FUNDAÇÃO DE ENSINO "EURÍPIDES SOARES DA ROCHA"
CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA – UNIVEM
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

LEONARDO BOUVIER GIRARDI

IMPLEMENTAÇÃO E AVALIAÇÃO DE UMA ESTRUTURA DE REDE DE VOZ SOBRE O PROTOCOLO IP

Segurança e Mobilidade

MARÍLIA
2014

LEONARDO BOUVIER GIRARDI

IMPLEMENTAÇÃO E AVALIAÇÃO DE UMA ESTRUTURA DE REDE DE VOZ SOBRE O PROTOCOLO IP

Segurança e Mobilidade

Trabalho de Curso apresentado ao Curso de Bacharelado em Sistemas de Informação da Fundação de Ensino "Eurípides Soares da Rocha", mantenedora do Centro Universitário Eurípides de Marília – UNIVEM, como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Orientadora
Profª: Me. Giulianna Marega Marques

MARÍLIA
2014

BOUVIER GIRARDI, Leonardo

Implementação e Avaliação de uma Estrutura de Rede de Voz Sobre o Protocolo IP – Segurança e Mobilidade / Leonardo Bouvier Girardi; orientadora: Profª. Me. Giulianna Marega Marques. Marília, SP: [s.n.], 2014.

81 folhas

Monografia (Bacharelado em Sistemas de Informação): Centro Universitário Eurípides de Marília.

CENTRO UNIVERSITÁRIO EURÍPIDES DE MARÍLIA
BACHARELADO EM SISTEMAS DE INFORMAÇÂO

TRABALHO DE CONCLUSÃO DE CURSO – AVALIAÇÃO FINAL

Leonardo Bouvier Girardi

IMPLEMENTAÇÃO E AVALIAÇÃO DE UMA ESTRUTURA DE REDE DE VOZ SOBRE O PROTOCOLO IP - SEGURANÇA E MOBILIDADE

Banca examinadora da monografia apresentada ao Curso de Bacharelado em Sistemas de Informação do UNIVEM/F.E.E.S.R., para obtenção do Título de Bacharel em Sistemas de Informação.

Nota: 90 (Nove)

Orientador: Giulianna Marega Marques

1°. Examinador: Ildeberto de Gênova Bugatti

2°. Examinador: Emerson Alberto Marconato

Marília, 03 de dezembro de 2014.

Dedico este trabalho à minha mãe Janice, meu irmão Edinho e a minha cunhada Carol por estarem presente desde o início, apoiando para que pudesse chegar ao fim de mais essa jornada e aos amigos que estiveram desde o início juntos nessa fase de estudos e de dedicação.

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus por ter me guiado nessa trajetória, por iluminar meu caminho e por ter me dado saúde, força e compreensão para superar as dificuldades.

A minha família que diante das dificuldades que apareceram nessa época de estudos e formação, que me apoiaram de forma incondicional para que não me deixassem desviar do foco do termino dessa etapa.

Aos amigos que conheci durante a graduação e que seguiram do início ao fim, ajudando com apoio, companheirismo nos momentos em que estivemos juntos. Levarei para sempre as amizades feitas durante essa jornada.

Ao Luiz Antônio Orlando por ter me dado a oportunidade de continuar essa fase de estudos, obrigado por tudo.

GIU! O meu sincero agradecimento a você. Minha querida orientadora, Giulianna Marega Marques, que desde o primeiro ano da graduação esteve presente me auxiliando não só de forma acadêmica mas também profissional. Obrigado “Mãe Giu”, pela dedicação e PACIÊNCIA nos momentos de pânico nessa reta final e em aceitar em orientar este trabalho, cuidando da melhor forma possível para que fosse concretizado.

Aos amigos de trabalho Rogério e Samuel, que ajudaram no desenvolvimento deste projeto. Pela paciência e por ajudar nos momentos de dúvidas que surgiram e que não foram poucos. Obrigado!

A todos que participaram de forma direta ou indireta da minha formação, obrigado.

“Não confunda derrotas com fracasso nem vitórias com sucesso. Na vida de um campeão sempre haverá algumas derrotas, assim como na vida de um perdedor sempre haverá vitórias. A diferença é que, enquanto os campeões crescem nas derrotas, os perdedores se acomodam nas vitórias. ”

Roberto Shinyashiki

RESUMO

A globalização das comunicações teve seu maior avanço com o advento da Internet, que permitiu trocas de informações de maneira mais rápida e dinâmica. Novas tecnologias surgiram e a relação custo/benefício das comunicações foi melhorando. Um dos frutos desta evolução foi permitir que a voz trafegasse sobre o protocolo IP. Com o intuito de contribuir para a redução de custo de telefonia, proporcionar mobilidade e melhor comunicação de empresas e instituições de ensino, tem-se como objetivo a implementação e avaliação de uma estrutura de rede de voz sobre o protocolo IP. Serão avaliados os quesitos de segurança, mobilidade, qualidade e custo, apresentando as tecnologias de hardware e redes envolvidas. Este projeto será implementado para que haja a expansão da rede local para uma rede móvel, privando a segurança e a qualidade da comunicação entre esses novos dispositivos.

Palavras-Chave: Voz sobre IP, Segurança, Mobilidade

ABSTRACT

The globalization of communications had its major advance with the advent of the Internet, allowing exchange of information faster and more dynamic. New technologies have emerged and the cost / benefit of communications were improving. One of the results of this development was to allow the voice to travel on IP protocol. In order to contribute to the reduction of telephony costs, providing better mobility and communication of companies and educational institutions, it has as objective the implementation and evaluation of a voice network structure over the IP protocol. It will be evaluate the safety questions, mobility, quality and cost of the hardware technologies and networks involved. This project will be implemented so that there is the expansion of the local network to a mobile network, depriving the safety and quality of communication between these new devices.

Keywords: Voice over IP, Security, Mobility

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ACK	Acknowledgement
ADSL	Asymmetric Digital Subscriber Line
AP	Access Point
ATA	Adaptador para Telefone Analogico
CODEC	Codificador/Decoficador
DDD	Discagem Direta à Distancia
DDI	Discagem Direta Internacional
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
GSM	Global System for Mobile
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control
MAN	Metropolitan Area Network
MITM	Man-In-The-Middle
MOS	Mean Opinion Score
NAT	Network Address Translation
NMAP	Network Mapper
OSI	Open Systems Interconnection
PABX	Private Automatic Branch Exchange

PAN	Personal Area Network
QoS	Quality of Service
RPTC/PSTN	Public switched telephone network
RTP	Real-time Protocol
RTCP	Real-Time Transport Control Protocol
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SSID	Service Set Identification
TCP	Transmission Control Protocol
TTL	Time to Live
UDP	User Datagram Protocol
VoIP	Voice of Internet Protocol
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WIFI	Wirelles Fidelity
WPA	Wi-Fi Protected Access

SUMÁRIO

INTRODUÇÃO

Em meados de 1995 iniciou-se um novo conceito para a área de telefonia com o surgimento da voz sobre o protocolo IP: do inglês, *Voice over Internet Protocol* (VoIP). Durante os anos vem avançando gradualmente e se tornando uma tecnologia forte e difundida no mercado. Embora ainda se tenha alguns problemas com confiabilidade, segurança e interoperabilidade com essa tecnologia, sua taxa de adesão e seu grande potencial fizeram do VoIP uma das grandes novidades para o atual cenário tecnológico.

Uma alternativa de baixo custo para telefonia fixa é o VoIP, que tem a função de codificar a voz em sinais de áudio analógico, comumente usados pelas operadoras de telefonia em dados digitais que são transmitidos por meio da Internet ou qualquer rede baseada no protocolo IP (Protocolo de Internet).

O VoIP permite que um aparelho com essa tecnologia, conectado à mesma rede de comunicação, possa fazer ligações a custo local, independentemente de sua localização e horário, parâmetros estes usados por companhias de telefonia para calcular o custo do uso de seus serviços, variando de umas para as outras.

Somente após o grande desenvolvimento de novas tecnologias e investimentos pesados é que a rede de Internet conseguiu ter seu amadurecimento. Com isso, novos protocolos de comunicação possibilitaram que as aplicações de voz deixassem de ser uma curiosidade de baixa qualidade para se transformar em uma grande oportunidade de novos negócios.

Se por um lado a nova tecnologia possibilita o nascimento de novas empresas no ramo emergente de telefonia, onde a tarifação para ligações está se mostrando mais barata do que as empresas convencionais, por outro lado, isso vem ameaçando empresas tradicionais, algumas influentes no mercado, que até hoje vendem o serviço telefônico que é cobrado a partir do cálculo dos fatores tempo de uso e distância percorrida.

As vantagens de se utilizar o VoIP como plataforma de telefonia em ambientes onde a demanda de telefonia é grande manifestam-se de diversas maneiras. Muitas delas por meio da transmissão de voz e dados sobre uma mesma infraestrutura de rede e de distribuição de forma inteligente, utilizando um sistema em que se há controle das diversas formas de como serão utilizados os aparelhos, obtendo-se um extenso controle do que está ocorrendo dentro

dessa rede em vez de concentrá-la em custosas centrais telefônicas. O resultado que se tem não é só uma grande redução de custos, mas também há a possibilidade de se utilizar serviços inovadores e de grande conveniência para os usuários.

Com a introdução da tecnologia VoIP, o usuário pode ter a flexibilidade de estruturar sua rede da forma como ele desejar. Sempre que conectar o dispositivo VoIP em uma rede banda larga, em qualquer lugar do mundo, poderá receber chamadas de forma "local" sem pagar interurbanos nacionais ou internacionais. Além disso, há a possibilidade de se gerenciar contas online, ouvir as mensagens da secretária eletrônica, programar a aceitação e desvios de chamada.

O desenvolvimento da tecnologia VoIP está ocorrendo em várias frentes. Muitos avanços já foram incorporados pelas empresas tradicionais de telefonia, principalmente na interligação entre centrais, mas muito pouco disso é sentido pelo cliente final. Há aquelas empresas que, mirando no mercado corporativo, desenvolvem soluções para aplicações específicas e que se valem das redes corporativas de seus clientes para conectar não só os computadores, mas, principalmente, os telefones, em qualquer lugar do mundo, e que falam entre si sem pagar um centavo.

Em resumo, quando falamos em VoIP falamos sobre comunicação de Voz sobre redes IP. Podemos classificar essas redes de duas formas mais utilizadas em ambientes corporativos e/ou por usuários convencionais. Podemos dizer que são os tipos P*úblicas* e P*rivadas.* Nas redes públicas a Internet representa a rede IP usada para comunicações VoIP. O usuário deve ter preferencialmente um acesso por banda larga (ADSL, cabo, rádio, Wimax, etc.) instalado para poder fazer uso do serviço VoIP.

Quando o usuário estiver conectado a qualquer tipo de rede de Internet, seu serviço precisa estar configurado de forma correta e autorizado a realizar uma autenticação para utilizar o item em questão. No caso da utilização dos serviços de telefonia, o usuário precisa estar cadastrado a um tipo de serviço e possuir um aparelho ou computador com o serviço VoIP habilitado.

As redes corporativas das empresas representam as redes privadas utilizadas para comunicações VoIP. Podem ser desde pequenas redes locais (LAN) até grandes redes corporativas (WAN) de empresas com presença global. Empresas com estruturas de grande porte, que possuem diversas sedes em diferentes localidades dentro de uma mesma cidade ou

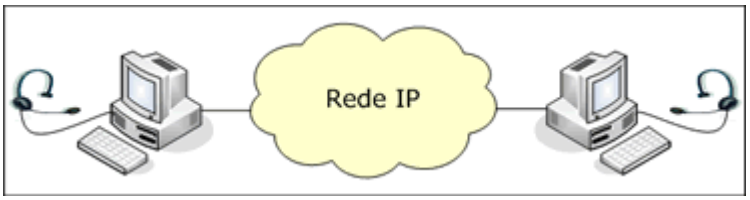
até mesmo em cidades, estados ou países diferentes, podem utilizar esses tipos de serviços tendo como custo de ligações “zero” e entre os telefones ou clientes configurados dentro da mesma rede e serviço, com a interligação de suas redes IP.

O uso mais simples de VoIP é a comunicação computador a computador utilizando a Internet, sendo o Skype o programa mais utilizado para este fim. Ele permite a realização de ligações a custo zero entre esses dois dispositivos e também podem ser realizadas vídeo-chamadas entre dois ou mais participantes, dentro de uma mesma conversa.

O serviço do Skype também permite a realização de chamadas para telefones comuns, como em uma residência, telefone móvel e até interurbanos que não estejam dentro da mesma rede. Para isso ser possível, é necessária a compra de “créditos” da operadora em questão que fornece o serviço de VoIP, no caso do exemplo acima citado, o Skype.

A figura 1 mostra, de forma bem simples, como é a abordagem dessa estrutura de telefonia local (LAN) em que é possível realizar ligações a custo zero dentro da mesma estrutura de rede e utilizando computadores.

Figura 1. Estrutura com a Utilização do VoIP



Fonte: TELECO

Motivação e Justificativa

A motivação para a construção deste trabalho deu-se com o intuito de acompanhar o desenvolvimento e a globalização das comunicações. Ainda utiliza-se infraestruturas de telecomunicações engessadas e de custo muito elevado. Com a implementação da estrutura de rede telefônica proposta neste trabalho, será possível expandir facilmente a rede de telefones, executar integrações de telecomunicação com gestão e também obter uma redução de custos com as operadoras de telefonia fixa e móvel. Outra questão desafiadora é prover mobilidade, garantindo a segurança das informações.

Objetivos Gerais

O objetivo pretendido é a proposição da expansão da rede local VoIP para uso com mobilidade e realizar testes de comunicação de segurança dessa rede que ficará disponível. Além disso, testar formas de segurança, bloqueios para evitar acessos indevidos de usuários vindos de outras redes sem autorização, avaliar o estado atual da rede e montar um mapeamento do que há na rede de telefones atuais. Após a implementação, comparar o custo de uso da rede VoIP com a atual linha de aparelhos móveis (celulares) que a empresa possui e também avaliar o desempenho das duas plataformas, demonstrando vantagens e desvantagens em relação à sua utilização.

Têm-se como objetivos específicos a realização de testes com chamadas por meio de telefones móveis (SOFTFONES). Os telefones móveis responderão a um serviço hospedado em um servidor local, onde estará configurado o gerenciador do VoIP.

O gerenciamento será realizado pela plataforma ASTERISK, configurado sobre um sistema operacional Linux.

Para a realização das chamadas, será também verificada a segurança dessa rede, com testes de tentativas de acesso a essa rede. Será verificado o desempenho durante as chamadas com relação a implementação de um *Firewall* para a segurança desse serviço, além de realizar uma forma de autenticação para a liberação somente dos equipamentos, evitando acessos indevidos à rede;

Organização do Trabalho

O trabalho foi organizado de forma a seguir o entendimento desde o surgimento das redes de telefonia por meio do funcionamento da rede de computadores. Após uma explicação de tal assunto, será abordado de forma sucinta um dos serviços mais utilizados para esse meio chamado de Asterisk, que tem por principal função a gerencia dessas ligações.

Para saber a forma funciona uma rede de computadores, o capítulo 2 trata de sua estrutura como um todo, e aborda os principais protocolos utilizados para uma rede de comunicação VoIP e de que são trabalhados esses protocolos para que haja o funcionamento desse serviço.

O foco deste trabalho tem por objetivo trabalhar com telefones móveis (SOFTFONES)

conectados a redes sem fio, a uma conexão a um roteador, como o caso deste trabalho. O capitulo 3, apresenta as principais características de uma rede sem fio de computadores, os diferentes tipos de padrões existentes para a comunicação e também as formas de seguranças que são implementadas nesse ambiente. É abordado os 2 principais tipos de segurança em torno de criptografia de dados.

Após essa revisão sobre a estrutura das redes, desde protocolos, pilha TCP/IP e suas camadas, o capítulo seguinte mostrara as ferramentas que serão utilizadas para elaboração do cenário dos testes. Esse capítulo falará de técnicas de invasão, monitoramento de portas de serviços e falhas em servidores. Será utilizado também ferramentas para o monitoramento por meio físico e lógico de desempenho dos equipamentos que serão utilizados durante os testes.

O capitulo 5, tratara da coleta dos dados, mostrando como fica o desempenho desses serviços sem a utilização de uma segurança e com utilização e por fim será mostrada a conclusão realizada no desenvolvimento deste projeto.

1 VOZ SOBRE O PROTOCOLO IP

Nos dias de hoje, presencia-se uma grande mudança ocorrendo nas telecomunicações, resultado do incrível crescimento das redes baseadas em pacotes, especialmente pela Internet. Esta revolução está unificando os mundos de Dados e Telecomunicações em uma só rede convergente.

A crescente e maciça utilização da Internet instigou o surgimento de novas tecnologias, muitas vezes, substituindo algumas já existentes, como no caso do VoIP. A sigla VoIP tem origem em “Voz sobre IP”, ou seja, é uma tecnologia que permite que chamadas telefônicas sejam feitas por meio de uma conexão de banda larga, no lugar dos serviços de telefonia convencionais.

O VoIP surge como um tema que abrange duas grandes áreas em crescimento: a *Internet* e a T*elefonia*, com uma certa abrangência sobre o segundo item. O VoIP basicamente significa o transporte sobre uma infraestrutura IP. Existem duas variações dessas infraestruturas: LAN - *Local Area Network* (rede local dentro de um determinado ambiente) ou WAN – *Wide Area Network (*rede de longo alcance). A ideia de se utilizar essa tecnologia é ter um tronco PABX ligado a um *gateway* (roteador ou *switch)* que faça a conversão tradicional do sinal analógico da voz para o sinal digital, que será transmitido como dado de uma rede comum de *Internet.* A implementação de VoIP permite o tráfego de voz, como, por exemplo, as chamadas telefônicas e as videoconferências sobre uma rede IP.

A proposta de convergência tornou-se tão interessante e importante para a manutenção da competitividade que mesmo as operadoras telefônicas, que fornecem as tecnologias tradicionais, estão se rendendo a essa nova forma de tecnologia, além de desenvolver soluções para racionalizar o uso de suas infraestruturas baseadas em circuitos, fazendo a atualização para comutação de pacotes.

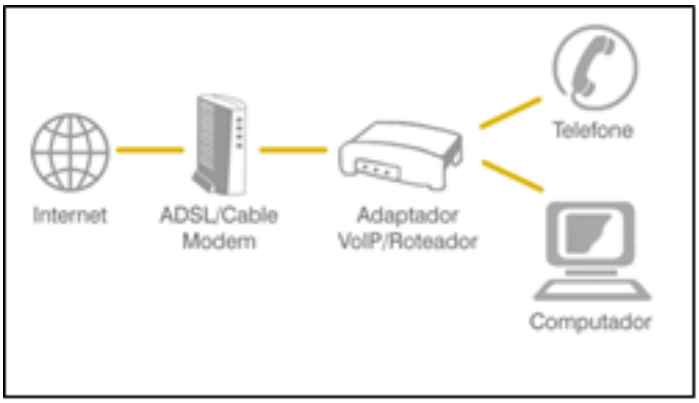
O VoIP é um protocolo de redes de computadores, isto é, ele trata de normas e regras implementadas em um determinado cenário para que a voz saia de uma origem, seja dividida em pacotes, trafegue por redes de dados por meio do TCP/IP e chegue ao destino. Os pacotes são reunidos e reorganizados, reconstruindo, assim, a voz, para que esta seja reproduzida para o destino.

Com o crescimento do tráfego de informações e da utilização das redes de Internet,

além do aumento da demanda por velocidades maiores e de se ter de acesso à Internet banda larga a qualquer momento e lugar, o VoIP passou a fazer parte do dia a dia das grandes corporações, tendo como objetivo inicial e principal reduzir o valor das contas telefônicas.

