UNIVERSIDADE DA BEIRA INTERIOR
Engenharia

Investigação, desenho e implementação de soluções de comunicação de Voz sobre IP

Euclides Hamilton Miúdo Gaspar

Dissertação para obtenção do Grau de Mestre em
Engenharia Informática
(2º ciclo de estudos)

Orientador: Prof. Doutor Nuno Manuel Garcia
Co-orientador: Prof. Doutor Lúcio Studer Ferreira
Co-orientador: Prof. Doutor Emmanuel Conchon

Covilhã, Junho de 2018

Agradecimentos

Primeiramente agradeço a DEUS e aos meus pais. A DEUS agradeço com duas passagens bíblicas, do livro de Filipenses capítulo 4 versículo 12 – Sei bem o que é passar necessidade e sei o que é andar com fartura. Aprendi o mistério de viver feliz em todo lugar e em qualquer situação, esteja bem alimentado, ou mesmo com fome, possuindo fartura, ou passando privações. Versículo 13 – Tudo posso naquele que me fortalece. Aos meus pais Mendes Lourenço Gaspar e Ana Maria Irene Miúdo, agradeço pela educação, amor, apoio incondicional amo-vos acima de tudo e todos.

Agradeço também aos meus irmãos Aires, Valéria, Eliane, Tximen, Melga, Emanuel, Dalva, primos, amigos e especialmente a minha namorada pelo apoio, amizade e amor, de igual modo.

Ao meu Orientador Prof. Nuno Manuel Garcia, pela ajuda e pelo o apoio concedido, disponibilidade e pelos conhecimentos partilhados durante a concretização desta dissertação. Também ao pessoal do laboratório ALLAB que sempre deram um contributo para a realização deste trabalho especialmente ao Henriques Zacarias, Virginie Felizardo, Professor Nuno Pombo e os demais colegas do ALLAB. Sem esquecer os meus colegas e amigos João Silva e Bárbara Matos que sempre se disponibilizaram em ajudar.

Resumo

O crescimento de implementação de soluções de Voz sobre o protocolo de Internet (VoIP) é notável, muitas são as empresas e utilizadores comuns que fazem uso dessa tecnologia, por ser de baixo custo e permitir diversos recursos. No entanto, este crescimento é acompanhado de fatores que comprometem a qualidade de serviço. Está dissertação descreve os elementos importantes para a implementação de uma solução VoIP, desde a segurança, a configuração da rede tendo atenção a tecnologia VoIP, alguns equipamentos, Softwares e provedores de serviço. Estes aspetos foram detalhados em alguns fatores como funcionalidades, suportes e entre outros. Por fim são apresentados o desenho e a implementação de uma solução VoIP, sendo estes os objetivos principais desta dissertação.

Palavras-chave

Qualidade de serviço, segurança, implementação de soluções VoIP.

Abstract

The growth of the implementation of voice over Internet Protocol (VoIP) solutions has been remarkable, and many companies and users choose to use this technology, because of its low implementation and maintenance costs, its versatility in the use of different resources. Nevertheless, its growth is also matched by factors that compromise the quality of the service.

This dissertation describes the elements that are important to the deployment of a VoIP solution, ranging from security, to network configuration, equipment requirements, software and service providers. These elements were detailed and studied regarding aspects such as functionality, support and other criteria. Finally, the design and implementation of a VoIP solution is presented as the major goal of this dissertation research.

Keywords

Service quality, Security, implementation of VoIP solutions.

Índice

Lista de Figuras

Lista de Tabelas

Acrónimos

AEC	*Acoustic Echo Canceller*
AGC	*Automatic Gain Control*
ALSA	*Advenced* Linux *Sound Architecture*
ATA	*Analog Telephone Adapter*
BYOD	*Bring Your Own Device*
CFCA	*Comunication Fraud Control Association*
CRM	*Customer Relationship Management*
CUCM	Cisco *Unified Communications Manager*
FEC	*Forward error correction*
GPL	*General Public License*
GPLv2	*General Public License version 2*
GSM	Global System for Mobile
IAX	*Inter-Asterisk eXchange*
IM	*Instant Messaging*
IP	Internet *Protocol*
ISDN	*Integrated* Service Digital *Network*
IVR	*Interactive Voice Response*
MDC	*Multiple descriptions coding*
MOS	*Mean Opinion Score*
NAT	*Network Address Translation*
NPESQ	*New Perceptual Evaluation of Speech Quality*
NS	*Noise Suppressor*
OSS	*Open Sound System*
PBX	*Private Branch Exchange*
PLC	*Packet Loss Concealment*
PSTN	*Public Switched Telephone Network*
QoS	*Quality of Service*
RAS	*Remote Access Service*

RTP	*Real-time Transport Protocol*
SCCP	*Skinny Client Control Protocol*
SIP	*Session Initation Protocol*
SRTP	*Secury Real-time Transport Protocol*
STUN	Session Traversal Utilities for NAT
TLS	*Transport Layer Security*
UA	*User Agent*
UC	*Unified Communications*
VoIP	*Voice Over* Internet *Protocol*
ZRTP	Zimmermann *Real-time Transport Protocol*

Capítulo 1

1 Introdução

O VoIP (Voz Sobre Protocolo de Internet) é uma tecnologia que permite fazer chamadas de voz operando sobre uma conexão de Internet de banda larga. A sua utilização vem crescendo e existem fatores que demonstram que essa tecnologia vai dominar completamente o público de redes telefónicas comutadas (PSTN) e redes móveis [1]. Entretanto a qualidade de serviço (QoS) pode ser comprometida, porque a transmissão de voz é feita através de protocolo IP (*Internet Protocol*), este tem características que podem comprometer a segurança e integridade da transmissão, o que faz com que sejam feitos estudos e consequentes descobertas de soluções que preservam a qualidade de serviço nas redes IP, especificamente no VoIP, mas também lembrando que ainda assim, a possibilidade de erros não pode ser descartada na prática [2].

No VoIP, os dados de voz são agrupados em pacotes RTP e enviados de um utilizador para outro. O serviço é baseado no padrão ITU-T H.323, de modo que a sinalização seja feita em conformidade com os protocolos H.255.0 e H.245. Estes protocolos demoram algum tempo para serem implementados e executados. Como consequência, também há demora para estabelecer uma conexão, isso motivou os desenvolvedores a encontrar um protocolo de sinalização mais simples e compacto, este protocolo é o *Session Initation Protocol* (SIP) [2].

O VoIP é um processo de transmissão em tempo real, cujo o sinal de transmissão na rede VoIP é em formato digital. O sinal de voz precisa ser digitalizado (processo que resulta na obtenção de sequências binárias pela transformação de um sinal analógico para digital) e codificado (processo de representação dos valores 0 e 1 numa sequência de *bits*) antes do pacote, ou seja, primeiro o sinal de voz é convertido de um sinal analógico para digital, depois o sinal digital é codificado dentro da tecnologia apropriada de codificação e compressão, como mostra a [3].

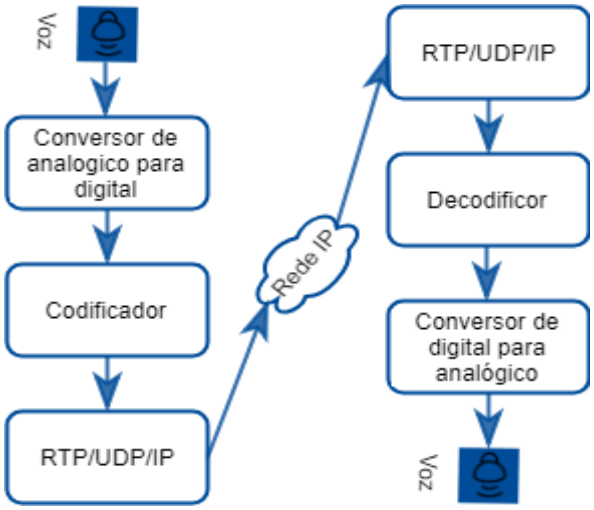

Figura 1.1: Princípio básico de transmissão.

1.1 Objetivo

O principal objetivo deste trabalho é o estudo, o desenho e a implementação de uma solução de comunicação de VoIP. Para isso será simulada uma solução VoIP baseada em equipamentos reais.

Os objetivos principais previstos no plano de trabalho são os seguintes:

- O estudo da plataforma de comunicação;
- O estudo e a análise dos protocolos utilizados pela tecnologia;
- A análise de requisitos de uma solução deste tipo;
- O desenho e a implementação de uma solução real;
- Os testes e a avaliação da solução.

1.2 Motivação

O serviço VoIP tem crescido muito no que concerne a utilização, tanto a nível empresarial, como utilizadores particulares. A implementação do VoIP é de extrema importância por ser uma tecnologia de comunicação de baixo custo tanto em chamadas locais como internacionais. O VoIP é uma tecnologia versátil, que possibilita fazer chamadas em qualquer dispositivo, que suporta a comunicação de voz e que esteja ligado a rede, a adaptação de muitos serviços como VoIP *Trunking* que possibilita a comunicação com outras redes como a PSTN. Essas são algumas das vantagens da tecnologia VoIP.

A comunicação VoIP é feita através da Internet, que é geralmente um canal de comunicação inseguro, o que compromete a segurança e privacidade da rede VoIP, por isso é importante um estudo sobre os protocolos a serem utilizados numa rede VoIP, também a sua estrutura e os equipamentos a serem utilizados de forma a identificar eventuais falhas de segurança.

1.3 Organização

Esta dissertação está organizada em 5 capítulos que mostram subsequentemente o processo de investigação desenvolvido. No presente capítulo é feita uma abordagem introdutória sobre a tecnologia VoIP, os objetivos e a motivação desta. Os seguintes capítulos encontram-se organizados da seguinte forma:

- **Capítulo 2 – Estado da arte:** neste capítulo são descritas todas as tecnologias abordadas ao longo da dissertação. Inicialmente são apresentados alguns protocolos utilizados na tecnologia VoIP, a QoS, a fraude e segurança VoIP, alguns dos sistemas e dispositivos mais utilizados no mercado numa solução VoIP;
- **Capítulo 3 – Implementação:** tem por objetivo abordar às técnicas utilizadas, os equipamentos e as configurações feitas para a implementação da solução proposta.
- **Capítulo 4 – Resultados**: este capítulo apresenta os resultados obtidos das configurações feitas nos servidores e nos Softphones, assim como teste de chamadas e as análises destes resultados
- **Capítulo 5 – Conclusão e Trabalhos e futuros**: referente as conclusões do trabalho desenvolvido e propostas para trabalhos futuros.

Capítulo 2

2 Estado da Arte

A tecnologia de Voz sobre o protocolo de Internet, cresce cada vez mais a nível de implementação, sendo a flexibilidade e a redução de custos os fatores fundamentais que levam as empresas a fazer a implementação ou migração para a tecnologia VoIP [4]. Com a implementação do VoIP podem surgir alguns problemas, de segurança, sobrecarga na rede (por consequência funcionamento indevido dos equipamentos), fraudes e entre outros. Este capítulo apresenta alguns dos protocolos frequentemente utilizados na tecnologia, CODECs, os fatores que comprometem a qualidade de serviço e soluções implementadas para solucionar estes problemas, assim como alguns sistemas para VoIP tais como, Softwares para PBX IP e Softwares para telefones IP nomeadamente os Softphones. Também é feita uma abordagem sobre os fornecedores de serviço VoIP.

2.1 Protocolos

O VoIP sendo uma tecnologia baseada em protocolo de Internet, utiliza alguns protocolos para fazer a conexão apropriada pela rede, além de ser possível manter a comunicação com outros tipos de serviços de telefonia como PSTN (*Public Switched Telephone Network*), PBX (Private Branch Exchange) e entre outros.

2.2 Protocolos de Sinalização

Esta subsessão aborda os dois protocolos mais utilizados para a sinalização em redes baseadas em IP [5], o H.323 e o SIP, ambos os protocolos foram desenvolvidos para controlo e sinalização de chamadas, sendo ainda assim o SIP mais popular entre os dois [5]. Devido à sua flexibilidade de implementação e à compatibilidade com novos CODECs [5].

2.2.1 Protocolo SIP

O SIP é um protocolo de sinalização de comunicação multimédia que utiliza técnicas de controlo em redes IP para trabalhar com a tecnologia de rede de transmissão de voz e vídeo [6].

Para lidar com as sessões (coleção de comunicação) multimédia na Internet o SIP envolve vários elementos como o agente do utilizador, que pode ser tanto do cliente como do servidor. O agente de utilizador do cliente é responsável por iniciar, registar, convidar e cancelar pedidos. Enquanto, que o agente de utilizador do servidor processa essa solicitação e responde diretamente ou redireciona ao cliente correspondente. O servidor de registo mantém uma base de dados que contém locais e propriedades de *User Agent* (UA). O servidor proxy recebe pedidos dos clientes e encaminha-os para o recetor correspondente, diretamente ou através de outro servidor que esteja próximo da localização atual do recetor [7].

- **Operações básicas SIP**

Para iniciar uma chamada baseada em SIP, o emissor, primeiro solicita o registo num servidor VoIP apropriado. O servidor VoIP atua como um *gateway* para encaminhar o pedido do emissor para o recetor correspondente. O fluxo do cenário de configuração na Figura 2.1, na qual o utilizador "A" solicita o estabelecimento da sessão VoIP com o utilizador "B". Inicialmente, o utilizador "A" (emissor) envia um convite para o utilizador "B" através de um servidor proxy. O convite contém determinadas informações, como linha de pedido, de, para, contacto e identificação de chamadas, o que ajuda o servidor proxy intermediário a autenticar o convite recebido e encaminhar um *Invited regenerated* para o recetor correspondente. O utilizador "B" (recetor) recebe um *INVITE* do servidor proxy e responde com um OK, se o utilizador que recebe a chamada do emissor estiver disposto a falar. O utilizador "A" (emissor) recebe uma resposta do utilizador "B" (recetor) e envia um ACK, que garante que utilizador "A" também esteja disposto a falar. Assim as chamadas de VoIP são estabelecidas entre ambas as

entidades. Para encerrar a sessão, o *BYE* é enviado por um utilizador e a chamada será encerrada após a receção do OK.

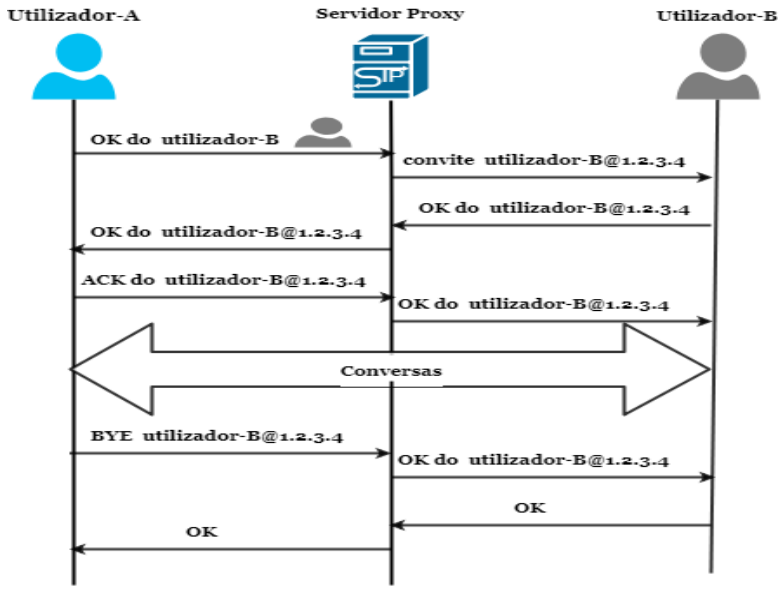

Figura 2.1: Chamada baseada em SIP

- **Mensagens SIP**

No SIP existem dois tipos de mensagens:

- Mensagem de pedido SIP, as mensagens mais utilizadas são: INVITE, ACK, BYE, REGISTER, CANCEL, OPTIONS.

