UNIVERSIDADE ESTADUAL DO NORTE DO PARANÁ

CAMPUS LUIZ MENEGHEL

ALEX SETOLIN BEIRIGO

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

BANDEIRANTES - PR

2009

ALEX SETOLIN BEIRIGO

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

Trabalho de Conclusão de Curso submetido à Universidade Estadual do Norte do Paraná - Campus Luiz Meneghel, como requisito parcial para a obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: Prof. Ms. Ricardo Gonçalves Coelho.

BANDEIRANTES - PR

2009

ALEX SETOLIN BEIRIGO

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

Trabalho de Conclusão de Curso submetido à Universidade Estadual do Norte do Paraná - Campus Luiz Meneghel, como requisito parcial para a obtenção do grau de Bacharel em Sistemas de Informação.

COMISSÃO EXAMINADORA

_____
Prof. Ms. Ricardo Gonçalves Coelho
Orientador

_____
Prof. Luiz Fernando L. Nascimento
Membro da banca examinadora

_____
Prof. Ms. Ailton Sergio Bonifácio
Membro da banca examinadora

Bandeirantes, ___ de _____ 2009.

A Jesus, minha família, professores e amigos que me deram condições para realizar este trabalho.

AGRADECIMENTOS

Agradeço primeiramente a Deus pela Vida e por esta oportunidade. Agradeço aos meus pais Wanderley de Moura Beirigo Júnior e Aparecida Setolin Beirigo, por terem me proporcionado esses anos de estudos, anos muito felizes de minha vida. Ao meu orientador Professor Ms. Ricardo Gonçalves Coelho por todos os ensinamentos repassados a mim. A todos os professores que contribuíram significativamente para minha formação. Agradeço a todos meus colegas de faculdade, foram quatro anos de total aprendizado e crescimento. Agradeço em especial aos meus irmãos que direta e indiretamente me proporcionaram condições para ter realizado esta empreitada e aos meus amigos Rafael Gustavo Paixão, Bruno Garcia e Claudemir Garcia por todos os momentos de fraternidades e alegrias. Por fim, agradeço a todos que não ajudaram, mas também não atrapalharam minha formação acadêmica.

A vida é realmente escuridão, exceto quando há impulso. E todo impulso é cego, exceto quando há saber. E todo saber é vão, exceto quando há trabalho. E todo trabalho é vazio exceto quando há amor.

Halil Gibran

RESUMO

À medida que o uso de redes sem fio e o desenvolvimento de novas tecnologias aumenta, acresce também a necessidade de mais segurança, já que esta relação também se aplica às fraudes e espionagens na rede. Entretanto, a implementação de técnicas de segurança acabam por interferir e, muitas vezes, degradar o desempenho da rede, uma vez que tais procedimentos requerem maior poder de processamento das máquinas, maior largura de banda, entre outros.

Um aspecto crítico em se tratando de segurança em redes sem fio, é a garantia de tráfego seguro dos dados diante de um possível ataque, e a integridade dos pacotes.

Este trabalho faz um estudo de VoIP relacionado aos métodos criptográficos de segurança: WEP (*Wired Equivalent Privacy*), WPA (*Wi-Fi Protected Access*) e VPN (*Virtual Private Networking*). Através de testes realizados em uma rede VoIP com *software* de gerenciamento de tráfego de rede Wireshark; criptografia: OpenVPN; gerenciamento de PABX: Asterisk e um *softphone* X-lite, foi possível fazer análises e comparações das informações capturadas.

Palavras-chave: VoIP, Asterisk, Segurança, OpenVPN, WEP, WPA.

ABSTRACT

As the use of wireless networks and the development of new technologies increases, there is also an additional need for more security, since this ratio also is applied to fraud and spy acts over the network. However, the implementation of security techniques ultimately interfere, and often degrade network performance, since these procedures require more processing power of machines, more bandwidth, among others.

A critical aspect in the case of networks without security-wire, is the guarantee of secure data traffic before a possible attack and the integrity of data packages.

This work is a study of Voip related to cryptographic methods of security: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) and Virtual Private Networking (VPN). Through tests on a network with VoIP and management software Wireshark network traffic; cryptography: openvpn; management PABX: Asterisk and a softphone x-lite was possible to make comparisons and analysis of information captured.

Key-words: VoIP, Asterisk, Segurança, OpenVPN, WEP, WPA.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

AH - *Authentication Header*
DHCP - *Dynamic Host Configuration Protocol*
EAP - *Extensible Authentication Protocol*
ESP - *Encapsulating Security Payload*
GNU - *General Public License*
HTTP - *Hypertext Transfer Protocol*
ICV - *Integrity Check Value*
IETF - *Internet Engineering Task Force*
IETF - *Internet Engineering Task Force*
IP - *Internet Protocol*
IPSEC - *Internet Protocol Security*
ISO - *International Organization for Standardization*
ITU - *International Telecommunications Union*
ITU-T - *International Telecomunication Union*
MC - *Multipoint Controller*
MCU - *Multipoint Control Unit*
MGCP - *Media Gateway Control Protocol*
MIC - *Message Integrity Check*
MP - *Multipoint Processors*
NAT - *Network Address Translation*
OSI - *Open Systems Interconnection*
PABX - *Private Automatic Branch Exchange*
PCM - *Pulse Code Modulation*
PDA - *Personal Digital Assistant*
PDU - *Protocol Data Unit*
RADIUS - *Remote Authentication Dial-In User Server*
RFC - *Request For Comments*
RTCP - *Real Time Trasnport Control Protocol*
RTP - *Real Time Transport Protocol*
SA - *Security Association*
SDP - *Session Description Protocol*

SIP - *Session Initiation Protocol*

SPI - *Security Parameter Index*

TCP - *Transmission Control Protocol*

UDP - *User Datagram Protocol*

URL - *Uniform Resource Locator*

VOIP - *Voz over Internet Protocol*

VPN - *Virtual Private Network*

WEP - *Wired Equivalent Privacy*

Wi-Fi - *Wireless Fidelity*

WLAN - *Wireless Local Area Network*

WPA - *Wi-Fi Protect Access*

WPA2 - *Wi-Fi Protect Access 2*

SUMÁRIO

1. INTRODUÇÃO

Hoje em dia, as operadoras de telefonia, abaixaram consideravelmente os preços das ligações de longa distância, e isso não acontece somente por causa da concorrência entre essas empresas, mas por causa do surgimento de alternativas de comunicações de baixo custo.

A Rede de comutação de circuitos nos permite efetuar o tráfego de informações em tempo real com baixo atraso e erro, porém devido à transmissão desnecessária de algumas informações, não tem um bom aproveitamento dos recursos de transmissão.

A Rede de Comutação de Pacotes foi projetada para o tráfego de dados e, por causa disso, ela tem um menor grau de confiabilidade na transmissão de informações em tempo real, com maior atraso e erro, porém proporciona um maior aproveitamento dos recursos de transmissão. A tendência no futuro é fazer as informações trafegarem em uma única infra-estrutura de rede, onde todos os serviços serão oferecidos por esse mesmo meio, também chamada de NGN (*Next Generation Networking*) ou redes multiserviços.

A transmissão de Voz sobre IP teve inicio em 1995. Com a tecnologia VoIP (*Voice over Internet Protocol*), espera-se uma diminuição dos custos de telefonia, principalmente nas ligações de longa distância. A idéia inicial é passar como é a comunicação de baixo custo dentro das empresas e fora delas.

Como todos os softwares de comunicação, é importante a implementação de segurança, para terceiros não conseguirem ter acesso às informações. Por isso podemos aplicar criptografia nos pacotes. Com esta implementação, o pacote tem um pequeno aumento de tamanho para trafegar na rede, mas isso não impede de termos uma comunicação de voz limpa e sem ruídos.

Quem usa Wireless, pode usufruir normalmente da tecnologia VoIP. As redes sem fio já possuem a sua própria criptografia em sua transmissão, o que nada impede de acrescentar outra criptografia, foco principal deste trabalho.

1.1 Objetivos

O Objetivo Geral do trabalho é fazer um estudo da qualidade da transmissão de voz em redes IP, associada com mecanismos de segurança.
Este trabalho tem como objetivos específicos:

- Explorar a tecnologia VoIP e seus protocolos utilizados;
- Aplicar medidas de segurança, criptografia e autenticidade dos dados através de uma VPN, WEP, WPA;
- Analisar a qualidade e segurança na transmissão de pacotes de voz com as medidas de segurança associadas;
- Realizar testes com redes sem fio e com os protocolos de criptografia disponíveis das redes sem fio, associados com uma ligação VPN;
- Realizar um estudo comparativo dos pacotes capturados.

1.2 Justificativas

O motivo de analisar e propor segurança na transmissão de pacotes de voz em redes IP, dá-se pelo crescimento das pessoas e empresas que utilizam VoIP. A grande preocupação ocorre, pois o VoIP integra serviços de comunicação de voz em uma infra-estrutura de dados exposta a uma série de ameaças enquanto antes, na telefonia convencional, esse serviço era restrito a uma rede planejada e dedicada para este fim.

Fazer análises em uma rede VoIP wireless e demonstrar o impacto que diversas criptografias mais utilizadas no momento causam nos pacotes, é essencial para quem usufrui ou quer implementar VoIP, seja em sua residência ou empresa.

O tráfego de voz por VoIP é considerado um tráfego em tempo real, diferentemente do tráfego de dados comuns, pois é muito sensível a atrasos. Aplicações multimídia, como o VoIP, são muito sensíveis a atrasos, mas toleram certa perda de pacotes. Por causa desta característica, é preciso dar prioridade ao tráfego de voz em uma rede congestionada, pois se houver atraso ou muita perda de pacotes, a qualidade da ligação vai cair até um ponto onde não é possível mais

manter uma conversa. Relacionar VoIP com segurança é essencial para ter qualidade em ligações, já que segurança causam impactos nas transmissões dos pacotes em redes, isto é, aumentam seu tamanho por causa da criptografia.

1.3 Organização do trabalho

A estrutura do trabalho apresenta-se distribuída da seguinte maneira: no capítulo 2 são apresentados os conceitos relacionados às transmissões de voz em redes IP´s e criptografia. No capítulo 3 apresentam-se os softwares utilizados para fazer os estudos na rede e suas configurações. No capítulo 4 mostra as análises e os resultados obtidos na rede. E finalmente no capitulo 5 é exposto as conclusões e sugestões para trabalhos futuros.

2. FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são apresentados os conceitos relacionados à tecnologia de voz sobre IP: o que é, como surgiu e conceitos dos protocolos utilizados para transmissão da voz. E também conceitos sobre criptografia WEP e WPA.

2.1 VoIP

VoIP é uma aglomeração de tecnologias que usa redes IP's ou Internet para a comunicação de Voz, trocando ou complementando os sistemas de telefonia. Permite a digitalização de voz e o empacotamento de dados IP para a transmissão em uma rede que utilize os protocolos TCP/IP.

A telefonia IP é um dos serviços da VoIP onde apresenta característica e funcionalidades equivalentes aos serviços telefônicos convencionais. Utilizamos um telefone IP ou um adaptador próprio IP para um telefone convencional, e uma conexão a internet para se conectar a rede de telefonia IP.

Segundo SOUZA 2003, a Telefonia IP é definida como a comunicação multimídia entre dois ou mais participantes, em outras palavras, significa dizer que é uma ligação telefônica realizada através da rede IP. Porém o uso comum do termo telefonia IP não deve ser entendido somente como transporte de voz, mas também como transporte de outros tipos de meios como vídeo e dados.

Para ter conversação entre participantes há necessidade haver sinal entre eles. Este sinal funciona como a criação, controle e a finalização de chamadas. O sinalizador ao capturar voz, imagens codifica e encapsula em pacotes. Assim usando os protocolos, são mandados estes pacotes através da rede. Do outro lado, esses pacotes são desencapsulados e decodificados, o sinal digital é convertido em sinal analógico e reproduzido em alto-falantes enquanto o vídeo é enviado para a tela.

Com um microfone, caixa de som e um software adequado, é possível fazer ligação para telefones fixo com o computador. Usando um softphone (cada fabricante tem o seu software). Existem aparelhos telefônicos que já são

aparelhos apropriados para as redes IP chamado de aparelhos IP (utilizando o mesmo critério cada fabricante possui o seu equipamento). Na transmissão de voz é necessário que esses pacotes tenham prioridade na transmissão, para que isto aconteça, é necessário que a rede possua a tecnologia de QOS (*Quality of Service*). Neste trabalho, abordaremos as principais características desta tecnologia (QOS) no tópico 2.5.

VoIP é também aplicado em PABX (Central de comutação automática interno e externo), os conhecidos sistemas de ramais telefônico. Adicionalmente pode acessar o serviço utilizando um computador com um programa especial para esse fim como usaremos neste projeto.

2.1.1 Benefícios da Tecnologia VoiP.

Um empreendimento pode obter uma grande economia utilizando essa rede para o tráfego de voz, e se ela já tiver uma rede de transferência de dados ela pode estar aproveitando o link. Caso a empresa ainda não transmite dados a melhor opção é adotar uma solução que utilize Voz sobre IP.

Em qualquer das situações, a economia com ligações locais e interurbanas traz retorno de investimentos em curto espaço de tempo. Essa economia é resultado de:

- ✓ De ligações telefônicas a custo zero ou (taxa bem menores);
- ✓ De envio e recebimento de Fax sem nenhum custo;
- ✓ Da utilização de uma única infra-estrutura para prover serviços de link de dados e telefonia.

