inUNIVERSIDADE ESTADUAL DO NORTE DO PARANÁ
FACULDADES LUIZ MENEGHEL

AMANDA ALVES PINHEIRO

UM ESTUDO DO TRÁFEGO NA TRANSMISSÃO DE VOZ EM REDES IP ASSOCIADA COM MECANISMOS DE SEGURANÇA

BANDEIRANTES - PR
2007

UNIVERSIDADE ESTADUAL DO NORTE DO PARANÁ,
CAMPUS BANDEIRANTES

AMANDA ALVES PINHEIRO

UM ESTUDO DO TRÁFEGO NA TRANSMISSÃO DE VOZ EM REDES IP ASSOCIADA COM MECANISMOS DE SEGURANÇA

Monografia apresentada ao curso de Sistemas de Informação da Universidade Estadual do Norte do Paraná, campus Bandeirantes, para a obtenção do grau de Bacharel em Sistemas de Informação, orientado pelo Prof. Ms. Ricardo Gonçalves Coelho.

BANDEIRANTES – PR
2007

AMANDA ALVES PINHEIRO

UM ESTUDO DO TRÁFEGO NA TRANSMISSÃO DE VOZ EM REDES IP ASSOCIADA COM MECANISMOS DE SEGURANÇA

Monografia apresentada ao curso de Sistemas de Informação da Universidade Estadual do Norte do Paraná, campus Bandeirantes, para a obtenção do grau de Bacharel em Sistemas de Informação.

BANCA EXAMINADORA

_____

Prof. Ms. Ricardo Gonçalves Coelho

Orientador

_____

Prof. Luiz Fernando L. Nascimento

Membro da banca examinadora

_____

Prof. Ms. Ailton Sergio Bonifacio

Membro da banca examinadora

Bandeirantes, _____ de _____ 2007.

Aos meus avós, Leonor e Carlos Pinheiro, e aos meus
Pais, meus heróis.

"É melhor tentar e falhar,
que preocupar-se e ver a vida passar;
é melhor tentar, ainda que em vão,
que sentar-se fazendo nada até o final.
Eu prefiro na chuva caminhar,
que em dias tristes em casa me esconder.
Prefiro ser feliz, embora louco,
que em conformidade viver ..."

Martin Luther King

AGRADECIMENTOS

Agradeço primeiramente a Deus pela Vida e por esta oportunidade. Agradeço aos meus pais Sérgio Alves Pinheiro e Leonilda Furlanetto Pinheiro, por me proporcionarem esses anos de estudos, talvez os melhores anos 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 as amigas: Fernanda Azevedo, Karina Baccili, Lilian Salvi, Mariana Bombonatti, Jacqueline Ferreira e Natália Benatto, pelos momentos de alegrias e tristezas compartilhadas. Agradeço a minha querida irmã Aline Alves, por me alegrar nas horas difíceis. Ao Marcos Vinícius Vascon pela compreensão e companheirismo nos momentos de minha ausência e nas horas que mais precisei para conclusão deste trabalho. E por fim, agradeço a todos que não ajudaram, mas também não atrapalharam minha formação acadêmica.

RESUMO

Diversos protocolos e ferramentas vêm sendo utilizados na transmissão de voz em redes IP associados com mecanismos de segurança. Neste contexto as ferramentas com o código livre estão se destacando. Este trabalho propõe um estudo das transmissões com o software livre Asterisk e a implementação de uma VPN como mecanismo de segurança para essas transmissões de voz. Mediante a utilização de softphone e software de captura de tráfego dos dados na rede, foram feitas análises e comparações das informações capturadas.

Palavras-chave: VOIP, Asterisk, Segurança, OpenVpn.

ABSTRACT

Several protocols and tools have been used in the voice transmission in nets IP associated with mechanisms of security. In this context the tools with free code are standing out. This work proposes a study of the transmissions with the free software Asterisk and the implementation of a VPN as mechanism of security for those voice transmissions. By the softphone and software use of data traffic capture in the net, they were made analyses and comparisons of the captured information.

Word-keys: VOIP, Asterisk, Safety, OpenVpn.

LISTA DE FIGURAS

Figura 1: Modelo OSI x TCP 18
Figura 2: Formato de um pacote TCP 22
Figura 3: Formato de um pacote UDP.....23
Figura 4: Protocolos utilizados em VOIP. (FONTE: www.teleco.com.br) 26
Figura 5: Componentes do padrão H.323 (FONTE: VOLTAN, 2005).....31
Figura 6: A Pilha de Protocolos H.323 (FONTE: COSTA, 2004).....32
Figura 7: Esquema para criptografia de Chaves Assimétricas (FONTE: TRINTA e MACEDO) 40
Figura 8: Os modos transporte e túnel no IPSec e as associações de segurança criadas (FONTE: PASSITO et. al). 43
Figura 9: A posição de um cabeçalho AH (PASSITO, et. al.).....44
Figura 10: A posição do cabeçalho ESP. (PASSITO, et. al.).....44
Figura 11: Soft Phone X-lite 2.0 48
Figura 12: Topologia da Rede. 49
Figura 13: Software Wireshark – Network Protocol Analyzer 50
Figura 14: Gráfico da porcentagem dos dados trafegados na rede. 54
Figura 15: Gráfico da porcentagem de pacotes de Voz trafegados pela Rede. 54
Figura 16: Conexão VPN entre duas máquinas na mesma rede ethernet (Fonte: CHIN, 1998). 57
Figura 17: Software Wireshark - Captura de um teste VOIP com conexão VPN ativa. 61
Figura 18: Gráfico da porcentagem de pacotes de dados trafegados na rede com conexão VPN. 61
Figura 19: Gráfico da porcentagem de pacotes de voz (VOIP) trafegados na rede com conexão VPN.....62
Figura 20: Gráfico comparativo dos tráfegos.....63

LISTA DE TABELAS

Tabela 1: Os métodos do SIP definidos na especificação do núcleo. 28
Tabela 2: Comparação entre o H.323 e o SIP.....34
Tabela 3: Todos os dados do Testedevoz2 capturados pelo Wireshark. 51
Tabela 4: Dados básicos das capturas do tráfego normal da rede. 52
Tabela 5: Dados básicos das capturas do tráfego com chamadas VOIP.....53
Tabela 6: Dados de um teste realizado com a ligação VOIP e conexão VPN ativa. .58
Tabela 7: Dados básicos das capturas do tráfego da rede realizados com mecanismos de segurança.....58
Tabela 8: Dados básicos das capturas realizadas com chamadas VOIP estabelecidas com mecanismos de segurança. 59
Tabela 9: Média dos dados coletados em geral. 64
Tabela 10: Dados dos dois testes com transmissão de voz gravada. 65

LISTA DE SIGLAS

Sigla	Significado
AH	*Authentication Header*
ARPANET	*Advanced Research Projects Agency Network*
DARPA	*Defense Advanced Research Projects Agency*
DHCP	*Dynamic Host Configuration Protocol*
ESP	*Encapsulating Security Payload*
HTTP	*Hypertext Transfer Protocol*
IETF	*Internet Engineering Task Force*
IKE	*Internet Key Exchange*
IP	*Internet Protocol*
IPSEC	*Internet Protocol Security*
ISAKMP	*Internet Security Association and Key Management Protocol*
ISO	*International Organization for Standardization*
ITU	*International Telecommunications Union*
MC	*Multipoint Controller*
MP	*Multipoint Processor*
MCU	*Multipoint Control Unit*
MGCP	*Media Gateway Control Protocol*
MEGACO	*Media Gateway Control*
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*
RFC	*Request For Comments*
RTCP	*Real Time Trasnport Control Protocol*
SA	*Security Association*
SPI	*Security Parameter Index*
SRTCP	*Secure Realtime Transport Control Protocol*

SRTP	*Secure Real-time Transport Protocol*
RTP	*Real Time Transport Protocol*
SDP	*Session Description Protocol*
SIP	*Session Initiation Protocol*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
URL	*Uniform Resource Locator*
VOIP	*Voz over Internet Protocol*
VPN	*Virtual Private Network*

SUMÁRIO

1. INTRODUÇÃO 13
1.1 Objetivos 14
1.2 Justificativas 15
1.3 Organização do trabalho 16
2. FUNDAMENTAÇÃO TEÓRICA 17
2.1 História do VOIP 17
2.2 Pilhas de Protocolos TCP/IP 18
2.2.1 Protocolo TCP 20
2.2.2 Protocolo UDP 22
2.2.3 O Protocolo IP 24
2.3 Protocolos Utilizados em VOIP 24
2.3.1 SIP 27
2.3.2 H323 29
2.3.3 H323 x SIP 33
2.3.4 RTP 34
2.3.5 RTCP 36
2.4. Segurança na Transmissão de Voz 37
2.4.1 Criptografia 38
2.4.2 Virtual Private Network 40
2.4.3 O Protocolo IP Security 41
3. ANÁLISES E CAPTURAS REALIZADAS 45
3.1 Asterisk 45
3.1.1 Configurando o Asterisk 46
3.2 Soft Phones 48
3.1.2. Captura do Tráfego 49
3.3 Segurança 55
3.3.1 OpenVpn 56
3.3.2 Captura do Tráfego 57
3.4 Análises dos Dados 63
4. CONCLUSÕES E TRABALHOS FUTUROS 66
5. REFERÊNCIAS 68
6. APÊNDICES 71

1. INTRODUÇÃO

Ao longo dos últimos anos a prestação de serviços de telecomunicações no mundo todo vem sofrendo diversas mudanças, e essas mudanças vêm caminhando lado a lado com a tecnologia (TANENBAUM, 2003).

Uma das mudanças mais recentes é a tecnologia de transmissão de voz sobre IP (*Internet Protocol*), mais conhecida como VOIP (*Voice Over Internet Protocol*).

VOIP é a tecnologia que permite conversações telefônicas através da Internet ou de qualquer rede IP, sendo assim uma nova alternativa para transmissão de voz (BERNAL, 2007).

Bernal (2007) também explica que o VOIP usa a Internet como um meio de diminuir os custos com ligações telefônicas, e surgiu como uma opção de redução de custos em chamadas de longa distância nacional ou internacional. Seus recursos permitem que a qualidade de som na transmissão de voz seja equivalente à telefonia convencional, utilizando apenas um telefone comum e um adaptador conectado a banda larga.

O sucesso da implantação do serviço de voz nas redes IP aponta para um grande desafio: proporcionar mecanismos de segurança para dados de voz sem comprometer a qualidade do serviço. Essa necessidade existe devido a redes IP não possuírem nenhuma segurança e, então, os serviços de transmissão de voz podem ser alvos de ataques de intrusos como, escutas telefônicas, falsificação dos dados e falta de privacidade.

Esse trabalho apresenta um estudo sobre a tecnologia de transmissão de Voz sobre IP e mecanismos para implantação de segurança na transmissão de dados na mesma.

1.1 Objetivos

O Objetivo Geral do trabalho é fazer um estudo e análise do tráfego na transmissão de voz em redes IP associada com mecanismos de segurança, em uma rede IP particular.

Dentre os objetivos específicos do estudo pode-se citar a exploração da tecnologia VOIP e seus protocolos utilizados. A análise do tráfego na transmissão de pacotes de voz sem criptografia associada. A aplicação de medidas de segurança, criptografia e autenticidade dos dados através da implementação de VPN *(Virtual Private Network)*. Analisar também o tráfego e a segurança na transmissão de pacotes de voz com as medidas de segurança associadas. E por fim, realizar um estudo comparativo de todos os testes e capturas realizadas.

1.2 Justificativas

A motivação para se analisar e propor segurança na transmissão de pacotes de voz em redes IP, se dá pela crescente utilização do VOIP por pessoas e empresas, e pela necessidade de que esses dados de voz estejam trafegando com total segurança pela rede.

Cada vez maior é a preocupação dos usuários e prestadores de serviço de voz sobre IP com relação às ameaças e aos riscos vinculados a este tipo de serviço.

Existe uma grande preocupação com o tema, visto que 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.

O tráfego de voz por VOIP é considerado um tráfego em tempo real, diferentemente do tráfego de dados comum, devido a esse fato 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 telefônica. Para isto, existem várias tecnologias que buscam garantir uma Qualidade de Serviço, priorizando o tráfego de voz sobre outros tráfegos que dividem a mesma banda.

Assim sendo, não é interessante transmitir dados sabendo que alguém pode estar tendo acesso a eles, ou ainda, que esses dados não estão chegando ao destino corretamente, então se faz necessárias ligações seguras, porém com uma boa qualidade. Neste trabalho serão realizadas análises no tráfego de voz para obter informações se há possibilidade de se implementar as duas técnicas na rede e ter um bom resultado.

1.3 Organização do trabalho

A estrutura do trabalho se apresenta distribuída da seguinte maneira: no capítulo 2 são apresentados os conceitos relacionados transmissão de voz em redes IP, os protocolos utilizados, e apresenta conceitos relacionados a mecanismos de segurança para VOIP. No capítulo 3 apresenta-se o estudo realizado, as análises e comparações. E por fim, no capítulo 4 são apresentados as considerações finais e as conclusões do trabalho.

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 mecanismos para prover segurança na transmissão de voz em redes IP. Para a realização deste capítulo foram usadas como base pesquisas bibliográficas através de sites, revistas e livros teóricos sobre assunto.

2.1 História do VOIP

A sigla VOIP significa "*Voice over IP*" ou voz sobre redes que utilizam o "*Protocolo Internet*". É uma tecnologia de convergência entre a Internet e a telefonia que leva para as redes de dados o tráfego de voz sob forma de pacotes comparando-se a telefonia convencional (ANDRADE; SANCHES; WYDRA, 2005).

O conceito do VOIP é simples: consiste em converter sinais de voz analógicos em sinais digitais, possibilitando assim o seu tráfego na rede.

A tecnologia VOIP teve início por volta de 1999 quando segundo Tanenbaum (2003, p. 730) o número de bits de dados transferidos igualou o número de bits de voz (pois a voz está codificada em PCM (*Pulse Code Modulation)* nos troncos, e assim pode ser medida em bits/s).

Em 2002, o volume do tráfego de dados era dez vezes maior que o volume do tráfego de voz, e ainda continua a crescer exponencialmente, enquanto o tráfego de voz permanece quase no mesmo nível, crescendo 5% ao ano (TANENBAUM, 2003).

No Brasil o maior responsável pela utilização do VOIP é a crescente utilização da internet banda larga, onde o número de assinantes ultrapassou 4,6 milhões em 2006 (BERNAL, 2007).

Devido a essas crescentes mudanças as operadoras de redes de dados viram na telefonia um modo de ganhar um bom dinheiro extra, nascendo assim a Telefonia da Internet, também conhecida como voz sobre IP.

2.2 Pilhas de Protocolos TCP/IP

Conforme Nazario (2003) a pilha de protocolos TCP/IP (*Transmission Control Protocol / Internet Protocol*) surgiu com a criação em 1966 da ARPANET (*Advanced Research Projects Agency Network)*, uma interligação de computadores iniciada pelo governo americano através da agência DARPA (*Defense Advanced Research Projects Agency)*, com o objetivo de criar um sistema de comunicação e controle distribuído para fins militares.

O modelo de referência mais conhecido (e um dos mais antigos) é o TCP/IP. Antes de sua criação cada rede tinha sua conexão à ARPANET feita através de diferentes tipos de enlaces (exemplos são os enlaces de rádio e satélites), porém, vários problemas começaram a surgir e a necessidade de um modelo ficou evidente. O modelo de referência concebido foi o TCP/IP (DANTAS, 2002, pág. 111).

A Figura 1 faz uma comparação entre o Modelo de Referência OSI (*Open Systems Interconnection*) e o Modelo TCP/IP.

OSI		**TCP/IP**
Aplicação		Aplicação
Apresentação		
Sessão		
Transporte		Transporte
Rede		Internet
Enlace		Acesso à Rede
Física		

Figura 1: Modelo OSI x TCP

O conjunto de protocolos TCP/IP foi projetado especialmente para ser o protocolo utilizado na Internet. Sua característica principal é o suporte direto a comunicação entre redes de diversos tipos. Então, a arquitetura TCP/IP é independente da infra-estrutura de rede física ou lógica empregada (JUNIOR, 2007).

A arquitetura TCP/IP, assim como OSI, realiza a divisão de funções do sistema de comunicação em estruturas de camadas.

Tanto o modelo OSI como o TCP/IP funcionam através de pilhas de protocolos, formando assim diversos níveis (camadas), onde um nível sempre utiliza os serviços do nível inferior (ALVES, 2007).

