UNIVERSIDADE DO EXTREMO SUL CATARINENSE - UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

ANDERSON TEIXEIRA BIANCHIN

GERENCIAMENTO DE ACESSO EM REDES MESH UTILIZANDO O PROTOCOLO RADIUS

CRICIÚMA

2013

ANDERSON TEIXEIRA BIANCHIN

GERENCIAMENTO DE ACESSO EM REDES MESH UTILIZANDO O PROTOCOLO RADIUS

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

Orientador: Prof. MSc.Paulo João Martins

CRICIÚMA

2013

ANDERSON TEIXEIRA BIANCHIN

GERENCIAMENTO DE ACESSO EM REDES MESH UTILIZANDO O PROTOCOLO RADIUS

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

Criciúma, 26 de Novembro 2013.

BANCA EXAMINADORA

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

Prof. MSc. Rogério Antônio Casagrande - (UNESC)

Prof. Esp. Sergio Coral - (UNESC)

À minha família, base para todos os meus projetos e conquistas.

AGRADECIMENTOS

Primeiramente, gostaria de agradecer ao meu orientador, Mestre Paulo João Martins, pelo incentivo, dedicação, apoio e paciência ao longo dessa jornada, e aos demais professores envolvidos do Curso de Ciência da Computação - UNESC.

Aos meus pais Urinaldo e Roseni, que sempre me incentivaram nos estudos, nunca consentindo que eu o abandonasse. À minha irmã Iane que tanto admiro por sua persistência nos estudos, com certeza fonte de minha aspiração para conclusão dessa graduação.

Aos meus amigos que muitas vezes entenderam minha ausência da vida social, aos colegas de treino do Jiu Jitsu e aos clientes e companheiros de trabalho da Fine Informática.

Às pessoas que de alguma forma me auxiliaram, seja com uma palavra de persistência e incentivo ou ajuda técnica, dentre elas destaco Eder Silva, João Paulo Cardoso e Margarete Dagostim.

“Há momentos em que a maior sabedoria é parecer não saber nada.”

Sun Tzu

RESUMO

As redes de computadores têm colaborado de forma incessante para um melhor aproveitamento dos recursos computacionais. As redes cabeadas possuem um papel extremamente importante no que se diz respeito à confiança e rapidez na troca de informações, porém os padrões das redes sem fios estão emergindo como uma nova tendência. A diversidade de dispositivos móveis no mercado está exigindo novas tecnologias de conexão em ambientes de diferentes perfis. O objetivo no emprego das tecnologias wireless está além da mobilidade, propõe-se uma área de cobertura maior que a convencional, acompanhada de segurança e velocidade no tráfego de dados. Abordam-se aqui os seguintes aspectos das redes: modelos de redes guiadas (fios), funcionamento dos padrões sem fios, aspectos de segurança nas redes wireless, extensão das mesmas através do padrão Mesh e aplicação de uma camada de segurança. Utilização dos conceitos de *Authentication, Authorization and Accounting* (AAA) em uma rede visível a um grande número de pessoas, empregando o protocolo/servidor RADIUS para autenticação desses possíveis usuários. Os testes empregados na rede em malha com autenticação centralizada foram totalmente positivos em relação à autenticação, conectividade e mobilidade. O protocolo OLSR se mostrou funcional, realizando o papel de escolha do melhor trajeto para encaminhamento das requisições, inclusive as solicitações de acesso requeridas pelos clientes.

Palavras-chave: Wireless.Rede Mesh.OLSR.AAA.RADIUS.

ABSTRACT

Computer networks have collaborated relentlessly for a better utilization of computational resource. Wired networks have an extremely importance about the reliability and speed of exchange information, but the patterns of wireless networks are emerging as a new trend. The diversity of mobile devices in the market is demanding new connection technologies within different profiles environments. The purpose of the use of technologies is beyond of the wireless mobility, propose a coverage area greater than conventional, combined with security and speed in data traffic. Some of the aspects of the networks are: network models guided (wires), wireless standards operations, security aspects in wireless networks, extending the same through the Mesh protocol and applying a layer of security. Using the concepts of Authentication, Authorization and Accounting (AAA) in a visible network to a large number of people, using a RADIUS protocol/server for authentication of these possible users. Tests used in the Mesh network with centralized authentication were totally positive about for authentication, connectivity and mobility. The OLSR protocol was functional, performing the role of choose the best path to forward the requests, including requests for access required by supplicants.

Keywords: Wireless.Mesh Network.OLSR.AAA.RADIUS.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
AM	Amplitude Modulation
AODV	Ad hoc On-Demand Distance Vector
AP	Access Point
APT-GET	Advanced Packaging Tool
BATMAN	Better Approach To Mobile Ad-hoc Networking
BSS	Basic Service Set
CCK	Complementary Code Keying
CD-ROM	Compact Disc Read-Only Memory
CHAP	Challenge-Handshake Authentication Protocol
DARPA	Defense Advanced Research Projects Agency
DHCP	Dynamic Host Configuration Protocol
DSDV	Destination Sequenced Distance-Vector
DSR	Dynamic Source Routing
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ESSID	Extended Service Set Identification
FHSS	Frequency Hopping Spread Spectrum
FM	Frequency Modulation
FSR	Fisheye State Routing
FTP	File Transfer Protocol
HR-DSSS	High Rate Direct Sequence Spread Spectrum
IAS	Internet Authentication Service
IBSS	Independent Basic Service Set
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPV6	Internet Protocol Version 6
ISM	Industrial, Scientific and Medical

LAN	Local Area Network
MAC	Media Access Control
MAN	Metropolitan Area Network
MANET	Mobile Ad hoc Networks
MIMO	Multiple Input and Multiple Output
MIT	Massachusetts Institute of Technology
MPR	Multi Point Relay
MS-CHAP	Microsoft Challenge-Handshake Authentication Protocol
NAS	Network Access Server
OFDM	Orthogonal Frequency Division Multiplexing
OLSR	Optimized Link State Routing
PAP	Password Authentication Protocol
PEAP	Protected Extensible Authentication Protocol
PING	Packet Internet Grouper
PPP	Point to Point Protocol
PPTP	Point to Point Tunneling Protocol
RADIUS	Remote Authentication Dial In User Service
RERR	Route Err
RREP	Route Reply
RREQ	Route Request
SSID	Service Set Identification
SSL	Secure Sockets Layer
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
XOR	Exclusive-Or
ZRP	Zone Routing Protocol
WAN	Wide Area Network
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WMN	Wireless Mesh Network
WPA	Wi-Fi Protected Access

WRP	Wireless Routing Protocol

SUMÁRIO

1 INTRODUÇÃO

Redes de computadores têm contribuído muito para disponibilização de conteúdos de pesquisas e recursos computacionais, sem elas não teríamos de maneira rápida informações e notícias em nível mundial ou até mesmo um dispositivo de impressão por departamento.

As redes são elaboradas em diferentes tamanhos e padrões, pode ser ela uma rede doméstica de dois computadores, uma empresa com centenas deles ou ainda uma rede mundialmente conectada por milhares desses dispositivos, a Internet. Além do tamanho, outra particularidade são os meios físicos por onde ela transmite os dados, algumas por cabeamento físico e outras por ondas eletromagnéticas (TANENBAUM, 2003).

As redes sem fio vêm evoluindo com rapidez e segurança, sempre se pautando nos padrões que são estudados e desenvolvidos por pesquisadores e empresas da área. Elas proporcionam inúmeros benefícios ao usuário, como o já consagrado compartilhamento de recursos computacionais, acesso em lugares onde não há possibilidade de instalação de cabos de rede, economia de recursos de hardware, mobilidade de dispositivos e portabilidade dos equipamentos de rede.

As redes wireless possuem diversos padrões, porém utilizam-se do ar para sua propagação de sinal e geralmente possuem uma estrutura do tipo centralizada, onde todos os dados enviados de um cliente ou nó precisam passar por um centralizador até chegar ao seu destino (KUROSE; ROSS, 2010).

As redes Mesh, também denominada Redes em Malha, quebram esse paradigma de centralização da rede, fazendo com que cada nó possa ser um cliente ou concentrador, tudo dependerá da topologia aplicada (AKYILDIZ; WANG, 2005, tradução nossa).

Redes em malha podem operar do mesmo modo que uma rede *Ad hoc* (fim específico), onde um dispositivo pode se conectar a outro sem a necessidade de um *Access Point* (AP), ou ainda havendo apenas um nó da rede com acesso à Internet, os outros conseguem chegar até esse por meio de saltos entre os demais dispositivos dessa rede (RUBINSTEIN, 2006).

Embora seja de grande importância o acesso à Internet via rede Mesh, não se pode deixar de salientar que esse pode ser obtido por qualquer dispositivo

que esteja ao alcance da mesma. Uma política de segurança deve acompanhar a implantação dessa a fim de evitar futuros aborrecimentos (SANTOS, 2012).

Fundamentado no âmbito da segurança da informação, propõe-se aplicar um dos critérios de segurança no ingresso à rede Mesh por meio de um protocolo de autenticação, autorização e auditoria, conhecido comercialmente como *Remote Authentication Dial In User Service* (RADIUS). Com a implantação de um servidor RADIUS, pode-se prevenir o acesso de equipamentos não autorizados, os que degradam a performance do link e ainda aqueles que causam inoperância da rede.

1.1 OBJETIVO GERAL

Implementar um servidor centralizado de controle de acesso em uma rede Mesh sem fios.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos desta pesquisa consistem em:

a) compreender aspectos gerais de redes de computadores;
b) estudar e descrever os protocolos de roteamento em redes Mesh;
c) implementar segurança no nível de acesso utilizando servidor RADIUS;
d) realizar integração de controle de acesso em redes Mesh;
e) realizar testes de acesso à rede Mesh.

1.3 JUSTIFICATIVA

Atualmente as redes sem fio estão presentes nos mais variados ambientes, não sendo vista exclusivamente só no meio corporativo, como há algum tempo atrás; devido a seu baixo custo e facilidade de implementação, ela se difundiu propiciando inúmeros benefícios sejam como um atrativo para seduzir clientes ou até mesmo como uma ferramenta de facilitação para o estudo e pesquisa.

Um tipo de rede sem fio com alto poder de cobertura também denominada rede Mesh ou Rede em Malha, está sendo utilizado dentro e fora do país, seja em locais de difícil acesso para na instalação da rede com cabeamento ou até mesmo

em locais próximos à universidades como fonte de projeto de pesquisa e/ou contribuição social (ALBUQUERQUE et al, 2005).

Alguns exemplos bem sucedidos de rede em malha estão ativos na Universidade do *Massachusetts Institute of Technology* (MIT) nos Estados Unidos, onde atende uma área de 4 Km² e possui centenas de computadores conectados. No Brasil existem alguns projetos de sucesso, como na cidade de Satarém-PA, lá foi desenvolvido um projeto em 2012 disponibilizando acesso à Internet aos moradores, onde antigamente só era possível com uso de satélite devido sua falta de infraestrutura.

O projeto ReMesh foi implantado na Universidade Federal Fluminense, sendo que em sua primeira fase de implantação, contemplou apenas alunos, professores e funcionários. Em testes de transferência de dados realizados na sua rede externa, foi obtido um resultado bem satisfatório, superando expectativas quanto à estabilidade.

Segundo Albuquerque et al (2005), os benefícios de uma rede em malha são coberturas maiores além das redes sem fio existentes que necessitam de um cabo em cada nó para retransmitir o sinal, só que esse cabeamento não é mais necessário em todos os nós da rede em malha.

A ampliação da rede em malha implica, teoricamente, em maior número de clientes na mesma, que por sua vez pode degradar o desempenho ou até mesmo chegar a um nível tão elevado de tráfego de dados e ocasionar interrupção dos serviços.

Em redes sem controle de acesso a possibilidade de pessoas mal intencionadas se infiltrarem para causar algum problema é muito comum. As redes em malha embora contribuam muito para mobilidade no acesso à informação, podem apresentar uma deficiência no controle de acesso.

O uso de uma camada de proteção, como a senha, não é totalmente suficiente nas redes sem fio, pois assim que esta é descoberta pelos outros usuários sem acesso à mesma, a rede passa a aceitar esse dispositivo que até então não estava autorizado. De acordo com as políticas abordadas em CERT.br (2012), o compartilhamento de uma senha para muitos usuários compromete a rede, tornando-a frágil e passível de ataques externos; nas redes sem fios o mesmo ocorre pois não existe impedimento físico para acesso à mesma.

O conceito de um servidor centralizado de autenticação é atribuir o acesso apenas para os usuários autorizados, mesmo que haja o compartilhamento da senha a negação do acesso pode ocorrer se a máquina não for a autorizada. O bloqueio é umas das funções dos servidores de *Authentication, Authorization and Accounting* (AAA), no caso o RADIUS; pois ainda consegue-se definir o que essa máquina vai utilizar e por quanto tempo ela vai usufruir do recurso liberado (NAKHJIRI, 2005, tradução nossa).

1.4 ESTRUTURA DO TRABALHO

O trabalho é composto por seis capítulos. O primeiro deles expõe a definição do problema encontrado, o objetivo geral, objetivos específicos que se pretende alcançar e uma justificativa para elaborar esse tema proposto. No segundo abordamos os aspectos das redes segundo seus padrões e topologias, bem como uma visão ampla das características primordiais das redes sem fios e os possíveis riscos de segurança encontrados nela.

O terceiro capítulo é sobre tecnologia de redes em malhas (Mesh), explanando seu funcionamento e peculiaridade. No trabalho descrevemos os protocolos constituintes dessa topologia assim como os *firmwares* compatíveis com esses protocolos. O quarto capítulo descreve o funcionamento básico de um servidor de AAA, no caso o RADIUS, e seus benefícios.

Quinto capítulo fala dos trabalhos correlatos na mesma linha de pesquisa e seus resultados. O sexto e último capítulo apresenta o trabalho desenvolvido, as técnicas empregadas, configurações e resultados obtidos.

2 REDES DE COMPUTADORES

Uma rede de computador se define por dispositivos conectados entre si através de um enlace de comunicação e comutadores de pacotes, com propósito de troca de dados (KUROSE; ROSS, 2010).

A relevância de uma rede de computadores se baseia em outros fatores, segundo Stemmer (2010) a importância se dá ainda pela confiabilidade do sistema, redução de custos e compartilhamentos dos recursos computacionais disponíveis.

Uma rede de computadores é constituída de um número ilimitado, mas finito, de módulos com processador capaz de trocar informações e partilhar recursos através de um meio de comunicação, não sendo necessário um sistema operacional único, mas que os envolvidos sejam cooperativos (SOARES; LEMOS; COLCHER, 1995).

As redes ultrapassaram a barreira do meio acadêmico, onde foram concebidas, e se fazem presentes em diversos meios, seja em uma casa com dois dispositivos conectados, um pequeno escritório com dezenas deles ou até mesmo uma empresa de porte internacional na qual possui centenas de computadores conectados acessando o mesmo ambiente corporativo.

A Internet é um dos exemplos mais bem sucedidos no que se refere à redes de computadores, pois nela encontra-se uma formidável quantidade e variedade de equipamentos conectados, diferentes sistemas operacionais, bem como inúmeras tecnologias de conexão e protocolos de troca de dados, tudo funcionando em perfeita harmonia.

2.1 PADRÕES

Segundo Tanenbaum (2003), as redes foram evoluindo em número de dispositivos e principalmente na área física que os envolvia, sendo necessário designar uma classificação conforme essa distância entre os nós. Essa classificação engloba diferentes tipos, os mais comuns são *Local Area Network* (LAN), *Metropolitan Area Network* (MAN) e *Wide Area Network* (WAN).

Na tabela 1 podem-se comparar as distâncias médias entre os processadores dos dispositivos da rede e observara qual categoria elas são pertencentes.

Tabela 1 – Classificação de processadores interconectados por escala.

Distância entre Processadores	Processadores localizados no (a) mesmo (a)	Exemplo
1 m	Metro quadrado	Personal Area Network
10 m	Sala	Local Area Network
100 m	Prédio	Local Area Network
1 Km	Campus	Local Area Network
10 Km	Cidade	Metropolitan Area Network
100 Km	País	Wide Area Network
1000 Km	Continente	Wide Area Network
10.000 Km	Planeta	Internet

Fonte: Adaptado de Tanenbaum (2003, p. 29).

2.1.1 Local Area Network (LAN)

A Rede de Área Local (LAN) é caracterizada por conectar dispositivos em uma pequena distância, geralmente estes estando na mesma sala, prédio ou até mesmo prédios bem próximos (STEMMER, 2010).

Em meados da década de 1990 Soares, Lemos e Colcher (1995) definiam a LAN como uma rede de características singular, onde somente nelas ocorreriam altas taxas de transferência de dados, baixa ocorrência de erros e pequena área de abrangência; mas previam que esses predicados seriam suscetíveis à evolução das tecnologias que existiam na época.

A Rede de Área Local é geralmente empregada para uso privado e em uma pequena área com no máximo algumas centenas de metros, no qual possuem algumas unidades de processamento compartilhando informação e/ou outros recursos comuns a esses, podendo ser uma impressora ou uma unidade de CD-ROM.

2.1.2 Metropolitan Area Network (MAN)

Rede de Área Metropolitana de acordo com Forouzan (2006) constitui uma interligação de dispositivos no nível de cidade, como por exemplo, uma empresa que possui várias filiais distribuídas e distanciadas dentro de uma cidade com alguns quilômetros quadrados. Pode-se considerar ainda uma empresa de

televisão a cabo ou um provedor de Internet como uma MAN, baseado na definição anterior.

2.1.3 Wide Area Network (WAN)

Uma rede que se estende por uma extensa distância, geralmente centenas de quilômetros ou até mesmo entre países de continentes diferentes são classificadas como redes geograficamente distribuídas, ou WAN conforme descrito por Tanenbaum (2003).

Os computadores de uma mesma rede onde a matriz localiza-se no Brasil e suas filiais em países vizinhos estão interconectados de tal modo que são considerados parte integrante de uma rede de longa distancia ou WAN (STEMMER, 2010).

Algumas das diferenças entre uma WAN e uma rede local estão na velocidade de transferência de dados, atraso entre as conexões e o fato de redes geograficamente distribuídas possuírem aparelhos mais complexos, como o comutador de pacotes; esse equipamento é responsável por garantir a entrega das informações de uma ponta à outra (COMER, 2006).

2.2 REDES SEM FIOS

Rede popularmente conhecida pelo nome de wireless ou ainda *Wireless Local Area Networks* (WLAN), onde as transmissões dos dados entre os dispositivos não se dão por meio de cabos, mas sim por ondas eletromagnéticas transportadas através do ar (MORAES, 2010).

Os primeiros experimentos na transmissão sem fios datam do inicio do século XX, onde um físico chamado Guglielmo Marconi conseguiu transmitir algumas instruções de código Morse entre um navio em alto mar e uma estação na costa terrestre (TANENBAUM, 2003)

Quando comparada com as atuais redes (guiada com cabo), elas se tornam uma alternativa muito atraente, pois eliminam custo de infraestrutura para acomodar cabos e são facilmente rearranjadas em caso de mudança de ambiente. A conveniência de não necessitar conectar um cabo em um dispositivo móvel, torna a wireless uma opção atrativa entre os usuários.

Na tabela 2 demonstra-se o comparativo entre algumas tecnologias que utilizam o ar como meio de transmissão; a velocidade média difere conforme o padrão de frequência empregado entre os componentes da rede.

Tabela 2 – Tecnologias de comunicação sem fios.

Tecnologia	Área Cobertura	Velocidade Média	Sistema Transmissão e Frequência
IrDA	4 m	4 Mbps	Infravermelho / Direcional
Bluetooth	10 m	3 Mbps	Radiofrequência / 2.4 GHz
Ronja	1,5 Km	10 Mbps	Óptico / Direcional
Wi-Fi	100 m	300 Mbps	Radiofrequência / 2.4 – 5 GHz
WiMAX	7 Km	1Gbps	Radiofrequência / 3.5 GHz
Mesh	Indefinido	54 Mbps	Radiofrequência / 2.4 – 5 GHz

Fonte: Adaptado de Held (2005, tradução nossa) e Gast (2002, tradução nossa).

O padrão estabelecido para comunicação sem fio nomeado de 802.11é composto por um *Basic Service Set* (BSS), área em comum (célula) para conexão dos dispositivos onde são cobertos e controlados por um AP. Encontra-se ainda o *Independent Basic Service Set* (IBSS) nesse modelo que faz o controle de transmissão são os próprios componentes da rede ou pode-se configurar um deles para fazer o gerenciamento (MORAES, 2010).

