; estabelece, gerencia e termina as conexões (sessões) entre aplicações cooperando.
- Transporte: possibilita a transferência de dados confiável e transparente entre as extremidades; oferece recuperação de erro e controle de fluxo de ponta a ponta.
- Rede: oferece às camadas superiores independência das tecnologias de transmissão e comutação de dados, usadas para conectar os sistemas; responsável por estabelecer, manter e terminar as conexões.
- Enlace de dados: oferece a transferência confiável de informações pelo enlace físico; envia blocos (quadros) com o sincronismo, controle de erro e controle de fluxo necessários.

- Física: trata da transmissão do fluxo de bits não estruturado pelo meio físico; lida com características mecânicas, elétricas, funcionais e de procedimento para acessar o meio físico.


**Figura 2 – As camadas OSI**
**Fonte: Adaptado de Stallings (2005b, p. 97)**

### 2.1.2 Modelo de Referencia TCP/IP

Segundo Stallings (2005b, p, 83) TCP/IP é, de longe, a arquitetura interoperável mais utilizada e é um resultado da pesquisa e desenvolvimento de protocolos realizados na rede experimental de comutação de pacotes, ARPANET, patrocinada pela *Defense Advanced Research Projects Agency* (DARPA), e geralmente é referenciada como conjunto de protocolos TCP/IP. Ainda segundo mesmo autor, não há um modelo de protocolo TCP/IP oficial, assim como no caso do OSI. Entretanto, com base nos padrões de protocolo que foram desenvolvidos, ele organiza a tarefa de comunicação para o TCP/IP em cinco camadas relativamente independentes:

- Camada de aplicação
- Camada host a host, ou transporte
- Camada de inter-rede
- Camada de acesso a rede
- Camada física

Stallings (2005b, p. 83) define as camadas física e de acesso à rede da seguinte forma:

- Camada física: abrange a interface física entre um dispositivo de transmissão de dados (por exemplo, estação de trabalho, computador) e um meio de transmissão ou rede. Essa camada trata da especificação das características do meio de transmissão, da natureza dos sinais, da taxa de dados e de questões relacionadas.
- Camada de acesso a rede: trata da troca de dados entre um sistema final (servidor, estação de trabalho, etc.) e a rede a qual está conectado. O computador de envio precisa fornecer à rede o endereço do computador de destino, de modo que a rede possa rotear os dados para o destino apropriado. O computador de envio pode querer invocar certos serviços, como prioridade, que poderiam ser fornecidos pela rede. O software específico utilizado nessa camada depende do tipo de rede a ser usado; diferentes padrões foram desenvolvidos para comutação de circuitos, comutação de pacotes (por exemplo, Frame Relay), LANs (por exemplo, Ethernet) e outros. Assim, faz sentido separar essas funções que têm a ver com acesso à rede em uma camada separada. Fazendo isso, o restante do software de comunicações, acima da camada de rede, não precisa se preocupar com os detalhes da rede a ser utilizada. O mesmo software da camada superior deverá funcionar corretamente, independente da rede em particular à qual o computador está conectado.

Segundo Tanenbaum (1997, p. 40), as camadas inter-redes, transporte e aplicação do modelo TCP/IP são definidas conforme segue:

- Camada Inter-redes: essa camada integra toda a arquitetura. Sua tarefa é permitir que os *hosts* injetem pacotes em qualquer rede e garantir que eles sejam transmitidos independentemente do destino (que pode ser outra rede). A camada inter-redes define um formato de pacote oficial e um protocolo chamado de IP (Internet Protocol). A tarefa da camada inter-redes é entregar pacotes IP onde eles são necessários. O roteamento é uma questão de grande importância nessa camada, assim como evitar congestionamentos. Por essas razões, é razoável dizer que a função da camada inter-redes TCP/IP é muito parecida com a da camada de rede OSI.
- Camada de Transporte: essa camada é localizada acima da camada inter-redes. A finalidade dessa camada é permitir que as entidades par dos *hosts* de origem e de destino mantenham uma conversação, como ocorre na camada de transporte OSI. Dois protocolos fim a fim foram definidos aqui: O TCP (Transmission Control Protocol) e UDP (User Datagram Protocol). O TCP é um protocolo orientado a conexão, confiável que permite a entrega sem erros de um fluxo de bytes originado de uma determinada máquina em qualquer computador da inter-rede. Esse protocolo fragmenta o fluxo de bytes de entrada em mensagens e passa cada uma delas para a camada inter-redes. No destino, o processo TCP remonta as mensagens recebidas no fluxo de saída. O TCP cuida também do controle de fluxo, impedindo que um transmissor rápido sobrecarregue um receptor lento com um volume de mensagens muito grande. O UDP é um protocolo sem conexão, não confiável, para aplicações que não necessitam nem de controle de fluxo, nem da manutenção da seqüência das mensagens enviadas. Ele é amplamente usado em aplicações em que a entrega imediata é mais importante do que a entrega precisa, como a transmissão de dados de voz ou de vídeo.
- Camada de aplicação: acima da camada de transporte está a camada de aplicação. Ela contém os protocolos de alto nível. Dentre eles estão o protocolo de terminal virtual (TELNET), o protocolo de transferência de arquivos (FTP) e o protocolo de correio eletrônico (SMTP).


**Figura 3 – Uma comparação das arquiteturas de protocolos OSI e TCP/IP.**

**Fonte: Adaptado de Stallings (2005b, p. 98)**

## 2.2 PADRÃO 802.11

Os padrões IEEE 802 fazem parte de um conjunto de padrões desenvolvidos pela IEEE, instituição responsável pela especificação e padronização nas áreas de elétrica, eletrônica e de computação (MENDES, 2008, p.17). O padrão 802.11 pode ser definido como o padrão de redes sem fio.

De acordo com Morimoto (2008, p. 235), o padrão 802.11 original, hoje chamado de 802.11-1997 ou 802.11 legacy foi publicado em 1997 e previa taxas de transmissão de 1 e 2 Mbps, usando a faixa de 2.4 GHz.

A especificação do padrão IEEE 802.11 refere-se à camada física e a camada de enlace restrita a sub-camada especificada no padrão IEEE 802.11 como

Media Access Control (MAC) (MENDES, 2008, p.17). A relação do 802.11 com o OSI pode ser visto na figura 4 abaixo:

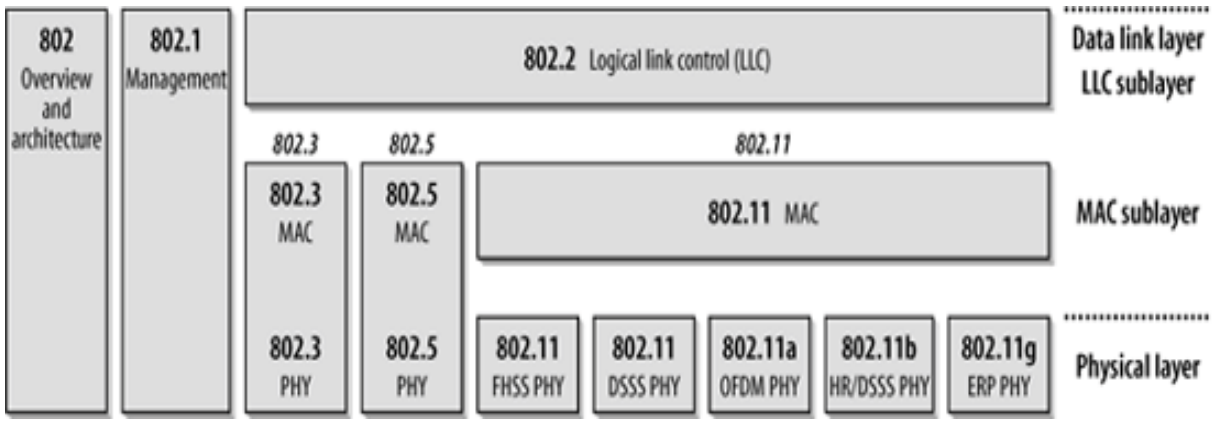



**Figura 4 – A família IEEE 802 e sua relação com o modelo OSI.**
**Fonte: Gast (2005, p.13)**

Um problema existente nas redes sem fio é o compartilhamento do meio, pois os vários dispositivos na rede podem transmitir ao mesmo tempo, podendo ocorrer colisões.

Segundo Mendes (2008, p. 18), dentre as principais modificações realizadas nas camadas física e de enlace em relação às redes cabeadas existentes no padrão IEEE 802.11, pode-se citar a sub-camada MAC, responsável pela definição do mecanismo de acesso ao meio. Esse é baseado no CSMA/CA (Carrier Sense Multiple Access – Collision Avoidance). Ainda de acordo com Mendes (2008, p. 20), o mecanismo de detecção de portadora possui como principal objetivo a detecção do status atual do meio de acesso, seja através da utilização de uma rede sem fio ou de uma rede cabeada. Para que seja possível a realização de uma transmissão é necessário identificar a disponibilidade do canal e caso esse esteja em uso, é necessário que a estação que deseja transmitir aguarde até que o canal se torne ocioso ou disponível para realizar a transmissão.

Segundo Stallings (2005b, p. 235), o comitê IEEE 802.11 desenvolveu um conjunto de padrões de LAN sem fio. O IEEE 802.11 define diversos serviços que precisam ser fornecidos pela LAN sem fio para prover funcionalidade equivalente à que é inerente às LANs com fio. Os serviços mais importantes são os seguintes:

- Associação: Estabelece uma associação inicial entre uma estação e um ponto de acesso. Antes que uma estação possa transmitir ou receber quadros em uma LAN sem fio, sua identidade e endereço precisam ser conhecidos.
- Reassociação: Torna possível uma associação estabelecida transferir-se de um ponto de acesso para outro, permitindo que uma estação móvel se mova.
- Desassociação: Uma notificação por parte de uma estação ou de um ponto de acesso de que uma associação existente está terminada.
- Autenticação: Usada para estabelecer a identidade das estações uma para outra.
- Privacidade: Usada para impedir que conteúdo de mensagens sejam lidos por outras pessoas além do destinatário pretendido. O padrão sugere o uso opcional da criptografia para garantir privacidade.

