UNIVERSIDADE DO EXTREMO SUL CATARINENSE - UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

IVAN JEREMIAS PEREIRA

ASPECTOS DE GERÊNCIA DE REDES SEM FIO, FOCO NO MONITORAMENTO DE UMA WLAN

CRICIÚMA

2015

IVAN JEREMIAS PEREIRA

ASPECTOS DE GERÊNCIA DE REDES SEM FIO, FOCO NO MONITORAMENTO DE UMA WLAN

Trabalho de Conclusão de Curso apresentado para obtenção do grau de Bacharel no curso de Ciência da Computação, da Universidade do Extremo Sul Catarinense, UNESC.

Orientador: Prof. MSc. Paulo João Martins

CRICIÚMA

2015

IVAN JEREMIAS PEREIRA

ASPECTOS DE GERÊNCIA DE REDES SEM FIO, FOCO NO MONITORAMENTO DE UMA WLAN

Trabalho de Conclusão de Curso aprovado pela Banca Examinadora para obtenção do Grau de Bacharel, no Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC, com Linha de Pesquisa em Redes de Computadores.

Criciúma, 26 de Novembro de 2015.

BANCA EXAMINADORA

Prof. Paulo João Martins - MSc - (UNESC) - Orientador

Prof. Rogério Antônio Casagrande - MSc - (UNESC)

Prof. Valter Blauth Junior - Esp - (UNESC)

A meus pais e minha família que tornaram possível a realização do trabalho.

AGRADECIMENTOS

Primeiramente, gostaria de agradecer a Deus, ao meu orientador, Mestre Paulo João Martins, pelo incentivo, dedicação, apoio e paciência ao longo dessa jornada, e aos demais professores envolvidos do curso.

Aos meus pais que sempre me incentivaram nos estudos, aos meus amigos que muitas vezes entenderam minha ausência da vida social.

RESUMO

Hoje muitas pessoas que usam a rede sem fio, por questão de mobilidade e praticidade, na hora de configurar os seus dispositivos acabam não levando em conta aspectos de gerência que podem tornar a rede mais confiável e segura. O objetivo do trabalho é descrever e documentar os aspectos de gerência de uma rede sem fio, o seu monitoramento e a utilização de ferramentas, de forma a auxiliar os administradores de redes. O gerenciamento permite controle sobre os recursos da rede, assim como a identificação e prevenção de problemas, serviços melhores e controle de custo. Envolve cinco pontos: desempenho, segurança, falhas, configuração e contabilização. Foi realizado um planejamento com o *FreeRADIUS* para autenticação de usuários. Os *softwares* utilizados para monitorar a rede sem fio auxiliaram na observação e configuração da mesma. Informações demonstradas foram SSID, canal utilizado, qualidade do sinal, padrão 802.11 utilizado, endereço MAC do dispositivo, taxa máxima de transferência de dados. Com os resultados, pode-se compreender o quanto é importante fazer um levantamento da rede como um todo, auxiliando para evitar problemas com configurações e segurança.

Palavras-chave: Rede sem fio**.** Monitoramento. Segurança. RADIUS.

ABSTRACT

Today many people who use the wireless network, as a matter of mobility and practicality, when configuring your devices end up not taking into account aspects of management that can make the most reliable and secure network. The objective is to describe and document the aspects of management of a wireless network, their monitoring and the use of tools in order to assist network administrators. The management allows control over network resources, as well as the identification and prevention of problems, better service and cost control. It involves five areas: performance, security, fault, configuration and accounting. It conducted a planning with FreeRADIUS for user authentication. The software used to monitor wireless network assisted in the observation and configuration of the same. Demonstrated information was SSID, channel used, signal quality, 802.11 used, MAC address of the device, maximum rate of data transfer. With the results, one can understand how important it is to survey the network as a whole, helping to avoid problems with settings and security.

Keywords: Wireless network. Monitoring. Security. RADIUS.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
ANATEL	Agência Nacional de Telecomunicações
AP	Access Point
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
dBi	Decibel isotrópico
dBm	Decibel *Miliwatt*
DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
FHSS	Frequency Hopping Spread Spectrum
GHz	Gigahertz
HR-DSSS	High Rate Direct Sequence Spread Spectrum
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISO	International Organization for Standardization
LAN	Local Area Network
MAC	Media Access Control
MAN	Metropolitan Area Network
Mbps	Megabits por segundo
MIB	Manager Information Base
NAS	Network Access Server
OFDM	Orthogonal Frequency-Division Multiplexing
PAN	Personal Area Network
PDU	Protocol Data Unit
RF	Radiofrequência
RSN	Robust Security Network
RSSI	Received signal strength indicator
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol

SO	Sistema Operacional
SSID	Service Set Identification
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TMN	Telecommunications Management Network
UDP	User Datagram Protocol
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WWAN	Wireless Wide Area Network

SUMÁRIO

1 INTRODUÇÃO

O aumento significativo das informações, o grande interesse das pessoas em se comunicar e a mobilidade dos dispositivos vêm aumentando o uso das redes sem fio. Nesse contexto, alguns usuários vêm implantando este tipo de rede, desconsiderando as melhores práticas recomendadas para o uso desta tecnologia, no que tange o seu gerenciamento. Baseado nisso, percebe-se esta necessidade, de forma a tentar minimizar certos problemas, tais como, segurança, conectividade, ruídos, interferências e uso errado da rede. São adequadas a situações de mobilidade, flexíveis e de fácil instalação. Os dispositivos sem fio permitem criar, ampliar e interligar redes locais em ambientes internos ou externos, sem a necessidade da utilização de fios.

Essa flexibilidade admite a conexão do usuário com a rede em locais aonde cabos dificilmente chegariam ou seu lançamento seria inviável, como, por exemplo, prédios tombados pelo patrimônio histórico, onde não é permitida a alteração das características locais para passagens de cabos ou, ainda, em locais de condições similares. Ao contrário das cabeadas, onde os dados trafegam em um meio guiado e acondicionados e protegidos, nas sem fio os dados trafegam pelo ar, e, por isso, estão sujeitos a diversas variáveis, cujos resultados podem colaborar de forma negativa para o correto funcionamento da rede (COMER, 2007).

O uso das redes sem fio vem crescendo, observa-se uma redução associada ao seu custo e, assim, a mesma fica mais acessível. A mobilidade no acesso à *Internet* tornou-se mundialmente popular em residências, escritórios, aeroportos e cafés, porém seu uso se estende muito além. Dessa forma, são apresentados alguns cenários relevantes, como: na indústria, a demanda na troca de informações entre máquinas, computadores e pessoas, como, por exemplo, o uso de redes sem fio no gerenciamento e monitoramento de tanques de mistura por parte da indústria química. Outro cenário é o mercado de pequenas e médias empresas, sendo muito útil a interconexão de alta velocidade entre prédios de matrizes e filiais. Diante disso, dispensa o alto custo dos contratos praticado pelas operadoras de telecomunicações para a mesma finalidade (LOPES, 2003).

O crescimento das redes tem tornado a gerência de redes cada vez mais

complexa; por menor ou mais simples que seja uma rede, esta necessita ser gerenciada a fim de garantir aos usuários a disponibilidade de serviços. O gerenciamento permite controle sobre os recursos da rede, assim como a identificação e prevenção de problemas, serviços melhores e controle de custo. Ele envolve cinco pontos: desempenho, segurança, falhas, configuração e contabilização (KUROSE, 2006).

Nesse contexto, essa pesquisa realizou um levantamento dos *softwares* de gerenciamento e monitoramento de redes sem fio, com o intuito de concretizar um estudo de caso, em uma pequena rede sem fio, para descrever e documentar algumas práticas para auxiliar os administradores destas redes, na escolha dos *softwares*, bem como na utilização de ferramentas para gerenciamento de redes sem fio.

1.1 OBJETIVO GERAL

Descrever e utilizar ferramentas para gerenciamento e monitoramento de redes sem fio.

1.2 OBJETIVOS ESPECIFICOS

Os objetivos específicos seguem abaixo:

a) Entender e aplicar os conceitos de gerência de redes sem fio;
b) Estudar e aplicar *softwares* de monitoramento de redes sem fio;
c) Compreender aspectos de segurança a serem avaliados na implantação de uma gerência de redes;
d) Demonstrar o estudo de caso de ferramentas de monitoramento de uma rede sem fio;
e) Propor uma gerência de segurança centralizada de redes.

1.3 JUSTIFICATIVA

Com o amplo crescimento e o alto interesse pela criação de ambientes

com mobilidade no acesso à rede em instituições públicas e privadas, torna-se essencial um estudo aprofundado na área, ao planejar o impacto de novas instalações, sempre buscando qualidade, confiabilidade e respeito às normas técnicas e legislação da Agência Nacional das Telecomunicações (ANATEL).

Uma rede que não é gerenciada fica sujeita a falhas, que normalmente são difíceis de ser diagnosticadas e localizadas, por exemplo, como saber se a conexão está lenta ou sem acesso à *Internet*, bem como se um dos computadores do conjunto não tem o controle de quem está conectado à rede, compartilhando a rede com pessoas não autorizadas, ficando lenta e influenciando na segurança, sendo estes alguns dos fatores importantes para gerenciar uma rede *wireless*.

No *campus* de uma Universidade, prioriza-se a segurança e integridade dos dados na parte de base de informação no meio computacional, com um gerenciamento e monitoramento, em que todos os usuários são monitorados com o que estão fazendo na rede, não deixando que a mesma seja usada de maneira incorreta e imprópria, podendo todos ter acesso com a condição normal de conexão.

Muitos ambientes estão recebendo *Access Points* e roteadores *wireless*. O uso errado de tais equipamentos causa a perda total de controle e de monitoramento da rede, bem como mostra de forma irrelevante a infraestrutura e os mais diversos tipos de ataque possíveis. Dentre estes, se destacam a multiplicação de vírus e o uso de *softwares* P2P por conta de usuários que não conhecem e pela equipe de segurança não identificar tais usuários. Muitas vezes os próprios usuários destes tipos de redes não sabem os riscos aos quais estão expostos ao usar as redes sem criptografia, utilizando tais redes para trafegar dados confidenciais de forma insegura (LOPES, 2003).

A utilização de *softwares* de gerência de redes sem fio procura minimizar e auxiliar a descoberta de problemas e, de certa forma, antecipar um mecanismo de tratamento das situações que podem prejudicar o bom funcionamento da rede.

1.4 ESTRUTURA DO TRABALHO

Para facilitar o entendimento dos assuntos aqui abordados, este trabalho foi dividido em seis capítulos. O primeiro apresenta a introdução, objetivos e

justificativa, de forma a situar o leitor acerca dos assuntos tratados neste Trabalho de Conclusão de Curso.

No segundo capítulo, é apresentada uma visão geral sobre redes sem fio, descrevendo o que é a infraestrutura da mesma, como ela funciona, quais frequências, a multiplexação do sinal, entre outros aspectos.

No terceiro capítulo, são apresentados alguns problemas em uma rede sem gerenciamento, bem como o conceito, a definição, o propósito, os pontos positivos, alguns *softwares* utilizados, tanto livres como comerciais.

No quarto capítulo, são abordados os trabalhos relacionados ao tema proposto.

No quinto capítulo, são abordadas as metodologias, os *softwares* utilizados de monitoramento e de gerenciamento, resultados obtidos.

No sexto capítulo, são apresentadas as conclusões sobre o trabalho.

2 REDES SEM FIO

Com a *Internet* diminuindo as fronteiras entre as pessoas em ambientes de trabalho, escolas e residências, tanto nas cidades quanto na zona rural, estão fazendo uso dessa tecnologia. Este cenário mostra a evolução das tecnologias a fim de serem utilizadas na comunicação das pessoas, nos mais remotos lugares. Nakamura e Geus (2007) salientam que o investimento aplicado cada vez mais, de forma a obter uma comunicação de boa qualidade e sem dificuldade no uso, com comodidade, sendo eficaz, resultou no uso notável da tecnologia de rede sem fio.

Conforme Tanenbaum e Wetherall (2011), essas tecnologias usam ondas de rádio para a transmissão dos dados, ou seja, todas as informações são transmitidas por meio do ar, meio este que pode ser facilmente interceptado por terceiros.

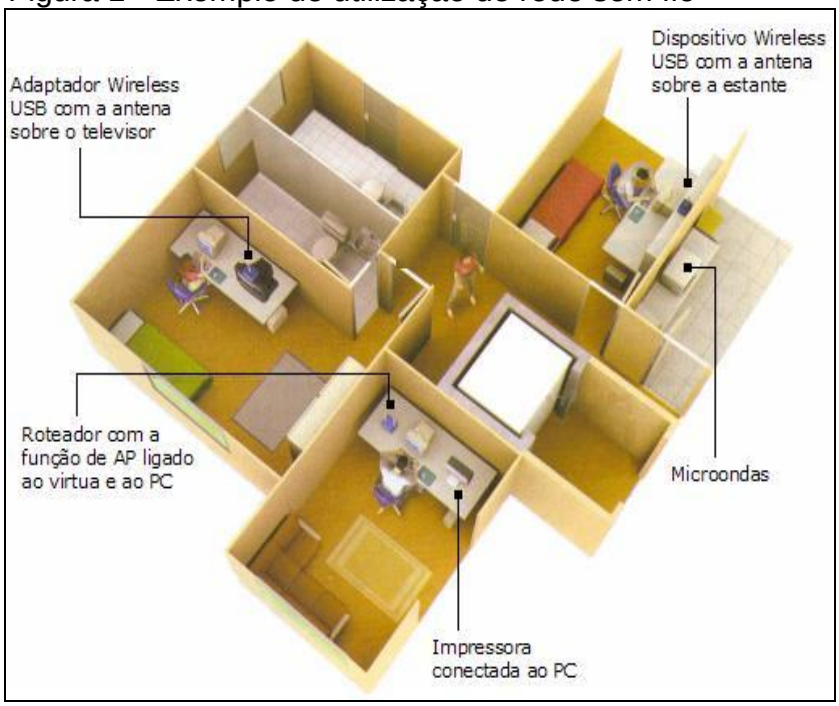
De acordo com Comer (2007), ao invés de fios, utilizam-se antenas para transmitir o sinal em rádio frequência, pelo ar, compartilhando o sinal localmente, com isso a troca de pacotes entre os computadores.

Segundo Tanenbaum e Wetherall (2011), persistem três principais categorias em redes sem fio:

a) interconexão de sistemas;
b) LANs sem fio;
c) WANs sem fio.

A interconexão de sistemas é a conexão de equipamentos de um computador utilizando ondas de rádio com o alcance restringido, como, por exemplo, *mouses* sem fio, pois utilizam a tecnologia *Bluetooth* para a conexão do dispositivo com o computador, sem a utilização de cabos (TANENBAUM; WETHERALL, 2011). Na figura 1, mostra-se exemplo de utilização da rede sem fio.

Figura 1 - Exemplo de utilização de rede sem fio

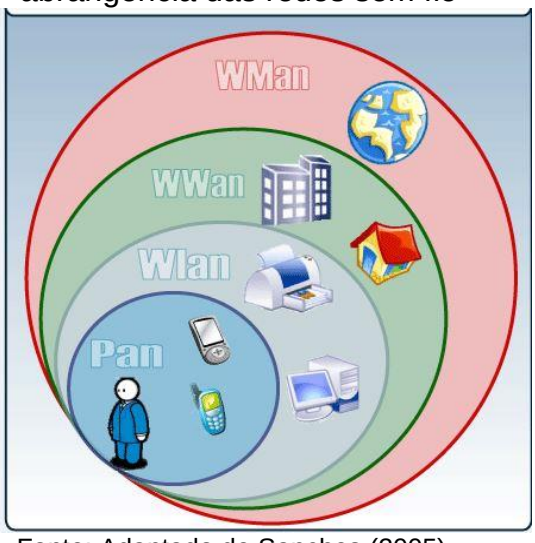


Fonte: Fortes (2004).

2.1 CARACTERÍSTICAS

Há conceitos específicos para redes sem fio, outros foram/vieram das redes cabeadas. Essas características estão ligadas às camadas perto do *hardware,* que tem influência na rede, na forma como as transmissões são realizadas (RUFINO, 2005). Na figura 2, há a classificação pela abrangência das redes sem fio.

Figura 2- Classificação pela abrangência das redes sem fio



Fonte: Adaptado de Sanches (2005)

Redes de área pessoal (PAN): são curta distância que se tornaram disponíveis, com a ambição de substituir o emaranhado de cabos que move dados entre dispositivos, como teclado, *mouse*, fone de ouvido, entre outros. Hoje ainda há a disponibilidade dos mesmos sem fio, como *Bluetooth* (CHANDRA et al., 2008, tradução nossa).

Redes locais sem fio (WLAN): os equipamentos ligados à rede necessitam ter um *modem* e uma antena de rádio para que possam se comunicar entre si diretamente ou por meio de concentradores de acesso, chamados *de Access Points* (AP). Essas redes estão sendo cada vez mais usadas em pequenas empresas e residências, onde a instalação com cabos é muito demorada e pode apresentar problemas na infraestrutura (TANENBAUM; WETHERALL, 2011).

Redes de longa distância (WWANs): permitem que sejam criadas redes geograficamente distribuídas. Alguns exemplos são: interligação de empresas, redes para telefonia celular e distribuição de *Internet* banda larga sem utilização de linha telefônica. Essas redes têm os aspectos semelhantes às LAN sem fio, o diferencial é o fato de que as distâncias entre elas são muito maiores (TANENBAUM; WETHERALL, 2011).

Redes metropolitanas sem fio (WMANs): utilizadas para conectar diferentes edifícios e instalações situadas na região de uma cidade ou povoado. São geralmente de propriedade de empresas de telefonia (CHANDRA et al., 2008, tradução nossa).

2.1.2 Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

Em redes de comunicação, diversas regras são necessárias para que o acesso seja compartilhado de forma efetiva entre todos os nós da rede. Hoje, o método mais utilizado em redes *wireless* é o CSMA/CA (COLEMAN; WESTCOTT, 2006, tradução nossa).

Nesta série de regras específicas, para que uma estação da rede possa transmitir, é necessário que esta verifique se algum outro dispositivo já esteja utilizando o meio. Durante este tempo, a estação continua monitorando o meio, a fim de assegurar que outro equipamento não esteja transmitindo, e só então começa

sua transmissão. Caso não esteja disponível, o protocolo manda instruções para que a estação entre em uma fila de prioridade para depois poder transmitir (ROSS, 2008, tradução nossa).

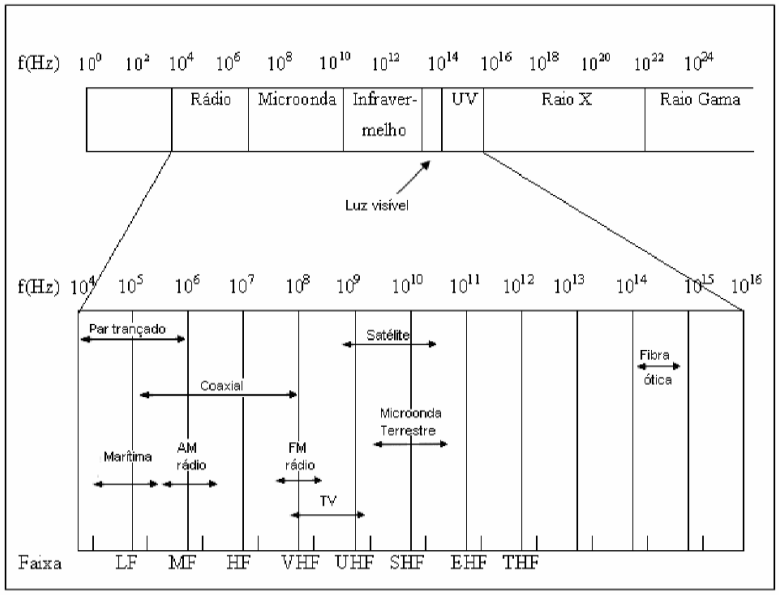
Este processo garante que apenas um nó seja transmitindo de cada vez. Isso ocorre porque as redes sem fio operam utilizando o mesmo canal, tanto para transmissão quanto para recepção, por isso não tem a capacidade de transmitir e detectar colisões simultaneamente (RUFINO, 2005).

2.3 FREQUÊNCIAS DE TRANSMISSÃO

As informações trafegam por ondas eletromagnéticas, que não utilizam os fios como na rede cabeada. As ondas podem trafegar por muitos metros ou quilômetros (COMER, 2001).

Com o movimento dos elétrons, são geradas essas ondas e frequências, que são as oscilações medidas em Hertz (Hz). Esse conjunto é denominado de espectro eletromagnético, conforme a figura 3 (TANENBAUM; WETHERALL, 2011):

Figura 3 - Espectro eletromagnético



Fonte: Adaptado de Tanenbaum e Wetherall (2011).

2.3.1 Antenas

São dispositivos utilizados para emitir sinal sem fio, sendo elas internas ou externas, como também em relação à direção que o sinal vai. Essas antenas são as direcionais que irradiam em uma direção apenas e as antenas omnidirecionais, que irradiam em um ângulo de 360 graus.

Figura 4 – Antena direcional setorial

Fonte: Mendes(2008)

Na figura 4, há a antena setorial, que é utilizada para atender uma determinada região. O ângulo de abertura pode ser 30, 60, 90 e 120 graus. O modelo STC-1624-S trabalha na frequência de 2.4Ghz, com potência de 16dBi (MENDES, 2008).

Figura 5 – Antena direcional grade

Fonte: Mendes(2008)

A antena da figura 5, que também capta sinais em apenas uma direção, na forma concentrada, utiliza uma grade que reduz a possibilidade de o vento mudá-la de lugar, ela trabalha na frequência 2.4Ghz, com potência de 25dB (MENDES, 2008).

Figura 6 – Antena omnidirecional

Fonte: Mendes(2008)

Na figura 6, mostra-se a antena omnidirecional, que com um ângulo que abrange ao redor dela, proporciona aos usuários conexão de qualquer lado. Ela trabalha na frequência de 2.4Ghz, com potência média de 16dBi (MENDES, 2008).

2.4 ARQUITETURA DO PROTOCOLO IEEE 802.11

As atividades mostradas pelo protocolo IEEE 802.11 utilizam a camada física e a camada de enlace, sendo direto na subcamada MAC. As outras camadas têm fatores diferentes, como endereçamento, integridade e formato de dados, não modificando se a transmissão for com rede sem fios ou por rede com cabos (ANDRADE, 2004).

O padrão 802.11 foi lançado em 1997 para rede sem fio, que utiliza os recursos de modulação *Direct Sequence Spread Spectrum* (DSSS) e *Frequency Hopping Spread Spectrum* (FHSS). Novas tecnologias com técnicas de modulação de sinal para melhorar foram desenvolvidas em 1999, sendo elas: *Orthogonal Frequency Division Multiplexing* (OFDM) e *Hight Rate Direct Sequence Spread Spectrum* (HR-DSSS).

2.4.1 Modulação de Sinal FHSS

Chamado de espectro de dispersão de saltos de frequência, utiliza 79 canais, começando na extremidade baixa da banda da *Industrial Scientific and Medical* (ISM) de 2,4 GHz, cada um contém 1 MHz de largura. A sequência de frequência de saltos é definida por meio de um gerador de saltos aleatórios, que são definidos por um gerador de números pseudoaleatórios, em que cada um desses números corresponde a uma frequência. A randomização oferece segurança, pois um invasor que não conhece a sequência dos saltos não poderá espionar as transmissões (TANENBAUM; WETHERALL, 2011).

Em longas distâncias, esta modulação apresenta bom desempenho. Como desvantagem, apresenta baixa largura de banda.

2.4.2 Modulação de Sinal DSSS

Neste método de modulação, o espectro de dispersão de sequência direta, da mesma forma que o FHSS, utiliza banda ISM de 2,4 GHz. A modulação é realizada por meio de quebra de sequência, conhecida como código de Barker.

O código de Barker consiste em substituir cada bit de valor 1 (um) por uma sequência de bits, enquanto o bit de valor 0 (zero), pela sequência oposta. Com essa redundância de valores, fica muito mais fácil de corrigir e controlar erros ocorrentes nas transmissões. O DSSS é utilizado no padrão IEEE 802.11b e é menos vulnerável a ruídos e ataques.

2.4.3 Modulação de Sinal OFDM

A multiplexação ortogonal por divisão de frequência pode transmitir até 54 Mbps na banda ISM mais larga, de 5 GHz. São utilizadas 42 frequências para dados e 4 para sincronização. Uma melhor imunidade à interferência é alcançada por meio da divisão de uma banda larga em várias bandas estreitas (TANENBAUM; WETHERALL, 2011).

Essa técnica tem boa eficiência de bits/Hz e boa imunidade em longas distâncias, utilizando vários caminhos, sendo esta modulação utilizada pelo IEEE 802.11a.

2.4.4 Modulação de Sinal HR-DSSS

É uma versão derivada da modulação DSSS, foi criada com a intenção de aumentar a velocidade de transmissão. Nela, são utilizados 11 milhões de *chips* para alcançar 11 Mbps na banda de 2,4 GHz. As taxas de dados admitidos são 1, 2, 5, 11, Mbps e podem ser adaptadas durante a operação para alcançar a melhor velocidade sob as condições atuais de carga e ruído. Este tipo de modulação é utilizado no padrão IEEE 802.11b (TANENBAUM; WETHERALL, 2011).

2.5 PADRÕES PARA REDES SEM FIO 802.11

O sinal sem fio trafega por meio de ondas de rádio, porém muitos outros meios de transmissão usam este método, com isso existem riscos de interferência nas transmissões (PETERSON; DAVIE, 2004).

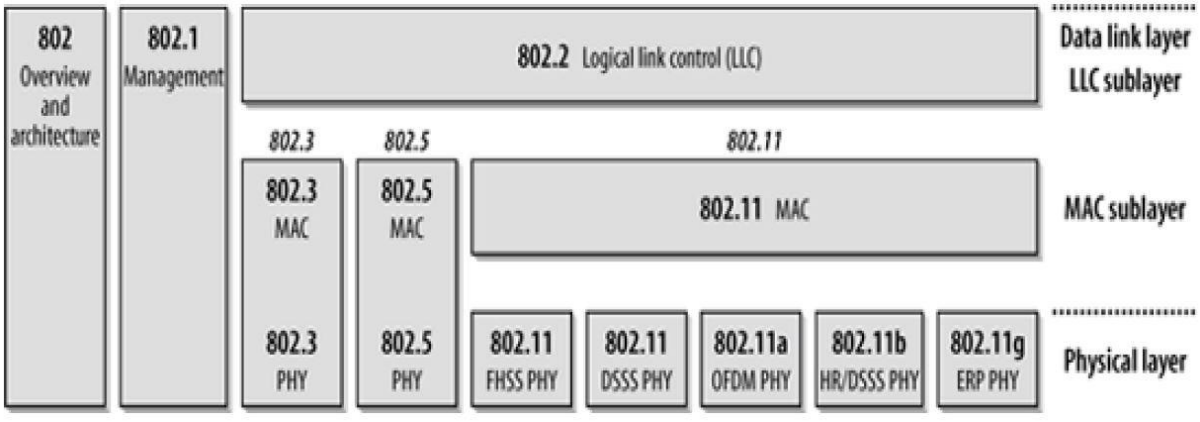
Com o objetivo de evitar que estes danos prejudicassem as transmissões, os sinais de radiofrequência foram divididos em faixas, geralmente por sua categoria de serviços, e definidos por órgãos regulamentadores ou padrões internacionais (COZER, 2006).

Os padrões de redes sem fio que se conhece foram criados pelo *Institute of Electrical and Electronics Engineers* (IEEE), que criou os padrões utilizados por outros tipos de redes. Eleito para criar na década de 90.

Em 1997, espelhando-se em regras que já existiam, foi lançado o IEEE 802.11, com normas voltadas às redes sem fios, procurando o aumento na confiabilidade de transmissão, com qualidade de sinal e uma padronização de equipamentos (COSTA, 2009). Como aspecto, possuía frequência de 2,4 GHz e taxa de transmissão de 2 Mbps (SILVA, 2006).

No padrão IEEE 802.11, relaciona-se à camada física e à camada de enlace limitada à sub-camada, estabelecido no padrão IEEE 802.11 como *Media Access Control* (MAC) (MENDES, 2008). Na figura 7, há a relação do 802.11 com o OSI:

Figura 7 - A família IEEE 802 e sua relação com o modelo OSI



Fonte: Adaptado de Gast (2005)

Será apresentado um pouco das características dos sub-padrões da IEEE 802.11 mais conhecidas: 802.11b, 802.11a, 802.11g, 802.11i, 802.11n e outros (COSTA, 2009).