A utilização de uma linha telefônica por meio de uma rede de computadores é representada na Figura 2.

Figura 2. Estrutura de uma rede VoIP com conexão a Internet



Fonte: Autor Desconhecido

A imagem mostra de forma resumida, o funcionamento de uma rede de telefones por *Internet*, onde se tem uma conexão comum com saída para a *Internet*, podendo conectar um dispositivo capaz de transformar o sinal tradicional de telefonia para pacotes de dados que trafeguem em redes de computadores, no caso um ATA (Adaptador para Telefone Analógico).

Um dos principais benefícios do VoIP são suas diversas funcionalidades, como conferência, reconhecimento de chamadas gratuito, gravação e redirecionamento de ligações. A infraestrutura deve ser muito bem organizada para garantir uma conexão de qualidade e para que nenhum serviço deixe a desejar durante seu uso, já que a rede voz depende da rede de dados.

A facilidade de gestão e autonomia sobre o cenário telefônico dentro da empresa é considerada mais uma das vantagens de se implementar uma infraestrutura VoIP. Com pouca burocracia e baixo custo (podendo chegando a ser zero em relação a utilização de chamadas), é possível ter um administrador, criar ramais e efetuar configurações de chamada e de usuários; tarefas que normalmente são executadas por especialistas em telecomunicações,

com custos elevados de licença e de serviços.

A seguir são citadas as principais características e benefícios da utilização de uma estrutura de telefonia VoIP: Funcionalidade; Redução de Custos; Infraestrutura; Mobilidade; Controle da Telefonia e Codificação de Voz;

Funcionalidades: Telefones IP ou ATAs (Adaptador para Telefones Analógicos), possui funções diferentes que as vezes não conseguem ser tratadas diretamente em linhas convencionais. No caso de uma rede de telefones, com esses equipamentos na ponta e devidamente configurados, é possível que durante uma chamada, até 3 participantes possam se comunicar sem nenhum problema (KELLER, 2011). Outra possibilidade é o reconhecimento de telefones ao receber uma chamada, que geralmente são cobradas pelas empresas de telefonia como um serviço adicional, mas na configuração da rede de telefonia, é possível habilitar essas opções de forma rápida e sem custos.

Reduzir Custos: A redução de custos nem sempre é aparente logo no início do uso de soluções VoIP. Segundo (KELLER, 2011), o tempo de retorno em relação ao investimento feito em uma estrutura de VoIP é diretamente ligado aos custos envolvendo a telefonia atual em que se apresenta no cenário da empresa em questão. Se a empresa em um cenário tem apenas uma pequena parte de seu uso para DDD/DDI, cerca de 20% e seu restante é apenas chamadas entre ramais, sem custos. Como seu custo com ligações externas é bem menor do que o com chamadas internas, a utilização de VoIP terá um retorno de investimento demorado, em relação à uma empresa que tem seu custo maior com ligações DDD/DDI. Se inverter o cenário, o retorno será mais rápido.

Infraestrutura: A unificação da rede de dados e voz, atingirá a nossa rede física (LAN), fazendo com que ela fique responsável por conduzir dois serviços em uma única rede. Por isso sua estruturação deve ser bem organizada e ter como conjunto uma conexão de qualidade para que nenhum serviço deixe de ser usado de forma agradável durante seu desempenho (MORIMOTO, 2008).

Mobilidade: Ter flexibilidade para pode trabalhar dentro de sua rede, é uma das vantagens de se usar redes sem fio. Dentro de uma rede cabeada, se caso haja a necessidade de se fazer uma mudança física de uma sala ou de um equipamento, pode gerar um grande transtorno dentro da disposição física do cabeamento e isso pode até gerar custos (OLIVEIRA, 2012).

Dentro de uma rede onde se pode conectar um notebook ou até mesmo um telefone IP Wi-Fi e usar a mesma rede cabeada, mas através de um roteador sem fio: mobilidade. De acordo com (KELLER, 2011), existem equipamentos com a possibilidade de ter um chip padrão GSM e também configurar uma rede VoIP, conectado dentro de seu provedor VoIP pela rede de dados da companhia de celular, utilizando por exemplo 3G. Isso permite que ocorra chamadas tanto pelo número tradicional de seu celular e até mesmo o VoIP, sem a necessidade de se ter dois aparelhos, um para cada cenário.

Controle da Telefonia: Ter livre controle sobre o cenário telefônico dentro da empresa: é uma das vantagens de se implementar uma infraestrutura VoIP, sendo mais correto dizer, um servidor Asterisk que controle o gerenciamento dessa rede.

É possível tornar-se o administrador, sem preocupação para criar, ramais configurações de chamada, entre outras tarefas, em que as vezes ficamos dependentes de Companhias Telefônicas. E por se tratar de uma plataforma de código aberto, possui uma farta documentação de fácil acesso e tem-se relativamente um nível mais simples de se administrar em caso de manutenções.

Codificação de Voz: De acordo com (KELLER, 2011), a digitalização ou a conversão da voz do som analógico tradicional, para sinais digitais é realizado pelos codificadores-decoficadores chamados Codecs (enCOde/DECode). Este tipo de componente é muito importante dentro da rede de telefonia VoIP, pois é ele que fica responsável por transformar a voz humana (sinal analógico) em uma sequência de *bits* (sinal digital) para que essa voz seja transmitida numa rede de dados convencional.

Existe uma variedade de CODECs e cada um provê uma certa qualidade de voz. Mas a qualidade da voz, pode ser boa ou ruim de acordo com o ouvinte em questão. Mas existe um método para que se possa medir a qualidade do som produzido por CODECs de voz durante uma chamada.

Essa medida é chamada de MOS (*Mean Opinion Score* – Pontuação Média de Opinião). Com o MOS, uma quantidade de ouvintes, podem testar e julgar a qualidade de um CODEC, numa escala de notas que vai de 1 a 5. De acordo com o site (ABREU E SOUZA; PEREIRA BUENO, 2006), a partir desses resultados é calculada a média dos *scores* para atribuir o MOS para aquela amostra.

Um dos componentes mais importantes para garantir qualidade de uma chama telefônica em uma rede IP é o Codec. Na seção 1.1 são apresentados mais detalhes.

1.1 Qualidade do Áudio em VoIP

Para que se tenha um bom funcionamento do VoIP, isto é, realizar uma chamada com um excelente nível de áudio, diversos fatores críticos que estão ligados uns aos outros interferem neste processo, como a qualidade dos CODECs e sua função de digitalizar o áudio recebido e dividir em pacotes para que se possa realizar sua transmissão de um ponto a outro, o conjunto de uma boa estrutura também influencia em um bom desempenho. Mas há alguns outros fatores que também devem ser levados em conta na hora de se medir a qualidade de uma chamada:

Latência (*Latency*): É o tempo que um pacote leva para sair de sua origem e chegar ao destino, dentro da mesma rede. Falando em telefonia, seria o tempo de uma saída de voz do transmissor até o receptor da mensagem. A latência coloca um *delay* à comunicação, sendo assim, é o tempo que o equipamento de roteamento da rede leva para poder processar o pacote de dados antes de encaminhá-lo ao seu destino. De acordo com (ABREU E SOUZA; PEREIRA BUENO, 2006) a latência dentro da rede de possuir um valor abaixo de 150ms para que se tenha uma boa qualidade da chamada. Já (KELLER, 2011), diz que dentro de cada passagem por roteadores, são adicionados em média 10ms de atraso nos pacotes, na transmissão de uma origem até seu destino, o atraso não pode passar de 250ms. Acima dessa medida de tempo, o usuário, poderá ter problemas com atrasos de áudio e sobreposição de áudio.

Delay: É o tempo que se leva para a emissão do som na sua origem chegar ao destino. Quanto maior o *delay,* maiores serão as chances de se ter uma chamada prejudicada, com atraso no áudio.

Perda de Pacotes (*Packet Loss*): A perda de pacotes é um outro grande fator que tem ligação direta com o serviço de telefonia. Dentro das possibilidades de perca de pacotes que ocorre dentro de uma rede, segundo (KELLER, 2011), um desses motivos deve-se aos roteadores que encaminham os pacotes dentro da rede, e o limite de perca de pacotes não deve ultrapassar 5% para que não possa prejudicar a chamada. Pacotes que são transmitidos via protocolos UDP (*User Datagram Protocol)* e RTP (*Real-Time Protocol),* não

podem ser retransmitidos, mesmo que se fosse possível, segundo (ABREU E SOUZA; PEREIRA BUENO, 2006), não seria aconselhável já que duas mensagens enviadas em sequência poderiam ter suas ordens trocadas, o que não é aceitável dentro de uma aplicação executada em tempo real.

Jitter: O *jitter* está relacionado com variação da latência. É uma variação do atraso na entrega de dados dentro da rede, pode ser definida como a medida da variação dos pacotes. Segundo (ABREU E SOUZA; PEREIRA BUENO, 2006), cada pacote pode percorrer uma rota diferente e também em diferentes meios, por isso, o tempo de chagada pode variar de acordo com a rota seguida. Quanto maior o número de *jitter* dentro da rede, a qualidade do áudio pode ser distorcida e em casos mais extremos a chamada pode ser cancelada.

Supressão de Silêncio: É uma forma de aplicação para se detectar a ausência de áudio durante uma chamada, tornando assim, o consumo da banda mais eficaz e inteligente, evitando assim o envio de pacotes com o tal "silêncio".

Eco: Ocorre devido a própria realimentação acústica do receptor de uma transmissão. De acordo com (KELLER, 2011), em toda comunicação há um retorno do áudio enviado, sempre ocorre eco, seja na telefonia convencional, seja VoIP. Existem fatores que aumentam o *delay* dentro da rede e reduz a velocidade de transmissão dos pacotes de retorno de áudio, e por isso nós ouvimos nossa própria voz. Alguns dos fatores que aumentam esse eco dentro da rede estão relacionados com: Codecs, *gateways*, roteadores, *switchs* e até VPNs.

QoS (*Quality of Service*): Tem por função, serviços de controle para priorizar fluxos de dados dentro da rede, tendo em vista, a garantia de um nível adequado de desempenho. Com esse tipo de tecnologia dentro da rede, pode-se dar prioridade nos dados de telefonia, para poder ter um desempenho melhor. No caso de redes externas, não é possível garantir o QoS, pois não se tem controle dos roteadores e *gateways* possam aceitar tais propriedades definidas (ALEN RIBEIRO, 2011).

MOS (*Mean Opinion Score*): Definido pelo *International Telecommunication Union* (ITU-T), é um padrão numérico que mede e reporta a qualidade da voz durante uma transmissão. De acordo com o ITU-T, esses níveis vão de 1 (ruim) a 5 (excelente). Essa pontuação pode ser medida de forma subjetiva, onde pode-se colocar um grupo de pessoas a um tipo de áudio durante uma chamada e eles irão atribuir um valor para tal. Se caso uma

chamada obtiver um nível de MOS abaixo de 3.5, a chamada é considerada inaceitável e precisa ser revisado para que possa haver uma melhora.

A digitalização ou a conversão da voz do som analógico tradicional para sinais digitais é realizado pelos codificadores-decoficadores chamados *codecs* (enCOde/DECode). Este tipo de componente é muito importante dentro da rede de telefonia VoIP, pois é ele que fica responsável por transformar a voz humana (sinal analógico) em uma sequência de *bits* (sinal digital) para que essa voz seja transmitida numa rede de dados convencional.

Existe uma variedade de *codecs* e cada um proporciona um nível de qualidade na conversão de voz. Existe um método para que se possa medir a qualidade do som produzido por codec de voz durante uma chamada, essa medida é chamada de MOS (*Mean Opinion Score* – Pontuação Média de Opinião). Com o MOS, uma quantidade de ouvintes, podem testar e julgar a qualidade de um codec, numa escala de notas que vai de 1 a 5. A partir desses resultados é calculada a média dos *scores* para atribuir o MOS para aquela amostra. A tabela 1 a seguir, mostra a escala utilizada para o cálculo de medida MOS:

Tabela 1. Medida do Codec por meio do MOS.

Score	Definição	Descrição
5	Excelente	Um sinal de voz perfeito gravado em um local silencioso
4	Bom	Qualidade de uma chamada telefônica de longa distância (PSTN)
3	Razoável	Requer algum esforço na escuta
2	Pobre	Fala de baixa qualidade e difícil de entender
1	Ruim	Fala não clara, quebrada

Fonte: (ABREU E SOUZA; PEREIRA BUENO, 2006)

Durante a realização de uma chamada utilizando o VoIP, há diversos recursos sendo executados simultaneamente, como a pilha de protocolos TCP/IP, que são responsáveis pela conexão e endereçamento das transmissões e também onde toda a rede de computadores está apoiada. Os protocolos de RTP/RTCP que junto ao TCP, são responsáveis por estabelecerem uma conexão em tempo real para a realização de chamadas de áudio e/ou videoconferências.

Esses são apenas alguns dos componentes utilizados quando se inicia a transmissão de informações, no caso de uma chamada VoIP, a voz é o principal recurso que será transmitido.

Para que se tenha um bom funcionamento do VoIP, isto é, realizar uma chamada com um bom nível de áudio, depende de diversos fatores críticos que estão ligados uns aos outros. Os codecs tem como principal função digitalizar o áudio recebido e dividir em pacotes para que se possa realizar sua transmissão de um ponto a outro. O conjunto de uma boa estrutura influencia em um bom desempenho, mas há alguns outros fatores que também que devem ser levados em conta na hora de se medir qualidade de uma chamada.

1.2 Principais Características dos Codecs

A quantidade de *bytes* que é passada a cada intervalo de amostra é conhecida como tamanho de amostra (kbps). Como é possível observar na Tabela 2, o codec G.729 opera em um intervalo (*delay*) de 10 ms, que corresponde a 10 *bytes (80 bits)* por amostra, a uma taxa de 8 kbps.

Tabela 2. Tabela de Codecs e suas Composições.

Método de Compressão	Bit Rate (kbit/s)	MOS Score	Delay (ms)
G.711 PCM	64	4.1	0.75
G.726 ADPCM	32	3.85	1
G.728 LD-CELP	16	3.61	3 to 5
G.729 CS-ACELP	8	3.92	10
G.729 x 2 encodings	8	3.27	10
G.729x 3 Encodings	8	2.68	10
G.729a CS-ACELP	8	3.7	10
G.723.1 MP-MLQ	6.3	3.9	30
G.723.1 ACELP	5.3	3.65	30

Fonte: (ABREU E SOUZA; PEREIRA BUENO, 2006)

O intervalo de amostra (ms) é a medida do intervalo em que o CODEC opera. A medida de intervalo do codec G.729, por exemplo, é calculada em 10 ms.

A taxa de bits (kbps) é quantidade de bits por segundo que precisa ser utilizada para a transmissão para que ocorra a entrega de um pacote de voz. O codec G.729 utiliza 8 bits a cada segundo.

O tamanho de *payload (bytes/ms)* para os pacotes que trafegam na rede pode influenciar de forma direta na largura de banda a ser utilizado e o *delay* da conversa, ou *lag*. O

payload é representado pela quantidade de bytes (ou *bits*) preenchida em um pacote de dados. Se caso o *payload* dentro da rede for alto, a quantidade de pacotes que irá trafegar dentro da rede será menor, junto com isso, será maior a quantidade de áudio necessária para se formar um pacote, necessitando assim uma largura maior de banda. No caso de um *payload* muito alto, a taxa de *delay* ou *lag* será grande, agravando o atraso da voz.

1.3 Telefonia IP

A telefonia IP utiliza a tecnologia VoIP, para poder fornecer os mesmos mecanismos utilizados em uma rede de telefonia comum, analógica. Segundo artigo escrito ao site (RIBEIRO, 2011), a telefonia IP tem como objetivo fornecer funcionalidades e qualidades iguais aos de telefonia tradicional como, transferir chamadas, implementação de ramais, chamadas em espera.

O grande fato é que a telefonia IP consegue realizar tais tarefas sem necessidade de se ter de centrais de telefones e ainda permite a junção com outros tipos de serviços de dados. Segundo o artigo (RIBEIRO, 2011), a telefonia IP pode ser vista como uma plataforma de integração que pode se tornar a próxima geração das redes de computadores.

Também realiza a digitalização e transporte da voz, pode realizar as mesmas funções de uma chamada comum como, transferir chamada de um telefone a outro, segurar uma chamada entre outras funções. A telefonia IP dispensa o uso de um PABX (*Private Automatic Branch eXchange)* para realizar sua conversão de sinal tradicional para digital. A voz quando transformada em sinal digital passa a ser transportada em forma de bits.

Uma vez que está digitalizada a voz passa a ser transmitida por pacotes de dados usando o protocolo IP, podendo ser transmitido para uma rede local ou até da Internet, que é passado, por exemplo, por um provedor de serviços de telefonia IP. Se a rede possuir uma boa estrutura, há garantias que o serviço será realizado de forma integra, sem atrasos em sua transmissão e comunicação. Tem como base, as mesmas regras aplicadas em uma rede baseada no protocolo TCP/IP.

1.4 Asterisk

O Asterisk é considerado uma central telefônica híbrida, por implementar tanto as funções de uma central telefônica tradicional quanto os protocolos VoIP, ou seja, o Asterisk gerencia o áudio trafegando em canais de comunicação digitais, analógicos e também em redes TCP/IP.

Criado originalmente em 1999 por Mark Spencer, o Asterisk se trata de um *software* que implementa um PABX (*Private Automatic Branch eXchange*) de telefonia. De acordo com (OLIVEIRA, 2012), o *Asterisk* é um *software* capaz de integrar redes VoIP com a rede de telefonia tradicional e sua utilização vem sendo amplamente usada nos mais diversos cenários. Devido ao seu código aberto, sua flexibilidade tem capacidade considerada ilimitada para o desenvolvimento de regras, podendo ser moldado para atender qualquer tipo de necessidade.

Há a possibilidade de comparar as funções do Asterisk com as de um tradutor; ambos realizam o intermédio do áudio, ou conversa, entre dois pontos, traduzindo de um idioma protocolo ou *codec* para outro, de forma transparente e simples.

Segundo o próprio desenvolvedor Mark Spencer (apud KELLER, 2011, p332) "O *Asterisk* é um PABX *Open Souce* e um conjunto de ferramentas para telefonia. É em certo sentido, um *middleware* entre a *Internet* e os canais de telefonia na base, e a *Internet* e as aplicações de telefonia no topo. No entanto, o *Asterisk* suporta mais interfaces de telefonia do que somente telefonia pela *Internet".*

O *Asterisk* é disponibilizado sob uma licença de *software* livre, lançado sob a GPL 2 (*General Public License* – Licença Pública Geral). Pode ter seu código utilizado, alterado e distribuído sem nenhum tipo de impedimento autoral. Existem distribuições do tipo *Unix-Like* que são compiladas exclusivamente para suportar o *Asterisk*. Entre as mais conhecidas atualmente estão o Astilinux e AsteriskNOW.

Com sua ideia inicial de desenvolvimento para Sistemas Operacionais *Linux*¸ atualmente o *Asterisk* pode ser implementado em distribuições como *FreeBSD e OpenBSD*, que são também distribuições de códigos abertos, mas também podem ser implementados em arquiteturas fechadas, como o *Mac OS X*. (KELLER, 2011).

Na estruturação da rede VoIP, busca-se mobilidade e segurança dentro de ambiente de testes. Neste trabalho, a mobilidade será provida por meio de equipamentos e tecnologias que suportam com eficiência o tráfego de dados gerado durante as chamadas telefônicas.

2 PROTOCOLOS DA CAMADA TCP/IP

O protocolo TCP/IP é um conjunto ou pilha de demais protocolos usados para estabelecer a conexão entre computadores conectados a uma rede. Seu nome e composição baseiam-se em dois protocolos principais: o protocolo TCP - *Transmission Control Protocol* (Protocolo de Controle de Transmissão) e IP - *Internet Protocol* (Protocolo de Internet). São dois protocolos diferentes, mas que trabalham de forma conjunta para que tudo possa funcionar de forma organizada. (MORIMOTO, 2008).