Em relação ao uso de usuários domésticos que possuem o serviço ADSL, na utilização do VoIP, não há garantia de qualidade com grande eficácia nas ligação, pois a rede não tem QoS, tornando a chamada inaudível em alguns momentos. Dependendo do tipo de interface podemos conectar um PABX ou um telefone diretamente no roteador. Todas as ligações entre as corporações (Matriz-Filiais) são redirecionadas na rede de dados da empresa. Ligações externas são redirecionadas para a rede da telefonia local.

Segundo VOIPME 2009**,** o provedor *Skype* que fornece de PC para Telefone, ligações grátis entre seus usuários, até agora foi o provedor que mais

abriu portas internacionalmente, possibilitando o melhor uso da tecnologia VoiP. Cerca de 130 milhões de usuários já fizeram o download do software desde julho de 2005.

A maioria dos provedores de voz sobre IP também proporcionam muitos outros serviços adicionais juntamente com o seu plano básico VoiP, sendo que nas linhas convencionais é cobrado extra para cada função adicionada. Enquanto a maioria das pessoas nos Estados Unidos pagam $20 (cerca de R$ 45) por mês para fazer somente ligações locais usando as linhas convencionais. Alguns provedores de VoiP oferecem ligações locais ilimitadas, de longa distância, e ligações internacionais para alguns países pelo mesmo preço. É possível ligar para uma pessoa que mora longe, em outro país sem custos adicionais de ligações de longa distância ou internacionais.

Normalmente os provedores em geral incluem alguns serviços grátis em planos VoiP, como: Identificador de chamadas, ligação de espera, ligação entre 3 pessoas, *voice mail* e outros mais. O VoiP também é um serviço de fácil mobilidade.É capaz de levar o número de telefone em outra cidade. (caso tenha conexão de banda larga nos locais).

Segundo ainda (**voipme 2008),** muitos usuários desta nova tecnologia também acham fácil lidar com o serviço ao consumidor dos provedores VoiP do que os das companhias de telefonia convencionais. A tecnologia VoiP é dependente de uma conexão banda larga.

2.2 Protocolos Principais no Uso no Voip

Existem alguns protocolos que são mais usados quando falamos de Telefonia VoIP. Iremos apresentá-los incluindo seus componentes e os seus funcionamentos.

2.2.1 RTP

O RTP ou Protocolo de Transporte em Tempo Real (*Real-Time Transport Protocol*) foi apresentado formalmente em janeiro de 1996 pelo Grupo de trabalho de Redes (*Networkig Working Group*) do IETF (*Internet Engineering Task Force*) com objetivo de fornecer uma padronização de funcionalidades para os

aplicativos de transmissão de dados em tempo-real como vídeo, áudio, tanto em redes *unicast* como nas *multicast*, sem entretanto garantir a qualidade de serviço QoS ou reservar recursos de endereçamento. O RTP roda sobre a camada UDP/IP utilizando os serviços de multiplexação e *cheksum* do UDP estabelecendo uma comunicação fim a fim. As porções de áudio e vídeo produzidas pelo aplicativo remetente são encapsuladas em pacotes RTP que por sua vez são encapsulados em um segmento UDP. Entretanto, apesar de utilizar o UDP e o IP, o RTP pode ser implementado em outros ambientes já que necessita apenas de serviços de transporte não orientado à conexão.

Normalmente, o RTP é implementado como parte da aplicação e não como parte do *Kernel* do sistema operacional. Basicamente, o protocolo permite a especificação dos requisitos de tempo e conteúdo pertinentes à transmissão de multimídia, tanto no envio quanto da recepção através de:

- numeração seqüenciada,
- selo de temporização (estampilho),
- envio de pacotes sem retransmissão,
- identificação de origem
- identificação de conteúdo,
- sincronismo.

2.2.2 RTCP (RTP Control Protocol)

O protocolo RTCP é muito utilizado em paralelo ao RTP contribuindo para que a distribuição dos dados ocorra de uma maneira escalável ao ponto de permitir grandes transmissões multidestinatárias e também provendo um certo controle e identificação dos participantes da comunicação.

Sendo a transmissão multidestinatária, se mostra importante haver relatórios do recebimento dos pacotes de modo que se possa identificar falhas na distribuição dos mesmos. Alguém observando os relatórios deve ser capaz de avaliar se um problema é local ou global. Pode-se inclusive ter uma entidade cuja única função é monitorar a distribuição sem participar da comunicação.

Já que há uma previsão de que todos os participantes estarão enviando pacotes RTCP a todo momento, é necessário restringir a taxa de

transmissões dos mesmos de acordo com o número de participantes de modo a não sobrecarregar a rede, de modo que este problema não restrinja o número de participantes na comunicação RTP. Ao iniciar-se uma sessão RTP cada participante deve enviar um pacote de controle a todos os outros de forma que cada participante saberá quantos outros fazem parte desta sessão e calculará qual deverá ser a taxa de seus pacotes de controle baseado neste número.

2.2.3 H.323

O protocolo H.323 do ITU-T (*International Telecomunication Union*), estipula padrões para codificar e descodificar informações de vídeo e áudio além de não depender da rede. O H.323 é um dos mais importantes protocolos quando falamos em VoIP. a seguir discutiremos o seu funcionamento.

2.2.3.1 Benefícios do H.323

O protocolo H.323 possui inúmeros benefícios. Segue abaixo alguns deles:

- Não depende da rede: O H.323 foi criado para ser usado em redes que utilizam pacotes, como rede IP. Em quase todos os casos as redes utilizam protocolos baseados em pacotes.
- Interoperabilidade entre dispositivos e aplicações de diferentes fabricantes.
- Independência, o H.323 não especifica o hardware ou sistema operacional que deve ser usado. Assim, as aplicações H.323 podem ser de naturezas distintas que podem focalizar mercados que vão desde *software* de vídeo conferência realizados em PCs, a telefones IP, adaptadores para Tv, sistemas dedicados, etc.
- Padronizar mídias: estabelece codificadores para compressão e descompressão de sinais de áudio e vídeo. É possível que um terminal com suporte apenas para áudio participe de uma conferência com terminais que tenha suporte adicional de vídeo ou dados.

- Interoperabilidade entre redes: é possível fazer conferências entre participantes de uma LAN em outras redes completamente diferentes, como a rede telefônica pública.
- Gerência a largura de banda: o tráfego dos fluxos de vídeo e áudio é caracteristicamente consumidor de largura de banda em uma rede
- Suporte em conferência multiponto: com três ou mais participantes simultâneos.
- Suporte a multicast: envia um único pacote a todo um subconjunto de destinatário na rede. Esse tipo de transmissão usa a largura de banda de uma forma mais adequada que as transmissões unicast.

2.2.3.2 Arquitetura H.323

O H.323 é um padrão que utiliza qualquer topologia de rede, isto é, uma ligação ponto a ponto, utiliza um segmento de rede ou até mesmo vários segmentos interligados.
Observe a figura 1 que mostra a comunicação entre dois terminais H.323 em uma rede com pacotes.

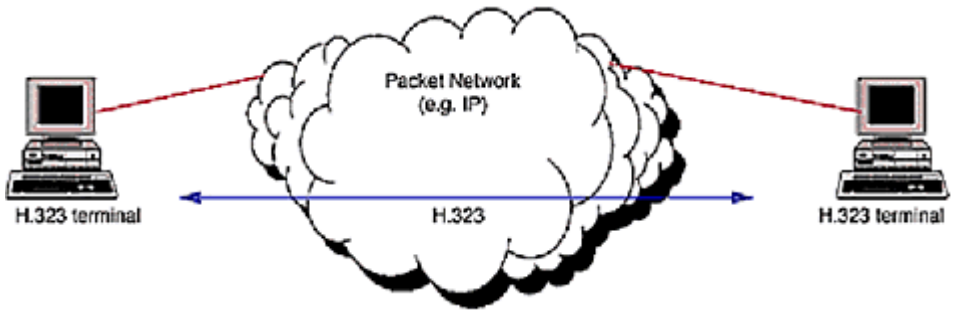

Figura 1: Comunicação entre dois terminais.

(FONTE: TELECO 2007)

O H.323 lista o áudio, vídeo e dados em uma comunicação multimídia, porém apenas o suporte à mídia de áudio é obrigatório. Cada mídia, quando utilizada, deve seguir sempre o padrão. Pode-se ter diversas formas de

comunicação: com áudio (telefonia IP), áudio e vídeo (vídeo Conferência), áudio e dados e, por fim, áudio, vídeo e dados.

Este tipo de redes é utilizada em *LAN* e *WAN*, e em lugares que não tem qualidade de serviço, ou seja, redes que sofram com atrasos de pacotes. Observe a figura 2, ela tem uma arquitetura do H.323. Na parte de cima da figura está à rede LAN, com quatro terminais que tem capacidade para utilizar todas as vantagens desta arquitetura, até vídeo conferências simultâneas em múltiplos pontos. A transmissão de voz sobre IP utiliza apenas algumas partes desta arquitetura. Quando a comunicação é em muitos pontos precisa-se de uma unidade controladora H.323 (multi-ponto MCU).

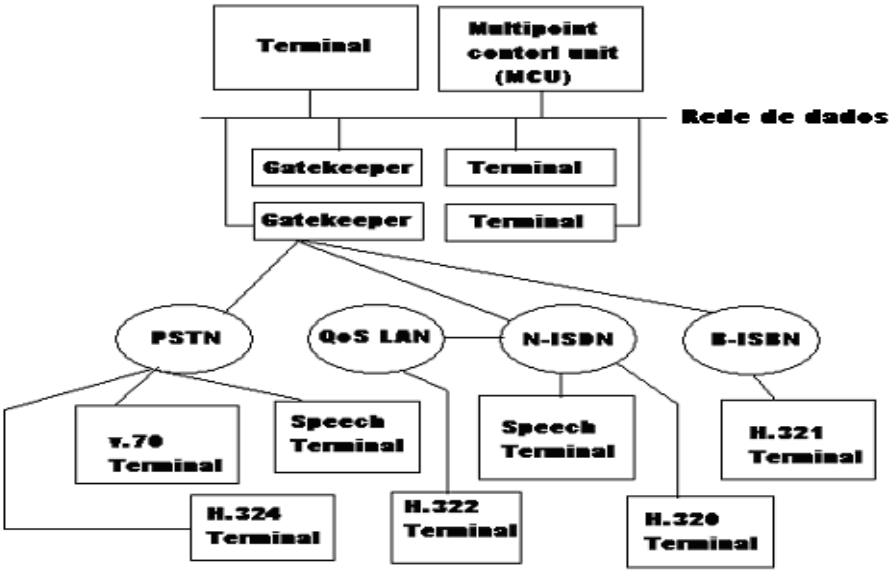

Figura 2: Arquitetura do H.323

(FONTE:UFRJ 2007)

O protocolo H.323 ainda pode estender através da *WAN's* e ficar disponível através dos seus dispositivos. A frente no tópico 2.2.3.6 é explicada a função de um dos dispositivo chamado *gatekeeper*. Se um *gatekeeper* não esta presente, o restante dos dispositivos devem ser capazes de produzir suas próprias mensagens de sinalização. Os links de *WAN* são ligado no *gateways* H.323.

2.2.3.3 Codec

É um amplificador que codifica ou descodifica um sinal. Por exemplo, companhias telefônicas utilizam *codecs* para transformar sinais binários transmitidos pelas redes digitais em sinais analógicos para rede analógica.

Alguns exemplos de codecs são G723 e G.711, juntamente com o protocolo RTP (*Real Time Protocol*).

Este procedimento é dividido em duas partes:

- Análise da voz: converte a voz em um formato digital, para que seja armazenada nos sistemas e transmitida em redes digitais ou rede IP.
- Sintetização da voz**:** Converte a voz da forma digital para forma analógica, própria para a audição humana.

2.2.3.4 Protocolo H.225 - sinalização de chamada (call signaling)

- ✓ Responsável pela estabelecimento da conexão entre dois *endpoints* H.323 (terminais ou *gateway*).
- ✓ Se não houver *gatekeeper* as mensagens H.323 são trocadas diretamente entre os *endpoints*.
- ✓ Se houver *gatekeeper*, as mensagens H.225 podem ser trocadas de duas maneiras:
- ✓ O método é decidido através do H.225 RAS (*Registration*, *Admission* e *Status*)

Na tabela 1 mostra alguns padrões de codec´s e seus significados

Padrões	Significado
H.225	**Procolo de controle de chamada**
H.245	**Protocolo de controle de mídia**
H.261	**Codec de vídeo para 64 kbps ou mais**
H.263	**Codec de vídeo para menos de 64 kbps**

G.711	**Codec de áudio PCM para 56/64 kbps**
G.722	**Codec de áudio para 7 kHz em 48/56/64 kbps**
G.723	**Codec de fala para 5,3 e 6,4 kbps**
G.723	**Codec de fala para 5,3 e 6,4 kbps**
G.728	**Codec de fala para 16 kbps**
G.729	**Codec de fala para 8/13 kbps**

Tabela 1 Padrões H.323 (FONTE: UCB 2007)

2.2.3.5 MCU

O MCU (*Multipoint Control Unit*) gerência e cuida da conferência com três ou mais usuários H.323.