Tabela 1 - Padrões de redes sem fio

Padrões de redes sem fio	Descrição
802.11a	Segunda versão lançada com frequência de 5,8 GHz, porém com menor alcance. Aceita 64 clientes conectados por AP, sua modulação consiste em 12 canais sobrepostos que permite uma melhor cobertura de áreas mais povoadas (COSTA, 2009). A segurança se baseia no protocolo WEP de 256 bits (COZER, 2006). O diferencial está no desempenho, pode atingir uma taxa de transferência de 54 Mbps, sendo cinco vezes mais rápida que o padrão IEEE 802.11b. Há problemas de incompatibilidade com outros dispositivos, pois opera em 5 GHz (FRASSON JUNIOR , 2008).
802.11b	Foi o primeiro sub-padrão lançado, em 1999, com velocidade máxima de 11 Mbps, mas se comunica com menos velocidade, usando a faixa 2,4 GHz (FRASSON JUNIOR , 2008). Trabalhando em uma faixa mais baixa, causa interferência de outros dispositivos que usam a mesma faixa. Permite conexões com 32 clientes por AP (COSTA, 2009). Está classificado como o mais popular, com uma tecnologia simples e de baixo investimento. Para clientes que não exigem muito, é aceitável (COZER, 2006).
802.11d	A compatibilidade faz o *hardware* operar em outros países, como o IEEE 802.11a que não opera na Europa.
802.11e	Permite que o tráfego de diferentes classes de tráfego na transmissão, com recurso de *Transmission Oportunity* (TXOP), permitindo a transmissão em rajadas, com uma melhor utilização da rede (COSTA, 2009).
802.11g	Surge como o sucessor do padrão IEEE 802.11b. Utiliza a banda de 2,4 GHz e permite que equipamentos dos padrões IEEE 802.11a e IEEE 802.11b sejam compatíveis (RUFINO, 2005). Usa a modulação complexa OFDM, com taxa de transmissão de 54 Mbps (FOUROZAN, 2006).
802.11h	Com dois mecanismos para melhorar a transmissão via rádio: a TPC permite que o rádio ajuste a potência do sinal de acordo com a distância do receptor e a tecnologia DFS permite a escolha automática

	de canal, minimizando interferência em sistemas operando na mesma banda (RUFINO , 2005).
802.11i	Segundo Costa (2009), este padrão se destaca pela busca da segurança e a autenticação dos dados por meio dos protocolos de segurança RSN (*Robust Security Network*) e *WAP Wi-Fi Protected Access*, para ter soluções mais robustas, em relação ao padrão *Wired Equivalent Privacy* (WEP). Há *Wired Equivalent Protocol* (WEP), *Temporal Key Integrity Protocol* (TKIP), *Advanced Encryption Standard* (AES) e IEEE 802.1x para autenticação e segurança.
802.11j	Usa as bandas que operam nas faixas 4.9 GHz e 5 GHz, há no Japão. (COZER, 2006).
802.11k	Possibilita um meio de acesso para *Access Points* transmitir dados de gerenciamento; utilizado na indústria para permitir transições transparentes do Conjunto Básico de Serviços no ambiente WLAN. Fornece informações para escolher de maneira a ter um melhor ponto de acesso que garanta o QOS necessário (COSTA, 2009).
802.11n	Com taxas de transferências disponíveis de 65 Mbps a 300 Mbps, a transmissão é MIMO-OFDM e a faixa de frequência é de 2,4 GHz e/ou 5 GHz (RUFINO ,2005).
802.11ac	Iniciado em 2012, opera em faixa de 5 GHz (menos interferência), com taxas nominais maiores que utilizam velocidade de até 1 Gbps, como no padrão 802.11n. Utiliza múltiplas conexões de alta velocidade para transferir conteúdo, em vez de propagar as ondas de modo uniforme para todas as direções. Os roteadores *Wi-Fi* reforçam o sinal para os locais onde há computadores conectados. Traz a possibilidade de conversar simultaneamente com diversos aparelhos conectados ao roteador, sem nenhuma interrupção. No padrão "N", só permite que essa conversa fosse feita com um dispositivo por vez. Com esse padrão, pode-se ter economia de energia nos dispositivos móveis (GAST, 2013).
802.11p	Usado na rede sem fio de veículos WAVE (*Wireless Access in Vehicular Environments*) (COZER, 2006).
802.11r	Padroniza o *hand-off* rápido quando um cliente *wireless* se reconecta ou quando estiver andando de um ponto de acesso para outro na mesma rede (RUFINO ,2005).
802.11s	Padroniza *self-healing/self-configuring* em Redes *Mesh* (malha) (COZER, 2006).
802.11t	Tem o objetivo de organizar métodos de medida e de métricas de desempenho em laboratórios independentes de teste (RUFINO ,2005).
802.11v	O padrão pode tem paradigmas de gerência semelhantes com os usados em redes de celulares.
802.11x	Não é usado, pois se confunde com o 802.1x.
802.11w	Criado para aumentar a segurança da transmissão dos pacotes de

	camada física.
802.11z	Usado para habilitar o equipamento sem fio, operando na frequência entre 3650 a 3700 MHz. Usado só nos Estados Unidos.

Fonte: Da pesquisa

2.6 TOPOLOGIA DE REDES WIRELESS

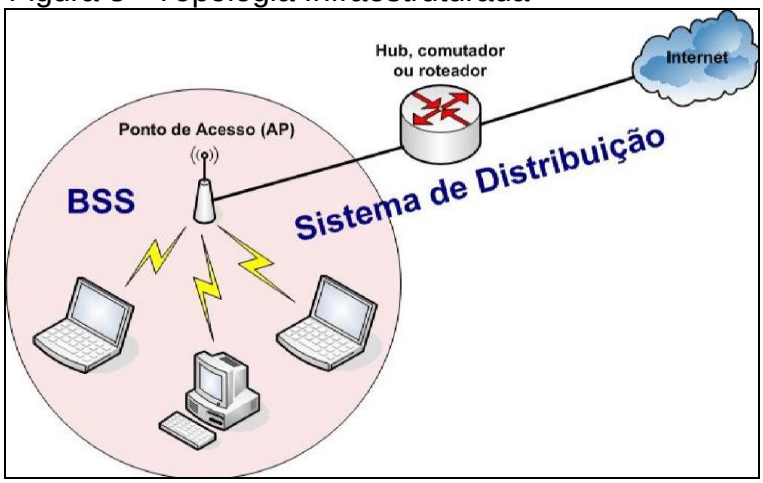
A topologia é um mapa da rede, sendo o lugar onde estão os computadores e equipamentos definidos na topologia física. Um planejamento mal elaborado de uma rede pode trazer mais tarde gastos desnecessários e prejudicar o desempenho dos recursos oferecidos.

As redes sem fio levam como critério de organização dois modos distintos, o Ad Hoc e a Infraestrutura.

2.6.1 Infraestrutura

Uma rede BSS ou Infraestrutura atua quando as estações são conectadas entre si ou com outras redes, usando um ponto de acesso (SANCHES, 2005). Na figura 8, mostra-se a topologia:

Figura 8 - Topologia Infraestruturada



Fonte: Adaptado de Rosnam e Leary (2003).

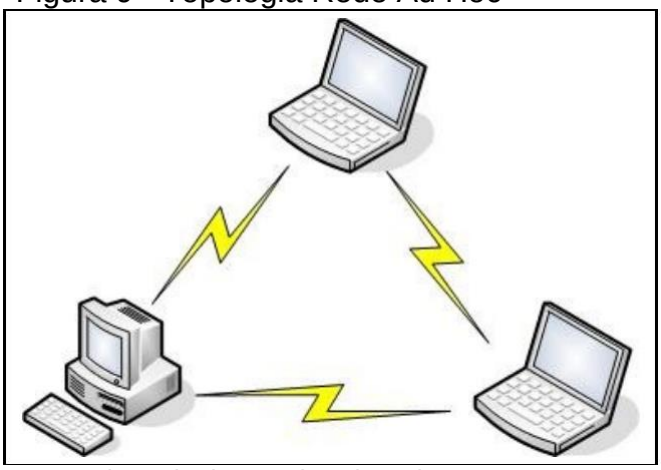
O tráfego entre as estações é obrigado a passar pelo AP, adicionando a comunicação entre os equipamentos que estão na mesma área de serviço (GAST, 2005, tradução nossa).

2.6.2 Ad Hoc

Nesta infraestrutura, há as estações que se comunicam uma com a outra de forma direta, sem precisar de um ponto de acesso, sendo que tem uma área de alcance limitada, conforme cada equipamento (GAST, 2002, tradução nossa).

É normalmente utilizada para fins específicos e esporádicos, como, por exemplo, compartilhamento de arquivos entre estações. Com isso, forma-se a rede conforme a necessidade, utilizando de equipamentos próximos aos outros e em locais sem uma infraestrutura. A rede pode ser formada por equipamentos portáteis, a fim de trocar dados quando não há pontos de acesso, exemplo, salas de conferências, trens ou até um carro (KUROSE; KEITH, 2007). Na figura 9, mostra-se a Arquitetura Rede Ad Hoc.

Figura 9 - Topologia Rede Ad Hoc



Fonte: Adaptado de Sanches (2005)

2.7 SEGURANÇA

A tecnologia de redes sem fio já conquistou grande parte das empresas ou corporações. Contudo, ainda existem restrições quanto ao seu uso para transmitir informações sigilosas ou críticas, principalmente pelo fato do meio de transmissão ser de domínio público e normalmente se estender para além da área geográfica da organização (RIBAS, 2002). Devido a essas características, as redes sem fio possuem vulnerabilidades que instigam tentativas de ataque. Logo, torna-se

necessário conhecer os detalhes dos vários tipos de ataques praticados, a fim de preparar defesas (FLECK; POTTER, 2002, tradução nossa).

> As ferramentas disponíveis para monitoração e até controle de redes sem fio não são projetadas com intenção nociva. Na sua maioria, elas foram desenvolvidas para demonstrar que fraquezas potenciais eram na verdade brechas de segurança. Os administradores de rede precisam desses tipos de ferramentas para entender como melhor proteger os dados que fluem por suas redes. Também são extremamente úteis para procurar por redes sem fio abertas quando você estiver em trânsito, para solucionar certos tipos de problemas de rede em sua própria rede e para planejar uma nova rede sem fio (ENGST; FLEISHMAN, 2005, p. 279).

2.7.1 Wired Equivalent Privacy (WEP)

É uma chave que compartilha uma senha utilizada para criptografar e descriptografar o tráfego de dados sem fios, em que somente serão lidas pelos outros dispositivos que possuam a mesma chave. A chave WEP é armazenada em cada computador da rede, de modo que os dados possam ser criptografados e descriptografados à medida que são transmitidos por ondas de rádio, na rede sem fios.

A criptografia pode ser realizada de dois modos: 64 bits, que compreendem cinco caracteres alfabéticos ou 10 números hexadecimais, ou 128 bits, que compreendem 13 caracteres alfabéticos ou de 26 números hexadecimais.

Nos algoritmos deste protocolo, foram encontradas algumas vulnerabilidades, não sendo muito confiável para a segurança. Alguns valores permitem a quebra da chave secreta, o protocolo ainda é utilizado pelas pessoas, sendo considerado um nível básico de proteção (GRÜNEWALD, 2005).

2.7.2 Wi-Fi Protected Access (WPA)

Com um nível maior de proteção e controle de acesso, utiliza-se a chave mestra compartilhada, sendo mais robusta. A chave pode ser atribuída por um servidor de modo dinâmico, com uma gestão centralizada para controle de acesso na autenticação (MORENO, 2005).

Em casas ou pequenas empresas, o WPA é executado de um modo casa especial, que é *Pre-Shared Key* (Chave pré-compartilhada – PSK), utilizando senhas em que a pessoa manualmente fornece para ter segurança.

Embora tanto as chaves WEP de 64 quanto as de 128 bits sejam vulneráveis, é recomendado usar chaves de 128 bits, sendo uma barreira a mais para sua quebra.

2.7.3 Wi-Fi Protected Access 2 (WPA2)

Baseia-se no padrão IEEE 802.11i e utiliza criptografia protocolo *Advanced Encryption Standard* (AES). Suporta as características adicionais de segurança do padrão 802.11i, não incluídas em equipamentos que suportam WPA. Assim como o WPA, o WPA2 provê autenticação e criptografia, propondo a garantia de confidencialidade, autenticidade e integridade em redes sem fio. Uma vantagem boa é que ele é compatível com o WPA, permitindo a utilização, além do AES, do TKIP e do EAP (SOUZA, 2005).

2.8 SITE SURVEY

O *Site Survey* é um método de análise de redes sem fio usado na implantação da mesma, visando à utilização de *softwares* para analisar a qualidade do sinal de transmissão, procurando problemas na rede que possam estar interferindo na qualidade da mesma (PINHEIRO, 2004). Nas redes que já existem, verificam-se as interferências, os dispositivos, entre outros. Com a conclusão, aplica-se as soluções necessárias para resolver os problemas encontrados (RODRIGUES; SANTOS, 2007).

Ele é classificado em duas categorias: *indoor* e *outdoor*. No *indoor,* realiza-se uma análise de interferências na rede sem fio, com relação aos APs localizados na área de teste, com gráficos de intensidade simples de compreender, sendo realizado em pequenos espaços. Essa pesquisa pode ser realizada em perímetros fechados, tipo *mono* ou *multifloor,* que se aplicam em um ou mais andares (GEIER, 2002). No *outdoor,* realizam-se testes de redes sem fio em perímetros maiores, englobando antenas de transmissão de grande porte, somando-se a vários APs na busca por interferências (GEIER,2002).

Como já mencionado anteriormente, o *Site Survey* pode ser aplicado tanto no projeto para novas redes sem fio quanto para análise de redes já existentes. A

metodologia em si envolve procedimentos no qual visam dimensionar adequadamente o local de instalação dos equipamentos transmissores e receptores de sinais RF, a fim de que todas as estações possam desfrutar de qualidade nas conexões (RODRIGUES; SANTOS, 2007).

Além dos dispositivos, pode ser aplicado este mecanismo para obter mapas ou plantas dos locais, utilizar um *software* com o funcionamento de acordo ao pretendido na inspeção, realizar uma visualização do local antes da aplicação, percorrer todo local para capturar os sinais de RF, reunir os resultados obtidos e compará-los, facilitando a compreensão.

3 GERENCIAMENTO DE REDES

Energia elétrica, água, telefone, todas essas organizações utilizam essa infraestrutura. Normalmente estas questões são seguras. Para que isso ocorra, elas são monitoradas e gerenciadas para o correto funcionamento, mostrando que a monitoração e o controle são necessários (CORREIA, 2004).

Toda rede de computadores, por menor e mais simples que seja, precisa ser gerenciada para garantir aos seus usuários a disponibilidade dos serviços, a um nível de desempenho aceitável. À medida que a rede cresce, aumenta a complexidade de seu gerenciamento, forçando a adoção de ferramentas automatizadas para a sua monitoração e controle.

A gerência de rede, englobam-se monitoramento e controle da rede com o uso de *softwares*, *hardwares* e conhecimentos de profissionais especializados. Com isso, obtém as informações da rede, diagnostica os possíveis problemas e encaminha as soluções; a forma errada de colocar esses elementos em um projeto, compromete-se o ambiente de rede como um todo (DANTAS, 2002).

Pensando de forma estruturada, a ISO dividiu o gerenciamento de redes em cinco áreas funcionais: falhas, configuração, contabilização, desempenho e segurança.

3.1 TIPOS DE GERÊNCIA DE REDES

Temos a monitoração e controle de rede onde na monitoração onde se analisa o estado das configurações e seus componentes, já no controle de rede se altera parâmetros e execução de determinada ação (DANTAS,2002).

Na monitoração se observa em modo estático a configuração atual como a identificação de portas no dispositivo; em modo dinâmico se observa os eventos como a transmissão de um pacote em modo estatístico como uma média de pacotes transmitidos em tempo em um sistema (STALLINGS, 2005).

No controle da rede temos a garantia de qualidade de serviços priorizando trafego de aplicações críticas; analisar o desempenho atual da rede; planejar o crescimento da rede com hardwares; avaliar o empaqueto de um novo

sistema de tomada dê decisão na rede; identificar e controlar os dispositivos periodicamente e softwares e conhecer a configuração e localização de todos os elementos da rede (DANTAS, 2002).

Com a gerência centralizada o processo é controlado de um ponto de gerência. Com o crescimento da rede, os problemas ficam mais críticos (LOPES, 2003).

Algumas vantagens são o processo de gerência mais simples, sendo que a informação necessária se encontra em um único local, ajudando a localizar erros e a relacionar os mesmos. Há mais segurança no acesso às informações, tendo a necessidade de um único ponto de acesso para controlar (DANTAS, 2002).

Como desvantagens a maior possibilidade de falhas no gerente com toda a base de dados; necessidade de cópia total da mesma para redundância do sistema, tornando difícil a expansão com uma baixa escalabilidade; muito tráfego de dados no gerente (STALLINGS, 2005).

Na gerência descentralizada as atividades são distribuídas com vários nós responsáveis pelo gerenciamento. O trabalho pode ser feito de forma hierárquica, sendo que cada nó fica responsável por um tipo de atividade gerencial.

As vantagens são a gerência não depende de um único sistema, tem uma distribuição das tarefas em cada gerente, o tráfego é balanceado. A desvantagem é: muitas réplicas de bases de dados (DANTAS, 2002).

Temos a gerência reativa quando os administradores de rede são alertados de problemas que ocorrem na infraestrutura para agir com uma solução, sendo o processo feito depois que ocorre a falha e perda de conexão ou queda de desempenho. Para resolver o problema, segue uma sequência que é detectar a falha, isolar, corrigir e documentar (STALLINGS, 2005).

Com gerência proativa o administrador pesquisa diariamente informações para ajudar a antecipar problemas. Com isso, usam-se meios estatísticos e monitoramentos diários para acompanhar as mudanças de comportamento e, assim, antecipar as falhas e perdas de desempenho (DANTAS,2002).

Usualmente a gerência de redes é dividida em três etapas:

a) **Balanço de dados**: é um processo normalmente automático, que compreende a monitoração sobre os meios gerenciados e que tem, da mesma forma, guardados em arquivos de log;
b) **Diagnóstico de valor e sítio de onde o empregar**: tem o tratamento e a análise feitos com os dados coletados, sendo também feito a detecção do que causou o problema no meio gerenciado. O computador de gerenciamento faz vários procedimentos manuais ou automáticos com a intervenção de um operador ou não, a fim de encontrar e resolver a causa do problema mostrado no recurso gerenciado (DANTAS, 2002);
c) **Ação fora de teoria**: com o diagnóstico do problema, há necessidade de uma ação ou controle sobre o recurso.

3.2 ELEMENTOS DE UM SISTEMA DE GERÊNCIA DE REDES

Um sistema de gerência de redes genérico é constituído por quatro elementos básicos (LOPES, 2003):

a) **Gerente**: um computador conectado à rede com *software* de protocolo de gerenciamento, solicitando informações dos agentes;
b) **Agente**: um *software* que roda um elemento ou sistema gerenciado, exportando uma base de dados de gerenciamento MIB para que o gerente possa ter acesso às informações;
c) **Management Information Base (MIB):** banco de dados de objetos gerenciados como uma tabela, em que são armazenados os dados coletados para serem enviados ao gerente (MAURO; SCHMIDT, 2005);
d) **Protocolo de gerenciamento**: fornece a comunicação entre o gerente e o agente.

3.3 MODELOS DE GERÊNCIA

São cinco modelos de gerência, sendo: *telecommunications management Network* (TMN); *Operation*, *Administration*, *Maintenance and Provisioning* (OAM&P); *Telecom Operations Map* (TOM); *Common Management* Inforimation *Protocol/ Common Management Information Service* (CMIP/CMIS); *Simple Network Management Protocol SNMP* e *Fault, Configuration, Accounting, Performance, Security (FCAPS).*

a) **TMN:** o objetivo é fornecer uma arquitetura organizada que permita interligar diversos tipos de sistema de operação de gerência de equipamentos e telecomunicação pelo uso de interfaces, protocolos e mensagens padronizadas. É possível ligar atributos e sistemas heterogêneos de vários fabricantes, possibilitando que os atributos, como redes locais, de longa distância, metropolitanas, *pabx*, dispositivos de telefonia móvel, estejam administrados de forma unida (LOPES,2003);

b) **OAM&P:** usado diariamente em um ambiente de rede que acha, diagnostica e corrige falhas, com isso fazendo o sistema funcionar normalmente (LOPES, 2003);

c) **TOM:** criado pelo *Telemanagement Forum*, ficando no lugar do modelo *Telecommunication Network Management* (LOPES, 2003);

d) **CMIP/CMIS**: é usado por algumas operadoras de telecomunicação, gerando no sistema de gerência da rede um mapa de projeto (LOPES, 2003);

e) **SNMP:** é o protocolo de gerenciamento de redes utilizado na *Internet*, do nível de aplicação, que utiliza UDP para transporte, utilizando três operações genéricas: *Get*, *GetRequest* e *GetNextRequest*. Ele pode apenas ler ou alterar o conteúdo de variáveis, que são instâncias de objetos gerenciados, possuindo três versões diferenciadas com níveis de segurança (DANTAS, 2002);

f) **FCAPS:** com o desenvolvimento do modelo OSI pela ISO, foram definidos os conceitos de áreas funcionais, modelos de informação para representar recursos de rede e protocolos para transferência de informações sobre gerências de rede. Ele serve de base para todos os demais, por definir as áreas funcionais da gerência de redes, que são: gerência de falhas, configuração, contabilidade, desempenho e segurança (DANTAS, 2002).

Na tabela 2, é apresentada a relação dos modelos de gerência de redes e suas principais características:

Tabela 2 - Principais características dos modelos

Modelo de gerência	**Órgão responsável**	**Tipo de gerenciamento**	**Utilização**
FCAPS	ISSO	Falhas, configurações, desempenho, contabilidade e segurança.	Estrutura conceitual popular para gerência de redes.
TMN	ITU-T	Negócios, serviços, redes e elementos.	Estrutura conceitual popular para gerência de redes, voltada para provedores de serviços de telecomunicações.
OAM&P	Provedores de Serviço	Operação, manutenção, administração e provisionamento.	Utilizado em redes de grandes provedores de serviços.
TOM	TeleManagement Forum	Redes e sistemas, desenvolvimento de serviços e operações e atendimento ao usuário	Ainda em estágio conceitual.
CMIP/CMIS	ISSO	Desempenho, falhas e configurações.	Desenvolvimento limitado baseado em redes, no modelo OSI.
SNMP	IETF	Desempenho e falhas.	Amplamente utilizado em redes de dados, especialmente em redes baseada no TCP/IP.

Fonte: Lopes (2003)

3.4 MODELO FCAPS

O modelo foi adotado no trabalho descrevendo cada parte do modelo, a fim de um melhor entendimento. As cinco áreas nele contidas são: falhas, configurações, desempenho, contabilidade e segurança.

3.4.1 Gerenciamento de falhas

Em uma rede funcionando, o administrador tem que cuidar para que o sistema todo, bem como cada componente individual, funcione normalmente. Quando ocorre uma falha, é importante agir rapidamente, a fim de determinar onde está o problema; observando o ocorrido, isola-se o resto da rede para certificar que a mesma continue funcionando normalmente sem interferências. Então, executa-se uma análise na configuração para minimizar o impacto feito pela falha e repara-se ou substitui-se o componente, fazendo a rede voltar ao seu estado normal (DANTAS, 2002).

Muito importante é o conceito de falha. Ela não é o mesmo que erro. Uma falha é uma condição anormal que precisa ser gerenciada, já um erro é um evento único. A falha ocorre por não operar normalmente ou por exagerada quantidade de erros (STALLINGS, 2005).

3.4.2 Gerenciamento de contabilidade

Em redes corporativas, o uso dos serviços na rede é cobrado, por assim dizer. São procedimentos contábeis internos, mas, no lugar do pagamento com dinheiro real, pode ser o uso de papel em uma impressora com cota, durante um mês. O administrador da rede pode monitorar o uso dos recursos de rede de cada usuário ou um grupo. Uma ou mais pessoas podem usar de mais a rede, sendo capaz de sobrecarregar a rede, prejudicando os demais. O administrador pode auxiliar em procedimentos que melhorem o desempenho, com melhores condições de planejar o crescimento da rede já que se conhecem as atividades dos usuários (DANTAS, 2002).

3.4.3 Gerenciamento de configuração

Com um conjunto de operações necessárias para a inicialização, término, alteração e armazenamento da configuração dos equipamentos da rede, a gerência pode alterar a configuração dos equipamentos, documentação sobre a configuração dos equipamentos, manutenção e atualização periódica, coletando dados da rede,

bem como inicializar e alterar a configuração de equipamentos. Ela ainda possui salvo uma cópia de configuração da rede. Funções importantes que devem ser observadas: documentação das configurações realizadas; ter mais de uma pessoa capaz de realizar o mesmo trabalho; configurações erradas podem gerar falhas. (STALLINGS, 2005).

3.4.4 Gerenciamento de desempenho

Os componentes de uma rede que se comunica entre si, como um roteador com um computador, precisam oferecer um desempenho aceitável para ter uma comunicação sem problemas (LOPES, 2003).

Este gerenciamento abrange duas grandes categorias funcionais: monitoramento e controle. Monitoramento é a função de observar as atividades da rede. A função de controle possibilita que se façam ajustes para melhorar o desempenho da rede. Algumas das questões envolvendo desempenho, com as quais o administrador da rede deve se preocupar são: qual é a capacidade da rede, quando se fala em desempenho? O tráfego atual é excessivo? A vazão tem diminuído para níveis inaceitáveis? Existe algum gargalo? Por mensurar os recursos e associar métricas apropriadas a eles, o administrador da rede pode analisar os resultados e estabelecer os níveis de desempenho aceitáveis, estando apto a detectar mudanças no comportamento da rede e tomar providências caso isso seja necessário (DANTAS, 2002).

3.4.5 Gerenciamento de segurança

Com foco em proteção das informações e controle de acesso por meio de *softwares*, senhas e outras informações de autorização devem ser mantidas e distribuídas, tem também que monitorar e controlar o acesso aos computadores da rede, coletando e examinando os registros de auditoria e de log, podendo desabilitar ou habilitar esses registros (STALLINGS, 2005).

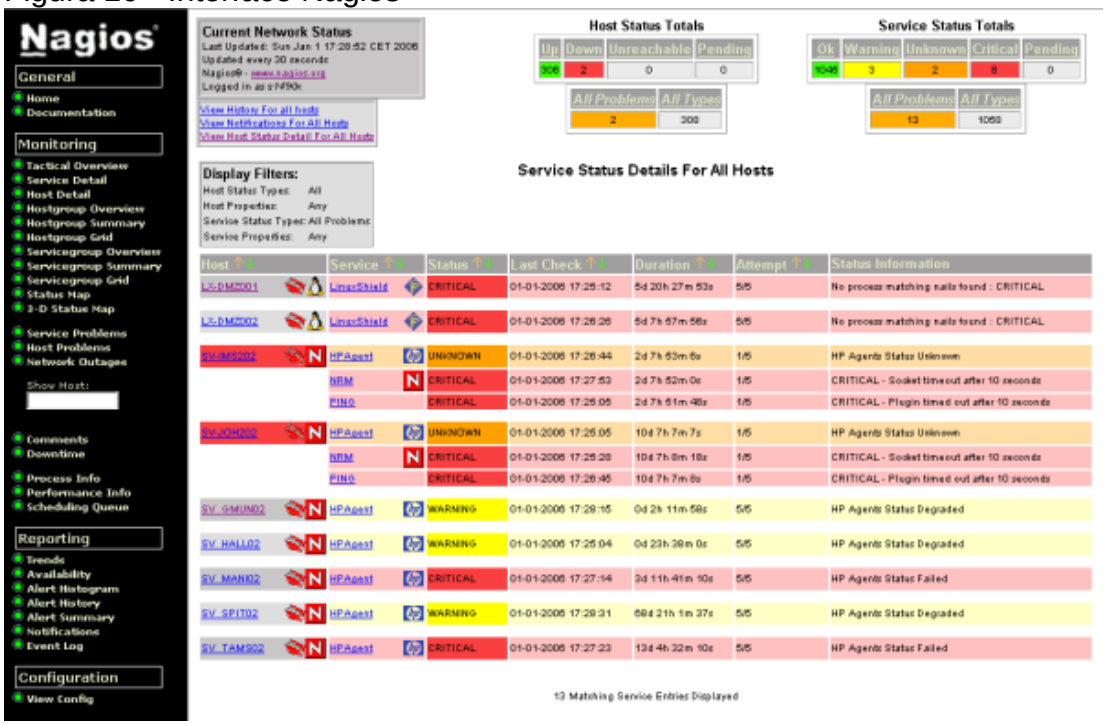
3.5 SOFTWARES DE GERENCIAMENTO

Softwares de gerência são utilizados para auxiliar os gestores das redes a identificar os problemas a fim de tomar decisões para o melhor funcionamento. As ferramentas de gerenciamento são usadas tanto em redes pequenas como em redes grandes, usando como exemplo as empresas e faculdades.

3.5.1 Nagios

É um aplicativo de gerenciamento distribuído com licença livre e disponibilizado de forma nativa para plataforma *Linux*. Alguns pacotes são feitos exclusivamente para distribuições como *Debian*, *Ubuntu*, *OpenSuse*, entre outras. Uma de suas grandes vantagens está nos *plugins*, que tem a comunidade de desenvolvimento ou os usuários que podem ser capazes de criar novos procedimentos para o gerenciamento (NAGIOS, 2006). Na figura 10, há a interface do *Nagios*.

Figura 10 - Interface Nagios



Fonte: Nagios (2006)

3.5.2 Cacti

É uma interface completa para RRDTool, que armazena todas as informações necessárias para criar gráficos e preenchê-los com dados em um banco de dados MySQL. A interface é completamente PHP orientado. Além de ser capaz de manter gráficos, fontes de dados e *round robin arquivos* em um banco de dados, lidando com a coleta de dados. Há também suporte da SNMP para criar gráficos de tráfego com MRTG. Na figura 11, há a interface do Cacti (CACTI, 2004).

