UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

FERRAZ AUGUSTO DIOGO MANUEL

PROJETO, INFRAESTRUTURA DE UMA REDE SEM FIO MESH, UTILIZANDO SOFTWARES LIVRES, E ASPECTOS DE SEGURANÇA

CRICIÚMA, DEZEMBRO DE 2010

FERRAZ AUGUSTO DIOGO MANUEL

PROJETO, INFRAESTRUTURA DE UMA REDE SEM FIO MESH, UTILIZANDO SOFTWARES LIVRES, E ASPECTOS DE SEGURANÇA

Trabalho de Conclusão do Curso apresentado para obtenção do Grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense.

Orientador: Prof. MSc. Paulo João Martins

CRICIÚMA, DEZEMBRO DE 2010

FERRAZ AUGUSTO DIOGO MANUEL

PROJETO, INFRAESTRUTURA DE UMA REDE SEM FIO MESH, UTILIZANDO SOFTWARES LIVRES, E ASPECTOS DE SEGURANÇA

Submetido ao corpo docente do Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense como um dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

Profa. MSc. Ana Claudia Garcia Barbosa
Coordenadora do Curso de Ciência da Computação

Banca Examinadora:

Prof. MSc. Paulo João Martins (UNESC)
Orientador

Prof. MSc. Rogério Antônio Casagrande (UNESC)

Prof. Esp. Sérgio Coral (UNESC)

A Deus por tudo quanto tem feito por mim, e a minha família por estarem comigo durante todo este processo, me apoiando e incentivando.

AGRADECIMENTOS

Agradeço a Deus, por ser o salvador da minha vida, minha fonte de força e inspiração para todas as realizações na minha vida e por me dar sabedoria, porque sei que tudo quanto existe foi feito por Ele e para Ele.

Aos meus pais, André August Manuel e Eva Diogo Adão, que sempre me apoiaram e em muitos momentos foram decisivos para a minha permanência na busca pela conclusão do curso. A Rosária dos Santos de Sousa Manuel que tem sido uma pessoa muito especial na minha vida, pelo incentivo, carinho e compreensão que teve ao longo desse caminho.

Por fim e não menos importante ao meu orientador e professor Paulo Martins que muito me ajudou na concretização deste trabalho.

RESUMO

O objetivo desde trabalho é propor e implementar uma rede *mesh* sem fio local, como estudo de caso, dentro das facilidades Universitárias, visando melhorar o acesso a rede aos estudantes e não só, e garantir conexão em locais onde não é possível a conexão por cabos. Por meio de roteadores wireless e pelo uso de radio frequências, ha compartilhamento de recursos e dados, pela interligação dos nós. Além do equipamento, o protocolo de roteamento pró-ativo OLSR e o firmware DD-WRT que suporta o mesmo protocolo, foram usados para a construção e segurança da rede, sendo que alguns softwares livres foram usados para testar o funcionamento da rede. Conclui-se que é possível a criação da rede proposta, a tecnologia funciona e soluciona o problema de acumulo de cabos de redes, diminui os custos de implantação e manutenção e um passo para criação de cidades digitais e inclusão digital.

Palavras-chaves: Redes de Computadores, Redes Sem Fio, Wireless, Redes Mesh, Protocolo OLSR (Optimized Link State Routing), Segurança de Redes.

ABSTRACT

The objective of this work is to propose and implement a local wireless mesh network, the study will be done within the University facilities, to improve network access to students and beyond, and to guarantee connection in places where it is not possible to connect by cables. Through wireless routers and the use of radio frequencies, the nodes will interconnect and share resources and data. Besides the equipment, the proactive routing protocol OLSR and the DD-WRT firmware that supports OLSR that was used for building and securing the network, and free software was used to test the network. Concluding it is possible to create the proposed network, as we see the technology works, and solves the problem of accumulation of cable networks, reduces deployment and maintenance costs and it is a step towards the creation of digital cities and digital inclusion.

Key-words: Computer Networking, Wireless, Mesh Networking, OLSR (Optimized Link State Routing) Protocol, Network Security.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS E ABREVIATURAS

AES	Advanced Encryption System
AM	Modulação por Amplitude
AP	Access Point
ASK	Amplitude Shift Keying
BSD	Berkeley Software Distribution
CDMA	Code Division Multiple Access
DHCP	Dynamic Host Configuration Protocol
DSR	Dynamic Source Routing
DSSS	Direct Sequence Spread Spectrum
ESS	Extended Service Set
ETX	Expected Transmission Count
FDMA	Frequency Division Multiple Access
FHSS	Frequency Hopping Spread Spectrum
FM	Modulação por Frequência
FSK	Frequency Shift Keying
GPL	General Public License
HNA	Host and Network Association
HSLS	Hazy Sighted Link State Routing Protocol
IANA	Internet Assigned Numbers Authority
IEEE	Institute of Electrical and Electronics Engineers, Inc
IETF	Internet Engineering Task Force
ISM	Industrial, Scientific and Medical

ISO	International Organization For Standardization
L2TP	Layer 2 Tunneling Protocol
MANET	Mobile Ad hoc NETwork
MIC	Message Integrity Code
MID	Multiple interface declaration
MIT	Massachusetts Institute of Technology
MNSG	Mesh Networking Study Group
MPR	Multi Point Relays
MPRs	Multipoint Relays
NAT	Network Address Translation
OLSR	Optimized Link State Routing
OLSR-ML	Optimized Link State Routing – Minimum Loss
P2P	Peer-to-Peer
PAN	Personal Area Network
PM	Modulação por Fase
PPTP	Point-to-Point Tunneling Protocol
PSK	Phase Shift Keying
RADIUS	Remote Access Dial In User Service
RFC	Request for Comment
SPI	Stateful Packet Inspection
SSID	Service Set Identifier
TDMA	Time Division Multiple Access
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol

UDP	User Datagram Protocol
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VPN	Virtual Private Network
WAP	Wired Protected Access
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
Wi-Max	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMN	Wireless Mesh Networks

SUMÁRIO

1 **INTRODUÇÃO**

O desenvolvimento da tecnologia da informação, no que se refere a redes de computadores proporcionou inúmeras melhorias às empresas, instituições e a usuários, uma maior capacidade de comunicação e transferência de dados, voz e imagem, tendo como consequência o surgimento de vários tipos de redes, com o objetivo de atender as mais diversas necessidades impostas pelo mercado.

A conexão de dispositivos por meio de transmissão como radiodifusão, infravermelho, satélites e outros sem a utilização de cabos sejam eles telefônicos, coaxiais ou ópticos chamam-se redes sem fio.

Apesar de ainda pouco difundida, a tecnologia de redes m*esh*, também conhecida como redes em malha, vem sendo apresentada como uma das possíveis soluções de comunicação sem fio. A tecnologia teve origem no *Defense Advanced Research Projects Agency*, centro de desenvolvimento de tecnologia militar dos Estados Unidos com o objetivo de buscar uma rede que permitisse uma comunicação fim-a-fim, sem a necessidade de comunicação com um nó central, os protocolos de roteamentos das redes *mesh* conseguem se conectar entre eles, formando uma teia dinâmica.

O termo “topologia *mesh*” refere-se à organização de redes, que oferece múltiplos caminhos entre dois pontos quaisquer. No caso específico das redes sem fio e da tecnologia *Wireless Fidelity* (*Wi-Fi*), o termo refere-se a um tipo de estrutura no qual cada nó da rede é potencialmente um roteador. Aplicada as redes sem fio, essa topologia traz a vantagem de necessitar apenas de enlaces de curta distância entre os nós, e de oferecer muitos caminhos redundantes entre dois pontos quaisquer da rede (BICKET et al, 2005).

O desenvolvimento atual adere a algumas especificações, como a 802.11 e 802.16, apresentam diversos aspectos particulares e patenteados pelas empresas desenvolvedoras. Existe atualmente um esforço, dentro do *Institute of Electrical and Electronics Engineers, Inc* (IEEE), para a incorporação de especificações da tecnologia nos diversos padrões. Para isto foi criado, em Janeiro de 2004, um grupo de estudos, segundo Bicket (2005) os grupos de trabalho 802.11 e o 802.16 do IEEE, iniciaram uma tarefa prevista para ser concluída ao longo dos próximos anos, com o objetivo do desenvolvimento para promover a padronização da mesma.

Existem várias propostas de algoritmos de roteamento para redes *mesh* dinâmicas, tanto ao nível acadêmico, quanto em equipamentos comerciais destinados especificamente à construção de redes sem fio.

Atualmente, tecnologias como pares de fios telefônicos, fibra ótica e redes de cabo coaxial são soluções correntes para construção de redes de acesso para *backbones* metropolitanos. Todavia, sua utilização é muitas vezes proibitiva para suprir o acesso às zonas metropolitanas de menor poder aquisitivo, ou em zonas de pouca densidade demográfica, pois essas tecnologias implicam um custo de implantação e manutenção muito altos, que só se justificam para uma demanda elevada. Essa é uma das motivações para a pesquisa de tecnologias alternativas de baixo custo que tenham potencial para atender esse tipo de demanda relacionada especialmente à inclusão digital tornando-se baratas e eficientes.

A proposta *Roofnet* do *Massachusetts Institute of Technology* (2005), por exemplo, define um tipo de rede no qual o próprio equipamento de acesso dos usuários é utilizado como roteador para os demais usuários da rede. Isto é, o equipamento de

cada usuário conecta-se aos equipamentos dos usuários próximos, sucessivamente, até atingir um ou mais pontos de escoamento para Internet.

As redes sem fio em geral são inseguras, segundo Kurose e Ross (2006), a definição de segurança concentrou-se primordialmente em proteger a comunicação e os recursos de rede, mas na prática a segurança de rede envolve não apenas a proteção, mas também a detenção de falhas em comunicações seguras e ataques a infraestruturas e a reação a esses ataques, então tem de haver um ciclo continuo de proteção, detenção e reação. Por isso, existe a necessidade de tratar das questões pertinentes a segurança, na implantação de um modelo de rede deste tipo.

Pode-se utilizar Software livre que é um programa de código aberto, que pode ter seu código fonte alterado por qualquer usuário, não existindo licença para distribuição e com isso nenhum custo de compra é adicionado ao mesmo, tanto para implementação da rede como na segurança da mesma.

Sendo assim, esta pesquisa baseia-se na proposta de um projeto de estudo, implementação e a segurança de uma rede mesh utilizando software livre.

1.1 OBJETIVO GERAL

Nesta monografia é feito o estudo sobre redes *mesh*, e a utilização de software livre na implementação da mesma, por meio do protocolo baseado no modelo IEEE 802.11 existente. O desenvolvimento foi pensado para determinar o funcionamento de uma rede *mesh* sua escalabilidade no cenário, simulação, e proporcionando certo grau de segurança.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos estudados são:

a) entender e aplicar os conceitos de Redes de computadores;

b) analisar as tecnologias de redes sem fio;

c) compreender e aplicar o conceito de redes *mesh*;

d) entender protocolos de roteamento de redes *mesh*;

e) compreender e implementar alguns mecanismos de segurança.

1.3 JUSTIFICATIVA

Redes *mesh* são redes *Ad Hoc*, que de acordo com Przybysz e Luiz (2007), se organizam e se configuram automaticamente, onde os nós possuem uma localização fixa (mas não pré-determinada) e são dispostos em uma topologia em malha.

Os nós normalmente desempenham dois papéis diferentes: Clientes e Roteadores. Nós clientes são os pontos onde a informação é gerada, já os nós Roteadores são os responsáveis em fazer com que esta informação da rede seja transmitida até o *gateway*. São também considerados sistemas distribuídos *multi-hop*, onde os nós podem ser alcançados por mais de um caminho e cada nó coopera ativamente para a entrega da informação a seu destino final. Como diferentes enlaces de rádio podem ser usados para alcançar quaisquer nós, as *Wireless Mesh Networks* (WMN) são confiáveis, porque podem rerotear o tráfego de rede por outros caminhos se um nó específico for removido (AKYILDIZ, 2005).

Os nós ou roteadores utilizam a tecnologia 802.11 em modo *Ad Hoc*, formam uma teia dinâmica devido aos protocolos de roteamentos especiais que conseguem se conectar entre eles construindo com isso um *backbone* sem fio para a transmissão dados e obtendo um ganho enorme tanto na localização quanto nos custos de comunicação que em outras redes é muito alto ou onde não exista infraestrutura física de redes.

A diminuição dos custos de conexão possibilita implantação em zonas de difícil acesso, rurais, periferias e centros urbanos. Incentivando redes sociais, públicas e a inclusão digital de um modo geral.

Para Luiz e Przybysz (2005) são redes de baixo custo porque o compartilhamento de recursos faz com que o custo total da rede caia, viabilizando a criação de redes comunitárias.

O sucesso das redes *mesh* está diretamente relacionado à garantia da qualidade. O problema do excessivo número de saltos pode ser inaceitável se a configuração da rede e/ou protocolos não lidar de forma eficiente com a competição entre as transmissões dos nós, com encaminhamento de pacotes, com diferenciação de serviços. Nesta problemática diversos níveis podem colaborar, porém o padrão 802.16 traz, já na especificação do nível de enlace, alguns parâmetros que, se adequadamente ajustados, podem favorecer a qualidade de toda a malha.

Devido à capacidade de roteamento dinâmico aliado a existência de múltiplas rotas de acesso a um nó faz com que a rede consiga se recuperar de falhas como a perda de um enlace de comunicação. Uma das melhores características das redes *mesh* é que sua capacidade de roteamento cresce conforme os nós são adicionados, logo

o crescimento das redes, diferente da arquitetura tradicional não é um problema (LUIZ , PRZYBYSZ, 2005).

Um nó pode ser implementado de várias formas, um requisito importante refere-se à escolha do padrão de operação (por exemplo, IEEE 802.1a ou g), da quantidade de interfaces, da forma de utilização dos canais para evitar interferência entre nós adjacentes e do tipo de antena mais adequado, ele pode ser roteador comercial com software alterado (como a proposta do *Roofnet* do *Massachusetts Institute of Technology* – MIT), um computador executando Linux ou Windows ou até mesmo um roteador especificamente projetado para este fim.

Segundo Damalio (2008) o conceito traz consigo uma série de vantagens que tornam cada vez mais interessantes a sua implantação, como possuem a característica de serem autoconfiguráveis, a sua implantação se torna fácil, pois não são necessárias configurações complexas, nem necessidade de mudança caso algum nó venha a entrar na rede.

Não requer licenciamento, pois usa frequências abertas (Wi-Fi), e podem ser integrado com o sistema de TV digital como fonte de ensino e aprendizado, não sendo necessário conectar todos os pontos de acesso a uma rede cabeada.

A segurança de qualquer rede deve ser uma função de todo o projeto de redes, por isso é necessário garantir a integridade, a privacidade da comunicação, e a autenticação das entidades envolvidas, elas são importantes devido às vulnerabilidades, ao processo de comunicação e ao fato de que os mecanismos desenvolvidos para redes convencionais não serem convenientes para utilização em redes sem fio.

1.4 ESTRUTURA DO TRABALHO

O presente trabalho de conclusão de curso foi iniciado com um amplo levantamento bibliográfico das publicações que abordam a tecnologia de redes sem fio, redes *mesh*, protocolos de roteamento e segurança de rede em software livre, constituindo em os capítulos: Introdução; Redes de computadores; Redes *Mesh*, Protocolo de Roteamento e Segurança de Redes, trabalho correlatos e o trabalho proposto.

A partir desse levantamento foi estabelecido um processo para discutir cada um dos capítulos e estabelecer um conjunto de atributos e métricas que serão relacionados na elaboração da referida síntese.

O Capitulo 1 Introdução é constituída de objetivo geral, objetivos específicos, justificativa e a estrutura do trabalho.

O Capitulo 2 aborda conceitos sobre redes de computadores, redes sem fio, características, tecnologias e infraestruturas.

O Capitulo 3 apresenta o estudo de caso sobre as redes *mesh*, os conceitos de protocolos de roteamento e alguns exemplos e também sobre de segurança de redes, sua importância, e certas maneiras ou formas de manter uma rede *mesh* segura.

O Capitulo 4 apresenta alguns estudos de caso sobre pesquisas realizadas e casos de sucesso da utilização das redes *mesh* no mercado.

O capitulo 5 o estudo proposto para a pesquisa da rede.

Com isso o termino do capitulo primeiro, objetivando a fundamentação teórica pela abordagem de conceitos referente a rede de computadores, características, tecnologias e infraestrutura no capitulo a seguir.

2 **REDES DE COMPUTADORES**

Segundo Forouzan (2006) uma rede é um conjunto de dispositivos, denominados frequentemente de nós, conectados por links de comunicação. Um nó pode ser um computador, uma impressora ou qualquer outro dispositivo capaz de enviar e ou receber dados gerados noutros nós da rede.

Salientar que as conexões podem ser cabeadas ou sem fio, por exemplo, o telefone celular, controle de televisão ou aparelho de som trabalham com conexões sem fio também chamadas de *Wireless*, mas dentro deste padrão de transmissão, existem várias tecnologias como: *Worldwide Interoperability for Microwave Access* (Wi-Max), *WI-FI*, *Bluetooth*, *Infrared* (infravermelho).

Wireless que marca qualquer conexão para transmissão de informação sem o emprego de nenhum tipo de cabo ou fio, que significa: *Wire* (fio); *Less* (sem); ou seja: sem fio.

2.1 REDES SEM FIO

Segundo Tanenbaum (2003) comunicação sem fio não é ideia nova, o físico Marconi demonstrou o funcionamento pela transmissão de códigos morse de um navio por meio de um telegrafo, e embora as redes sem fio tenham desempenho melhor a ideia básica ainda é a mesma.

Rede sem fio é uma tecnologia que permite uma maior mobilidade e redução de custo comparado com as redes tradicionais e por ser uma comunicação entre

equipamentos sem a necessidade de utilizar cabos a sua instalação é mais simples e rápida.

Redes *wireless* tem como proposto funcionar em dois modos; na presença de uma estação base e na ausência de uma estação base. Pelo o padrão 802.11 a estação base chamada de ponto de acesso onde toda comunicação tinha de passar por ele. Quando os computadores simplesmente transmitem uns aos outros este modo é chamado de interligações de redes de acesso *Ad Hoc* (KUROSE e ROSS, 2009).

Para que os equipamentos possam se comunicar entre si, devem usar os mesmos padrões de comunicação e possuir algumas características similares.

A Figura 1 representa o diagrama de uma rede sem fio com repetidores de fornecedores diferentes (Linksys, D-Link e TP-Link), sem problemas de compatibilidade.

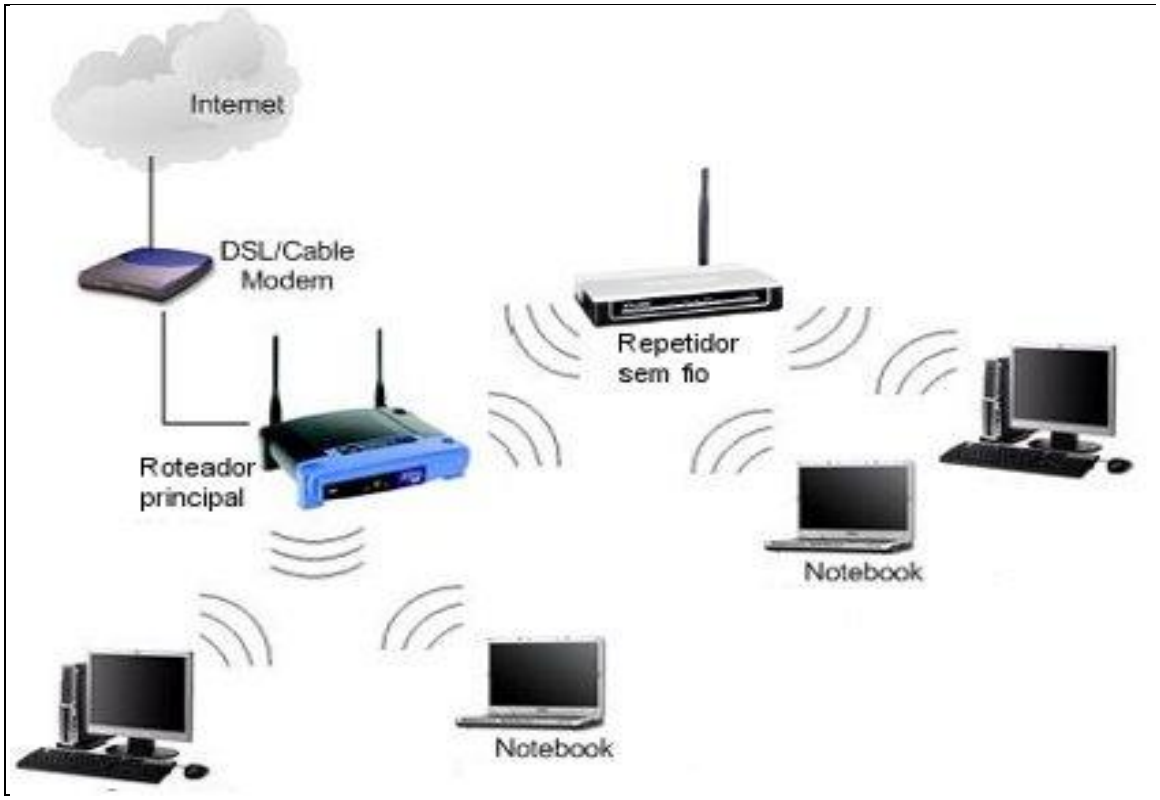

Figura 1. Diagrama de uma rede sem fio com repetidor
Fonte: Augusto Campos (2009).

A rede sem fio está fundamentada no padrão IEEE 802.11, criado pelo IEEE, que define o conjunto de regras para a comunicação sem fio de diferentes tipos de equipamentos. Esses padrões são conhecidos como ISO 8802 elaborados por um comitê chamado de 802 compostos de engenheiros, cientistas e estudantes (TANENBAUM, 1997). Com o objetivo de garantir a interoperabilidade dos diversos tipos de equipamentos e fabricantes existentes.

2.1.1 **Características**

Os equipamentos enviam e recebem sinais por meio do ar, utilizando uma faixa de frequência não licenciada e, portanto, não necessitam de permissão para seu uso, mas com taxas de transferências, área de cobertura do sinal, canais e frequência de operação devidamente padronizada são algumas das características das redes sem fio precisa ter para um bom funcionamento.

2.1.1.1 Modulação do Sinal

Modulação é o processo ou a técnica em que se modificam as características de uma onda de rádio ou elétrica é com a finalidade de se transmitir informações significativas para o ser humano ou para uma máquina.

Para Mathias e Pavão (2006) é possível identificar dois tipos básicos de modulação: analógica e digital. Que altera a amplitude da onda, modulação em amplitude (AM), ou sua frequência, modulação em frequência (FM), ou sua fase, modulação por deslocamento de fase (PM), ou ainda combinar várias dessas alterações.

Modulação analógica, as técnicas mais utilizadas são: AM, FM e PM. AM a amplitude da onda é varia de acordo a estática e a outras interferências elétricas. FM mais constante em relação a AM, mas altera a frequência de acordo com a variação do sinal e requer maior largura de banda. PM transforma a fase de acordo com os dados a serem enviados.