Segundo Junior (2007) o modelo OSI é dividido em sete níveis, sendo que cada um deles possui uma função distinta no processo de comunicação entre dois sistemas abertos. Este modelo é mais utilizado para fins acadêmicos, enquanto o TCP/IP é um modelo implementado e utilizado na comunicação entre máquinas em rede.

Como visto na Figura 1, Alves (2007) explica que o modelo TCP/IP não faz distinção entre as camadas superiores. As três camadas superiores são estritamente equivalentes aos protocolos de processos da Internet. Os processos possuem o nome do próprio protocolo utilizado, porém é importante não confundir o protocolo em si com a aplicação que geralmente apresenta uma interface com usuário amigável para utilização do protocolo. No modelo ISO/OSI, a camada de transporte é responsável pela liberação dos dados para o destino. No modelo Internet (TCP/IP) isto é feito pelos protocolos “ponto a ponto” TCP e UDP que são descritos posteriormente.

De acordo com Alves (2007) deve se considerar o TCP/IP como sendo constituído por quatro camadas apenas. A camada superior, camada de aplicação é responsável por permitir que aplicações possam se comunicar através de hardware e software de diferentes sistemas operacionais e plataformas. Muitas vezes este processo é chamado de cliente-servidor. A aplicação cliente em geral está em um equipamento mais simples e com uma boa interface com usuário. Esta aplicação envia requisições à aplicação servidor, que normalmente está em uma plataforma mais robusta, e que tem capacidade para atender várias requisições diferentes de clientes diferentes.

Alves ainda afirma que a camada que segue a camada de Transporte ou “Ponto a Ponto”, tem a função principal de começar e terminar uma conexão e ainda controlar o fluxo de dados e de efetuar processos de correção e verificação de erros.

Para Alves (2007) a camada de Rede/Internet é a responsável pelo roteamento. Comparando os modelos ela corresponde no modelo ISO/OSI a camada de Rede e parte da camada Enlace. Esta camada é usada para atribuir endereço de rede (IP) ao sistema e rotear a informação para a rede correta. Tem

ainda a função de ligação entre as camadas superiores e os protocolos de hardware. Em essência pode-se afirmar que sem esta camada, as aplicações teriam que ser desenvolvidas para cada tipo de arquitetura de rede, como por exemplo: Ethernet ou Token Ring.

A primeira camada, camada Física, não é definida pelo TCP/IP, porém é nítida sua importância em relação à parte física da mídia de comunicação, de bits, de quadros, de endereços MAC, na camada de Acesso a Rede (ALVES, 2007).

2.2.1 Protocolo TCP

De acordo com Tanenbaum (2003, p.558) a internet tem dois protocolos principais na camada de transporte, um protocolo sem conexões e outro orientado a conexões.

O conjunto de protocolos de transporte orientado a conexão é conhecido como TCP.

Conforme Dantas (2002), o protocolo TCP é um protocolo caracterizado por oferecer um serviço confiável entre aplicações. Com o objetivo de efetuar suas tarefas com sucesso, o protocolo identifica os pacotes recebidos fazendo uma correlação de cada pacote com suas respectivas conexões.

Exemplos de serviços feitos pelo TCP são: a identificação dos pacotes, a correção numa eventual perda de pacotes e a garantia da seqüência de entrega dos pacotes (DANTAS, 2002).

A PDU (*Protocol Data Unit*) do TCP é conhecida como segmento, mas é chamada também de pacote (DANTAS, 2002). O formato do pacote TCP é mostrado na Figura 2.

Portas de origem e destino: Possuem o tamanho de 16 bits cada campo, esses campos são as identificações dos processos de origem e destino envolvidos numa conexão TCP. Os números das portas obedecem a uma padronização no sentido de que algumas portas são reservadas (DANTAS, 2002, pág. 123).

Número de seqüência: Possui o tamanho de 32 bits, esse campo informa o número de um segmento numa conexão TCP, com exceção quando o

pacote é SYN, pois quando um segmento começa com SYN, significa que esta é a primeira representação da seqüência e o primeiro octeto de dados vem a seguir (DANTAS, 2002, pág. 124).

Número de reconhecimento: Possui o tamanho de 32 bits, indica o número do reconhecimento dos segmentos ACKs.

Tamanho do cabeçalho: Possui o tamanho de 4 bits, este campo informa o número de palavras de 32 bits que existem no segmento TCP.

Flags: Seis (6) bits, conforme Dantas (2002):

URG – campo significativo 0 ou 1 que indica, ou não, segmento urgente.

ACK – campo significativo 0 ou 1 de reconhecimento, ou não, positivo.

PSH – com ele o receptor é solicitado a entregar dados à aplicação mediante sua chegada, em vez de armazená-los até que um buffer completa tenha sido recebido (TANENBAUM, 2003).

RST – reinicialização de conexão por motivo de falha.

SYN – utilizado para o estabelecimento de uma conexão.

FIN – utilizado para finalizar uma conexão, nenhum dado será mais enviado pelo remetente.

Tamanho da janela: Possui o tamanho de 16 bits, representa o tamanho da janela, para o controle do fluxo.

Checksum: Possui o tamanho de 16 bits, este é o campo de verificação do cabeçalho através do cálculo baseado em todos os campos do segmento.

Ponteiro de urgência: Possui o tamanho de 16 bits, este campo permite que o destinatário saiba quantos dados urgentes serão enviados.

Opções: Possui o tamanho de 32 bits, este campo foi projetado para prover serviços extras, como por exemplo, o tamanho máximo de um segmento que deverá ser aceito.

Dados: Dados das camadas inferiores. (DANTAS, 2002, pág. 124).

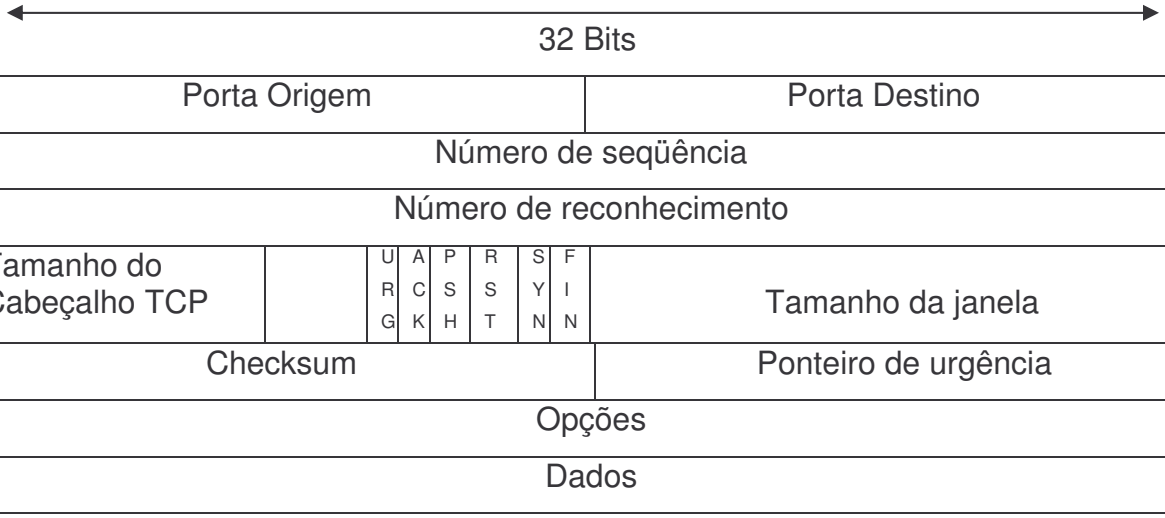

Figura 2: Formato de um pacote TCP

Segundo Dantas (2002), o mecanismo de comunicação entre duas entidades TCP é caracterizado pelas seguintes etapas:

- Abertura de uma conexão.
- Envio e recebimento de dados.
- Obtenção de informações sobre a conexão.
- Fechamento da conexão.

Com base em Dantas (2002), o TCP é conhecido por ser um protocolo pessimista, uma vez que o mesmo acredita que no envio dos segmentos sempre irão ocorrer perdas e que os pacotes vão chegar fora de ordem. Devido a este fato, o protocolo tem uma implementação complexa.

2.2.2 Protocolo UDP

Como já dito, a internet tem dois protocolos principais na camada de transporte, um protocolo sem conexões e outro orientado a conexões.

O Conjunto de protocolos de transporte sem conexão é conhecido como UDP (*User Datagram Protocol*).

O protocolo UDP é conhecido por sua característica de ser um protocolo otimista. Dantas (2002) afirma que protocolo otimista é aquele que efetua o envio de todos os seus pacotes, acreditando que estes irão chegar sem problemas e em seqüência ao destinatário.

O UDP oferece um meio para as aplicações enviarem datagramas IP encapsulados sem que seja necessário estabelecer conexão. O UDP é descrito na RFC 768.

Tanenbaum (2003, p.566) diz que o protocolo UDP é bem simples, mas possui alguns usos específicos, como interações cliente/servidor e multimídia, porém para a maioria das aplicações, faz-se necessário uma entrega dos dados em seqüência e confiável, o protocolo UDP já não garante isso.

Um exemplo de situação em que não é necessário estabelecer conexão entre o dispositivo de origem e destino é a Videoconferência.

Queiroz (2002) afirma que como as aplicações de voz em tempo-real são sensíveis ao atraso, por esse motivo o protocolo UDP é o ideal para aplicações de voz sobre IP.

De acordo com Tanenbaum o UDP transmite segmentos que consistem em um cabeçalho de oito (8) bytes, seguido pela carga útil. O cabeçalho mostrado na Figura 3 identifica que, as duas portas servem para identificar os pontos extremos nas máquinas de origem e destino. A porta de origem e destino possui um tamanho de 16 bits cada. O campo *Tamanho do UDP* informa o tamanho do cabeçalho, possui um tamanho de 16 bits, e o campo *Checksum* é opcional e armazenado como 0 se não for calculado (um valor 0 verdadeiro calculado é armazenado com todos os bits iguais a 1). É sempre bom deixar este campo ativado, a menos que a qualidade dos dados não tenha importância, por exemplo, voz digitalizada.

O formato do pacote UDP é ilustrado na figura abaixo:

Porta de Origem	Porta de Destino
Tamanho do UDP	Checksum
Dados	

Figura 3: Formato de um pacote UDP

2.2.3 O Protocolo IP

Conforme Queiroz (2002) o Protocolo IP foi criado com o objetivo de transportar dados entre diferentes tipos de redes, e segundo Tanenbaum ele é o principal protocolo do nível de Rede do Modelo de referência OSI é também o protocolo mais conhecido e o mais utilizado.

Sua função é transportar os pacotes de dados da origem para o destino, da melhor forma possível (QUEIROZ, 2002).

De acordo com Dantas (2002) o endereçamento IP é o responsável pelo roteamento em ambientes de redes TCP/IP (*Transmission Control Protocol / Internet Protocol*). A versão do protocolo IP utilizada atualmente na Internet é a versão Ipv4. Porém, já existe uma nova proposta do protocolo que visa atacar os problemas encontrados na versão atual. Esta nova implementação é conhecida como Ipv6.

Segundo Dantas (2002) o Ipv4 considera cinco endereços com quatro octetos. Estes octetos definem um único endereço dividido em uma parte que representa a rede a qual pertence o endereço, em alguns casos a sub-rede também, e por fim a representação particular daquele sistema na rede.

2.3 Protocolos Utilizados em VOIP

Kurose e Ross (2006) demonstram algumas situações que podem ocorrer com as tecnologias atualmente: Imagine uma situação na qual, enquanto você está trabalhando em seu computador você recebe suas chamadas telefônicas pela internet, e quando você sai para descansar um pouco, as novas chamadas telefônicas que chegam são automaticamente roteadas para seu PDA (*Personal Digital Assistant*). Outra situação interessante seria quando você está dirigindo. Novas chamadas telefônicas são automaticamente roteadas para algum equipamento conectado à Internet instalado no seu carro, ou ainda, durante uma conferência em rede você pode acessar uma agenda de endereços e convidar outras pessoas para participar da reunião virtual. Esses outros participantes poderão estar trabalhando em seus computadores ou em trânsito com seus PDAs à mão ou

em seus carros – não importa onde estejam, seu convite será roteado para eles de modo transparente. Ou ainda, quando você visitar alguma home page pessoal, encontrará um link ‘Ligue pra mim’; ao clicar sobre esse link, será estabelecida uma sessão de telefone Internet entre seu computador e o proprietário da home page.

Com essas situações não existirão mais uma rede de telefonia por comutação de circuitos. Em vez disso, todas as chamadas telefônicas passarão pela Internet – fim-a-fim. Empresas não utilizarão mais centrais privadas de comunicação telefônica (PABX – *Private Automatic Branch Exchange*), isto é, mesas locais de comutação de circuitos, para manipular chamadas telefônicas internas. Em vez disso, o tráfego telefônico interno fluirá pela LAN de alta velocidade da empresa (KUROSE; ROSS, 2006, p. 471). Isso tudo se torna acessível através de protocolos e produtos já existentes. Serão descritos a seguir os protocolos mais promissores para essa finalidade.

A Figura 4 apresenta a estrutura dos principais protocolos utilizados em redes VOIP. O protocolo IP (camada de rede) e os protocolos TCP/UDP (camada de transporte) são os componentes básicos de uma rede IP usada pelos sistemas VOIP (BERNAL, 2007).

Na camada de aplicação são utilizados para a sinalização (controle de chamada) os protocolos H.323 e o SIP (*Session Initiation Protocol*). O protocolo H.323 é utilizado pelos telefones IP, computadores, adaptadores IP, controladores de sinalização (soft-switches e call managers) e gateways para estabelecimento, controle e término das chamadas. É um protocolo mais antigo e complexo e atualmente tem sido menos utilizado pelos sistemas de telefonia IP. O protocolo SIP tem a mesma finalidade do H.323, porém é mais moderno e menos complexo, e vem sendo adotado com maior freqüência pelos sistemas VOIP (BERNAL, 2007).

Ainda embasado no tutorial de Bernal (2007), na camada de aplicação são utilizados para o controle de Gateway os protocolos MGCP (*Media Gateway Control Protocol*) e MEGACO (*Media Gateway Control*). O MGCP é utilizado pelos controladores de gateways e gateways para estabelecimento, controle e término das chamadas. O protocolo MEGACO tem a mesma finalidade do MCGP, porém foi desenvolvido para ser uma alternativa a esse protocolo, adequando-se também a controladores distribuídos de gateways, a controladores multiponto (Conferência) e a unidades interativas de resposta audível (BERNAL, 2007).

Para o transporte da voz são utilizados dois protocolos de tempo real o RTP (*Real Time Transport Protocol*) e o RTCP (*Real Time Transport Control Protocol*). O RTP é o protocolo responsável pelo transporte de Voz em tempo real entre os computadores e gateways. É o padrão mais utilizado atualmente para esta finalidade**.** O RTCP é o protocolo responsável pelo controle do transporte de Voz realizado pelo RTP nos sistemas VOIP.

De acordo com Bernal (2007) os Codecs de Áudio são os programas responsáveis pela conversão e compressão dos sinais de Voz para uso nos sistemas VOIP. De acordo com o nível de compressão do sinal final, pode-se fazer uma sintonia adequada para a relação banda x qualidade de voz para cada sistema VOIP. A arquitetura é demonstrada na Figura 4:

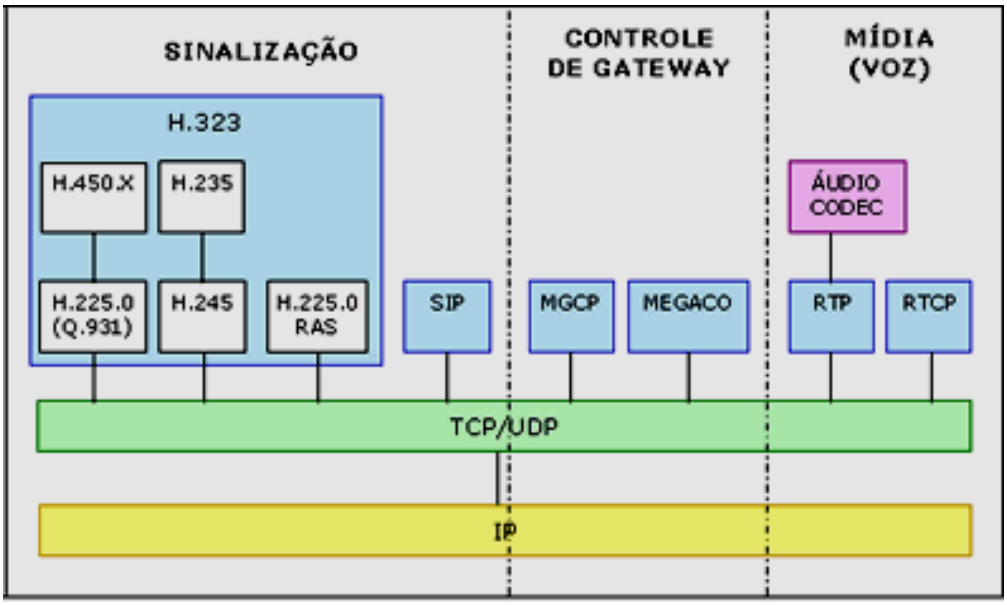

Figura 4: Protocolos utilizados em VOIP. (FONTE: www.teleco.com.br)

Nas próximas seções são apresentados, mais detalhadamente, os protocolos para aplicações interativas em tempo real, H323, SIP, RTP. Todos os três conjuntos de padrões estão sendo implementados amplamente em produtos do setor (KUROSE; ROSS, 2006, p. 465).

