UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC

CURSO CIÊNCIA DA COMPUTAÇÃO

GILSON ROBERTO PASETO

VPN EM UMA REDE SEM FIO MESH UTILIZANDO O PROTOCOLO DE ROTEAMENTO OLSR

CRICIÚMA, DEZEMBRO DE 2011

GILSON ROBERTO PASETO

VPN EM UMA REDE SEM FIO MESH UTILIZANDO O PROTOCOLO DE ROTEAMENTO OLSR

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

Orientador: Prof. MSc. Paulo João Martins

CRICIÚMA, DEZEMBRO DE 2011

GILSON ROBERTO PASETO

VPN em uma Rede Sem Fio Mesh Utilizando o Protocolo de Roteamento OLSR

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

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

Banca Examinadora:

Prof. MSc. Paulo João Martins (UNESC)
Orientador

Prof. MSc. Rogério Antônio Casagrande (UNESC)

Prof. Gilberto Vieira da Silva (UNESC)

Dedico este trabalho aos meus pais e minha família, que sempre me incentivaram dando força para seguir em frente, e a todos que me ajudaram e principalmente a mim.

AGRADECIMENTOS

Agradeço primeiramente a Deus, por tudo de bom que acontece em minha vida, por minhas conquistas, e principalmente quando preciso de forças para seguir em frente.

Agradeço a minha família, por toda atenção, dedicação e compreensão que me deram durante esta longa caminhada.

Agradeço aos amigos e colegas que me incentivaram e me ajudaram de todas as formas possíveis.

Agradeço a Tamilis F. Bif que esteve sempre esteve ao meu lado pra todas as horas me aconselhando e me ajudando.

Agradeço ao meu professor e orientador Paulo João Martins, pelo empenho, dedicação e atenção que teve em me mostrar quais os devidos caminhos a serem tomados.

RESUMO

As redes sem fio estão em constante evolução, porém os usuários devem sempre estar ao raio de alcance do dispositivo que transmite o sinal. Para aumentar esse raio surgiram as redes Mesh, onde por meio de *Firmwares* e protocolos compatíveis é possível aumentar seu alcance. Este trabalho tem por objetivos o estudo das redes sem fio, redes Mesh, protocolo de roteamento OLSR e da Virtual Private Network. Onde foi possível verificar e implantar esta tecnologia em dois roteadores por meio da utilização do Freifunk que tem disponível o protocolo OLSR para a implantação das redes Mesh e posteriormente a criação da VPN entre eles. Após instalação e configuração foi possível efetuar testes, onde verificou-se o completo funcionamento da rede sem fio e também da rede virtual privada. Sendo assim teve-se um maior raio de disponibilidade do sinal sem fio e por meio da VPN pode-se perceber que existe segurança, onde na conexão via LAN foi possível ter os dados totalmente criptografados, porém por não haver nenhum método de segurança para com os clientes que utilizam a conexão sem fio, houve a captura das informações que trafegavam pela mesma.

Palavras chave: Freifunk; Protocolo OLSR; Redes Sem Fio; Redes Mesh; VPN.

ABSTRACT

The Wireless Networks are constantly evolving, but users should always be in the range of the device that transmits the signal. To increase this range appeared in the Mesh Networks because of the Firmware and compatible protocols can increase their reach. This work aims to study wireless networks, Mesh Networks, OLSR routing protocol and Virtual Private Network. Where it was possible to verify and implant this technology on two routers through the use of Freifunk, which is available in the OLSR protocol for the implantation of Mesh, and then creating the VPN between them. After installation and configuration it was possible to perform tests, where there was a fully functional wireless network and virtual private network. So, this had a great range of availability of the wireless signal because of the VPN and you can have security, where the LAN connection was possible to have the data fully encrypted, but there is no security method for the customers using the wireless connection, there is a capture of information that travel through it.

Palavras chave: Freifunk; OLSR Protocol; Wireless Network; Mesh Network; VPN.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS E ABREVIATURAS

3DES	*Triple Data Encryption Standard*
AES	*Advanced Encryption Standard*
AH	*Authentication Header*
AM	*Amplitude Modulation*
AODV	*Ad Hoc On-Demand Distance Vector*
CEDAR	*Core Extraction Distributed Ad Hoc Routing*
DARPA	*Defense Advanced Research Projects Agency*
DCMP	*Dynamic Core-Based Multicast Routing Protocol*
DES	*Data Encryption Standard*
DSDV	*Destination-Sequenced Distance-Vector*
DSR	*Dynamic Source Routing*
DSSS	*Direct Sequence Spread Spectrum*
ESP	*Encapsulating Security Payload*
FHSS	*Frequency Hopping Spread Spectrum*
FM	*Frequency Modulation*
FTP	*File Transfer Protocol*
HNA	*Host and Network Association*
IANA	*Internet Assigned Numbers Authority*
IEEE	*Institute of Electrical and Electronic Engineers*
IETF	*Internet Engineering Task Force*
IKE	*Internet Key Exchange*
INRIA	*Institut National de Recherche en Informatique Et en Automatique*
IP	*Internet Protocol*

IPSec	*Internet Protocol Security*
IPV6	*Internet Protocol Version 6*
ISAKMP	*Internet Security and Key Management Protocol*
L2F	*Layer 2 Forwarding*
L2TP	*Layer 2 Tunneling Protocol*
LAN	*Local Area Network*
MAC	*Media Access Control*
MANET	*Mobile Ad-Hoc Network*
MAODV	*Multicast Ad Hoc On-Demand Distance Vector*
MID	*Multiple Interface Declaration*
MPR	*Multipoint Relay*
MZRP	*Multicast Zone Routing Protocol*
NAT	*Network Address Translation*
ODMRP	*On-Demand Multicast Routing Protocol*
OFDM	*Orthogonal Frequency Division Multiplexing*
OLSR	*Optimized Link State Routing*
P2P	*Peer-to-Peer*
PM	*Phase Modulation*
PPP	*Point-to-Point Protocol*
PPTP	*Point-to-Point Tunneling Protocol*
PTP	Point-to-Point
QoS	*Quality of Service*
RC4	*Ron's Code 4*
RFC	*Request For Comments*
RRD	*Round Robin Database*

RSA	*Rivest Shamir Adleman*
SPF	*Shortest Path First*
SSH	*Secure Shell*
SSL	*Secure Socket Layer*
TC	*Topology Control*
TTL	*Time To Live*
UDP	*User Datagram Protocol*
VoIP	*Voice Over Internet Protocol*
VPN	*Virtual Private Network*
WEP	*Wired Equivalent Privacy*
Wi-Fi	*Wireless Fidelity*
WLAN	*Wireless Local Area Network*
WMN	*Wireless Mesh Networks*
WPA	*Wi-Fi Protected Access*
WPA2	*Wi-Fi Protected Access 2*
WRP	*Wireless Routing Protocol*
ZRP	*Zone Routing Protocol*

SUMÁRIO

1 INTRODUÇÃO

No mundo globalizado é imprescindível a convivência e a utilização dos meios tecnológicos para nosso aperfeiçoamento, podendo citar mais precisamente a Internet onde é possível trocar informações com o mundo todo. Para poder usufruir deste grande poder de obtenção de conhecimento é necessário à pessoa estar ligada a uma rede, seja ela com fio ou sem fio, e estar conectada a Internet.

O padrão de redes sem fio IEEE 802.11, conhecidas mais popularmente como *Wireless Fidelity* (Wi-Fi) ou *Wireless* (sem fio), proporciona o acesso sem fio a redes de computadores.

Os sinais de redes sem fio geralmente são transmitidos por rádio frequência, sendo assim não necessitam de uma conexão física com computadores, porém necessita-se apenas de uma antena para a comunicação. Por meio desta rádio frequência forma-se uma rede sem fio onde será possível transmitir dados por meio de ondas de rádio eletromagnéticas (COMER, 2001).

Na conexão com a rede onde utiliza-se o fio como o meio de ligação e transmissão de informações o usuário fica limitado ao local onde se tenha um ponto disponível para o acesso. Na conexão com a rede sem a utilização do fio como meio de conexão o usuário elimina a necessidade de utilização de cabos e tem uma maior mobilidade, ficando dependente do sinal de algum dispositivo que distribua a conexão, porém ele fica limitado ao raio em que o aparelho consegue transmitir o sinal.

Foi então que surgiu um novo modelo em conexão de redes sem fio. As Redes Mesh também conhecida como redes em malha, vieram com o intuito de prover esta mobilidade disponível dos aparelhos sem fio, mas não de ficar limitada ao raio de conexão somente de um aparelho. Com isto é possível fazer com que vários equipamentos se

comuniquem entre si, ou seja, apesar de se ter vários aparelhos provendo sinal sem fio, o usuário terá a visão de apenas uma única rede.

Por ser uma tecnologia recente, estas redes precisam de estudos mais aprofundados. Uma questão muito sensível é a de segurança, pois há sempre a necessidade de se ter mecanismos de segurança bem desenvolvido para evitar que intrusos se aproveitem das informações transmitidas pela rede.

Sendo assim uma rede segura precisa ter uma comunicação segura, onde é necessário que a mensagem seja confidencial, tenha autenticação para confirmar a identificação de quem está transmitindo, seja íntegra para assegurar que a mensagem que foi enviada não tenha sido alterada em seu percurso. Por fim o gerenciador da rede precisa ter um controle de acesso dos usuários da sua rede, a fim de garantir a legitimidade (KUROSE; ROSS, 2006).

O protocolo *Optimized Link State Routing* (OLSR), é um dos principais protocolos de roteamento para redes Mesh. Está na categoria dos protocolos pró-ativos, cujo objetivo é periodicamente fazer a troca de informações com os nós da rede a fim de atualizar sua tabela de roteamento.

A *Virtual Private Network* (VPN) é um mecanismo utilizado para se ter uma maior segurança na transmissão de dados pela rede. Onde a VPN utiliza protocolos de criptografia por tunelamento, ou seja, os dados vão trafegar por um túnel onde estas informações estarão seguras durante sua transmissão.

1.1 OBJETIVO GERAL

Estudo do protocolo de roteamento OLSR e implementação de uma rede virtual privada.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos seguem abaixo:

a) aplicar os conceitos de redes sem fio MESH;

b) analisar e descrever alguns métodos de ataques em redes sem fio;

c) descrever a cerca dos métodos de segurança em redes sem fio;

d) descrever sobre o protocolo de roteamento OLSR;

e) aplicar e entender os conceitos acerca da Virtual Private Network.

1.3 JUSTIFICATIVA

As redes sem fio estão tendo uma enorme aceitação no mercado tanto para os usuários domésticos como para as organizações públicas e privadas, devido a seu baixo custo na implantação e por ser bastante acessível. Com isso está ocorrendo grande ascensão das redes sem fio em malha por cobrir um campo maior, sendo mais maleável ao acréscimo de novos equipamentos para a sua expansão.

As redes sem fio Mesh são compostas por pontos de acesso sem fio, estes pontos são considerados como nós de uma rede, onde a comunicação é dada por meio de *multi-hop* (múltiplos saltos) até chegar a seu destino. Neste modelo de rede não há a necessidade de ser ter um nó central.

Wireless Mesh Networks (WMN) ou redes sem fio em malha são formados basicamente por Roteadores e Clientes Mesh, onde o primeiro possui uma mobilidade mínima e formam um *backbone* (espinha dorsal) da rede em malha onde é possível a integração de outros tipos de redes. O segundo é possível criar a rede somente acrescentando novos

aparelhos sem a necessidade de ter um backbone[1] central provedor de sinal, porém é necessário configurar todos os aparelhos (AKYILDIZ; WANG, 2009, tradução nossa).

As redes em malha também são conhecidas como redes comunitárias devido a sua fácil integração de centros de cidades de forma simples e barata. Existem projetos implantados em pequenos centros de cidades onde por meio desta tecnologia, foi disponibilizada a conexão com a Internet com a maioria da população a fim de oferecer a inclusão digital e interligar pequenos estabelecimentos públicos como as escolas.

No modo como a rede trabalha pode observar-se que é possível haver a integração de vários tipos de redes, como as redes de celulares e as via cabo, desse modo as redes Mesh perderam o caráter centralizado, devido ao poder de se auto-configurar e auto-organizar além de cada nó poder se comportar como repetidor de sinal (FONTOURA, 2007).

As redes Mesh são redes *ad-hoc* que significa "para este objetivo". Elas são semelhantes às redes *ad-hoc*, pois ambas utilizam transmissão sem fio, tem sua topologia dinâmica, variável e seu crescimento é orgânico, portanto a sua principal diferença é que os seus nós têm sua localização fixa, porém seu local não é pré-determinado (ALBUQUERQUE, 2006).

Atualmente os protocolos de roteamento para as redes Mesh estão divididos em protocolos *Unicast* e *Multicast*. Onde no protocolo *Unicast* o pacote a ser transmitido tem somente um destinatário, já no *Multicast* o pacote tem um grupo definido de destinatários dentro da rede.

Um dos focos que se deve dar para as redes sem fio é a questão da segurança, pois a propagação do sinal é por meio de ondas de rádio frequência, ou seja, o sinal fica disponível para qualquer pessoa sem precisar de uma conexão física com a rede. Deste modo a rede pode se tornar um alvo fácil de pessoas com más intenções, sendo assim o usuário fica com receio

[1] esquema de ligações centrais de um sistema mais amplo, tipicamente de elevado desempenho

de utilizar esta conexão, por não saber se há algum mecanismo de segurança que lhe proteja de possíveis ataques.

Atualmente nas VPNs existem alguns protocolos de tunelamento que tratam da segurança entre a transmissão de informações. Estes protocolos visam a integridade das informações que trafegam pelo seu meio.

As redes virtuais privadas são recomendadas por garantir a integridade das informações, além de possuir um baixo custo na sua implantação e possuir escalabilidade, que é a facilidade de aumentar a quantidade de VPNs.

1.4 ESTRUTURA DO TRABALHO

O Capítulo 1 deste projeto apresenta a definição do problema bem como objetivo geral e objetivos específicos e também sua justificativa.

O Capítulo 2 descreve sobre redes de computadores, com foco em redes sem fio, trazendo informações de padrões, frequência, modulação. Abortando questões de segurança assim como alguns mecanismos de segurança e também tratando sobre ataques em redes sem fio. Outra parte deste capítulo trata-se acerca de redes Mesh, assim como seus tipos, características, arquitetura e alguns protocolos de roteamento existentes atualmente em redes Mesh.

O Capítulo 3 irá abordar acerca do protocolo de roteamento OLSR, trazendo informações de como é feita a transmissão de mensagens pela rede a fim de evitar a sobrecarga, assim como informações sobre o formato do pacote, mensagens de declaração de interface, mensagens de detecção de topologia, mensagens de controle de topologia e mensagens de associação de redes externas. Também será abordado sobre a tabela de

roteamento, cálculo da tabela e algumas informações sobre segurança e protocolo da Internet versão 6.

O Capítulo 4 descreve sobre as redes virtuais privadas, assim como as formas de utilização e arquitetura. Também serão abordadas informações sobre tunelamento, alguns de dos protocolos responsáveis por criar esse túnel e acerca de criptografia.

O Capítulo 5 faz uma abordagem sobre trabalhos já realizados sobre redes Mesh.

O Capítulo 6 descreve sobre o trabalho proposto, as metodologias utilizadas para pesquisa e coleta de informações, além dos equipamentos de hardware e software utilizados. Também estarão disponíveis as configurações básicas e os resultados obtidos com os testes que foram aplicados.

2 REDES DE COMPUTADORES

O surgimento das redes de computadores deu-se por volta de 1980, devido a curiosidade de certas instituições de ensino. A partir de então houve um grande crescimento na tecnologia para a ligação de computadores entre si, podendo ser caracterizada esta ligação como um grupo de computadores autônomos interconectados com o intuito de haver troca de informações (TANENBAUM, 1997).

2.1 REDES SEM FIO

As redes sem fio não necessitam de uma conexão física com computadores, pois os dados são transmitidos por ondas eletromagnéticas, ou seja, por rádio frequência onde os receptores precisam trabalhar na mesma frequência do remetente (COMER, 2001).

De acordo com Zacker e Doyle (2000, p. 875, tradução nossa) "...uma rede sem fio pode ser constituída de quase qualquer tipo de máquina de computação e pode estender-se por qualquer área."

Conforme Reynolds (2003, tradução nossa), em 1990 por meio do *Institute of Electrical and Electronic Engineers* (IEEE) foi criado um grupo de trabalho para estudos das redes sem fio, a partir de então começaram a surgir os padrões.

De acordo com Dornan (2001), as redes sem fio possuem a tecnologia *Frequency Hopping Spread Spectrum* (FHSS) dispõem de 79 faixas de frequência onde será escolhido para enviar o pacote e caso haja perda o pacote será reenviado, e também possui a tecnologia *Direct Sequence Spread Spectrum* (DSSS) que transmite em todas as frequências, com isso aumenta sua velocidade, porém, há um maior consumo de energia.

2.1.1 Frequência

Os sinais de frequência são utilizados para transmitir os dados, estes dados percorrem por uma faixa e sua medição é feita em *Hertz*. No Brasil as faixas de frequência disponíveis estão entre 2.4GHz a 2.5GHz (RUFINO, 2007).

2.1.2 Modulação

Para que as informações possam ser transmitidas via rádio frequência é necessário que o sinal seja convertido, esse processo de conversão é chamado de modulação. Este processo de conversão para colocar as informações na frequência desejada é conhecido como onda portadora. A modulação está composta de três formas, *Modulation Amplitude* (AM), *Modulation Frequency* (FM) e *Phase Modulation* (PM) (DORNAN, 2001).

Na modulação AM o sinal é sobreposto na onda portadora, gerando ondas que variam de altura e assim podendo transmitir as informações. Por se tratar de uma transmissão não muito eficiente, ou seja, podendo ter perdas ela é atualmente ainda utilizada em transmissão de rádio (DORNAN, 2001).

A modulação FM mantém a altura da onda sempre constante, podendo assim trabalhar sempre no máximo. Sendo assim ela se torna mais resiste e pode ser utilizada na transmissão de rádio e sistemas de TV (DORNAN, 2001).

A modulação PM é uma variação da modulação FM, onde de acordo com Dornan (2001, p. 28): “Em vez de apenas compactar e expandir as ondas, a modulação PM move rapidamente as ondas para um ponto diferente em seus ciclos.” Desta forma pode ser utilizada na transmissão de dados.

2.1.3 Padrões de Redes Sem Fio

As redes sem fio são compostas pelos seguintes padrões:

a) 802.11: foi o primeiro padrão de redes sem fio, onde se tem os mesmos protocolos de comutação das redes com fio, porém a transmissão dos dados é feita com de sinais de rádio (DORNAN, 2001);
b) 802.11a: neste padrão conseguiu-se atingir a velocidade de transmissão de até 54Mbps e utiliza a técnica *Orthogonal Frequency Division Multiplexing* (OFDM) para diminuir interferências (DORNAN, 2001);
c) 802.11b: utiliza a tecnologia DSSS e pode alcançar até 11Mbps nas suas transmissões (DORNAN, 2001);
d) 802.11c: faltaram informações para o modo ponte (*Bridging*), portanto este padrão não chegou a ser publicado (REYNOLDS, 2003, tradução nossa);
e) 802.11d: atende a requisitos internacionais da camada física para sua utilização (REYNOLDS, 2003, tradução nossa);
f) 802.11e: trouxe *Quality of Service* (QoS) para as redes sem fio gratuitas no gerenciamento de dados, voz e vídeos (REYNOLDS, 2003, tradução nossa);
g) 802.11f: teve sua aprovação em 2003 como um guia de recomendações para melhorar a transmissão do sinal sem fio (REYNOLDS, 2003, tradução nossa);
h) 802.11g: aprovado no mesmo ano que o anterior e acabou tornando-se um dos melhores padrões já criados, trabalhando na faixa de 2.4GHz e com transmissão de dados de 54Mbps (REYNOLDS, 2003, tradução nossa);
i) 802.11h: procurou melhorar os requisitos na Europa de seleção dinâmica de frequência e o controle do poder de transmissão na faixa de 5Ghz, sendo finalizado em 2003 (PRASAD, A.; PRASAD, N., 2005, tradução nossa);

j) 802.11i: trouxe melhorias para autenticação e na segurança (GANZ, A., GANZ, Z.; WONGTHAVARAWAT, 2003, tradução nossa);

k) 802.11j: foi regulamentado na faixa de 4.9GHz e 5Ghz para a utilização no Japão de acordo com normas e regras do país (PRASAD, A.; PRASAD, N., 2005, tradução nossa);

l) 802.11k: possibilitou a obtenção informações sobre os pontos de acesso sem fio e seus clientes (REYNOLDS, 2003, tradução nossa);

m) 802.11l: não teve avanço devido a confusões da letra “l” com o número “1” (REYNOLDS, 2003, tradução nossa);

n) 802.11m: criado para corrigir erros do padrão 802.11 (REYNOLDS, 2003, tradução nossa);

o) 802.11n: foi projetado para trabalhar com altas velocidades de transmissão, podendo transmitir dados entre 150Mbps e 600Mbps de velocidade, além de ter compatibilidade com os padrões 802.11 a, b e g (CHANDRA, 2009, tradução nossa);

p) 802.11p: desenvolvido para ser utilizado em veículos, onde se tem comunicação entre os mesmos ou com um ponto fixo na estrada e trabalha na faixa de 5.9GHz (CHANDRA, 2009, tradução nossa);

q) 802.11r: permite transições para dispositivos móveis e serviços como o *Voice Over Internet Protocol* (VoIP) (CHANDRA, 2009, tradução nossa);

r) 802.11s: criado para redes auto-configuráveis e topologias de múltiplos saltos sendo utilizado para as redes Mesh (CHANDRA, 2009, tradução nossa);

s) 802.11t: desenvolvido não para ser um padrão, mas sim para dizer como utilizar os métodos de medição e as métricas de desempenho e procedimentos das redes 802.11 (CHANDRA, 2009, tradução nossa);

t) 802.11u: trouxe uma abordagem genérica e padronizada das camadas *Media Access Control* (MAC) e física para o funcionamento de redes como o *Bluetooth* (CHANDRA, 2009, tradução nossa);

u) 802.11v: teve melhorias no rendimento, redução de interferências e confiabilidade das redes (CHANDRA, 2009, tradução nossa);

v) 802.11w: criado para aumentar a segurança da rede 802.11 (CHANDRA, 2009, tradução nossa).

Type	Radio Frequency	Signal Range	Maximum Data Speed	Typical Speed
802.11b	2.4 GHz	~30 meters (indoor) ~100 meters (outdoor)	11Mbps	4Mbps
802.11a	5 GHz	~35 meters (indoor) ~110 meters (outdoor)	54Mbps	23Mbps
802.11g	2.4 GHz	~35 meters (indoor) ~110 meters (outdoor)	54Mbps	20Mbps
802.11n (proposed)	2.4 GHz	~70 meters (indoor) ~160 meters (outdoor)	300Mbps	120Mbps

Figura 1. Comparação entre padrões
Fonte: ROSS, J. (2008, p. 27)

Na Figura 1 pode-se verificar uma pequena comparação entre os padrões 802.11b, 802.11a, 802.11g e 802.11n, mostrando sua frequência, alcance do sinal e velocidade de transmissão.

