

**UNIVERSIDADE SAGRADO CORAÇÃO**

**ALEXANDRE MEIRA LIMA**

**UM ESTUDO DE TRANSMISSÃO DE VOZ EM REDES  
SEM FIO IP COM WDS ASSOCIADAS COM  
MECANISMOS DE SEGURANÇA**

BAURU  
2014

**ALEXANDRE MEIRA LIMA**

**UM ESTUDO DE TRANSMISSÃO DE VOZ EM REDES  
SEM FIO IP COM WDS ASSOCIADAS COM  
MECANISMOS DE SEGURANÇA**

Trabalho de conclusão de curso apresentado ao Centro de Ciências Exatas como parte dos requisitos para obtenção do título de bacharel em Ciência da Computação, sob orientação do Prof. Esp. Alex Setolin Beirigo.

**BAURU  
2014**

Lima, Alexandre Meira.

L7324e

Um estudo de transmissão de voz em redes sem fio IP com WDS associadas com mecanismos de segurança / Alexandre Meira Lima. -- 2014.

59f. : il.

Orientador: Prof. Esp. Alex Setolin Beirigo.

Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Universidade do Sagrado Coração – Bauru – SP.

1. Asterisk. 2. Voip. 3. WDS. 4. Criptografia. 5. VPN. I. Beirigo, Alex Setolin. II. Título.

**ALEXANDRE MEIRA LIMA**

**UM ESTUDO DE TRANSMISSÃO DE VOZ EM REDES SEM FIO IP  
COM WDS ASSOCIADAS COM MECANISMOS DE SEGURANÇA**

Trabalho de conclusão de curso apresentado ao Centro de Ciências Exatas como parte dos requisitos para obtenção do título de bacharel em Ciência da Computação, sob orientação do Prof. Esp. Alex Setolin Beirigo.

Banca Examinadora:

---

Prof. Esp. Alex Setolin Beirigo  
Universidade do Sagrado Coração

---

Prof. Esp. Henrique Pachioni Martins  
Universidade do Sagrado Coração

---

Prof. Me. Wallace de Paula  
Universidade do Sagrado Coração

Bauru, 02 de dezembro de 2014.

## RESUMO

A necessidade de comunicação entre todos os pontos de uma organização é de fundamental importância, mas muitas vezes ocorre de determinados setores estarem em um espaço geográfico muito distante, fazendo-se necessário a utilização da tecnologia para realizar a comunicação entre estes pontos; comunicação esta que deve ser provida de qualidade e segurança. Entretanto as empresas de telefonia cobram altos valores para prover este tipo de serviço, fazendo com que as empresas demandem grandes quantias de recursos para conseguirem se comunicar. Uma alternativa para reduzir os custos com telefonia, mas ainda mantendo qualidade na comunicação, é a implementação de um servidor Asterisk, em conjunto com VPNs configuradas de forma criptografada, garantindo segurança e qualidade dos dados trafegados. Atualmente o uso de equipamentos sem fio tem aumentado significativamente, mas o hardware destes dispositivos é um pouco mais limitado, necessitando a tomada de cuidados ao se utilizar técnicas de segurança muito complexas, pois quanto maior o nível de complexidade, maior será o impacto causado à rede, então usando a tecnologia WDS para ampliar a capacidade do sinal wireless, o objetivo deste trabalho será o monitoramento de chamadas, avaliando assim quais serão as técnicas mais viáveis para rede sem fio.

**Palavras-chave:** Asterisk. Voip. WDS. Criptografia. VPN.

## ABSTRACT

The need for communication between all points of an organization is crucial, but occurs in certain sectors are in a very distant geographical space, the use of technology is needed to realize the communication between these points, this communication should be provided with quality and safety, however the telephone companies charge high values to provide this type of service, causing companies demanding large amounts of resources to manage to communicate. An alternative to reduce telephony costs, while still maintaining quality in communication, is implementing an Asterisk server, in conjunction with VPNs configured with encryption types, ensuring safety and quality of data traffic. Currently the use of wireless devices has increased significantly, but the hardware of these devices is a bit more limited, requiring taking care when using very complex security techniques, because the higher the level of complexity, the greater the impact on network, then using the WDS technology to expand the capacity of the wireless signal, the goal will be monitoring calls, thus assessing what will be the most viable techniques for wireless network.

**Keywords:** Asterisk. Voip. WDS. Encryption. VPN.

## LISTA DE FIGURAS

Figura 1 - Protocolo TCP/IP .....	11
Figura 2 - Arquitetura Voip .....	12
Figura 3 - Conexão Voip .....	14
Figura 4 - Comparativo WEP/WPA .....	18
Figura 5 - Integridade WPA 2 .....	19
Figura 6 - Demonstrativo de Possíveis VPNs .....	20
Figura 7 - Arquitetura Asterisk .....	22
Figura 8 - Rede WDS .....	25
Figura 9 - Cenário para testes WDS .....	27
Figura 10 - Roteador Principal .....	28
Figura 11 - Roteador WDS .....	29
Figura 12 - Roteador WDS configuração segurança .....	30
Figura 13 - Status Openvpn .....	31
Figura 14 - Executar OpenVpn como Administrador .....	33
Figura 15 - Verificação Asterisk .....	35
Figura 16 - Login Asterisk .....	36
Figura 17 - Interface Asterisk .....	36
Figura 18 - Funcionamento Asterisk .....	37
Figura 19 - Cadastrar Novo Usuário Asterisk .....	38
Figura 20 - Cadastrando Novo Usuário Asterisk .....	39
Figura 21 - Status Asterisk .....	39
Figura 22 - X-Lite 4.0 Interface .....	40
Figura 23 - Configuração Nova Conta X-Lite .....	41
Figura 24 - Dados Conta X-Lite .....	41
Figura 25 - X-Lite Conectado .....	42
Figura 26 - Interface Zoiper .....	43
Figura 27 - Configuração Conta Zoiper .....	43
Figura 28 - Zoiper Conectado .....	44
Figura 29 - Interface Wireshark .....	45
Figura 30 - Resultados Wireshark .....	46
Figura 31 - Resultados Sem Criptografia .....	47
Figura 32 - Resultados Criptografia WEP .....	47
Figura 33 - Resultados Criptografia WAP .....	47
Figura 34 - Resultados Criptografia WPA-PSK .....	48
Figura 35 - Gráfico Pacotes .....	48
Figura 36 - Gráfico Média Pacotes p/ Segundo .....	49
Figura 37 - Gráfico Média Tamanho Pacotes .....	49

## LISTA DE SIGLAS

AP.....	ACCESS POINT
ATM.....	ASYNCHRONOUS TRANSFER MODE
CODEC.....	CODIFICADOR/DECODIFICADOR
IP.....	INTERNET PROTOCOL
IPSEC.....	INTERNET PROTOCOL SECURITY PROTOCOL
L2F.....	LAYER 2 FORWARDING
L2TP.....	LAYER 2 TUNNELING PROTOCOL
MCU.....	MULTIPOINT CONTROL UNITS
MGCP.....	MEDIA GATEWAY CONTROL PROTOCOL
NAT.....	NETWORK ADDRESS TRANSLATION
PBN.....	PACKET BASED NETWORK
POP3.....	POST OFFICE PROTOCOL
PPTP.....	POINT-TO-POINT TUNNELING PROTOCOL
RC4 .....	RIVEST CIPHER 4
RDSI.....	REDE DIGITAL DE SERVIÇOS INTEGRADOS
RTPC.....	REAL TIME CONTROL PROTOCOL
SIP.....	SESSION INITIATION PROTOCOL
TCP/IP.....	TRANSMISSION CONTROL PROTOCOL/ INTERNET PROTOCOL
TLS/SSL.....	TRANSPORT LAYER SECURITY/ SECURE SOCKET LAYER
TKIP .....	TEMPORAL KEY INTEGRITY PROTOCOL
VOIP.....	VOICE OVER INTERNET PROTOCOL
VPN.....	VIRTUAL PRIVATE NETWORK
WDS.....	WIRELESS DISTRIBUTION SYSTEM
WEP.....	WIRED EQUIVALENT PRIVACY
WPA.....	WI-FI PROTECTED ACCESS
WPA2-PKS.....	WI-FI PROTECTED ACCESS 2 PRE-SHARED KEY



## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO .....</b>	<b>8</b>
1.1	JUSTIFICATIVA .....	8
1.2	OBJETIVOS .....	9
1.2.1	<b>Objetivo Geral .....</b>	<b>9</b>
1.2.2	<b>Objetivo Específico .....</b>	<b>9</b>
1.3	ESTRUTURA DO TRABALHO .....	10
<b>2</b>	<b>REFERENCIA TEÓRICO .....</b>	<b>11</b>
2.1	PROTOCOLO TCP/IP .....	11
2.2	VOICE OVER INTERNET PROTOCOL .....	12
2.3	CRIPTOGRAFIA .....	15
2.3.1	<b>Wired Equivalent Privacy .....</b>	<b>16</b>
2.3.2	<b>Wi-Fi Protected Access .....</b>	<b>17</b>
2.3.3	<b>Wi-Fi Protected Access 2 Pre-Shared Key .....</b>	<b>18</b>
2.4	VIRTUAL PRIVATE NETWORK .....	19
2.5	ASTERISK .....	21
2.6	WIRESHARK .....	23
2.7	WIRELESS DISTRIBUTION SYSTEM .....	24
<b>3</b>	<b>METODOLOGIA .....</b>	<b>26</b>
3.1	EQUIPAMENTOS .....	26
3.2	WDS .....	27
3.2.1	<b>Roteador Principal .....</b>	<b>27</b>
3.2.2	<b>Roteador WDS .....</b>	<b>29</b>
3.3	OPENVPN .....	30
3.3.1	<b>Servidor Openvpn .....</b>	<b>31</b>
3.3.2	<b>Clientes Openvpn .....</b>	<b>32</b>
3.4	ASTERISK .....	35
3.5	X-LITE .....	40
3.6	ZOIPER .....	42
3.7	WIRESHARK .....	44
3.8	RESULTADOS .....	46
<b>4</b>	<b>CONSIDERAÇÕES FINAIS .....</b>	<b>50</b>
4.1	TRABALHOS FUTUROS .....	50
	<b>REFERÊNCIAS .....</b>	<b>51</b>
	<b>APÊNDICE A - CONFIGURAÇÃO SERVIDOR OPENVPN UBUNTU .....</b>	<b>54</b>
	<b>APÊNDICE B - CONFIGURAÇÃO SERVIDOR ASTERISK .....</b>	<b>57</b>

## 1 INTRODUÇÃO

Com o avanço da tecnologia, as redes de computadores vêm crescendo cada vez mais, e não somente as cabeadas, pois hoje o WDS (*Wireless Distribution System*) possui a capacidade e ampliar o sinal wireless e garante a melhor rota para que os pacotes possam ser trafegados, tornando o uso das redes sem fio mais frequentes. (ALBUQUERQUE, 2014).

As redes de computadores tornaram-se essenciais para a sociedade humana, pois elas estão presentes desde as grandes corporações até nossas casas interligando dispositivos entre si, e com a internet, nos trazendo grandes praticidades e nos proporcionando os mais variados tipos de serviços.

Dentre todos os serviços disponíveis alguns vêm ganhando grande espaço, como o VOIP (*Voice Over Internet Protocol – Voz sobre Protocolo de Internet*) que realiza a transformação de sinais de áudio analógicos, como os de uma chamada telefônica, em dados digitais, assim podendo ser transferidos através de uma rede de computadores ou Internet. (SHALDERS, 2010).

Também podemos citar a VPN (*Virtual Private Network – Rede Privada Virtual*) que consiste em uma rede privada construída sobre uma infraestrutura de uma rede pública, normalmente a Internet, usada para interligar de modo seguro de baixo custo redes distantes. Como ela estará trabalhando sobre uma rede pública é preciso tomar medidas de segurança, ou seja, utilizar técnicas de criptografia para que caso os dados trafegados por esta rede sejam interceptados não possam ser decifrados. (MARTINS, 2009).

Com o crescimento da internet, o tráfego de dados tem sobressaído sobre o tráfego telefônico, tornando o VOIP uma opção bastante atrativa, pois seu custo é muito menor quando comparado com as companhias telefônicas. (TANENBAUM, 2003). Entretanto é preciso verificar a segurança e a qualidade dos dados trafegados, principalmente em redes sem fio, que possuem uma largura de banda e processamento mais baixo se comparados a uma rede cabeada, é preciso garantir tráfego seguro dos dados e integridade dos pacotes, sem utilizar grandes técnicas de segurança para não acabar interferindo e degradando o desempenho da rede, conseguindo segurança e desempenho satisfatórios.

### 1.1 JUSTIFICATIVA

Atualmente a comunicação é de vital importância, principalmente em empresas, pois precisam estar sempre a par do que está acontecendo para tomar as melhores decisões,

entretanto empresas de telefonia cobram caro por seus serviços, tornando necessária à busca por soluções mais baratas. Uma alternativa para contornar estes altos custos de telefonia seria a utilização da internet, com serviços VoIP, ou seja, realizar ligações entre equipamentos da rede através da internet.

Para utilizar os serviços VoIP é necessário a configuração de um servidor PABX, como o Asterisk que se trata de um software completo para o gerenciamento de telefonia. Ele possui licença GPL - *General Public License*, não gerando custos para sua utilização.

O tema “Um Estudo de Transmissão de Voz em Redes sem Fio IP com WDS Associadas com Mecanismos de Segurança” foi escolhido, pois os novos equipamentos nos proporcionam uma forma mais fácil e rápida de se manter conectado e realizar chamadas através da rede, mas é preciso analisar o quanto isso é viável e seguro. Entretanto não basta apenas baratear os custos, mas o serviço precisa ser de qualidade.

Visando verificar a eficiência deste serviço, este trabalho visa realizar um comparativo utilizando cenários com configurações de criptografias diferentes, analisando o desempenho das chamadas em redes sem fio.

## 1.2 OBJETIVOS

### 1.2.1 Objetivo Geral

O objetivo deste trabalho é a criação e configuração de uma rede sem fio utilizando WDS com um servidor Asterisk. Realizando chamadas entre os equipamentos que estarão interligados utilizando uma VPN, implementada com métodos de criptografia, analisando o desempenho da rede durante as chamadas.

### 1.2.2 Objetivo Específico

Para alcançar os objetivos gerais, alguns objetivos específicos serão necessários:

- Levantamento bibliográfico;
- Criação e configuração de uma rede sem fio com WDS;
- Instalação e configuração de servidor Linux com Asterisk;
- Implementação de VPN com métodos de criptografia;
- Utilizar os tipos de criptografia WEP, WPA, WPA2-PSK;

- Instalação de duas estações Windows com softphones para comunicação;
- Configuração softphone em Android para comunicação;
- Captura dos pacotes trafegados com o software Wireshark;
- Análise dos pacotes em diferentes tipos de criptografia;
- Exibir os resultados obtidos em relatórios de fácil leitura.

### 1.3 ESTRUTURA DO TRABALHO

Para melhor compreensão, este trabalho está organizado da seguinte maneira:

O capítulo 2 corresponde ao referencial teórico, estando dividido em subseções.

O capítulo 2.1 é apresentado o protocolo TCP/IP, bem como sua importância para as redes de computadores.

O capítulo 2.2 será apresentado o conceito de VOIP, ou seja, voz sobre IP, como este serviço pode ser usado para realizar ligações entre empresas.

No capítulo 2.3 será tratada criptografia, como proteger os pacotes que são trafegados na rede, garantindo que apenas o usuário de destino possa interpretar a mensagem, este capítulo está dividido nos três métodos de criptografias: WEP, WPA e WPA2-PKS que serão utilizadas para a realização do estudo.

No capítulo 2.4 está o conceito de VPN, como é a ideia do túnel virtual bem como o OPENVPN que se trata de uma melhoria ao VPN convencional.

Já no capítulo 2.5 estará o Asterisk, um software para gestão de telefonia de baixo custo.

No capítulo 2.6 será apresentado o Wireshark, um software para captura e análise de pacotes trafegados na rede.

No capítulo 2.7 estará o WDS, que funciona como uma espécie de repetidor para rede sem fio.

No capítulo 3 será apresentada a metodologia que se pretende seguir para a realização do trabalho.

Já no capítulo 4 estará apresentado o cronograma em que este trabalho está sendo desenvolvido.

Por fim no capítulo 5 estará apresentado o que se espera conseguir com este trabalho.

## 2 REFERENCIA TEÓRICO

### 2.1 PROTOCOLO TCP/IP

Quando começaram a surgir às redes de rádio e satélite, os protocolos existentes até então começaram a ter problemas de interligação, forçando a necessidade de uma nova arquitetura de referência que pudesse conectar várias redes de modo uniforme. (BARBOSA, 2012).

Essa arquitetura é conhecida hoje como modelo de referência TCP/IP, pois ela consiste em um conjunto de protocolos diferentes, tendo entre eles os dois principais, TCP (*Transmission Control Protocol*) e IP (*Internet Protocol*), dando origem a seu nome. (TORRES, 2007).

Este modelo foi definido pela primeira vez em 1974, sendo projetado para sempre se manter funcionando, mesmo que parte dos hosts pare, sem comprometer o resto da rede. (TANEMBAUM, 2011).

O TCP/IP está dividido em quatro camadas, sendo Aplicação, Transporte, Internet e Interface, que são demonstradas na Figura 1:

Figura 1 – Protocolo TCP/IP.