2.3.1 SIP

Conforme Nazario (2003) o SIP *(Session Initiation Protocol)* é um protocolo de controle usado para criar, modificar e terminar sessões com um ou mais usuários (participantes). Estas sessões incluem conferências multimídia para internet, chamadas de telefone para internet e distribuição multimídia. Participantes em uma sessão podem se comunicar via *multicast* ou *unicast*, ou uma combinação de ambos. O SIP foi definido pelo IETF (*Internet Engineering Task Force)* e está definido no RFC 3261 (2003) do IETF.

Para Tanenbaum (2003) este protocolo descreve como instalar chamadas telefônicas na internet, videoconferências e outras conexões. Diferente do H.323 que é um conjunto de protocolo completo, o SIP é um único módulo, mas foi projetado para interoperar bem com aplicações da Internet existentes. Por exemplo, ele define números de telefones como URL´s, de forma que as páginas Web possam conter esses números, permitindo que em apenas um clique em um link inicie uma ligação telefônica.

De acordo com Kurose e Ross (2006) o SIP é um protocolo simples que faz o seguinte:

- Provê mecanismos para estabelecer chamadas entre dois interlocutores por uma rede IP. Permite que quem chame avise ao que é chamado que quer iniciar uma chamada. Permite que os participantes concordem com a codificação da mídia. E também permite que encerrem as chamadas;
- Provê mecanismos que permite a quem chama determinar o endereço IP corrente de quem é chamado. Os usuários não têm um endereço IP único, fixo, porque podem receber endereços dinamicamente (usando DHCP - *Dynamic Host Configuration Protocol*) e porque pode haver vários equipamentos IP, cada um com um endereço IP diferente;
- Provê mecanismos para gerenciamento de chamadas, tais como adicionar novas correntes de mídia, mudar a codificação, convidar outros participantes, tudo durante a chamada, e ainda transferir e segurar chamadas.

Conforme Tanenbaum (2003, pág.734), o SIP cuida apenas da configuração, do gerenciamento e do encerramento de sessões. Outros protocolos, como RTP/RTCP, são usados para o transporte dos dados. O SIP é um protocolo da camada de aplicação e pode funcionar sobre o UDP ou TCP.

Tanenbaum (2003) também explica que o SIP é um protocolo de texto modelado sobre o HTTP *(Hypertext Transfer Protocol)*. Uma parte envia uma mensagem em texto ASCII que consiste em um nome de método na primeira linha, seguido por linhas adicionais contendo os cabeçalhos para passagem de parâmetros.

Os seis métodos definidos pela especificação do núcleo são mostrados na Tabela 1.

O método *INVITE* é enviado na mensagem da primeira linha quando se deseja criar uma conexão, tanto TCP como UDP. Se o chamado aceitar a ligação (conexão) ele responderá com o código de resposta. Se o chamador receber a mensagem de resposta ele envia então um *ACK.* O término de uma sessão se dá por qualquer uma das partes, enviando a mensagem com o método *BYE.* O método *OPTIONS* é usado para consultar uma máquina sobre seus próprios recursos. O método *REGISTER* se relaciona com a habilidade do SIP para localizar e se conectar a um usuário.

Tabela 1: Os métodos do SIP definidos na especificação do núcleo.

Método	**Descrição**
INVITE	Solicita a inicialização de uma sessão
ACK	Confirma que uma sessão foi inicializada
BYE	Solicita o término de uma sessão
OPTIONS	Consulta um host sobre seus recursos
CANCEL	Cancela uma solicitação pendente
REGISTER	Informa um servidor de redirecionamento sobre a localização atual do usuário.

2.3.1.1 Protocolo SDP

SDP (*Session Description Protocol* – Protocolo de Descrição de Sessão) está definido na RFC 2237. O SDP é um protocolo utilizado pelo SIP para descrever sessões.

Voltan (2005) diz que este protocolo define para um utilizador informações como tipos de áudio e vídeo que ele suporta, define também a porta

onde deverá receber os dados, o nome da sessão e propósito, a duração da sessão, informação de contato, largura de banda e etc., estas informações são transportadas juntamente com a mensagem SIP.

A sua finalidade é atuar como um negociador entre as partes envolvidas na chamada já que este carrega consigo todas as informações que são úteis para o estabelecimento da chamada. Visto que nem sempre as partes se entendem, por exemplo, o tipo de áudio e vídeo que irá ser utilizado, então o SDP de ambas as partes fica fornecendo informações sobre esses áudios e vídeos, entre outras informações, que suportam até que ambos entrem em um consenso (VOLTAN, 2005, pág. 46).

2.3.2 H323

Segundo Tanenbaum (2003) o protocolo H.323 foi desenvolvido em 1996 pela ITU (*International Telecommunications Union*), e foi revisada em 1998, e essa recomendação foi a base para os primeiros sistemas amplamente difundidos de telefonia da Internet.

De acordo com Kurose e Ross (2006), o H.323 é um protocolo alternativo ao SIP, ele é um padrão popular para audioconferência e videoconferência entre sistemas finais na Internet. Como visto na Figura 5, o padrão H.323 também abrange a maneira como sistemas finais ligados à Internet se comunicam com telefones ligados às redes normais de telefonia de comutação de circuitos. A Figura 5 mostra também os elementos utilizados em uma rede H.323.

Voltan (2005) define os elementos H.323 da seguinte forma:

- *Gatekeeper*: É considerado o componente mais complexo da estrutura da recomendação H.323. Foi introduzido na primeira versão, H.323v1, apesar de na época poucos entenderem sua utilidade. Contudo na segunda versão, a recomendação H.323 esclareceu o papel do gatekeeper, e hoje o que se entende como sendo um elemento opcional da(s) rede(s), com funções como: tradução de endereços que é usado para se encontrar um alias; controle de chamadas o qual verifica a disponibilidade de recursos da rede; controle de admissão tanto à rede como a terminais, Gateways e MCU, cuja função é verificar o direito de acessar recursos; controle de registro para poder contactar alguém que está conectado ao

sistema; reserva de recursos como largura de banda; localização de gateways. Enfim resume-se gatekeeper como sendo um servidor que provê serviços multimídia para as entidades da rede e ainda gerencia toda a conferência;

- *MCU*: *(Multipoint Control Unit – Unidade de Controle Multiponto)*: entidade, dispositivo que permite que vários terminais e/ou gateways participem de uma conferência Multiponto. Esta conferência pode ser iniciada apenas com dois terminais (ponto-a-ponto) e logo após poderá tornar-se uma conferência multiponto, com a entrada de mais terminais. A MCU é composta de duas partes, o MC (multipoint Controller) que é obrigatório, e o MP (Multipoint Processor) que é opcional. *MC (Multipoint Controller – Controladora Multiponto)*: geralmente é um software que controla o uso de recursos nas conferências multiponto, fazendo negociação com todos os terminais para obter uma comunicação igualitária. Também pode controlar outros recursos como por exemplo saber de quem é uma emissão de vídeo multicast. *MP (Multipoint Processor – Processador Multiponto)*: é uma entidade, geralmente um hardware, fornecida para processar o fluxo de áudio, vídeo e/ou dados em conferência multiponto. O MP ainda pode prover o processamento, mistura ou comutação de fluxos de mídia sob o controle do MC;

- *Gateway:* elemento da rede que realiza conversão (tradução de protocolo) entre terminais distintos, permitindo a interoperabilidade entre sistemas H.323 e outros sistemas em redes distintas. Também realiza serviços como compressão e empacotamento. Basicamente transforma a voz do usuário em pacotes de dados e vice-versa;

- *Terminal:* É um *endpoint* (ponto final), terminal, de uma rede. Provê uma interface que permite ao usuário realizar a comunicação bidirecional em tempo real (transferência de áudio, vídeo e/ou dados) com outro terminal H.323, gateway ou MCU. Um terminal H.323 pode ser um hardware (telefone IP), ou um computador multimídia (microfone, caixas de som e câmera) que esteja utilizando um *softphone* (software que simula um telefone IP).

A Figura 5 mostra como esses elementos são interligados.

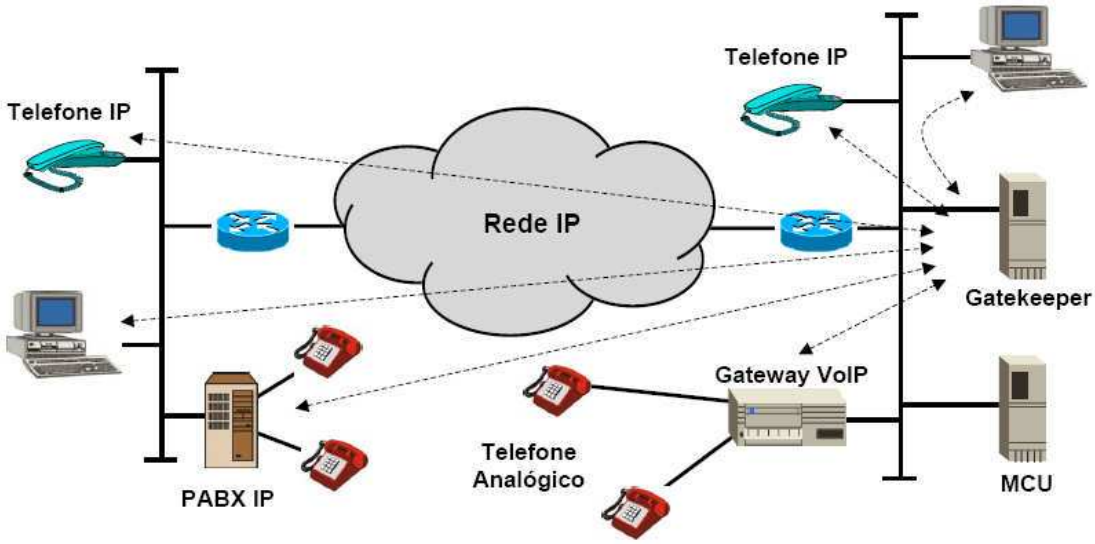

Figura 5: Componentes do padrão H.323 (FONTE: VOLTAN, 2005).

Conforme Costa (2004), uma rede H.323 não é um novo tipo de rede, mas sim uma rede tipicamente IP, que possui serviços especiais voltados para as comunicações multimídia. Tais serviços especiais são implementados através da implantação, em uma rede IP, de MCUs, gatekeepers e gateways. Logo, diz-se que uma rede H.323 é uma rede IP que fornece, via MUCs, gatekeepers e gateways, serviços multimídia aos terminais H.323 a ela conectados. MCUs e gateways não precisam estar presentes em todas as situações de comunicação multimídia, uma vez que apresentam funções específicas: um gateway só se faz necessário quando terminais de padrões diferentes do H.323 precisam se comunicar com terminais H.323 e um MCU só será necessário numa conferência multiponto.

Em um sistema H.323 são definidos alguns componentes conforme a recomendação H.323: Gatekeeper, MP, Terminal H.323, MC, MCU e Gateway. Esses componentes possuem características distintas, e podem pertencer a uma única rede ou várias redes independentemente de conter uma ou várias infra-estruturas (VOLTAN, 2005).

2.3.2.1 Pilha de Protocolos

O posicionamento da pilha de protocolos do padrão H.323 é apresentada na Figura 6 de forma simplificada. Embora o RTP e o RTCP não façam parte do padrão H.323, esses protocolos são recomendados na implementação de aplicações seguindo esse padrão (COSTA, 2004).

Costa (2004) explica os protocolos H.225 e H.245, mostrado na Figura 6. O protocolo H.225 serve para o gerenciamento de conexão, esse protocolo define o procedimento inicial para o estabelecimento de uma chamada H.323. É a partir desse padrão que os terminais informam, a um destino chamado, sobre suas intenções de comunicação.

O H.245 é o protocolo de controle de mídia que os sistemas H.323 utilizam depois que a fase de estabelecimento da chamada foi completada. Em outras palavras, o H.245 especifica o conjunto de comandos e requisições que cada terminal deve seguir, a fim de obter uma comunicação satisfatória com outro terminal.

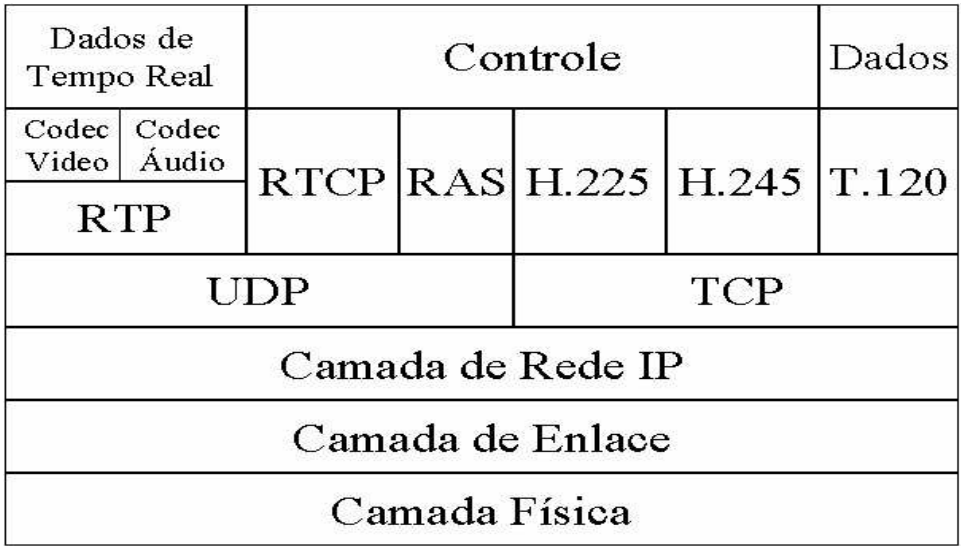

Figura 6: A Pilha de Protocolos H.323 (FONTE: COSTA, 2004).

A ITU também desenvolve outras recomendações que estendem as funcionalidades do H.323 ou adicionam novos serviços.

Uma delas é o H.235, um protocolo de segurança e criptografia para terminais com multimídia H.323. O H.235 é a recomendação da segurança para os sistemas da série H.3xx. Ele fornece procedimentos de segurança para H.323, H.225, H.245 e sistemas baseados no H.460. O H.235 é aplicável ao Point-to-Point simples e às conferências Multipoint para todos os terminais que utilizarem H.245 como um protocolo de controle. A função do H.235 é fornecer autenticação, privacidade e integridade para sistemas baseados no H.323.

O H.235 fornece meios para uma pessoa, melhor que um dispositivo, a ser identificado. Inclui a habilidade de negociar serviços e funcionalidade de uma maneira genérica, e habilidades a respeito das técnicas de criptografia e das potencialidades utilizadas. A maneira específica em que são usados relaciona-se às potencialidades dos sistemas, às exigências da aplicação e aos confinamentos específicos da política da segurança.

Este protocolo suporta algoritmos de criptografia variados, com as opções variadas apropriadas para finalidades diferentes. Não há nenhum algoritmo especificamente exigido (OPEN H.323).

2.3.3 H323 x SIP

Os protocolos H.323 e SIP são muito semelhantes, porém, apresentam algumas diferenças. Tanenbaum (2003) diz que ambos permitem chamadas com dois ou mais participantes, usando computadores e telefones como terminais. Ambos admitem a negociação de parâmetros e criptografia.

A RFC 4123 do IETF define algumas funcionalidades do SIP juntamente com o H.323, como por exemplo, os dois meios transportam os mesmos protocolos, tais como RTP/RTCP, entre outros.