2.1.4 Segurança em Redes Sem Fio

A segurança em redes sem fio é frágil, pois a propagação do sinal é feita por meio de ondas de rádio frequência, ou seja, o sinal fica disponível para qualquer pessoa sem precisar de uma conexão física com a rede. Sendo assim a rede pode se tornar um alvo fácil para pessoas com más intenções. Deste modo o usuário fica com receio de utilizar esta

conexão, por não saber se há algum mecanismo de segurança que lhe proteja de possíveis ataques.

Para garantir que se tenha segurança em uma rede é necessário que se atenda alguns requisitos como:

a) autenticidade: quando se faz a validação do usuário na rede, sendo assim é garantido que o usuário é autêntico (CHEN; ZHANG, 2004, tradução nossa).

b) autorização: é responsável por controlar o acesso do usuário na rede, disponibilizando recursos e serviços (CHEN; ZHANG, 2004, tradução nossa).

c) disponibilidade: se refere a garantir que o usuário registrado possa ter sempre disponível o serviço de rede (VINES, 2002, tradução nossa).

d) integridade: visa garantir o conteúdo das informações não seja alterada durante o processo de envio (VINES, 2002, tradução nossa).

e) não repúdio: é responsável por guardar todas as informações que o usuário transmitiu (CHEN; ZHANG, 2004, tradução nossa).

f) privacidade: serve para garantir que somente os usuários registrados possam ler a mensagem, evitando que terceiros invadam sua privacidade (CHEN; ZHANG, 2004, tradução nossa).

2.1.4.1 Mecanismos de Segurança

Os tipos mais comuns de mecanismos de segurança implementados em redes sem fio são: *Wired Equivalent Privacy* (WEP), *Wi-Fi Protected Access* (WPA) e *Wi-Fi Protected Access 2* (WPA2).

De acordo com Earle (2006, p. 188), “O padrão Wired Equivalent Privacy (WEP) foi criado para dar proteção a redes sem fio e recursos de segurança semelhante ao de redes cabeadas.”

A segurança WEP foi definida no padrão 802.11b, que visa garantir a privacidade dos dados, este modelo de segurança utiliza um algoritmo de criptografia chamado RC4 e trabalha de forma assimétrica, ou seja, o mesmo algoritmo e a mesma chave são utilizados tanto na criptografia dos dados como na descriptografia (VINES, 2002, tradução nossa).

Existem dois níveis de criptografia no modelo WEP: um utiliza 64 bits e o outro utiliza 128 bits.

No primeiro nível são utilizados 40 bits para a criptografia dos dados e 24 bits para inicialização do vetor dando um total de 64 bits, e o segundo, são utilizados 104 bits para a criptografia dos dados e 24 bits para inicialização do vetor, dando um total de 128 bits (EARLE, 2006, tradução nossa).

De acordo com Earle (2006, tradução nossa), o método de segurança WPA foi criado após ser detectadas falhas no modelo de segurança WEP.

O método de segurança WPA aumentou o nível de segurança devido a criptografia e serviço de autenticação, sendo assim os usuários tem segurança na utilização da rede, pois seus dados serão protegidos, além de somente usuários cadastrados terão acesso a rede (RAO; RADHAMANI, 2008, tradução nossa).

A criação do modelo WPA2 trouxe um alto nível de segurança para o controle de acesso de usuários onde somente aquele que estiver cadastrado poderá acessar a rede. Este modelo pode ser encontrado na versão Pessoal que garante o acesso por meio de senha e a versão Empresarial que faz a validação do usuário por meio da utilização de um servidor (RAO; RADHAMANI, 2008, tradução nossa).

2.1.4.2 Ataques em Redes Sem Fio

Alguns ataques a redes sem fio são conhecidos como: *Channel Jamming, Denial of Service, Device Theft, Eavesdropping, Masquerade, Message Forgery, Message Replay, The DoCoMo E-Mail Virus, The Man In The Middle, Traffic Analysis, Unauthorized Access* e *War Driving*.

Channel Jamming visa atacar a camada física, é o ataque mais comum que utiliza a força bruta como tentativa de acessar a rede (AKYILDIZ; WANG, 2009, tradução nossa).

Denial of Service ou negação de serviço é quando a rede ou o servidor que disponibiliza acesso é inundado de informações, geralmente com e-mails falsos, sobrecarregando o mesmo, e assim parando ou negando a prestação do serviço de conexão com os usuários (SWAMINATHA; ELDEN, 2003, tradução nossa).

Device Theft é quando o usuário tem a impressão de que o dispositivo de rede foi roubado, não fisicamente, porém é esta a impressão que o usuário tem (SWAMINATHA; ELDEN, 2003, tradução nossa).

Eavesdropping ou espionagem acontece quando a rede ou as informações que trafegam por ela não possuem nenhum tipo de criptografia, facilitando a espionagem (AKYILDIZ; WANG, 2009, tradução nossa).

Masquerade acontece quando um invasor consegue a identidade de um usuário cadastrado e passa a obter informações e recursos da rede (CHEN; ZHANG, 2004, tradução nossa).

Message Forgery, este ataque é responsável por falsificar mensagens, no caso da rede possuir alguma falha o invasor insere mensagens indevidas a fim de diminuir o desempenho da rede, isto é comum acontecer nas camadas MAC e de roteamento (AKYILDIZ; WANG, 2009, tradução nossa).

Message Replay é quando o invasor repete as mensagens podendo ocasionar o mal funcionamento da rede (AKYILDIZ; WANG, 2009, tradução nossa).

De acordo com Swaminatha e Elden (2003, tradução nossa), o ataque *The DoCoMo E-Mail Virus* não é muito comum e recebeu este nome pois foi diagnosticado na rede de telefonia da *DoCoMo* no Japão, neste caso o vírus se instala no telefone celular e faz discagens automáticas para o número da polícia.

De acordo com Swaminatha e Elden (2003, tradução nossa) e Akyildiz e Wang (2009, tradução nossa), *The Man In The Middle* ocorre quando o invasor fica entre o usuário e o servidor, interceptando as mensagens que são transmitidas.

Traffic Analysis ou análise de tráfego, dificilmente o intruso é detectado pois não causa nenhum dano a rede, no entanto, ele fica observando as informações que trafegam pela rede e podendo se aproveitar das mesmas (AKYILDIZ; WANG, 2009, tradução nossa).

Unauthorized Access acontece durante a autorização e autenticação do usuário na rede, pois durante esse processo pode ocorrer de algum intruso se conectar sem a autorização necessária (AKYILDIZ; WANG, 2009, tradução nossa).

War Driving, este termo surgiu por volta dos anos 2000, pois naquele tempo não se tinha muita segurança implantada nas redes sem fio e portanto pessoas mal intencionadas saiam de carro a busca de redes sem fio vulneráveis para que pudessem acessar (SWAMINATHA; ELDEN, 2003, tradução nossa).

2.2 REDES MESH

Este modelo de tecnologia teve seu desenvolvimento por volta de 1970, projeto liderado pela agência de defesa dos Estados Unidos, *Defense Advanced Research Projects*

Agency (DARPA). O objetivo principal era ter comunicação e transferência de dados e voz pelo campo de batalha sem ter a necessidade de centralizar o sinal.

Para Akyildiz e Wang (2009, tradução nossa), as redes sem fio Mesh serão uma tecnologia chave para a próxima década, pois poderão realizar um grande sonho de poder ter conectividade em qualquer lugar e a qualquer momento. Tendo um papel fundamental para a próxima geração da Internet, devido ao seu poder de auto-organização, auto-configuração, baixo custo e a redução da complexidade em implantação e manutenção.

As redes em malha, ou simplesmente redes Mesh, tem uma arquitetura diferente de uma rede sem fio convencional ou de telefonia móvel, pois os nós tem um tratamento igual onde todos podem participar da rede, sendo ele uma fonte de sinal ou um simples usuário (METHLEY, 2009, tradução nossa).

2.2.1 Tipos de Redes Mesh

Segundo Methley (2009, tradução nossa), atualmente as redes Mesh estão divididas em três formas diferentes, são elas:

a) **pura:** desta forma apenas um nó é responsável por todo o tráfego da rede, neste caso o nó do usuário;

b) **híbrida:** consiste em ter uma rede pura e um *backbone*;

c) **acesso:** esta rede contém *gateways* para redes externas, como a Internet.

2.2.2 Características

De acordo com Methley (2009, tradução nossa), estas redes possuem as seguintes características:

a) ad-hoc: é a área de cobertura e interferência não é controlada, ou seja, é possível ter pontos de acesso em qualquer lugar;

b) infraestrutura não separada: neste caso o controle é feito dentro da rede;

c) mobilidade: os nós são dinâmicos onde eles são livres para se moverem e desaparecerem;

d) wireless: proporcionam a mobilidade da ausência de cabos e pode evitar o modo infraestrutura;

e) relay: todos os nós podem ser obrigados a transmitir informações para os outros nós da rede;

f) roteamento: neste caso todos os nós devem possuir o mesmo protocolo de roteamento;

g) múltiplos saltos: fundamental para lugares com irregularidades de terreno, tendo assim uma maior cobertura;

h) homogeneidade: onde não há a necessidade de todos os nós da rede serem iguais.

As redes Mesh podem possuir outras características tais como: auto-organização, auto-formação e integração.

Na auto-organização e auto-formação novos nós podem ser inseridos conforme a demanda da rede, possuindo uma grande flexibilidade de expansão (AKYILDIZ; WANG, 2009, tradução nossa).

A integração é responsável por integrar outros tipos de redes sem fio como: redes de celular, Internet e sensores, utilizando funcionalidades dos roteadores Mesh (AKYILDIZ; WANG, 2009, tradução nossa).

2.2.3 Arquitetura de Rede

As WMN ou redes sem fio em malha são formadas por roteadores e por clientes Mesh.

Os roteadores possuem uma mobilidade mínima e formam um *backbone* (espinha dorsal), onde é possível a integração de outros tipos de redes (AKYILDIZ; WANG, 2009, tradução nossa).

Nos nós clientes é possível criar uma rede somente acrescentando novos aparelhos como: notebook, PDA, entre outros sem a necessidade de ter um *backbone* (AKYILDIZ; WANG, 2009, tradução nossa).

A arquitetura destas redes pode ser dividida em três principais grupos, são eles: infraestrutura/*backbone*, clientes e híbridos.

Na primeira (Figura 2) é criada uma infraestrutura de roteadores para que os clientes possam conectar-se, sendo assim é possível disponibilizar conexão com a Internet (AKYILDIZ; WANG, 2009, tradução nossa).

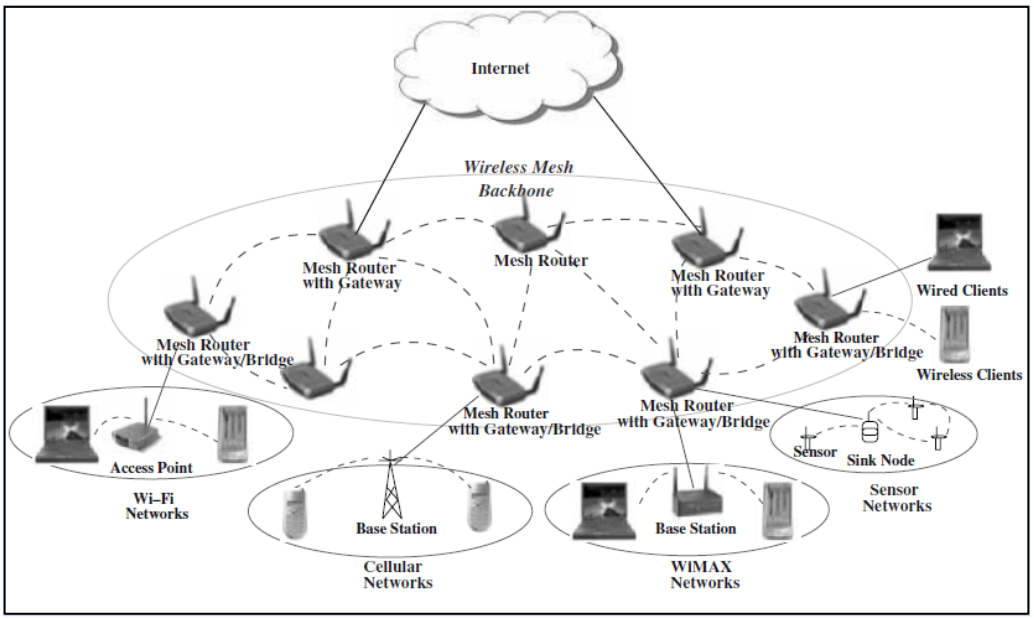


Figura 2. Arquitetura infraestrutura/*backbone*
Fonte: AKYILDIZ F., I; WANG X. (2009, p. 4)

Os clientes (Figura 3) caracterizam uma conexão *Peer-To-Peer* (P2P), onde não há a necessidade de um roteador e a comunicação e a transmissão de dados é feita entre os clientes (AKYILDIZ; WANG, 2009, tradução nossa).

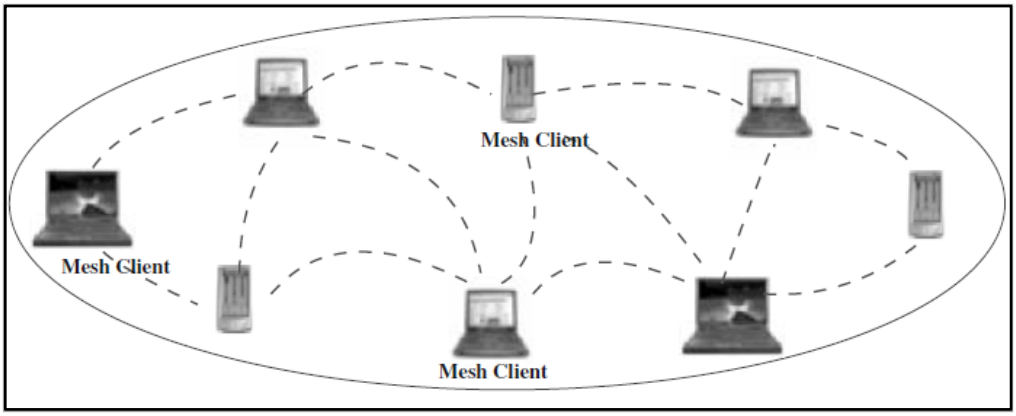


Figura 3. Arquitetura cliente
Fonte: AKYILDIZ F., I; WANG X. (2009, p. 5)

A arquitetura híbrida (Figura 4) caracteriza a junção da infraestrutura e dos clientes, onde a mesma irá prover uma conectividade pelos roteadores para que os clientes possam se conectar e assim aumentar a cobertura da rede (AKYILDIZ; WANG, 2009, tradução nossa).

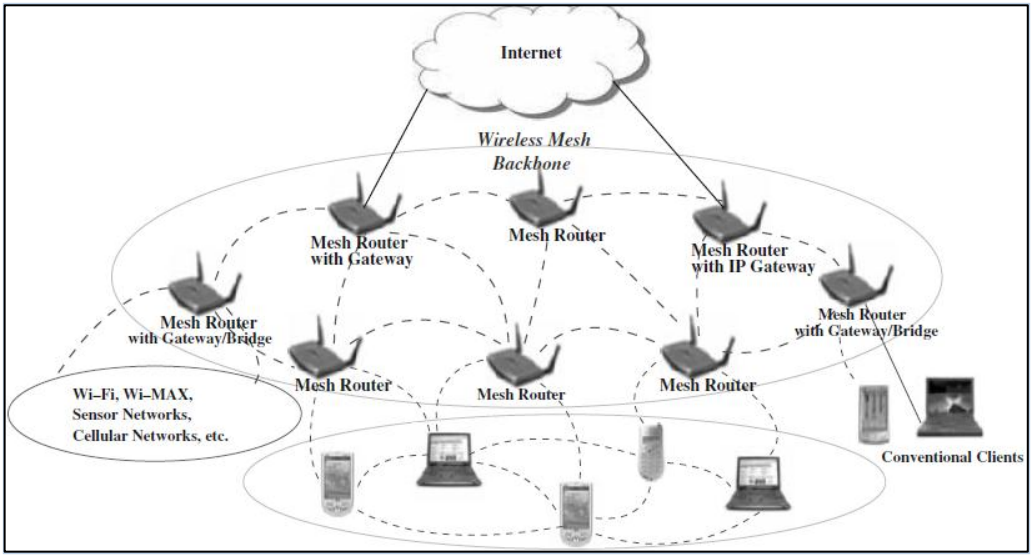


Figura 4. Arquitetura híbrida
Fonte: AKYILDIZ F., I; WANG X. (2009, p. 5)

2.2.4 Protocolo de Roteamento

O protocolo de roteamento é responsável por fazer chegar a mensagem ao seu destino, onde se tem em cada nó uma tabela de roteamento com os possíveis destinatários que se encontram na rede.

De acordo com Santos (2011), os protocolos de roteamento estão divididos de acordo com o tipo de comunicação neste caso: *Unicast* e *Multicast*.

2.2.4.1 Protocolos de Roteamento Unicast

Este tipo de roteamento acontece quando uma mensagem é direcionada para somente um usuário da rede (MURHAMMER, 2000).

Os protocolos *Unicast* estão divididos em: Proativos, Reativos e Híbridos.

No caso dos protocolos Proativos cada nó que pertencente à rede possui uma tabela de roteamento que contém informações sobre o restante dos nós, esta tabela é atualizada de tempo em tempo por meio da troca de informações entre eles (HELD, 2005, tradução nossa).

Exemplos deste modelo são: *Wireless Routing Protocol* (WRP) e *Destination-Sequenced Distance-Vector* (DSDV).

De acordo com Held (2005, tradução nossa) o protocolo Reativo também é conhecido como "*on-demand*", pois pode-se dizer que ele trabalha de modo estático, ou seja, ele somente irá verificar a sua rota quando alguém solicitar. Deste modo há uma diminuição considerável de overhead.

Exemplos deste modelo são: *Dynamic Source Routing* (DSR) e *Ad Hoc On-Demand Distance Vector* (AODV).

O protocolo Híbrido tem como objetivo unir as melhores características dos Proativos e dos Reativos. Neste caso o protocolo Proativo tem como função manter a tabela de roteamento atualizada para os nós mais próximos e/ou para as rotas que são usadas com mais frequência, já o protocolo Reativo tem a função de cuidar dos nós mais longes e os que são pouco usados (MISRA; MISRA; WOUNGANG, 2009, tradução nossa).

Exemplos deste modelo são: *Zone Routing Protocol* (ZRP) e *Core Extraction Distributed Ad Hoc Routing* (CEDAR).

2.2.4.2 Protocolos de Roteamento Multicast

Este protocolo faz com que a mensagem seja enviada para um grupo específico de usuários (MURHAMMER, 2000).

Os *Multicast* são divididos em: Tree-based e Mesh-based.

De acordo com Santos (2011) o protocolo Tree-based possui um caminho único entre remetente e destinatário, no qual sua característica é a criação de uma Árvore Multicast que compões o grupo de usuários.

Exemplos deste modelo são: *Multicast Ad Hoc On-Demand Distance Vector* (MAODV) e *Multicast Zone RoutingProtocol* (MZRP).

No protocolo Mesh-based existirá vários caminhos para os nós remetentes e para os nós destinatários da rede (SANTOS, 2011).

Exemplos deste modelo são: *On-Demand Multicast Routing Protocol* (ODMRP) e *Dynamic Core-Based Multicast Routing Protocol* (DCMP).

3 PROTOCOLO OPTIMIZED LINK STATE ROUTING

A partir do projeto Hipercom desenvolvido na França pela *Institut National de Recherche en Informatique Et en Automatique* (INRIA), surgiu o protocolo de roteamento em redes Mesh OLSR. Teve sua padronização iniciada em Outubro de 2003 na *Internet Engineering Task Force* (IETF) sob a *Request For Comments* (RFC) 3626, porém ainda está em fase experimental, ou seja, ainda poderá ter alterações até sua finalização.

O protocolo OLSR é um protocolo proativo utilizado em *Mobile Ad-Hoc Networks* (MANETs), ele se adapta bem em grandes redes devido a sua forma de roteamento, pois cada nó é responsável por fazer sua própria transmissão de seus pacotes. Este protocolo também pode ser recomendado em lugares onde a rede é variável, ou seja, onde haja constantes alterações em sua topologia (CLAUSEN; JACQUET, 2003, tradução nossa).

Este protocolo utiliza um algoritmo chamado *Link State* que de acordo com Frosi e Schaeffer (2011, p. 2):

> O algoritmo Link State é uma evolução natural do algoritmo Distance Vector, uma vez que o primeiro utiliza informações como largura disponível de banda, e o segundo somente utiliza o tempo calculado de resposta. O algoritmo Link State funciona através de uma representação de um grafo, onde a conexão entre nodos é representada por uma aresta. Às arestas é atribuído um custo, que é proveniente de um cálculo definido que utiliza diversas variáveis, dentre elas, a largura disponível de banda e a latência ou tempo de resposta.

O protocolo OLSR herda a estabilidade do algoritmo Link State, além de possuir uma vantagem de ter rotas disponíveis sempre quando for solicitado e de mantê-las atualizadas para todos os nós que se encontram na rede (CLAUSEN; JACQUET, 2003, tradução nossa).

Conforme Carvalho (1997), no algoritmo Link State cada *gateway* conhece toda a topologia da rede sendo responsável por testar periodicamente os seus vizinhos e informar

com periodicidade o estado dos seus vizinhos aos outros *gateways* da rede. A rota é calculada pelo do algoritmo *Shortest Path First* (SPF), mais conhecido como o algoritmo *Dijkstra*.

3.1 MULTIPOINT RELAY

O protocolo OLSR diminui a sobrecarga da rede (*overhead*) pela inundação (*flooding*), utilizando a técnica de *Multipoint Relay* (MPR).

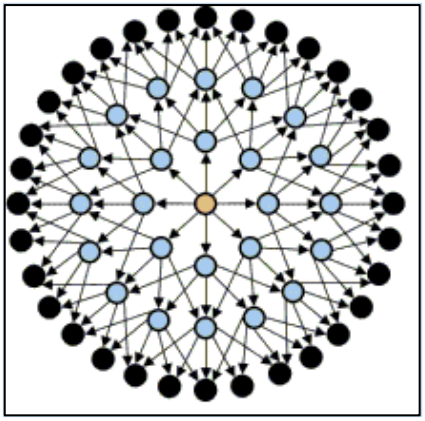


Figura 5. Protocolo OLSR sem a utilização da técnica MPR
Fonte: FSTC (2005?)