CAMADAS	DEFINIÇÃO	PROTOCOLOS
Aplicação	Faz interface entre a rede e softwares aplicativos. Inclui também serviços de autenticação.	HTTP, POP3, SMTP
Transporte	Fornecer uma variedade de serviços entre os dois computadores hosts, incluindo o estabelecimento e a finalização da conexão, controle de fluxo, recuperação de erros e segmentação de grandes blocos de dados em partes menores para transmissão.	TCP, UDP
Internet	Endereçamento lógico, roteamento e determinação de caminhos.	IP
Interface	Define os detalhes elétricos, óticos, de cabeamento, de conectores e de procedimentos requeridos para se transmitirem os bits, representados como alguma forma de energia e se movendo através de um meio físico.	Ethernet, Frame Relay

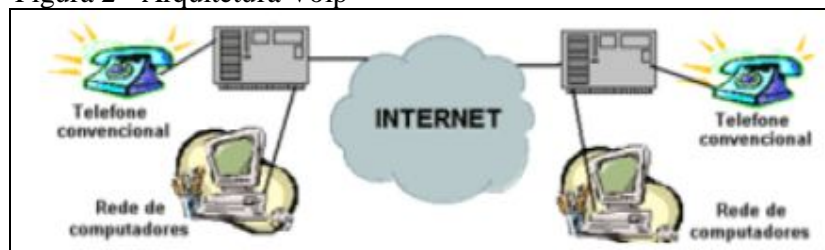
Fonte: TCP/IP (2014?).

## 2.2 VOICE OVER INTERNET PROTOCOL

Atualmente a comunicação de dados cresceu intensamente, tornando-se a representativa da “Era da Informação”, devido a Internet, ultrapassando o tráfego tradicional telefônico. A internet é capaz de realizar chamadas telefônicas, mas para que o sistema de pacotes de voz seja implementado, este deve ter a mesma qualidade que o sistema público de telefonia vem trazendo a seus usuários, para que assim as corporações possam integrar voz e dados em uma mesma infraestrutura. Desta forma reduzirá custos com equipes técnicas, infraestrutura diferenciada e ligações internacionais. (ROSA, 2007).

O VoIP (Voz sobre IP) trata-se de um modo de digitalizar, codificar, empacotar e enviar dados de voz através de uma rede utilizando protocolos TCP/IP. A Figura 2 exemplifica como seria uma arquitetura para serviços Voip. (PINHEIRO, 2006).

Figura 2 - Arquitetura Voip



Fonte: Pinheiro (2006).

Com o objetivo de unificar em uma única rede, a transmissão de dados e voz, para isso ser possível um conjunto de protocolos foi criado, chamado de H.323 que consiste em permitir comunicação de terminais utilizando aplicações de áudio, vídeo e multimídia. (H.323, 2006).

Sistemas VoIP permitem três tipos de arquitetura, sendo elas:

- **PC-a-PC:** nesta arquitetura, dois computadores em uma rede IP se comunicam para a troca de sinais de voz, sendo todo o tratamento realizado nos próprios computadores. A chamada de voz é estabelecida com base no endereço IP. Nesta arquitetura é possível utilizar telefones IP para substituir um PC. (ROSA, 2007).
- **Gateway:** aqui todas as chamadas passarão por um telefone padrão que ficará responsável por validar e transmitir as chamadas entre o destino e o fim.

Comumente é utilizado o protocolo H.323 para a transmissão dos pacotes de voz. (ROSA, 2007).

- **Híbridas:** como o próprio nome sugere, nesta arquitetura é realizada uma união entre PC-a-PC e Gateway. Para isto ser possível é preciso um serviço de mapeamento ou translação de endereços IP. (ROSA, 2007).

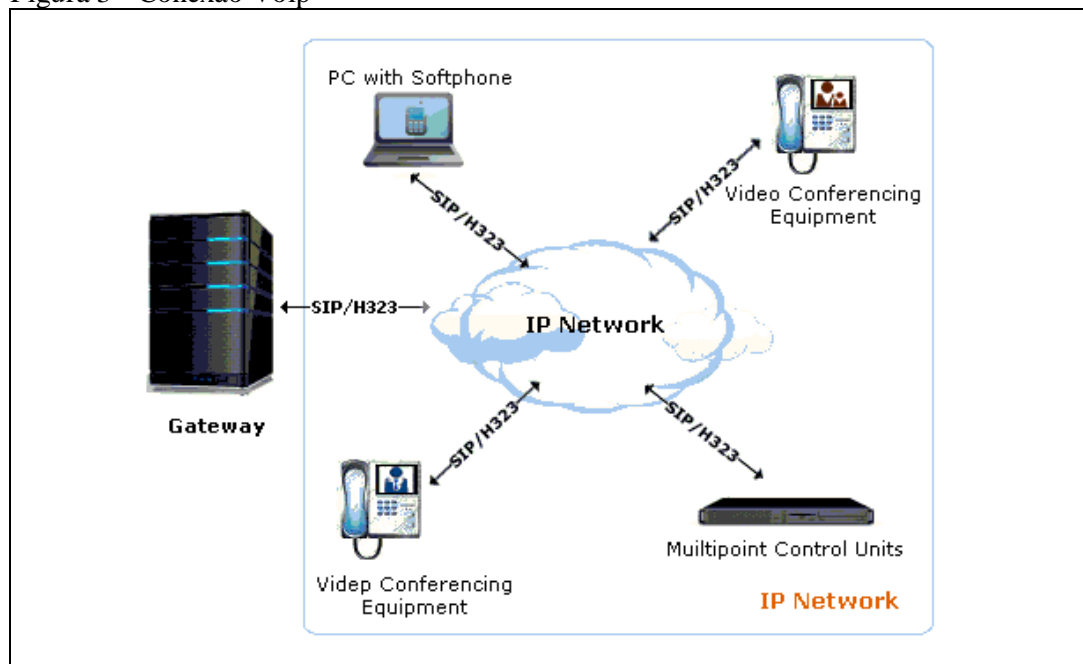
Os sistemas VoIP apresentam os seguintes protocolos, o SIP (*Session Initiation Protocol*), sendo a forma mais simples de modular e usar voz sobre IP e o MGCP (*Media Gateway Control Protocol*), que possui o controle de chamadas, transmissões e sinalização, monitorando os troncos de telefonia e enviando mensagens de mídia para os endereços específicos.

O SIP é um protocolo baseado em texto, como HTML e SMTP, usado para iniciar, modificar ou terminar sessões ou chamadas multimídia entre usuários, ele usa conexões ponto-a-ponto, utilizando o protocolo UDP para transportar suas mensagens. O SIP define recomendações para serviços VoIP adicionais, como conferência, transferência, identificação, redirecionamento e distribuição de chamadas. Este protocolo possui dois tipos de agentes, sendo agentes usuários clientes e agentes usuários servidores. Os do tipo cliente realizam chamada SIP a outro terminal, já os servidores recebem a ligação de um terminal, por exemplo, usuários clientes seriam telefones IP, softphones e gateways; os de servidores seriam: *Proxy Server* que é responsável por receber os pedidos do cliente e encaminhar para o agente usuário, ou outro servidor de proxy, caso o usuário não esteja sob sua administração. Como o usuário não se conecta diretamente com o agente servidor garante maior segurança, prove também funções como autenticação, controle de acesso, segurança e roteamento. O *Redirect Server* que recebe a conexão do usuário e repassa ao solicitante com informações do servidor, deixando que todo o gerenciamento da chamada seja realizado pelo usuário cliente. O *Register Server* apenas recebe registros do usuário cliente, e armazena informações como IP e ID do cliente em um Servidor de Banco de Dados. O Servidor de Banco de Dados é utilizado para armazenar as informações que são recebidas do *Register Server*. (ROSA, 2007).

O H.323 especifica um sistema de comunicação multimídia baseado em pacotes PBN (*Packet Based Network*), que sejam LANs, MANs, Intranets, Internet e conexões ponto-a-ponto, mas não prove uma qualidade de serviço garantida. Estabelece também padrões de codificação e decodificação e fluxos de áudio e vídeos, para que desta forma produtos de fabricantes diferentes possam interoperar em si, permitindo utilizar quaisquer tecnologias de enlace ou topologia de rede. (ROSA, 2007).

A Figura 3 demonstra uma conexão IP típica utilizando o protocolo SIP/H.323.

Figura 3 - Conexão Voip



Fonte: H. 323 (2006).

O H.323 possibilita a comunicação multimídia com quatro componentes trabalhando juntos, sendo eles:

**Terminais:** Computadores pessoais ou dispositivos, não sendo necessário que suportem vídeo e dados, apenas voz, aplicativo de multimídia e suportar H. 323. (ROSA, 2007).

**Gateways:** elementos que fornecem a comunicação entre os terminais com o H. 323 e padrões diferentes, ou até mesmo outra rede, como a RTCP (Rede Telefônica Pública Comutada). (ROSA, 2007).

**Gatekeepers:** é a central para todas as chamadas dentro do conjunto de terminais, gateways e MCUs, estes são os componentes mais importantes, dentre outras funcionalidades, também gerenciam a largura de banda em conferência H. 323. (ROSA, 2007).

**Multipoint Control Units (MCUs):** gerenciamento da conexão de todos os terminais, codificadores/decodificadores de áudio, garante suporte a conferências com mais de dois terminais H. 323, podendo ainda ser implementados em conjunto com os gatekeepers, gateways em um único dispositivo físico. (ROSA, 2007).



O algoritmo responsável pela conversão de sinal analógico em sinal digital é chamado de CODEC. Durante a conversão eles realizam compactação ou descompactação dos dados. Para todos os CODEC a qualidade de som, largura de banda e processamento serão diferenciados. Esta diferença é necessária para definir o melhor custo/benefício, em relação ao equipamento e conexões existentes. (ROSA, 2007).

### 2.3 CRIPTOGRAFIA

Para a sociedade humana, é preciso compartilhar informações para que assim possa evoluir. Entretanto algumas informações podem não dizer respeito a todos do grupo, surgindo à necessidade de procurar formas de manter a informação, ou ao menos parte dela, segura e confidencial. A humanidade procurou por anos, mas foram os gregos que encontraram as primeiras técnicas de encriptar suas mensagens, garantindo assim sua confidencialidade, estas técnicas foram descobertas por volta do século VI A. C. (WEBER, 1998).

Atualmente estamos na “Era da Informação”, com todos os avanços tecnológicos, surgiram muitos meios de se compartilhar a informação em tempo real, como a Internet, que está incrustada em todos os aspectos da sociedade moderna. A informação eletrônica está gerando um conjunto de novas relações econômicas e sociais, vivenciadas pela sociedade. (MITZCUN, 2007).

Devido a essa grande facilidade em transmitir a informação é preciso aderir a políticas de segurança adequadas, para que a informação possa ser transmitida e utilizada de forma ampla e confiável. Para a segurança da informação eletrônica é preciso seguir alguns requisitos, como a integridade, confidencialidade e autenticidade. Quando uma informação é transmitida, se ela puder ser lida e entendida sem qualquer modificação, significa que esta é uma informação não criptografada. A técnica de ocultar uma informação, garantindo sua confidencialidade é chamada de encriptação, e o processo inverso, descriptação. (MITZCUN, 2007).

A criptografia consiste em métodos para cifrar a informação que garantam sua confidencialidade, para que esta possa ser transmitida pelo emissor, e caso uma pessoa diferente do receptor a receba não possa saber seu conteúdo, pois o único capaz de decifrar a informação, ou seja, transformá-la de volta ao conteúdo inicial é o receptor. As regras que determinam como serão as transformações da informação são chamadas de algoritmos, ou seja, uma sequência de operações que devem ser realizadas, com o parâmetro que determina as condições da transformação chamado de chave. (MITZCUN, 2007).

A criptografia é implementada por um conjunto de métodos de tratamento e transformação dos dados que serão transmitidos pela rede pública. Um conjunto de regras é aplicado sobre os dados, empregando uma sequência de bits (chave) como padrão a ser utilizado na criptografia. Partindo dos dados que serão transmitidos, o objetivo é criar uma sequência de dados que não possa ser entendida por terceiros, que não façam parte da VPN, sendo que apenas o verdadeiro destinatário dos dados deve ser capaz de recuperar os dados originais fazendo uso de uma chave".

ROSSI, FRANZIN (2000)

Existem dois tipos de chaves para a criptografia, as chaves simétricas e as chaves assimétricas.

- **Chave Simétrica ou Chave Privada:** este método é baseado em apenas uma chave, denominada de chave secreta. Esta chave é utilizada tanto para cifrar a informação quanto para decifra-la, fazendo que emissor e receptor tenham-na para poder utilizar a informação. (WEBER, 1998).
- **Chave Assimétrica ou Chave Pública:** este método utiliza chaves diferentes para o método de cifrar e decifrar a informação, sendo, no entanto relacionadas. Cada tipo é composto por duas chaves, sendo uma pública e uma privada, apenas a chave privada deve ser mantida em segredo, permitindo que as chaves públicas circulem livremente, pois somente com o conjunto de chaves correto que será possível decifrar a informação. (WEBER, 1998).

### 2.3.1 Wired Equivalent Privacy

O protocolo WEP vem sendo o mais popular responsável pela proteção dos pacotes em redes sem fio, pois se trata de um protocolo de segurança de nível de enlace de dados, garantindo assim uma segurança equivalente a existente em redes cabeadas, provendo confidencialidade e integridade dos dados. (LUCAS, 2006).

Utilizando uma função checksum, o protocolo WEP garante que o conteúdo da mensagem esteja inalterado e protegido, o protocolo também garante impedir intrusos de ler, modificar ou inserir, garantindo que ela chegue a seu destino, ele também controla o acesso à rede sem fio, impedindo assim a entrada de intrusos, garantindo a autenticidade. Apenas pacotes que contenham a chave de criptografia WEP são considerados, descartando todos os demais. (PEREIRA JUNIOR et al., 2004).

Apesar de sua grande popularidade, o protocolo WEP ainda possui falhas, mas ainda assim garante maior segurança à rede. Por ser constituído de algoritmo simétrico ele utiliza

chaves simétricas, das quais devem ser as mesmas tanto do lado do cliente quanto do ponto de acesso, elas são chamadas de chaves WEP. (PEREIRA JUNIOR et al., 2004).

As chaves WEP não possuem um padrão especificado, podendo estar pré-carregadas pelo fabricante, pela rede fisicamente conectada, etc., fazendo com que elas possam ficar estáveis por muito tempo, portanto o recomendado é que o vetor de inicialização seja modificado em cada pacote, evitando ataques de reutilização de fluxo. (TANENBAUM, 2003).

O WEP foi baseado no método RC4, que consiste em um algoritmo de fluxo, ou seja, criptografa os dados ao mesmo tempo em que são transmitidos os pacotes trocados através da comunicação sem fio. (PEREIRA JUNIOR et al., 2004).

A chave WEP contém 40 ou 140 bits e um vetor de inicialização público de 24 bits. MARTINS (2003). A chave RC4 pode conter 64 ou 128 bits, pois consiste na soma do vetor de inicialização com a adição da chave WEP. (LUCAS, 2006).

Atualmente o padrão WEP 64 bits é compatível com todos os produtos que sigas o padrão WI-FI, para se usar o padrão WEP de 128 bits, é preciso que todos os componentes da rede suportem este padrão, caso contrário este componente não conseguirá interligar com os demais da rede. (LUCAS, 2006).

### **2.3.2 Wi-Fi Protected Access**

Outro protocolo de segurança de redes sem fio é o WPA (*Wi-Fi Protected Access*) também chamado de WEP2, que foi desenvolvido com o intuito de suprir as vulnerabilidades apresentadas pelo WEP, garantindo maior segurança que seu antecessor. (BARROZO, 2009).

A grande diferença entre este protocolo e o WEP é que ele tem como propósito uma troca constante da chave criptográfica, apenas sendo possível, pois houve uma melhoria na criptografia de dados, utilizando um protocolo de chave temporária chamada de TKIP (*Temporal Key Integrity Protocol*), tornando a criação dinâmica das chaves por quadro e um mecanismo de distribuição de chaves. (BARROZO, 2009).

Diferentemente do WEP, no WPA as chaves contam com um vetor de inicialização de 48 bits, ele também utiliza o padrão RC4, mas com outras técnicas, tendo como o objetivo suprir assim a fragilidade do protocolo WEP, ou seja, com seu forte algoritmo de criptografia o WPA surgiu para substituir o WEP. (BARROZO, 2009).

Com o WPA a autenticação dos usuários passa a se obrigatória utilizando o protocolo 802.1x e o EAP (*Extensible Authentication Protocol*), sendo um modelo para autenticação em nível de usuário, autenticando cada usuário que entra na rede. (BARROZO, 2009).

A Figura 4 mostra um comparativo entre WEP e WPA.

Figura 4 - Comparativo WEP/WPA.

<b>Características de Segurança</b>	<b>WEP</b>	<b>WPA</b>
Algoritmos de cifração	RC4	RC4
Gerenciamento de chaves	Nenhum	Baseado em EAP
Tamanho de chaves	40 ou 104 bits	128 bits (64 bits para manutenção)
Chave do pacote	Criada por concatenação	Criada por função de mistura
Integridade de dados/cabeçalho	CRC32/nenhum	MIC
Proteção contra reprodução	Nenhuma	Uso do VI

Fonte: Barrozo (2009).