Seu objetivo quando desenvolvido foi de se criar conexões de comunicação com alta velocidade, dentro de uma rede de comutação por pacotes. Um de seus fundamentos é de que ele poderia ser capaz de identificar uma rota dentro da rede entre dois indivíduos (computadores, servidores) e também calcular rotas mais rápidas para se chegar ao destino desejado, no caso de alguma outra rota não estar funcionando. Tendo dois caminhos em seu conhecimento, o protocolo TCP/IP calcula a rota e distância para o destino e usa a mais curta, evitando atrasos e consumo de banda.

O conjunto de protocolos que compõem a pilha TCP/IP é representado por meio de camadas, baseado no modelo de referência OSI. Sua composição é constituída por cinco camadas lógicas para melhor entendimento de suas pilhas de protocolos e, dentro de cada camada, são utilizados diversos protocolos, cada um com uma função especifica. O modelo TCP/IP segue a seguinte ordem de divisão: (MORIMOTO, 2008).

> 5 – Aplicação: Onde funcionam os serviços em que ocorre a interação do usuário com a aplicação.
>
> 4 – Transporte: Camada responsável pela passagem eficiente das informações entre dois pontos: Origem e destino.
>
> 3 – Rede: Controla as operações de roteamento de pacotes entre origem e destino, passando por diversos pontos.
>
> 2 – Enlace: Trata as informações vindas da camada 1 (Física), corrigindo erros e analisando a recepção e transmissão dos pacotes.
>
> 1 – Física: Função exclusiva para a parte de *hardware* que compõe a estrutura das redes, desde cabos até roteadores e *switches.*

A figura 3, a imagem de uma tabela com a composição de protocolos presentes dentro das camadas do protocolo TCP/IP:

Figura 3. Representação das Camadas Presentes no TCP/IP.

Protocolos Internet (TCP/IP)	
Camada	Protocolo
5.Aplicação	HTTP, SMTP, FTP, SSH,Telnet, SIP, RDP, IRC,SNMP, NNTP, POP3, IMAP,BitTorrent, DNS, Ping ...
4.Transporte	TCP, UDP, RTP, SCTP,DCCP ...
3.Rede	IP (IPv4, IPv6) , ARP, RARP,ICMP, IPsec ...
2.Enlace	Ethernet, 802.11 WiFi, IEEE 802.1Q, 802.11g, HDLC,Token ring, FDDI,PPP,Switch ,Frame relay,
1.Fisica	Modem, RDIS, RS-232, EIA-422, RS-449, Bluetooth,USB, ...

Fonte Adaptada: Wikipédia

Nos tópicos seguintes, são descritos os principais protocolos utilizados dentro de uma estrutura de rede de telefones. A base da estrutura como explicado anteriormente vem da estrutura de protocolos de TCP/IP, separados por camadas, outros protocolos trabalham de forma simultânea garantindo que as conexões entre usuários possam ser realizadas sem algum tipo de interferência ou problemas.

2.1 Protocolo IP e Utilização de Mascaras de Rede

Uma rede é a interligação de um conjunto de dispositivos capazes de se comunicar. Nesta definição um dispositivo pode ser um host (ou um sistema final, como as vezes é chamado), tal como um grande computador, *desktop*, *laptop*, estação de trabalho, telefone celular ou sistema de segurança. Um dispositivo nessa definição também pode ser um dispositivo de conexão, tal como um roteador, que liga uma rede a outras redes, um switch (ou comutador) que liga dispositivos entre si (MORIMOTO, 2008).

Os endereços IP são sempre um tema importante, já que são eles que permitem que o número atual de redes e hosts que formam a *Internet* seja capaz de se comunicar entre si.

Atualmente, existem duas versões do protocolo IP (protocolo utilizado dentro da camada 3 do modelo TCP/IP): o **IPv4,** atual versão que utilizamos no cenário das redes de

computadores. Por outro lado, existe um novo protocolo: o **Ipv6**. É a nova versão que prevê um número muito maior de endereços do que o atual protocolo Ipv4 e que já está sendo atualizado para sua nova versão. Durante os próximos anos poderá ser utilizado quase que exclusivamente dentro da rede mundial de computadores *(Internet) (MORIMOTO. 2008).*

No Ipv4, os endereços IP são estruturados por 4 blocos de 8 bits, totalizando 32 bits, que são representados por números entre 0 a 255 (permitindo a combinação total de 256 possibilidades permitidas por 8 bits), por exemplo “192.168.200.1”, “200.162.160.72”. Essas separações de 8 bits que formam o endereço, recebem o nome de “octetos”. Essa forma de organização dos endereços IP serve para facilitar a configuração, em que os computadores e roteadores interpretam de forma binária esses endereços como “11001000100110010001011100101011” (MORIMOTO, 2008).

Além dos endereços IP usados para identificar dispositivos dentro de uma rede, utilizamos a Máscara de Rede. É um número também composto por 4 blocos de 8 bits, (32 bits). Esse número serve para destacar, no endereço IP, a sua porção correspondente de rede, que pode ser organizada por meio de classes.

2.1.1 Protocolo TCP

O protocolo TCP (*Transmission Control Protocol*), ou Protocolo de Controle de Transmissão, é a outra parte do conjunto TCP/IP que sustenta a atual rede mundial de computadores conhecida como *Internet.* Sua capacidade o tornou um dos mais adequados protocolos para as redes globais, já que é ele que fica responsável por verificar se os dados são transmitidos de forma correta da origem até o seu destino final, mantendo a sequência correta das informações transmitidas e não permitindo erros dentro da rede (MORIMOTO, 2008).

Por ser um protocolo que sustenta grande parte das operações da *Internet*, sua estrutura é orientada pela conexão, ou seja, a aplicação de origem faz o pedido para que haja uma conexão entre ela e o seu destino e, através disso, a “conexão” é usada para transferir informações. Sempre a conexão é feita entre uma origem e destino, por isso, fica conhecida também como uma conexão Ponto a Ponto.

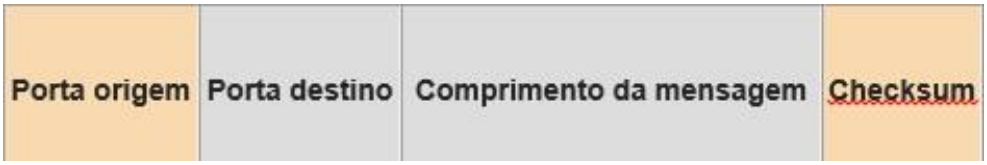
Sua composição oferece uma grande confiabilidade, pois o protocolo TCP utiliza diversas ferramentas para que proporcione uma entrega de pacotes de dados confiável, o que é uma grande vantagem em relação ao protocolo UDP *(User Datagram Protocol).* O protocolo TCP permite a retransmissão dados perdidos durante a transmissão, recupera pacotes corrompidos, solicitando a sua retransmissão e também consegue restabelecer a conexão no caso de alguma falha durante a transmissão (MORIMOTO, 2008).

2.1.2 Protocolo UDP

Conhecido com protocolo UDP *(User Datagram Protocol), é* um dos grandes responsáveis pelo funcionamento de uma rede de telefonia sobre o protocolo TCP/IP. Sua funcionalidade ocorre na camada 4 do modelo TCP/IP e tem como principal função permitir a criação de um datagrama. Pode ser encapsulado dentro de um pacote IPv4 e também do protocolo IPv6 (protocolos usados na camada 4 do modelo TCP/IP) (MORIMOTO, 2008). Por se tratar de um protocolo simples para transmitir informações, ele não é orientado à conexão, ou seja, não há garantias de que quando for enviado um pacote usando o protocolo UDP haverá uma confirmação do recebimento ao seu destino.

O cabeçalho de estrutura do protocolo é bem simples, contendo apenas 4 tipos de informações: a porta de origem da transmissão, a porta de destino, o tamanho da mensagem e a verificação da integridade dos dados que estão sendo transmitidos. Segue abaixo imagem com a estrutura de pacote usando o protocolo UDP (MORIMOTO, 2008):

Figura 4. Forma do Pacote do Protocolo UDP



Fonte Adaptada: Autor Desconhecido

2.2 Protocolo RTP/RTCP

Tratando-se de um serviço em tempo real como o VoIP, o protocolo RTP (*Real-Time Transport Protocol)* é um protocolo de rede importante para aplicações em tempo real. Ele

define como é feita a divisão do áudio durante o fluxo de transmissão em uma conexão, colocando em ordem cada fragmento da divisão para serem entregues. Seu funcionamento fica especificado dentro da camada 4 (transporte) do modelo TCP/IP, usando como base o protocolo UDP para transporte de seus fragmentos. O protocolo RTP não garante em seu desempenho o QoS (*Quality of Service)* e nem reserva algum tipo de recurso, mas sua utilização é usado paralelamente com o seu "irmão", o protocolo RTCP (*Real-Time Transport Control Protocol),* permitindo que haja um monitoramento de seu desempenho. RTP e RTCP são usando em conjunto, mas cada um deles tem uma forma diferente de ser transmitidos. (ALMEIDA, 2006).

Dentro de sua estrutura, podem ser enviadas diferentes tipos de mídias em diferentes sessões, mesmo que façam parte da mesma comunicação. Um exemplo de tal diferença entre as mídias é uma videoconferência, em que são transmitidos dois tipos diferentes de mídia (áudio e vídeo). Os pacotes de áudio serão passados por uma sessão RTP, enquanto que, por outro lado, as transmissões dos pacotes com os fragmentos de vídeo serão transportadas por outra sessão RTP, diferente e independente. (ALMEIDA, 2006).

Trabalhando em paralelo ao RTP, o protocolo RTCP (*Real-Time Transport Control Protocol)* foi definido através do IETF (*Internet Engineering Task Force),* e tem sua função baseada no envio periódico de pacotes, para assegurar o controle do protocolo RTP e de participantes durante uma conexão ou chamada.

Permitindo que se possa trabalhar com diversas mídias dentro de sua estrutura, ele mostra uma maneira de haver relatórios de recebimento dos pacotes, podendo, assim, identificar falhas nas distribuições, ao contrário do RTP, no qual não é possível fazer esse tipo de verificação. Por isso, os dois protocolos RTP e RTCP trabalham em paralelo. (ALMEIDA, 2006).

Quando há uma comunicação com diversos usuários, no caso de uma videoconferência, tem-se uma previsão de que todos os participantes estão enviando pacotes RTCP durante sua conexão. Assim, é necessário restringir a taxa de transmissões, variando de acordo com o número de participantes, para que não haja sobrecarga na rede.

2.3 Protocolo SIP

A tecnologia VoIP permite a transmissão de voz por redes TCP/IP (Protocolo de Controle de Transmissão / Protocolo de Internet), após fragmentar em as informações e encapsular trechos de voz em pacotes. Para a transmissão de serviços multimídia, como o VoIP e vídeo-chamadas torna-se necessário estabelecer uma conexão entre pelo menos uma origem e um ou mais destinos. O SIP pode convidar usuários para participar de uma nova sessão ou para uma sessão multimídia já existente. Essa forma conexão é denominada sessão e os dois principais protocolos que a estabelecem são o H.323 e o SIP (REGISTRO.BR).

Segundo (KELLER, 2011), SIP (*Session Initiation Protocol*), trata de um controle referente à camada 5 do modelo TCP/IP, usado para iniciar, modificar e/ou terminar chamadas e sessões entre usuários, durante comunicação no serviço VoIP. Seu padrão está estabelecido pelo IETF (*Internet Engineering Task Force* – Força Tarefa para Engenharia da Internet*).* Teve seu desenvolvimento iniciado nos anos de 1990. Segundo (OLIVEIRA, 2012), seu princípio de funcionamento é similar ao protocolo HTTP (*Hypertext Transfer Protocol* – Protocolo de Transferência de Hipertexto). Com essas semelhanças, deixam que o protocolo SIP controle a aplicação em seu terminal, o que elimina uma central de respostas como no anterior protocolo H.323.

Dentre suas funcionalidades tem-se a localização de usuários, o estabelecimento de chamadas, o suporte a *unicast* ou *multicast*, possibilita a administração na participação de chamadas (transferências, conferência, entre outros) e também é compatível com o antigo protocolo utilizado para comunicação e participação, o H.323, via gateway. De acordo com artigo escrito pelo (OLIVEIRA, 2012), é um protocolo cliente-servidor similar ao HTML no tocante à sintaxe e semântica das estruturas empregadas, com campos explicitamente descritos.

O protocolo SIP pertence ao grupo dos protocolos da camada de aplicação e de sinalização fim-a-fim baseado em texto, o qual sinaliza o início, a modificação e o encerramento das sessões. As sessões se baseiam no modelo cliente-servidor e independem do tipo de dado trafegado dentro do canal estabelecido. Os protocolos de sinalização para VoIP, como o SIP, devem ter como a prioridade a codificação de voz, a configuração das chamadas, o transporte de dados, a forma de autenticação, os requisitos físicos como telefones, estrutura de redes dentre outros tipos de equipamentos, além das tecnologias de segurança, as

primitivas de comunicação, o formato do cabeçalho e do endereçamento e a sintaxe das mensagens.

Como já descrito, o SIP por se tratar de um protocolo com estrutura de cliente/servidor (pedidos realizados por um cliente e que são atendidos pelo servidor), pode ocorrer também dessa chamada envolver diversos servidores à um único cliente. O protocolo SIP deve também oferecer funções básicas como:

- Conversão de nomes e localização de usuários:

Envolve o mapeamento entre nomes de diferentes tipos de abstração, tais como nomes de um domínio e o nome de um usuário em servidor *Internet*, isto é necessário para que um determinado usuário, que possui um nome qualquer, possa ser convertido em um endereço IP, de modo que possa ser localizado a qualquer momento da ligação. Função igual a um DNS (REGISTRO.BR).

- Negociação de configuração:

Permite que um grupo de usuários defina que tipo de informações será trocada e seus respectivos parâmetros. O conjunto e o tipo dos dados que estão sendo enviados não precisam ser uniformes dentro de uma chamada, como diferentes conexões ponto a ponto pode envolver diferentes tipos de codificações, sendo restritos ao enviar apenas um tipo de dado em cada fluxo (REGISTRO.BR).

- Alteração de configuração:

Torna possível a alteração, de maneira dinâmica, ou seja, durante a utilização de uma conexão por seus usuários, dos parâmetros definidos no momento do estabelecimento da conexão (REGISTRO.BR).

2.3.1 Sinalização SIP

O protocolo SIP tem como base o HTTP, e como tal, consegue suportar o transporte de qualquer tipo de carga em seus pacotes. Como o SIP funciona em uma arquitetura de cliente/servidor, suas funções são envolvidas em apenas métodos de requisição e resposta, como de forma realizado também no protocolo HTTP. A forma de requisição no protocolo SIP, ocorre da seguinte forma.

- INVITE: Em uma conexão, indica que o usuário de um lado, está convidando um outro para uma sessão multimídia. O corpo da mensagem com a requisição pode conter uma descrição da sessão, utilizando-se o protocolo de descrição de sessão SDP (*Session Description Protocol)* (REGISTRO.BR).

- ACK: Mensagem de recebimento como resposta final ao INVITE inicial. A requisição ACK pode conter o SDP contendo a descrição da sessão negociada entre o cliente inicial e o final. Se caso o SDP não estiver presente, o usuário chamado, pode assumir a descrição vinda pelo primeiro INVITE, se caso houver (REGISTRO.BR).

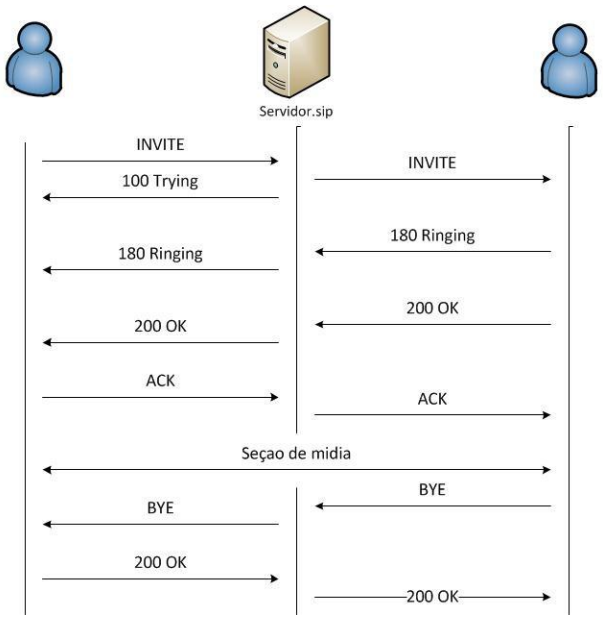
- OPTIONS: Pergunta sobre quais métodos e extensões o servidor suporta, através do usuário descrito dentro do campo do cabeçalho de origem. O servidor que for requisitado, responde a esta pergunta com o conjunto de extensões solicitados pelo usuário que fez essa requisição (REGISTRO.BR).

- BYE: Libera os recursos associados a conexão e força a desconexão da mesma (REGISTRO.BR).

- CANCEL: Tem como função principal, cancelar uma requisição que possa estar pendente, ou seja, que ainda está em andamento. Uma requisição pode ser considerada pendente, se e somente se, ela não obtiver uma resposta de sua requisição (REGISTRO.BR).

- REGISTER: Uma solicitação realizada por um cliente, usa este método para criar um “alias” (apelido), do seu endereço em algum servidor SIP (REGISTRO.BR). Na figura 5 é mostrado o caminho de uma chamada entre dois usuários por meio de um servidor SIP:

Figura 5. Sinalização do Protocolo SIP.



Fonte: REGISTRO BR

O Usuário A disca para o Usuário B. Neste momento o ramal do Usuário A encaminhou o INVITE para o servidor.sip (servidor em que está registrado). O servidor encaminhou o INVITE para o ramal do Usuário B que está registrado no mesmo servidor (ligação interna), e respondeu ao A "100 Trying" informando que está tentando efetuar a ligação.

O Usuário B quando recebe a solicitação da chamada e envia o "180 Ringing" para o servidor, informando que recebeu o INVITE e está chamando.

O servidor repassa para o ramal do Usuário A a mensagem informando que o telefone está chamando. O Usuário B atende o telefone, neste momento o ramal dele envia "200 OK" informando que o telefone foi atendido e já é possível estabelecer o fluxo de mídia.

O servidor repassa o "200 OK" para o ramal originador da chamada do Usuário A que responde com "ACK" (*Acknowledge*) confirmando que recebeu o "200 OK".

O servidor repassa o "ACK" para o ramal do Usuário B que ao receber a confirmação abre a sessão de mídia diretamente entre os dois ramais, dando início a conversa entre os dois usuários. O usuário B encerra a chamada, nesse momento o ramal envia a mensagem de BYE, informando o sinal de desligamento.

O servidor repassa o BYE para o ramal do Usuário A, que responde com 200 Ok, confirmando o encerramento da chamada (REGISTRO.BR).

2.4 Protocolo SNMP

O protocolo SNMP (*Simple Network Management Protocol)* é um protocolo da camada de aplicação criado para transportar informações de rede entre os dispositivos gerenciados. Ele permite que administradores de rede administrem o desempenho de uma rede monitorando interfaces de rede, processadores, memórias de equipamentos como roteadores, *switches*, dispositivos wireless e servidores (SALVO, 2011).

O sistema de gerenciamento de rede baseia-se em dois elementos principais: um supervisor e agentes. O supervisor é o que permite ao administrador executar a gestão. Os agentes são entidades que se encontram a nível de cada interface que liga o equipamento monitorado à rede e que permite recuperar informações sobre diferentes dispositivos (KIOSKEA, 2014).