Na Figura 5 é possível visualizar como seria o protocolo sem a utilização da técnica MPR, onde aconteceria a inundação de mensagens na rede ocasionando a sobrecarga.

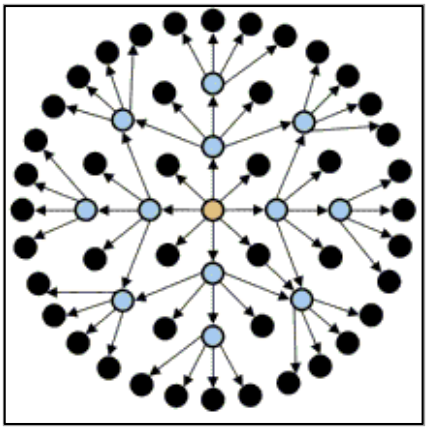


Figura 6. Protocolo OLSR utilizando da técnica MPR
Fonte: FSTC (2005?)

Na Figura 6 pode-se verificar como a técnica MPR funciona, evitando consideravelmente a sobrecarga da rede.

De acordo com Clausen e Jacquet (2003, tradução nossa), cada nó pertencente a rede irá definir um grupo de nós que esteja a 1 salto de distância, de forma assimétrica (transmissão aconteça de forma bidirecional) e que possa retransmitir as mensagens. Esses nós escolhidos são chamados de MPRs, pois serão responsáveis por transmitir as mensagens adiante.

OLSR utiliza o protocolo *User Datagram Protocol* (UDP) para comunicação e a *Internet Assigned Numbers Authority* (IANA) definiu a porta 698 como sendo exclusiva do protocolo (CLAUSEN; JACQUET, 2003, tradução nossa).

3.2 FORMATO DO PACOTE

A Figura 7 representa o formato do pacote de acordo com a norma RFC 3626, definido por Clausen e Jacquet (2003, tradução nossa).

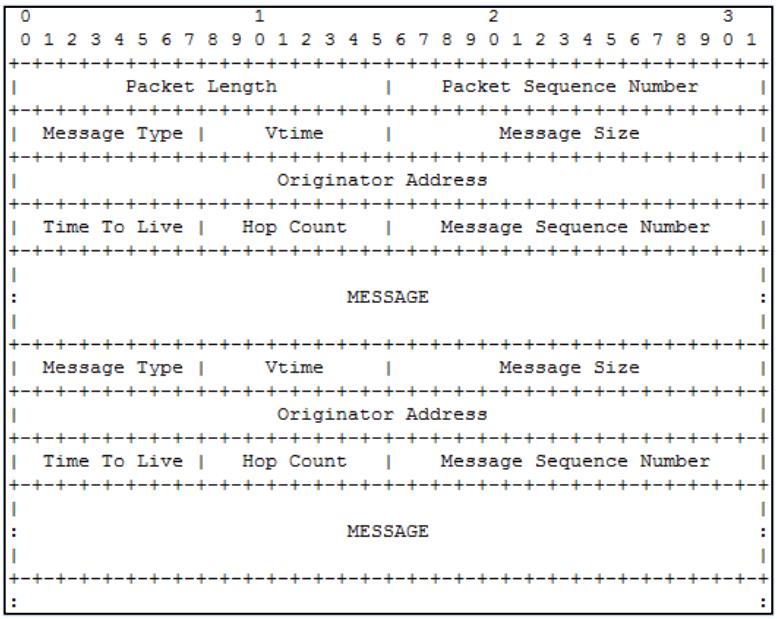


Figura 7. Formato do pacote OLSR
Fonte: CLAUSEN; JACQUET (2003, p. 13)

A seguir pode-se verificar a descrição do formato do pacote de acordo com Clausen e Jacquet (2003, tradução nossa), onde:

a) packet lenght: este campo representa o comprimento do pacote em bytes;

b) packet sequence number: este campo armazena um número sequencial do pacote onde o mesmo é incrementado toda vez que um novo pacote OLSR é transmitido;

c) message type: este campo representa qual o tipo da mensagem que está contida no campo “MESSAGE”, sendo que no intervalo de 0 a 127 está reservado pelo protocolo;

d) vtime: este campo indica quanto tempo depois da recepção da mensagem o nó irá considerar como informações válidas. Cálculo do tempo C*(1+a/16)* 2^b onde C é uma constante (1/16), a é representado pelos quatros maiores bits e b é representado pelos quatros menores bits do campo Vtime;

e) message size: este campo é responsável pelo tamanho da mensagem em bytes, sendo medida a partir do inicio do tipo da mensagem até o próximo tipo da mensagem ou o fim do pacote;

f) originator address: este campo contém o endereço do nó principal que gerou a mensagem. Devido aos possíveis saltos, este endereço nunca deve ser alterado;

g) time to live: mais conhecido pela sigla TTL, este campo é responsável pelo número máximo de saltos que um pacote deve dar. Antes da retransmissão da mensagem ele decrementa 1 da sua contagem. Quando um nó recebe uma mensagem com o TTL igual a 0 ou 1, está mensagem não deve ser retransmitida;

h) hop count: este campo contém o número de saltos da mensagem, sendo incrementado em 1 antes da mensagem ser retransmitida;

i) message sequence number: neste campo o nó que criar uma mensagem fica responsável por atribuir um valor único a sequência de números da mensagem;

j) message: este campo é responsável por conter a mensagem a ser enviada.

3.3 MENSAGENS DO PROTOCOLO

As mensagens do protocolo são responsáveis por descobrir interfaces de redes, detectar a topologia da rede, controlar a topologia ou até mesmos ser responsável por ligar o protocolo OLSR a um rede externa.

3.3.1 Mensagens MID

As mensagens *Multiple Interface Declaration* (MID) são transmitidas quando um nó da rede possui mais de uma interface de rede e que está utilizando o protocolo OLSR. Estas mensagens são transmitidas pelos nós MPRs (CLAUSEN; JACQUET, 2003, tradução nossa).

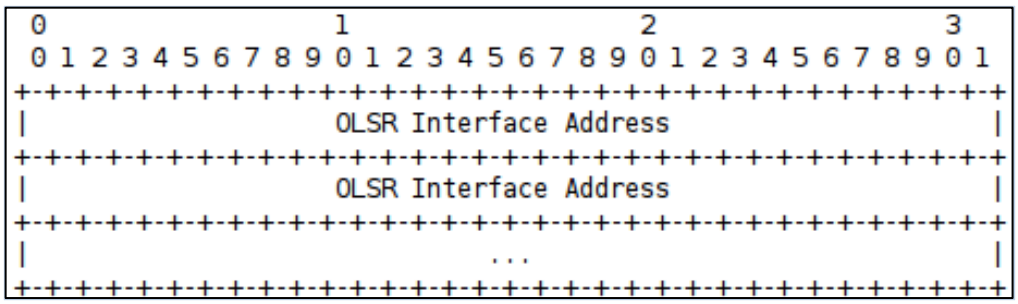


Figura 8. Formato da mensagem MID
Fonte: CLAUSEN THOMAS, H; JACQUET, P. (2003, p. 25)

Na Figura 8 pode-se visualizar o formato da mensagem MID e conforme Clausen e Jacquet (2003, tradução nossa), o campo *OLSR Interface Address* é responsável por armazenar o endereço das interfaces da rede, excluindo o endereço principal do nó.

3.3.2 Mensagens HELLO

As mensagens *HELLO* são responsáveis pela detecção da topologia de rede OLSR e ela segue um formato padrão que é possível verificar na Figura 9.

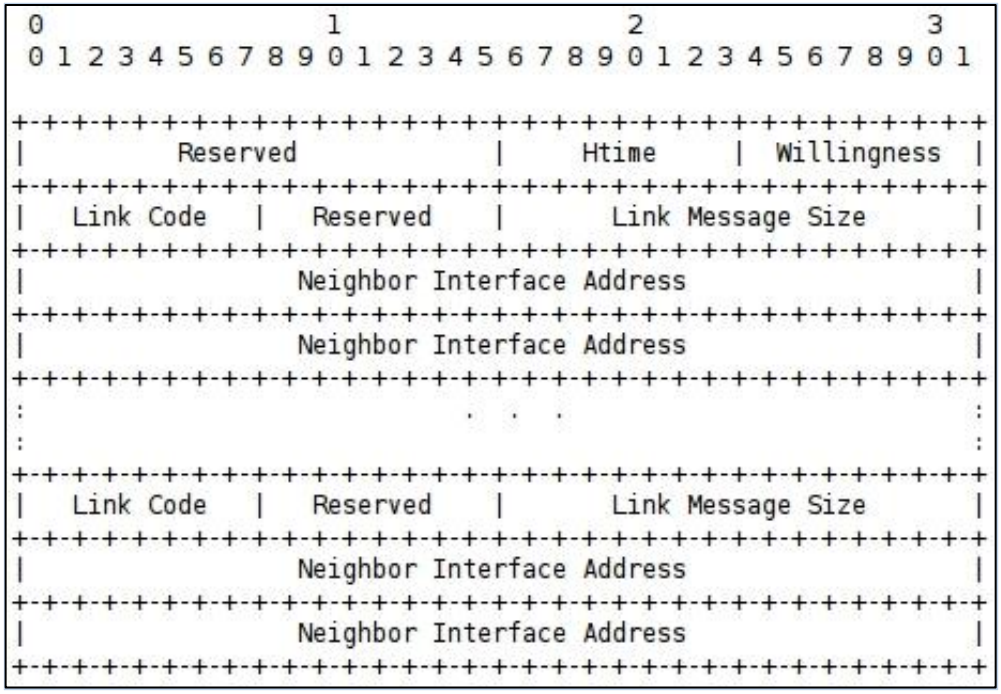


Figura 9. Formato das mensagens HELLO
Fonte: CLAUSEN THOMAS, H; JACQUET, P. (2003, p. 28)

A seguir pode-se verificar a descrição do formato das mensagens de acordo com Clausen e Jacquet (2003, tradução nossa), onde:

a) reserved: este campo tem como valor padrão “0000000000000” devido a necessidade de estar em conformidade com a especificação;

b) htime: este campo é responsável por estabelecer um tempo para o envio de mensagens, calculo utilizado é C*(1+a/16)* 2^b. Onde C é uma constante (1/16), a é representado pelos quatros maiores bits e b é representado pelos quatros menores bits do campo Htime;

c) willingness: é responsável por especificar a disponibilidade do nó encaminhar e transportar o tráfego da rede, sendo definido como: WILL_NEVER (peso 0), WILL_LOW (peso 1), WILL_DEFAULT (peso 3), WILL_HIGH (peso 6), WILL_ALWAYS (peso 7). O nó que possui peso 0 nunca poderá ser um MPR já o com peso 7 deve ser um MPR e por padrão o nó tem peso 3;

d) link code: contém informações sobre a ligação entre o nó remetente e o nó vizinho, também pode conter informações sobre o estado do vizinho;

e) link message size: é o tamanho do link da mensagem em bytes contado do inicio do primeiro “Link Code” até o próximo “Link Code”;

f) neighbor interface address: este campo contém o endereço da interface do nó vizinho.

3.3.3 Mensagens TC

As mensagens *Topology Control* (TC) são enviadas somente pelos nós MPRs, e de acordo com Clausen e Jacquet (2003, p. 43, tradução nossa) “Um nó deve pelo menos divulgar as ligações entre si e entre os nós de seu conjunto seletor MPR, a fim de fornecer informações suficientes para permitir o roteamento.”

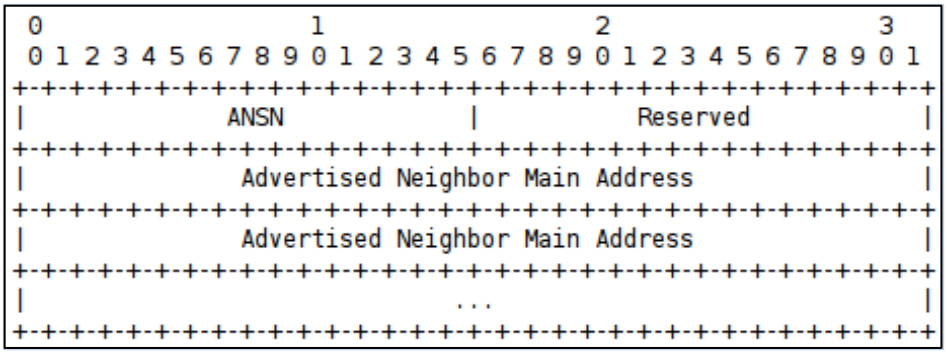


Figura 10. Formato da mensagem TC
Fonte: CLAUSEN THOMAS, H; JACQUET, P. (2003, p. 43)

A seguir há a descrição dos campos TC (Figura 10) de acordo com Clausen e Jacquet (2003, tradução nossa), onde:

a) advertised neighbor sequence number (ANSN): este campo armazena um número seqüencial, onde sempre quando houver alteração em algum de seus nós vizinhos o valor é incrementado. Permitindo que outros nós da rede saibam qual a informação é mais recente;

b) reserved: campo reservado e tem como valor “0000000000000000” devido a necessidade de estar em conformidade com a especificação;

c) advertised neighbor main address: contém o endereço principal de um nó vizinho, sendo que todos os endereços principais dos vizinhos são colocados no TC pelo nó que originalmente gerou a mensagem.

A responsabilidade pelo envio das mensagens TC fica por conta dos nós MPRs.

3.3.4 Mensagens HNA

Um nó da rede pode ter mais de uma interface, portanto as mensagens *Host and Network Association* (HNA) permite ter conectividade com outras redes, como a Internet (CLAUSEN; JACQUET, 2003, tradução nossa).

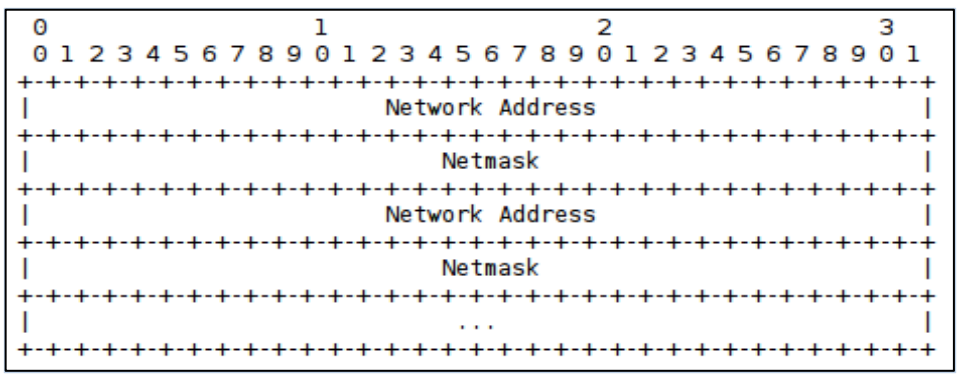


Figura 11. Formato da mensagem HNA
Fonte: CLAUSEN THOMAS, H; JACQUET, P. (2003, p. 52)

Abaixo segue a descrição dos campos HNA (Figura 11) de acordo com Clausen e Jacquet (2003, tradução nossa), onde:

a) network addresss: contém o endereço da rede;

b) netmask: corresponde a máscara de rede do endereço acima.

As mensagens HNA são emitidas com periodicidade a fim de permitir a montagem da tabela de roteamento, anunciando assim que há uma rota externa para a rede (CLAUSEN; JACQUET, 2003, tradução nossa).

3.4 TABELA DE ROTEAMENTO

A tabela de roteamento serve para identificar os nós da rede, sendo assim cada nó da rede possui sua própria tabela de roteamento. Caso haja alteração na topologia da rede ou alterações nos nós é feito um novo cálculo para atualizar os nós da rede (CLAUSEN; JACQUET, 2003, tradução nossa).

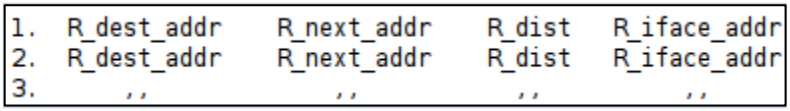


Figura 12. Formato da tabela de roteamento
Fonte: CLAUSEN THOMAS, H; JACQUET, P. (2003, p. 47)

Na Figura 12 pode-se verificar o formato da tabela de roteamento, onde de acordo com Schiller (2007):

a) r_dest_addr: este campo contém o endereço do nó destinatário;

b) r_next_addr: este campo contém o endereço do próximo nó;

c) r_dist: este campo é responsável por armazenar a distância entre os nós;

d) r_iface_addr: este campo contém o endereço do nó local.

3.4.1 Cálculo da Tabela de Roteamento

Conforme Clausen e Jacquet (2003, tradução nossa) o cálculo da tabela de roteamento é feita basicamente quando um novo nó é adicionado a rede ou quando um nó é perdido da rede, para ambos os casos se tem os mesmos procedimentos, que são:

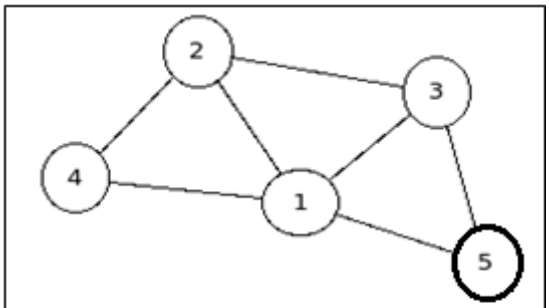
a) todas as entradas da tabela são removidas;

b) novas entradas são adicionadas a tabela de roteamento para vizinhos que estão a 1 salto de distância, onde R_dist receberá 1;

c) novas entradas são adicionadas à tabela de roteamento, para vizinhos que estão a 2 saltos de distância, onde R_dist receberá 2 e R_dest_addr recebe o endereço deste nó;

d) novas entradas são adicionadas a tabela de roteamento para vizinhos que possuem distâncias maiores que 2 saltos, onde R_dist receberá R_dist + 1. Este processo terminará somente quando chegar até o ultimo nó da rede.

Sendo assim, o cálculo da tabela de roteamento tem sempre por base a distância dos vizinhos (R_dist).



R_dest_addr	R_next_addr	R_dist	R_iface_addr
1	1	1	5
2	3	2	5
3	3	1	5
4	1	2	5

Figura 13. Exemplo de um grafo e sua tabela de roteamento

Na Figura 13 é possível verificar um grafo para uma rede Mesh onde os nós representam os pontos de acessos e uma tabela de roteamento. Neste caso, o nó principal (R_iface_addr) é o de número 5 e suas possíveis rotas.

3.5 IPV6 E SEGURANÇA

Todas as operações do protocolo OLSR podem ser feitas utilizando o protocolo IPv4 e também o protocolo IPv6 (CLAUSEN; JACQUET, 2003, tradução nossa).

No momento, o protocolo OLSR não implementa nenhum modelo de segurança, ficando vulnerável a ataques externos (CLAUSEN; JACQUET, 2003, tradução nossa).

Neste capítulo foi possível verificar a cerca do protocolo de roteamento OLSR e no capítulo seguinte será abordado a cerca das redes virtuais privadas.

4 VIRTUAL PRIVATE NETWORK

As VPNs surgiram com o intuito de prover uma maior segurança em transações por meio da conexão entre redes e computadores via Internet.

De acordo com Tanenbaum (2003, p. 828), as VPNs foram criadas com o intuito de serem "... redes sobrepostas às redes públicas, mas com a maioria das propriedades de redes privadas. Elas são chamadas "virtuais" porque são meramente uma ilusão, da mesma forma que os circuitos virtuais não são circuitos reais e que a memória virtual não é memória real."

Conforme Murhammer (2000, p. 329), "Uma rede virtual privada (VPN) é uma extensão da intranet privada de uma empresa, através de uma rede pública como a Internet, criando uma conexão privada segura, essencialmente por meio de um *túnel* privado."

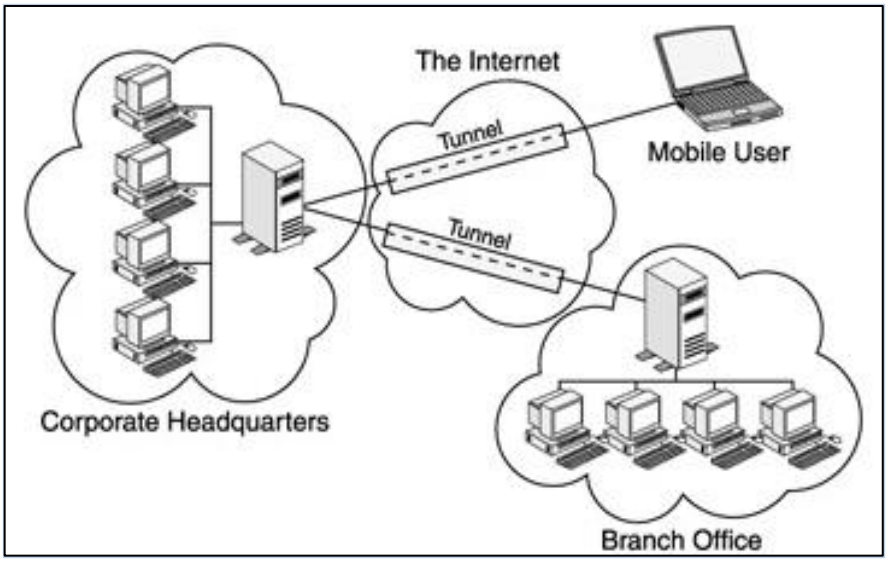


Figura 14. Típica VPN
Fonte: GUPTA (2002, p. 5)

Na Figura 14 visualiza-se o funcionamento de uma típica VPN, que de acordo com Peikari e Fogie (2002), a VPN nos traz comunicação segura e criptografada de duas formas:

a) **usuário para rede:** neste caso o usuário pode estar em qualquer lugar e a partir de uma conexão com a Internet é possível conectar-se a uma rede;

b) **rede para rede:** neste modelo trata-se de uma filial que já possua sua própria rede interna e deseja se conectar a matriz, desta forma a filial poderá conectar-se na rede da matriz utilizando a Internet.

4.1 ARQUITETURA VPN

A arquitetura VPN é composta basicamente por: dependentes, independentes e VPNs híbridas.

Os dependentes são quando uma empresa prestadora de serviços faz toda a implantação da VPN garantindo seu funcionamento e segurança, sendo ela responsável por toda a solução (GUPTA, 2002, tradução nossa).

Os independentes é o contrário dos dependentes, pois neste caso a própria organização monta sua VPN ficando a cargo da mesma garantir a segurança e criptografia dos dados (GUPTA, 2002, tradução nossa).

Nas VPNs híbridas a organização fica responsável por parte da solução VPN e terceiriza outra a parte da solução (GUPTA, 2002, tradução nossa).