A Tabela 2 mostra um resumo das semelhanças e diferenças entre estes dois protocolos.

Segundo Tanenbaum (2003) os dois protocolos diferem extensamente na filosofia. O H.323 é um padrão pesado, típico da indústria de telefonia, especificando a pilha de protocolos completa e definindo com precisão o que é permitido e proibido. É um protocolo de grande padrão, complexo e rígido, difícil de adaptar a aplicações futuras.

Já o SIP, é um protocolo típico da internet e funciona permutando pequenas linhas de texto ASCII. É um módulo leve que interopera bem com outros protocolos da Internet, mas não muito bem com os protocolos de sinalização do sistema telefônico existente. Este modelo da IETF é flexível e pode ser adaptado com facilidade a novas aplicações (TANENBAUM, 2002, pág. 737).

Tabela 2: Comparação entre o H.323 e o SIP.

Item	H.323	SIP
Projetada por	ITU	IETF
Compatibilidade com PSTN	Sim	Ampla
Compatibilidade com a Internet	Não	Sim
Arquitetura	Monolítica	Modular
Completeza	Pilha de protocolos completa	O SIP lida apenas com a configuração
Negociação de parâmetros	Sim	Não
Sinalização de chamadas	Q.931 sobre TCP	SIP sobre TCP ou UDP
Formato de mensagens	Binário	ASCII
Transporte de mídia	RTP/RTCP	RTP/RTCP
Chamadas de vários participantes	Sim	Sim
Conferências de Multimídia	Sim	Não
Endereçamento	Número de host ou telefone	URL
Término de chamadas	Explicito ou encerramento por TCP	Explicito ou por timeout
Transmissão de mensagens instantâneas	Não	Sim
Criptografia	Sim	Sim
Tamanho do documento de padrões	1.400 páginas	250 páginas
Implementação	Grande e complexa	Moderada
Status	Extensamente distribuído	Boas perspectivas de êxito

2.3.4 RTP

O RTP é um protocolo de transporte de tempo real genérico para varias aplicações (TANENBAUM, 2003, pág. 563). Ele é descrito na RFC 1889.

Em aplicações multimídia o lado remetente anexa campos de cabeçalho às porções de áudio/vídeo antes de passá-las à camada de transporte. Esses campos de cabeçalhos contêm números de seqüência e de marcas de tempo. Já que a maioria das aplicações de rede multimídia pode fazer uso de números de

seqüência e de marcas de tempo, é conveniente ter uma estrutura de pacote padronizada que inclua campos para dados de áudio/vídeo, números de seqüência e marcas de tempo, bem como outros campos potencialmente úteis. O RTP é um padrão desse tipo. Ele pode ser usado para transportar formatos comuns como PCM, GSM e MP3 para som e MPEG e H.263 para vídeo. Este protocolo também pode ser usado para transportar formatos proprietários de som e de vídeo. Hoje, o RTP é amplamente implementado em centenas de protótipos de produtos e de pesquisa. Também é complementar a outros protocolos interativos de tempo real, como o SIP e H.323 (KUROSE; ROSS, 2006, p. 465).

2.3.4.1 O Básico do RTP

Conforme Kurose e Ross (2006) o RTP usualmente roda sobre UDP. O lado remetente encapsula o pacote em um segmento UDP, e então passa o segmento para o IP. O lado receptor extrai o pacote RTP do segmento UDP, em seguida extrai a porção de mídia do pacote RTP e então passa para decodificação e apresentação.

Um exemplo que Kurose e Ross (2006) apresentam é a utilização do RTP para transportar voz. Suponha que a fonte de voz esteja codificada (amostrada, quantizada e digitalizada) em PCM a 64 kbps. Suponha também que a aplicação colete dados codificados em porções de 20 milissegundos, isto é, 160 bytes por porção. O lado remetente precede cada porção dos dados de áudio com um cabeçalho RTP que contem o tipo de codificação de áudio, um número de seqüência e uma marca de tempo. O tamanho do cabeçalho RTP é normalmente 12 bytes. A porção de áudio, juntamente com o cabeçalho RTP, forma o pacote RTP. O pacote RTP é, então, enviado para dentro do socket de interface UDP. No lado receptor, a aplicação recebe o pacote RTP da interface do seu socket. A aplicação extrai a porção de áudio do pacote RTP e usa os campos de cabeçalho do pacote RTP para decodificar e reproduzir adequadamente a porção de áudio.

Para Tanenbaum (2003) a função básica do RTP é multiplexar diversos fluxos de dados de tempo real sobre um único fluxo de pacotes UDP. O fluxo UDP pode ser enviado a um único destino (unidifusão) ou a vários destinos (multidifusão). Como o RTP utiliza simplesmente o UDP normal, seus pacotes não são tratados de maneira especial pelos roteadores, a menos que alguns recursos de

qualidade de serviço normais do IP estejam ativos. Em particular, não há nenhuma garantia especial sobre entrega, flutuação, etc.

2.3.5 RTCP

O RFC 1889 também especifica o RTCP, criado pelo IETF, um protocolo que uma aplicação de rede multimídia pode usar juntamente com o RTP.

Tanenbaum (2003) explica o protocolo RTCP como sendo um irmão caçula do RTP. Segundo ele o RTCP cuida do feedback, da sincronização e da interface com o usuário, mas não transporta quaisquer dados. A primeira função pode ser usada para fornecer feedback sobre retardo, flutuação, largura de banda, congestionamento e outras propriedades de rede para as origens. Essas informações podem ser usadas pelo processo de codificação para aumentar a taxa de dados (e oferecer melhor qualidade) quando a rede estiver funcionando bem e para reduzir a taxa de dados quando houver problemas na rede.

Kurose e Ross explicam que pacotes RTP e RTCP se distinguem uns dos outros pela utilização de números de portas diferentes. O número de porta RTCP é configurado para ser igual ao número da porta RTP mais uma unidade. Conforme a teoria deles pacotes RTCP não encapsula porções de áudio ou de vídeo. Em vez disso, eles são enviados periodicamente, e contêm número relatórios de remetente e/ou receptor com dados estatísticos que podem ser úteis para a aplicação. Esses dados contêm número de pacotes enviados, número de pacotes perdidos e atraso.

Resumindo, ele é usado para transmitir aos participantes, de tempos em tempos, pacotes de controle relativos a uma sessão RTP em particular (VOLTAN, 2005).

O RTCP também cuida da sincronização entre fluxos. O problema é que diferentes fluxos podem utilizar tempos diferentes. O RTCP pode ser usado para garantir a sincronização (TANENBAUM, 2003, pág. 566).

Por fim, segundo Tanenbaum (2003) o RTCP fornece um modo para nomear as diversas origens, por exemplo, texto ASCII. Essas informações podem ser exibidas na tela do receptor, a fim de indicar quem está se comunicando no momento.

2.4. Segurança na Transmissão de Voz

Com o desenvolvimento das novas tecnologias, tornou-se possível a evolução dos sistemas de transmissão, o que viabilizou a criação de redes de pacotes muito mais velozes. Todo esse desenvolvimento tem permitido a evolução das redes convergentes, que são redes capazes de transportar pacotes de dados e voz digitalizados. Hoje existem vários tipos de redes que são capazes de transportar pacotes de dados e voz, por exemplo, redes baseadas em ATM, Frame Relay e TCP/IP. Destas apenas o TCP/IP é utilizado com mais freqüência. O Transporte através da tecnologia TCP/IP é conhecido como VOIP. A diferença entre a utilização de tais redes é referente ao seu custo/beneficio. As redes IP, estão associadas à camada de rede do modelo OSI, o que lhe da muitas vantagens, entre elas o baixo custo e a capacidade de operação em redes heterogêneas, em contrapartida recebe como desvantagens a qualidade de serviço e questões relacionadas com a segurança (VOLTAN, 2005).

Segurança e eficiência são muitas vezes requisitos conflitantes. Apesar de haver áreas na Internet onde o impacto desses mecanismos de segurança é menor, as aplicações em tempo real como VOIP podem ser seriamente afetadas. Com a introdução de outra camada para garantir a segurança, esses serviços oferecidos podem tornar mais lentas as transmissões de pacotes, muitas vezes não sendo aceitáveis para transmissões em tempo real, como alguns mecanismos de criptografia. Então vários aspectos devem ser analisados quando se tenta transmitir voz através de canais seguros (PASSITO et. al.).

A falta de segurança em redes VOIP pode causar vários problemas, alguns deles são citados abaixo:

- Ameaças;
- Captura do trafego;
- Acesso a informações;
- Fraudes.

E para se defender destes ataques são apresentadas a seguir algumas práticas para a implantação de uma estrutura VOIP segura:

- Segmentar o trafego de voz e de dados;

- Controlar o acesso ao segmento de voz com um Firewall especializado;
- Evitar o uso de aplicações de telefones para microcomputadores (PC-Based IP phones), utilizando preferencialmente telefones IP;
- Usar endereços IP privativos e inválidos;
- Configurar os telefones IP com endereços IP estáticos, associados ao MAC Address;
- Utilizar servidores DHCP separados para voz e dados;
- Monitorar os endereços MAC no segmento de voz Implementar mecanismos que permitam autenticar os usuários dos telefones IP;
- Implementar um sistema de detecção de intrusos;
- Monitorar o desempenho e status dos serviços de VOIP;
- Restringir o acesso físico;
- Criptografar o tráfego de VOIP.

Um dos principais mecanismos para garantir segurança, é criptografar o seu conteúdo, assim, mesmo que um atacante consiga capturar os pacotes, o conteúdo dos pacotes continuará protegido, a seguir são explicadas algumas técnicas de criptografia.

2.4.1 Criptografia

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

Para Kurose e Ross (2006) as técnicas criptográficas permitem que um remetente disfarce os dados de modo que um intruso não consiga obter nenhuma informação dos dados interceptados. O destinatário é claro, deve estar habilitado a recuperar os dados originais a partir dos dados disfarçados.

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.

Tanenbaum (2003) explica que criptografia em sistemas de chaves simétricas utiliza a mesma chave para codificação e decodificação.

Esse método, segundo Santos (2005) é conhecido também como criptografia tradicional, funciona bem em aplicações limitadas, onde o remetente e o destinatário se preparam antecipadamente para o uso da chave. Para que esse método funcione, todas as pessoas envolvidas devem conhecer a chave, pois quando uma mensagem criptografada chega à caixa de entrada, ela só pode ser aberta por quem possui a chave. Esse método não é muito eficiente em conexões inseguras, no entanto, quando é utilizado sobre conexões seguras, a criptografia simétrica se torna bem eficiente.

Santos (2005) define criptografia de chaves assimétricas como sendo um modelo de criptografia que trabalha utilizando duas “senhas”. Uma delas, denominada chave pública, deve ser conhecida por todas as pessoas envolvidas no processo e a outra, denominada chave privada, que deve ser conhecida apenas por uma pessoa.

A Figura 7 ilustra um esquema de criptografia usando o método de chave assimétrica. A chave usada para cifrar recebe o nome de chave pública porque ela deve ser publicada e amplamente divulgada pelo seu possuidor, fazendo com que qualquer pessoa possa lhe enviar mensagens cifradas. Já a chave privada que é usada para decifrar as mensagens, deve ser mantida em sigilo, somente o possuidor desta chave conseguirá decifrar e ler a mensagem. Geralmente, os usuários deste tipo de criptografia publicam suas chaves públicas em seu home pages, assinaturas dos e-mails, etc.

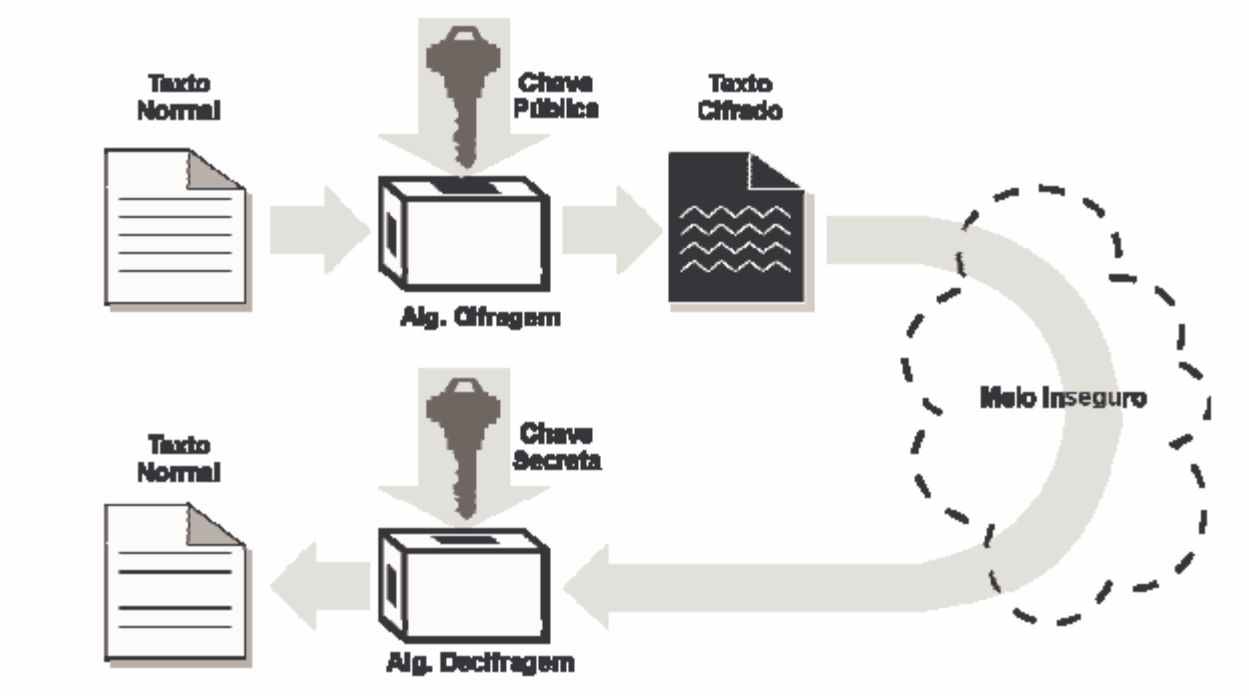

Figura 7: Esquema para criptografia de Chaves Assimétricas (FONTE: TRINTA e MACEDO)

Martins et. al (2006) afirma que para implementar mecanismos de criptografia existe alguns equipamentos Voip que suportam a encriptação das mensagens utilizando o SRTP (*Secure Real-time Transport Protocol*) e o SRTCP *(Secure Realtime Transport Control Protocol),* outros não. No caso dos equipamentos que não suportam o SRTP, pode-se encriptar o tráfego através da utilização do IPsec (*Internet Protocol Security*). Neste caso, a encriptação ocorre nos gateways com suporte a IPsec, como os concentradores de VPN (*Virtual Private Networks*).

2.4.2 Virtual Private Network

Rede Virtual Privada mais conhecida como VPN, é uma rede com acesso restrito, onde os dados enviados nessa rede são criptografados, fazendo assim com que a rede seja virtualmente privada.

Para Tanenbaum (2003, pag. 828) VPN's são redes sobrepostas às redes públicas, mas com a maioria das propriedades de redes privadas. Elas são chamadas "virtuais" porque são meramente uma ilusão, da mesma forma que os circuitos virtuais não são circuitos reais e que a memória virtual não é memória real.

Silva (2002) também explica o conceito de VPN, como sendo uma rede privativa construída sobre a infra-estrutura de uma rede pública, geralmente a Internet. Utiliza as mais avançadas tecnologias de criptografia, assegurando privacidade e integridade das comunicações, substituindo com vantagem os links dedicados e de longa distância. Além da redução dos custos com links, permite que as empresas criem uma rede totalmente integrada, conectando escritórios, filiais e fábricas, com tráfego de voz, dados e vídeo.

Pode-se implementar VPN's em diferentes tipos de aplicações, abaixo são descritas as três mais importantes (CHIN, 1998):

- Acesso Remoto Via Internet;
- Conexão de LAN's via Internet;
- Conexão de Computadores numa Intranet.

Algumas características mínimas desejáveis em uma VPN são: Autenticação de usuários, Gerenciamento de Endereço, Criptografia dos dados, Gerenciamento de chaves e Suporte a múltiplos protocolos.

2.4.2.1 Tunelamento

Segundo Chin (1998) as redes virtuais privadas baseiam-se na tecnologia de tunelamento. Ele pode ser definido como processo de encapsular um protocolo dentro de outro. O uso do tunelamento nas VPNs incorpora um novo componente a esta técnica: antes de encapsular o pacote que será transportado, este é criptografado de forma a ficar ilegível caso seja interceptado durante o seu transporte. O pacote criptografado e encapsulado viaja através do túnel até alcançar seu destino onde é desencapsulado e descriptografado, retornando ao seu formato original.