Segundo Kurose e Ross (2006, p. 402), o bloco construtivo fundamental da arquitetura 802.11 é o conjunto básico de serviço (basic service set - BSS). Um BSS contém uma ou mais estações sem fio e uma estação-base central, conhecida como um ponto de acesso (access point - AP) na terminologia da 802.11. Em uma rede residencial típica, há apenas um AP e um roteador (quase sempre acompanhado de um modem a cabo ou ADSL, formando um só pacote) que conecta o BSS a Internet.

Ainda segundo os mesmos autores, LANs sem fio que disponibilizam APs normalmente são denominadas LANs sem fio de infra-estrutura. Estações IEEE 802.11 também podem se agrupar e formar uma rede ad hoc – rede sem nenhum controle central e sem nenhuma conexão com o “mundo externo”. Nesse caso, a rede é formada conforme a necessidade, por equipamentos móveis que, por acaso, estão próximos uns dos outros, tem necessidade de se comunicar e não dispõem de infra-estrutura de rede no lugar em que se encontram.

### 2.2.1 802.11b

Publicado em outubro de 1999, o 802.11b foi o primeiro padrão wireless usado em grande escala. Ele marcou a popularização da tecnologia, permitindo que

placas de diferentes fabricantes se tornassem compatíveis e os custos caíssem, graças ao aumento da demanda e à concorrência (MORIMOTO, 2008, p. 235).

De acordo com Kurose e Ross (2006, p. 401), o padrão 802.11b opera na faixa de freqüência de 2.4 - 2.485 GHz e sua taxa de dados é de até 11Mbps.

Segundo Rufino (2011, p. 25), o padrão 802.11b utiliza a modulação DSSS.

De acordo com Morimoto (2008, p. 238), nas redes 802.11b e 802.g estão disponíveis 11 canais de transmissão (originalmente são 14, mas três deles não podem ser usados devido à questão da legislação), que englobam as freqüências de 2.412 GHz (canal 1) a 2.462 GHz (canal 11), com intervalos de 5 MHz entre eles. Como os canais utilizam uma banda total de 22 MHz (em muitas citações o valor é arredondado para 20 MHz), as freqüências acabam sendo compartilhadas, fazendo com que redes operando em canais próximos interfiram entre si. O canal 6, cuja freqüência nominal é 2.437 GHz, opera na verdade entre 2.426 e 2.448 GHz, invadindo as freqüências dos canais 2 até o 10.

| Canal | Frequência nominal | Frequência nominal |
|---|---|---|
| 1 | 2.412 GHz | 2.401 a 2.423 GHz |
| 2 | 2.417 GHz | 2.405 a 2.428 GHz |
| 3 | 2.422 GHz | 2.411 a 2.433 GHz |
| 4 | 2.427 GHz | 2.416 a 2.438 GHz |
| 5 | 2.432 GHz | 2.421 a 2.443 GHz |
| 6 | 2.437 GHz | 2.426 a 2.448 GHz |
| 7 | 2.442 GHz | 2.431 a 2.453 GHz |
| 8 | 2.447 GHz | 2.436 a 2.458 GHz |
| 9 | 2.452 GHz | 2.441 a 2.463 GHz |
| 10 | 2.457 GHz | 2.446 a 2.468 GHz |
| 11 | 2.462 GHz | 2.451 a 2.473 GHz |

**Figura 5 – Canais suportados pelos padrões 802.11b e 802.11g**

**Fonte: Adaptado de Morimoto (2008, p. 238)**

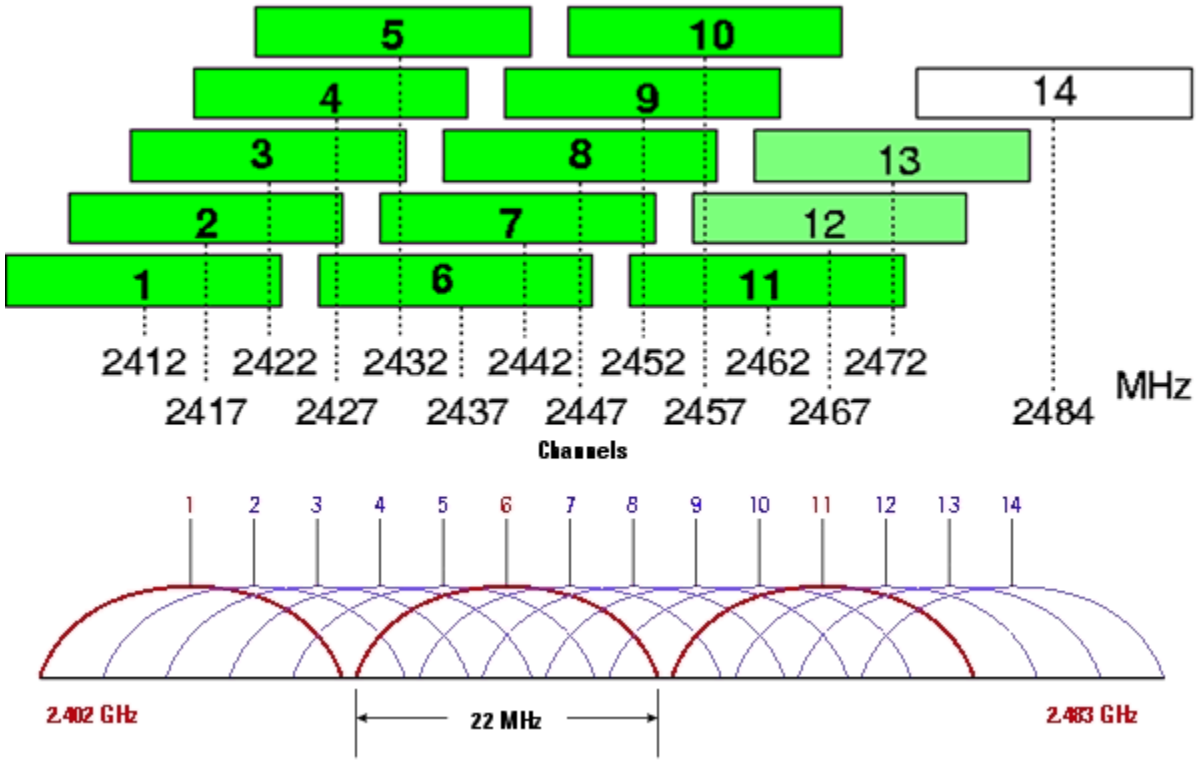



**Figura 6 – Ilustração dos canais suportados pelos padrões 802.11b e 802.11g**

**Fonte: AIR-STREAM (2011)**

### 2.2.2 802.11a

Segundo Kurose e Ross (2006, p. 401), o padrão 802.11a opera na faixa de freqüência de 5.1 - 5.8 GHz e sua taxa de dados é de até 54Mbps.

De acordo com Rufino (2011, p. 26), o padrão 802.11a utiliza modulação OFDM.

### 2.2.3 802.11g

Segundo Sanches (2007, p. 224), o padrão 802.11g foi ratificado pela IEEE em 2003. Este padrão utiliza a faixa de 2.4GHZ e opera em velocidade máxima de até 54Mbps e próximo de 26Mbps de velocidade efetiva.

De acordo com Morimoto (2008, p. 237), apesar do crescimento do padrão 802.11n, o 802.11g ainda é utilizado na maioria das instalações. Ele utiliza a mesma faixa de freqüência do 802.11b: 2.4GHz. Isso permite que os dois padrões sejam intercompatíveis.

Apesar de o padrão 802.11g operar em uma faixa de freqüência inferior ao padrão 802.11a, a velocidade de transmissão no 802.11g é de 54Mbps, assim como no 802.11a. Segundo Morimoto, (2008, p. 237), isso é possível porque o padrão 802.11g é mais recente e por isso incorpora novas tecnologias de modulação de sinal.

O padrão 802.11g utiliza modulação OFDM (*Orthogonal Frequency Division Multiplexing/Modulation*). Segundo Rufino (2011, p. 21), OFDM é tipo de modo de transmissão (mais eficiente) utilizado não somente por equipamentos sem fio, mas também por redes cabeadas, como ADSL, cujas características de modulação do sinal e isolamento de interferências podem também ser bem aproveitadas. A maioria dos padrões atuais de redes sem fio adota esse modo de transmissão, principalmente por sua capacidade de identificar interferências e ruídos, permitindo troca ou isolamento de uma faixa de frequência, ou mudar a velocidade de transmissão.

De acordo com Gast (2005, p. 298) o ERP-OFDM (Extended Rate PHY-OFDM) é o principal modo do padrão 802.11g e suporta as seguintes velocidades: 6, 9, 12, 18, 24, 36, 48 e 54 Mbps.

Os canais suportados pelo padrão 802.11g são os mesmos suportados pelo padrão 802.11b, descritos na figura 4 acima.

### 2.2.4 802.11n

Segundo Rufino (2011, p. 30), o padrão 802.11n é também conhecido como World Wide Spectrum Efficiency (WWiSE) e tem como foco principal o aumento da velocidade (cerca de 100 a 500 Mbps). Paralelamente, deseja-se um aumento da área de cobertura. Em relação aos padrões atuais há poucas mudanças. A mais significativa delas diz respeito a uma modificação de OFDM, conhecida como Multiple Input, Multiple Out-OFDM (MIMO-OFDM). Outra característica desse padrão é a compatibilidade retroativa com os padrões vigentes atualmente. O 802.11n pode trabalhar com canais de 40 Mhz e, também, manter compatibilidade com os 20 MHz atuais, mas, nesse caso, as velocidades máximas oscilam em torno de 135 Mbps. Esse padrão foi homologado no último trimestre de 2009.