4.2 TUNELAMENTO

Tunelamento é uma técnica utilizada em comutação de pacotes onde consiste em adicionar um novo cabeçalho ao pacote original criando assim uma camada sobre o mesmo. Isto serve para garantir que o pacote não seja alterado durante sua transmissão mantendo a integridade do mesmo (MURHAMMER, 2000).

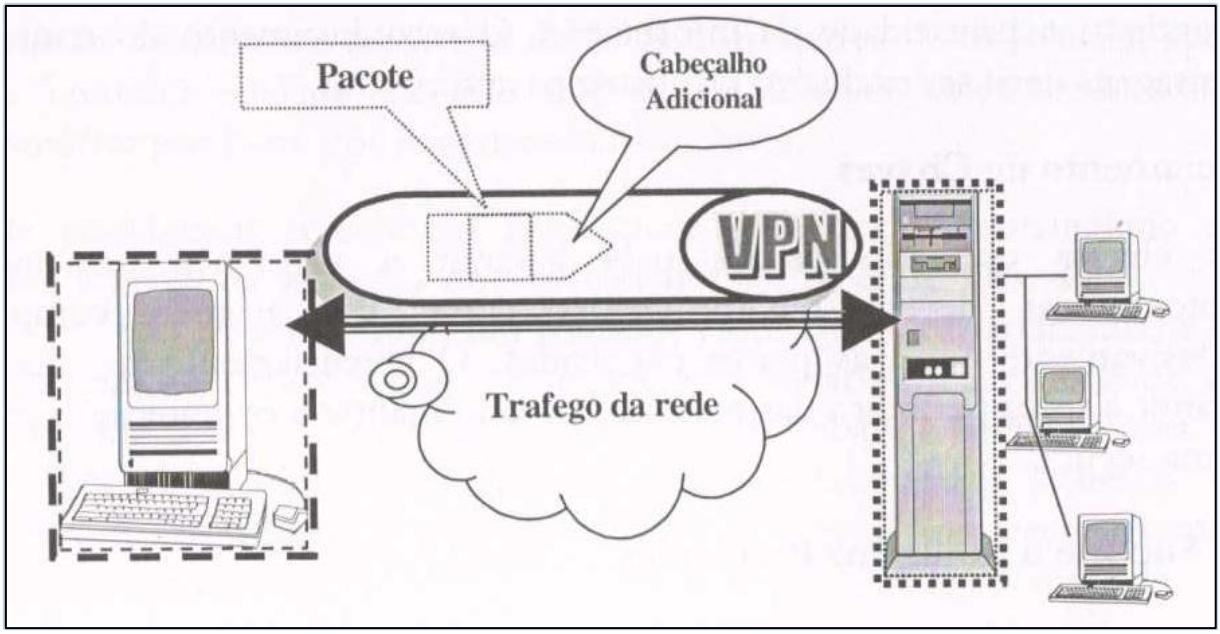


Figura 15. Modelo de tunelamento
Fonte: STARLIN, G; NOVO, R. (2000, p. 262)

Na Figura 15 pode-se verificar um modelo básico de como ocorre o tunelamento, neste caso um novo cabeçalho é encapsulado ao pacote.

Utilizar um meio público para o envio de mensagens privadas que tenha segurança, economia na implantação e garantias de confidencialidade, integridade e autenticação, são algumas das vantagens das VPNs (NORTHCUTT, 2002).

Sobrecarga de processamento, de pacotes, problemas com implantação e com a disponibilidade da Internet são algumas das desvantagens do uso das VPNs (NORTHCUTT, 2002).

4.2.1 Protocolos de Tunelamento

Para ser possível a comunicação por meio de um túnel é necessário que o remetente e o destinatário possuam o mesmo protocolo, para que deste modo possa haver a troca de informações.

4.2.1.1 Point-to-Point Tunneling Protocol

De acordo com Gupta (2003, tradução nossa), o protocolo PPTP atua na segunda camada do modelo OSI é um protocolo proprietário desenvolvido pelas empresas: Microsoft, Ascend, 3COM, US Robotics e ECI. Fornecendo por meio da criação de um túnel a transmissão de informações seguras nas redes públicas como se o usuário estive-se em uma rede privada.

O protocolo PPTP é baseado no protocolo *Point-to-Point Protocol* (PPP), que oferece a ligação ponto a ponto ao qual normalmente era utilizado nas redes de conexão discada (THOMAS, 2007).

Para Thomas (2007) "O PPTP empacota dos dados dentro dos pacotes PPP e então encapsula os pacotes PPP dentro dos pacotes IP (datagrama) para transmissão pela Internet via túnel VPN."

4.2.1.2 Layer 2 Forwarding

O protocolo L2F foi desenvolvido pela Cisco, atua na segunda camada do modelo OSI e a falta de incentivo por parte da empresa acabou extinguindo o protocolo (PEIKARI; FOGIE, 2002, tradução nossa).

Antes do L2F sair do mercado ele proporcionou um avanço considerável na tecnologia VPN, pois com a utilização deste protocolo foi possível criar mais de uma sessão utilizando o mesmo túnel, o que não era possível anteriormente (GUPTA, 2002, tradução nossa).

4.2.1.3 Layer 2 Tunneling Protocol

L2TP foi desenvolvido pela IETF, este protocolo atua na segunda camada do modelo OSI e combina as melhores técnicas do PPTP e L2F (GUPTA, 2002, tradução nossa).

Conforme diz Starlin e Novo (2000, p. 262), o protocolo L2TP "... permite que o tráfego IP seja criptografado e enviados através de canais de comunicação de datagrama ponto a ponto tais como o X25, Frame Relay ou ATM."

4.2.1.4 Internet Protocol Security

De acordo com Starlin e Novo (2000), o protocolo IPSec foi desenvolvido pela IETF e atua na terceira camada do modelo OSI. O IPSec fornece segurança, criptografia e integridade das informações transmitidas.

O protocolo IPSec possui três componentes principais que são: *Authentication Header* (AH), *Encapsulating Security Payload* (ESP) e *Internet Key Exchange* (IKE).

a) o componente AH é o cabeçalho de autenticação responsável por promover integridade e autenticidade para datagramas, porém seu uso é opcional (MURHAMMER, 2000).

b) o componente ESP é a carga de segurança encapsulada, este componente garante a confidencialidade além ter autenticação e integridade (STARLIN; NOVO, 2000).

c) o componente IKE é o intercâmbio de chaves da Internet responsável também é conhecido como *Internet Security Association and Key Management Protocol* (ISAKMP) ele é utilizado antes de iniciar a sessão ficando responsável por

negociar as chaves de autenticação e métodos de segurança (GUPTA, 2002, tradução nossa).

4.3 SEGURANÇA

De acordo com Murhammer (2000), existe um modelo de segurança chamado: AAA (triplo A). O triplo A é composto por:

a) Autenticação que serve para identificar o usuário na rede, geralmente utiliza-se nome de usuário e senha para ter acesso;

b) Autorização que visa verifica se o usuário que quer acessar a rede tem permissão para executar suas ações;

c) contabilização ou *accounting* é responsável por registrar todas as ações do usuário na rede.

A rede pública pode ser caracterizada por ter certa insegurança durante a transmissão de informações. Com isso as VPN visam garantir que os dados não sejam alterados durante sua trajetória.

4.3.1 Criptografia

Conforme Gupta (2003, tradução nossa), a criptografia dos dados nas VPNs tem um papel muito importante, pois é com a criptografia que os dados serão convertidos em dados inelegíveis e depois quando chegar a seu destino serão novamente convertidos para que seja possível entende-los.

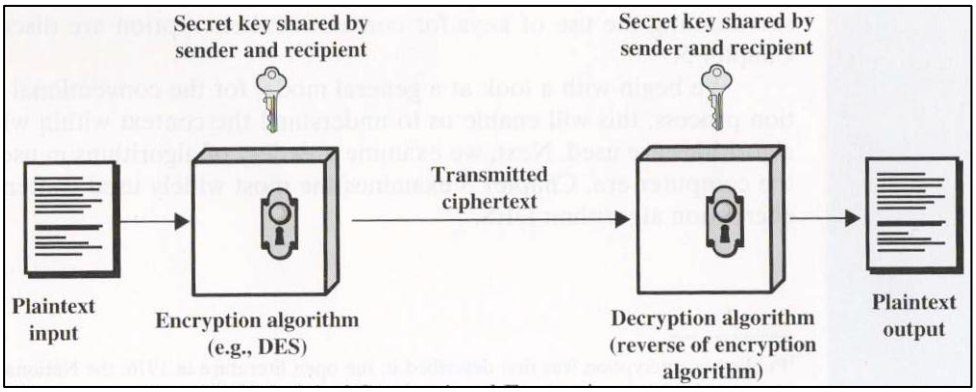


Figura 16. Criptografia
Fonte: STALLINGS, W. (1998, p. 22)

Na Figura 16 pode-se visualizar um modelo convencional de criptografia, onde os dados são criptografados e descriptografados por uma chave que é compartilhada pelos usuários.

4.3.2 Chaves Simétricas

Conforme Buchmann (2002, p. 87), as chaves são simétricas quando "Se em um criptossistema a chave de codificação criptográfica *e* é sempre igual à chave de decodificação criptográfica, então o criptossistema é chamado *simétrico*."

Deste modo pode-se concluir que a pessoa que deseja transmitir uma informação que seja criptografada, deve fornecer ao seu destino uma cópia da chave que será responsável pela criptografia da informação na sua origem.

As chaves simétricas também podem ser conhecidas por chave única ou chave secreta.

4.3.2.1 Algoritmos Simétricos

Alguns dos algoritmos simétricos existentes são:

a) *Data Encryption Standard* (DES), foi desenvolvida pela IBM e inicialmente possuía uma chave de 128 bits, porém o governo dos Estados Unidos decidiu diminuir seu tamanho para 56 bits, a fim de deixá-lo mais rápido. Hoje este algoritmo é considerado fraco devido ao tamanho de sua chave (GUPTA, 2002, tradução nossa);

b) *Triple Data Encryption Standard* (3DES), também projetado pela IBM possui as mesmas características do DES, porém é dividido em três etapas. Primeira criptografa as informações, segunda descriptografa e por último novamente é criptografado (TANENBAUM, 2003);

c) *Advanced Encryption Standard* (AES), foi projetado para substituir o DES e 3DES, sendo que o tamanho da chave e de bloco podem variar de 128 bits a 256 bits (TANENBAUM, 2003);

d) *Ron's Code 4* (RC4), foi desenvolvido por Ronald Rivest, este algoritmo pode ter chave de comprimento de até 256 bytes onde aplica-se a operação lógica XOR para sua geração (GUPTA, 2002, tradução nossa).

4.3.3 Chaves Assimétricas

A proposta de chaves assimétricas surgiram em 1976 na Universidade de Stanford por Diffie e Hellman, no qual as chaves de criptografia e descriptografia teriam de ser diferentes e uma não poderia ter relação com a outra (TANENBAUM, 1997).

Neste modelo cada usuário possuirá duas chaves, uma denominada privada que jamais deverá ser compartilhada e outra denominada pública, está será compartilhada com os demais usuários, desta forma somente o usuário que tiver a chave pública do seu destino poderá efetuar a conexão (STALLINGS, 1998, tradução nossa).

4.3.3.1 Algoritmos Assimétricos

Alguns dos algoritmos assimétricos existentes são:

a) Diffie-Hellman é um algoritmo responsável por efetuar a troca de chaves entre os usuários, para que posteriormente as mensagens possam ser trocadas de forma segura (STALLINGS, 1998, tradução nossa);

b) *Rivest Shamir Adleman* (RSA) publicado em 1978 é bastante seguro e de acordo com Buchmann (2002, p. 161) "Sua segurança está intimamente relacionada à dificuldade de encontrar a fatoração de um número inteiro positivo múltiplo, que é o produto de dois números primos grandes."

Desta forma vimos que utilização da criptografia na transmissão de informação por meio da VPN é fundamental para que haja a segurança.

5 TRABALHOS CORRELATOS

Atualmente existem vários projetos e implementações da tecnologia de transmissão de dados sem fio Mesh, dentre esses projetos pode-se destacar os seguintes: Case de Tiradentes, MotoMesh, GTMesh e MeshNet.

5.1 CASE TIRADENTES

Este projeto foi implantado em 2006 na cidade histórica de Tiradentes em Minas Gerais, foi feito pelo Ministério das Comunicações e a Cisco do Brasil com parceria da Prefeitura Municipal e consultoria técnica da Companhia de Processamento de Dados do Município de Belho Horizonte (PRODABEL).

Alguns dos desafios foram devido a esta cidade ser tombada pelo Patrimônio Histórico Nacional e por ser em uma região serrana. Desta forma os aparelhos da Cisco foram implantados de forma estratégica em pontos da cidade. Uma das principais característica foi a questão da segurança onde se utilizou o mecanismo WPA2 e WPA com criptografia AES e entre os links foi utilizado a tecnologia VPN por meio do protocolo IPSec.

Com isso foi possível melhorar serviços de educação e saúde além de promovem o desenvolvimento da região. Desta forma foi possível promover a inclusão digital na região de Tiradentes.

5.2 MOTOMESH – TEXAS

O projeto *MOTOMESH* foi implantado na cidade de Plano, Texas. Com isso foi possível interligar departamentos como o de polícia, saúde e corpo de bombeiros.

Neste caso foram utilizados a largura de banda de 4.9Ghz para a segurança pública e a 2.4Ghz para o restante dos serviços públicos da cidade.

Com essa interligação foi possível obter informações em tempo real da situação, sendo assim o agente público pode chegar mais preparado na ocorrência e saber por onde começar. Os principais requisitos necessários foram a segurança da rede, privacidade dos dados e capacidade de interoperabilidade entre os diversos órgãos públicos.

5.3 GTMESH

Este projeto é formado por professores e alunos da Universidade Federal Fluminense. Sendo implantado dentro da instituição de ensino, onde foram utilizados os protocolos de roteamento OLSR e AODV. Teve como alguns de seus objetivos a implantação e desenvolvimento um protótipo de redes em malha, comparativos entre protocolos e também estudos sobre o fornecimento de QoS para as redes sem fio.

5.4 MESHNET

Projeto desenvolvido na Universidade da Califórnia e implantada no campus de Santa Barbara conta com 25 nós e estão dispostos em um prédio de cinco andares.

O principal objetivo da implantação de redes Mesh no campus foi para a pesquisa de protocolos de roteamento, para a transmissão multimídia, QoS e gerenciamento eficiente da rede.

6 IMPLANTAÇÃO DE UMA REDE SEM FIO MESH

Este projeto tem como objetivo pesquisar sobre o funcionamento de uma rede sem fio Mesh e também sobre o protocolo de roteamento OLSR que é responsável por organizar os nós na rede. Após este estudo foi realizada a montagem da rede entre os roteadores a fim de verificar o funcionamento. Posteriormente foi estudado o funcionamento de uma rede virtual privada com este modelo de rede para assim ter algum tipo de segurança baseada nos recursos utilizados.

6.1 METODOLOGIA

A parte inicial desta pesquisa compreendeu no levantamento bibliográfico, realizada no decorrer do desenvolvimento do projeto, a cerca das redes sem fio, redes Mesh, protocolo de roteamento OLSR, segurança e VPN.

Sendo que para redes sem fio objetivou-se conhecer seu funcionamento, quais frequências e a forma de modulação, na sequência descreveram-se os padrões, aspectos segurança e também alguns tipos de ataques que as redes sem fio estão sujeitas.

Para redes Mesh a pesquisa descreve seu funcionamento e tipos existentes, características, arquitetura e os protocolos de roteamento disponíveis.

Dentro das redes Mesh optou-se pelo protocolo OLSR onde foi possível compreender melhor o seu funcionamento, características e detalhes mais precisos como sobre o formato de suas mensagens.

Por fim da parte teórica estudou-se sobre VPN visando suas características, arquitetura, protocolos disponíveis para a criação do tunelamento para que os dados possam trafegar, além da criptografia.

Finalizado estudo sobre o projeto, analisou-se alguns trabalhos nesta área, principalmente na utilização da tecnologia Mesh no Brasil e no exterior.

A partir disso passou para a etapa prática do projeto. Deste modo o primeiro passo a ser dado foi a escolha do *Firmware* a ser utilizado, sendo analisado os principais disponíveis atualmente no mercado e que também conseguissem atender as necessidades do projeto. Em seguida houve a escolha do software VPN e logo após foram feitas as configurações necessárias para a realização do projeto.

6.1.1 ESCOLHA DO FIRMWARE

Firmwares são pequenos softwares capazes de serem instalados em um dispositivo de hardware onde tenha memória disponível para instalação, cujo principal objetivo é promover o funcionamento do mesmo.

Existem dois *Firmwares* mais conhecidos que são: DDWRT e OpenWRT. Ambos suportam diversos dispositivos, sendo que o segundo possui algumas derivações entre eles o Freifunk que foi a tecnologia implantada neste trabalho. Um detalhe a ser observado é que todos os *Firmwares* são derivados a partir do Linux e são de código fonte aberto.

6.1.1.1 DDWRT

Bastante conhecido, pois suporta diversos roteadores de diferentes marcas. Depois do estudo percebeu-se a impossibilidade de instalar o protocolo OLSR e a VPN juntos, pelo motivo dos pacotes serem separados, portanto fica impossibilitada a integração. A versão utilizada para os testes de compatibilidade foi a número 24.

6.1.1.2 OpenWRT

Este *Firmware* tem como *slogan* “Wireless Freedom”, ou seja, visa promover a liberdade da utilização da rede sem fio, também é bastante conhecido e possui suporte a vários roteadores e marcas (OPENWRT, 2004). Além disso, ele possui algumas derivações entre elas está o Freifunk. Sendo utilizada a versão Backfire 10.03.1-rc5 para testes de verificação de compatibilidade com o projeto.

6.1.1.3 Freifunk

Desenvolvido na Alemanha como o intuito de promover o acesso a Internet gratuita para todos, na tradução deste nome temos “rádio livre”. Uma das suas intenções é que um usuário que tenha um roteador disponível e compatível com o *Firmware* possa se conectar a rede e assim promover um maior alcance de rede e também o compartilhamento de arquivos (FREIFUNK, 2004).

Para os testes foi utilizada a versão 1.7.4 em português. Na Figura 17 pode-se visualizar um pequeno comparativo entre os *Firmwares* citados anteriormente.

	Modo Ad-hoc	OLSR	VPN	OLSR e VPN	Idioma Português
DDWRT	X	X	X	-	X
OPENWRT	X	X	X	X	-
FREIFUNK	X	X	X	X	X

Figura 17. Comparativo entre *Firmwares*

Para a escolha do *Firmware* foi levado em conta a possibilidade de utilização da VPN e do OLSR, para assim alcançar os objetivos que o projeto se propõe e também que o mesmo tivesse o idioma em português, para que caso alguém tenha interesse em utilizá-lo e não possua conhecimento em outras línguas possa perfeitamente configurá-lo e assim poder montar sua própria rede.

6.1.2 ESCOLHA DO SOFTWARE VPN

O *Firmware* escolhido possui em seu repositório diversos pacotes com diferentes programas que possam ser utilizados. Para VPN é disponibilizado três diferentes programas que são: Tinc, OpenSwan e OpenVPN.

6.1.2.1 Tinc

O programa Tinc é um software livre que possui versões para diversos sistemas operacionais e atualmente está na versão 1.0.16, algumas características são de possuir autenticação, criptografia e compressão, conforme Timmermans e Sliepen (2000?, tradução nossa).

Após pesquisas pode-se verificar que é um software pouco desmistificado, portando possui pouco material para seu estudo, onde a maior parte que pode ser encontrada está no próprio site do Tinc.

6.1.2.2 OpenSwan

Pouca informação é encontrada sobre seu desenvolvimento, porém o que há de disponível é que esta implementação trata-se de uma derivação do já descontinuado FreeS/Wan.

Conforme Richardson (2003?) o OpenSwan é uma implementação para distribuições do sistema operacional Linux baseado no IPSec, sendo suportada pelos *Kernels* nas versões 2.0, 2.2, 2.4 e 2.6.

A respeito do OpenSwan é possível verificar que não há disponível um vasto material sobre o mesmo. Sendo que a maior parte dele é encontrado em seu próprio site na Internet.

6.1.2.3 OpenVPN

OpenVPN é uma implementação VPN baseada no *Secure Socket Layer* (SSL), possui código fonte aberto e está disponível para diversos sistemas operacionais. Esta implementação foi considerada em 2007 a melhor implementação SSL pela revista InfoWorld, dentro da categoria *Open Source* e em 2010 pelo site LifeHacker a melhor ferramenta VPN. Atualmente sua comunidade possui cerca de 5 milhões de usuários (DINHA; YONAN, 2002, tradução nossa).

Optou-se pela escolha do OpenVPN por ser uma das aplicações mais utilizadas, além de possuir o *Firmware* Freifunk e uma interface intuitiva e fácil de ser utilizada.

6.2 ESPECIFICAÇÃO DOS EQUIPAMENTOS

Para a realização dos testes de funcionamento das redes Mesh, foram utilizados dois roteadores sem fio da marca Linksys e modelo WRT54GL V1.1, como pode-se visualizar na Figura 18.

Figura 18. Roteador Linksys

Dos roteadores as principais características são:

a) Padrões: IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE 802.11b;

b) Canais: 11 Canais (EUA, Canadá) e 13 Canais (Europa, Japão);

c) Portas: 1 para Internet 10/100 RJ45, 4 para LAN 10/100 RJ45;

d) Potência da radio frequência: 18 dBm;

e) Segurança sem fio: WPA2, WEP e filtragem endereços MAC pela interface sem fio.

6.3 IMPLANTAÇÃO DA TECNOLOGIA

Os roteadores sem fio já vem por padrão com um *Firmware* proprietário instalado, porém não é possível integrá-lo com a tecnologia de redes Mesh. Mas por serem compatíveis com o *Firmware* a ser instalado optou-se pela escolha do mesmo, pelo motivo de ser disponibilizado pelo orientador e assim não gerou custo.

Deste modo é possível iniciar a implantação da tecnologia, onde deve-se seguir os seguintes passos:

a) download do *Firmware* de acordo com o modelo do roteador;

b) instalação do mesmo no roteador;

c) atualização do mesmo;

d) configuração diversas no roteador para o funcionamento do OLSR;

e) configuração da VPN.

Na Figura 19 pode-se visualizar o local onde deve-se atualizar o *Firmware*.

Figura 19. *Firmware* Linksys

Quando o *Firmware* estiver instalado no aparelho irá abrir uma nova interface no lugar da anterior como é possível visualizar na Figura 20.