- Mensagens de resposta SIP, estas são numeradas, onde o primeiro dígito em cada número de resposta indica o tipo de resposta. Os tipos de respostas são os seguintes:

- 1xx - resposta de informação, por exemplo, 180 toque;
- 2xx – respostas bem-sucedidas, por exemplo, 200 OK;
- 3xx-resposta de redireccionamento, por exemplo, 302 movido temporariamente;
- 4xx – solicitar resposta de falha, por exemplo, 402 proibido;

- 5xx-resposta de falha do servidor, por exemplo, 504 tempo limite de *gateway*;
- 6xx-respostas globais de falha, por exemplo, 600 ocupado em todo lugar.

A qualidade do SIP depende do sistema de implementação SIP que é utilizado e do nível do suporte que o sistema de rede oferece para os serviços da camada de aplicação [8].

O SIP possui algumas vulnerabilidades que por consequência são responsáveis pela maioria dos ataques VoIP. O SIP é vulnerável a vários ataques como espionagem, interrupção intencional, interceção, modificação e interrupção involuntária. A principal causa destes ataques é devido ao mecanismo de autenticação utilizado na fase de consolidação da sessão. Como solução para esse problema os autores Ubaid Ur Rehman e Abdul Ghafoor Abbasi [7] propõem utilizar o conceito de *Single Sign-On* utilizando um *token* criptográfico para a autentificação da tecnologia VoIP, afirmando que esta técnica garante um método de autentificação eficiente e forte.

2.2.2 H.323

O H.323 é um aglomerado de protocolos que são interligados para garantir três tarefas principais - a sinalização, a negociação dos *Encoding/Decoding* (CODECs) e o transporte de dados VoIP. Este protocolo garante o controlo sobre a utilização dos recursos da rede [9].

Este aglomerado de protocolos é composto pelo protocolo H.245 que é responsável por negociar a abertura, a utilização de canais e as configurações da comunicação VoIP. O protocolo Q.931 que fornece sinalização e estabelecimento de chamadas, protocolo *Remote Access Service* (RAS) utilizado pelo terminal para comunicar com o *gatekeeper* [9]. O protocolo H.235 define a segurança dentro do protocolo H.323 [10].

2.2.3 Media *gateway* control Protocol (MGCP)

O Protocolo MGCP comumente conhecido como H.248, é um protocolo padrão para trabalhar com a sinalização e a gestão das sessões necessárias durante uma conferência multimédia. Isso acontece quando os dispositivos de controlo de chamada utilizam um protocolo de texto simples, o MGCP, para administrar o *gateway* de telefonia IP, tendo como vantagens a criação de uma gestão de *gateway* centralizada e as soluções de telefonia em larga escala [11].

O estado de cada porta individual no *gateway* é conhecido e controlado com o protocolo pelo controlador de chamadas, permitindo o controlo completo do plano de discagem e permite fornecer controlo das portas de conexões da rede telefónica pública comutada (PSTN), PBX, sistema de correio de voz, telefones POTS entre outros [11].

2.2.4 Skinny client control protocol (SCCP)

É um protocolo VoIP proprietário da Cisco, que fornece sinalização entre o *Cisco Unified* e os telefones Cisco IP. Esse protocolo tem o propósito de permitir que numa rede com um pequeno número de clientes comuniquem com o sistema VoIP baseado no protocolo H.323, colocando a maioria dos recursos necessários de processamento H.323 num dispositivo intermediário chamado *CallManager*. O cliente e o administrador de chamadas utilizam um conjunto de mensagens simples SCCP, para comunicar entre si por meio do protocolo TCP/IP, também utilizam um proxy para a sinalização H.225, H.245 e os protocolos RTP/UDP/IP para áudio [10].

2.2.5 Comparação entre os protocolos SIP e H.323

Segundo Rakesh Arora [12], os proponentes do SIP afirmam que o protocolo H.323 foi projetado com a sinalização ATM e *Integrated* Service Digital *Network* (ISDN), sendo assim afirmam que é um protocolo inadequado para controlar os sistemas de voz sobre IP.

Também os autores Ala' Aburumman, Wei Jye Seo, Christian Esposito, Aniello Castiglione ,Rafiqul Islam and Kim-Kwang Raymond Choo [5] referiram que,

os protocolos SIP e H.323 são dos mais populares para tecnologia VoIP, sendo o SIP mais popular entre os dois, talvez devido a sua flexibilidade e relativa simplicidade, a Tabela 2.1 mostra a comparação entre o protocolo SIP e H.323.

Tabela 2.1: Comparação entre SIP e H.323.

H.323	SIP
Protocolo complexo	Comparativamente mais simples
Representação binária para mensagens	Representação textual
Requer total compatibilidade com versões anteriores	Não requer total compatibilidade com versões anteriores
Pouco modular	Muito modular
Pouco escalável	Altamente escalável
Sinalização complexa	Sinalização simples
Grande parte do mercado	Apoiado pelo IETF
Centenas de elementos	Apenas 37 cabeçalhos
A deteção de *loop* é difícil	A deteção de *loop* é comparativamente fácil

2.3 Protocolo de multimédia para VoIP

2.3.1 Real Time Protocol (RTP)

O VoIP tornou a utilização frequente do RTP como o seu protocolo de multimédia que apresenta sessões multimédia sobre rede baseada em IP, por fazer o transporte de media em tempo real [13].

O RTP apresenta muitas fragilidades, como por exemplo, ataques de inundações de media que causam inconsistência na transmissão de media, o que degrada a qualidade de serviço e aumenta o consumo desnecessário de

recursos em servidores. Como solução a este problema os autores G. Vennila e M.S.K Manikandan [13] propõem a projeção de um sistema de segurança VoIP com a técnica especifica para ataques de inundações RTP, técnica denominada PIS.

2.4 Qualidade de serviço (QoS)

A segurança das chamadas é um dos principais objetivos que compõem serviço com QoS reconhecida, fazendo com que a comunicação e a eficácia do mecanismo de segurança sejam muito importantes. A qualidade de voz é afetada por uma diversidade de fatores, como a perda de pacotes, tremulação e latência. No VoIP, ter uma qualidade de serviço significa falar e ouvir de uma forma clara e contínua, sem ruido e sem demora [14]. Para obter uma comunicação VoIP com qualidade, é preciso minimizar o atraso, a perda de pacotes e o jitter. A QoS pode ser calculada com base no jitter, na latência e na percentagem de perdas de pacotes. A latência é medida pelo tempo que um pacote leva a ser enviado de uma pessoa "A" que fala com uma pessoa "B". A perda de pacotes afeta os pacotes que não conseguem alcançar outro lado, portanto, estes pacotes são considerados perdidos na rede e são interpretados como um erro de transmissão. O jitter é definido como uma elevada variação do tempo de chegada entre pacotes, no caso do VoIP, o jitter é causado pelo atraso na chegada dos pacotes causado pelos routers que estão no caminho de transmissão, alterando o caminho dos vários pacotes, por *firewalls* e por outros fatores [14]. As técnicas de codificação de voz também são um dos fatores que afetam a compreensão de voz na rede VoIP [3].

2.5 Fatores que afetam a qualidade do sinal

A qualidade da voz em sistemas de comunicação é influenciada por muitos fatores, como atraso de pacotes, jitter, perda de pacotes, tipo e quantidade da compressão da voz. Por causa destes fatores de distorção, o sinal de voz na rede VoIP pode perder qualidade. Essas questões de degradação precisam de ser analisadas com atenção para a uma implementação bem sucedida do VoIP [15].

2.5.1 Delay

É o tempo que a voz leva para chegar do falante ao ouvinte. O atraso de ida e volta é a soma de dois atrasos unidirecionais que ocorrem na chamada do utilizador. No sistema VoIP, o atraso de propagação também é afetado por dois atrasos adicionais, ou seja, o atraso de empacotamento e o tempo necessário para propagar os pacotes através da rede [15]. Isso varia o atraso de propagação durante a comunicação. De acordo com a recomendação G.14 da ITU-T, o atraso unidirecional entre 150 e 400 ms pode ser aceitável com alguma distorção tolerável. Tabela 2.1 descreve o atraso de acordo com a satisfação do utilizador [15].

Tabela 2.2: Limites de atraso unidirecional de ponta a ponta.

Intervalo do atraso	Descrição
0-150	Tolerável para a maioria das soluções
150-400	Tolerável desde que o utilizador tenha conhecimento do impacto
Acima de 400	Intolerável para fins de planeamento de rede

A tecnologia VoIP transmite tráfego em tempo real, consequentemente a rede de comunicação em VoIP é mais sensível a atrasos [16]. O VoIP é extremamente vulnerável às condições da rede e a qualidade de uma chamada pode degradar-se se houver atrasos. Como solução os autores Cristian Olariu, martin Zuber, Christina Thorpe [17] propuseram um esquema de fila com base em atrasos de pacotes, dando prioridade às chamadas VoIP feitas através de *Software Defined Network* (SDN).

2.5.2 Jitter

No sistema VoIP, o processo de comunicação da fonte para os destinos é feito através de pequenas mensagens encapsuladas em pacotes de dados. Estes pacotes passam por alguns atrasos para chegar ao destino. A variação dos atrasos é denominada *jitter*, que sendo alto afeta a qualidade de serviço

(QoS) prestado, resultando em alguns sons indevidos por causa da perda de pacotes. Uma das formas de minimizar o efeito do *jitter* pode ser o uso de *buffers* de *jitter* [3].

2.5.3 Problema de compressão de voz

Um dos componentes necessários para o sistema VoIP é a compressão/descompressão, uma vez que a largura de banda da rede depende do método de compressão para suportar o número máximo de utilizadores [15]. Os CODEC de voz são muito importantes para o processamento de voz em redes IP, são utilizados para codificar as amostras de voz de um pequeno número de bits. A chamada é estabelecida entre os terminais utilizando os protocolos de sinalização quando ambos os utilizadores concordam com a escolha do CODEC a ser utilizado para a codificação/decodificação de voz. No sistema VoIP existe uma lista de vários CODECs capazes de funcionar na rede, estes CODECs podem ser de alta taxa de bits ou de baixa taxa de bits [15].

2.5.4 Técnicas de codificação (CODECs)

O primeiro passo para a comunicação de voz é a aplicação de um CODEC de voz, cujas as funções primárias são fazer a conversão de sinal de voz analógico/digital e a compressão digital, com a finalidade de obtenção de menor fluxo de bits possível após a conversão sem degradar a qualidade do sinal. Várias técnicas de codificação foram desenvolvidas e padronizadas pela ITU-T. A Tabela 2.1 mostra alguns dos CODECs padrão do ITU-T frequentemente utilizados e lista seus atributos [18].

Tabela 2.3: Alguns CODECs padrão do ITU-T.

CODEC	Taxa de bits (kbps)	Tamanho amostra (Bytes)	Pacotes por segundo	Tamanho da carga útil (bytes)
G.711	64	80	50	160
G.723.1	6,3	24	34	20
G.726.A	32	20	34	80
GSM	13,2	20	50	33

A codificação de voz é utilizada em VoIP para reduzir a taxa de bits de transmissão. Existem padrões de codificação de fala de banda estreita e de banda larga e são utilizados para evitar que existam perdas de pacotes. É importante que se tenha um esquema de otimização para recuperação de perdas de pacotes de acordo com condições de instabilidade da rede [19].

CODECs como G.711 (ITU-T, 1988), G.726 (ITU-T, 1990), G.728 (ITU-T, 1992), G.729 (ITU-T, 2007).), G.723.1 (ITU-T, 2006) e AMR (*Adaptive Multi-Rate*) (3GPP, 2001) são muito utilizados na comunicação de voz de banda estreita, com um limite de 200Hz a 3400Hz e amostrado a uma taxa de 8kHz [19].

A codificação de voz de banda larga tnuma extensão de alta frequência de 3400 a 7000 Hz, o que melhora a clareza e simplicidade da fala. Os CODECs de voz de banda larga G.722 (ITU-T, 1988) com 48, 56 e 64 kb/s e o CODEC G.722.1 (ITU-T, 2005) com 24 e 32 kb/s não são apropriados para o VoIP por causa das suas altas taxas [19].

O CODEC AMR espelha a nova geração de algoritmos de codificação desenvolvidos para funcionar com canais de transportes ambíguos, a maleabilidade nos requisitos de largura de banda e a tolerância de erros de

bits de AMR e CODECs não têm apenas benefícios para ligações sem fios, mas também são necessários para aplicativos VoIP [3].

Entre os vários CODECs existe ainda o AMR-WB (*Adaptive Multi-Rate Wideband*), padronizado para aplicações de comunicação de voz de banda larga, pelo 3GPP (3GPP, 2001) e ITU-T (ITU -T,2003), para aplicações de comunicação de voz de banda larga, pela primeira vez o mesmo CODEC foi utilizado para serviços de rede sem fios e de redes cabladas, eliminando a utilização de transcodificação e simplifica a implementação de aplicativos e serviços de voz de banda larga numa vasta gama de sistemas e plataformas de comunicação [19].

Os autores Z. Li, S. Zhao, J. Wang e J. Kuang [19] compararam o desempenho de várias técnicas *Forward error correction* (FEC) e *Multiple descriptions coding* (MDC) para o CODEC AMR-WB de forma analítica e experimental, e obtiveram resultados de configurações vantajosas tanto para o FEC como o MDC para o CODEC AMR-WB e propuseram um sistema de otimização de recuperação de perdas de pacotes de acordo com as condições da rede.

Outra pesquisa e simulação foi feita pelos autores Subhabrata Dhar e Sabyasachi Chatterjee, objetivando cada uma das simulações a comparação do *jitter* de *unicast*, atraso médio, perda média de ligação, interferência média, potencia média de sinal utilizadas em CODECs VoIP. Eles utilizaram uma medida comum para determinar a qualidade do som produzido pelos CODECs específicos denominada *Mean Opinion Score* (MOS). O valor médio de MOS varia de 1 a 5, onde '1' é dado como inadmissível e o valor '5' como excelente. Os resultados obtidos foram que o CODEC G.711 tem o MOS médio igual a 4 com exceção para alguns pontos de conexão (nós) onde MOS médio é menor, esse CODEC apresenta bons resultados para as três simulações: MOS média, *jitter* médio de *unicast* e atraso médio de uma via e é perfeito para uma boa qualidade de chamada. Nos CODECs G.726ar24, G.729, G.726ar3, o MOS médio estão muito abaixo de 5, valores que geralmente não são admitidos.

2.6 Fraude em sistemas VoIP

Fraude em geral é a tentativa de obter gratuitamente um serviço pago. A fraude em VoIP tem como a principal finalidade a faturação de uma chamada telefónica à custa da vítima de fraude com o propósito de lucrar [20]. Numa suposição de simulação de fraude, diferentes componentes estão conjuntamente envolvidos. Existe um utilizador VoIP que tem o seu sistema, geralmente conectado ao provedor VoIP por meio de uma WAN, em contrapartida existe o atacante que procura invadir o sistema e por fim o provedor do serviço de Internet (ISP). É preciso fazer uma boa analise na rede para detetar a proveniência dos ataques, visto que o atacante pode tentar invadir o sistema VoIP em todos os pontos existentes, como mostra a Figura 2.2 [20].