Administradores de redes conseguem verificar o *status* atual da rede, manter um histórico de atividades, assim como receber avisos de forma imediata para ajudar na resolução de problemas.

A primeira versão do SNMP foi implementada como padrão em 1989 e quatro anos depois teve uma atualização para a versão 2. O SNMPv2 (versão 2) fornece uma administração de rede concentrado e distribuído incluindo refinamentos na sua estrutura e gerenciamento. Ambas as versões 1 e 2 do SNMP não são seguras (SALVO, 2011).

O SNMPv3 (versão 3), foi desenvolvido e implementado para solucionar questões de segurança, provendo acesso seguro às informações de gerenciamento por meio de autenticação e criptografia dos pacotes transportados dentro da rede (SALVO, 2011).

3 REDES DE COMUNICAÇÃO

Segundo (MORIMOTO, 2008), utilizar algum tipo de cabo, seja ele par trançado ou até mesmo a fibra óptica, é, quase sempre, a forma mais rápida de se transmitir dados.

Os cabos de par trançado *cat5e* (Categoria 5e), podem transmitir dados a até 1 gigabit a uma distância de até 100 metros, enquanto os cabos de fibra óptica são usados em links de longa distância. Usando interfaces de 10 Gigabit *Ethernet* e cabos de fibra monomodo, é possível atingir distâncias de até 40km, sem necessidade de usar repetidores.

Tratando-se de flexibilidade, a rede cabeada acaba levando desvantagem, pois se for necessário a mudança no cenário, que seja para adicionar algumas máquinas ou outros tipos de equipamentos que dependem dessa rede cabeada, será necessário alterar o projeto original.

3.1 Redes sem Fio (*Wireless*)

As redes *wireless* permitem suprir esta lacuna, permitindo flexibilizar o cabeamento de rede. Você pode então combinar o uso de cabos e de conexões wireless, usando uma ou outra forma de conexão de acordo com a situação (MORIMOTO, 2008).

Além dos PCs, as redes *wireless* são a forma preferida de conexão para *smartphones*, *tablets* e diversos outros dispositivos móveis. Mesmo que você tenha em seu *smartphone* um plano de acesso 3G, você vai preferir usar a rede *wireless* em vez da rede celular sempre que possível, já que ela será quase sempre muito mais rápida do que as conexões que são disponíveis pelas operadoras de celulares, além de reduzir o consumo da bateria do aparelho em questão. Seja em escritórios, fábricas, bancos, lanchonetes, escolas ou residências, as redes *wireless* estão em toda parte (MORIMOTO, 2008).

Existem vários tipos e padrões de redes *wireless*, como por exemplo, o *WiMax*, *Bluetooth*, *Wi-Fi (Wireless Fidelity)*, *InfraRed*(Infravermelho) (ARTHAS,2004).

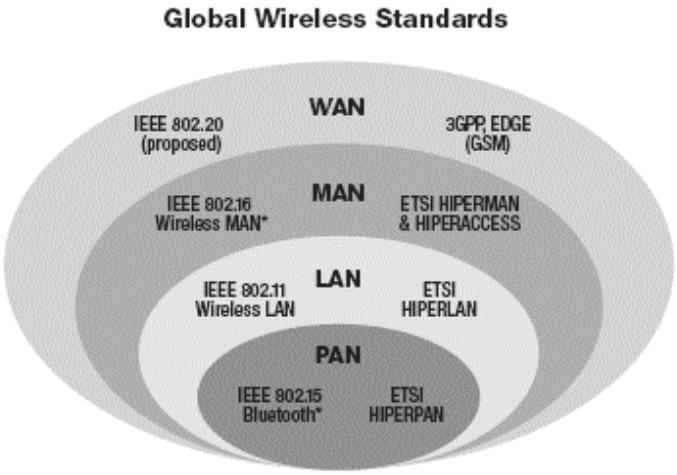
Uma rede *wireless* é reconhecida por ser sem fio, pois o transmissor e o receptor estão se comunicando sem a presença de fios, no nosso caso, por ondas de rádio. (ENGST & FLEISHMAN, 2005)

No caso de uma rede *wireless* de telefonia VoIP, precisa-se ter uma rede com

disposição física bem estruturada e um *link* separado para suprir somente a telefonia em si. No caso da empresa onde será realizado os testes, a telefonia é separada da rede de *Internet* para não haver problemas de sobrecarga de uso de uma rede sobre outra. Com a possível expansão da rede VoIP cabeada para a rede sem fio, haverá um aumento de equipamentos, o que pode aumentar o consumo de banda.

Na figura 6 são classificados os níveis de redes, separadas por sua capacidade de transmissão e nomenclatura:

Figura 6. Classificação das Redes e Capacidade de Transmissão.



Fonte Adaptada: Intel

Uma rede sem fio pode ser considerada desde uma conexão *Bluethooth*, entre dois dispositivos como celulares, rádios e outros equipamentos que possam transmitir dados em distâncias pequenas, ou até mesmo redes de longo alcance como uma WAN (*Wide Area Network),* que cobre grandes distancias e que são responsáveis por realizar a comunicação de locais distantes entre si, como cidades, estados e até países, de modo geral e a forma como é estrutura a atual rede mundial de computadores.

Segundo (TEIXEIRA, 2005), o WiMAX, que utiliza o padrão IEEE 802.16, foi ratificado em Dezembro de 2001, estava focando basicamente as faixas de frequências situadas entre 10GHz e 66GHz considerando sempre aplicações com linha de visada, obtendo até 34Mbps.

3.1.1 Padrões de Rede Sem Fio

De acordo com (MORIMOTO, 2008), o padrão 802.11 é um conjunto de padrões criados pelo IEEE para o uso de redes *wireless.* O padrão 802.11 original, hoje chamado de 802.11-1997 ou 802.11 *legacy* foi publicado em 1997 e previa taxas de transmissão de 1 e 2 *megabits*, usando a faixa dos 2.4GHz, escolhida por ser uma das poucas faixas de frequência não licenciadas, de uso livre.

Além dos padrões IEEE, temos também o Wi-Fi (*Wireless Fidelity),* uma certificação opcional para produtos que se tem o uso do tradicional 802.11, que assegura que eles sejam compatíveis entre si.

É bastante comum que usemos o termo "*Wi-Fi*" em referências aos produtos baseados nos padrões 802.11 de uma forma geral mas, tecnicamente falando, apenas os produtos que passam pela certificação podem ser chamados de "*Wi-Fi*", embora na prática isso não faça muita diferença (MORIMOTO, 2008).

Segundo (ARTHAS, 2004), quando se discute a configuração de uma WLAN existem alguns padrões, desenvolvidos ou em desenvolvimento pelo I*EEE (Institute of Eletrical and Eletronic Engineers)* que devem ser considerados:

IEEE 802.11a – Padrão que é constituído dentro das características das camadas de enlace e física para as redes sem fio que trabalham na frequência de 5GHz. Firmado em 1999, não existem muitos equipamentos atualmente que trabalhem nessa frequência.

IEEE 802.11b – Atualmente é um dos tipos que está mais presente dentro do cenário de rede sem fio. Possui aspectos da implementação dos sistemas de rádio e também já inclui aspectos de segurança como a WPA *key*. Foi aprovado em 2003 pelo IEEE.

IEEE 802.11g – O padrão 802.11g utiliza a mesma frequência de seu antigo padrão o 802.11b e com isso, é possível que os dois padrões se comuniquem entre si. A ideia é permitir que novos equipamentos usando o novo 802.11g possam trafegar em uma rede do padrão anterior, sem a necessidade se alterar a rede toda. Seu padrão foi definido em 2006.

IEEE 802.11n – É o padrão mais atual para as redes sem fio, tem como principais características, conectar ou aceitar qualquer tipo padrão em sua topologia. O segundo ponto é a capacidade de transferência, que foi aumentada em nível de transferência equiparado a uma

rede cabeada local. Seu lançamento aconteceu em 2009, mas seu desenvolvimento final aconteceu em meados de 2003.

3.2 Segurança em Redes Sem Fio

Segundo (OLIVEIRA, 2012), a utilização desse tipo de tecnologia implica em uma questão maior em relação a sua segurança para uma rede cabeada convencional.

Os ataques mais comuns em redes sem fio referem-se à obtenção de informações sem autorização, acesso indevido à rede e ataques de negação de serviços. Esses ataques possuem graus de dificuldade que dependem das características de implementação da rede. Para que uma rede sem fios possua as mesmas características de segurança de uma rede com fios, existe a necessidade de inclusão de mecanismos de autenticação de dispositivos e confidencialidade de dados (OLIVEIRA, 2012).

Uma forma de proteção aos dados trafegados na rede é conhecido como criptografia. No possível ataque de algum individuo a rede sem fio para tentar obter dados que estão sendo transmitidos, a criptografia irá cuidar para que os dados em questão fiquem embaralhados a ponto de não serem montados e o ataque não consiga realizar a extração de qualquer tipo de informação.

Para que haja tal segurança com as criptografias, existem sistemas que realizam o trabalho de “bagunçar” as informações. Quando o seu transmissor, um AP (*Access Point),* por exemplo, transmitir a informação ela será criptografada e um dispositivo compatível com esse tipo de criptografia, ao receber a informação tem a capacidade de remontar a informação transmitida. Quando se fala em tipos de criptografia para redes *wireless*, estão os principais tipos: WEP, WPA/WPA2.

3.2.1 Criptografia WEP

O *Wired Equivalency Privacy* (WEP), é o método de criptografia usado nas redes wireless 802.11. O WEP tem sua operação na camada dois (Enlace) do modelo de rede TCP/IP e fornece segurança entre o cliente e o *Access Point.*

Como forma de proteção, o WPE tem como base o método criptográfico RC4

(Route Coloniale 4), da RSA, que inicialmente usa um Vetor de Inicialização (IV) de 24 *bits* e também uma chave secreta compartilhada *(secret shared key),* de 40 ou 104 bits. O IV é concatenado com a *secret shared key* para formar uma chave de 64 ou 128 *bits* que é usada para criptografar os dados. (GIMENES, 2005). O Access Point e todas as estações que se conectam a ele dever usar a mesma chave compartilhada.

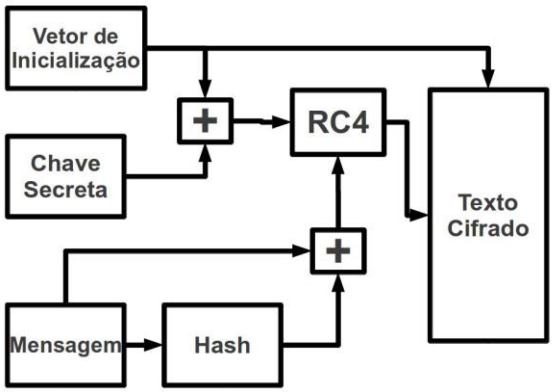
O surgimento do WEP, tem como fundamento ter um nível de segurança equivalente à de redes cabeadas. Em prática o WEP possui suas falhas, mas oferece uma essencial camada de proteção, sendo mais difícil de se invadir do que o SSID (*Service Set Identification)* ou até uma lista de endereços físicos, os MAC ADDRESS *(Media Access Control).*

Para os pacotes de dados enviados em qualquer direção, o transmissor combina o conteúdo do pacote com uma soma de verificação desse pacote. O padrão WEP pede, então, que o transmissor crie um (IV) (*Inititialization Vector* – Vetor de Inicialização) especifico para o pacote, que é combinado com a chave e usado para criptografar o pacote. O receptor gera seu próprio pacote correspondente e usa-o para descriptografar (OLIVEIRA, 2012).

Segundo a (MICROSOFT, 2004) o WEP se encarrega de criptografar os dados que são transmitidos dentro da rede. Para esse tipo de criptografia: 64 e 128 *bits.* O primeiro tipo (64 *bits*), é suportado por qualquer tipo de interface ou ponto de acesso que siga o padrão *WI-FI,* o que cobre praticamente todos os equipamentos fabricados atualmente. Já o segundo tipo (128 *bits),* não possui essa flexibilidade. Para poder obter seu uso, é necessário que todos os equipamentos instalados e conectados à rede, tenham suporte para padrão para esse tipo de arquitetura, caso os equipamentos não possuírem, ficarão presos somente a arquitetura de 64 *bits.*

Na figura 7 é mostrado como fica a estrutura para que as informações sejam criptografadas

Figura 7. Estrutura de Criptografia por meio da Criptografia WEP.



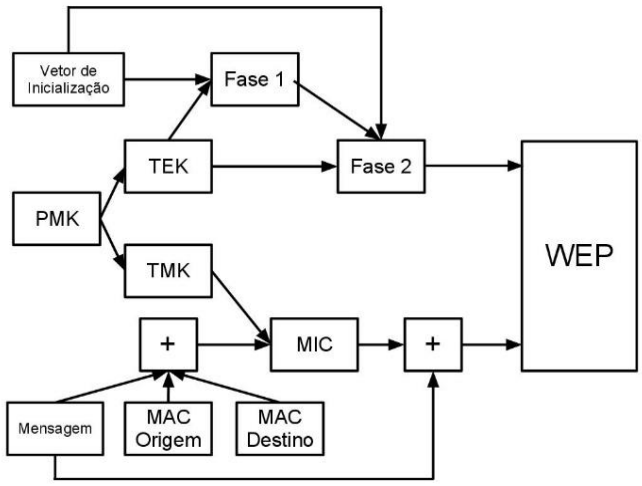
Fonte Adaptada: PAIM, Rodrigo R.

3.2.2 Criptografia WPA/WPA2

Sucessor do WPE, o WPA (*Wi-Fi Protected Access),* veio para seu atual lugar como protocolo-padrão para os modelos de rede sem fio. Foi incorporado em 2003, trazendo como sua principal novidade, 256 *bits* de encriptação ao invés de seu antecessor de 64 ou 128 *bits*, gerando assim uma maior segurança as redes.

De acordo com (OLIVEIRA, 2012), o WPA ainda não é um padrão IEEE oficial, embora seja compatível com o padrão 802.11i, as vezes chamado de WPA2. O WPA consegue solucionar a questão dos cabeçalhos do antigo protocolo WEP, que eram conhecimentos como Vetor de Inicialização (IV) e que eram relativamente "fracos", em relação aos pacotes transmitidos dentro da rede. De certa forma, essa nova estrutura de criptografia oferece uma solução para garantir que as mensagens transmitidas pelo MIC (*Message Integrity Code),* conhecido como Michael, usando TKIP (*Temporal Key Integrity Protocol),* para a melhoria de criptografia dos dados. O WPA-PSK (WPA – *Pre Shared Key)* é um modo especial do WPA para os usuários domésticos sem um servidor de autenticação corporativo e oferece a mesma proteção forte de criptografia.

Figura 8. Estrutura de Criptografia por meio da Criptografia WPA.



Fonte Adaptada: PAIM, Rodrigo R.

3.2.3 Criptografia WEP x WPA/WPA2

Com o surgimento e substituição do WEP pelo WPA, há a vantagem de melhoria em relação a criptografia dos dados e informações ao utilizar um protocolo de chave temporária, como no caso o TKIP, que tem a possibilidade da criação de chaves por pacotes. O vetor de inicialização de 48 bits, ao invés de 24 como no seu antecessor WEP e possui também um mecanismo de distribuição de chaves. Além disso, uma outra vantagem apresentada na nova versão de criptografia é a melhoria no processo de autenticação de usuários. Na tabela 3, é mostrada alguma das vantagens e desvantagens dos dois tipos abordados nos itens anteriores:

Tabela 3. Tabela de Comparação entre WEP e WPA.

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

Fonte Adaptada: (VILELA; RIBEIRO)

4 MÉTODOS DE AVALIAÇÃO PARA DESCOBERTA DE VULNERABILIDADES E ATAQUES

Ao desenvolver o cenário para a implementação dos serviços e realização dos ataques, foram utilizadas diversas ferramentas para diversos tipos de serviços, desde o monitoramento do desempenho do servidor, roteadores sem fio, tráfego de rede e avaliação de pacotes, até mesmo a implementação de segurança com a utilização de um *Firewall*. Este capítulo descreve as ferramentas e seus respectivos aspectos e funcionalidades.

4.1 Zabbix

De acordo com o site oficial do desenvolvedor (ZABBIX.COM), o Zabbix é o software de nível empresarial projetado para disponibilidade e desempenho de componentes de infraestrutura de TI para monitoramento. Zabbix é *open source* e não há custos em sua utilização.

Com Zabbix é possível reunir tipos diversos de dados da rede que trafegam dentro da rede. Ele permite um monitoramento em tempo real de alto desempenho de diversos servidores, máquinas virtuais e dispositivos de rede conectados simultaneamente em uma rede.

Ainda segundo o site do desenvolvedor, com os dados de armazenamento, os recursos de visualização estão disponíveis por (sínteses, mapas, gráficos, telas, etc), bem como formas muito flexíveis de analisar os dados com a finalidade de alertar. Para isso são definidos limites aceitáveis para que quando atingir esse tipo de margem definida pelo administrador da rede, seja gerado um alerta em tempo real. Assim que esses limites são ultrapassados, Zabbix pode entregar notificações por e-mail informando os administradores de rede sobre o atual ou um problema em potencial.

O Zabbix coloca módulos de coleta de dados. Além de usar scripts personalizados, agora um módulo pode ser usado no Zabbix Agent, *server* ou *proxy* para coletar dados. Ele pode ser compilado ou carregado em tempo de execução.

As informações são extraídas por dois tipos de formas: Protocolo SNMP; Agente Zabbix (*Zabbix Agent*).

4.1.1 Protocolo SNMP

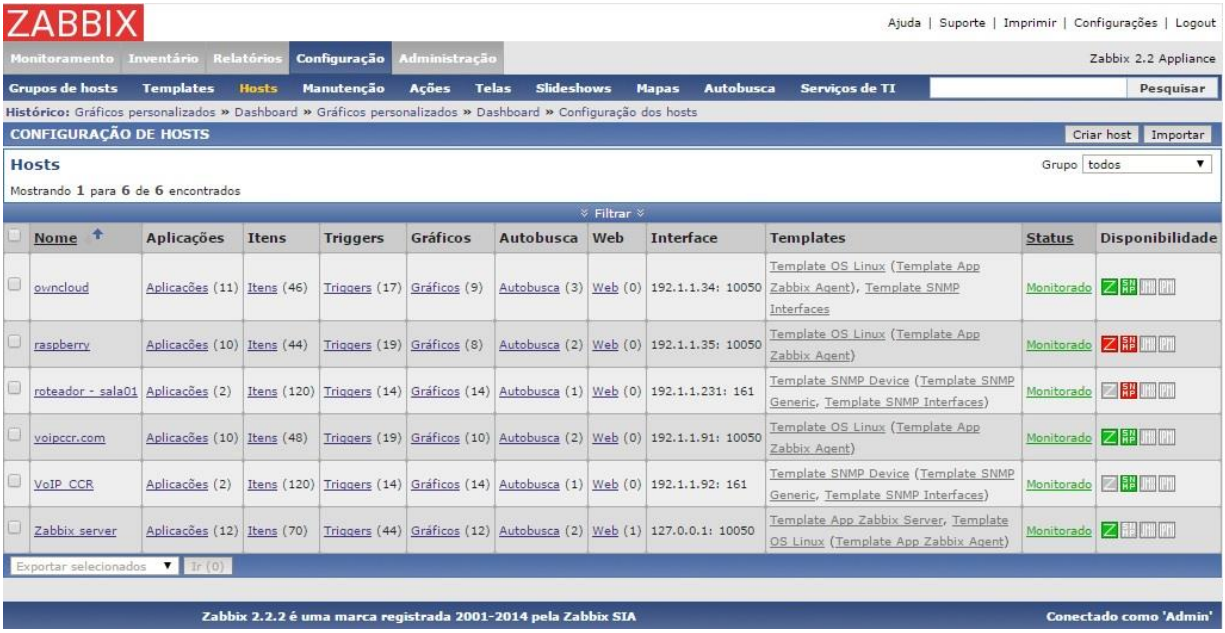
O protocolo SNMP (*Simple Network Management Protocol)* é um protocolo da camada de aplicação criado para transportar informações de administração de rede entre os dispositivos gerenciados e os sistemas que deem suporte a gestão de redes. Ele possibilita que administradores de rede gerenciem o desempenho da uma rede monitorando interfaces, processadores, memórias de equipamentos como roteadores, *switches*, dispositivos *wireless* e servidores.