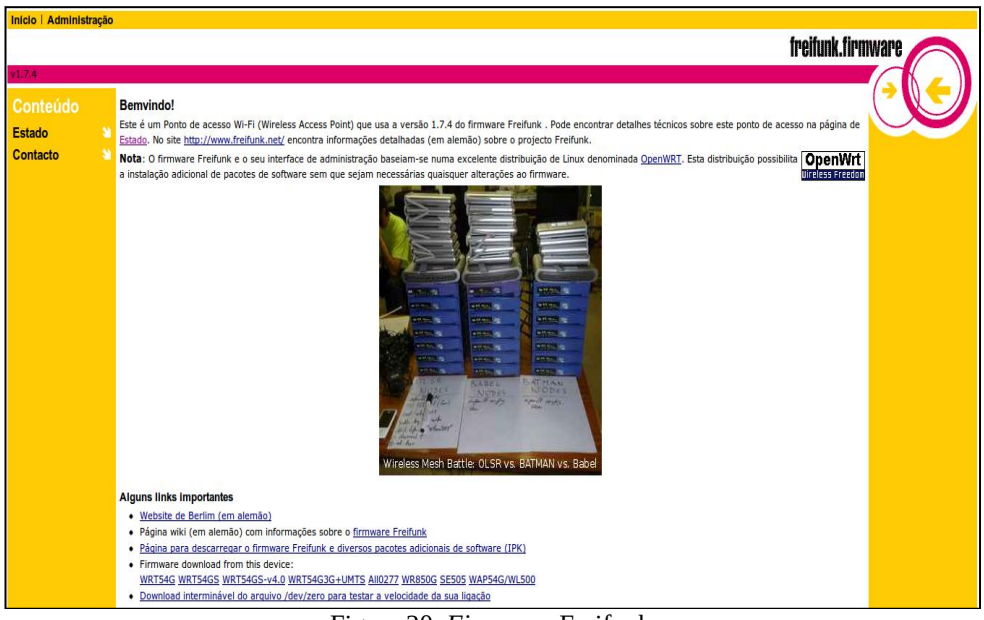


Figura 20. *Firmware* Freifunk

Após a instalação deve-se atualizar o mesmo, dessa forma serão instalados automaticamente os seguintes pacotes:

a) freifunk-dnsmasq: fornece algumas customizações;

b) busybox-ping6: programa que fornece suporte para o comando *ping*.

c) kmod-ipv6: módulo do *kernel* para IPv6;

d) libncurses: biblioteca de manipulação;

e) libpcap: biblioteca de captura de pacotes de baixo nível;

f) nc6: programa NetCat reescrito para IPv6;

g) zlib: biblioteca para corrigir erros de *overflow*;

h) freifunk-ipv6: programa para executar IPv6 no OLSR;

i) freifunk-map-en: ferramenta baseada no Google maps;

j) freifunk-olsr-viz-en: aplicação para exibir graficamente os nós da rede OSLR;

k) librrd1: biblioteca de gerenciamento do *Round Robin Database* (RRD);

l) xyssl: uma implementação do SSL;

m) rrdcgi1: ferramenta gráfica do RRD;

n) rrdcollect: programa de coleta do RRD;

o) rrdtool1: programa RRD, responsável por armazenar e exibir informações de dados;

p) xrelayd: reposição do stunnel;

q) freifunk-secureadmin-en: suporte para *HyperText Transfer Protocol Secure* (HTTPS);

r) freifunk-statistics-en: responsável pela exibição das estatísticas da rede baseado nas informações coletadas pelo RRD;

s) freifunk-tcpdump: programa para monitoramento de rede;

t) horst: ferramenta para escanear redes próximas;

u) freifunk-recommended-pt: programa para o idioma em português.

Na Figura 21 pode-se visualizar um pequeno comparativo antes e depois da atualização do *Firmware*.

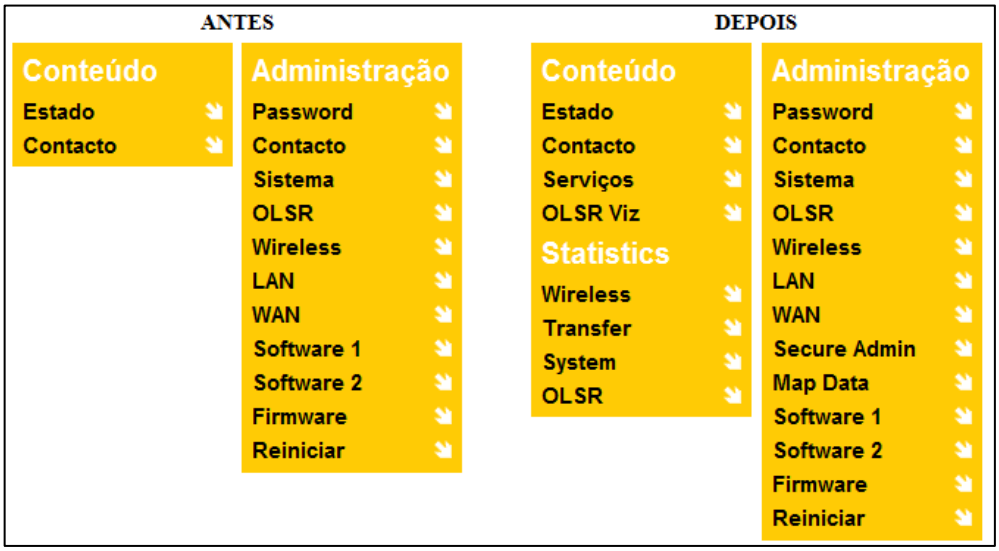


Figura 21. Comparativo dos Menus

Em seguida a atualização, é possível verificar que algumas opções novas apareceram na página, deste modo agora é possível iniciar a configuração da rede para o funcionamento da rede sem fio e do protocolo OLSR consecutivamente. O manual de instalação está disponível no Apêndice A e a configuração detalhada utilizadas nos roteadores está disponível no Apêndice B.

Os itens necessários para a configuração estão na aba administrativa que são: *Wide Area Network* (WAN), *Local Area Network* (LAN), Wireless e OLSR.

A opção WAN é responsável pela conexão com a Internet, deste modo deixa-se com a opção de "Usar servidor DHCP", para atribuição automática do endereçamento do *Internet Protocol* (IP). Outra alteração necessária é habilitar os campos: Permitir SSH, acesso via HTTP, acesso via HTTPS e *Ping*, desta forma é possível conectar no dispositivo via *Secure Shell* (SSH), *HyperText Transfer Protocol* (HTTP), HTTPS e testar a conectividade via *Ping*.

A opção LAN fica responsável pelo endereçamento da conexão via cabo de rede. Por padrão cada dispositivo possui o mesmo endereço IP, mas para evitar confusões é recomendável que cada dispositivo tenha endereços diferentes.

Na aba Wireless tem-se configurações importantes para que a rede Mesh funcione perfeitamente. Para um melhor gerenciamento divida a rede em pequenas subredes onde cada roteador ficará responsável por uma pequena gama de usuários e coloque o endereço identificador da mesma como IP fixo, porém deixe a máscara com a classe cheia para que os clientes possam se comunicar.

Para isso é necessário definir o endereço IP como fixo para cada dispositivo e ter uma máscara cheia de acordo com sua classe. Outra informação importante a ser especificada é em relação ao modo de operação, onde deve-se alterar para modo *Ad-Hoc*, além de definir um nome para a rede e um canal de atuação da mesma.

Na aba OLSR apenas um item é importante para que clientes possam conectar-se a rede, este campo é o DHCP-OLSR. Aqui tem-se a seguinte configuração: *endereço_ip_roteador/máscara,máscara* neste caso deve-se colocar o IP da interface Wireless junto com sua respectiva máscara e por fim outra máscara ficando da seguinte forma 192.160.1.64/26,255.255.255.0 desta forma os clientes estarão na dentro da faixa de IP permitida por cada roteador e também poderão se comunicar entre si. Sendo assim os clientes que se conectarem a rede receberam um endereço IP automático de acordo com o dispositivo que estarão conectados.

Após todas as configurações feitas em ambos roteadores é possível verificar no item “OLSR VIZ” que se encontra na página inicial do dispositivo a exibição dos nós da rede (Figura 22). Sendo que o nó que está conectado a Internet automaticamente muda de cor, neste caso é o primeiro.

Figura 22. Rede Mesh com Dois Nós

Sendo assim já é possível utilizar a rede sem fio com o protocolo funcionando. O próximo passo é a instalação e configuração do OpenVPN. Deste modo é necessário instalar os pacotes:

a) libopenssl: biblioteca de criptografia SSL;

b) kmod-tun: modulo de tunelamento;

c) openvpn: software OpenVPN;

d) freifunk-openvpn-en: interface de configuração do OpenVPN.

A VPN foi criada entre as interfaces sem fio, ou seja, será criado um tunelamento pela *Wireless Local Area Network* (WLAN). Neste caso a primeira configuração a ser definida é o modo de tunelamento, sendo disponibilizados dois modos que são:

a) ponto-a-ponto: este modelo utiliza o conceito de chaves simétricas onde tanto o servidor como o cliente utilizam a mesma chave;

b) multi-ponto: utiliza o conceito de chaves assimétricas e há a necessidade da instalação de pacotes adicionais para que haja a geração dos arquivos necessários para sua configuração.

Deste modo escolheu-se a primeira opção para a implantação da VPN. Na página de configuração, as principais alterações a serem feitas são:

a) modo de conexão: onde deve-se escolher Point-to-Point (PTP);

b) modo de operação: onde um dos dispositivos deve ser o servidor e o outro o cliente;

c) túnel com *Network Address Translation* (NAT): deve ser habilitado no cliente para que haja acesso ao servidor;

d) estação remota: este campo deve ser preenchido somente no cliente, onde deve-se colocar o endereço do servidor;

e) compressão LZO: deve-se habilita-la em ambos para que haja a compactação dos dados;

f) chave compartilhada: deve-se gerar a chave e copiá-la para o outro dispositivo.

Depois de tudo configurado deve-se aplicar as alterações e em seguida é necessário reiniciá-lo.

Pra que seja possível acessar LAN do outro dispositivo deve-se adicionar a rota para a mesma, sendo assim deve-se entrar no dispositivo configurado como cliente via um programa de SSH editar o arquivo do OpenVPN localizado em */etc/openvpn/freifunk.conf* adicionar no final a linha *route 192.168.1.0 255.255.255.0* e depois reiniciar o serviço pelo comando */etc/init.d/openvpn restart*.

6.4 RESULTADOS OBTIDOS

Para os resultados obtidos durante os testes criou-se dois cenários distintos, o primeiro para os testes somente com o protocolo OLSR, trata-se de uma arquitetura de infraestrutura/*backbone*, onde os clientes possam se conectar a rede.

No segundo cenário utilizou-se a mesma topologia do anterior, porém com a criação da VPN entre os roteadores onde utilizou-se a forma de rede para rede.

6.4.1 Primeiro Cenário

Os testes iniciais deram-se somente com o protocolo de roteamento funcionando. É possível visualizar na Figura 23 que trata do primeiro cenário a ser testado, para isto foram utilizados dois roteadores, sendo que um deles está conectado a Internet e dois computadores com interface de rede sem fio. A seguir serão demonstrados três testes aplicados ao primeiro cenário.

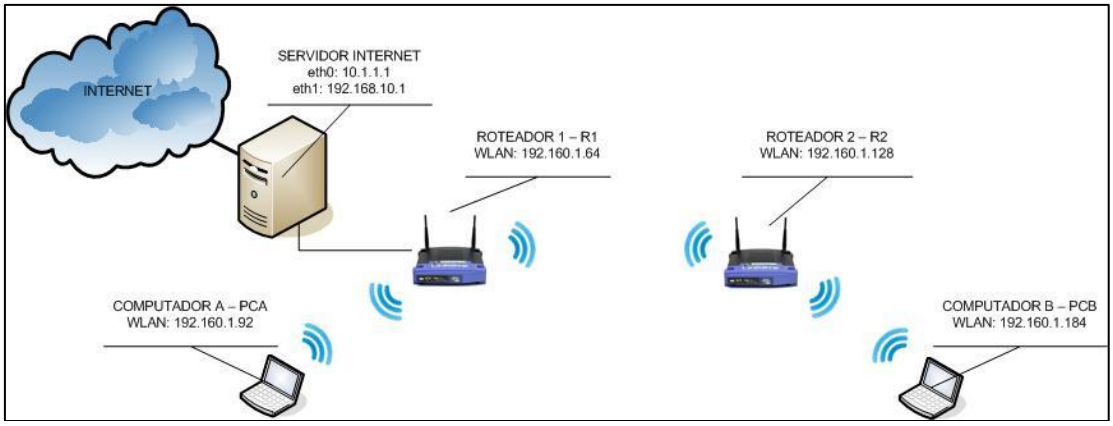


Figura 23. Primeiro Cenário

O primeiro teste a ser aplicado foi o *Ping* (Figura 24). Com este comando é possível verificar se o IP de destino pode ser encontrado, deste modo o computador PCA conectado no roteador R1 obteve sucesso na comunicação com o PCB que estava conectado no roteador R2

```
PING 192.160.1.184 (192.160.1.184) 56(84) bytes of data.
64 bytes from 192.160.1.184: icmp_seq=1 ttl=128 time=4.14 ms
64 bytes from 192.160.1.184: icmp_seq=2 ttl=128 time=2.82 ms
64 bytes from 192.160.1.184: icmp_seq=3 ttl=128 time=1.29 ms
64 bytes from 192.160.1.184: icmp_seq=4 ttl=128 time=9.58 ms
64 bytes from 192.160.1.184: icmp_seq=5 ttl=128 time=1.59 ms
64 bytes from 192.160.1.184: icmp_seq=6 ttl=128 time=1.57 ms
^C
--- 192.160.1.184 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 1.295/3.501/9.580/2.888 ms
```

Figura 24. *Ping* entre Máquinas

O segundo teste foi a execução do comando *Traceroute* (Figura 25). Sendo responsável por verificar se um endereço IP de destino pode ser encontrado, além de exibir todos os saltos até chegar a seu destino. Para este caso o comando a ser executado teve seu inicio no computador PCB conectado ao roteador R2 com o destino de um site na Internet.

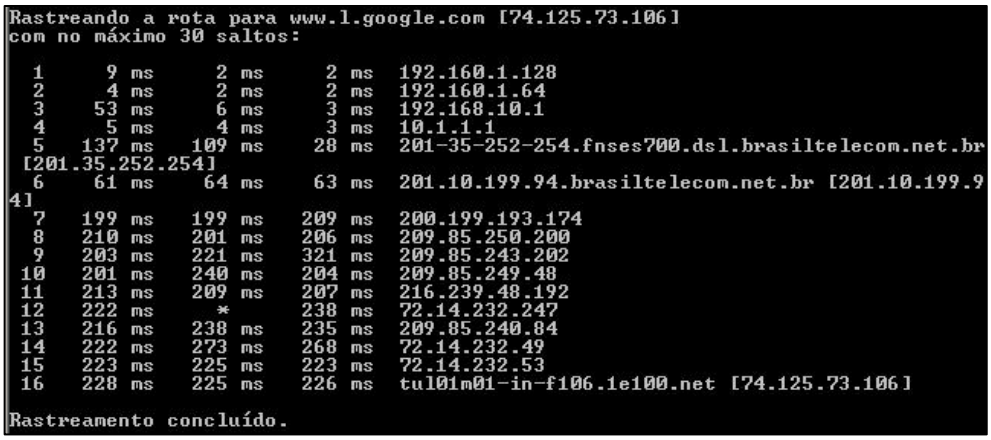


Figura 25. *Traceroute* para a Internet

Por último houve a troca e acesso de arquivos. Na Figura 26 é possível verificar o computador PCA conectado ao PCB e possibilitando acesso a arquivos e a edição de um documento de texto.

Figura 26. Compartilhamento de Arquivos

Deste modo percebeu-se o perfeito funcionamento do protocolo OLSR em todos os testes descritos acima.

6.4.2 Segundo Cenário

No segundo cenário como pode-se visualizar na Figura 27, está implantada a VPN entre os roteadores por meio do tunelamento ponto a ponto. Neste cenário observa-se que o primeiro roteador possui um servidor conectado a sua porta LAN, onde após a adição da rota para a LAN do servidor o cliente poderá usufruir dos serviços prestados pelo mesmo, como por exemplo o compartilhamento de arquivos.

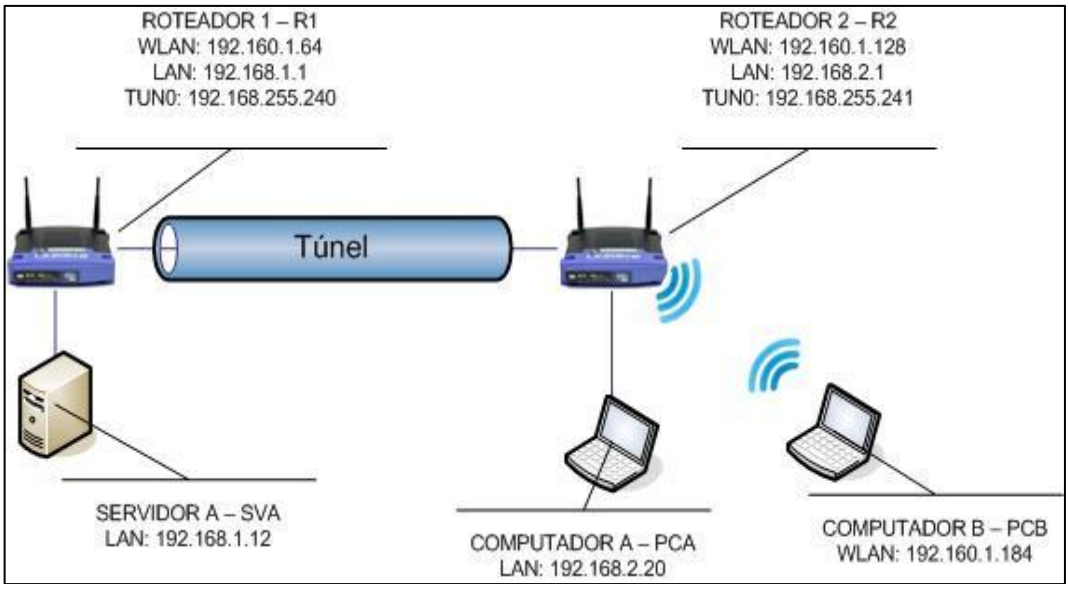


Figura 27. Segundo Cenário

Os primeiros testes a serem apresentados referem-se a conexão entre PCB para com SVA, neste caso PCB estará utilizando uma conexão sem fio.

Na Figura 28 pode-se visualizar que por meio do comando *traceroute* verificou-se que o mesmo passou pelo endereço criado a partir da VPN.

```
Rastreando a rota para 192.168.1.12 com no máximo 30 saltos

  1     1 ms     1 ms     1 ms  192.160.1.128
  2     6 ms     6 ms     6 ms  192.168.255.240
  3     6 ms     6 ms     8 ms  192.168.1.12

Rastreamento concluído.
```

Figura 28. *Traceroute* para o Servidor

Para os testes de captura de pacotes, utilizou-se outro computador com interface de rede sem fio onde o mesmo esteve localizado entre os roteadores.

Mesmo as informações estarem sendo acessadas pela VPN foi possível verificar que por meio da utilização do programa *open source* Wireshark, responsável pela captura de pacotes, que o mesmo não está totalmente criptografado (Figura 29).

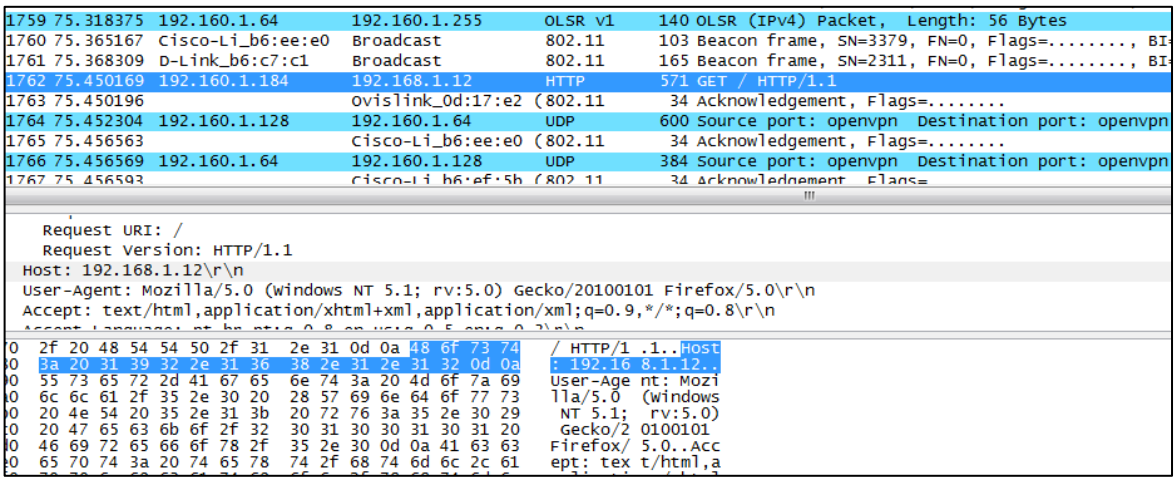


Figura 29. Captura de Pacotes pelo Wireshark

Os demais testes a seguir são em relação ao cliente PCA conectado a sua interface LAN, ou seja, por meio de cabos para com o servidor SVA.

Na Figura 30 pode-se visualizar o resultado do comando *Traceroute*, onde é possível perceber sua trajetória até seu destino.

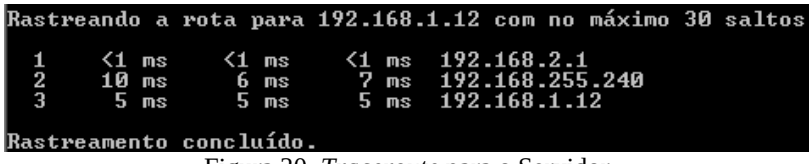


Figura 30. *Traceroute* para o Servidor

Por último foi realizado a utilização de um serviço HTTP do servidor.

Na Figura 31 é possível observar os pacotes capturados por meio do *Wireshark*, onde exibem que os mesmos passaram pelo túnel, mas que as informações capturada não são legíveis.