Modulação digital é usada quando se está interessado em transmitir uma forma de onda, mensagem ou um código. As técnicas de modulação para sinais digitais mais utilizadas atualmente são: *Frequency Shift Keying* (FSK), *Phase Shift Keying* (PSK) e *Amplitude Shift Keying* (ASK).

ASK modifica a amplitude da onda em função do sinal digital a ser transmitido. FSK é a variação da frequência da onda em função do sinal digital a ser transmitido. PSK altera a fase da onda em função do sinal digital a ser transmitido.

2.1.1.2 Frequência

A medida da variação na frequência chama-se também de *BandWith* (largura de banda), termo bastante usado também em Radio-física, mede o número de oscilações por segundo e sua grandeza física é o Hertz (Hz); pelo comprimento de onda que é distância entre dois pontos máximos chamados cristas ou mínimos chamados de vales, sendo universalmente designada pela letra grega lambda (λ).

Pelo projeto um Computador por Aluno (2010) frequência normalmente medida em Hertz é a taxa com que a onda eletromagnética se alterna. Os dispositivos por usarem frequências de 2,4 GHz e 5 GHz não necessitam de autorização (licenças) para o uso, enquanto as estações de rádio e TV necessitam de autorização para

transmissões por usarem frequências maiores. Estas são utilizadas equipamentos, como forno de micro-ondas, telefones sem fio, dispositivos *bluetooth* e outros.

Os dispositivos que operam em 2,4 GHz são mais difundidos e por sua popularidade sofrem maior interferência, prejudicando a qualidade da comunicação do que aqueles que operam em 5 GHz. A Interferência pode provocar a perda da mensagem caso o dispositivo não consiga isolar o sinal original do indesejado.

O uso das frequências dentro do espectro eletromagnético obedece a acordos e convenções nacionais e internacionais e a maior parte é mantida sob-rígido controle da legislação, onde as licenças de uso representam um enorme fator econômico no Brasil regulado pela Anatel.

2.1.1.3 Taxa de Transferência

A taxa de transferência é a velocidade que um dispositivo de comunicação transmite dados em uma rede e é medida em *bits* por segundo e em uma rede sem fio, a taxa de transmissão varia de acordo com a qualidade da comunicação e a distância entre os dispositivos.

A taxa de transferência sofre muita variação nos dispositivos que trabalham na mesma faixa de frequência na qual estão os padrões *wireless*, devido a não necessidade de licenças, por serem bandas mantidas abertas para o uso genérico pela *Industrial, Scientific and Medical* (ISM). As que mais nos interessam estão entre 2,400 e 2,495 GHz, que são utilizadas pelos padrões de rádio 802.11b e 802.11g, o comprimento de onda correspondente de cerca de 12,5 cm e as que opera na faixa de

5,150 a 5,850 GHz, com comprimento de onda entre 5 e 6 cm, utilizam o padrão 802.11a para redes sem fio (ANGELO e BARBOSA, 2003).

Existem fatores externos que também reduzem a qualidade e a velocidade na transmissão dos dados na comunicação como; presença de obstáculos, interferências de outros equipamentos e outros.

2.1.1.4 Canais de Operação

Um equipamento de rede sem fio é configurado para operar em um determinado canal, o que significa que os dispositivos que operam nesta rede devem ajustar o equipamento a este canal.

Na Figura 2 detalhes dos canais e frequências na banda de 2,4 GHz no padrão 802.11b. O espectro é dividido em pedaços uniformemente distribuídos dentro da banda como canais individuais. Repare que cada canal tem a largura de 22 MHz, mas estão apenas separados por 5 MHz. Isto significa que existe intersecção entre canais adjacentes eles podem interferir um com o outro.

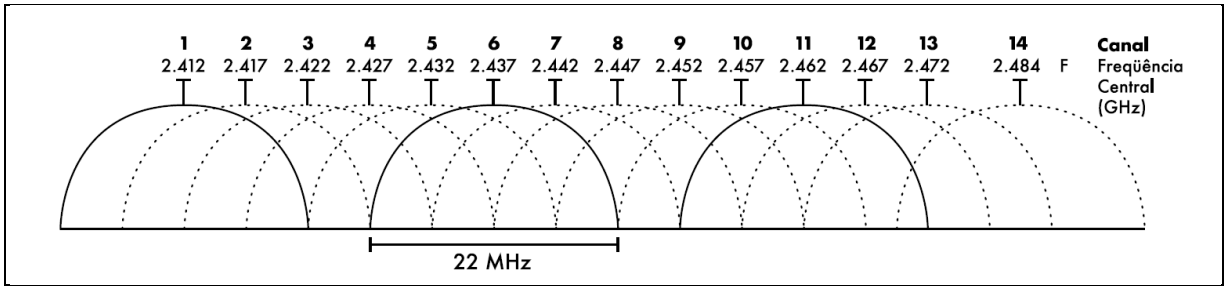

Figura 2. Canais e frequências centrais para o 802.11b
Fonte: WNDW, Redes sem fio no Mundo em Desenvolvimento (2008, tradução nossa).

As características do canal nas redes sem fio é suscetível a diversos problemas na transmissão como: atenuação, interferência, bloqueio, taxa de

transmissão, confiabilidade, entre outros. Sendo que existem os componentes do sinal transmitido que são os diretos que se da normalmente pela potência do sinal transmitido e a potência do mesmo recebido no receptor em um dado momento em função da distância de propagação dependendo de fatores como frequência de rádio e natureza do terreno e os indiretos que compreendem a refração, difração e espalhamento que causam um deslocamento na amplitude e na frequência e na fase.

Segundo Silva (2006) existem ainda dois tipos de flutuações na força do sinal no receptor; rápido ou de pequena escala que são flutuações rápidas na amplitude, fase ou atrasos em múltiplos caminhos no sinal recebido devido à interferência entre múltiplas versões do mesmo sinal e o lento ou de larga escala que acontece quando objetos absorvem parcialmente o sinal, que pode ser diminuída por modulação adaptativa, quando se faz uma estimativa e envia-se um retorno, mas são normalmente muito complexas de implementar.

Quanto à interferência de canais, tem as de canais adjacentes que frequências próximas possuem componentes fora de sua faixa podem interferir na transmissão que pode ser evitado pela introdução de bandas de guarda entre as faixas frequências alocadas e as interferências de co-canais ou banda estreita quando sistemas próximos; difusão de AM ou FM, celulares usando a mesma frequência, mas podem ser evitadas com mecanismos de detecção de multiusuários, antenas direcionais e métodos de alocação dinâmicos de canais ou ainda a equalização adaptativa é que baseia-se no princípio de estimação do pulso de resposta do canal transmitindo periodicamente padrões de bits bem conhecidos.

A capacidade de um canal está diretamente ligada a sua largura de banda, apesar de ser um limite teórico, não alcançável na prática, o teorema de *Hartley*

Shannon provê um padrão de medida pelo qual os esquemas de comunicações práticos podem ser medidos (CASTRO, 2006).

2.1.1.6 Alcance e Largura de Banda

Alcance ou área de cobertura do sinal de uma rede sem fio é a distância máxima que um equipamento é capaz de se comunicar ou trocar informações com outro em uma rede sem fio.

A largura de banda é simplesmente a medida da variação de frequência, então se a variação entre 2,40 GHz e 2,48 GHz é usada, a largura de banda será de 80 MHz. Ela está intimamente relacionada com a quantidade de dados que se pode transmitir dentro dela quanto mais espaço possível na variação da frequência, mais dados é possível colocar neste espaço em um dado momento (WNDW, 2008).

A área de cobertura embora varie devido à capacidade dos equipamentos pode passar os 300m em ambientes abertos e sem obstáculos. Já em ambientes fechados com paredes, portas e até mesmo pessoas entre os equipamentos em geral o alcance fica em torno de 50m.

2.1.2 **Padronização**

Os padrões de redes foram criados para regulamentar as indústrias e permitir que os computadores se comuniquem assim os fabricantes e fornecedores não tem que criar a sua própria regra de concepção.

Segundo Forouzan (2006) existem duas categorias de padrões de fato e de jure (lei), os padrões de fato são os que ainda não foram aprovados por um comitê organizado, mas tem sido muito difundido, aqueles que se consagraram naturalmente sem plano formal, e os padrões de jure são padrões legais e formais adotados por um corpo, comitê organizado ou instituição de padronização autorizada.

O padrão utilizado pelas redes wireless que é o 802.11, que com o passar do tempo sofreu alterações devido a alguns fatores como velocidade, taxa de frequência, modulação, alcance, segurança. Estas melhorias foram incorporadas sob emendas, designadas por letras acrescentadas ao nome do padrão, como o IEEE 802.11g (KUROSE e ROSS, 2009). Algumas emendas:

a) **802.11a** foi lançado no mesmo ano que o 802.11b (1999), taxas adicionais oferecidas pela emenda "a" são: 6 *megabit* por segundo (Mbps), 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps e 54 Mbps e frequências entre 5,725 e 5,875 GHz.

b) **802.11b** foi o primeiro padrão IEEE 802.11 a se popularizar. Ele opera na faixa entre 2,4 e 2,4835 GHz e velocidades de transmissão: 1 Mbps, 2 Mbps, 5,5 Mbps e 11 Mbps.

c) **802.11g** na mesma faixa de frequência que o padrão 802.11b, especificado muitas vezes como dispositivos 802.11b/g operam com taxas de transmissão de até 54 Mbps.

d) **802.11n** iniciado em 2004, com previsão de publicação em 2010, pode operar nas faixas de 2,4 GHz e 5 GHz, o que o torna compatível com os padrões anteriores. Com várias vias de transmissão (múltiplas

antenas) pode operar com taxas de transmissão de dados de até 300 Mbps.

A Figura 3 tabela que mostra um resumo dos padrões para WLANs IEEE 802.11 mais utilizados atualmente.

Padrão	Freqüência	Taxa máxima da camada física	Método de transmissão	Área de cobertura (*indoor*)
802.11	2.4GHz	2Mbps	FHSS/DSSS	
802.11a	5GHz	54Mbps	OFDM	~ 30m
802.11b	2.4GHz	11Mbps	DSSS	~50m
802.11g	2.4GHz	54Mbps	OFDM	~30m

Figura 3. Comparativo entre os padrões de WLAN IEEE 802.11
Fonte: Gonçalves e Endo (2008)

O IEEE formou o *Extended Service Set* (ESS) *Mesh Networking Study Group* (MNSG) com o objetivo de criar um protocolo padrão permitindo que os fornecedores certifiquem seus equipamentos como 802.11s, sem data de previsão para resolver a questão da capacidade, escalabilidade, onipresença e outras características relacionadas à tecnologias de transmissão para as rede *mesh*.

2.1.3 **Tecnologias de Transmissão**

As tecnologias envolvidas para os sistemas de transmissão de redes sem fio possuem as suas peculiaridades, limitações e suas vantagens. No entanto essas redes usam basicamente, alguns tipos específicos de procedimentos para a comunicação da informação, abaixo algumas dessas tecnologias.

2.1.3.1 Espalhamento de Espectro (*Spread Spectrum*)

Mais utilizados nos sistemas de redes locais sem fio, uma técnica de codificação para transmissão digital, confiáveis, seguros e de missão crítica pela troca de maior consumo de banda e o uso de bandas não licenciadas é utilizada pelos produtos que seguem normalmente os padrões 802.11b, 802.11g.

O padrão IEEE 802.11 para Held (2001) especifica alguns métodos de transmissão e dentro do espalhamento de espectro se encontra um replicador e um transmissor dos bits de dados que são: a *Frequency-Hopping Spread Spectrum* (FHSS) e o *Direct-Sequence Spread Spectrum* (DSSS).

Frequency Hopping Spread Spectrum usada para suportar a modulação *frequency hopping* , sinal portador de banda estreita salta de frequência em frequência pseudo-aleatóriamente ou pelo *dwell time,* era relativamente barata e não requeria alta potência, tinha vantagem pelo grande número de redes coexistentes. O grande *throughput* agregado para todas as redes em uma dada área deixou de ser devido ao sistema *direct sequency* que possui uma melhor taxa de transferência, (MALBURG, 2004).

A largura de banda disponível pelo FHSS é dividida em um certo número de canais de banda estreita, caso dois sistemas *Frequency Hopping* precisam ocupar uma mesma banda, eles podem ser configurados com sequencias de saltos diferentes e não haverá interferência. Sendo que é um método no qual transmissor e receptor saltam de uma frequência para outra ao longo de padrões acertados entre ambos, é considerado também como resistente à interferência, mas não imune, de banda estreita.

Direct Sequency Spread Spectrum é uma técnica usada para transmitir um sinal sobre uma ampla banda de frequência, por uma sequência de espalhamento chamada de sequência de Barker de 11 *chips* que é dada por (1 0 1 1 0 1 1 1 0 0 0). Após espalhado, o sinal é modulado em uma portadora. Os esquemas de modulação para DSSS usados são: *Differential Binary Phase Shift Keying*, que permite uma taxa de 1Mbps e o *Differential Quadrature Phase Shift Keying*, que permite uma taxa de 2Mbps, (MALBURG, 2004).

Apresenta um módulo dentro do transceiver chamado correlator que dá proteção contra interferências de ruídos que tendem a ter uma forma de pulsos relativamente estreitos produzindo efeitos coerentes por meio da banda de frequência a função da correlação é desprezar o ruído ao longo da banda e o sinal original é recuperado a principal vantagem da transmissão está no fato de que ela está mais apta a altas taxas de transferência do que o FHSS.

2.1.3.2 Sistemas *Narrowband*

Banda estreita (*Narrowband*) são sistemas de rádio frequência específicas que transmite e recebe informações mantendo o sinal o mais estreito possível o suficiente para passar a informação havendo uma filtragem das frequências pelo receptor, exceto a determinada pelo sistema, mas se torna pouco adequado a transmissão de dados, pois operam numa frequência de rádio específica (SILVA, 2007).

Para não haver colisão de dados nos vários canais de comunicação, deve haver coordenação cuidadosa entre os diferentes usuários nos diferentes canais de frequência.

2.1.3.3 Sistemas *Infrared*

Sistemas *Infrared* (infravermelhos) segundo Silva (2007) utilizam altas frequência, abaixo da luz visível no espectro eletromagnético, para transmitir dados. Também consideradas transmissões difusas ou direitas por não poder atravessar objetos opacos, limitando seu alcance. Sendo que os infravermelhos direitos oferecem uma distancia aproximada de 1,5m comumente utilizados em *Personal Area Network* (PAN) e ocasionalmente são utilizados em *Wireless Local Area Network* (WLAN).

2.1.3.4 Radiofrequência

Radiofrequência, segundo Santos (2005), são correntes alternadas de alta frequência que passam por meio de condutores de cobre e, então, são irradiadas pelo ar por meio de antenas, transformam o sinal do cabo em uma onda eletromagnética que se propaga no espaço e vice-versa, as ondas de rádio propagam-se, afastando-se da antena em todas as direções. Rádios transmitem e recebem sinais por meio de longas distâncias na forma de onda eletromagnética.

2.1.3.5 Ortogonal Frequency Division Multiplexing

Combinação de modulação e esquemas de múltiplo acesso que segmentam um canal de comunicação usa a largura de banda de um canal de frequência, quebrando-a em vários subcanais de espaçamento igual em que cada subcanal carrega

um pedaço da informação, sendo que os mesmos então multiplexados, independentes produzidos por fontes diferentes, compartilhando banda com outros canais, em um canal combinado (SANTOS,2005).

No controle de acesso de um canal compartilhado, tem de haver uma determinada maneira com que o canal será compartilhado entre os nós. As técnicas baseadas na ortogonalização de sinais, cada sinal representado como uma função de tempo, frequência e código, a multiplexação então é realizada com respeito a um desses três parâmetros; *Frequency Division Multiple Access (FDMA)*, *Time Division Multiple Access (TDMA)* e *Code Division Multiple Access (*CDMA), (CHEUNG, 2002).

2.1.3.6 Antenas

Uma antena pode ser definida segundo Ângelo e Barbosa (2003) como sendo um condutor elétrico ou um sistema de condutores usados tanto para irradiar energia eletromagnética no espaço quanto para captar energia eletromagnética do espaço.

Para fazer a transmissão uma antena deve converte a energia elétrica em energia eletromagnética que irradia no ambiente ao redor, para receber faz o contrário, para captar ou irradiar usa-se a mesma antena. Uma antena irradia potência em todas as direções, mas o seu desempenho não é igual em todas as direções.

Para analisar o desempenho de uma antena usa-se as linhas de radiação (uma representação gráfica das propriedades de radiação em função das coordenadas espaciais), outra mais simples é a isotrópica, a qual é um ponto no espaço que irradia potência igualmente em todas as direções. A atual representação de radiação para antena

isotrópica é uma esfera com a antena no centro. Linhas de radiação são quase sempre representadas pela secção transversal do formato de radiação tridimensional.

No mercado, existem varias antenas, mas todas podem ser genericamente distribuídas em dois tipos básicos; o *Dipolo* e a antena vertical. O primeiro se subdivide em antena dipolo de meia onda, ou antena Hertz, e o segundo em um quarto de onda, ou antena *Marconi*, (ÂNGELO E BARBOSA, 2003).

O dipolo de meia onda consiste em dois condutores retilíneos horizontais e colineares de mesmo comprimento, separados por um pequeno espaço de alimentação. O comprimento da antena é de um meio de comprimento de onda do sinal que pode ser transmitido mais eficientemente. O tipo dipolo tem linha de radiação uniforme ou omnidirecional, porém configurações mais complexas de antenas dipolos fornecem raios direcionais.

2.1.4 **Infraestrutura**

A utilidade de ter dispositivos conectados o tempo todo sem possibilidade de usar um cabo de rede é inegável e indiscutível, no entanto há dois modos diferentes de configurar dispositivos sem fio segundo o padrão 802.11que são Infraestrutura e *Ad Hoc* (RUFINO, 2005).

Porém em qualquer um dos modos de operação um *Service Set Identifier* (SSID), também conhecido como nome da rede, será utilizado pelas estações para identificar e/ou conectar as redes sem fio disponíveis (GAST, 2002).

2.1.4.1 Modo Infraestrutura

Neste modo a transferência de dados nunca ocorre diretamente entre duas estações, existe a presença de um nó central ou ponto de acesso – *Access Point* (AP) por onde toda a comunicação é dirigida, inclusive comunicação entre computadores que estiverem na mesma área de serviço, permite com isso um maior controle (Gast, 2002).

Normalmente usada em redes de topologia estrela que exista um centralizador que controla o fluxo de toda a rede, com ou sem colisão. Sendo que os AP como nós especiais podem controlar quaisquer possibilidades de colição caso estejam eles controlando o meio.

Este modo Figura 4 é normalmente o mais encontrado, utiliza um concentrador ou centralizador de acesso.

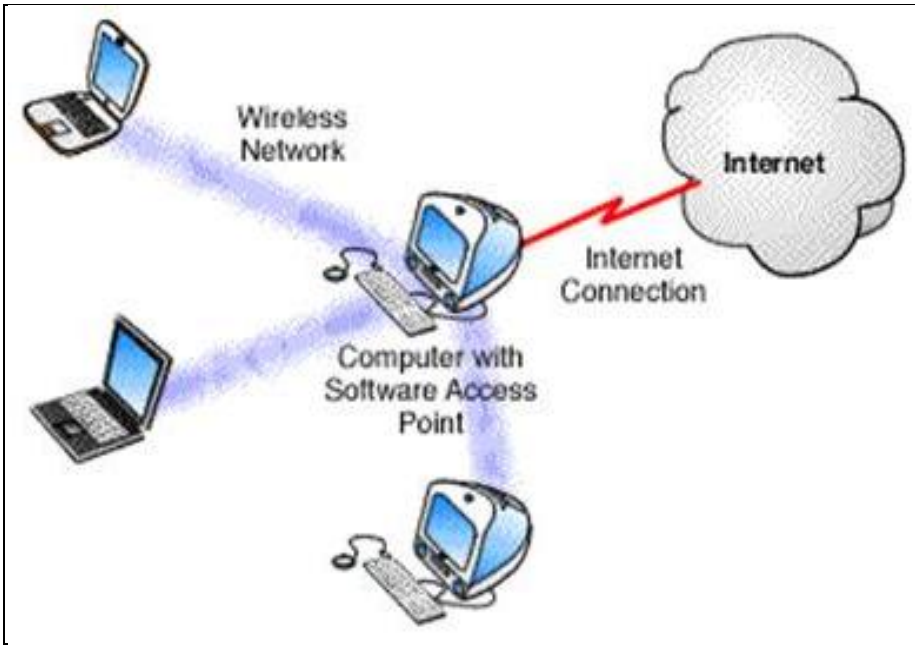

Figura 4. Modo Infraestrutura
Fonte: Pinheiro (2004)

Entre as suas vantagens ele facilita a interligação com a rede sem fio, rede cabeada e/ou com Internet, já que em geral o concentrador também desempenha o papel de gateway ou ponte providenciando com isso todas as configurações necessárias para que possa haver tal ligação (RUFINO, 2005).

2.1.4.2 Modo Ad Hoc

Esta rede pode ser formada por equipamentos portáteis, com o intuito de trocar dados na ausência de pontos de acesso, cada estação se comunica diretamente com outra estação (KUROSE & ROSS, 2006).

De acordo com Farias (2006) as redes Ad Hoc como não possuem uma infraestrutura física, são geralmente pequenas e normalmente não possui uma conexão com a rede com cabo, não existe um limite máximo definido para o número de dispositivos que podem fazer parte dessa rede, mas o controle da mesma é de forma distribuída. Figura 5 três máquinas se comunique diretamente, sem a necessidade de um ponto de acesso.

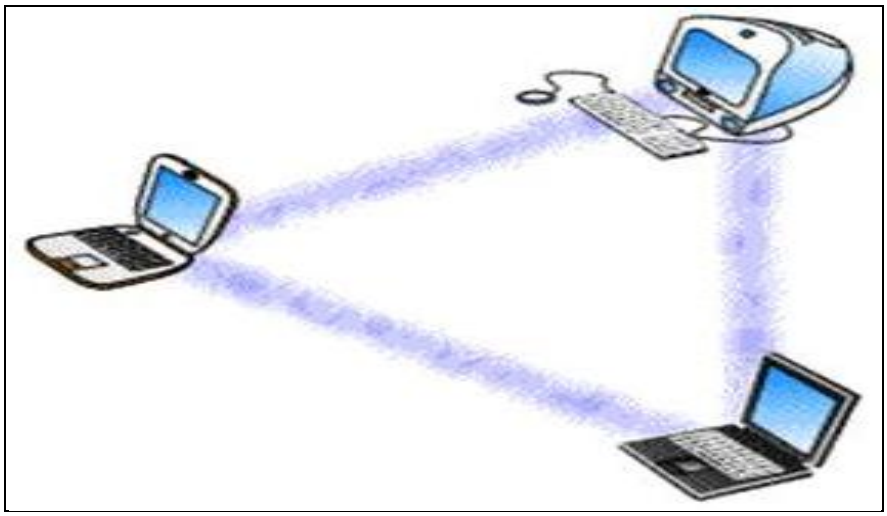

Figura 5. Modo Ad Hoc
Fonte: Pinheiro (2004)

Segundo Rufino (2005) a ausência de uma infraestrutura física leva as redes Ad Hoc apresentar as seguintes desvantagens: problemas de comunicação, devido ao problema do nó escondido; problema de segurança, administração e gerência de rede e a alta complexidade da rede.