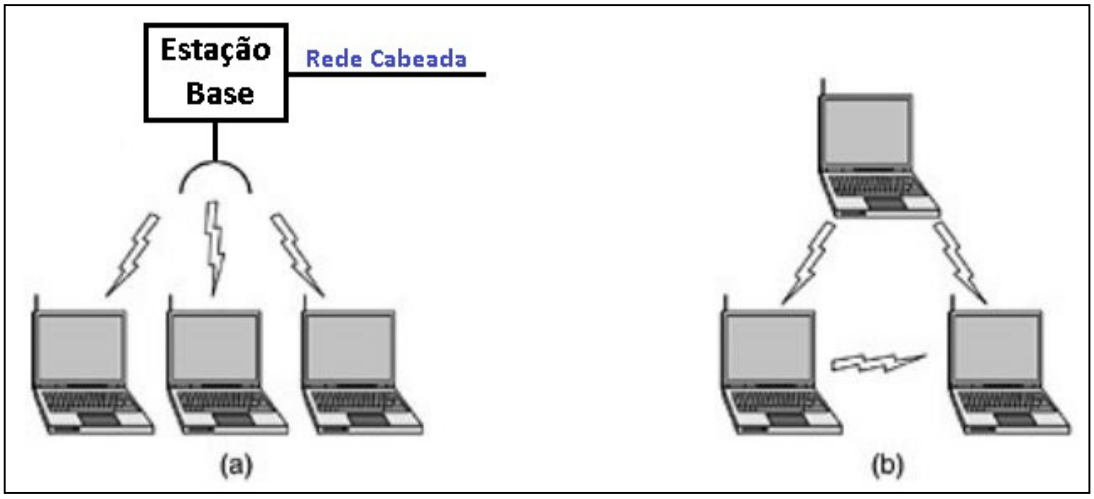
Muito popular na atualidade, as redes wireless estão presentes em vários ambientes privados e públicos; em uma casa onde se tem um notebook ou um *tablet* é indispensável o uso da tecnologia que não necessita de fios conectados aos dispositivos. Além da notável mobilidade que ela proporciona, outro fator é a facilidade de adicionar nós na rede sem que se instalem cabos por dentro de paredes ou dutos.

Para que houvesse uma compatibilidade dos diferentes fornecedores de produtos wireless foi criada a *Wireless Ethernet Compatibility Alliance* (WECA), uma associação que testa e certifica esses produtos que atendam os requisitos exigidos para operar com qualquer fabricante. Esse consórcio é formado por mais de 70 fabricantes e tornaram o padrão conhecido comercialmente com o nome de *Wi-Fi* (MORAES, 2010).

As redes wireless funcionam por meio de duas topologias fundamentais, conforme ilustradas na figura 1, uma quando utiliza uma estação-base para conectar

todos os nós participantes da mesma rede, também conhecida como rede de **Modo Infraestruturado** e a outra cuja ligação entre eles é administrada pelos próprios dispositivos, denominada **Rede Ad hoc** (fim específico) (KUROSE; ROSS, 2010).

Figura 1 – Rede sem fio com estação base - Infraestruturada (a) e Rede Ad hoc (b).



Fonte: Adaptado de Tanenbaum (2003, p. 68).

Em Moraes (2010) usa-se a analogia de células para as redes de topologia estruturada, sendo o limite dessa o alcance do sinal transmitido pelo AP. Na rede de fim específico não existe a presença de um concentrador para interconectar os dispositivos, o que a torna uma rede totalmente dinâmica e não fixa, competindo a esses a função de gerência de roteamento de pacotes e gestão de energia.

2.2.1 Padrões

Na mesma época em que os notebooks se tornaram elementos de ambientes corporativos, houve um grande anseio por parte dos usuários em ligar seus equipamentos e simplesmente estar conectado automaticamente na Internet, sem a necessidade de instalar fios de rede; baseados nesse desejo surgiram grupos de pesquisas para a concepção de uma rede na qual não precisaria mais de fios (TANENBAUM, 2003).

Na década de 1990 muitos padrões de redes sem fios foram criados, porém um deles que se destacou e está presente até hoje é o *Institute of Electrical*

and Electronics Engineers (IEEE) 802.11, popularmente conhecido como Wi-Fi, esse modelo foi aperfeiçoado com o passar do tempo e serviu de base para os demais, outra característica do Wi-Fi é que ele utiliza faixas de frequência que não necessitam de licença para seu funcionamento (KUROSE; ROSS, 2010).

Alguns problemas ocorreram quando diferentes empresas começaram a desenvolver seus projetos de equipamentos sem fios, como não havia um padrão estabelecido naquela época ocorreram incompatibilidades entre as marcas, tornando inviável o funcionamento da rede entre aparelhos de diferentes fabricantes (TANENBAUM, 2003).

A tabela 3 ilustra os padrões IEEE 802.11 desenvolvidos e suas principais características de funcionamento, salientando que alguns destes trabalham com mecanismos em modo composto, como o 802.11a/b ou 802.11b/g/n, para se adequar padrões mais antigos ou atuais.

Tabela 3 – Especificação dos principais protocolos IEEE 802.11.

Tecnologia	Frequência GHz	Velocidade Mbps	Ano Padronização	Características
802.11	2.4	1-2	1997	Primeiro padrão criado (1997), após sete anos de estudo.
802.11b	2.4	11	1999	Amplamente utilizado por provedores de serviço de Internet.
802.11a	5.8	54	1999	Livre de interferências comuns. Opera em frequência gratuita.
802.11g	2.4	54	2003	Possui mecanismos de autenticação, como o WPA.
802.11n	2.4/5	54-600	2009	Utiliza mais de uma antena para aumento de transmissão de dados.
802.11s	2.4	11/54	Em estudo	Criado para estabelecer padrões de comunicação em redes Mesh.
802.11ac	5	1000	Em estudo	Em desenvolvimento, porém com alto poder de transmissão de dados.

Fonte: Adaptado de Moraes (2010) e Stallings (2005).

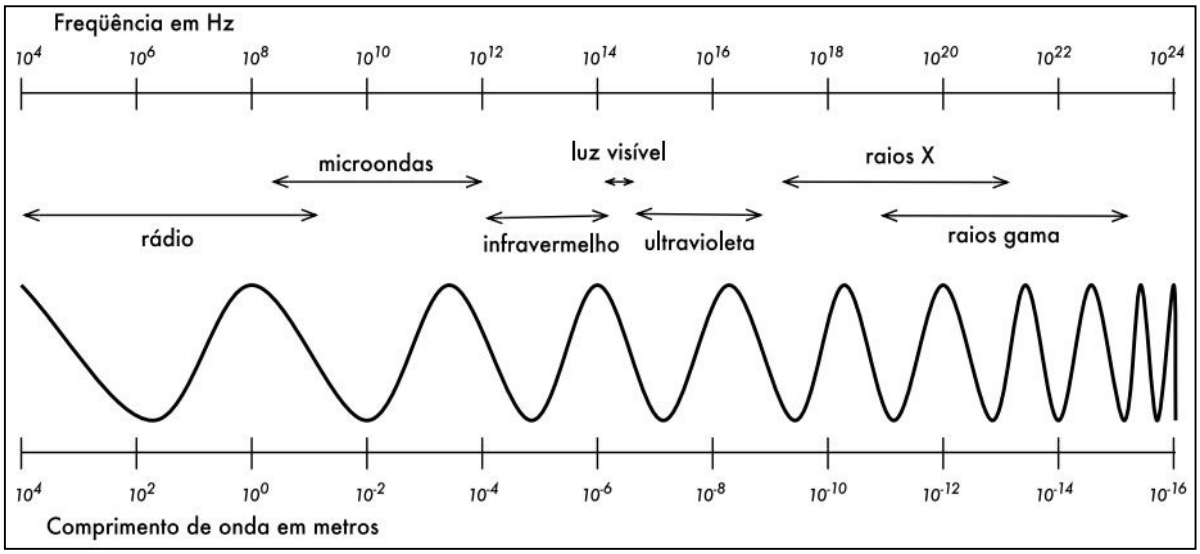
2.2.2 Ondas

É um pulso energético que se propaga por um meio; embora carregue energia, ele não transporta matéria. Uma onda pode se propagar em meios físicos, como o ar, fio, água ou até mesmo no vácuo, comprovadamente o caso das ondas eletromagnéticas (RAPPAPORT, 2009).

As propriedades de uma onda são o seu comprimento, frequência e velocidade. O comprimento está relacionado a um ponto qualquer dessa onda até o momento seguinte em que ela torna ao mesmo ponto dando inicio a uma nova onda. A frequência é a quantidade de ondas geradas em um determinado intervalo de tempo. Sua velocidade se dá pela multiplicação da frequência que ela ocorre por seu comprimento de onda (IDRC, 2008).

Na figura 2pode-se mensurar o comprimento da onda baseado na sua frequência. É possível ainda acompanhar quais comprimentos de onda não são visíveis ao olho humano. Todas as frequências possuem uma utilização específica, sejam para equipamentos de comunicação ou até mesmo equipamentos médicos.

Figura 2 – O espectro eletromagnético.



Fonte: IDRC (2008, p. 14).

2.2.3 Frequências

Os elétrons ao se deslocarem pelo ar ou até mesmo no vácuo criam ondas eletromagnéticas; conforme a quantidade desse evento ocorre em um determinado tempo, denomina-se de frequência e quantifica-se em Hertz ou Hz (TANENBAUM, 2003).

Os padrões de redes wireless se diferenciam, além de sua velocidade de transmissão de dados, por frequência de operação. A tecnologia 802.11a padronizada em 1999 pela IEEE opera na frequência de 5.8 Gigahertz (GHz);

enquanto o padrão do mesmo ano definido como 802.11b opera em 2.4 GHz. Essas diferenças de faixas de frequências são devido a alguma melhoria da tecnologia ou até mesmo por leis federais em que será utilizado o equipamento.

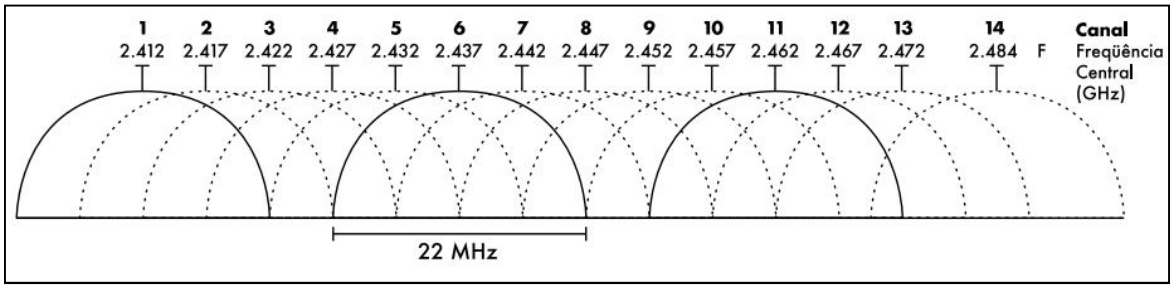
Dispositivos de uso comum em escritório e lar podem atrapalhar o desempenho das redes wireless, pois operam na mesma de 2.4 GHz; por essa não necessitar de qualquer autorização para seu uso, se faz presente em eletrodomésticos, telefone sem fios, mouse/teclado sem fios e alguns dispositivos Bluetooth (KUROSE; ROSS, 2010).

2.2.4 Canais

São subdivisões das divisões da frequência, ou seja, uma determinada faixa é fracionada para que haja a comunicação em paralelo com outros concentradores e não cause interferência em outros canais (RUFINO, 2011).

Os canais de radiofrequência estão presentes em equipamentos do nosso cotidiano, que acaba por vezes ficando despercebido, um bom exemplo são os canais de televisão e rádio (AM/FM). Eles são categorizados devido às diferentes faixas de frequência. Na rede sem fio também se observa a presença de canais como segue na figura 3.

Figura 3 – Canais e frequências centrais para o 802.11b.



Fonte: IDRC (2008, p. 15).

O padrão 802.11b utiliza frequência de 2.4 GHz, que vai de 2.4 a 2.485 GHz, esse escopo de 85 MHz é dividido em 11 canais que se sobrepõe parcialmente, no Japão são utilizados mais dois canais acima; para que diferentes canais não sejam sobrepostos parcialmente, eles devem estar separados por mais

quatro canais, ou seja, o canal 1 não interfere no canal 6 assim como o canal 3 não sobrepõe o 8 ou acima (KUROSE; ROSS, 2010).

2.3 MODULAÇÃO DE FREQUÊNCIA WIRELESS

O *Spread Spectrum* é uma tecnologia de modulação bem resistente a interferências e ruídos, ela preenche toda a faixa de frequência, o que torna mais fácil sua detecção; embora degrade a banda, ela possui maior integridade e capacidade em relação ao transporte dos dados. Ela foi concebida inicialmente para uso militar na década de 1950, vindo então a ser utilizada nas redes wireless décadas depois (RUFINO, 2011).

O IEEE definiu alguns padrões de codificação e transmissão por radio frequência sobre a norma 802.11, entre eles estão *Frequency Hopping Spread Spectrum* (FHSS) e o *Direct Sequence Spread Spectrum* (DSSS). Após alguns anos houve a necessidade de desenvolver outras técnicas cujo benefício principal era aumentar o transporte de dados, entre elas surgiram *Orthogonal Frequency Division Multiplexing* (OFDM) e o *High Rate DirectSequence Spread Spectrum* (HR–DSSS) (TANENBAUM, 2003).

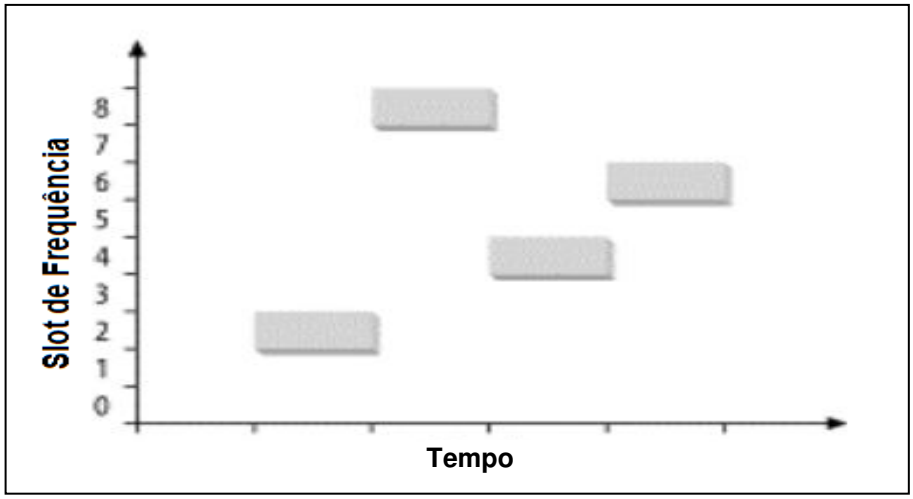
2.3.1 Frequency Hopping Spread Spetcrum (FHSS)

Espalhamento Espectral por Saltos de Frequência ou *Frequency Hopping Spread Spetcrum* (FHSS) é um dos métodos utilizados para transmissão com rádio frequência nas bandas *Industrial, Scientific and Medical* (ISM), garantindo assim certa privacidade nos dados trafegados (SOARES; LEMOS; COLCHER, 1995).

Esse método realiza a divisão da banda em diferentes canais e envia os dados a um receptor em um canal e em uma sequência de tempo pré-determinada, após o envio desses dados, ele salta para outro canal e continua a emissão, caso seja necessário. Com esse método é muito difícil a interceptação das informações, uma vez que somente o transmissor e o receptor conhecem o padrão dos saltos, o que pode ser de forma fixa ou aleatória (FOROUZAN, 2006).

Na figura 4 observam-se os pacotes sendo transmitidos em frequências diferentes conforme o tempo transcorre, essa mudança de modulação caracteriza-se por saltos pré-estabelecidos entre transmissor e receptor.

Figura 4 – Modulação por Salto de Frequência.



Fonte: Adaptado de Gast (2002, p. 171).

De acordo como exposto em Gast (2002, tradução nossa), o FHSS foi amplamente utilizado devido o baixo valor de custo e não necessitar de equipamentos com grande poder de transmissão. No inicio a principal vantagem era utilizar modulação por frequência de saltos, pois várias redes poderiam atuar no mesmo ambiente sem que houvesse conflito e com alta taxa de transferência.

2.3.2 Direct Sequency Spread Spectrum (DSSS)

Direct Sequency Spread Spectrum ou sequência direta de espalhamento do espectro é outra técnica de difusão que para cada bit a ser enviado ele substitui por uma sequência aleatória de *N* bits, que é de conhecimento do receptor. Essa técnica também é empregada na banda de 2.4GHz como o FHSS (FOROUZAN, 2006).

O conjunto de bits a ser enviado é criado por um gerador de números que ainda aplica a técnica lógica de *OU Exclusivo* (XOR) nesses mesmos bits; a banda de frequência utilizada é ajustada para *N* vezes mais larga do que seria necessário para transmitir a sequência original. Esse método faz o sinal parecer uma espécie de ruído para o interceptor que não possui a sequência gerada pelo emissor (PETERSON; DAVIE, 2004).

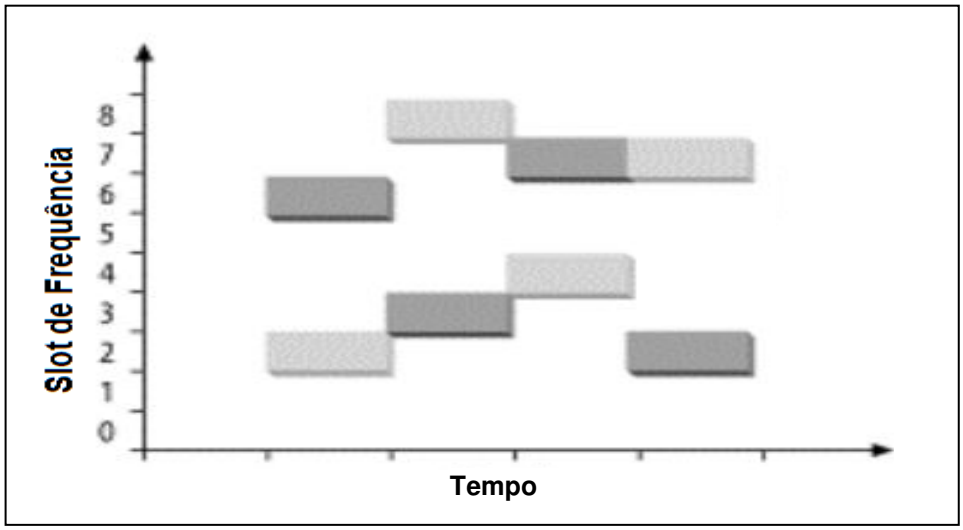
2.3.3 Orthogonal Frequency Division Multiplexing (OFDM)

Multiplexação ortogonal por divisão de frequência ou *Orthogonal Frequency Division Multiplexing,* essa tecnologia de modulação é bem complexa, pois emprega alguns procedimentos de código de correção de erros e entrelaçamento dos dados. Várias portadoras de frequências distintas são empregadas para modular o sinal, sendo essas responsáveis pelo transporte de alguns bits apenas (GAST, 2002, tradução nossa).

Essa técnica de modulação embora apresente um gasto elevado de energia, possui diversas vantagens em relação a transmissões onde os locais sejam mais hostis, adaptando-se rapidamente às possíveis interferências encontradas, é bem tolerante a erros de sincronia de sinal, sendo que sua transmissão é feita do modo paralelo (MORAES, 2010).

O método OFDM é representado na figura 5, sendo possível ver a ortogonalidade entre os pacotes de cor mais escura e os de cor mais clara.

Figura 5 – Modulação por Multiplexação Ortogonal.



Fonte: Adaptado de Gast (2002, p. 172).

A técnica multiplexação ortogonal está presente no padrão 802.11a, onde a frequência de transmissão é dividida em 52 portadoras, na qual 48 são utilizadas para comunicação de dados e as outras 4 exercem a sincronização. A divisão em bandas mais estreitas tem algumas vantagens sobre uso de uma única banda mais

larga, imunidade a interferências de banda estreita e o fator de utilizar bandas não adjacentes (TANENBAUM, 2003).