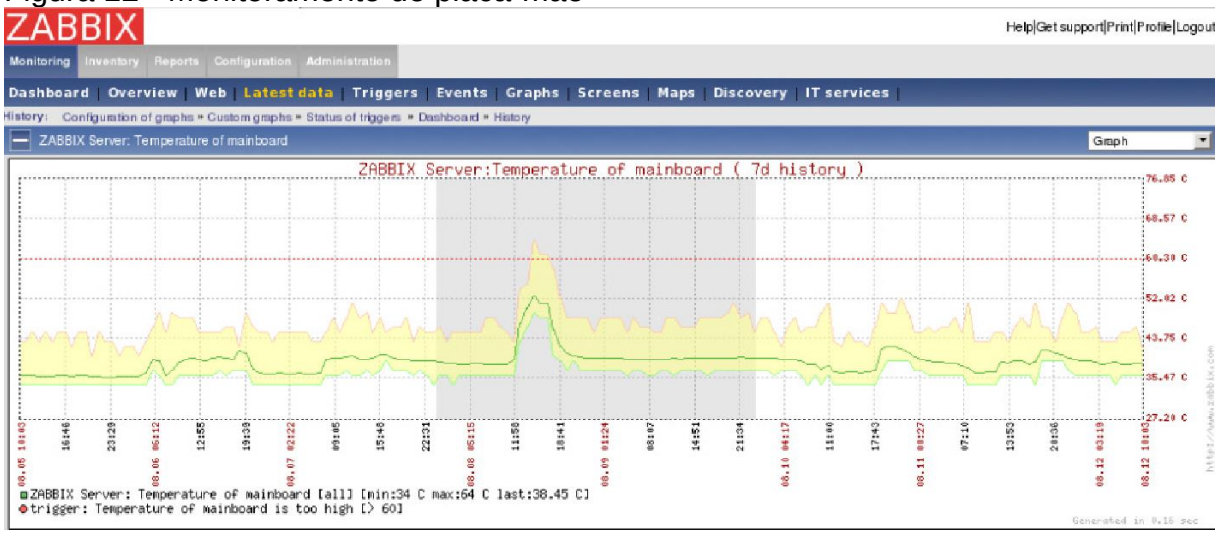
Figura 11 - Interface Cacti

Fonte: Cacti (2004)

3.5.3 Zabbix

Zabbix é uma ferramenta que pode ser utilizada para monitorar toda infraestrutura de rede, incluindo aplicações. Como características, possui suporte a sistemas *Linux*, *Solaris*, *HP-UX*, *AIX*, *FreeBSD*, *OpenBSD*, *NetBSD*, *Mac OS X*, *Windows*, entre outros. Monitora serviços simples (*http*, *pop3*, *imap*, *ssh*) sem o uso de agentes. Há suporte a SNMP. Tem interface de gerenciamento *Web* e integração com banco de dados (*MySQL*, *Oracle*, *PostgreSQL* ou *SQLite*). Há a geração de gráficos em tempo real, podendo ser modificado, e agentes disponíveis para vários sistemas operacionais como *Linux*, *Solaris*, *HP-UX, AIX, FreeBSD, OpenBSD, SCO-OpenServer, Mac OS X, Windows 2000/XP/2003/Vista* (ZABBIX, 2003). Na figura 12, mostra-se o *Zabbix.*

Figura 12 - Monitoramento de placa-mãe



Fonte: Zabbix

3.5.4 FreeRADIUS

É um *software* servidor que utiliza o *Remote Authentication Dial in User Services* (RADIUS) para fazer uma autenticação centralizada em redes *dial-up*, *Virtual Private Network* (VPN's) e redes sem fio. Usa o método *Authentication, Authorization and Accounting* (AAA). O AAA funciona com autenticação, que é a senha do usuário, autorização que o usuário tem e que está cadastrada no banco de dados. A contabilização, no histórico de acessos, fica registrada para uma nova autorização (HASSELL et al., 2002, tradução nossa).

Há um modelo cliente-servidor, em que o cliente é o *Network Access Server* (NAS). O servidor é responsável por buscar a informação sobre o cliente e transmitir para o servidor *RADIUS*, além de interpretar a resposta, permitindo ou não o acesso ao cliente. É responsável por receber pedidos de conexão, autenticar o usuário e repassar ao AP, que é o NAS, as informações para o usuário ter acesso à rede. Os provedores de *internet* usam-no para autenticação dos usuários, a fim de se conectar à rede com um IP (HASSELL et al., 2002, tradução nossa).

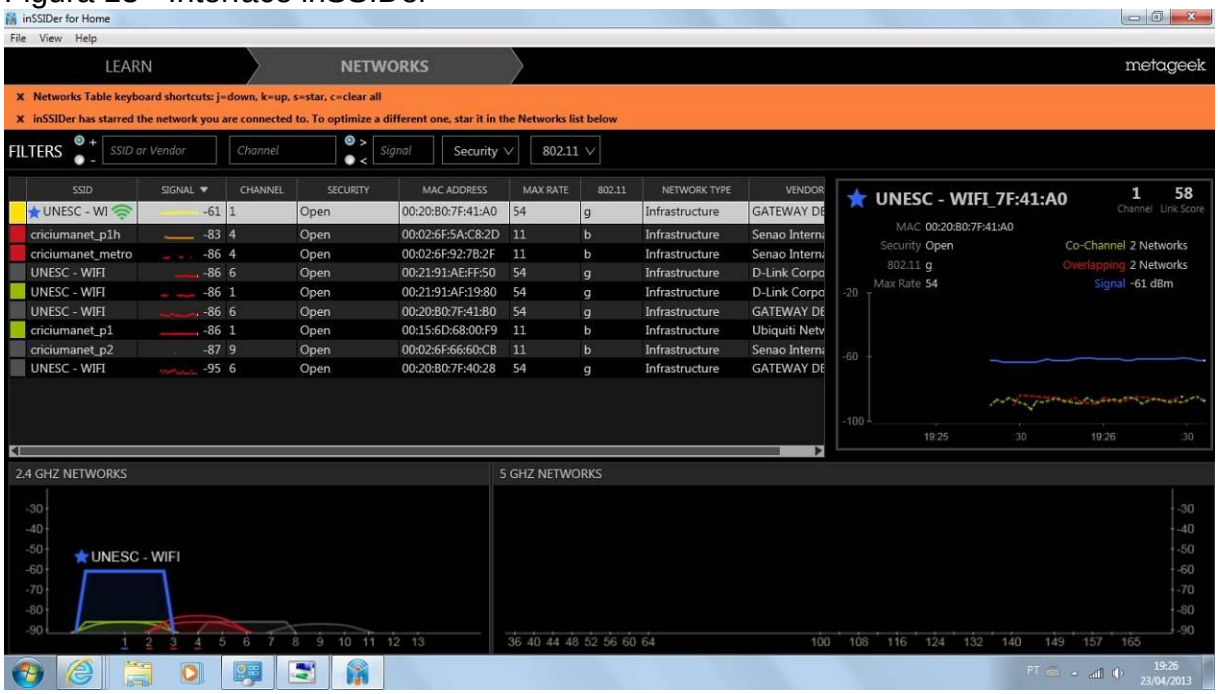
3.6 SOFTWARES DE MONITORAMENTO

Os dados nos *softwares* de monitoramento ajudam a ver possíveis problemas para solução dos mesmos, a fim de facilitar ao máximo o trabalho do administrador da rede, para ter o diagnóstico da mesma. Como característica, o monitoramento é a visualização da topologia. A qualidade do sinal visto pela potência evita falhas. Se possível, mostrar a posição no espaço como um rodar, facilitando a identificação de um problema na rede (NADEU, et al., 2003, tradução nossa).

3.6.1 inSSIDer

O *inSSIDer* é um *software* que substituiu o antigo programa chamado *NetStumbler,* utilizado para escanear redes *Wi-Fi*. Ele mostra informações sobre redes como: SSID, MAC, ponto de acesso, taxa de dados, força do sinal, segurança e também mostra como as redes *Wi-Fi* se sobrepõem. Na figura 13, mostra-se a tela:

Figura 13 - Interface inSSIDer



Fonte: Do Autor.

São informações contidas no *software*: SSID é um identificador único que identifica a rede sem fio, como *Service Set Identifier* (SSID). O equipamento *wireless* para se conectar à rede deve corresponder ao ponto de acesso.

Canais: cada rede sem fio opera em um canal *Wi-Fi* específico. Canais 1-14 estão na gama de frequência de 2,4 GHz, enquanto os canais de 30-160 estão no intervalo de 5 GHz.

Received Signal Strength Indication (RSSI) é a amplitude do nível de rede sem fio, como visto por meio da placa de rede sem fio do PC. InSSIDer representa RSSI em dBm. O mesmo ajuda a determinar o intervalo, que pode ser de -100 a -20 amplitude (dBm), sendo que, quanto menor for a amplitude em dBm, melhor será o sinal da rede com relação ao canal em que se encontra, indo do canal 1 ao 14. Na figura 14, mostra-se a qualidade da potência do sinal.

Figura 14 - Qualidade da Potência do Sinal

Quality	dBm
Excellent	>-51
	-53
	-55
	-57
	-59
	-61
Good	-63
	-65
	-67
	-69
	-71
	-73
Fair	-75
	-77
	-79
	-81
	-83
	-85
Poor	-87
	-89
	-91
	-93
	-95
	-97
Very Poor	-99
	-101
	-103
	-105
	-107
	-109
No Signal	-111
	<-113

Fonte: Adaptado de MetaGeek

O *Media Access Control* (MAC) é um endereço físico associado à interface de comunicação, que conecta um dispositivo à rede. O MAC é um endereço “único”, não havendo duas portas com a mesma numeração, é usado para controle de acesso em redes de computadores. Sua identificação é gravada em *hardware*, isto é, na memória ROM da placa de rede de equipamentos, como

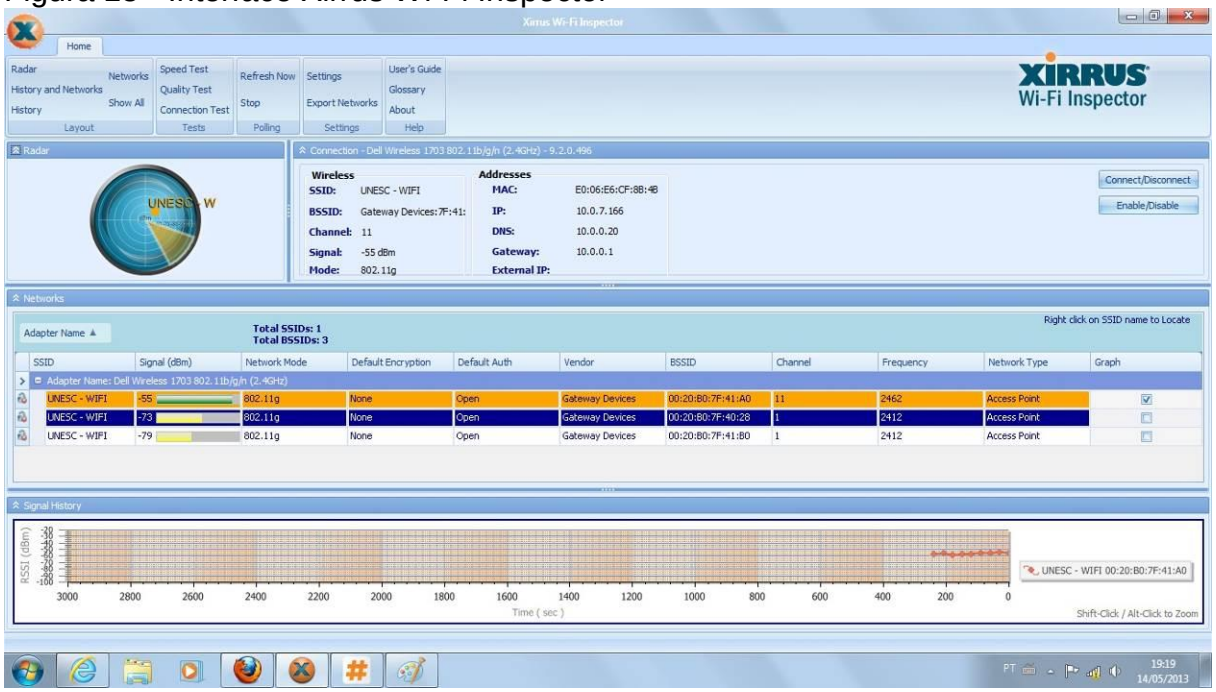
desktops, *notebooks*, roteadores, *smartphones*, *tabletes*, impressoras de rede, entre outros.

Security informações sobre qual segurança está sendo implantada na rede, podendo ela ser aberta: sem segurança; fechada; usando WEP, WPA, WPA2; entre outros.

3.6.2 Xirrus Wi-Fi Inspecto

O *Xirrus Wi-Fi Inspector* é uma ferramenta para gerenciar e solucionar problemas do *Wi-Fi* no *Windows*. Permite caracterizar a integridade e o desempenho da conexão, além de procurar por redes sem fio e gestão. Soluciona problemas de conexões, verificando a cobertura *Wi-Fi*, e localiza dispositivos sem fio e detecção de *access points.* Na figura 15, tem-se a sua tela:

Figura 15 - Interface Xirrus Wi-Fi Inspector



Fonte: Do Autor.

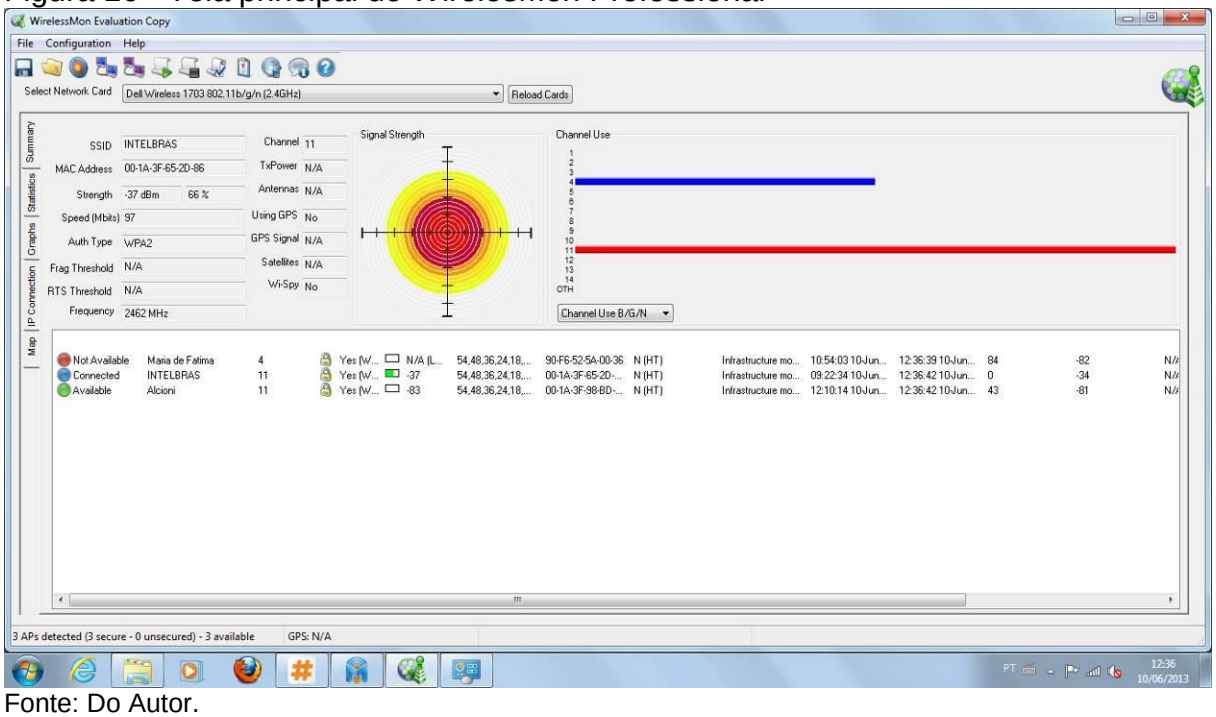
É dividido em: *home* (menu com todas as opções de configuração e utilização do sistema); *radar* (gráfico em dB, que apresenta a APs encontrados e a potência de seu sinal); *connection* (apresenta o detalhamento da conexão *wireless* atual); *networks* (mostra a relação dos equipamentos encontrados e seus detalhes

de operação); *signal history* (gráfico que mostra até onde o AP tem cobertura, quanto mais alta a linha no gráfico, melhor será o sinal).

3.6.3 Wirelessmon

Apresentado em duas versões, *Standard* e *Professional*, este programa exibe os principais dados sobre as redes sem fio, estatísticas sobre o adaptador de rede escolhido e gráficos de utilização sobre o tempo, em percentual, do nível de sinal, da taxa de recebimento de dados, da taxa de transmissão de dados e da taxa total de dados. Conhecendo os dados para conexão com as redes detectadas, é possível também obter as informações sobre a conexão, como IP, máscara, *gateway*, servidor DHCP e demais parâmetros de conexão. Na figura 16, mostra-se o *software*.

Figura 16 - Tela principal do WirelesMon Professional



Fonte: Do Autor.

Ele permite a gravação dos dados em arquivos de logs e suporta o uso do analisador de espectros desenvolvido pela *metageek*, suporta o *wi-spy* nos modelos 2.4i, 2.4x e dbx, útil para encontrar a interferência de dispositivos com 802.11a/b/g, transmitindo na mesma frequência. Cria mapas de intensidade de sinal de uma área,

suporte a GPS para registrar e mapear a intensidade do sinal, verifica as configurações de segurança para pontos de acesso locais.

4 TRABALHOS CORRELATOS

Neste capítulo, são apresentados os trabalhos relacionados mais importantes que serviram de base para este projeto, com o objetivo de transmitir melhor entendimento das propostas apresentadas.

4.1 INTEGRANDO FERRAMENTAS DE SOFTWARE LIVRE PARA GERENCIAMENTO E MONITORAÇÃO DE REDES LOCAIS

Este projeto foi realizado em 2004, na cidade de Porto Alegre, no Rio Grande do Sul, foi feito pelo acadêmico Sílvio Luís Leite, da Universidade Federal do Rio Grande do Sul, Instituto de Informática Programa de Pós-graduação em Computação, como requisito parcial para a obtenção do título de Mestre em Informática.

Este trabalho teve como objetivo o estudo e a integração, como forma de validação, de ferramentas de *software* livre para o uso em gerência e monitoração de redes de computadores. Com o crescimento das redes, surgiu a necessidade por controle de seus recursos. Dessa necessidade, foi criado o protocolo SNMP, utilizado nos dias de hoje como padrão de fato na gerência e monitoração de redes.

Anteriormente ao surgimento do *software* livre, para a atividade de gerência e monitoração, existiam apenas produtos proprietários, os quais estavam restritos a poucas empresas que podiam arcar com seus custos. Com o surgimento do *software* livre, ferramentas simples de gerência e monitoração começaram a ser criadas. Estas ferramentas simples necessitam ser integradas de forma a prover maior quantidade de recursos. O método proposto desenvolve um protótipo capaz de integrar várias ferramentas de gerência e monitoração, utilizando exclusivamente ferramentas de *software* livre.

Para demonstrar a ideia na prática, um estudo de caso é apresentado, utilizando um protótipo desenvolvido. Nos resultados, durante o período de teste do protótipo, foram identificados problemas de desempenho e falhas em alguns equipamentos.

4.2 COMPARAÇÃO DE FERRAMENTAS DE GERENCIAMENTO DE REDES

Este projeto foi realizado em 2008, na cidade Porto Alegre, no Rio Grande do Sul, foi feito pelo acadêmico Tomas Lovis Black, da Universidade Federal, Instituto de Informática Curso de Especialização em Tecnologias, Gerência e Segurança de Redes de Computadores, como requisito parcial para a obtenção de grau Especialista.

O trabalho consiste na apresentação e comparação de nove dessas ferramentas de gerenciamento e monitoramento de rede: o *CACTI*, um *front-end* para ferramentas de gerenciamento baseado em RRD, *ZENOSS*, *ManageOP Engine*, *BigBrother4*, *SpiceWorks*, *Look@LAN*, *Zabbix* e *Nagios*.

São muitos os parâmetros de comparação destas ferramentas e não é objetivo dessa dissertação apontar o melhor *software* dentre os analisados, mas auxiliar o pesquisador a tomar a melhor escolha de acordo com suas necessidades. Em particular, são observados os parâmetros mais relevantes dentre os procurados pelos administradores de rede: performance, facilidade de utilização e necessidade de recursos, tanto de *hardware* quanto humanos.

Como resultado, após análise, verifica-se que não há um produto apenas que disponibiliza, de forma satisfatória, todos os recursos existentes no âmbito do gerenciamento de redes. Para o pesquisador, a melhor combinação é unir duas ou mais ferramentas para, então, atingir a totalidade do conceito de gerenciamento de redes.

4.3 GERÊNCIA DE REDES DE COMPUTADORES UTILIZANDO O ZABBIX: UM ESTUDO DE CASO

Este projeto foi realizado em 2008, na cidade de Goiana, em Goiás, foi feito pelos acadêmicos Ivandro José de Freitas Rocha e Marcel Oliveira Serradourada, da Universidade Católica de Goiás, como requisito parcial para obtenção do título de Bacharel em Ciência da Computação.

O trabalho traz o tema de gerenciamento de redes de computadores, mantendo seu histórico e conceitos. São apresentadas as características e funcionalidades da arquitetura do protocolo *Simple Network Management Protocol*

(SNMP) e também as características de alguns dos principais *softwares* de gerenciamento de redes (livres e proprietários) existentes. Dentre elas, é apresentada a ferramenta *ZABBIX*, bem como suas principais características.

Além do estudo teórico, foi realizado um estudo de caso na SANEAGO (Empresa de Saneamento de Goiás), utilizando a ferramenta *ZABBIX*, a fim de apresentar uma proposta para solucionar um problema da empresa atualmente, que é o gerenciamento de espaço em discos dos servidores.

Nos resultados, o estudo de caso prático que foi solicitado pela empresa, para resolver o problema de notificação de espaço dos discos dos servidores. Foi apresentada uma proposta de solução utilizando o *ZABBIX*, que monitora um vasto número de parâmetros, facilitando o monitoramento desse espaço em discos, sendo que todo esse processo foi descrito para posteriormente ser aprovado e implantado na empresa.

4.4 IMPLANTAÇÃO E GERENCIAMENTO DE UMA REDE SEM FIO NOS DOMÍNIOS DE UM CAMPUS UNIVERSITÁRIO

Este projeto foi realizado em 2007, na cidade Lavras, em Minas Gerais, foi feito pelo acadêmico Vicente de Luca, da Universidade Federal de Lavras, como parte das exigências do curso para obtenção do título de Bacharel em Ciência da Computação.

O trabalho descreve boas práticas no uso de diversas tecnologias de rede, com o objetivo de criar uma ampla área de cobertura para acesso móvel a uma rede IP acadêmica, em um *campus* universitário. O benefício das redes sem fio é a realidade diária para usuários de recursos de TI. Pesquisas recentes apontam o setor educacional como o maior responsável pelos investimentos na criação de redes móveis em países de primeiro mundo. Propomos neste trabalho um estudo de caso na Universidade Federal de Lavras para criação de uma rede sem fio, com baixo custo comparado a soluções proprietárias, de forma a prover acesso ubíquo em alta velocidade para *notebooks* e dispositivos W*i-Fi*.

Como resultados, são mostradas a convergência da rede dentro dos requisitos técnicos e de legislação e normas, capacidades de monitoramento e

gerenciamento desta rede, bem como trabalhos futuros no sentido de ampliar a cobertura móvel e possibilitar novas interconexões.

4.5 PROCESSO DE PLANEJAMENTO PARA ELABORAÇÃO DE POLÍTICA DE GERENCIAMENTO DE REDE PARA MICRO E PEQUENAS EMPRESAS

Este trabalho foi realizado em 2004, na cidade São José em Santa Catarina, foi feito pelo acadêmico Rafael van de Sande Silveira, da Universidade do Vale do Itajaí, como requisito parcial para a obtenção do título de Bacharel em Ciência da Computação.

O trabalho tem como objetivo desenvolver uma proposta de planejamento para elaboração de políticas de gerenciamento de rede, focalizando em micro e pequenas empresas e propondo ferramentas tecnológicas baseadas na filosofia de *software* livre. Para alcançar tal objetivo, foi realizada uma pesquisa em 14 micro e pequenas empresas, visando identificar o perfil das mesmas em relação ao gerenciamento de suas redes. Nesta pesquisa, identificou-se que as principais necessidades de gerenciamento estão relacionadas às áreas funcionais de gerenciamento de falhas, desempenho e configuração. A partir da identificação dos requisitos de gerenciamento de micro e pequenas empresas, foi proposto um processo de planejamento para a elaboração de políticas de gerenciamento, composto de três fases: identificação dos dados de entrada, processo de planejamento e elaboração de planos. Como resultado dessas etapas, definiu-se um plano que constitui um modelo de política de gerenciamento para micro e pequenas empresas. Além disso, apresenta-se um conjunto de ferramentas de *software* de gerenciamento livre, para serem utilizados como ferramentas de suporte para a implantação da política definida.

Como resultado, definiu-se um plano que constitui um modelo de política de gerenciamento para micro e pequenas empresas.

5 GERENCIA DE REDE SEM FIO, MONITORAMENTO EM WLAN

Com a popularização da rede sem fio, torna-se importante o controle da mesma, com aspectos de segurança, configuração, falhas, contabilização e desempenho no intuito de ter a rede sempre acessível.

Esta pesquisa se restringe a uma rede infraestruturada, descrevendo alguns *softwares* de gerenciamento, dos quais apenas o *FreeRadius*, na área de segurança, foi aplicado, para descrever os aspectos de importância da segurança e as políticas. Esta pesquisa é focada fortemente no aspecto de monitoramento. A ideia era a aplicação em redes domésticas e corporativa, mas, pela dificuldade de conseguir um ambiente coorporativo, a mesma ateve-se em aplicar em ambiente residencial e simular o modelo coorporativo.

5.1 METODOLOGIA

A primeira etapa desta pesquisa compreendeu o levantamento bibliográfico. Com pesquisa em livros, artigos e *Internet*, coletando e buscando-se as bibliografias necessárias para a elaboração deste projeto de pesquisa, a escrita e o desenvolvimento do Trabalho de Conclusão de Curso.

Foi realizado o estudo sobre as redes sem fio, suas características e padrões. Abordaram-se as áreas da gerência e suas classificações.

Foram descritas as características de cada *software* com relação as áreas de gerência. Para este projeto, foram descritos aspectos de redes domésticas e redes corporativas.

5.2 TOPOLOGIA DE REDE

Na escolha da topologia a utilizar entre infraestrutura ou ad-hoc, optou-se pela infraestruturada, com um *Access Point* instalado em local que o sinal possa trafegar uniforme. A escolha da estrutura é pensada nos aspectos residenciais e pesquisada acerca dos dispositivos portáteis mais utilizados como: *notebooks*, *tablets* e celulares. Com isso, a infraestrutura suporta equipamentos nos padrões 802.11b, 802.11g, 802.11n, entre outros. O AP escolhido utilizado foi o da *Intelbras,*

modelo WRN 240, roteador *Wireless* N 150 Mbps, um modelo que se destina a uso doméstico, mas com uma configuração flexível. Foram realizados alguns experimentos e separados por monitoramento e gerenciamento de redes sem fio.

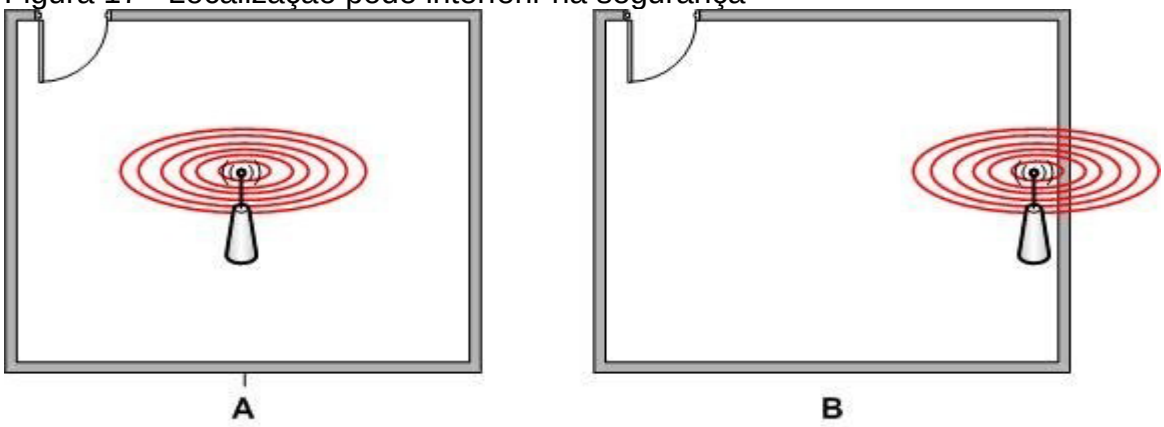
5.3 ACCESS POINT

É um ponto de acesso que retransmite o sinal, com funcionalidade semelhante como um *hub*. Há vários tipos de APs, desde os mais simples até os mais avançados, com características comuns e diferentes, como taxa de transferência de dados, que varia de 54 a 108 Mbps, padrões utilizados tipo b, g e n, entre outros, canais utilizados tipo do 1 ao 14, potência do sinal para estabelecer seu alcance, dependendo da sua localização no ambiente e de outros fatores e a utilização de *Radius*.

5.3.1 Localização do Access Point

Diferente das redes cabeadas, a localização dos roteadores se torna importante na qualidade e segurança da rede sem fio. Muitos roteadores wireless utilizam antenas omnidirecionais, neste caso fica complicado gerenciar o alcance do sinal e alguns não contam com configuração da potência do sinal, pois, como visto no quadro B, o roteador colocado próximo à parede faz com que o sinal passe para fora do ambiente, irradiando o sinal para fora da área estabelecida. Já colocando mais ao centro, como no quadro A, tem-se um melhor aproveitamento do sinal, como visto na figura 17, não impedindo o alcance por outros, mas minimizando a situação.

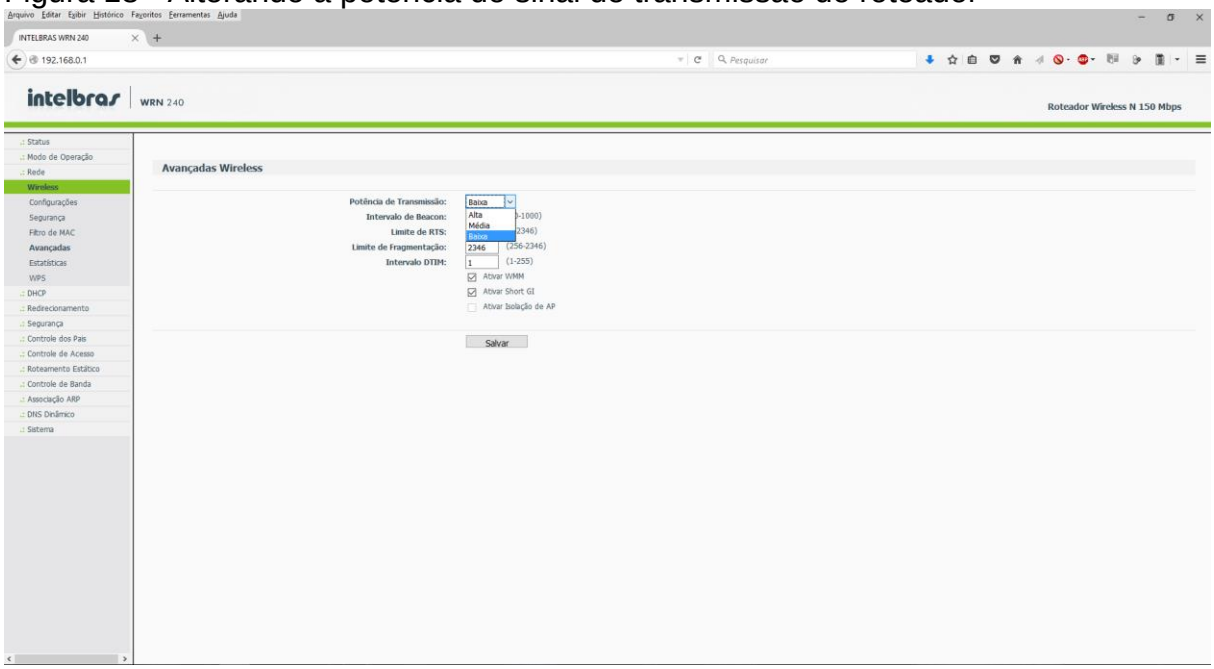
Figura 17 - Localização pode interferir na segurança



Fonte: Do Autor.