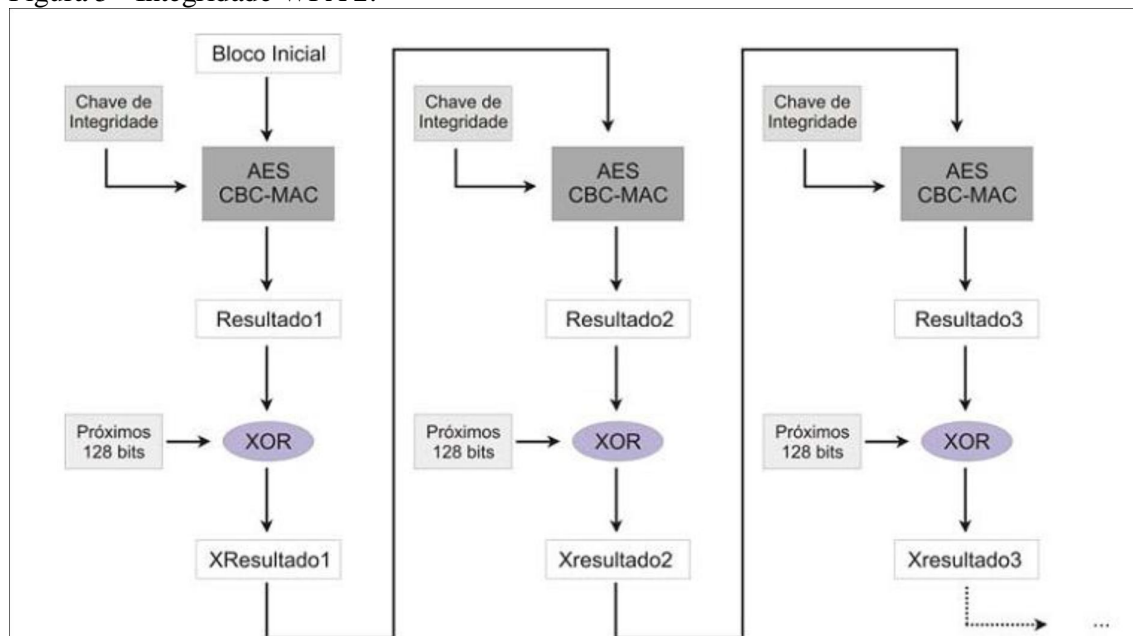
### 2.3.3 Wi-Fi Protected Access 2 Pre-Shared Key

Apesar de o protocolo WPA ter corrigido as vulnerabilidades do WEP, ele ainda manteve algumas falhas no algoritmo de criptografia, sendo necessário o desenvolvimento de um novo protocolo, este que foi intitulado de WPA2, possuindo um novo padrão chamado de PSK (*Pre-Shared Key*), fazendo com que cada usuário tenha uma senha frase. Este novo protocolo consiste basicamente na implementação de novos algoritmos de criptografia e de integridade. (BARROZO, 2009).

“Neste caso o protocolo responsável pela integridade e confiança é o CCMP (*Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol*) e é baseado no algoritmo de encriptação AES (*Advanced Encryption Standard*).” (BARROZO, 2009, p. 37).

Na Figura 5 está representada a Integridade do WPA2, sendo que no bloco inicial estão os dados a serem criptografados, utilizando o algoritmo AES para criptografar o dado e aplicando a operação lógica XOR entre o dado e o próximo bloco, que passará pelo mesmo processo sucessivamente. Este sistema é extremamente seguro, sendo que atualmente poucas vulnerabilidades foram descobertas.

Figura 5 - Integridade WPA 2.



Fonte: Linhares, Gonçalves (s.d.)

## 2.4 VIRTUAL PRIVATE NETWORK

Através da infraestrutura da internet podemos simular um caminho privativo para conectar dois computadores ou redes entre si. Este caminho se comporta como uma linha privada, sem compartilhamento, dando segurança a conexão. (SOUZA, 2006).

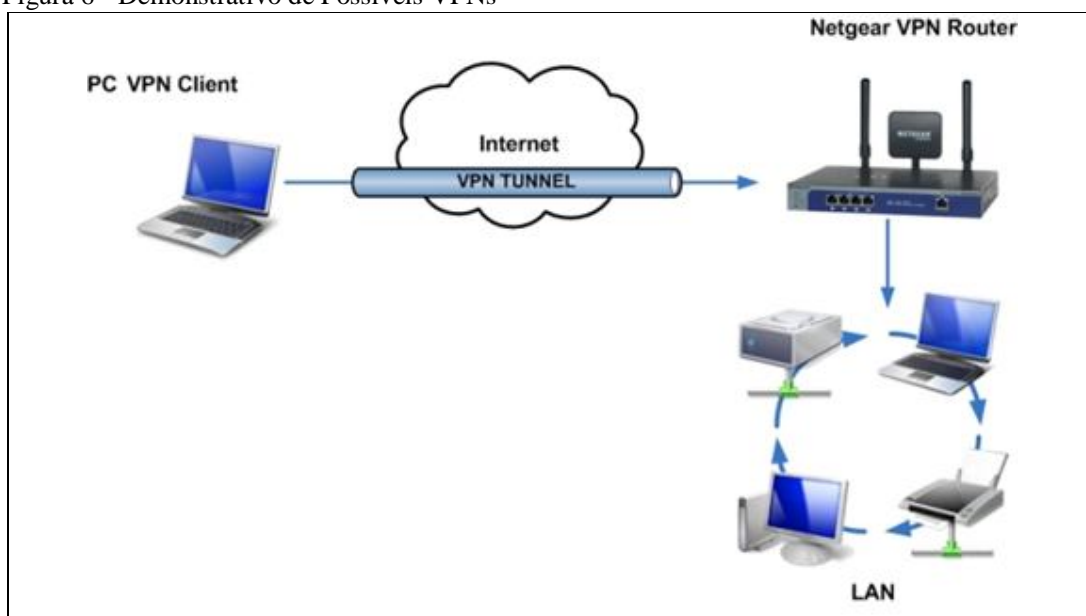
Antes da utilização da VPN para se interligar redes distantes, eram utilizadas linhas privativas, tais como Frame Relay e ATM. Já para escritórios móveis eram utilizados servidores de acesso remoto com modem de discagem gratuita ou conexões RDSI (Rede Digital de Serviços Integrados). No entanto, estes serviços eram caros e tornavam as redes complexas demais, chamadas Intranets, as pequenas ou médias empresas que não podiam arcar com os custos, utilizavam serviços de comutação de circuito de baixa velocidade. (ROSSI; FRANZIN, 2000).

Com os avanços da Internet, sua largura de banda aumentou, e ela passou a estar mais acessível, permitindo que as companhias migrassem suas Intranets para ela, criando assim as Extranets. Com o baixo custo e a grande disponibilidade, esta seria a solução ideal, se não fosse o fato da ausência da segurança para as informações que trafegavam na rede. Para solucionar este problema, as VPNs foram criadas, usando protocolos de tunelamento e procedimentos de encriptação, garantindo a integridade e autenticidade dos dados, e como

elas ocorrem sobre uma rede pública seus custos são bem abaixo do que serviços dedicados. (MITZCUN, 2007).

A VPN cria um túnel privativo lógico virtual entre dois pontos, fornecendo à criptografia dos dados entre a origem e destino (criptografia end-to-end), de forma que teoricamente somente o transmissor e o receptor conseguem entender os dados, dando a impressão do canal privativo, já que ninguém externo poderia fazer uso destes dados. Utilizando a Internet como meio de transmissão, é possível interligar redes locais fisicamente distantes entre si com o comportamento de uma rede privada, gerando uma grande vantagem sobre links dedicados, pois a empresa pode montar sua rede corporativa com um baixo investimento e grande segurança de seus dados. A Figura 6 demonstra uma possível VPN. (ROSSI; FRANZIN, 2000).

Figura 6 - Demonstrativo de Possíveis VPNs



Fonte: VPN (2010?)

A maior vantagem no uso das VPNs é o baixo custo, pois por utilizar a Internet como meio de transmissão, e mesmo a usando, podemos dizer que estamos na rede privada da empresa devido à privacidade fornecida pelos túneis. Embora se diga túnel, o caminho entre origem e destino se comporta como qualquer outro tráfego na Internet, ou seja, pode passar por diferentes caminhos até chegar ao destino final. O nome “túnel” foi empregado por que apenas o destino, após a transmissão é que pode ver a informação original. (MITZCUN, 2007).

A informação é encriptada e encapsulada com um determinado protocolo de rede dentro de um pacote IP, para que este possa ser roteado, filtrado e aplicado a dispositivos, de modo como já é realizado com WANs tradicionais. Os protocolos utilizados pela VPN no processo de criptografia são: IPSec (*Internet Protocol Secutiy*), L2TP (*Layer Turnneling Protocol*), L2F (*Layer 2 Forwarding*) e PPTP (*Point to Point Tunneling Protocol*). (ROSSI; FRANZIN, 2000).

Para a transmissão ser segura, o protocolo VPN antes de enviar através da rede criptografa os dados. No receptor é feito o processo inverso, retornando os dados ao formato original para que eles possam ser utilizados. (MITZCUN, 2006).

As VPNs podem ser implementadas em redes heterogéneas, ou seja, com diversos equipamentos e sistemas operacionais, mas é importante ressaltar que para garantir um bom nível de segurança, analisar as particularidades de cada sistema e hardware quanto a sua configuração. (ROSSI; FRANZIN, 2000).

Uma excelente solução para VPN é o OpenVPN, que utiliza padrões SSL/TLS para criptografar os dados, tendo como objetivos tornar as VPNs mais seguras, estáveis e flexíveis. O protocolo SSL/TLS permite autenticação mútua e segura entre cliente e servidor, sendo implementado como uma camada adicional entre o TCP/IP e protocolos de nível superior, como HTTP, SMTP, etc. (LEVANDOSKI et al., 2010).

O OpenVpn dá suporte a IP dinâmico e NAT, definindo uma negociação de endereçamento IP entre o servidor VPN e seus clientes, eliminando configurações manuais de protocolo IP, também permite a utilização de técnicas mais complexas de criptografia, podendo utilizar toda a biblioteca OpenSSL, protegendo todo o tráfego da rede privada enquanto é transmitido pela Internet. (LEVANDOSKI et al., 2010).

## 2.5 ASTERISK

O Asterisk foi desenvolvido sob a licença GPL (*General Public License*), com o objetivo de implementar uma central de telefonia, permitindo que clientes conectados a ele façam ligações uns para os outros ou para telefones conectados em outras centrais, como por exemplo a central pública de telefonia. Desenvolvido inicialmente para sistemas Linux, possuindo código aberto, dezenas de programadores contribuíram para seu desenvolvimento, e hoje ele pode ser executado também em FreeBSD, OpenBSD, Mac OS X, Sun Solaris e Microsoft Windows, estando atualmente na versão 3.0.1. (ASTERISK, 2006).

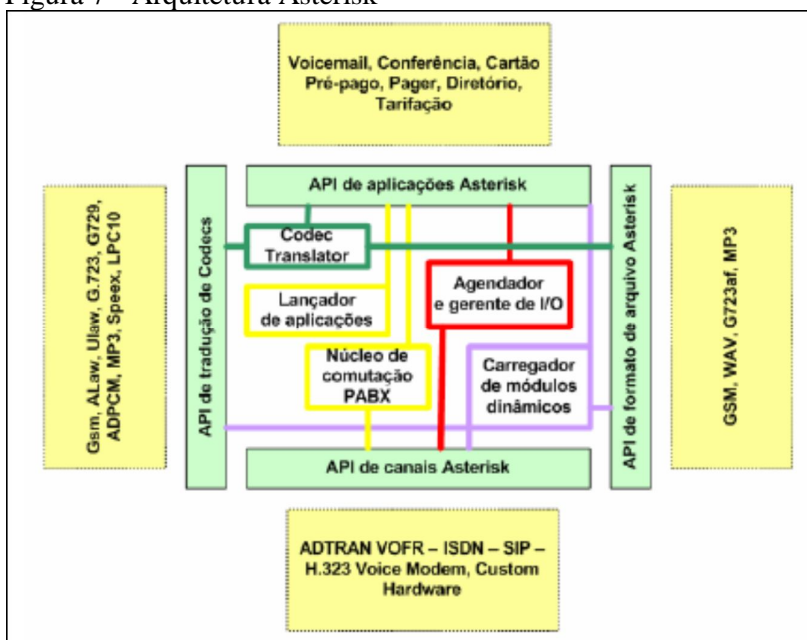
O Asterisk contém características como correio de voz, respostas interativas, distribuição automática de chamadas e conferência em chamadas, recursos antes apenas encontrados em sistemas telefônicos caros e proprietários, possuindo grande versatilidade, pois permite a criação de scripts com módulos escritos em linguagem C, além de outras formas de customização. Com a adição de um hardware especial é possível conectar telefones convencionais ou linhas trancos de uma central telefônica convencional. (ASTERISK, 2006).

O Asterisk pode trabalhar com a maioria dos telefones SIP, pois suporta muitos protocolos de voz sobre IP (VoIP), podendo atuar como um registrador ou gateway entre IP e a telefonia convencional, para ele foi criado um novo protocolo, o IAX, que garante melhoria no entroncamento entre servidores Asterisk. (GONÇALVES, 2005).

Com o Asterisk é possível uma construção eficaz de novos sistemas de telefonia, pois ele suporta a mistura de sistemas convencionais e sistemas VoIP, podendo substituir centrais telefônicas antigas, para assim obter novas funcionalidades e reduzir os custos telefônicos, pois estará usando a internet em suas ligações. (ROSA, 2007).

Seus desenvolvedores tiveram todo o cuidado com sua criação, desenvolvendo APIs específicas definidas em torno de um núcleo PBX, para obter máxima flexibilidade no sistema. O núcleo está encarregado de gerenciar as conexões PBX, independentes de hardware, protocolos ou codecs utilizados, estando dividido em quatro módulos principais. A Figura 7 demonstra a arquitetura do Asterisk. (ROSA, 2007).

Figura 7 - Arquitetura Asterisk



Fonte: Gonçalves (2005).



**Núcleo de Comutação PABX:** o núcleo é responsável por todas as conexões e tarefas do sistema, age de modo transparente, independente de hardware ou software. (ASTERISK, 2006).

**Lançador de Aplicações:** responsável pelo gerenciamento das aplicações que prestarão serviços aos usuários, como correio de voz, listagem de diretórios e reprodução de arquivos. (ASTERISK, 2006).

**Codec Translator:** responsável por realizar todas as codificações e decodificações de todos os formatos de áudio utilizados na telefonia. (ASTERISK, 2006).

**Agendamento e Gerenciador E/S:** responsável por gerenciar o sistema e otimizar o desempenho, bem como agendamento de tarefas de baixo nível.

As APIs, da mesma forma são divididas em quatro grupos: (ROSA, 2007).

**Canais:** conexão os módulos são carregados dinamicamente, controlando cada tipo de conexão, seja ela VoIP, ISDN ou outra tecnologia. (ASTERISK, 2006).

**Aplicações:** para as aplicações serem utilizadas pelo sistema, ele carrega módulos específicos que desempenham as funções, como por exemplo: correio de voz, listagem de diretórios, conferencia e etc. (ASTERISK, 2006).

**Traduções de codecs:** responsáveis para suportar os diversos formatos de compressão de áudio. (ASTERISK, 2006).

**Formato de arquivos:** gerenciamento de diversos formatos de arquivos para leitura, gravação e armazenamento. (ASTERISK, 2006).

O sistema utiliza recursos da CPU do computador para processar os canais de voz, sendo assim, o porte do hardware onde ele será instalado determinará o número de conexões que o sistema irá gerenciar. Caso ele seja usado apenas para soluções VoIP não é preciso hardware adicional, sendo necessário apenas quando precisar interconectar com a rede pública de telefonia. Apesar de suas grandes funções, o Asterisk mantém todas suas configurações localizadas na pasta /etc/asterisk. Esses arquivos são semelhantes aos \*.ini utilizados nos sistemas Windows, sendo formatados em ASCII, tornando assim, mais fácil o gerenciamento de suas configurações. (ASTERISK, 2006).

## 2.6 WIRESHARK

O Wireshark é um software utilizado para monitoramento de informações que trafegam através de uma rede de computadores, um analisador de protocolos, funciona como o tcpdump, mas utiliza uma interface gráfica, dando mais informações e a possibilidade de

utilização de filtros, permitindo que se saiba tudo o que entra e sai da rede. Atualmente está sendo considerado um dos mais utilizados e confiáveis para esta tarefa. (FERRARI, 2008).

Com ele é possível controlar o tráfego de um determinado dispositivo, filtrar quais pacotes serão capturados, captções do wireless, etc. Ele está atualmente na versão 1.12, desenvolvido sob licença GPL (*General Public License*), sendo assim livre de custos ou prazo de validade para sua utilização, podendo ser executado em sistemas Unix, Linux, Solaris, FreeBSD, NetBSD, OpenBSD, Mac OS X e Microsoft Windows. (HEMEL, 2007).

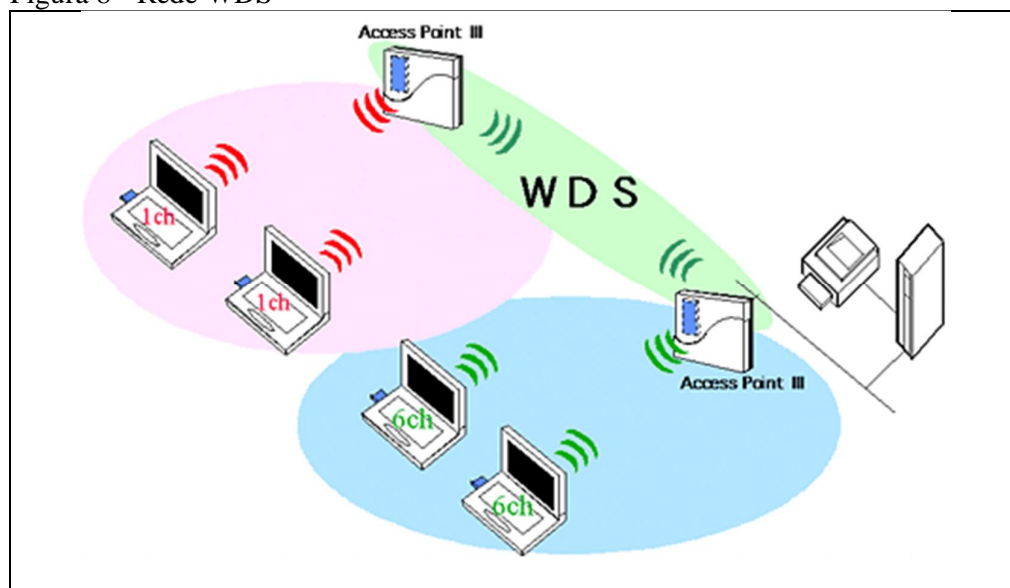
## 2.7 WIRELESS DISTRIBUTION SYSTEM

No mercado existem muitos roteadores e pontos de acesso que oferecem a função de repetidor universal, atuando como clientes de outros equipamentos, estas funções são oferecidas em sua maioria como sendo uma implementação do WDS (*Wireless Distribution System*). (PETROCELLO, 2011).