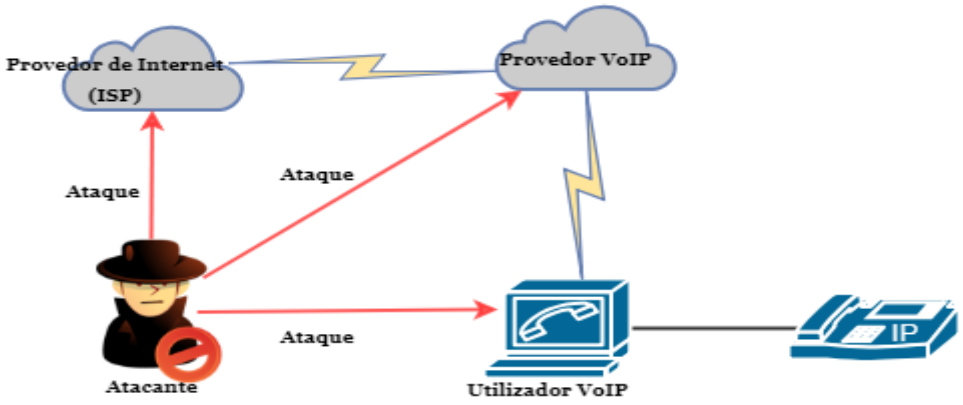

Figura 2.2: Ambiente de fraude geral VoIP.

É de salientar que podem existir cenários em que o atacante é um provedor. Este provedor não confiável tenta organizar o atendimento das suas chamadas através de outro sistema de VoIP, fazendo com que essa vítima de fraude pague os custos da chamada VoIP [20].

2.6.1 Proveniência da fraude VoIP

A fraude VoIP acontece em todo mundo, sendo a África o continente com o maior número das fraudes de telecomunicações, porque os custos de rescisão são muitos altos e não é controlado como noutras partes do mundo [21] . No entanto, um estudo de 2011 da Associação de Controlo de Fraudes de Comunicações (CFCA) descobriram que os 5 principais países que deram

origem a fraude são Estados Unidos, Índia, Reino Unido, Paquistão e as Filipinas [21]. Por outro lado, países como Cuba, Somália, Serra Leoa, Zimbábue e Letónia são os cinco países que terminaram com a fraude [21].

2.6.2 Prejuízos da fraude VoIP

A fraude VoIP é um problema significativo e crescente no sector das telecomunicações. Na maioria dos casos a fraude costuma acontecer durante os finais de semana, o que faz com que o evento de fraude passe despercebido por muitas horas. Um único evento de fraude pode causar prejuízos a nível de custos a uma empresa, num intervalo de 3.000 a 50.000 dólares [21]. Em 2009 um ataque ao PBX VoIP de uma empresa Australiana resultou em 11.000 chamadas internacionais em apenas 46 horas, deixando o provedor SIP com uma conta 120.000 dólares. Ainda assim um ataque em 2011 na África do Sul resultou numa conta de mais de 12.000 dólares, também nos EUA com um custo acima de 1,4 milhões de dólares [21].

Os especialistas têm dificuldades em estimar uma perda global do total anual, porque os cálculos geralmente são baseados por padrões subjetivos e individuais. No entanto a maioria dos especialistas concorda que as perdas estão estimadas entre 3% e 10% do custo pago. Isto traduz-se numa perda global com um valor total estimado entre 30 e 50 mil milhões de dólares por ano. De acordo com o relatório da *Communication Fraud Control Association* (CFCA), a fraude telefónica vai crescendo a uma taxa de 29% por ano [21]. De igual modo vai crescendo a popularidade do VoIP, o que será uma ameaça crescente para o mercado VoIP [21].

2.6.3 Tipos de Fraude

Segundo a empresa TransNexus [21], explanam os inúmeros tipos de atividades fraudulentas, isso porque os fraudulentos criaram uma infinidade de técnicas para explorar a industria VoIP. Alguns são atacados por táticas tradicionais de fraude telefónica, outros com técnicas de hackers e outros ainda exploram equipamentos e softwares específicos para VoIP. Estes são apenas alguns exemplos dos muitos tipos de fraudes, os fraudulentos estão

constantemente a criar novas maneiras de atacar. A maioria dos fraudulentos utiliza algum tipo de combinação das técnicas listadas abaixo.

Estouro de buffer

Algumas fraudes de VoIP dependem de métodos normalmente utilizados para fraudes de computadores. Neste caso, os fraudulentos utilizam erros de estouro ao manipular pacotes *INVITE* ou SIP. A falha pode ser utilizada para parar aplicações ou executar código arbitrário. Esta técnica era um problema para os utilizadores do Asterisk no passado, embora já tenha sido remediada [21].

Fraude de desvio

Fraude de desvio é a inserção não autorizada de tráfego na rede de outra operadora. Podemos encontrar este tipo de fraude denominada por fraude de interconexão, fraude de gateway *Global System for Mobile* (GSM) ou *SIM* boxing. Este cenário exige que os atacantes tenham acesso a tecnologia avançada, capaz de fazer com que as chamadas internacionais pareçam chamadas domésticas mais baratas, com o efeito de contornar o sistema normal de pagamento para chamadas internacionais. Os fraudulentos normalmente vendem cartões telefónicos interurbanos noutros países. Quando os clientes ligam para o número dos cartões, os operadores podem trocar a chamada para que pareça uma chamada doméstica [21].

Fraude de Transferência de chamada

Este tipo de fraude tem sido um problema específico para os utilizadores *softswitch*, neste cenário, o fraudulento invade um PBX e usa os serviços desse PBX para fazer chamadas gratuitas de longas distâncias. Ao instruir o PBX comprometido a transferir a chamada para o serviço telefónico do hacker, os assinantes do serviço telefónico do fraudulento podem falar com os seus destinos internacionais por meio do *softswitch* fraudado e o operador do *softswitch* não pode cobrar o assinante do hacker. [21].

Fraude de Assinatura

Fraude de assinatura é simplesmente a utilização de um serviço sem intenção de pagar. Muitas vezes este tipo de fraude está associado a outros crimes, como roubo de entidade. O verdadeiro impacto da fraude de assinatura geralmente não é conhecido porque os provedores confundem-na com dívidas incobráveis [21].

2.7 Segurança VoIP

A proteção de uma rede VoIP é um problema complexo que envolve muitos fatores, incluindo elementos exclusivos de cada configuração de rede específica, o mesmo acontece com qualquer rede baseada em IP. Os sistemas VoIP são alvos possíveis de muitos tipos de ataques. A lista de possíveis ameaças de um sistema VoIP (ou qualquer sistema IP) é extensa e novos problemas podem ser descobertos continuamente, não há uma solução definitiva para impedir que alguém encontre ou explore uma vulnerabilidade específica [22].

Um sistema VoIP pode ser composto por equipamentos diferentes como terminais de voz (telefones VoIP), servidores, *gateways*, firewalls, entre outros. É importante serem aplicadas soluções de seguranças a estes equipamentos. Nesta secção serão discutidas alguns destes ataques e apresentados alguns mecanismos que podem ser incorporados para tornar o serviço VoIP seguro [22] .

2.7.1 Possíveis ameaças

Como já foi acima descrito, as redes VoIP estão sujeitas as mesmas ameaças que qualquer rede baseada em IP enfrenta. Para maior profundidade do conhecimento pode ser feita a investigação noutros sítios (Internet e livros), entretanto serão de breve forma abordadas algumas ameaças que o VoIP pode enfrentar [22]:

- Negação de serviços (DoS);
- Ataque *Man-in-the-Middle*;
- *Call Hijacking*;

- Terminação de chamada;
- Quebra de senha (força bruta e outros);
- *Server Impersonation;*
- Escutas;
- Ataques de pacotes de exceção;
- *Disturbance call attacks* contra endpoints;
- *Call leaflet attacks*.

Para a proteção dessas ameaças a solução VoIP precisa de executar as seguintes funções [22]:

- **Autenticação** – devem ser autenticados os participantes de uma comunicação.
- **Proteção de dados** -proteger os dados trocados para que não sejam intercetados por outras pessoas.
- **Integridade dos dados**- capacidade de confirmar se os dados recebidos não foram adulterados (se realmente foi recebido o que foi enviado)
- **Não repúdio** – capacidade de provar que a mensagem realmente veio do destino certo. Isso é especialmente importante se a mensagem de sinalização estiver a ser utilizada para gerar informações de cobrança.

2.7.2 Proteção ao canal de sinalização

O canal de sinalização pode ser protegido utilizando o protocolo padrão como o IPSec2 ou TLS3 [22]. A escolha de qual protocolo utilizar pode depender de problemas ao nível de arquitetura do sistema. O IPsec, por exemplo, destina-se a proteger uma conexão executada por IP. O TLS, por outro lado destina-se a proteger uma conexão executada num protocolo de transporte, como o TCP ou SCTP. Ambos os protocolos estão aptos para a proteção do sinal num sistema VoIP. É comum nos aplicativos de comércio eletrónico, que a autenticação aconteça somente numa direção [22]. Para trocas de sinalização, na maioria dos casos, a autenticação é feita em ambas as direções. O utilizador precisa de saber que o servidor é o servidor real (não um servidor fraudulento) e o servidor precisa de se certificar que é o utilizador real e não alguém que está a tentar fazer chamadas fraudulentas fazendo-se passar por ele [22].

2.7.3 Proteção ao canal de media

Os dispositivos VoIP normalmente utilizam o Protocolo de transporte em tempo real (RTP) para trabalhar com os fluxos de media. O RTP não fornece nenhum mecanismo para proteger o fluxo de media. Os Protocolos tradicionais de segurança, como o IPSec, podem ser utilizados, mas na maioria dos casos pode comprometer a QoS devido os rigorosos requisitos de desempenho dos fluxos de media. Então é proposto um protocolo eficiente para tratar das necessidades de segurança do fluxo de media VoIP, esse protocolo é o protocolo em tempo real seguro (SRTP) [22].

O SRTP fornece confidencialidade à autenticação de mensagens e proteção de repetição (de chamadas gravadas) para o tráfego RTP e tráfego de controlo para o protocolo de controlo de transporte em tempo real (RTPC). O SRTP foi projetado para ser eficiente e adiciona um mínimo de sobrecarga aos pacotes RTP e RTPC, também utiliza pouca memória para um conjunto de chaves criptográficas e uma lista de conversas guardadas que podem ser implementadas num espaço de código pequeno, por estas razões o SRTP parece ser o protocolo certo para proteger o canal de media VoIP [22].

2.8 Softwares para servidores VoIP

O Software para a montagem de PBX IP, é utlizado com a finalidade de gerir as chamadas fazendo o encaminhamento , em redes baseadas em protocolo de Internet, permitindo que dispositivos conectados a ele façam e recebam chamadas de voz e vídeo através da rede IP com funcionalidades padrão da maioria dos telefones convencionais [15]. Os subtemas abaixo descrevem alguns softwares para servidores VoIP:

2.8.1 Asterisk

O Asterisk é um sistema gratuito e de código aberto utilizado para a construção de aplicações de comunicação. É capaz de transformar um computador comum num servidor de comunicações. Serve sistemas PBX IP, *gateways* VoIP, servidores de conferência e outras operações personalizadas. Pequenas e grandes empresas também utilizam o Asterisk, tal como as

centrais telefónicas, operadoras e instituições governamentais. Existem atualmente mais de 1 milhão de sistemas de comunicação baseados no Asterisk (a nível de implementação na rede), com uma estimativa de mais de 170 países [23].

O Asterisk é uma plataforma que suporta múltiplos protocolos de voz por pacote, gera uma aplicação PBX de alto nível, aumenta o suporte da rede, fornece suporte aberto à comunidade Asterisk, mantem-se confiável e a par da tecnologia mais recente. O Asterisk pode ser integrado com telefone IP, telefone analógico, telefone ADSI e *softphones* [23].

Serviços e funcionalidades

- **SIP Trunking**: com várias funções como a facilidade de remoção e adição de canais tornando-o **escalável**, com a conexão de ponta a ponta com *Switchvox* resultando numa ligação ininterrupta, funciona praticamente com qualquer PBX o que faz dele universal, facilidade em conectar a um sistema antigo facilitando a migração [23];
- **Cartões de Telefonia:** servem de interface de telefonia analógica, digital e híbrida, existe também o processo de transcodificação que é a conversão de media de um CODEC para outro (Cartões de compreensão de media) [23];
- **IP PBX:** Manter, e manipular chamadas entre os nós finais. Para soluções de implementação do IP PBX a empresa Asterisk propõe também o Sistema Switchvox PBX IP [23];
- ***Gateways* VoIP:** São utilizados nos casos em que os servidores não possuem *slots* de cartão, quando Asterisk é executado num ambiente virtualizado ou quando os circuitos PSTN precisam de se conectar a vários sistemas asterisk [23]

2.8.2 Cisco Unified CallManager

O Cisco *Unified Communications Manager* (CUCM) é um sistema que fornece controlo de chamadas, gestão de sessão. É muito utilizado em ambientes empresariais com mais de 200 mil clientes em todo mundo [24]. Dispõe de

soluções para implementação de controlo de chamada como a *Enterprise Unified Communications,* Solução de Colaboração em pacotes, *Cloud Calling* e UC como Serviço [24]. A Cisco oferece soluções de comunicações unificadas híbridas, locais, atendendo às necessidades do cliente[24].

Serviços e funcionalidades

- **Controlo de Chamadas:** Possibilita encontrar a melhor implantação do controlo de chamadas, como *Enterprise Unified Communications* que contem o pacote *CallManager*, este fornece gestão de chamadas e sessão, segurança e escalabilidade. Soluções de Colaboração em Pacotes que contem os pacotes Cisco Business Edition 7000, Cisco Business Edition 6000, Cisco Business Edition 4000. *Cloud Calling* e UC como Serviço que é composto pela Solução Cisco *Hosted Collaboration* e Cisco *Spark* [24]**;**
- ***Gateways* de Comunicações:** segundo a Cisco [24], os *gateways* da *Unified Communications* ajudam a permitir qualquer colaboração em qualquer lugar, por qualquer pessoa e em qualquer dispositivo. Fornecem proteção de investimento para implementações de tecnologias existentes. Os *Gateways* da Cisco oferecem soluções para qualquer dimensão de negócios [24];
- **Aplicações de Comunicações Unificadas:** existe o produto **Cisco Jabber** que permite a colaboração em qualquer lugar, entre dispositivos, navegadores e novos aplicativos de Comunicações Unificadas (UC). A obtenção de recursos amplos de telefonia, conferência e ponte de vídeo. **Conexão Cisco *Unity*** permite o acesso de mensagens de voz a qualquer momento, em qualquer lugar e em qualquer dispositivo. **Reuniões Cisco WebEx** permitem organizar e gerir todas as atividades da reunião e a compartilha de arquivos com facilidade [24];
- **Soluções de colaboração de médio porte:** permite que funcionários, clientes e parceiros colaborem de forma simples (sem problemas) em

qualquer lugar, em qualquer dispositivo, do navegador para a sala de reuniões [24].

2.8.3 Elastix

É um software de serviço de UC de código aberto com a finalidade de estabelecer comunicações unificadas que juntam PBX IP, email, IM, fax e funcionalidades de cooperação. Tem como objetivo unir todas as opções de comunicação, acessíveis dentro da classe empresarial, para uma solução única [25]. Foi feito o seu lançamento como uma distribuição Linux com Asterix, Zaptel e um conjunto de pacotes que foram administrados por meio de uma interface, destacando-se em dezembro de 2006. O Elastix dispõe uma interface Web e inclui alguns recursos como central de atendimentos, software com discagem preditiva. Possui suporte para hardware de telefonia e também suporta distintas marcas de telefone com o auxílio dos protocolos SIP e IAX implementados pelo Asterisk, estes dois protocolos baseiam-se em padrões públicos disponíveis. Assim sendo, qualquer fabricante pode criar um produto que os suporte [25].