O H.323 faz com que o MCU faz que com que uma conferência tenha mais de dois usuários que sigam estes mesmos padrões utilizando protocolos orientados a conexão para ter controle das conferências. Essa característica impede a utilização completa de transmissão *multicast* (como no padrão IETF SIP).

Um MCU divide-se em MC (*Multipoint Controller*) e MP (*Multipoint Processors*). O MC controla conferências com mais de dois participantes utilizando protocolos de sinalização e controle do H323. O MP executa funções, entre os usuários, para chavear mídia.

2.2.3.6 Gatekeeper

Gatekeeper traduz endereços, e controla acesso à LAN por terminais e roteadores. O “*gatekeeper*” (GK) faz parte do H.323 que atua como um ponto central para as chamadas de uma “zona H.323”. Esse conceito de zona refere-se à gerência do “*gatekeeper*”. Este componente é o mais importante de uma rede H.323. Ele é ponto central de uma “zona H.323”, oferece uma série de serviços aos seus “clientes” cadastrados. Como por exemplo: controle da sinalização de chamada.

O “*gatekeeper*”, utiliza o H.245 para fazer negociações quando uma chamada esta ocorrendo. Uma zona H.323 é o conjunto de dispositivos (terminais, “gateways” e MCUs) que são gerenciados por um “*gatekeeper*”. Os terminais H.323 se cadastram nos “*gatekeepers*” para enviar e receber chamadas e este último oferece serviços de rede para os componentes da zona que gerenciam. principais funções do *gatekeepers*:

- Traduzir os endereços *aliases* para endereços IP ou IPX;
- Gerenciamento de largura de banda, permitindo a definição da quantidade máxima permitida para os recursos da conferência;
- Roteamento de chamadas H.323;
- Controle do número e do tipo de conexões permitidas;
- Controle de admissão de acesso em uma “zona H.323”;

Existem muitas características ligadas ao “*gatekeeper*” são fundamentais à comunicação H.323 na Internet. Por exemplo, se o usuário não querer trabalhar com endereços de rede, poderá trabalhar com nomes que sejam facilmente associado às pessoas. Outra opção é a permissão ou não a inclusão de um determinado usuário ao “*gatekeeper*”.

De uma maneira geral, as funções de registro, admissão e estado do “*gatekeeper*” são desempenhadas pelo protocolo RAS (*Registration*, *Admission and Status*).

Existem dois métodos para encontrar um “*gatekeeper*”. O primeiro é através do seu endereço de rede, UDP 1719 (porta padrão). O segundo método é utilizar *multicast*, através do uso de mensagens num processo de localização dinâmica, usando o endereço de grupo *multicast* 224.0.1.41 (todo “*gatekeeper*” é membro desse grupo), agora na porta UDP 1718.

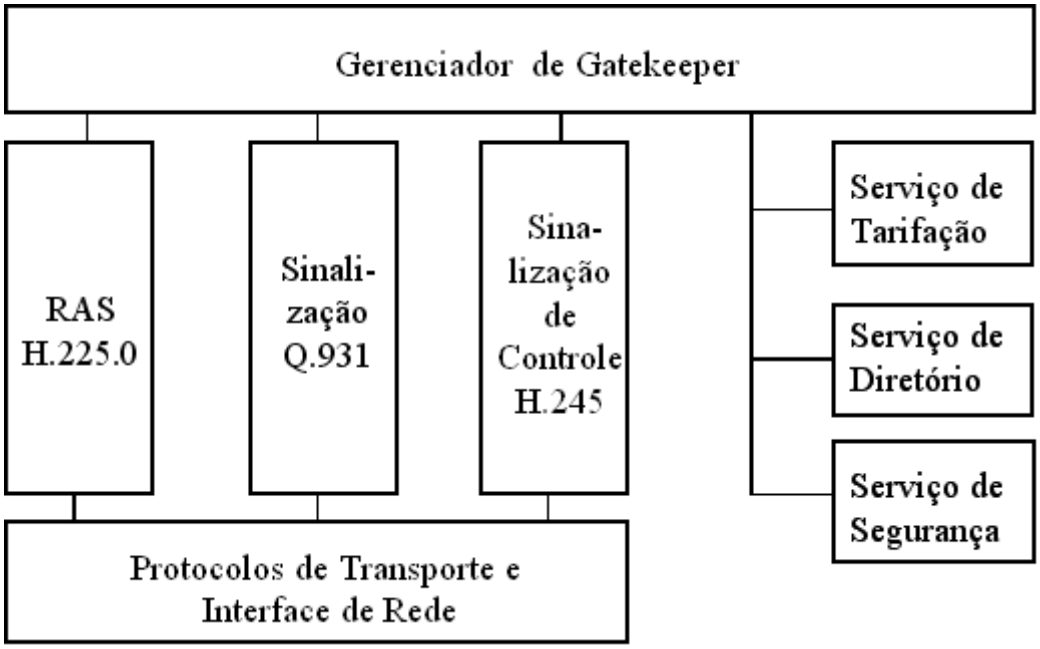

Figura 3: Estrutura de Camada Gatekeeper

(FONTE: FCCN 2008)

2.2.3.7 Gateway H.323

É um dispositivo que localiza entre uma rede de telecomunicação e uma rede IP. Um gateway H.323 é o ponto final da rede que fornece comunicação em tempo real nas duas direções entre terminais H.323 em uma rede IP e outros terminais ITU (Internation Telecomunication Union) em uma rede comutada ou para outro gateway H.323. Eles executam a função de transporte entre diferentes formatos de dados. Quando os terminais precisam se comunicar com um ponto final em outra rede, esta comunicação é feita através do gateway pelos protocolos H.245 e Q.931.

2.2.4 Protocolo de Iniciação De Sessão (*SIP)*

SIP é um temo inglês que tem como significado Protocolo de Inicialização de Sessão, ele é um protocolo de telefonia IP que produz, modifica e finaliza chamadas telefônicas VoIP.

O SIP foi criado pelo IETF (*Internet Engineering Task Force*), faz comunicação que produz uma ligação telefônica. Todos os detalhes estão escritos no protocolo SDP. O protocolo parece se com o HTTP, e baseia-se em texto. Ele substitui amplamente o padrão H323. O Protocolo de Iniciação de Sessão (SIP) utiliza “requisição-resposta”, parecido com o HTTP, para dar início sessões de comunicação entre usuários ele estabelece chamadas através de sinal e realiza conferências através de redes via Protocolo IP. A mudança ou a finalização da sessão não depende do tipo de mídia ou aplicação que será utilizada na chamada; cada chamada tem capacidade de suportar diferentes tipos de dados, incluindo áudio e vídeo.

O SIP teve seu início logo após os anos de 90 (naquele tempo o H.323 estava começando a se padronizar. O aperfeiçoar o SIP talvez tem um impacto tão forte quanto o protocolo HTTP, a tecnologia que está na web que permite que uma página tenha links e conecte a outras páginas.

O SIP foi modelado e baseado em outros protocolos baseados em texto: SMTP (e-mail) e o HTTP (páginas da web). Ele foi criado para estabelecer, mudar e terminar chamadas em um ou mais usuários em uma rede IP de uma maneira que não depende do conteúdo de mídia. Parecido com o HTTP, o SIP leva a aplicação para o terminal, extinguindo a necessidade de uma central.

2.2.4.1 Aspectos Gerais.

Resumidamente, o SIP tem as seguintes características:

- É baseado em texto. As mensagens do SIP são muito mais aderentes as aplicações do que H.323, que usa o padrão de codificação..

- Envolve menos sinalização. O SIP atende os requisitos básicos de um protocolo de sinalização como criar, modificar e terminar sessões de chamadas, para que a sinalização seja o mais simples possível. Fazer com que uma chamada seja rápida, é importante para uma alta qualidade de serviço (QoS).
- Independe do protocolo de transporte utilizado. Embora o SIP tenha sido desenvolvido para ser independente do protocolo da camada de transporte, tipicamente ele roda sobre UDP em vez de TCP. O estabelecimento de conexões TCP e suas rotinas de confirmações introduzem atrasos, que são cômodos e devem ser evitados em transmissões de voz. Adotando o UDP, entretanto, o tempo das mensagens e suas retransmissões devem ser controlados pela camada de aplicação.

2.2.4.2 Agente Do Usuário.

O Agente do Usuário é um terminal SIP ou o software de estação final. Este funciona como um cliente, que faz pedido para inicializar uma sessão. Também tem função de um servidor, quando responde a uma solicitação da sessão. O Agente do Usuário armazena e gerencia situações de chamada. O Agente do Usuário pode fazer chamadas, com endereços parecidos com o de e-mail ou número de telefone. Exemplo: (E.158), *SIP:user@proxy.university.*

2.2.4.3 O “SIP” No Mercado Atual.

Há vários produtos comerciais que estão no mercado atualmente para serem comprados (Gratuito para Testar) ou de fonte aberta do SIP (gratuito).
O lado do comércio tem foco nos Agentes do Usuário, como o telefone SIP e os softwares do Agente do Usuário. Um exemplo evidente que tem grande influência no mercado é o “Messenger”, da Microsoft.
Os produtos com esse tipo de arquitetura SIP podem ser encontrados pela Cisco, *PingTel*, 3COM, entre outros.

A Microsoft anunciou que não desenvolverá mais o H.323 (NetMeeting e Exchange *Conferencing* Server), e passará exclusivamente a desenvolver produtos dentro do SIP. O "Windows Messenger" transforma o PC em um software de telefone (um dispositivo de voz sobre IP) com as ferramentas adicionais de vídeo, Chat e compartilhamento de dados. A versão beta foi finalizada em 2006, e teve no início de 2007 uma grande repercussão no mercado. Quanto aos componentes do servidor SIP, alguns estão em desenvolvimento e outros já lançaram e estão presentes no mercado.

2.3 A Relação do SIP e do H.323

O SIP e o H.323 são padrões que realizam chamada, sinal de chamada, controle de mídia e serviços adicionais. A força do H.323 tem sido a sua interoperabilidade com a rede telefônica pública (PSTN) [1], e tem capacidade para sistemas/aplicações desktop e salas de videoconferência, de preço acessível e confiável.

O SIP é um protocolo desenvolvido designadamente para Internet e garante grande flexibilidade. É provável que o H.323 fique como a tecnologia de conferência para administrar serviços de conferência/colaboração futuramente.

H.323 e SIP foram aperfeiçoados para controle e sinalização de chamadas distribuídas. O H.323 é formado em protocolos do ITU-T já existentes, e tem uma arquitetura voltada para equipamentos terminais. Como dito, o SIP é semelhante ao HTTP, e trata de usuários e serviços integrados na Internet.

Em relação à complexidade, a implementação do H.323 é maior em relação ao SIP. A documentação do H.323 tem 736 páginas, contra apenas 128 do SIP, o que leva o desenvolvedor a prestar mais tempo para entender o funcionamento do H.323.

O SIP trabalha com apenas 37 tipos de cabeçalhos enquanto que o H.323 tem centenas. O H.323 trabalha com muitos protocolos sem uma separação clara, isto é,

---

[1] PSTN: Public Switched Telephone Network. Sigla de Rede Pública de Telefonia Comutada, é a rede acessada por telefones comuns, sistemas de ramais, troncos PBX e equipamento de transmissão de dados. Em inglês, PSTN ou Public Switched Telephone Network.

esses protocolos são usados por vários serviços. Já no SIP, em uma mesma requisição estão todas as informações e serviços são necessários. No SIP devido sua estrutura novas características são incluídas de forma fácil e compatível com versões anteriores e novas funcionalidades podem ser colocados em qualquer parte de mensagem.

No H.323 existem campos já definidos para essas novas inclusões. Se um novo “codec” é registrado, é possível ter capacidade para o SIP, enquanto no H.323 há um maior trabalho para acrescentar “codecs”, porque eles têm que ser padronizados pelo ITU-T. No SIP, o Proxy tem duas mídias, e possui endereços para o transporte da mídia, enquanto no H.323 temos vários subprotocolos (H.245, H.225, etc).

Os servidores ou gateways SIP podem funcionar nos modos *stateful* ou *stateless*, sendo que, no segundo caso, os servidores recebem e transferem os pedidos sem guardar tipo algum de informação, já que as mensagens possuem dados suficientes para garantir que a mensagem seja enviada corretamente.

O H.323 é *stateful*, ou seja, ele mantém todo o controle do estado da chamada durante todo período, em um ambiente onde pode muitas chamadas simultâneas, implicando em problemas de desempenho.

O fato de o SIP usar mensagens de texto, utilizar apenas um pedido para enviar toda a informação necessária para fazer uma chamada ser baseada no UDP, tornando-se um protocolo com mais suporte para ser usado na telefonia IP. Assim o H.323 tem uma vantagem de já ter muitos sistemas implementados, o que obrigará o SIP a fornecer mecanismos de interoperabilidade.

Conforme Souza 2003, quanto ao H.323, tem os seguintes componentes: terminal, gateway, *gatekeeper* e MCU; o SIP tem UA e *Servers*. Os protocolos no H.323 são: H.245, RAS/ Q.931, H.225, enquanto no SIP, é o próprio SIP e SDP

A interoperabilidade entre as versões e a completa compatibilidade existente no H.323 fazem com que todas as implementações, baseadas nas diferentes versões, possam ser integradas. Já no SIP, uma nova versão pode anular um atributo antigo que não é mais utilizado, o que conduz um

aproveitamento melhor do tamanho, do código e diminui a complexidade do protocolo, porém perdendo algumas compatibilidades em diferentes versões.