A rede WDS funciona de modo a monitorar todos os endereços MAC de todas as máquinas, esta lista é transmitida entre todos os APs (*Access Point*), fazendo com que todas as máquinas possam se conectar. Deste modo quando um equipamento deseja enviar pacotes a outro que esteja em um AP diferente o WDS assegura que os pacotes serão entregues, passando por APs intermediários até chegar ao seu destino. (MORIMOTO, 2011).

O WDS fornece suporte de como distribuir o sinal wireless por uma grande área, permitindo criar uma rede completamente sem fio utilizando APs, como demonstrado na Figura 8. Ele faz parte da especificação 802.1b original, criado em 1999, mas apenas em 2003 começou a surgir em equipamentos padronizados e baratos. (PETROCELLO, 2011).

Figura 8 - Rede WDS



Fonte: Ferreira (2010).

Para que o WDS funcione corretamente é necessário que todos os equipamentos sejam configurados no mesmo canal, sendo recomendado o uso do canal 1, 6 ou 11, pois estes canais não permitem que o sinal se sobreponha. (MORIMOTO, 2011).

Apesar de o WDS permitir que expanda a rede com facilidade, ele possui algumas limitações, como não oferecer compatibilidade entre os fabricantes, ou mesmo entre versões diferentes de um mesmo fabricante, sendo necessário a tentativa e erro, e quando conseguem conectar ele não oferece garantia de funcionamento. Outro problema se dá ao fato de apesar da rede poder crescer sem limites, é preciso se atentar, pois a cada novo equipamento conectado, a taxa de transmissão é cortada pela metade. (MORIMOTO, 2011).

O WDS possui restrições quanto aos algoritmos de encriptação, prevendo apenas o uso de redes protegidas com o WEP, utilizando uma chave de encriptação fixa, pois no WDS as chaves são rotacionais, tornando muito difícil manter o sincronismo dos equipamentos. Alguns fabricantes desenvolveram extensões para que assim permita o WDS utilizar o WPA e o WPA2, mas estas extensões geralmente são suportadas apenas dentro de produtos do mesmo fabricante e baseados chipset similares. (PETROCELLO, 2011).

### 3 METODOLOGIA

Este trabalho foi dividido em duas etapas distintas, um levantamento bibliográfico e a implementação de uma rede sem fio utilizando o WDS. Nesta rede foram realizadas ligações de uma estação para outra através de uma VPN utilizando os seguintes modos de criptografia:

- sem criptografia;
- criptografia WEP;
- criptografia WPA;
- criptografia WPA2-PSK.

Cada ligação foi monitorada com o software Wireshark, tendo os pacotes trafegados capturados para analisar o desempenho da rede sem fio. Posteriormente foi apresentado o método que apresentou o melhor resultado em relação ao custo benefício.

#### 3.1 EQUIPAMENTOS

Para este trabalho foi configurado um servidor com o sistema operacional UBUNTU instalado em um computador com a seguinte configuração: processador AMD FX(tm)-6100 Six-Core Processor de 3.30 GHZ, 8 GB de RAM, 2 TB de HD e Realtek® 8111E Gigabit como interface de rede. Esta configuração foi escolhida, pois o Asterisk pode fazer uso intensivo do processador. Ele usa o processador da própria máquina em que está instalado para realizar o processamento dos sinais digitais.

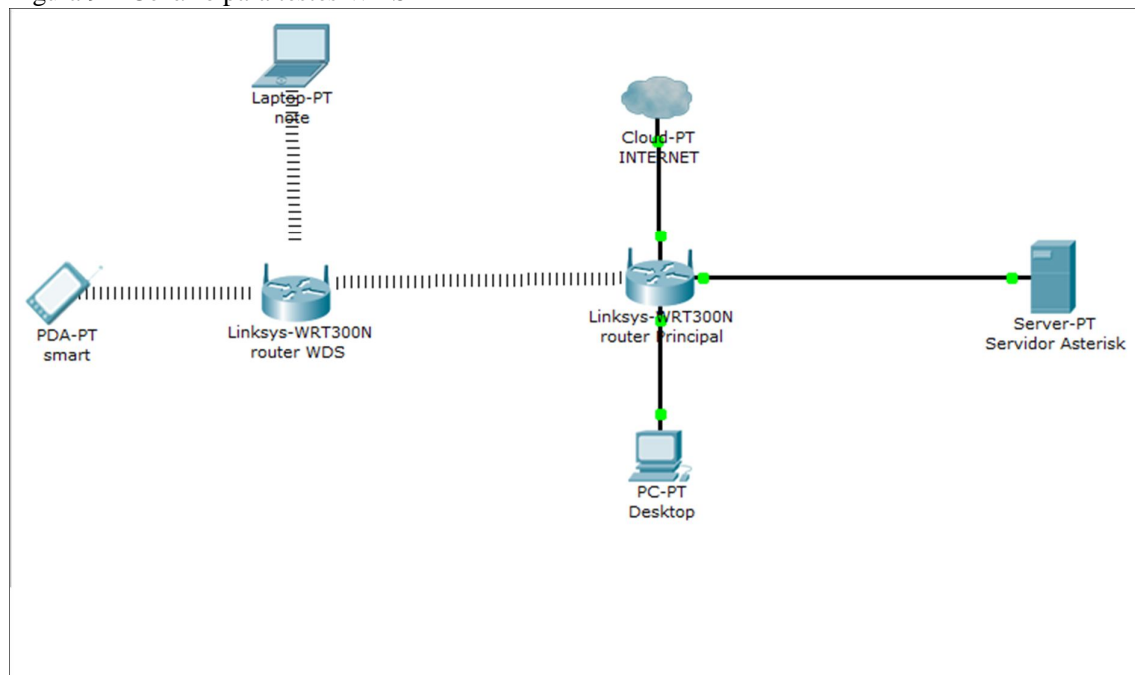
Foram configurados duas estações de trabalho, uma sendo um notebook rodando o Windows 7 com a seguinte configuração: processador core 2 duo 3.0 GHZ, 4 GB de RAM, 160 GB de HD com placa Wireless integrada para conectar-se a rede sem fio. A outra estava rodando o sistema operacional Windows XP com a seguinte configuração: processador Intel Pentium 4 3.0GHZ, 1 GB de RAM, 120 de HD e Ethernet 10/100, ambas estações estavam com um software para realizações de chamadas conhecido como ‘SoftPhone’, sendo este o X-Lite 4.7.1. Para o Windows 7 e o Zoiper na versão 3.6 para o Windows XP. Também para o Windows 7 foi instalado o Wireshark, na versão 1.10.7 para analisar os pacotes.

Também para este trabalho foi utilizado um smartphone Samsung Galasy S3 - Android, ele foi conectado a rede e estava com o “SoftPhone” Zoiper na versão 1.19.1.

Foram usados também dois roteadores TP-Link, um para a conexão com a internet e configuração dos modos de criptografia, e outro para realização do papel de WDS, ou seja,

ampliar o sinal para os demais equipamentos da rede, este cenário estava bem próximo de um cenário real, permitindo dados mais precisos ao realizar o estudo. A Figura 9 demonstra este cenário.

Figura 9 – Cenário para testes WDS



Fonte: Elaborado pelo autor.

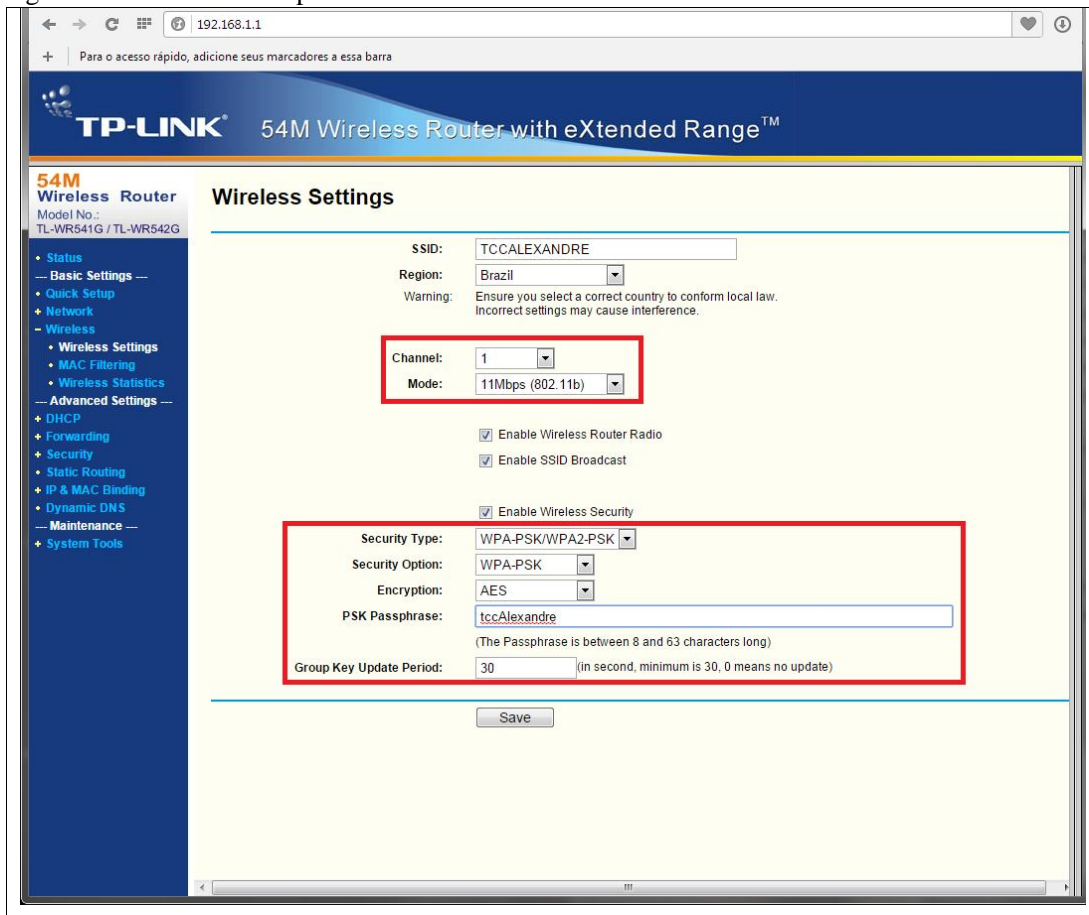
## 3.2 WDS

Para se utilizar o WDS é preciso que um roteador se conecte a outro através da rede sem fio, para que ele funcione corretamente é preciso configurar cada um dos equipamentos.

### 3.2.1 Roteador Principal

O roteador principal foi configurado com o IP 192.168.1.1, ele será o responsável pela mudança da criptografia e troca de canais evidenciados pela Figura 10.

Figura 10: Roteador Principal



Fonte: Elaborado pelo autor.

Foram realizados testes com as seguintes configurações:

- Sem Criptografia: ou seja, desabilitar a segurança da rede sem fio;
- WEP;
- WPA;
- WPA2-PSK.

Para cada um destes tipos foram usados os seguintes canais:

- 1;
- 6;
- 11.

Estes canais foram definidos, pois para eles o sinal não se sobrepõe, garantindo assim um maior desempenho.

### 3.2.2 Roteador WDS

Para configurar o segundo roteador como WDS é preciso que ele esteja trabalhando na mesma faixa de IP que o roteador principal, portanto o IP do segundo roteador foi 192.168.1.2. É recomendado manter o mesmo SSID e ele precisa operar no mesmo canal. Também é preciso marcar a caixa de seleção informando que o WDS estará ativado, com isso novos campos aparecerão, bastando clicar no botão “Survey” que encontrará automaticamente a quais dispositivos ele pode se conectar, deve ser informado o tipo de criptografia utilizado bem como a senha, deste modo ele estará operando perfeitamente. A Figura 11 mostra como ele ficará após configurado.

Figura 11: Roteador WDS

The screenshot displays the configuration page for a TP-Link 150Mbps Wireless N Router (Model No. TL-WR720N). The browser address bar shows 192.168.1.2. The page title is "TP-LINK® 150Mbps Wireless N Router Model No. TL-WR720N". The left sidebar contains navigation menus for Status, Basic Settings, Quick Setup, WPS, Network, Wireless, Advanced Settings, and Maintenance. The main content area is titled "Wireless Settings".

Key configuration fields are highlighted with red boxes:

- SSID1:** TCCALEXANDRE
- SSID2:** TP-LINK\_F7B012\_2
- SSID3:** TP-LINK\_F7B012\_3
- SSID4:** TP-LINK\_F7B012\_4
- Region:** Brazil
- Channel:** 1
- Mode:** 11bgn mixed
- Channel Width:** Auto
- Enable WDS:**
- SSID(to be bridged):** TCCALEXANDRE
- BSSID(to be bridged):** C8-3A-35-24-E6-98
- Key type:** WPA-PSK/WPA2-PSK
- WEP Index:** 1
- Auth type:** open
- Password:** tccAlexandre

A "Survey" button is located below the BSSID field. A "Save" button is at the bottom of the configuration area.

Fonte: Elaborado pelo autor.

É possível configurar um tipo de criptografia diferente bem como a senha em “Wireless Security”, mas é recomendado manter como o principal, pois se o usuário sair do alcance de um e se conectar ao outro ele perderá a conexão, sendo obrigado a se conectar novamente e informar a nova senha. Neste trabalho foi mantida a mesma configuração, como mostrado na Figura 12.

Figura 12: Roteador WDS configuração segurança

The screenshot displays the configuration interface for a TP-Link 150Mbps Wireless N Router (Model No. TL-WR720N). The browser address bar shows the IP address 192.168.1.2. The left sidebar contains a navigation menu with the following items: Status, Basic Settings, Quick Setup, WPS, Network, Wireless, Wireless Settings, Wireless Security (highlighted), Wireless MAC Filtering, Wireless Advanced, Wireless Statistics, Advanced Settings, DHCP, Forwarding, Security, Parental Control, Access Control, Static Routing, IP QoS, IP & MAC Binding, Dynamic DNS, Maintenance, and System Tools. The main configuration area is divided into three sections: WEP, WPA/WPA2, and WPA-PSK/WPA2-PSK. The WPA-PSK/WPA2-PSK section is highlighted with a red border and contains the following settings: Version: WPA2-PSK, Encryption: AES, PSK Password: tccAlexandre, and Group Key Update Period: 30 (in second, minimum is 30, 0 means no update). A 'Save' button is located at the bottom of the configuration area.

Fonte: Elaborado pelo autor.

### 3.3 OPENVPN

O OPENVPN é capaz de realizar conexões ponto-a-ponto ou servidor-a-hospedeiro entre vários computadores, sendo capaz de estabelecer conexões diretas a estações que estejam por trás de firewalls NAT sem exigir reconfiguração. Ele está licenciado sob a licença GPL, podendo ser utilizado sem gerar custos. Neste estudo ele estará realizando a interconexão entre as estações de trabalho e o smartphone, criando a rota em que os pacotes devam ser trafegados.

Para realizar a configuração da OPENVPN primeiramente deve-se configurar o servidor OpenVpn, que neste caso está na mesma máquina que o servidor Asterisk, configuração dos clientes openvpn Windows e Android que se conectaram ao servidor através de usuário e senha.

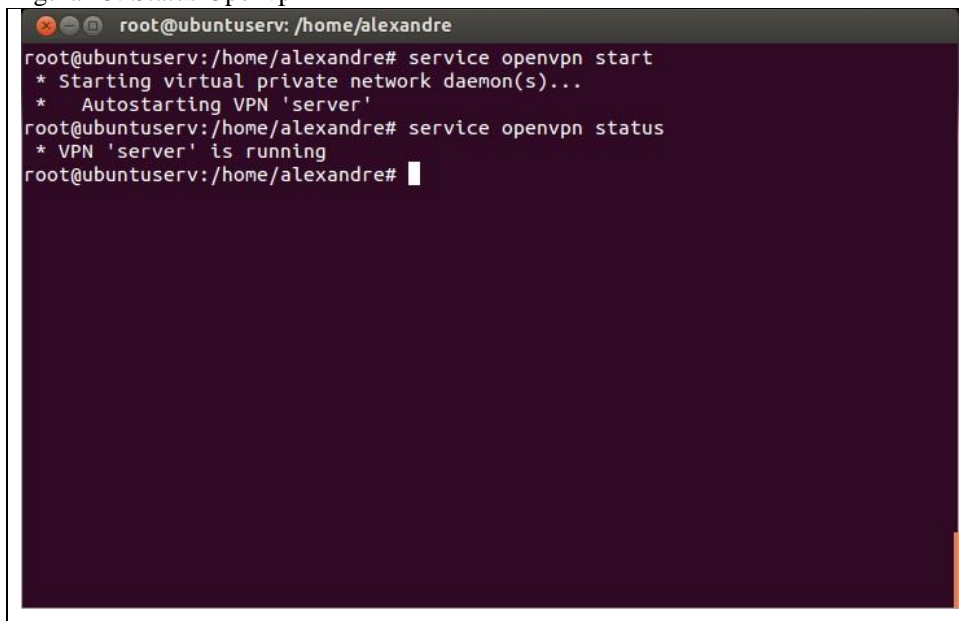


### 3.3.1 Servidor Openvpn

O servidor OpenVpn foi configurado diretamente no servidor Ubuntu.(APÊNDICE A).

A Figura 13 mostra que o serviço está rodando corretamente no servidor.

Figura 13: Status Openvpn

A terminal window with a dark purple background and white text. The prompt is 'root@ubuntuser: /home/alexandre'. The user enters 'service openvpn start', followed by output: '\* Starting virtual private network daemon(s)...', '\* Autostarting VPN 'server''. Then the user enters 'service openvpn status', followed by output: '\* VPN 'server' is running'. The prompt returns to 'root@ubuntuser: /home/alexandre#'.

```
root@ubuntuser: /home/alexandre# service openvpn start
* Starting virtual private network daemon(s)...
* Autostarting VPN 'server'
root@ubuntuser: /home/alexandre# service openvpn status
* VPN 'server' is running
root@ubuntuser: /home/alexandre#
```

Fonte: Elaborado pelo autor.