2.4.3 O Protocolo IP Security

O IPSec é a forma abreviada do Internet Protocol Security , uma especificação que define procedimentos de segurança em redes públicas. Em particular, o IPSec é um conjunto de protocolos que está sendo desenvolvido e aprimorado pelo IETF, e está descrito nas RFC´s 2401, 2402 e 2406.

Segundo Tanenbaum (2003, pág. 821) o projeto do IPSec é uma estrutura para vários serviços, algoritmos e granularidades. O motivo para haver

vários serviços é que nem todas as pessoas querem pagar o preço de todos os serviços o tempo todo. Os principais serviços são sigilo, integridade dos dados e proteção contra ataques. Todos eles se baseiam na criptografia de chave simétrica.

De acordo com Passito et. al. o uso do protocolo IPSec resulta na autenticação, integridade e confidencialidade dos dados na camada de rede. O IPSec pode ser utilizado na implementação de VPNs que oferecem o serviço de transporte de voz através de um canal seguro, onde os pacotes Voip ficam protegidos no interior de um túnel criado pelo IPSec através de uma arquitetura robusta de segurança.

Tecnicamente, Tanenbaum (2003) diz que o IPSec tem duas partes principais. A primeira descreve dois novos cabeçalhos que podem ser acrescentados a pacotes, a fim de transportar o identificador de segurança, os dados de controle de integridade e outras informações. A segunda parte, é chamada se ISAKMP (*Internet Security Association and Key Management Protocol*) lida com o estabelecimento de chaves, para isso ele utiliza o protocolo IKE (*Internet Key Exchange*).

Para proteger um canal de comunicação entre dois sistemas finais diretamente conectados ou entre dois sistemas intermediários, Passito et. al. explica que são oferecidos serviços através de dois protocolos de segurança de tráfego, o protocolo AH (*Authentication Header*) que realiza a autenticação e o protocolo ESP (*Encapsulating Security Payload*) que é uma combinação de autenticação e criptografia. Estes protocolos podem ser implementados sozinhos ou ao mesmo tempo, dependendo das necessidades do serviço de segurança.

2.4.3.1 Associação de Segurança

Passito et. al. afirma que uma conexão que utiliza o protocolo IPSec possui criptografia e autenticidade dos dados, e para que isso funcione é necessário que os dois lados determinem quais algoritmos utilizar e compartilhem as chaves criptográficas das sessões. Uma associação de segurança (SA - *Security Association*) é o método que o IPSec utiliza para gerenciar as particularidades das sessões seguras entre duas ou mais entidades, transformando a camada de rede, que não é orientada à conexão, em uma rede com conexões lógicas.

Uma SA pode operar de duas maneiras: transporte e túnel.

No modo de transporte, em uma SA entre duas entidades, somente o segmento da camada de transporte é criptografado e autenticado. O cabeçalho do protocolo de segurança (AH ou ESP) aparece imediatamente após o cabeçalho IP e antes dos protocolos das camadas superiores. O endereço IP de origem e destino ainda estão abertos para verificação, caso os pacotes sejam interceptados.

No modo túnel, o tráfego IP gerado pelas entidades é capturado por um gateway de segurança e são criptografados. Esses pacotes são encapsulados novamente em pacotes IP, com endereços de origem e destino dos gateways de segurança, e enviados pela rede para outro gateway de segurança, que irá desencapsular a informação e a enviará para o destino. (PASSITO, et. al.)

A Figura 8 mostra como os dados trafegam na rede nos dois modos, transporte e túnel.

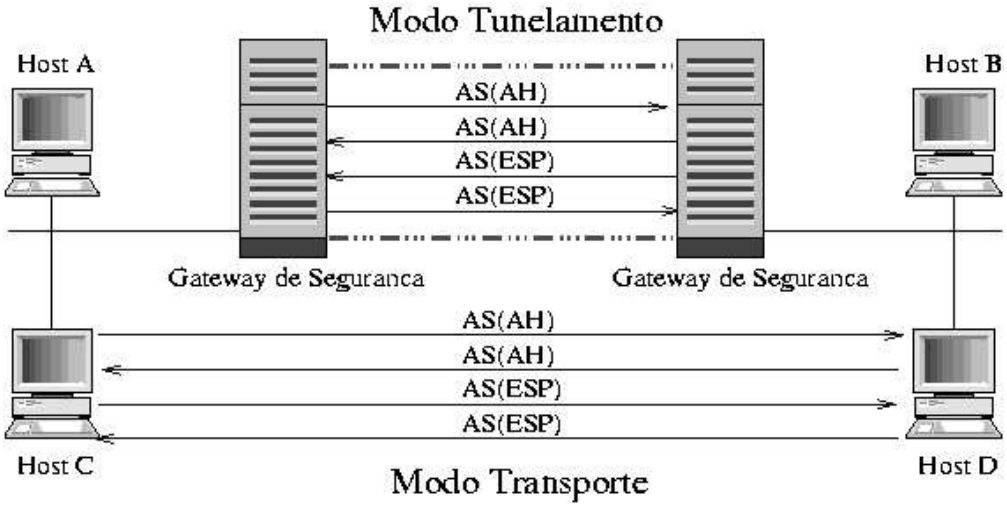

Figura 8: Os modos transporte e túnel no IPSec e as associações de segurança criadas (FONTE: PASSITO et. al).

2.4.3.2 Os protocolos AH e ESP

De acordo com Tanenbaum (2003) o protocolo AH não permite criptografia de dados, então sua principal utilidade é quando a verificação da integridade for necessária, mas não o sigilo. Esta característica do AH é mostrada na Figura 9.

O cabeçalho AH possuí além de um SPI (*Security Parameter Index*), um campo chamado Autenticação de dados, que contém um resumo da mensagem e uma assinatura digital. O resumo da mensagem é calculado em cima do datagrama IP original, fornecendo, desse modo, autenticação do sistema de origem

e integridade ao datagrama IP. A assinatura digital é processada utilizando o algoritmo de autenticação especificado na associação de segurança (PASSITO, et. al.).

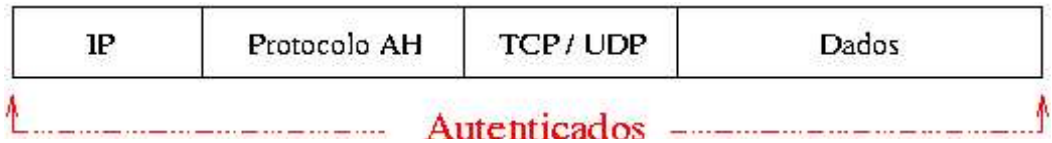

Figura 9: A posição de um cabeçalho AH (PASSITO, et. al.).

O outro cabeçalho IPSec alternativo é a ESP, sua utilização é mostrada na figura 10. Este cabeçalho consiste em duas palavras de 32 bits (TANENBAUM, 2003).

O protocolo ESP (*Encapsulating Security Payload*) foi projetado para oferecer um conjunto de serviços de segurança para o IPv6 e IPv4, como autenticação e confidencialidade através de criptografia. Esses serviços dependem das opções selecionadas no estabelecimento da AS.

Como visto na figura 10, um datagrama seguro é criado envolvendo o datagrama IP original com campos de cabeçalho e de *trailer* e, em seguida, inserindo esses dados encapsulados no campo de dados de um novo datagrama IP. Semelhante ao protocolo AH, o cabeçalho ESP possuí um valor de SPI para identificar a associação de segurança e um número de seqüência de datagramas para evitar possível ataque de reprodução. O valor presente no cabeçalho de *trailer* indica qual é o próximo protocolo (UDP, TCP, entre outros). Após o *trailer* há o campo de autenticação de dados do ESP que é semelhante ao campo de mesmo nome do cabeçalho AH (PASSITO, et. al.).

Conforme Passito et. al. o datagrama IP original e o *trailer* são criptografados, não sendo possível saber o tipo de protocolo de transporte que está sendo utilizado, evitando que monitoramentos cheguem a conclusões sobre o tráfego.

Figura 10: A posição do cabeçalho ESP. (PASSITO, et. al.).

3. ANÁLISES E CAPTURAS REALIZADAS

Neste Capítulo são mostradas as capturas do tráfego na rede e as análises realizadas. Para a realização do estudo foi utilizado um servidor para sistemas de telefonia, o Asterisk versão 1.4, instalado no sistema operacional Linux UBUNTU.

3.1 Asterisk

Segundo Gomillion e Dempster (2005, pág. 05) há inúmeras definições, que respondem a pergunta, o que é o Asterisk?

Traduzindo, asterisco é um símbolo (*). O símbolo representa o coringa em diversas linguagens de programação. Isto dá uma indicação de esperança dos desenvolvedores com relação ao Asterisk. Ele foi projetado para ser suficientemente flexível para satisfazer qualquer necessidade na telefonia.

Asterisk é um programa de código livre. Então milhares de desenvolvedores estão trabalhando diariamente no Asterisk, em suas extensões, programas compatíveis e instalações customizadas. A flexibilidade do produto vem do fato de o código fonte estar disponível, o que significa que se pode mudar o comportamento do Asterisk para satisfazer as necessidades de qualquer desenvolvedor.

De acordo com Gomillion e Dempster (2005) ele também funciona como um sistema de Voz sobre IP, pois, permite a utilização do protocolo de Internet IP para chamadas telefônicas, em harmonia com as tecnologias de telefonia tradicionais.

O Asterisk utiliza o protocolo SIP para a comunicação VOIP, este protocolo por sua vez utiliza o protocolo de tempo real RTP, e utiliza portas UDP da pilha TCP/IP.

3.1.1 Configurando o Asterisk

De acordo com Gomillion e Dempster (2005, pág. 60) os arquivos básicos de configuração que necessitam de alterações para a realização do estudo e para o funcionamento do Asterisk são o sip.conf e extensions.conf.

- **sip.conf:** Configura-se o protocolo SIP através da edição do arquivo /etc/asterisk/sip.conf. Este arquivo tem uma serie de configurações na seção, seguida das definições de usuários.

Um exemplo de cadastro de clientes SIP:

```
[8011]
callerid=Amanda
username=8011
secret=123456
host=dynamic
type=friend
context=interno
```

Onde,

[8011]: 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”.

Type: Há três tipos de usuários: user: esta conexão pode fazer chamadas; peer: esta conexão pode receber chamadas e friend: esta conexão pode fazer e receber chamadas.

Context: define o contexto padrão das ligações para as ligações chegando do servidor. Este contexto é configurado no arquivo extensions.conf.

- **extensions.conf:** Configura-se a extensão através da edição do arquivo /etc/asterisk/extensions.conf. Neste arquivo é configurado o plano de discagem, a parte mais importante no Asterisk.

A sintaxe genérica para uma linha no extensions.conf é:

Exten => número_da_extensão, prioridade, ação

Um exemplo de como criar uma Extensão:

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

Onde,

Dial (tecnologia/id, opções): é aqui que se diz ao Asterisk para que faça o telefone tocar, e quando a linha for atendida, conectar a ligação.

${EXTEN}: utiliza a extensão corrente, variável pré-definida

Hangup: é utilizado para que a ligação consiga se desconectar

3.2 Soft Phones

Para a realização de chamadas foi utilizado um software, conhecido como ‘Soft Phone’, o X-Lite 2.0, desenvolvido pela CounterPath Solutions, este Soft Phone se baseia no protocolo SIP, e sua versão é free.

Figura 11: Soft Phone X-lite 2.0

Gomillion e Dempster (2005, pág. 26) dizem que assim como telefones hard são implementados em hardware, telefones soft (Soft Phones) são implementados em software. Estes são mais baratos de serem implementados.

Quanto à qualidade do som percebida em um soft phone isso depende dos recursos disponíveis no PC, na qualidade do software utilizado e da rede de dados entre o cliente e o servidor.

A desvantagem de usar soft phones para VOIP é a questão que muitos usuários não aceitam ou não de adaptam. Na questão da energia também há desvantagens.

Porém, a vantagem mais significativa do uso de um soft phone é o custo (GOMILLION; DEMPSTER, 2005).

3.2.1 Captura do Tráfego

As capturas do tráfego realizadas para este estudo foram feitas em uma rede ethernet de 100mbps, com seis máquinas (o servidor e mais cinco máquinas), com link ADSL para internet de 400Kbps.

A Figura 12 mostra a topologia da rede utilizada no estudo.

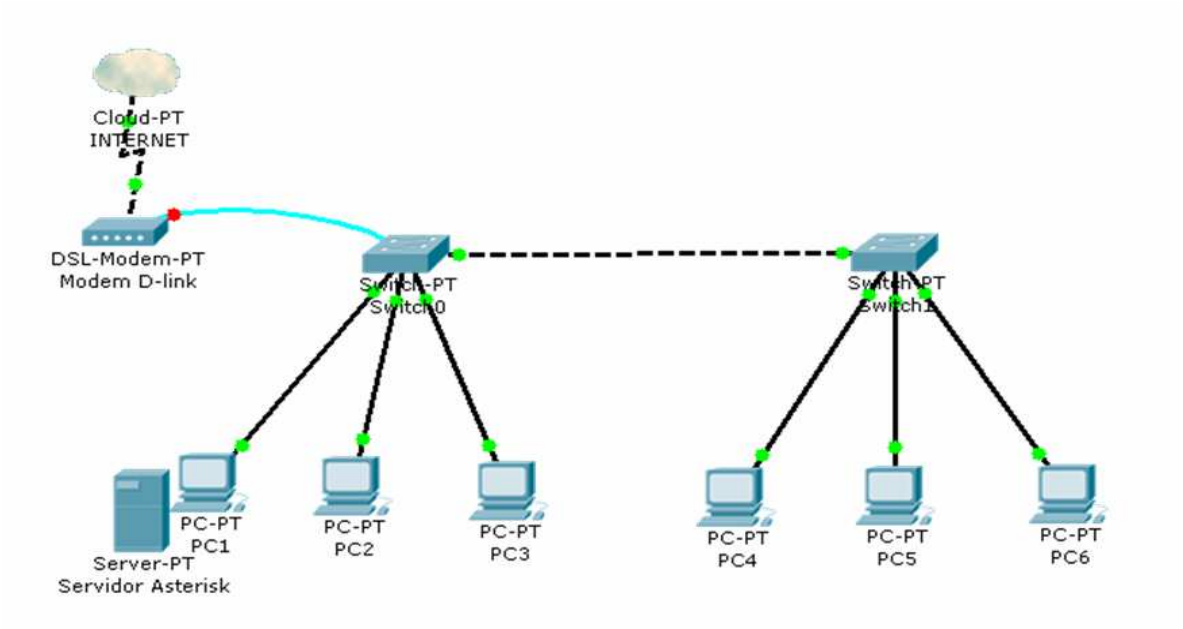

Figura 12: Topologia da Rede.

Após a instalação e configuração do servidor Asterisk, realizou-se chamadas VOIP utilizando o soft phone x-lite, foram feito testes entres pc's em uma rede IP, esses dados foram capturados pelo software Wireshark – Network Protocol Analyzer, versão 0.99.6a.