2.4 Interoperabilidade SIP com o H.323

As organizações estão em geral trabalhando para acontecer interoperabilidade entre SIP-H.323, tornando possível a transmissão entre a tecnologias H.323 e SIP. Duas organizações que estão especialmente interessadas nesse Assunto: a IMTC (*International Multimedia Telecommunications* Consortium), uma corporação sem fins lucrativos, com mais de 100 organizações pelo mundo, e a ETSI (*European Telecommunications Standards Institute*).

A Open H.323 *Organization* já criou um gateway de trabalho H.323 para SIP. O H323 é um protocolo relativamente antigo que está atualmente sendo substituído pelo SIP como já mencionado neste trabalho. Isto reflete no mercado fazendo que a maioria dos equipamentos VoIP atualmente a seguir o padrão SIP.

2.5 QoS em Voip

Desde sua origem, o protocolo IP foi desenvolvido e implementado como um protocolo de comunicação com controle de tráfego utilizando a regra do melhor esforço (*Best-effort Service ou Lack of QoS*), que não provê nenhum mecanismo de qualidade de serviços e, conseqüentemente, nenhuma garantia de alocação de recursos da rede. Na época, ninguém imaginava que a Internet se tornaria a grande rede mundial que é atualmente. E, desse rápido crescimento da Internet, a tendência atual é a integração de voz (telefonia) e dados numa única infra-estrutura de redes de pacotes, a rede IP. Essa emergente e crescente demanda pelos serviços IP *Telephony*, como chamado pelo mercado, provocou uma corrida frenética dos fabricantes de equipamentos de redes para desenvolver protocolos que garantissem qualidade de serviços fim-a-fim.

Em uma rede que utiliza a tecnologia pode ocorrer:

2.5.1 Atraso

- ✓ *Echo* (eco) – Causado pela reflexão de sinal. Significativa quando *rountrip* > 50 ms.
- ✓ Sobreposição – Quando a voz de um interlocutor atravessa a do outro. Ocorre quando o atraso fica grande (>250ms)
- ✓ Algoritmo – Necessidade de receber uma quantidade de frames de voz para só então processá-los.
- ✓ Processamento – Causado pela codificação e encapsulamento para transmissão na rede: *Jitter* Buffer.
- ✓ Atraso da rede – Tempo usado pelo meio físico para transmissão (Velocidade do meio; atrasos em *routers*; buffer contra variação.

2.5.2 Soluções de Contorno

Algumas soluções que podem ser tomadas *Echo Cancellation* e *Minimizar delay x Jitter.*

2.5.2.1 Echo Cancellation

- ✓ -Necessário na maioria dos casos (*delay* > 50ms)
- ✓ -Requerimentos de desempenho definidos na ITU G.165
- ✓ -Componentes: Correlator (tamanho do atraso); FIR *Filter* (remove o *echo*); Speech detector (detecta voz)

2.5.2.2 Jitter

- ✓ -Uso de buffer para aguardar os *packets* mais lentos – causa *delay* adicional
- ✓ Objetivos conflitantes: Minimizar *delay* x *Jitter*

2.6 Criptografia

A palavra criptografia vem das palavras gregas que significam “escrita secreta”.

Segundo Palu (2005) a criptografia pode ser usada para codificar dados e mensagens antes que esses sejam enviados por vias de comunicação, mesmo que sejam interceptados, dificilmente possam ser decodificados (decifrados).

Para garantir a privacidade, são usados algoritmos que funcionam como uma fórmula ou uma função matemática que converte os dados originais em um texto cifrado. Esses algoritmos dependem de uma variável chamada chave, que é fornecida pelo usuário e funciona como uma senha, pois somente de posse dela será possível decifrar o texto. Existem dois tipos de chaves: Chaves Simétricas e Chaves Assimétricas.

Em ambientes de rede que utilizam tecnologias sem fio, as questões relativas à segurança tornam-se críticas, uma vez que os dados e informações trafegam pelo ar, e não por um meio guiado. Assim, tais ambientes possuem uma necessidade maior de mecanismos que venham a prover segurança no acesso à rede propriamente dita, dentre os quais, destacam-se os mecanismos de criptografia.

Dentre os padrões de criptografia adotados pelo IEEE 802.11, tem-se o WEP (*Wired Equivalency Privacy*) e o WPA (*Wi-Fi Protected Acccess*), VPN apresentados a seguir.

2.6.1 WEP (Wired Equivalent Privacy)

O protocolo WEP, prove cifração de dados e privacidade nas informações trafegadas pelas redes wireless. (RUFINO, 2005). Utiliza o conceito de chaves compartilhadas ou *Shared Key* e processa os dados utilizando chaves idênticas em ambos os dispositivos de conexão. Para cifrar informações uma chave de 64 ou 128 bit é utilizada, sendo desses valores 24 bits de um Vetor de

Inicialização, que a cada pacote é alterado aleatoriamente para melhor proteger a chaves. (BRAGA EDNEY; ARBAUGH, 2003).

O protocolo WEP utiliza uma função chamada CRC-32 para detecção de erros que realiza um cálculo sobre os dados a serem transmitidos e gera um resultado ICV (*Integrity Check Value*), este resultado é checado no momento em que chega ao receptor, o intuito é verificar se a mensagem foi alterada durando a transmissão de dados. (MARTINS AGUIAR).

2.6.2 WPA

De acordo com RUFINO (2005), o protocolo WPA (*Wi-fi Protect Access*), é um protocolo posterior ao WEP, trouxe algumas modificações como autenticação de usuários, para isto faz uso do padrão 802.1x e EAP (*Extensible Authentication Protocol*), podendo também ser utilizado com chaves compartilhadas, dessa forma se comporta exatamente como o WEP. Oferece segurança para diferentes tipos de redes, atendendo desde pequenas redes domesticas até grandes corporações

Rufino afirma ainda que, pode ser configurado em redes do tipo infra-estrutura, utilizando um servidor RADIUS (*Remote Authentication Dial-In User Server*) para autenticação de usuários.

Além do valor do ICV, já utilizado pelo WEP, a integridade no WPA é composta por mais um valor que é adicionado ao quadro uma mensagem de verificação de integridade denominada MIC (Message Integrity Check). O algoritmo que implementa o MIC denomina-se Michael.

Cifragem	WEP	WPA
	Com falhas, segurança quebrada por cientistas e hackers	Resolve todas as falhas do WEP
	Chaves de 64 e 128 bits estáticas, sendo 24 bits para o Vetor de Incialização	Chaves dinâmicas de 128 bits + combinação de sessão de logon.
	Distribuição de chaves manual	Distribuição de chaves automática.
Autenticação	Com falhas; Autentica somente o dispositivo	Autenticação baseada no usuário, com a utilização da arquitetura 802.1x/EAP

Tabela 2 de comparação WEP e WPA

2.6.3 VPN

Uma Rede Particular Virtual (Virtual Private Network - VPN) é uma rede de comunicações privada normalmente utilizada por uma empresa ou um conjunto de empresas e/ou instituições, construída em cima de uma rede de comunicações pública (como por exemplo, a Internet). O tráfego de dados é levado pela rede pública utilizando protocolos padrão, não necessariamente seguros.

VPNs seguras usam protocolos de criptografia por tunelamento que fornecem a confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas. Quando adequadamente implementados, estes protocolos podem assegurar comunicações seguras através de redes inseguras.

OpenVPN é código um livre e aberto de rede privada virtual (VPN). É um programa para criar ponto-a-ponto ou servidor-a-hospedeiro, cifrados entre vários computadores. É capaz de estabelecer ligações diretas entre computadores que estão por trás de *firewalls* NAT, sem exigir reconfiguração. Foi escrito por James Yonan e publicado sob a GNU *General Public License* (GPL).

O OpenVPN permite que suas interligações usem uma chave secreta pré-compartilhada, certificados, ou nome de usuário e senha. Quando usado

em várias arquiteturas clientes/servidor, permite que o servidor libere para cada cliente a autenticação de certificado para utilizar assinatura e o Certificado Autoridade. Ele utiliza a criptografia *OpenSSL*, assim como o protocolo *SSLv3*/TLSv1. Ele está disponível para *Solaris, Linux, OpenBSD, FreeBSD*, *NetBSD*, Mac OS X e Windows 2000/XP/Vista. Ele contém muitas funcionalidades de segurança e controle. Não se trata de uma web baseada em VPN, e não é compatível com o *IPSec*, VPN ou qualquer outro pacote. Sua conexão cliente e servidor pode ser configurada para um ou mais arquivos chaves, dependendo do método de autenticação usado. Muitas vezes, é utilizada para games de computadores, como modo de proteção à *LAN* e jogos através da Internet.

2.6.3.1 Funcionamento

Basicamente, quando uma rede quer enviar dados para a outra rede através da VPN, um protocolo, exemplo IPSec, faz o encapsulamento do quadro normal com o cabeçalho IP da rede local e adiciona o cabeçalho IP da Internet atribuída ao Roteador, um cabeçalho AH, que é o cabeçalho de autenticação e o cabeçalho ESP, que é o cabeçalho que provê integridade, autenticidade e criptografia à área de dados do pacote. Quando esses dados encapsulados chegarem à outra extremidade, é feito o desencapsulamento do IPSec e os dados são encaminhados ao referido destino da rede local.

3. MATERIAL E MÉTODOS

Neste capitulo será mostrado os materiais utilizado nas análises e suas configurações, os resultados será visto no capitulo 4.

3.1 Asterisk

Segundo o autor Flávio Eduardo de Andrade, Asterisk é um software de PABX que usa o conceito de *software* livre (GPL), criado pela Digium Inc., e uma base de usuários em contínuo crescimento.

Segundo a Digium, ela tem investido tanto no desenvolvimento do código fonte do Asterisk, quanto em hardware de telefonia de baixo custo, que tem funcionamento com o Asterisk. O Asterisk é compatível com a plataforma Linux e em plataformas Unix, com ou sem hardware conectado à rede pública de telefonia, PSTN (*Public Service Telephony Network*). O Asterisk permite conectividade em tempo real entre as redes PSTN e redes Voip. Com o Asterisk, você não apenas tem uma troca excepcional do seu PABX. O Asterisk é muito mais que um PABX padrão. Com o Asterisk em sua rede, você pode criar coisas novas em telefonia. Por exemplo: Conectar empregados trabalhando de casa ao PABX do escritório, sobre conexões de banda larga

3.1.1 Configuração dos telefones IP SIP

O SIP é configurado no arquivo /etc/asterisk/sip.conf, o qual contém parâmetros para configurar os telefones e operadoras SIP. Para fazer e receber chamadas, os clientes devem estar configurados. O arquivo SIP é lido de cima para baixo. Na primeira parte, encontram-se as opções globais [*general*]. Estas opções são: o endereço IP e número de porta ao qual o servidor está ligado. Logo depois se encontram os parâmetros de clientes, tais como o nome do usuário, senha, e endereço IP default para clientes não registrados.

3.1.2 Configurações globais (Seção [general])

allow: Permite que um determinado *codec* seja usado.
bindaddr: Endereço IP onde o Asterisk irá esperar pelas conexões SIP. O comportamento padrão é esperar em todas as interfaces e endereços secundários.
context: Configura o contexto padrão, onde todos os clientes serão colocados, a menos que seja sobrescrito na definição da entidade.
disallow: Proíbe um determinado *codec*.
port: Porta que o Asterisk deve esperar por conexões de entrada SIP. O padrão é 5060.
tos: Configura o campo TOS (tipo de serviço) usado para o SIP e RTP.
Os valores aceitáveis são *lowdelay, throughput, reliabilit*y e *mincost*. Um inteiro de 0-255 deve ser especificado.
maxexpirey: Tempo máximo para registro em segundos.
defaultexpirey: Tempo padrão para registro em segundos.
register: Registra o Asterisk com outro host. O formato é um endereço

3.1.3 Opções para cada telefone

As entradas são divididas em três categorias:
peer Entidade para o qual o Asterisk envia chamadas (Provedor).
user: Entidade que faz chamadas através do Asterisk.
friend: Os dois ao mesmo tempo, o que faz sentido para os telefones
type: Configura a classe de conexão. As opções são *peer*, *user* e *friend*.
host: Configura o endereço IP ou o nome do *host*. Pode se usar também a opção ‘dynamic’, onde se espera que o telefone seja registrado. É a opção mais comum.
username: Esta opção configura o nome do usuário que o Asterisk tenta conectar, quando uma chamada é recebida. Usado por alguma razão, o valor não é o mesmo do nome de usuário do cliente registrado.
secret Um segredo compartilhado, usado para autenticar os *peers* e *users* fazendo uma chamada.

3.1.4 Configuração do Asterisk para as análises.

Para a realização do estudo, foi utilizado um servidor para sistemas de telefonia: o Asterisk versão 1.4, instalado no sistema operacional Linux UBUNTU. Sua configuração está expressa abaixo:

Cadastro de clientes SIP:

[8000]
callerid=Alex
username=8000
secret=1379
host=dynamic
type=friend
context=interno

Onde,

[*8000*]: número do ramal
Callerid: define o identificador de chamada
Username: define o nome do usuário para a autenticação
Secret: define a senha utilizada na autenticação
Host: define o endereço IP do usuário. Pode ser um endereço estático ou a palavra chave "*dynamic*".