Devido o padrão OFDM utilizar técnicas avançadas de processamento de sinal, ele consegue transmitir os dados por várias portadoras menores, mas com a frequência exata para cada bloco de bits enviados, dado essa “perfeita cópia” de multiplexação em portadoras menores tal como em uma banda mais larga, titula-se de ortogonalidade (STALLINGS, 2005, tradução nossa).

2.3.4 High Rate Direct Sequence Spread Spectrum (HR-DSSS)

High Rate Direct Sequence Spread Spectrum ou espectro de dispersão de sequência direta de alta velocidade é uma técnica utilizada no modelo 802.11b e com frequência de 2.4 GHz, velocidades de transmissão podem ser de 1; 2; 5,5 e 11 Mbps, embora as duas primeiras operem em caráter de compatibilidade com o padrão DSS, todas podem se auto ajustar para alcançar ótima relação entre taxa de transferência e ruído, o que prevalece nesse aspecto é uma cobertura de até sete vezes maior (TANENBAUM, 2003).

A parte prática de seu funcionamento se assemelha ao DSSS, porém o HR-DSSS utiliza um método diferente para codificação, o *Complementary Code Keying* (CCK) que codifica 4 ou 8 bits em um único símbolo para transmissão (FOROUZAN, 2006).

2.3.5 Multiple-Input and Multiple-Output (MIMO)

Padrão de modulação da frequência geralmente utilizado na tecnologia 802.11n, cuja característica principal é a ampliação da velocidade entre o emissor e o receptor do sinal. Opera com mais de uma antena em cada ponta e ambos os dispositivos devem possuir compatibilidade com essa tecnologia; a vazão dos dados é expandida conforme o número de antenas instaladas.

De acordo com Zhang; Zheng e Hu (2009, tradução nossa) o uso do padrão MIMO com múltiplas antenas aumenta notavelmente a área de cobertura e a taxa de transferência dos dados. O mecanismo de ampliação da velocidade sem alterar a potência de transmissão se deve a aplicação da técnica de propagação

multi-caminhos. Essa mesma técnica é empregada juntamente com OFDM no padrão IEEE 802.16 (WiMAX).

Além da característica de transmitir dados com velocidades superiores a 300 Mbps, o sistema de várias antenas, podendo chegar até quatro, permite a melhora na transmissão de dados onde existem muitos obstáculos e interferências. Ele é compatível com os padrões anteriormente lançados, porém com a velocidade de operação diminuída (TSE; VISWANATH, 2005, tradução nossa).

Produtos da especificação 802.11n estão surgindo no mercado com maior frequência, geralmente permitindo a retro compatibilidade com os padrões 802.11b e 802.11g. Seu preço está bem acessível em comparação como benefício e há possibilidades de se tornar presente por um longo período.

2.4 INSEGURANÇA EM REDES WIRELESS

A conveniência de fácil acesso ao meio físico, o ar, por onde as redes sem fios transmitem os dados, tornam essas um alvo de simples alcance para qualquer dispositivo que esteja na área de cobertura do sinal transmitido. Diferente das redes cabeadas que possuem uma segurança física, as redes wireless podem contar apenas com políticas de configuração para minimizar suas vulnerabilidades.

Em uma rede onde o ingresso dos dispositivos é feita de maneira controlada, com usuários confiáveis e topologia fixa, pensa-se relacioná-la como possivelmente segura, embora exista outro fator como usuários mal intencionados ou descuidados. Nas redes wireless o sinal pode ir muito além de alguns metros como muitos idealizam, munido de uma antena especial pode-se capturar o sinal a quarteirões de distância (IDRC, 2008).

A implantação das camadas de segurança de qualquer rede não pode anular seu principal objetivo, que é a comunicação entre os envolvidos desta. Você deve aplicar políticas de segurança sem tornar o sistema inoperante, indo ao encontro de um ditado antigo que fala o seguinte:

> A única maneira de tornar um computador completamente seguro é desligá-lo, colocá-lo em um cofre, destruir a chave do cofre e enterrar tudo isto em concreto. Mesmo que um sistema destes seja completamente “seguro”, ele é inútil para a comunicação. (IDRC, 2008, p. 157)

Em Moraes (2010) aborda-se a expressão “política de segurança”, que explicita uma estrutura de rede confiável baseada em uma série de procedimentos, especificações, concessões e negações de direitos, tudo a fim de manter a rede segura.

Os principais serviços coadjuvantes de uma rede confiável são:

a) **integridade:** possui o papel de manter a informação sem alteração tanto no envio quanto no armazenamento, evitando assim erros de processamentos e falsificação. A adulteração pode ocorrer de forma voluntária (maliciosa) ou acidentalmente;
b) **auditoria:** serviço responsável por registrar em arquivos todos os acontecimentos no acesso à informação, desse modo identificam-se os usuários responsáveis por cada transação;
c) **disponibilidade**: garante que a informação estará sempre a disposição do usuário quando solicitado. Ataques de negação de serviço e infortúnios de ordem natural contribuem para graves falhas nesse item. A disponibilidade deve estar de acordo com o desempenho perante as solicitações, sempre havendo uma atualização dos sistemas e equipamentos para um desempenho satisfatório;
d) **confidencialidade:** pauta-se no sigilo da informação disponível na rede, não sendo permitido o acesso às pessoas sem autorização, nele é imprescindível o uso de recursos de identificação, autenticação e autorização.

Todos os itens acima são discutidos em Moraes (2010) e ainda que haja tantos outros, esses são os de maior preocupação, se analisados e empregados em uma rede sem fios. Salientando que, conforme o segmento de negócio, alguns desses serão mais significativos que outros, devendo esses ser mais considerados na sua implantação.

A segurança na rede sem fio necessita de um treinamento e acompanhamento dos seus próprios usuários, orientando eles a manter o máximo de sigilo sobre senhas de sistemas, perfil de informação que trafega na rede, detalhes sobre equipamentos empregados na estrutura e impondo limites no acesso de alguns módulos operacionais e áreas físicas da empresa.

Basicamente na WLAN utilizam-se alguns modelos de criptografia para manter um mínimo de segurança possível nos dados trafegados pelo ar. Alguns dos

mais utilizados métodos de segurança serão descritos a seguir.

2.4.1 Wired Equivalent Privacy (WEP)

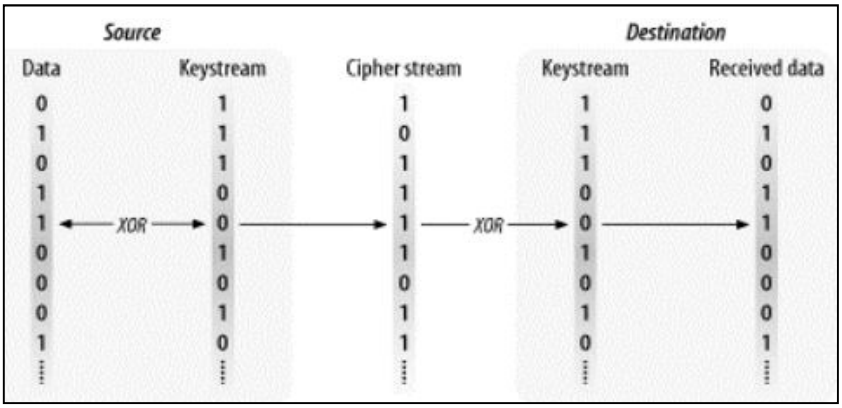
Foi um dos primeiros protocolos de segurança desenhado para redes do padrão 802.11, à medida que as redes se tornaram importantes para os negócios, foram descobrindo falhas nesse protocolo e em pouco tempo ele já não era tão seguro quanto se dizia ser (GAST, 2002, tradução nossa).

Desde sua criação em 1999, vários grupos colocaram à prova sua criptografia de 64 bits (mais utilizado) e descobriram sérias falhas no algoritmo empregado (RC4), principalmente quando conseguiram rompê-lo em 2001, nesse mesmo ano a IEEE reconheceu a total violação do mesmo e aconselhou uma série de medidas, incluindo nelas a troca por outro protocolo e prometeu melhorias em um novo modelo (TANENBAUM, 2003).

O funcionamento do protocolo WEP consistia em apanhar um bloco de dados e aplicar uma operação de OU Exclusivo em cima de fluxo de chaves, gerada por um vetor de inicialização (24 bits), essa sequência gera um texto cifrado que só poderá ser interpretada pela outra ponta que possui o segredo dessa chave (TANENBAUM, 2003).

Na figura 6 percebe-se o emprego de todos os processos na encriptação dos dados, tais como aplicação de OU Exclusivo através de uma chave gerada pelo vetor na fonte até o processo reverso no seu destino.

Figura 6 – Funcionamento da cifragem no WEP.



Fonte: GAST (2002, p.97).

2.4.2 Wi-Fi Protected Access (WPA)

Esse foi um modelo desenvolvido para sanar as falhas de construção do renunciado WEP. Com intuito de conceber um protocolo que fosse além de mais seguro, mas também compatível com o antecessor, eles acabaram incorporando algumas das falhas, porém, esse tinha um diferencial, suporte aos servidores de autenticação centralizada (MORIMOTO, 2008).

Esse novo padrão utiliza um sistema de criptografia muito mais avançado que o anterior, podendo ainda fazer uso de certificados de *Secure Sockets Layer* (SSL), chaves específicas para cada usuário ou ainda autenticação em servidor como o RADIUS. O WPA conta com um mecanismo de cifragem dinâmico nomeado de *Temporal Key Integrity Protocol* (TKIP), essas chaves se alternam com o passar do tempo, fica muito mais difícil decifrar a sequência para quebra da segurança (IDRC, 2008).

A utilização de criptografia em 128 bits e um vetor de inicialização agora com 48 bits torna bem difícil a invasão da rede. A chave sofre alteração conforme um tempo pré-estabelecido ou caso não seja configurado ele alterna a cada 10.000 quadros transmitidos. Na pior das hipóteses, o invasor conseguirá apenas um pequeno fragmento dos dados nesse tempo de troca da chave (DUARTE, 2010).

2.4.3 Wi-Fi Protected Access 2 (WPA2)

Com o mesmo propósito que o WPA substituiu seu antecessor, o WPA2 é nomeado pela Wi-Fi Alliance como o novo padrão de segurança nas redes sem fios. A segunda versão do WPA traz ainda uma melhora de desempenho e estabilidade devido à troca do algoritmo criptográfico. Tendo seu nível de confiança elevado, esse novo método segue como solução definitiva aos usuários de redes sem fios (WI-FI Alliance, 2010).

O aspecto de diferenciação entre a primeira e segunda versão está no emprego de engenharia superior na criptografia dos dados, enquanto o WPA utilizava o frágil RC4 em conjunto com o TKIP, a versão seguinte passou a utilizar o *Advanced Encryption Standard* (AES) + TKIP, aumentando ainda mais a confiança no sigilo de transporte de dados.

O WPA2 divide-se em dois segmentos de encriptação, um deles atende redes de menor porte, pois utiliza apenas uma chave pré-compartilhada, esse método nomeia-se de *WPA2 Personal Mode*. Outra solução foi criada devido a mobilidade de alguns usuários dentro de uma rede com vários pontos de acesso, a essa se nomeia de *WPA2 Enterprise Mode,* ela utiliza o padrão 802.1x unido ao protocolo RADIUS (MORAES, 2010).

O emprego das técnicas de criptografias acima explanado contribui consideravelmente para uma rede mais segura e estável, mas não elimina por completo a possibilidade de um acesso sem permissão violar alguns dos aspectos fundamentais da segurança da informação.

Atualmente existem muitas técnicas para interceptação e roubo dos dados que trafegam pelas redes sem fios, sendo necessária a implantação de mecanismos coerentes de segurança conforme a importância da informação para a pessoa ou negócio. Uma simples senha já não garante a privacidade total, nessa condição devem-se utilizar mais algumas barreiras para impedir esse acesso desautorizado.

3 REDES MESH

As redes Mesh surgiram mediante necessidade de transmitir informações sem a obrigatoriedade da existência de uma arquitetura física do tipo infraestruturada e fixa. Desenvolvida pela *Defense Advanced Research Projects Agency* (DARPA) na década de 1970, ela foi inicialmente destinada para o uso militar em campos de batalhas. A estratégia era utilizar uma comunicação de dados e voz através dos próprios nós da rede, no caso os veículos e combatentes, para aquisição de informações em tempo real.

Em Held (2005, tradução nossa) a topologia da rede é descrita como dinâmica, pois os elementos que a compõem não são totalmente estáticos, os nós são geralmente dispositivos móveis que se conectam a outros equipamentos cuja área de cobertura os envolve, criando assim um aspecto de “malha” entre todos eles; devido a esse fato, as redes Mesh também são citadas como *Redes em Malha.*

O padrão proposto pelo grupo de estudo IEEE foi nomeado de 802.11s, cuja característica básica é o *Self-Healing/Self-Configuring, auto-cura/auto-configuração.* Existe um grupo de discussão que pretende formalizar de vez o padrão de redes em malha, embora criado no início do ano de 2005, ainda não chegaram às especificações finais do modelo.

As equipes envolvidas são compostas por pesquisadores de empresas com grandes qualificações no cenário de tecnologia mundial, como a Motorola, Philips, Texas Instruments, Cisco dentre outras. Existem duas propostas atualmente em discussão nomeadas de WI-Mesh e SEEMesh. Dados atualizados revelam que mais de 97% do projeto já estavam encaminhadas e aprovadas por ambas as equipes em Junho de 2011 (IEEE, 2011).

A topologia de rede utilizada por uma *Wireles Mesh Networks* (WMN) pode ser de até três formas distintas, conforme descrito em Akyildiz e Wang (2005, tradução nossa), a seguir os modelos com suas características fundamentais:

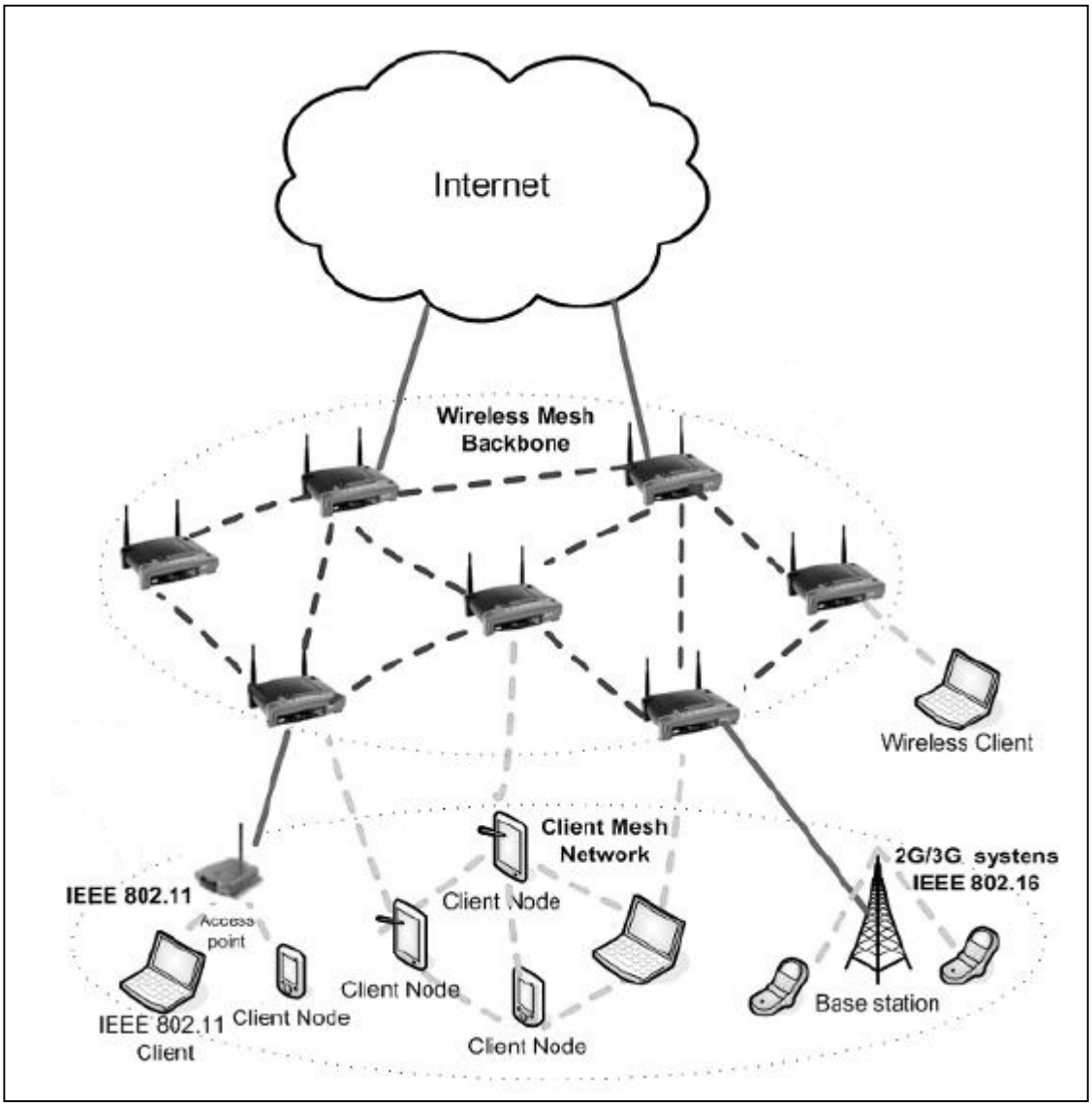
a) **modo infraestruturado:** nesse modelo de configuração os nós se conectam à um ponto de acesso, podendo esse estar ou não conectado à outro ponto de acesso, que possui acesso à Internet. Esses pontos de acesso ou *Mesh Routers* são roteadores que trabalham no sistema de *Self-Healing/Self-Configuring,*sempre se ajustando e se configurando conforme existe uma modificação nos

gateways da rede. A WMN pode conter apenas um *Mesh Router* ou vários deles interligados e corretamente configurados; essa interligação denomina-se *Backbone,* pois é literalmente considerada a espinha dorsal por onde trafegam de dados solicitados pelos clientes Mesh. Essa topologia de rede geralmente contém equipamentos de radiofrequência utilizando o padrão IEEE 802.11. Clientes de mesmo fabricante dos *gateways* podem ter acesso às configurações desses através do sinal sem fio, mas nada impede de conectarmos um cliente de outra marca por meio de uma conexão *Ethernet;*

b) **modo cliente:** trabalha na forma de rede ponto a ponto, não possuindo nenhum roteador entre os nós. Esse modelo geralmente é utilizado para aplicações de usuário final sem acesso à Internet, onde um cliente se conecta a outro sem a necessidade de um equipamento central de controle de conexão. O modo cliente também é conhecido como conexão *Ad hoc*, cabendo a esses nós interconectados todo o trabalho de roteamento de pacotes e configuração automática das conexões. Essa arquitetura pode apresentar uma variedade muito grande de marcas e modelos, embora todos tenham que possuir compatibilidade com o padrão 802.11s;

c) **modo híbrido:** essa arquitetura une os modos de operação infraestrutura e *Ad hoc* em uma rede mista, onde um nó pode transferir dados à outro através de um *Mesh Router* ou um próprio nó da rede. Nessa disposição física da rede encontra-se o benefício do modo Cliente WMN, que aumenta a área de cobertura; e o padrão com roteadores próprios onde é possível a utilização do link principal para prover Internet. Na figura 7 observa-se a disposição de uma rede em malha onde a topologia é bem distinta, possuindo, às vezes, mais de uma rota para o acesso ao nó principal que está conectado na Internet.

Figura 7 – Rede Mesh Híbrida.



Fonte: Hossain e Leung (2007, p. 135).

Uma analogia às redes em malha é que a Internet seria a maior rede Mesh existente, pois contém algumas características básicas que são o encaminhamento de dados com vários saltos entre o destinatário e o remetente, diversidade de equipamentos operando em conjunto, aprendizado de rotas subjacentes entre outros fatores.

Em Held (2005, tradução nossa), um assunto muito salientado nas redes Mesh é o da segurança da informação, uma vez que esse padrão não possui um mecanismo centralizado de controle de acesso à rede, qualquer dispositivo pode se conectar a malha o que facilita a presença de dispositivos não desejados e

consequentemente existe uma maior chance de um computador operado por hacker interceptar os dados.