Outra maneira de reforçar a segurança quanto à irradiação do sinal é utilizando antenas direcionais ou se no *firmware* do roteador ter a opção de diminuir a potência do sinal entre alta, média e baixa, como mostrado na figura 18.

Figura 18 - Alterando a potência do sinal de transmissão do roteador



Fonte: Do Autor.

Foram realizados alguns testes com vários *softwares*, analisando a potência do sinal, diante da localização do mesmo, dentro do ambiente, no estilo *Site Survey indoor,* com o seguinte cenário: foi instalado o roteador no centro de uma determinada residência, no piso superior a 4 metros de altura. Foram realizadas

medições para encontrar a parte central, medindo-se o perímetro do local (com 15 metros de frente e 24,50 metros de área lateral), fixando o *Access Point* com a antena para baixo na horizontal, alterando a senha padrão de acesso ao mesmo e a segurança usando o protocolo WPA2, utilizando senha com números e letras, potência do AP em alta, média e baixa para os testes. Para ver o alcance do sinal, foram usados alguns *softwares,* sendo eles: *InSSIDer*, *WirelessMon*, *Xirrus Wi-Fi Inspector* e *WIFi Locator*, colocando o computador em 4 locais distintos, para obter a intensidade do sinal e perceber a diminuição do mesmo. Esses testes foram repetidos por quatro vezes, por meio de um *Notebook Dell,* modelo 5420, com um core I5, 6 Gb de ram, Sistema *Microsoft Windows* 7 *Ultimate*.

Tem-se à frente uma rua e, logo após, uma residência. Ao lado direito, há outra, separada por um muro com 10 cm de espessura. Ao lado esquerdo, há mais uma sem muro, mas a parede é o que separa uma da outra e atrás, tem-se uma área de serviços com duas paredes para chegar ao próximo local, com as paredes medindo 10 cm de espessura.

Com essas informações, verificou-se o alcance do sinal medido em dBm, utilização do canal, se há interferência, se existe acesso à rede, se obteve os resultados de quatro cantos, por ter mais barreiras, até chegar neles, conforme descrito nas tabelas a seguir.

Tabela 3 - Análise de potência do sinal e localização do Access Point, por meio de alguns softwares de monitoramento com BAIXA potência

Baixa	**Atrás Esquerda**	**Frente Esquerda**	**Frente Direita**	**Atrás Direita**
inSSIDer	77-79 dBm	68-75 dBm	75-80 dBm	75-80 dBm
WirelessMon	77-81 dBm	68-72 dBm	75-78 dBm	72-75 dBm
Xirrus Wi-Fi Inspector	81-83 dBm	69-72 dBm	71-76 dBm	67-75 dBm
WIFi Locator	72-75 dBm	68-71 dBm	80-82 dBm	66-72 dBm

Fonte: Do Autor.

Na tabela 3, com a potência em baixa nos quatro cantos do local, observou-se que o acesso à rede era permitido, mas a qualidade do sinal ficou em média de 36%, sendo as partes de trás esquerda e frente direita as de menos potência. Com esse valor, para ser ter um bom aproveitamento, fica abaixo do esperado, ainda irradiando um pouco para fora do perímetro da residência. Contudo,

o sinal não tem grande estabilidade, reduzindo um pouco os problemas com segurança, mas ainda havendo o acesso por pessoas não autorizadas, devido ao alcance, necessitando, assim, de procedimentos de segurança.

Tabela 4 - Análise de potência de sinal e localização do Access Point, por meio de alguns softwares de monitoramento MÉDIA potência

Média	**Atrás Esquerda**	**Frente Esquerda**	**Frente Direita**	**Atrás Direita**
inSSIDer	75-77 dBm	69-72 dBm	80-85 dBm	74-77 dBm
WirelessMon	75-79 dBm	72-74 dBm	74-77 dBm	77-80 dBm
Xirrus Wi-Fi Inspector	77-79 dBm	69-71 dBm	79-81 dBm	72-75 dBm
WIFi Locator	76-78 dBm	73-75 dBm	78-81 dBm	72-75 dBm

Fonte: Do Autor.

Na tabela 4, com a potência em média nos quatro cantos do local, observou-se que o acesso à rede era permitido, com a qualidade do sinal em média (52%), com as áreas de trás esquerda e frente direita as mais afetadas. Esse valor fica na média, mas não é o aceitável para uma boa conexão para os dispositivos que vêm a utilizar a rede.

Tabela 5 - Análise de potência de sinal e localização do Access Point, por meio de alguns softwares de monitoramento ALTA potência

Alta	**Atrás Esquerda**	**Frente Esquerda**	**Frente Direita**	**Atrás Direita**
inSSIDer	73-77 dBm	66-71 dBm	76-78 dBm	73-77 dBm
WirelessMon	74-77 dBm	66-69 dBm	77-79 dBm	71-74 dBm
Xirrus Wi-Fi Inspector	73-79 dBm	69-73 dBm	78-81 dBm	70-73 dBm
WIFi Locator	70-74 dBm	70-75 dBm	76-80 dBm	71-78 dBm

Fonte: Do Autor.

Na tabela 5, com a potência em alta nos quatro cantos do local, observou-se que o acesso à rede era permitido, a qualidade do sinal ficou em média de 58%. Com esse valor, há o melhor aproveitamento da rede. Contudo, com a irradiação passando do perímetro desejado, é necessário aplicar aspectos de gerência para rede.

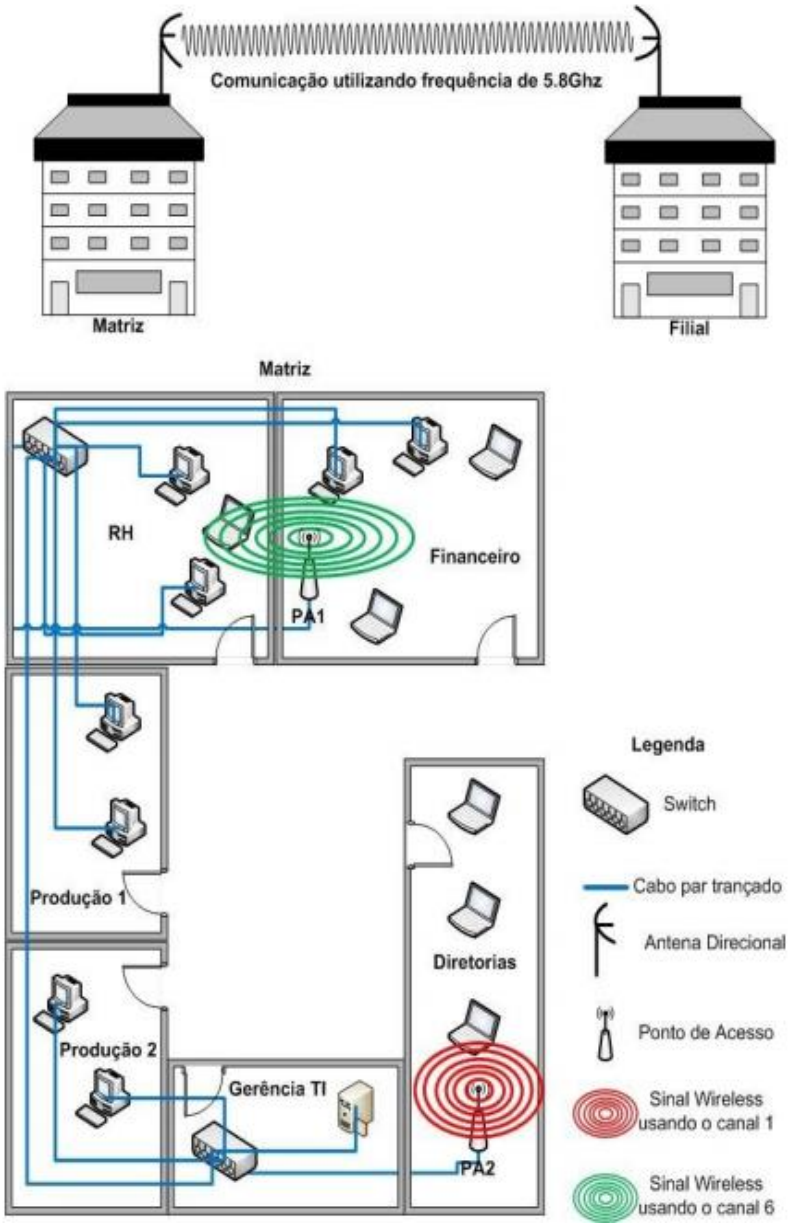
Com a análise da potência foram encontrados os resultados que com o *Access Point* centralizado e com a potência do sinal em Alta a uma melhor

abrangência no perímetro, sendo que com a saída do sinal fora do quadrante. Há a necessidade de aprimorar a segurança, como alterações em parâmetros da rede na forma de assegurar a integridade dos dados.

Terminada a análise na rede doméstica, nesta parte, inicia-se um aspecto de simulação da rede corporativa, onde se adota medidas de segurança principalmente pelas informações que contêm na empresa, que, com a utilização de rede sem fio, tem uma cautela na hora de projetar a rede. A figura 19, mostra-se um exemplo de configuração de uma empresa que, além de aplicar meios sem fio no modo interno, tem a necessidade de transmitir com os mesmos fins para uma filial, que fica a alguns quilômetros da matriz, para a retransmissão do sinal para outra rede, utilizando-se antenas direcionais que têm um alcance maior e utilizando um único sentido, com frequência de 5,8Ghz de potência, não tendo a necessidade de contratar uma operadora de *Internet* para cada unidade, aumentando, com isso, o valor da aquisição no projeto.

Com a estrutura externa concluída, há a interna, que, com a abordagem de um *Site Survey,* se observou que precisaria de dois pontos de acesso para cobrir alguns setores da empresa e todos os dispositivos sem fio nessas áreas: um utilizando o canal 1, que abrange a sala de Diretorias, e outro utilizando o canal 6, que abrange os setores de RH e Financeiro, a fim de evitar interferências. Para os computadores, utiliza-se *Switch,* com a utilização de cabos trançados de rede para interligá-los com os dispositivos.

Figura 19 - Rede corporativa



Fonte: Da pesquisa

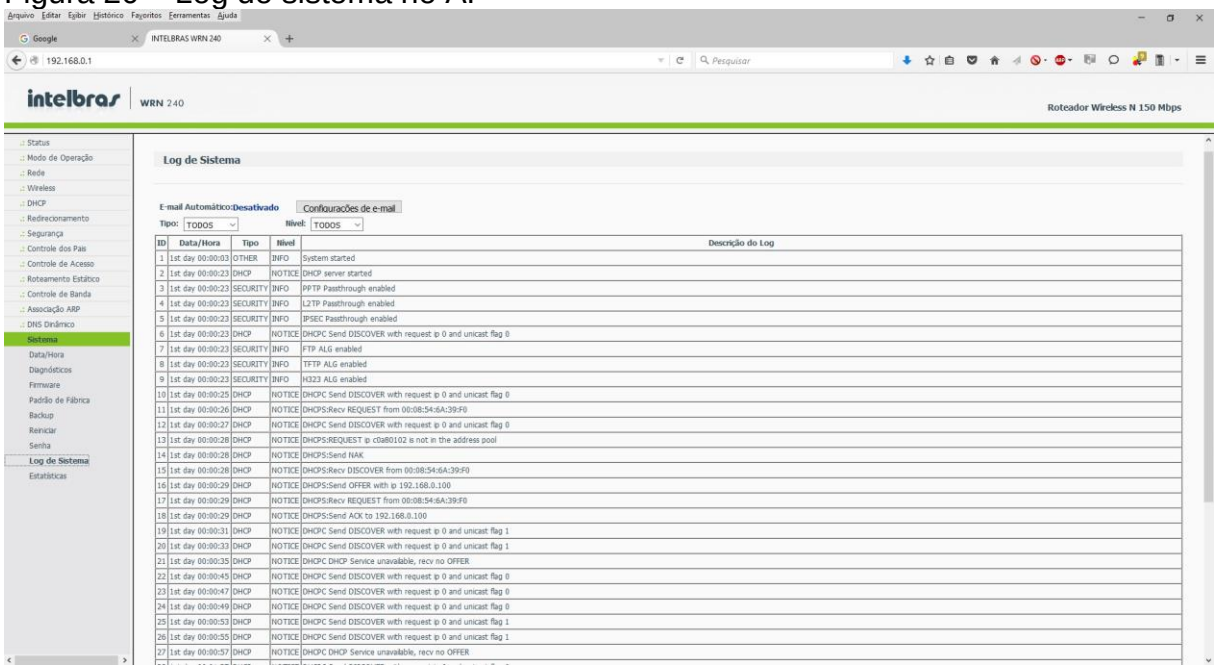
5.3.2 Falha

Na parte de falhas, há como exemplo o acesso a um *site* ao qual ele não responde, que pode ser por falha no roteador, em que o mesmo pode estar desligado, não servindo acesso, também o *modem* pode se encontrar na mesma situação, não conseguindo navegar ou o acesso à rede teve uma queda por parte da operadora contratada.

O administrador da rede deve ter um monitoramento constante na rede para mantê-la sempre acessível, verificando se as configurações foram alteradas e se os equipamentos estão atualizados e funcionando.

O administrador pode verificar o log do sistema do roteador para verificar possíveis falhas, indo em nas configurações do AP em < aba de menu < Sistema < Log de Sistema, como mostrado na figura 20. Com essas informações, sendo analisadas periodicamente, podem-se fazer as medidas possíveis para evitá-las.

Figura 20 – Log do sistema no AP



Fonte: Do Autor.

5.3.3 Desempenho

Um conjunto de fatores pode determinar o desempenho da rede, como a configuração do AP nos quesitos de alocação de um canal, tipo de segurança com a escolha de WEP, WPA ou WPA2, localização do AP em relação aos equipamentos que vão se conectar a ele.

Para a análise dos protocolos de segurança no tráfego da rede, utilizou-se o *software iperf,* que foi desenvolvido pela NLANR (*National Laboratory for Applied Network Research*), como alternativa para medir o desempenho de largura de banda

máxima do TCP e UDP. Ele pode ajustar parâmetros no uso do protocolo UDP, reportar a largura de banda utilizada, jitter e perda de pacotes (IPERF, 2015).

Foi utilizado o protocolo de transporte UDP, por não ter controle de congestionamento, evitando a degradação do desempenho nos testes. Segundo Kurose e Ross (2006), o congestionamento do TCP limita a capacidade de transmissão de um processo entre o cliente e o servidor quando a rede é utilizada pelos mesmos.

No computador, foi executado o *iperf* com cada velocidade e cada mecanismo de segurança. Os comandos utilizados foram:

Servidor: iperf –s –i 1 –u

Onde:

-s: específica que este dispositivo será o servidor;

-i: específica a cada quanto tempo será mostrado o resultado na tela, foi usado de 1 segundo;

-u: específica que o protocolo de transporte UDP será utilizado.

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

Onde:

-c: específica que este dispositivo será o cliente;

-i: específica a cada quanto tempo será mostrado o resultado na tela, foi usado de 1 segundo

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

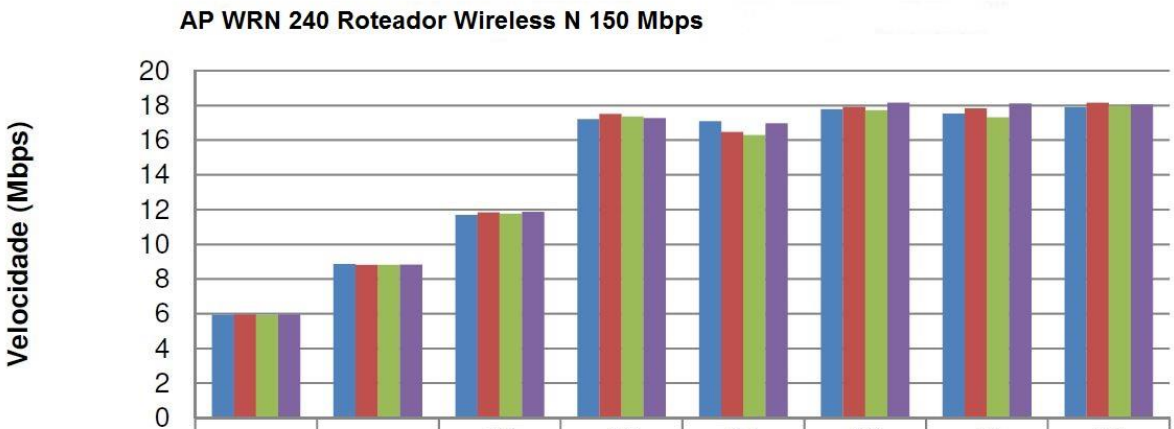
-t: específica por quanto tempo o teste será feito. Foi feito com 180 segundos.

Com o ponto de acesso fixo, para não ter alteração de resultados no cliente, devido a diferentes distâncias entre o ponto de acesso, os testes foram feitos com as velocidades no padrão 802.11g: 6, 9, 12, 18, 24, 36, 48 e 54 Mbps. Para melhorar seu desempenho, testou-se em todas as velocidades, tornando-se mais completo nas criptografias aberta; WEP 128 bits; WPA-TKIP e WPA2-AES.

Os resultados foram salvos em arquivos de texto e, logo após, calculadas as médias de desempenho do roteador, com cada tipo de criptografia.

Como mostrado na figura 21, houveram poucas diferenças de desempenho em todas as velocidades testadas, em que o WPA2 teve um bom desempenho e o WPA teve o pior resultado.

Figura 21 - Teste AP com as criptografias

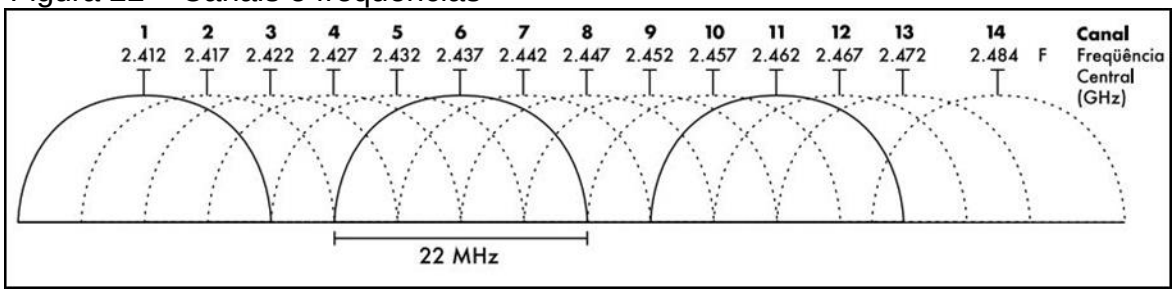


	6 Mbps	9 Mbps	12 Mbps	18 Mbps	24 Mbps	36 Mbps	48 Mbps	54 Mbps
Aberta	5,94	8,86	11,68	17,21	17,08	17,78	17,53	17,9
WEP	5,96	8,81	11,85	17,52	16,47	17,91	17,83	18,14
WPA-TKIP	5,91	8,82	11,77	17,36	16,3	17,73	17,31	17,95
WPA2-AES	5,96	8,84	11,87	17,27	16,97	18,14	18,11	18,06

Fonte: Do Autor.

A alocação dos canais tem uma faixa de 2,4 GHz, dividida em 11 canais na América do Norte, 13 na Europa e 14 no Japão. Estes canais são separados por 5 MHz, com uma largura de banda de 22 MHz. Com isso, há uma sobreposição de canais, já que existe essa sobreposição é recomendado usar os canais 1,6 ou 11, que não têm interferência quando há vários APs, além de ajustar os canais de 3 em 3 (KUROSE; ROSS, 2010). Na figura 22, mostram-se canais e frequências:

Figura 22 – Canais e frequências



Fonte: IDRC (2008)

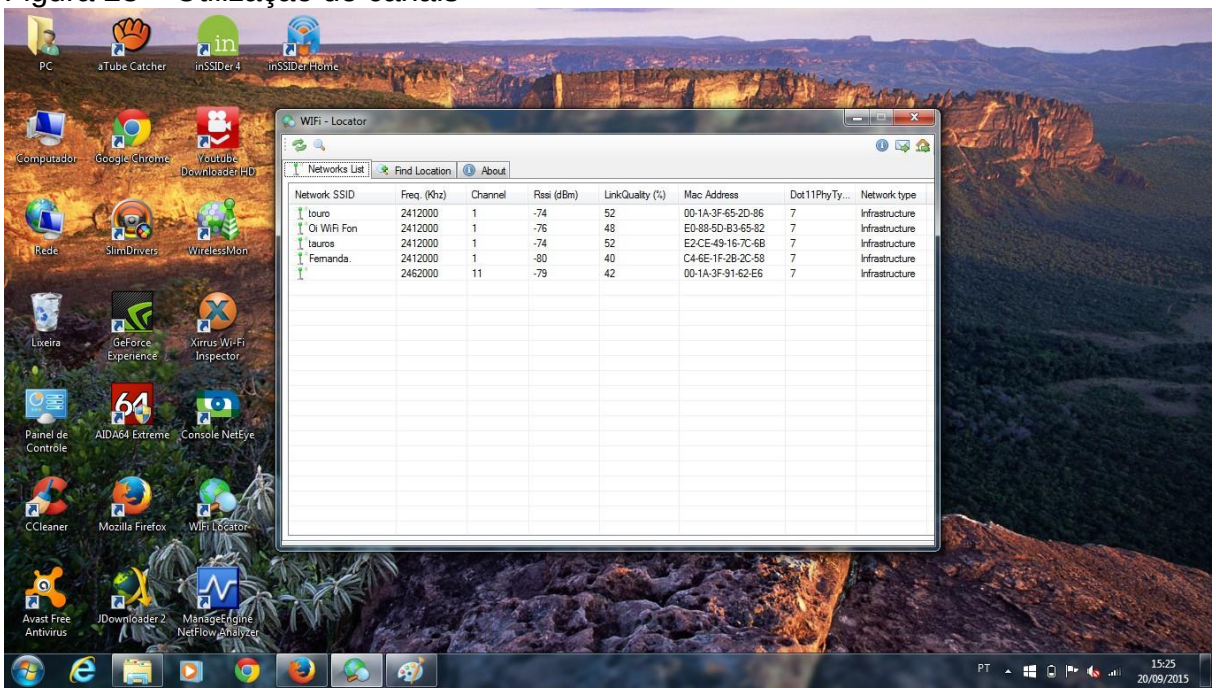
A potência do sinal: a antena do AP tem um alcance de 100 metros, sem barreiras. Com isso, a potência depende de onde o AP se localiza, tipo de antena utilizado e barreiras. O equipamento utilizado no meio da residência em um local no alto do ambiente tem uma maior área de cobertura, o posicionamento da antena será sempre na posição vertical para radiação do sinal.

As principais barreiras que podem afetar a transmissão do sinal da rede sem fio são: antenas ou pontos de acesso baixos, onde eles têm que estar em uma superfície mais alta, com menos barreiras, possibilitando que o sinal chegue ao dispositivo receptor de forma mais fácil. Micro-ondas e telefones, por utilizar da frequência 2.4 Ghz, disputam o mesmo canal de frequência (FLICKENGER,2008).

Outros tipos de barreiras que interferem no sinal: concreto e trepadeira juntos prejudicam totalmente o sinal, água em aquário, bebedouro, vidro e árvore (o vidro pode prejudicar a qualidade do sinal, porém na presença de árvores, dividindo os ambientes, como, por exemplo, primeiros andares de dois prédios da mesma companhia) e a influência negativa aumenta entre as duas antenas (FLICKENGER,2008).

Uma situação que leva a troca de canal para evitar interferência é mostrada na figura 23. Nela, há quatro dispositivos utilizando o canal, um e outro usando o 11. Nesse cenário, trocou-se o canal 1 pelo canal 6.

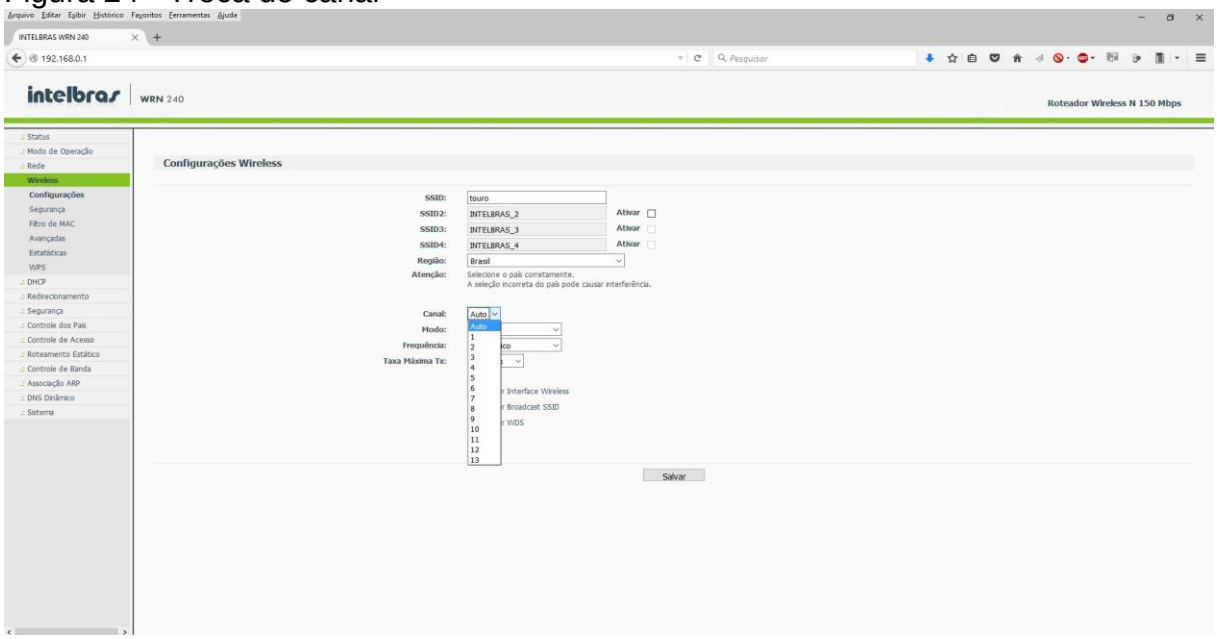
Figura 23 – Utilização de canais



Fonte: Do Autor.

No roteador, para efetuar a troca e canal, deve-se nas configurações do AP na parte de *wireless* no item canal e trocar pelo 6, como mostra a figura 24. Com essa alteração, há um melhor aproveitamento do sinal:

Figura 24 - Troca de canal

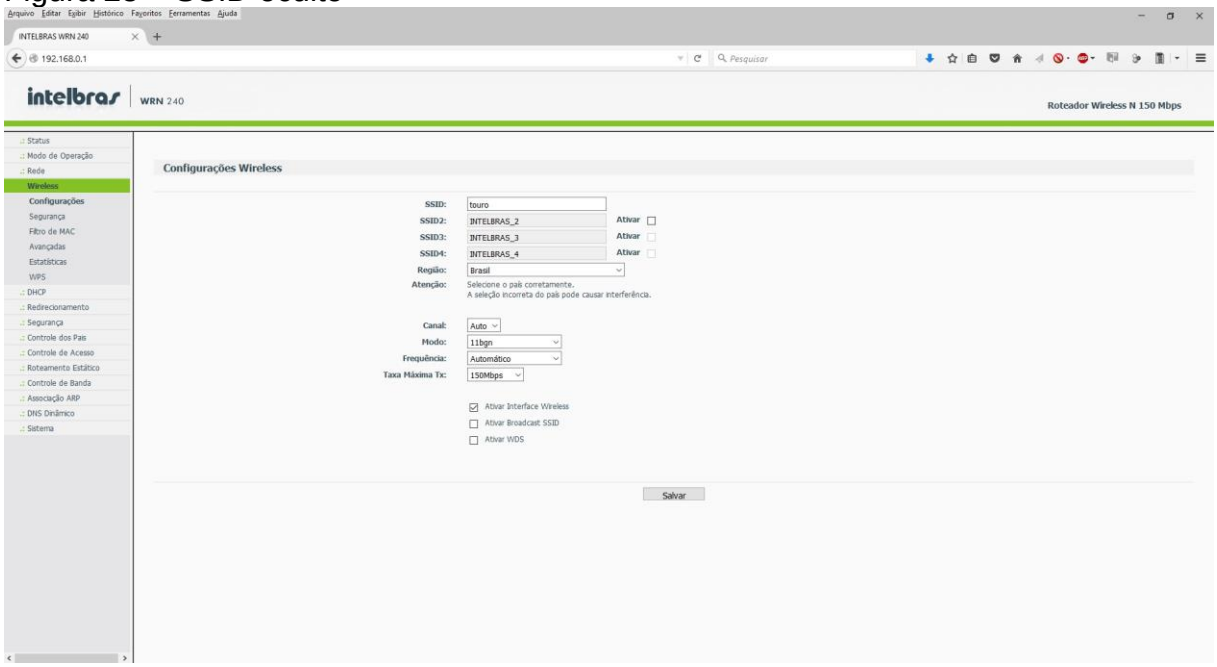


Fonte: Do Autor.