Para configurar o sip.conf, editamos o arquivo /etc/asterisk/sip.conf. Este arquivo tem uma série de configurações na seção. Configuramos a seção [GENERAL].

Foi cadastrado outro usuário com os mesmos procedimentos, alterando apenas o ramal, utilizando outro número.

No asterisk não basta somente essas configurações. Para que um telefone possa comunicar-se com o outro, é necessário configurar um arquivo encontrado em */etc/asterisk/extensions.conf*. Neste arquivo, configura-se o plano de discagem, cuja configuração está logo abaixo:

exten => _8XXX,1,Dial(SIP/${EXTEN})
exten => _8XXX,2,Hangup()

onde o ‘X’ é o ramal que foi escolhido

3.2 Configuração do OpenVPN para a realização das análises.

Primeiramente, é necessário abrir o *console* do servidor, criar uma interface com o comando ***openvpn server.ovpn &.***

Para configurar o OpenVPN, temos que gerar uma chave secreta na própria opção do OpenVPN, situada na sua pasta de instalação chamada *Generate a Static OpenVPN key*. Após criá-la, é necessário criar outro arquivo com extensão .ovpn que será salva na pasta *config*, como mostra as configurações abaixo.

dev tun
port 5000
ifconfig 10.0.0.1 10.0.0.2
secret server.key

Após isso, é necessário copiar e colar estes dois arquivos no servidor, na pasta *config*. Para ligar o tunelamento, é necessário ir à pasta de instalação do OpenVPN e clicar numa aplicação chamada OpenVPN GUI.
Quando este tiver vermelho na barra, significa que estará desconectado; amarelo indica a espera de conexão com o servidor e, finalmente verde, significa que a conexão foi realizada com sucesso. Observe as figuras abaixo:

Figura 4: Vpn Desconectada

Figura 5 Vpn Esperando O Servidor Se Conectar

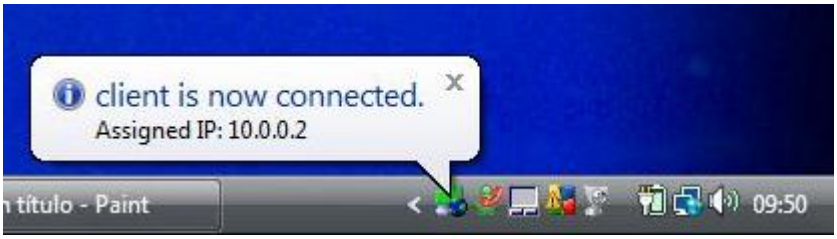

Figura 6: Vpn Conectada

3.3 Configuração do X-lite para análises

Clica-se no X-Lite, Sip Account Settings. Depois que o servidor estiver configurado como mostra no tópico 3.1.4, apenas é colocado os seguintes dados:

Figura 7: Sip Account Settings

Após o clique, apenas preenchemos como mostra abaixo:

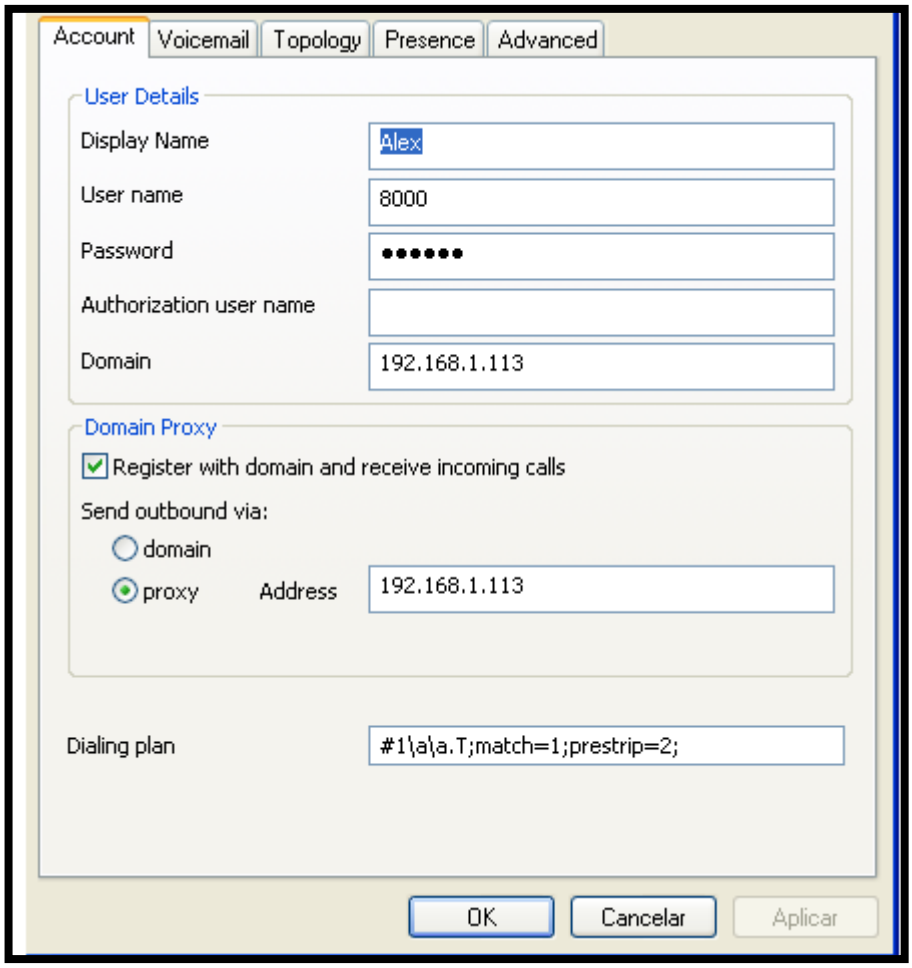

Figura 8: Conexão com o Servidor

Para fazer a ligação com VPN, após conectar o cliente com o servidor pelo software OpenVPN, como mostrado no 3.2, alteramos o IP do *domain* e *proxy* como mostra na figura 17, ficando desta forma:

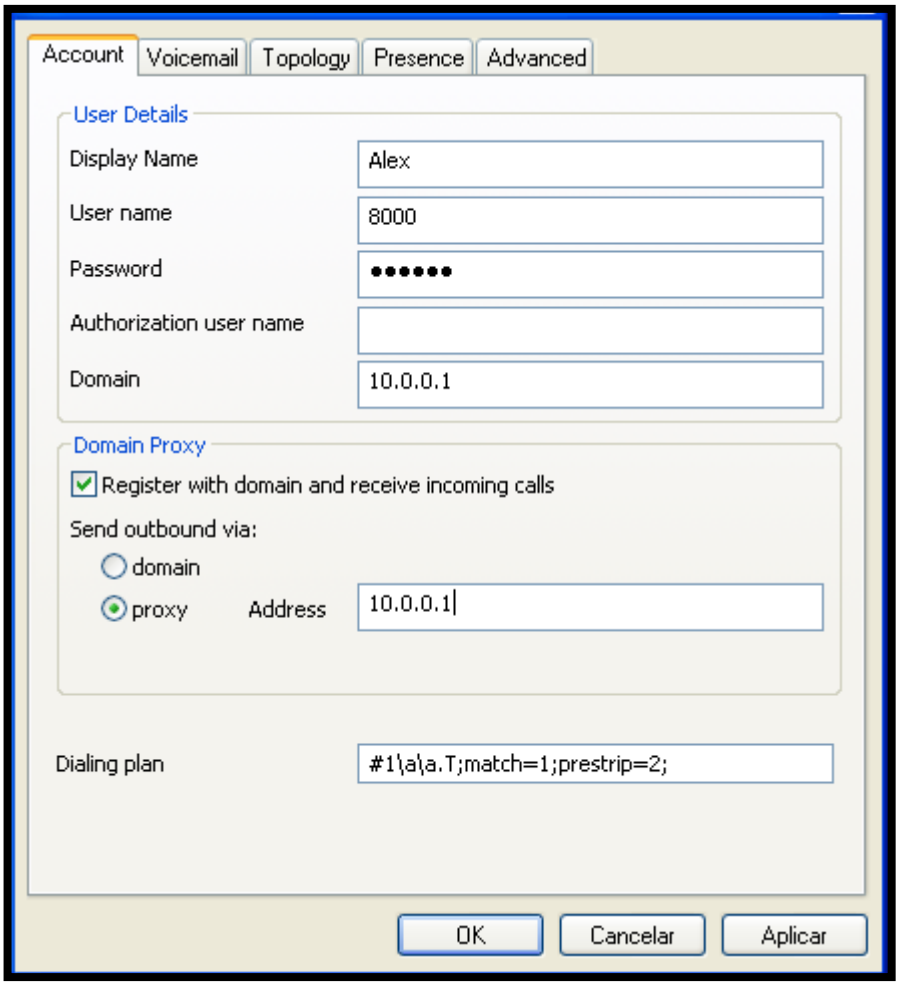

Figura 9: Conexão com o Servidor utilizando VPN

3.4 Wireshark

Wireshark é um dos principais protocolos analisador de tráfego, e é muito utilizado em indústrias e instituições educacionais. Wireshark é a principal rede mundial analisadora de protocolo, e é, de fato, padrão em muitas indústrias e instituições educacionais.

O Wireshark teve seu desenvolvimento, graças às contribuições de especialistas do mundo todo. O início de seu desenvolvimento começou em 1998, e até hoje o *software* passa por mudanças e transformações. O Wireshark possui um rico conjunto de recursos e características, dentre os quais podemos destacar alguns:

- Faz inspeção de centenas de protocolos todo o tempo.
- Faz captura e análise *offline*.
- Funciona em *Windows, Linux, OS X, Solaris, FreeBSD, NetBSD*, e muitos outros .
- Um dos mais poderosos filtros de exibição na indústria.

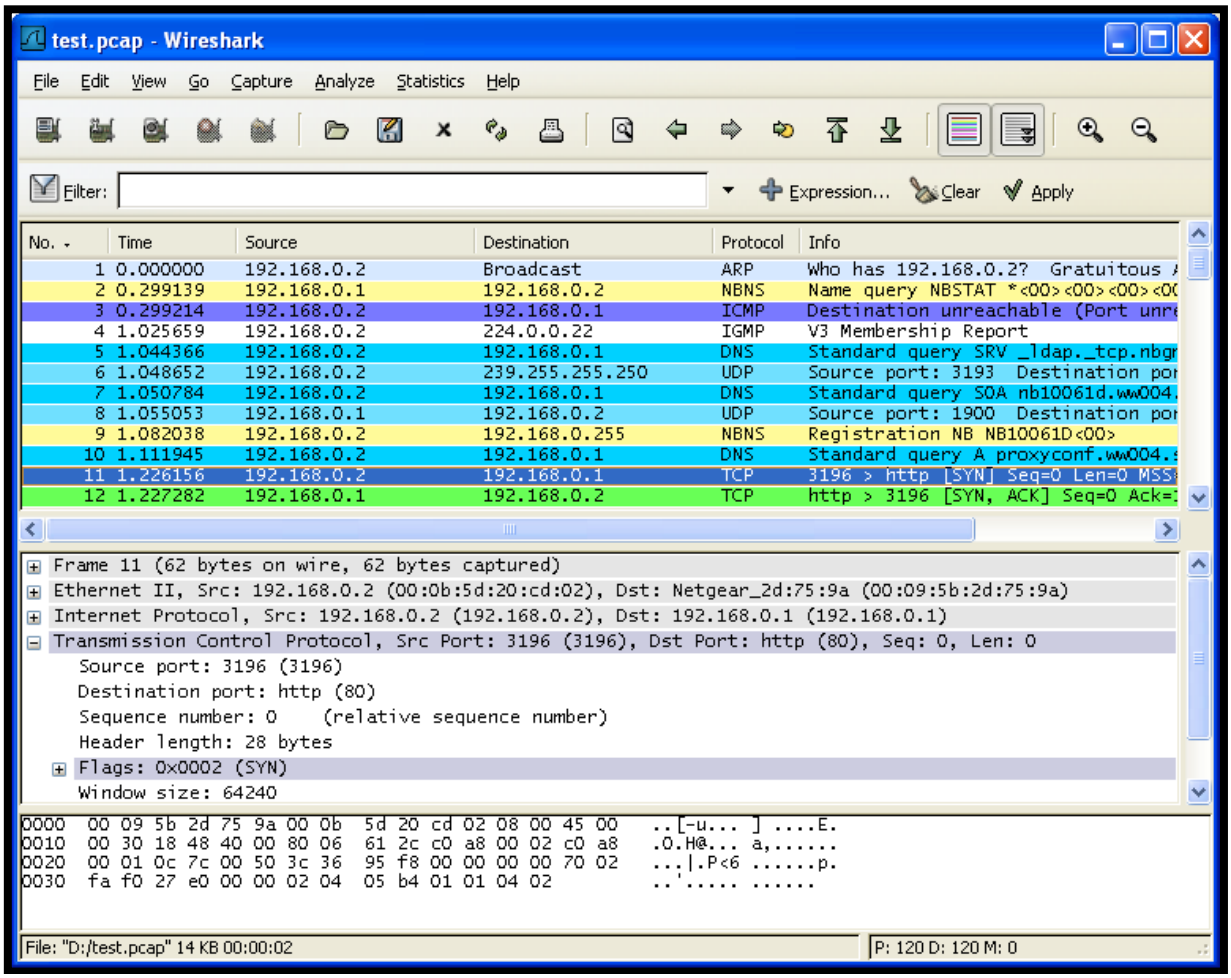

Figura 10: Demonstração Wireshark

4. ANÁLISES E CAPTURAS REALIZADAS

Depois de instalado e configurados todos os softwares apresentado no capitulo 3. Foi escolhida duas músicas para realização dos testes. A primeira com 8min e 12seg, a segunda com 2min e 25seg. Foram realizado testes em rede wireless com tipos de segurança distintas:

Criptografias Utilizadas:

- WPA
- WPA+vpn
- WEP 128 +Vpn
- WEP 128
- WEP + vpn
- WEP

As análises seguem nas figuras 19 a 24, retirado do programa Wireshark (tópico 3.4) que fez as coletas do tráfego na rede:

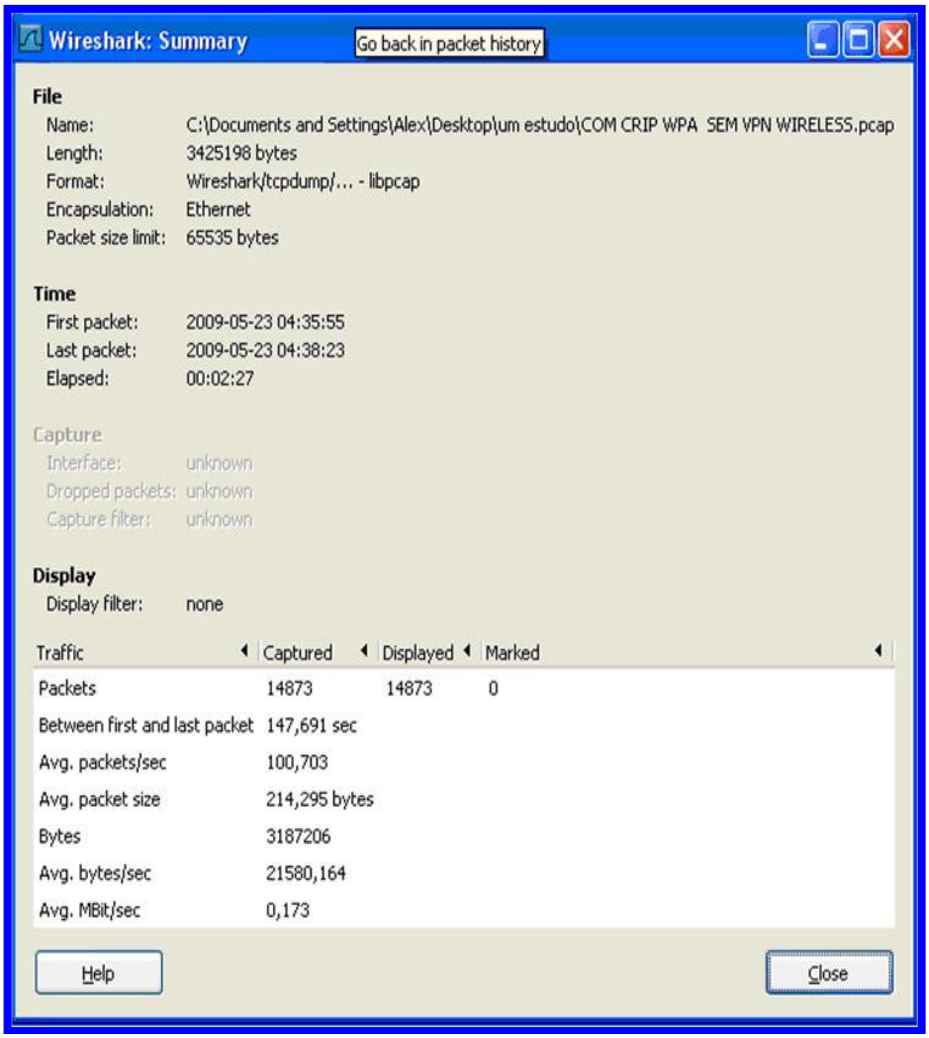

Figura 11: Análise com a Criptografia WPA TKIP

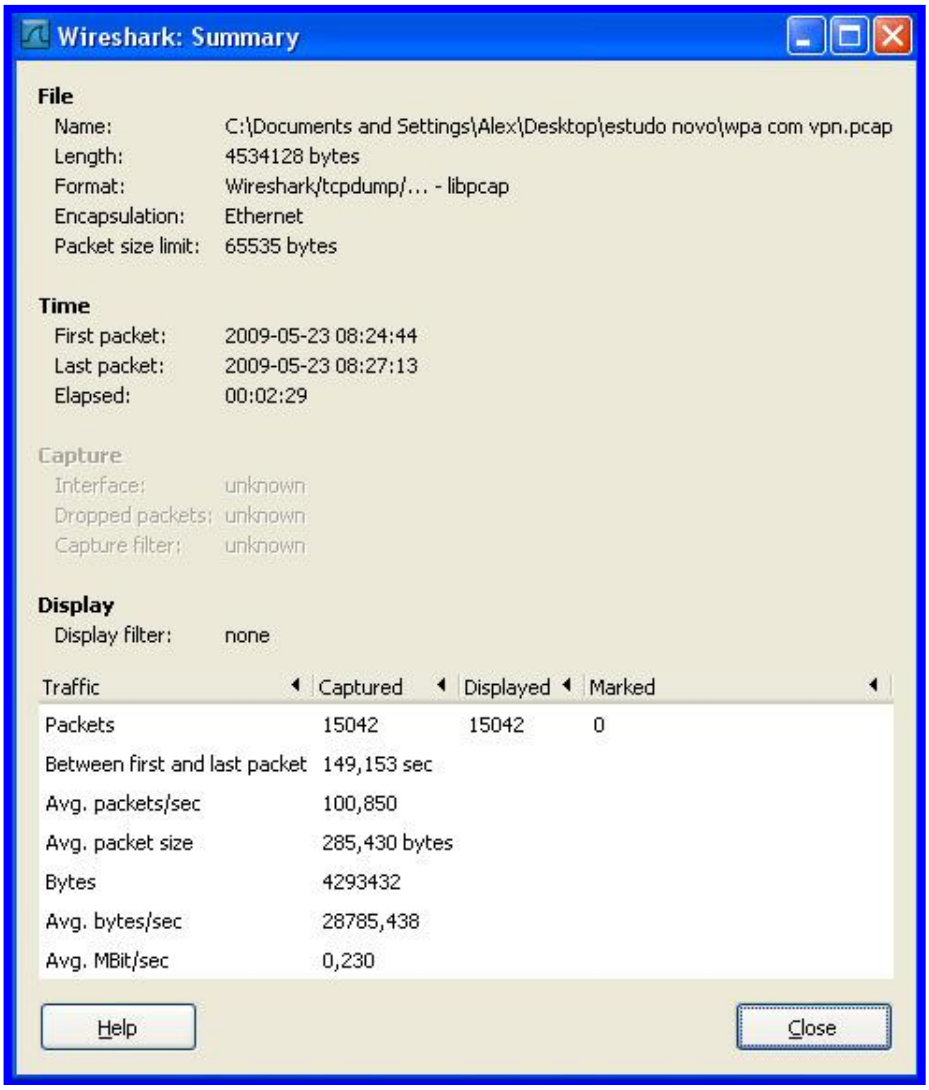

Figura 12: Análise com a Criptografia WPA + VPN.

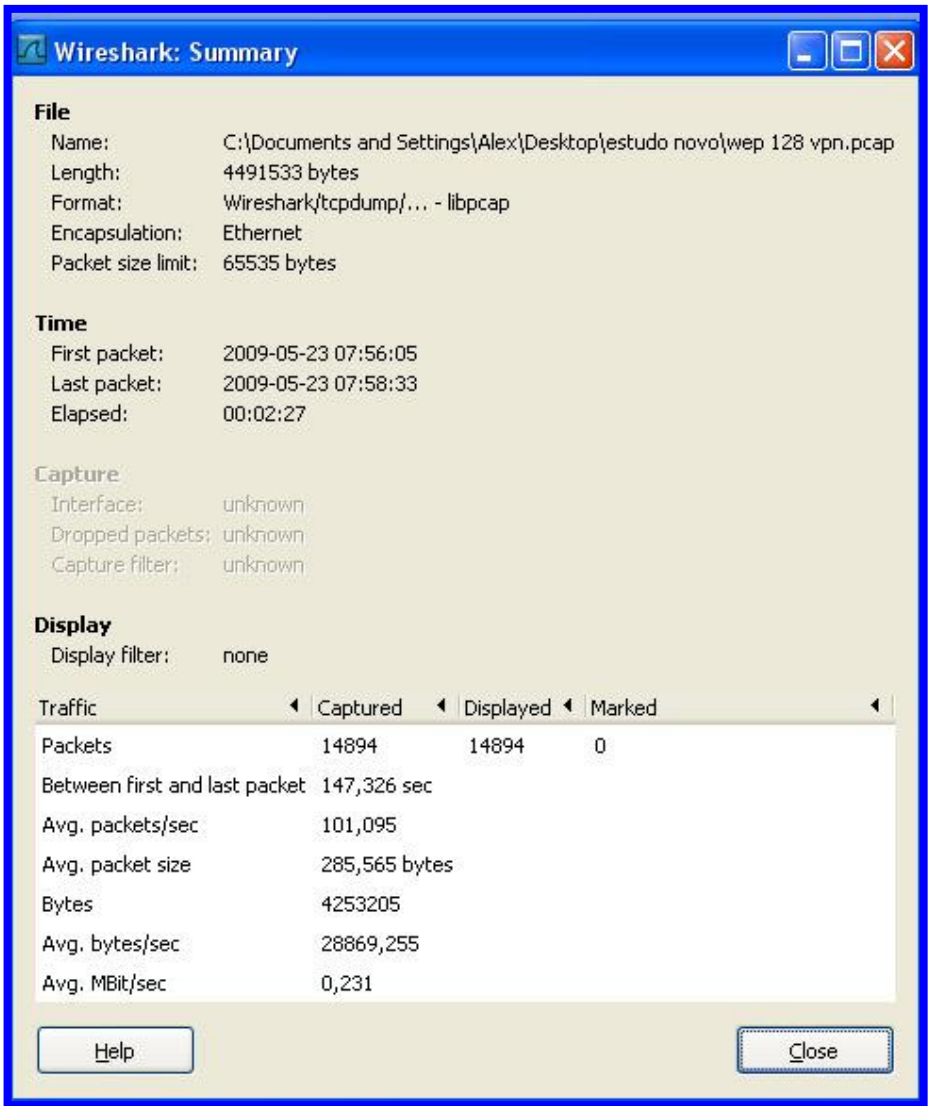

Figura 13: Análise com a Criptografia WEP 128 + VPN.