## 2.3 SEGURANÇA EM REDES SEM FIO

De acordo com Stallings (2005b, p. 380), a segurança de computador e de rede trata de quatro requisitos:

- Privacidade: Exige que os dados sejam acessíveis apenas por pessoas autorizadas. Esse tipo de acesso inclui impressão, exibição e outras formas de exposição de dados, inclusive simplesmente revelar a existência de um objeto.
- Integridade: Exige que apenas pessoas autorizadas possam modificar dados. A modificação inclui escrever, alterar, mudar o estado, excluir e criar.
- Disponibilidade: Exige que os dados estejam disponíveis às pessoas autorizadas.
- Autenticidade: Exige que um host ou serviço seja capaz de verificar a identidade de um usuário.

Kurose e Ross (2006, p. 512) identificam as seguintes propriedades desejáveis em uma comunicação segura:

- Confidencialidade: Somente o remetente e o destinatário pretendido devem poder entender o conteúdo da mensagem transmitida.
- Autenticação: O remetente e o destinatário precisam confirmar a identidade da outra parte envolvida na comunicação – confirmar que a outra parte realmente é quem alega ser.
- Integridade e não-repudiação de mensagem: Mesmo que o remetente e o destinatário consigam se autenticar reciprocamente, eles também querem assegurar que o conteúdo de sua comunicação não seja alterado, por acidente ou por má intenção, durante a transmissão.
- Disponibilidade e controle de acesso: Um requisito fundamental para comunicação segura deve ser, antes de mais nada, que ela possa ocorrer – que os "bandidos" não possam impedir que a infra-estrutura seja utilizada por usuários legítimos. O fato de que alguns desses usuários possam ser legítimos, enquanto outros não, leva, naturalmente, à noção de controle de acesso, para garantir que entidades que procuram obter acesso a recursos possam fazê-lo somente se tiverem os direitos de acesso apropriados e realizarem seus acessos de uma maneira bem definida.

Este projeto focará a análise da redução do desempenho das redes sem fio com a utilização de métodos mais robustos de segurança. Não há como abordar a segurança sem mencionar a criptografia.

> Desde que o ser humano entendeu as vantagens que o conhecimento de determinadas informações podem trazer, surgiu a necessidade de protegê-las de terceiros que poderiam se beneficiar delas: assim, nasceu a criptografia. Do grego Kriptos, secreto, e Graphos, escrita, a criptografia surgiu como a ciência ou, para alguns, arte de escrever mensagens de forma codificada, impossibilitando a leitura a terceiros não autorizados. (SECURITY OFFICER, 2007, p. 15)

Existem alguns mecanismos criptográficos específicos para redes sem fio, como o WEP, WPA e WPA2. Os três serão utilizados nos testes práticos deste projeto e são muito utilizados e suportados pela maioria dos equipamentos disponíveis no mercado.

Redes sem fio dependem de um meio aberto, e o risco de utilizá-las aumenta se não for utilizada proteção criptográfica. Com um meio de rede aberto, tráfego desprotegido pode ser visto por qualquer pessoa com o equipamento correto (GAST, 2005, p. 114).

Os sistemas de encriptação visam garantir a confidencialidade dos dados. Eles não fazem nada para impedir que intrusos captem o sinal da rede, mas embaralham os dados de forma que eles não façam sentido sem a chave de desencriptação apropriada (MORIMOTO, 2008, p. 247).

### 2.3.1 WEP (Wired-Equivalent Privacy)

De acordo com Morimoto (2008, p. 248), existem dois padrões WEP: de 64 e 128 bits. Os primeiros pontos de acesso e placas 802.11b suportavam apenas o padrão de 64 bits, mas logo o suporte ao WEP de 128 bits virou norma. O grande problema é que o WEP é baseado no uso de vetores de inicialização que, combinados com outras vulnerabilidades, tornam as chaves muito fáceis de quebrar, usando ferramentas largamente disponíveis. As chaves de 128 bits são tão fáceis de quebrar quanto as de 64 bits, já que os bits extra apenas tornam o processo um pouco mais demorado.

Segundo Gimenes (2011, p. 24) o WEP opera na camada de enlace de dados e fornece criptografia entre o cliente e o Access Point. O WEP é baseado no método criptográfico RC4 (*Route Coloniale* 4) da RSA, que usa um vetor de inicialização (IV) de 24 bits e uma chave secreta compartilhada (*secret shared key*) de 40 ou 104 bits. O IV é concatenado com a *secret shared key* para formar uma chave de 64 ou 128 bits que é usada para criptografar os dados. Além disso, o WEP utiliza CRC-32 (*Cyclic Redundancy Check*) para calcular o *checksum* da mensagem, que é incluso no pacote, para garantir a integridade dos dados. O receptor então recalcula o checksum para garantir que a mensagem não foi alterada.

Ainda segundo Gimenes (2011, p. 25), em resumo o problema do WEP consiste na forma com que se trata a chave e como ela é "empacotada" ao ser agregada ao pacote de dados.

### 2.3.2 WPA (Wired Protected Access)

Segundo Morimoto (2008, p. 248), o WPA foi criado em 2003 com o objetivo de substituir o WEP, devido às suas vulnerabilidades. WPA utiliza o sistema TKIP (*Temporal Key Integrity Protocol*), no qual a chave de encriptação é trocada periodicamente e a chave definida na configuração da rede (*a passphrase*) é usada apenas para fazer a conexão oficial. È possível quebrar chaves WPA fáceis ou com poucos caracteres usando alguns programas, mas chaves com mais de 20 caracteres ou mais são inviáveis de se quebrar devido ao enorme tempo que seria necessário para testar todas as combinações possíveis. Ainda segundo Morimoto (2008, p. 249), WPA utiliza algoritmo RC4, o mesmo utilizado pelo WEP.

Segundo Gimenes (2005, p. 26) o protocolo TKIP é o responsável pelo gerenciamento da troca de chaves. No WEP as chaves eram estáticas e seu vetor de inicialização era de apenas 24bits, passando agora para 48bits. O TKIP pode ser programado para alterar o vetor de inicialização a cada pacote, por sessão ou por período, tornando mais difícil a obtenção do mesmo via captura de tráfego.

### 2.3.3 WPA2

Diferente dos padrões anteriores, o WPA2 utiliza o AES como sistema de encriptação, mais seguro e também mais complexo do que o RC4. De acordo com Morimoto (2008, p. 249), o AES é um sistema de criptografia bastante seguro, baseado no uso de chaves de 128 a 256 bits. Ainda segundo Morimoto (2008, p. 249), usar o AES garante uma maior segurança, mas ele exige mais processamento, o que pode ser um problema no caso dos pontos de acesso mais baratos, que utilizam controladores de baixo desempenho. Muitos pontos de acesso e algumas

placas antigas simplesmente não suportam o WPA2 por não terem recursos ou poder de processamento suficientes. Existem também casos em que o desempenho da rede é mais baixo ao utilizar o WPA2.

Gimenes (2005, p. 32) menciona que o AES permite a descoberta de uma chave de criptografia de difusão ponto a ponto inicial exclusiva para cada autenticação, bem como a alteração sincronizada da chave de criptografia de difusão ponto a ponto para cada quadro. Como as chaves AES são descobertas automaticamente, não há necessidade de se configurar uma chave de criptografia para o WPA2. O WPA2 é a modalidade de segurança sem fio mais forte.

# 3 AMBIENTE DE TESTES

Foram utilizados equipamentos do padrão 802.11g e 802.11n trabalhando no padrão 802.11g, que ainda é o mais utilizado.

Equipamentos utilizados nos testes:

- Computador *desktop* com processador Intel Core 2 Duo E7500 2,93GHZ, memória RAM de 2GB, sistema operacional Windows 7 32 bits. O mesmo computador foi utilizado para todos os testes para evitar alterações nos resultados provenientes de diferença de capacidade de processamento dos computadores.
- Netbook Acer com processador Intel Atom 1.33GHz, memória RAM de 2GB, sistema operacional Windows 7 32 bits.
- Roteador wireless Linksys WRT54G com firmware DD-WRT. O DD-WRT é um firmware baseado em software livre para pontos de acesso ou roteadores sem fio que disponibiliza funcionalidades avançadas aos equipamentos (DD-WRT, 2011).
- Roteador wireless Linksys WRT54G com firmware original
- Roteador wireless D-Link WBR-1310 com firmware original
- Placa de rede wireless PCI Encore N300, chipset Realtek RTL8190 com duas antenas.
- Placa de rede wireless PCI AIOX A-WN300P, chipset Ralink RT2760T com duas antenas.
- Placa de rede wireless PCI Encore xxxx, chipset Marvell Libertas 802.11b/g com uma antena.

Para a análise do tráfego de rede foi utilizado o software iperf. O Iperf foi desenvolvido pela NLANR (*National Laboratory for Applied Network Research*) como um modelo alternativo para medir o desempenho de largura de banda máxima do TCP e UDP. O Iperf permite o ajuste de vários parâmetros utilizando o protocolo UDP. O Iperf reporta a largura de banda utilizada, jitter e perda de pacotes (IPERF, 2011).

O protocolo de transporte utilizado foi o UDP, devido à inexistência de controle de congestionamento, evitando assim a degradação do desempenho nos testes, já que segundo Kurose e Ross (2006, p. 66) o mecanismo de controle de congestionamento do TCP limita a capacidade de transmissão de um processo (cliente ou servidor) quando a rede está congestionada entre cliente e servidor.