Com o servidor rodando, é preciso gerar as chaves para que os clientes possam acessar a rede openvpn através da internet, para gerar estas chaves primeiramente deve-se executar o comando:

```
source /etc/openvpn/vars
```

Para que assim as variáveis de ambiente da sessão corrente sejam alimentadas conforme informado no arquivo “vars”, bastando apenas ir confirmando os valores através da tecla Enter. Com as variáveis alimentadas é recomendado para a geração das chaves, utilizar o comando:

```
/etc/openvpn/build-key-pass cliente
```

Pois com este comando o openvpn irá solicitar uma senha ao cliente, garantindo assim uma maior segurança, para o nome do cliente também é recomendado não utilizar espaços ou

caracteres especiais, pois algumas versões podem apresentar algum tipo de problema. Com este comando sempre serão geradas três chaves, sendo elas:

- cliente.csr: Solicitação do novo certificado;
- cliente.crt: Certificado público;
- cliente.key: Chave privada.

Para a realização deste trabalho foram geradas três chaves para os seguintes clientes: alexandreNote – Windows 7; alexandreDesk – Windows XP; alexandreSmart – Android. Cada cliente teve uma cópia do certificado público e chave privada, bem como o certificado público da CA (“ca.crt”) e a chave privada de assinatura de pacotes TLS (“ta.key”). (NERD, 2012).

### **3.3.2 Clientes Openvpn**

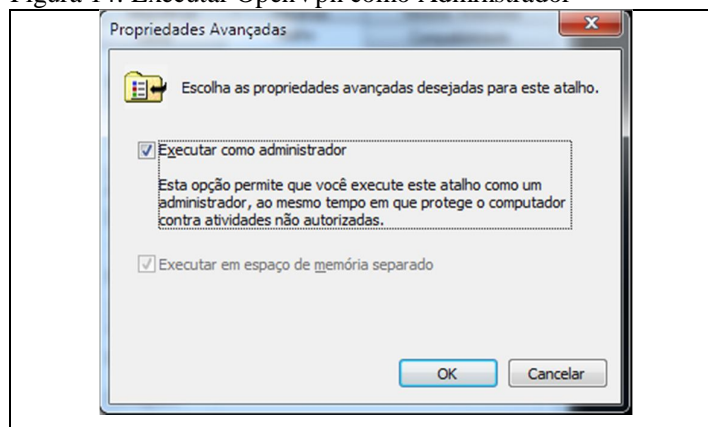
Os clientes openvpn deste trabalho foram três:

- Windows XP;
- Windows 7;
- Android.

Para a instalação do openvpn para os clientes Windows, foi acessado a página de download oficial e escolhido de acordo com a versão do Sistema Operacional. Sua instalação é típica para ambiente Windows, bastando avançar entre as telas que serão apresentadas.

Após a instalação no Windows 7 foi preciso configurar para que o executável seja sempre executado como administrador, isso é importante pois as regras do roteador enviadas do servidor só serão atribuídas se o cliente openvpn possuir privilégios de administrador. Para isso basta clicar com o botão direito do mouse no ícone openvpn e acessar Propriedades/Avançados, marcar a caixa Executar como Administrador, como mostrado na Figura 14.

Figura 14: Executar OpenVpn como Adminstrador



Fonte: Elaborado pelo autor.

Para o Windows XP é preciso que a solução de DNS funcione corretamente, para isso devem-se seguir os seguintes passos:

1. Clicar em Iniciar, Executar..., digitar regedit na caixa de diálogo e então clicar em OK.
2. Navegar até a chave de registro:  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\  
Linkage.
3. No painel da direita, clicar duas vezes no item Bind.
4. Na caixa que se abre selecionar o item "\Device\NdisWanIp", pressionar CTRL+X, clicar no topo da lista de dispositivos, e pressionar CTRL+V. Em outras palavras: o que deve ser feito é passar o item "\Device\NdisWanIp" para o primeiro da lista.
5. Clicar em OK e fechar o Editor do Registro.
6. Reinicializar o computador.

Para a instalação no Android não foi preciso configurações adicionais, bastando apenas instalá-lo pelo Google Play.

O openvpn utiliza apenas um arquivo de configuração, sendo este com a extensão “.ovpn”, para este trabalho este arquivo foi chamado de “openvpn.ovpn”; para que este arquivo possa ser o mesmo para os três clientes, a cópia da chave para cada cliente teve seu nome alterado para “client.crt” e “client.key”; o arquivo de configuração é apresentado abaixo sem os comentários para não ficar muito extenso:

```
client
dev tun
script-security 2
proto udp
remote 192.168.1.100 1194
resolv-retry infinite
nobind
persist-key
persist-tun
mute-replay-warnings
ca ca.crt
cert client.crt
key client.key
ns-cert-type server
tls-auth ta.key 1
cipher AES-128-CBC
comp-lzo
verb 3
```

Neste arquivo vale destacar que ele está usando o protocolo udp para conectar ao servidor openvpn de IP 192.168.1.100 na porta 1194, sendo informada a certificação pública, a do cliente e a chave privada do cliente, bem como a chave privada de assinatura tls. Para os clientes Windows, o arquivo “openvpn.ovpn” mais as respectivas chaves previamente copiadas do servidor e alterados os nomes para client foram ser colocas no diretório “C:\Arquivos de Programa\OpenVpn\config”, para o cliente Android eles precisam apenas estar na mesma pasta, pois o openvpn android permite uma busca para localizar o arquivo de configuração, para isso basta pressionar “menu/Import/Import Profile from SD card” e localizar a pasta onde esta o arquivo “openvpn.ovpn”.

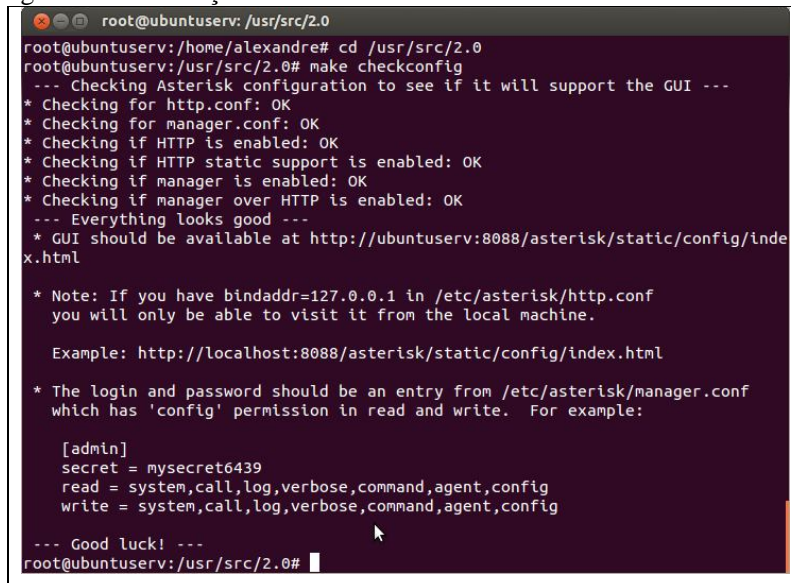
Ao conectar ao openvpn é preciso informar a senha previamente cadastrada no servidor, deste modo todos os clientes estarão todos conectados. (NERD, 2012).

### 3.4 ASTERISK

O servidor Asterisk bem como sua interface gráfica foi configurado diretamente no servidor Ubuntu.(APÊNDICE B).

A Figura 15 mostra que o serviço está rodando corretamente no servidor.

Figura 15: Verificação Asterisk



```
root@ubuntuser: /usr/src/2.0
root@ubuntuser:/home/alexandre# cd /usr/src/2.0
root@ubuntuser:/usr/src/2.0# make checkconfig
--- Checking Asterisk configuration to see if it will support the GUI ---
* Checking for http.conf: OK
* Checking for manager.conf: OK
* Checking if HTTP is enabled: OK
* Checking if HTTP static support is enabled: OK
* Checking if manager is enabled: OK
* Checking if manager over HTTP is enabled: OK
--- Everything looks good ---
* GUI should be available at http://ubuntuser:8088/asterisk/static/config/index.html

* Note: If you have bindaddr=127.0.0.1 in /etc/asterisk/http.conf
you will only be able to visit it from the local machine.

Example: http://localhost:8088/asterisk/static/config/index.html

* The login and password should be an entry from /etc/asterisk/manager.conf
which has 'config' permission in read and write. For example:

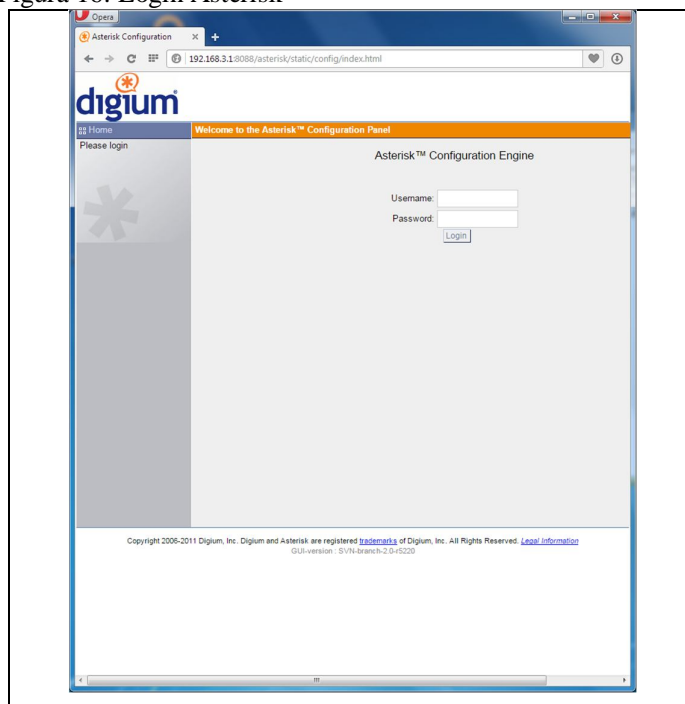
[admin]
secret = mysecret6439
read = system,call,log,verbose,command,agent,config
write = system,call,log,verbose,command,agent,config

--- Good luck! ---
root@ubuntuser:/usr/src/2.0#
```

Fonte: Elaborado pelo autor.

Com a interface gráfica instalada pode-se acessar o servidor via navegador, isso pode ser feito utilizando o IP do próprio servidor, que para este trabalho foi 192.168.1.100 ou o IP que foi atribuído a openvpn, que neste trabalho foi 192.168.3.1 seguido da porta configurada no arquivo “http.conf”, como é demonstrado na Figura 16.

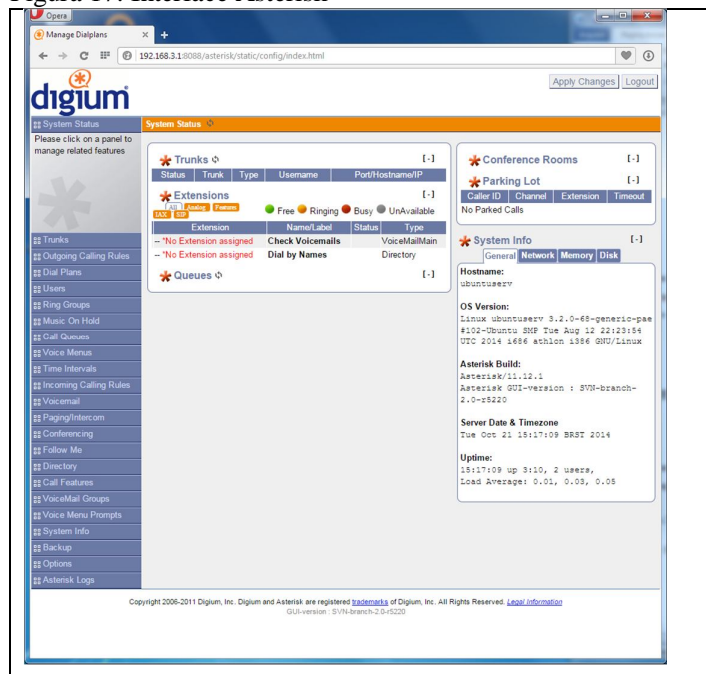
Figura 16: Login Asterisk



Fonte: Elaborado pelo autor.

Para acessar a página de configuração é preciso primeiro logar, com usuário e senha que foram definidos no arquivo “manager.conf” na chave “[admin]” onde o nome da chave é o username, e a senha é o parâmetro informado em secret. Como demonstra a Figura 17.

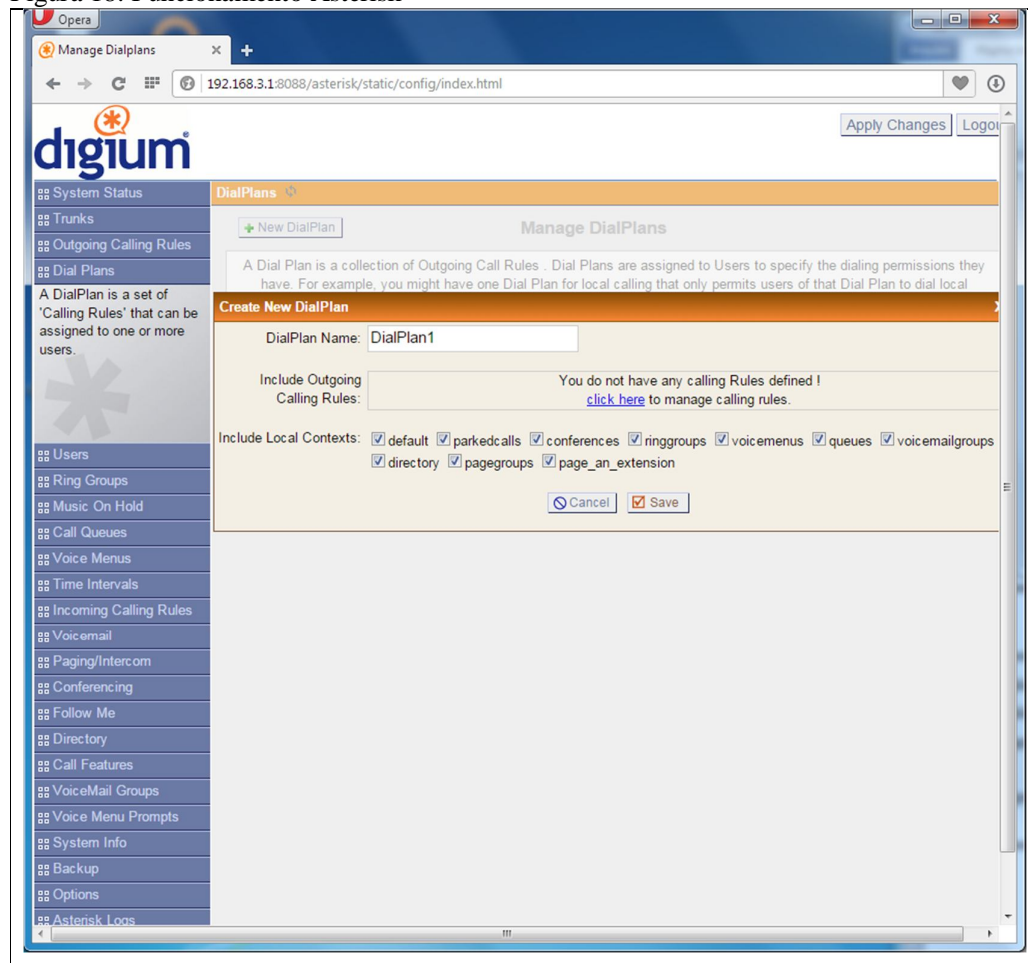
Figura 17: Interface Asterisk



Fonte: Elaborado pelo autor.

O servidor Asterisk ainda não possui nenhuma configuração, para que as estações possam realizar as ligações entre si, primeiramente é preciso configurar um plano de discagem, para isso basta acessar o “Dial Plans” no menu esquerdo e clicar no botão “New DialPlan”, uma tela igual a Figura 18 será apresentada.

Figura 18: Funcionamento Asterisk



Fonte: Elaborado pelo autor.

Como o foco deste trabalho é o monitoramento das chamadas, será configurado apenas o nome do plano, que para este trabalho foi definido como “plano1” mantendo as outras informações com os valores padrões.

Tendo um plano de discagem é preciso ter usuários cadastrados no sistema, para que os Softphones possam se conectar e conversar entre si, para isso acessar o item “Users” do menu a esquerda e clicar no botão “Create New User”, a tela que abrirá será igual a da Figura 19.

Figura 19: Cadastrar novo Usuário Asterisk

The screenshot shows the Asterisk web interface in a browser window. The main content area is titled "User Extensions on PBX" and contains a "Create New User" form. The form is divided into several sections:

- General:** Extension: 6000, CallerID Name: [empty], DialPlan: plano1, Internal CallerID: 6000, CallerID Number: [empty].
- Enable Voicemail for this User:**  Enable Voicemail for this User. VoiceMail Access PIN code: [empty], Email Address: [empty].
- Technology:**  SIP,  IAX, Analog Station: None, flash: 750, rxflash: 1250. Codec Preference: First: u-law, Second: GSM, Third: None, Fourth: None, Fifth: None.
- VoIP Settings:** MAC Address: [empty], Line Number: 1, LineKeys: 1, SIP/IAX Password: [empty], IAX: Require Call Token: [empty], IAX: Max Call Numbers: [empty], NAT:  Can Reinvite:  DTMF Mode: RFC2833, insecure: no.
- Other Options:**  3-Way Calling (analog),  In Directory,  Call Waiting (analog),  ADA User,  Is Agent, Pickup Group: 1.