2.1.4.3 Modelo Open System Interconnection (OSI)

Segundo Tanenbaum (2003) modelo OSI é chamado de modelo de referência OSI, pois trata da interconexão de sistemas abertos, ou seja, sistemas que estão abertos à comunicação com outros sistemas, e apresenta sete camadas; física, enlace de dados, rede, transporte, sessão, apresentação e aplicação.

O modelo OSI define as funções necessárias para que haja a interconexão entre sistemas distribuídos, para as redes sem fio, as camadas; física (também camada de PHY) e enlace (camada ligação de dados, ou *Logical Link Control* - LLC), são estabelecidos na norma 802.11 como camadas baixas do modelo OSI para uma ligação sem fios que utiliza ondas electromagnéticas.

O posicionamento na estrutura de camadas física e enlace no modelo OSI do protocolo 802.11 Figura 6.

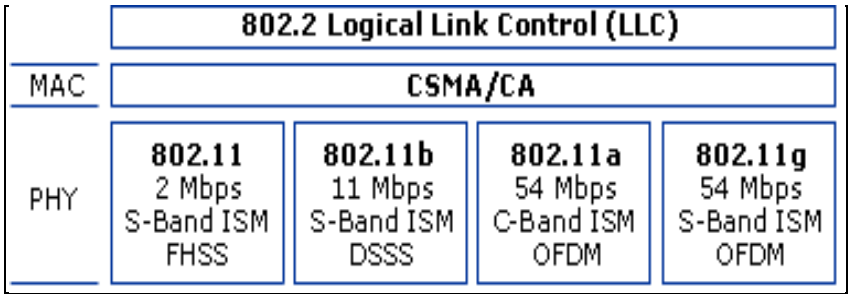

Figura 6. Camadas Física e de Enlace de uma rede 802.11.
Fonte: André Pimenta Mathias (2000).

O quadro MAC do 802.11, consiste em um cabeçalho (*header*) MAC, o corpo do quadro e o campo *frame check sequence*.

Os números na Figura 7 representam o número de bytes de cada campo.

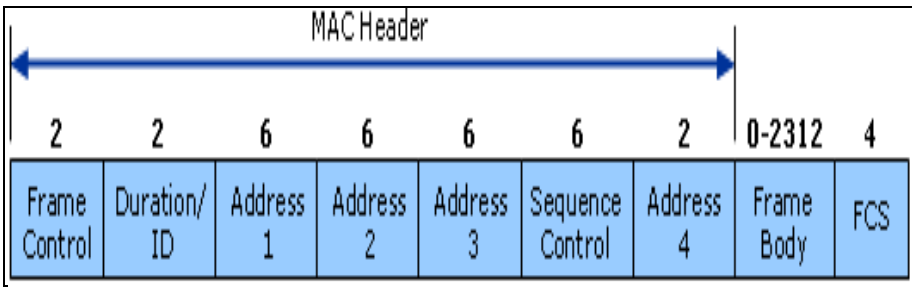

Figura 7. Quadro MAC de uma rede 802.11.
Fonte: André Pimenta Mathias (2000)

2.1.4.3.1*Camada Física (PHY)*

Os protocolos que trabalham nesta camada preocupam-se em definir basicamente, o tempo de transferência entre os bits, se a comunicação acontece nos dois sentidos simultaneamente (*full-duplex*), ou em um sentido de cada vez (*half-duplex*) e ainda na função de cada pino utilizado pelos conectores de rede (TANENBAUM, 2003).

A camada física é responsável pela transmissão dos *bits*, definindo as características elétricas, mecânicas e funcionais envolvidas nesta transmissão, além de tratar os procedimentos que definem o início e o fim da transmissão de bits por um canal, comunicando-se diretamente com o controlador da interface de rede.

O 802.11 define uma série de padrões de transmissão e codificação para comunicações sem fio, sendo os mais comuns: FHSS, DSSS e OFDM. As funções dessa camada são: codificação e decodificação de sinais, geração/remoção de parâmetros para

sincronização, recepção e transmissão de bits, incluí especificação do meio de transmissão, entre outros.

2.1.4.3.2 *Camada de Enlace*

Tem como principal objetivo oferecer a camada superior uma linha de transmissão que pareça livre de erros (TANENBAUM, 2003), verificando os bits que chegam pelo meio físico.

As principais funções desta camada são: reconhecer e montar quadros (frames) de dados com os bits que chegam da camada física passando os para camada de rede; tratar do controle de fluxo dos dados transmitidos, evitando que a estação emissora sobrecarregue a estação receptora; detectar erros e se possível corrigi-los, ocasionados por problemas na camada física ou na própria camada de enlace (EMBRATEL, 1997).

Também é conhecida como camada de ligação de dados detecta e corrige erros que possam acontecer no nível físico, responsável pela transmissão e recepção de quadros e pelo controle de fluxo, estabelece um protocolo de comunicação entre sistemas diretamente conectados. O padrão 802.11 define duas camadas separadas, o LLC que fornece uma interface para camada superior (rede) e controle de acesso ao meio físico o MAC que acessa diretamente o meio físico e controla a transmissão de dados.

As funções da camada MAC são: aspectos de transmissão, de recepção, controle de acesso ao meio de transmissão *Local Área Network*.

A função da camada LLC é de prover interface para a camada superior e executa controle de fluxo e erro de pacotes.

Além das características, modos de transmissões, tecnologias e infraestruturas existem diferentes tipos de redes sem fio, que para o caso abordaremos a rede *mesh*, arquitetura, protocolos e segurança.

3 **REDES MESH**

A Internet é considerada a maior rede *mesh* do mundo, isso porque as informações percorrem passando automaticamente de um roteador a outro, até chegarem a seu destino é descrita também como uma nuvem de conectividade, devido aos múltiplos caminhos por onde os dados podem passar.

O baixo custo da infraestrutura para a criação de redes mesh, a sua capacidade de autoconfiguração e a topologia de roteamento dinâmico vem sendo considerado, para as redes de acesso comunitárias e também para as consideradas cidades digitais.

As redes *mesh*, conhecidas como redes comunitárias de acesso sem fio, podem ser usadas para reduzir o custo da "última milha" no acesso à Internet, por meio da colaboração entre nós, compartilhando um enlace com a rede fixa e permitindo uso mais eficiente da banda sem custos com cabeamento até o usuário final (BREUEL, 2004), como na Figura 8.

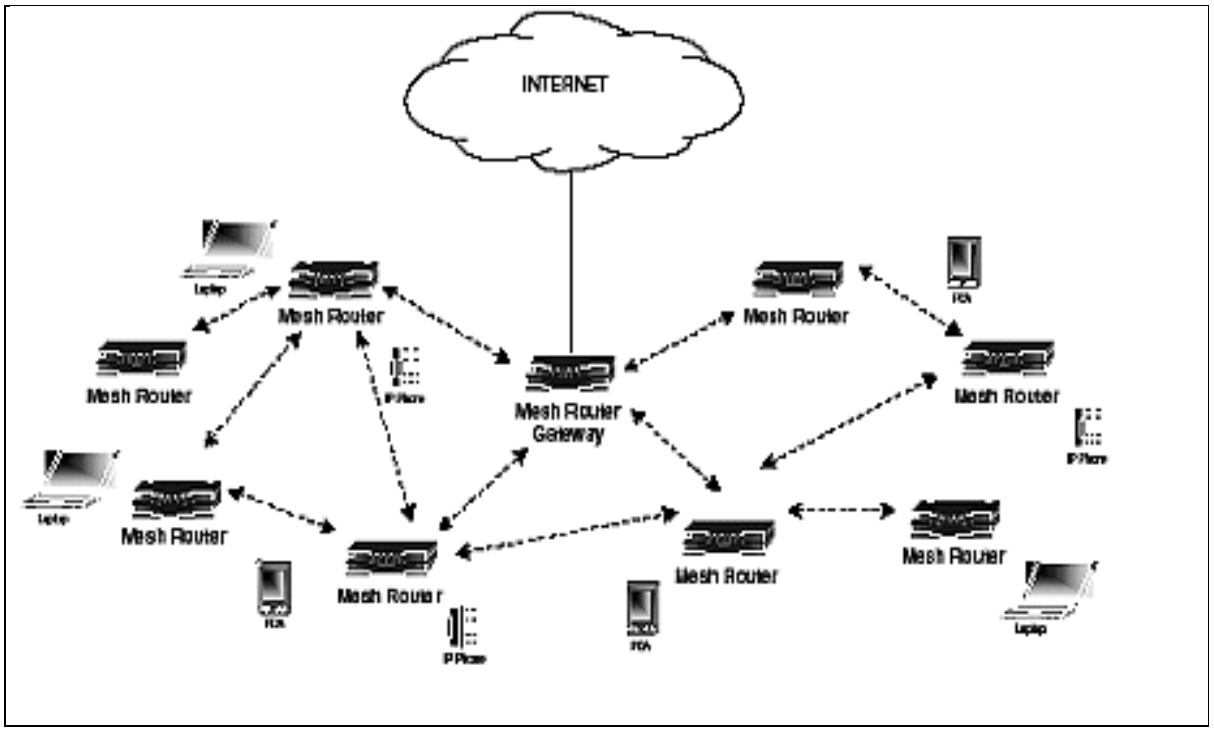

Figura 8. Exemplo de uma Rede *wireless mesh*
Fonte: Tomazeti e Pontes (2007)

As redes *mesh* são redes autoconfiguráveis e administráveis com topologia de crescimento orgânico, constituídas cuja comunicação é feita por meio de uma das variantes do padrão IEEE 802.11, e cujo roteamento é dinâmico.

3.1 ARQUITETURA

As redes possuem diferentes arquiteturas, mas neste contexto, dois tipos de nós que podem ser encontrados nas redes *mesh*, no entanto elas aceitam a comunicação com outros tipos de redes e seus respectivos equipamentos.

3.1.1 **Mesh Routers**

Roteadores que possuem uma mobilidade quase nula, em muitos casos podendo ate possuir certa mobilidade formando o *backbone*, a infraestrutura e a malha de autocorreção e autoconfiguração da rede para os clientes.

Suportam diversas tecnologias *wireless* em sua interface, conectam-se também com outras redes wireless ou com redes ethernet por meio de um *link*, possuem as mesmas funcionalidades de roteadores convencionais, capacidade de funcionar como *gateways* e *bridges*, podendo ser ligada com a Internet, por meio da função de *gateway*.

Para que todos estes recursos possam ser executados de maneira satisfatória é necessário um maior poder computacional, necessitando normalmente de um computador para realizar o papel de nó central ou simplesmente fazer uso de um sistema embarcado (AKYILDIZ; WANG, 2005).

3.1.2 **Mesh Clientes**

Os *mesh* clientes são uma forma de redes *peer-to-peer* entre os clientes onde cada estação possui capacidade e responsabilidades equivalentes, têm a habilidade de funcionar como roteadores e também como *gateways* caso necessário.

Clientes podem tanto acessar a rede via *mesh* routers quanto diretamente por outros clientes, realizam funções de roteamento e configuração, a possibilidade de perda de desempenho dos usuários finais devido à realização de tarefas de autoconfiguração e roteamento.

Podem realizar o processo de encaminhamento de pacotes entre os demais elementos *mesh* da rede, no entanto não podem exercer na integra as funções de *bridge* ou *gateway*. Em contrapartida, este tipo de nó apresenta apenas uma interface de rede e um *hardware* bem mais simples, podendo variar desde um *laptop* até um telefone IP (AKYILDIZ; WANG, 2005).

3.1.4 **Mesh Routers e Clientes**

A combinação dos roteadores e clientes *mesh* juntamente com a utilização de interfaces de redes não *mesh*, podem ser formadas três tipos de arquiteturas:

a) **Arquitetura Cliente**: Só os nós clientes são usados nesta arquitetura cada um desempenha o papel de cliente e o de roteador. Eles se comunicam como em uma rede *peer-to-peer* formando uma estrutura muito similar a de uma rede *Ad Hoc*, diferindo apenas na utilização de uma única tecnologia de transmissão Akyildiz e Wang (2005).

b) **Arquitetura Infraestruturada**: os roteadores *mesh* formam o *backbone* da rede que conecta clientes não *mesh*, por meio deste *backbone* formado é possível interligar diferentes redes com diferentes tecnologias de transmissão. Esse é o tipo de rede *mesh* mais usada, pois necessita de modificações apenas nos seus roteadores que normalmente utilizam duas antenas com canais

distintos, uma para o *backbone* e outra para atender os clientes Akyildiz e Wang (2005).

c) **Arquitetura Híbrida**: esta arquitetura é uma combinação entre as arquiteturas *mesh routers* e *mesh* clientes, melhorando com isso a interoperabilidade e a conectividade na rede, suportam as redes *Ad Hoc* e possuem a dedicação dos roteadores que compreendem as funções de roteamento, autoconfiguração e autocorreção sendo ainda multi-saltos (AKYILDIZ; WANG, 2005).

Das arquiteturas divulgadas cada uma tem seu grau de utilização e aplicação, lembrar que a infraestrutura wireless suporta a mobilidade dos nós finais, integram diferentes tipos de redes, possuindo restrições no consumo de energia e como todas as arquiteturas em todas as redes possuem os seus prós e contras.

3.2 VANTAGENS

As vantagens das redes mesh sem fios incluem: custo, robustez, mobilidade e flexibilidade, simplicidade, escalabilidade, segurança, alta imunidade a ruídos, inclusão digital, *gateway* entre outros.

Custo – redução do custo de implementação, menos cabos significa um custo menor de *hardware* para montar uma rede especialmente sem a necessidade de obras e tarefas tortuosas, menor custo de cobertura das tecnologias atuais, baixo custo de manutenção, não existe a tarifação de impulso telefônico e ainda os *kits* "*mesh boxes*" (LUIZ; JUNIOR, 2005).

Robusteza – dinamismo em estruturas instáveis, o roteamento e a autorreparação significam que a adição ou remoção de um nó, bloqueio, perda de sinal ou interferência em um *link*, à rede se adapta sem a necessidade de interferência humana (BREUEL, 2007).

Mobilidade e Flexibilidade – tecnologia sem fio permite que as redes cheguem aonde cabos não podem ir e prover aos usuários acesso à informação em tempo real em qualquer lugar.

Simplicidade – instalação rápida e simples para de alguns *kits mesh* em que o usuário final precisa ligar o roteador *mesh* à tomada, ou instalar um *software* no computador do usuário (BREUEL, 2007).

Escalabilidade – pode ser definida como o nível de serviço de pacotes aceitável na presença de um grande número de nós na rede (RAMANATHAN & REDI, 2002). É fator importante pela potencial redução de desempenho com o incremento do número de nós. Por isto, todos os protocolos das camadas envolvidas devem ser escaláveis (INTEL, 2004).

Segurança – suporta encriptação com chave igual ou superior a 128 bits, o tráfego de rede pode passar por uma *Virtual Private Network* (VPN) que utiliza o protocolo de segurança de IP com chave de até ou superior a 1024 bits, garantindo proteção à rede contra ataques externos.

Tolerante a falhas – capacidade de roteamento dinâmico aliado à existência de múltiplas rotas de acesso faz com que a rede consiga se recuperar de falhas como a perda de um enlace de comunicação (DAMALIO, 2008).

Inclusão Digital – permite a inclusão digital pelo baixo custo, à fácil instalação e a gerência, sendo que quase todas as configurações de rede são automáticas.

Incentiva compartilhamento coresponsável entre usuários e permite compartilhamento seguro e ordenado de acesso digital.

Gateways – a redundância de *gateways* pode possibilitar fim da ociosidade das conexões e aumentar a velocidade pela soma da velocidade dos *gateways.*

3.3 DESVANTAGENS

As desvantagens das redes *mesh* sem fios incluem: Questões econômicas e sociais, segurança e privacidade, aumento no tráfego devido aos protocolos de roteamento e degradação da largura de banda, interferência eletromagnética e protocolos ainda não homologados, perda frequente de pacotes, soluções proprietárias, restrições e outros.

Questões econômicas e sociais – o compartilhamento de recursos quando se trata de indivíduos, é provável que haja conflitos e abuso na utilização, injustiça nos valores investidos por cada um, ou violações de privacidade e os altos preços dos aparelhos (DAMALIO, 2008).

Segurança e privacidade – a principal dificuldade é garantir a privacidade dos dados trafegados entre os nós da rede, a interface de rádio aberta é muito mais fácil de ser burlada do que sistemas físicos tradicionais, outra questão é a permissão de acesso à rede, a chance de que a chave compartilhada não é a melhor das soluções, criptografia apenas em nível de aplicação (BREUEL, 2007).

Aumento no tráfego devido aos protocolos de roteamento e degradação da largura de banda – a troca de informações de roteamento pode

produzir uma grande quantidade de tráfego, a tabela de roteamento completa pode ficar muito grande. Há também o perigo de roteamento *loops* que podem aparecer por causa de informações de roteamento.

Interferência eletromagnética e Protocolos ainda não homologados – a interferência eletromagnética é inerente a toda rede sem fios, devido à utilização dos padrões da família IEEE 802.11, que são de uso livre. Devido a isso, existem diversos equipamentos sem fio, que utilizam o mesmo espectro (DAMALIO, 2008).

Perda frequente de pacotes – a perda frequente de pacotes, causada por interferência de obstáculos e recepção por múltiplos caminhos.

Soluções proprietárias – o lento procedimento de padronização derivou a criação de soluções proprietárias, que oferecem funções padronizadas mais características adicionais que funcionam apenas em um ambiente homogêneo quando adaptadores do mesmo fabricante são utilizados em todos os nós da rede. (DAMALIO, 2008).

Restrições – os produtos sem fio precisam respeitar os regulamentos locais, as instituições governamentais e não governamentais regulam e limitam a operação das faixas de frequência para que a interferência seja minimizada.

3.4 PROTOCOLOS DE ROTEAMENTO

Protocolos de roteamente possuem estrutura de compartilhamento de informações de rotas entre os dispositivos, servem para trocar informações de construção de uma tabela de roteamento na camada de rede permitindo o roteamento dos pacotes de um protocolo roteado.

Os aspectos a serem analisados, e considerados quando se refere ao estudo dos protocolos de roteamento, de qualquer rede de comunicação de dados, incluem a confiabilidade, a disponibilidade e o desempenho da rede.

Importante observar que, segundo Freitas (2001), na análise do desempenho de um protocolo, deve ser considerado o contexto topologia da rede, cujos atributos essenciais incluem: tamanho da rede, conectividade da rede, taxa de mudança de topologia, capacidade do enlace, fração de enlaces unidirecionais, padrões de tráfego, mobilidade, entre outros.

Os protocolos de roteamento ad hoc são divididos em duas categorias (SESAY, YANG & HE, 2004), quanto à construção de rotas, mas a união dos mesmos forma um terceiro protocolo, sendo eles: os reativos, os pró-ativos e os híbridos.

Os reativos ou *on demand* usado nas redes *Ad Hoc* tradicionais genéricas a descoberta da rota é sob demanda, sem ter dados para enviar, eles não atualizam as tabelas de roteamento, para enviar os reativos inundam a rede com pacotes de controle até receber uma resposta do host destinatário, assim que a rota é descoberta o pacote é enviado, isso diminui o tráfego de pacotes de controle, aumentando assim a capacidade de transmissão de dados (FARIAS ET al, 2005).

Demandar um pequeno *overhead* de controle porque não há a necessidade de manter as tabelas dos roteadores constantemente atualizadas com a topologia da rede, ao enviar um dado para um nó que o roteador não sabe a rota, tem-se um retardo maior no envio enquanto o roteador tenta descobrir o destino.

Os Pró-ativos, ou *table driven*, são os protocolos de roteamento baseados em tabelas de roteamento que são atualizadas com toda a topologia da rede, utilizam algoritmos específicos para calcular o caminho de menos custo, mas possuem um alto

custo para manter as tabelas constantemente atualizadas devido à troca de mensagens de controle que tomam parte da capacidade de comunicação das redes (FARIAS ET al, 2005).

As características dos protocolos pró-ativos e reativos combinadas deu a criação dos protocolos de classe Híbridos, que de acordo com Yang e Tseng (2005), esses protocolos estabelecem uma zona onde se tem um conhecimento parcial ou total da topologia da rede e, caso necessite enviar alguma informação para um nó mais distante este protocolo atuaria como um protocolo *on demand*.

O *Zone Routing Protocol* é um bom exemplo, pois que estabelece uma zona onde ele vai atuar como pró-ativo, a partir do limite dessa zona ele passa a atuar como *on demand*, inundando pacotes de atualização para descobrir qual rota utilizar para enviar a informação.

3.4.1 **Optimized Link State Routing**

Optimized Link State Routing (OLSR) protocolo pró-ativo mais utilizado atualmente é um dos primeiros para redes mesh, considerado como mais estável e documentado, apresentando já interfaces gráficas para configuração, uma versão otimizada do algoritmo estado de enlace puro é padronizado pelo *Internet Engineering Task Force* (IETF) por meio do Request for Comment (RFC) 3626.

Reduz *overhead* de controle na rede utilizando o conceito de *Multipoint Relays* (MPRs) que deve ser mantido pela eficiente, selecionados dinamicamente, conforme o crescimento da rede, por meio deles os roteadores enviam informações que tem como destino, nós, mais distantes, diminuindo assim o tráfego na rede e a colisão de

informações na camada de transporte, decide pela melhor rota apenas pelo menor número de saltos, o que não é a melhor alternativa. Uma proposta é a utilização da extensão *Optimized Link State Routing – Minimum Loss* (OLSR-ML) onde a taxa de perda dos links é monitorada, e quando a topologia é montada, o roteador decide pela rota com a menor taxa de perda acumulada. Protocolo a ser tratado aqui com um pouco de mais atenção uma vez que será utilizado no trabalho prático.

3.4.1.1 Funcionamento e Comportamento Do Protocolo OLSR

Comparado com o software pré-instalado em muitos roteadores WLAN, o DD-WRT permite um funcionamento fiável e claramente definida no OLSR usando o *User Datagram Protocol* (UDP) na transmissão e comunicação de pacotes sendo que o port 698 lhe foi atribuído pela *Internet Assigned Numbers Authority* (IANA, autoridade que atribui os números na Internet) para uso exclusivo.

O OLSR esta dividido em duas partes: em um núcleo funcionalidade e um conjunto de funções auxiliares, isso para que o protocolo possa ser simples de compreender e fácil de adicionar alguma complexidade a onde for necessário adicionar alguma nova funcionalidade. O núcleo especifica o protocolo que fornece roteamento e o conjunto de funções auxiliares possibilita a adição e a compatibilidade à medida que qualquer subconjunto for adicionado ao núcleo.

Especificamente, o núcleo é composto de seguintes componentes: formato e encaminhamento de pacotes, sensoriamento de links, detecção de vizinho, seleção e sinalização de *Multi Point Relays* (MPR), difusão e controlo mensagem, e cálculo de rota.

Formato e encaminhamento de pacotes especifica universalmente o formato de pacote e utiliza um mecanismo otimizado de alagamento que serve como mecanismo de transporte para todos os pacotes de controle de tráfego.

Link Sensoriamento realizado por meio da emissão periódica de mensagens OLÁ sobre as interfaces através das quais a conectividade é marcada. Resulta um conjunto de ligações local, que descreve as relações entre s interfaces de nós vizinhos. Olá mensagens são trocadas periodicamente entre os nós vizinhos, para detectar relações e identidade entre vizinhos a e sinal de seleção MPR.