4.1.2 Zabbix Agent

O agente Zabbix é instalado nos hosts que irão ser monitorados e permite coletar métricas comuns - especificação de um sistema operacional, como CPU e memória.

Há agentes Zabbix disponíveis para Linux, Solaris, HP-UX, AIX, FreeBSD, OpenBSD, OS X, Tru64/OSF1, Windows NT, Windows Server, Windows XP e Windows Vista.

Figura 9. Interface de Monitoramento de hosts por meio da ferramenta Zabbix.



Fonte: Servidor Zabbix

A figura 9 mostra uma das telas principais para avaliação dos servidores. Essa imagem mostra o *status* do monitoramento e por qual tipo de protocolo ou serviço ele realiza essa tarefa. Os mais comuns são por meio do protocolo SNMP e o *Zabbix Agent*. Além do status dos servidores em questão, é mostrado ao usuário, informações adicionais como: IP e porta em que o serviço está rodando. Se caso for o *Zabbix Agent* a porta utilizada será a UDP 10050. No caso de dispositivos de rede, como um roteador ou *switch* a avaliação é realizada por meio do protocolo de camada 5 SNMP. A porta que o serviço é utilizado é a UDP 161 e 162. O serviço também mostra a quantidade de aplicações que estão sendo monitoradas, itens de avaliação como, rede, cpu, memória ram, etc. As *triggers* são os avisos automáticos criados pelo administrador, ao definir limites de carga a qualquer tipo de item monitorado nos servidores.

Para a realização da varredura a procura por falhas de segurança em servidores ou serviços que trabalham com a utilização de redes, é utilizado um programa *OpenSource* chamado NMAP.

4.1.3 NMAP

De acordo com o site (NMAP.ORG), o *Nmap ("Network Mapper")* é uma ferramenta de código aberto para exploração de rede e auditoria de segurança. Ela foi criada com a função de mapear rapidamente redes de grande porte, no entanto também funciona muito bem contra hosts individuais. O Nmap utiliza pacotes IP em estado bruto (raw) de maneira para determinar quais hosts estão disponíveis na rede, quais serviços (nome da aplicação e versão) os hosts atacados oferecem, quais sistemas operacionais (e versões de SO) eles estão executando em suas máquinas, que tipos de filtro de pacotes/*firewalls* estão em uso, e dezenas de outras características.

O retorno ao realizar um mapeamento utilizando o Nmap é uma lista de alvos mapeados, com informações adicionais de cada um dependendo das opções utilizadas. Abaixo segue alguns exemplos da sua utilização e parâmetros mais básicos:

nmap –sV 192.168.0.1 – Obtém informações de portas abertas e versão de serviços de um único host;

nmap 192.168.0.1-254 – Scanear uma faixa inteira de endereços de rede;

nmap -O 192.168.0.1 – Obtém informações do S.O que está rodando no alvo;

nmap -sU 192.168.0.1 – Faz um mapeamento de todas as portas UDP de um alvo;

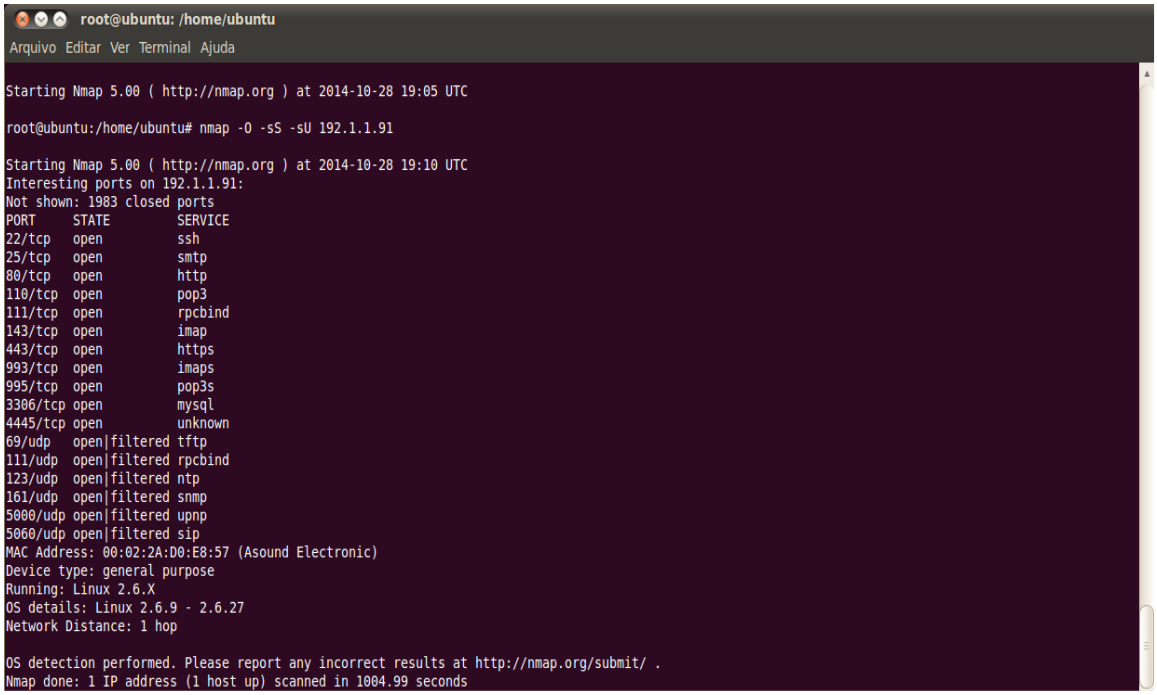
nmap -p 0-65535 192.168.0.4 – Faz um mapeamento de todas as portas TCP e UDP de um alvo.

Para a realização do monitoramento ao alvo desejado, foi realizado a seguinte linha de comando:

nmap – O –sS -sU 192.1.1.91

O retorno da verificação pode ser avaliado na figura 10.

Figura 10. Mapeamento Utilizando NMAP a um host alvo sem Firewall.



Fonte: NMAP

Os parâmetros utilizados ao realizar o mapeamento mostram as seguintes informações, como as portas TCP e UDP (-sU) e os serviços que estão sendo utilizados pelas mesmas e a versão do S.O (-O), no caso é uma distribuição LINUX com a versão do *Kernel* 2.6.9. Também é mostrado a distância em que o host que realizou o ataque está do host alvo, apenas 1 salto. Após uma avaliação das portas que estão desprotegidas, a escolha será a porta 80 que

utiliza os serviços HTTP. Os ataques serão realizados com injeção de pacotes UDP e será monitorado o desempenho do servidor ao sofrer tal ataque.

A realização dos ataques a este *host* alvo, será elaborado algumas regras de segurança com a utilização de um *Firewall*. O próximo item desta monografia irá descrever com alguns detalhes o funcionamento de um *Firewall* dentro de um sistema operacional *Linux* e como é feita o tratamento das informações recebidas pelo mesmo (NMAP.ORG).

4.2 Firewall

Firewall é um *software* ou um *hardware* que verifica informações originárias da *Internet* ou de uma rede, e as bloqueia ou permite a chegada delas ao seu servidor ou computador dentro de sua rede, dependendo das configurações do firewall (MICROSOFT, 2004).

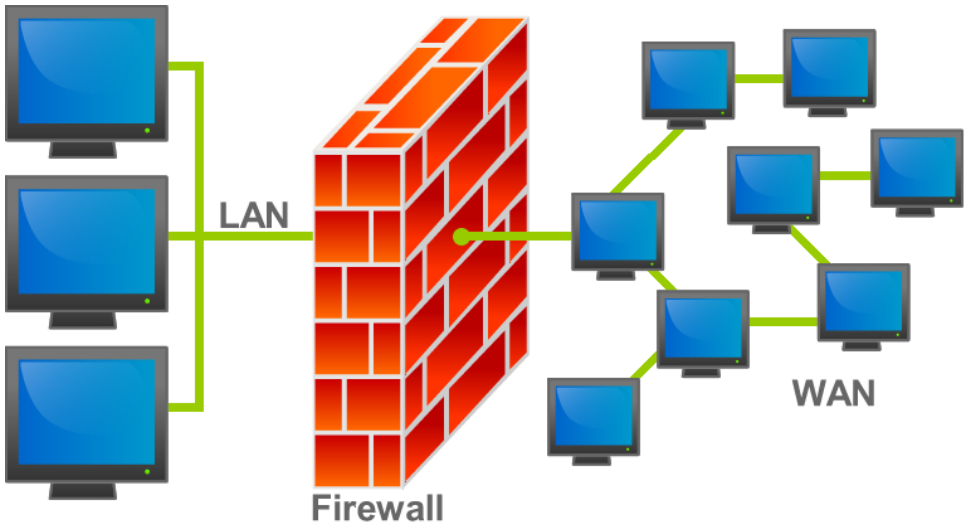
Um *firewall* pode auxiliar e impedir que *hackers* ou *softwares* mal-intencionados (*worms)* consigam acesso a um computador por meio de uma rede ou da *Internet*. Um *firewall* também pode ajudar a impedir o computador de enviar *software* mal-intencionado para outros computadores.

Embora existam diversas formas de se invadir uma rede, apenas uma pequena parte dessa enorme massa possui algum tipo de “inteligência” para realizar tais tarefas como extrações de informação, e que, mesmo estas formas, fazem o mais simples que são de aproveitar falhas, por mais pequenas que sejam e que estão presentes em serviços de redes ou mesmo em protocolos (NETO, 2004).

Desenvolvido pela Bell Labs em meados de 1980, a pedido de uma das maiores empresas de telecomunicações do mundo a AT&T, o primeiro *Firewall* do mundo foi desenvolvido com o objetivo de “filtrar” informações que entravam e saiam da sua rede empresarial, de forma que fossem flexíveis para a manipulação seguindo especificações presentes as regras definidas pelos cientistas e desenvolvedores da Bell Labs (NETO, 2004).

Na figura 11, é mostrado de forma simples o papel de um firewall presente em redes de computadores.

Figura 11. Firewall e sua Estrutura dentro de uma rede.



Fonte Adaptada: Wikipédia

De acordo com (NETO, 2004), as funções do *Firewall* em um sistema operacional *Linux* são agregadas à própria arquitetura do *Kernel*, tornando-o, superior em comparação a seus concorrentes. Enquanto a maioria dos "produtos" denominados *Firewall*, podem ser classificadas como um subsistema, o *Linux* permite transformar-se em próprio *Firewall*.

Tudo o que é recebido ou enviado de um *host* é interpretado e/ou processado por seu *Kernel*, independente de sistema operacional. A diferença que ocorre no *Linux* faz diferente de seus concorrentes é agregar, via *Netfilter* (*software* presente ao sistema) que tem a função de fluxo interno em termos de *Firewall.*

Para que o *Kernel* possa trabalhar controlando seu próprio fluxo de dados interno, foi desenvolvido a ferramenta chamada de *Netfilter.* Criada com um conjunto de situações de fluxo de dados presas inicialmente ao *Kernel* do *Linux* e dividido em tabelas:

4.2.1 Tabela Filter

Tabela padrão do *Netfilter* e trabalha as situações implementadas por um *Firewall* de pacotes. Existem 3 tipos em que essa tabela trabalha:

- INPUT: Pacotes que chegam ao *host;*

- OUTPUT: Pacotes que saem do *host;*

- FORWARD: O que chega a um *host* e precisa ser redirecionado a um outro host ou outra interface de rede (NETO, 2004).

4.2.2 Tabela NAT

O NAT (*Network Address Translation)* responsável pelas funções que chegam ao host que opera o *Firewall*. Suas funções são:

- PREROUTING: Quando há necessidade de realizar alterações em pacotes antes serem roteados ao seu destino;

- POSTROUTING: Quando há necessidade de realizar alterações depois que os pacotes forem roteados ao seu destino;

- OUTPUT: Realiza a verificação em pacotes emitidos pelo *host Firewall* (NETO, 2004).

4.2.3 Tabela Mangle

Implementa modificações especiais em um nível mais complexo. Essa tabela é capaz de alterar a prioridade de entrada e saída de um pacote ao qual ele se destinava. Suas tratativas são:

- PREROUTING: Modifica os pacotes antes deles serem roteados;

- OUTPUT: Modifica pacotes gerados localmente antes de serem roteados.

Após um sucinto entendimento sobre o funcionamento de um *Firewall*, serão realizados, testes de ataque com e sem a sua utilização. Os ataques ao serviço de telefonia, serão realizados por injeção de pacotes UDP (UDPFLOOD). Para que seja mostrado o que é enviado ao *host* alvo por esse tipo de ataque, será monitorado a entrada de rede do servidor, por meio de uma outra ferramenta *OpenSource* chamada TCPDUMP, nativa dos sistemas operacionais *Linux*. Abaixo segue um breve resumo de sua principal utilização como ferramenta de monitoramento.

4.3 TCPDUMP

O TCPDUMP é um analisador de pacotes utilizado por *Shell Scripts* em distribuições *Linux*. Seu desenvolvimento é baseado em linguagem de programação C e C++ (TCPDUMP.ORG). Foi desenvolvido em 1987 por do Lawrence Berkeley, do Laboratory Network Research Group.

Com ele é possível realizar análises e solucionar problemas referentes a redes de computadores. Sua utilização é simples, tendo que por base, conhecimento na área de protocolos redes *TCP/IP*.

Um de seus recursos mais importantes são os filtros de pacotes. Com eles é possível especificar em detalhes qual o tráfego que você quer que seja capturado e analisado em um arquivo *log* para análise mais detalhada (PEREIRA, 2014).

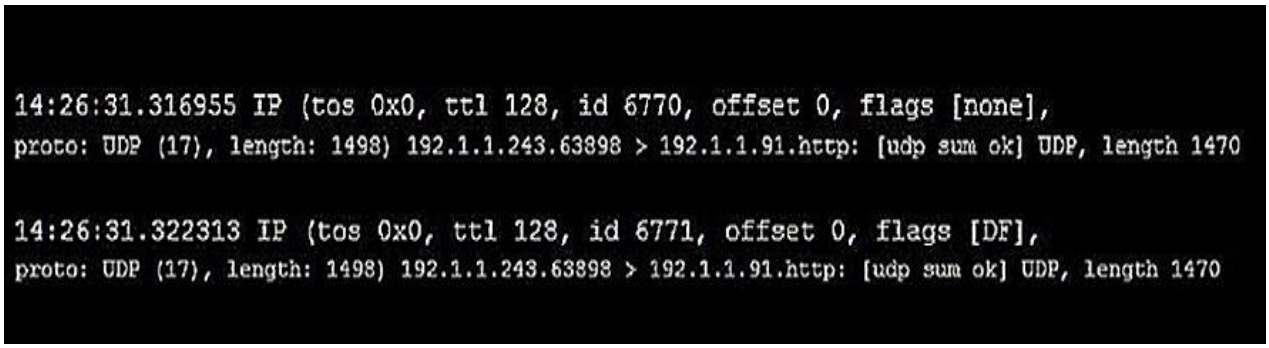
Utilizando parâmetros simples, como qual a placa de rede, endereço do alvo a ser monitorado e quantidade de pacotes, é possível gerar um *log* detalhado do que está ocorrendo na rede, como em:

```
# tcpdump –vv –s 2000 –i eth0 –c 300 src host 192.1.1.243 and dst port 80 > /home/ataque_udp.txt
```

Neste caso, foi pedido um nível de detalhes (-vv), o tamanho máximo de pacotes que devem ser filtrados (-s 2000), a interface que será monitorada do alvo (-i eth0), a quantidade de pacotes que o *log* irá salvar no máximo (-c 300), de onde vem o fluxo de pacotes (src host 192.1.1.243) e por último a porta que deverá ser monitorada, no caso, quando realizado o mapeamento de portas e foi verificado que a 80 correspondente ao serviço HTTP, estava aberta e sem nenhuma segurança, foi a utilizada como parâmetro para o colhimento de informações (dst port 80). A última parte da linha de comando especifica um local para ser gerado o *log* em um arquivo texto simples.

Logo abaixo, na figura 12, é gerado um arquivo de *log* com as saídas de resultados de acordo com os parâmetros passados.

Figura 12. Arquivo de Log TCPDUMP.



Fonte: TCPDUMP

Ao se gerar o *log*, o TCPDUMP foi adiciona ainda algumas informações a mais como: hora de entrada, o tempo de vida do pacote (*TTL – Time to Live)*, o *ID* gerado para cada pacote que chega a interface de rede, o protocolo que corresponde o pacote recebido, o tamanho desse pacote, o IP de origem juntamente com a porta de saída do mesmo, o IP de destino que no caso é o servidor e a porta em que ele está recebendo esses pacotes, no caso a porta 80 (HTTP).

O capítulo a seguir mostrará de forma prática, o desenvolvimento do cenário prático para a realização dos testes de ataque, com a utilização de gráficos de monitoramento do desempenho do servidor e da rede sem fio, sem a implementação de segurança e após a coleta de dados, será realizado novamente os mesmos testes mas com a implementação de um *Firewall*, com bloqueios. Também será avaliado o fluxo de pacotes transmitidos ao servidor destino, com avaliação ao protocolo UDP.

5 IMPLEMENTAÇÃO E AVALIAÇÃO DE UMA ESTRUTURA DE REDE DE VOZ SOBRE O PROTOCOLO IP – SEGURANÇA E MOBILIDADE

A telefonia VoIP aparece com uma das melhores e mais utilizadas tecnologias para a área de comunicação por meio da Internet, com baixos custos, fácil expansão de sua dimensão e alto gerenciamento. O VoIP promete, eventualmente, acabar com mais de um século de rede pública de telefonia comutada (RPTC), transferindo a inteligência do sistema para as bordas da rede, seguindo a tradição da Internet.

Como aplicações IP são flexíveis e mais facilmente criadas e distribuídas, tem-se visto um crescimento do número de soluções VoIP, sendo apresentadas ao mercado. Neste modelo, os próprios usuários terão um importante papel na definição, implementação e controle dos serviços de telefonia (SICKER e LOOKBAUGH, 2004).

Junto a todas essas tecnologias, a flexibilidade do SIP (*Session Initiation Protocol*), atualmente o protocolo mais usado para o estabelecimento de sessões VoIP, faz com que essa tecnologia fique cada vez mais viável e atrativa economicamente quando comparada com o serviço oferecido pela RPTC (SIÉCOLA, 2010).

Por outro lado, toda esta flexibilidade e disseminação também atrai a atenção dos *hackers*. O modo que essa tecnologia se prolifera, não quer dizer que as infraestruturas para comunicações VoIP apresentadas pelos diversos fornecedores têm se preocupado em blindar as ameaças que são inerentes ao SIP, e nem pouco as conhecidas brechas de segurança que circulam as redes IP e praticamente ou todo e qualquer serviço oferecido sobre elas.