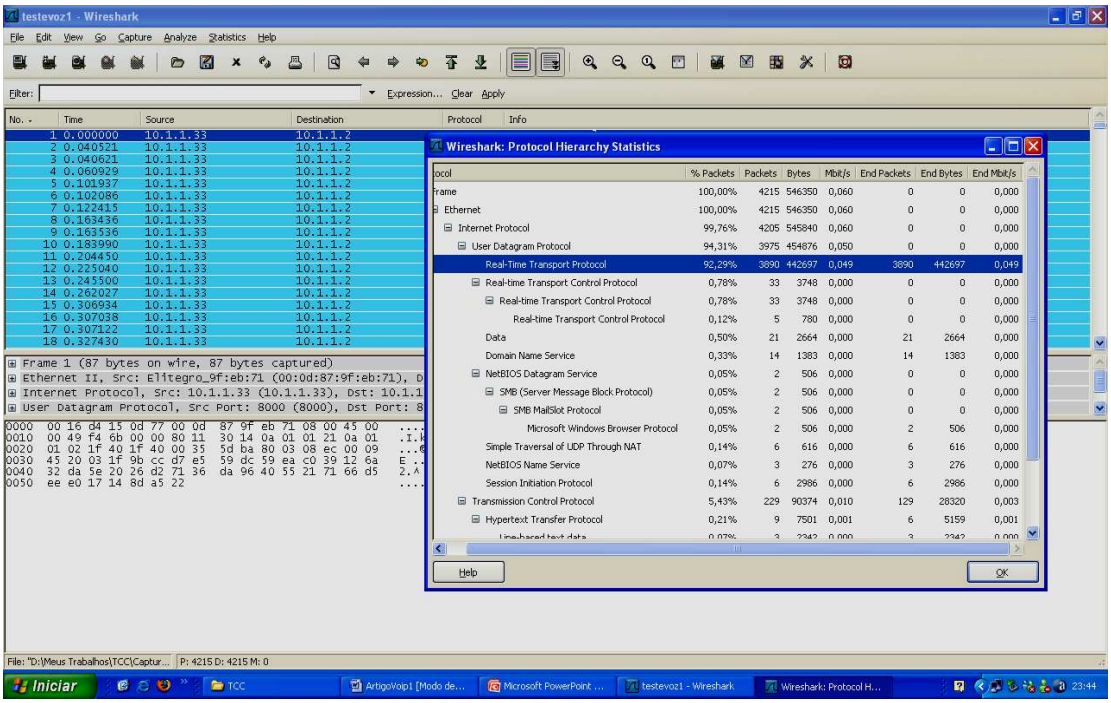

Figura 13: Software Wireshark – Network Protocol Analyzer

Todos os testes de capturas de tráfego dos dados na rede foram feitos durante dois meses, não ininterrupta, somente algumas capturas por semana, totalizando quarenta testes, sendo dez testes de cada modo. Foram realizadas dez capturas do tráfego normal da rede, dez capturas do tráfego com ligações VOIP ativas, dez capturas do tráfego normal com conexão VPN entre os pc's e dez capturas do tráfego com ligações VOIP ativas e com conexão VPN. Todos estes testes têm duração média de um minuto.

Em cada teste é analisado todas as informações do tráfego capturado, como: o protocolo utilizado, números de pacotes enviados e recebidos, número total de bytes, número de Mbit por segundo, o IP da origem e do destino, portas, tempo das chamadas e também a porcentagem utilizada da rede.

A Tabela 3 mostra todos os dados transmitidos pelo protocolo UDP, retirado de um teste onde havia uma chamada VOIP estabelecida, estes dados foram capturados pelo software Wireshark.

Tabela 3: Todos os dados do Testedevoz2 capturados pelo Wireshark.

Adress A	Port A	Adress B	Port B	Packets	Bytes	Packtes A->B	Bytes A->B	Packtes A<-B	Bytes A<-B
10.1.1.5	5060	10.1.1.2	4678	2	1076	1	497	1	579
10.1.1.27	138	10.255.255.255	138	7	1616	7	1616	0	0
10.1.1.5	5060	10.1.1.33		10	3230	3	1563	7	1667
10.1.1.2	137	10.255.255.255	137	11	1156	11	1156	0	0
10.1.1.33	15801	10.1.1.5	8001	30	4020	0	0	30	4020
10.1.1.5	10185	10.1.1.33	8001	51	5756	22	1892	29	3864
10.1.1.5	8000	10.1.1.33	8000	6550	724663	1219	260866	5331	463797

Neste teste estava ativa uma conversa via VOIP entre dois participantes, com duração de um pouco mais de um minuto, a tabela mostra o IP de origem e destino, portas de origem e destino e também a quantidade de pacotes e de bytes trafegados pela rede.

Para a realização de análises foram realizados capturas do tráfego normal de dados na rede. A Tabela 4 mostra um resumo dos dados mais importantes das capturas de tráfego normal de uma rede IP.

Tabela 4: Dados básicos das capturas do tráfego normal da rede.

Teste	Protocolo	Tráfego (%)	Pacotes	Bytes	Kbps
Teste1	TCP	95,4	519	298964	27
Teste2	TCP	94,5	468	285636	35
Teste3	TCP	96,12	1140	739280	60
Teste4	TCP	98,83	2874	2521792	192
Teste5	TCP	90,63	300	89663	4
Teste6	TCP	91,93	740	373001	54
Teste7	TCP	91,90	737	393798	37
Teste8	TCP	97,13	1625	1395181	127
Teste9	TCP	73,33	110	13545	2
Teste10	TCP	92,70	736	366541	37

Fazendo uma média da porcentagem dos dados trafegados na rede tem-se um total de 92,25% (noventa e dois vírgula vinte e cinco por cento) de utilização do tráfego total. São enviados em média 925 (novecentos e vinte e cinco) pacotes por teste, em média 57,5Kbps.

Já a tabela 5 mostra os dados de todos os testes realizados capturando o tráfego na rede no momento em havia uma ligação VOIP ativa entre duas máquinas.

Tabela 5: Dados básicos das capturas do tráfego com chamadas VOIP.

Teste	Protocolo	Tráfego (%)	Pacotes	Bytes	Kbps
Testevoz1	RTP	92,29	3890	442697	49
Testevoz2	RTP	98,17	6550	724663	53
Testevoz3	RTP	91,37	6785	1331947	87
Testevoz4	RTP	98,05	5467	998107	97
Testevoz5	RTP	91,84	6795	1267567	71
Testevoz6	RTP	97,05	1972	395564	64
Testevoz7	RTP	95,53	2161	431692	90
Testevoz8	RTP	91,56	4427	888163	74
Testevoz9	RTP	97,58	4563	480293	45
Testevoz10	RTP	98,41	4699	528320	52

Agora, analisando estes dados a média da porcentagem dos pacotes de voz trafegados na rede, é de 95,18% (noventa e cinco vírgula dezoito por cento) de utilização do tráfego total. E são enviados em média 4730 (quatro mil setecentos e trinta) pacotes de voz por teste, na média de 68,2Kbps.

Na máquina onde estavam sendo realizadas as capturas funcionava também como cliente VOIP, devido a esse fato o fluxo de pacotes transmitidos pelo protocolo RTP foi bem amplo, utilizando quase todo o trafego da rede.

A seguir apresentam-se os gráficos para uma melhor ilustração do tráfego na rede.

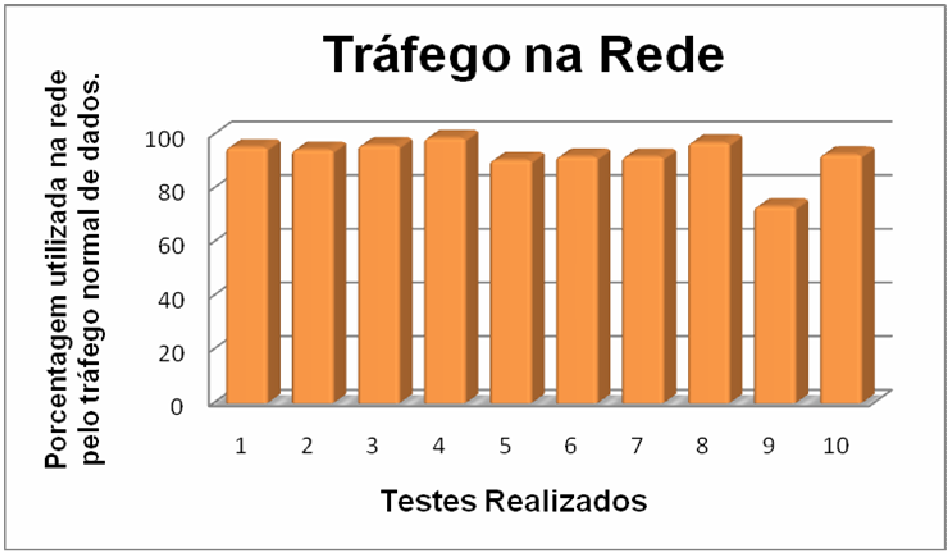

Figura 14: Gráfico da porcentagem dos dados trafegados na rede.

Com base nos dados da Tabela 4, criou-se este gráfico (Figura 14), avaliando o gráfico e a tabela nota-se que a maioria dos testes utilizaram quase todo o trafego da rede para transmitir de pacotes de dados através do protocolo TCP. No gráfico o eixo x (porcentagem utilizada na rede pelos pacotes de voz), mostra que dos dez testes realizados mais da metade ultrapassou noventa por cento (90%) do tráfego na rede.

Figura 15: Gráfico da porcentagem de pacotes de Voz trafegados pela Rede.

Logo, o gráfico acima (Figura 15) deu-se com base nos dados da Tabela 5.

Analisando a Figura 15 e a Tabela 5, tem-se também uma grande utilização do tráfego, porém agora são pacotes de voz transmitidos pelo protocolo UDP. Observando o eixo x (porcentagem utilizada na rede pelos pacotes de voz) do gráfico, nota-se que todos os testes utilizou mais que noventa por cento (90%) do tráfego da rede.

3.3 Segurança

Em virtude dos fatos anteriormente descritos com relação à segurança das informações que trafegam em uma rede IP, faz-se então necessário, o estabelecimento de um canal seguro para o tráfego da voz.

Para a implementação do esquema proposto foi utilizado uma Ferramenta VPN para garantir a segurança no tráfego de voz entre o cliente e o servidor, foi estabelecido um túnel VPN dentre duas máquinas em uma rede ethernet.

Existem dois softwares para VPN, duas formas diferentes de se implementar:

- FreeSwan: Utiliza o IPSec para fazer o tunelamento. O FreeSwan é pouco usado pela sua complexidade na implementação e, por sua deficiência ao tratar com roteadores que utilizam o NAT (*Network Address Translation* ou Tradução de Endereço de Rede).
- OpenVPN: Comparado ao FreeSwan, este oferece muito mais flexibilidade na implementação, além de não ter problemas em estruturas com o gateway fazendo NAT (OPENVPN, 2006).

A ferramenta escolhida foi o OpenVPN, por se tratar de uma implementação baseada em software e que garante alta confiabilidade para a comunicação, além de ter seu custo bastante reduzido, em virtude de não necessitar de hardware específico.

3.3.1 OpenVpn

Neste estudo de caso foi utilizado o software OpenVpn, para prover mecanismos de segurança.

O OpenVPN usa criptografia de chaves ao invés de usuário e senha para fechar um túnel de VPN. Basicamente o OpenVpn pega a informação que ele precisa mandar para a outra ponta, criptografa ela, e manda pela internet ou pela ethernet por um pacote UDP. A grande vantagem, é que ele não tem muitos problemas para passar por firewalls, e por roteadores que fazem NAT.

Atualmente, o OpenVPN roda nas seguintes plataformas: Linux, Windows 2000/XP ou superior, OpenBSD, FreeBSD, NetBSD, Mac OS X, e Solaris.

O OpenVPN pode operar com 3 tipos de criptografia. Nenhuma criptografia (apenas o túnel), criptografia com chaves estáticas e no modo TLS, em que as chaves são trocadas periodicamente. No estudo foi configurado para ser utilizada uma chave estática de 2048 bits entre cliente e servidor.

Após a instalação do software Openvpn, é necessário configurar as duas máquinas que irão se conectar na VPN. A configuração básica do OpenVpn é a edição de dois arquivos de texto: client.conf e server.conf.

Abaixo são descritos os arquivos de texto utilizados para a configuração das duas máquinas que se conectam na VPN. É utilizada uma mesma chave de criptografia tanto para a máquina que funciona como cliente, quanto para a máquina que funciona como o servidor. Esta chave é chamada de static.key, e o próprio software OpenVpn gera aleatoriamente uma chave, porém as duas máquinas tem que possuir a mesma chave gerada, no mesmo diretório onde está localizado o arquivo de texto. Como por exemplo, na máquina do cliente, deve conter em um diretório especificado o arquivo client.conf e o arquivo static.key. Assim sendo para que haja uma conexão Vpn, na máquina do servidor deve conter o arquivo server.conf e o arquivo static.key.

client.conf:
remote 10.1.1.2
dev tun
Ifconfig 10.8.0.2 10.8.0.1

server.conf:
dev tun
ifconfig 10.8.0.1 10.8.0.2
secret static.key

secret static.key

A Figura 16 ilustra o cenário da conexão VPN utilizada no estudo realizado, um cliente conectado em uma mesma rede ethernet (rede corporativa) na qual o servidor se encontra.

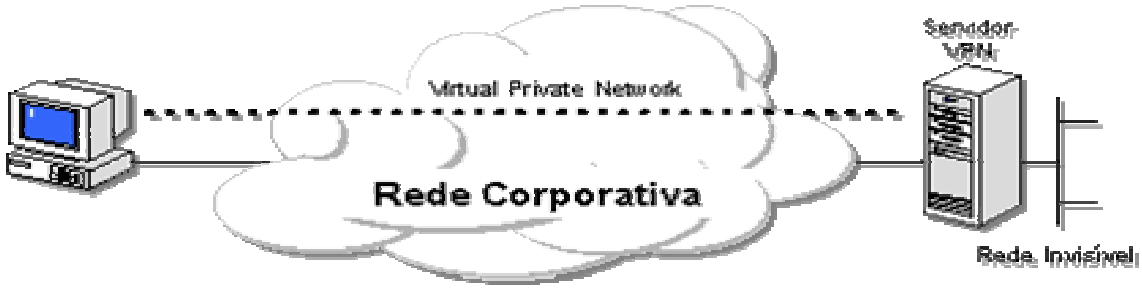

Figura 16: Conexão VPN entre duas máquinas na mesma rede ethernet (Fonte: CHIN, 1998).

Esta configuração de transmissão de voz com métodos seguros foi uma solução proposta funcional. A seguir são descritos os testes de transmissão de voz realizados para verificação da viabilidade desses métodos de segurança.

3.3.2 Captura do Tráfego

Após a instalação e configuração da rede virtual privada, realizaram-se mais testes, porém agora capturando o tráfego na rede com e sem chamadas VOIP ativas, entre duas máquinas do túnel VPN.

Agora se apresenta os testes realizados com estes mecanismos de segurança implementados, este tráfego dos dados na rede foi capturado durante três semanas, não ininterrupta, somente algumas capturas ao dia, totalizando vinte testes, dez testes capturando o tráfego de dados transmitidos com mecanismos de segurança e dez testes capturando o tráfego de voz (VOIP), transmitidos com mecanismos de segurança.

Aqui também são analisadas todas as informações dos pacotes capturados, porém agora existe uma conexão VPN entre os dois participantes da chamada VOIP.

A Tabela 6 mostra todos os dados transmitidos pelo protocolo UDP retirado de um teste onde havia chamada VOIP estabelecida e túnel VPN conectado, estes dados foram capturados pelo software Wireshark.

Tabela 6: Dados de um teste realizado com a ligação VOIP e conexão VPN ativa.

Adress A	Port A	Adress B	Port B	Packet	Bytes	Packtes A->B	Bytes A->B	Packtes A<-B	Bytes A<-B
10.1.1.7	138	10.255.255.255	138	1	252	1	252	0	0
10.1.1.2	16907	10.1.1.33	8001	7	602	7	602	0	0
10.1.1.33	11983	10.1.1.2	8001	9	1194	0	0	9	1194
10.1.1.2	8000	10.1.1.33	8000	304	26448	304	26448	0	0
10.1.1.2	1194	10.1.1.33	1194	1782	508908	0	0	1782	508908

A seguir são mostrados os dados capturados em um teste onde no momento da captura havia uma conexão VPN entre duas máquinas da rede. A Tabela 7 mostra um resumo dos dados mais importantes das capturas de tráfego normal de uma rede IP, transmitidos com mecanismos de segurança.

Tabela 7: Dados básicos das capturas do tráfego da rede realizados com mecanismos de segurança.

Teste	Protocolo	Tráfego (%)	Pacotes	Bytes	Kbps
TesteVpn1	TCP	89,67	243	32877	1
TesteVpn2	TCP	74,76	462	141733	4
TesteVpn3	TCP	89,67	214	53631	2
TesteVpn4	TCP	80,00	68	6738	1
TesteVpn5	TCP	95,64	329	169779	11
TesteVpn6	TCP	90,06	136	31721	3
TesteVpn7	TCP	87,16	353	116910	11
TesteVpn8	TCP	87,30	969	723603	71
TesteVpn9	TCP	96,43	459	215925	12
TesteVpn10	TCP	86,49	192	101181	8

Analisando estes dados temos uma média da porcentagem dos pacotes de voz trafegados na rede, onde se tem 87,71% (oitenta e sete vírgula setenta e um por cento) de utilização do tráfego total. Enviados em média 342 (trezentos e quarenta e dois) pacotes de voz por teste, em 12,4Kbps.