O software NetStumbler foi utilizado para definir o melhor canal a ser utilizado durante os testes. Segundo Souza (2005, p. 48) esta ferramenta é um scanner para ser utilizado nas redes sem fio, funciona em ambiente Windows e com ela pode-se obter informações como: potência do sinal, ESSID da rede e localização da rede, pois possui suporte a GPS. Para os testes, com o uso deste software foi verificado que o canal 1 não estava sendo usado por mais nenhum ponto de acesso ao alcance das placas receptoras.

A topologia utilizada nos testes foi a seguinte:

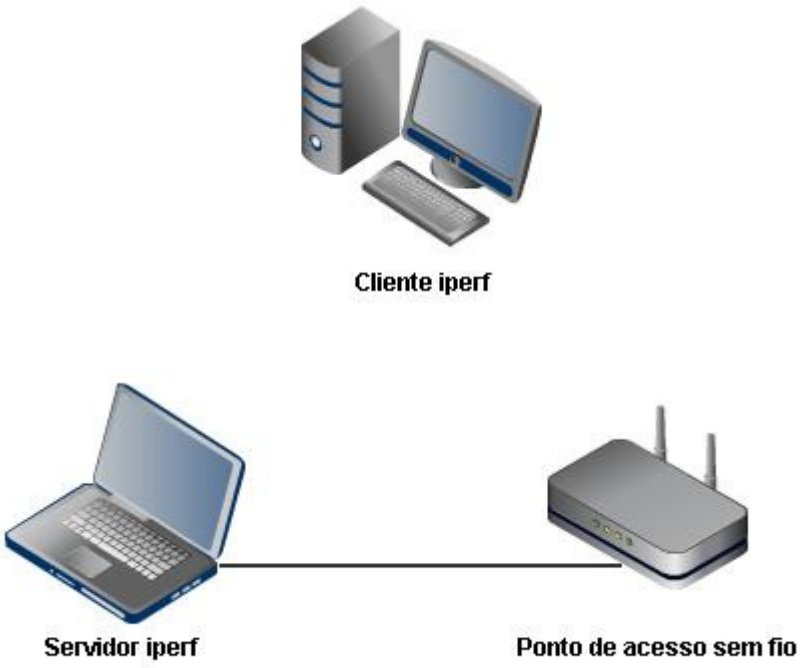



**Figura 7 – Topologia adotada nos testes**
**Fonte: Autoria Própria**

O netbook foi conectado pela sua porta Fast Ethernet (100 Mbps) via cabo de rede a uma porta LAN do ponto de acesso sem fio. Neste netbook foi executado

o iperf como servidor. Como a fast ethernet trabalha a uma velocidade maior do que os 54 Mbps do padrão 802.11g, os resultados dos testes não foram comprometidos por baixo desempenho do servidor.

No computador desktop foi executado o iperf como cliente e as placas foram testadas uma a uma com cada ponto de acesso, cada velocidade e cada mecanismo de segurança. Os pontos de acesso foram ligados um a um assim como as placas e não simultaneamente. Os comandos iperf utilizados foram os seguintes:

- Servidor:

**iperf –s –i 1 –u**, onde:

-s: especifica que este equipamento será o servidor

-i: especifica a cada quanto tempo será mostrado o resultado na tela, que neste caso foi de 1 segundo

-u: especifica que o protocolo de transporte utilizado será o UDP

- Cliente:

**iperf –c <IP servidor> -i –b <bandwidth> -t <tempo em segundos>**, onde:

-c: especifica que este equipamento será o cliente

-i: especifica a cada quanto tempo será mostrado o resultado na tela, que neste caso foi de 1 segundo

-b: especifica o bandwidth que neste caso foi 6, 9, 12, 18, 24, 36, 48 e 54 Mbps.

-t: especifica por quando tempo o teste será feito. Cada um foi feito com 180 segundos.

Os pontos de acesso foram mantidos na mesma posição, assim como o computador cliente, para não haver alteração nos resultados dos testes devido a diferentes distâncias entre as placas receptoras e os pontos de acesso.

Os testes foram executados com as velocidades possíveis no padrão 802.11g: 6, 9, 12, 18, 24, 36, 48 e 54Mbps. Este método foi utilizado porque por

padrão, devido à utilização das técnicas de modulação, quando ocorre alguma interferência no momento da transmissão, o ponto de acesso passa a trabalhar na velocidade imediatamente inferior (conforme valores acima) para melhorar seu desempenho. Dessa forma, os testes feitos com todas as velocidades tornam-se mais completos.

Para evitar diferenças nos resultados causados por possível aquecimento das placas, os testes foram feitos seguindo sempre a mesma ordem de configuração das chaves criptográficas, sendo:

1. Aberta (sem nenhuma chave)
2. WEP 128 bits
3. WPA-TKIP
4. WPA2-AES

Os resultados dos testes foram salvos em arquivos de texto e depois foram calculadas as médias dos desempenhos de cada placa com cada roteador, cada bandwidth e cada mecanismo de criptografia.

# 4 RESULTADOS OBTIDOS

Em geral, pode-ser perceber pelos testes que houve pouca diferença de desempenho, quando existe diferença. Em muitos casos a velocidade com chaves criptográficas mais robustas foi até maior do que com as outras chaves ou até mesmo sem criptografia. Considerando o maior processamento necessário para enviar um pacote quando a chave criptográfica é mais robusta, a velocidade não deveria ser maior com qualquer uma das chaves do que com a rede aberta, por exemplo. Isso demonstra que as especificações do padrão IEEE 802.11 podem não estar sendo seguidas pelos fabricantes como deveriam.

O fato de o mecanismo WEP ser mais antigo do que as outras criptografias talvez explique seu baixo desempenho em algumas situações.

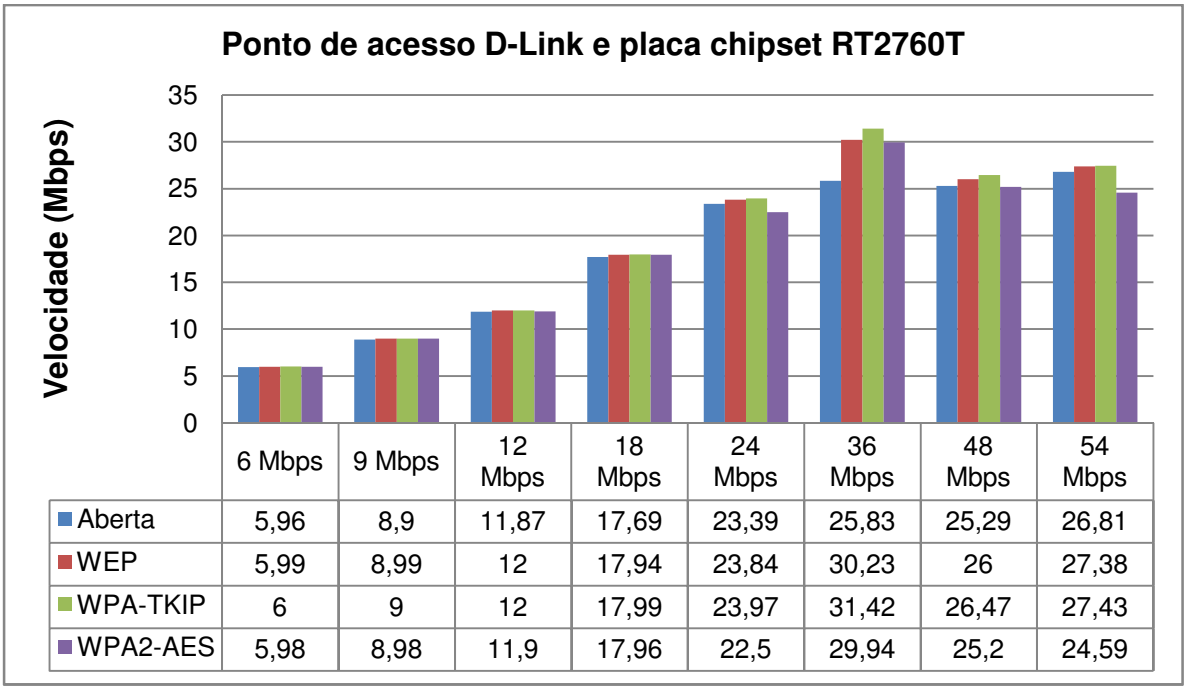
Outro fato identificado é que não se chega perto dos 54Mbps definidos pelo padrão 802.11G. A velocidade máxima atingida nos testes foi de 32Mbps com a placa PCI AIOX que tem duas antenas conectada ao roteador Linksys WRT54G com o firmware original.

Inicialmente os testes seriam feitos com notebooks e suas placas de rede sem fio acopladas, mas o desempenho ficou muito baixo e o melhor desempenho foi atingido com as placas PCI. Ainda analisando este ponto, o desempenho da placa com apenas uma antena é bem inferior as outras duas placas com duas antenas, tendo sido seu melhor resultado de 21.8 Mbps com o ponto de acesso da marca D-Link.

Nas velocidades mais baixas (6, 9 e 12Mbps) ocorrem poucas diferenças de desempenho entre as criptografias testadas. Nas velocidades mais altas as diferenças são mais evidentes, como pode ser visto nos gráficos abaixo.

Nas análises abaixo, quando indicados os mecanismos de criptografia com melhor e pior desempenho, foi considerada, entre todas as velocidades testadas naquele cenário, a quantidade de vezes em que cada mecanismo teve o melhor desempenho. Para definir os mecanismos de melhor e pior desempenho em cada cenário não foram considerados os resultados das redes abertas e as oscilações na performance de alguns mecanismos, como pode ser visto a seguir.