Detecção de vizinho se os nós forem de interface única, ele pode deduzir o nó mais próximo (vizinho) a partir das informações trocadas como o endereço principal de um único nó de interface é, por definição, um endereço único. Caso seja uma rede com nós de interface múltipla, informação adicional é necessária e adquirida através da *Multiple interface declaration* (MID).

Seleção e sinalização de MPR com a troca periódica de mensagens OLÁ é calculada o MPR, com isso feito, é possível que um nó para selecione um subconjunto de nós vizinhos, de forma que uma mensagem de broadcast será recebida por todos os nós e a sinalização é fornecida de acordo as disposições.

Difusão e Controle de Mensagem, a topologia mensagens de controle é difundida, com o objetivo de proporcionar a cada nó na rede com um número suficiente de links de informações, para permitir o cálculo da rota.

O protocolo de roteamento OLSR inclui uma especificação universal de mensagens e sua transmissão por meio da rede possuem interfaces sendo integrantes das *Mobile Ad hoc NETwork* (MANET, são redes criadas por uma reunião de nodos móveis sem disporem de alguma infraestrutura pré existente).

Figura 9 Layout básico de qualquer pacote no OLSR, omitindo IP e cabeçalhos UDP.

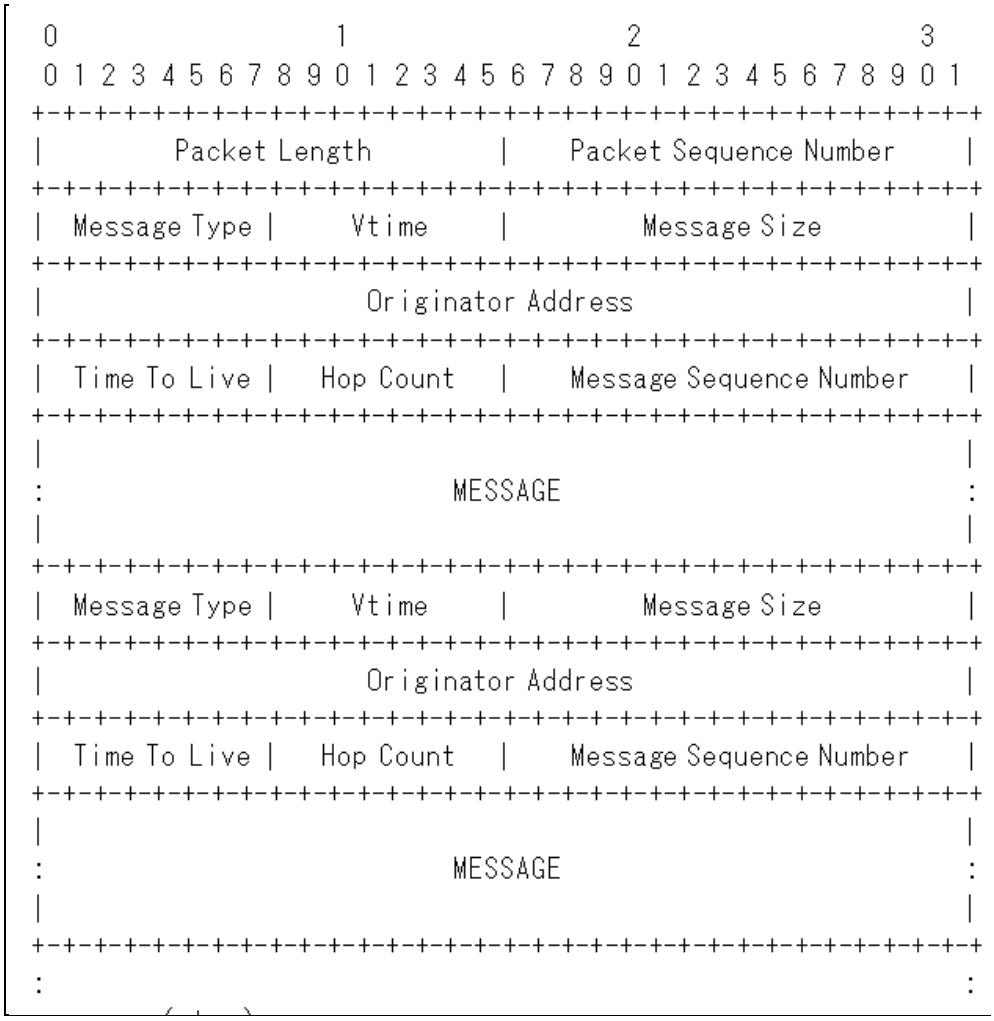

Figura 9. layout básico de qualquer pacote no OLSR
Fonte: RFC 3626 Optimized Link State Routing (2003)

Cálculo de Rota a tabela de roteamento para cada nó pode é computada usando as informações de estado do link adquirido através de periódicos de troca de mensagens, bem como a configuração da interface dos nós.

A rede é dividida, onde cada divisão tem um nó especial, que contém a tabela de roteamento para outros, os nós encaminham pacotes para o nó principal na sua rota o mesmo encaminha para outros nós principais através de nós considerados gateways até chegar ao nó de destino.

Além do funcionamento do núcleo do OLSR, há situações onde a funcionalidade adicional é desejada como: interface com protocolos não OLSR, notificações Link-layer, sensoriamento avançado, redundancia de topologia, inundações MPR reduntdantes e também situações onde um nó possui várias interfaces, algumas das quais participam outro domínio de roteamento.

3.4.2 **High Throughput Routing Protocol**

High Throughput Routing Protocol também conhecido como SrcRR é um protocolo de roteamento reativo, que utiliza heurísticas, para evitar a mudança de rotas devido à interferência entre os dados, e pacotes de roteamento. Semelhante ao *Dynamic Source Routing* (DSR) que é um protocolo de roteamento utilizado em redes sem fio *Ad Hoc*, que tem como propriedade o estabelecimento de uma rota, nó a nó, até o destino, onde todos os nós são móveis. A diferença do SrcRR está na métrica *Expected Transmission Count* (ETX) utilizada para determinação da rota ótima, que leva em conta a taxa de perda de pacotes entre os nós.

A proposta em Couto et al (2003) tem por objetivo aumentar a vazão conseguida na rede, sugerem ainda escolher rotas que diminuam o número total de transmissões no nível de enlace, ao longo do caminho. A métrica mede o número previsto de transmissões necessárias para transmitir um pacote sobre um *link*, incluindo retransmissões.

Sofreu mudanças e melhorias para ser um SrcRR mais completo, utiliza o tempo de transmissão estimado que o tornou mais tolerante a falhas, possui controle da taxa de bit, redução das oscilações, reordenação de pacotes, possibilidade de transmissão de pacotes maiores com reduzido tempo de transmissão e mais persistente.

3.4.3 **Hazy Sighted Link State Routing Protocol**

Hazy Sighted Link State Routing Protocol (HSLS), protocolo baseado em estado de enlaces tem por objetivo minimizar o custo da manutenção de uma visão consistente da rede, sua sobrecarga da rede é teoricamente ideal, sendo híbrido (pró-ativo e reativo) limita as atualizações constantes da tabela de roteamento de rede no espaço e no tempo.

A um equilíbrio projetado na frequência de atualizações e extensões a fim de propagar a informação na tabela de forma otimizada, não inundando com isso a rede ao contrário dos métodos tradicionais, e não exige que cada nó tenha a mesma visão da rede, reduzem o desperdício de capacidade de transmissão porque encontram a rota mais certa.

Possui características para lidar com os casos que são comuns nas redes de rádio, tais como as ligações unidirecionais, e na de laços-transmissão causada por

tabelas de roteamento não atualizadas. As transmissões são redistribuídas aos próximos nós sempre que uma ligação é perdida, vantajoso porque as ligações em uma rede de rádio são menos confiáveis.

Indiferente do protocolo, uma coisa a se ter em conta para que uma rede funcione sem muitos sobressaltos, que é a segurança da mesma, pois nas redes sem fio a uma maior importância quanto a isso, por serem mais vulneráveis.

4 SEGURANÇA DE REDES SEM FIO

A segurança é parte inquietante de qualquer projeto de rede, por isso deve ser muito bem analisada, existem riscos potenciais de segurança com as comunicações sem fio, uma vez que ninguém precisa de acesso físico à rede cabeada tradicional para acessar os dados, pode-se facilmente interceptar a transmissão, sem necessariamente estar no mesmo ambiente à medida que viaja via aérea.

Apresentam diversos benefícios tais como: flexibilidade, facilidade de instalação, redução do custo agregado, entre outros. Em contrapartida, apresentam diversos problemas tais como: qualidade de serviço, custo de equipamentos elevados, baixa taxa de transmissão, baixa segurança, entre outros, que devem ser cuidadosamente examinados. (BULHMAN; CABIANCA, 2006).

O padrão IEEE 802.11 fala da confiabilidade e integridade na aplicação de alguns mecanismos de segurança, em que o *Wired Equivalent Privacy* (WEP) é o responsável pela execução dos mecanismos de segurança na camada de enlace de dados. Pela insatisfação nas falhas de garantias de segurança, lançou-se o padrão *Wired Protected Access* (WAP) que tentou eliminar as falhas do WEP, ganhou grande notoriedade e já se encontra em versões bem mais avançadas como WAP 2.

O monitoramento das redes *wireless* também é importante porque ela pode detectar; clientes conectados em um dado instante com ou sem autorização de acesso, instalação de aplicativos não autorizados, dispositivos que não estejam usando WEP ou um WAP, ataques contra os clientes *wireless*, mudanças de endereços MAC, mudanças de canal e DoS (CERT, 2003).

A Figura 10 os usuários autorizados devem usar a mesma chave de criptografia. O menor nível de segurança que podem ser implantados em uma rede sem fio é o padrão WEP. WEP permite 40 *bits* ou chaves de 128 *bits* para ser inscrito tanto no ponto de acesso e os clientes para criptografar o tráfego entre o PC e o ponto de acesso.

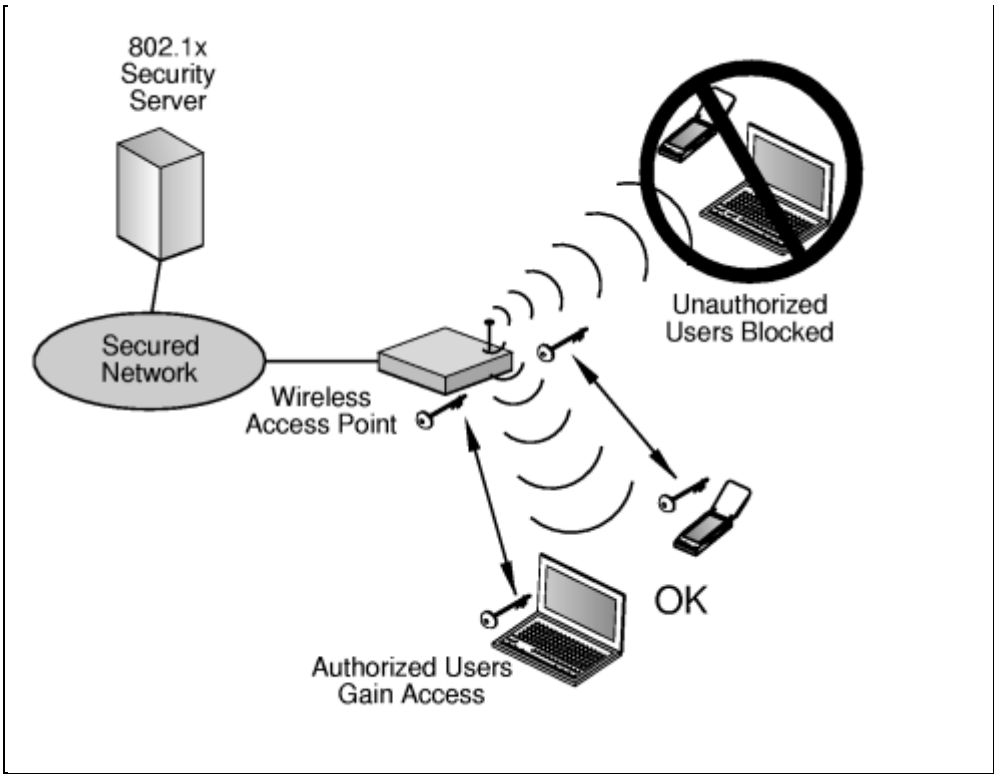

Figura 10. padrão WEP para segurança de redes Wireless
Fonte: http://docs.hp.com/en/T1428-90017/ch01s04.html (2010)

No caso particular das redes *mesh* é um tema muito importante, devido a sua fácil e simples configuração, veem se disponibilizando protocolos que garantam as comunicações, mas muitos não garantem a segurança mínima da transmissão e da informação então estas podem ser capturadas por equipamentos especiais ou dispositivos que utilizam o padrão 802.11.

Segundo Duarte (2003) a rede deve estar operante e garantir, que o sinal transmitido pela rede pode ser captado por qualquer receptor atuante na área em que o sinal estiver ativo, que os dados trafegados na rede não sejam alterados entre o receptor e o transmissor, manter a rede acessível, e fazer com que a autenticação para o acesso à rede ocorra.

A segurança da rede é normalmente obtida por meio de vários métodos de autenticação, e o *Efficient Mesh Security and Link Establishment Association* que rege o padrão 802.11s no que concerne a segurança, usa o padrão 802.11i como base que por sua vez utiliza o *Pairwise Master Key*.

A tecnologia *SecureMesh* dos sistemas *HotZone Duo* embora seja uma encriptação proprietária para os enlaces entre os nós, cumpre com os mais novos padrões de encriptação do padrão IEEE 802.11i, é desenhada para ser compatível com os métodos de segurança que estão sendo desenvolvidos como parte do padrão 802.11s.

Outro bom exemplo de segurança é o caso *WifiDog* de *open source* (Licença GNU GPL), escrito em PHP o *gateway/firewall* roda dentro do roteador, gera estatísticas de uso de banda por cliente dentro do servidor de autenticação. Aborda os aspectos de *Quality of Service* e segurança a fim de garantir que os serviços não sejam inadequadamente expostos na rede compartilhada por diferentes entidades.

Firewall, Virtual Private Networks (VPN), são também propostas de segurança necessário para o cenário da segurança de redes *mesh*, uma vez que a distribuição dos nós gerenciados define uma importante área de estudo, devido à configuração e a distribuição dos nós. Alguns casos de sucesso de redes mesh de grande porte implemantadas em algumas cidades pelo mundo.

5 **TRABALHOS CORRELATOS**

Dentre os muitos projetos de redes em malha sem fios que existem alguns merecem notoriedade, por se destacarem pela abrangência, contribuição técnica e científica, dos experimentos e em função das vantagens e do avanço proporcionado.

Dos diversos grupos de pesquisa que buscam a implementação e validação destas redes encontram-se alguns projetos como: Microsoft Research, RoofNet, VMesh, Wireless África entre outros.

5.1 MICROSOFT RESEARCH

Self-Organizing Neighborhood Wireless Mesh é o nome atribuído ao projeto com uma equipe de pesquisar sobre as redes em malhas sem fios, priorizando tecnologias que viabilizem esse tipo de rede a médio e longo prazo. Considerado de escala reduzida poucas dezenas de nós, sendo que foram realizados experimentos em apartamentos de um condomínio localizado próximo à sede da empresa e também em uma das sedes da mesma.

Com computadores dos funcionários, software que cria uma camada virtual entre a camada de enlace e a de rede e o protocolo reativo Multi-Radio Link-Quality Source Routing, concluíram que elas são viáveis e que com o desenvolvimento da indústria de hardware e dos organismos de padronização, será possível em algum tempo ter essas redes.

5.2 ROOFNET

Com o objetivo de estudar as questões envolvidas em redes sem fios de grande escala o MIT por meio do Laboratório de Ciência da Computação e Inteligência Artificial, realisou experimento com uma rede de 50 nós numa área urbana adjacente á universidade, computadores operando Linux, e uma antena, protocolo híbrido desenvolvido o chamado SrcRR combinando a técnica de *link state* e a descoberta sobdemanda.

Embora fosse preciso uma boa distribuição de nós com acesso fixo à internet, um protocolo que escalasse acima de poucas centenas de nós e um custo de hardware relativamente alto do ponto de vista tecnológico, o uso prático de redes como a RoofNet seria mais viável que implementadas na atualidade.

5.3 VMESH

O projeto desenvolvido na Universidade *Thessaly* na Grécia, e tem como objetivo implantar uma rede de baixo custo na cidade de *Volos*. A rede é formada por roteadores que funcionam no modo Ad Hoc e por elementos estacionários e móveis, tendo como objetivo fornecer a conexão de um ou mais dispositivos ao restante da rede.

O protocolo de roteamento utilizado nos roteadores é o Optimized Link State Routing pró-ativo, usuários finais são conectados aos pontos de acesso *mesh* por meio de Ethernet cabeada ou acesso WiFi.

5.4 WIRELESS ÁFRICA

O grupo Wireless África investe em formas e meios para o desenvolvimento de tecnologias da comunicação nos países em desenvolvimento para que possam ter uma informação sustentável, considera que este objetivo só pode ser alcançado por meio de softwares e protocolos não proprietários construídos sobre código aberto e utilizando a tecnologia de propriedades *mesh*.

Tendo como caso de sucesso as cidades de Pretoria e Mpumulanga na África do Sul em que a rede foi configurada como uma rede *mesh* ao ar livre, utilizado protocolo pró-ativo de roteamento nos roteadores OLSR, a fim de obter uma compreensão dos problemas que as mesmas enfrentariam do mundo real.

6 **IMPLANTAÇÃO DE UMA REDE MESH WIRELESS LOCAL**

No desenvolvimento do projeto foi preciso à utilização de alguns recursos de hardware e software, ferramentas já prontas, na implantação da rede *mesh* e observado alguns fatores que fazem deste tipo de redes muito importante tanto tecnicamente e cientificamente para a sociedade.

Pois são redes que configuradas, se organizam automaticamente, com seus nós estabelecendo uma conexão *ad hoc* e mantendo a conectividade em malha. Os roteadores formam a infraestrutura para os clientes e a malha de autocorreção e autoconfiguração da rede, permite também outras redes *wireless* ou ethernet se conectem a ela por meio de uma ligação com um roteador que suporta a tecnologia *mesh*, há ainda a possibilidade de ser ligada a Internet com o uso da função de gateway do mesmo.

Como foi explicado, utiliza-se a rede *wireless* para realizar a transferência de dados, o que torna aplicável aonde houver necessidade para a formação de uma rede local de comunicação mais robusta. O surto pela busca por serviços de comunicações e com a carente e cara infraestrutura física de telecomunicações existente para transmissão de dados esta tecnologia pode de certa forma suprir essa demanda, possibilita a criação das cidades digitais conectando centros urbanos e regiões distantes com a utilização dos roteadores *mesh* outdoor com transferências em alta velocidade o que facilmente providenciaria serviços como acesso à banda larga, automação residencial e não só, serviços de vigilância, vídeo sob demanda, entre outros.

O proposto trabalho explana um estudo da tecnológia de redes *mesh* na comunicação e transmissão de dados. Criou-se uma rede wireless LAN, com a

tecnologia *mesh Indoor*, com roteadores distribuídos em algumas partes da universidade no bloco XXI, nos laboratórios de informática, objetivando ver o funcionamento das mesmas, enxergando a transmissão de dados suas conexões, praticidade, notar ainda a possibilidade de autoconfiguração e autocorreção como características principais deste tipo de redes, entre outros.

6.1 LOCAL E ESPECIFICAÇÃO DOS EQUIPAMENTOS

A UNESC entende que a pesquisa é uma dimensão própria da Universidade, sem a qual o próprio sentido de Universidade se perde. Assim, estimula e fortalece o desenvolvimento da pesquisa nos vários níveis de sua atuação, como uma forma estratégica de garantir a sua consolidação enquanto Universidade.

Figura 11. Universidade do Extremo Sul Cartarinense.

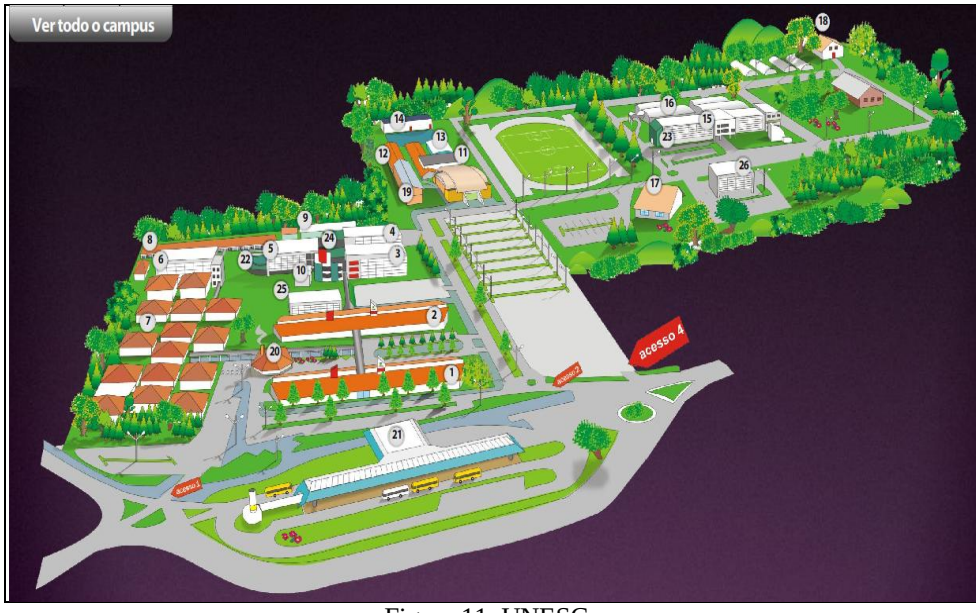

Figura 11. UNESC.
Fonte: http://www.unesc.net/testes/mapa/ (2010)

Pelo entendimento da própria universidade se utilizou as facilidades da mesma, que promove qualitativamente no que se refere ao ambiente de trabalho, possuir

em suas instalações tecnologias necessária, proporcionou um ambiente ideal para a realização dos trabalhos, que visou à criação de uma rede local *mesh*, para avaliar a aplicabilidade da tecnologia.

Para a realização dos testes com a tecnologia de rede *mesh Indoor* foram utilizados três roteadores *Wireless linksys* Figura 12 com as especificações conforme apresentada.

Figura 12.Roteador Linksys WRT54G
Fonte: homesupport.cisco.com/en-us/wireless/lbc/WRT54G (2010)

O roteador *Wireless Linksys* WRT54GS V7.2 foi adquirido em uma loja de vendas on-line de São Paulo a partir do mercado livre no dia 06 de Março de 2010, por R$ 208,59. De fabricação Chinesa, importado da fabricante com o conteúdo na

embalagem; roteador WRT54GS, CD de instalação, fonte 110V, um cabo ethernet de 1,8 metros categoria 5e com RJ 45, e manuais.