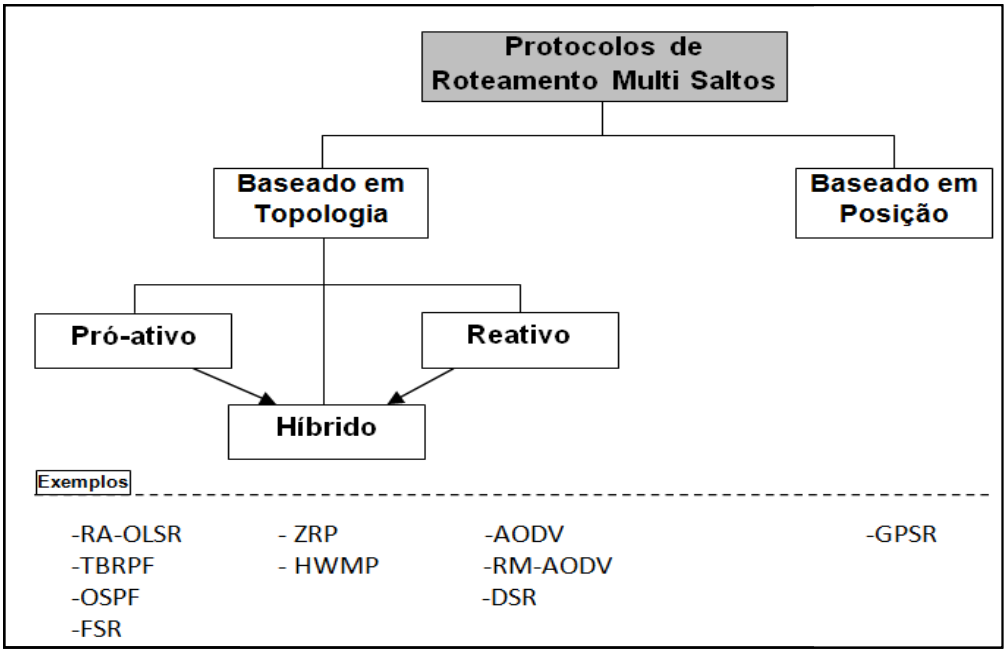
3.1 PROTOCOLOS DE ROTEAMENTO EM REDES MESH

As redes wireless Mesh estão crescendo em números de utilizadores e em tecnologias para ampliação da cobertura do sinal, sustentado nesse aumento, diversas empresas estão desenvolvendo e comercializando produtos voltados a esse ramo. Grupos de pesquisa empenham-se em estudar e propor novas técnicas de transmissão contribuindo para uma padronização eficaz dessa tecnologia e objetivando uma adoção universal.

Zhang, Luo e Hu (2007, tradução nossa) descrevem que os diferentes tipos de redes Mesh trabalham fundamentados no mesmo princípio, a comunicação dos nós através de múltiplos saltos na rede, porém as *Mobile Ad hoc Networks* (MANET) trabalham com dispositivos móveis de usuários finais, enquanto as WMNs se baseiam em dispositivos pertencentes a estruturas mais estáticas.

Na figura 8 representam-se alguns protocolos conforme categoria de descoberta de rotas para transmissão em redes Mesh.

Figura 8 – Classificação dos protocolos de roteamento.



Fonte: Adaptado de Zhang, Luo, Hu (2007, p. 117).

3.1.1 Protocolos Pró-ativos

São protocolos que estão em constante comunicação com a rede a fim de manter uma rota para todos os destinos quando um novo nó associa-se no enlace. Os nós mantêm sempre uma tabela atualizada dos possíveis caminhos, gerando assim duas circunstâncias, uma baixa latência no momento da transmissão, pois conhecem o melhor trajeto, e um assíduo tráfego na rede (MISRA; WOUNGANG, 2009, tradução nossa).

Esse mecanismo de descoberta e exportação contínua das tabelas de possíveis rotas, pode gerar um inconveniente problema de segurança, caso algum nó malicioso envie uma tabela falsa, ele pode propositalmente direcionar o tráfego à outro ponto da rede que intercepte pacotes ou ainda repassar uma lista com endereços incorretos, acarretando uma ruptura no caminho (XIAO; SHEN; DU, 2007, tradução nossa).

Existem vários protocolos de descoberta de caminhos pré-estabelecidos nas redes Ad hoc, dentre os mais utilizados encontram-se o *Destination Sequenced Distance-Vector* (DSDV), *Wireless Routing Protocol* (WRP), *Fisheye State Routing* (FSR), *Optimized Link State Routing* (OLSR).

3.1.1.1 Protocolo DSDV

É um dos protocolos pró-ativos que informa apenas à seus vizinhos sua tabela de roteamento, nela está contida todos os seus possíveis IP destino, a distância entre eles e o nó seguinte do caminho. Toda essa informação é repassada periodicamente entre os roteadores e a cada nova alteração do arranjo da rede (XIAO; SHEN; DU, 2007, tradução nossa).

O protocolo baseado em *Distance-Vector* tem uma visão geral da topologia da rede e a que “custo” está um roteador do outro, esse custo é baseado por meio do número de saltos até ele, caso ele deixe de existir na rede o novo valor passa a ser infinito e ele é descartado da tabela. Todo esse calculo de rota demanda mais processamento e memória para alocar os inventários de trajetos.

A sua característica de anunciação frequente das tabelas de roteamento em conjunto com a constante mobilidade dos nós na rede, causa um relevante

tráfego na rede, em contra partida esse método tem baixo *delay* no início da transmissão entre os dispositivos (MISRA; WOUNGANG, 2009, tradução nossa).

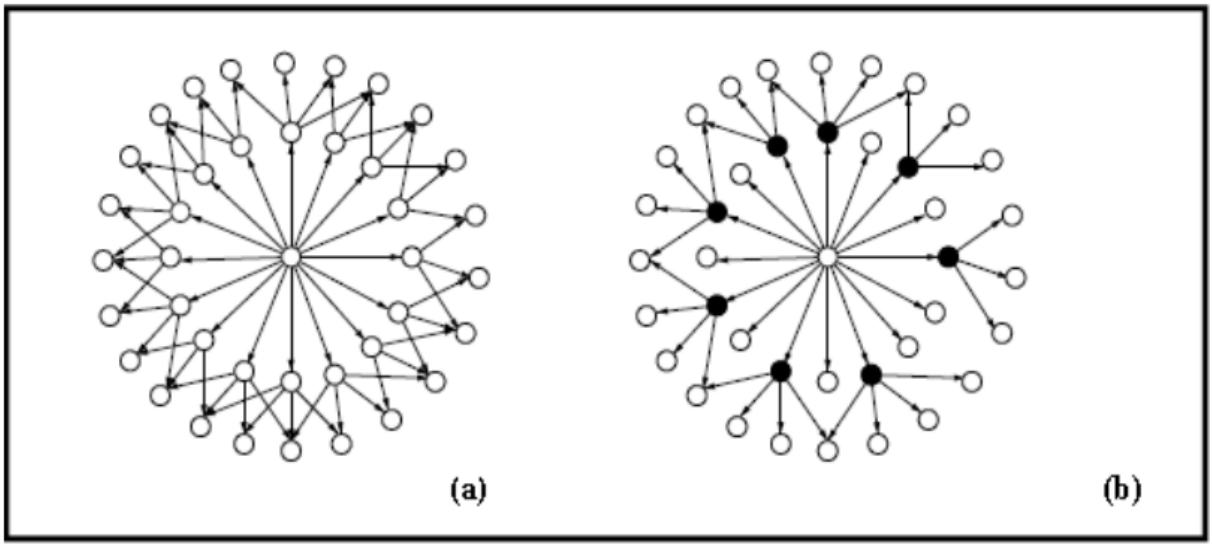
3.1.1.2 Protocolo OLSR

Protocolo popularmente utilizado nas MANETs e padronizado pela IETF como experimental sob a RFC 3623 que descreve seu funcionamento baseado no algoritmo de menor caminho (contagem de saltos), porém as informações de rota são enviadas de mais forma aprimorada que os outros modelos pró-ativos (ZHANG, LUO; HU, 2007, tradução nossa).

O padrão OLSR utiliza um mecanismo de *Multi Point Relay* (MPR) para alguns de seus nós adjacentes, esses quando recebe um determinado sinal no pacote indicando que ele é um MPR *Selector* (MPRs) ele deve informar a todos os seus vizinhos alcançáveis as possíveis rotas, os outros nós de um salto apenas que não são MPR *Selector* não necessitam enviar suas tabelas, diminuindo o *broadcast* na rede (KHAN; PATHAN, 2013, tradução nossa).

Um exemplo prático de visualizar o funcionamento do conceito de MPR é demonstrado na figura 9 e pode-se concluir a diminuição de *broadcasting* nos últimos dispositivos da rede; nodos de cor preta identificam os MPRs.

Figura 9 – Descoberta pró-ativa habitual (a) e utilizando MPRs em OLSR (b).



Fonte: Khan e Pathan (2013, p. 239).

O mecanismo de não propagação do estado de link a todos os nós da rede evita a redundância na transmissão de pacotes, pois nem todos irão transmitir a seus vizinhos, e aperfeiçoa o trajeto ponto a ponto por meio de sua atualização eficiente. Em uma rede com vários nós e muitos saltos entre o destinatário e o solicitante o protocolo se mostra mais eficiente.

3.1.2 Protocolos Reativos

São fundamentados na atualização de suas tabelas de roteamento somente quando necessita transmitir informações, assim não existe um constante envio da topologia de rede a todo o momento. Eles possuem um *cache* dos caminhos conhecidos, porém quando não os possuem, enviam pacotes *broadcast* pela rede a fim de conhecer e atualizar novamente suas rotas (METHLEY, 2009, tradução nossa).

Em Zhang; Zheng e Hu (2009, tradução nossa) é exposto que embora o tráfego para atualização de caminhos atenue o atraso fim a fim aumenta devido a novos cálculos de rota quando se quer transmitir um pacote de dados à um destino desconhecido.A redução dos pacotes de controle influência na ampliação de largura de banda no enlace.

Podemos considerar o protocolo reativo como uma implementação que minimiza a requisição de processamento e em consequência um menor consumo de baterias, uma vez que os dispositivos são usualmente móveis. Os protocolos mais empregados são o *Adaptive On-Demand Distance Vector* (AODV) e o *Dynamic Source Routing* (DSR).

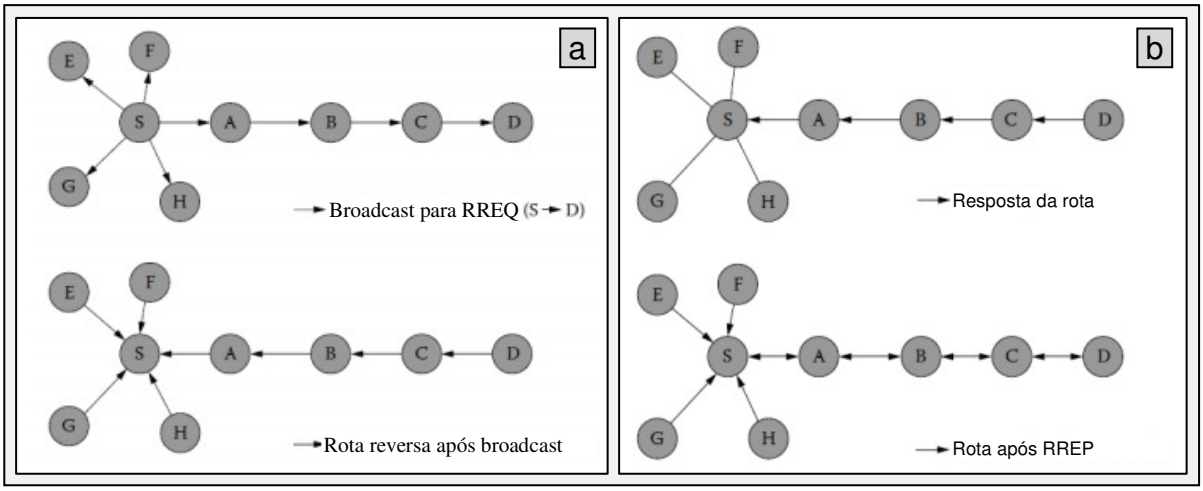
3.1.2.1 Protocolo AODV

Atua na classe dos protocolos reativos e constrói suas informações de rota enviando um pacote de requisição de rota denominado RREQ ao nó seguinte, esse faz uma entrada em sua tabela contendo o IP de onde partiu o pedido e não competindo à ele a solicitação, envia ao seu vizinho até que o mesmo seja o destinatário. O destino agora informa o pedido com um pacote RREP (RouteReply) através da rede e assim que o solicitante recebe-o, ele atualiza sua tabela de caminhos(XIAO; SHEN; DU, 2007, tradução nossa).

Em Zhou (2012, tradução nossa) entende-se que no método AODV elimina integralmente os *loopings* na rede, visto que todo o trajeto para entrega do pacote é construído antes do envio. Quando um link do conjunto fica indisponível, o mesmo possui mecanismos de reconstrução de percurso, contudo ele origina um pequeno retardo na rede, o que não impede sua ausência de *looping*.

Mesmo não contendo uma visão geral da rede, a fonte sabe precisamente a rota para seu destino e vice-versa. No envio de requisição de rota o pacote enviado é através de *broadcast* e a rota reversa é construída com pacotes *unicast*; rotas não mais presentes são atualizadas na tabela com RouteError (RERR)(FUNABIKI, 2011, tradução nossa). A seguir na figura 10 demonstram-se os pedidos de RREQ e RREP no protocolo AODV.

Figura 10 – Requisição de rota (a) e Resposta de rota (b) protocolo AODV.
S é o nó de origem e D o destino.



Fonte: Adaptado de Funabiki (2011, p. 266).

3.1.2.2 Protocolo DSR

Um dos primeiros protocolos de descoberta de rotas sob demanda em rede Ad hoc; opera com os mesmos pacotes de RREQ, RREP e RERR a fim de estabelecer comunicação entre a fonte e o destino. Todos os nós que recebem o pacote de requisição e não são identificados como destinatário em seu cabeçalho, reenviam a solicitação ao próximo nó sucessivamente até localizá-lo; em seguida ele retorna toda sua rota reversa e atualiza o *cache* (ZHANG, LUO; HU, 2007, tradução nossa).

Protocolo bem similar ao AODV, embora ambos armazenem em sua tabela de roteamento o caminho até o destino desejado, o protocolo baseado na fonte (DSR) preserva todos os caminhos possíveis entre a origem e o destino, gerando uma maior base de dados sobre os saltos disponíveis (XIAO; SHEN; DU, 2007, tradução nossa).

3.1.3 Protocolos Híbridos

É uma categoria criada para conciliar os benefícios dos protocolos pró-ativos e reativos a fim de alcançar melhor desempenho e escalabilidade na rede Ad hoc. Entre os nós próximos e para aquelas rotas frequentemente utilizada emprega-se a métrica pró-ativa, nos dispositivos onde a distância é maior e raramente são utilizados para troca de dados adota-se o mecanismo reativo (MISRA; WOUNGANG, 2009, tradução nossa).

Em Xiao; Shen e Du (2007, tradução nossa) o *Zone Routing Protocol* (ZRP) é destacado como um dos protocolos híbridos. Ele utiliza o algoritmo pró-ativo para descobrir os nós mais próximos e os denomina de zona; quando o destino solicitado está fora da zona então é enviado um pedido aos nós da borda (reativamente) se eles possuem esse caminho na tabela, caso contenham, este é retornado ao ponto de origem, caso contrário a solicitação é repassada até que se encontre o destino ou que os saltos máximos sejam alcançados.

A engenharia dos protocolos híbridos tem um desempenho significante em uma rede com vários nós, se comparados com os outros modelos de comunicação em rede Ad hoc, pois eles diminuem o tráfego de pacotes duplicados e desnecessários, utilizando essa maior largura de banda para transferência de dados.

3.2 FIRMWARES COMPATÍVEIS

O *firmware* de um dispositivo, em uma definição bem elementar, seria um conjunto de procedimentos que é inserido em uma memória do dispositivo eletrônico, esse software define quais serão os possíveis comportamentos do equipamento.

Alguns estudos e testes conseguem aprimorar algumas características no *firmware*, como agilidade no processamento de instruções, adição de funções,

melhorias no consumo de energia, correção de erros entre outros. Esses procedimentos usualmente acatam os limites do *hardware* onde estão inseridos.

De maneira que o *firmware* fica instalado na memória do equipamento, vale ressaltar que o tamanho dele deve ser menor e compatível com as características do dispositivo a ser instalado. A seguir a lista de alguns *firmwares* modificados e que operam de maneira normal em alguns roteadores no mercado.

a) **openwrt:** *firmware* concebido em 2004 e até então em desenvolvimento, atualmente possui mais de cinco versões estáveis e serviu de base para outros projetos de desenvolvimento em código aberto. A base de implementação é o kernel GNU/Linux, a partir daí eles adéquam e re-compilam os fontes para o tamanho e utilidade necessária do roteador. À medida que um hardware com o OpenWrt possui mais recursos, como (memória/processador), ele pode envolver mais funcionalidades, pois é permitido a instalação de módulos em separado, tais como servidor FTP de arquivos, servidor de impressão, central multimídia entre outros (OpenWrt);
b) **freifunk:** esse projeto é de nacionalidade alemã e utiliza como fundamento o *firmware* OpenWrt, com ele é possível a criação de redes Mesh utilizando o protocolo OLRS e *Better Approach To Mobile Ad-hoc Networking* (B.A.T.M.A.N.). Possui milhares de usuários pela Alemanha e outros países, isso apenas reforça a funcionalidade desse *firmware* em conjunto com as redes Mesh, uma vez que suas funções são especialmente facilitadas para gerenciar uma rede em malha com vários dispositivos;
c) **ddwrt:** é um outro *firmware* baseado em Linux para roteadores sem fios, possui vasta compatibilidade com equipamentos do padrão 802.11a/b/g. Interface de configuração Web com fácil entendimento e suporte a várias linguagens, podendo ser facilmente configurado por usuários sem muito conhecimento. Possui uma grande comunidade de desenvolvedores e usuários ao redor do mundo, contendo em seu fórum uma ampla base de conhecimento; existe ainda a comercialização do suporte técnico avançado para empresas.

.

4 PROTOCOLO RADIUS

Protocolo desenvolvido para prover um controle de acesso e uma comunicação segura entre o cliente/requerente e o servidor/autenticador. O *Remote Access Dial In User Service* (RADIUS) veio para centralizar as autenticações de usuários distintos no acesso de alguns recursos da rede (HASSELL et al, 2002, tradução nossa).

O RADIUS foi baseado em uma arquitetura de *Network Access Server* (NAS) onde podia prover além do simples acesso demais funcionalidades, como em servidores *Authentication, Authorization and Accounting* (AAA). Além da autenticação do usuário, foram incorporadas funções para autorização de que serviços ele poderia usufruir e por quanto tempo ou em que período ele poderia utilizar o recurso (NAKHIJIRI, 2005).

O funcionamento de um servidor de AAA pode ser descrito comparando-se com algumas das atividades diárias, por exemplo, uma pessoa vai ao banco sacar dinheiro e precisa se autenticar com cartão e senha (AUTENTICAÇÃO), posteriormente precisará informar que tipo de serviço pretende utilizar, como saldo, extrato ou saque; em um saque ele será informado se tem ou não crédito suficiente conforme solicitado (AUTORIZAÇÃO), todo esse serviço ficou registrado e servirá de recurso para uma nova autorização, no caso o dinheiro (CONTABILIZAÇÃO).