## 4.1 CENÁRIO 1 - AP D-LINK E PLACA CHIPSET RT2760T




| | 6 Mbps | 9 Mbps | 12 Mbps | 18 Mbps | 24 Mbps | 36 Mbps | 48 Mbps | 54 Mbps |
|---|---|---|---|---|---|---|---|---|
| Aberta | 5,96 | 8,9 | 11,87 | 17,69 | 23,39 | 25,83 | 25,29 | 26,81 |
| WEP | 5,99 | 8,99 | 12 | 17,94 | 23,84 | 30,23 | 26 | 27,38 |
| WPA-TKIP | 6 | 9 | 12 | 17,99 | 23,97 | 31,42 | 26,47 | 27,43 |
| WPA2-AES | 5,98 | 8,98 | 11,9 | 17,96 | 22,5 | 29,94 | 25,2 | 24,59 |

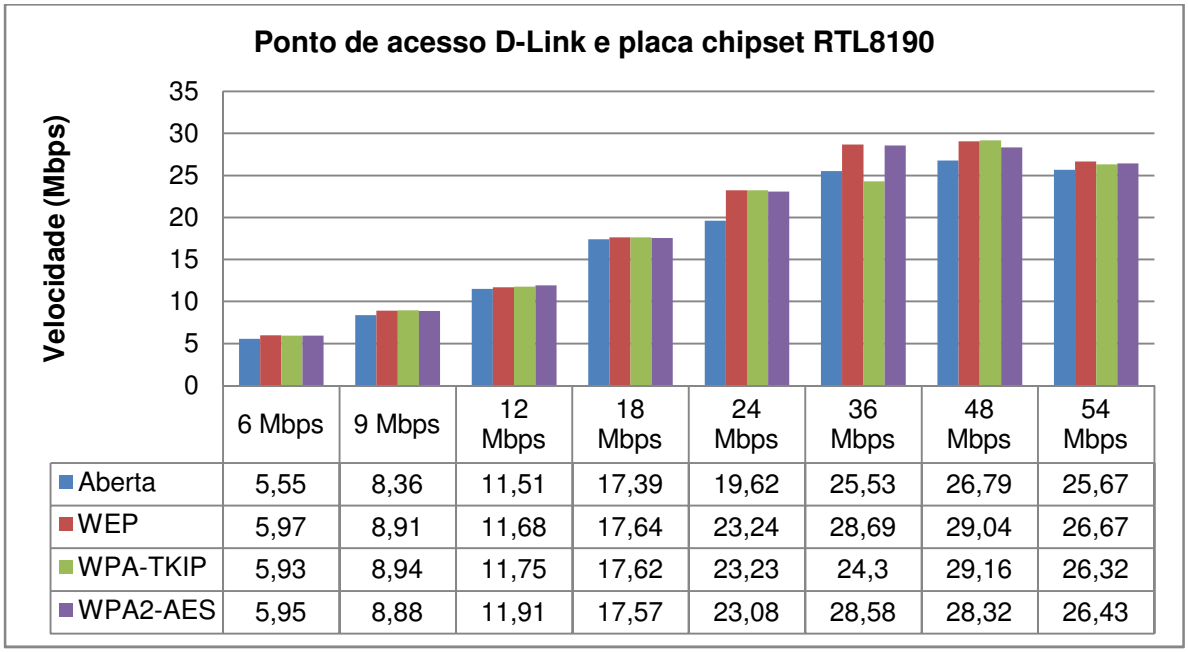
**Gráfico 1 – Ponto de acesso D-Link e placa chipset RT2760T**

**Fonte: Autoria própria**

Neste cenário pode-se perceber com os resultados que apenas nas velocidades mais altas (48 e 54Mbps) teve-se um desempenho menor na transmissão de dados utilizando o mecanismo mais robusto de segurança, WPA2. Nas demais velocidades e demais chaves pode-se perceber pelo gráfico que não houve diferença significativa nas velocidades mais baixas e nas intermediárias o desempenho da rede aberta foi até menor do que com a segurança configurada no ponto de acesso.

Considerando apenas os testes com os três mecanismos de segurança, o WPA2 teve o pior desempenho, o que já era esperado.

## 4.2 CENÁRIO 2 - AP D-LINK E PLACA CHIPSET RTL8190



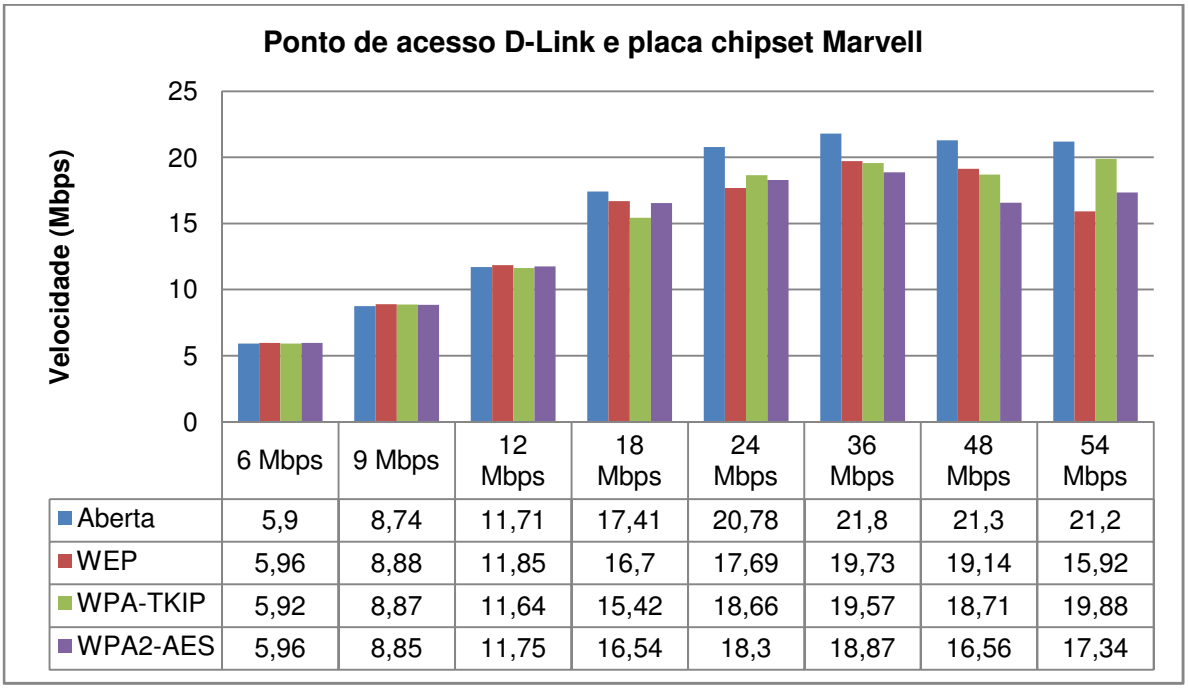

| | 6 Mbps | 9 Mbps | 12 Mbps | 18 Mbps | 24 Mbps | 36 Mbps | 48 Mbps | 54 Mbps |
|---|---|---|---|---|---|---|---|---|
| Aberta | 5,55 | 8,36 | 11,51 | 17,39 | 19,62 | 25,53 | 26,79 | 25,67 |
| WEP | 5,97 | 8,91 | 11,68 | 17,64 | 23,24 | 28,69 | 29,04 | 26,67 |
| WPA-TKIP | 5,93 | 8,94 | 11,75 | 17,62 | 23,23 | 24,3 | 29,16 | 26,32 |
| WPA2-AES | 5,95 | 8,88 | 11,91 | 17,57 | 23,08 | 28,58 | 28,32 | 26,43 |

**Gráfico 2 – Ponto de acesso D-Link e placa chipset RTL8190**

**Fonte: Autoria própria**

Neste cenário, com o ponto de acesso D-Link com a placa Encore pode-se perceber que a rede aberta teve desempenho inferior àqueles com os mecanismos de segurança em todas as velocidades. Entre as chaves criptográficas não é possível identificar diferenças significativas entre o uso de uma chave ou outra. Considerando apenas os testes utilizando mecanismos de segurança, o WEP teve o melhor desempenho.

## 4.3 CENÁRIO 3 - AP D-LINK E PLACA CHIPSET MARVELL




| | 6 Mbps | 9 Mbps | 12 Mbps | 18 Mbps | 24 Mbps | 36 Mbps | 48 Mbps | 54 Mbps |
|---|---|---|---|---|---|---|---|---|
| Aberta | 5,9 | 8,74 | 11,71 | 17,41 | 20,78 | 21,8 | 21,3 | 21,2 |
| WEP | 5,96 | 8,88 | 11,85 | 16,7 | 17,69 | 19,73 | 19,14 | 15,92 |
| WPA-TKIP | 5,92 | 8,87 | 11,64 | 15,42 | 18,66 | 19,57 | 18,71 | 19,88 |
| WPA2-AES | 5,96 | 8,85 | 11,75 | 16,54 | 18,3 | 18,87 | 16,56 | 17,34 |

**Grafico 3 - Ponto de acesso D-Link e placa chipset Marvell**

**Fonte: Autoria própria**

Neste cenário, com o ponto de acesso D-Link e placa Encore chipset Marvell, pode-se perceber um desempenho dentro do esperado com relação ao melhor desempenho da rede com a rede aberta na maioria das velocidades. Com relação às chaves de segurança, não é possível estabelecer um padrão de chave a ser utilizada pois em algumas velocidades o desempenho com a WPA2 foi menor conforme esperado, mas em outras velocidades foi praticamente o mesmo ou até melhor como, por exemplo, em 54 Mbps, em que o desempenho com o WPA2 foi melhor do que com WEP.