Especificações Técnicas:

a) Padrão: IEEE 802.3, 802.3u 802.11g, 802.11b;
b) Canais: 11 (US, Canadá), 13 (Europa, Japão);
c) 1 porta 10/100 RJ-45 para conexão com o modem
d) 4 portas de switch 10/100 RJ-45
e) Suporte a VPN, IPSec, PPTP Pass-Through
f) Suporte a DDNs, RIP1 e 2 e DMZ Hosting
g) Segurança: Stateful Packet Inspection (SPI) Firewall, Internet Policy, Packet Filters, WEP, WPA, Filtro de endereços MAC, não divulgação do código Wireless (SSID)
h) Todas as portas LAN suportam Auto-Crossover (MDI/MDI-X)
i) Leds: power, DMZ, WLAN, LAN (1,2,3,4/DMZ)
j) Alcance de até 100m (condições ideais)
k) Dimensões: 4,8x18,6x20cm (AxLxP)
l) Peso líquido: 48g

Os outros dois roteadores são pertencentes a estudantes da própria universidade, que também intencionam em utilizá-los para observações e testes na tecnologia *mesh*, sendo também roteadores *Wireless* da *Linksys* modelo WRT54GL e o modelo WRT54G.

No primeiro modelo observam-se as especificações técnicas com relação ao WRT54GS diferenciando-se nos quesitos: um botão Secure Easy Setup, nas

dimensões que são 18,6 x 4,8 x 15,4 cm e no peso líquido que é 371g sendo da versão 3.0.

No segundo modelo o mesmo possui as especificações técnicas semelhantes ao WRT54GS, mas com as mesmas diferenciações apresentadas pelo WRT54GL sendo que apenas de uma versão mais antiga 1.1.

Portanto, com a montagem e o funcionamento da estrutura da rede *mesh*, tornou-se possível a visualização das características inerentes a tais redes e também a realização de testes nas facilidades da universidade.

6.2 IMPLANTAÇÃO DA TECNOLOGIA

Os roteadores da *Linksys* como todos os produtos da *Cisco* traz por padrão instalado um *firmware* que é um conjunto de instruções operacionais, armazenado na memória do hardware, funcionando como o sistema operacional do dispositivo, proprietário.

Infelizmente o referido não oferece a possibilidade da criação de uma rede *mesh* ainda que a empresa ofereça a possibilidade de criação desde tipo de rede seria necessário adquirir-se este tipo de serviço.

Por isso fez-se necessário estudar antes de mais alguns roteadores existentes no mercado, para chegar a uma conclusão sobre qual usar e saber quais protocolos de roteamento de redes se adéquam ou se ajustam aos mesmos para a criação da referida rede.

Figura 13 Firmware encontrada nos roteadores da Linksys neste caso o do WRT54GS V7.2.

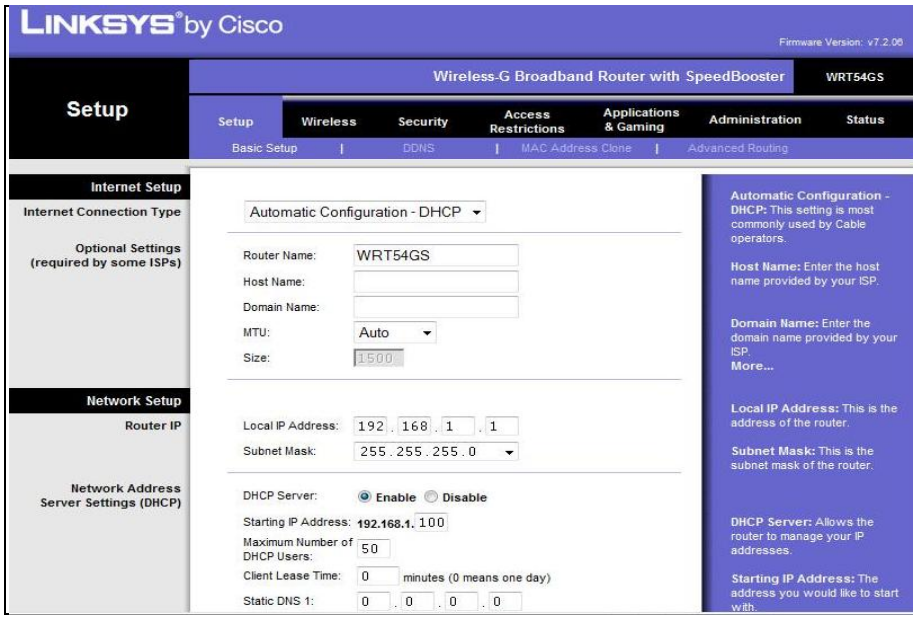

Figura 13. Firmware da Linksys

Entre os firmware mais utilizados no mercado que suportem esta tecnologia, dois se destacam, o DD-WRT e o OPEN-WRT, sem muito nem saber qual deles funciona melhor foi na base dos comentários dos utilizadores que se optou pelo DD-WRT após uma pesquisa realizada na Internet.

Para que a tecnologia pudesse estar em uso teve-se de instalar um novo firmware, que para o caso foi utilizado o DD-WRT por ser simples e fácil de instalar, fornece um grande número de funcionalidades para plataforma de hardware e ser grátis. A instalação de um firmware num roteador é conhecido como *flashing* ou *flashear*.

DD-WRT é um firmware baseado em Linux de código aberto, com uma interface gráfica bem estruturada, operacional por meio de um navegador web, adequado para uma grande variedade de roteadores WLAN e sistemas embarcados, de fácil configuração com as características principais: o suporta mais de 200 dispositivos diferentes, a funcionalidade considerada completa, suporta todos os atuais padrões de

WLAN (802.11a/b/g/n), suporte à implantação *outdoor*, suporta melhor as frequências, integração VPN, suporta vários sistemas de Hotspot, gerenciamento de banda, interface do usuário multilíngue, Figura 14 Firmware da DD-WRT instalado nos roteadores da Linksys.

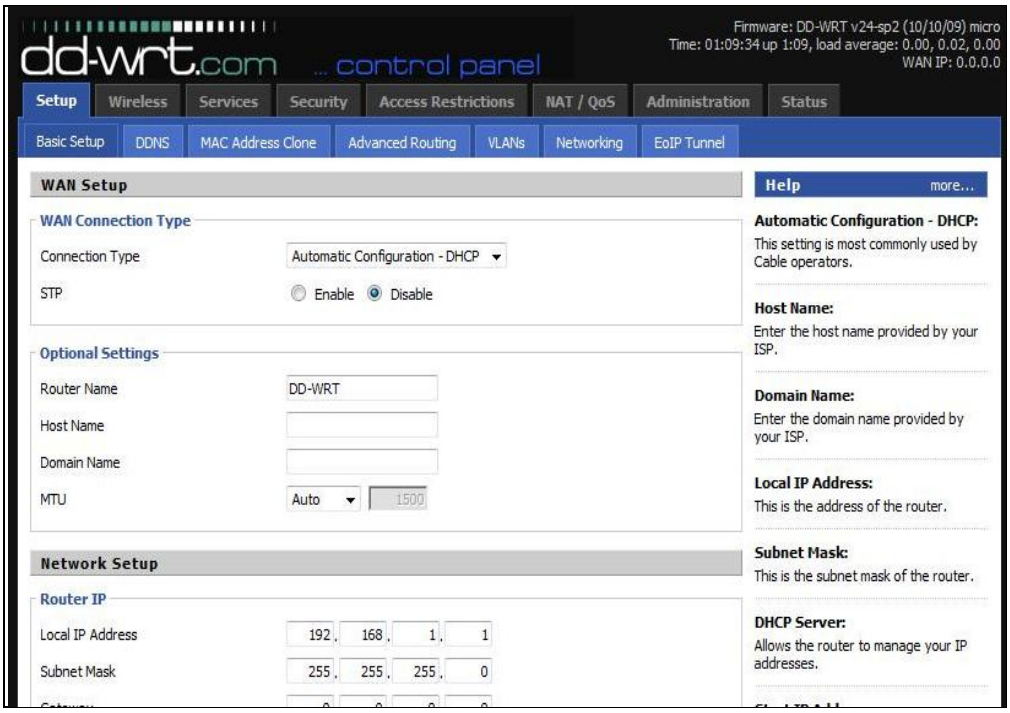

Figura 14. Setup, Firmware DD-WRT.

Instalar o DD-WRT no roteador foi bastante simples, pois com o uso do navegador facilitou de sobremaneira, pois não foi para o caso necessário à utilização do terminal com a utilização de linhas de comandos *ifconfig*, embora fizesse uma reinstalação em um dos roteadores para a abordagem do processo para aqueles mais aficionados por programação e pelo uso de linhas de comandos.

Antes de qualquer instalação normal é preciso uma atenção especial a algumas precauções, no caso a mais importante é não comprometer o roteador, tornar-lhe inútil, isso é apagar o firmware proprietário e não conseguir instalar o firmware

desejado. Salientar que se não possui nenhuma versão do DD-WRT no roteador, precisara que se rode um programa que elimine o firmware em seu roteador antes.

No site da DD-WRT, tem a página da *wiki Supported Devices* encontra-se em Inglês, possui uma lista de dispositivos suportados por este firmware, como são muitos os dispositivos que ele presta suporte, basta para tal, escrever o nome do roteador que ele mostrara exatamente caso suporte, pois que a escolha do firmware correto é extremamente importante.

Para os roteadores simplesmente pesquisou-se a marca (*Linksys*) e o modelo (WRT54 G) do roteador especificando versão do mesmo, uma vez identificado seu roteador precisamente, um clique e irá direto para a página de *dowloads* do DD-WRT e ver os arquivos necessários para este roteador específico.

Para todos os roteadores fez-se o download dos arquivos que se encontravam disponíveis, nomeadamente o *vxworkskiller_versão.bin* que serve para apagar o firmware existente no roteador, o *vxworksrevert_versão.bin* é basicamente um restaurador do último firmware existente no referido dispositivo, o *dd-wrt. _versão_micro_generic.bin* versão mais genérica do firmware necessária para este aparelho e o *dd-wrt. _versão _std_olsrd_generic.bin* que é a versão mais completa do firmware e que possibilita a criação de uma rede *mesh*, havendo ainda a ferramenta tftp.exe para os clientes usando Windows.

Após a instalação do firmware que suporta o protocolo de roteamento, e que permite roteamento *mesh*, fez-se necessário escolher exatamente o que roda em qualquer placa *wi-fi* que suporta o modo *ad hoc* e, claro, em qualquer dispositivo ethernet.

OLSR é um protocolo de roteamento para redes móveis *ad hoc*, pró-ativo, que utiliza tabela de roteamento e a técnica de inundação de mensagens, com uma estrutura fácil de manter, ampliar e portar para outras plataformas, descrita no RFC3626 é liberado sob a licença livre de código aberto *Berkeley Software Distribution* (BSD), capaz de ser incorporado a produtos proprietários, o que facilita a incorporação em projetos.

Amplamente utilizado e bem testado, funciona perfeitamente nos sistemas operacionais mais comuns, desde os proprietários aos livres até aos dispositivos embarcados, rápido, leve altamente escalável de camada 3 podendo agregar um limite de usuários, como tal um dos dois principais padrões para redes *mesh*.

Para que o protocolo OLSR funciona-se no firmware é necessário à configuração do mesmo com alguns requisitos básicos como: Em *setup*, tipo de conexão escolher a *automatic configuration* do *Dynamic Host Configuration Protocol* (DHCP) também o servidor; *Setup, Network setup* colocar o IP padrão 192.168.1.1 e o *subnet mask* pode ser da classe 255.255.255.0 o gateway o DNS a principio deixa-se em branco e as outras opções como vem por padrão.

Em *Wireless* permitir que o seu modo de rede preferencial seja o *ad hoc;* Definir o modo de *wireless network mode* como mixed; Ainda em Wireless *wireless network name* ou SSID definir o mesmo nome em todos os roteadores. O canal definir também o mesmo para todos para o caso o 6-2,437GHz; *Unbridge* o *Networking configuration;* Definir um ip e manter a máscara de rede; Adicionar a interface WLAN .

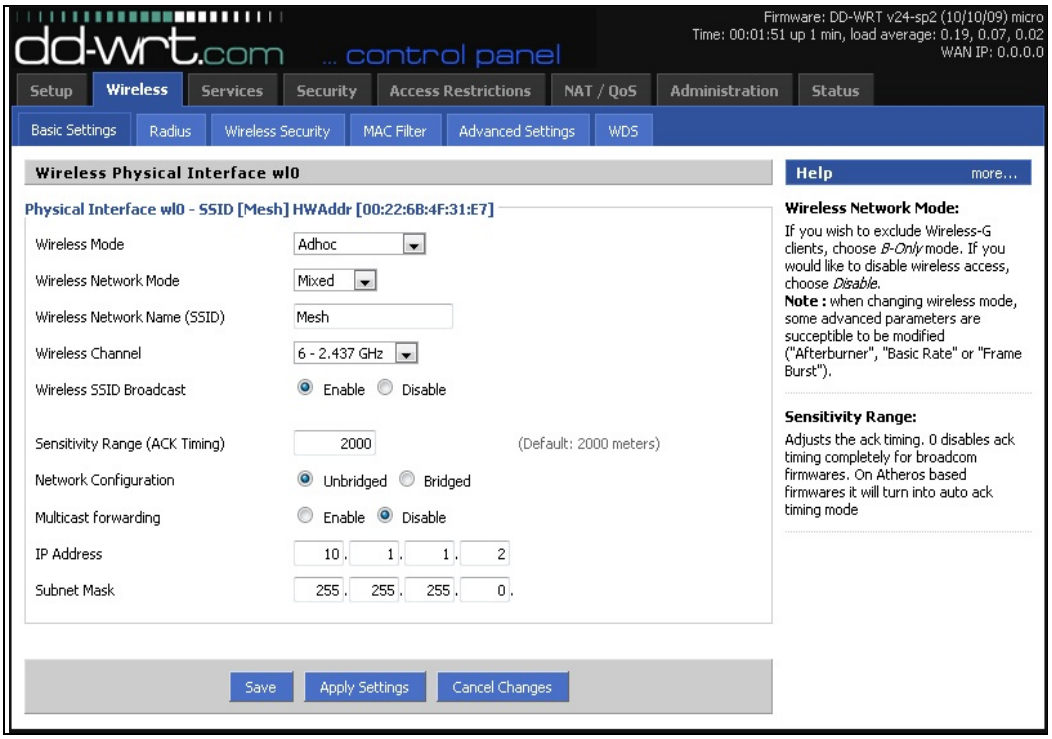

Figura 15. Aba wireless, Firmware DD-WRT

Figura 15 configurações wireless em modo *ad hoc* do firmware DD-WRT para o funcionamento da tecnologia *mesh.*

Dentro de *Setup* mas na aba *Advanced Routing* mudar o modo de operação para OLSR Router e mudar a interface para eth1 e não mexer nas outras configurações. Na aba *Networking* em *port setup*, escolher *unbridge* o eth1 atribui um IP, correspondente e manter a *subnet Mask*.

Para os computadores não esquecer que as placas wireless que alguns trazem, requer uma configuração de acordo a necessidade, tendo em consciência que a rede será como uma ad hoc deve-se ver as propriedades das configurações das placas de rede para darem suporte a tecnologia, no caso atribui-se um IP manualmente a cada microcomputador. Há a necessidade de se mexer nas configurações das placas de rede para funcionarem em modo *ad hoc*, pois a maioria dos microcomputadores teve

dificuldade em se autenticar na rede automaticamente, embora pudessem ver a existência da rede e tentar se autenticar, foi necessário fazê-lo manualmente.

6.3 SEGURANÇA DA REDE MESH

O firmware DD-WRT instalados nos roteadores suportam diferentes tipos de configurações para a segurança da rede, que podem ser selecionados a partir de algumas listas, como: SPI Firewall, WPA *Personal e Enterprise*, WPA2, WPA2 *Mixed*, *WPA Remote Access Dial In User Service* (RADIUS), WEP, Virtual LAN(VLAN), *Virtual Private Network* (VPN), possuí também filtros e bloqueio de pedido de WAN.

Garante filtros para *proxy, cookies, java applets, activex,*redirecionando *Network Address Translation* (NAT), identificador da porta (port 113) e o *Wireless MAC Filter* que permite controlar o que os dispositivos que podem se comunicar com o roteador, por meio dos seus endereços MAC, mas como padrão vem todos desativados e implementa VPN de passagem para IP *Security Protocol* (IPsec), *Point-to-Point Tunneling Protocol* (PPTP) e *Layer 2 Tunneling Protocol* (L2TP) Figura 15. Providência bloqueio de web sites por palavras chaves ou pelo próprio endereço de *Uniform Resource Locator* (URL) e também de serviços como o caso do *Peer-to-Peer* (P2P).

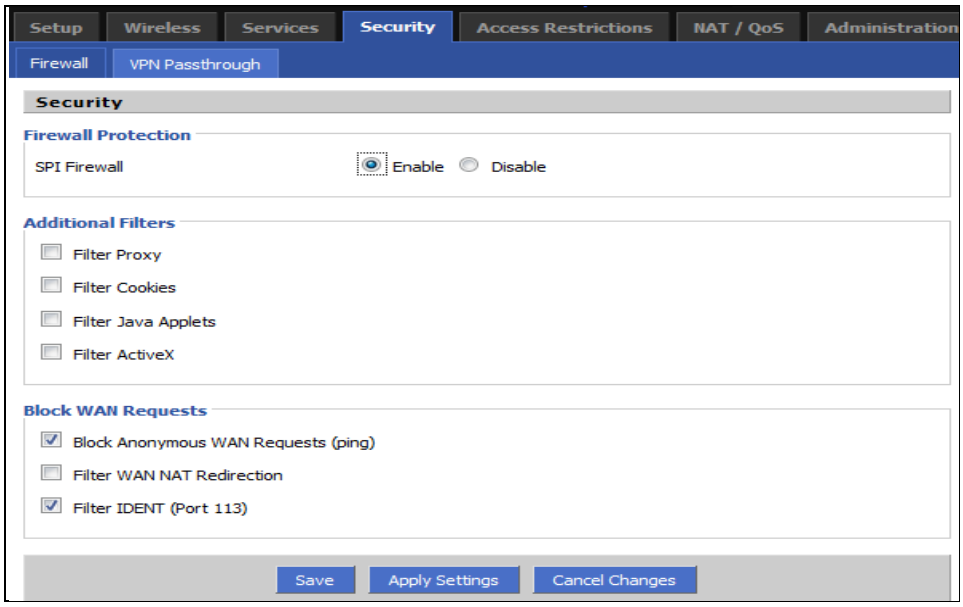

Figura 16. Aba Segurança, Firmware DD-WRT

De salientar que para o melhor funcionamento dos roteadores envolvidos na rede definirem-se iguais parâmetros de segurança para todos, iniciou-se, ativando o SPI Firewall, como medida de segurança para proteger a rede local à Internet, pois inspeciona os pacotes de dados recebidos para assegurar que correspondam a uma solicitação de saída e rejeita os pacotes não solicitados potencialmente prejudiciais, considerado mais avançado que a NAT.

No DD-WRT o RADIUS só é aceitável no modo de ponto de acesso, para a criação de uma rede *mesh* não é aceitável a utilização do mesmo pelo próprio firmware, mas não tira com isso a possibilidade de autenticação, pois ainda pode ser realizada pelos padrões WEP e/ou WAP, embora venha definido como automático por padrão que permite a qualquer sistema aberto ou autenticação de chave compartilhada seja usada.

Para sistemas abertos não é aconselhável à utilização do padrão WEP, mas a chave compartilhada pelo padrão *WAP2 personal mixed*,com o intuito de se

combinar os algoritmos *Temporal Key Integrity Protocol* (TKIP) e *Advanced Encryption System* (AES), possibilitando não só o emprego de chave compartilhada mas também de um período para a renovação da mesma.

Figura 17 aplicação do WPA 2 Personal mixed (TKIP e AES).

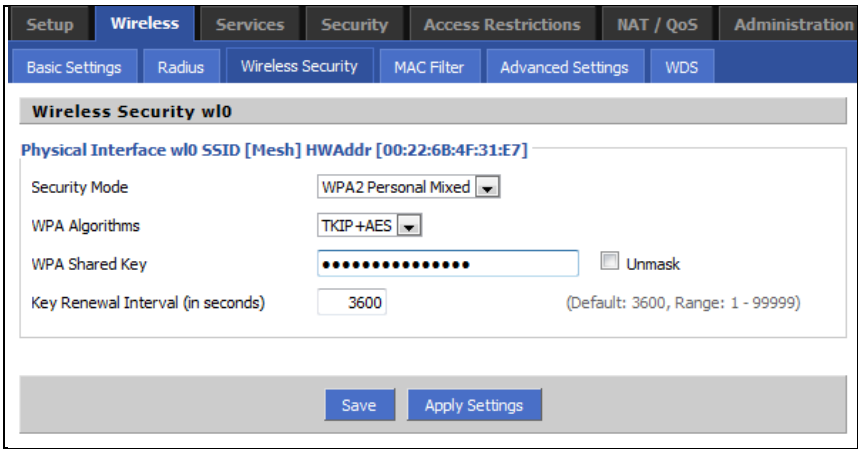

Figura 17. Wireless setup, Firmware DD-WRT

WPA2 Personal Mixed, esta sendo usado pelo simples fato de que todos os roteadores suportam este modo de segurança, uma vez que é a mistura do WAP2 com o próprio WAP que maximiza a interoperabilidade, aceita uma senha no campo chave de compartilhamento entre 8 e 63 caracteres, que pode ser renovada num intervalo de 1 a 99.999 segundos como obrigatoriedade.

TKIP emprega um tecnologia de criptografia considerada melhor e mais forte que o WEP, e se associa ao *Message Integrity Code* (MIC) para fornecer proteção contra pacote certos pacotes. AES utiliza um simétrica de 128 bits no bloco de criptografia de dados e MIC.

Necessário ter em mente que para a utilização do mesmo deve-se a aceitação de todos os roteadores, por possuírem o *WPA2 Personal Mixed*, mas para

muitos caso não é possível, mas os clientes conectados nos mesmos também terão de suportar este tipo de segurança, caso contrario seria inviável a utilização da mesma.

6.4 TESTES APLICADOS A REDE

A partir da estrutura montada foi possível à realização de alguns testes para verificar a tecnologia, os cenários desenvolvidos testam a topologias de comunicação, na mudança, variação e a distância dos nós, com isso apresenta-se e censura-se os resultados obtidos, permitindo tirar conclusões dos mesmos.

No decorrer dos testes foram os mesmos realizados com os três roteadores, mencionados no decorrer do trabalho, mas o número de microcomputadores variou de 2 a 5 microcomputadores e não foi utilizado nenhum outro dispositivo de conexão wireless que pudesse testar a sua inserção na rede.

Iniciou-se a realização de testes com simples comandos como: ping e tracert para testar a conexão entre os microcomputadores e roteadores conectados à rede. Ratificou-se que todos os pacotes enviados foram respondidos pelo microcomputador e roteadores de destino, sem a perda de pacotes.

A inclusão e remoção de nós clientes e roteadores foi testada na rede para analisar a aceitação da escalabilidade, embora não foi possível ver o limite Maximo de nós que ela possa aceitar devido à falta de microcomputadores wireless que suportassem essa tecnologia com isso se torna impossível analisar ao máximo a escalabilidade.

Figura 18 uso do comando Tracert no comand prompt do Windows, na busca do rastreamento das rotas dos nós e no número de saltos.