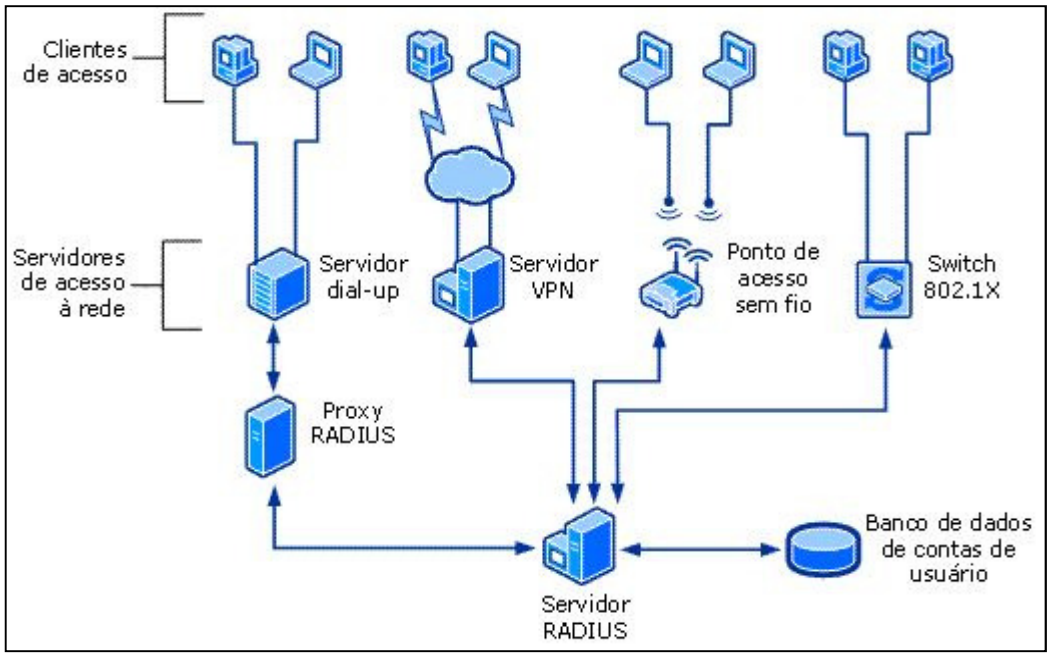
Os provedores de Internet foram os pioneiros na utilização da tecnologia RADIUS, pois eles mantinham um controle de seus clientes através de sua autenticação via usuário e senha informados na conexão. O cliente podia ver no fim do mês quanto tinha usado do recurso solicitado para manter um controle do seu gasto ou até mesmo os provedores poderiam utilizar essa contabilização para negar o acesso caso o plano fosse contratado com base em minutos de uso.

O protocolo foi criado primeiramente por uma empresa privada e posteriormente foi padronizado pela *Internet Engineering Task Force* (IETF) para operar em diversas topologias de rede e aparelhos; embora ele tenha sido inicialmente desenhado para redes cabeadas na época, o padrão foi bem aceito posteriormente na rede wireless. Ele passou por algumas correções e melhorias, sendo uma recente em Abril de 2013 para adaptação do *Internet Protocol Version 6* (IPV6) (DEC et al, 2013).

O funcionamento do serviço de AAA requer apenas a disposição dos componentes básicos, como o servidor RADIUS, clientes e roteadores, em alguns casos pode haver uma base de dados com as credenciais dos usuários, conectada ao servidor, dispostos em uma rede que interligue todos. A disposição física de cada elemento básico independe para o correto funcionamento (RUFINO, 2011).

A infraestrutura com os possíveis componentes de uma arquitetura com autenticação é representada na figura 11, nela entende-se que o servidor de autenticação está localizado na extremidade da rede.

Figura 11 – Componentes da infraestrutura RADIUS.



Fonte: Microsoft (2013).

Os princípios integrados no padrão 802.1X se referem ao controle de acesso a rede baseados em porta e são fundamentados no Triplo A (AAA), abaixo se apresenta uma rápida explanação de cada componente desses três As:

a) authentication: autenticação é o primeiro passo para se ter acesso à rede e utilizar os serviços que ela oferece. Ela consiste em conferir a identidade de uma máquina/pessoa geralmente através de uma identificação e senha; podendo ainda ser empregado para identificação um leitor biométrico, certificados digitais entre outros (WALT, 2011, tradução nossa);

b) **authorization:** a autorização confere os recursos solicitados, se disponíveis, para o usuário em questão, podendo negá-los ou permiti-los. Nessa etapa pode ser definida a não duplicidade de requisição para um mesmo usuário, pode-se ainda restringir o acesso baseado em sua disposição física da rede ou em horário de uso (HASSELL et al, 2002, tradução nossa). Na autorização os administradores podem controlar não somente o acesso, mas o nível deste para cada usuário, bem como especificar quais protocolos ele vai poder invocar, como Telnet, FTP ou outros (THOMAS, 2007);

c) **accounting:** auditoria ou contabilização é uma maneira de contabilizar e registrar os recursos utilizados pelo solicitante. Com base nesses dados ele pode gerar relatórios para melhoramento de uso da rede, analisar atividades incomuns e prever futuros de investimentos na área de maior consumo (WALT, 2011, tradução nossa).

Todos os passos para identificação do dispositivo que solicita um recurso na rede provida de um servidor de autenticação baseado no modelo AAA foram descritos acima, porém cada item possui uma série de especificações e tratamentos.

O protocolo RADIUS fundamenta-se em sua transmissão de dados no conceito cliente/servidor, existindo em um lado o *Network Access Server* (NAS) ou cliente e na outra extremidade o servidor. O NAS geralmente é um AP ou um concentrador proprietário que gerencia as estações, mas nesse modelo ele possui funcionalidades de cliente.

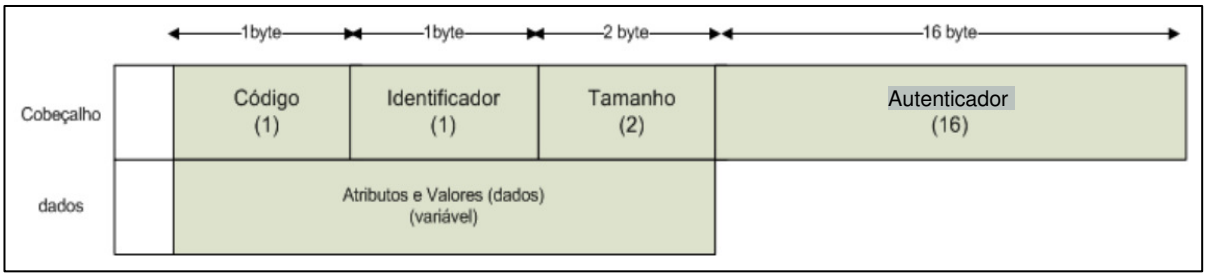
Desde o pedido de ingresso na rede pelo usuário até sua concessão pelo servidor RADIUS, são realizados através de pacotes *User Datagram Protocol* (UDP). O uso do UDP mantém um baixo tráfego na rede e elimina alguns controles no cabeçalho do pacote, sendo que neste já estão inseridos diversos atributos, como nome do cliente, senha, identificador, dados, dentre outros (HASSEL et al, 2002, tradução nossa).

Sistemas de autenticação baseados em RADIUS são geralmente utilizados onde um grande número de usuários necessita de autenticação para ingressar e utilizar os serviços da rede. Os parâmetros de usuário e senha podem ser adquiridos por meio de um banco de dados existente e compatível com o padrão configurado do RADIUS. Muito útil também em ambientes onde existem vários

pontos de acesso sem fio e o utilizador precise deslocar-se constantemente, sem que haja necessidade de nova autorização para uso dos serviços.

A seguir na figura 12 a composição de um pacote transmitido em uma comunicação através do protocolo RADIUS, nele pode-se observar a estrutura que contém todos os parâmetros de identificação e carga.

Figura 12 – Representação da estrutura pacote de dados RADIUS.



Fonte: Adaptado de Hassel et al (2002, p. 17).

Um dos inconvenientes de não utilizar o *Transmission Control Protocol* (TCP) ao invés do UDP, se dá ao fato que as transmissões não possuem um controle nativo de retransmissão em caso de falhas, como no TCP, mas por outro lado tem-se um protocolo leve e vantajoso em reles mais lentas (WALT, 2011).

Conforme figura 12 será apresentado individualmente cada campo e seus valores, segundo descrito em Hassel et al (2002, tradução nossa), ele ainda menciona que os pacotes com código inválido são descartados sem nenhuma notificação.

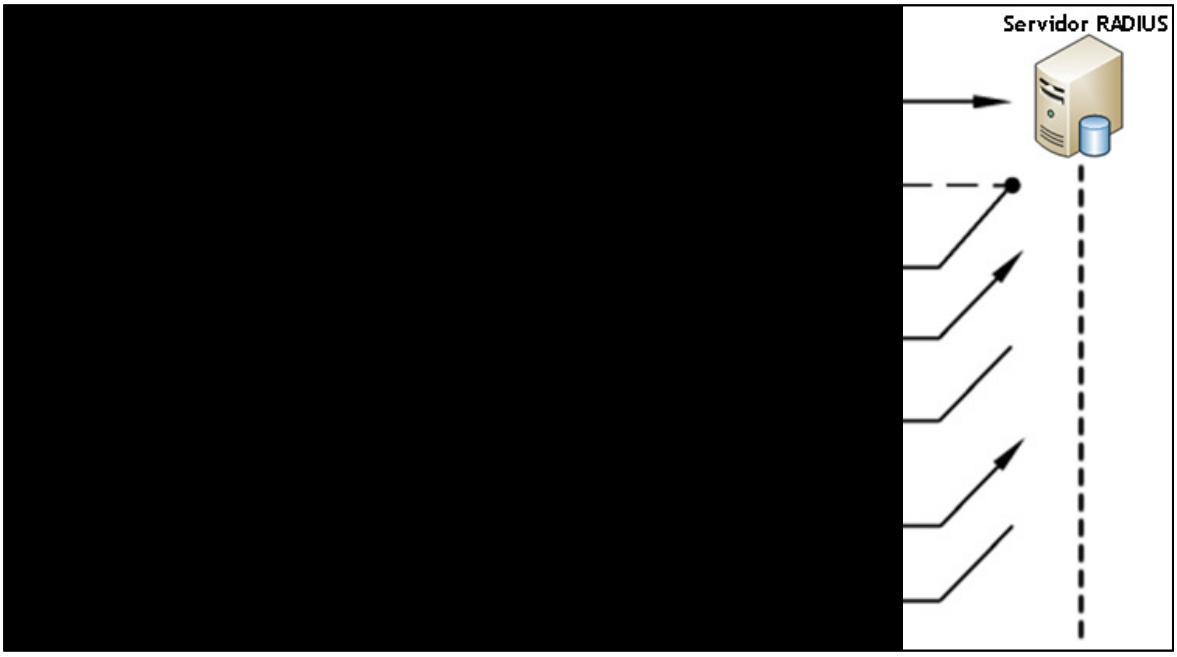
a) **código:** campo destinado a identificar o tipo de mensagem RADIUS que está sendo enviado, como *Access-Request, Access-Accept, Access-Reject, Accounting-Request, Accounting-Response, Access-Challenge* ou *Reserved*;
b) **identificador:** composto por um octeto gerado pelo cliente e o identifica, ele é útil em caso de vários pedidos simultâneos ou até mesmo em uma retransmissão da solicitação anterior;
c) **tamanho:** especifica qual o comprimento da mensagem no todo, ele é calculado através de uma somados outros campos e gera um número entre 20 e 4096. Ele também garante a integridade do dado recebido;
d) **autenticador:** o maior campo do cabeçalho, nele encontra-se dois tipos de dados, a requisição de algum cliente ou a resposta do servidor.

Nesse campo emprega-se uma técnica de criptografia para transmitir o segredo da rede entre o servidor e o NAS;

e) **dados:** são transmitidos os dados solicitados, bem como várias informações do cliente/NAS, podendo ser estas o IP, algumas especificações do fabricante (podendo agregar algum benefício no pacote) ou ainda o controle de comunicação entre o servidor e o cliente.

Na figura 13 uma maneira reduzida e ilustrada do procedimento de requisição entre o requerente, NAS e servidor. Nela podem-se observar os valores dos campos explanados anteriormente:

Figura 13– Passo a passo na autenticação cliente/servidor RADIUS.



Fonte: Adaptado de Nakhjiri (2005).

A comunicação entre o requerente e o servidor RADIUS passa ainda pelo NAS que agrega algumas informações ao cabeçalho transmitido. Existem algumas maneiras confiáveis de enviar esses pacotes de dados contendo a senha para autenticação, em Nakhjiri (2005, tradução nossa) são citados os seguintes métodos, *Password Authentication Protocol* (PAP), *Challenge-Handshake Authentication Protocol* (CHAP) e o *Extensible Authentication Protocol* (EAP).

Protocolo projetado para ampliação do *Point to Point Protocol* (PPP), foi nomeado de EAP e permite operar em conjunto com outros mecanismos de segurança, como um cartão inteligente; ele ainda tem como característica a eventualidade de consultas frequentes a esse mecanismo (NAKHJIRI, 2005, tradução nossa).

O protocolo PAP é empregado em autenticações RADIUS, sendo que cliente envia ao servidor um código obtido de um *hash* entre a senha e outro identificador, não sendo obrigatório o envio de outras informações, como nome usuário; nessa condição o servidor RADIUS ao receber um pacote com o *hash* incorreto, não retorna uma resposta clara se o erro foi de senha do usuário ou o segredo entre o NAS e o servidor (HASSEL et al, 2002, tradução nossa).

No método de autenticação CHAP as informações passadas pelo usuário são submetidas a um algoritmo de cifragem, sendo praticamente impossível sua descoberta em caso de interceptação, nesse trâmite ocorre um processo chamado de *Challenge*, onde o cliente envia um desafio ao servidor, que é calculado e retornado para concretização da requisição (WALT, 2011, tradução nossa).

Existem diversos métodos de transporte de requisições, como o *Protected Extensible Authentication Protocol* (PEAP), o *Microsoft Challenge-Handshake Authentication Protocol (*MS-CHAP), *Point to Point Tunneling Protocol* (PPTP), dentre vários outros, todos eles vão sofrendo aprimoramentos e funcionalidades na medida em que surgem novas necessidades.

As opções de autenticação para sistemas de rede sem fios são amplas, porém o emprego das mesmas não é frequentemente implantado. A falha ou inexistência desses benefícios de segurança pode ser por imperícia técnica ou mesmo desatenção. A prática de utilizar uma senha não tão elaborada é comumente encontrada e se caracteriza pelos motivos de fácil memorização, o que torna a rede insegura.

Ainda que a rede possua uma senha de acesso, a mesma está vulnerável se um usuário compartilhar desse segredo com pessoas externas e não autorizadas. Uma política de segurança deve ser elaborada e executada sob todos os integrantes da rede, destacando os prejuízos decorrentes do vazamento de informações técnicas da organização.

5 TRABALHOS CORRELATOS

A rede Mesh é objeto de interesse nos estudos relacionados à interligação de dispositivos móveis e também na pesquisa e desenvolvimento de métodos mais eficazes de transferência de dados. Devido sua resiliência em relação às condições dos nós, que não tem local fixo, e por ser empregada em hardwares de fácil acesso no mercado, ela compreende um vasto campo de pesquisas.

A busca pela explanação e melhora das redes em malha incita a aplicação de projetos como meio de observar suas limitações e desenvolver técnicas que a ajudem ter um melhor proveito dessa tecnologia. Confrontar as opções de firmwares em equipamentos mais poderosos com intuito de conceber melhor processamento e disponibilização de dados a preços realmente acessíveis também justifica seu estudo.

Os trabalhos na área de redes sem fios e especificamente naquelas de arquitetura não definida são amplos e vem aumentando com a agregação de serviços, dentre alguns de renome internacional destacam-se: Wireless África e V-Mesh, a seguir as principais características de implantação dos projetos.

5.1 CASE WIRELESS ÁFRICA

O objetivo era levar Internet às cidades e bairros rurais da África do Sul onde não havia infraestrutura disponível para acesso a rede mundial de computadores. Foi então desenvolvido um projeto de inclusão digital a essas pessoas pelo Instituto Meraka, que introduz alunos e recém-graduados em pesquisas de desenvolvimento sustentável e tecnologias de comunicação.

A idéia tinha objetivos mais específicos com a implantação dessa comunicação digital até então não conhecida, que era entregar melhor qualidade de vida aos habitantes por meio de aplicação em educação e saúde. Outro fator importante foi o aprendizado em relação à pesquisa e testes em equipamentos de baixo custo para funcionamento da rede Mesh que pode prover comunicação de voz, troca de mensagens, segurança entre outros.

A utilização dos materiais foi pensada em sempre obter um menor custo possível, primeiramente o *firmware* é baseado em GNU/Linux, código livre, as antenas para interligação de longo alcance foram desenvolvidas com latas de café e

tubos metálicos dos raios de bicicleta. O protocolo utilizado na rede foi o OLSR juntamente com DD-WRT ou Freifunk e conta contava com roteadores Cisco/Linksys WRT54G.

Atualmente o Grupo Meraka já levou Internet para milhares de habitantes da África do Sul e países vizinhos através de seus projetos de baixo custo e utilização de estudantes em pesquisas dessa natureza. O projeto foi tão bem sucedido que rendeu alguns prêmios, inclusive uma bolsa de estudo para conclusão de um doutorado.

5.2 CASE ROOFNET

Projeto criado na universidade de *Massachusetts Institute of Technology* (MIT) (USA) pelo departamento de Ciência da Computação a fim de estudar e desenvolver novos protocolos para redes Ad hoc. Inicialmente começou com poucas dezenas de roteadores distribuindo o sinal nas proximidades do campus. Esse projeto leva em consideração o custo de aquisição dos equipamentos que é relativamente baixo.

Atualmente com seu próprio protocolo de roteamento criado e funcionando, eles estão distribuindo acesso para estudantes que moram próximo a universidade. Instalam antenas de transmissão via rádio no telhado das casas, descem um cabo para conexão no computador e vão distribuindo o sinal para o próximo ponto através de saltos, de modo que todos tenham alcance ao nó principal localizado na universidade.

Com base nos dados colhidos em testes e uso cotidiano da rede, eles estão em constante aprimoramento do seu mecanismo de roteamento, sempre seguindo os padrões da IEEE e enfocados na entrega dos pacotes pelo melhor caminho. Assim que conseguirem uma versão estável, vão disponibilizar de forma gratuita e em código aberto.

Casos de sucesso também são encontrados no Brasil, sendo um dos principais objetivos por aqui a implantação dessas redes em malha para cidades mais carentes e distantes dos grandes centros. Os casos de maior notoriedade são encontrados na cidade de Santarém-PA e na Universidade Federal Fluminense (UFF) - RJ.

5.3 CASE NAVEGAPARÁ

Este case foi desenvolvido e apoiado por várias entidades publica e privada, atualmente gerida pela Universidade Federal do Pará, onde a rede em malha trabalha com equipamentos mais sofisticados que os convencionais radiotransmissores embarcados com Linux.

Foram instalados por volta de 55 equipamentos nos postes da cidade e proporcionaram uma cobertura de quatro quilômetros quadrados. O sinal é distribuído para infocentros, moradores e público do comércio local. O NavegaPará levou informatização à pessoas que não tinham a gratuidade da Internet e seu único acesso dava-se apenas por satélites, o que tornava a implantação impraticável em termos de custo.

Os Mesh Routers são fabricados pela Motorola e operam com protocolo híbrido proprietário. Atuam com até dois tipos de frequência livre, 5.8 Ghz para interligação com outros nós e 2.4 GHz para conexão dos dispositivos móveis, sua construção foi concebida para uso externo.

5.4 CASE REMESH

Projeto de pesquisa aplicado em prover acesso à Internet aos alunos que moram próximo à Universidade Federal Fluminense por meio da topologia Mesh. Utilizam transmissores de baixo custo com *firmware* OpenWRT (código livre) e protocolo de envio de pacotes OLSR.

Mediante os resultados dos testes com o protocolo escolhido pelo grupo de pesquisa, observou-se que havia necessidade de algumas alterações para que o mesmo tivesse melhor eficiência. Foi utilizada em conjunto com o protocolo outra métrica que levava em consideração não apenas o caminho com menor salto, mas sim aquele que possuía uma velocidade de entrega mais rápida e confiável. O resultado após várias tentativas foi animador, pois aumentou a taxa de transferência e diminui a perda de pacotes.

O projeto se estendeu para outros *campi* contemplando agora alguns moradores próximos a essas unidades. O papel de inclusão social pela

informatização da informação oferecido pela universidade desperta a vontade de se obter mais conhecimento através de pesquisa e dos meios dispostos.

Outras aplicações de rede em malha foram aplicadas no Brasil, entretanto não foram descritas, com anseio de beneficiar-se dessa tecnologia, que objetiva a ubiquidade da informação e facilidade de implantação e manutenção. As “Cidades Digitais” tornaram-se elementos de referência em pesquisas e divulgação de benfeitorias por governos municipais, sem deixar de salientar o lado da inclusão ao acesso da Internet, que no Brasil, sobretudo, ainda é baixo.