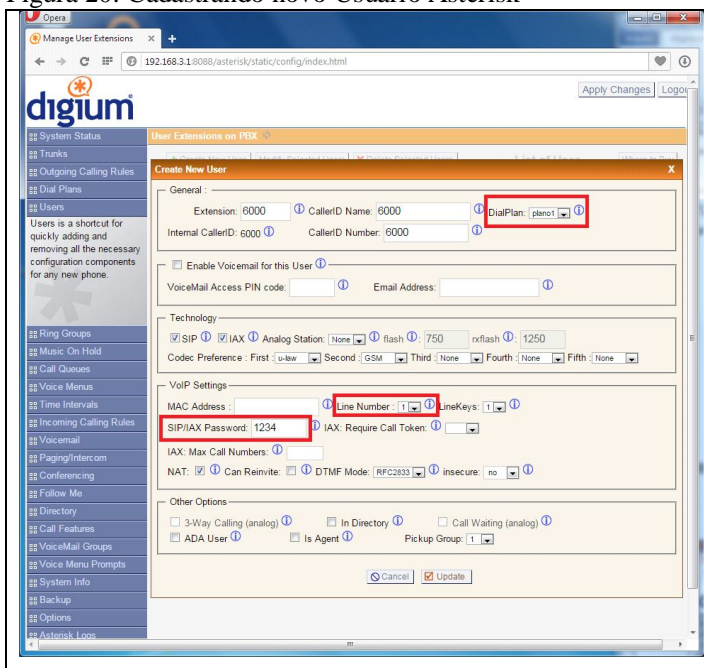
Buttons for "Cancel" and "Update" are located at the bottom of the form.

Fonte: Elaborado pelo autor.

Embora o sistema permita que seja cadastrado um nome, é recomendado utilizar apenas números para a identificação dos usuários, deste modo evitam-se confusões. Para cadastrar um novo usuário bastará informar os seguintes campos como mostrado na Figura 20. O campo “Line Number” deve ser diferente para cada novo usuário e o campo “SIP/IAX Password” é necessário para que assim o softphone apenas se conecte se tiver conhecimento da senha.



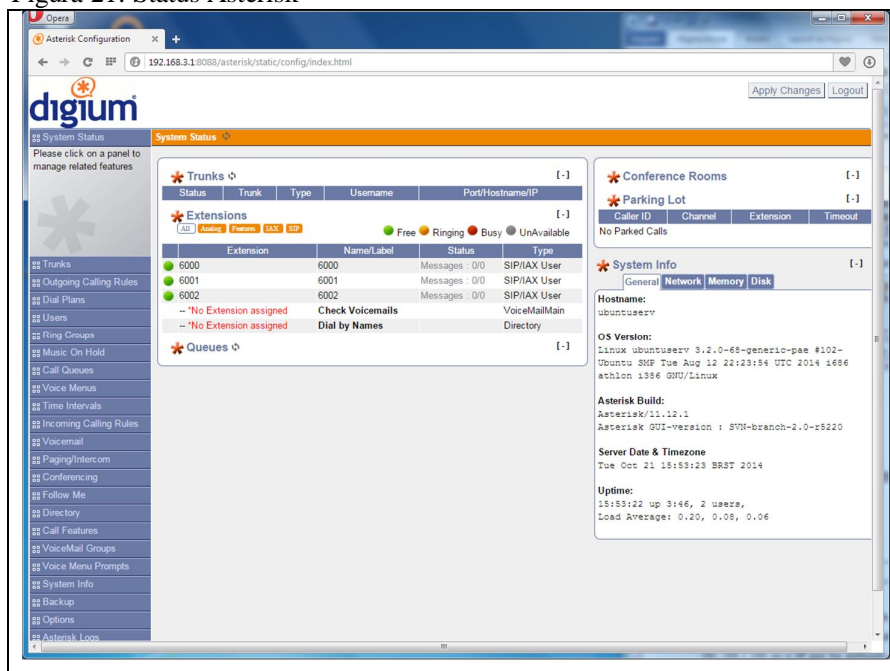
Figura 20: Cadastrando novo Usuário Asterisk



Fonte: Elaborado pelo autor.

Com o plano de discagem e os usuários cadastrados, a tela inicial do “System Status” estará como mostra a Figura 21. Com isso o Asterisk está pronto para realizar a chamadas entre os clientes. (MESTRE, 2009).

Figura 21: Status Asterisk



Fonte: Elaborado pelo autor.

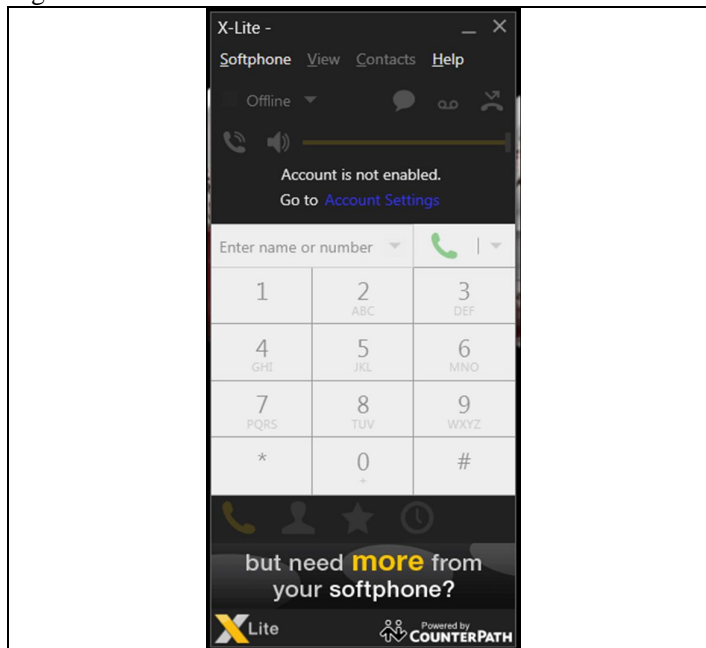
### 3.5 X-LITE

O X-Lite foi instalado nas duas estações, este software foi escolhido por possuir uma versão GPL, estando disponível para as plataformas 32 e 64 bits e por não possuir uma rede própria, tornando-o um software mais versátil, contando também com vários recursos, como:

- Duas linhas;
- Opção Mute – sem som;
- Remarcar;
- Colocar em espera;
- Opção Dnd (Do not disturb) – Não incomodar;
- Histórico de chamadas – recebidas, efetuadas e perdidas;
- Reencaminhamento de chamadas;
- Gravação de chamadas;
- Suporte de codecs.

O X-Lite possui uma instalação típica para plataforma Windows, bastando avançar entre as telas até ser concluído, após sua instalação ele apresentará a seguinte interface apresentada na Figura 22.

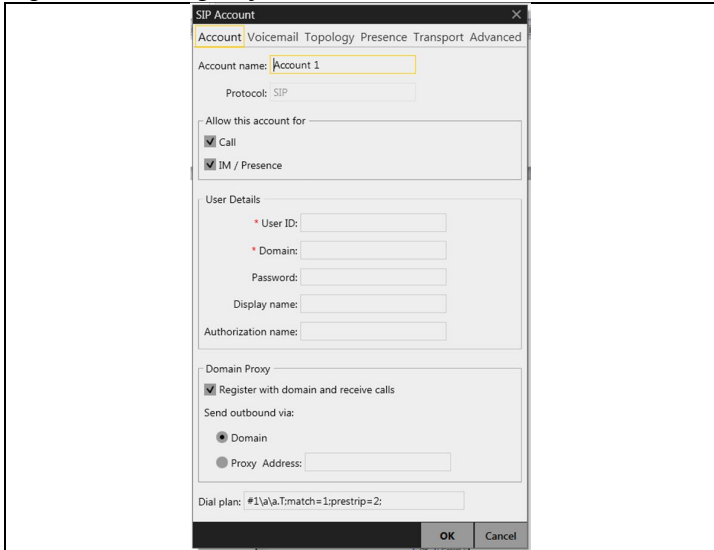
Figura 22 - X-Lite 4.0 Interface



Fonte: Counter Path (2014).

Como é possível observar, para sua utilização requer a configuração de uma conta. Esta conta deverá conter os dados do servidor de telefonia, permitindo assim que ele realize e receba chamadas, a tela de configuração da conta é apresentada como a Figura 23.

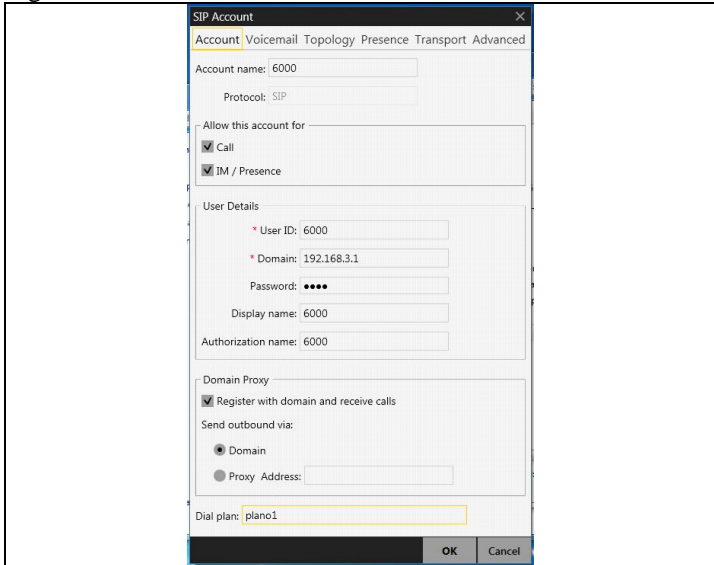
Figura 23 - Configuração Nova Conta X-Lite



Fonte: Counter Path (2014).

Para a realização dos testes foi preciso realizar a seguinte configuração, de acordo com o ramal que foi configurado previamente no servidor, como demonstrado na Figura 24.

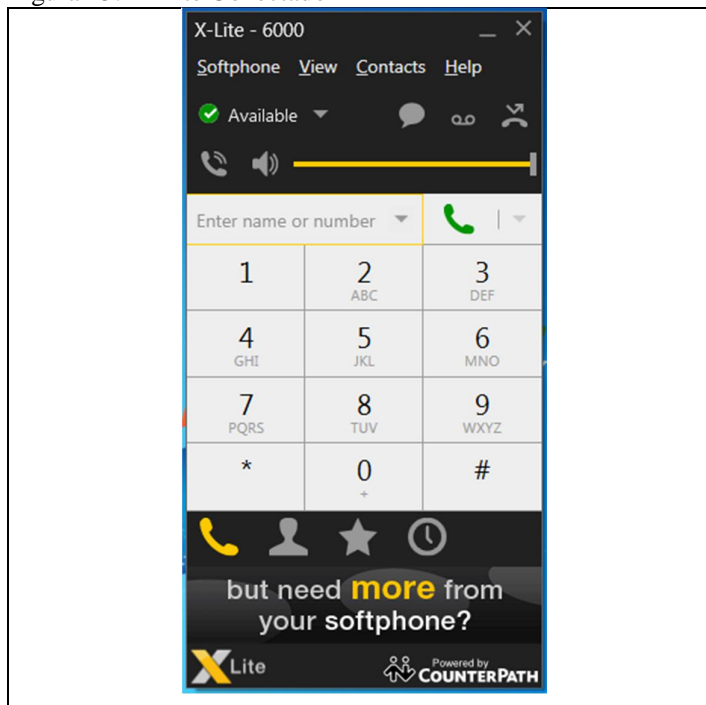
Figura 24: Dados conta X-Lite



Fonte: Counter Path (2014).

Após a configuração é possível notar que o softphone estará pronto para realizar e receber chamadas, como demonstrado na Figura 25.

Figura 25: X-Lite Conectado

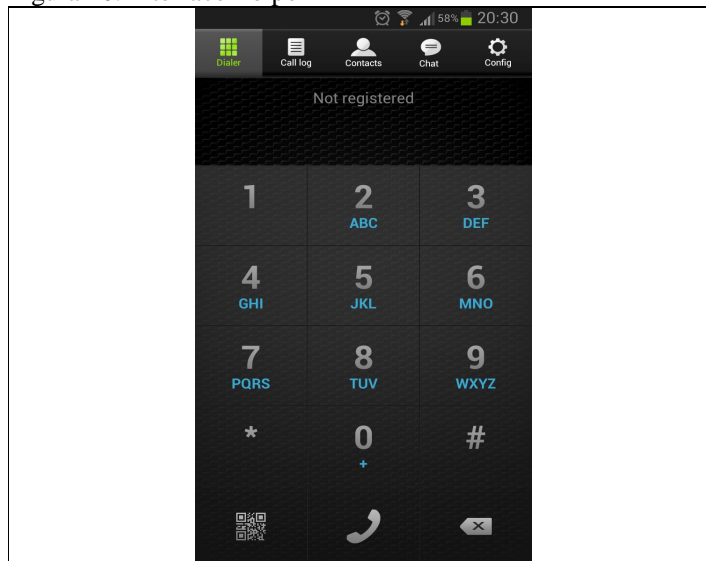


Fonte: Counter Path (2014).

### 3.6 ZOIPER

Assim como o X-Lite o Zoiper é um Softphone muito versátil, por ele ser mais leve que o X-Lite e possuir uma versão para Android, ele foi instalado tanto na máquina que está rodando o Windows XP, bem como no SmartPhone Samsung Galaxy S3. Sua instalação no Windows é muito semelhante ao X-Lite, bastando avançar entre as telas, para instalá-lo no Android, basta acessar o Google Play, e realizar o Download. A Figura 26 apresenta sua interface no Android.

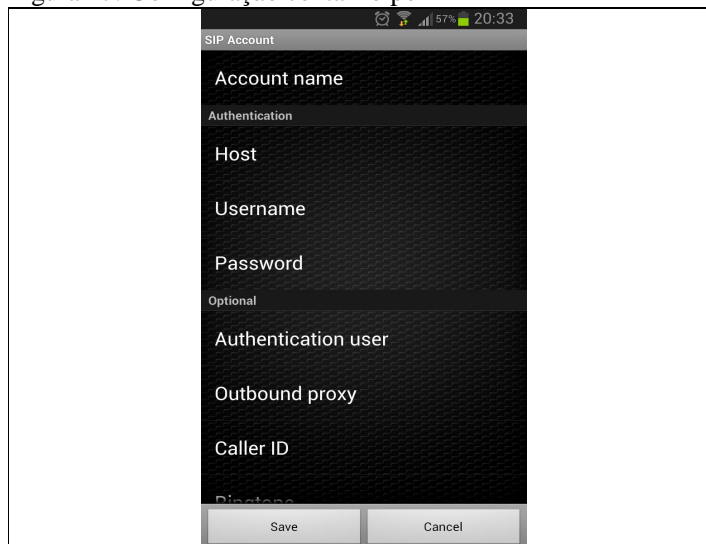
Figura 26: Interface Zoiper



Fonte: Zoiper (2014).

Como no X-Lite, no Zoiper é preciso configurar uma conta que já esteja previamente configurada no servidor Asterisk, a tela de configuração da conta no Zoiper é apresentada na Figura 27.

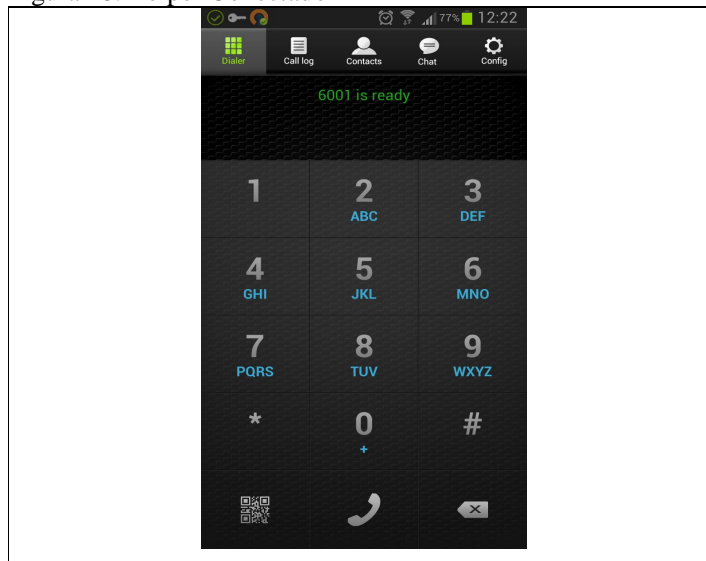
Figura 27: Configuração conta Zoiper



Fonte: Zoiper (2014).

Após a conta configurada é possível notar que o Zoiper estará pronto para realizar e receber chamadas, como mostrado na Figura 28.

Figura 28: Zoiper Conectado



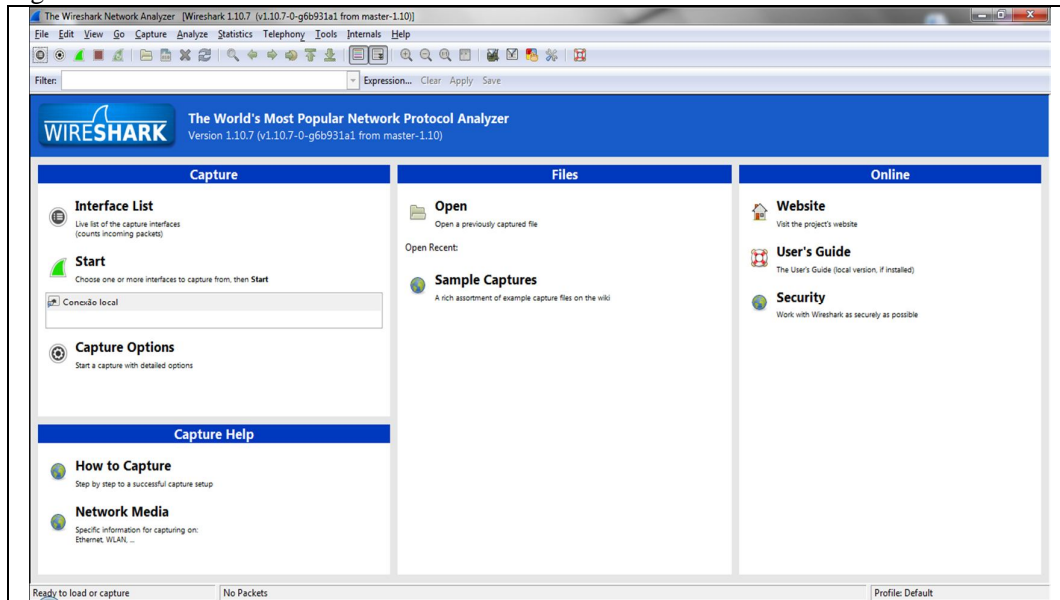
Fonte: Zoiper (2014).