O Elastix tem vários recursos e funcionalidades. Essas funcionalidades estão relacionadas com todos os serviços disponíveis - Telefonia IP, Servidor de Correio, Servidor de Fax, Conferências, Servidor de Mensagens Instantâneas. A sua funcionalidade integra alguns projetos de código aberto com a inclusão do Asterisk, HylaFAX, Openfire e Postfix. Estes pacotes de softwares executam Funções PBX, mensagens instantâneas, email e fax. O PBX é uma funcionalidade de extrema importância no Elastix.

Elastix PBX, é uma central telefónica que serve um determinado negócio ou empresa. A central telefónica privada (PBX) utiliza o Asterisk como software para o servir, ou seja, pode ser utilizado o Asterisk para construir um PBX. O Asterisk permite que os telefones conectados efetuem chamadas entre si, de modo a haver conexão entre diferentes serviços telefónicos como a rede telefónica comutada pública (PSTN) e VoIP. O Asterisk compõe-se de muitos recursos acessíveis em sistemas PBX como - correio de voz, conferência,

resposta interativa (opções do telefone) e distribuição automática de chamadas. Para fazer a conexão de telefones analógicos tradicionais e da rede PSTN ao Asterisk o servidor deve ser equipado com o software especial. O Elastix faz a gestão do Asterisk PBX através de FreePBX na telefonia IP. O SIP, IAX2, *Custom* e ZAP são protocolos que podem ser suportados pelo PBX [25].

Características e Funcionalidades

- **Fax Virtual:** O servidor de Fax Virtual Elastix é baseado em HylaFa (servidor de fax livre, para sistemas do tipo Unix), possibilitando enviar de modo personalizado, baixar fax no formato pdf, controlo de acesso para clientes fax e pode ser integrado com Winprint HylaFax [25];
- **Colaboração:** A colaboração Elastix é um trabalho de escritório, contendo um calendário integrado no PBX com suporte para notificações de voz, lista telefónicas com recursos adicionais como produtos de CRM integrados [25];
- **Mensagem Instantânea:** O *Instant Message* (IM) do Elastix é baseado no servidor de mensagens instantâneas *Openfire*, as suas características abrangnuma gestão baseada na Web para um servidor de IM, plugins e suporte LDAP, chamadas iniciadas por clientes, suporte a outros *gateways* de IM como MSN, Yahoo Messenger, GTalk e ICQ [25] ;
- **Email:** O servidor de correio com um módulo que suporta múltiplos domínios, cotas, gestão baseadas na Web, clientes de email e *antisspam*. Com o Elastix é possível escolher onde se deseja ser implantado o sistema PBX, localmente ou na *Cloud*, a plataforma, Windows ou Linux utiliza a virtualização de maquinas ou não, o que resulta na liberdade total e escolha da instalação, também a escolha do provedor da respetiva *Cloud* é opcional e quais SIP *Trunks* ou telefones IP podem ser utilizados [25].

2.8.4 Telzio

Telzio é uma solução na Cloud para sistemas de telefonia comercial. A Telzio oferece ás empresas integração entre equipes de trabalho, escritórios e dispositivos móveis por meio de uma plataforma *Cloud*. Segundo Telzio [26] a implantação dessa solução evita a construção de uma infraestrutura dispendiosa e a compra de equipamentos, licenças de Softwares, tendo impacto na redução de custos. Toda a infraestrutura do sistema telefónico é alojada na nuvem [26].

Características e funcionalidades

- **Gestão de Chamadas:** permite fazer a gestão de fluxos de chamadas, que possibilita a gestão de vários recursos e opções avançadas de roteamento de chamadas, atendentes automático, filas de chamadas que são importantes para a gestão de chamadas recebidas em linhas telefónicas ocupadas, encaminhamento de chamadas úteis em situações diversas em que as chamadas recebidas sejam encaminhadas para mais de um telefone [26];
- **Conferência:** O Telzio permite fazer chamadas em conferência a partir de qualquer local, sem que haja a necessidade da criação de uma sala de conferências, basta que se tenha o aplicativo móvel da Telzio. Para as chamadas de conferência maiores e agendadas, é possível adicionar uma linha de conferência ao sistema existente onde um número limitado de chamador pode discar [26];
- **Correio de Voz:** o Telzio transcreve as mensagens de voz para que sejam visualizadas num computador ou telefone. Permite a personalização de serviços de correio de voz em que os funcionários podem ter os seus correios separados, os correios de voz podem ser recebidos por Email onde podem ser ouvidos ou lidos como textos [26].

2.8.5 3CX

O 3CX é uma solução feita de comunicações unificadas, que inclui conferência em Web, presença, *softphones*, clientes de movéis, entre outros

serviços, sem custo e é possível fazer até 8 chamada grátis, permite a liberdade de instalação e de configuração, o que possibilita definir quais SIP *trunk* ou telefones IP a serem utilizados. Este sistema de telefone é baseado em *software* aberto que funciona com telefones IP populares e SIP *trunk*, ou seja local ou na nuvem [27].

2.9 Comparação entre softwares VoIP

A Tabela 2.4 mostra a comparação entre softwares VoIP para servidores desde a compatibilidade com diferentes plataformas, protocolos, algumas funcionalidades e o mercado alvo.

Tabela 2.4-Comparação entre Softwares VoIP para servidores

Programa	Sistema operativo	Licença	Protocolos	Criptografia	Outras Caraterísticas	Mercado alvo	última versão
Asterisk	Linux, BSD, OS X	Dupla: GNUv2 Pago	H323, IAX, MGCP, SIP	TLS, SRTP	Não precisa de software adicional para VoIP	Pequenas e grandes empresas, *Call centers*	15.4.0
Cisco Unified CallManager	Linux, OS X, Windows	Pago	H323, MGCP,	SSL	Possibilita agrupar vários servidores de processamento de chamada numa rede IP, e são administrados por uma única entidade.	Pequenas, médias e grandes empresas	12.0
Elastix	Linux, Windows	Dupla: GPLv2 pago	IAX, SIP	TLS	Permite utilizar uma edição gratuita com a capacidade de até 8 chamadas	Call center, Grandes empresas	5.0
Telzio	Baseado em nuvem	Pago	SIP, RTP	TLS, SRTP	IVR, integração móvel, configuração *Web*, monitoramento de chamadas	Pequenas e grandes empresas	4.2.9
3CX	Linux, Windows, também é baseado na *cloud*	Proprietário	SIP	TLS, SRTP	Call Parking Call Recording Telefonia IP de voz e vídeo, voz e vídeo conferência, correio de voz e mensagens instantâneas	Pequenas, grandes e médias empresas	3CX Versão 15

2.10 Softphones VoIP

Softphone é um telefone IP que funciona como um software num PC ou dispositivo portátil. Um softphone é definido por um identificador de ponto final exclusivo que pode ser um número de telefone, um número de extensão ou um endereço MAC, que são pré-registados num provedor [28].

Softphone VoIP é um programa que pode ser instalado em computadores e telemóveis para fazer chamadas pela Internet, utilizando aplicações como Skype, Ichat, GoogleTalk entre outras. Os Softphones VoIP são projetados de forma a parecer um telemóvel real, possibilitando o acesso a uma interface para a discagem de números ou utilizando um teclado. Os Softphone beneficiam pequenos negócios, trabalhadores viajantes, turistas e outros, possibilitando as chamadas frequentes de longa distância, o que tem um impacto significativo a nível da redução de custos [29].

O VoIP utiliza diferentes protocolos para determinar como os dados são processados e transferidos pela rede, portanto o Sofphone VoIP suporta os mesmos protocolos que o serviço VoIP utiliza. Abaixo são apresentados alguns Softphones VoIP:

2.10.1 Vbuzzer

Vbuzzer permite fazer chamadas telefónicas VoIP, com conexão à Internet. As chamadas são encaminhadas pela conexão de Internet existente, em vez da linha telefónica, com um adaptador Vbuzzer. O recetor das chamadas não precisa de ser membro do Vbuzzer ou utilizadores de serviços Vbuzzer, basta que se tenha um telefone normal [30].

Para a sua utilização existem requisitos como conexão à Internet, um telemóvel, um adaptador de VoIP, dispositivo que conecta o equipamento de telefone à Internet. O Vbuzzer utiliza um adaptador para fornecer um serviço de telefone residencial via Internet. O adaptador pode ser da empresa Vbuzzer, como podem ser utilizados outros adaptadores VoIP [30].

O Vbuzzer possui um serviço de chamada com funções como chamada em espera, encaminhamento de chamadas, Vbuzzer-to-Vbuzzer chamada sem custo para clientes Vbuzzer em qualquer parte do mundo, número de telefone virtual [30].

2.10.2 Skype

O Skype é um aplicativo e serviço VoIP utilizado para comunicação via Internet, como envio de mensagens instantâneas, chamadas VoIP, compatibilidade com sistema de vídeo conferência, permitindo chamada de vídeo conferência com várias pessoas. O Skype pode ser utilizado em computadores e telefones [31].

Recursos do Skype

- **Chamada**:

- **Chamada do Skype para o Skype** essas chamadas podem ser locais ou internacionais, podem ser feitas a qualquer momento e são sempre gratuitas [32];

- **Chamada para outras linhas** o Skype permite fazer chamadas para utilizador de outras redes telefónicas como PSTN entre outros. Para esse tipo de chamada existe um custo [32];

- **Chamadas em grupo** é possível fazer chamadas em grupo no Skype, o que permite a partilha de informação, colaboração em equipe. Nas chamadas em grupo estão incluídas chamadas em conferência, e mensagens de texto, num limite de 25 pessoas;

- **Encaminhamento de chamadas** possibilita receber chamadas encaminhadas para qualquer telefone. Caso o utilizador esteja offline, pode encaminhar as suas chamadas utilizando os serviços de encaminhamento de chamadas do Skype e a chamada é encaminhada automaticamente para o número de telefone a sua escolha [32];

- **Mensagem** é um dos recursos do Skype que possibilita a troca de mensagens de textos, mensagem de voz, e o envio de vídeos e fotos. Com funcionalidades como emoticons e emojis, mensagem instantânea, mensagens de vídeo e *groupme* que é a troca de mensagens em grupo [32].
- **Compartilha** permite a troca e acesso aos arquivos, fotos, vídeos, compartilhamento de tela que é a possibilidade de compartilhar a tela do computador com quem desejamos, esse compartilhamento pode ser com um único utilizador ou em grupo [32].
- **Skype *Translator*** é o tradutor *on-line* do Skype que ajuda na comunicação de pessoas de idiomas diferentes, fazendo a tradução de chamadas de voz, chamadas de vídeo e mensagens instantâneas [32].

2.10.3 KPhone

O KPhone é um *User Agents* (UA) SIP para Linux. Ele implementa a funcionalidade de um VoIP softphone, mas não está restrito a isso. O KPhone foi escrito em C++ e usa o kit de ferramentas Qt. O KPhone estabelece sessões através da Internet e assim permite a comunicação entre *endpoints*. [29].

O KPhone também suporta agentes SIP proxy como comunicação direta entre *User Agents*. Essa ligação não funciona se os *firewalls e NATs* restringirem a comunicação ponto a ponto [29].

Caraterísticas Principais do KPhone

- Suporte IPv4 e IPv6;
- Várias sessões paralelas (no caso do áudio, uma pode estar ativa, as outras são mantidas);
- *Ringtones* definidos pelo utilizador ou “toque de música”;
- NAT *traversal* e suporte STUN;
- Suporte ALSA e OSS;

- Criptografia SRTP para voz (ainda não existe para processadores de 64 bits);
- Chama em espera;
- Encaminhamento de chamas;
- Respostas automáticas.

Tipos de media suportados

- Áudio;
- Informação de presença;
- Mensagem instantânea;
- Vídeo (com a aplicação externa VIC);
- Aplicativos externos;

2.10.4 ZoiPer

O ZoiPer é um Softphone que foi escrito em oldsk00l C / C++ e *Assembly*, resultando na pouca utilização da memoria e da CPU o para a melhor qualidade de áudio até em Hardwares antigos. Pode ser executado em várias plataformas diferentes. Independente do sistema a ser utilizado como MacOS, Linux, Windows, iOS e Android.

O ZoiPer é compatível com a maioria dos provedores de serviços VoIP e PBX. Os Softphones Zoiper funcionam com: Asterisk, FreeSwitch, Cisco *CallManager*, 3CX, Elastix e outros PBX baseados em SIP. As chamadas são gratuitas entre utilizadores do ZoiPer. O ZoiPer tem funcionalidades de Callcenter como Respostas automáticas, Aprovisionamento, Gravação de chamadas, integração de CRM.

Zoiper por padrão vem com criptografia *end-to-end* de qualidade militar gratuita para voz e vídeo (se o servidor ou provedor de serviço o suportar). O ZoiPer suporta os seguintes métodos de criptografia padronizada:

- TLS;
- SRTP;

- ZRTP (Telemovel e ZoiPer *desktop* beta).

2.10.5 Mizu

Mizu Softphone (MizuPhone) é um Softphone profissional VoIP baseado no protocolo SIP padrão com uma interface para o sistema operativo Microsoft Windows. Com o MizuPhone é possível conectar a qualquer servidor que suporta o protocolo SIP na Internet ou na rede privada [33].

O MizuPhone tenta combinar a compatibilidade SIP com a inteligência P2P e uma *Graphical User Interface* (GUI) simples. O MizuPhone pode trabalhar com qualquer servidor SIP e telefone IP, sua arquitetura modular permite customizar, ativar ou desativar qualquer funcionalidade. Este Softphone é construído exclusivamente em tecnologias padrão da indústria VoIP [33].

Recursos do Softphone Mizu

- Teleconferências (com conversor local ou conversor de CODECs quando necessário);
- Chamada em espera;
- VoiceMail (remoto e local);
- Transferência de chamada;
- Chamadas de vídeos HD (dependendo da camara a ser utilizada e da largura de banda);
- Compartilha de arquivos (compatível com qualquer servidor SIP);
- Fax (versão beta);
- Gravação de áudio e vídeo;
- CODECs de áudio: G.711-Alaw, G.711-uLaw, G.723.1, G.729, iLBC, L16, Speex;
- Ocultação de perdas de pacotes (PLC);
- Controlo de ganho Automático (AGC);
- Cancelamento de eco acústico (AEC);
- Detenção de atividade de voz (VAD);
- Supressor de ruido (NS);

- Solução de CRM;
- Interface e idiomas personalizáveis.

2.10.6 CallCentric

O CallCentric é um Softphone VoIP baseado no SIP que é executado em plataformas como - iOS, Android, que permite fazer e receber chamadas até internacionais através de uma conexão de Internet. As chamadas são feitas com o protocolo SIP / 2.0, que é construído para funcionar com conexões ponto a ponto. As chamadas são gratuitas entre membros CallCentric, e com diversos planos de tarifas com custos para chamadas de telefones tradicionais [34].