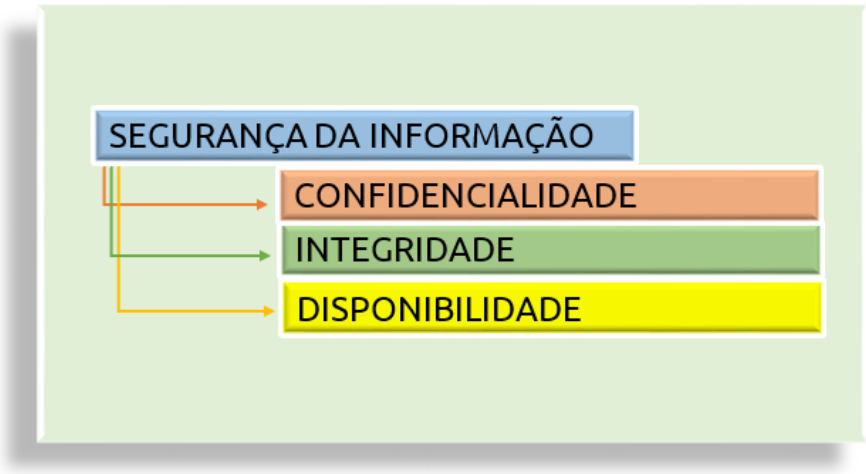
Diante disto, este trabalho se propõe a examinar quais são os principais protocolos que oferecem suporte à telefonia VoIP sem fio e mostra algumas das ameaças que devem ser levadas em consideração ao se preparar uma infraestrutura baseada em SIP, preocupando-se inclusive com as ameaças legadas das já existentes redes IP.

5.1 VoIP: Segurança da Informação

A informação tornou-se o item mais valioso das corporações e como tal, independente da forma como existe e é manipulada (em papel ou eletronicamente), sua proteção passou a ser obrigatória, pois a "vida" e continuidade da empresa está presente em tais tipos de informações.

A norma ABNT NBR ISO/IEC 27002 define segurança da informação como a proteção da informação contra os diferentes tipos de ameaças a fim de minimizar o risco ao negócio. Existem três aspectos chave da segurança da informação que são sempre lembrados como *CIA Triad*, ou Tríade CID: Confidencialidade, Integridade e Disponibilidade, conforme mostrado na figura 13:

Figura 13. Propósitos da Composição para a Segurança da Informação.



Fonte: Próprio Autor

Abaixo serão descritos estes conceitos de maneira breve e posteriormente apresentam-se definições para alguns dos termos mais usados em se tratando de segurança da informação.

5.1.1 Confidencialidade

A confidencialidade é compreendida como a proteção de dados e informações trocadas entre um emissor e um ou mais destinatários contra algum tipo de terceiro. Isto deve ser feito independentemente do sistema de comunicação utilizado: uma questão de grande relevância é a forma de garantir o sigilo de comunicação quando utilizado um meio não seguro, como no caso a *Internet*.

A confidencialidade, conforme (BRAUMANN, CAVIN e SCHMID, 2011), que nenhum acesso à informação deverá ser permitido ou garantido a sujeitos ou sistemas não autorizados, isto é, apenas aqueles autorizados ou que possuem os direitos e privilégios necessários serão capazes de acessar a informação, esteja ela armazenada, em processamento ou em transação.

Em um sistema que garante a confidencialidade, caso um terceiro capture informações trocadas entre o remetente e o destinatário, a segurança não deve permitir que o invasor capture alguma informação “legível”, ou seja, utilizar algum tipo de criptografia.

Utilizam-se mecanismos de criptografia de forma a gerar a ocultação de comunicação para sujeitos não autorizados. Digitalmente podem manter a confidencialidade de um documento com o uso de chaves assimétricas. Os mecanismos de segurança que envolvem algum tipo de criptografia devem garantir a confidencialidade durante o tempo necessário para a informação seja descodificada. Em alguns casos, por esta razão, é necessário determinar quanto tempo a mensagem deve permanecer confidencial. Lembrando que não há nenhum mecanismo de segurança absolutamente seguro (ALMEIDA e REZENDE, 2012).

A violação da confidencialidade da informação pode ocorrer por modo intencional por meio de ataques, captura de tráfego, engenharia social, entre outros *(hackers)*, bem como de forma não deliberada ou falhas presentes na segurança do serviço prestado.

No caso do VoIP, a confidencialidade preocupa-se com a não intercepção de uma conversa por uma terceira parte não autorizada, como nos ataques do tipo *man-in-the-middle* (MITM).

5.1.2 Integridade

A integridade é o aspecto que se tem preocupação com a confiança que sem pode ter sobre uma informação obtida. Além disto, uma informação é dita íntegra se não sofreu nenhuma alteração entre os momentos de transmissão e recepção.

Desta forma, (BRAUMANN, CAVIN e SCHMID, 2011) define duas categorias de integridade: integridade de fonte e integridade de dados.

A integridade de fonte define-se como que a garantia que uma informação realmente

vem do remetente correto, ou seja, ela não ser alterada para vir de um terceiro não pertencente a comunicação inicial.

A integridade dos dados refere-se à confiabilidade da informação em si, isto é se a informação não foi comprometida em algum momento anterior à leitura pelo destinatário final.

(BRAUMANN, CAVIN e SCHMID, 2011) atribui à integridade três objetivos:

- Impedir que sujeitos externos e não autorizados realizem modificações na informação que está sendo transmitida;

- Impedir que sujeitos externos e autorizados realizem modificações não autorizadas;

- Garantir a legitimidade, veracidade e consistência da informação, esteja ela armazenada, em trânsito ou em processamento.

Tratando de VoIP, a integridade deve garantir que os pacotes de mídia cheguem ao destinatário sem sofrerem nenhum tipo de alterações, sejam elas maliciosas ou não.

Segurança da informação integridade significa ter ao alcance informações confiáveis, de forma correta e dispostas em formato compatível com o seu tipo de utilização, ou seja, informações íntegras. Se a informação sofrer algum tipo de alteração, seja ela de forma errada ou mesmo falsificada ela perde sua eficácia e confiabilidade (ALMEIDA e REZENDE, 2012).

5.1.3 Disponibilidade

Aspecto de segurança da informação que diz que o mesmo deve estar disponível para ser acessada quando solicitada por qualquer pessoa ou sistema que esteja dentro das recomendações de segurança (BRAUMANN, CAVIN e SCHMID, 2011). Isto é, que toda estrutura que permite acesso e transporte da informação deve ser protegida para que não seja modificada.

Em termos de disponibilidade, os tipos de ataque que representam maior ameaça são DoS (*Denial of Service*) e DDoS (*Distributed Denial of Service*), que tem por objetivos principais de danificar ou sobrecarregar sistemas, fazendo com que haja uma “parada de emergência”.

Para o VoIP, disponibilidade significa garantir que o serviço esteja operante para os usuários, evitando qualquer problema resultante provido de um ataque, cujas consequências podem ser perda total ou parcial da comunicação (BRAUMANN, CAVIN e SCHMID, 2011).

A avaliação do desempenho do servidor e rede estabelecida para a comunicação dos dispositivos, será feita por monitoramento de um serviço gratuito chamado Zabbix. Esse serviço será hospedado em um servidor Linux, baseado em uma distribuição *OpenSUSE*.

5.2 Ataques as Redes de Telefonia VoIP

Do mesmo modo que uma rede de computadores necessita de mecanismos de segurança para se proteger das ameaças derivadas de diversas fontes, a tecnologia VoIP também pode sofrer com essas ameaças e precisa dessa mesma segurança.

Na prática, um telefone SIP é um dispositivo IP e como tal também herda os mesmos problemas de segurança recorrentes as redes IP. Telefones e servidores SIP tipicamente contam com implementações de uma série de serviços de rede da camada TCP/IP, incluindo HTTP, TELNET, SNMP, TFTP, UDP, TCP, IP, entre outros que são protocolos base para sustentar os serviços de telefonia IP (ENDLER e COLLIER, 2007).

A infraestrutura que sustenta VoIP pode sofrer ataques denominados de *Deny of Service* (DoS), que tem como principal objetivo interromper o serviço de VoIP. É importante observar que há os ataques de negação de serviço típicos de uma rede IP e os ataques de negação de serviço específicos destinados aos protocolos e aos atributos particulares de VoIP (RIBEIRO, 2011). De acordo (RIBEIRO, 2011), dentre esses ataques, destacam-se:

Distributed Deny of Service (DDoS): se utiliza de programas maliciosos como vírus e *worms* capazes de afetar o funcionamento dos equipamentos de VoIP;

SIP Flooding – Inundação SIP: esse ataque realiza a inundação de envio de mensagens *INVITE* do protocolo SIP ao destino de forma a interromper o desempenho de servidores *proxy* SIP, impossibilitando que os terminais façam ligações;

VoIP Packet Replay Attack – Ataque de Resposta de Pacotes VoIP: consiste na captura e reenvio de pacotes de voz fora da sequência, gerando atraso e degradação na qualidade das chamadas;

QoS Modification Attack – Ataque de Modificação de QoS: modifica os campos de marcação dos pacotes de tempo real que necessitam de prioridade no tráfego da rede anulando o mecanismo de QoS;

VoIP Packet Injection – Injeção de Pacotes VoIP: insere na rede pacotes VoIP falsificados, com falas, ruídos e lacunas nas chamadas ativas (RIBEIRO, 2011).

Um dos casos que afetam o funcionamento de redes de telefonia é ataques ao protocolo SIP, um dos principais responsáveis para o funcionamento correto de uma chamada telefônica utilizando VoIP.

5.3 SIP Invite Flood

Dentro de uma comunicação VoIP o servidor *proxy* é um elemento chave para dispositivos SIP, sendo o responsável pelo processamento de todas as chamadas entre sistemas finais, incluindo telefones SIP, *gateways* de mídia e outros *proxies*. Se o serviço fornecido pelo servidor *proxy* for parcial ou completamente comprometido, toda comunicação VoIP pode ser afetada (ENDLER e COLLIER, 2007).

DAGIUKLAS(2005) explica que um elemento SIP torna-se mais vulnerável se o mesmo necessitar manter seu estado por certo período, como é o caso do processo de INVITE. Um exemplo é quando um UAC (*User Agent Client*) necessita retransmitir um INVITE, caso não obtenha resposta até no máximo em 32s. Durante este período, o UAC mantém seu estado de INVITE, necessitando manter este estado para outros 32s após o encaminhamento das respostas.

Uma ameaça com este potencial consiste no envio de uma imensa quantidade de mensagens SIP INVITE para um servidor *proxy*. A requisição INVITE tem um aspecto computacional importante porque ela é o disparo de uma carga maior de processamento e reserva de recursos num dispositivo SIP. Assim, se um servidor *proxy* puder ser inundado com requisições INVITE, uma interrupção parcial ou total do serviço pode ocorrer (ENDLER e COLLIER, 2007).

Praticamente todos os ataques do tipo DoS e DDoS são especialmente prejudiciais à comunicação VoIP, uma vez que esta é uma aplicação de tempo real e, portanto, qualquer deterioração do serviço ou congestionamento causados por esta classe de ataques causa

impacto significativo ao serviço (THERMOS e TAKANEN, 2007).

A seguir, será abordado diversos cenários com um dos protocolos mais utilizados dentro de uma rede de telefonia VoIP, o protocolo UDP. Testes com ataques com injeção de pacotes UDP, sem a utilização nenhuma de segurança em cima do serviço em questão, para avaliação de seu desempenho. Para iniciar os ataques é preciso saber por onde começar a injeção de pacotes. Será utilizado o NMAP, para verificar quais portas estão disponíveis para início dos ataques.

Para início dos ataques com a injeção de pacotes UDP, abaixo será descrito o funcionamento do ataque e o que ele afeta em caso de ser realizado com sucesso por um ou mais atacantes, utilizando o UDPFLOOD.

5.3.1 UDP Flood

O protocolo de datagrama do usuário (em inglês "*User Datagram Protocol*", UDP) é um protocolo sem sessão, que tem por função o envio de pacotes ou grupos de dados. Os protocolos são escritos de forma a seguir conjuntos de orientações ou normas, que conduzem como os dados serão transmitidos por meio de redes, como a *Internet*. O protocolo UDP pode ser usado para iniciar um ataque de inundação UDP, também conhecido como flood UDP (Andrea Stein).

Ataques *Flooding* tem como objetivo o DoS (*Denial of Service*) ou Negação de Serviço, cujo objetivo principal é consumir recursos e desempenho de rede e de sistemas a fim de causar indisponibilidade total ou parcial de um ou vários serviços (ENDLER e COLLIER, 2007).

O UDP *Flood* consiste na emissão de centenas de milhares de datagramas UDP direcionados para uma porta específica, causando uma “enchente” de pacotes. O efeito é que o alvo terá que colocar recursos “reservas” a disposição do sistema para suprir valiosos recursos (processamento e memória) para tratar os muitos pacotes que chegam, deixando de atender a outras solicitações legítimas naquela e em outras portas.

Dependendo da intensidade do ataque e principalmente se este for realizado de forma distribuída, como no caso de um ataque com maior intensidade DDoS (*Distributed Denial-of-Service*), o excesso de tráfego pode causar congestionamento na rede, aumentando a cadeia de

efeitos colaterais.

Por exemplo, um ataque UDP *Flood* que pode parar completamente a comunicação VoIP (e praticamente a comunicação de qualquer aplicação numa rede IP) é aquele direcionando à porta 53 de host funcionando como servidor DNS. Neste caso, o ataque é conhecido também como DNS *Flood*. O DNS é um serviço crítico para realização de chamadas SIP, portanto seu comprometimento significa a inviabilização de toda comunicação VoIP baseada em SIP dentro do domínio (ALMEIDA e REZENDE, 2012).

Ao realizar os ataques foi utilizado um programa chamado UDP FLOOD, que tem por característica principal o envio de pacotes UDP a um determinado endereço dentro ou fora de uma rede local. Para que o ataque seja efetivado, basta apenas dentro do *software* passar o endereço desejado e a porta de serviço que deseja atacar. No caso de teste foi especificado o endereço local do servidor e a porta 80, que corresponde ao serviço HTTP do servidor Asterisk. A figura 14 mostra o início do envio de pacotes UDP ao destino informado:

Figura 14. Utilização do UDP FLOOD para início dos ataques.

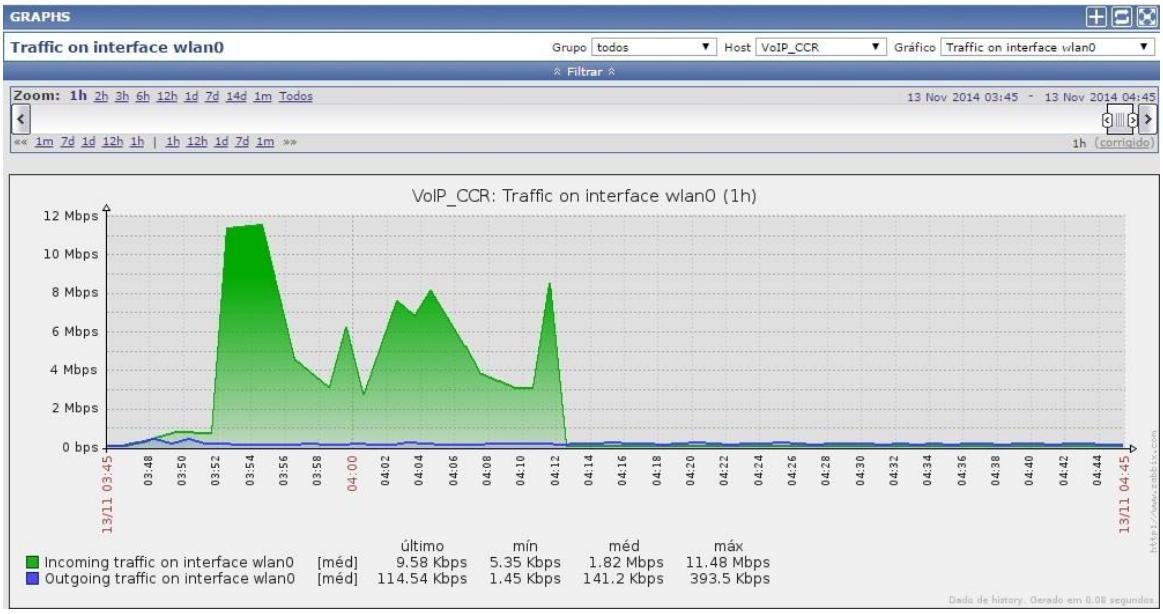
Fonte: UDPFLOOD

Por um período de 10 minutos, o ataque realizou um envio de um pouco mais de 9.000.00 (9 milhões) de pacotes UDP ao destino solicitado.

Conexão dos aparelhos e o serviço para estressar a conexão foram realizados por meio de um roteador sem fio. A figura 15, mostra o desempenho do roteador com relação a ligação

e o ataque de UDP Flood.

Figura 15. Monitoramento da Rede Sem Fio Com Ataque UDP Flood sem a utilização de Firewall.

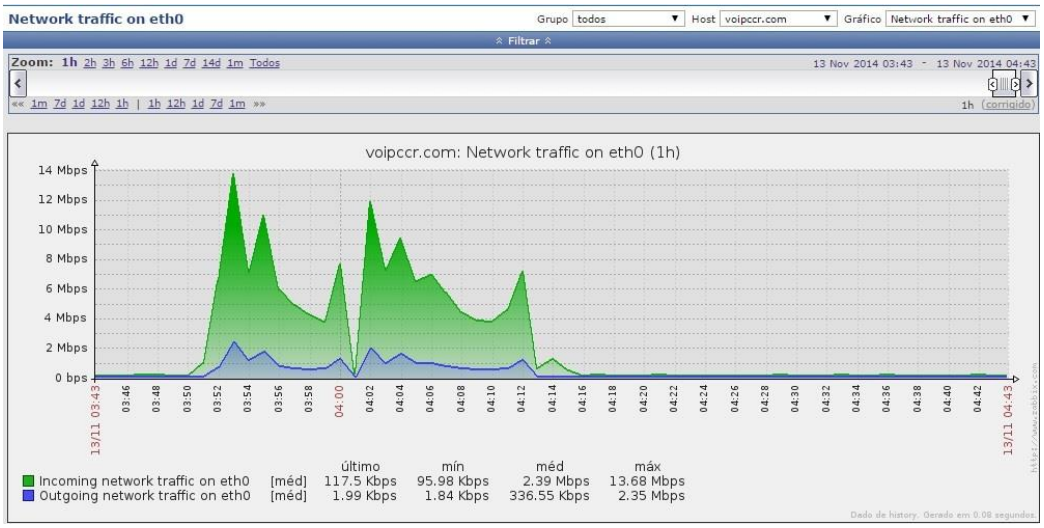


Fonte: Servidor Zabbix

No roteador, a carga de pacotes que foi monitorada durante o período de 10 minutos atingiu um pico de 11 megas por segundo (11Mbps). A entrada de trafego na rede (*Incoming Network Traffic)* atingiu um pico de 11.48 megas por segundo (11.48Mbps), já a saída (*Outgoing Network Traffic)* da rede foi de apenas 393.5Kbytes por segundo (393.5Kbps).

Na Figura 16 é mostrado um gráfico com o monitoramento da rede com a simulação de um ataque realizado com ataque de *UDP Flood*. A simulação ocorre no servidor que hospeda o serviço de telefonia, mas sem nenhum tipo de segurança implementada. Dentro do teste está ocorrendo uma chamada entre dois ramais. Antes do ataque a qualidade da chamada é normal, ouvindo-se claramente a voz e sem nenhum tipo de corte ou interferência. Após o início do ataque, a voz fica metalizada e não se escuta a voz do outro usuário.

Figura 16. Monitoramento da Rede Com Ataque UDP Flood sem a utilização de Firewall.