5.3.4 Configuração

SSID identifica a rede, mas também pode ser usado de forma a identificar a rede que alguém mal-intencionado pode tentar acessar. Com isso, pode se fazer uma alteração para ocultar. Nas configurações do AP, onde se encontra o SSID, deve-se desmarcá-lo para ficar oculto e desmarca o *broadcast*, muda o nome da rede antes de autenticar o *notebook*, por exemplo, depois confirma a modificação no AP e a rede estará oculta. Com isso, quando alguém procurar a rede, não vai achar. Outra coisa que pode fazer é diminuir a potência do sinal em configurações no AP. Na figura 25, mostra-se como se oculta o SSID da rede:

Figura 25 – SSID oculto

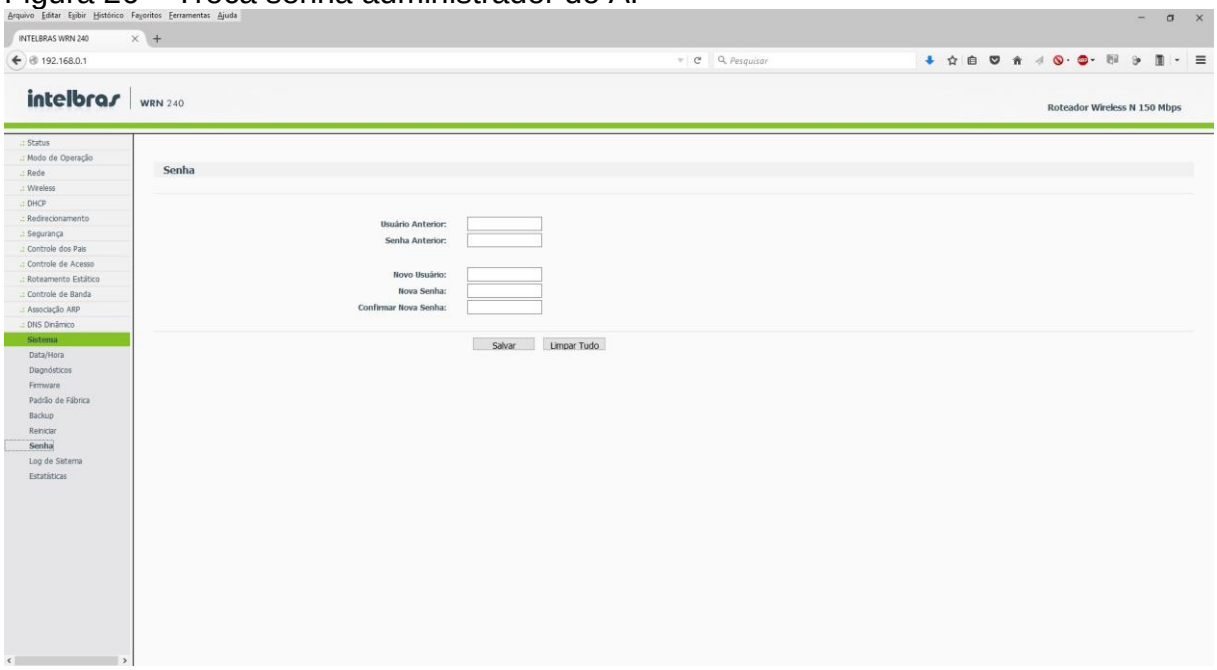


Fonte: Do Autor.

Outra forma de melhorar o acesso ao AP, restringindo apenas ao administrador da rede, é trocar o nome de usuário e senha padrão de fábrica, que normalmente não é feito pelo usuário comum. Para a troca dessas informações, deve-se acessar no navegador por 192.168.0.1 > login: admin > senha: admin >. Depois, deve-se ir ao Menu Sistema > Senha (digitar usuário e senha anterior) e logo abaixo digitar novo usuário e senha, repetindo a senha. Por último, deve-se

salvar e reiniciar o roteador. A figura 26 mostra a troca de senha do administrador da rede:

Figura 26 – Troca senha administrador do AP



Fonte: Do Autor.

Com a troca de senha do dispositivo, evita-se um ataque em massa, que foi descoberto há pouco tempo, onde a maioria dos fabricantes tem como *login* e senha de acesso o padrão admin, e os usuários não o trocam, com um ataque se modificava o DNS da rede responsável por traduzir os endereços IP de cada *site* em nome, fazendo com que o usuário seja direcionado para uma página falsa, tendo os seus dados roubados.

5.3.5 Segurança

Para o tipo de segurança na autenticação com a escolha de WEP, WPA ou WPA2, hoje está sendo mais usado o WPA2, por maior dificuldade de uma pessoa descobrir a senha e acessar a rede (CARMONA, 2005). Para senhas seguras, não se deve usar dados pessoais, não anotar senhas, utilizar senhas com vários tipos de caracteres, contendo no mínimo oito caracteres, trocar no intervalo mínimo de três meses e sem usar sequencias do teclado. Utilizando de *RADIUS*

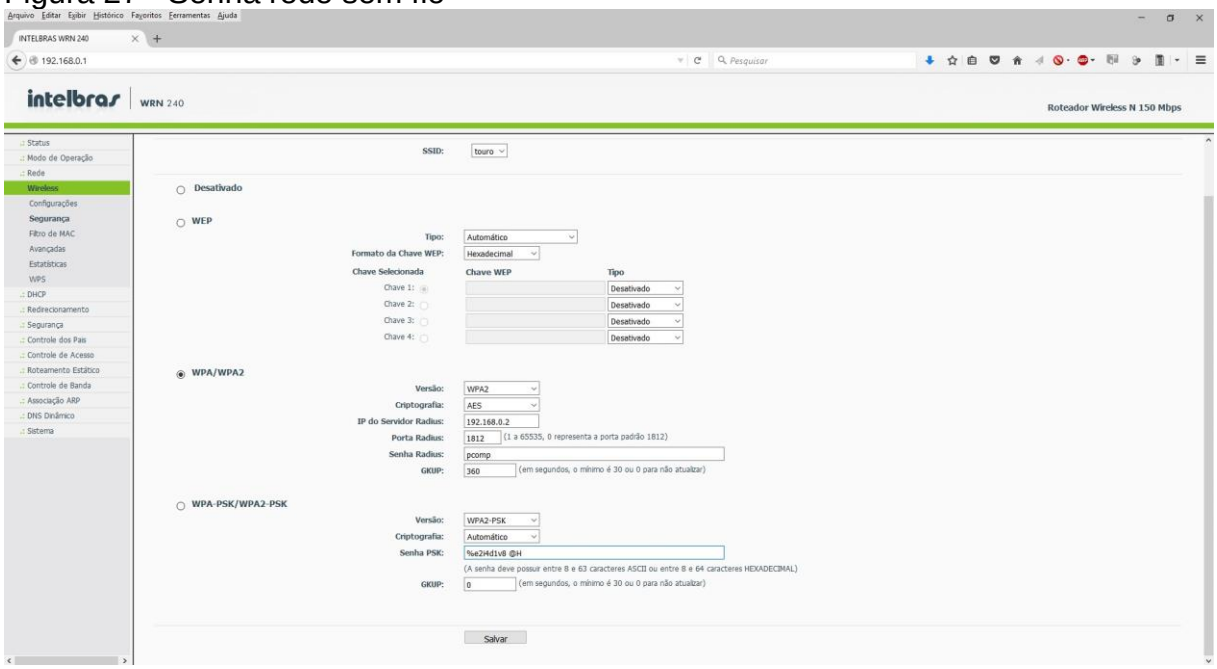
para se autenticar, a rede é uma forma de dificultar ataques, sendo que, para entrar, precisa de usuário e senha, cada um cadastrado no servidor utilizado em Universidades e no setor corporativo.

A política de segurança de informação em um ambiente corporativo ou universitário relaciona normas, ferramentas, procedimentos e compromissos para ter o controle e conseguir a segurança das informações utilizadas nas organizações (NAKAMURA, 2007).

Na forma de dificultar que uma pessoa mal-intencionada tente invadir a rede de forma indevida e não autorizada, deve-se criar uma senha que seja fácil para decorar, mas difícil para se pensar, que seja segura, a fim de auxiliar nessa proposta, têm-se *softwares* e até *sites* que geram senhas, com responsabilidade ao administrador da rede na criação da senha e, assim, evitar só números, letras, sequência de caracteres

Para trocar a senha, na aba de Menu > *Wireless* > Segurança na opção WPA-PSK/WPA2-PSK, em “Senha *psk*” coloca-se a nova senha e, em seguida, salvar, após deve-se reiniciar o roteador.

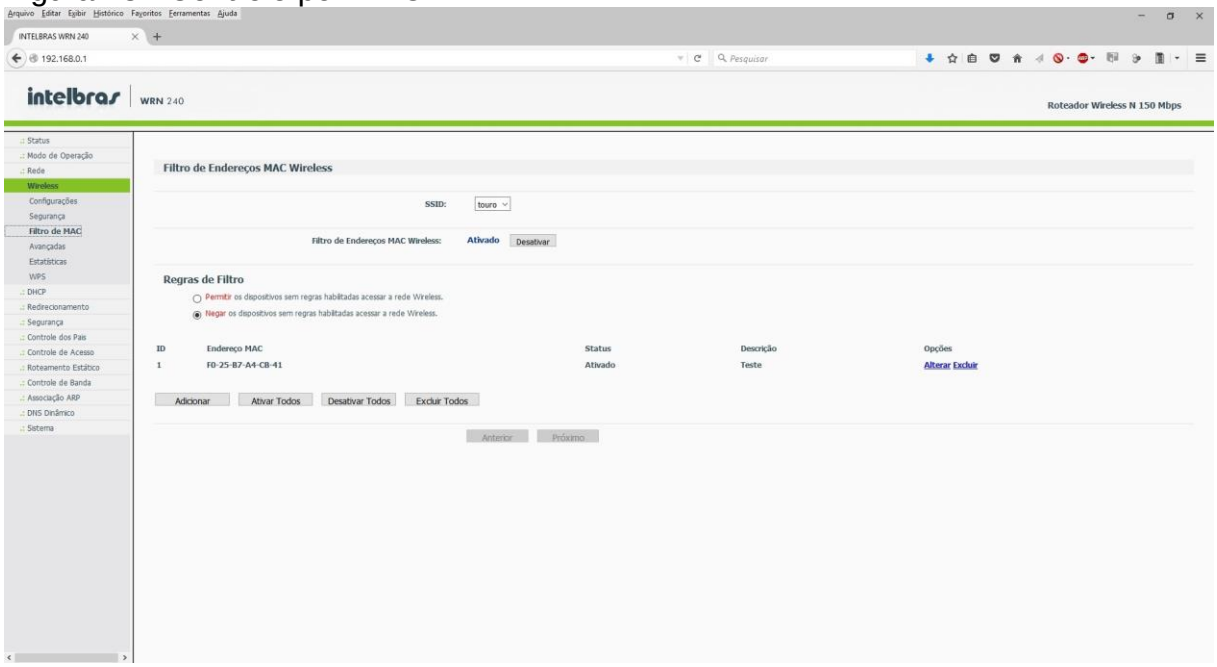
Figura 27 - Senha rede sem fio



Fonte: Do Autor.

Em uma rede com poucos usuários, pode-se aplicar o filtro por endereço MAC, mostrado na figura 28, para filtrar na aba de Menu > *Wireless* > Filtro de MAC. Ativa-se a opção “Filtro de Endereço MAC *Wireless*”, ativa-se a opção “Negar os dispositivos sem regras habilitadas acessar à rede *Wireless*”. Com isso, vai-se em adicionar, preenchendo os campos com endereço MAC do dispositivo, descrição do dispositivo e, por fim, vai até salvar.

Figura 28 - Controle por MAC



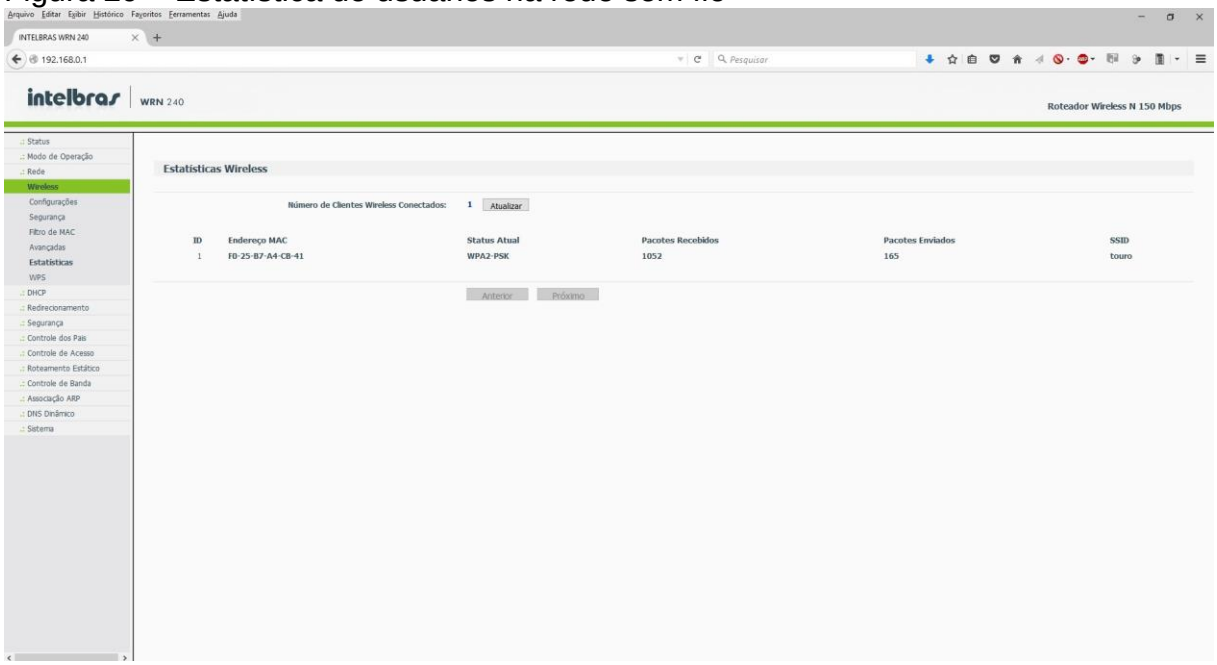
Fonte: Do Autor.

Com a filtragem por MAC, tem-se um maior controle quando cadastrar um cliente a rede sem fio, pois o mesmo, além da senha de autenticação, terá que estar na lista de permissão com o MAC do dispositivo. Quando há muitos dispositivos e uma troca frequente dos mesmos, fica difícil o controle. Quando ninguém estiver usando a rede, deve-se desligar o roteador, pois é um aspecto de segurança.

5.3.6 Contabilização

Para uma avaliação na questão de contabilização, há no AP, na aba de Menu > *Wireless*> Estatísticas, que, na figura 29, mostra os clientes que estão utilizando a rede sem fio.

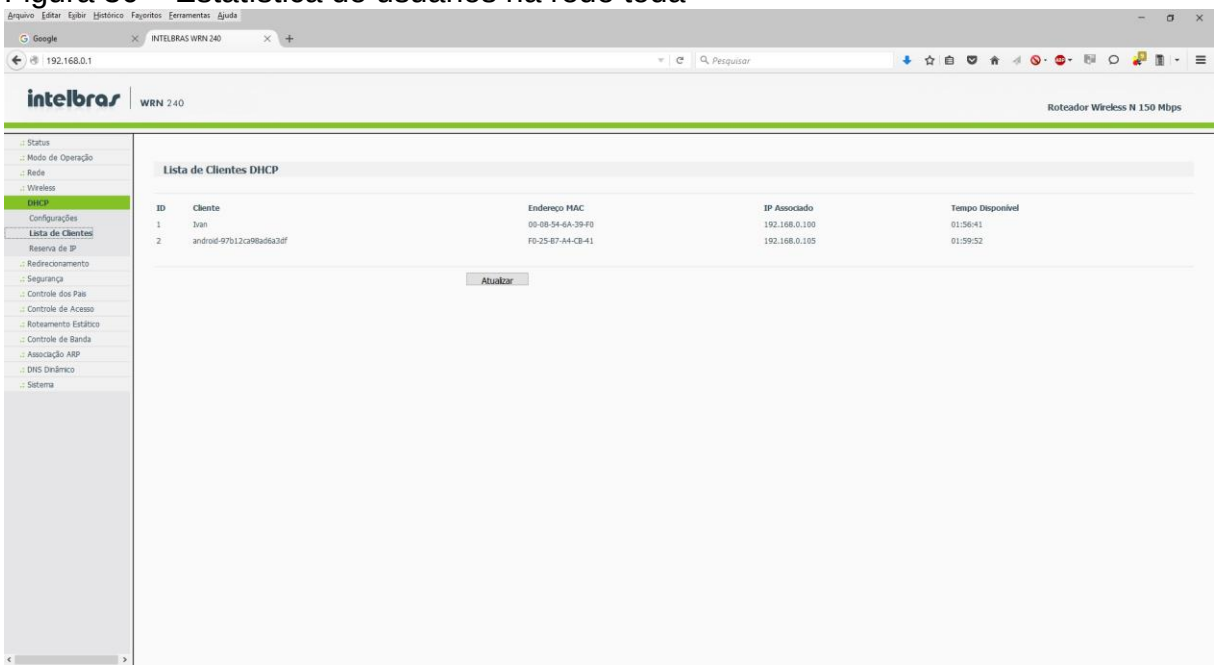
Figura 29 – Estatística de usuários na rede sem fio



Fonte: Do Autor.

Com essas informações, o administrador da rede pode verificar quantos usuários estão utilizando a rede. Para acessar os clientes que estão utilizando toda a rede, deve-se ir ao AP, na aba de menu > DHCP > Lista de Clientes, mostrado na figura 30, todos conectados.

Figura 30 – Estatística de usuários na rede toda



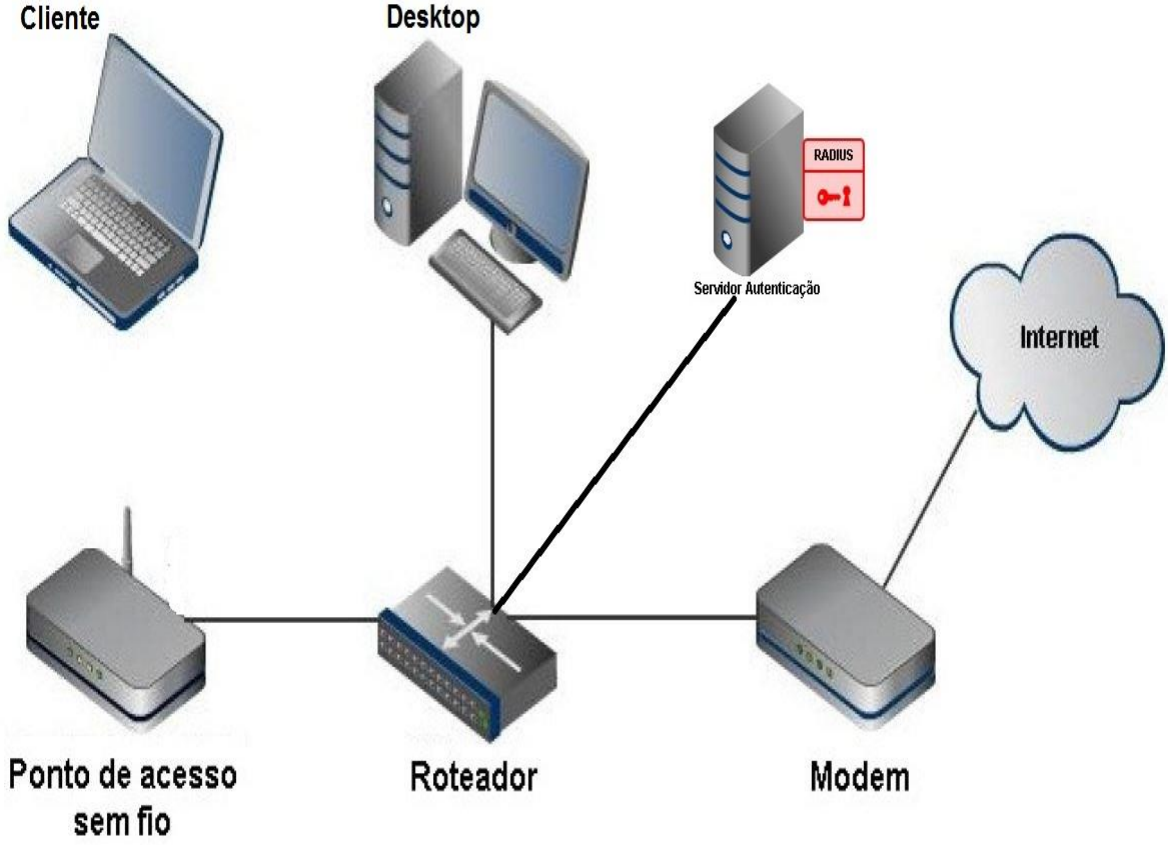
Fonte: Do Autor.

5.4.1 Utilizando FreeRadius

Foi utilizado o *FreeRADIUS* no *Linux,* versão do *Ubuntu* 14.04.3, de forma centralizada, em um ambiente controlado, com supervisão no laboratório, onde o servidor fica em uma máquina que gerencia a autenticação de cada usuário.

O cenário é composto por uma máquina com *Linux*, *access point* e *notebook* funcionando como clientes mostrado na figura 31.

Figura 31 - Topologia da rede



Fonte:Do Autor.

Como mostrado na figura 31 temos em detalhe: Internet para o acesso e navegação; modem ADSL para fazer a conexão com Internet; servidor autenticação: autentica os usuários que querem entrar na rede; switch que interliga o Modem com nó, no caso o “Ponto de acesso sem fio”, onde irá disponibilizar o acesso à rede mundial de computadores; desktop como um computador físico que se conecta

através de uma porta local à interface LAN do “Roteador” e notebook para testes de conexão e verificar o sinal se deslocando pela área de cobertura da rede.

Na utilização de um computador com sistema operacional de código aberto que permite a manipulação, adaptação dos pacotes se tem uma diminuição no custo, pois várias pessoas se dispõem a aprimorar e garantir a funcionalidade do mesmo.

O Linux possui uma comunidade com vários desenvolvedores ao redor do mundo, que estão procurando e corrigindo falhas de programação, garantindo a estabilidade do sistema. Como possui escalabilidade de softwares por utilizar uma linguagem única, se torna mais fácil encontrar programas para fins específicos, como para autenticação utilizou-se o FreeRADIUS.

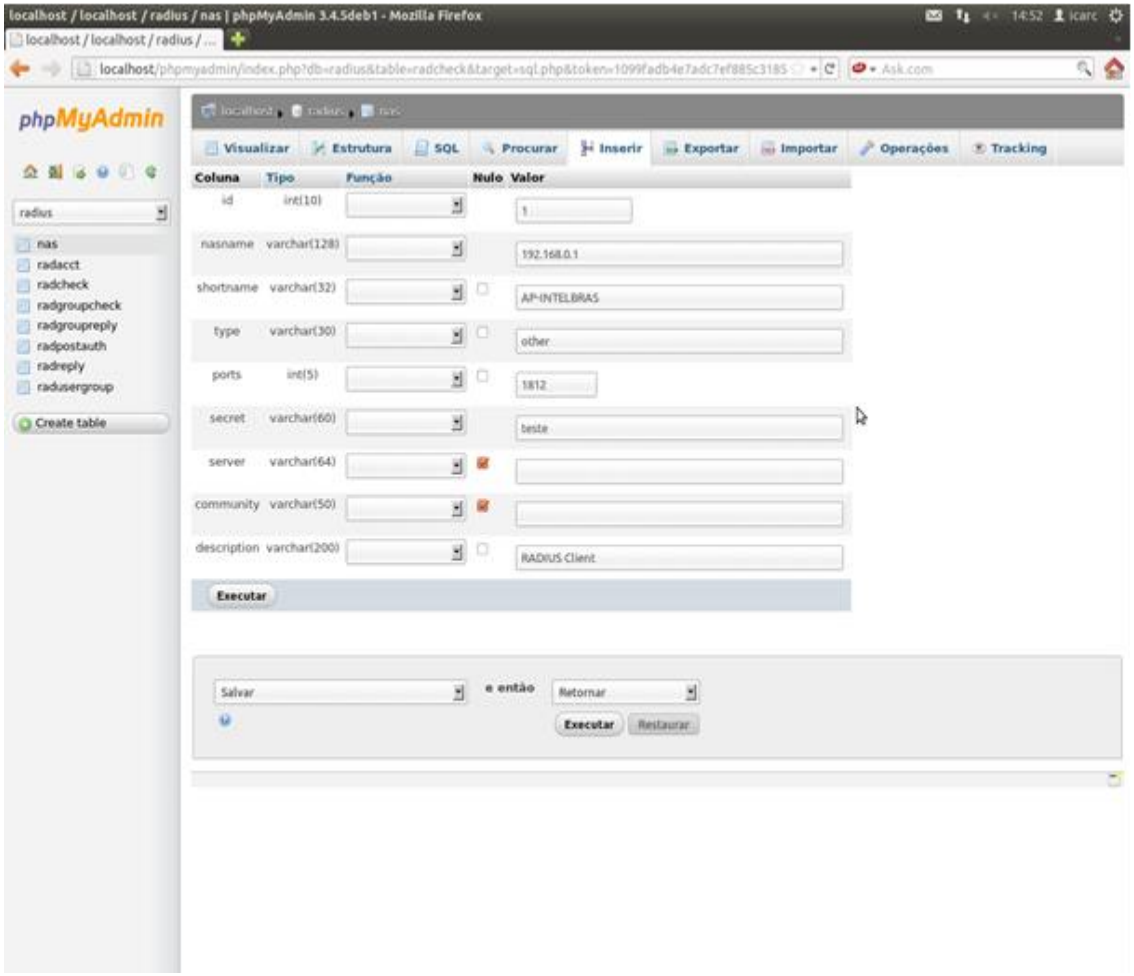
O FreeRADIUS pode ser utilizado na maioria das distribuições Linux permitindo a configuração de várias diretivas de segurança. Sendo um programa de código aberto e implementado para autorizar ou não o acesso do usuário na rede, possui mecanismos de confiança baseados em algoritmos atualmente seguros (WALT, 2011, tradução nossa).

Além do FreeRADIUS, existem ainda o Terminal Access Controller Access-Control System (TACACS); o Kerberos, que trabalha com tickets e faz com que seus clientes tenham o horário sempre ajustado para evitar negação de serviço, sendo pouco utilizado. Para o sistema operacional Microsoft nas versões de servidor comercializa uma opção em autenticação de Internet Authentication Service (IAS).

A instalação e configuração se encontram no Apêndice A. Foi instalado e configurado os *FreeRADIUS*, *phpmyadmin*, *mysql server*, *apache* 2. Com essa instalação e configuração, há dois pontos importantes: que são o cadastro do AP, que pode ser mais de um, e o cadastro de cliente, que são todos administrados no *phpmyadmin*, importante salientar que foi usado um AP comum, e não um com configurações avançadas e com custo elevado.

Na figura 32, mostra-se o cadastro do AP, que vai servir para receber as solicitações dos usuários para entrar na rede, colocando um *id* para o dispositivo, número de IP do mesmo, nome para identificar, porta para o servidor *RADIUS* se conectar com ele, e a senha de acesso para servidor.

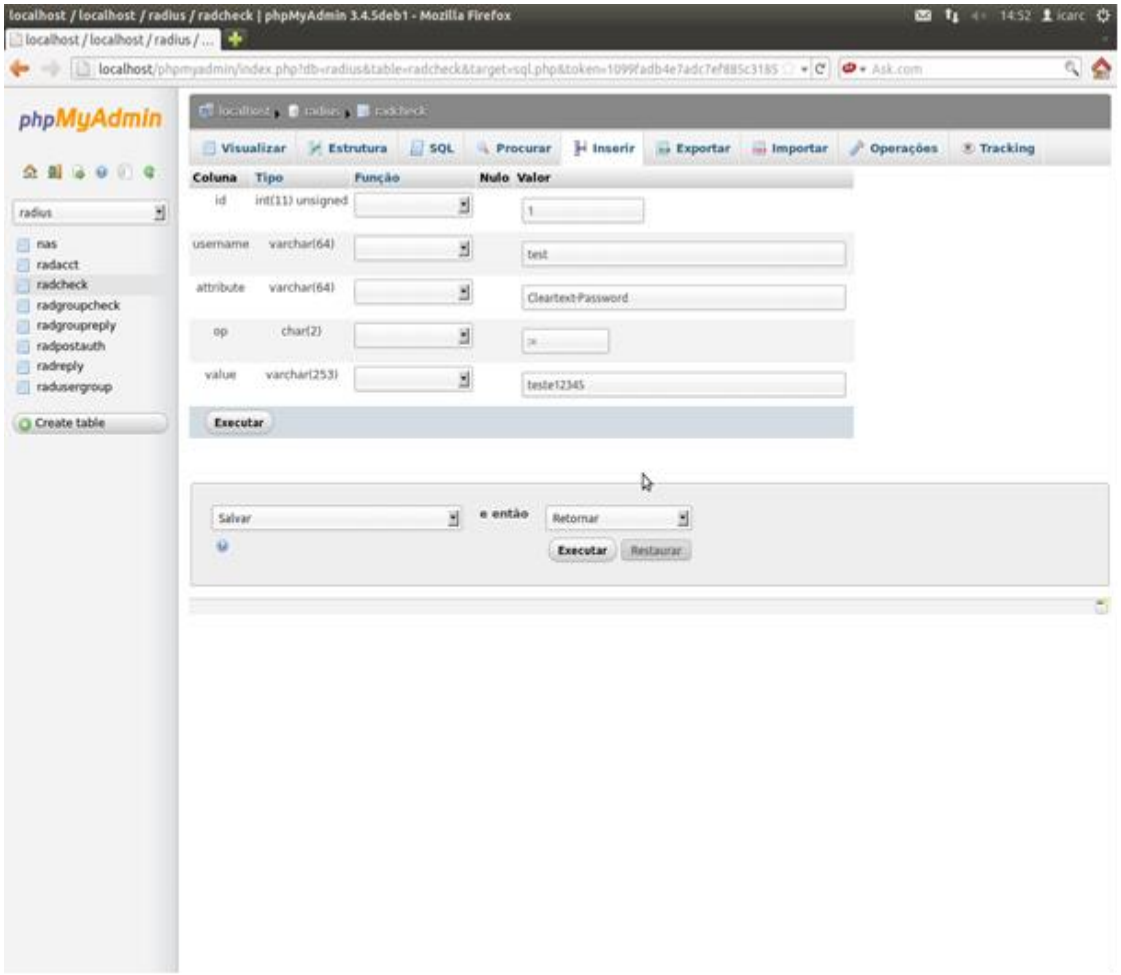
Figura 32 - Cadastro do AP



Fonte: Do Autor.