6 REDES EM MALHA COM AUTENTICAÇÃO NO ACESSO

Na pesquisa empreendida foram realizados os procedimentos de composição de uma rede em malha com alguns nós e um servidor de autenticação para os usuários que pretendiam o acesso à mesma.

Na concepção do servidor de autenticação de usuários foi utilizado o sistema operacional Linux distribuição não comercial, com instalação tradicional e posteriormente adição de alguns pacotes necessários para certificação do usuário. O computador utilizado não necessitou de nenhuma configuração extraordinária, apenas interface de rede.

A rede Mesh foi realizada com roteadores que possuíam configuração mínima especificada pelo fornecedor do *firmware* e com custo/benefício mais acessível no mercado. *Firmware* utilizado foi de distribuição gratuita e acessível na Internet.

A integração dos procedimentos acima após vários testes e configurações foi de total sucesso, confirmando que é possível unir o acesso a Internet com uma centralização das configurações de rede e usuários. A interface de configuração pode ser acessada em modo texto ou modo gráfico, nesse último é empregado uma linguagem de fácil entendimento e bem intuitiva.

6.1 ESPECIFICAÇÕES DOS COMPONENTES DA PESQUISA

Todos os elementos foram criteriosamente escolhidos conforme especificações do *firmware* e ou tecnologia empregada na administração dos usuários solicitantes de acesso. Também se aplicou o critério de valor de hardware para uma possível implantação da solução, gerando um menor custo possível e mantendo a estabilidade do projeto.

a) **computador:** a instalação do sistema de controle de acesso deu-se em um computador Intel Pentium 4 3.0 Ghz, memória de 1GB DDR-2 e disco rígido de 160GB;
b) **sistema operacional:** Linux distribuição Debian 7.0 (Wheezy);
c) **roteador sem fios:** TP-Link TL-WR841n com uma interface WAN e quatro LAN;

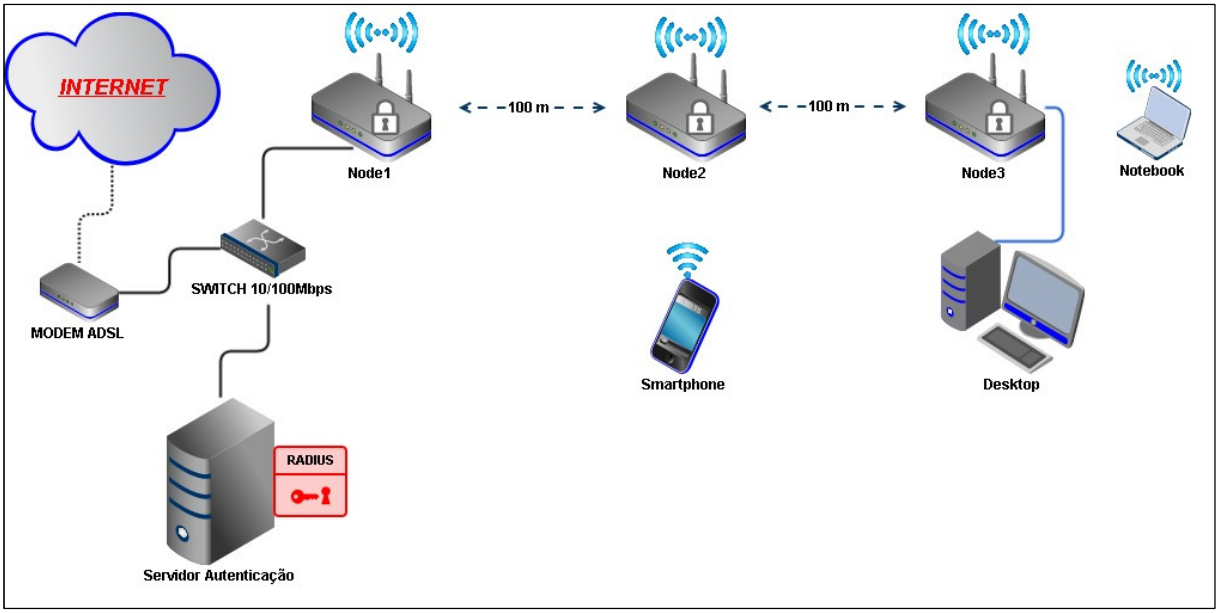
d) **firmware:** OpenWRT/Freifunk Attitude Adjustment Meshkit 12.09-rc1 (MeshKit/r35891/2013-03-09) com OLSR.

Demais configurações e pacotes instalados serão apresentados na sequência do trabalho, juntamente com suas opções mais indicadas no funcionamento do conjunto.

6.1.1Topologia Física Da Rede

A disposição física dos elementos da rede é exibida na figura 14 e representa o cenário real de como foram concebidos os testes de conectividade, autenticação e navegação.

Figura 14 – Topologia física da rede em teste.



Fonte: Do autor.

Conforme representado na figura 14a rede é composta por:

a) **Internet:** acesso à Internet para atualização/instalação dos pacotes necessários no funcionamento da rede Mesh;

b) **modem ADSL:** responsável por fazer a conexão com Internet;

c) **servidor autenticação:** autentica os usuários que pretendem entrar na rede Mesh;

d) **switch:** interliga o Modem com nó, no caso o “Node1”, onde irá disponibilizar o acesso a rede mundial de computadores;
e) **node1:** roteador wireless que possui conexão à Internet na porta WAN e a transfere para os demais repetidores e dispositivos;
f) **node2:** está no limite da área de cobertura de sinal do “Node1” e “Node3” e os interliga através de uma conexão Ad hoc sem fio;
g) **node3:** está no limite da área de cobertura de sinal do “Node2”, interligado através de uma conexão Ad hoc sem fio e não está ao alcance físico do “Node1”;
h) **smartphone:** dispositivo para testes de navegação, podendo alternar sua posição entre os nós de forma transparente;
i) **desktop:** computador físico que se conecta através de uma porta local à interface LAN do “Node3”;
j) **notebook:** equipamento para testes de conexão e aferição do sinal, podendo se deslocar pela área de cobertura da ESSID.

6.1.2 Firmware Designado

A escolha do *firmware* foi definida por meio de alguns requisitos, dentre eles, custo de aquisição conforme apêndice A, compatibilidade com as especificações mínimas do equipamento (memória e *chipset* wireless), disponibilidade de materiais para consulta, escalabilidade e funcionamento. O OpenWRT/Freifunk foi o *firmware* perfeito para uso nesse cenário. O Freifunk é de nacionalidade alemã e está presente em várias partes do mundo provendo o compartilhamento de recursos por meio das redes em malha.

O valor empregado na obtenção do *firmware* é zero, disponível no site *www.freifunk.net*. Desenvolvido especialmente para aparelhos que são dotados de configurações mais acessíveis, mostra compatibilidade com diversos modelos presentes no mercado. O software tem um gerenciador de pacotes onde os mesmos podem ser instalados, alterados ou removidos.

Na parte técnica o Freifunk permite configuração de rede Mesh com o protocolo OLSR ou *Better Approach To Mobile Ad-hoc Networking* (BATMAN), contêm algumas opções de virtualização de redes, controle de tráfego, ponte entre

interfaces, firewall, servidor de endereços de IP, gráficos de tráfego, entre outros que podem ser instalados conforme necessidade.

Outros *firmwares* testados, tais como o HS-MMMesh, DD-WRT e Sveasoft, não tinham interface de fácil compreensão, possibilidade de instalação de pacotes posteriores, incompatibilidade dos serviços necessários (RADIUS e Mesh), alto custo, conforme apêndice A, incapacidade de uso com dispositivos atuais e poucas opções de modificação.

6.1.3 Serviço de Autenticação

A utilização de um computador com sistema operacional de código aberto permite a manipulação, adaptação dos pacotes necessários e uma diminuição no custo de aquisição e manutenção, pois várias pessoas se dispõem em um proveito comum para aprimorar e garantir a funcionalidade do mesmo.

Linux possui uma comunidade de diversos desenvolvedores ao redor do mundo, procurando e corrigindo falhas de programação, o que garante a estabilidade do sistema em si. Como possui escalabilidade de softwares por utilizar uma linguagem única, é muito fácil encontrar programas para fins específicos, no caso da autenticação utilizou-se um pacote nomeado de FreeRADIUS versão 2.1.12, construída em dezembro 2012.

O FreeRADIUS integra-se à maioria das distribuições Linux e permite a configuração de várias diretivas de segurança no que tange o triplo A. É um programa de código aberto e implementado para autorizar ou não o ingresso do usuário na rede, possui mecanismos de confiança baseados em algoritmos atualmente seguros (WALT, 2011, tradução nossa).

Além da opção do FreeRADIUS, existem ainda o *Terminal Access Controller Access-Control System* (TACACS); o Kerberos, que trabalha com tickets e necessita que seus clientes tenham o horário sempre ajustado para evitar negação de serviço, pouco utilizado. Para os adeptos do sistema operacional Microsoft, a mesma comercializa uma opção em autenticação nomeada de *Internet Authentication Service* (IAS).

6.1.4 Roteador Sem Fio

O equipamento é responsável por abrigar o software de gerenciamento da rede em malha, encaminhar o tráfego requisitado ao destino e, nesse caso, fazer a comunicação entre os clientes e o servidor RADIUS, bem como prover acesso pelas interfaces LAN.

Todos os *firmwares* necessitam de um espaço na Memória Flash destinado ao funcionamento do mesmo, em roteadores mais simples esse espaço está sendo reduzido a fim de diminuir custos de produção. Alguns roteadores bem antigos possuíam essa área de memória um tanto que superior aos atuais, porém sua disponibilidade no mercado está baixa e isso eleva o seu valor.

De acordo com os equipamentos testados, o roteador da TP Link modelo TL-WR841N versão 8.1 de fabricação internacional, possui preço acessível e amplamente disponível no comércio, além de conter diferentes normas de qualidade e características técnicas ideais para o fim proposto.

O roteador que já foi abundantemente empregado em outras propostas e utilização para projetos de “Cidade Digital” não foi compatível com o *firmware* escolhido e apresentava tecnologia um pouco obsoleta é o WRT54GL da Linksys/Cisco possui pouca memória e trabalha apenas nos padrões 802.11b/g. O escolhido além de possuir tecnologia de transmissão atual, MIMO, também apresenta um processamento mais ágil, conforme se pode observar na tabela 4.

Tabela 4 – Comparativo entre roteadores sem fio.

Marca / Modelo	Memória Flash	Memória RAM	Processador	Velocidade Máxima
Linksys (Cisco) / WRT54GL	4 MB	16 MB	200 Mhz	54 Mbps
TP Link / WR841N	4 MB	32 MB	533 Mhz	300 Mbps

Fonte: Site dos fabricantes.

6.2 CONFIGURANDO O SERVIDOR DE AUTENTICAÇÃO

O servidor foi dotado do sistema operacional GNU/Linux distribuição Debian, uma das mais recentes e estáveis, tendo sua instalação apenas os pacotes

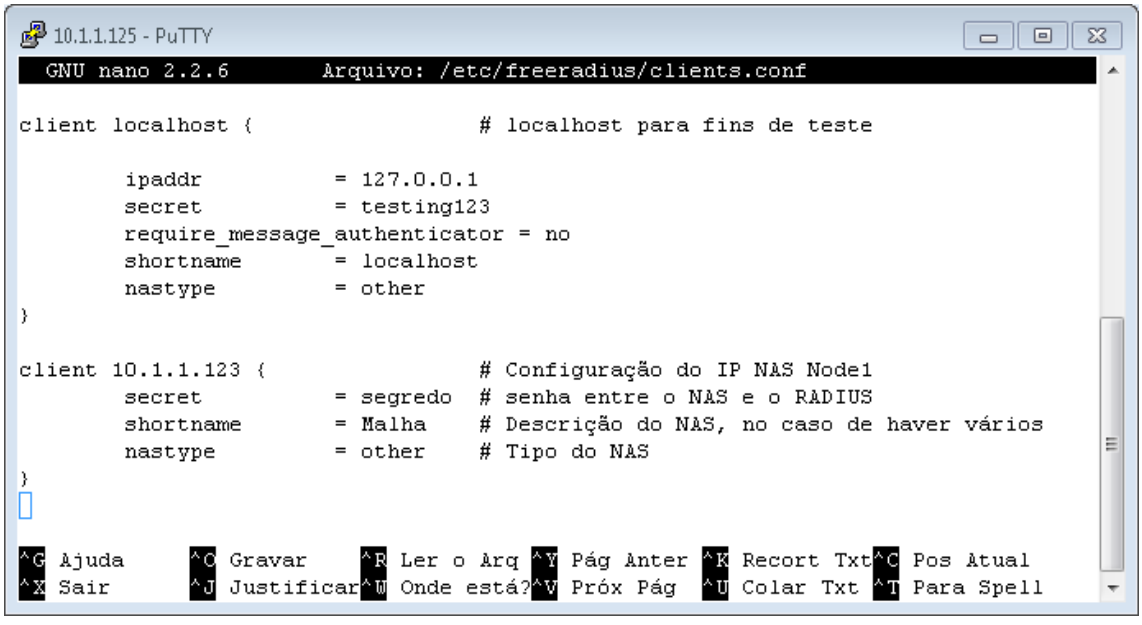
básicos e configurados para iniciar em modo texto. O requisito fundamental para desempenhar sua função é uma interface de rede compatível com padrão EIA/TIA 568A.

Os pacotes necessários para autenticação dos usuários no NAS são os seguintes: *mysql-client, mysql-server, freeradius, freeradius-utils e freeradius-mysql*. Todos foram instalados com o gerenciador de pacotes *Advanced Packaging Tool* (APT-Get) na seguinte sintaxe: `#apt-getinstall "nome do pacote"`

Após instalação das dependências e o programa desejado, foi necessário o ajuste dos arquivos para funcionamento do serviço. O FreeRADIUS possui dois arquivos principais, o *clients.conf* e o *users*, no primeiro definimos as características do NAS que permite acesso aos clientes.

O *clients.conf* está localizado no diretório `/etc/freeradius/`, nele pode-se configurar o IP do roteador, o segredo compartilhado com o servidor RADIUS, entre outros. A figura 15 apresenta parte do arquivo comentado anteriormente.

Figura 15 – Arquivo de configuração *clients.conf.*

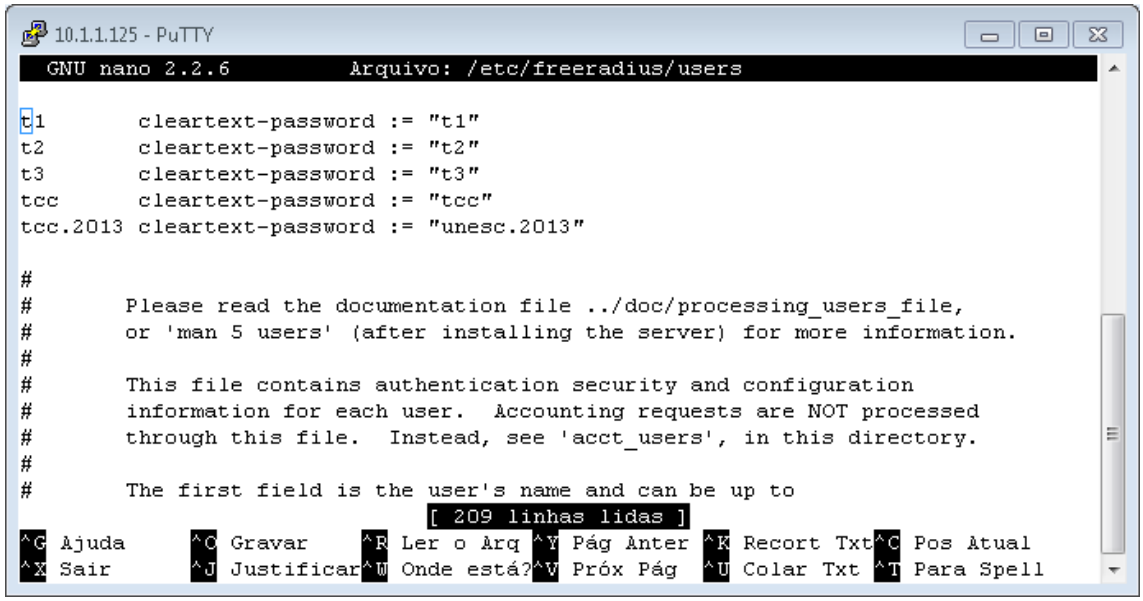


Fonte: Do autor.

O outro arquivo que contém os usuários propriamente autorizados é o *users* e está localizado no mesmo diretório que o *clients.conf*. Nele atribui-se o nome

de usuário e senha que serão conferidos no *login* do solicitante. Pode-se observar na figura 16 que existe a possibilidade de incluir vários usuários.

Figura 16 – Arquivo de configuração *users.*



Fonte: do autor.

Existe a possibilidade várias configurações no *users*, tais como mensagem de boas vindas, IP de origem do usuário solicitante, tipo de serviço admitido, modo de autenticação, dentre outros. Nessa pesquisa utilizou-se apenas a configuração básica na conferência de usuário e senha.

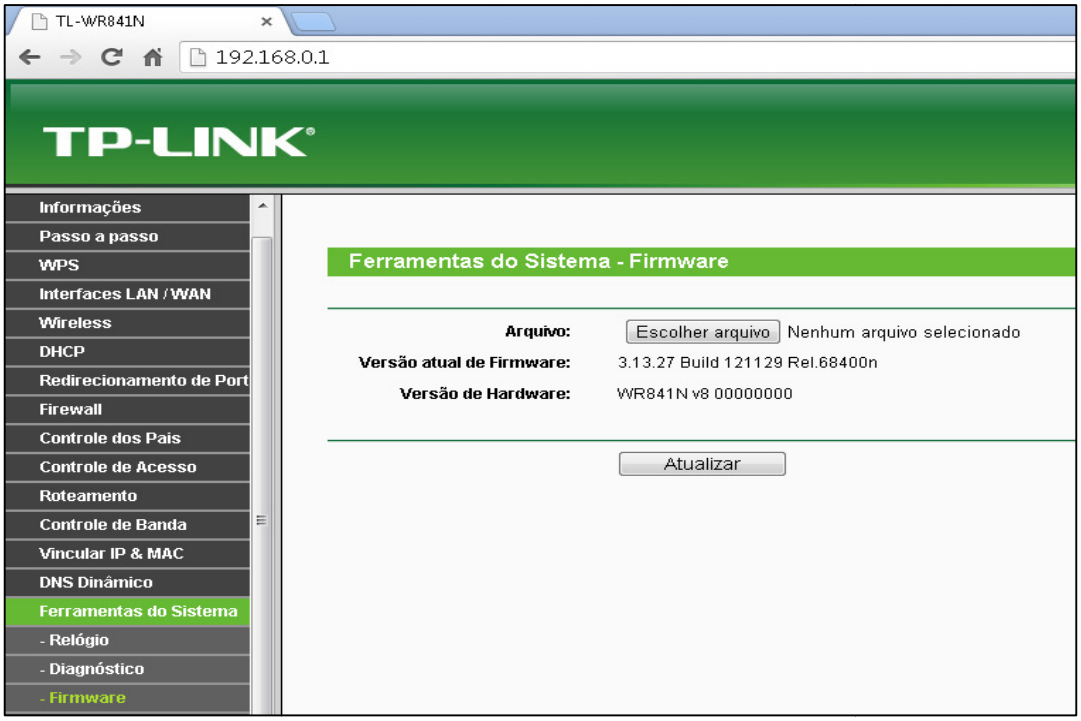
Após a instalação e ajustes dos arquivos requeridos, deve-se reiniciar o serviço *freeradius* para aplicar o conjunto de mudanças realizadas. A sintaxe para renovar o serviço em modo texto é `#service freeradius restart` ou vá à pasta onde o serviço se encontra, `/etc/init.d` e aplique o comando de parada do serviço, `#service freeradius stop` e em seguida reinicie-o com `#service freeradius start`.

A conclusão dos procedimentos acima deve criar condições para satisfazer um teste localmente no servidor mediante o comando *radtest "usuário" "senha" "nome da máquina" "porta" "senha"* no caso real ficaria desta maneira `#radtest tcc tcc localhost 1812 testing123`, se os dados inseridos estiverem corretos ele retorna uma mensagem de *Access-Accept*.