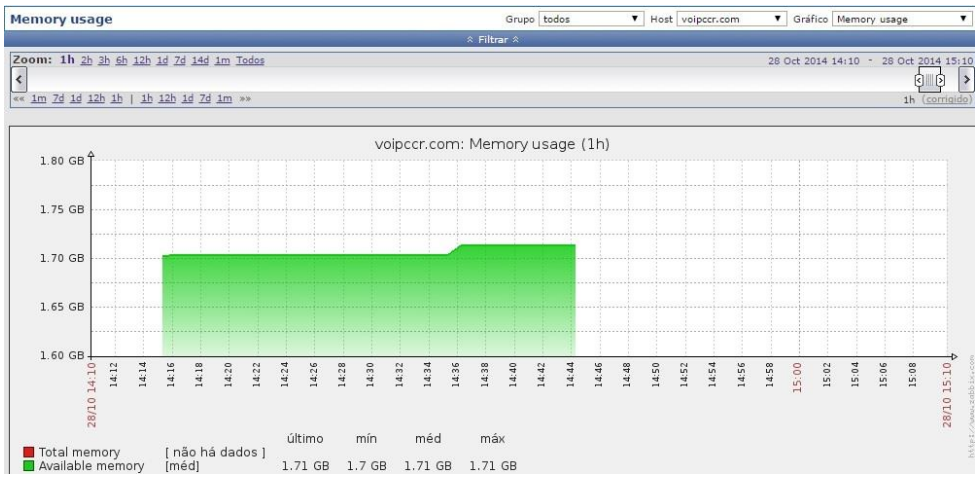


Fonte: Servidor Zabbix

A rede em questão, durante um período de 10 (dez) minutos, sofreu um ataque de *UDP Flood*, gerando uma sobrecarga na rede de aproximadamente 13 megas por segundo (13Mbps). A entrada de tráfego na rede (*Incoming Network Traffic)* atingiu um pico de 13.68 megas por segundo (13.68Mbps), já a saída (*Outgoing Network Traffic)* da rede foi de 2.35 Megabytes por segundo (2.35Mbps). Durante a realização da chamada entre 2 usuários via telefones sem fio (SOFTFONES), a ligação ficou com a voz “metalizada” e um atraso ao enviar e receber a voz do outro usuário.

O desempenho Memória RAM, foi altamente consumido durante o ataque via UDP. Ao tentar realizar outras chamadas durante o teste, as chamadas não chegavam a ser completadas ou se completavam não havia comunicação. O gráfico com o desempenho do servidor está representado logo abaixo, na Figura 17.

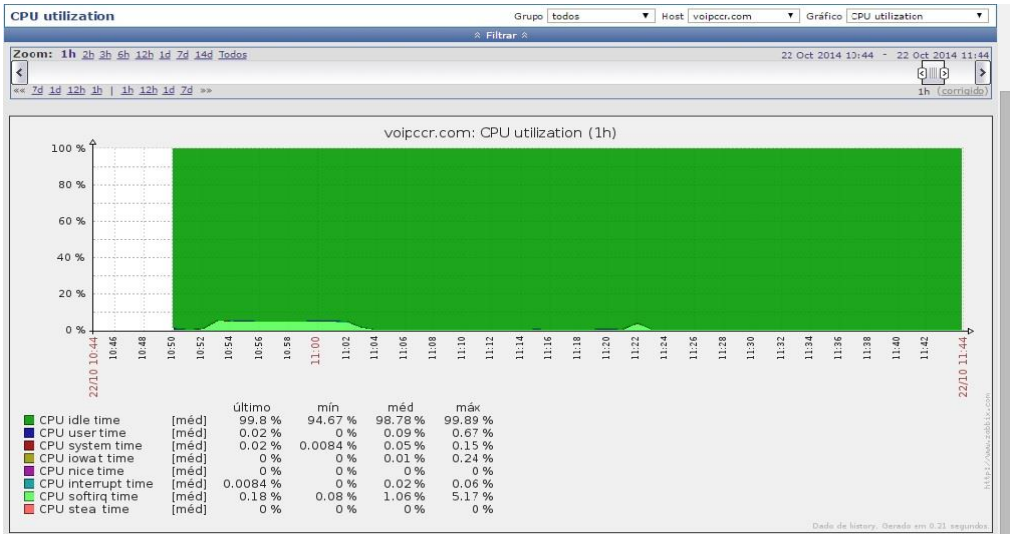
Figura 17. Monitoramento da Memória RAM Com Ataque UDP Flood sem a utilização de Firewall.



Fonte: Servidor Zabbix

Já o desempenho do processador ficou ao máximo durante um período superior a uma hora (1 hora). Uma conexão via SSH que estava sendo executada durante o período de testes foi derrubada. Na Figura 18 é ilustrado o monitoramento da CPU.

Figura 18. Monitoramento da CPU Com Ataque UDP Flood sem a utilização de Firewall.

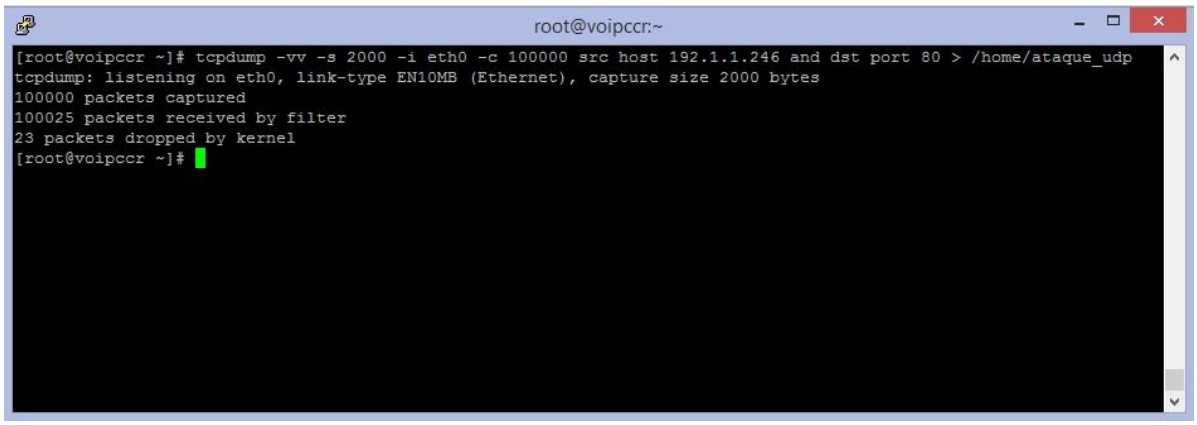


Fonte: Servidor Zabbix

Para uma melhor avaliação dos pacotes que foram enviados durante o ataque ao serviço de telefones, foi utilizado o serviço presente em distribuições *Linux*, chamado TCPDUMP, que tem por utilização, verificar informações de tráfego e pacotes que transitam

dentro da rede. Na figura 19 é mostrado o resultado final de um ataque com o UDPFLOOD:

Figura 19. Resultado final de ataque com pacotes UDP



Fonte: TCPDUMP

Para o monitoramento do TCPDUMP, foi passado um parâmetro para gerar um arquivo de texto simples, pedindo para registrar 100000 (Cem mil pacotes). A quantidade de pacotes recebidas pela interface de rede (eth0) (100025), a quantidade de pacotes capturados 100000 (Cem mil Pacotes) e quantos pacotes o *kernel* do *Linux* descartou apenas (23). O ataque enviou uma grande quantidade de pacotes ao servidor de forma que não houve nenhum tipo de bloqueio, gerando assim um "stress" no desempenho do servidor.

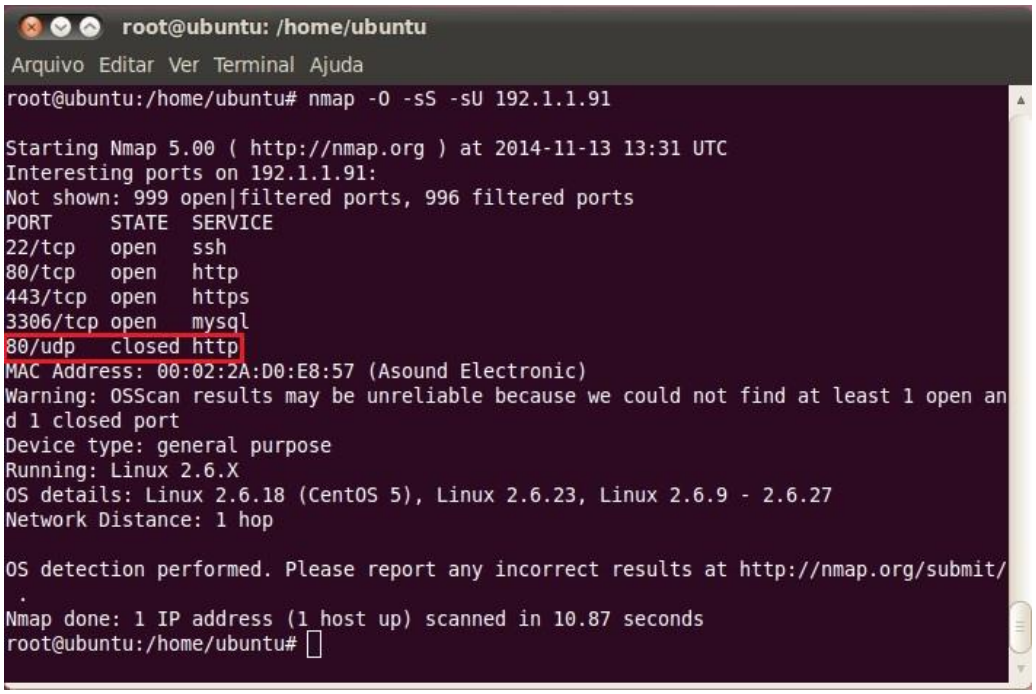
Para que os SOFTFONES conectados à rede *wireless* pudessem realizar as chamadas, foi realizado uma forma de autenticação para cada usuário por meio de um código de 4 dígitos que são utilizados antes de se discar o número destino. Caso o usuário digite o código de forma incorreta, a linha não é liberada e não é possível realizar uma ligação.

5.4 UDP Flood com a utilização de Firewall

Para dar início aos testes de ataque com um *Firewall*, foi refeito todo o processo de verificação desde varredura das portas disponíveis com a utilização do *Nmap*, e caso haja alguma porta disponível realizar o ataque e testar o desempenho de *hardware* e desempenho das ligações durante a realização dos testes.

Na figura 20, é mostrado uma nova varredura de portas e serviços por meio da ferramenta *Nmap*:

Figura 20. Mapeamento Utilizando NMAP a um host alvo com Firewall.

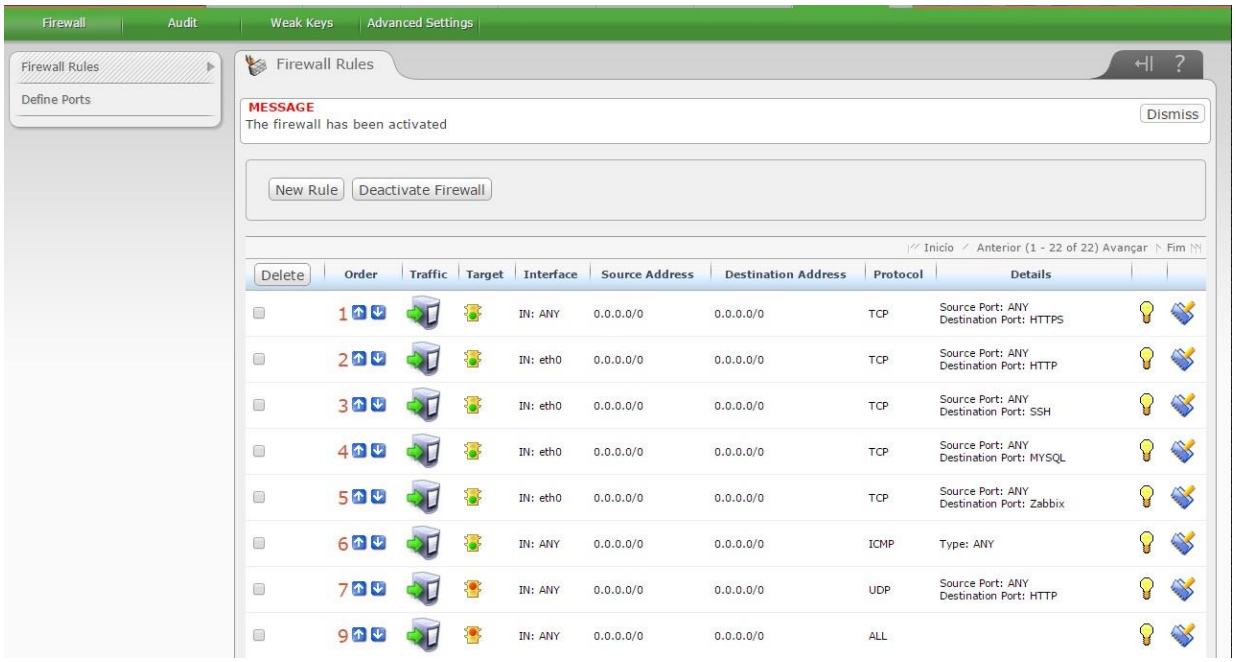


Fonte: NMAP

Com a implementação de um *firewall*, ao realizar um novo mapeamento utilizando NMAP, algumas das portas foram bloqueadas pois não haviam utilização e alguns serviços não estavam sendo utilizados. A porta 80 (HTTP) que foi alvo nos testes realizados anteriormente continua aberta, porém, foi adicionada uma regra a mais a porta 80, onde qualquer pacote UDP, que venha a ser recebido pela placa de rede correspondente, no caso (eth0), seja descartado.

A configuração do *firewall* do serviço de telefonia é feita de forma gráfica com a utilização da ferramenta ELASTIX. O funcionamento do *firewall* afeta a estrutura do *kernel* do sistema operacional, no caso a plataforma é baseada em um sistema *Linux*, conforme escrito acima no item sobre *firewall.* Conforme a figura 21, é mostrado as regras implementadas para o fechamento das portas:

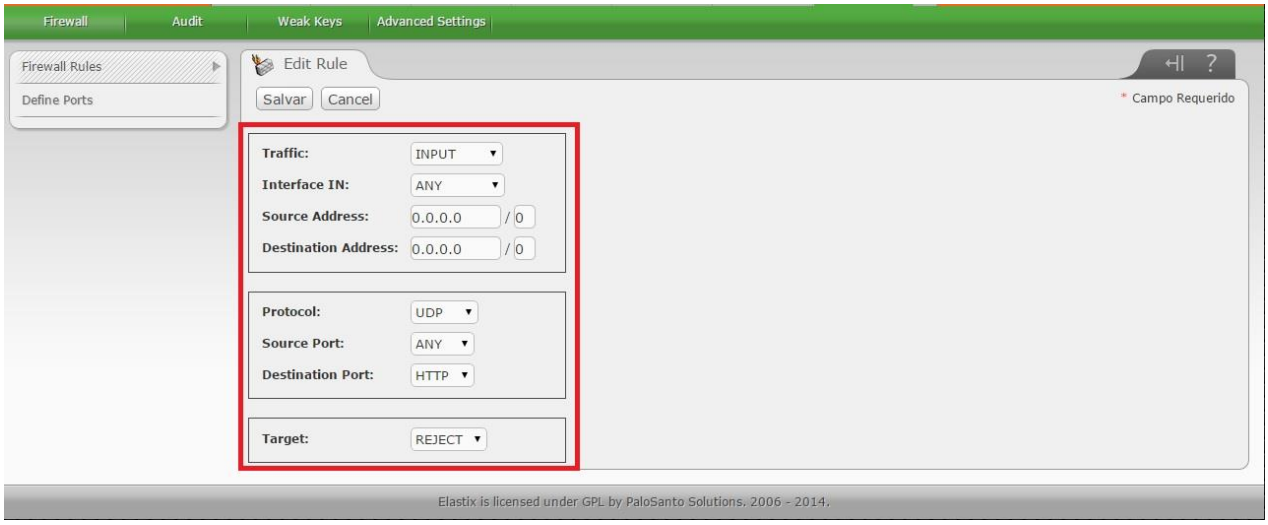
Figura 21. Configuração do Firewall



Fonte: Servidor Elastix

As regras mostradas acima, validam apenas as portas mostradas no mapeamento do *Nmap*. Ela segue uma ordem de liberação de portas apenas a serviços utilizados pelo sistema de telefonia. Ao final das liberações, é criada uma regra onde ela tem por método recusar todo e qualquer tipo de pacote e ou qualquer tipo de protocolo recebido em qualquer outra interface de rede do servidor. A figura 22, mostra a criação da regra para a porta 80 para bloqueio de pacotes UDP:

Figura 22. Configuração da Porta 80 para Bloqueio de Pacotes UDP



Fonte: Servidor Elastix

Como a verificação apontou ainda a porta 80 (HTTP), está aberta, o novo ataque será realizado novamente na mesma porta, porém com uma nova regra implementada. A regra trata as seguintes opções:

Traffic: INPUT – Como a interface de rede vai responder, no caso a entrada de pacotes;

Interface IN: *Ethernet 0* – A placa de rede que recebe a conexão;

Source Address: 0.0.0.0/0 – Recebe qualquer IP, sem restrições de *range*;

Destination Address: 0.0.0.0/0 – Responde a qualquer IP, sem restrições de *range;*

Protocol: UDP – Especifica no caso somente protocolo UDP;

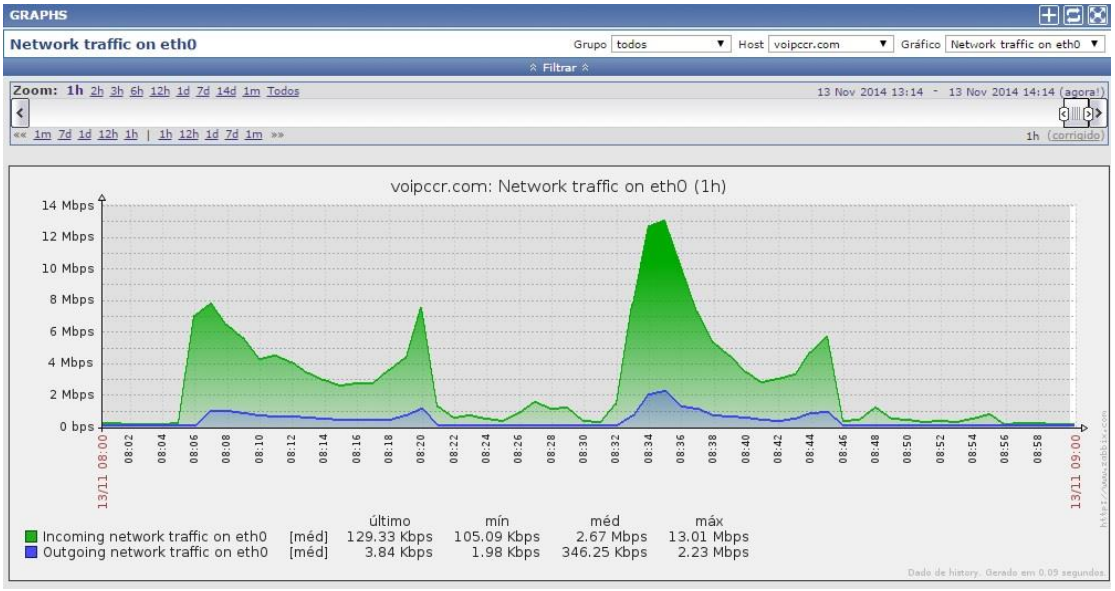
Source Port: ANY – A porta de origem dos pacotes;

Destination Port: HTTP – A porta que recebe as conexões;

Target: Reject – A forma que a regra vai agir sobre os pacotes recebidos. No caso ela vai descartar todos os pacotes UDP recebidos naquela interface.

Na figura 23, é mostrado a utilização e o desempenho da placa de rede do servidor com a utilização do UDP FLOOD e com a regra do *firewall* recusando os pacotes UDP recebidos pela porta 80 (HTTP).