Para o cadastro de usuários, para se conectarem à rede sem fio no *phpmyadmin*, na Figura 33, mostram-se os itens do cadastro do cliente: *id* para ordenar cada um, nome do usuário, tipo de senha, que é *Cleartext-Password*, atributo da senha com valor e, por último, a senha do cliente.

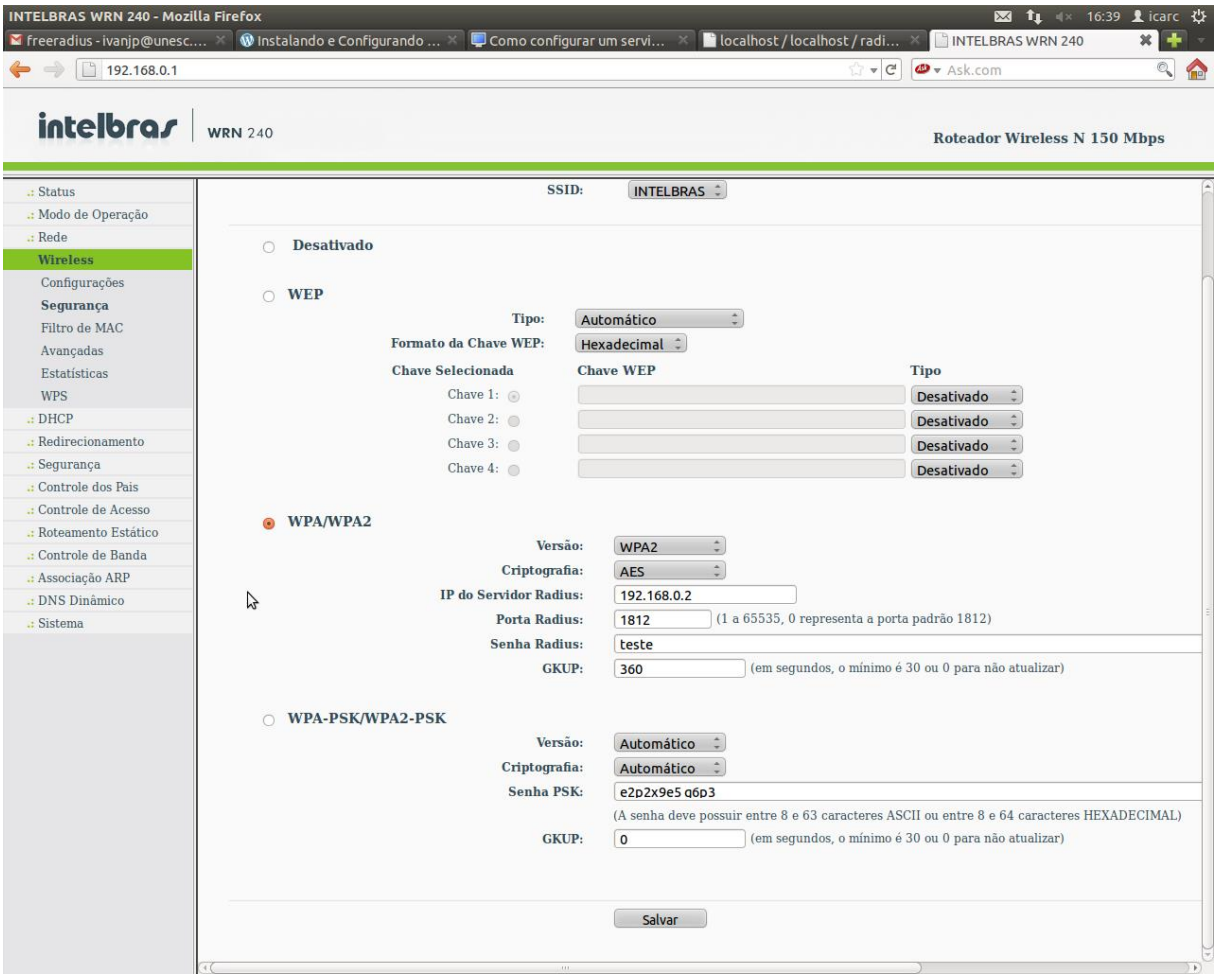
Figura 33 - Cadastro do usuário



Fonte: Do Autor.

Na figura 34 temos o AP e fazermos a configuração do *RADIUS,* acessando pelo navegador e na opção *Wireless*, depois em segurança, marcamos a opção WPA/WPA2. Em versões, escolhemos WPA2. Em criptografia, escolhemos AES. Em IP do Servidor *Radius,* colocamos 192.168.0.2. Em Porta *Radius,* colocamos 1812. Na senha *Radius,* colocamos teste. O DHCP foi habilitado permitindo acesso à rede, com distribuição de IP para os computadores que vão se conectar. Iniciamos o *freeradius* com modo de *debug*: # *freeradius* –X. Em outro terminal, usamos o *radtest* novamente para testar a conexão.

Figura 34 – Configuração RADIUS no AP



Fonte: Do Autor.

Com os usuários devidamente armazenados na base de dados, eles podem se conectar às plataformas *Windows*, *Linux*, *Android* e *IOS*. Assim, usando a rede, informando seu *login* e senha, para quem não tem cadastro, o acesso será negado, fazendo com que cada um seja responsável por seu sigilo de acesso.

5.5 RESULTADOS OBTIDOS

Com os *softwares* apresentados de monitoramento de rede sem fio, bem como com a análise utilizando *softwares,* a rede tem que ser configurada nos aspectos de configuração, falha, contabilização, desempenho e segurança, a fim de ter uma rede operando de forma a não ter problemas futuros.

Em configuração, o administrador da rede, com o auxílio do manual para as configurações de seu *access point*, ajuda a diminuir problemas com os *softwares* de monitoramento, mostrando os APs mais próximos, com informações importantes, como SSID, canal utilizado, qualidade do sinal, padrão 802.11 utilizado, endereço MAC do dispositivo, taxa máxima de transferência de dados. Altera-se o que for necessário para ter a rede funcionando, a fim de atender a todos os clientes da rede, de forma a ter desempenho e segurança.

Para conter as falhas, a prevenção é uma medida que ajuda, pois há falhas em nível de *softwares* e *hardware*, analisando os *logs* do roteador e verificando se todos os dispositivos que compõem a rede estão funcionando normalmente.

Disponível de 14 canais no modo de 2,4Ghz e com apenas três canais que não se sobrepõem, analisando *Site Survey indor*, com programas de monitoramento para diminuir a interferência por utilização de canais, há duas soluções que são: escolher entre os três de forma a utilizar o mesmo, usando os canais no salto de três em três, a fim de melhorar o desempenho e com o uso de criptografia WPA2 para senhas de rede.

Na contabilização, há por parte do administrador da rede uma lista de clientes, que deve ser inspecionada periodicamente para controle de usuários autorizados.

No aspecto de segurança, há a utilização de autenticação por meio de *RADIUS*, que se mostrou uma alternativa viável para controle de usuários de uma rede sem fio, servindo para um modelo corporativo e para universidades de maneira a ter mais controle sobre quem está utilizando, sendo que, com a adoção deste modelo, os usuários não vão disponibilizar seu *login* e senha, sabendo que tudo que for feito será de sua responsabilidade.

5.5.1 SOFTWARES DE GERENCIA E MONITORAMENTO

Na ferramenta de gerência de rede sem fio, espera-se que tenha o controle de usuários que acessam à rede. Também que ela forneça informações sobre os usuários registrados e sobre o perfil de cada um. Sobre a conexão dos usuários, são informados usuários conectados, endereço IP de cada conexão, data e hora de início de cada conexão. Na de monitoramento, visualizam-se as informações para um diagnóstico de um possível problema (NADEU et al., 2003, tradução nossa).

O *software* de gerência abordado no trabalho foi o *FreeRADIUS,* que atende as gerências de contabilização e de segurança. Na contabilização, há uma lista com os usuários que têm permissão para acessar à rede sem fio, cadastrados em um banco de dados, que é o *phpmyadmin,* sendo ele acessado apenas pelo administrador da rede e na segurança com a autenticação do usuário com *login* e senha cadastrados no banco.

Já nos *softwares* de monitoramento, há as informações de SSID com o nome da rede; MAC com o endereço único de cada dispositivo, canal de 1 a 14, de 36 ou de 100, a 161; potência do sinal de -35 a -110 dbm; padrão de rede com 802.1ª/b/g/n/AC/entre outros; tipo de segurança, sendo aberta, WEP, WPA, WPA2 e entre outros; GPS com localização, dependendo do dispositivo utilizado; modo de operação, sendo infraestruturada ou Ad-hoc; frequência utilizada, sendo 2.4 Ghz e 5 Ghz; outras informações peculiares a dos *softwares* mostrados na tabela 6.

Tabela 6 - Funcionalidade dos softwares de monitoramento

Funcionalidades/ softwares	inSSIDer	WirelessMon	Xirrus Wi-Fi Inspector	WIFi Locator
Visualização do SSID	X	X	X	X
MAC	X	X	X	X
Canal Utilizado	X	X	X	X
Potência do Sinal	X	X	X	X
Padrão de Rede	X	X	X	X
Tipo de Segurança	X	X	X	
GPS	X	X	X	X
Frequência	X	X	X	X
Sobreposição de Canais	X	X		
Modo de operação: infraestrutura ou Ad-hoc	X	X	X	X

Fonte: Do Autor.

Na tabela 6, mostra-se que usando estes programas se pode ter uma noção de como a rede está em relação aos outros dispositivos e que o *InSSIDer* e o *WirelessMon* se destacam, com um gráfico que mostra a sobreposição dos canais em relação aos demais equipamentos.

6 CONCLUSÃO

Este trabalho abordou aspectos de gerência e monitoramento em uma WLAN, local para implantar, verificando aspectos de desempenho, contabilização, configuração, falhas e segurança.

Entender e aplicar os conceitos de gerência de redes sem fio foi atingido com sucesso, com cada uma das partes de gerência detalhada de forma clara e usadas na parte de monitoramento com seus aspectos e, na de gerência, apenas em contabilização e segurança.

Estudar e aplicar *softwares* de monitoramento de redes sem fio foi concluído de forma que, com o uso de mais de um programa, pode-se ter uma melhor compressão de como a rede está em relação às outras, de forma a analisar e tomar as devidas alterações no equipamento que transmite o sinal sem fio pelo perímetro.

Compreender aspectos de segurança a serem avaliados na implantação de uma gerência de redes mostrou que se deve preocupar com a segurança das informações que trafegam na rede, com configurações e *softwares* que auxiliam na análise da rede, e as residências próximas para dificultar os ataques de pessoas que tentam se conectar de forma não autorizada.

Demonstrar o estudo de caso de ferramentas de monitoramento de uma rede sem fio que a configuração certa diminui os ataques, tornando mais difícil a entrada de intrusos na rede, evitando, assim, interferências com outros equipamentos, comparando as informações obtidas dos outros dispositivos com o da pesquisa.

Propor uma gerência de segurança centralizada de redes foi muito bom, bem como trabalhar com o *FreeRADIUS* foi bom, pois mostrou que autenticação dos usuários facilita o controle e monitoramento da rede, ainda mais se for implantada em uma empresa e em uma universidade, que têm suas políticas de segurança como prioridade.

Foram encontradas dificuldades na hora de implantar a rede sem fio WLAN, no aspecto de como configurar, pois, as vezes não era possível autenticar o usuário, sendo resolvido mais tarde.

No diferencial com outros trabalhos, teve a utilização e um equipamento de baixo custo para realização dos testes e análise dos mesmos. Para utilização de *RADIUS,* têm-se dispositivos mais robustos, com custos elevados para aquisição, e não se tinha esse propósito. E também a gerência a ser aplicada de uma forma menos complexa, na forma de que aplicado em uma residência ou pequena empresa se tenha um resultado satisfatório.

Dos resultados obtidos com as análises, pode-se afirmar que configurar o AP de forma a olhar todas as opções possíveis é uma forma de gerenciar a rede, de forma que a verificação com os *softwares* de monitoramento como o *inSSIDer*, *Xirrus Wi-Fi Inspector*, *Wirelessmon* e o *Wifi Locator*. No desempenho, diminuindo a interferência e com o uso de canais diferentes dos APs encontrados mais próximos da rede e alterando a potência do sinal para um alcance controlado. Em segurança, mostrando os tipos de autenticações possíveis para ter uma rede mais segura usando o protocolo WPA2, com uma senha segura, evitando possíveis ataques mostrados com o monitoramento e com a gerência da rede com *FreeRADIUS.* Foi um sucesso.

Espera-se que o levantamento bibliográfico e as análises realizadas neste trabalho possam ser ampliados e utilizados nos quesitos configuração, desempenho e segurança, que esta contribuição efetue mais um passo para assegurar maior controle em uma rede sem fio.

A partir desta pesquisa, pode-se dar continuidade por meio de algumas sugestões de trabalhos futuros: utilizar o *RADIUS* em uma empresa com muitos equipamentos sem fio e utilizar gerência com outros modelos apresentados neste trabalho.

REFERÊNCIAS

ANATEL. **Lei geral das telecomunicações**. Disponível em: <http://www.anatel.gov.br>. Acessado em: 20 out. 2011.

ANDRADE, L. P. **Análise das vulnerabilidades de segurança existentes nas redes locais sem fio:** um estudo de caso do projeto Wlaca**.** 2004. 78 f. Trabalho de Conclusão de Curso (Curso de Ciência da Computação) Universidade Federal do Pará, Belém, 2004.

CACTI. **The complete RRDTool-based graphing solution**. Disponível em: <http://www.cacti.net>. Acesso em: 12 mai. 2012.

CARMONA, T. **Segredos da espionagem digital**. São Paulo: UNIVERSO DOS LIVROS ,2005.

CHANDRA, P. et al. **Wireless networking**: know it all. Burlington: Elsevier, 2008.

COLEMAN, D. D.; WESTCOTT, D. A. **CWNA – Certified Wireless Network Administrator**: study guide. Indianapolis: Wiley Publishing, 2006.

COMER, D. E. **Redes de computadores e internet.** 4. ed. Porto Alegre: Bookman. 2007.

CORREIA, M. **Gerência de redes**. 2004. 220 f. Tese (Doutorado em Sistemas de Informação) União Educacional de Minas Gerais, Uberlândia, 2004.

COSTA, F. W. **Análise de padrões de segurança em redes sem fio IEEE 802.11.** 2009. 89 f. Trabalho de Conclusão de Curso (Curso de Ciência da Computação) Universidade do Extremo Sul Catarinense, Criciúma, 2009.

COZER, F. L. **Segurança redes sem fio.** 2006. 98 f. Trabalho de Conclusão de Curso (Curso de Ciência da Computação) Faculdade de Jaguariúna, São Paulo, 2006. Disponível em: < http://bibdig.poliseducacional.com.br/document/?down=100>. Acesso em: 12 mar.2012.

DANTAS,M.**Tecnologias de redes de comunicação e computadores**. Rio de Janeiro: Axcel Books, 2002.

ENGST, A.; FLEISHMAN, G. **Kit do iniciante em redes sem fio:** o guia prático sobre redes Wi-Fi para Windows e Macintosh. São Paulo: Pearson Makron Books, 2005.

FLECK, B.; POTTER, B. **802.11 Security**. Sebastopol: O'Reilly, 2002.

FLICKENGER, Rob. **Redes sem fio no Mundo em Desenvolvimento:** Um guia prático para o planejamento e a construção de uma infra-estrutura de

telecomunicações. 2. ed. Washington: Hacker Friendly Llc, 2008. 397 p.

FRASSON JUNIOR, D.**. Análise de vulnerabilidades envolvendo aplicações móveis:** estudo de caso na aplicação móvel de acesso à base de dados de um sistema de registro eletrônico em saúde para UTI. 2008. 76 f. Trabalho de Conclusão de Curso (Curso de Ciência da Computação) Universidade do Extremo Sul Catarinense, Criciúma, 2008.

FOUROZAN, B. A. **Comunicação de dados e redes de computadores**. 3. ed. Porto Alegre: Bookerman, 2006.

GAST, Matthew**. 802.11ac a survival guide**. Sebastopol: O´Reilly, 2013**.. 802.11 Wireless Networks**: the definitive guide. Sebastopol: O´Reilly, 2002.

GRUMEWALD, M. A. **Redes sem fio**. 2007. 45 f. Monografia (Especialização em Tecnologia da Informação) Faculdade de Informática Pulista, São Pulo, 2007.

GEIER, J. **RF site survey steps.** 2002. Disponível em: <http://www.wi-fiplanet.com/tutorials/article.php/1116311/RF-Site-Survey-Steps.htm>. Acesso em: 16 set. 2015.

HASSELL, J. **RADIUS.** Sebastopol: O´reilly, 2002.

IPERF. Disponível em: <http://iperf.sourceforge.net/>. Acesso em: 12 out. 2015.

KUROSE, J. F.; ROSS, K. W**. Redes de computadores e a internet**: uma abordagem top-down. 3. ed. São Paulo: Pearson Addison Wesley, 2006.

LOPES, R. V. et al. **Melhores práticas para gerência de redes de computadores**. Rio de Janeiro: Campus, 2003.

MAURO, D. R.; SCHMIDT, K. J. **Essential SNMP**. 2. ed. Sebastopol: O´reilly, 2005.

MENDES, C. C. S. **Gerenciamento de recursos em redes sem fio IEEE 802.11**. 2008. 92 f. Dissertação (Mestrado em Engenharia Elétrica e Informática Industrial) Universidade Tecnológica Federal do Paraná, Curitiba, 2008.

MORENO, E. D.; PEREIRA, F. D.; CHIARAMONTE, R. B. **Criptografia em software e hardware**. São Paulo, 2005.

NAKAMURA, E. T.; GEUS, P. L. **Segurança de redes:** em ambientes cooperativos. São Paulo: Novatec, 2007.

NADEU, T. D. **MPLS network management M1Bs, tools and techniques**. San Francisco: Morgan Kaufmann Publishers, 2003.

NAGIOS**. Official Nagios documentation**. Disponível em: <http://www.nagios.org>. Acesso em: 10 mai. 2012.

PETERSON, L. L; DAVIE, B. S**. Redes de computadores:** uma abordagem de sistemas. Rio de Janeiro: Elsevier, 2004.

PINHEIRO, J. M. S. **Site survey:** o segredo de um bom projeto. Disponível em: <http://www.projetoderedes.com.br/artigos/artigo_site_survey.php>. Acesso em: 17 set. 2015.

RIBAS, J. C. C**. Perfil de link sem fio em ambiente aberto:** avaliação através de medições. 2002. 175 f. Dissertação (Mestrado em Ciências da Computação) Universidade Federal de Santa Catarina, Florianópolis, 2002.

RODRIGUES, W. C. J.; SANTOS, E. F. Site survey: mapeamento, detecção de vulnerabilidades e análise de sinal de redes sem fio**. Revista Exacta,** São Paulo, v. 5, p. 69-78, 2007. Disponível em: <http://www.redalyc.org/articulo.oa?id=81050107>. Acesso em: 16 set. 2015.

ROSNAM, P.; LEARY, J. **Wireless LAN fundamentals**. Cisco Press, 2003.

ROSS, J. **The book of wireless:** a painless guide to Wi-Fi and broadband wireless. 2. ed. San Francisco: No Press, 2008.

RUFINO, N. M. O. **Segurança em redes sem fio:** aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth. São Paulo: Novatec, 2005.

SANCHES, Carlos Alberto**. Projetando redes WLAN**: conceitos e práticas. Rio de Janeiro**:** Érica, 2005.

SILVA, A. Q**. Planejando redes com acesso sem fio à internet utilizando a tecnologia Wimax integrada a tecnologia Wi-Fi.** 2006. 80 f. Trabalho de Conclusão de Curso (Curso de Ciência da Computação) Universidade Federal de Pará, Belém, 2006.

SOUZA, L. B. **Redes de computadores**: dados, voz e imagem. 8.ed. São Paulo: Érica, 2005.

STALLINGS, W. **Redes e sistemas de comunicação de dados.** Rio de Janeiro: Elsevier, 2005.

TANENBAUM, R. S.; WETHERALL, T. U. **Computer networks**. 5. ed. Boston: Pearson, 2011.

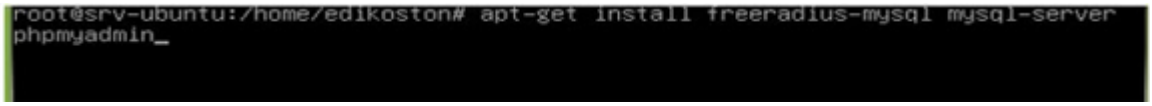
WALT, Dirk Van Der. **FreeRADIUS Beginner's Guide.** Birmingham: Packt Publishing, 2011.

ZABBIX. **The ultimate monitoring solution**. Disponível em: <http://www.zabbix.com>. Acesso em: 12 mai. 2012.

APÊNDICE(S)

APÊNDICE A – INSTALAÇÃO E CONFIGURAÇÃO FREERADIUS

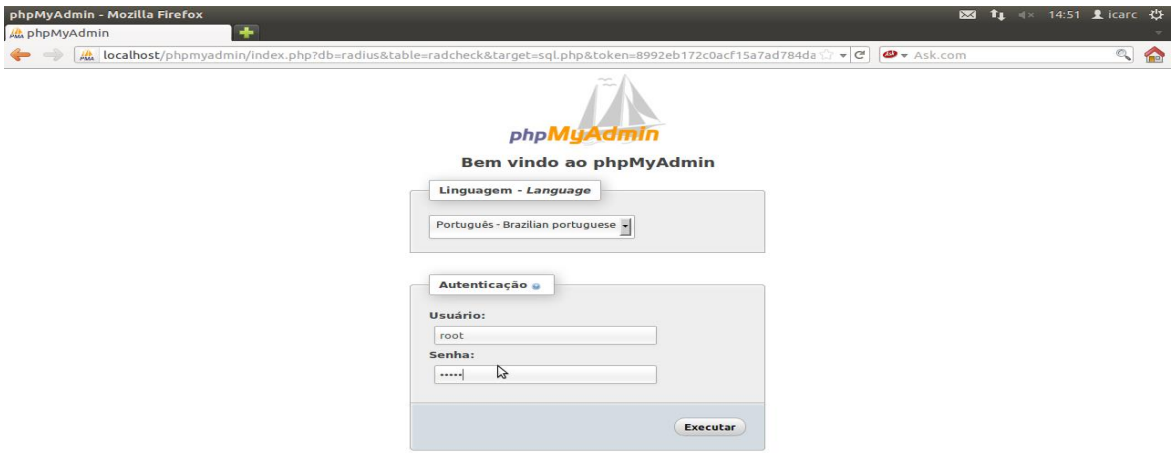
Instalando e configurando o servidor *RADIUS,* responsável pela autenticação dos usuários que irão usar a rede *Wi-Fi, e c*om o usuário *root* e com o comando sudo –i, colocando logo após a senha de usuário, vamos instalar os pacotes necessários para criar o servidor de autenticação:



Em seguida, vamos definir uma senha para o usuário *Mysql*, a fim de facilitar, definimos nossa senha com *icarc,* como na imagem. Depois confirmamos a senha digitada anteriormente, por segurança.

Logo após, vamos fazer a instalação do *phpmyadmin,* que serve para interagir diretamente com a base de dados *MySql,* em uma interface gráfica amigável para o administrador de rede.

Com o *apache2,* façamos o mesmo que o anterior, defindo a senha. Quando escolhida a opção “SIM”, indica que vamos ligar a base de dados *mysql* ao *phpmyadmin.* Em seguida, serão apresentadas as telas para a senha do usuário da base de dados, que é *icarc*,



Agora abrimos o navegador de qualquer máquina que esteja na estação do servidor *Linux,* digitando localhost/phpmyadmin. Colocamos o usuário e senha do *phpmyadmin,* que no nosso caso é *user*: *root* e *password*: *icarc*.

Em seguida, criamos um banco de dados onde este irá receber todas as tabelas do *freeradius-mysql*. Acessamos à aba “Banco de Dados”, no campo “Criar novo Banco de Dados”. Criamos um banco chamado “*radius*”, *clicamos* no botão “Criar”.

Em seguida, vamos transportar todas as tabelas do *freeradius* para dentro do *Mysql-server*. Importamos o *arquivo.sql* de */etc/freeradius/sql/mysql/schema.sql*: com *mysql -u root -p radius < /etc/freeradius/sql/mysql/schema.sql* e *mysql -u root -p radius < /etc/freeradius/sql/mysql/nas.sql*.

Vamos preparar alguns **.conf do freeradius* para que o *freeradius* e o MySql possam trocar informações dentro do diretório “/etc/freeradius/”. Vamos procurar pelo arquivo “radiusd.conf”, com o editor de arquivos preferido. Abrimos o *radiusd.conf*. *pico radiusd.conf.* Procuramos pelo campo *“$INCLUDE sql.conf*” e descomentamos, removendo o símbolo “#” que se encontra no início da *linha.#$INCLUED sql.conf* para *$INCLUDE sql.conf*, e depois salvamos.

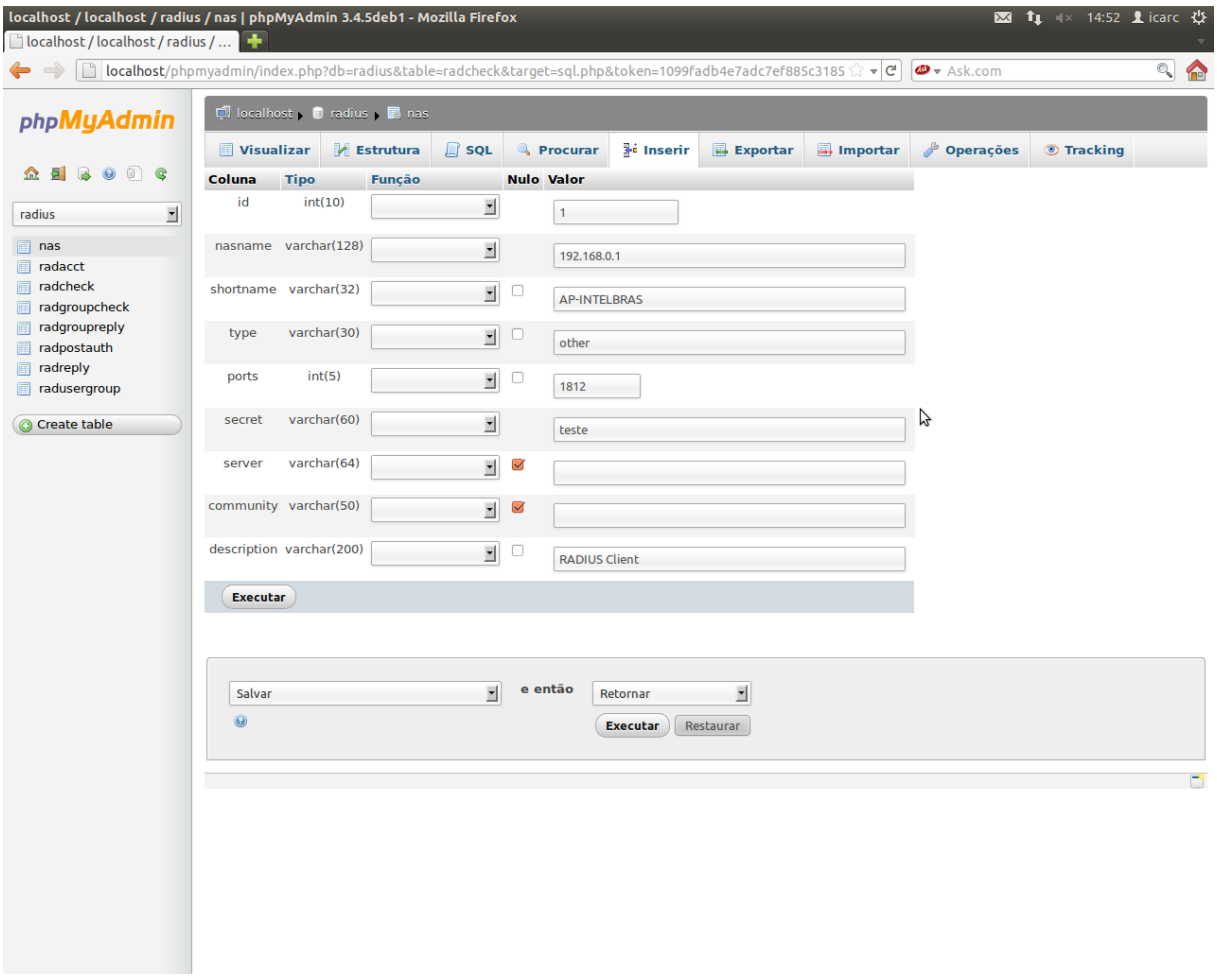
Em seguida, editamos o arquivo *“sql.conf”,* procuramos pelo campo *login = “radius”* e *password = “radpass”.* Trocamo-no no campo *login* o “*radius*”

pelo usuário do banco de dados que é o “*root*” e, no campo *password,* a senha de “*radpass*” para a senha do usuário do banco de dados “*icarc*”, OBS1: O usuário e senha devem estar entre aspas “ “.