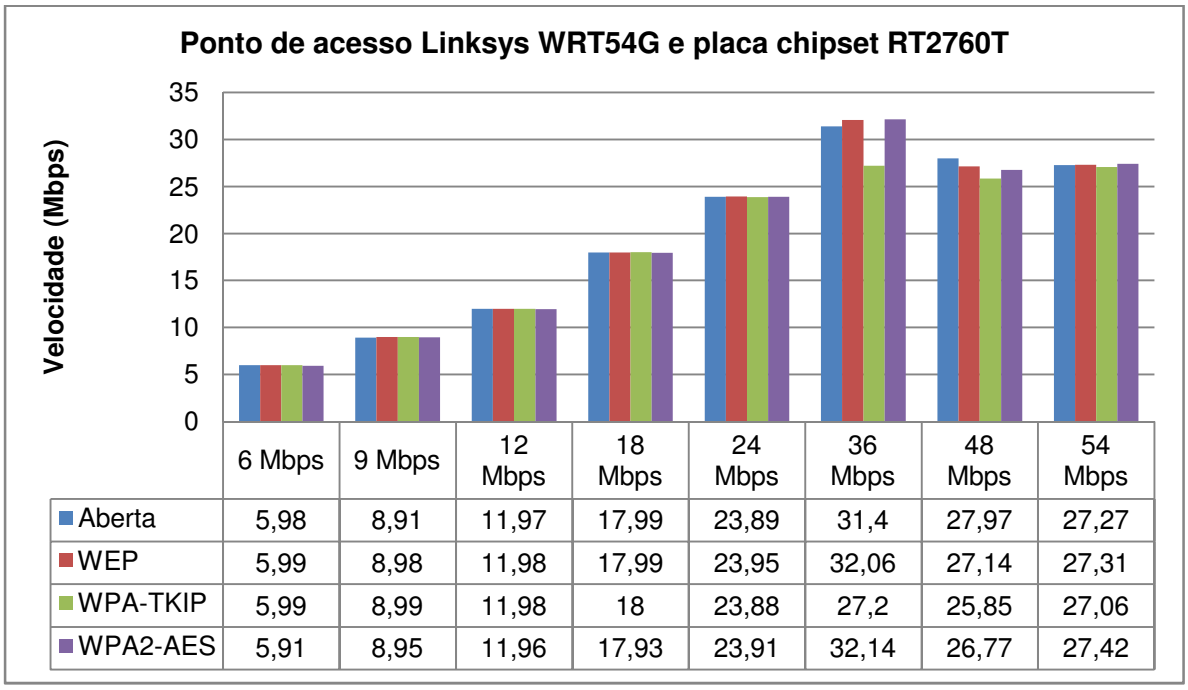
Os resultados obtidos nas velocidades de 36 e 48 Mbps foram conforme esperado, ou seja, melhor desempenho com a rede aberta, reduzindo-se gradativamente do WEP ao WPA e finalmente ao WPA2.

Neste teste, considerando apenas os testes com algum mecanismo de segurança, o WEP teve o melhor desempenho e a WPA2 o pior resultado.

Considerando a grande oscilação de desempenho do mecanismo WEP, que pode ser facilmente identificada pelo gráfico, pode-se levantar a hipótese de que a

implementação do mecanismo pelo fabricante não seguiu os padrões determinados pelo comitê da IEEE 802.11.

## 4.4 CENÁRIO 4 - AP LINKSYS WRT54G E PLACA CHIPSET RT2760T



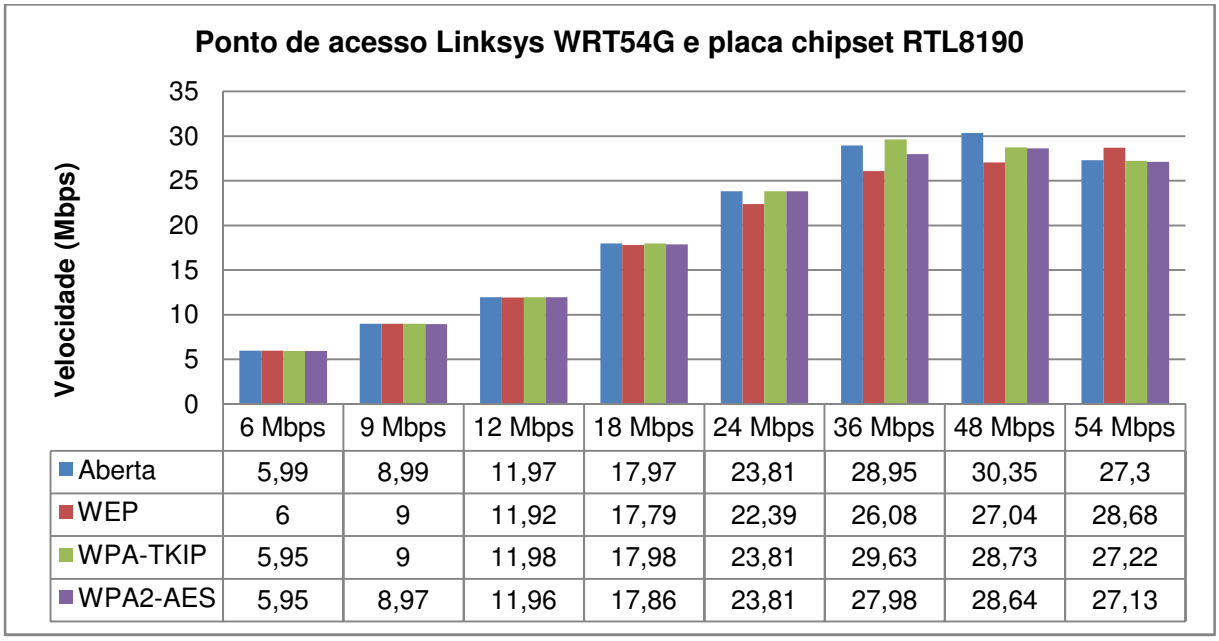

| | 6 Mbps | 9 Mbps | 12 Mbps | 18 Mbps | 24 Mbps | 36 Mbps | 48 Mbps | 54 Mbps |
|---|---|---|---|---|---|---|---|---|
| Aberta | 5,98 | 8,91 | 11,97 | 17,99 | 23,89 | 31,4 | 27,97 | 27,27 |
| WEP | 5,99 | 8,98 | 11,98 | 17,99 | 23,95 | 32,06 | 27,14 | 27,31 |
| WPA-TKIP | 5,99 | 8,99 | 11,98 | 18 | 23,88 | 27,2 | 25,85 | 27,06 |
| WPA2-AES | 5,91 | 8,95 | 11,96 | 17,93 | 23,91 | 32,14 | 26,77 | 27,42 |

**Gráfico 4 - Ponto de acesso Linksys WRT54G e placa chipset RT2760T**

**Fonte: Autoria própria**

Neste cenário pode-se verificar através dos resultados acima que nas velocidades de 6, 12, 18 e 24 Mbps os resultados foram praticamente os mesmos, o que não poderia ocorrer já que os mecanismos de segurança são diferentes uns dos outros. Neste cenário, para as maiores velocidades, o mecanismo WEP teve os melhores resultados de desempenho.

## 4.5 CENÁRIO 5 - AP LINKSYS WRT54G E PLACA CHIPSET RTL8190




| | 6 Mbps | 9 Mbps | 12 Mbps | 18 Mbps | 24 Mbps | 36 Mbps | 48 Mbps | 54 Mbps |
|---|---|---|---|---|---|---|---|---|
| Aberta | 5,99 | 8,99 | 11,97 | 17,97 | 23,81 | 28,95 | 30,35 | 27,3 |
| WEP | 6 | 9 | 11,92 | 17,79 | 22,39 | 26,08 | 27,04 | 28,68 |
| WPA-TKIP | 5,95 | 9 | 11,98 | 17,98 | 23,81 | 29,63 | 28,73 | 27,22 |
| WPA2-AES | 5,95 | 8,97 | 11,96 | 17,86 | 23,81 | 27,98 | 28,64 | 27,13 |

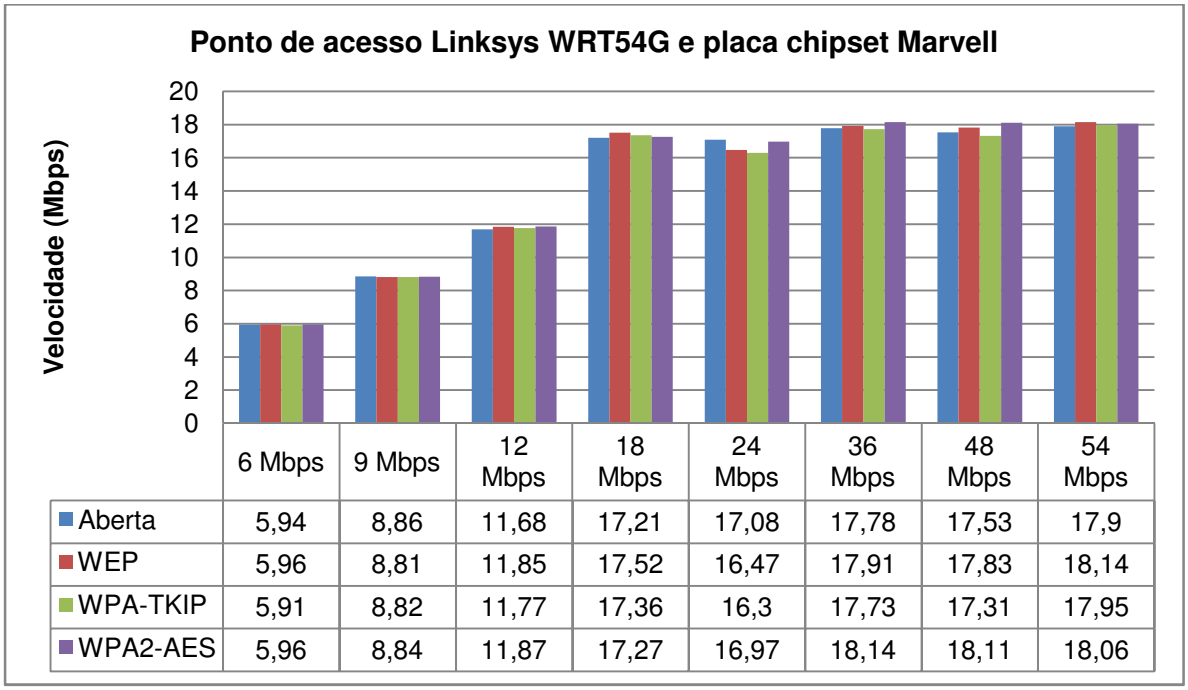
**Gráfico 5 - Ponto de acesso Linksys WRT54G e placa chipset RTL8190**

**Fonte: Autoria própria**

Neste cenário, mais uma vez nas velocidades mais baixas (6, 9, 12 e 18 Mbps) os resultados foram quase idênticos, o que não deveria ocorrer. Pode-se dizer que neste cenário em geral, o mecanismo WEP teve um baixo desempenho em relação aos demais mecanismos de segurança testados.