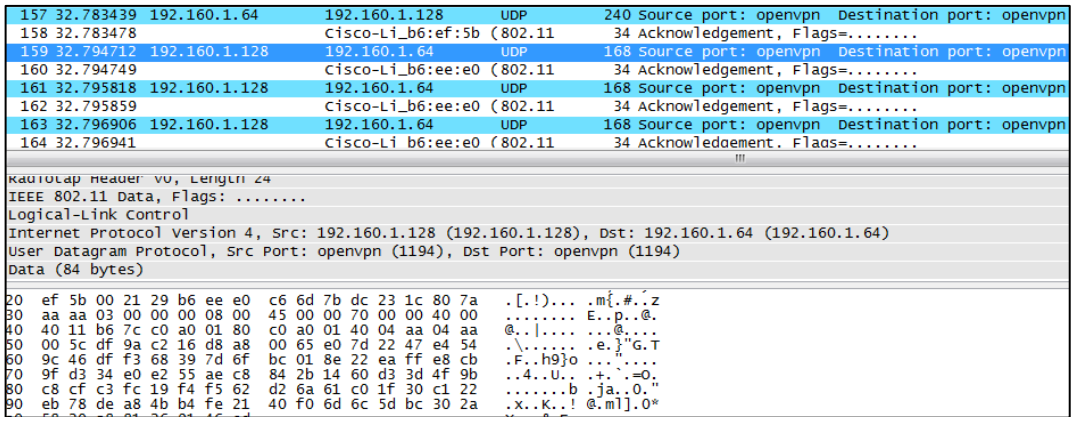


Figura 31. Captura de Pacotes pelo Wireshark

Todos os testes aplicados a VPN foram bem sucedidos, porém o único local onde houve a captura de informações foi por meio da conexão sem fio, pelo motivo de não possuir nenhum tipo de mecanismo segurança como autenticação dos clientes para com os roteadores.

6.5 INFORMAÇÕES ADICIONAIS

As informações apresentadas aqui são de recursos que o próprio Freifunk fornece, além de uma demonstração com mais de dois nós na rede.

Por meio do recurso de visualização disponível pelo *Firmware*, a Figura 32 pode-se verificar a rede Mesh com três nós, esta formação somente foi possível no início do desenvolvimento do projeto, quando se tinha disponíveis três roteadores.

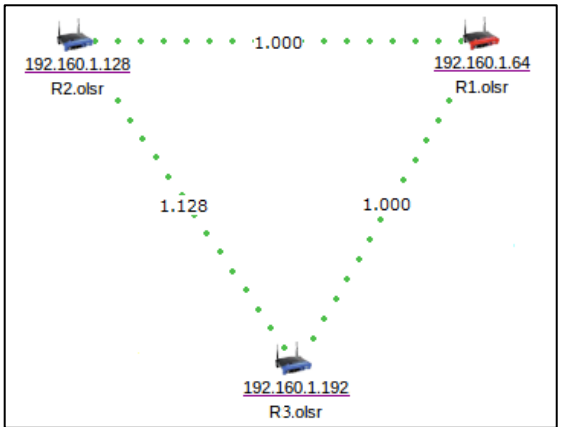


Figura 32. Rede Mesh com Três Nós

As Figuras apresentadas abaixo foram retiradas do roteador R1, com dois roteadores na rede. A Figura 33, Figura 34, Figura 35 e Figura 36 foram retiradas da página inicial na opção “Estado”.

Como pode-se visualizar na Figura 33 a aba “Resumo” que fornece diversas informações sobre o roteador.

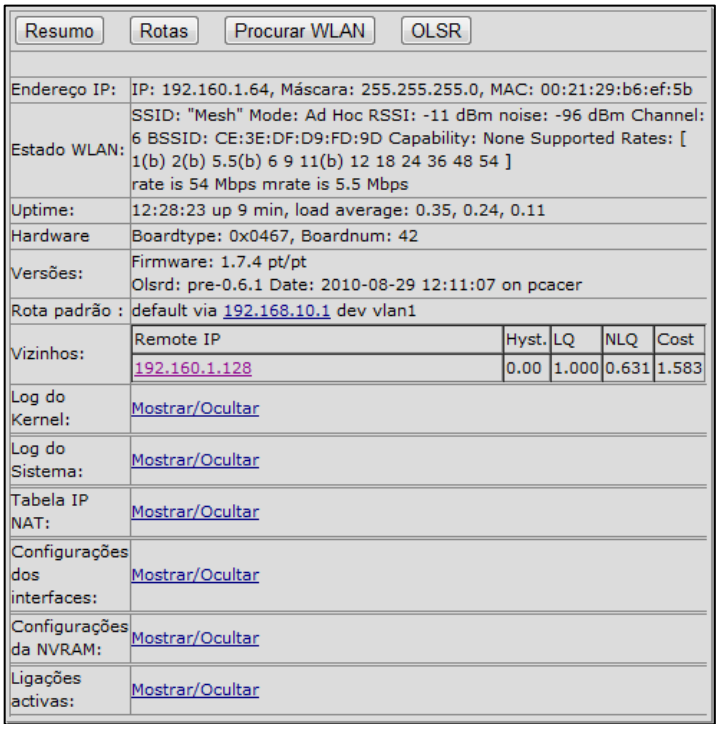


Figura 33. Resumo do OLSR

Na aba “Rotas” que pode ser visualizada na Figura 34 exibe todas as rotas disponíveis.

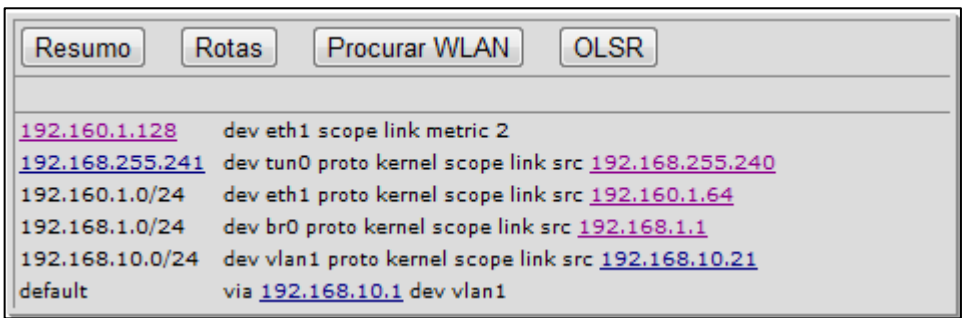


Figura 34. Rotas Disponíveis

Na Figura 35 pode-se visualizar a aba “Procurar WLAN”, onde é possível verificar todas as redes sem fio que estejam ao seu alcance.

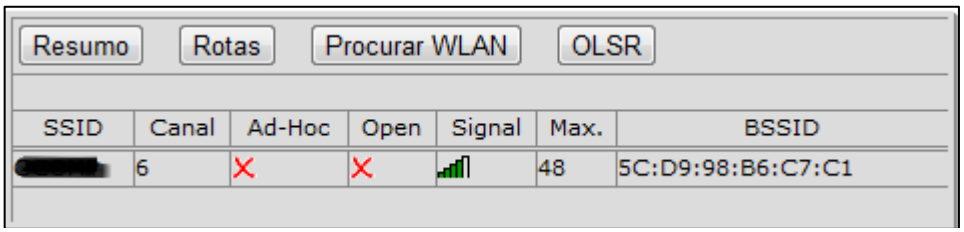


Figura 35. Redes Sem Fio Disponíveis

Na Figura 36 referente ao OLSR, exibe diversas informações sobre o protocolo de roteamento OLSR como: links, nós vizinhos ao roteador, topologia, mensagens HNA e MID e as rotas.

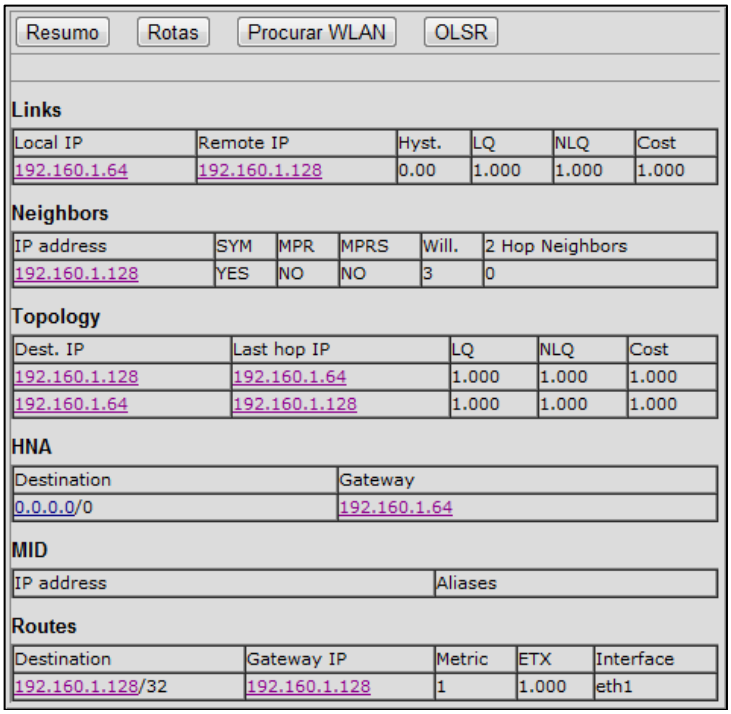


Figura 36. Informações Específicas do OLSR

Na parte de estatísticas o Freifunk disponibiliza em gráficos algumas de informações. Como a tráfego que passa pelas interfaces, uso do sistema, informações sobre a Wireless e sobre o OLSR.

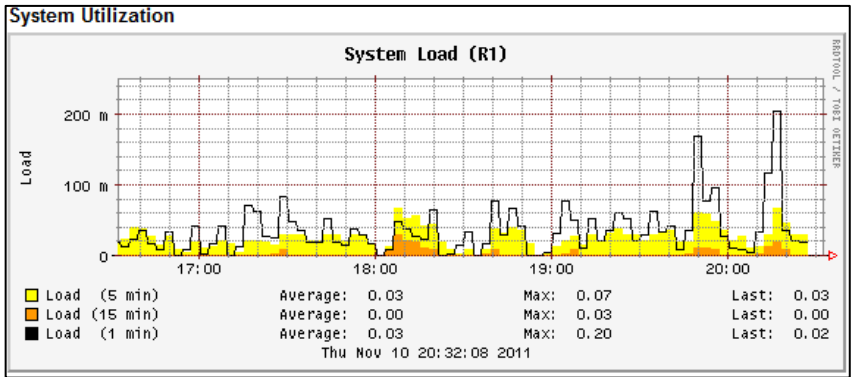


Figura 37. Utilização do Sistema

Na opção “System” pode-se visualizar um gráfico com a utilização do sistema (Figura 37).

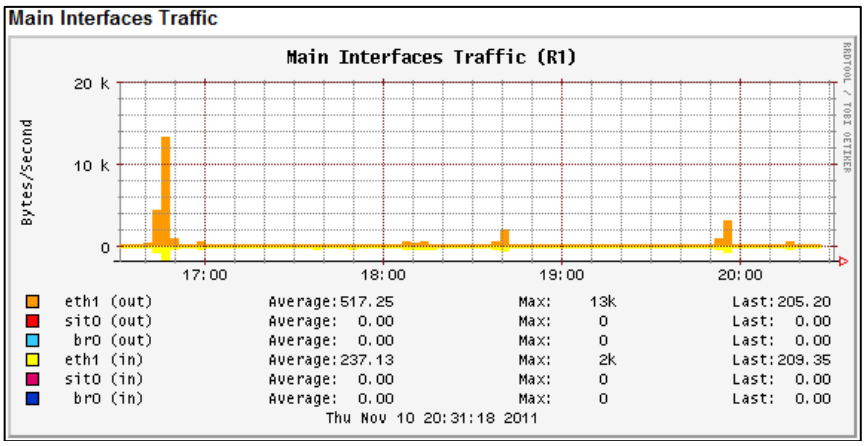


Figura 38. Tráfego de Rede

Na opção “Transfer” visualiza-se um gráfico com o tráfego das principais interfaces de rede (Figura 38).

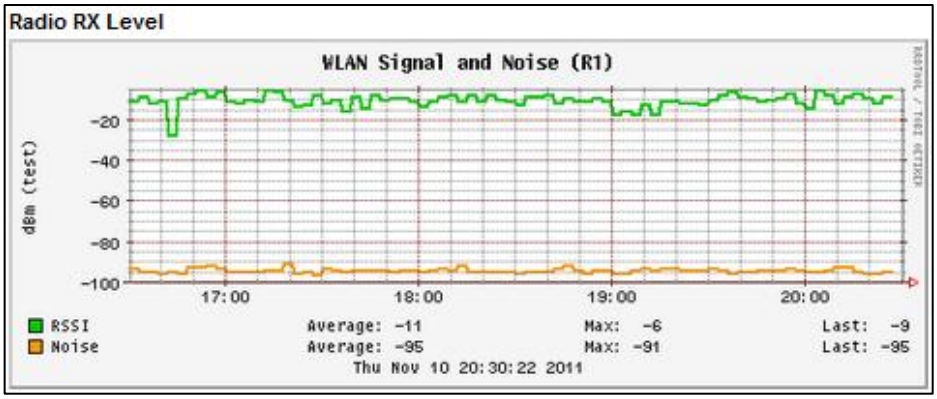


Figura 39. Sinal e Noise WLAN

Na opção “Wireless” pode-se verificar dados referente a WLAN (Figura 39).

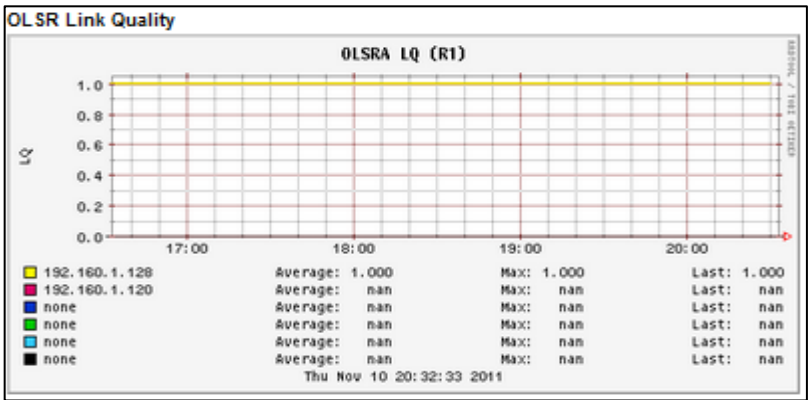


Figura 40. Qualidade do Link OLSR

Na opção “OSLR” verifica-se a cerca do link do protocolo OLSR (Figura 40).

6.6 OLSR SWITCH

O software OLSR SWITCH é disponibilizado no próprio site do protocolo onde com ele é possível o usuário se tornar um nó da rede e assim aumentar o alcance, desta maneira a arquitetura da rede se tornará híbrida.

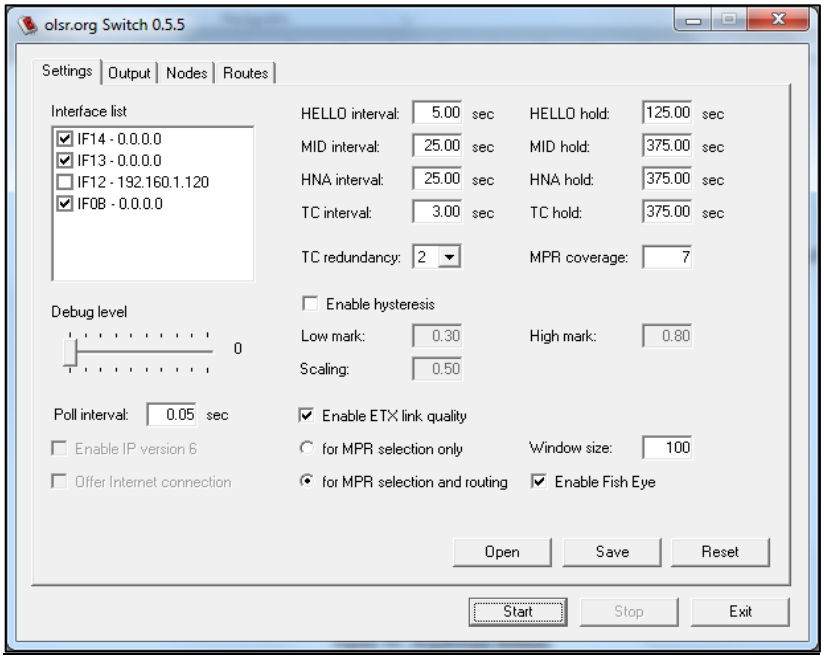


Figura 41. OLSR SWITCH

Na Figura 41 tem-se uma imagem do programa, onde tem-se várias informações referente ao protocolo e configurações que podem ser feitas.

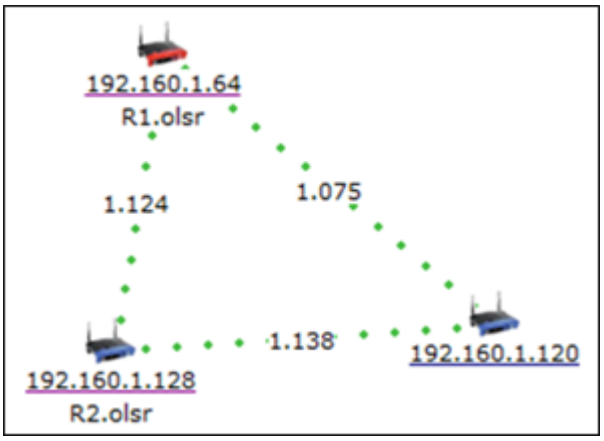


Figura 42. Arquitetura Híbrida

Na Figura 42 exibe a rede Mesh com um cliente que está participando como um nó, deste modo a rede se torna híbrida.

Sendo assim para que o usuário possa criar sua própria rede sem fio Mesh, por meio da utilização de computadores ou outros dispositivos com interface sem fio poderão estar utilizando este programa.

CONCLUSÃO

Este trabalho teve como objetivos a realização de estudos das redes sem fio Mesh para assim descrever suas funcionalidades, o protocolo OLSR e o funcionamento das redes virtuais privadas.

Para as redes sem fio buscou-se seu histórico, deste modo também possibilitou descrever sobre suas fragilidades na questão de segurança e podendo verificar melhor alguns ataques que as mesmas estão sujeitas.

Foi possível obter um melhor conhecimento no funcionamento de uma rede sem fio Mesh, assim como características, arquiteturas e protocolos atualmente disponíveis.

A cerca do protocolo de roteamento OLSR, pode-se verificar seu funcionamento por meio de pesquisas e consulta a RFC 3626. Foi possível então ter uma visão aprofundada sobre a técnica que evita a sobrecarga da rede, formatação de pacotes, mensagens transmitidas, tabela de roteamento e por fim uma pequena observação sobre segurança e sobre a sexta versão do protocolo IP.

O conhecimento obtido por pesquisas da VPN trouxe grande contribuição para ajudar na segurança, onde pode-se conhecer melhor sobre alguns dos protocolos existentes atualmente, além de seu funcionamento e a forma em que se estabelece o tunelamento.

Desta forma, os objetivos que eram montar uma rede sem fio Mesh utilizando o protocolo de roteamento OLSR pode ser concluído com êxito. Após a rede estar em funcionamento foi possível implementar uma VPN por meio da utilização do OpenVPN entre os roteadores a fim de promover segurança no acesso de clientes a um determinado servidor.

Verificou-se que por meio da utilização de softwares livres como o Freifunk é possível criar uma rede sem fio com um maior alcance e com baixo custo. Também foi

possível por meio do software OLSR SWITCH, visualizar a expansão da rede sem a necessidade de equipamento específico.

Por meio de roteadores pode-se implantar uma rede com grande alcance, para que seja disponibilizada Internet para várias pessoas de forma simples.

Em relação a VPN observou-se que é possível ter um determinado computador que possa prestar algum tipo de serviço como armazenamento de arquivos e acesso a um servidor HTTP. Também foi possível analisar que a implementação VPN tornou-se segura somente na conexão via cabos e por não haver nenhum tipo de segurança dos clientes para com os roteadores ainda tem-se o vazamento das informações.

A principal dificuldade encontrada foi em relação a configuração do *Firmware* Freifunk. Pois devido sua origem ser na Alemanha boa parte do material encontrado estava no idioma alemão, mas com a ajuda de programas de tradução foi possível compreender e poder efetuar a configuração dos roteadores.

Foi possível analisar que na conexão do cliente utilizando a interface de rede sem fio não deu-se de forma totalmente segura, neste caso seria necessário um novo estudo para promover esta segurança.

Para trabalhos futuros pode-se verificar uma solução dos clientes que irão usar a conexão sem fio como algum tipo de autenticação e validação de usuários.

Também poderá ser feita uma implementação das outras tecnologias VPN disponibilizadas pelo Firmware.

Outro trabalho pode sem em relação a análise de desempenho de protocolos de roteamento, desta forma deve-se analisar outros protocolos em redes Mesh.

Por último, foi possível por meio deste trabalho obter conhecimento das redes sem fio, redes Mesh, OSLR e VPN, sendo que deste modo há um grande crescimento profissional.

REFERÊNCIAS

AKYILDIZ, F. Ian; WANG, Xudong. **Wireless Mesh Networks.** United Kingdom: John Wiley & Sons Ltd, 2009.

BUCHMANN, Johannes A. **Introdução à criptografia.** São Paulo: Berkeley, 2002.

CARVALHO, Tereza Cristina Melo de Brito. **Arquitetura de redes de computadores OSI e TCP/IP.** 2 ed. São Paulo: Makron Books, 1997.

CHANDRA, Praphuletal. **Wireless Security:** Know it all. Oxford: Elsevier, 2009.

CHEN, Jyh-cheng; ZHANG, Tao. **IP-based next-generation wireless networks:** systems, architectures, and protocols. New Jersey: John Wiley & Sons, 2004.

CISCO. **Tecnologia Cisco Promove Inclusão Digital na cidade histórica de Tiradentes (Minas Gerais).** 2006. Disponível em: <http://www.cisco.com/web/BR/microsites/ps/portugues/downloads/CaseTiradentes.pdf>. Acesso em: abr. 2011.

CLAUSEN, Thomas Heide; JACQUET , Philippe. **Optimized Link State Routing Protocol (OLSR).** 2003. Disponível em: <http://www.ietf.org/rfc/rfc3626.txt>. Acesso em: abr. 2011.

COMER, Douglas E.. **Redes de Computadores e Internet.**2 ed. Porto Alegre: Bookman, 2001.

DINHA, Francis; YONAN, James; NIMON, Bob. **OpenVPN.** 2002. Disponível em: <http://openvpn.net>. Acesso em: out. 2011.

DORNAN, Andy. **Wireless communication:** o guia essencial de comunicação sem fio. Rio de Janeiro: Campus, 2001.

EARLE, Aaron E.. Wireless security handbook. Florida: Auerbach Publications, 2006.

FREIFUNK. **Freifunk.** 2004. Disponível em: <http://start.freifunk.net>. Acesso em: 10 ago. 2011.

FROSI, Bruno Gehlen; SCHAEFFER, Carlos Adriani Lara. **Definições da RFC3626 e o Protocolo OLSR.** 2010. Universidade de Passo Fundo, Passo Fundo – RS. Disponível em: <www.upf.br/computacao/images/stories/TCs/201001/Bruno_Frosi_a.pdf>. Acesso em: 2011.