Já a Tabela 8 mostra os dez testes realizados capturando o tráfego de voz, transmitidos com segurança, ou seja, no momento das capturas havia um túnel VPN conectado entre duas máquinas e também havia uma ligação VOIP estabelecida entre as duas máquinas da conexão VPN, estes pacotes de voz transmitidos pelo protocolo UDP estavam então criptografados.

Tabela 8: Dados básicos das capturas realizadas com chamadas VOIP estabelecidas com mecanismos de segurança.

Teste	Protocolo	Tráfego (%)	Pacotes	Bytes	Kbps
TestevozVpn1	UDP	97,68	2130	537404	121
TestevozVpn2	UDP	97,45	5383	878963	53
TestevozVpn3	UDP	93,01	6230	1593975	108
TestevozVpn4	UDP	99,81	6394	1207344	67
TestevozVpn5	UDP	99,72	4591	1234604	91
TestevozVpn6	UDP	99,40	4164	1044331	139
TestevozVpn7	UDP	98,72	4407	1103410	139
TestevozVpn8	UDP	98,83	3561	918176	133
TestevozVpn9	UDP	92,64	6077	1686855	93
TestevozVpn10	UDP	93,77	4214	1156952	92

Analisando estes dados calculou-se a média da porcentagem dos pacotes de voz trafegados na rede, resultando em 97,10% (noventa e sete vírgula dez por cento) de utilização do tráfego total. Sendo enviados em média 4715 (quatro mil setecentos e quinze) pacotes de voz por teste, na média de 103,6Kbps.

Para um melhor entendimento da Tabela 8, é ilustrada a seguir em forma de gráfico pizza a quantidade de pacotes enviados nos dez testes realizados com mecanismos de segurança implementados e com tráfego de voz (VOIP), e a quantidade de Kbps também transmitidos em cada um destes testes.

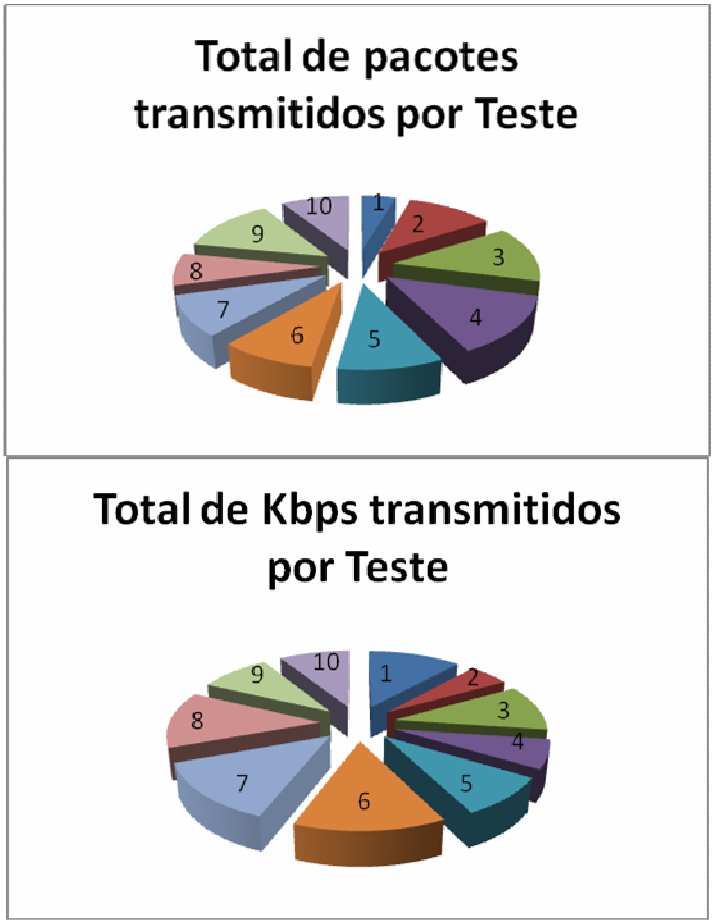

Figura 17: Gráfico do total de Pacotes e Kbps transmitidos nos testes de VOIP pelo túnel VPN.

Observando a tabela e o gráfico (Figura 17) percebe-se que na maioria dos casos a quantidade de pacotes enviados é relativamente proporcional a quantidade de Kbps, onde cada número na figura corresponde a cada teste realizado (TestevozVpn1 ao TestevozVpn10).

A figura a seguir mostra uma tela do software Wireshark capturando o tráfego na rede no momento em que havia uma conexão VPN entre duas máquinas que estavam conversando via VOIP. Notam-se na imagem que as portas de origem e destino são as portas destinadas ao tráfego de VPN.

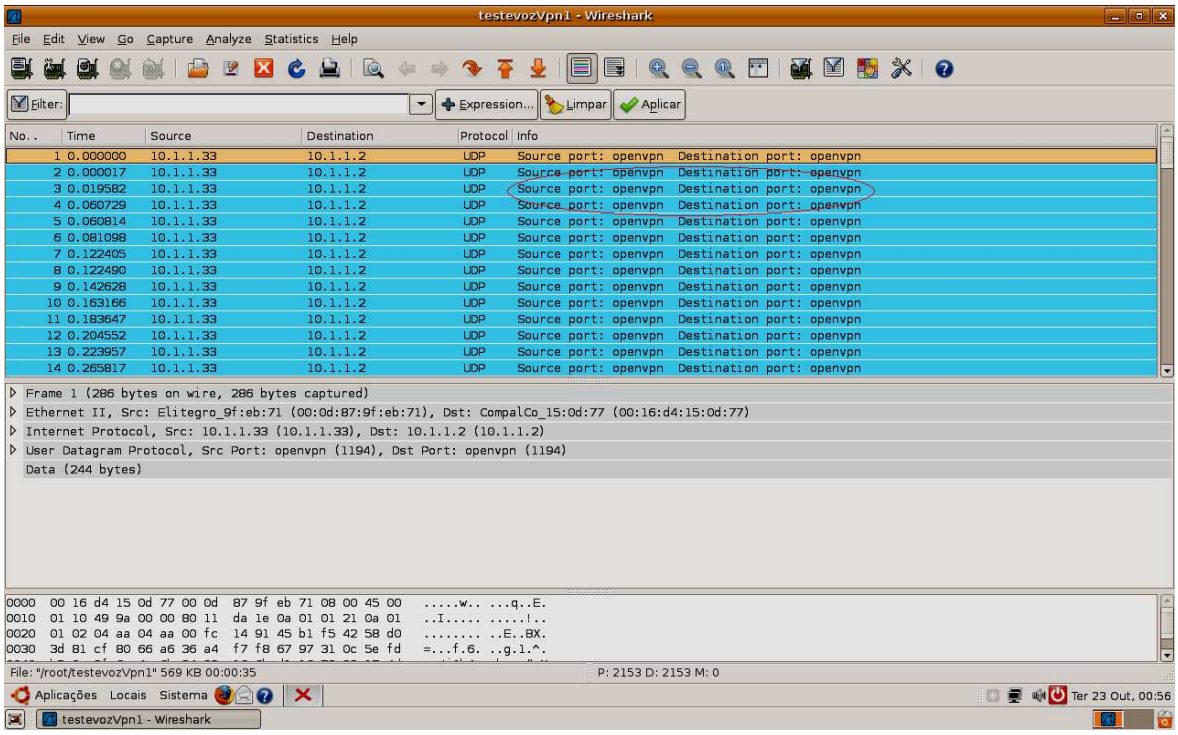

Figura 18: Software Wireshark - Captura de um teste VOIP com conexão VPN ativa.

A seguir apresentam-se os gráficos ilustrando a porcentagem da utilização do tráfego na rede IP, com mecanismos de segurança implementados.

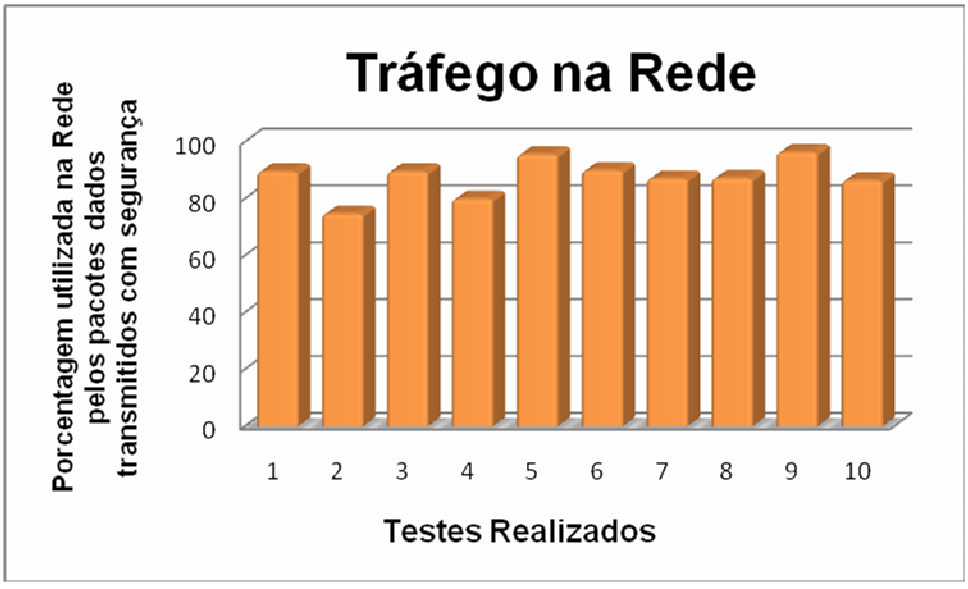

Figura 19: Gráfico da porcentagem de pacotes de dados trafegados na rede com conexão VPN.

A Figura 19 ilustra de maneira gráfica os dados coletados sobre o percentual do tráfego utilizado na rede por pacotes de dados transmitidos no momento em que havia um túnel VPN conectado na rede, mostrados na Tabela 7.

Com base nos dados da Tabela 7, criou-se este gráfico (Figura 19), avaliando o gráfico e a tabela nota-se que a maioria dos testes não ultrapassaram os noventa por cento (90%) do tráfego na rede, como nos outros casos, ou seja, não trafegou muitos pacotes de dados através do protocolo TCP, pelo túnel VPN.

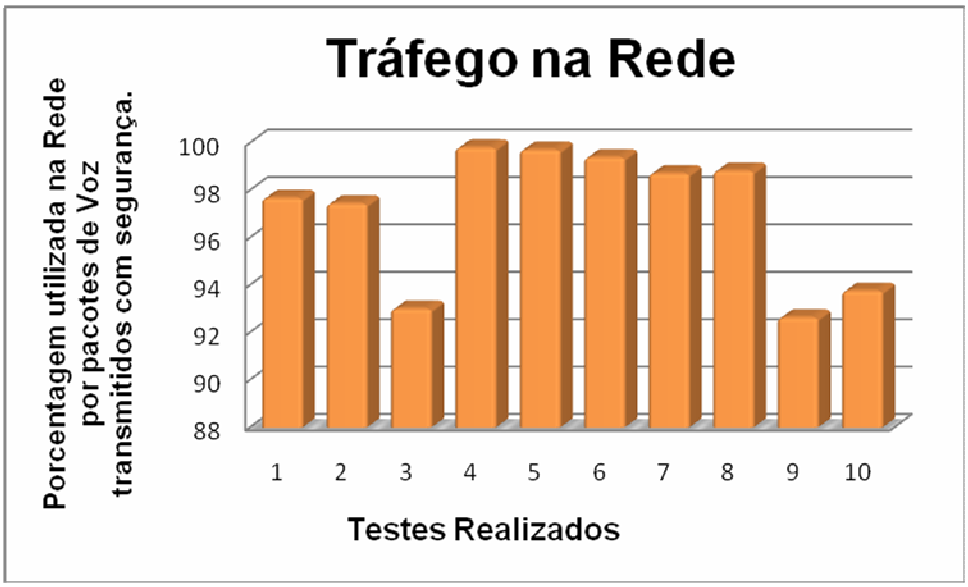

Figura 20: Gráfico da porcentagem de pacotes de voz (VOIP) trafegados na rede com conexão VPN.

Já a Figura 20 ilustra de maneira gráfica os dados coletados sobre o percentual do tráfego utilizado na rede por pacotes de voz (VOIP) transmitidos no momento em que havia uma conexão VPN entre os participantes da chamada, ou seja, essa voz trafegava pela rede com total segurança, os pacotes estavam criptografados.

Considerando o gráfico acima e a Tabela 8 nota-se que todos os testes ultrapassou os noventa por cento (90%) do tráfego na rede, alguns quase atingiram a utilização total do tráfego (100%), ou seja, houve um tráfego intenso devido ao grande fluxo de pacotes de voz transmitidos com segurança, através do protocolo UDP, pelo túnel VPN.

A seguir é mostrado um gráfico comparando a utilização do tráfego de voz, transmitidos sem segurança, e com mecanismos de segurança.

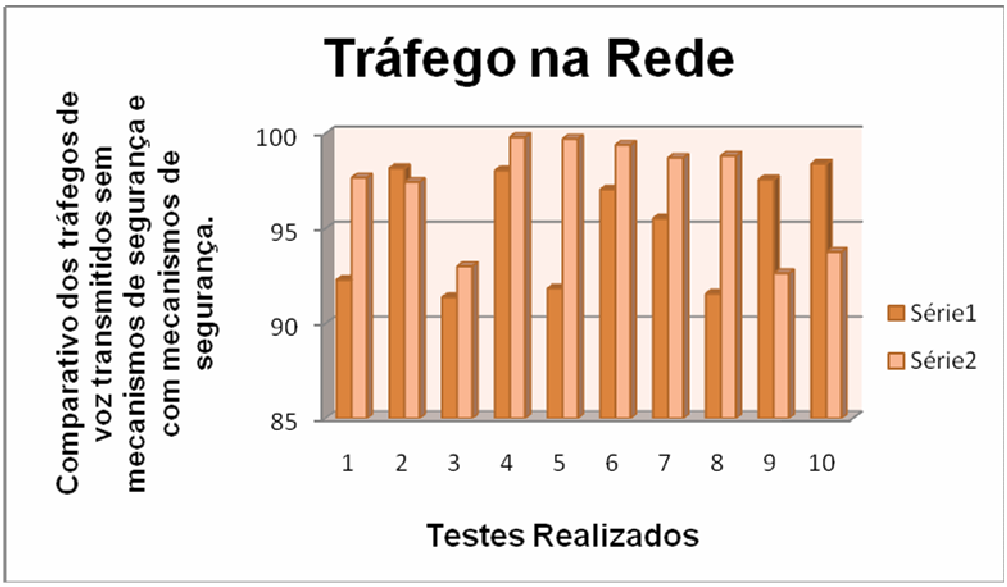

Figura 21: Gráfico comparativo dos tráfegos

A Figura 21 mostra uma comparação dos dois tráfegos de voz, onde a Série1 representa a utilização do tráfego na transmissão de pacotes de voz enviados sem mecanismos de segurança. E a Série2 representa o tráfego na transmissão de pacotes VOIP enviados com mecanismos de segurança, via túnel VPN. Nota-se que a porcentagem do tráfego de voz sem mecanismos de segurança (Série1) na maioria dos testes, foi menor que a porcentagem utilizada pelo tráfego de pacotes de voz enviados com métodos seguros.

3.4 Análises dos Dados

Analisando todos os testes realizados, com e sem chamadas VOIP ativas, antes e depois da implementação de mecanismos de segurança (VPN) podemos notar algumas diferenças nos dados capturados.

Com base nos dados coletados pode-se informar que:

Tabela 9: Média dos dados coletados em geral.

Tipo do Teste	Média do Tráfego (%)	Média dos pacotes	Média em Kbps
Tráfego normal de Dados	**92,25**	**924**	**57,5**
Tráfego de voz (VOIP)	**95,18**	**4730**	**68,2**
Tráfego de Dados c/ VPN	**87,71**	**342**	**12,4**
Tráfego de voz (VOIP) c/ VPN	**97,10**	**4715**	**103,6**

A Tabela 9 apresenta as medianas dos dados analisados (média do tráfego, média dos pacotes enviados, e a média do tráfego em Kbps). Fazendo comparações nota-se que a porcentagem do tráfego utilizada por todos os testes não se difere muito, a grande diferença encontra-se na quantidade de pacotes transmitidos e a quantidade de Kbps. Essa diferença acontece pelo fato dos pacotes de dados não passarem pelo túnel VPN, somente pacotes VOIP trafegaram via conexão VPN.