Recursos do CallCentric

- SIP Truking
- Filtro de chamada de spam
- *Telemarketer block*
- Chamada Ilimitada de URI SIP
- Encaminhamento DID
- Chamada em espera
- Encaminhamento de chamadas
- Receber Fax
- Utilização de qualquer Softphone ou adaptador desde que suporte o SIP
- Cartão de chamada
- Rejeição de Chamadas anônimas
- Bloqueio do ID do chamador por chamada
- IVR (Atendimento automatizado)

2.11 Comparação entre Softphones VoIP

A Tabela 2.5 mostra a comparação entre os Softphone desde a compatibilidade com diferentes plataformas, protocolos, algumas funcionalidades e o mercado alvo.

Tabela 2.5-Comparação entre alguns Softphones.

Softphone	Plataforma	Licença	Protocolo	Criptografia	Outras características	Mercado alvo	Última versão
Vbuzzer	Android, iOS, Windows, Mac, Linux	*Freeware* proprietário	SIP	TLS	IM (MSN), correio de voz, saudação de voz personalizada	Empresas e particulares	2.7 build 2.7.009 Beta
Skype	Windows, Mac Linux, Andoid, iOS	*Freewire* Proprietário fechado	Protocolo P2P	TLS, SRTP	Correio de voz, gravar e encaminhar chamadas	Empresas e particulares	Skype 8.22.0.2
KPhone	Linux	GPLv2	SIP, NAT-STUN NAPTR	(SRTP)	Vídeo, IM, sessões externas, suporte IPv6 para UDP	Empresa e particulares	Kphone SI v1.1
Zoiper	MacOs, Linux, Windows, iOS, Android	*Freewire* proprietário fechado	SIP, SDP, RTP, IAX2, STUN, UDPTL	TLS, SRTP, ZRT	Integração com CRM, *plug-ins* do Outlook e do Thunderbird	Empresas e particulares	V5.2.16

Mizu	Windows, Android, iOS, Symbian	GPLv2	RTP, RTPC, UDP, TCP, SIP, STUN	SRTP, TLS	Scripts, gravação de chamadas, transferência de arquivos	Empresas e particulares	MizuPhone 3.6
Bria	Windows, MacOS, Andorid, iOS	Proprietário	SIP, XMPP, STUN, ICE	TLS, SRTP	Chamadas de vídeos HD (120 x 720p), conexão com *call center* na cloud	Empresas e particulares	v5.3
iCall	Windows, MacOS, iOS, Windows mobile	*Freeware*	SIP, IAX,	TS, ZRTP	Transferência de arquivos, IM (MSN, AIM, ICQ, Yahoo!, XMPP, Google *Talk*), correio de voz	Empresas e particulares	v7.1.521

2.12 Dispositivos VoIP

Para fazer e receber chamadas utilizando VoIP, é preciso uma configuração de Hardware, pode ser utilizado um ATA para chamadas com outras redes como PSTN ou ISDN, que se conecta a um telefone. [35]. Assim sendo a abordagem que se segue é sobre as funcionalidades de alguns dispositivos VoIP.

2.12.1 Adaptador de Telefone Analógico

Adaptador de Telefone Analógico (ATA), é um dispositivo utilizado para conectar um ou mais telefones analógicos padrão a um sistema de telefone digital (como VoIP) ou a um sistema telefónico não padrão [35]. O Dispositivo ATA, pode ser chamado por nomes diferentes entre a diversidade de fabricantes, mas a sua função essencial é a mesma, converter o sinal de voz em pacotes de dados, autenticar o dispositivo no serviço VoIP, fornecer *dial tone*, interpretar *ring tones*, entre outras funções [36].

Um dispositivo ATA geralmente consiste num pequeno Hardware com várias portas, que servem para fornecer conexão ao telefone fixo e ao router, assim como uma fonte de energia. O ATA pode ter uma ou mais portas *Ethernet* que permitem que o dispositivo faça a conexão com o router para acesso á Internet. Igualmente, o dispositivo terá uma ou mais portas FXS, que são utilizadas para conectar o dispositivo fixo. Em contrapartida alguns dispositivos também vêm com portas FXO, que podem conectar uma linha POTS ao dispositivo e é frequentemente utilizada, como *failover* ou *lifeline* no caso do serviço de perder conexão com o serviço de Internet [36].

2.12.2 Tipos de adaptadores VoIP

- **Single FXS -** como diz o nome estes adaptadores vêm com uma única porta FXS, que pode conectar um telefone fixo ao serviço VoIP [36];
- **Dual FXS -** são adaptadores que oferecem portas FXS duplas para utilizadores que se desejam conectar a um ou mais dispositivos, como um dispositivo de fax [36];

- **FXS / FXO -** estes adaptadores incluem portas FXS e FXO que podem ser utilizadas para conectar equipamentos fixos analógicos e conexões fixas [36];

2.12.3 Como escolher um ATA para compra

Existem muitas alternativas disponíveis no mercado, mas o número de portas Ethernet, FXS e FXO determinará quantos dispositivos podem ser conectados. Para um consumidor médio, um ATA simples com uma Ethernet e uma ou duas portas FXS é suficiente. Normalmente o fornecedor VoIP fornece a ATA se o cliente assinar um contrato [36].

O custo não é um fator decisivo quando se trata da compra de adaptadores. Deve-se considerar quantas linhas precisam se conectar, e a disponibilidade de portas Ethernet, a necessidade de enviar fax e a compatibilidade com o serviço VoIP [36].

2.12.4 Funcionamento do adaptador VoIP

O ATA trabalha com um protocolo VoIP específico e um CODEC de áudio para executar suas funções. O protocolo VoIP é utilizado para a comunicação com o servidor Web remoto, e o CODEC executa a função de converter sinais de áudio. Para o funcionamento e utilização do adaptador VoIP é importante saber qual o protocolo suportado pelo seu provedor e os CODECs de áudios específicos utilizados determinarão a qualidade das chamadas, tal como a quantidade de largura de banda exigida por cada chamada.

2.12.5 Telefone IP

O termo “telefone IP” refere-se a um telefone, que permite o processamento e comunicação de voz através do protocolo IP e da Internet ou intranet. O telefone IP converte sinais de voz analógicos em sinais de voz digitais e empacota-os em dados para que possam ser transmitidos via IP [37].

Os telefones IP podem ser feitos como dispositivos de hardware e também soluções de software puro (Softphones). Um telefone IP de software é um programa que é instalado num computador e que se conecta a Internet para

trocar dados de voz, para essa comunicação é necessário ligar ao computador um microfone, alto-falante ou um fone de ouvido. Também é possível converter telefones convencionais em telefones VoIP utilizando adaptadores apropriados [37]. Muitos telefones IP utilizam o protocolo SIP, independentemente de serem de hardware ou de software.

2.12.6 Tipos de Telefones VoIP

- **Telefones VoIP Desktop**: é um telefone padrão de classe empresarial. Que se conecta ao sistema de telefone VoIP ou ao provedor de serviços via Ethernet e vem com todos os recursos básicos de um telefone comum[38];
- **Telefones IP sem fio:** é um telefone com uma unidade de transceptor wi-fi ou DECT incorporada que conecta a um *access point* ou *base station*. Permitindo que haja movimentos em casa e / ou escritório durante a chamada [38];
- **Telefone IP com fio e DECT:** um telefone IP com fio é um telefone de secretária que permite fazer chamadas em qualquer lugar do mundo através de uma conexão de IP de banda larga. Podem ser usados também para videoconferências caso suporta vídeos [37] ;
- **Telefones de conferência:** é um tipo especial de telefone projetado especificamente para utilização em chamadas telefónicas com várias pessoas. Está equipado com um ou mais alto-falantes e microfones para permitir uma audição confortável e o uso de mãos-livres. Isso permite que vários participantes numa sala que acompanham a conversa e dão o seu contributo. Existe uma variedade de telefones de conferência para as diferentes tecnologias de linhas telefónicas diferentes como para o uso de conexões analógicas, ISDN e VoIP [39].

2.12.7 Funcionamento de telefones VoIP

Para fazer chamadas primeiramente deve-se registar o telefone VoIP numa conta, este é o processo de conexão do telefone ao provedor de serviços para que eles possam comunicar uns com os outros. Alguns provedores de VoIP suportam o IP *phone booting* para determinados telefones VoIP, o que

acelera o acesso de registo do telefone utilizando um servidor de inicialização.

2.13 Gateway VoIP

A função básica de um *gateway* é converter o tráfego de diferentes tipos de redes. No ambiente de dados, um gateway pode fazer a conversão entre uma rede *Frame Relay* e uma rede Ethernet. Num ambiente VoIP, o gateway é a porta entre uma rede VoIP e a rede telefónica pública comutada, uma central privada de intercâmbio (PBX) ou dispositivos analógicos como máquinas de fax. Na sua forma mais simples, um gateway VoIP possui uma interface IP e uma interface telefónica inserida, e trabalha com muitas tarefas envolvidas na conversão entre formatos de transmissão e protocolos. O gateway é uma parte essencial de qualquer rede telefónica IP que tem uma interação com a rede PSTN ou com dispositivos analógicos [40]. A Figura 2.3 mostra o funcionamento do gateway numa rede VoIP.

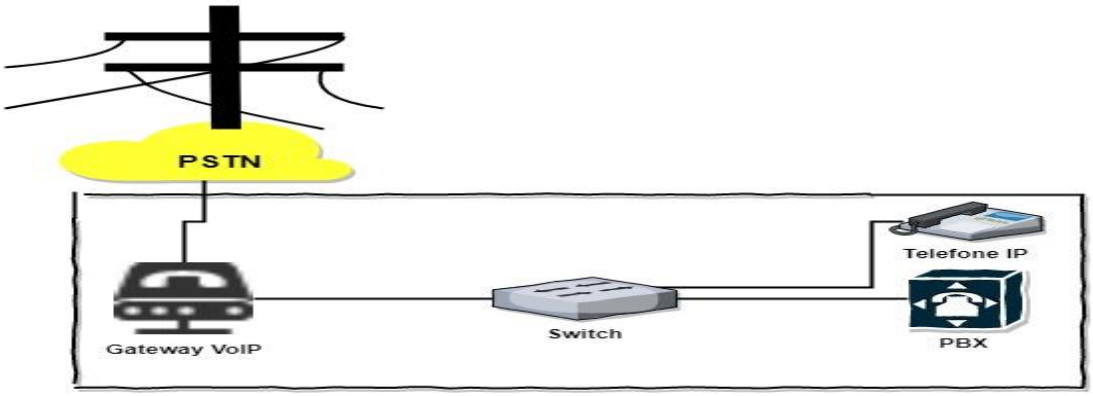

Figura 2.3: Funcionamento do Gateway.

O gateway permite a comunicação entre as duas redes executando as seguintes tarefas:

- Interface com a rede IP e a PSTN ou PBX [40];
- Suporta protocolos de controlo de chamadas IP, além de controlo de chamadas de multiplexagem por tempo (TDM) [40];

- Realização de configuração de chamadas, desvio de chamada entre as redes VoIP e PST, encerrar e reorientar a call media e a sinalização [40];
- Fornecer serviços suplementares, como retenção e transferência de chamadas [40];
- Retransmissão de *Dual-Tone Multi-Frequency* (DTMF) [40];
- Suporte de faxes analógicos e modems através da rede IP [40].

2.13.1 Protocolos usados para sinalização de voz e media em *gateways* VoIP

Para que o *gateway* funcione corretamente é preciso uma compreensão básica de protocolos e CODEC*s* VoIP. Deve ser utilizado um protocolo compatível com o sistema de telefone VoIP. O CODEC e o protocolo a serem utlizados podem aumentar ou diminuir drasticamente a qualidade das chamadas [40] .

- Protocolo de controlo de *gateway* de media (MGCP) [40];
- H. 323 [40];
- Protocolo de Inicialização de Sessão (SIP) [40];
- *Skinny Client Control Protocol* (SCCP) [40];
- Protocolo de transporte em tempo real (RTP) [40].

2.13.2 CODEC*s* de voz para gateways

Para a configuração, instalação e manutenção de um *gateway* VoIP é preciso aprimorar o conhecimento na área de protocolos e CODEC*s*. De outro modo é necessário certificar-se de que o *gateway* VoIP suporta os mesmos protocolos e CODEC*s* que o serviço VoIP e o sistema de telefone VoIP. Um *gateway* VoIP normalmente suporta vários CODEC*s* de voz. Os CODECs de voz mais comuns são [41]:

- GSM - 13 Kbps [41];
- iLBC - 15 Kbps [41];
- G. 711 - 64 Kbps [41];

- G. 722 - 48/56/64 Kbps [41];
- G. 726 - 16/24/32/40 Kbps [41];
- G. 728 - 16 Kbps [41];
- G. 729 - 8 Kbps [41].

2.13.3 Tipos de Gateway

Segundo o *VoIPSUPPLY* [41] existem dois principais tipos de *gateway*: analógico e digital.

Analógico

Um gateway VoIP analógico é utilizado para conectar telefones analógicos tradicionais a um sistema de telefone VoIP ou para conectar o sistema de telefone VoIP à PSTN. Devido a essa dupla finalidade, um gateway VoIP vem em duas formas diferentes, que são FXS e FXO [41].

- *Gateways* FXS, utilizado para conectar telefones tradicionais e máquinas de fax a um sistema de telefone VoIP [41];
- *Gateways* FXO, utilizado para conectar sistema de telefone VoIP nas linhas PSTN [41].

Digital

Um gateway VoIP digital é utilizado para conectar sistema de telefone VoIP às linhas de voz digitais, como T1 / E1 / BRI. Também pode ser utilizado para conectar seu PBX tradicional a uma rede IP [41].

2.14 *Gatekeepers*

Um *gatekeeper* é uma entidade H.323 na rede que fornece serviços como a tradução de endereços e controlo de acesso de rede para terminais H.323, *gateways* e MCUs. Também podem fornecer outros serviços, tais como gestão de banda, contabilidade e planos de discagem que podem ser centralizados para fornecer *salabity* [42].

2.14.1 Funcionalidade do *gatekeeper*

Segundo a Cisco [42], o padrão H.323 define as funções de gatekeeper como sendo **obrigatórias** e **opcionais**:

Funções obrigatórias do *gatekeeper*

- **Tradução de endereços** - transmite endereços H.323 (como gwy1@domain.com) e números E.164 (números de telefone padrão) para endereços IP de ponto final [42];
- **Controlo de Admissão** – para controlar a entrada do ponto final na rede H.323 o *gatekeeper* usa serviços como, Mensagens de registro, admissão e status (RAS) H.225, pedido de admissão (ARQ) confirmação de admissão (ACF), rejeição de admissão (ARJ) [42].
- **Controlo de largura de banda** - atende à gestão dos requisitos de largura de banda do ponto final. Para conseguir isso, o *gatekeeper* usa mensagens RAS H.225 como solicitação de largura de banda (BRQ), confirmação de largura de banda (BCF), rejeição de largura de banda (BRJ) [42].
- **Gestão de zona** - o *gatekeeper* fornece gestão de zona para todos os pontos finais registados na zona, por exemplo, o controlo do processo de registro do ponto final [42].

Funções de *gatekeeper* opcionais

- **Autorização de chamada** - com esta opção, o *gatekeeper* pode restringir o acesso a determinados terminais ou *gateways* e / ou ter políticas para restringir o acesso [42];
- **Gestão de chamadas** - nesta opção, o *gatekeeper* mantém as informações de chamadas ativas e utiliza-as para indicar pontos finais ocupados ou redirecionar chamadas [42];
- **Gestão da largura de banda** - aqui, o gatekeeper pode rejeitar a admissão quando a largura de banda necessária não está disponível [42];

- **Sinalização de controlo de chamada** –possibilita o *gatekeeper* rotear mensagens de sinalização de chamada entre os pontos finais H.323 com o uso do modelo GKRCS (gestor do router de chamada de *gatekeeper*). Alternativamente, permite que os pontos finais enviem mensagens H.225 de sinalização de chamadas diretamente entre si [42].