Assim como no cenário 3, pode-se perceber pelo gráfico que o WEP também apresentou oscilações neste cenário e pode não ter sido implementado conforme a especificação do padrão IEEE 802.11.

## 4.6 CENÁRIO 6 - AP LINKSYS WRT54G E PLACA CHIPSET MARVELL



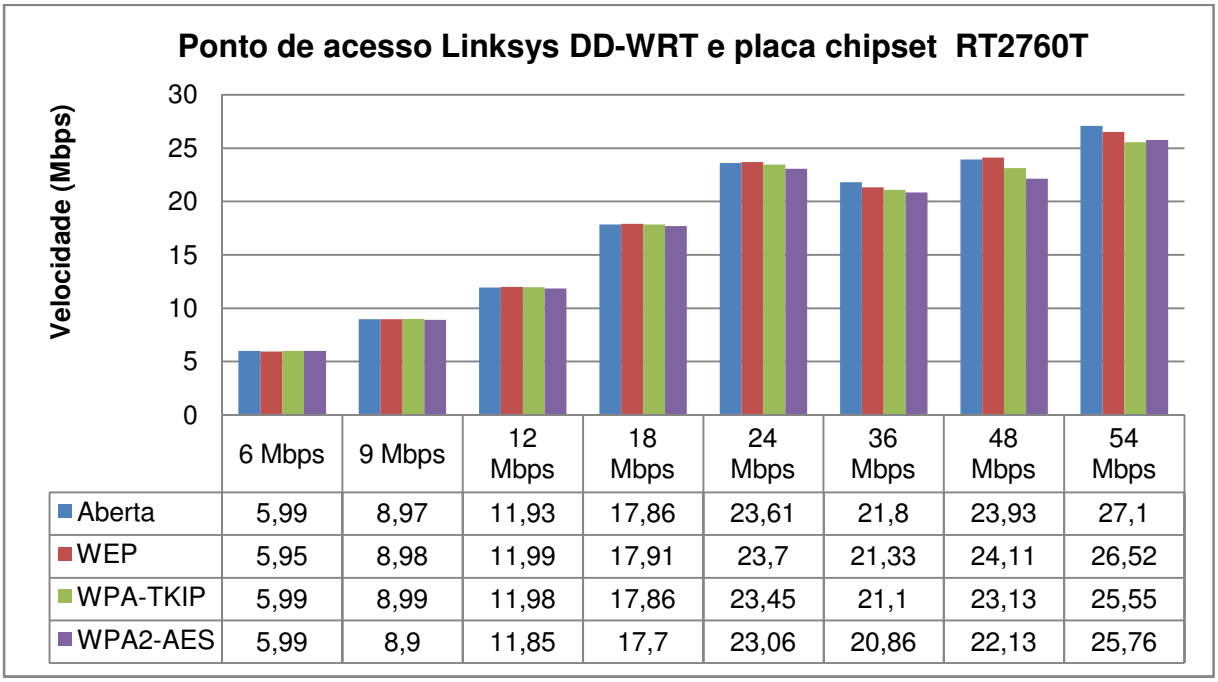

| | 6 Mbps | 9 Mbps | 12 Mbps | 18 Mbps | 24 Mbps | 36 Mbps | 48 Mbps | 54 Mbps |
|---|---|---|---|---|---|---|---|---|
| Aberta | 5,94 | 8,86 | 11,68 | 17,21 | 17,08 | 17,78 | 17,53 | 17,9 |
| WEP | 5,96 | 8,81 | 11,85 | 17,52 | 16,47 | 17,91 | 17,83 | 18,14 |
| WPA-TKIP | 5,91 | 8,82 | 11,77 | 17,36 | 16,3 | 17,73 | 17,31 | 17,95 |
| WPA2-AES | 5,96 | 8,84 | 11,87 | 17,27 | 16,97 | 18,14 | 18,11 | 18,06 |

**Gráfico 6 - Ponto de acesso Linksys WRT54G e placa chipset Marvell**

**Fonte: Autoria própria**

Neste cenário houve poucas diferenças de desempenho em todas as velocidades testadas. Neste cenário, dentre os mecanismos de segurança, o WPA2 teve o melhor desempenho e o WPA obteve o pior resultado. O WPA2 não deveria ter o melhor desempenho por ser o mecanismo mais robusto. Pode-se ver pelo gráfico que houve algumas oscilações no WPA2, levantando a hipótese deste mecanismo ter sigo mal implementado pelo fabricante.

## 4.7 CENÁRIO 7 - AP LINKSYS COM DDWRT E PLACA CHIPSET RT2760T




| | 6 Mbps | 9 Mbps | 12 Mbps | 18 Mbps | 24 Mbps | 36 Mbps | 48 Mbps | 54 Mbps |
|---|---|---|---|---|---|---|---|---|
| Aberta | 5,99 | 8,97 | 11,93 | 17,86 | 23,61 | 21,8 | 23,93 | 27,1 |
| WEP | 5,95 | 8,98 | 11,99 | 17,91 | 23,7 | 21,33 | 24,11 | 26,52 |
| WPA-TKIP | 5,99 | 8,99 | 11,98 | 17,86 | 23,45 | 21,1 | 23,13 | 25,55 |
| WPA2-AES | 5,99 | 8,9 | 11,85 | 17,7 | 23,06 | 20,86 | 22,13 | 25,76 |

**Grafico 7 - Ponto de acesso Linksys WRT54G DDWRT e placa chipset RT2760T**

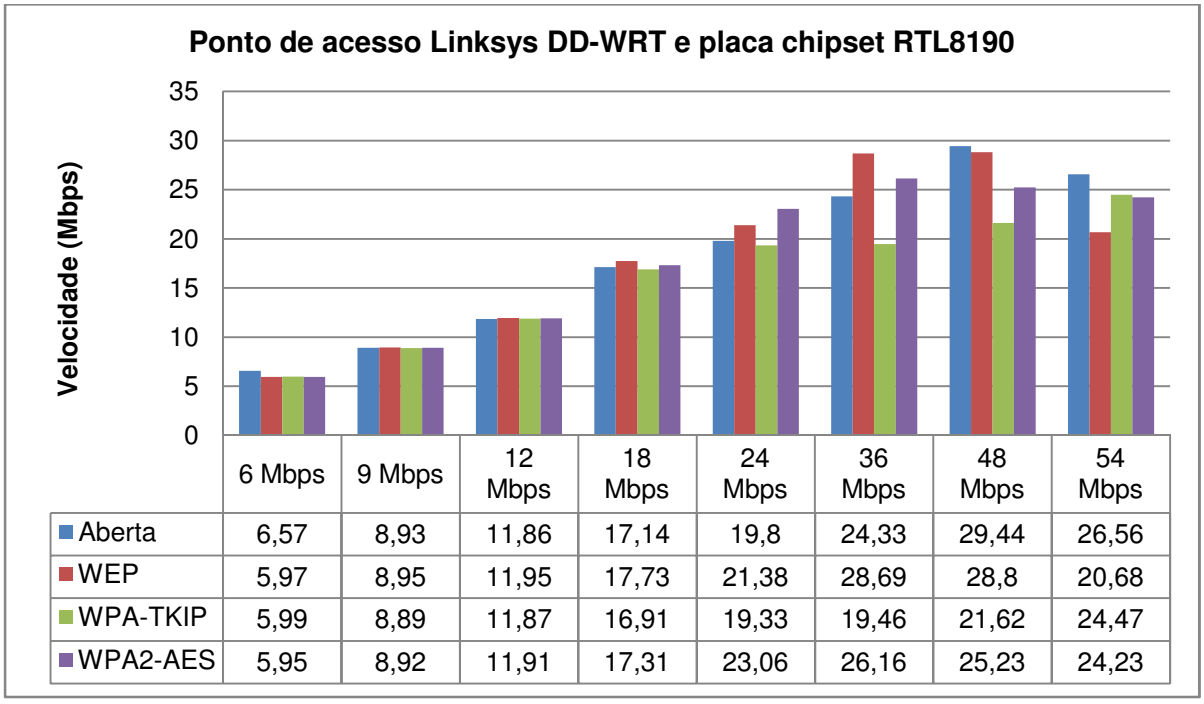
**Fonte: Autoria própria**

Neste cenário na velocidade de 6 Mbps novamente os resultados foram quase iguais para a rede aberta e mecanismos de segurança.

Nas velocidades de 24, 36 e 48 Mbps os resultados foram dentro do esperado considerando os testes com mecanismos de segurança implementados.

Neste cenário o WEP teve o melhor desempenho na maioria das velocidades.