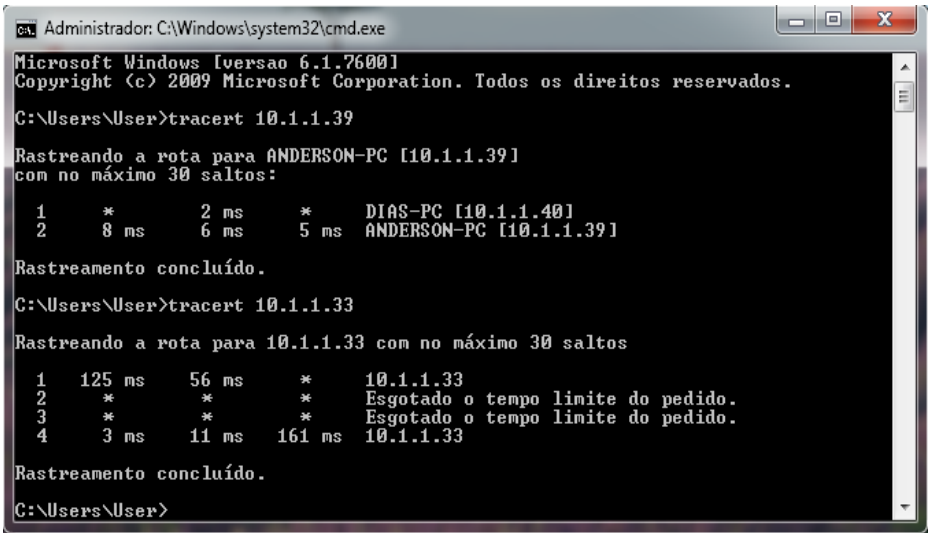

Figura 18. Command Prompt Tracert

Switch é um dispositivo utilizado em redes de computadores para reencaminhar módulos (frames) entre os diversos nós. No site da OLSR (olsr.org) está disponível uma ferramenta de nome OLSR Switch em Inglês de licença livre para teste da tecnologia e suas funcionalidades, sendo que possui para ambientes Linux e Windows.

Assim como os Switches normais ela pode gerenciar certas funcionalidades que influem no funcionamento direto das redes, mas ela serve mesmo para ver e analisar se a rede realmente é *mesh* utilizando o protocolo pró-ativo OLSR.

Figura 19 OLSR Switch, para a análise e gerencia da rede *mêsh.*

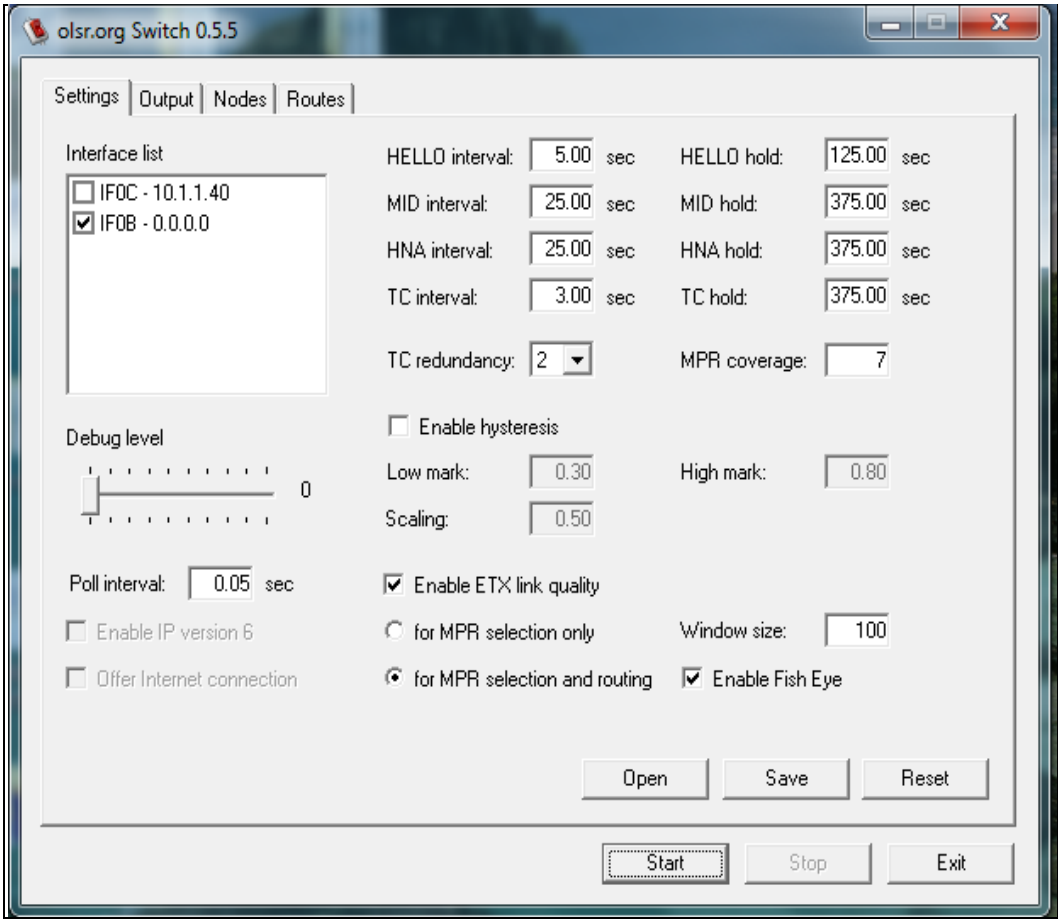

Figura 19. OLSR Switch.

Com esta mesma ferramenta além de das informações que observadas na tela principal do mesmo ainda podemos ver os resultados na aba output, que nos revela os saltos multiplos saltos dados pelos nós com ênfase no computador aonde a ferramenta esta instalada.

Os links (nós, IP's) que se encontram na rede, o nó principal de cada rota, são normalmente os roteadores, a métrica utilizada, os vizinhos de um ou dois

saltos, e faz toda a topologia de rede, mostrando as conexões dos IP's fonte e destino, Figura 20.

Na mesma ainda visualiza-se todos os endereços de IP's conectados a rede isso na aba nodes, que traz também o MPR que fazem o trabalho de retransmissão das mensagens entre os nós, possuem também a principal tarefa de rotear selecionando o melhor caminho de qualquer fonte para qualquer destino.

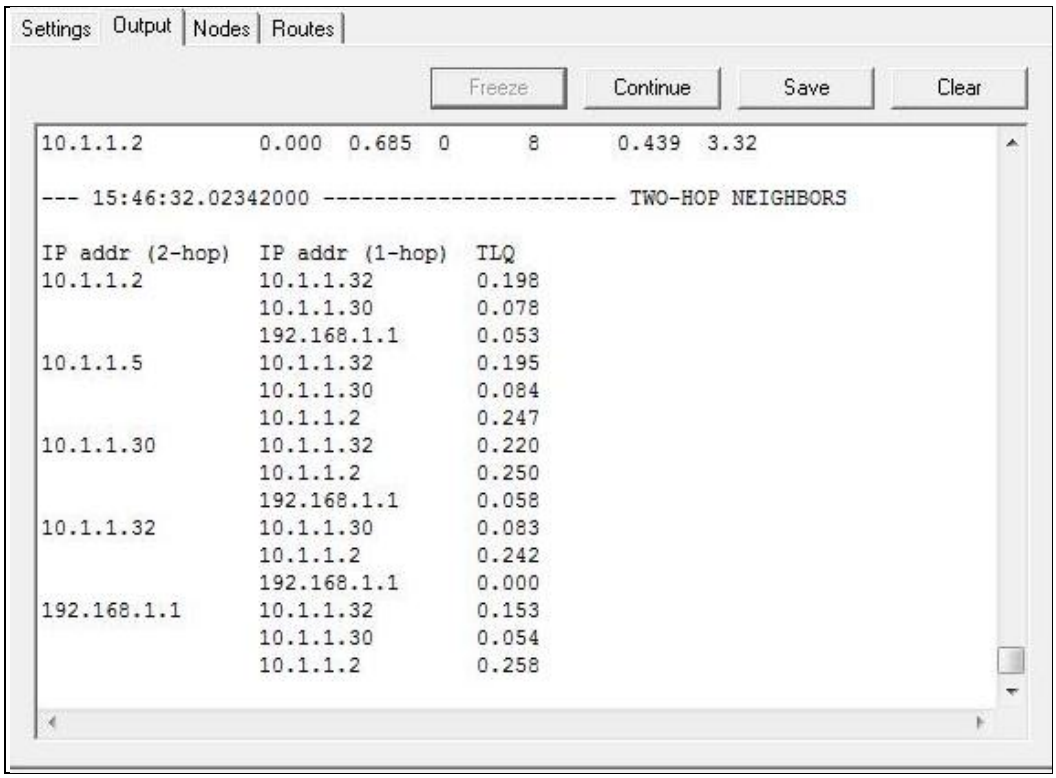

Figura 20. Output do OLSR Switch.

MID que refere-se a lista de endereços que estão a utilizar o modo OLSR difundindo mensagens. *Host and Network Association* (HNA) mostra os nós que possuem a capacidade de injetarem informações externas e contem informação apropriada para construir uma tabela de roteamento de nós.

Aba Routes traz a tabela de roteamento do nó na qual a ferramenta esta instalada, mostrando as informações como: destino, gateway, metric e a interface do mesmo.

As redes *mesh* são conhecidas por duas características, que se pode considerar como as mais importantes, quando algum protocolo que proporciona esta especialidade é concebido, a autocorreção e a autoconfiguração.

Figura 21 Nodes da rede com os respetivos MID, HNA e MPR de toda rede.

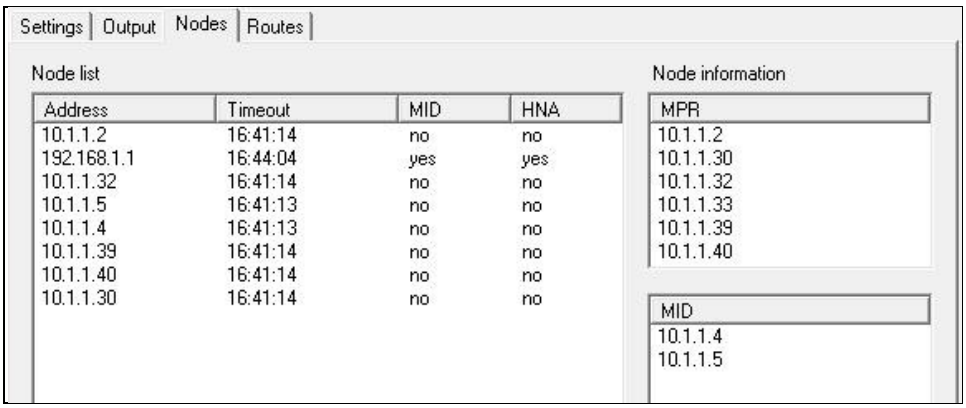

Figura 21. Nodes aba do OLSR Switch.

Autoconfiguração é a configuração automática de um dispositivo sem intervenção manual, sem nenhuma configuração de software ou de jumpers. Os dispositivos ideais de autoconfiguração seriam os equipamentos *plug and play*, que se tornaram comuns devido ao baixo custo dos microprocessadores e dispositivos embarcados.

No nosso caso a rede *mesh* para a configuração automática, configura-se primeiro os roteadores até serem considerados roteadores *mesh* que pudessem não só suportar a tecnologia, mas utilizá-la em si Figura 22, só a partir deste processo poderão fazer a autoconfiguração.

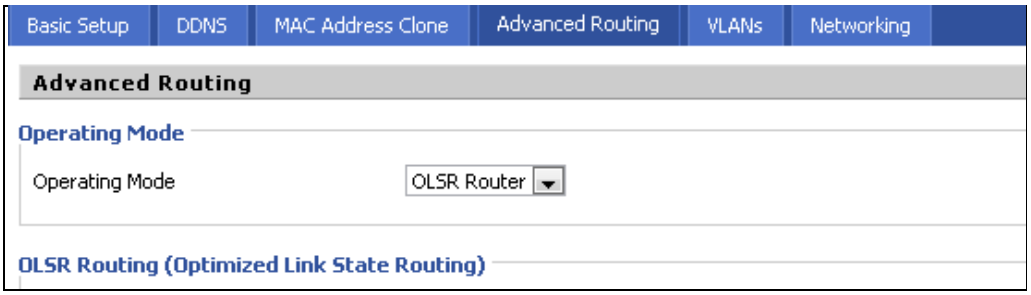

Figura 22. Modo de operação OLSR

Após estarem em modo *mesh* funcionais, elas não precisam de receber nenhuma configuração extra para se organizarem automaticamente, pois os nós estabelecerão uma conexão *ad hoc* e automaticamente manterão uma conectividade em malha.

Autocorreção é a habilidade do sistema de se reparar caso aconteça alguma falha. Em Inglês *self-healing* ou *auto recovering* que significam cura ou recuperação automática espelha melhor o que acontece nas redes *mesh*.

Entre os testes realizados para se avaliar a veracidade desta característica, após, a redes estar ligada e já operando, simulou-se uma falha geral ao desligar todos os roteadores, e os nós que utilizavam o OLSR *Switch* o que fez com que todos conectados na rede ficassem momentaneamente sem a conexão, pois logo que se volta a ligar os roteadores é foi preciso fazer absolutamente nada, para que os roteadores se encontrassem e começassem a trocar informações e atualizarem de prontidão a tabela de roteamento mostrada pelo OLSR *switch*.

Simulou-se ainda a queda de todos os roteadores, mas não em uníssono desta feita foi um por um e observa-se pelo OLSR *Switch*, à reação dos nós que estavam conectados a eles se mudarem para os roteadores mais próximos. Figura 23 mostra uma das tabelas de roteamento quando se removeu o roteador com IP 10.1.1.5.

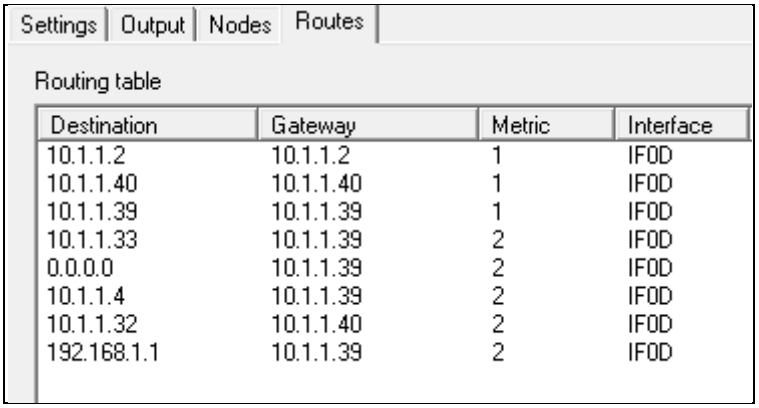

Figura 23. Modo de operação OLSR

A distância influencia na conexão ao ponto mais próximo e no caso que tiver mais de um ponto muito próximo ele (cliente), vai alternando segundo a rota que estiver menos congestionada.

Para não focar só em uma ferramenta para os testes procurou-se também utilizar o *Wireshark*, que é uma ferramenta livre, de licença *GNU General Public License* (GPL), que funciona em varias plataformas, desenvolvido pela *Ethereal*.

WireShark precisa da biblioteca WinPcap de captura de pacotes para funcionar, na maioria dos casos ela está incluída no instalador, reconhece aproximadamente 836 tipos de pacotes (protocolos) diferentes o que faz dela uma excelente ferramenta para inspecionar redes.

Ele como um analisador de protocolos, que serve para monitorar os pacotes de informações que trafegam através da rede, pode ter o controle de tudo o que sai e entra na rede sendo que no momento, é considerado um dos mais utilizados.

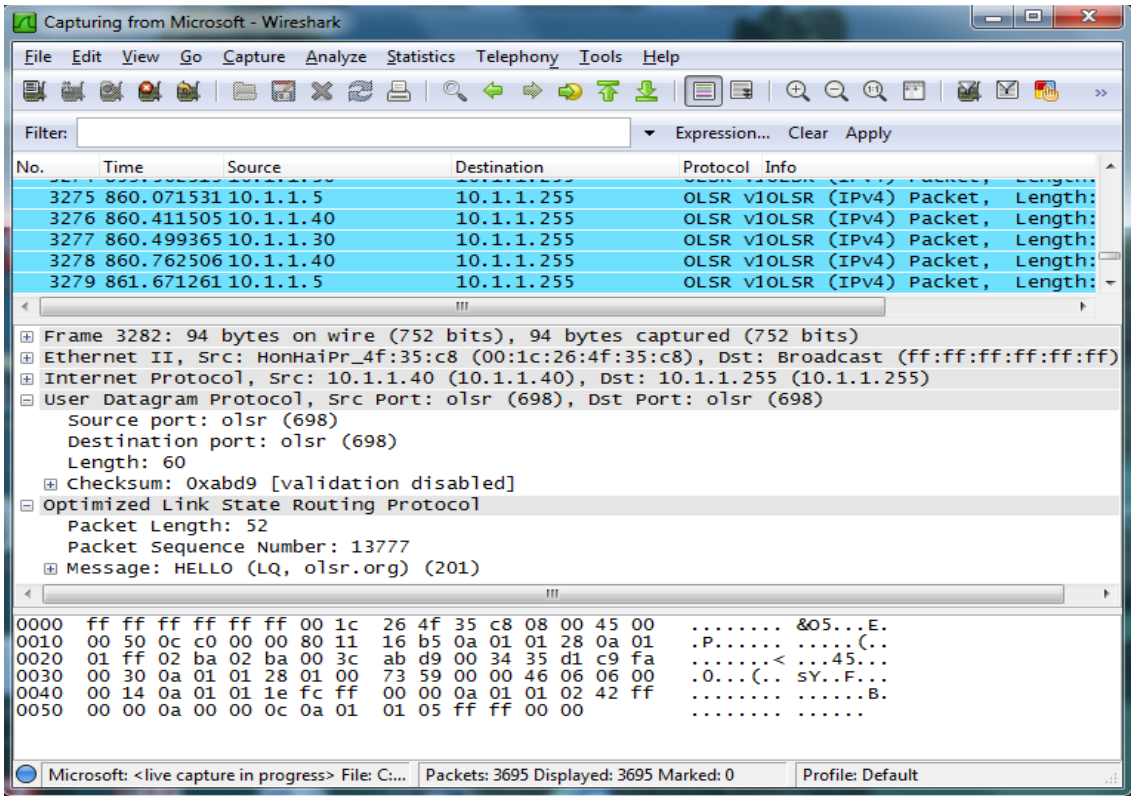

Figura 24. Wireshark

O painel superior contém a lista dos pacotes capturados, os outros dois painéis contêm informações sobre estes pacotes. No centro aparecem quatro barras com um botão (+) no lado esquerdo, clicando neste botão, as informações sob este título são mostradas Figura 24.

Observou-se na tela superior de captura informações que nos ajudam a ver a fonte, o destino, o número, o tempo e informações relevantes sobre o protocolo no caso observa-se a transmissão de pacotes pelo protocolo OLSR.

O OLSR esta a usar o protocolo de camada de transporte *User Datagram Protocol* (UDP), pois permite a escrita no pacote IPv4 ou IPv6 encapsulado, para quando for enviado ao destino ele possa receber algumas informações relevantes sobre a rede, pela troca de mensagens que é característico do protocolo OLSR, embora o UDP não garanta a chegada do pacote, pois o mesmo envia mas não faz o controle.

Durante a transmissão e captura de dados observou-se o transporte dos dados pelo processo *Unicast*, em que um pacote sai direcionado de um IP especifico a outro, *Musticast*, a informção parte de um IP especifico para um grupo de IP's específicos, mas uma coisa que chama a atenção é o processo broadcast mostrados na Figura 24 na qual todos os IP source (fonte), enviam os pacotes para basicamente toda rede. Esse processo deve-se a atualização constante que esses protocolos (OLSR pró-ativos) realizam, na sua tabela de roteamento, por isso espalham as informações para que todos os nós principais possam estar atualizados.

CONCLUSÃO

A necessidade sempre foi uma força motriz por trás do desenvolvimento humano, na busca pela solução dos seus problemas. O homem inventa, cria, melhora, evolui e transforma a tecnologia para o seu suporte. As tecnologias desde a sua criação e/ou invenção tem se transformado e melhorado para oferecer um respaldo melhor as nossas indigências.

Os equipamentos de transmissão assim como tudo têm sofrido mudanças com o passar do tempo, até ao surgimento das redes, se notabilizando este progresso pela rapidez com que ocorre, sendo viabilizadas por padrões, especificações e regulamentações. O uso de meios sem a obrigação de cabos de conexão, padrão 802.11, dá-se pela relativa melhora na velocidade de transmissão de dados, também pelo aumento da cobertura que proporcionam.

As redes wireless têm ainda outras vantagens como: os atuais baixos custos dos equipamentos, pela produção em massa dos grandes fabricantes, a redução de gastos com manutenção, preservação das instalações, não é necessário destruir alguma coisa para instalar, preservando ainda a infraestrutura e a mobilidade que oferecem, com a possibilidade de cobertura de grandes distâncias.

O estudo abordou tecnologias, padrões, características, técnicas, infraestruturas entre outros, que possuem fundamental valor para o entendimento de uma rede *mesh*, padrão IEEE 802.11s, seus protocolos de roteamento sem deixar de parte alguns aspectos relacionados à segurança de redes sem fio.

Os vários projetos nesta área demonstra o interesse dos profissionais e não só, às possibilidades e benefícios, que as redes *mesh* possam prover a sociedade,

pela possibilidade de criação de cidades digitais e a inclusão digital, como fator de agregação pela disseminação da informação, promovendo o conhecimento.

Alguns projetos de universidades, empresas e governo já tem saído do papel e estão com testes de certa forma avançados, tanto na estrutura física como em modelagem de protocolos que satisfaçam melhor as suas necessidades, ou na melhoria de protocolos abertos para se ajustarem e satisfizer os propósitos pretendidos. Por isso na maioria dos estudos nota-se a rede *mesh* como uma rede que se autoconfigura, que é um dos reais propósitos da tecnologia, que no estudo parcialmente acontece, uma vez que temos de configurar qualquer novo roteador e em muitos casos ate mesmo os clientes que se hão de conectar a rede.

Governos como no caso do Brasileiro, Americano e Sul Africano e outros estão em conjunto com Universidades investindo nessa tecnologia para prover a democratização da informação e a sedimentação do conhecimento, ajustando os protocolos e acertando os hardwares para satisfazerem as necessidades.

Os pontos positivos de qualquer rede sem fio como mobilidade e outros encontram-se presente nesta tecnologia, mas o que o torna especial é a praticidade da mesma ao se corrigir automaticamente, na mudança ou remoção de um nó sem comprometer a rede, a portabilidade dos nós dentro da malha sem precisarem se desconectar da rede quando se movem de um lado a outro, a queda da rede só é possível caso desconecta-se todos os nós na rede.

A baixa de preços dos roteadores embora seja uma coisa boa, esta na realidade dificultando de certa forma o crescimento e a disseminação das redes *mesh*, pois os roteadores que suportam essa tecnologia são muito caros comparados com os

roteadores disseminados no mercado e com isso restam apenas às empresas comerciais que oferecem os chamados pacotes *mesh* que é o roteador com o protocolo já embutido.

Outro ponto critico é o fato de existir uma boa quantidade de informação, mas infelizmente quase tudo em Inglês entre artigos e livros, mas ao que se refere a parte pratica entre instruções e informações de como fazer as coisas, não há praticamente nada de referencial aceitável nem por parte de empresas e nem universidades, o passo a passo de como fazer as coisas estão sendo guardadas a sete chaves.