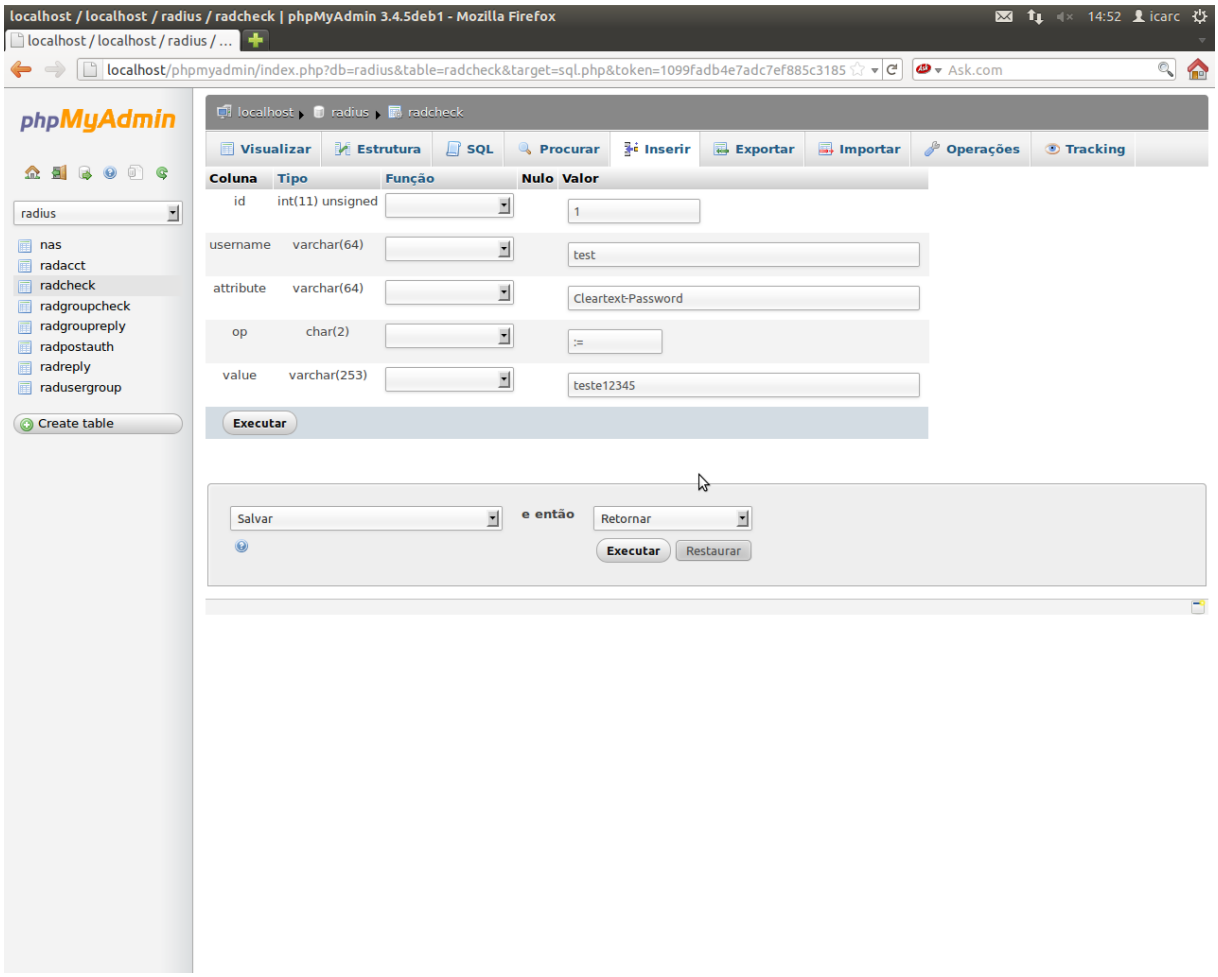
Ainda faltam mais dois arquivos de texto para ser alterado um “*default*” e outro *“inner-tunnel”,* ambos se encontram no diretório *“/etc/freerdius/sites-available/”.*

No arquivo “*default*”, abaixo da linha “*authorize*”, procuramos por *sql* e descomentamos. Mais abaixo procuramos por “*accounting*” e também descomentamos as linhas *sql*. Salvamos e saímos do arquivo de texto *default*. Salvamos e saimos do arquivo de texto *“inner-tunner”.*

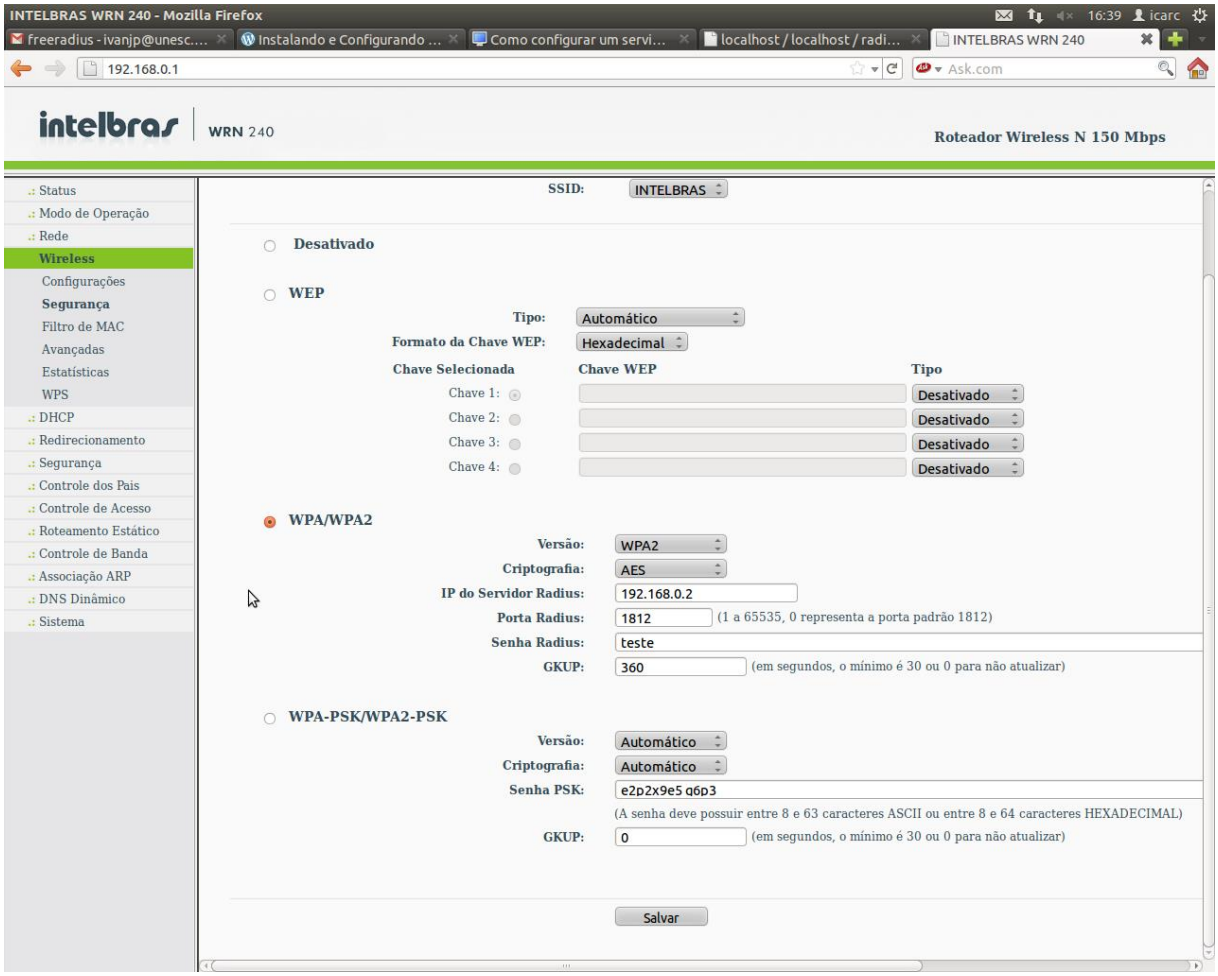
Vamos voltar ao *phpmyadmin* e editar as seguintes tabelas (nas, *radcheck*). Começaremos pelo “nas”, em *nasname,* colocamos o *ip* da AP. No campo *shortname*, uma identificação do equipamento que está fazendo a consulta no servidor *RADIUS*. No campo *ports,* a porta que o serviço *radius* trabalha para autenticação 1812. Por último, em *secret,* a senha para a autenticação. Para fins didáticos, colocamos senhas fáceis. Na sequência, mandamos executar.



Em seguida, cadastramos os usuários que terão permissão para utilizar a rede *Wi-Fi*, lembrando que no passo anterior cadastramos o equipamento que fará a consulta ao servidor *RADIUS.* Dessa vez, será o usuário que fará a consulta ao servidor. Caso um usuário não esteja cadastrado, seu acesso à rede *Wi-Fi* será negado.



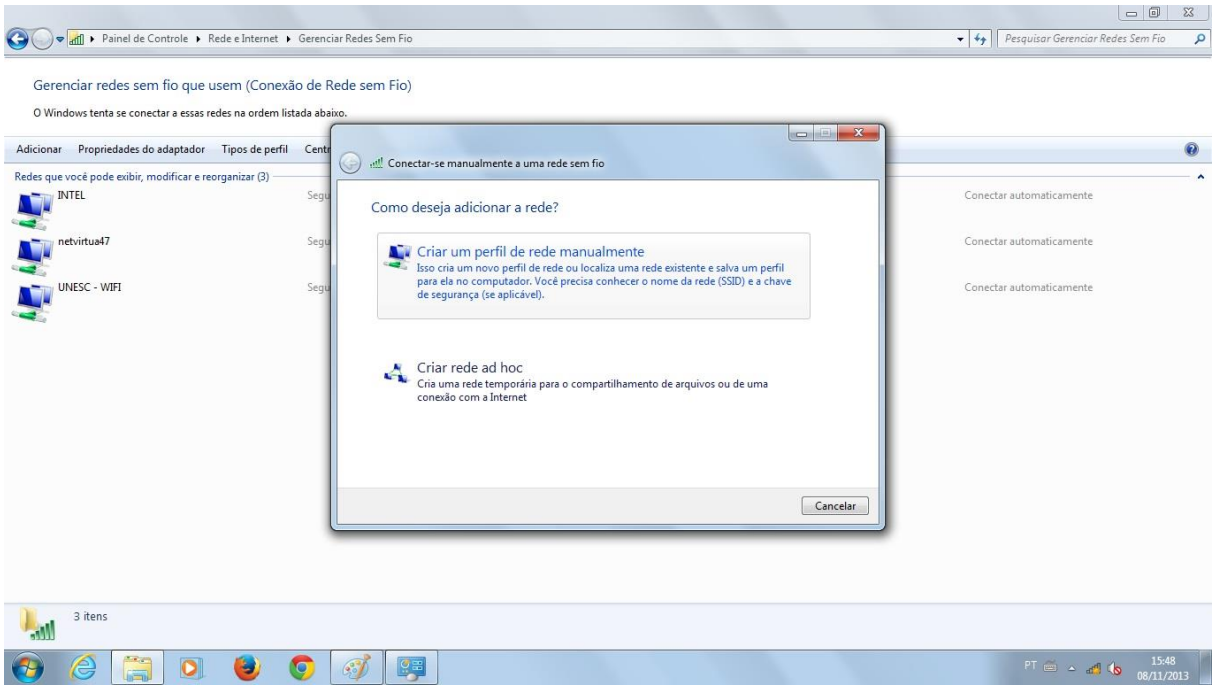
Fizemos um cadastrado com um usuário chamado *test,* com a senha *teste12345*. Com a base de dados do *radius* configurada, vamos configurar o AP para receber a autenticação no servidor *RADIUS*.



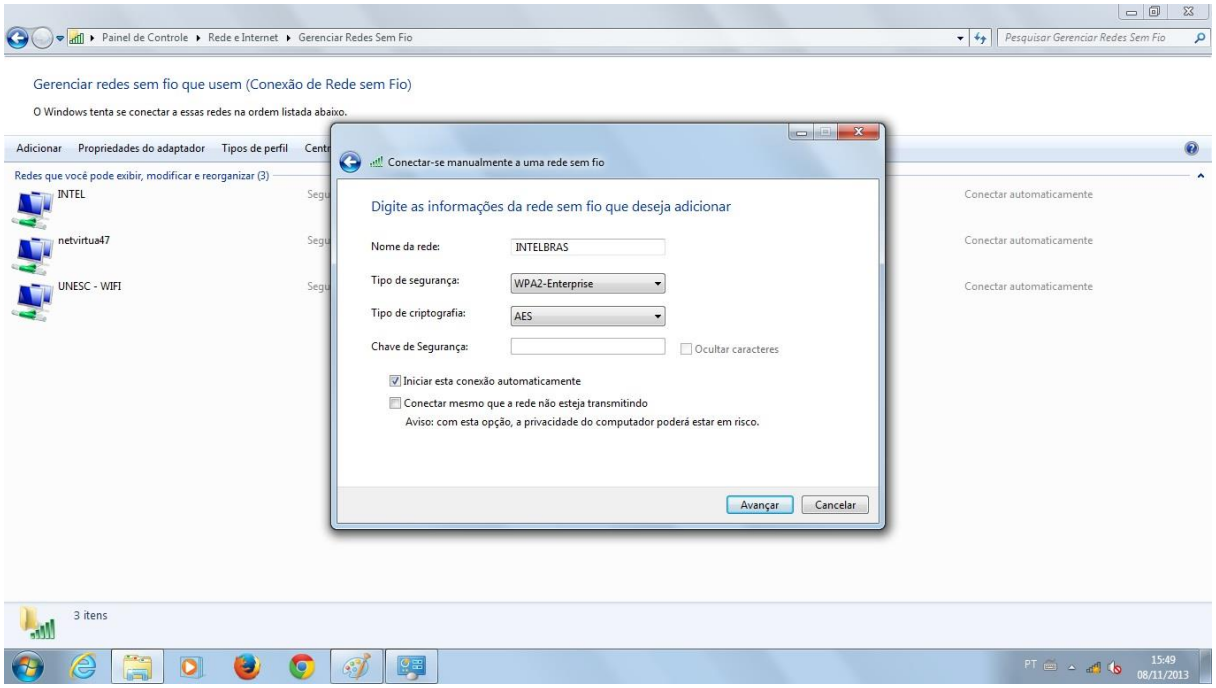
Voltamos ao AP para fazermos a configuração do *RADIUS,* acessando pelo navegador, com 192.168.0.1, com senha e *login* admin. Na opção *Wireless*, depois em segurança, marcamos a opção WPA/WPA2. Em versões, escolhemos WPA2. Em criptografia, escolhemos AES. Em IP do Servidor *Radius,* colocamos 192.168.0.2. Em Porta *Radius,* colocamos 1812. Na senha *Radius,* colocamos teste. O DHCP foi habilitado permitindo acesso à rede, com distribuição de IP para os computadores que vão se conectar. Iniciamos o *freeradius* com modo de *debug*: # *freeradius* –X. Em outro terminal, usamos o *radtest* novamente para testar a conexão.

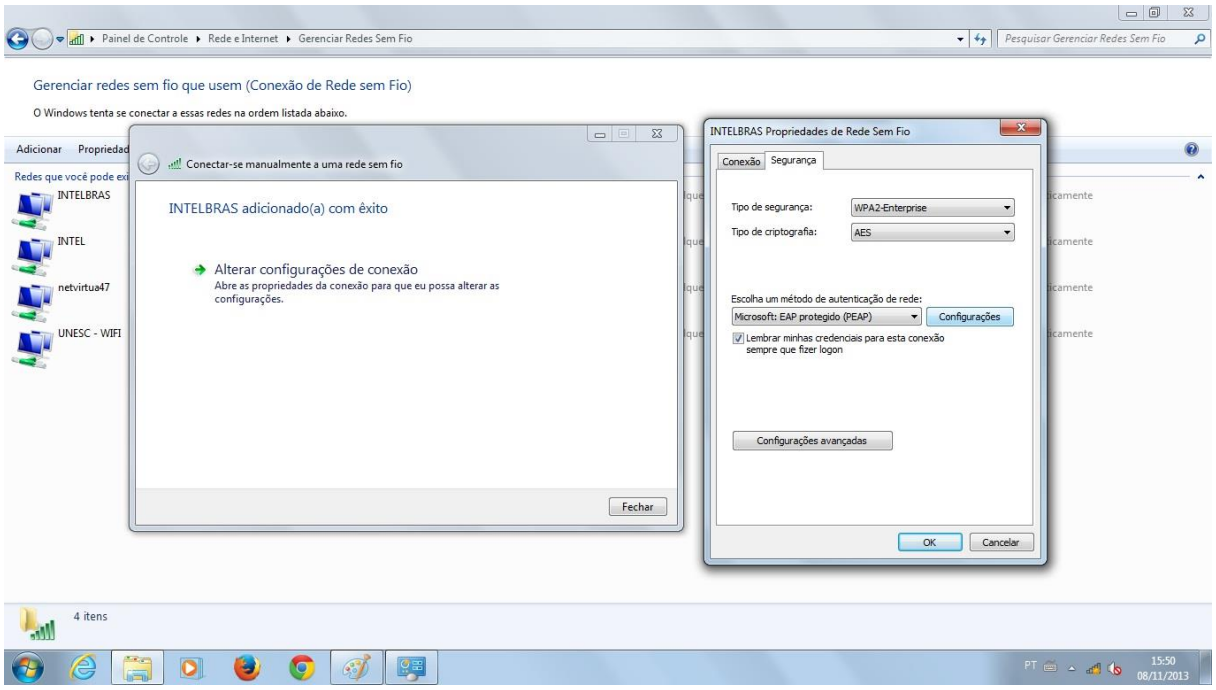
Em seguida, configuramos a máquina do usuário final e essa configuração será realizada em uma máquina *Windows* 7 *Ultimate*. Segue o passo a passo desta configuração.

Abrindo a central de rede e compartilhamento, vamos até gerenciar redes sem fio, logo em criar um perfil de rede manual.

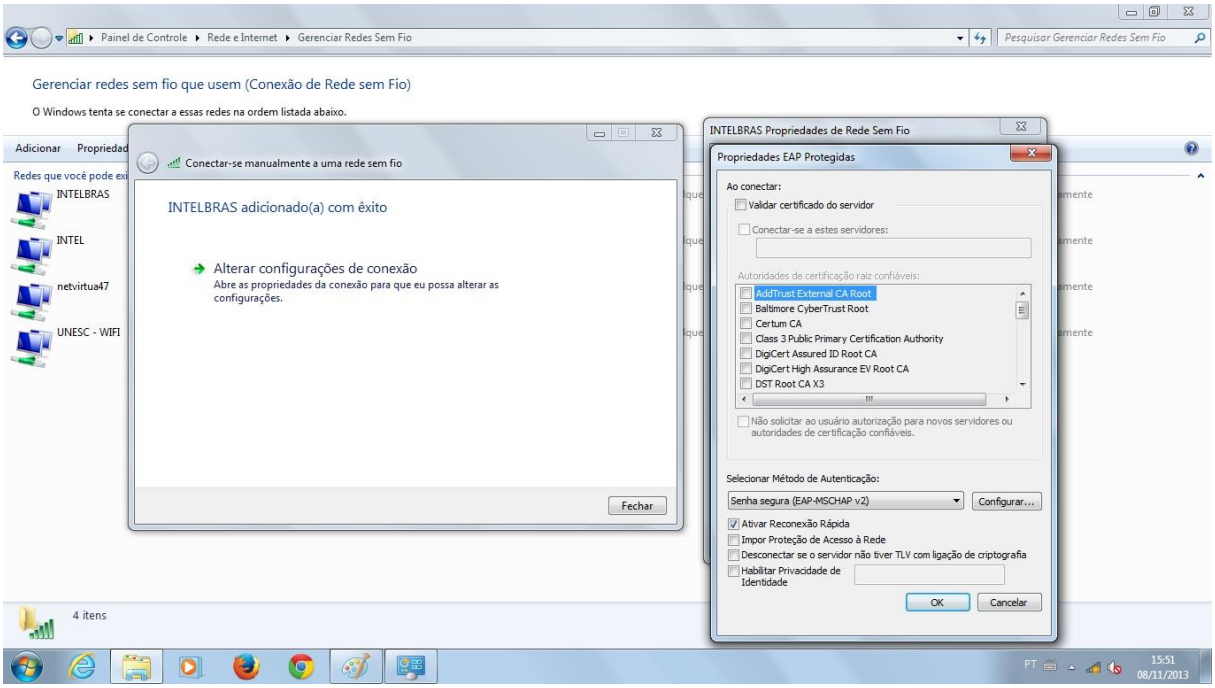


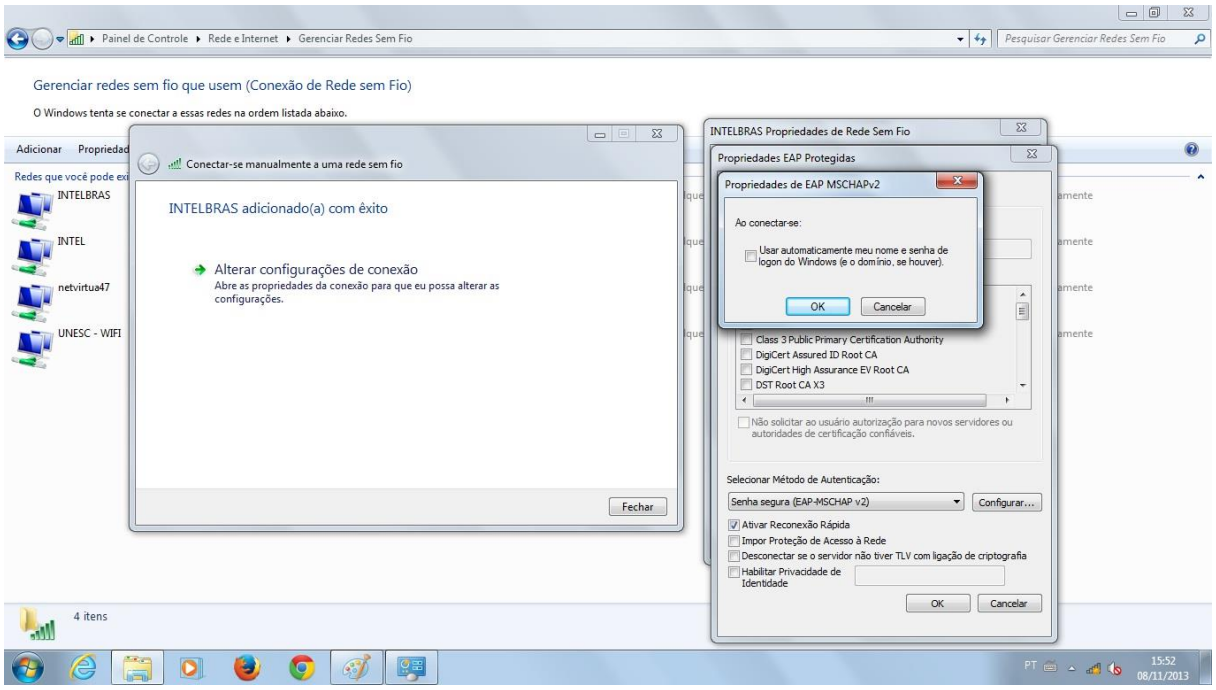
Na sequência, colocamos as informações conforme configurado no roteador.

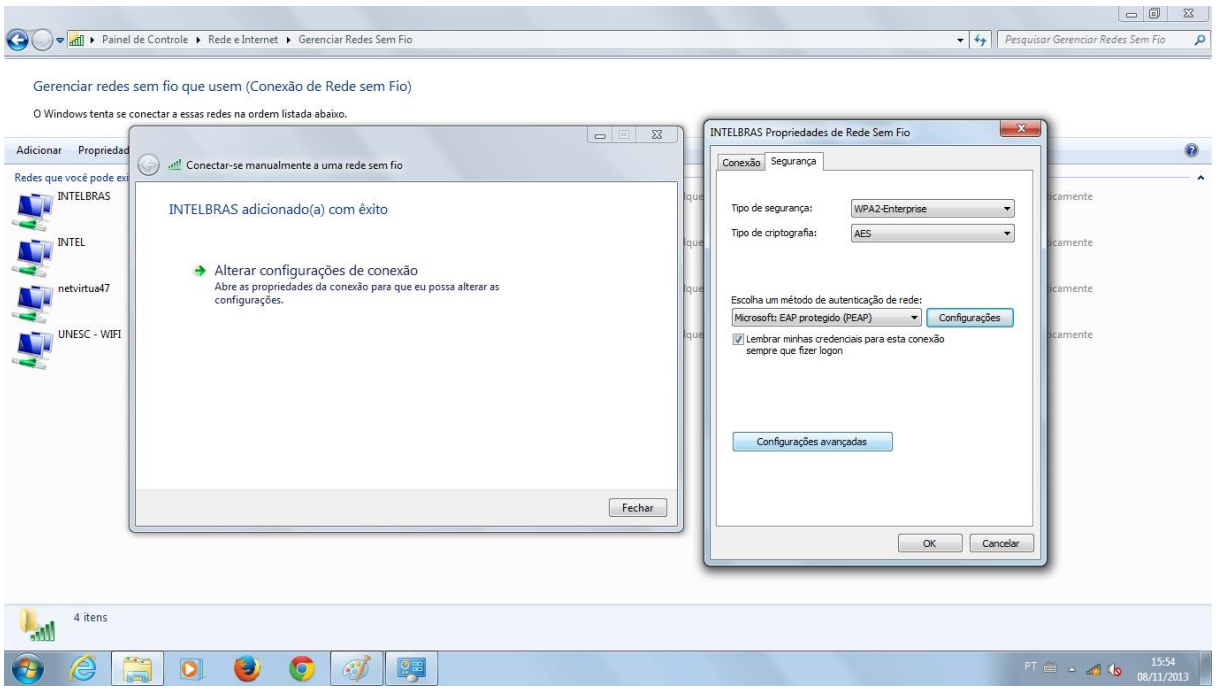


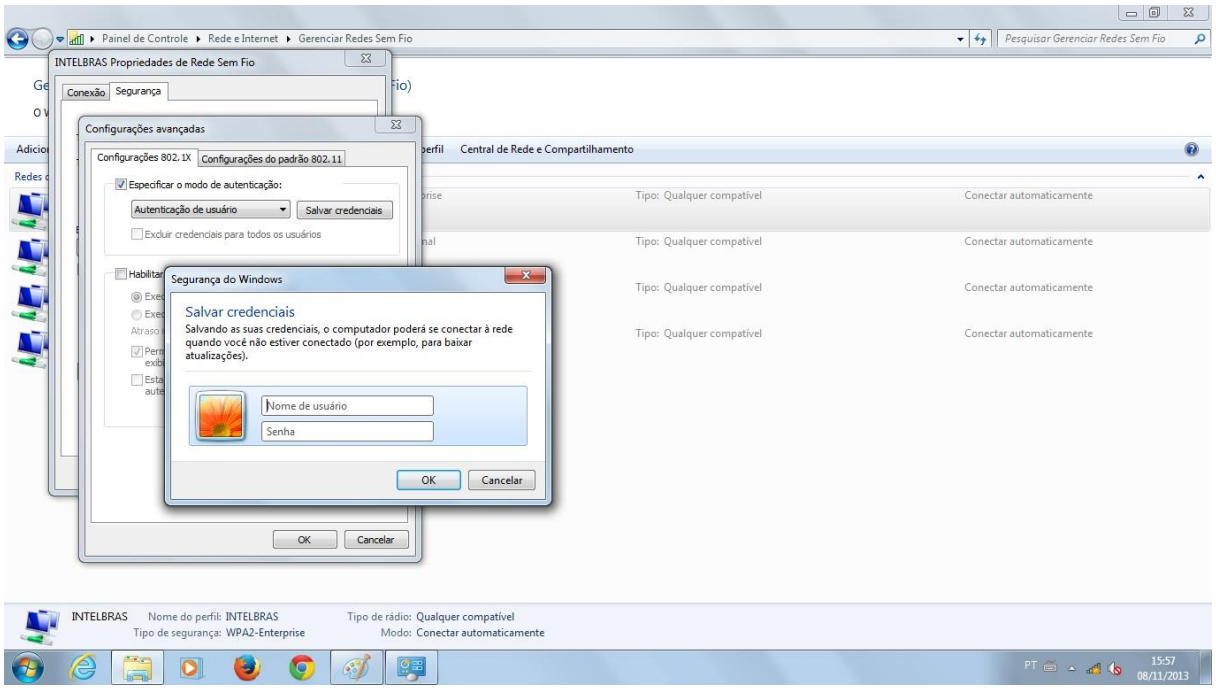


Se a opção “Validar Certificado do Servidor” estiver marcada, devemos desmarcar. No depois, desmarcamos também a opção “Usar automaticamente meu nome e senha de *logon* do *Windows* (e o domínio, se houver) ”. Confirmamos esta etapa e voltamos para a tela “Propriedades EAP protegidas” e confirmamos novamente.