### 3.7 WIRESHARK

Para ser realizada a captura dos dados trafegados na rede, foi utilizado o software Wireshark, pois ele é um dos principais analisadores de tráfego atualmente, sendo amplamente utilizado tanto por empresas quanto por instituições educacionais. Outro ponto a seu favor, é que o software está sob a licença GPL, permitindo sua utilização sem gerar custos com licença.

Ele foi instalado apenas no notebook, pois a demanda de pacotes é muito grande e a máquina que estava rodando o Windows XP é mais modesta, podendo não suportar a captura. Como os pacotes transmitidos sempre serão capturados, para o estudo não faz diferença que seja em apenas uma máquina. Sua instalação é simples, basta ir avançando entre as telas, depois de instalado ao executar o software será apresentada como a Figura 29:

Figura 29 - Interface Wireshark



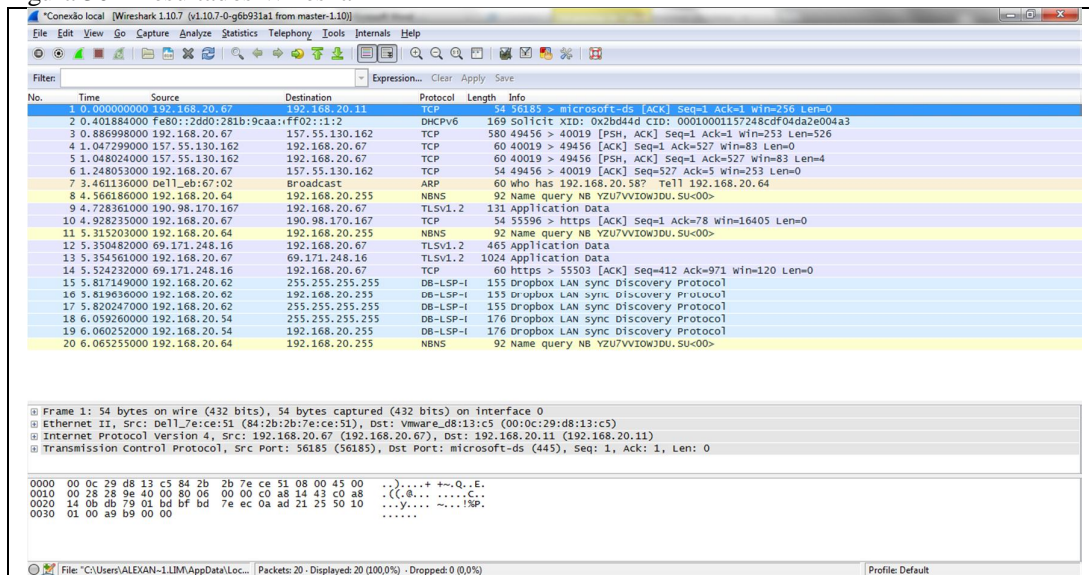
Fonte: Whireshark (2014).

Apesar da interface intuitiva do Wireshark, ele nos possibilita grandes recursos, como:

- Inspeção profunda de centenas de protocolos;
- Pacote de motor de busca padrão;
- Multi plataforma;
- Os dados da rede capturados podem ser registrados em uma GUI;
- Análise de Rich VoIP;
- Lê e escreve em diversos formatos de arquivos;
- Os dados podem ser lidos em Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB;

Na Figura 30 segue um exemplo de captura realizado pelo wireshark.

Figura 30 - Resultados Wireshark



Fonte: Wireshark (2014).

Para este estudo as ligações que tiveram os pacotes capturados seguiram a regra:

- Cada captura teve a duração de exatos três minutos;
- Para cada ligação utilizou-se o mesmo áudio, sendo este uma música que supera os três minutos, para que a captura seja sempre interrompida no mesmo ponto;
- Foram testados os seguintes modos de criptografia: sem criptografia, WEP, WPA, WPA2-PSK;
- Para cada tipo de criptografia foram testados os seguintes canais: 1, 6 e 11.

### 3.8 RESULTADOS

Com as ligações efetuadas e seus pacotes capturados, o wireshark apresentou os seguintes resultados, sendo o número total de pacotes trafegados, tempo entre primeiro e ultimo pacotes e algumas médias relevantes ao estudo, evidenciados nas Figuras 31, 32, 33 e 34.



Figura 31 - Resultados Sem Criptografia

Sem Criptografia	Canais		
	1	6	11
PACOTES	18336	18481	18528
SEG. ENTRE PRIMEIRO E ÚLTIMO PACOTE	179,251	179,102	179,746
MÉDIA DE PACOTES P/ SEG	102,292	103,187	103,079
MÉDIA TAMANHO DOS PACOTES BYTES	283	283	283
BYTES	5197573	5223509	5242126
MÉDIA BYTES P/ SEG	28996,065	29165,011	29164,089
MÉDIA MB P/ SEG	0,232	0,233	0,233

Fonte: Elaborado pelo autor.

Figura 32 - Resultados Criptografia WEP

WEP	Canais		
	1	6	11
PACOTES	18115	18573	18493
SEG. ENTRE PRIMEIRO E ÚLTIMO PACOTE	178,567	178,983	179,277
MÉDIA DE PACOTES P/ SEG	101,446	103,770	103,153
MÉDIA TAMANHO DOS PACOTES BYTES	283	282	281
BYTES	5127882	5228820	5203338
MÉDIA BYTES P/ SEG	28716,783	29214,129	29023,994
MÉDIA MB P/ SEG	0,230	0,234	0,232

Fonte: Elaborado pelo autor.

Figura 33 - Resultados Criptografia WPA

WPA	Canais		
	1	6	11
PACOTES	18407	18399	18612
SEG. ENTRE PRIMEIRO E ÚLTIMO PACOTE	179,767	179,927	179,996
MÉDIA DE PACOTES P/ SEG	102,394	102,258	103,402
MÉDIA TAMANHO DOS PACOTES BYTES	284	284	283
BYTES	5231074	5228887	5262959
MÉDIA BYTES P/ SEG	29099,239	29061,118	23239,362
MÉDIA MB P/ SEG	0,233	0,232	0,234

Fonte: Elaborado pelo autor.

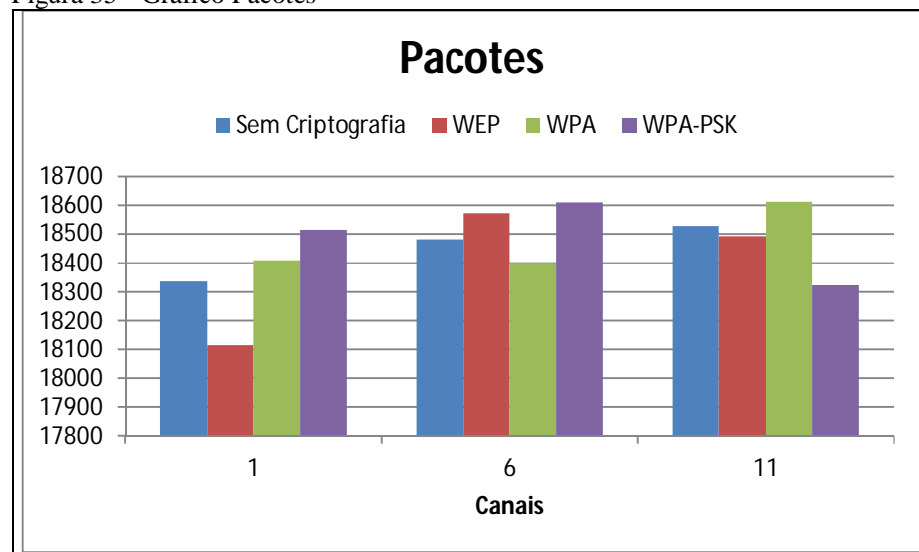
Figura 34 - Resultados Criptografia WPA2-PSK

WPA-PSK	Canais		
	1	6	11
PACOTES	18513	18609	18323
SEG. ENTRE PRIMEIRO E ÚLTIMO PACOTE	179,445	179,513	179,047
MÉDIA DE PACOTES P/ SEG	103,168	103,664	102,336
MÉDIA TAMANHO DOS PACOTES BYTES	283	282	283
BYTES	5240547	5254317	5209024
MÉDIA BYTES P/ SEG	29204,119	29269,801	29093,094
MÉDIA MB P/ SEG	0,234	0,234	0,233

Fonte: Elaborado pelo autor.

Para uma melhor análise alguns gráficos foram gerados, como o número total de pacotes trafegados em cada ligação nos diferentes canais, apresentado na Figura 35.

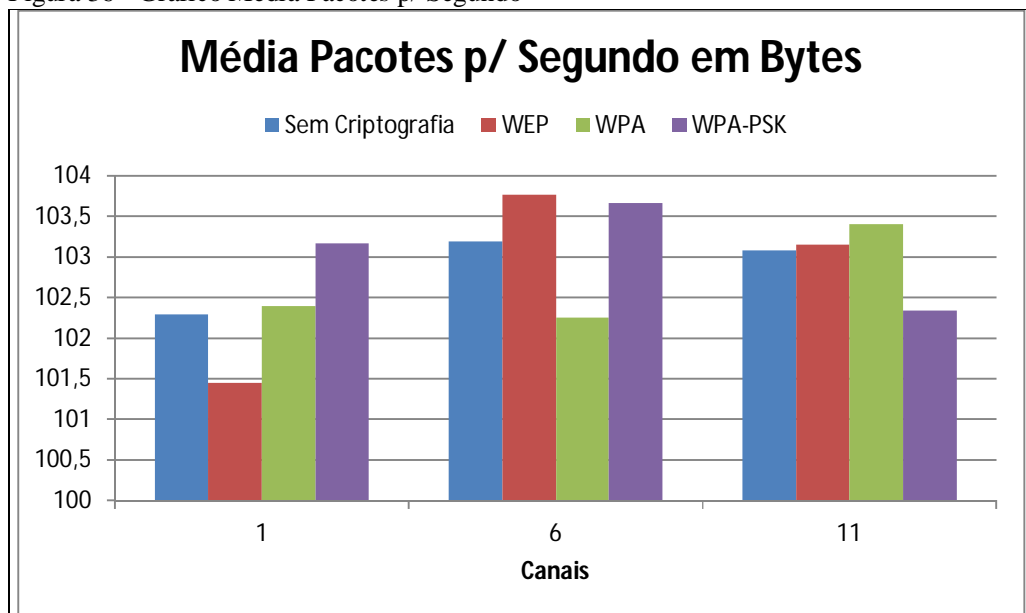
Figura 35 - Gráfico Pacotes



Fonte: Elaborado pelo autor.

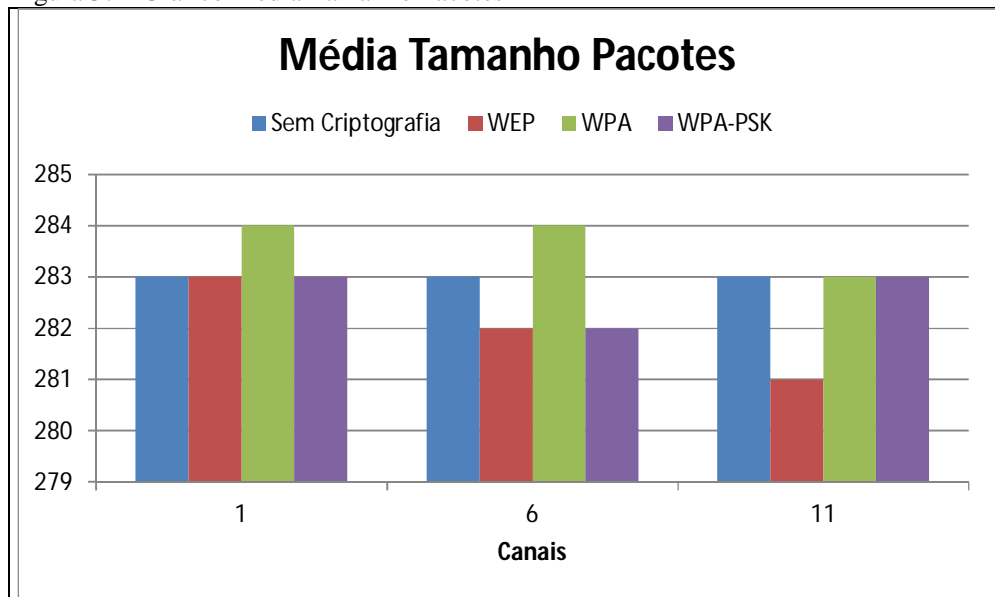
A média de quantos pacotes foram trafegados por segundo, mostrados na Figura 36, bem como o tamanho médio de cada pacote, mostrado na Figura 37.

Figura 36 - Gráfico Média Pacotes p/ Segundo



Fonte: Elaborado pelo autor.

Figura 37 - Gráfico Média Tamanho Pacotes



Fonte: Elaborado pelo autor.

## 4 CONSIDERAÇÕES FINAIS

A análise levou em consideração o desempenho da rede sem fio durante as chamadas. Para que os testes fossem mais precisos, foram utilizados o mesmo tempo e a mesma faixa de áudio. Foi efetuada uma chamada para cada tipo de criptografia e canal.

Com os dados obtidos do Wireshark foram gerados gráficos comparativos, com eles é possível observar que não há diferenças muito significativas para a troca dos tipos de criptografia e canais.

Com este estudo pode-se notar que a não utilização de criptografia em redes sem fio não contribuirá com o desempenho da rede como um todo, e com base nele, recomenda-se o uso da criptografia WPA-PSK, pois seu impacto a rede mostrou-se na média das demais, e como ela é tida como a mais segura, recomenda-se seu uso, pois seu impacto é pequeno em relação ao custo benefício.

O estudo mostra também que dependendo do canal escolhido pode-se ter um ganho no desempenho da rede, que neste caso é mostrado ao utilizar o canal 11, que está utilizando menos recursos que o canal 1 ou 6, e com a mesma informação trafegada, com base nestes resultados é possível afirmar que a melhor utilização para ligações VOIP em uma rede sem fio com WDS é a criptografia WPA-PSK operando no canal 11.

### 4.1 TRABALHOS FUTUROS

Como não há muitas pesquisas realizadas sobre o WDS, podem-se sugerir alguns pontos de estudo.

Um deles seria a realização deste trabalho utilizando no servidor outro sistema operacional, como Windows ou Solaris.

Também se pode sugerir realizar três capturas por chamada, fazendo-se uma média entre elas para a obtenção de resultados mais precisos.

Outro estudo interessante seria na utilização de mais um ponto para o WDS, podendo assim observar qual o impacto causará a adição deste ponto à rede sem fio.

## REFERÊNCIAS

- ALBUQUERQUE, S. Aprenda a Amplificar o Sinal de Redes Wireless Usando o WDS. **Canal Tech**, 2014. Disponível em: <http://canaltech.com.br/tutorial/redes/Aprenda-a-amplificar-o-sinal-de-redes-wireless-usando-o-wds/>> Acesso em: 14 maio 2014.
- ASTERISK, **Asterisk**, 2014. Disponível em: <http://www.asterisk.org/downloads>> Acesso em: 14 maio 2014.
- ASTERISK. **An Open Source PBX and telephony toolkit**. 2006. Disponível em: <<http://www.asterisk.org/>>. Acesso em: 14 maio 2014.
- BARBOSA, G. F. Implementação de uma Estrutura de Rede Usando o Modelo Hierárquico. **Repositório de Outras Coleções Abertas**, 2012. Disponível em: [http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/1826/1/CT\\_GESER\\_II\\_2012\\_03.pdf](http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/1826/1/CT_GESER_II_2012_03.pdf) > Acesso em: 14 maio 2014.
- BARROZO, L. L. Segurança nas Redes: Wireless e Wimax. **Repositório Institucional Univem** , 2009. Disponível em: <http://aberto.univem.edu.br/bitstream/handle/11077/285/Seguran%C3%A7a%20nas%20redes%20sem%20fio%3a%20Wireless%20e%20Wimax.pdf?sequence=1>> Acesso em: 14 maio 2014.
- COUNTERPATH, **X-Lite**, 2014. Disponível em: <http://www.counterpath.com/x-lite-for-windows-download.html>> Acesso 14 maio 2014.
- FERRARI, S. R. WireShark. **Viva o Linux**, 2008. Disponível em: <http://www.vivaolinux.com.br/artigo/Wireshark-Artigo> > Acesso em: 14 maio 2014.
- FERREIRA, A. T. WDS – Vários Roteadores u Aps, numa única rede!. **Revolução Linux**, 2010. Disponível em: <http://revolucaolinux.blogspot.com.br/2010/07/wds-varios-roteadores-ou-aps-numa-unica.html>> Acesso em: 14 maio 2014.
- GONÇALVES, F. E. A. **Asterisk PBX: Guia de Configuração**. V. Office Networks, 2005.
- FRANCISCO, P. K. **Asterisk: Como instalar manualmente em seu Linux**. 2013. Disponível em: <http://gerencievocemesmo.com.br/site/?p=449>>. Acesso em: 25 outubro 2014.
- H.323. ITU-T Recommendation H.323. **Telecommunication Standardization Sector of Itu – Packet Based Multimedia Communications Systems**. 2006. Disponível em: <http://www.itut.int.com/>>. Acesso em: 14 maio 2014.
- HEMEL, Armijn. Tubarão Multiuso. **Linux Magazine Online**, 2007. Disponível em: [http://www.linuxnewmedia.com.br/images/uploads/mags/lm/articles/LM32\\_wireshark.pdf](http://www.linuxnewmedia.com.br/images/uploads/mags/lm/articles/LM32_wireshark.pdf)> Acesso em: 14 maio 2014.