A questão da vulnerabilidade na segurança foi de certa forma bem resolvida pelo firmware DD-WRT, pois oferece uma vasta gama de mecanismo para garantir a segurança da rede, sem esforço nenhum de nossa parte que tão somente bastou selecionar algumas das opções disponíveis. De salientar que protocolos de segurança bem atualizados e variados.

Hoje as redes *mesh* são a bola da vez, e embora muitos afirmem que é uma tecnologia promissora para próxima geração das redes sem fio, eu afirmo que elas são para hoje até porque existe tudo a nossa disposição para o funcionamento desta tecnologia, claro que ainda há muito espaço para um estudo mais aprofundado, mas em todas as vertentes da vida existe esse espaço.

Finalmente, o trabalho de pesquisa apresentado contribuir para a investigação e desenvolvimento, das redes *mesh*, ajudando a melhorar o sistemas de transmissão de dados atuais. Com isso pode-se sugerir como trabalhos futuros:

a) comparação e avaliação de protocolos *mesh*;

b) comparação e avaliação de firmware que suportam a tecnologia;

c) ampliar os estudos de segurança das redes *mesh*;

d) realizar estudos detalhados com a tecnologia conectando rede WAN;

e) fazer um estudo aprofundado das métricas.

REFERÊNCIAS

ABELEM, A. J. G., Albuquerque, C. V. N., Saad, D. C. M., Aguiar, E. S., Duarte, J. L., Fonseca, J. E. M., e Magalhães, L. C. S. **Redes Mesh: Mobilidade, Qualidade de Serviço e Comunicação em Grupo**. Editora da UFPA, Belém, PA, 2007.

AKYILDIZ, Ian F., XUDONG, Wang. WEILING, Wang. **Wireless Mesh Networks: a survey**, Computer Network, 47, paginas 445-487, 2005.

BICKET, John. AGUAYO, Daniel. BISWAS, Sanjit and MORRIS, Robert. **MIT Roofnet Implementation 802.11b. Mesh Network**. In: Mobicom, Agosto de 2003. Disponível em:< http://pdos.csail.mit.edu/roofnet/doku.php?id=design&s=mesh> Acesso em: 30 Outubro de 2009.

BICKET, John. AGUAYO, Daniel. BISWAS, Sanjit. and MORRIS, Robert. **Architecture and Evaluation of an Unplanned 802.11b Mesh Network**. In: Mobicom, Agosto 2005 Disponível em:< http://aib.informatik.rwth-aachen.de/2006/2006-10.pdf> Acesso em: 31 Outubro de 2009.

BREUEL, C. M. **Redes em malha sem fios**. Instituto de Matemática e Estatística, USP. Dezembro de 2004 Disponível em: <http://grenoble.ime.usp.br/movel/Wireless_Mesh_Networks.pdf> Acesso em: 30 Outubro de 2009.

BULHMAN H, CABIANCA L. **LAN/MAN Wireless III: Segurança**. Março de 2006 Disponível em: < http://www.teleco.com.br/tutoriais/tutorialrwlanman3/pagina_3.asp > Acesso em: 30 Outubro de 2009.

CERT.br. **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**. Cartilha de Segurança para internet Disponível em: <http://cartilha.cert.br/bandalarga/sec2.html >. Acesso em: 10 de Novembro de 2009.

CHEUNG, B. Patrick. **Simulation of adaptive array algorithms for OFDM and adaptive vector OFDM systems**. Virginia Polytechnic Institute and State University, Virginia, 2002.

COUTO, D. D. AGUAYO, D. BICKET, J.e MORRIS, R. **A high-throughput path metric for multi-hop wireless routing**. In MobiCom '03: Proceedings of the 9th annual
international conference on Mobile computing and networking, 2004, pages 134–146.

C.-C. Yang and L.-P. Tseng, "**Fisheye zone routing protocol for mobile ad hoc networks**,"
Consumer Communications and Networking Conference, 2005. CCNC. 2005 Second IEEE,
pp. 1–6, Jan 2005.

DAMALIO, Douglas B. **Proposta de Implementacao de Ferramenta de Autenticacao de Accesso para Redes em Malha sem Fio**. Universidade Federal Do Pará, 2008.

DANTAS, Mario. **Computação Distribuída de Alto Desempenho – Redes, Clusters e Grids computacionais**. Rio de Janeiro: Axcel Books do Brasil, 2005.

FOUROZAN, Behrouz A**. Comunicação de Dados e Redes de computadores**. 3. ed. Porto Alegre: Bookerman, 2006.

Gast, M. **802.11Wireless Networks**: The Definitive Guide. Editora O'Reilly. 2002.

HELD, G (2001) The ABCs of IEEE 802.11. In: IEEE IT Professional, Volume 3, Edição 6, Novembro-Dezembro de 2001, pp. 49 - 52

Ho, Krishna R, Kevin C. A. e Elizabeth M. Belding-Royer (2004). **A Scalable Framework for Wireless Network Monitoring**. In: 2nd ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots (WMASH). Philadelphia, PA. Setembro 2004. Disponível em:<http://moment.cs.ucsb.edu/meshnet/>Acesso em: 05 Novembro de 2009.

IEEE 802.16, IEEE Standard for Local and Metropolitan Area Networks – Part 16: **Air interface for Fixed Broadband Wireless Access Systems**, IEEE Std. 802.16, Oct. 2004 Disponível em:< http://standards.ieee.org/> Acesso em: 02 Novembro de 2009.

Intel Corp., **Understanding Wi-Fi and Wi-Max as Metro-Access Solutions**, In: Intel 2004 Disponível em: <http://whitepapers.silicon.com/0,39024759,60107942p,00.htm> Acesso em: 30 Outubro de 2009

Junior, C. Brabo, G. & Amoras, R. **Segurança em redes wireless padrão IEEE 802.11b: Protocolos WEP, WPA e análise de desempenho**. 2004 Disponível em: <http://www.cci.unama.br/margalho/portaltcc/tcc2004/carlosgustavo&romulo.pdf> Acesso em: em Abril 2010.

KUROSE, James F. e ROSS Keith W. **Redes de Computadores e a Internet – Uma abordagem top down**. 3. ed. São Paulo: Person Addison Wesley, 2006.

LUIZ, A., and Junior, O. L. **Infra-estrutura e Roteamento em Redes Wireless Mesh**. Pontifícia Universidade Católica do Paraná (PUC-PR), 2005.

Mathias M. A. e Pavão A. C. **Modulação de Sinais**. IMT - Instituto Maua de Tecnologia
2006.

MALBURG, Maria Moura. **Modulação**. Rio de Janeiro, 2004.

M. M. Farias, A. G. de Souza, D. S. Wanzeller, and A. J. F. Cardoso, "**Análise de queimadas**

na região amazônica através de redes sensoriais," in Simpósio de Informática da Região
Centro do Rio Grande do Sul, IV, Ed., November 2005..

MUNARETTO, A e FONSECA, M, **Routing and Quality of Service Support for Mobile Ad Hoc Networks**, Junho 2006.

PAIVA, Gilberto da Fonseca. **Segurança em Redes Sem Fio 802.11**. 2006. 36 f. Monografia de conclusão de curso (Especialista em Redes de Computadores e Comunicação de Dados) – Universidade Estadual de Londrina, Londrina, 2006.

Projeto UCA: **Redes sem fio Um Computador por Aluno Ministério da Educação** http://www.mec.gov.br: Universidade Federal Fluminense (UFF)

PROJETO REMESH Disponível em: < http://mesh.ic.uff.br.> Acesso em: 11 de Setembro de 2009.

PROJETO Roofnet MIT Disponível em: < http://pdos.csail.mit.edu/roofnet> Acesso em: 10 de Maio de 2010.

PRZYBYSZ, A. L.; LUIZ, O. J. **Infra-estrutura e Roteamento em Redes Wireless Mesh**. 2007. 10f. Monografia (Especialização) – Programa de Pós-Graduação em Informática Aplicada, Pontifícia Universidade Católica do Paraná, Curitiba, 2007.

RAMANATHAN, R. & REDI, J, A **Brief Overview of Ad Hoc Networks**: Challenges and Directions, IEEE Communications Magazine, Maio 2002.

ROOFNET MIT PROJECT Disponível em: <http://pdos.csail.mit.edu/roofnet> Acesso em: 31 Outubro de 2009.

Rufino, N. **Segurança em Redes sem Fio**. Editora Novatec. 2ª. Edição, São Paulo-SP. 2005.

SANTOS, Arthur R. Dos, **Wireless LAN – Projeto de Redes Locais Sem Fio.** Editora Instituto On- line Informática Ltda, Belo Horizonte 2004.

SESAY, S, YANG, Z e HE, J, **A Survey on Mobile Ad Hoc Wireless Networks**, Departamento de Telecomunicações e Tecnologia da Informação, Universidade de Ciência e Tecnologia de Huazhong, 2004.

TANENBAUM, Andrew S. **Redes de Computadores**. 4. ed. Rio de Janeiro: Elsevier, Campos. 2003.

YAN, Zhang; Mingtuo, Zhou; Shaoqiu, Xiao; Masayuki, Fujise. **An Effective QoS Scheme in WiMAX Mesh Networking for Maritime ITS**. In: International Conference on ITS Telecommunications Proceedings, Junho 2006.

WNDW **Redes sem fio no Mundo em Desenvolvimento.** 2008

ZHAO, R., Walke, B., Hiertz, G.R. **An Efficient IEEE 802.11 ESS Mesh Network Supporting Quality-of-Service**. In: IEEE Journal on Selected Areas in Communications, Novembro 2006.

REFERÊNCIAS COMPLEMENTARES

Angelo L. A. e Barbosa V. A. M. **Redes Wireless – Conceitos, Projetos e Especificações.** 2003.

BEAL, Adriana. **Segurança da informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005. 175 p.

BELLER, André ; JAMHOUR, E. ; MAZIERO, Carlos . **Defining Reusable Business-Level QoS Policies for DiffServ**. In: 15th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management, 2004, Davis. Lecture Notes in Computer Science, 2004. p. 40-51.

Draves, J. Padhye, and B. Zill, **Comparison of Routing Metrics for Static Multi-Hop Wireless Networks**, ACM SIGCOMM, Portland, OR, Agosto de 2004.

Farias, P. (2006). Redes Básico Disponível em http://www.juliobattisti.com.br/tutoriais/paulocfarias/redesbasico008.asp, consultado em
Março 2010.

KYASANUR, P., So, J., Chereddi, C., and Vaidya, N. H. **Multi-Channel Mesh Networks: Challenges and Protocols**. Disponível em: < http://www.hserus.net/ cck/pubs/wcom.pdf > Acesso em: 29 Outubro de 2009.

NORTHCUTT, Stephen et al. **Desvendando Segurança em Redes Sem Fio**. Rio de Janeiro: Ed. Campus, 2002.

PASSOS, Diego; Douglas V. T, Débora C. M, Luiz C. S. e Célio Albuquerque. **Mesh Network Performance Measurements**. In: 5th International Information and Telecommunicatios Technologies Symposium, Cuiabá, MT, Brasil, Dezembro, 2006.

PROJETO RUCA Disponível em: <http://www.midiacom.uff.br/ruca> Acesso em: 02 de Setembro de 2009.

SÊMOLA, Marcos. **Gestão da segurança da informação**: uma visão executiva. Rio de Janeiro: Campus, 2003.

SILBERCHATZ, Abraham. Galvin, Peter, B. **Sistemas operacionais – Conceitos e Aplicações**. 3. Ed. São Paulo Campus, 2001;

Silva M. W. R. **Alocação de Canal em Redes Sem Fio IEEE 802.11 Independentes** Disponível em: < http://www.gta.ufrj.br/ftp/gta/TechReports/Marcel06/tese.pdf > Acesso em: 02 de Setembro de 2010.

VLADIMIROV, Andrew; GAVRILENKO, Konstantin V.; MIKHAILOVSKY, Andrei A. Wi-Foo: **The Secrets of Wireless Hacking**. Indianápolis, Addison-Wesley, 2004.

APÊNDICE A – INSTALAÇÃO DO DD-WRT FIRMWARE NO ROTEADOR

Vamos instalar o firmware nos roteadores, generalizarei as instruções e mostrarei em passos os dois métodos diferentes que foram usados; usando um navegador web padrão e por meio de linha de comando no linux primando sempre pela utilização de softwares livres no processo.

Navegador Web padrão

a) Antes de começar aconselho a restauração do roteador para os padrões de fabrica uma vez que para o caso os roteadores foram testados de varias formas para garantir que os mesmo se encontravam em pleno funcionamento, para tal conectei ao mesmo com o Web GUI (*graphic user interface*) por meio do *Mozilla Firefox* com *Java Script* habilitado, pelo IP (*internet protocol*) padrão 192.168.1.1, na guia administração, em subaba Padrões de Fabrica, seleciona sim e cliquei em salvar configurações e continuar.
b) Abra o Navegador novamente após alguns segundos e faça logon no Web GUI, digite o endereço IP do roteador novamente 192.168.1.1 na barra de endereços do seu navegador.
c) Será solicitado nome e senha os roteadores, note que é muito importante que não se interrompa a instalação, desligando o computador, fechando o navegador ou ainda desligando o roteador durante o processo.
d) Faça o *upload* do firmware clicando na guia Administração na sub aba *Firmware Upgrade*, no botão Procurar e selecione

vxworkskiller_versão.bin, baixado previamente e clique no botão *Upgrade* as luzes do roteador piscarão e ele instalara ou apagara o firmware original, e preparara o mesmo para receber o DD-WRT micro. Uma nova página será aberta, confirmando que foi bem sucedido, esperar alguns minutos antes de clicar em Continuar.

e) Reinicie o roteador refaz o caminho até chegar em *Firmware Upgrade* novamente, faz o *Upload* do *dd-wrt._versão-micro_generic.bin* e faz o Upgrade instalando com isso a versão mais leve e genérica do firmware DD-WRT.

f) Finalmente reinicie novamente o roteador e refaça novamente o caminho até *Firmware Upgrade*, faz o Upload do *dd-wrt._versão _micro_olsrd_generic.bin* o *Upgrade* instalando com isso a versão final do *firmware* DD-WRT que suporta a criação de redes *mesh*.

Linha de Comando Linux

a) Habilitar o Telnet / SSH é recomendado para atualizar e instalar o roteador sem fio, abra o terminal e insira o comando sudo ifconfig eth0 192.168.1.1.

b) No Linux tftp usa o sudo apt-get install tftp (*Trivial File Tranfer Protocol*) ou outro equivalente como atftp.

c) Após a instalação ainda no terminal digite o comando # Tftp 192.168.1.1 modo tftp> binário, > Tftp colocar *vxworkskiller_versão.bin*, > Tftp sair.

d) Agora instala o modo genérico do DD-WRT genérico, ainda no terminal digite o comando # Tftp 192.168.1.1 modo tftp> binário, > Tftp colocar wrt.v24_micro_generic.bin-dd, > Tftp sair.

e) Finalizando instala a versão completa, no terminal digite o comando # Tftp 192.168.1.1 modo tftp> binário, > Tftp colocar *dd-wrt._versão _micro_olsrd_generic.bin*, > Tftp sair.

Apêndice B - Artigo Sobre o Trabalho

Implantação de uma Rede Mesh Wireless Local

Ferraz Augusto Diogo Manuel[1], Paulo João Martins[1]

[1]Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC)

Criciúma – SC – Brazil

ferraz_manuel@hotmail.com, pjm@unesc.net

Abstract. *The objective of this work is to propose and implement a local wireless mesh network, the study will be done within the University facilities, to improve network access to students and beyond, and to guarantee connection in places where it is not possible to connect by cables. Through wireless routers and the use of radio frequencies, the nodes will interconnect and share resources and data. Besides the equipment, the proactive routing protocol OLSR and the DD-WRT firmware that supports OLSR that was used for building and securing the network, and free software was used to test the network. Concluding it is possible to create the proposed network, as we see the technology works, and solves the problem of accumulation of cable networks, reduces deployment and maintenance costs and it is a step towards the creation of digital cities and digital inclusion.*

Resumo. *O objetivo desde trabalho é propor e implementar uma rede mesh sem fio local, como estudo de caso, dentro das facilidades Universitárias, visando melhorar o acesso a rede aos estudantes e não só, e garantir conexão em locais onde não é possível a conexão por cabos. Por meio de roteadores wireless e pelo uso de radio frequências, ha compartilhamento de recursos e dados, pela interligação dos nós. Além do equipamento, o protocolo de roteamento pró-ativo OLSR e o firmware DD-WRT que suporta o mesmo protocolo, foram usados para a construção e segurança da rede, sendo que alguns softwares livres foram usados para testar o funcionamento da rede. Conclui-se que é possível a criação da rede proposta, a tecnologia funciona e soluciona o problema de acumulo de cabos de redes, diminui os custos de implantação e manutenção e um passo para criação de cidades digitais e inclusão digital.*

1. Introdução

Apesar de ainda pouco difundida, a tecnologia de redes mesh, também conhecida como redes em malha, vem sendo apresentada como uma das possíveis soluções de comunicação sem fio.

No caso específico das redes sem fio e da tecnologia Wireless Fidelity (Wi-Fi), o termo refere-se a um tipo de estrutura no qual cada nó da rede é potencialmente um roteador. Aplicada as redes sem fio, essa topologia traz a vantagem de necessitar apenas de enlaces de curta distância entre os nós, e de oferecer muitos caminhos redundantes entre dois pontos quaisquer da rede (BICKET et al, 2005).

Existem várias propostas de algoritmos de roteamento para redes mesh dinâmicas, tanto ao nível acadêmico, quanto em equipamentos comerciais destinados especificamente à construção de redes sem fio.

As redes sem fio em geral são inseguras, segundo Kurose e Ross (2006), a definição de segurança concentrou-se primordialmente em proteger a comunicação e os recursos de rede, mas na prática a segurança de rede envolve não apenas a proteção, mas também a detenção de falhas em comunicações seguras e ataques a infraestruturas e a reação a esses ataques, então tem de haver um ciclo continuo de proteção, detenção e reação.

2. Redes de Computadores

Segundo Forouzan (2006) uma rede é um conjunto de dispositivos, denominados frequentemente de nós, conectados por links de comunicação. Um nó pode ser um computador, uma impressora ou qualquer outro dispositivo capaz de enviar e ou receber dados gerados noutros nós da rede.

2.1. Redes Sem Fio

Segundo Tanenbaum (2003) comunicação sem fio não é ideia nova, o físico Marconi demonstrou o funcionamento pela transmissão de códigos morse de um navio por meio de um telegrafo, e embora as redes sem fio tenham desempenho melhor a ideia básica ainda é a mesma.

Redes wireless tem como proposto funcionar em dois modos; na presença de uma estação base e na ausência de uma estação base. Pelo o padrão 802.11 a estação base chamada de ponto de acesso onde toda comunicação tinha de passar por ele. Quando os computadores simplesmente transmitem uns aos outros este modo é chamado de interligações de redes de acesso Ad Hoc (KUROSE e ROSS, 2009).

2.1.1. Padronização

Os padrões de redes foram criados para regulamentar as indústrias e permitir que os computadores se comuniquem assim os fabricantes e fornecedores não tem que criar a sua própria regra de concepção.

O IEEE formou o Extended Service Set (ESS) Mesh Networking Study Group (MNSG) com o objetivo de criar um protocolo padrão permitindo que os fornecedores certifiquem seus equipamentos como 802.11s, sem data de previsão para resolver a questão da capacidade, escalabilidade, onipresença e outras características relacionadas à tecnologias de transmissão para as rede mesh.

2.1.2. Infraestrutura

A utilidade de ter dispositivos conectados o tempo todo sem possibilidade de usar um cabo de rede é inegável e indiscutível, no entanto há dois modos diferentes de configurar dispositivos sem fio segundo o padrão 802.11que são Infraestrutura e Ad Hoc (RUFINO, 2005).

Infraestrutura, neste modo a transferência de dados nunca ocorre diretamente entre duas estações, existe a presença de um nó central ou ponto de acesso – Access Point (AP) por onde toda a comunicação é dirigida, inclusive comunicação entre computadores que estiverem na mesma área de serviço, permite com isso um maior controle (Gast, 2002).

De acordo com Farias (2006) as redes Ad Hoc como não possuem uma infraestrutura física, são geralmente pequenas e normalmente não possui uma conexão com a rede com cabo, não existe um limite máximo definido para o número de dispositivos que podem fazer parte dessa rede, mas o controle da mesma é de forma distribuída.

3. Redes Mesh

As redes mesh, conhecidas como redes comunitárias de acesso sem fio, podem ser usadas para reduzir o custo da "última milha" no acesso à Internet, por meio da colaboração entre nós, compartilhando um enlace com a rede fixa e permitindo uso mais eficiente da banda sem custos com cabeamento até o usuário final (BREUEL, 2004).

3.1. Arquitetura

As redes possuem diferentes arquiteturas, mas neste contexto, dois tipos de nós que podem ser encontrados nas redes mesh, no entanto elas aceitam a comunicação com outros tipos de redes e seus respectivos equipamentos.

Mesh Routers - Roteadores que possuem uma mobilidade quase nula, em muitos casos podendo ate possuir certa mobilidade formando o backbone, a infraestrutura e a malha de autocorreção e autoconfiguração da rede para os clientes.

Mesh Clientes - Os mesh clientes são uma forma de redes peer-to-peer entre os clientes onde cada estação possui capacidade e responsabilidades equivalentes, têm a habilidade de funcionar como roteadores e também como gateways caso necessário.

Mesh Routers e Clientes - A combinação dos roteadores e clientes mesh juntamente com a utilização de interfaces de redes não mesh, podem ser formadas três tipos de arquiteturas: Arquitetura Cliente, Arquitetura Infraestruturada e Arquitetura Híbrida.

3.2. Protocolos de Roteamento

Importante observar que, segundo Freitas (2001), na análise do desempenho de um protocolo, deve ser considerado o contexto topologia da rede, cujos atributos essenciais incluem: tamanho da rede, conectividade da rede, taxa de mudança de topologia, capacidade do enlace, fração de enlaces unidirecionais, padrões de tráfego, mobilidade, entre outros.

Os protocolos de roteamento ad hoc são divididos em duas categorias (SESAY, YANG & HE, 2004), quanto à construção de rotas, mas a união dos mesmos forma um terceiro protocolo, sendo eles: os reativos, os pró-ativos e os híbridos.

Os reativos ou on demand usado nas redes Ad Hoc tradicionais genéricas a descoberta da rota é sob demanda, sem ter dados para enviar, eles não atualizam as tabelas de roteamento, para enviar os reativos inundam a rede com pacotes de controle até receber uma resposta do host destinatário, assim que a rota é descoberta o pacote é enviado, isso diminui o tráfego de pacotes de controle, aumentando assim a capacidade de transmissão de dados (FARIAS ET al, 2005).

Os Pró-ativos, ou table driven, são os protocolos de roteamento baseados em tabelas de roteamento que são atualizadas com toda a topologia da rede, utilizam algoritmos específicos para calcular o caminho de menos custo, mas possuem um alto custo para manter as tabelas constantemente atualizadas devido à troca de mensagens de controle que tomam parte da capacidade de comunicação das redes (FARIAS ET al, 2005).