FSTC, Faculty of Science, Technology and Communication. **Optimized Link State Routing Protocol.** Universidade de Luxemburgo [2005?].Disponível em: <http://wiki.uni.lu/secan-lab/Optimized+Link+State+Routing+Protocol.html>. Acesso em: abr. 2011

GANZ, Aura; GANZ, Zvi; WONGTHAVARAWAT, Kitti. **Multimedia Wireless Networks:** Technologies, Standards, and QoS. Pretince Hall, 2003.

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

GUPTA, Meeta. **Building a Virtual Private Network.** Ohio: Premier Press, 2003.

HELD, Gilbert. **Wireless mesh networks.** New York: Auerbach Publications, 2005.

METHLEY, Steve. **Essentials of Wireless Mesh Networking.** New York: Cambridge University Press, 2009.

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

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

MURHAMMER, Martin W. et al. **TCP/IP:** Tutorial e Técnico. São Paulo: Makron Books, 2000.

NORTHCUTT, Stephen et al. **Desvendando segurança em redes:** o guia definitivo para fortificação de perímetros de rede usando Firewalls, VPNs, roteadores e sistemas de detecção de invasores. Rio de Janeiro: Campus, 2002.

OPENWRT. **OpenWRT Wireless Freedom.** 2004. Disponível em: <https://openwrt.org/>. Acesso em: ago. 2011.

PEIKARI, Cyrus; FOGIE, Seth. **Maximum Wireless Security.** Usa: Sams Publishing, 2002.

PRASAD, Anand R.; PRASAD, Neeli R.. **802.11 WLans and IP Networking:** Security Qos and Mobility. London: Artech House, 2005.

RAO, G.S.V. Radha Krishna; RADHAMANI G.. **WiMAX:** A Wireless Technology Revolution. Florida: Auerbach Publications, 2008.

REDES Mesh na cidade de Plano, Texas.[2006?]. Produção Motorola. Disponível em: <http://www.youtube.com/watch?v=g77A0rOUr-E&feature=related>. Acesso em: abr. 2011.

REYNOLDS, Janice. **Going Wi-Fi:** A Practical Guide to Planning and Building an 802.11 Network. San Francisco, USA: CMP Books, 2003.

RICHARDSON, Michael et al. **OpenSwan.** [2003?]. Disponível em: <http://openswan.org>. Acesso em: out. 2011.

ROSS, John. **The Book of Wireless:** A Painless Guide to Wi-Fi and Broadband Wireless. 2nd ed. San Francisco: No Starch Press, 2008.

RUFINO, Nelson Murilo de O.. **Segurança em redes sem fio:** aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooh. 2. ed. São Paulo: Novatec, 2007.

SANTOS, Edimar Babilon Dos et al. **Redes sem fio em malha.**[2006?]. Universidade Federal do Rio de Janeiro. Disponível em: <http://www.gta.ufrj.br/grad/10_1/malha/index.html>. Acesso em: abr. 2011.

SCHILLER, Felipe Ortigão Sampaio Buarque. **Estudo, Implementação e Análise de Métricas Baseadas na Qualidade do Enlace para o Protocolo OLSR**.2007. Universidade Federal do Rio de Janeiro. Disponível em: <http://www.gta.ufrj.br/ftp/gta/TechReports/Felipe07/Felipe07.pdf> Acesso em: abr. 2011.

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, William. **Cryptography and network security: principles and practice.** 2.ed. New Jersey: Prentice Hall, 1998.

STARLIN, Gorki; NOVO, Rafael. **Segurança contra hacker.** Rio de Janeiro: Book Express, 2000.

SWAMINATHA, Tara M.; ELDEN, Charles R..**Wireless Security and Privacy:** Best Practices and Design Techniques. Boston: Addison-Wesley Professional, 2003.

TANENBAUM, Andrew S.. **Redes de Computadores.** 4. ed. Rio de Janeiro: Campus, 1997.

_____. **Redes de Computadores.** 5. ed. Rio de Janeiro: Campus, 2003.

THOMAS, Tom. **Segurança de redes:** primeiros passos. Rio de Janeiro: Ciência Moderna, 2007.

TIMMERMANS, Ivo; SLIEPEN, Guus. **Tinc.** [2000?]. Disponível em: <http://tinc-vpn.org>. Acesso em: out. 2011.

UCSB, University of Carolina, Santa Barbara. **MeshNet.**[2005?]. Disponível em: <http://moment.cs.ucsb.edu/meshnet/>. Acesso em: abr. 2011

VINES, Russell Dean. Wireless Security Essentials: Defending Mobile Systems from Data Piracy. Indianapolis: Wiley Publishing, 2002.

ZACKER, Craig; DOYLE, Paul. **Redes de computadores:** configuração, manutenção e expansão. São Paulo: Makron Books, 2000.

APÊNDICE A – VPN EM UMA REDE MESH COM O PROTOCOLO OLSR

VPN em uma Rede Sem Fio Mesh Utilizando o Protocolo de Roteamento OLSR

Gilson Roberto Paseto[1], Paulo João Martins[2]

[1]Acadêmico do Curso Ciência da Computação - Universidade do Extremo Sul Catarinense (UNESC) – Criciúma – Brasil.

[2]Professor MSc. do Curso Ciência da Computação - Universidade do Extremo Sul Catarinense (UNESC) – Criciúma – Brasil.

gilrpx@gmail.com, pjm@unesc.net

ABSTRACT. *The Wireless Networks are constantly evolving, but users should always be in the range of the device that transmits the signal. To increase this range appeared in the Mesh Networks because of the Firmware and compatible protocols can increase their reach. This work aims to study wireless networks, Mesh Networks, OLSR routing protocol and Virtual Private Network. Where it was possible to verify and implant this technology on two routers through the use of Freifunk, which is available in the OLSR protocol for the implantation of Mesh, and then creating the VPN between them. After installation and configuration it was possible to perform tests, where there was a fully functional wireless network and virtual private network. So, this had a great range of availability of the wireless signal because of the VPN and you can have some degree of security, where the LAN connection was possible to have the data fully encrypted, but there is no security method for the customers using the wireless connection, there is a capture of information that travel through it.*

RESUMO. *As redes sem fio estão em constante evolução, porém os usuários devem sempre estar ao raio de alcance do dispositivo que transmite o sinal. Para aumentar esse raio surgiram as redes Mesh, onde por meio de Firmwares e protocolos compatíveis é possível aumentar seu alcance. Este trabalho tem por objetivos o estudo das redes sem fio, redes Mesh, protocolo de roteamento OLSR e da Virtual Private Network. Onde foi possível verificar e implantar esta tecnologia em dois roteadores por meio da utilização do Freifunk que tem disponível o protocolo OLSR para a implantação das redes Mesh e posteriormente a criação da VPN entre eles. Após instalação e configuração foi possível efetuar testes, onde verificou-se o completo funcionamento da rede sem fio e também da rede virtual privada. Sendo assim teve-se um maior raio de disponibilidade do sinal sem fio e por meio da VPN pode-se ter certo grau de segurança, onde na conexão via LAN foi possível ter os dados totalmente criptografados, porém por não haver nenhum método de segurança para com os clientes que utilizam a conexão sem fio, houve a captura das informações que trafegavam pela mesma.*

1. Introdução

No mundo globalizado é imprescindível a convivência e a utilização dos meios tecnológicos para nosso aperfeiçoamento, podendo citar mais precisamente a Internet onde é possível trocar informações com o mundo todo. Para poder usufruir deste grande poder de obtenção de conhecimento é necessário à pessoa estar ligada a uma rede, seja ela com fio ou sem fio, e estar conectada a Internet.

Os sinais de redes sem fio geralmente são transmitidos por rádio frequência, sendo assim não necessitam de uma conexão física com computadores, porém necessita-se apenas de uma antena para a comunicação. Por meio desta rádio frequência forma-se uma rede sem fio onde será possível transmitir dados por meio de ondas de rádio eletromagnéticas (COMER, 2001).

As Redes Mesh também conhecida como redes em malha, vieram com o intuito de prover desta mobilidade disponível dos aparelhos sem fio, mas não de ficar limitada ao raio de conexão somente de um aparelho. Com isto é possível fazer com que vários equipamentos se comuniquem entre si, ou seja, apesar de se ter vários aparelhos provendo sinal sem fio, o usuário terá a visão de apenas uma única rede.

O protocolo Optimized Link State Routing (OLSR), é um dos principais protocolos de roteamento para redes Mesh. Está na categoria dos protocolos pró-ativos, cujo objetivo é periodicamente fazer a troca de informações com os nós da rede a fim de atualizar sua tabela de roteamento.

A Virtual Private Network (VPN) é um mecanismo utilizado para se ter uma maior segurança na transmissão de dados pela rede. Onde a VPN utiliza protocolos de criptografia por tunelamento, ou seja, os dados vão trafegar por um túnel onde estas informações estarão seguras durante sua transmissão.

2. Redes de Computadores

O surgimento das redes de computadores deu-se por volta de 1980, devido a curiosidade de certas instituições de ensino. A partir de então houve um grande crescimento na tecnologia para a ligação de computadores entre si, podendo ser caracterizada esta ligação como um grupo de computadores autônomos interconectados com o intuito de haver troca de informações (TANENBAUM, 1997).

2.1 Redes Sem Fio

As redes sem fio não necessitam de uma conexão física com computadores, pois os dados são transmitidos por ondas eletromagnéticas, ou seja, por rádio frequência onde os receptores precisam trabalhar na mesma frequência do remetente (COMER, 2001).

De acordo com Zacker e Doyle (2000, p. 875, tradução nossa) "...uma rede sem fio pode ser constituída de quase qualquer tipo de máquina de computação e pode estender-se por qualquer área."

Conforme Reynolds (2003, tradução nossa), em 1990 por meio do *Institute of Electrical and Electronic Engineers* (IEEE) foi criado um grupo de trabalho para estudos das redes sem fio, a partir de então começaram a surgir os padrões.

2.2 Redes Mesh

Este modelo de tecnologia teve seu desenvolvimento por volta de 1970, projeto liderado pela agência de defesa dos Estados Unidos, *Defense Advanced Research Projects Agency*

(DARPA). O objetivo principal era ter comunicação e transferência de dados e voz pelo campo de batalha sem ter a necessidade de centralizar o sinal.

Para Akyildiz e Wang (2009, tradução nossa), as redes sem fio Mesh serão uma tecnologia chave para a próxima década, pois poderão realizar um grande sonho de poder ter conectividade em qualquer lugar e a qualquer momento. Tendo um papel fundamental para a próxima geração da Internet, devido ao seu poder de auto-organização, auto-configuração, baixo custo e a redução da complexidade em implantação e manutenção.

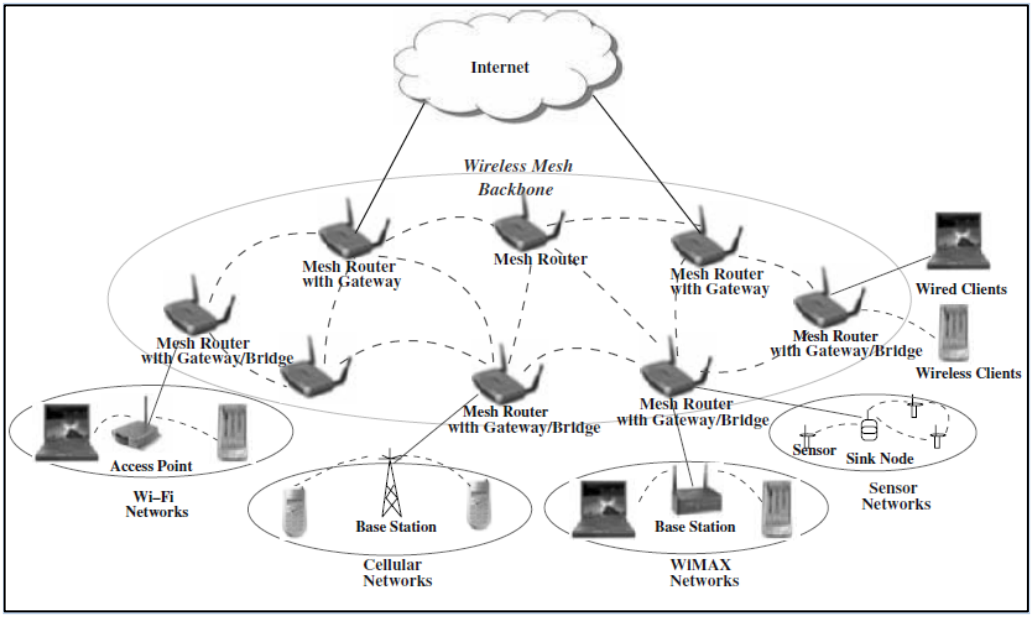


Figura 43. Arquitetura infraestrutura/backbone
Fonte: AKYILDIZ F., I; WANG X. (2009, p. 4)

Na Figura 1 pode-se visualizar a arquitetura modelo infraestrutura/*backbone* onde tem-se os roteadores que formam a infraestruruta para que os clientes possam conectar-se, sendo assim é possível disponibilizar conexão com a Internet (AKYILDIZ; WANG, 2009, tradução nossa).

3. Protocolo Optimized Link State Routing

A partir do projeto Hipercom desenvolvido na França pela *Institut National de Recherche en Informatique Et en Automatique* (INRIA), surgiu o protocolo de roteamento em redes Mesh OLSR. Teve sua padronização iniciada em Outubro de 2003 na *Internet Engineering Task Force* (IETF) sob a *Request For Comments* (RFC) 3626, porém ainda está em fase experimental, ou seja, ainda poderá ter alterações até sua finalização.

O protocolo OLSR é um protocolo proativo utilizado em *Mobile Ad-Hoc Networks* (MANETs), ele se adapta bem em grandes redes devido a sua forma de roteamento, pois cada nó é responsável por fazer sua própria transmissão de seus pacotes. Este protocolo também pode ser recomendado em lugares onde a rede é variável, ou seja, onde haja constantes alterações em sua topologia (CLAUSEN; JACQUET, 2003, tradução nossa).

4. Virtual Private Network

As VPNs surgiram com o intuito de prover uma maior segurança em transações por meio da conexão entre redes e computadores via Internet.

De acordo com Tanenbaum (2003, p. 828), as VPNs foram criadas com o intuito de serem "... redes sobrepostas às redes públicas, mas com a maioria das propriedades de redes privadas. Elas são chamadas "virtuais" porque são meramente uma ilusão, da mesma forma que os circuitos virtuais não são circuitos reais e que a memória virtual não é memória real."

Conforme Murhammer (2000, p. 329), "Uma rede virtual privada (VPN) é uma extensão da intranet privada de uma empresa, através de uma rede pública como a Internet, criando uma conexão privada segura, essencialmente por meio de um *túnel* privado."

5. Implantação de uma Rede Sem Fio Mesh

Este projeto tem como objetivo pesquisar sobre o funcionamento de uma rede sem fio Mesh e também sobre o protocolo de roteamento OLSR que é responsável por organizar os nós na rede. Após este estudo foi realizada a montagem da rede entre os roteadores a fim de verificar o funcionamento. Posteriormente foi estudado o funcionamento de uma rede virtual privada junto com a rede Mesh para assim ter algum tipo de segurança baseada nos recursos utilizados.

5.1 Firmware

Firmwares são pequenos softwares capazes de serem instalados em qualquer dispositivo de hardware onde tenha memória disponível para instalação, cujo principal objetivo é promover o funcionamento do mesmo.

Desenvolvido na Alemanha como o intuito de promover o acesso a Internet gratuita para todos, na tradução deste nome temos "rádio livre". Uma das suas intenções é que um usuário que tenha um roteador disponível e compatível com o *Firmware* possa se conectar a rede e assim promover um maior alcance de rede e também o compartilhamento de arquivos (FREIFUNK, 2004).

5.2 Software VPN

OpenVPN é uma implementação VPN baseada no *Secure Socket Layer* (SSL), possui código fonte aberto e está disponível para diversos sistemas operacionais. Esta implementação foi considerada em 2007 a melhor implementação SSL pela revista InfoWorld, dentro da categoria *Open Source* e em 2010 pelo site LifeHacker a melhor ferramenta VPN. Atualmente sua comunidade possui cerca de 5 milhões de usuários (DINHA; YONAN, 2002, tradução nossa).

5.3 Implantação da Tecnologia

Foram utilizados roteadores da marca Linksys e modelo WRT54GL V1.1, todos vem por padrão com um *Firmware* proprietário instalado, porém não é possível integrá-lo com a tecnologia de redes Mesh. Mas por serem compatíveis com o *Firmware* a ser instalado optou-se pela escolha do mesmo, pelo motivo de ser disponibilizado pelo orientador e assim não gerou custo.

Deste modo é possível iniciar a implantação da tecnologia, onde deve-se seguir os seguintes passos:

f) download do *Firmware* de acordo com o modelo do roteador;
g) instalação do mesmo no roteador;
h) atualização do mesmo;

i) configuração diversas no roteador para o funcionamento do OLSR;
j) configuração da VPN.

Na Figura 2 pode-se visualizar o local onde deve-se atualizar o *Firmware*.

Figura 44. *Firmware* Linksys

Quando o *Firmware* estiver instalado no aparelho irá abrir uma nova interface no lugar da anterior como é possível visualizar na Figura 3.

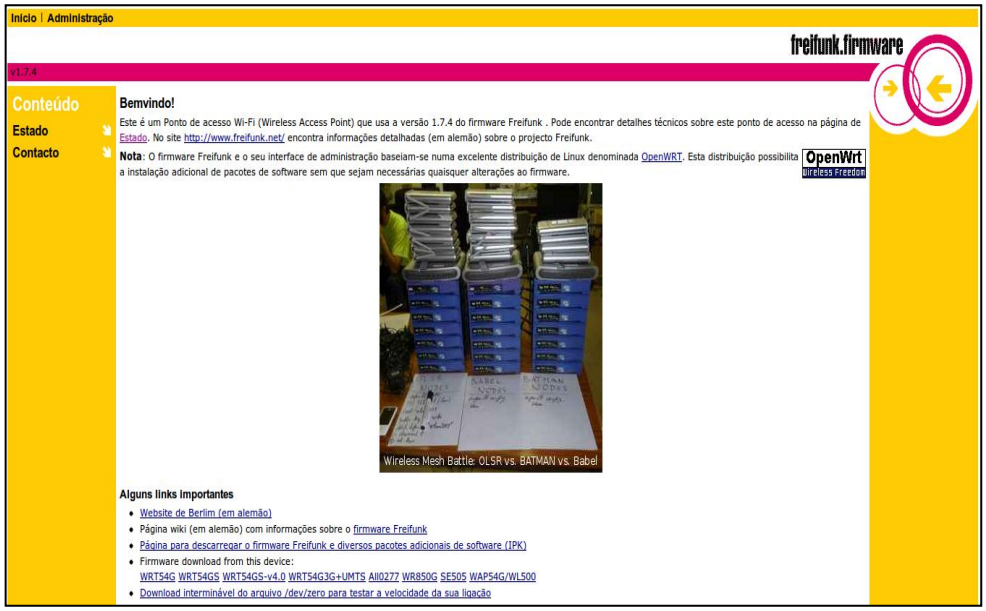


Figura 45. *Firmware* Freifunk

Os itens necessários para a configuração estão na aba administrativa que são: *Wide Area Network* (WAN), *Local Area Network* (LAN), Wireless e OLSR.

A opção WAN é responsável pela conexão com a Internet, deste modo deixa-se com a opção de "Usar servidor DHCP", para atribuição automática do endereçamento do *Internet Protocol* (IP). Outra alteração necessária é habilitar os campos: Permitir SSH, acesso via HTTP, acesso via HTTPS e *Ping*, desta forma é possível conectar no dispositivo via *Secure Shell* (SSH), *HyperText Transfer Protocol* (HTTP), HTTPS e testar a conectividade via *Ping*.

A opção LAN fica responsável pelo endereçamento da conexão via cabo de rede. Por padrão cada dispositivo possui o mesmo endereço IP, mas para evitar confusões é recomendável que cada dispositivo tenha endereços diferentes.

Na Wireless tem-se configurações importantes para que a rede Mesh funcione perfeitamente. Para um melhor gerenciamento divida a rede em pequenas subredes onde cada roteador ficará responsável por uma pequena gama de usuários e coloque o endereço identificador da mesma como IP fixo, porém deixe a máscara com a classe cheia para que os clientes possam se comunicar.

Para isso é necessário definir o endereço IP como fixo para cada dispositivo e ter uma máscara cheia de acordo com sua classe. Outra informação importante a ser especificada é em relação ao modo de operação, onde deve-se alterar para modo *Ad-Hoc*, além de definir um nome para a rede e um canal de atuação da mesma.

Em OLSR apenas um item é importante para que clientes possam conectar-se a rede, este campo é o DHCP-OLSR. Aqui tem-se a seguinte configuração: *endereço_ip_roteador/máscara,máscara* neste caso deve-se colocar o IP da interface Wireless junto com sua respectiva máscara e por fim outra máscara ficando da seguinte forma 192.160.1.64/26,255.255.255.0 desta forma os clientes estarão na dentro da faixa de IP permitida por cada roteador e também poderão se comunicar entre si. Sendo assim os clientes que se conectarem a rede receberam um endereço IP automático de acordo com o dispositivo que estarão conectados.

O próximo passo é a instalação e configuração do OpenVPN. Deste modo é necessário instalar os pacotes:

e) libopenssl: biblioteca de criptografia SSL;
f) kmod-tun: modulo de tunelamento;
g) openvpn: software OpenVPN;
h) freifunk-openvpn-en: interface de configuração do OpenVPN.

Na página de configuração, as principais alterações a serem feitas são:

a) modo de conexão: onde deve-se escolher Point-to-Point (PTP);
b) modo de operação: onde um dos dispositivos deve ser o servidor e o outro o cliente;
c) túnel com *Network Address Translation* (NAT): deve ser habilitado no cliente para que haja acesso ao servidor;
d) estação remota: este campo deve ser preenchido somente no cliente, onde deve-se colocar o endereço do servidor;
e) compressão LZO: deve-se habilita-la em ambos para que haja a compactação dos dados;
f) chave compartilhada: deve-se gerar a chave e copiá-la para o outro dispositivo.

Depois de tudo configurado deve-se aplicar as alterações e em seguida é necessário reiniciá-lo.

Pra que seja possível acessar LAN do outro dispositivo deve-se adicionar a rota para a mesma, sendo assim deve-se entrar no dispositivo configurado como cliente via um programa de SSH editar o arquivo do OpenVPN localizado em */etc/openvpn/freifunk.conf* adicionar no final a linha *route 192.168.1.0 255.255.255.0* e depois reiniciar o serviço pelo comando */etc/init.d/openvpn restart*.

5.4 Resultados Obtidos

Para os resultados obtidos durante os testes criou-se dois cenários distintos, o primeiro para os testes somente com o protocolo OLSR, trata-se de uma arquitetura de infraestrutura/*backbone*, onde os clientes possam se conectar a rede.