6.3 CONFIGURANDO O ROTEADOR COMO NÓ DA REDE MESH

O roteador utilizado vem de fábrica com *firmware* proprietário contendo funções básicas destinadas a usuários domésticos, existindo então a necessidade em efetuar o procedimento de substituição desse software para funcionamento da rede em malha. O acesso é obtido através do menu *>Ferramentas do Sistema >Firmware*. A figura 17 demonstra a tela para troca do *firmware* original.

Figura 17 – Interface de atualização do *firmware* no WR841N.



Fonte: Do autor.

O *firmware* pode ser personalizado conforme a necessidade da aplicação, nesse caso ele foi modificado seguindo as configurações mínimas de funcionamento para rede Mesh e às características do chip presente no roteador. Obtido através de um site que customiza o *firmware*, o Meshkit foi obtido em menos de um minuto e no atual momento computava mais de mil personalizações requeridas.

A customização através da web segue um perfil de configuração pré-definida, esse tem ligação direta com o nome de uma das cidades alemãs, onde já possuem alguns pontos Mesh com Freifunk, facilitando a instalação por um usuário leigo e posterior ampliação da rede conectada.

Após execução do método de atualização para o novo *firmware*, o Freifunk, percebe-se algumas mudanças visuais e de funções, inclusive a troca do IP para acesso à interface de configuração, agora modificada para 192.168.1.1, conforme exposta na figura 18.

Figura 18 – Interface do *firmware* Freifunk customizado.

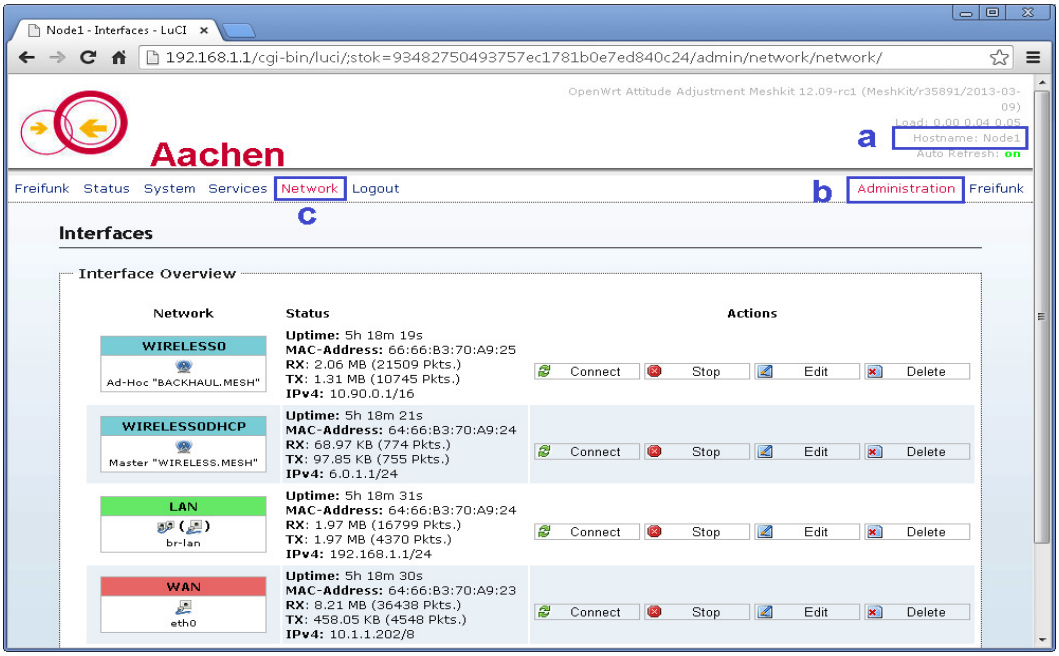
Fonte: Do autor.

Mesmo possuindo interface com linguagem estrangeira, esse *firmware* tem uma apresentação bem limpa e possui dicas para maioria dos ajustes. Os relatórios de dados referentes às conexões de rede, monitoramento de tráfego, identificação do aparelho e outras informações não necessitam de credencial para acesso, sendo apenas solicitada nas configurações técnicas.

O próximo passo para configuração da rede Mesh é obtido nas opções de interfaces do *firmware*, acessadas em *>Network >Interfaces*, necessário a substituição do IP das interfaces "*Wireless0", "Wireless0DHCP"* e *"LAN"*. Para o gerenciamento de vários nós e identificação das rotas, recomenda-se a troca do *hostname* na guia *>System*. Todos os procedimentos que envolva alteração das configurações devem ser feitas no modo "*Administration"* contido no menu superior direito, a senha padrão é "*admin*".

Para um fácil entendimento dos campos abordados no parágrafo anterior, eles foram destacados e demarcados na figura 19, sendo a identificação do *hostname* atribuída à letra “a”, o atalho para acesso como administrador na letra “b” e o menu onde se localizam as opções para configuração das interfaces de rede na letra “c”. Esses mesmos acessos podem ser encontrados em outras imagens personalizadas no site do *firmware*.

Figura 19 – Painel de interfaces de rede no *firmware* Freifunk.



Fonte: Do autor.

Ajustes nas interfaces dos roteadores foram necessárias para criação de uma rede Ad hoc entre eles, permitindo o total transporte de dados independentemente do nó solicitado. Um detalhe importante está em deixar a rede com mesmo SSID, frequência de operação e IP diferente dos demais nós.

A rede destinada à comunicação dos roteadores foi nomeada de “*Backhaul Mesh*” e configurada em modo Ad hoc. Para prover acesso à Internet criou-se a rede “*Wireless Mesh*”, que provê conexão aos dispositivos móveis através de atribuição dinâmica de endereço IP. A interface de rede “*WAN*” recebeu identificação somente no roteador que faz comunicação via cabo com o barramento da rede, pois será encarregada de trocar informações com o a porta LAN do

Servidor RADIUS. A interface “LAN” dos nós possui IP fixo e concedem conexão para *desktops* via cabo par trançado.

Para fins experimentais na avaliação de sinal recebido, foi empregada uma ferramenta de análise espectral, obtida na Internet e sem custos para uso não comercial. O inSSIDer versão 3.0.7.48 exibe na figura 20, os nós operando com a mesma identificação de rede e canal, porém com valor de sinal diferente, pois foi alterado propositalmente a potência de transmissão do aparelho para melhor visualização dos diferentes nós.

Figura 20 – Sinal da rede “Wireless Mesh” com os três nós.

Fonte: Do autor.

A escolha do canal foi realizada após verificação de todas as frequências utilizadas naquela área, dado que, a número um possuía menor interferência. A distinção lógica do equipamento foi realizada através do *Media Access Control* (MAC), número hexadecimal único para cada aparelho fabricado, uma vez que o canal e o identificador da rede eram idênticos. Ressaltando que a rede ainda não possuía sistema de encriptação nos roteadores.

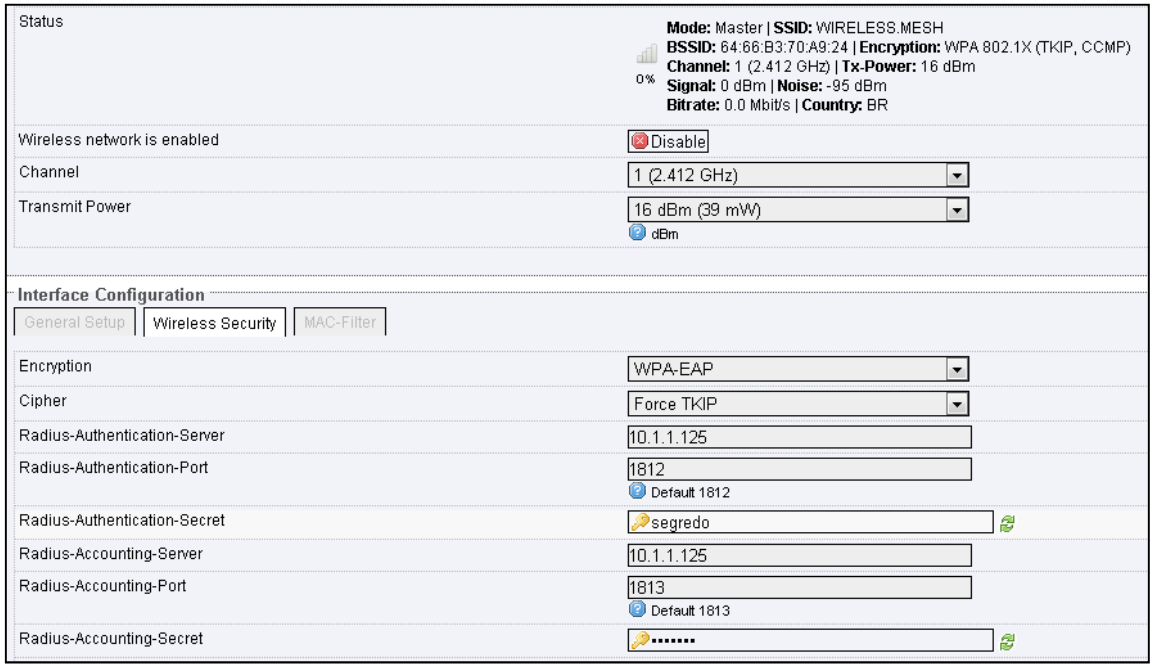
6.4 CONFIGURANDO O ROTEADOR COMO NAS

Os ajustes no roteador para comunicação entre o servidor RADIUS e o NAS se deram através de um *firmware* disponível na *web* e de custo livre. Desenvolvido a partir do OpenWRT, o Freifunk se mostrou bastante amigável e flexível nas configurações solicitadas.

Fez-se necessário a instalação do pacote *wpad* versão 20130405-1 para adicionar a funcionalidade de autenticação por método IEEE 802.1x/ WPA/EAP/RADIUS. Após instalação por meio do menu *>System>Software* contido no *firmware*, reiniciou-se o aparelho acessando o menu *>System >Reboot*.

A configuração da autenticação foi aplicada na interface “Wireless Mesh”, especificada para acesso à rede aos clientes. Em nossos testes foram aplicados a criptografia WPA-TKIP e o segredo foi definido por “segredo”, tudo devidamente conferindo com as configurações pré-ajustadas no servidor. Na figura 21 podem-se comparar as configurações do NAS com as contidas na figura 15 do servidor.

Figura 21–Módulo de configuração para autenticação 802.1x.



Fonte: Do autor.

6.5 RESULTADOS OBTIDOS

A rede Mesh foi elaborada juntamente com o protocolo OLSR e roteadores com bom desempenho, se comparado a outros dispositivos atuais no mercado. A sua função de interligar dispositivos por meio de saltos entre os nós foi completamente alcançada, satisfazendo o quesito de conexão com roteamento dinâmico.

O servidor de autenticação foi ajustado para realizar apenas a autenticação dos novos usuários na rede, permitindo o acesso somente através de usuário e senha válida, caso contrário não era validado seu ingresso. A tarefa foi alcançada de modo a restringir usuários inexistentes ou com senhas incorretas.

A seguir serão comentados detalhadamente os resultados das ações em separado e também com as tecnologias integradas e operando em total funcionamento.

6.5.1 TESTES DE CONECTIVIDADE

Após a configuração dos dispositivos empregados na construção da rede Mesh, foram realizados vários testes de conectividade a fim de certificar que todos os elementos estavam corretamente configurados e pertencentes à mesma rede em questão. Para comunicação das interfaces, de ambos os aparelhos, foram empregadas diferentes classes e máscaras de rede, conforme tabela 5.

Tabela 5 – Configuração das interfaces de rede nos dispositivos.

Equipamento	**LAN**	**WAN**	**Wireless / Mesh**	**Wireless / Ad hoc**
NAS	192.168.1.X / 24	DHCP*	6.0.1.X / 24	10.90.0.X / 16
RADIUS	10.1.1.125 / 8	na	na	Na
Dispositivos	DHCP	na	DHCP	Na
Modem ADSL	10.1.1.1 / 8	DHCP	na	Na

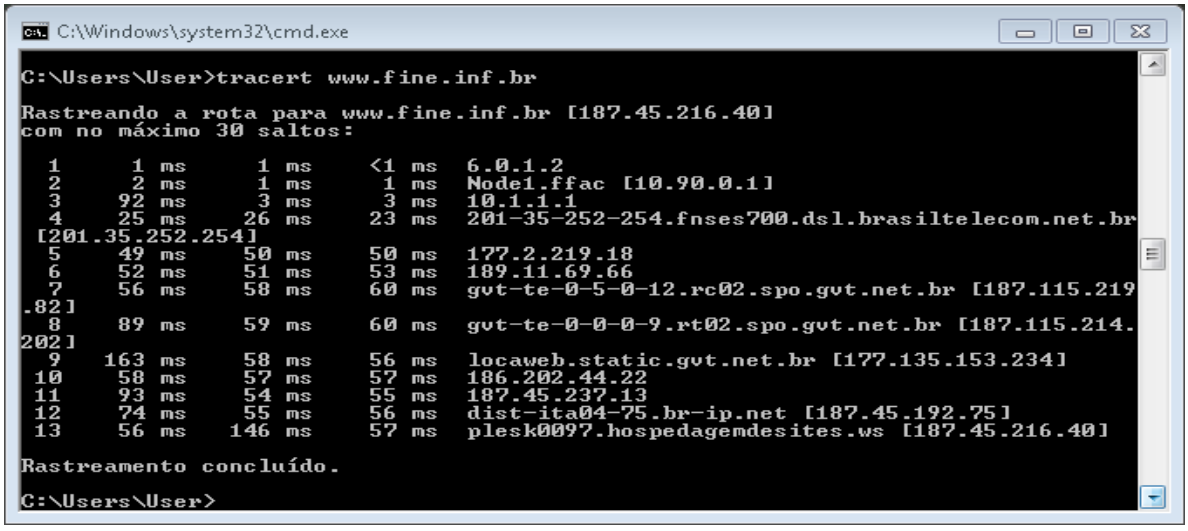
Nota. Fonte: Do autor. *NAS com conexão na porta WAN deve estar com IP atribuído conforme configurações no servidor RADIUS; na = não apresenta.

O *firmware* dispõe de módulos que exibem os nós vizinhos e as tabelas de roteamento, facilitando assim a análise em uma possível manutenção. No apêndice B é possível verificar as rotas e os vizinhos próximos ao “Node1”.

Testes foram realizados mediante topologia da figura 14 e sem a aplicação de criptografia no ingresso ao conjunto; no primeiro experimento o notebook conectou-se à rede “Wireless Mesh” por meio do “Node1” onde recebeu desse o IP, por meio de *Dynamic Host Configuration Protocol* (DHCP). Foram disparados pacotes de *Internet Control Message Protocol* (ICMP) com o comando *Packet Internet Grouper* (PING) contra o IP do “Node1”, “Servidor RADIUS” e endereço válido da Internet, todos responderam sem nenhuma perda de pacote.

O segundo teste incidiu com a conexão “*Wireless Mesh*” através do “Node2”, que estava interligado ao Node1 através da conexão “*Wireless Ad hoc*”, testes de Ping sobre “Node2”, “Node1”, “Servidor RADIUS” e Internet realizados com sucesso. A figura 22 exibe o trajeto percorrido entre a conexão do “Notebook” e um site qualquer, nota-se que a rota é iniciada no “Node2”, passando pelo “Node1”, logo após o “Modem ADSL” e em seguida pelos concentradores até atingir a máquina que hospeda o site.

Figura 22 – Rota de um pacote entre usuário e site solicitado.



Fonte: Do autor.

O terceiro experimento foi realizado com o notebook estando apenas na cobertura do sinal sem fio do “Node3”. Sinal wireless do “Node1” e “Node2” não

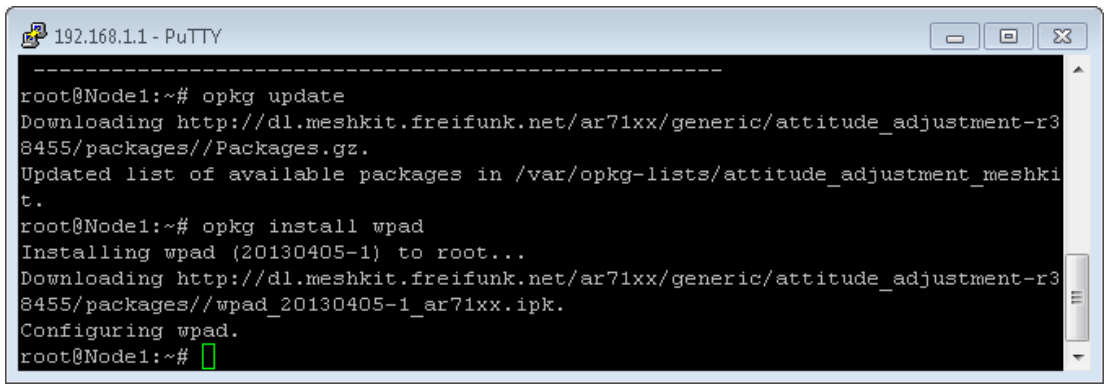
estava ao alcance do “Notebook”. Conexão na interface “*Wireless Mesh*” do “Node3” empreendida com sucesso, obtendo IP automaticamente e navegação à Internet.

6.5.2 APLICAÇÃO DE CRIPTOGRAFIA NA REDE

O emprego da autenticação, no início dos testes não foi feito, devido o fato de se isolar qualquer fator, e que esse viesse a causar algum comprometimento ao funcionamento da rede. Com todos os nós operacionais e trocando informações de roteamento mediante protocolo OLSR, inicia-se a instalação do pacote “wpad”, responsável pela autenticação dos usuários.

A configuração deste pacote pode ser efetuada no modo texto ou mesmo no modo gráfico, que é mais intuitivo ao administrador e não demanda conhecimento técnico em editores de texto Unix. Após instalação do pacote necessário, nesse caso instalado em modo texto conforme figura 23, cabe apenas a reinicialização do roteador para ativar o módulo de segurança.

Figura 23 – Instalação do pacote *wpad* em modo texto.

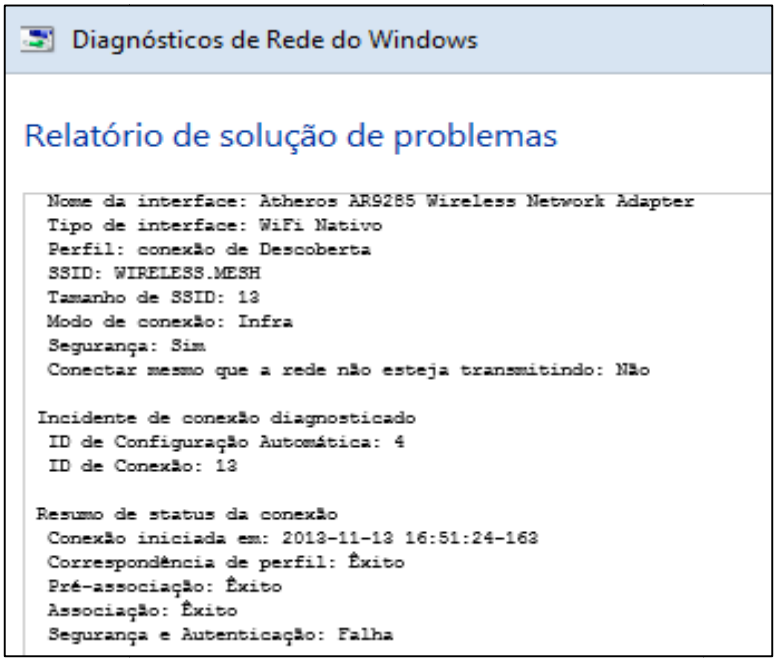


Fonte: Do autor.

O primeiro teste na nova rede dotada de segurança conforme os padrões 802.1x foram realizados através de um smartphone com sistema operacional iOs 7.0.3 e um notebook com sistema operacional Windows 7 SP1, ambos fizeram o pedido de ingresso na rede por meio do “Node2”, na sequência ao pedido de conexão na rede “*Wireless Mesh*” foi informado uma caixa de *login* solicitando usuário e senha. Na primeira tentativa simulou-se um usuário válido e senha incorreta, como usuário não existia na tabela do Servidor RADIUS ele negou o

acesso e o Windows retornou uma mensagem de erro conforme figura 24. O Smartphone não conectou sem exibir erro algum. Na segunda tentativa foram inseridos dados válidos e o acesso foi garantido à ambos de modo transparente.

Figura 24 – Mensagem erro no acesso não autorizado pelo servidor.