## 4.8 CENÁRIO 8 - AP LINKSYS COM DDWRT E PLACA CHIPSET RTL8190




| | 6 Mbps | 9 Mbps | 12 Mbps | 18 Mbps | 24 Mbps | 36 Mbps | 48 Mbps | 54 Mbps |
|---|---|---|---|---|---|---|---|---|
| Aberta | 6,57 | 8,93 | 11,86 | 17,14 | 19,8 | 24,33 | 29,44 | 26,56 |
| WEP | 5,97 | 8,95 | 11,95 | 17,73 | 21,38 | 28,69 | 28,8 | 20,68 |
| WPA-TKIP | 5,99 | 8,89 | 11,87 | 16,91 | 19,33 | 19,46 | 21,62 | 24,47 |
| WPA2-AES | 5,95 | 8,92 | 11,91 | 17,31 | 23,06 | 26,16 | 25,23 | 24,23 |

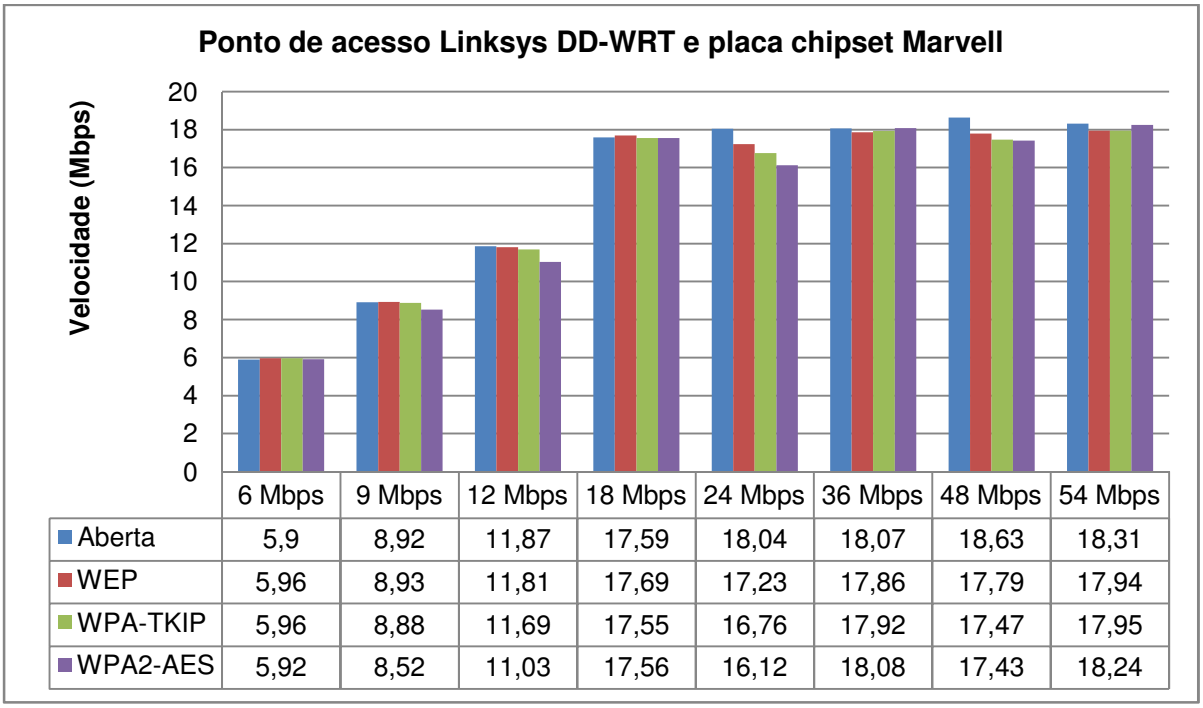
**Gráfico 8 - Ponto de acesso Linksys WRT54G DDWRT e placa chipset RTL8190**

**Fonte: Autoria própria**

Este cenário mostra o WEP com o melhor desempenho entre os mecanismos de segurança e em algumas velocidades, como 9, 12, 18 e 36 Mbps o seu desempenho foi até melhor do que na rede aberta. Já o WPA apresentou os piores resultados, como pode-se verificar em 9, 18, 24, 36 e 48 Mbps.

Analisando apenas o mecanismo WPA e a rede aberta pode-se perceber que a rede aberta apresentou melhor desempenho. As grandes oscilações sofridas pelos mecanismos WEP e WPA2 levantam a hipótese de que ambos podem ter sido mal implementados pelo fabricante.

## 4.9 - CENÁRIO 9 – AP LINKSYS COM DDWRT E PLACA CHIPSET MARVELL




| | 6 Mbps | 9 Mbps | 12 Mbps | 18 Mbps | 24 Mbps | 36 Mbps | 48 Mbps | 54 Mbps |
|---|---|---|---|---|---|---|---|---|
| Aberta | 5,9 | 8,92 | 11,87 | 17,59 | 18,04 | 18,07 | 18,63 | 18,31 |
| WEP | 5,96 | 8,93 | 11,81 | 17,69 | 17,23 | 17,86 | 17,79 | 17,94 |
| WPA-TKIP | 5,96 | 8,88 | 11,69 | 17,55 | 16,76 | 17,92 | 17,47 | 17,95 |
| WPA2-AES | 5,92 | 8,52 | 11,03 | 17,56 | 16,12 | 18,08 | 17,43 | 18,24 |

**Gráfico 9 - Ponto de acesso Linksys WRT54G DDWRT e placa chipset Marvell**

**Fonte: Autoria própria**

Neste cenário ocorreram alguns resultados dentro do esperado, como em 12, 24 e 48 Mbps. Mais uma vez nas velocidades mais baixas os resultados ficaram praticamente iguais.

Desconsiderando o mecanismo WEP, na maior parte dos testes o resultado foi conforme o esperado, pois este mecanismo apresentou oscilações, levando a crer que talvez ele não tenha sido implementado incorretamente pelo fabricante.

# CONCLUSÃO

Ao mesmo tempo em que foi possível avaliar que existe uma pequena diferença no desempenho entre os mecanismos criptográficos, foi possível também verificar o desempenho de alguns equipamentos encontrados facilmente no mercado e o mais interessante foi verificar que o desempenho dos equipamentos está abaixo do que é especificado no padrão IEEE 802.11g, o que indica que os fabricantes podem não estar seguindo as diretrizes do padrão.

Devido aos resultados inconclusivos dos testes, não foi possível mensurar uma redução média no desempenho do padrão 802.11 com a utilização dos diferentes mecanismos de criptografia disponíveis no mercado.

Devido à pequena e às vezes inexistente diferença de desempenho entre o uso das chaves WEP, WPA e WPA2, pode-ser dizer que o mais interessante é o uso da WPA2 que é mais segura e não degrada significativamente o desempenho das redes que utilizam os equipamentos atualmente presentes no mercado.

Mesmo quando o desempenho do WPA2 ficou abaixo dos outros mecanismos de segurança, a diferença foi pequena, ou seja, o uso de WPA2 é o mais indicado devido a maior segurança que ele proporciona e a pequena redução de desempenho que ele apresenta.

Como sugestão para projetos futuros pode-se indicar testes similares aos executados neste projeto utilizando diferentes equipamentos, principalmente diferentes placas receptoras, com chipsets diferentes dos aqui testados.

## REFERÊNCIAS


AIR-STREAM. Disponível em <http://www.air-stream.org.au/channel_802_11g>. Acesso em: 20 nov. 2011.

ANATEL. Disponível em< http://www.anatel.gov.br>. Acesso em: 02 nov. 2011.

COMER, Douglas E. **Redes de Computadores e Internet**. 4. ed. Porto Alegre: Bookman, 2007.

DD-WRT. Disponível em <http://www.dd-wrt.com/site/index>. Acesso em: 23 nov. 2011.

GAST, Matthew S. ***802.11 Wireless Networks: The Definitive Guide***. 2. ed. O'Reilly, 2005.

GIMENES, Eder C. **Segurança de Redes Wireless.** 2005. 58 f. Monografia (Tecnologia em Informática com ênfase em Gestão de Negócios) - Centro de Educação Tecnológica Paula Souza - Faculdade de Tecnologia de Mauá, Mauá, 2005.

IPERF. Disponível em <http://iperf.sourceforge.net/>. Acesso em: 01 nov. 2011.

KUROSE, James F; ROSS, Keith W. **Redes de Computadores e a Internet: uma abordagem top-down.** 3. ed. São Paulo: Pearson Addison Wesley, 2006.

MENDES, Christian C. S. **Gerenciamento de Recursos em Redes Sem Fio IEEE 802.11**. 2008. 92 f. Dissertação (Mestrado em Engenharia Elétrica e Informática Industrial) - Departamento de Pesquisa e Pós-Graduação, Universidade Tecnológica Federal do Paraná, Curitiba, 2008.

MORIMOTO, Carlos E. **Redes, guia prático**. Porto Alegre: Sul Editores, 2008.

RUFINO, Nelson M. de O. Segurança em redes sem fio : aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth. 3. ed. São Paulo : Novatec Editora, 2011.

SANCHES, Carlos A. **Projetando Redes WLAN – Conceitos e Práticas**. São Paulo: Érica, 2007.

Security Officer – 2: Guia Oficial para Formação de Gestores em Segurança da Informação. Módulo Security Solutions. Porto Alegre, RS: Zouk, 2007.

STALLINGS, William. ***Wireless Communications & Networks.*** *New Jersey: Pearson Prentice Hall*, 2005a.

------. Redes e Sistemas de Comunicação de Dados. 5. ed. Rio de Janeiro: Elsevier, 2005b.

SOUZA, Ricardo de M. A**nálise das Vulnerabilidades e Ataques Existentes em Redes Sem Fio.** 2005. 60 f. Trabalho de Final de Curso (Bacharelado em Sistemas de Informação) – Faculdade de Ciências Aplicadas de Minas, Uberlândia, 2005.

SUZIN, C; PRIESNITZ FILHO, W; CAMARGO, M. E. **Análise de desempenho de protocolos de criptografia em redes sem fio**, Conferência IADIS Ibero-Americana WWW/Internet 2007, Vila Real, Portugal, 2007.

TANENBAUM, Andrew S. Redes de Computadores. 3. ed. Rio de Janeiro: Campus, 1997.