Os testes com tráfego de voz necessitam de mais largura de banda, ou seja, necessita enviar mais pacotes de voz por segundo, comparado com os pacotes de dados, isto se dá pelo fato da voz ser trafegada em tempo real, contudo pacotes de voz têm prioridade no tráfego o que ocasiona uma grande utilização do tráfego na rede.

Para uma melhor análise da transmissão de voz com mecanismos de segurança, realizou-se o mesmo teste duas vezes, com chamadas VOIP estabelecidas (com a mesma gravação de voz, no mesmo período de tempo), porém uma vez com a conexão VPN ativa, e o outro teste sem conexão VPN, ou seja, sem mecanismos de segurança.

E o resultado são os dados que constam na tabela a seguir:

Tabela 10: Dados dos dois testes com transmissão de voz gravada.

Teste	Tráfego (%)	Protocolo	Pacotes	Bytes	Kbps
Testegravado1	**99%**	**UDP/RTP**	**2233**	**207552**	**38**
Testegravadovpn1	**99%**	**UDP**	**2532**	**239598**	**38**

Observando estes dados da Tabela 10 pode-se notar que a porcentagem do tráfego da rede utilizada pelos pacotes de voz foi o mesmo, noventa e nove por cento (99%), e a quantidade de Kbps transmitidos também se iguala, o que se diferenciou foi a quantidade de pacotes enviadas por testes, onde o teste de voz sem métodos de segurança teve um total de 2233 pacotes enviados, enquanto no teste de voz transmitidos com segurança (dados criptografados) enviou 2532 pacotes, ou seja, mais pacotes.

Também na quantidade de Bytes total enviados houve diferenças, enquanto no teste de voz sem métodos de segurança deu-se um total de 207552 (duzentos e sete mil, quinhentos e cinqüenta e dois) bytes transmitidos, no teste de voz transmitidos com segurança (dados criptografados) foram enviados 239598 (duzentos e trinta e nove mil, quinhentos e noventa e oito) bytes, ou seja, mais bytes.

Entende-se então que pacotes com mecanismos de segurança necessitam de um link de transmissão maior que o link para transmissão de pacotes de voz sem métodos de segurança, segundo dados uma quantidade necessária seria 64Kbps, para se obter uma ligação satisfatória. Neste estudo a maioria dos testes de voz transmitidos com segurança obteve essa quantia mínima, pois se trata de uma rede interna de 100Mbps.

4. CONCLUSÕES E TRABALHOS FUTUROS

Como já dito, a tecnologia VOIP surgiu para integrar duas redes muitos 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, mostrar seu funcionamento e características gerais, e compreender os impactos que a transmissão de voz ocasiona em redes IP, além disso, transmitida com segurança.

Diante da necessidade da transmissão de voz em redes IP de maneira segura, pela questão do sigilo, privacidade e integridade dos dados, surgiu este estudo, analisar a qualidade da voz quando transmitida com mecanismos de segurança.

Durante o estudo, na fase de implementação de medidas de segurança notou-se a possibilidade de se estar implementando uma VPN através do OpenVpn, ferramenta na qual não utiliza o protocolo IPSEC. Como o estudo visa a implementação de uma VPN entre duas máquinas de uma mesma rede e não entre redes externas, o mecanismo de tunelamento e criptografia do OpenVpn atende a necessidade deste estudo.

Visando solucionar esta questão e devido ao fato deste protocolo ser grande e complexo, foram realizadas medidas de segurança implementando o OpenVpn, já que analisadas as finalidades e funcionalidades, este, o OpenVpn se aplica melhor no caso.

Pode-se concluir que se a tecnologia VOIP for implantada corretamente, fazendo pré-analises da rede, ela trará muitos benefícios para a organização, como, economia, versatilidade, flexibilidade.

Conclui-se também que a característica, os equipamentos e as tecnologias utilizadas para se implementar VOIP influenciam diretamente na qualidade e na vantagem de se utilizá-lo. Para a utilização em uma rede local onde a largura de banda é alta, as chamadas atendem perfeitamente, o problema passa a ser quando se utiliza um link com menos de 64Kbps, neste caso as ligações podem chegar cortadas, com atraso, com eco e também pode ocorrer a perda de pacotes.

Visto que os pacotes de voz trafegando na rede utilizam em média 95,18% do total da rede. E os pacotes de voz com métodos de transmissão seguros utilizam em média 97,10% do tráfego total da rede.

Conclui-se então que a tecnologia VOIP necessita de uma largura de banda bastante considerável para não ocasionar congestionamento na rede, e também para que a voz chegue ao seu destino com uma boa qualidade.

O VOIP mesmo sendo uma tecnologia nova, já esta mudando a maneira de comunicação entre muitas pessoas, e promete revolucionar a maneira como nos comunicamos.

Dentre as sugestões para trabalhos futuros, pode-se colocar o estudo da Segurança em chamadas VOIP entre redes externas. Implementando assim o método VPN FreeSwan, utilizando o protocolo de segurança IPSEC.

Outra sugestão seria um estudo da transmissão de voz em redes Wireless, poderia também ser implementado uma VPN, para que haja transmissão segura, pois o atual modelo de redes sem fio não é totalmente seguro, mesmo alterando as configurações de segurança no Access Point, ou fazendo controle de acesso por endereços MAC, a rede não está imune à invasões ou captura de dados sigilosos.

5. REFERÊNCIAS

ALVES, Nilton Jr. **Protocolos TCP/IP.** CENTRO BRASILEIRO DE PESQUISAS FÍSICAS (CBPF). **Protocolos TCP/IP.** Disponível em: <http://mesonpi.cat.cbpf.br/naj/tcpipf.pdf>. Acesso em 03 de abril de 2007.

ANDRADE, D. B. F. de; SANCHES, T. A.; WYDRA, R. **Projeto VOIP – Pesquisa sobre hábitos e costumes dos internautas no uso de Messenger.** Projeto Interdisciplinar do 4º Período do Curso de Comunicação Social, habilitação em Publicidade e Propaganda, Gestão de Pesquisa de Mercado da Universidade Anhembi Morumbi, 2005. Disponível em: <http://www.despensa.com.br/Trabalho%20Inter.pdf>. Acesso em 17 de abril de 2007.

BERNAL, Huber Filho. **Banda Larga e VOIP.** Teleco informações em telecomunicações (2007). Disponível em: <http://www.teleco.com.br>. Acesso em 26 de março de 2007.

CHIN, Liou Kuo. **Virtual Private Network.** Rede Nacional de Ensino e Pesquisa (RNP), 1998. Disponível em http://www.rnp.br/newsgen/9811/vpn.html. Acesso em 22 de outubro de 2007.

COSTA, Daniel G. **Uma Introdução ao padrão ITU H.323.** Rede Nacional de Ensino e Pesquisa. Natal – RN, 2004.

DANTAS, Mario. **Tecnologia de Redes de Comunicação e Computadores**. Axcel Books. 2002.

FORUM. **Voice Over Packet Security Forum.** Disponível em: <http://www.vopsecurity.org/>. Acesso em: 02 de maio de 2007.

GOMILLION, David; DEMPSTER, Barrie. **Construindo Sistemas de Telefonia com o Asterisk.** Packt Publishing. 2005.

INTERNET ENGINEERING TASK FORCE (IETF). Disponível em: <http://www.ietf.org>. Acesso em: abril 2007.

JUNIOR, Renato. **Apostila de "Internet e Arquitetura TCP/IP".** Volume I, 2007. Disponível em: <http://www.rjunior.com.br/download/tcp.pdf>. Acesso em: 26 de setembro de 2007.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet**. 3. ed. Pearson Education. 2006.

MARTINS, Alan Diego et al. **Segurança aplicada à VOIP sobre o protocolo SIP:** Estudo das vulnerabilidades e suas soluções (2006). Disponível em: <http://www.modulo.com.br/pdf/VoIP-TCCvfinal.pdf>. Acesso em: 13 de maio de 2007.

NAZARIO, Débora L. **Protótipo de um Sistema de Telefonia IP para LANs baseado no Padrão SIP**. 2003. 50 f. Trabalho de Conclusão de Curso – Universidade Regional de Blumenal, Blumenal - SC.

OPENH.323. **The OpenH323 Project.** Disponível em: < http://www.openh323.org/>. Acesso em 23 de maio de 2007.

OPENVPN. **OpenVpn.** 2006. Disponível em: http://openvpn.net/. Acesso em 29 de setembro de 2007.

PALU JR, Ari **Interface Administrativa para Firewall de Internet em Ambiente Linux**. 2005. 115 f. Monografia de Pós Graduação – Universidade Federal de Lavras, Lavras – MG. Disponível em: <http://www.ginux.ufla.br/documentacao/monografias/mono-AriJunior.pdf>. Acesso em: 04 de abril de 2007.

PASSITO, Alexandre et. al. **Análise de desempenho de tráfego VOIP utilizando o Protocolo IP Security.** Laboratório de Voz sobre IP. Universidade Federal do Amazonas. Manaus – AM.

QUEIROZ, Daniel Cruz **Voz Sobre IP em Redes Corporativas.** 2002. 63 f. Trabalho de Conclusão de Curso – Universidade de Fortaleza, Fortaleza – CE.

SANTOS, Eduardo. **Segurança:** Chaves assimétricas e a assinatura digital. Disponível em: <http://www.imasters.com.br/artigo/3624/seguranca/chaves_assimetricas_e_a_assinatura_digital/>. Acesso em: 29 de abril de 2007.

SILVA, Lino Sarlo. **Virtual Private Network**. Aprenda a construir redes privadas virtuais em plataformas Linux e Windows. Editora Novatec. 2002.

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

TRINTA, F.A.M.; MACÊDO, R.C. **Um Estudo sobre Criptografia e Assinatura Digital**. Pernambuco: DI/UFPE, 1998. Disponível em: <http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm>. Acessado em: 16 de maio de 2007.

VOLTAN JR, Guilherme **Voz sobre IP Segurança de Transmissões**. 2005. 104 f. Trabalho de Conclusão de Curso – Universidade Católica de Goiás, Goiás – GO. Disponível em: <http://www.apostilando.com/download.php?cod=2340&categoria=Outras%20Apostilas >. Acesso em: 31 de março de 2007.

6. APÊNDICES

6.1 Mini-Tutorial – Instalação e Configuração do Asterisk 1.4

Apresenta-se passo a passo para instalar e configurar o Asterisk, deixando-o pronto para a configuração do plano de discagem, abrangendo desde a preparação do Linux Ubuntu até o teste de funcionamento.

Para baixar e compilar todos os pacotes utilizados para o funcionamento do Asterisk, utilizando o sistema operacional Ubuntu, no modo terminal execute os comandos a seguir:

 # cd /usr/src
 # mkdir asterisk
 # cd asterisk
 # wget http://ftp.digium.com/pub/libpri/releases/libpri-1.4.0.tar.gz
 # tar -xvzf libpri-1.4.0.tar.gz
 # cd libpri-1.4.0
 # make
 # make install
 # cd ..
 # wget http://ftp.digium.com/pub/zaptel/releases/zaptel-1.4.0.tar.gz
 # tar -xvzf zaptel-1.4.0.tar.gz
 # cd zaptel-1.4.0
 # ./configure
 # make
 # make install
 # cd ..
 # wget http://ftp.digium.com/pub/asterisk/releases/asterisk-1.4.1.tar.gz
 # tar -xvzf asterisk-1.4.1.tar.gz
 # cd asterisk-1.4.1
 # ./configure
 # make
 # make install

 # make samples
 # cd ..
 # wget http://ftp.digium.com/pub/asterisk/releases/asterisk-addons-1.4.0.tar.gz
 # tar -xvzf asterisk-addons-1.4.0.tar.gz
 # cd asterisk-addons-1.4.0
 # ./configure
 # make
 # make install
 # make samples
 # cd ..
 # wget http://ftp.digium.com/pub/asterisk/releases/asterisk-sounds-1.2.1.tar.gz
 # tar -xvzf asterisk-sounds-1.2.1.tar.gz
 # cd asterisk-sounds-1.2.1
 # make
 # make install

Para testar se o Asterisk está funcionando digite os comandos:

 # /etc/init.d/asterisk start
 # asterisk -r

Se você estiver acessando o console de comandos do Asterisk, então a instalação deu certo.

Agora já se pode realizar a configuração, os arquivos básicos de configuração que precisam ser alterados para o funcionamento são: sip.conf e extensions.conf

Configurando o sip.conf:

#/etc/cd asterisk
#vi sip.conf

Agora no modo de edição de texto é necessário estar digitando as linhas a seguir, este é um exemplo de cadastro SIP utilizado no estudo de caso:

[8011]
callerid=Amanda
username=8011
secret=123456
host=dynamic
type=friend
context=interno

Configurando o extensions.conf:

#/etc/cd asterisk
#vi extensions.conf

Também no modo de edição de texto é necessário estar digitando as linhas a seguir, este é um exemplo de como criar uma extensão, também utilizado no estudo de caso:

[interno]

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

exten => _8XXX,2,Hangup()

Pronto o servidor de telefonia VOIP Asterisk está configurado, agora é só configurar no softphone escolhido os ramais, nome e senha, e já pode realizar as chamadas.

6.2 Mini-Tutorial – Instalação e Configuração do OpenVpn 2.0.9

Apresenta-se passo a passo para instalar e configurar o OpenVPN, deixando-o pronto para uma conexão segura entre cliente e servidor.

Para baixar e compilar todos os pacotes utilizados para a conexão do túnel VPN, utilizando o sistema operacional Ubuntu, execute os comandos a seguir no modo terminal:

Primeiro baixe os pacotes de biblioteca de compressão de dados (Lzo-1.08.tar.gz) <http://www.oberhumer.com/opensource/lzo/download/LZO-v1/lzo-1.08.tar.gz>

#tar zxvf lzo-1.08.tar.gz
#cd lzo-1.08
#./configure
#make
#make install

Depois baixe os pacotes de instalação da VPN (openvpn-2.0.9.tar.gz) <http://openvpn.net/release/openvpn-2.0.9.tar.gz>

#tar zxvf openvpn-2.0.9.tar.gz
#cd openvpn-2.0.9
#./configure
#make
#make install

Pronto. O OpenVPN já está instalado no sistema com suporte à biblioteca de compressão de dados. Agora só resta a configuração desta VPN.

O OpenVPN pode operar com 3 tipos de criptografia. Nenhuma criptografia (apenas o túnel), criptografia com chaves estáticas e no modo TLS, em que as chaves são trocadas periodicamente. Neste exemplo, é usada criptografia com chaves estáticas.

Para configurar a máquina onde será o Servidor, utilizando o sistema operacional Linux Ubuntu, no modo terminal digite os seguintes comandos:

 # mkdir /etc/openvpn
Cria o diretório onde estarão todos os arquivos de configuração.

 # openvpn --genkey -secret /etc/openvpn/static
Foi gerada uma chave de criptografia com o nome de static (pode ser qualquer nome de arquivo) dentro do diretório /etc/openvpn.

 # cat /etc/openvpn/static
Só para visualizarmos o conteúdo da chave que geramos.

 # cd etc/openvpn/server.conf
Crie esse arquivo com o seguinte conteúdo:

dev tun *// Usa como interface o driver TUN*
ifconfig 10.8.0.1 10.8.0.2 *//10.8.0.1 ip que será assumido no servidor e 10.8.0.2 ip remoto, ou seja, esse será o ip do cliente.*
secret static.key *// Indica que esse túnel possui uma chave de criptografia.*

Em seguida, inicia-se a conexão no servidor, faltando apenas configurar o cliente. Execute o seguinte comando na maquina do servidor:

 # cd etc/openvpn
#openvpn server.conf

Pronto agora o túnel só espera a conexão do cliente para estabelecer a VPN. Então na máquina do cliente, instale também todos os pacotes OpenVPN como foi feito na máquina do servidor, e após faça as seguintes configurações:

 # mkdir /etc/openvpn
Copie a chave gerada no servidor para o cliente com seguinte comando:
 # scp /etc/openvpn/static ip_client:/etc/openvpn
 # cd etc/openvpn/client.conf
Crie esse arquivo com o seguinte conteúdo:

remote 10.1.1.2 *// ip da máquina do servidor*
dev tun *// Usa como interface o driver TUN*
Ifconfig 10.8.0.2 10.8.0.1 *// ip do cliente e do servidor no túnel VPN*
secret static.key *// Indica que esse túnel possui uma chave de criptografia, a mesma do servidor.*

Agora é só conectar no túnel:

 # cd etc/openvpn
#openvpn client.conf

Pronto, agora é só testar, pingando de uma ponta a outra. Se der tudo certo, a VPN já está funcionando.