Figura 23. Monitoramento da Placa de Rede do Servidor com Implementação de um Firewall



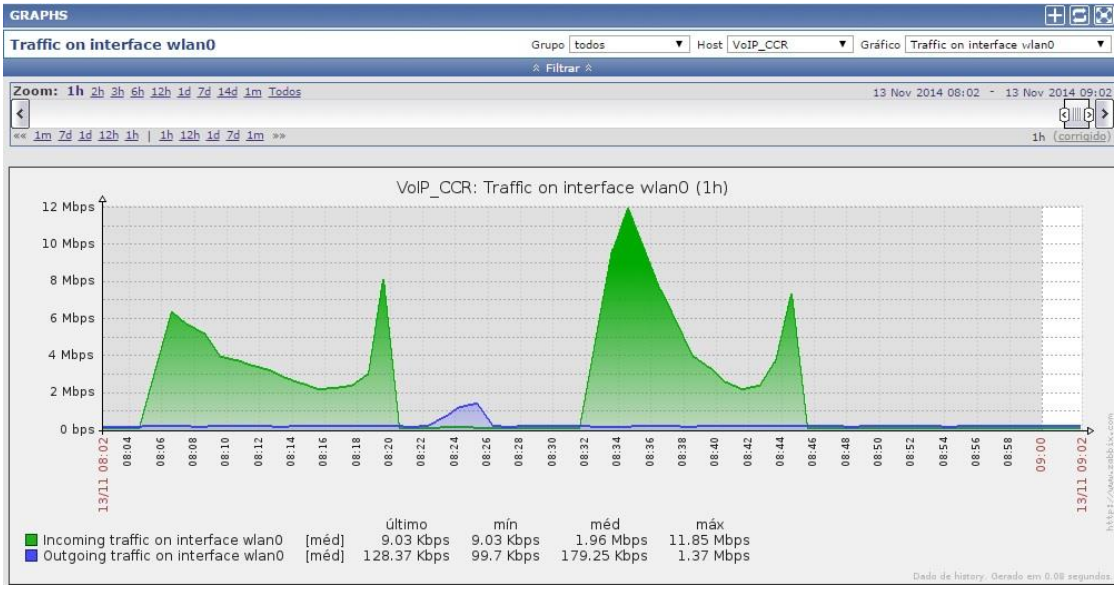
Fonte: Servidor Zabbix

A rede em questão, novamente durante um período de 10 (dez) minutos com o *Firewall* sendo intercalado a cada intervalo de tempo, sofreu um ataque de *UDP Flood*, gerando uma sobrecarga na rede de aproximadamente 13 megas por segundo (13Mbps). A entrada de tráfego na rede (*Incoming Network Traffic)* atingiu um pico de 13.01 megas por segundo (13.01Mbps), já a saída (*Outgoing Network Traffic)* da rede foi de apenas 2.23Mbytes por segundo (2.23Mbps). Durante a realização da chamada entre 2 usuários via telefones (SOFTFONES), a ligação ficou com a voz sofrendo distorções e ouvia-se apenas alguns pedaços da conversa e um atraso ao enviar e receber a voz do outro usuário.

A carga de pacotes recebidas com essa regra implementada pelo *firewall* foi menor em relação ao teste realizado sem nenhum tipo de regra.

O desempenho do roteador é mostrado na figura 24:

Figura 24. Monitoramento da Rede sem Fio do Roteador.

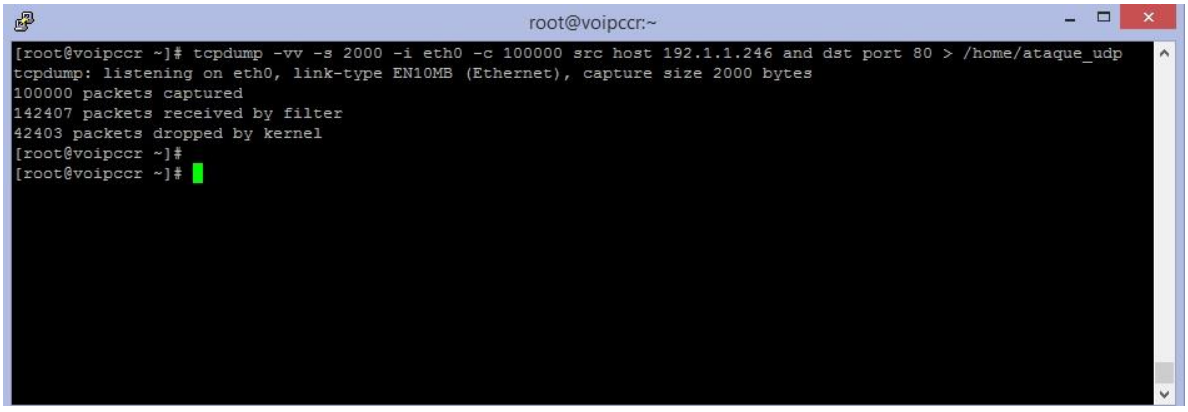


Fonte: Servidor Zabbix

O roteador durante o mesmo período com o *Firewall* sendo intercalado recebeu uma carga aproximadamente 11 megas por segundo (13Mbps). A entrada de tráfego na rede (*Incoming Network Traffic)* chegou a 11.85 megas por segundo (11.85Mbps). A saída (*Outgoing Network Traffic)* da rede foi de apenas 1.37Mbytes por segundo (1.37Mbps). Durante a realização da chamada entre 2 usuários via telefones (SOFTFONES), a ligação ficou com a voz sofrendo distorções e ouvia-se apenas alguns pedaços da conversa e um atraso ao enviar e receber a voz do outro usuário.

Ao ligar o *Firewall*, houve uma diminuição de entrada de pacotes. O TCPDUMP mostra, na figura 25, a quantidade de pacotes descartadas pelo *kernel* do Linux durante o ataque realizado:

Figura 25. Resultado de Monitoramento com TCPDUMP



Fonte: TCPDUMP

Neste cenário, o TCPDUMP, mostra que o ataque realizado ao servidor com um *Firewall* monitorando a porta 80 (HTTP), foi um reduzido em relação ao cenário anterior sem utilização de segurança.

A quantidade de pacotes que foi rejeitada pelo *kernel*, durante o período de ataque foi de 42000 pacotes.

5.5 Resultados e Contribuições

Como resultados deste trabalho, sempre que ao utilizar serviços que tenham como meio de ligação uma rede de computadores, é necessário estar visando a questão de segurança que envolva tanto os usuários quanto o serviço que ficará disponível.

Em vista da realização dos ataques com dois tipos de cenários, foi mostrado de forma prática que nem sempre um único tipo ou regra de segurança pode ser suficiente para evitar danos a um serviço.

São consideradas contribuições deste trabalho, ambientes de estudos acadêmicos para avaliação e desempenho de redes e funcionamento de protocolos em relação a segurança. Empresas que utilizam o VoIP como um fim, devem sempre priorizar a questão de segurança de serviço e de seus clientes.

Esta monografia mostrou apenas uma das diversas formas de se realizar ataques contra algum tipo de rede ou sistema que dependa do mesmo.

CONCLUSÃO

Mesmo a tecnologia VoIP sendo relativamente nova, ela vem sofrendo um grande crescimento, diante do atual sistema telefônico tradicional. Parte das ligações telefônicas hoje em dia passam por caminhos intermediários que utilizam VoIP, ou seja, tem por base de tráfego de dados as redes de *Internet*.

Quando se tem uma estrutura de Telefonia IP, seu objetivo é ter um controle sobre as operações telefônicas, redução de custos, alta confiabilidade e qualidade assim como na RTPC. Ainda existem algumas barreiras técnicas a serem ultrapassadas para obter as mesmas características que tornaram a RPTC tão eficaz.

O VoIP pode ser utilizado por adaptações em redes de telefonias tradicionais, com a utilização de ATAs que estão configurados para receberem conexões de rede e realizar chamadas, mas também pode ser configurado em dispositivos móveis (SOFTFONES) tendo mobilidade sem ficar preso a uma estrutura dentro de residências ou empresas.

Por seu funcionamento ser baseado em protocolos tradicionais de rede, estando conectado em uma rede móvel (3G e 4G) ou até mesmo conexões *wireless*, que estão disponíveis praticamente em diversos pontos, é possível realizar as suas ligações a custo zero de qualquer lugar, dependendo de como o serviço está configurado, ou seja, diminuir o custo com telefonia móvel e/ou fixa.

Uma grande limitação para a utilização de uma estrutura desse porte, ainda é dado pela falta de largura de banda adequada, que temos em utilização atualmente e para transportes de dados em tempo real, acaba gerando uma grande perda de pacotes e, consequentemente, redução da qualidade.

A criação de protocolos padronizados para VoIP, assim como ferramentas de qualidade de serviço e segurança, adéqua o surgimento crescente de produtos, implementações e empresas que fornecem o serviço de telefonia IP.

O VoIP ainda tem alguns desafios a serem batidos, que são compensados pelos benefícios que ela pode trazer ao ambiente doméstico e corporativo. Essa tecnologia veio para mudar as telecomunicações, ocorrendo a tão mencionada convergência de dados e voz, e um gasto reduzido com ligações telefônicas para se preocupar.

Por se tratar de um serviço que funciona sob a rede de computadores, sua segurança deve ser bem estrutura, para que não haja riscos a seus serviços e também a seus usuários. Como a sua principal função é a transmissão de voz, o VoIP precisa ter sua rede e serviços bem configurados, de forma segura para que não tenha problemas e acabe gerando prejuízos a quem utiliza tal plataforma. Como forma de mostrar como uma rede sem segurança pode ser afetada, os testes realizados comprovam que um ataque simples, pode acabar gerando transtornos em uma pequena rede, podendo ser uma empresa ou até mesmo um provedor de serviços VoIP.

Ao aplicar uma pequena regra para que seja evitado tal tipo de ataque, os resultados mostram que houve uma diminuição de pacotes enviados ao servidor que hospeda o serviço, mas ainda houve problemas com o desempenho do mesmo. Ao pensar em estruturas como esta, é necessário priorizar formas de se prevenir os possíveis ataques e ameaças vindas de fora, como *hackers*.

O ataque UDP *Flood* é apenas uma das formas de “estressar” uma rede ou serviço que tenha como base a pilha de protocolos TCP/IP, como por exemplo os serviços de telefonia VoIP. No caso simulado anteriormente, a injeção de pacotes UDP em uma determinada porta, mostrou que se caso não houver uma forma de segurança implementada por mais simples que seja, a carga injetada durante os ataques derrubou chamadas entre usuários e afetou também o desempenho do *hardware* onde o serviço está hospedado.

Com base nos testes efetuados e nas pesquisas de campo, conclui-se que uma implementação a partir de um *Firewall*, controlando o fluxo de pacotes que chegam e saem nas portas onde rodam diversos tipos de serviços, é possível “frear” ataques específicos a um alvo fixo, como uma porta, no caso dos testes a porta 80 (HTTP). Como foi registrado um grande volume de pacotes UDP recebidos nessa porta, o *Firewall* foi implementado para fechar as demais sobressalentes e aumentar a rigidez com relação as portas que se manterão abertas. No caso da porta 80, a liberação foi mantida mas foi especificado para todo pacote UDP vindo de redes de fora, que seja descartado ao chegar na placa de rede. O desempenho do servidor e do serviço ainda sofreram alterações durante a sua utilização, como no caso das chamadas que eram realizadas durante o ataque, houve alterações na qualidade da voz, com uma perda menor de áudio, em relação ao teste anterior.

Conclui-se com os resultados obtidos nesse trabalho que serviços que tenha a sua

plataforma sob rede de *Internet*, seja ela um meio ou um fim para serviço, precisa estar cercado por regras de segurança que visam proteger seus usuários. A *Internet* é um local onde milhares de pessoas utilizam para diversas tarefas, mas há também pessoas que visam gerar prejuízos.

Por fim o trabalho desenvolvido permitiu o desafio, levando ao aprendizado em áreas de infraestrutura, redes de computadores, configuração de servidores, Sistemas Operacionais Linux e a área de telecomunicações onde foi abordado grande parte deste trabalho, com alto valor de crescimento profissional e acadêmico.

Trabalhos Futuros

Como sugestão para trabalhos futuros, estudar a criação de uma segurança para as redes, evitando com que ataques cheguem a atingir diretamente o seu alvo final. Utilização de ferramentas de maior segurança para monitoramentos em tempo de real de trafego de redes e de serviços que estão em funcionamento dentro da rede.

Como tentativa de sanar totalmente o ataque, evitando a sobrecarga no servidor em questão, realizar testes com a mudança de portas de serviços e fechamento das mesmas para avaliar o desempenho de novas regras tratando tipos de ataques ou um teste com a porta 80 (HTTP), mas com ela recusando conexões tanto para o protocolo TCP e UDP.

REFERÊNCIAS

ABREU E SOUZA, Fabiano Nunes Machado; PEREIRA BUENO, Mateus Cunha. **Monitoração de Desempenho de Voz sobre IP**, Disponível em < http://www.teleco.com.br/tutoriais/tutorialmondesvoip/pagina_4.asp > Acessado em: 02/05/2014

ALEN RIBEIRO, Rodiney. **Qualidade de Serviço (QoS): Estudo de Caso de Otimização de Recursos de Rede**, Disponível em < http://www.teleco.com.br/tutoriais/tutorialqosotm/pagina_5.asp > Acessado em: 02/05/2014

ALMEIDA, Juliana. **Transmissão de Multimídia Multidestinatária**, Disponível em < http://www.gta.ufrj.br/grad/01_2/vidconf/rtp.html > Acessado em: 02/05/2014

ARTHAS, Kael. **Tutorial Wireless.** 2004. Disponível em < http://www.babooforum.com.br/idealbb/view.asp?topicID=269602 > Acessado em: 20/04/2014

ATS, Gustavo. **Entenda WEP e WPA, Protocolos de Segurança de Rede Wi-Fi,** Disponível em < http://www.techtudo.com.br/artigos/noticia/2012/02/entenda-wep-e-wpa-protocolos-de-seguranca-de-rede-wi-fi.html > Acessado em: 01/05/2014

BRAUMANN, R., CAVIN, S., SCHMID, S. Voice Over IP – Security and SPIT. Disponível em < http://scholar.googleusercontent.com/scholar?q=cache:uYD9e_DMEZsJ:scholar.google.com/+VoIP+Security+Threats&hl=pt-BR&as_sdt=0 > Acessado em: 18/08/2014

Cisco Systems, **O Que é VoIP? (Voz Sobre IP)**. Disponível em < http://www.sibra.com.br/ArtigoVoip.pdf > Acessado em: 10/03/2014

DAGIUKLAS, Tasos. et al. Low Cost Tools for Secure and Highly Available VoIP Communication Services. SNOCER (2005) 74p.

Definição do termo SNMP, Disponível em < http://pt.kioskea.net/contents/283-o-protocolo-snmp > Acessado em: 05/04/2014

E. MORIMOTO, Carlos. **Guia Prático de Redes**, São Paulo, 2008. 560p.

E. MORIMOTO, Carlos. **Servidores Linux, Guia Prático**, São Paulo, 2008. 746p.

ENGST, Adam; FLEISHMAN, Glenn. **Kit do Iniciante em Redes Sem Fio:** O guia Prático sobre Redes *Wi-Fi* para Windows e Macintosh. 2ª ed.: São Paulo. Ed.: Pearson Makron Books. 2005

ENDLER, D., COLLIER, M. **Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions***: McGraw-Hill, 2007.*

JORDÃO, Fábio. **DDoS: Como Funciona um Ataque Distribuído por Negação de Serviço**, Disponivel em < http://www.tecmundo.com.br/seguranca/10970-ddos-como-funciona-um-ataque-distribuido-por-negacao-de-servico.htm > Acessado em: 18/08/2014

KELLER, Alexandre. **Asterisk na Prática, 2ª ed., vol. 2**. São Paulo, 2011. 332p.

LIMA, André de Almeira; SANTOS, Guilherme Rezende. **VoIP: Segurança da Informação em Telefonia Baseada em SIP**, Disponível em < http://www.teleco.com.br/tutoriais/tutorialvoipsip/default.asp > Acessado em: 02/05/2014

NASCIMENTO, Célia Regina; DOS SANTOS, Dagoberto; MENEZES, Loreno; PERDIGUEIRO, Miguel; FERREIRA, Roberto. **Redes Wi-Fi: O Padrão IEEE 802.11n,** Disponível em < http://www.teleco.com.br/tutoriais/tutorialwifiiee/pagina_4.asp > Acessado em: 20/04/2014

NETO, Urubatan. **Dominando Linux Firewall Iptables**, Rio de Janeiro, 2004. 97p.

NMAP, Disponível em < http://nmap.org/man/pt_BR/ > Acessado em: 05/04/2014

OLIVEIRA, Thiago Vinícius V. **Implementação de Comunicação VOIP em Rede Sem Fio com Utilização de Telefones WLAN-VOIP**, Rio de Janeiro, 2012. 97p.

O Que é Zabbix?, Disponível em < http://www.zabbix.com.br/?gclid=CKDNtd3IzMECFQ8R7AodXmoAQg > Acessado em: 19/08/2014

Padrão IEEE 802.11n, Disponível em < http://manfred.com.br/index.php/artigos/82-padrao-ieee-80211n > Acessado em: 20/04/2014

PAIM, Rodrigo R. **WEP, WPA e EAP**, Disponível em < http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/rodrigo_paim/wep.html > Acessado em 01/05/2014

PEREIRA, Pedro. **Como usar o TCPDUMP**, Disponível em < http://www.pedropereira.net/como-usar-o-tcpdump/ > Acessado em 19/09/2014

Protocolo SNMP, Disponível em < http://www.ti-redes.com/gerenciamento/snmp/intro/ > Acessado em: 05/04/2014

RIBEIRO, Glaucia da Silva. **Voz Sobre IP I: A Convergência de Dados e Voz**, Disponível em < http://www.teleco.com.br/tutoriais/tutorialvoipconv/pagina_4.asp > Acessado em: 02/05/2014

SANTOS PINHEIRO, José Maurício. **Telefonia IP x Voz Sobre IP**, Disponível em < http://www.projetoderedes.com.br/artigos/artigo_telefoniaip_x_voip.php > Acessado em: 06/04/2014

SIÉCOLA, P. C. **VoIPFix: Uma ferramenta para análise e detecção de falhas em sistemas de telefonia IP.** Dissertação (Mestrado em Ciência da Computação) - São Paulo: Universidade de São Paulo, 2010.

STEIN, Andreia. **O que é flood por UDP**, Disponível em < http://www.ehow.com.br/flood-udp-fatos_170675/ > Acessado em: 18/08/2014

Adaptado, TAROUCO, L.; FABRE, M.; GRANVILLE, L.; TAMUSIUNAS, F. **Videoconferência, RNP – Rede Nacional de Pesquisa**, Disponível em < http://eng.registro.br/inoc/SIP_iNOC.pdf > Acessado em: 05/04/2014

TEIXEIRA, Edson Rodrigues Duffles. **Tutoriais: Banda larga e VOIP.** 2005.

Disponível em: < http://www.teleco.com.br/tutoriais/tutorialwimax/default.asp >

Acessado em: 20/04/2014

TCPDUMP, Disponível em < http://www.tcpdump.org/ > Acessado em 19/09/2014

THERMOS, P., TAKANEN, A. ***Securing* VoIP *Networks: Threats, Vulnerabilities, Countermeasures***.Boston: Pearson Education, 2007.

WANDERLEY, Bruno Lima; MORAES DOS SANTOS, Bruno. **Telefonia IP: QoS e Interconexão com a Rede Pública Comutada**, Disponível em < http://www.teleco.com.br/tutoriais/tutorialtelip2/pagina_3.asp > Acessado em: 02/05/2014

VILELA, Roberto Rivelino da Silva; RIBEIRO, Deimar da Silva. **Estudo Comparativo Entre os Protocolos WEP e WPA para Implementação de Segurança em Empresas e Residência.** Disponível em < http://www.sucesumt.org.br/mtdigital/anais/files/RedesWirelessWEP.pdf > Acessado em 01/05/2014