Híbridos, que de acordo com Yang e Tseng (2005), esses protocolos estabelecem uma zona onde se tem um conhecimento parcial ou total da topologia da rede e, caso necessite enviar alguma informação para um nó mais distante este protocolo atuaria como um protocolo on demand.

3.2.1. Optimized Link State Routing

Optimized Link State Routing (OLSR) protocolo pró-ativo mais utilizado atualmente é um dos primeiros para redes mesh, considerado como mais estável e documentado, apresentando já interfaces gráficas para configuração, uma versão otimizada do algoritmo estado de enlace puro é padronizado pelo Internet Engineering Task Force (IETF) por meio do Request for Comment (RFC) 3626.

3.2.1.1. Funcionamento e Comportamento Do Protocolo OLSR

Usa o User Datagram Protocol (UDP) na transmissão e comunicação de pacotes sendo que o port 698 lhe foi atribuído pela Internet Assigned Numbers Authority (IANA, autoridade que atribui os números na Internet) para uso exclusivo.

O OLSR esta dividido em duas partes: em um núcleo funcionalidade e um conjunto de funções auxiliares, isso para que o protocolo possa ser simples de compreender e fácil de adicionar alguma complexidade a onde for necessário adicionar alguma nova funcionalidade. O núcleo especifica o protocolo que fornece roteamento e o conjunto de funções auxiliares possibilita a adição e a compatibilidade à medida que qualquer subconjunto for adicionado ao núcleo.

4. Segurança De Redes Sem Fio

No caso particular das redes mesh é um tema muito importante, devido a sua fácil e simples configuração, veem se disponibilizando protocolos que garantam as comunicações, mas muitos não garantem a segurança mínima da transmissão e da informação então estas podem ser capturadas por equipamentos especiais ou dispositivos que utilizam o padrão 802.11.

Segundo Duarte (2003) a rede deve estar operante e garantir, que o sinal transmitido pela rede pode ser captado por qualquer receptor atuante na área em que o

sinal estiver ativo, que os dados trafegados na rede não sejam alterados entre o receptor e o transmissor, manter a rede acessível, e fazer com que a autenticação para o acesso à rede ocorra.

5. Implantação de uma Rede Mesh Wireless Local

No desenvolvimento do projeto foi preciso à utilização de alguns recursos de hardware e software, ferramentas já prontas, na implantação da rede mesh e observado alguns fatores que fazem deste tipo de redes muito importante tanto tecnicamente e cientificamente para a sociedade.

5.1. Local e Especificação dos Equipamentos

A UNESC entende que a pesquisa é uma dimensão própria da Universidade, sem a qual o próprio sentido de Universidade se perde. Assim, estimula e fortalece o desenvolvimento da pesquisa nos vários níveis de sua atuação, como uma forma estratégica de garantir a sua consolidação enquanto Universidade.

Para a realização dos testes com a tecnologia de rede mesh Indoor foram utilizados três roteadores Wireless linksys WRT54G.

Figura 1. Roteador Linksys WRT54G

5.2. Implantação da Tecnologia

Os roteadores da Linksys como todos os produtos da Cisco traz por padrão instalado um firmware que é um conjunto de instruções operacionais, armazenado na memória do hardware, funcionando como o sistema operacional do dispositivo, proprietário.

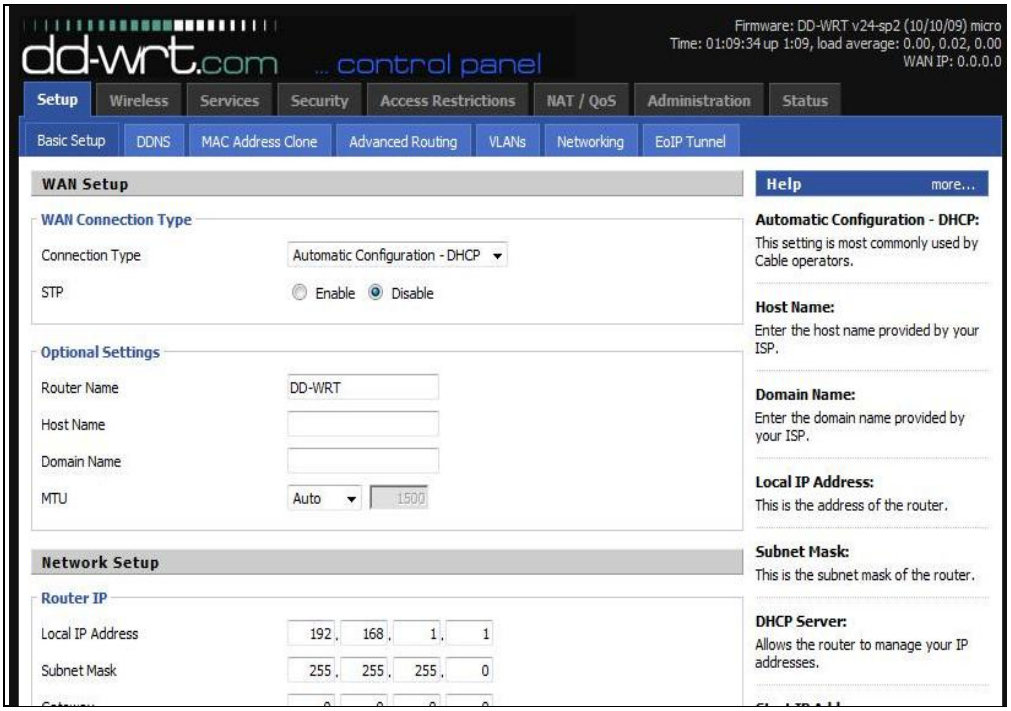

Figura 2. Setup, Firmware DD-WRT.

Para que a tecnologia pudesse estar em uso teve-se de instalar um novo firmware, que para o caso foi utilizado o DD-WRT por ser simples e fácil de instalar, fornece um grande número de funcionalidades para plataforma de hardware e ser grátis, baseado em Linux de código aberto, com uma interface gráfica bem estruturada.

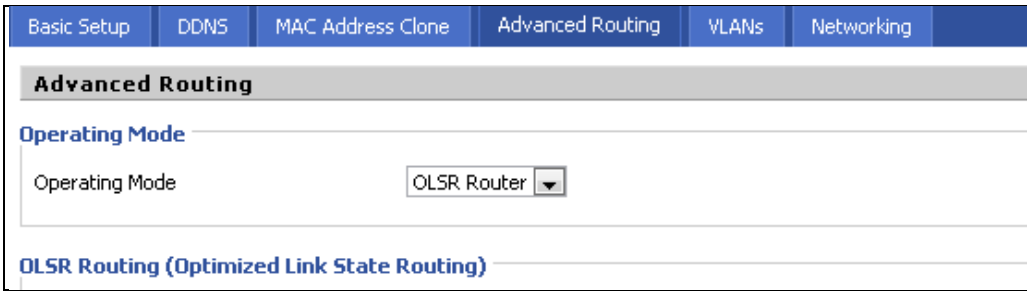

Figura 3. Modo de operação OLSR.

Para que o protocolo OLSR funciona-se no firmware é necessário à configuração do mesmo com alguns requisitos altamente necessários.

Para os computadores não esquecer que as placas wireless que alguns trazem, requer uma configuração de acordo a necessidade, tendo em consciência que a rede será como uma ad hoc deve-se ver as propriedades das configurações das placas de rede para

darem suporte a tecnologia, no caso atribui-se um IP manualmente a cada microcomputador.

5.3. Segurança

O firmware DD-WRT instalados nos roteadores suportam diferentes tipos de configurações para a segurança da rede, que podem ser selecionados a partir de algumas listas, como: SPI Firewall, WPA Personal e Enterprise, WPA2, WPA2 Mixed, WPA Remote Access Dial In User Service (RADIUS), WEP, Virtual LAN(VLAN), Virtual Private Network (VPN), possuí também filtros e bloqueio de pedido de WAN.

No DD-WRT o RADIUS só é aceitável no modo de ponto de acesso, para a criação de uma rede mesh não é aceitável a utilização do mesmo pelo próprio firmware, mas não tira com isso a possibilidade de autenticação, pois ainda pode ser realizada pelos padrões WEP e/ou WAP, embora venha definido como automático por padrão que permite a qualquer sistema aberto ou autenticação de chave compartilhada seja usada.

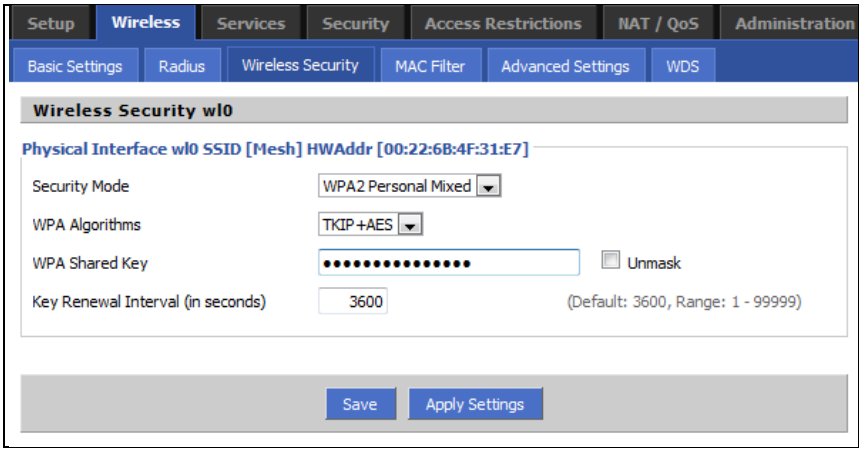

Figura 4. Wireless setup, Firmware DD-WRT.

Para sistemas abertos não é aconselhável à utilização do padrão WEP, mas a chave compartilhada pelo padrão WAP2 personal mixed,com o intuito de se combinar os algoritmos Temporal Key Integrity Protocol (TKIP) e Advanced Encryption System (AES), possibilitando não só o emprego de chave compartilhada mas também de um período para a renovação da mesma.

Necessário ter em mente que para a utilização do mesmo deve-se a aceitação de todos os roteadores, por possuírem o WPA2 Personal Mixed, mas para muitos caso não é possível, mas os clientes conectados nos mesmos também terão de suportar este tipo de segurança, caso contrario seria inviável a utilização da mesma.

5.4. Testes Aplicados a Rede

No site da OLSR (olsr.org) está disponível uma ferramenta de nome OLSR Switch em Inglês de licença livre para teste da tecnologia e suas funcionalidades, sendo que possui para ambientes Linux e Windows.

Assim como os Switches normais ela pode gerenciar certas funcionalidades que influem no funcionamento direto das redes, mas ela serve mesmo para ver e analisar se a rede realmente é mesh utilizando o protocolo pró-ativo OLSR.

Aba Routes traz a tabela de roteamento do nó na qual a ferramenta esta instalada, mostrando as informações como: destino, gateway, metric e a interface do mesmo.

No nosso caso a rede mesh para a configuração automática, configura-se primeiro os roteadores até serem considerados roteadores mesh que pudessem não só suportar a tecnologia, mas utilizá-la em si.

Entre os testes realizados para se avaliar a veracidade desta característica, após, a redes estar ligada e já operando, simulou-se uma falha geral ao desligar todos os roteadores, e os nós que utilizavam o OLSR Switch o que fez com que todos conectados na rede ficassem momentaneamente sem a conexão, pois logo que se volta a ligar os roteadores é foi preciso fazer absolutamente nada, para que os roteadores se encontrassem e começassem a trocar informações e atualizarem de prontidão a tabela de roteamento mostrada pelo OLSR switch.

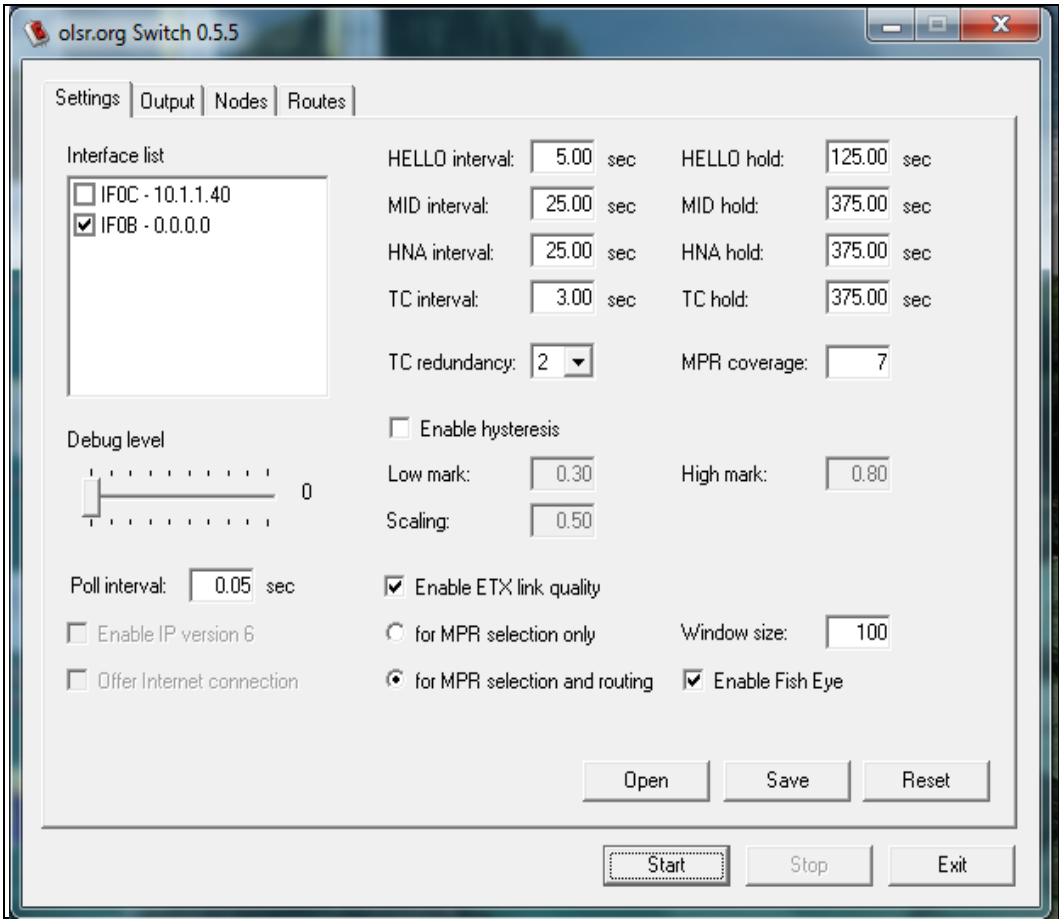

Figura 19. OLSR Switch.

Simulou-se ainda a queda de todos os roteadores, mas não em uníssono desta feita foi um por um e observa-se pelo OLSR Switch, à reação dos nós que estavam conectados a eles se mudarem para os roteadores mais próximos.

WireShark precisa da biblioteca WinPcap de captura de pacotes para funcionar, na maioria dos casos ela está incluída no instalador, reconhece aproximadamente 836 tipos de pacotes (protocolos) diferentes o que faz dela uma excelente ferramenta para inspecionar redes.

Ele como um analisador de protocolos, que serve para monitorar os pacotes de informações que trafegam através da rede, pode ter o controle de tudo o que sai e entra na rede sendo que no momento, é considerado um dos mais utilizados.

Observou-se na tela superior de captura informações que nos ajudam a ver a fonte, o destino, o número, o tempo e informações relevantes sobre o protocolo no caso observa-se a transmissão de pacotes pelo protocolo OLSR.

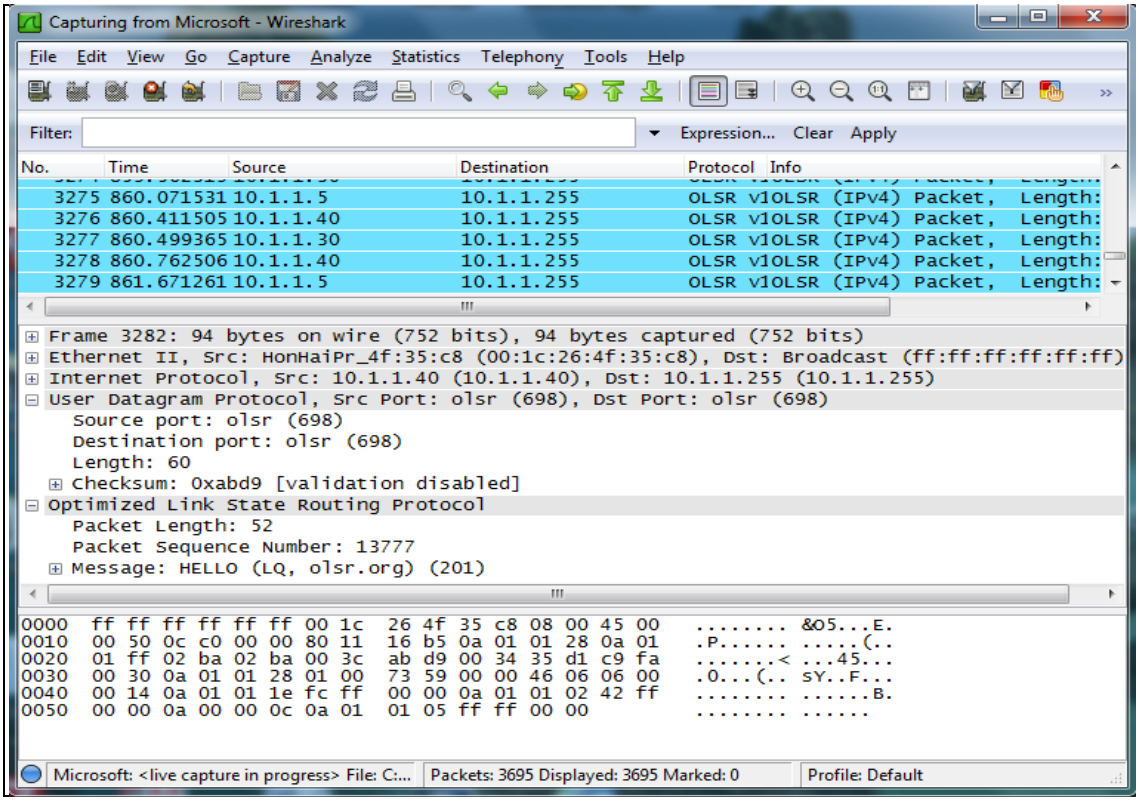

Figura 24. Wireshark.

6. Conclusão

O estudo abordou tecnologias, padrões, características, técnicas, infraestruturas entre outros, que possuem fundamental valor para o entendimento de uma rede mesh, padrão IEEE 802.11s, seus protocolos de roteamento sem deixar de parte alguns aspectos relacionados à segurança de redes sem fio.

Os vários projetos nesta área demonstra o interesse dos profissionais e não só, às possibilidades e benefícios, que as redes mesh possam prover a sociedade, pela possibilidade de criação de cidades digitais e a inclusão digital, como fator de agregação pela disseminação da informação, promovendo o conhecimento.

Os pontos positivos de qualquer rede sem fio como mobilidade e outros encontram-se presente nesta tecnologia, mas o que o torna especial é a praticidade da mesma ao se corrigir automaticamente, na mudança ou remoção de um nó sem comprometer a rede, a portabilidade dos nós dentro da malha sem precisarem se desconectar da rede quando se movem de um lado a outro, a queda da rede só é possível caso desconecta-se todos os nós na rede.

A baixa de preços dos roteadores embora seja uma coisa boa, esta na realidade dificultando de certa forma o crescimento e a disseminação das redes mesh, pois os roteadores que suportam essa tecnologia são muito caros comparados com os roteadores disseminados no mercado e com isso restam apenas às empresas comerciais que oferecem os chamados pacotes mesh que é o roteador com o protocolo já embutido.

Outro ponto critico é o fato de existir uma boa quantidade de informação, mas infelizmente quase tudo em Inglês entre artigos e livros, mas ao que se refere a parte pratica entre instruções e informações de como fazer as coisas, não há praticamente nada de referencial aceitável nem por parte de empresas e nem universidades, o passo a passo de como fazer as coisas estão sendo guardadas a sete chaves.

A questão da vulnerabilidade na segurança foi de certa forma bem resolvida pelo firmware DD-WRT, pois oferece uma vasta gama de mecanismo para garantir a segurança da rede, sem esforço nenhum de nossa parte que tão somente bastou selecionar algumas das opções disponíveis. De salientar que protocolos de segurança bem atualizados e variados.

Hoje as redes mesh são a bola da vez, e embora muitos afirmem que é uma tecnologia promissora para próxima geração das redes sem fio, eu afirmo que elas são para hoje até porque existe tudo a nossa disposição para o funcionamento desta tecnologia, claro que ainda há muito espaço para um estudo mais aprofundado, mas em todas as vertentes da vida existe esse espaço.

7. REFERÊNCIAS

BICKET, John. AGUAYO, Daniel. BISWAS, Sanjit and MORRIS, Robert. MIT Roofnet Implementation 802.11b. **Mesh Network**. In: Mobicom, Agosto de 2003. Disponível em:< http://pdos.csail.mit.edu/roofnet/doku.php?id=design&s=mesh> Acesso em: 30 Outubro de 2009.

BICKET, John. AGUAYO, Daniel. BISWAS, Sanjit. and MORRIS, Robert. **Architecture and Evaluation of an Unplanned 802.11b Mesh Network**. In: Mobicom, Agosto 2005 Disponível em:< http://aib.informatik.rwth-aachen.de/2006/2006-10.pdf> Acesso em: 31 Outubro de 2009.

BREUEL, C. M. **Redes em malha sem fios**. Instituto de Matemática e Estatística, USP. Dezembro de 2004 Disponível em: <http://grenoble.ime.usp.br/movel/Wireless_Mesh_Networks.pdf> Acesso em: 30 Outubro de 2009.

FOUROZAN, Behrouz A. **Comunicação de Dados e Redes de computadores**. 3. ed. Porto Alegre: Bookerman, 2006.

Gast, M. **802.11Wireless Networks: The Definitive Guide**. Editora O'Reilly. 2002.

Farias, P. (2006). **Redes Básico.** Disponível em http://www.juliobattisti.com.br/tutoriais/paulocfarias/redesbasico008.asp, consultado em Março 2010.

KUROSE, James F. e ROSS Keith W. **Redes de Computadores e a Internet – Uma abordagem top down**. 3. ed. São Paulo: Person Addison Wesley, 2006.

LUIZ, A., and Junior, O. L. **Infra-estrutura e Roteamento em Redes Wireless Mesh**. Pontifícia Universidade Católica do Paraná (PUC-PR), 2005.

Rufino, N. **Segurança em Redes sem Fio**. Editora Novatec. 2ª. Edição, São Paulo-SP. 2005.

SESAY, S, YANG, Z e HE, J, A Survey on **Mobile Ad Hoc Wireless Networks**, Departamento de Telecomunicações e Tecnologia da Informação, Universidade de Ciência e Tecnologia de Huazhong, 2004.

TANENBAUM, Andrew S. **Redes de Computadores.** 4. ed. Rio de Janeiro: Elsevier, Campos. 2003.

YAN, Zhang; Mingtuo, Zhou; Shaoqiu, Xiao; Masayuki, Fujise. **An Effective QoS Scheme in WiMAX Mesh Networking for Maritime ITS**. In: International Conference on ITS Telecommunications Proceedings, Junho 2006.