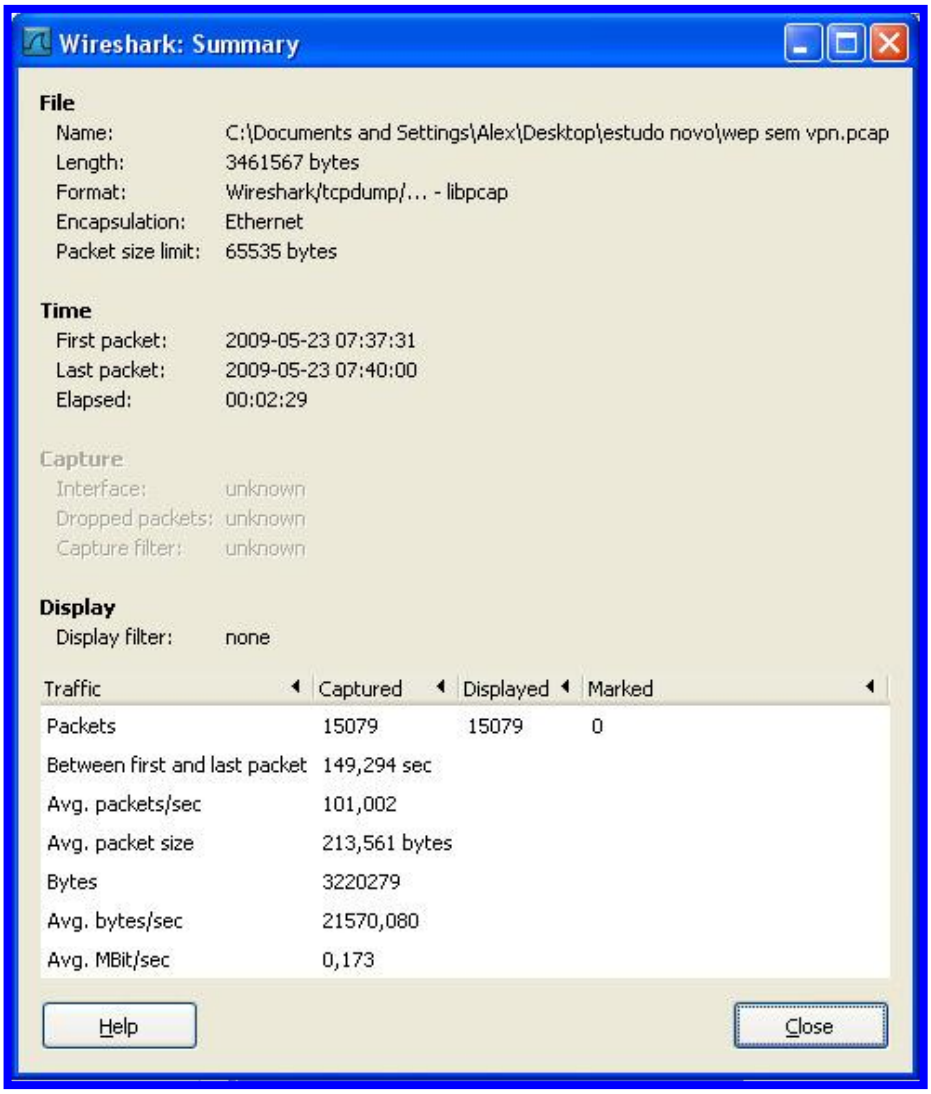

Figura 14: Análise com a Criptografia WEP 128

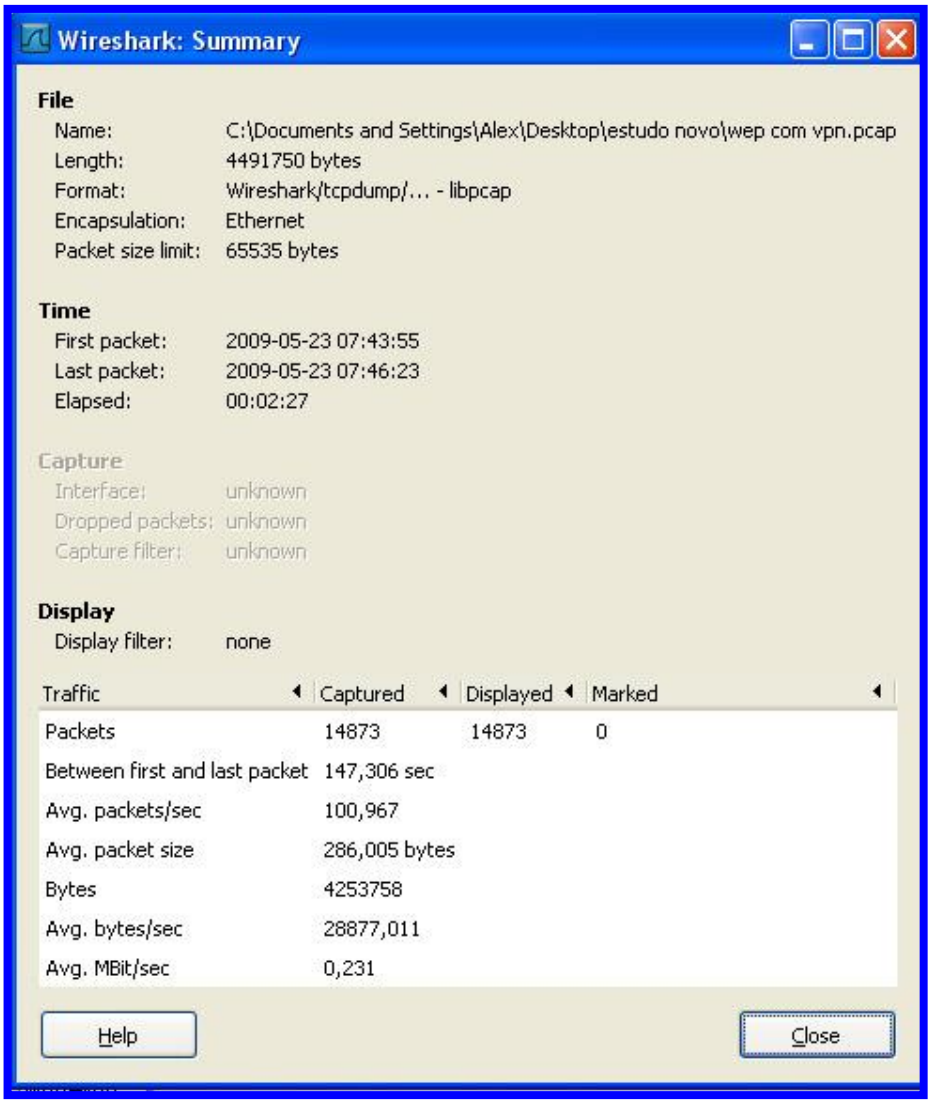

Figura 15: Análise com a Criptografia WEP + VPN.

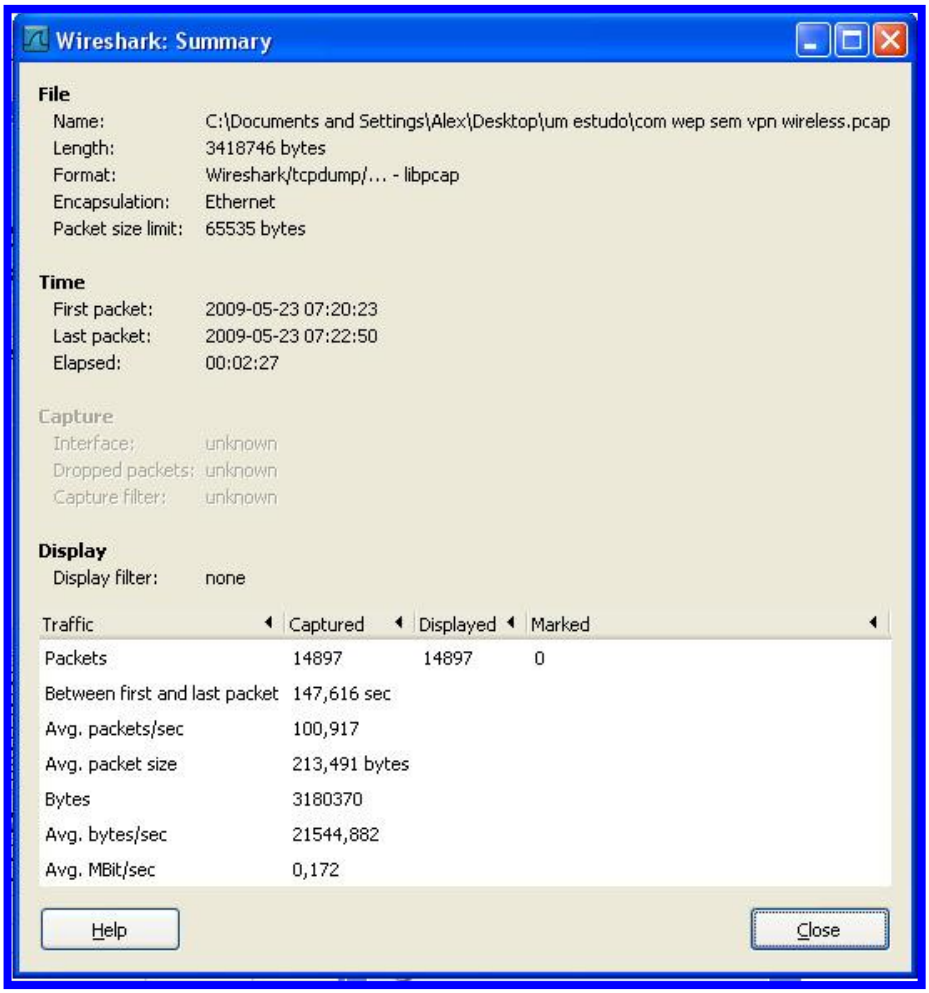

Figura 16: Análise com a Criptografia WEP.

Na figura 25, apresenta os resultados comparativos das capturas, com a implementação de diferentes criptografias.

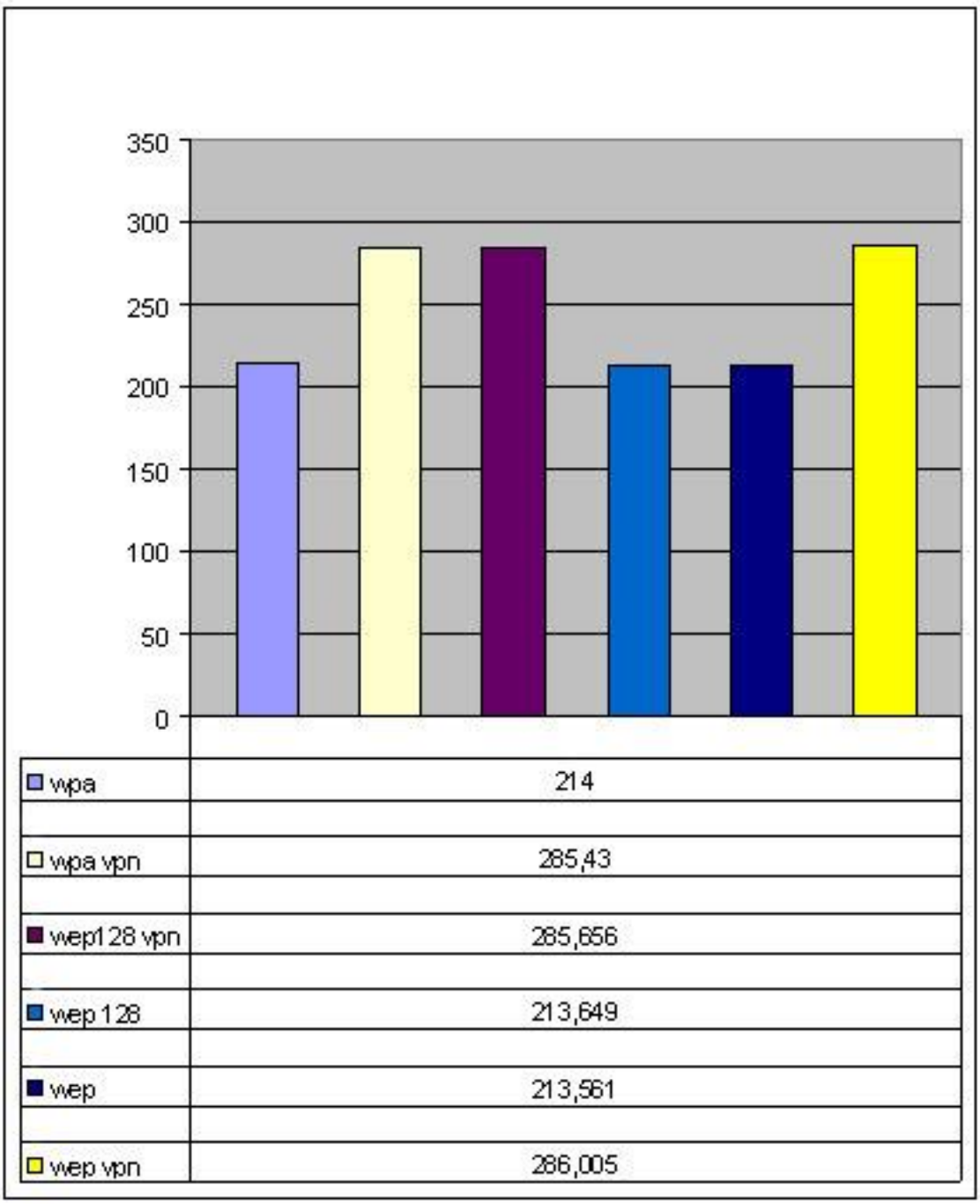

Figura 17: Tamanho dos pacotes com Distintas Criptografias.

A rede divide uma mensagem em partes de um determinado tamanho em bytes. Estes são os pacotes. Cada pacote carrega a informação que o ajudará a chegar a seu destino que contém o endereço IP do emissor e o endereço IP do destinatário pretendido.

Nas capturas realizadas, há semelhança nos tamanhos dos pacotes com criptografias WPA, WEP e WEP128. Outra semelhança encontra nos pacotes com WPA+VPN, WEP+VPN e WEP128+VPN.

Em telecomunicações, a largura da banda ou apenas banda (também chamada de débito) refere-se à rede de transferência de dados, ou seja, a quantidade em bits/s que a rede suporta.

Segundo às coletas do tráfego, quando uma VPN é colocada junto com outra criptografia, os pacotes tem aumento de tamanho. Foi possível analisar as velocidades consumida nas bandas em cada ligação VoIP. Cada criptografia faz com que a conexão requeira distintamente velocidades como mostra na figura 26.