LEVANDOSKI, F. et al. OpenVPN. **Fausto Levandoski**, 2010. Disponível em: [http://www.faustolevandoski.com.br/downloads/Artigo\\_OpenVPN.pdf](http://www.faustolevandoski.com.br/downloads/Artigo_OpenVPN.pdf)> Acesso em: 14 maio 2014.

LINHARES, A. G.; GONÇALVES, P. A. S. Uma Análise dos Mecanismos de Segurança de Redes IEEE 802.11: WEP, WPA, WPA2 e IEEE 802.11w, **Centro de Informática UFPE**, S.d.. Disponível em: <http://www.cin.ufpe.br/~pasg/gpublications/LiGo06.pdf>> Acesso 14 maio 2014.

LINKSYS. Configurando segurança sem fio WEP, WPA ou WPA2 em um roteador. **Linksys**, 2014. Disponível em: [http://kb.linksys.com/Linksys/GetArticle.aspx?docid=4cb4233a9ab24a5188470e95d880eb7e\\_20202.xml&pid=28](http://kb.linksys.com/Linksys/GetArticle.aspx?docid=4cb4233a9ab24a5188470e95d880eb7e_20202.xml&pid=28)> Acesso em: 14 maio 2014.

LUCAS, A. S. Avaliação de Desempenho do Protocolo WEP em Redes Sem Fio AD HOC Usando um Simulador de Redes. **Repositório Institucional Univem**, 2006. Disponível em: <http://aberto.univem.edu.br/bitstream/handle/11077/276/Avalia%C3%A7%C3%A3o%20de%20desempenho%20do%20protocolo%20WEP%20em%20redes%20sem%20fio%20Ad%20Hoc%20usando%20um%20simulador%20de%20redes.pdf?sequence=1> > Acesso em: 14 maio 2014.

MARTINS, E. O Que é VPN. **TecMundo**, 2009. Disponível em: <http://www.tecmundo.com.br/1427-o-que-e-vpn-.htm>> Acesso em: 14 maio 2014.

MESTRE, A. **Asterisk - Instalação e configuração no Debian Lenny**. 2009. Disponível em: < <http://www.vivaolinux.com.br/artigo/Asterisk-Instalacao-e-configuracao-no-Debian-Lenny?pagina=3/>>. Acesso em: 14 maio 2014.

MITZCUN, J. F. Implantação de uma Rede Virtual Privada (VPN) na Procuradoria da República no RN. **Biblioteca Digital do MPF**, 2007. Disponível em: [http://bibliotecadigital.mpf.mp.br/xmlui/bitstream/handle/123456789/36273/Mitzcun\\_Joao\\_i\\_mplantacao\\_rede\\_virtual\\_39\\_pgs.pdf?sequence=1](http://bibliotecadigital.mpf.mp.br/xmlui/bitstream/handle/123456789/36273/Mitzcun_Joao_i_mplantacao_rede_virtual_39_pgs.pdf?sequence=1) > Acesso em: 14 maio 2014.

MORIMOTO, C. E. Expandindo a rede Wi-Fi com Pontos de Acesso Adicionais. **Guia do Hardware**, 2011. Disponível em: <http://www.hardware.com.br/tutoriais/expandindo-wifi/wds-outras-opcoes.html>> Acesso em: 14 maio 2014.

NERD. **OpenVPN – Servidor Ubuntu e Clientes Windows e Linux**, 2012. Disponível em: <http://blogdonerd.com.br/2012/06/openvpn-servidor-ubuntu-e-clientes-windows-e-linux/>> Acesso em: 25 outubro 2014.

O modelo TCP/IP. **TechNet**, [2014?]. Disponível em: [http://technet.microsoft.com/pt-br/library/cc786900\(v=ws.10\).aspx](http://technet.microsoft.com/pt-br/library/cc786900(v=ws.10).aspx)> Acesso em: 14 maio 2014.

PEREIRA JUNIOR, C. A. C. V. ; BRABO, G. S.; AMORAS, R. A. S. Segurança em Redes Wireless Padrão IEEE 802.11b: Protocolos WEP, WPA e Análise de Desempenho. **Prof. Marcio R.G. de Vazzi**, 2004. Disponível em: [http://www.vazzi.com.br/moodle/pluginfile.php/705/mod\\_resource/content/1/Atividade\\_1\\_-\\_seguranca\\_em\\_redes\\_wireless.pdf](http://www.vazzi.com.br/moodle/pluginfile.php/705/mod_resource/content/1/Atividade_1_-_seguranca_em_redes_wireless.pdf) > Acesso em: 14 maio 2014.

PETROCELLO, M. Montando uma rede WDS com Roteadores ou APs, em uma única rede Wirelles. **Maryell Petrocello**, 2011. Disponível em: <http://maryell.blog.com/2011/04/01/wds-varios-roteadores-ou-aps-em-uma-unica-rede-wireless/>> Acesso em: 14 maio 2014.

PINHEIRO, J. M. S. Redes de Telefonia IP – 2ª Parte. **Projeto de Redes**, 2006. Disponível em: [http://www.projetederedes.com.br/tutoriais/tutorial\\_redes\\_telefonia\\_ip\\_02.php](http://www.projetederedes.com.br/tutoriais/tutorial_redes_telefonia_ip_02.php)> Acesso em: 14 maio 2014.

ROCHA, J. W. V. Redes WLAN de Alta Velocidade I: Características. **Núcleo de Tecnologias Interativas de Aprendizagem**, 2006. Disponível em: <http://www3.iesampa.edu.br/ojs/index.php/TELECOM/article/viewFile/687/561>> Acesso em: 14 maio 2014.

ROSA, R. H. Ferramenta para Desenvolvimento de Planos de Discagem no Asterisk. **Universidade Federal de Santa Catarina**, 2007. [https://projetos.inf.ufsc.br/arquivos\\_projetos/projeto\\_753/Projetos%20II%20-%20Richard%20Hobold.pdf](https://projetos.inf.ufsc.br/arquivos_projetos/projeto_753/Projetos%20II%20-%20Richard%20Hobold.pdf)> Acesso em: 14 maio 2014.

ROSSI, M. A. G.; FRANZIN O. **VPN – Virtual Private Network (Rede Pública Virtual)**. GPr Sistemas/ASP Systems, 2000.

SHALDERS, F. Voip: O Que É? Como Funciona?. **Nimbuzz**, 2010. Disponível em: <http://brasil.blog.nimbuzz.com/2010/08/02/voip-o-que-e-como-funciona/>> Acesso em: 14 maio 2014.

SOUZA, A. G. Spanning Tree Protocol. **Sistemas de Informação**, 2009. Disponível em: <http://www.si.lopesgazzani.com.br/TFC/monografias/Monografia%20Alessandro.pdf> > Acesso em: 14 maio 2014.

TANENBAUM, A. S., WETHERALL, D. **Redes de Computadores**. 5. ed. São Paulo: Pearson Education do Brasil, 2011.

TANENBAUM, A. **Redes de Computadores**. 4. ed. Rio de Janeiro: Campus/Elsevier, 2003.

TORRES, Gabriel. Como o protocolo TCP/IP funciona. **Clube do Hardware**, 2007. Disponível em: <http://www.clubedohardware.com.br/artigos/1351> > Acesso em: 14 maio 2014.

UBUNTU, Comunity. Wireless VPN. **Ubuntu Wiki**, 2008. Disponível em: <http://wiki.ubuntu-br.org/WirelessVPN>> Acesso em: 14 maio 2014.

WEBER, R. F. **Criptografia Contemporânea**. Porto Alegre: Instituto de Informática UFRGS, 1998.

What is VPN. **NetGear**, [2010?]. Disponível em: [http://kb.netgear.com/app/answers/detail/a\\_id/1128/~/what-is-vpn-\(virtual-private-networking\)%3F](http://kb.netgear.com/app/answers/detail/a_id/1128/~/what-is-vpn-(virtual-private-networking)%3F)> Acesso em: 14 maio 2014.

WIRESHARK, **Wireshark**, 2014. Disponível em: <http://www.wireshark.org/download.html>> Acesso em: 14 maio 2014.

## APÊNDICE A - CONFIGURAÇÃO SERVIDOR OPENVPN UBUNTU

Para a instalação primeiramente deve-se logar no terminal com acesso root (administrador) para isso basta inserir o seguinte comando seguido da senha:

```
sudo su
```

É preciso atualizar os repositórios de dados do servidor, isso é feito com o seguinte comando:

```
apt-get update;
```

Após a atualização será de fato instalado o serviço de openvpn com o seguinte comando:

```
apt-get install openvpn
```

Agora será preciso copiar os arquivos de exemplo de configuração para a pasta openvpn, para isso utiliza-se o seguinte comando:

```
cp /usr/share/doc/openvpn/examples/easy-rsa/2.0/* /etc/openvpn
```

É recomendável realizar um backup de segurança do arquivo “openssl-1.0.0.cnf” localizado no diretório “/etc/openvpn/”; para isso será utilizado o seguinte comando:

```
cp /etc/openvpn/openssl-1.0.0.cnf /etc/openvpn/openssl.cnf
```

O próximo passo será editar o arquivo “vars” localizado no diretório “/etc/openvpn”, ajustando as últimas linhas iniciadas por KEY, para que assim o ambiente possa ser refletido, estes parâmetros ficaram com valores:

```
export KEY_COUNTRY="BR"  
export KEY_PROVINCE="SP"  
export KEY_CITY="Pederneiras"  
export KEY_ORG="Trabalho Conclusão de Curso"  
export KEY_EMAIL="alexandre87ml@gmail.com"  
export KEY_CN="ubuntuserv"  
export KEY_NAME="Alexandre Lima"  
export KEY_OU="TCC"
```

```
/etc/openvpn/vars
```

Agora bastará compilar a openvpn para que ela funcione corretamente, os parâmetros informados no arquivo “vars” serão apresentados, bastando confirma-los com a tecla Enter. Para compilar primeiramente deve-se entrar no diretório, e executar os comandos:

```
cd /etc/openvpn  
source /etc/openvpn/vars
```

Deste modo os parâmetros do arquivo “vars” serão reconhecidos, depois o comando:



```
/etc/openvpn/clean-all
```

Para que seja limpo para a compilação, em seguida:

```
/etc/openvpn/build-ca
```

```
/etc/openvpn/build-dh
```

Com estes comandos a pasta “keys” será criada dentro do “/etc/openvpn” nesta pasta existirão cinco arquivos que são referentes a nova certificação criada:

- ca.crt: Certificação pública da CA;
- ca.key: Chave privada da CA;
- dh1024.pem: Parâmetros para a troca de chaves;
- index: Controle das chaves geradas pela CA;
- serial: Controle de número serial das chaves geradas pela CA.

Para que o openvpn funcione corretamente é preciso gerar um certificado para o servidor para isso será utilizado o seguinte comando:

```
/etc/openvpn/build-key-server server
```

Novamente os parâmetros do arquivo “vars” serão exibidos, bastando ir os confirmando, ao término da confirmação, duas novas chaves serão geradas na pasta “keys” sendo elas, “server.crt” e “server.key”. (NERD, 2012).

Para realizar a configuração do openvpn é preciso ter um arquivo no diretório “/etc/openvpn” com a extensão “.conf” sendo permitido ter mais de um serviço openvpn em outras portas, desde que cada serviço possua um arquivo de configuração. O arquivo “.conf” neste estudo foi denominado por “server.conf”, este arquivo é apresentado abaixo:

```
local 192.168.1.100
port 1194
proto udp
dev tun0
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/server.crt
key /etc/openvpn/keys/server.key # This file should be kept secret
dh /etc/openvpn/keys/dh1024.pem
server 192.168.3.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 192.162.1.0 255.0.0.0"
push "dhcp-option DNS 192.168.0.1"
push "dhcp-option DNS 192.168.1.1"
keepalive 10 120
tls-auth /etc/openvpn/keys/ta.key 0 # This file is secret
cipher AES-128-CBC # AES
comp-lzo
```

```

max-clients 100
user nobody
group nogroup
persist-key
persist-tun
status /var/log/openvpn/openvpn-status.log
log-append /var/log/openvpn/openvpn.log
verb 3

```

Seguindo algumas explicações:

A linha “local 192.168.1.100” indica ao openvpn o IP do servidor em que ele está rodando, para ouvir as novas conexões.

A linha “port 1194”, indica em qual porta o serviço openvpn está rodando.

A linha “proto udp”, indica que o serviço está executado utilizando o protocolo udp.

A linha “dev tun0”, indica a nova interface de rede que foi criada para a utilização do túnel virtual.

As linhas “ca /etc/openvpn/keys/ca.crt”; “cert /etc/openvpn/keys/server.crt” e “key /etc/openvpn/keys/server.key” representa a chave de acesso que a openvpn usará para autenticar os clientes openvpn.

A linha “server 192.168.3.0 255.255.255.0” informa ao openvpn que a rede que ele estará gerenciando é a 192.168.3.0/24, sendo que o primeiro IP desta rede é o próprio servidor openvpn. (NERD, 2012).

Como último passo é preciso criar um diretório onde os arquivos de log serão armazenados, usando o seguinte comando:

```
mkdir /var/log/openvpn
```

Com tudo configurado agora basta iniciar o serviço, para isso utiliza-se o seguinte comando:

```
service openvpn start
```

Podemos ver que o serviço está sendo executado usando o comando:

```
service openvpn status
```

## APÊNDICE B - CONFIGURAÇÃO SERVIDOR ASTERISK

O Asterisk está rodando diretamente no servidor Linux, sendo responsável por todo o gerenciando das ligações realizadas através das estações, para instala-lo primeiramente deve-se ter acesso como administrador no terminal, depois atualizar os repositórios de dados, como qualquer outro programa de distribuição unix. (FRANCISCO, 2013).

Agora deve instalar os pacotes essenciais para que o Asterisk possa funcionar corretamente, para isso utiliza-se o comando:

```
apt-get -y install build-essential wget libssl-dev libncurses5-dev libnewt-dev libxml2-
dev linux-headers-$(uname -r) libsqlite3-dev
```

Com os pacotes essenciais instalados é preciso acessar o diretório para download dos fontes do Asteriks, para isso utiliza-se o comando:

```
cd /usr/src
wget http://downloads.asterisk.org/pub/telephony/DAHDI-linux-complete/DAHDI-linux-
complete-current.tar.gz

wget http://downloads.asterisk.org/pub/telephony/libpri/libpri-1.4-current.tar.gz
wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-11-current.tar.gz
```

Agora é preciso descompactar, para isso é só executar o comando:

```
tar xzvf DAHDI-linux-complete-current.tar.gz
tar xzvf libpri-1.4-current.tar.gz
tar xzvf asterisk-11-current.tar.gz
```

Para compilar o Asterisk, é preciso acessar o diretório que foi realizado o download e compilar, é importante compilar os pacotes na ordem correta, pois alguns pacotes dependem de outros, deste modo à instalação ocorrerá sem erros, primeiramente compila-se o pacote DAHDI, para isso é só executar os comandos em sequencia:

```
cd /usr/src/DAHDI-linux-complete-2.10.0.1+2.10.0.1/
make
make install
make config
```

Agora é preciso compilar o libpri, de modo semelhante será executado o comando:

```
cd /usr/src/libpri-1.4.15/
make
make install
```

E por fim o Asterisk, para ele o comando será:

```
cd /usr/src/asterisk-11.12.1/
./configure
make menuselect
make
make install
make config
```

```
make samples
```

Com todos os pacotes compilados, é preciso iniciar os serviços, tanto o DAHDI quanto o próprio Asterisk, isso será feito com o comando:

```
/etc/init.d/DAHDI start
/etc/init.d/asterisk start
```

É possível notar que o Asterisk está funcionando perfeitamente, mas totalmente em modo texto, tornando a configuração um pouco mais complexa, então para facilitar a configuração bem como o gerenciamento do servidor, é possível instalar uma interface gráfica, que será acessada através de qualquer navegador, para isso será preciso acessar o diretório que se deseja e realizar o download, com o seguinte comando:

```
cd /usr/src
svn co http://svn.asterisk.org/svn/asterisk-gui/branches/2.0
```

Agora acessar o diretório que foi baixado e a realizar instalação do novo pacote:

```
cd 2.0/
./configure
make
make install
```

Com os novos pacotes instalados, será preciso apenas alterar dois arquivos de configuração, que ficarão encarregados do gerenciamento quando o navegador tentar acessar o servidor, o primeiro arquivo é “manager.conf”, localizado em “/etc/asterisk/” será preciso alterar a chave “[general]” e “[admin]”, como demonstrado abaixo:

```
[general]
enabled = yes
webenabled = yes
port = 5038
httptimeout = 60
bindaddr = 192.168.1.100
```

```
[admin]
secret = secret
read = system,call,log,verbose,agent,user,config,dtmf,reporting,cdr,dialplan
write = system,call,agent,user,config,command,reporting,originate
```

O segundo arquivo é o “http.conf” localizado também no diretório “/etc/asterisk/”, para ele será preciso alterar apenas a chave “[general]” como mostrado abaixo:

```
[general]
enabled = yes
enablestatic = yes
bindaddr= 192.168.1.100
bindport=8088
```

Como são configurações do servidor é preciso reiniciar o serviço para que este possa atualizar e utilizar as novas configurações, para isso basta executar o comando:

```
/etc/init.d/asterisk reload
```

Para verificar se tudo estará funcionando corretamente utiliza-se o seguinte comando:

```
cd /usr/src/2.0  
make checkconfig
```