No segundo cenário utilizou-se a mesma topologia do anterior, porém com a criação da VPN entre os roteadores onde utilizou-se a forma de rede para rede.

5.4.1 Primeiro Cenário

Os testes iniciais deram-se somente com o protocolo de roteamento funcionando. É possível visualizar na Figura 4 que trata do primeiro cenário a ser testado, para isto foram utilizados dois roteadores, sendo que um deles está conectado a Internet e dois computadores com interface de rede sem fio. A seguir serão demonstrados três testes aplicados ao primeiro cenário.

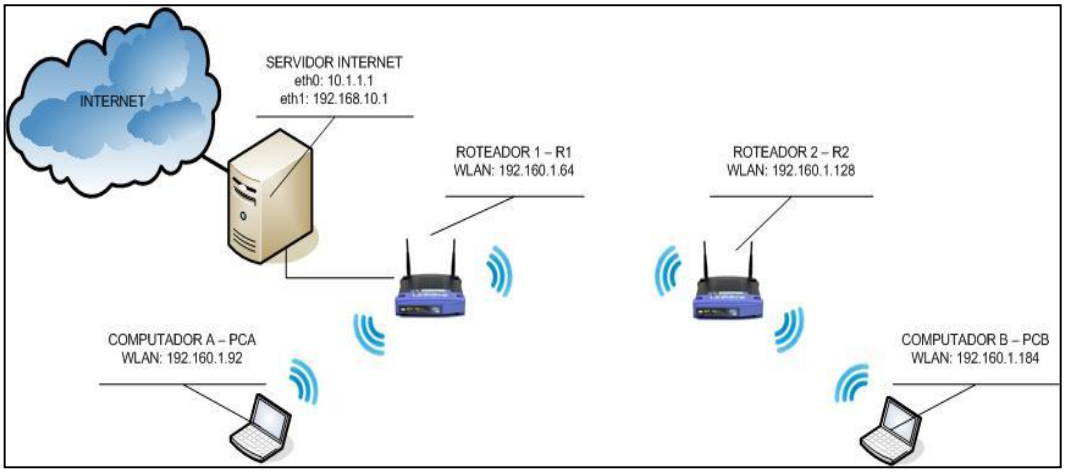


Figura 46. Primeiro Cenário

O primeiro teste a ser aplicado foi o *Ping* (Figura 5). Com este comando é possível verificar se o IP de destino pode ser encontrado, deste modo o computador PCA conectado no roteador R1 obteve sucesso na comunicação com o PCB que estava conectado no roteador R2

```
PING 192.160.1.184 (192.160.1.184) 56(84) bytes of data.
64 bytes from 192.160.1.184: icmp_seq=1 ttl=128 time=4.14 ms
64 bytes from 192.160.1.184: icmp_seq=2 ttl=128 time=2.82 ms
64 bytes from 192.160.1.184: icmp_seq=3 ttl=128 time=1.29 ms
64 bytes from 192.160.1.184: icmp_seq=4 ttl=128 time=9.58 ms
64 bytes from 192.160.1.184: icmp_seq=5 ttl=128 time=1.59 ms
64 bytes from 192.160.1.184: icmp_seq=6 ttl=128 time=1.57 ms
^C
--- 192.160.1.184 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 1.295/3.501/9.580/2.888 ms
```

Figura 47. *Ping* entre Máquinas

O segundo teste foi a execução do comando *Traceroute* (Figura 6). Sendo responsável por verificar se um endereço IP de destino pode ser encontrado, além de exibir todos os saltos até chegar a seu destino. Para este caso o comando a ser executado teve seu inicio no computador PCB conectado ao roteador R2 com o destino de um site na Internet.

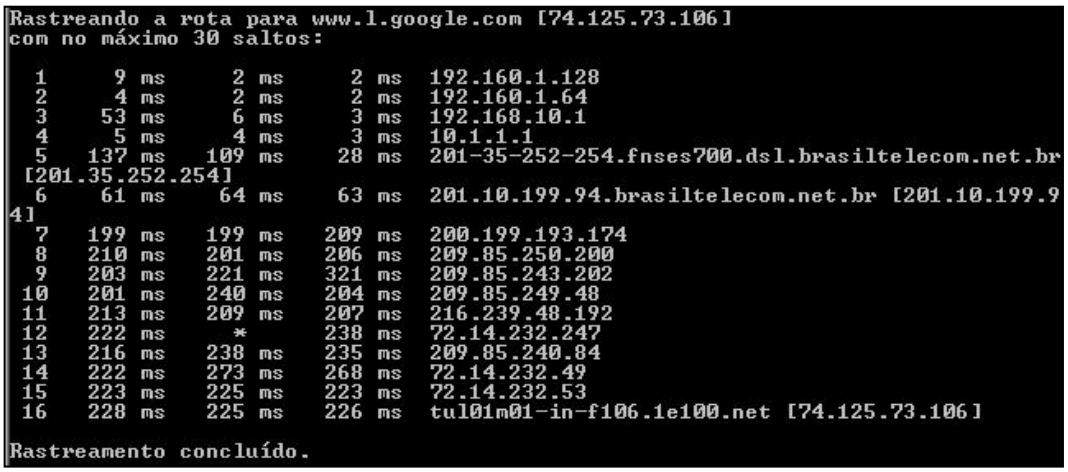


Figura 48. *Traceroute* para a Internet

Por último houve a troca e acesso de arquivos. Na Figura 7 é possível verificar o computador PCA conectado ao PCB e possibilitando acesso a arquivos e a edição de um documento de texto.

Figura 49. Compartilhamento de Arquivos

Deste modo percebeu-se o perfeito funcionamento do protocolo OLSR em todos os testes descritos acima.

5.4.2 Segundo Cenário

No segundo cenário como pode-se visualizar na Figura 8, está implantada a VPN entre os roteadores por meio do tunelamento ponto a ponto. Neste cenário observa-se que o primeiro roteador possui um servidor conectado a sua porta LAN, onde após a adição da rota para a LAN do servidor o cliente poderá usufruir dos serviços prestados pelo mesmo, como por exemplo o compartilhamento de arquivos.

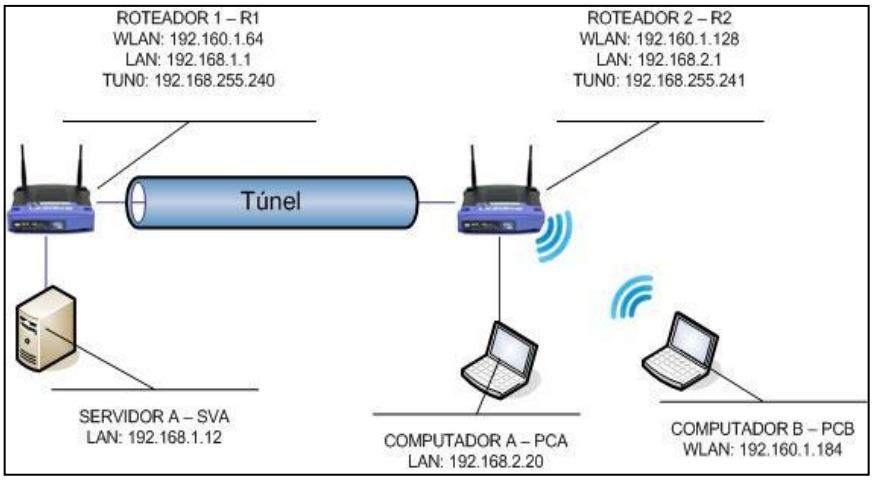


Figura 50. Segundo Cenário

Os primeiros testes a serem apresentados referem-se na conexão entre PCB para com SVA, neste caso PCB estará utilizando uma conexão sem fio.

Na Figura 9 pode-se visualizar que por meio do comando *traceroute* verificou-se que o mesmo passou pelo endereço criado a partir da VPN.

```
Rastreando a rota para 192.168.1.12 com no máximo 30 saltos

  1     1 ms     1 ms     1 ms  192.160.1.128
  2     6 ms     6 ms     6 ms  192.168.255.240
  3     6 ms     6 ms     8 ms  192.168.1.12

Rastreamento concluído.
```

Figura 51. *Traceroute* para o Servidor

Para os testes de captura de pacotes, utilizou-se outro computador com interface de rede sem fio onde o mesmo esteve localizado entre os roteadores.

Mesmo as informações estarem sendo acessadas pela VPN foi possível verificar que por meio da utilização do programa *open source* Wireshark, responsável pela captura de pacotes, que o mesmo não está totalmente criptografado (Figura 10).

```
1759 75.318375  192.160.1.64      192.160.1.255     OLSR v1     140 OLSR (IPv4) Packet,  Length: 56 Bytes
1760 75.365167  Cisco-Li_b6:ee:e0  Broadcast         802.11      103 Beacon frame, SN=3379, FN=0, Flags=........, BI
1761 75.368309  D-Link_b6:c7:c1    Broadcast         802.11      165 Beacon frame, SN=2311, FN=0, Flags=........, BI
1762 75.450169  192.160.1.184      192.168.1.12      HTTP        571 GET / HTTP/1.1
1763 75.450196                     Ovislink_0d:17:e2 (802.11      34 Acknowledgement, Flags=........
1764 75.452304  192.160.1.128      192.160.1.64      UDP         600 Source port: openvpn  Destination port: openvpn
1765 75.456563                     Cisco-Li_b6:ee:e0 (802.11      34 Acknowledgement, Flags=........
1766 75.456569  192.160.1.64       192.160.1.128     UDP         384 Source port: openvpn  Destination port: openvpn
1767 75.456593                     Cisco-Li_b6:ef:5b (802.11      34 Acknowledgement, Flags=

   Request URI: /
   Request Version: HTTP/1.1
 Host: 192.168.1.12\r\n
 User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n

0  2f 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f 73 74   / HTTP/1 .1..Host
0  3a 20 31 39 32 2e 31 36  38 2e 31 2e 31 32 0d 0a   : 192.16 8.1.12..
0  55 73 65 72 2d 41 67 65  6e 74 3a 20 4d 6f 7a 69   User-Age nt: Mozi
0  6c 6c 61 2f 35 2e 30 20  28 57 69 6e 64 6f 77 73   lla/5.0  (Windows
0  20 4e 54 20 35 2e 31 3b  20 72 76 3a 35 2e 30 29    NT 5.1;  rv:5.0)
0  20 47 65 63 6b 6f 2f 32  30 31 30 30 31 30 31 20    Gecko/2 0100101
0  46 69 72 65 66 6f 78 2f  35 2e 30 0d 0a 41 63 63   Firefox/ 5.0..Acc
0  65 70 74 3a 20 74 65 78  74 2f 68 74 6d 6c 2c 61   ept: tex t/html,a
```

Figura 52. Captura de Pacotes pelo Wireshark

Os demais testes a seguir são em relação ao cliente PCA conectado a sua interface LAN, ou seja, por meio de cabos para com o servidor SVA.

Na Figura 11 pode-se visualizar o resultado do comando *Traceroute*, onde é possível perceber sua trajetória até seu destino.

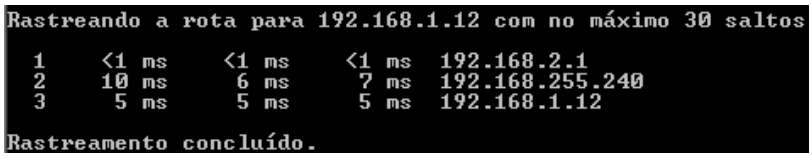


Figura 53. *Traceroute* para o Servidor

Por último foi realizado a utilização de um serviço HTTP do servidor.

Na Figura 12 é possível observar os pacotes capturados por meio do *Wireshark*, onde exibem que os mesmos passaram pelo túnel, mas que as informações capturada não são legíveis.

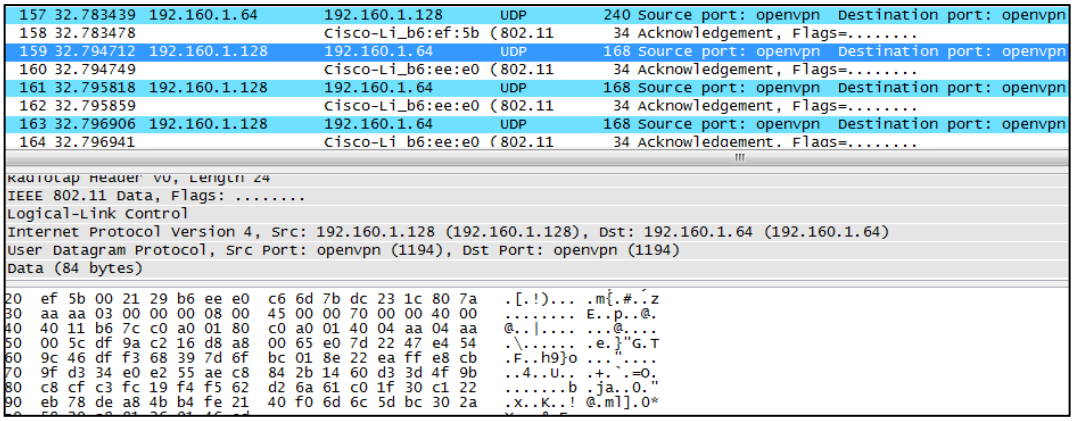


Figura 54. Captura de Pacotes pelo Wireshark

Todos os testes aplicados a VPN foram bem sucedidos, porém o único local onde houve a captura de informações foi por meio da conexão sem fio, pelo motivo de não possuir nenhum tipo de mecanismo segurança como autenticação dos clientes para com os roteadores.

6. Conclusão

Este trabalho teve como objetivos a realização de estudos das redes sem fio Mesh para assim descrever suas funcionalidades, o protocolo OLSR e o funcionamento das redes virtuais privadas.

Para as redes sem fio buscou-se seu histórico, deste modo também possibilitou descrever sobre suas fragilidades na questão de segurança e podendo verificar melhor alguns ataques que as mesmas estão sujeitas.

Foi possível obter um melhor conhecimento no funcionamento de uma rede sem fio Mesh, assim como características, arquiteturas e protocolos atualmente disponíveis.

A cerca do protocolo de roteamento OLSR, pode-se verificar seu funcionamento por meio de pesquisas e consulta a RFC 3626. Foi possível então ter uma visão aprofundada sobre a técnica que evita a sobrecarga da rede, formatação de pacotes, mensagens transmitidas, tabela de roteamento e por fim uma pequena observação sobre segurança e sobre a sexta versão do protocolo IP.

O conhecimento obtido por pesquisas da VPN trouxe grande contribuição para ajudar na segurança, onde pode-se conhecer melhor sobre alguns dos protocolos existentes atualmente, além de seu funcionamento e a forma em que se estabelece o tunelamento.

Desta forma, os objetivos que eram montar uma rede sem fio Mesh utilizando o protocolo de roteamento OLSR pode ser concluído com êxito. Após a rede estar em

funcionamento foi possível implementar uma VPN por meio da utilização do OpenVPN entre os roteadores a fim de promover certo grau de segurança no acesso de clientes a um determinado servidor, porém nem tudo pode ser criptografado.

Em relação a VPN observou-se que é possível ter um determinado computador que possa prestar algum tipo de serviço como armazenamento de arquivos e acesso a um servidor HTTP. Também foi possível analisar que a implementação VPN tornou-se segura somente na conexão via cabos e por não haver nenhum tipo de segurança dos clientes para com os roteadores ainda tem-se o vazamento das informações.

A principal dificuldade encontrada foi em relação a configuração do *Firmware* Freifunk. Pois devido sua origem ser na Alemanha boa parte do material encontrado estava no idioma alemão, mas com a ajuda de programas de tradução foi possível compreender e poder efetuar a configuração dos roteadores.

Foi possível analisar que na conexão do cliente utilizando a interface de rede sem fio não deu-se de forma totalmente segura, neste caso seria necessário um novo estudo para promover esta segurança.

Referências

AKYILDIZ, F. Ian; WANG, Xudong. **Wireless Mesh Networks.** United Kingdom: John Wiley & Sons Ltd, 2009.

CLAUSEN, Thomas Heide; JACQUET , Philippe. **Optimized Link State Routing Protocol (OLSR).** 2003. Disponível em: <http://www.ietf.org/rfc/rfc3626.txt>. Acesso em: abr. 2011.

COMER, Douglas E.. **Redes de Computadores e Internet.**2 ed. Porto Alegre: Bookman, 2001.

DINHA, Francis; YONAN, James; NIMON, Bob. **OpenVPN.** 2002. Disponível em: <http://openvpn.net>. Acesso em: out. 2011.

FREIFUNK. **Freifunk.** 2004. Disponível em: <http://start.freifunk.net>. Acesso em: 10 ago. 2011.

MURHAMMER, Martin W. et al. **TCP/IP:** Tutorial e Técnico. São Paulo: Makron Books, 2000.

REYNOLDS, Janice. **Going Wi-Fi:** A Practical Guide to Planning and Building an 802.11 Network. San Francisco, USA: CMP Books, 2003.

TANENBAUM, Andrew S.. **Redes de Computadores.** 4. ed. Rio de Janeiro: Campus, 1997.

_____. **Redes de Computadores.** 5. ed. Rio de Janeiro: Campus, 2003.

ZACKER, Craig; DOYLE, Paul. **Redes de computadores:** configuração, manutenção e expansão. São Paulo: Makron Books, 2000.

APÊNDICE B – MANUAL DE INSTALAÇÃO DO FIRMWARE

Deve-se acessar o endereço *http://download.berlin.freifunk.net/ipkg/* na Internet e efetuar o download do arquivo *openwrt-g-freifunk-1.7.4-pt.bin* que está localizado no diretório *_g+gl*.

Para a instalação é necessário acessar a página de configuração do aparelho utilizando um navegador para Internet, bastando digitar no campo de navegação o endereço 192.168.1.1 e informar o nome de usuário e senha de acordo com o manual do fabricante.

Posteriormente deve-se acessar *Administration > Firmware Upgrade* selecionar o novo *Firmware* e clicar no botão *Upgrade*.

Outro modo de efetuar a instalação é via linha de comando com a utilização de um programa *File Transfer Protocol* (FTP) onde será executado o seguinte comando: *ftp –i 192.168.1.1 put openwrt-g-freifunk-1.7.4-pt.bin* este comando será responsável pela instalação.

Após a instalação deve-se atualizá-lo para isto é necessário ter disponível conexão com a Internet, caso disponha conecte o cabo de rede na entrada “Internet” localizado na parte de trás do aparelho. Em seguida entre na parte de administração, informe o usuário e senha, neste caso deverá ser preenchido com “**root**” e “**admin**” respectivamente, entre na opção “Software 1” localizado no menu a esquerda, neste local é possível instalar pacotes, alterar a imagem da página inicial. Selecionando a opção “freifunk-recommended-pt” e “Carregar arquivo-Software” o *Firmware* será atualizado, isto pode demorar alguns minutos.

APÊNDICE C – CONFIGURAÇÃO DOS ROTEADORES

Para que haja o funcionamento dos roteadores devem-se alterar as configurações: WAN, LAN, Wireless, OLSR e por último o OpenVPN.

ROTEADOR R1:

WAN: deve-se deixar para usar servidor DHCP e deve-se ativar as opções de SSH, HTTP, HTTPS e *Ping*.

LAN: deve-se atribuir o endereço 192.168.1.1 e máscara 255.255.255.0

Wireless: utiliza-se configuração manual e atribui-se o endereço 192.160.1.64 e máscara 255.255.255.0;

Deve-se alterar o modo de operação para AD-HOC, definir ESSID neste caso utilizou-se “Mesh” e por último o canal de atuação, para este utilizou-se o canal 6;

OLSR: o único campo a ser alterado é DHCP-OLSR onde inseriu-se o valor 192.160.1.64/26, 255.255.255.0

Para a configuração do OpenVPN é necessário colocar o “Operation Role” para “Server”, “Device” para “Tunnel (tun)”, “Protocol” selecionar “UDP”, “LZO Compression” para “Enable” e por último gerar a chave compartilhada clicando no botão “Generate”, após isto é necessário salvar e reiniciar.

ROTEADOR R2:

WAN: deve-se deixar para usar servidor DHCP e deve-se ativar as opções de SSH, HTTP, HTTPS e *Ping*.

LAN: deve-se atribuir o endereço 192.168.2.1 e máscara 255.255.255.0

Wireless: utiliza-se configuração manual e atribui-se o endereço 192.160.1.128 e máscara 255.255.255.0;

Deve-se alterar o modo de operação para AD-HOC, definir ESSID neste caso utilizou-se “Mesh” e por último o canal de atuação, para este utilizou-se o canal 6;

OLSR: o único campo a ser alterado é DHCP-OLSR onde inseriu-se o valor 192.160.1.128/26, 255.255.255.0

Para a configuração do OpenVPN é necessário colocar o “Operation Role” para “Client”, “Device” para “Tunnel (tun)”, habilitar “Tunnel with NAT”, colocar o endereço 192.160.1.64 em “Remote Station”, “Protocol” selecionar “UDP”, “LZO Compression” para “Enable” e por último copiar a chave compartilhada do roteador que é o servidor, após isto é necessário salvar e reiniciar.

Na tabela abaixo pode-se visualizar um resumo da configuração

	ROTEADOR R1	**ROTEADOR R1**
WAN	IP DHCP, HABILITAR SSH, HTTP, HTTPS e PING	IP DHCP, HABILITAR SSH, HTTP, HTTPS e PING
LAN	IP: 192.168.1.1 Mascará: 255.255.255.0	IP: 192.168.2.1 Mascará: 255.255.255.0
Wireless	IP: 192.160.1.64 Mascará: 255.255.255.0 Modo Ad-Hoc (Peer-To-Peer) ESSID: Mesh Canal: 6	IP: 192.160.1.128 Mascará: 255.255.255.0 Modo Ad-Hoc (Peer-To-Peer) ESSID: Mesh Canal: 6
OLSR	DHCP-OLSR: 192.160.1.64/26,255.255.255.0	DHCP-OLSR: 192.160.1.128/26,255.255.255.0
OpenVPN	Connection Mode: Point-to-Point Operation Role: Server Device: Tunnel (TUN) Protocol: UDP LZO Compression: Enable Shared Key: -----BEGIN OpenVPN Static key V1----- 0343eb2f13c181709da8022cc4dd6a25 ... f58cf513b60b4999920d31a3abf46805 375983e6d64c0baa18199c8f0877c79b 9b5fa3d662cf37be6c2958bd08624920 -----END OpenVPN Static key V1-----	Connection Mode: Point-to-Point Operation Role: Server Device: Tunnel (TUN) Tunnel with NAT: Enable Remote Station: 192.160.1.64 Protocol: UDP LZO Compression: Enable Shared Key: -----BEGIN OpenVPN Static key V1----- 0343eb2f13c181709da8022cc4dd6a25 … 375983e6d64c0baa18199c8f0877c79b 9b5fa3d662cf37be6c2958bd08624920 -----END OpenVPN Static key V1-----