O *Gatekeeper* (GK) é utlizado no contexto do protocolo H.323 e em outros protocolos de controlo de media. O GK é considerado o "cérebro" de um sistema de sinalização H.323. Normalmente, um GK é necessário quando mais [43]mantém uma tabela de registos onde os endereços IP privados dos *hosts* locais são mapeados para o *alias* desse *host* local particular [28].

O *gatekeeper* interage e troca informações com o *gateway*. Essa interação e troca de informações é baseada no protocolo H.225 RAS, embora possam ser utilizados outros protocolos que oferecem funções de sinalização RAS [28].

2.15 Provedores VoIP

Um provedor de serviços VoIP, oferece um serviço que permite aos clientes fazer ou receber chamadas de voz pela Internet. Outro termo para provedor de serviços VoIP é "provedor de serviços de telefonia via Internet" (ITSP) [44]. O provedor de serviços VoIP fornece soluções telefónicas VoIP para clientes residenciais e comerciais, geralmente fornece o hardware VoIP e serviços aos assinantes a uma taxa mensal, embora os serviços *hosted* VoIP também são muitos comuns. De igual modo acontece com as soluções de VoIP, os provedores de serviço VoIP utilizam a telefonia com comutação de pacotes para fazer chamadas via Internet [45].

Os provedores VoIP oferecem diferentes tipos de serviços. Estes tipos de serviços são escolhidos dependendo de como e onde desejamos comunicar uns com os outros [43]. Assim sendo os provedores VoIP podem ser categorizados como [43]:

- Provedores VoIP residenciais[43];
- Provedores VoIP baseados em dispositivos [43];
- Provedores de VoIP baseados em software [43];
- Provedores de VoIP Móvel [43];
- Provedores de VoIP hospedados na *Cloud* [43].

2.15.1 Provedor VoIP Residencial

Um serviço VoIP residencial pode ser implementado quando substituímos o nosso sistema de telefone doméstico tradicional por um sistema de telefone VoIP. Essa mudança e implementação é popular nos EUA e na Europa, onde existem vários provedores desse tipo. Num serviço VoIP residencial faz-se a conexão do telefone com um modem wi-fi utilizando um adaptador. A cobrança é feita mensalmente por um serviço, como um serviço ilimitado ou por um número específico de minutos, dependendo do plano a ser escolhido [43].

Com o VoIP residencial, é possível utilizar telefones comuns para fazer e receber chamadas. Deve-se perguntar ao provedor de serviços VoIP residencial se permite *Bring Your Own Device (BYOD)*. Então o que é preciso é um adaptador de telefone analógico (ATA), para conectar o telefone ao router ou hub Ethernet [46].

Também é preciso garantir que temos a velocidade certa de Internet, e verificar o equipamento que o provedor em questão precisa. O que possibilita fazer a comparação de provedores VoIP com base nos equipamentos que eles fornecem e exigem. Os equipamentos comuns solicitados a um serviço de VoIP residencial são [46]:

- ATA [46];
- Telefone IP [46];
- Softphone [46].

2.15.2 Provedores VoIP baseados em dispositivos

Os serviços fornecidos pelos provedores de VoIP baseados em dispositivos são chamados de serviços sem fatura mensal. A empresa provedora vende um dispositivo, que pode ser utilizado com o sistema de telefone tradicional para

fazer chamadas gratuitas. A box é conectada ao equipamento existente o que elimina a necessidade de um computador para o seu funcionamento, embora seja preciso uma conexão à Internet de alta velocidade. Como exemplo desse tipo de serviço temos Ooma e o MagicJak [43].

2.15.3 Provedores Baseados em Software

Os provedores de serviços VoIP baseados em Software, são os serviços mais comuns em todo mundo [43]. Estes serviços trabalham frequentemente com uma aplicação de Software que emula um telefone chamado Softphone. A aplicação pode ser utilizada num computador para fazer e receber chamadas, utilizando o dispositivo de entrada e saída de áudio para falar e ouvir. Alguns provedores de VoIP baseados em Software, são baseados na Web e, em vez de exigirem a instalação de uma aplicação, o serviço é fornecido por meio de interface Web. [43].

2.15.4 Provedores VoIP de comunicação móvel

Os provedores de comunicação móvel vão surgindo em grande escala, desde que o VoIP conquistou o mercado telefónico móvel, permitindo que milhões de pessoas carreguem o poder do VoIP nos seus bolsos e façam chamadas gratuitas e baratas onde quer que estejam. Por exemplo a utilização do Skype, Viber e WhatsApp [43].

2.15.5 Provedores de PBX alojado na *Cloud*

Um PBX alojado na *Cloud*, é um serviço telefónico baseado em *Cloud* que oferece recursos de PBX e de plataforma de chamada. Como a solução é baseada na *Cloud*, a funcionalidade do PBX é alojada e administrada pelo provedor de serviços. Este serviço é fornecido às pequenas, médias e empresas corporativas [47].

Visto que o serviço é alojado, as empresas não precisam de pagar por equipamentos. Os provedores de PBX alojados fornecem o mesmo padrão de serviço, bem como os mesmos recursos e funcionalidades. Os provedores de PBX na *Cloud* mantêm os seus próprios *Data Centers* para fornecer serviços a um grande número de empresas. Normalmente os provedores terão vários

data centers em diferentes locais para garantir um serviço de qualidade em todo mundo, bem como redundância em caso de interrupções [47].

2.15.6 Fatores a considerar antes de escolher um Provedor de VoIP

Provedores de VoIP variam muito no custo e no nível de serviço que eles fornecem, no entanto, quando vamos escolher um provedor deve-se ter atenção se eles oferecem os recursos e o nível de serviço que a empresa precisa. Abaixo estão alguns fatores importantes a considerar na escolha de um provedor de VoIP [48].

- **Benefícios** – o fornecedor tem de atender às necessidades do cliente, fornecendo um sistema de suporte com base nos requisitos especificados pela empresa, deve também simplificar a utilização do serviço para obter a adaptação do serviço em toda organização. Examinar atentamente se o provedor prioriza o aconselhamento, o treinamento e a adaptação do utilizador final, para que possam aproveitar devidamente as comunicações unificadas (UC) [48];
- **Custos** - ao pagar por um fornecedor, devem ser definidas necessidades de negócios em termos de requisitos de telefonia antes de solicitar uma cotação. Isso ajuda a garantir que a cota seja feita numa boa base, também devemos nos certificar de que o preço é transparente e os serviços de suporte incluídos devem estar bem explícitos. Podemos ver que alguns provedores oferecem pacotes com todos estes requisitos inclusos, nos quais todos os recursos estão incluídos por um único preço, por utilizador mensalmente, enquanto outros propõem uma taxa inicial baixa com cada recurso suplementar, resultando numa cobrança adicional. Podemos evitar surpresas desagradáveis informando-nos sobre os custos das chamadas em pacotes, bem como qualquer extra que o provedor adicione [48];
- **Integração com outros serviços** - outro aspeto importante a considerar é se o provedor de VoIP funciona com outros serviços, por exemplo se já existir implementado um serviço na empresa, sem a integração de serviços perde-se tempo migrando ou recriando dados corporativos existentes [48].

2.16 Trabalhos relacionados

Os autores Sarwar Khan e Nouman Sadiq [49] descrevnum esquema PBX baseado em VoIP utilizando um servidor Asterisk e a plataforma OPNET. O OPNET é um simulador de rede e foi utilizado para implementar a mesma topologia de rede para diferentes números utilizadores e diferentes CODECs de voz, o atraso de ponta a ponta é medido de um cliente para outro. Também foi feita uma comparação para descobrir qual o CODEC tem o mínimo de atraso.

A medida em que a Internet evolui para uma comunicação onipresente, a rede VoIP se torna mais importante e popular, Wewei Zhang, Youngyu Chang, Yitong Liu e Yuan Tian [3] realizaram uma investigação para quantificar o impacto do comprometimento da rede e a voz relacionando parâmetros na perceção de QoS em redes VoIP, dando uma contribuição tripla. Primeiro: é feita uma simulação, o software de simulação de rede é Wanem, o Protocolo de comunicação de voz é implementado pelo OpenPhone. Segundo: Foram analisados os fatores que afetam a perceção da QoS das redes VoIP. Terceiro: foi usado o algoritmo *New Perceptual Evaluation of Speech Quality* (NPESQ) para valiar o valor de Qos percebido sob diferentes parâmetros de deterioração IP para redes VoIP.

O protocolo de voz sobre Internet (VoIP) é uma nova maneira de se comunicar, permitindo aos utilizadores fazerem chamadas telefónicas através de rede IP. Os autores Sheetal Jalendry, Shradha Verma [50], descrevem o VoIP á nível de implementação atendendo a preocupação das empresas como os fatores que afetam a qualidade de serviço, os componentes de um sistema VoIP como equipamentos de utilizadores finais, equipamentos de redes, processadores de chamadas, *gateways*, além de uma introdução sobre a tecnologia VoIP: estrutura de rede, protocolos. A pesquisa é finalizada com uma discussão sobre a viabilidade de fornecer serviços VoIP sobre links de satélite.

A Internet revolucionou os sistemas de telecomunicações ao suportar novos aplicações e serviços. O *Voice Over Internet Protocol* (VoIP) é um dos serviços de telecomunicação notáveis baseados no protocolo de Internet (IP). A qualidade do sinal de sistema VoIP depende de vários fatores, como a condições de rede, processos de codificação, conteúdo de voz e esquemas de correção de erros. Os autores Harjit Pal Singh, Sarabjeet Singh, J Singh, S.A. Khan [15] revisam estas questões, utilizadas para fornecer serviço de comunicação de qualidade em comparação com as chamadas de rede telefónica pública comutada (PSTN), e de forma resumida foram abordados os avanços para melhorar o serviço do sistema VoIP.

Os autores Benedikt Machens, Olaf Gebauer e Diederich Wermser [20], explicam como funciona a fraude nos sistemas VoIP e quais ataques são executados. Essas pesquisam foram feitas utilizando como exemplo um PBX em *HONEY POST* ferramenta que tem a função de simular falhas de um sistema e colher informações do invasor, e são apresentadas possibilidades de proteção de sistemas VoIP contra fraude. Também os autores Stefan Hofbauer, Kristian Beckers e Gerald Quichmayr [51] propõe um método para analisar registos de comunicação com o objetivo principal de prevenir ataques de VoIP.

2.17 Conclusão

Em suma, após serem analisados os trabalhos, conclui-se que para desenhar e implementar uma solução VoIP, é importante um estudo dos componentes desta solução como protocolos, QoS, CODECs, Softwares e fatores que a afetam (Fraude VoIP, qualidade de sinal), o que possibilita entender o funcionamento, aplicabilidade e o custo tanto a nível monetário como a nível de utilização de recursos de hardware.

Capítulo 3

3 Implementação

Neste capítulo são apresentados o desenho e a solução proposta, e os mecanismos de implementação da solução no âmbito dos objetivos propostos para esta dissertação. A primeira parte do capítulo são apresentados o desenho e a arquitetura da rede, assim como os equipamentos de rede utilizados para a implementação dessa solução. A segunda parte do capítulo são apresentadas as configurações dos servidores e dos clientes.

3.1 Fases de desenvolvimento

A Figura 3.1 descreve as fases de trabalho, que teve início em outubro de 2017, começando por fazer um estudo sobre a tecnologia VoIP, seu crescimento a nível de implementação ou utilização, os critérios a serem levados em conta para a escolha de PBX IP, Sofphone, provedores VoIP e equipamentos VoIP. Com o crescimento dessa tecnologia também têm surgido alguns problemas, como atrasos na comunicação, perda de pacotes, fraude e outros, que também foram investigados para a escrita desta dissertação. Após serem feitos os estudos sobre o funcionamento da tecnologia foi definida a arquitetura e desenho da solução, dando seguimento com a implementação da solução.

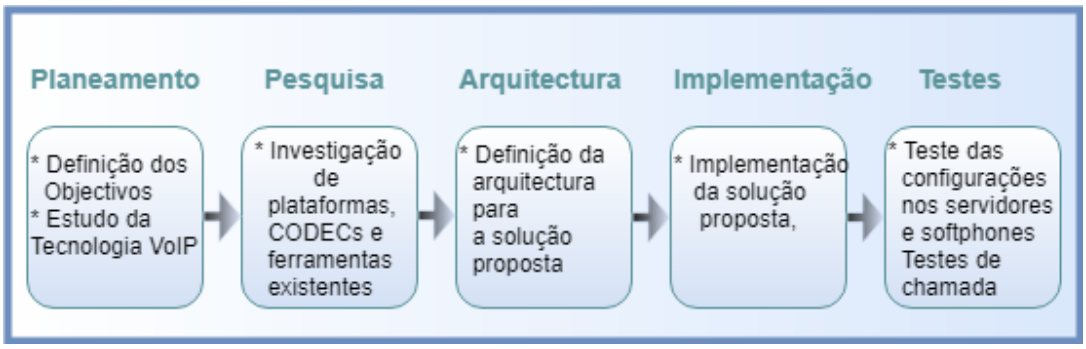

Figura 3.1: Fases de Desenvolvimento.

3.2 Desenho e arquitetura da rede

Na solução propõe-se duas redes para uma empresa com uma Matriz e uma Filial, a rede Matriz com o endereço IP 192.168.20.0 máscara de rede

255.255.225, e a outra Filial com o endereço IP 192.168.10.0 e máscara de rede 255.255.225.0, objetivando a comunicação local e externa. A infraestrutura proposta é composta por dois routers supostamente localizados em diferentes cidades. Os mesmos farão a transferência de pacotes de um ponto para o outro (Matriz e Filial), são conectados a provedores de Internet por um cabo direto de fibra ótica. Também são utilizados dois switch em cada rede (Matriz e Filial) para permitir a comunicação local e externa dos nós. No switch de cada rede é conectado um servidor VoIP, estes servidores farão a gestão central da telefonia VoIP. Por fim os clientes que são os Telefones IP, lembrando que um softphone é um telefone IP (capítulo 2, subtítulo 2.6). Neste cenário tanto para Matriz, como para Filial, existe a chamada local (dispositivos na mesma rede comunicam-se) e a externa (dispositivos em redes distintas comunicam-se) com o número 1000 para Matriz e 2000 para Filial, tendo a comunicação dependente dos equipamentos de redes acima referidos. Este cenário é baseado em simulação com equipamentos reais, a Figura 3.2 mostra o desenho da rede.

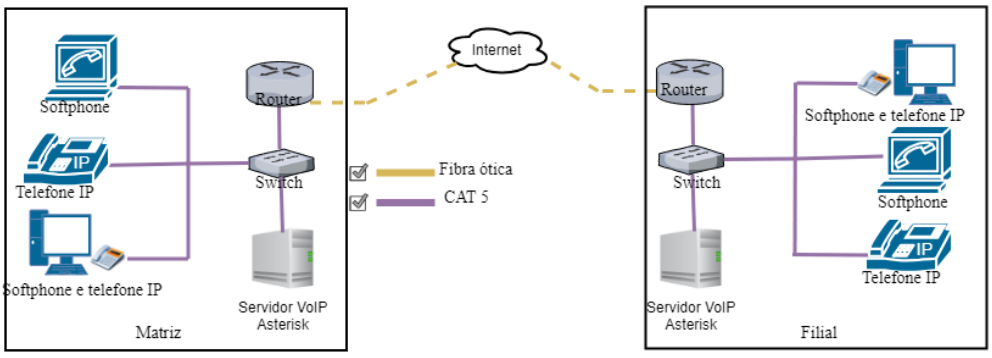

Figura 3.2: Desenho da solução proposta.