Painel de Controle ▸ Rede e Internet ▸ Gerenciar Redes Sem Fio
Pesquisar Gerenciar Redes Sem Fio
Gerenciar redes sem fio que usem (Conexão de Rede sem Fio)
O Windows tenta se conectar a essas redes na ordem listada abaixo.
Adicionar
Redes que você pode ex
INTELBRAS
INTEL
netvirtua47
UNESC - WIFI
Conectar-se manualmente a uma rede sem fio
INTELBRAS adicionado(a) com êxito
Alterar configurações de conexão
Abre as propriedades da conexão para que eu possa alterar as configurações.
Fechar
INTELBRAS Propriedades de Rede Sem Fio
Propriedades EAP Protegidas
Propriedades de EAP MSCHAPv2
Ao conectar-se:
Usar automaticamente meu nome e senha de logon do Windows (e o domínio, se houver).
OK
Cancelar
Class 3 Public Primary Certification Authority
DigiCert Assured ID Root CA
DigiCert High Assurance EV Root CA
DST Root CA X3
Não solicitar ao usuário autorização para novos servidores ou autoridades de certificação confiáveis.
Selecionar Método de Autenticação:
Senha segura (EAP-MSCHAP v2)
Configurar...
Ativar Reconexão Rápida
Impor Proteção de Acesso à Rede
Desconectar se o servidor não tiver TLV com ligação de criptografia
Habilitar Privacidade de Identidade
OK
Cancelar
4 itens
PT
15:52
08/11/2013


Painel de Controle ▸ Rede e Internet ▸ Gerenciar Redes Sem Fio
Pesquisar Gerenciar Redes Sem Fio
Gerenciar redes sem fio que usem (Conexão de Rede sem Fio)
O Windows tenta se conectar a essas redes na ordem listada abaixo.
Adicionar
Redes que você pode ex
INTELBRAS
INTEL
netvirtua47
UNESC - WIFI
Conectar-se manualmente a uma rede sem fio
INTELBRAS adicionado(a) com êxito
Alterar configurações de conexão
Abre as propriedades da conexão para que eu possa alterar as configurações.
Fechar
INTELBRAS Propriedades de Rede Sem Fio
Conexão
Segurança
Tipo de segurança:
WPA2-Enterprise
Tipo de criptografia:
AES
Escolha um método de autenticação de rede:
Microsoft: EAP protegido (PEAP)
Configurações
Lembrar minhas credenciais para esta conexão sempre que fizer logon
Configurações avançadas
OK
Cancelar
4 itens
PT
15:54
08/11/2013


Painel de Controle ▸ Rede e Internet ▸ Gerenciar Redes Sem Fio
Pesquisar Gerenciar Redes Sem Fio
INTELBRAS Propriedades de Rede Sem Fio
Conexão
Segurança
Configurações avançadas
Configurações 802.1X
Configurações do padrão 802.11
Especificar o modo de autenticação:
Autenticação de usuário
Salvar credenciais
Excluir credenciais para todos os usuários
Segurança do Windows
Salvar credenciais
Salvando as suas credenciais, o computador poderá se conectar à rede quando você não estiver conectado (por exemplo, para baixar atualizações).
Nome de usuário
Senha
OK
Cancelar
Central de Rede e Compartilhamento
Tipo: Qualquer compatível
Conectar automaticamente
INTELBRAS
Nome do perfil: INTELBRAS
Tipo de segurança: WPA2-Enterprise
Tipo de rádio: Qualquer compatível
Modo: Conectar automaticamente
PT
15:57
08/11/2013


Lixeira
Spiceworks Desktop
WiFi Protector
AVG 2014
Contato
inSSIDer
Jogar
AIDA64 Extreme Edition
GeForce Experience
Motivação
Pastas do Network Magic
Xirrus Wi-Fi Inspector
NetTools
CPUID CPU-Z
02-SegWireless
Ares
Network Magic
Mozilla Firefox
Google Chrome
Vinicius_Segura...
DVD Shrink 3.2
CCleaner
NetBeans IDE 7.2.1
Revo Uninstaller
TCC
EasyBCD%202.0.2
inSSIDer 3
HD Tune Pro
SlimDrivers
µTorrent
EasyBCD 2.0
EaseUS Partition Master 9.2.1 H...
My Shared Folder
WirelessMon
TCC_2013_02
Conectado no momento a:
INTELBRAS
Sem acesso à Internet
Conexão de Rede sem Fio
INTELBRAS
Conectado
UNESC - WIFI
HP78E8DA
Centro_de_Copias
Abrir a Central de Rede e Compartilhamento
PT
15:45
08/11/2013

APENDICE B - ASPECTOS DE GERÊNCIA DE REDES SEM FIO, FOCO NO MONITORAMENTO DE UMA WLAN

Aspectos de Gerência de Redes Sem Fio, foco no Monitoramento de uma WLAN

Ivan J. Pereira[1], Paulo J. Martins[2]

[1]Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC)
Av. Universitária, 1105 – Bairro Universitário – Criciúma – SC – Brasil

ivanjp@unesc.net, pjm@unesc.net

Abstract. *Today many people who use the wireless network, as a matter of mobility and practicality, when configuring your devices end up not taking into account aspects of management that can make the most reliable and secure network. The objective is to describe and document the aspects of management of a wireless network, their monitoring and the use of tools in order to assist network administrators. The management allows control over network resources, as well as the identification and prevention of problems, better service and cost control. It involves five areas: performance, security, fault, configuration and accounting. It conducted a planning with FreeRADIUS for user authentication. The software used to monitor wireless network assisted in the observation and configuration of the same. Demonstrated information was SSID, channel used, signal quality, 802.11 used, MAC address of the device, maximum rate of data transfer. With the results, one can understand how important it is to survey the network as a whole, helping to avoid problems with settings and security.*

Resumo. *Hoje muitas pessoas que usam a rede sem fio, por questão de mobilidade e praticidade, na hora de configurar os seus dispositivos acabam não levando em conta aspectos de gerência que podem tornar a rede mais confiável e segura. O objetivo do trabalho é descrever e documentar os aspectos de gerência de uma rede sem fio, o seu monitoramento e a utilização de ferramentas, de forma a auxiliar os administradores de redes. O gerenciamento permite controle sobre os recursos da rede, assim como a identificação e prevenção de problemas, serviços melhores e controle de custo. Envolve cinco pontos: desempenho, segurança, falhas, configuração e contabilização. Foi realizado um planejamento com o FreeRADIUS para autenticação de usuários. Os softwares utilizados para monitorar a rede sem fio auxiliaram na observação e configuração da mesma. Informações demonstradas foram SSID, canal utilizado, qualidade do sinal, padrão 802.11 utilizado, endereço MAC do dispositivo, taxa máxima de transferência de dados. Com os resultados, pode-se compreender o quanto é importante fazer um levantamento da rede como um todo, auxiliando para evitar problemas com configurações e segurança.*

1. Introdução

O aumento significativo das informações, o grande interesse das pessoas em se comunicar e a mobilidade dos dispositivos vêm aumentando o uso das redes sem fio. Nesse contexto, alguns usuários vêm implantando este tipo de rede, desconsiderando as melhores práticas

recomendadas para o uso desta tecnologia, no que tange o seu gerenciamento. Baseado nisso, percebe-se esta necessidade, de forma a tentar minimizar certos problemas, tais como, segurança, conectividade, ruídos, interferências e uso errado da rede. São adequadas a situações de mobilidade, flexíveis e de fácil instalação. Os dispositivos sem fio permitem criar, ampliar e interligar redes locais em ambientes internos ou externos, sem a necessidade da utilização de fios.

O crescimento das redes tem tornado a gerência de redes cada vez mais complexa; por menor ou mais simples que seja uma rede, esta necessita ser gerenciada a fim de garantir aos usuários a disponibilidade de serviços. O gerenciamento permite controle sobre os recursos da rede, assim como a identificação e prevenção de problemas, serviços melhores e controle de custo. Ele envolve cinco pontos: desempenho, segurança, falhas, configuração e contabilização (KUROSE, 2006).

A utilização de softwares de gerência de redes sem fio procura minimizar e auxiliar a descoberta de problemas e, de certa forma, antecipar um mecanismo de tratamento das situações que podem prejudicar o bom funcionamento da rede. Com o objetivo de descrever e utilizar ferramentas para gerenciamento e monitoramento de redes sem fio.

2. Redes Sem Fio

Com a *Internet* diminuindo as fronteiras entre as pessoas em ambientes de trabalho, escolas e residências, tanto nas cidades quanto na zona rural, estão fazendo uso dessa tecnologia. Este cenário mostra a evolução das tecnologias a fim de serem utilizadas na comunicação das pessoas, nos mais remotos lugares. Nakamura e Geus (2007) salientam que o investimento aplicado cada vez mais, de forma a obter uma comunicação de boa qualidade e sem dificuldade no uso, com comodidade, sendo eficaz, resultou no uso notável da tecnologia de rede sem fio.

Redes locais sem fio (WLAN): os equipamentos ligados à rede necessitam ter um *modem* e uma antena de rádio para que possam se comunicar entre si diretamente ou por meio de concentradores de acesso, chamados *de Access Points* (AP). Essas redes estão sendo cada vez mais usadas em pequenas empresas e residências, onde a instalação com cabos é muito demorada e pode apresentar problemas na infraestrutura (TANENBAUM; WETHERALL, 2011). Uma rede BSS ou Infraestrutura atua quando as estações são conectadas entre si ou com outras redes, usando um ponto de acesso (SANCHES, 2005).

3. Gerência de Redes

Toda rede de computadores, por menor e mais simples que seja, precisa ser gerenciada para garantir aos seus usuários a disponibilidade dos serviços, a um nível de desempenho aceitável. À medida que a rede cresce, aumenta a complexidade de seu gerenciamento, forçando a adoção de ferramentas automatizadas para a sua monitoração e controle. A gerência de rede, englobam-se monitoramento e controle da rede com o uso de *softwares*, *hardwares* e conhecimentos de profissionais especializados. Com isso, obtém as informações da rede, diagnostica os possíveis problemas e encaminha as soluções; a forma errada de colocar esses elementos em um projeto, compromete-se o ambiente de rede como um todo (DANTAS, 2002).

Pensando de forma estruturada, a ISO dividiu o gerenciamento de redes em cinco áreas funcionais: falhas, configuração, contabilização, desempenho e segurança.

3.2.Modelo FCAPS

Com o desenvolvimento do modelo OSI pela ISO, foram definidos os conceitos de áreas funcionais, modelos de informação para representar recursos de rede e protocolos para transferência de informações sobre gerências de rede. Ele serve de base para todos os demais, por definir as áreas funcionais da gerência de redes, que são: gerência de falhas, configuração, contabilidade, desempenho e segurança (DANTAS, 2002).

3.2.1.Gerenciamento de falhas

Em uma rede funcionando, o administrador tem que cuidar para que o sistema todo, bem como cada componente individual, funcione normalmente. Quando ocorre uma falha, é importante agir rapidamente, a fim de determinar onde está o problema; observando o ocorrido, isola-se o resto da rede para certificar que a mesma continue funcionando normalmente sem interferências. Então, executa-se uma análise na configuração para minimizar o impacto feito pela falha e repara-se ou substitui-se o componente, fazendo a rede voltar ao seu estado normal (DANTAS, 2002).

Muito importante é o conceito de falha. Ela não é o mesmo que erro. Uma falha é uma condição anormal que precisa ser gerenciada, já um erro é um evento único. A falha ocorre por não operar normalmente ou por exagerada quantidade de erros (STALLINGS, 2005).

3.2.2.Gerenciamento de contabilidade

Em redes corporativas, o uso dos serviços na rede é cobrado, por assim dizer. São procedimentos contábeis internos, mas, no lugar do pagamento com dinheiro real, pode ser o uso de papel em uma impressora com cota, durante um mês. O administrador da rede pode monitorar o uso dos recursos de rede de cada usuário ou um grupo. Uma ou mais pessoas podem usar de mais a rede, sendo capaz de sobrecarregar a rede, prejudicando os demais. O administrador pode auxiliar em procedimentos que melhorem o desempenho, com melhores condições de planejar o crescimento da rede já que se conhecem as atividades dos usuários (DANTAS, 2002).

3.2.3.Gerenciamento de configuração

Com um conjunto de operações necessárias para a inicialização, término, alteração e armazenamento da configuração dos equipamentos da rede, a gerência pode alterar a configuração dos equipamentos, documentação sobre a configuração dos equipamentos, manutenção e atualização periódica, coletando dados da rede, bem como inicializar e alterar a configuração de equipamentos. Ela ainda possui salvo uma cópia de configuração da rede. Funções importantes que devem ser observadas: documentação das configurações realizadas; ter mais de uma pessoa capaz de realizar o mesmo trabalho; configurações erradas podem gerar falhas. (STALLINGS, 2005).

3.2.4.Gerenciamento de desempenho

Os componentes de uma rede que se comunica entre si, como um roteador com um computador, precisam oferecer um desempenho aceitável para ter uma comunicação sem problemas (LOPES, 2003).

Este gerenciamento abrange duas grandes categorias funcionais: monitoramento e controle. Monitoramento é a função de observar as atividades da rede. A função de controle possibilita que se façam ajustes para melhorar o desempenho da rede. Algumas das questões envolvendo desempenho, com as quais o administrador da rede deve se preocupar são: qual é a capacidade da rede, quando se fala em desempenho? O tráfego atual é excessivo? A vazão

tem diminuído para níveis inaceitáveis? Existe algum gargalo? Por mensurar os recursos e associar métricas apropriadas a eles, o administrador da rede pode analisar os resultados e estabelecer os níveis de desempenho aceitáveis, estando apto a detectar mudanças no comportamento da rede e tomar providências caso isso seja necessário (DANTAS, 2002).

3.2.5.Gerenciamento de segurança

Com foco em proteção das informações e controle de acesso por meio de *softwares*, senhas e outras informações de autorização devem ser mantidas e distribuídas, tem também que monitorar e controlar o acesso aos computadores da rede, coletando e examinando os registros de auditoria e de log, podendo desabilitar ou habilitar esses registros (STALLINGS, 2005).

4. GERENCIA DE REDE SEM FIO, MONITORAMENTO EM WLAN

Esta pesquisa se restringe a uma rede infraestruturada, descrevendo alguns *softwares* de gerenciamento, dos quais apenas o *FreeRadius*, na área de segurança, foi aplicado, para descrever os aspectos de importância da segurança e as políticas. Esta pesquisa é focada fortemente no aspecto de monitoramento. A ideia era a aplicação em redes domésticas e corporativa, mas, pela dificuldade de conseguir um ambiente coorporativo, a mesma ateve-se em aplicar em ambiente residencial e simular o modelo coorporativo.

4.1.Metodologia

Foram realizados alguns testes com vários *softwares*, analisando a potência do sinal, diante da localização do mesmo, dentro do ambiente, no estilo *Site Survey indoor,* com o seguinte cenário: foi instalado o roteador no centro de uma determinada residência, no piso superior a 4 metros de altura. Foram realizadas medições para encontrar a parte central, medindo-se o perímetro do local (com 15 metros de frente e 24,50 metros de área lateral), fixando o *Access Point* com a antena para baixo na horizontal, alterando a senha padrão de acesso ao mesmo e a segurança usando o protocolo WPA2, utilizando senha com números e letras, potência do AP em alta, média e baixa para os testes.

Para ver o alcance do sinal, foram usados alguns *softwares* de monitoramento*,* sendo eles: *InSSIDer*, *WirelessMon*, *Xirrus Wi-Fi Inspector* e *WIFi Locator*, colocando o computador em 4 locais distintos, para obter a intensidade do sinal medidas em dBm para perceber a diminuição do mesmo. Esses testes foram repetidos por quatro vezes, por meio de um *Notebook Dell,* modelo 5420, com um core I5, 6 Gb de ram, Sistema *Microsoft Windows* 7 *Ultimate*.

Na tabela 1, com a potência em alta nos quatro cantos do local, observou-se que o acesso à rede era permitido, a qualidade do sinal ficou em média de 58%. Com esse valor, há o melhor aproveitamento da rede. Contudo, com a irradiação passando do perímetro desejado, é necessário aplicar aspectos de gerência para rede.

Tabela 1. Análise de potência de sinal e localização do Access Point, por meio de alguns softwares de monitoramento ALTA potência

Alta	Atrás Esquerda	Frente Esquerda	Frente Direita	Atrás Direita
inSSIDer	73-77 dBm	66-71 dBm	76-78 dBm	73-77 dBm
WirelessMon	74-77 dBm	66-69 dBm	77-79 dBm	71-74 dBm
Xirrus Wi-Fi Inspector	73-79 dBm	69-73 dBm	78-81 dBm	70-73 dBm
WIFi Locator	70-74 dBm	70-75 dBm	76-80 dBm	71-78 dBm

Com a análise da potência foram encontrados os resultados que com o *Access Point* centralizado e com a potência do sinal em Alta a uma melhor abrangência no perímetro, sendo que com a saída do sinal fora do quadrante. Há a necessidade de aprimorar a segurança, como alterações em parâmetros da rede na forma de assegurar a integridade dos dados.

4.2.1.Falha

Na parte de falhas, há como exemplo o acesso a um *site* ao qual ele não responde, que pode ser por falha no roteador, em que o mesmo pode estar desligado, não servindo acesso, também o *modem* pode se encontrar na mesma situação, não conseguindo navegar ou o acesso à rede teve uma queda por parte da operadora contratada. O administrador da rede deve ter um monitoramento constante na rede para mantê-la sempre acessível, verificando se as configurações foram alteradas e se os equipamentos estão atualizados e funcionando.

4.2.2.Desempenho

Um conjunto de fatores pode determinar o desempenho da rede, como a configuração do AP nos quesitos de alocação de um canal, tipo de segurança com a escolha de WEP, WPA ou WPA2, localização do AP em relação aos equipamentos que vão se conectar a ele. As principais barreiras que podem afetar a transmissão do sinal da rede sem fio são: antenas ou pontos de acesso baixos, onde eles têm que estar em uma superfície mais alta, com menos barreiras, possibilitando que o sinal chegue ao dispositivo receptor de forma mais fácil. Micro-ondas e telefones, por utilizar da frequência 2.4 Ghz, disputam o mesmo canal de frequência (FLICKENGER,2008).

4.2.3.Configuração

SSID identifica a rede, mas também pode ser usado de forma a identificar a rede que alguém mal-intencionado pode tentar acessar. Com isso, pode se fazer uma alteração para ocultar. Nas configurações do AP, onde se encontra o SSID, deve-se desmarcá-lo para ficar oculto e desmarca o *broadcast*, muda o nome da rede antes de autenticar o *notebook*, por exemplo, depois confirma a modificação no AP e a rede estará oculta. Com isso, quando alguém procurar a rede, não vai achar. Outra coisa que pode fazer é diminuir a potência do sinal em configurações no AP.

Outra forma de melhorar o acesso ao AP, restringindo apenas ao administrador da rede, é trocar o nome de usuário e senha padrão de fábrica, que normalmente não é feito pelo usuário comum. Com a troca de senha do dispositivo, evita-se um ataque em massa, que foi descoberto há pouco tempo, onde a maioria dos fabricantes tem como *login* e senha de acesso

o padrão admin, e os usuários não o trocam, com um ataque se modificava o DNS da rede responsável por traduzir os endereços IP de cada *site* em nome, fazendo com que o usuário seja direcionado para uma página falsa, tendo os seus dados roubados.

4.2.4.Contabilização

Para uma avaliação na questão de contabilização, há no AP, na parte *Wireless*> Estatísticas, mostra os clientes que estão utilizando a rede sem fio, com seus respectivos endereços MAC. Com essas informações, o administrador da rede pode verificar quantos usuários estão utilizando a rede e também acessando os clientes que estão utilizando toda a rede, em > DHCP > Lista de Clientes. Para análise de uso da rede contabilizando os usuários com um maior controle dos recursos utilizados.

4.2.5.Segurança

Para o tipo de segurança na autenticação com a escolha de WEP, WPA ou WPA2, hoje está sendo mais usado o WPA2, por maior dificuldade de uma pessoa descobrir a senha e acessar a rede (CARMONA, 2005). Para senhas seguras, não se deve usar dados pessoais, não anotar senhas, utilizar senhas com vários tipos de caracteres, contendo no mínimo oito caracteres, trocar no intervalo mínimo de três meses e sem usar sequencias do teclado. Utilizando de *RADIUS* para se autenticar, a rede é uma forma de dificultar ataques, sendo que, para entrar, precisa de usuário e senha, cada um cadastrado no servidor utilizado em Universidades e no setor corporativo.

A política de segurança de informação em um ambiente corporativo ou universitário relaciona normas, ferramentas, procedimentos e compromissos para ter o controle e conseguir a segurança das informações utilizadas nas organizações (NAKAMURA, 2007).

Na forma de dificultar que uma pessoa mal-intencionada tente invadir a rede de forma indevida e não autorizada, deve-se criar uma senha que seja fácil para decorar, mas difícil para se pensar, que seja segura, a fim de auxiliar nessa proposta, têm-se *softwares* e até *sites* que geram senhas, com responsabilidade ao administrador da rede na criação da senha e, assim, evitar só números, letras, sequência de caracteres

4.2.6. Utilizando FreeRadius

Foi utilizado o *FreeRADIUS* para gerencia de rede sem fio de contabilização e segurança no *Linux,* versão do *Ubuntu* 14.04.3, de forma centralizada, em um ambiente controlado, com supervisão no laboratório, onde o servidor fica em uma máquina que gerencia a autenticação de cada usuário. O cenário é composto por uma máquina com *Linux*, *access point* e *notebook* funcionando como clientes mostrado na figura 1.

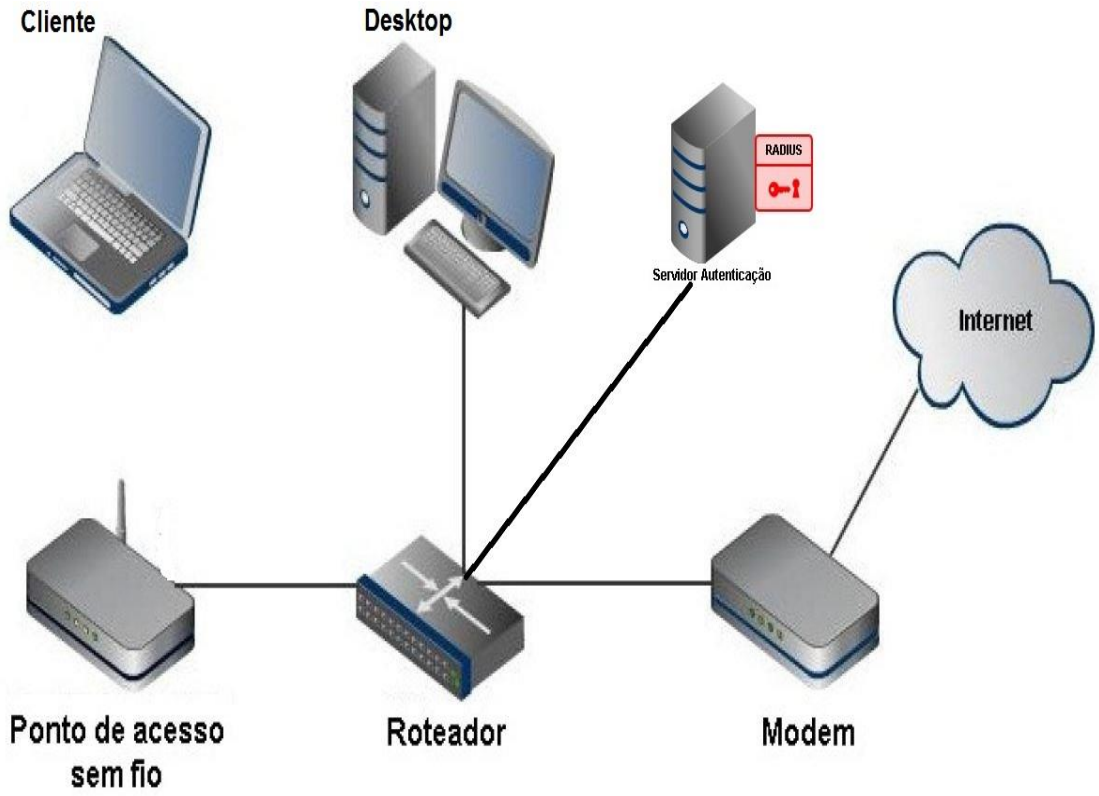


Figura 1. Topologia da rede

Como mostrado na figura 1 temos em detalhe: Internet para o acesso e navegação; modem ADSL para fazer a conexão com Internet; servidor autenticação: autentica os usuários que querem entrar na rede; switch que interliga o Modem com nó, no caso o "Ponto de acesso sem fio", onde irá disponibilizar o acesso à rede mundial de computadores; desktop como um computador físico que se conecta através de uma porta local à interface LAN do "*Roteador*" e notebook para testes de conexão e verificar o sinal se deslocando pela área de cobertura da rede.

Foi instalado e configurado os *FreeRADIUS*, *phpmyadmin*, *mysql server*, *apache* 2. Com essa instalação e configuração, há dois pontos importantes: que são o cadastro do AP, que pode ser mais de um, e o cadastro de cliente, que são todos administrados no *phpmyadmin*; importante salientar que foi usado um AP comum, e não um com configurações avançadas e com custo elevado.

4.3.Resultados Obtidos

Com os *softwares* apresentados de monitoramento de rede sem fio, bem como com a análise utilizando *softwares,* a rede tem que ser configurada nos aspectos de configuração, falha, contabilização, desempenho e segurança, a fim de ter uma rede operando de forma a não ter problemas futuros.

Em configuração, o administrador da rede, com o auxílio do manual para as configurações de seu *access point*, ajuda a diminuir problemas com os *softwares* de monitoramento, mostrando os APs mais próximos, com informações importantes, como SSID, canal utilizado, qualidade do sinal, padrão 802.11 utilizado, endereço MAC do

dispositivo, taxa máxima de transferência de dados. Altera-se o que for necessário para ter a rede funcionando, a fim de atender a todos os clientes da rede, de forma a ter desempenho e segurança.

Para conter as falhas, a prevenção é uma medida que ajuda, pois há falhas em nível de *softwares* e *hardware*, analisando os *logs* do roteador e verificando se todos os dispositivos que compõem a rede estão funcionando normalmente.

Disponível de 14 canais no modo de 2,4Ghz e com apenas três canais que não se sobrepõem, analisando *Site Survey indoor*, com programas de monitoramento para diminuir a interferência por utilização de canais, há duas soluções que são: escolher entre os três de forma a utilizar o mesmo, usando os canais no salto de três em três, a fim de melhorar o desempenho e com o uso de criptografia WPA2 para senhas de rede.

Na contabilização, há por parte do administrador da rede uma lista de clientes, que deve ser inspecionada periodicamente para controle de usuários autorizados.

No aspecto de segurança, há a utilização de autenticação por meio de *RADIUS*, que se mostrou uma alternativa viável para controle de usuários de uma rede sem fio, servindo para um modelo corporativo e para universidades de maneira a ter mais controle sobre quem está utilizando, sendo que, com a adoção deste modelo, os usuários não vão disponibilizar seu *login* e senha, sabendo que tudo que for feito será de sua responsabilidade.

Nos *softwares* de monitoramento, há as informações de SSID com o nome da rede; MAC com o endereço único de cada dispositivo, canal de 1 a 14, de 36 ou de 100, a 161; potência do sinal de -35 a -110 dBm; padrão de rede com 802.1ª/b/g/n/AC/entre outros; tipo de segurança, sendo aberta, WEP, WPA, WPA2 e entre outros; GPS com localização, dependendo do dispositivo utilizado; modo de operação, sendo infraestruturada ou Ad-hoc; frequência utilizada, sendo 2.4 Ghz e 5 Ghz; outras informações peculiares a dos *softwares* mostrados na tabela 2.

Tabela 2. Funcionalidade dos softwares de monitoramento

Funcionalidades/ softwares	**inSSIDer**	**WirelessMon**	**Xirrus Wi-Fi Inspector**	**WIFi Locator**
Visualização do SSID	X	X	X	X
MAC	X	X	X	X
Canal Utilizado	X	X	X	X
Potência do Sinal	X	X	X	X
Padrão de Rede	X	X	X	X
Tipo de Segurança	X	X	X	
GPS	X	X	X	X
Frequência	X	X	X	X
Sobreposição de Canais	X	X		
Modo de operação: infraestrutura ou Ad-hoc	X	X	X	X

Usando estes programas se pode ter uma noção de como a rede está em relação aos outros dispositivos e que o *InSSIDer* e o *WirelessMon* se destacam, com um gráfico que mostra a sobreposição dos canais em relação aos demais equipamentos.

5. Conclusão

Este trabalho abordou aspectos de gerência e monitoramento em uma WLAN, local para implantar, verificando aspectos de desempenho, contabilização, configuração, falhas e segurança. Entender e aplicar os conceitos de gerência de redes sem fio foi atingido com sucesso, com cada uma das partes de gerência detalhada de forma clara e usadas na parte de monitoramento com seus aspectos e, na de gerência, apenas em contabilização e segurança.

Estudar e aplicar *softwares* de monitoramento de redes sem fio foi concluído de forma que, com o uso de mais de um programa, pode-se ter uma melhor compressão de como a rede está em relação às outras, de forma a analisar e tomar as devidas alterações no equipamento que transmite o sinal sem fio pelo perímetro.

Compreender aspectos de segurança a serem avaliados na implantação de uma gerência de redes mostrou que se deve preocupar com a segurança das informações que trafegam na rede, com configurações e *softwares* que auxiliam na análise da rede, e as residências próximas para dificultar os ataques de pessoas que tentam se conectar de forma não autorizada.

Demonstrar o estudo de caso de ferramentas de monitoramento de uma rede sem fio que a configuração certa diminui os ataques, tornando mais difícil a entrada de intrusos na rede, evitando, assim, interferências com outros equipamentos, comparando as informações obtidas dos outros dispositivos com o da pesquisa.

Propor uma gerência de segurança centralizada de redes foi muito bom, bem como trabalhar com o *FreeRADIUS* foi bom, pois mostrou que autenticação dos usuários facilita o controle e monitoramento da rede, ainda mais se for implantada em uma empresa e em uma universidade, que têm suas políticas de segurança como prioridade.

6. Referencias

CARMONA, T. Segredos da espionagem digital. São Paulo: Universo dos Livros ,2005.

DANTAS,M.Tecnologias de redes de comunicação e computadores. Rio de Janeiro: Axcel Books, 2002.

FLICKENGER, Rob. Redes sem fio no Mundo em Desenvolvimento: Um guia prático para o planejamento e a construção de uma infra-estrutura de telecomunicações. 2. ed. Washington: Hacker Friendly Llc, 2008. 397 p.

KUROSE, J. F.; ROSS, K. W. Redes de computadores e a internet: uma abordagem top-down. 3. ed. São Paulo: Pearson Addison Wesley, 2006.

LOPES, R. V. et al. Melhores práticas para gerência de redes de computadores. Rio de Janeiro: Campus, 2003.

NAKAMURA, E. T.; GEUS, P. L. Segurança de redes: em ambientes cooperativos. São Paulo: Novatec, 2007.

SANCHES, Carlos Alberto. Projetando redes WLAN: conceitos e práticas. Rio de Janeiro: Érica, 2005.

STALLINGS, W. Redes e sistemas de comunicação de dados. Rio de Janeiro: Elsevier, 2005.

TANENBAUM, R. S.; WETHERALL, T. U. Computer networks. 5. ed. Boston: Pearson, 2011.