Fonte: Do autor.

O segundo teste foi realizado com um notebook que estava na área de cobertura sem fio do “Node3”, ao solicitar ingresso na rede o mesmo foi convidado a informar credenciais de identificação, usuário e senha. Com o acesso à Internet através do “Node3” foi realizado um teste de proximidade do “Node2” e desligou-se o “Node3”, em poucos segundos a conexão foi associada ao novo nó que proveu o mesmo tipo de acesso.

O teste final contou com outro dispositivo, um *tablet*, agora utilizando o sistema operacional Android 4.0.3 Ice Cream Sanduiche, nesse último experimento foi objetivada a conexão da rede por meio de um dos nós distanciados de mesmo modo, constatou-se que o roteador escolhido sempre era o de melhor sinal na ocasião, conectando momento por um e momento por outro. Realizou-se ainda o teste de deslocamento entre as áreas de cobertura dos nós, obtendo *roaming* automático entre os aparelhos.

7 CONCLUSÃO

Mediante a ampla utilização de dispositivos móveis no mundo atual, necessita-se a ampliação da cobertura nas comunicações sem fios, prezando sempre pela boa qualidade do sinal, disponibilidade e segurança no tráfego das informações. A idéia de se levar acesso à Internet aos menos favorecidos socialmente implicou na busca por métodos não convencionais, já que esses agregam um custo elevado de aquisição, implantação e manutenção. A utilização de tecnologias existentes vinculadas ao desenvolvimento de programas que pudessem uní-los resultou nas redes em malha.

As redes Mesh surgiram pra contemplar a mobilidade exigida pelo público que precisa de conectividade ubíqua e também para aqueles que não possuem infraestrutura e condições suficientes de implantação de uma rede com tamanha abrangência. A disponibilização de uma rede ampla foi uma barreira superada pela pesquisa e adaptação, agora nos deparamos com um fator relacionado ao mau uso dessa tecnologia. A segurança da informação zela não somente pela confidencialidade dos dados, mas também pelo bem estar e pela velocidade de comunicação.

As redes descentralizadas proclamam a liberdade de conexão em qualquer ambiente, sendo esse o mais longínquo ou mesmo em grandes centros comerciais onde milhares de pessoas utilizam os mais variados equipamentos de compartilhamento de conteúdo. A aplicação de uma solução que identifique e avalie os usuários de uma rede “aberta” é de grande valia para adotar decisões sobre os nós que prejudicam de alguma forma o sistema num todo.

Um dos componentes de segurança da informação foi implantado em uma rede Mesh, experimental, de modo a autenticar os usuários que por ela requeriam acesso à Internet. Várias tecnologias foram integradas nessa solução, como software livre, dispositivos portáteis, redes de computadores, transmissão sem fios e protocolos de roteamento.

Após diversos testes com a estrutura montada e adequada a uma situação real, pode-se perceber que o advento da mobilidade é algo extraordinário e quase imperceptível nas redes em malha. Constatou-se a eficácia do serviço FreeRADIUS na autenticação dos usuários, sempre negando acesso aos roteadores e requerentes não listados em sua tabela de autorização. O fato de cada usuário

possuir uma senha individual e controle sobre o que utiliza, o torna mais responsável no manejo dos recursos a ele confiado.

Concluiu-se que é possível a utilização de um servidor de AAA nessas redes descentralizadas que não apresentem tamanho totalmente definido. O protocolo utilizado conseguiu encaminhar todas as solicitações de ingresso a rede e sempre optou pela melhor rota, levando em consideração que a rede estava com alto nível de criptografia aplicada.

Os testes de disponibilidade da rede, tráfego de informações, conexão através de todos os nós, seleção de melhor rota e mobilidade foram todos positivos, mesmo utilizando tecnologias recentes e algumas em fase final de lançamento, como a versão do firmware utilizado.

Algumas dificuldades foram encontradas na escolha do equipamento responsável pelo acesso sem fio. Em alguns trabalhos e projetos pesquisados optou-se por utilizar um dispositivo que não era tão acessível em termos de custos e disponibilidade, e inclusive em capacidade de processar as requisições de uma rede dinâmica. O problema foi contornado mediante substituição do firmware que era compatível com equipamentos disponíveis no mercado.

Os firmwares disponíveis são bem operacionais, porém não são simples de realizar configurações desejadas, necessitando na maioria das vezes um conhecimento mais profundo em outras áreas para colocá-lo em funcionamento, mas o infortúnio de uma possível manutenção acaba descartando-o como opção favorável.

Unir dois sistemas distintos, autenticação de usuário e redes Mesh com protocolo de roteamento pró-ativo, foi uma tarefa bem desafiadora, pois abordou temas que são, usualmente, empregados de formas distintas. Mesclar diferentes tecnologias pode agregar o valor da solução e consequentemente obterem melhores resultados.

A sugestão para trabalhos futuros seriam pelo menos três aplicações nesse mesmo foco de pesquisa, a ampliação do acesso sem fios e a segurança aplicada. A primeira consiste em fazer um controle efetivo do usuário em uma rede empresarial privada, definindo horários de uso, dispositivos permitidos mediante usuário informado e até mesmo cota de utilização dos serviços solicitados. Outro ponto importante seria desenvolver e aplicar juntamente algumas políticas de plano de segurança à rede corporativa.

A segunda proposta de pesquisa está no âmbito da rede em malha e uma aplicação de painéis solares inteligentes, garantindo a auto-sustentabilidade da estrutura, entregando o acesso às regiões mais remotas ainda ou em parques florestais, com objetivo de comunicação entre possíveis identificadores anexos aos animais para coleta dos dados sobre seus hábitos de locomoção.

A terceira sugestão poderia contemplar uma rede em malha na própria Universidade do Extremo Sul de Santa Catarina para fins de pesquisa nos protocolos de roteamento, observando o comportamento da rede à medida que aumentam os nós e futuramente após essa análise, a aplicação da estrutura em toda abrangência do *campus* e vizinhança.

REFERÊNCIAS

AKYILDIZ, Ian F.; WANG, Xudong. **A Survey on Wireless Mesh Networks**. IEEE Radio Communications, Setembro 2005. Disponível em: <http://www.ece.gatech.edu /research/labs/ bwn/papers/2005/j4.pdf>. Acesso em 10 ago. 2013, 16:40:00.

ALBUQUERQUE de, Célio Vinícius Neves et al. **Rede Mesh de acesso universitário faixa larga sem fio.** Rede Nacional de Pesquisas, Setembro 2005. Disponível em: <http://www.rnp.br/_arquivo/gt/2005/GT_Rede_Mesh.pdf>. Acesso em 29 ago. 2013, 20:30:00.

CERT.br. **Cartilha de Segurança para Internet.** Versão 4.0. São Paulo: Comitê Gestor da Internet noBrasil, 2012. Disponível em: <http://cartilha.cert.br/livro/ cartilha-seguranca-internet.pdf>. Acesso em 8 nov. 2013, 19:00:00.

COMER, Douglas E. **Interligação de redes com TCP/IP** - Princípios, protocolos e arquitetura vol. 1. Rio de Janeiro: Elsevier, 2006.

DEC et al. **RFC 6911: RADIUS Attributes for IPv6 Access Networks**. Abril 2013. Disponível em <http://tools.ietf.org/pdf/rfc6911.pdf>. Acesso em 15 set. 2013, 20:10:00h.

DUARTE, C. A. A. **A evolução dos protocolos de segurança das redes sem fio -** do WEP ao WPA2 passando pelo WPA**.** 2010. 51 f. Monografia (Pós-Graduação em Redes de Computadores) - Escola Superior Aberta Do Brasil – Espírito Santo, 2010.

FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores**. 3. ed. Porto Alegre: Bookman, 2006.

FUNABIKI, Nobuo. **Wireless Mesh Networks.** India: InTech, 2011.

GAST, Matthew S. **802.11 Wireless Networks** - The Definitive Guide - Creating and Administering Wireless Networks. California: O´Reilly, 2002.

HASSELL, Jonathan et al. **RADIUS**. California: O'Reilly, 2002**.**

HELD, Gilbert. **Wireless Mesh Network**. Flórida: Auerbach Publications, 2005.

HOSSAIN, Ekran; LEUNG, Kin K. **Wireless Mesh Networks: Architectures and Protocols.** Nova Iorque: Springer, 2007.

IEEE.**Status of Project IEEE 802.11s.** Julho 2011. Disponível em <http://grouper.ieee.org/groups/802 /11/Reports/tgs_update.htm>. Acesso em 25 set. 2013, 19:00:00.

International Development Research Centre - IDRC.**Redes sem fio no mundo em desenvolvimento**. Setembro 2008. Disponível em <http://wndw.net/download /WNDW_Standard.pdf>. Acessoem 18 set. 2013, 15:00:00.

KHAN, Shafiullah; PATHAN, Al-Sakib Khan. **Wireless Networks And Security** - Issues, Challenges And Research Trends. Berlin: Springer, 2013.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a Internet**- uma abordagem top-down. 5. ed. São Paulo: Pearson Addison Wesley, 2010.

METHLEY, Steve. **Essentials of Wireless Mesh Networking.** Nova Iorque: Cambridge University Press, 2009.

MISRA; Sudip, Subhas Chandra; WUONGANG, Isaac. **Guide to Wireless Mesh Networks.** Londres: Springer, 2009.

MORAES, Alexandre Fernandes de. **Redes sem Fio** - Instalação, Configuração e Segurança: Fundamentos. São Paulo: Érica, 2010.

MORIMOTO, Carlos E. **Redes e Servidores** - Guia Prático. 2. ed. São Paulo: GDH Press e Sul Editores, 2008.

NAKHJIRI, Madjid; Mahsa.**AAA and Network Security for Mobile Access** - Radius, Diameter, EAP, PKI and IP Mobility. Wiltshire: John Wiley& Sons, 2005.

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

RAPPAPORT, Theodore S. **Comunicação sem fio: princípios e práticas.** 2. ed. tradução Daniel Vieira. São Paulo: Pearson Prentice Hall, 2009.

RUBINSTEIN, Marcelo G. et al. **A Survey on Wireless Ad hoc Networks.** PEL/DETEL/FEN – Universidade do Estado do Rio de Janeiro, 2006.

RUFINO, Nelson Murilo de Oliveira. **Segurança em Redes sem Fio: Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth.** 3. ed. São Paulo: Novatec, 2011.

SANTOS, R. R. **Implementação de uma rede sem fio Mesh com autenticação centralizada utilizando um servidor RADIUS**. 2012,69 f. Trabalho de Conclusão de Curso (Curso de Tecnologia em Sistema para Internet). Universidade Tecnológica Federal do Paraná. Curitiba, 2012.

SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER, Sérgio. **Redes de Computadores: Das LANs, MANs e WANs às Redes ATM**. 2. ed. Rio de Janeiro: Campus, 1995.

STALLINGS, Willian. **Wireless Communications and Networks**. 2. ed. Nova Jérsei: Pearson Prentice Hall, 2005.

STEMMER, Ricardo Marcelo. **Redes Locais industriais: A Integração da produção através das redes de comunicação**. Florianópolis: UFSC, 2010.

TANENBAUM, Andrew S. **Redes de Computadores**. 4. Ed. Rio de Janeiro: Campus, 2003.

THOMAS, Tom. **Segurança de Redes - Primeiros Passos.** Rio de Janeiro: Ciência Moderna, 2007.

TSE, David; VISWANATH, Pramod. **Fundamentals of Wireless Communication.** Nova Iorque: Cambridge University Press, 2005.

XIAO, Yang; SHEN, Xuemin; DU, Ding-Zhu.**Wireless Network Security**. Nova Iorque: Springer, 2007.

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

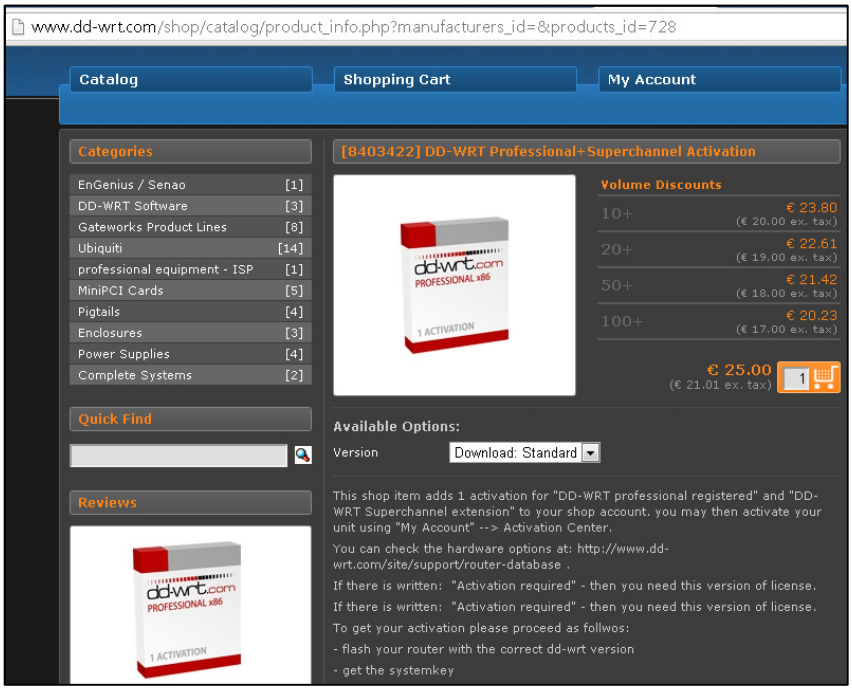
ZHANG, Yan; LUO, Jijun; HU, Honglin.**Mesh Networking - Architectures, Protocols and Standards.** Nova Iorque:Auerbach Publications, 2007.

ZHANG, Yan; ZHENG, Jun; HU, Honglin.**Security in WirelessMesh Networking.** Flórida:Auerbach Publications, 2009.

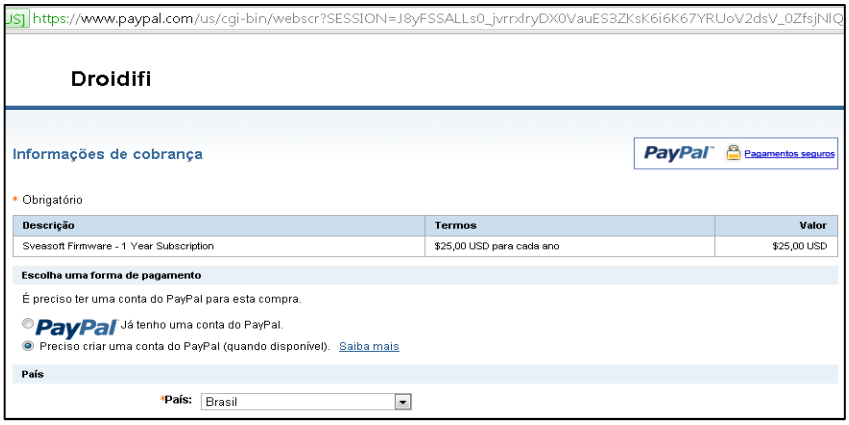
ZHOU, Hongbo. **Wireless Ad-Hoc Networks.** Croácia: InTech ,2012.

APÊNDICE A – REFERÊNCIA DE VALORES PARA FIRMWARES MESH

Abaixo a captura de tela dos sites que comercializam o firmware e seu suporte. Pode-se ver na primeira imagem o custo do firmware DD-Wrt e na sequência o Sveasoft. O valor atual da licença de uso para o DD-Wrt é aproximadamente R$ 78,00, sem taxas. O firmware Sveasoft é comercializado por assinatura anual a um custo próximo de R$ 60,00.



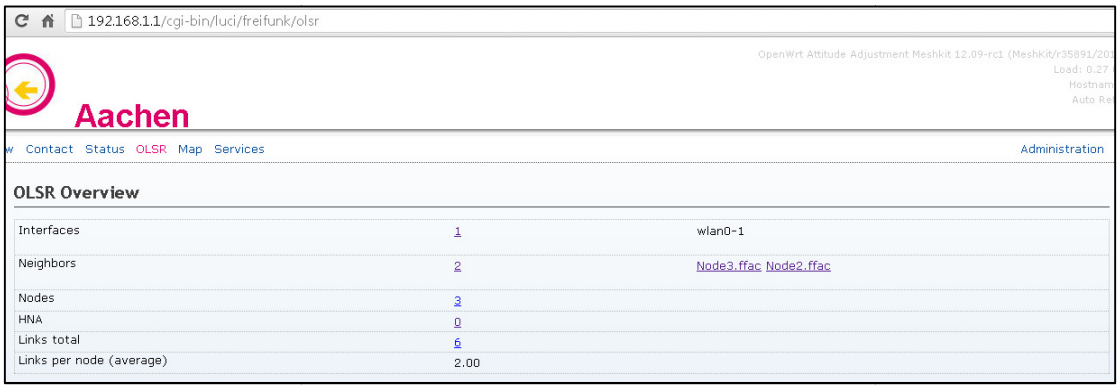
Fonte: Site www.dd-wrt.com/shop/catalog/.



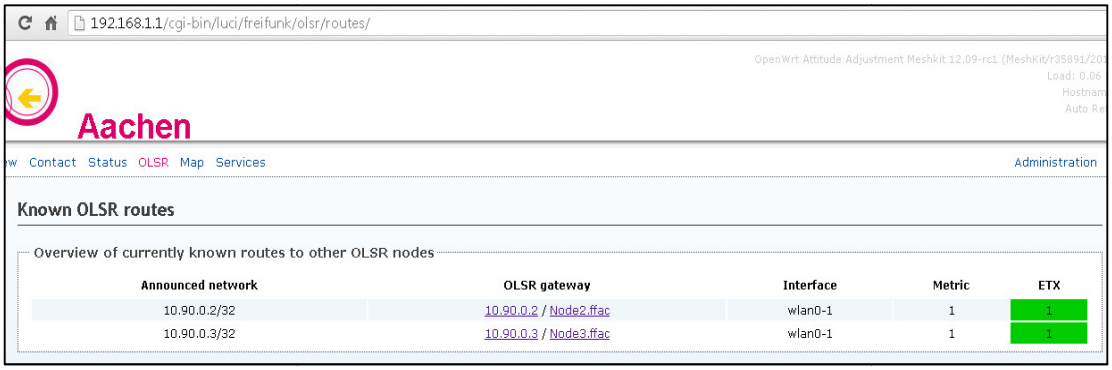
Fonte: Site http://www.sveasoft.com/index.php/buy-firmware.

APÊNDICE B – INFORMAÇÕES SOBRE O GERENCIADOR OLSR

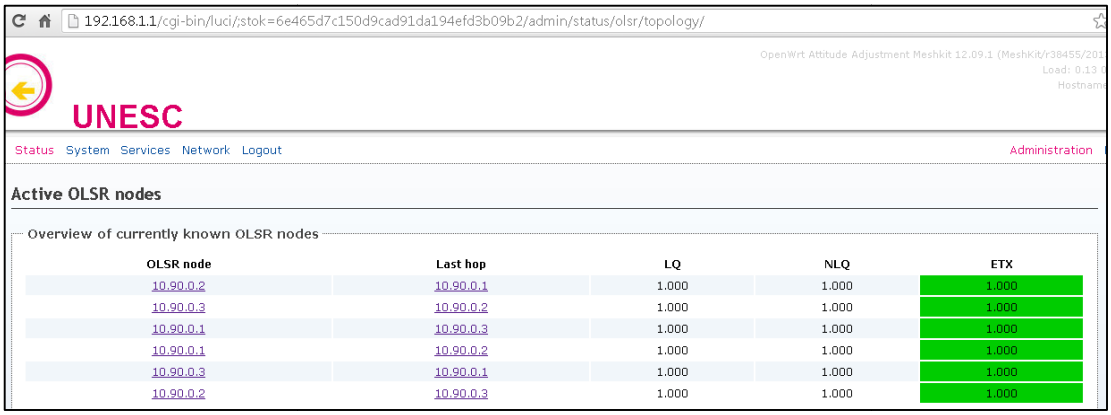
Assim que os nós estão configurados corretamente na rede, o roteador localiza os nós vizinhos e agrega a sua rede, criando uma malha entre os nós, abaixo nas figuras podem-se ver em painel geral sobre as conexões OLSR, possíveis rotas e nós ativos, respectivamente.



Fonte: Do autor.



Fonte: Do autor.



Fonte: Do autor.