Este é o desenho real proposto, que para sua implementação seriam necessários os seguintes equipamentos de rede, tais como, dois routers (um para Matriz e outro para Filial), de igual modo dois switchs, além de computadores (Softphones) e outros telefones IP. Mas devido a dificuldades na obtenção de equipamentos para a implementação e consequentes testes, foi preciso simplificar, fazendo um router *on-a-stick*, que é uma técnica utilizada para permitir que diferentes redes se comuniquem com apenas um

único router. Dentro da mesma dificuldade também será utilizado apenas um switch, a Figura 3.3 ilustra a técnica router *on a stick*.

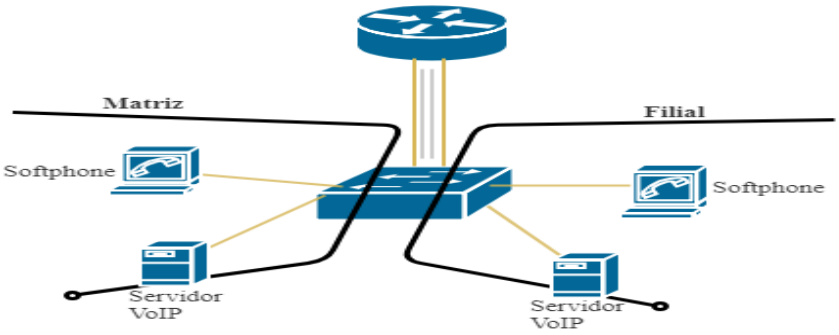

Figura 3.3: Router *on a Stick*.

3.3 Equipamentos e ferramentas utilizadas

A solução foi implementada com o auxílio de equipamentos de redes router e switch Cisco, Softwares VoIP Astrisk e X-lite, e a ferramenta para virtualização de máquinas Oracle VirtualBox, como ilustrado na Figura 3.4.

Figura 3.4: Equipamentos e ferramentas utilizadas.

Após o desenho deste cenário são descritas nesta subseção as funções e configurações que foram feitas nos equipamentos que compõe a infraestrutura de rede proposta:

- **Router** – Para a arquitetura de rede deste cenário, foi o utilizado o router CISCO 2600 com apenas uma porta FastEthernet que é a 0/0 , o router terá como função encaminhar os pacotes entre as redes (Matriz e Filial), foram feitas configurações como a criação de duas interfaces lógicas, a interface lógica FastEthernet0/0.10 com o endereço IP 192.168.10.1 e a máscara de rede 255.255.255, a outra

é a FastEthernet0/0.10 com o endereço IP 192.168.20.1 e máscara de rede 255.255.255, fazendo com que na mesma porta haja comunicação entre as duas redes diferentes.

- **Switch** – O switch a ser usado é o CISCO Catalyst 2950, de switch 24 portas com a função de encaminhar os pacotes, manter a comunicação local e externa. Nos switchs foram configurados as duas VLANs uma representa a rede Matriz que é a VLAN 20 e outra representa a rede Filial que é a VLAN 10, também foram associadas às VLANs às portas do switch, a VLAN 20 associada a porta fa0/2 e VLAN 20 na porta fa0/3 FastEthernet0/1, a porta *trunk é* fa0/1.

Numa única rede podemos ter dados e voz, mas para uma boa implementação VoIP numa rede convém que seja feita a segmentação de VLAN, ou seja uma VLAN de dados e uma VLAN de voz, o que é benéfico tanto para o sistema de voz tanto para a rede como um todo. Estes benefícios podem ser:

- **Qualidade de chamada (desempenho)**: com a segmentação de VLANs é provável um aumento na qualidade das chamadas, porque os pacotes VoIP não competem com os pacotes de dados pela prioridade, o VoIP é muito menos tolerante a pacotes perdidos do que os serviços de dados. Colocar o VoIP em sua própria VLAN permite que se tenha prioridade máxima na rede, o que permite uma análise eficiente dos fatores que comprometem a qualidade de serviço e monitoração da qualidade de voz [52].
- **Segurança**: Uma grande preocupação entre as empresas que implementam o VoIP é o aumento dos riscos de segurança. Pela existência de fraudes em VoIP. A segmentação de VLAN permite que seja implementado sistema de seguranças mais fortes, possibilitando a implantação de protocolos de segurança específicos para VoIP que mantêm as chamadas seguras, mas podem interferir no tráfego de dados caso as redes estejam numa única VLAN [52].
- **Resolução de Problemas**: Geralmente, é difícil identificar um dispositivo com desempenho inadequado ou um desempenho inferior numa rede mista, por haver tipos diferentes de tráfego fluindo de uma só vez. O que dificulta a identificação de um elo fraco na rede ou a localização de dispositivos que criam afunilamento no tráfego. Com a segmentação o tráfego de VoIP é distinto e mantido somente para o VoIP. Os dispositivos que usam essa VLAN lidam com tipos de pacotes muito regulares e previsíveis, o que facilita muita a solução de problemas. Quando há apenas um tipo de tráfego, os pontos de uma rede se destacam muito facilmente [52].

3.4 Servidor VoIP

O servidor VoIP é a parte de telefonia VoIP que auxilia no processamento de dados e também responde as solicitações recebidas dos clientes. Um servidor pode ser um Software Asterisk ou Hardware, sendo um Software pode ser na maioria dos casos mais económico a nível de implementação e manutenção. Com um funcionamento adequável às necessidades dos utilizadores. Um servidor pode ou não ter grandes capacidades em termos de memória e armazenamento em disco, dependendo das solicitações de chamadas simultâneas, assim sendo para um grande número de solicitações é necessário um servidor potente em termos de processamento, para responder de forma eficiente a solicitações simultâneas de clientes na rede [53].

No entanto, o servidor VoIP disponibiliza recursos de dados e hardware, como impressoras, dispositivos de armazenamento e processadores acessíveis a partir de outros computadores. O servidor VoIP ou o IP PBX é extremamente importante para as soluções VoIP. Para aumentar ainda mais a sua utilidade, é possível adicionar recursos, como videoconferência, IVR (resposta de voz interativa). É no servidor VoIP onde são configuradas as extensões, o encaminhamento de chamadas, o tipo de comunicação e outros serviços VoIP [53].

3.4.1 Funcionamento de um servidor VoIP

O funcionamento de um servidor VoIP é semelhante a um servidor proxy. O servidor recebe as solicitações dos clientes e através de vários processos auxilia na implantação do sistema de telefonia IP. O processo envolve simplesmente o encaminhamento de solicitações ou processamento de informações á medida que elas passam pelo servidor. Por exemplo, quando o servidor recebe uma mensagem de solicitação do utilizador convidando um outro cliente para ingressar numa sessão, o servidor atua como um proxy e encaminha esse convite ao destino. Por meio de um servidor VoIP, é possível transferir o sistema de telefonia tradicional para um sistema dedicado baseado em servidor [53].

3.4.2 Funções de um servidor VoIP

São apresentadas algumas das funções importantes de um servidor VoIP:

- **Roteamento** – um servidor VoIP faz a gestão do roteamento de chamadas. Ele procura por dois pontos de extremidade e encontra o melhor caminho para enviar as informações de uma extremidade para à outra. Existem algoritmos que ajudam a determinar o caminho mais curto e seguro, sendo esse um processo automatizado, exclui-se a necessidade de uma entrada manual [53].
- **Conexão com protocolos diversos** – o servidor VoIP permite a comunicação com vários protocolos. Podem ser adicionados módulos que implementam diferentes protocolos, ou seja os servidores VoIP assumem o papel de um conversor para interconexão de diferentes tipos de protocolos.
- **Administrar Clientes** – para uma QoS reconhecida numa solução VoIP, é importante administrar os clientes existente numa rede VoIP, desde registos que contêm as contas dos mesmos e o número de clientes que usam o serviço VoIP na rede.
- **Outras funções** – existem também outras funções como, rejeição de chamadas desconhecidas, *black list*, encaminhamento de chamadas, chamada em espera, identificador de chamadas, bloqueio de indentificadores de chamada e outras.

Para a configuração de um servidor VoIP existem vários softwares pagos e gratuitos (capítulo 2, subtítulo 2.4). Para solução proposta, entre os softwares para servidores VoIP, será utilizado o Asterisk por ser gratuito sem custos de licença, pode ser executado em qualquer máquina sem grandes requisitos a nível de processamento e armazenamento, dependo claro do número de utilizadores ou clientes na rede, funciona com os mais diversos telefones utilizados em VoIP. É muito escalável, ou seja, o Asterisk pode ser implantado numa empresa com um número pequeno de utilizadores inicialmente e depois permite que o número de utilizadores aumente. Também funciona com a maioria dos provedores de telecomunicações. O Asterisk é diferente de muitos outros softwares para servidores VoIP pois permite personalizar o PBX IP à nossa maneira.

3.4.3 Instalação do Asterisk

De modo a poupar recursos de hardware o que tem impacto no custo, e como anteriormente foi exposta a dificuldade de equipamentos para a

implementação desta solução, atendendo a esse impasse, optou-se por alojar os servidores em máquinas virtuais, essas máquinas virtuais foram criadas em dois computadores. Num computador foi criada uma máquina virtual para alojar o servidor Matriz e no outro para alojar o servidor Filial, foi instalado o sistema operativo (S.O) Linux Ubuntu 17.10 nas máquinas virtuais de ambos os computadores. O Hypervisor utilizado é o Oracle VM VirtualBox.

Depois de serem criadas e ser feita a instalação do S.O (Ubuntu 17.10) nas máquinas virtuais alojadas nos distintos computadores, seguiu-se com a instalação do Asterisk no S.O das mesmas hospedadas em ambos os computadores, a instalação do Asterisk foi feita via terminal Figura 3.5.

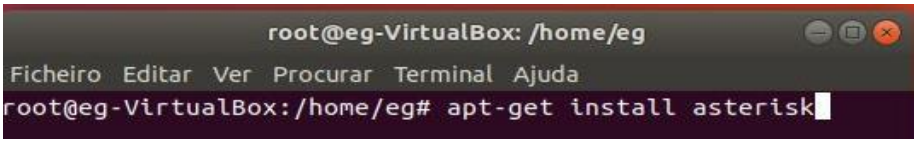

Figura 3.5: Instalação do Asterisk.

A seguir a mensagem de confirmação caso não existam erros na atualização de pacotes úteis para o funcionamento do Asterisk contendo informações da utilização de espaço em disco, pacotes sugeridos e instalação automática de alguns pacotes necessários Figura 3.6.

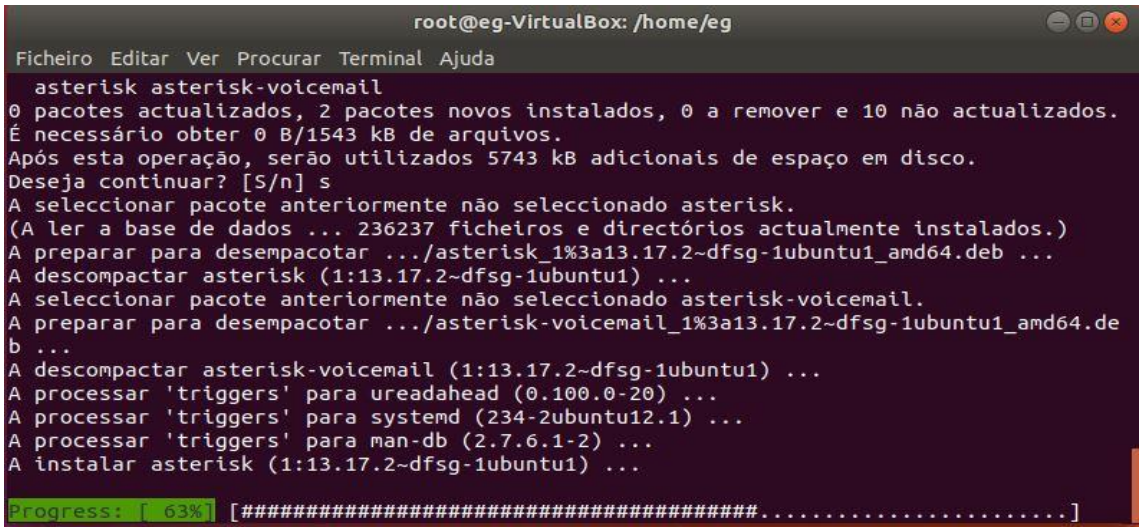

Figura 3.6: Instalação em Progresso.

Pode-se confirmar se a instalação foi bem-sucedida Figura 3.7, com o comando `asterisk -r cvv`.

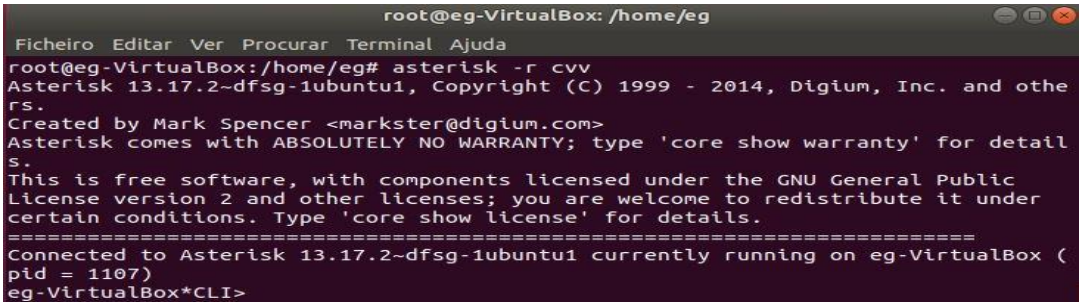

Figura 3.7: Abrindo o Asterisk.

3.4.4 Diretorias de alguns ficheiros

Depois da instalação do Asterisk são criadas uma série de arquivos e diretórios:

- `/etc/asterisk`

O Asterisk, é configurado através de ficheiros de configuração que podem ser localizados no diretório acima citado. Após entrar na pasta ou diretório, com o comando pode-se listar os ficheiros de configuração do Asterisk Figura 3.8. O Asterisk funciona com os comandos Linux desde que colamos o caracter especial “!” antes do comando.

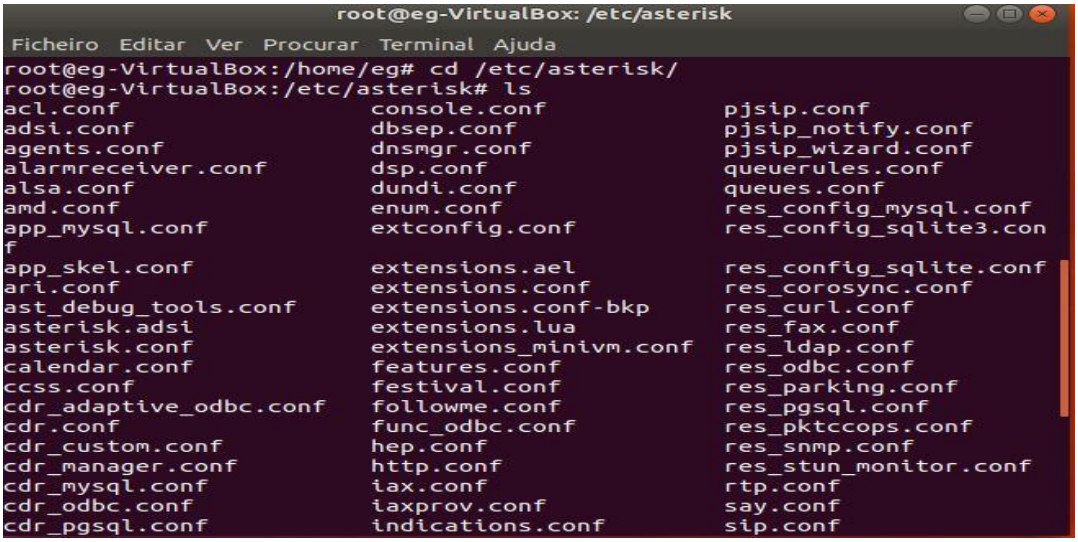

Figura 3.8: Ficheiros de configuração.