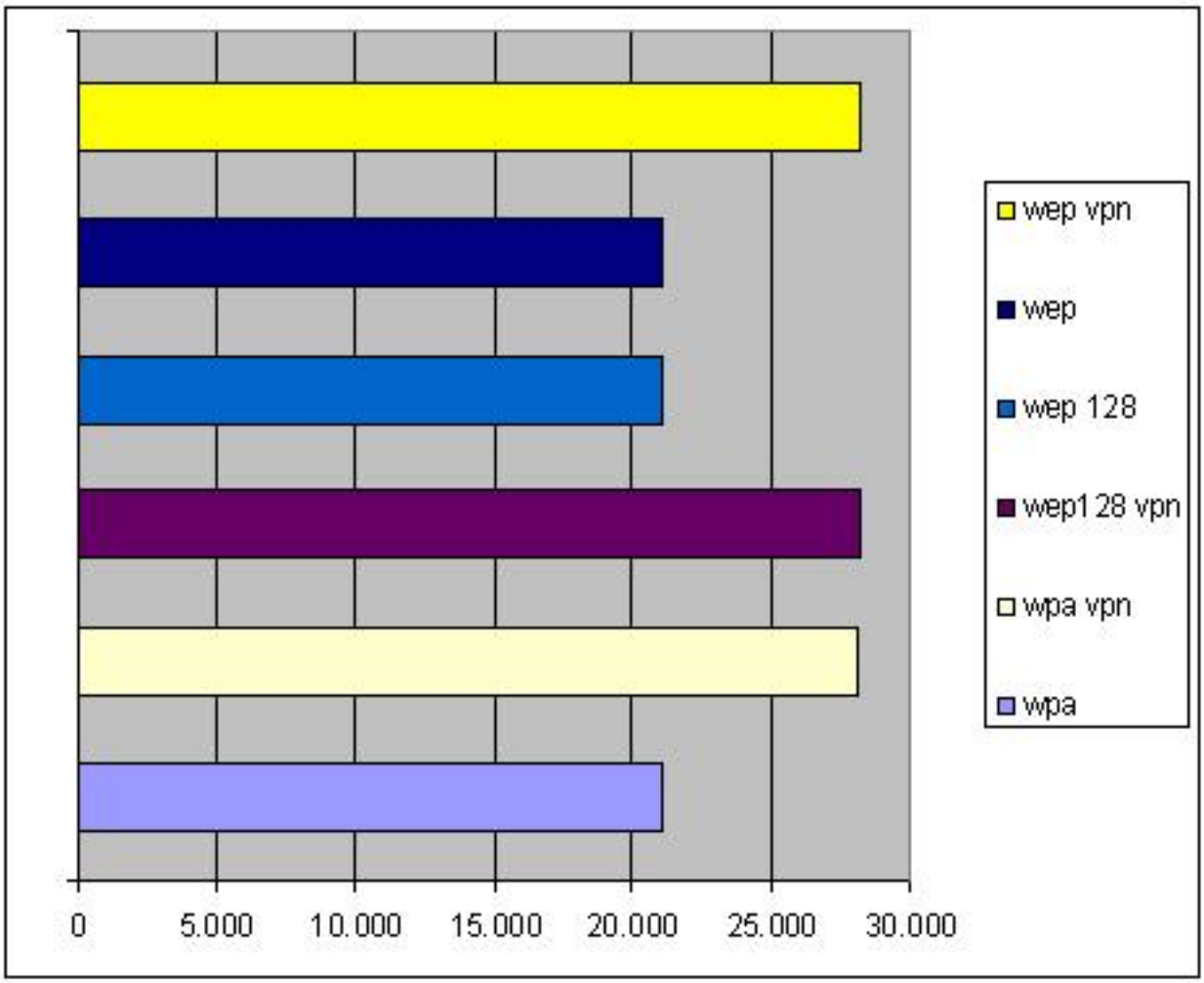

Figura 18: Consumo de Banda em Kbps.

5. CONCLUSÕES E TRABALHOS FUTUROS

Como mencionado, a tecnologia VOIP surgiu para integrar duas redes muito importantes dentro de uma organização: a rede de dados e a de telefonia. Atualmente estudos e implementações VoIP vem sendo um grande foco para pesquisadores e organizações.

Este estudo teve como objetivo apresentar a tecnologia VOIP, seu funcionamento, suas características gerais, e compreender os impactos que a criptografia causa nos pacotes de voz e no consumo de banda em redes IP´s *wireless*.

Através dos testes realizados, constatou-se que a utilização de criptografia como o WPA, WEP, WEP 128 causam tanto na largura de Banda como nos pacotes impactos equivalentes, distintamente de uma Rede Virtual Privada, que causam em torno de 34,7% de aumento nos pacotes a mais além de consumir maior banda. Isto diferencia das outras criptografias que causam impactos bem menores como mostrado no capitulo 4.

Pelos resultados das análises mostram também que é viável usar criptografia WEP e WPA para quem possui consumo de banda escassa do que estar implementando uma VPN, que muito diferencia no consumo de banda.

O trabalho mostrou que é possível colocar duas criptografias em uma ligação Voip. Quando colocado WPA, WEP e WEP 128 é possível estar implementando uma Rede Virtual Privada, mas não é possível usar WPA e WEP ao mesmo tempo.

No levantamento bibliográfico, diversas foram as falhas encontradas no protocolo WEP, tanto no aspecto de integridade, pois uma mensagem poderia ser alterada, como na autenticação com a captura da chave secreta. Estas falhas foram exploradas e publicadas na internet, fato este que levou a criação de uma força tarefa para solucionar os problemas apresentados: Criaram a criptografia WPA, que logo após encontraram falhas e surgiu a WPA2.

Em qualquer situação, cabe mencionar, que é preciso analisar com atenção os requisitos e especificações do ambiente em questão, tais como qualidade de serviço, proteção de ativos, confidencialidade de dados; avaliando a melhor relação custo X benefício para aplicar criptografias.

Como sugestão para trabalhos futuros, pode-se ampliar o rol de protocolos utilizados nos testes, bem como os ambientes de rede, diversificando os cenários de testes e aumentando a inserção de tráfego. Pode-se, ainda, avaliar outros mecanismos de segurança, como o WPA2 .

APÊNDICE I - SoftPhone X-Lite

A figura 1 mostra um telefone IP, *softphone* que será utilizado para fazer as análises.

Figura 1: SoftPhone X-Lite na versão 3.0

Fonte: CounterPath, 2008

Características Gerais do SoftPhone X-Lite.

O X-Lite é um software que apresenta todas as características de um terminal VoIP, entre as quais se sublinham as seguintes:

1. Duas Linhas;
2. Opção *Mute* – Sem Som;
3. Remarcar;
4. Colocar em Espera;
5. Opção DND (Do *Not Disturb*) – Não incomodar;
6. Histórico de Chamadas – recebidas, efetuadas, perdidas;
7. Reencaminhamento de chamadas;
8. Gravação de Chamadas;

9. Suporte de *Codecs*: G.711aLaw, G.711uLaw, GSM e iLBC.

Utilização do Softphone X-Lite

Nesta seção, será indicado como o Utilizador facilmente pode efetuar as funcionalidades base que o X-Lite SoftPhone permite. Estas funcionalidades são:

1. Efetuar, Receber e Terminar Chamadas;
2. Colocar Chamada em Espera;
3. Efetuar Conferências, utilizando as duas Linhas Disponíveis;
4. *Auto-Attend, Do Not Disturb* e *Auto-Conference.*

Efetuar, Receber e Terminar Chamadas

1. Para efetuar uma chamada, deverá digitar um número através do seu teclado ou, utilizando o rato (mouse), através do teclado disponível no X-Lite, e assinalado a azul na figura 2. Depois, deverá pressionar o botão assinalado a verde.

2. Para Receber uma chamada quando o X-Lite tocar, sinalizando uma chamada, deverá somente pressionar o botão assinalado a verde, possibilitando o início da conversação.

3. Para Terminar uma chamada, deverá somente pressionar o botão assinalado a vermelho.

Figura 2: – Efetuar, Receber e Terminar Chamadas

Fonte: CounterPath, 2008

Colocar Chamadas em Espera

Para Colocar uma chamada em Espera é necessário apenas selecionar o Botão HOLD, indicado a vermelho na imagem. Para retirar a chamada de espera, deverá selecionar novamente o botão

Figura 3: Chamadas em Espera, (utiliza o botão HOLD)

Fonte: CounterPath, 2008

Utilizar Duas Linhas

Para manter duas chamadas em duas linhas separadas, deverá primeiro efetuar uma chamada de acordo com o primeiro ponto desta seção. Depois, deverá pressionar o botão *FLASH* assinalado a vermelho na Figura 4. Finalmente, deverá repetir o processo de execução de uma nova chamada. Para trocar entre as duas chamadas, colocando uma delas em espera e a outra ativa, deverá utilizar os botões 1 e 2, assinalados a verde na imagem

Figura 4: Utilizar Duas Linhas

Conferências

Para Efetuar Conferências, deverá primeiro executar o processo indicado no ponto anterior, para a utilização de duas linhas. Deverá efetuar as chamadas para os destinatários, com os quais se pretende efetuar uma conferência. Depois, será apenas necessário selecionar o botão assinalado em vermelho na Figura 5, para a conferência ser executada.

Figura 5: Conferências

ANEXO I - Telefone IP wireless

São equipamentos que estão à venda no mercado que possibilitam maior mobilidade, por não precisarem de fios para o seu funcionamento, e serem pequenos e leves. Com as redes wireless, é possível fazer ligações de qualquer lugar. Só é preciso que o telefone IP wireless localize um ponto de acesso que esteja disponível. Sua aparência é parecida com os aparelhos celulares padrões, onde tem aplicações em comum: calculadora, agenda telefônica, calendário, horas, entre outros.

Normalmente, os telefones IP wireless tem o recurso *roaming*, permitindo que os usuários se locomovam em grandes áreas revestidas por mais de um ponto de acesso e, assim, mantendo a comunicação VoIP sem interrupções. Também é possível fazer uso de chaves criptográficas (WEP, WAP) para maior privacidade e segurança nas conversas. Existem tanto telefones IP wireless simples, como também os mais modernos, como é o caso da Figura 1: o da LinkSys, modelo WIP330 IP Phone (LINKSYS, 2007).

Figura 1 Telefone IP wireless da Linksys modelo WIP330 IP Phone

Fonte: LinkSys, 2007

Características:

a) LCD colorido;
b) chamada em espera;
c) identificador de chamada, siga-me e mudo;
d) duração da bateria 3h de conversação;
e) criptografia WEP de 64 e 128 bits;
f) recurso *roaming*.

Telefone IP

Figura 2 Telefone IP GrandStream BudgeTone 200

(Fonte: GrandStream, 2007)

Tem as opções básicas em um ramal IP, dando facilidade e autonomia nas ligações, como mostra o exemplo na Figura 2: um telefone IP da GrandStream, modelo BudgeTone 200 (GRANDSTREAM, 2007).

Características:

a) Visor de Cristal Líquido (LCD);

b) identificador de chamadas;

c) data e a hora;

d) viva voz;

e) duas linhas simultâneas, mudo, conferência;

f) entrada para *HeadSet*.

Telefone IP avançado

Possui todas as funcionalidades de um telefone IP simples, além de outras funcionalidades e facilidades mais aprimoradas para fazer e receber ligações. O telefone *Unified* Cisco 7970G, conforme Figura 3, é estimado atualmente como um dos telefones IP mais modernos achado no mercado, disponibilizando os últimos avanços da telefonia IP (*SYSTEM, 2007*).

Figura 3 : Telefone IP Cisco Unified IP Phone 7970G

Fonte: Cisco, 2007

Referências Bibliográficas

SOUZA, JOÃO PAULO PEREIRA DE. sIPtel –**Um sistema de IPtel com suporte para vídeo, utilizando o protocolo SIP**. Utad: Universidade de Trás-os-Montes e Alto Douro, 2003. 134p.

OPENVPN. **OpenVPN.** Disponível em: http://openvpn.net/. Acesso em 16 de setembro de 2008.

SILVA, Adailton. **As tecnologias de Rede Wireless Artigo**. Disponível em < http://www.rnp.br/newsgen/9805/wireless.html>. Acesso em: 21 de setembro de 2008.

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

FAGUNDES, Eduardo Mayer. **A convergência das redes de voz.** Disponível em <http://www.platina.unisal.com.br/site/arquivo/Convergencia_das_redes_de%20voz.pdf>. Acesso em: 22 de setembro de 2008.

PINHEIRO, José Maurício Santos. **Vulnerabilidade em Redes Wireless**. Disponível em:<http://www.projetoderedes.com.br/artigos/artigo_vulnerabilidades_em_redes_wireless.php>. Acesso em: 11de outubro de 2008.

HERSENT, Oliver; GUIDE, David; PETIT, Jean Pierre. **Telefonia IP – Comunicação multimídia baseada em pacotes**. 1. ed. Makron Books. Rio de Janeiro: 2002.

VOLTAN JR, Guilherme. **Voz sobre IP - Segurança de Transmissões**. 2005. 104 f. Trabalho de Conclusão de Curso – Universidade Católica de Goiás, Goiás – GO.

FERNANDES, Nelson Luiz Leal. **Voz sobre IP: Uma visão geral**. 2006. 22p.

QUEIROZ, Daniel Cruz **Voz Sobre IP em Redes Corporativas.** 2002. 63 f. Trabalho

de Conclusão de Curso – Universidade de Fortaleza, Fortaleza – CE.

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

TELECO, **Conhecimento em Telecomunicações.** Disponível em < http://www.teleco.com.br/tecvoip.asp >. Acesso em: 03 de março de 2009

UFRJ, **Universidade Federal do Rio de Janeiro,** Disponível em < http://www.voip.nce.ufrj.br/>. Acesso em: 24 de março de 2009

UFRJ, **RTP.** Disponível em < http://www.gta.ufrj.br/grad/03_1/rtp/rtp.htm>. Acesso em: 24 de março de 2009

BRAGA**, R. R. Estudo e análise dos protocolos de segurança em redes sem fio 802.11 e suas vulnerabilidades. Parque Tecnológico de Itaipu: Um estudo de caso. Uberlândia, 2006.** Disponível em: <http://www.datasecur.com.br/academico/Seguranca_em_Sistemas_Voz_sobre_IP.pdf> Acesso em: 17 de março de 2009.

Cisco**, VoIP**. Disponível em < http://www.cisco.com/en/US/tech/tk652/tk701/tsd_technology_support_protocol_home.html>. Acesso em: 03 de abril de 2009