Dentro detse diretório existem vários ficheiros de configuração Figura 3.9, como o **sip.conf**, onde serão feitas as configurações dos clientes SIP, **extensions.conf** onde serão feitas as configurações do plano de marcação, **iax.conf** ficheiro de configuração de clientes IAX, **meetme.conf** para configurar salas de conferências, **queues.conf** para configurar filas de atendimento, **musiconhold.conf** configurar música de espera e **logger.conf** para habilitar e desabilitar *logs* do Asterisk . A lista é enorme para uma investigação mais profunda podemos pesquisar em www.asterisk.org.

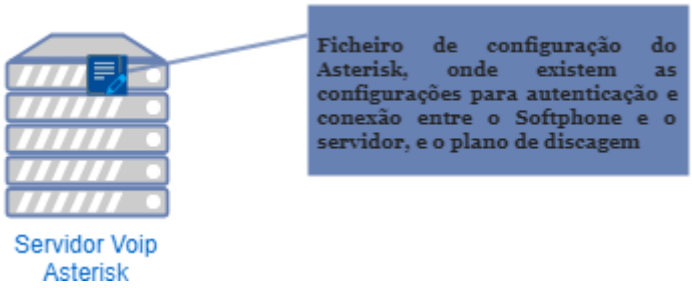

Figura 3.9: Processo de configuração.

- /usr/lib/asterisk/modules

Módulos Asterisk, módulos carregáveis no formato *Shared object*, carregados na instalação do Asterisk, também podem ser criados pelos utilizadores. Existe uma variedade de módulos, diferentes e cada um fornece suas funcionalidades próprias e recursos para o asterisk.

- /var/lib/asterisk

Diretório de Base de Dados, é utilizado para guardar o ficheiro de dados da base de dados interna do Asterisk. Esta base de dados é usada internamente e é disponibilizada para os programadores e administradores do Asterisk. As versões do Asterisk até 1.8 utilizavam o Berkeley DB, e na versão 10 o projeto foi mudado para a base de dados SQLite3.

- /var/spool/asterisk

Diretórios de *spool*, este diretório é utilizado para armazenar ficheiros de spool de vários componentes fornecidos módulo e pelo núcleo do Asterisk. A maioria destes ficheiros utilizam os seus próprios subdiretórios, são eles - *dictate*, meetme, *monitor, outgoing, recording, system, tmp, voicemail*.

- /var/log/asterisk

Saída de registos, diretório de armazenamento de configuração de saída de registos. O login no Asterisk é um mecanismo importante que pode ser utilizado para extrair informações precisas de um sistema em execução. Atualmente o Asterisk tem a capacidade de registar mensagens em vários locais (diretórios) engloba ficheiros, consolas e o recurso de syslog.

- /usr/sbin

Diretório do código binário, por padrão, o Asterisk procura neste diretório por quaisquer binários do sistema que ele utiliza.

3.5 Configuração dos Servidores

Antes de serem feitas as configurações do servidor, foram utilizados os nomes Covilhã que representa o servidor da rede Matriz e Lisboa que representa o servidor da rede filial nos ficheiros de configuração de cada um dos servidores correspondentes (Matriz e Filial), lembrando que A rede Filial foi configurada com o endereço IP 192.168.10.1 e o seu servidor com o endereço 192.168.10.101, já a rede Matriz com o IP 192.168.20.1 e o seu servidor 192.168.20.201.

- **Configuração Servidor (Filial)**

Para a solução proposta entre os ficheiros acima mencionados foram configurados os ficheiros **sip.conf** e **extensions.conf.** No ficheiro **sip.conf** do servidor Filial (Lisboa) que foi configurado com o IP 192.168.10.101, teve as seguintes configurações, registo do Matriz configurado com o IP 192.168.20.201, para dar início ao processo de registo do servidor um no outro, almejando como consequência a comunicação entre os servidores.

De seguida foram criadas as contas dos clientes do servidor Filial (1000, 1001) com as suas respetivas senhas e o tipo de CODEC a ser usado, não é obrigatório no ato de configuração definir o nome do utilizador assim como também, definir senhas.

Ainda no servidor Filial no ficheiro **extensions.conf**, foram feitas a seguintes configurações para o plano de discagem local e externo. Quando um cliente da rede Filial disca para um número fazendo um pedido ao servidor (Filial), o servidor recebe o pedido e verifica se o número existe ou está operacional (online), se estiver o servidor Filial redireciona a chamada para o destinatário (prioridade da chamada definida 1), se não estiver envia o pedido para o outro servidor, no caso o servidor Matriz (prioridade da chamada definida 2), se o servidor Matriz verificar que o número ou conta exista e está operacional, faz o mesmo que o servidor Filial "redireciona a chamada para o destinatário correspondente, se o servidor Matriz não encontrar esse número, a chamada é rejeitada, essa configuração foi feita nos dois servidores e o funcionamento é exatamente o mesmo .

- **Configuração Servidor (Matriz)**

No servidor Matriz (Covilhã) com o IP 192.168.20.201, também foram configurados os ficheiros **sip.conf** e **extensions.conf.** O ficheiro sip.conf teve as mesmas configurações que o ficheiro **sip.conf** do servidor Filial, diferenciando apenas o IP para fazer o registo do servidor Filial no servidor Matriz 192.168.10.101(IP servidor Filial), o que possibilita a comunicação

entre os servidores. A criação dos clientes SIP (2000,2001) com as suas respetivas senhas.

As configurações do ficheiro **extensions.conf** neste servidor também são parecidas, se um cliente nessa rede faz um pedido ao servidor discando para um número *online*, o servidor (Matriz) encaminha a chamada para o destinatário (prioridade da chamada definida 1), caso o servidor Matriz não encontre esta conta correspondente ao pedido ou esteja *offline*, o pedido é transferido para o outro servidor (Filial) (prioridade da chamada definida 2), o servidor Filial recebe o pedido e verifica se o cadastro existe, se existir redireciona ao destinatário, senão existir rejeita a chamada.

3.6 Softphone

Para os clientes, na solução foram utilizados telefones IP no caso softphones nos dois computadores. O softphone utilizado é o x-lite versão 5.2.0, porque funciona com o protocolo SIP e IAX flexível a nível de interação e configuração, além de ser gratuito e com uma interface mais parecida a um telemóvel, com histórico de chamadas e lista detalhada das mesmas.

3.6.1 Instalação e configuração

- **Instalação**

O softphone x-lite Figura 3.10, foi instalado em dois computadores (ASUS e TOSHIBA). Ambos com o sistema operativo Windows 10, com o IP 192.168.10.100 para o ASUS que representa a rede Filial e, com o IP 192.168.20.200 Toshiba que representa a rede Matriz. É possível fazer o *download* deste softphone que é gratuito para testes no site oficial www.counterpath.com.

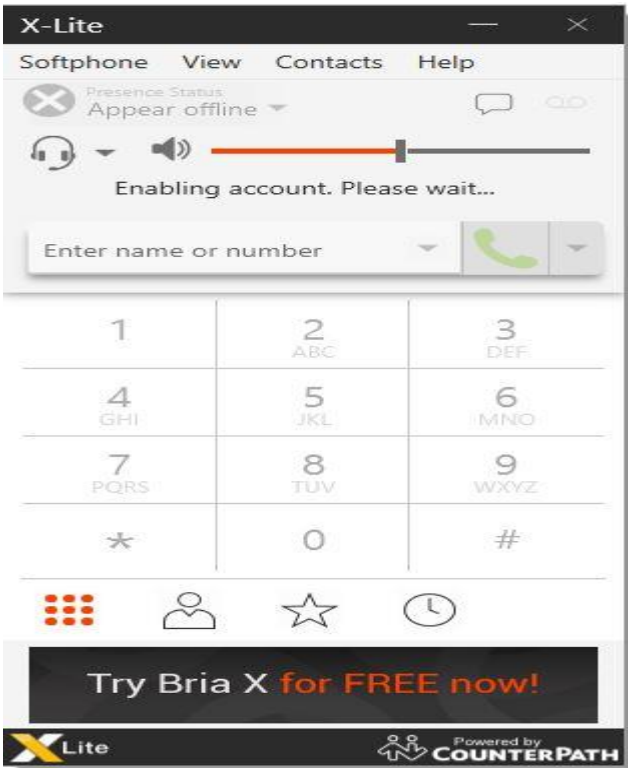

Figura 3.10: Softphone X-Lite.

- **Configuração**

O propósito dessa configuração é fazer com o que os clientes através dos sofphones se comuniquem. Para tal é necessário que o softphone faça a autenticação no servidor Figura 3.11, com a respetiva senha e nome da conta, para que a autenticação se efetive o nome da conta e senha devem ser correspondentes a uma das contas criadas num dos servidores.

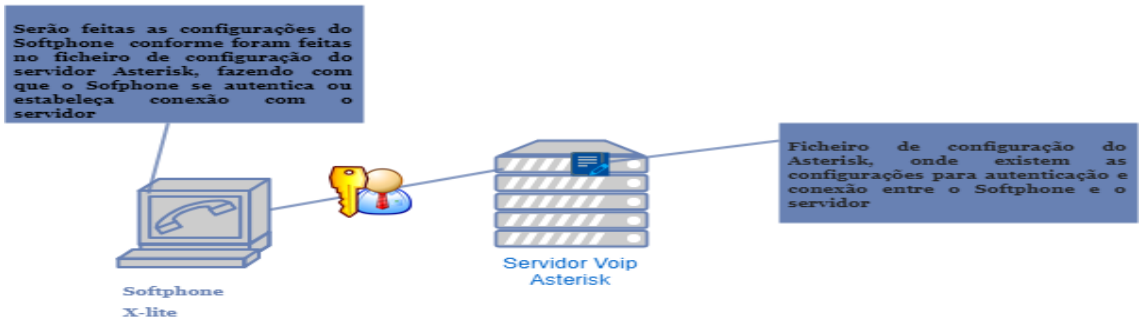

Figura 3.11: Configuração para autenticação dos Softphones no servidor.

Para a configuração do x-lite lembrado que a configuração é a mesma para os outros softphones a serem utilizados temos os seguintes passos:

- 1º Executar o x-lite;
- 2º Clicar em no menu softphone, abrirão dois submenus *accounting settings* e *preferences*, Figura 3.12;

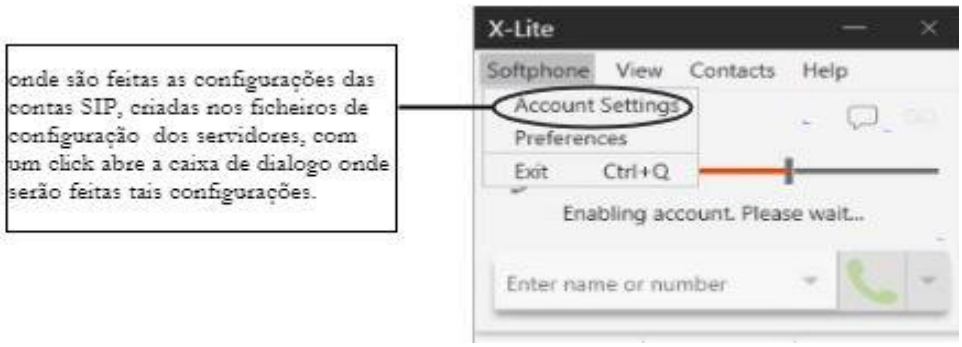

Figura 3.12: Abrir o formulário de configuração.

- 3º Pressionar no submenu *accouting settings*, abre a janela SIP *Account*, Figura 3.13.

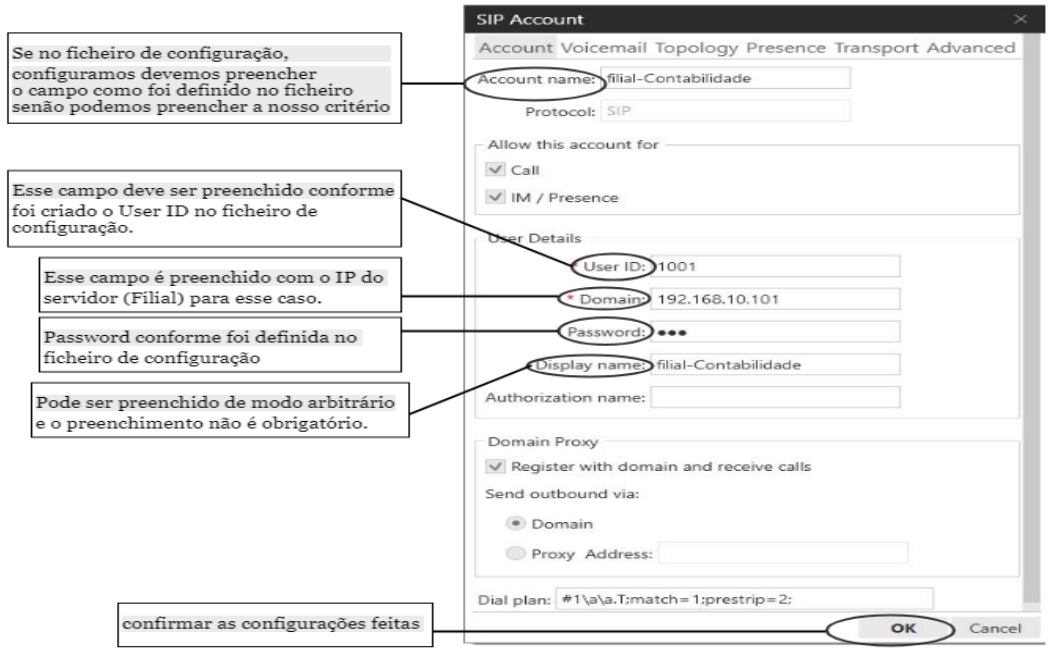

Figura 3.13: Configurando conta de utilizadores no Softphone

Após a configuração podemos ver o softphone conectado ao servidor e disponível, ou seja, pronto para receber e fazer chamadas como mostra a Figura 3.14.

Figura 3.14: Sofphone conectado.

Capítulo 4

4 Resultados

Neste capítulo são apresentados os resultados e analises destes resultados, desde a configuração de utilizadores nos ficheiros de configuração dos servidores o que permite a autenticação dos mesmos aos servidores, até os recursos que a solução oferece aos utilizadores finais.

Na primeira parte da secção são apresentados os utilizadores configurados nos servidores lembrando que o servidor Filial cadastrado no servidor Matriz é um cliente, o mesmo serve para o servidor Matriz cadastrado no servidor Filial, também são apresentados os passos de autenticação nos servidores, em ambiente gráfico, que envolvem os utilizadores desde autenticação até a realização de chamadas tanto locais como as externas.

Para ambos os casos de ligação serão também apresentados alguns testes que de rejeição de chamada de um uma conta inexistente no servidor apresentando um relatório no servidor na CLI do Asterisk.

4.1 Clientes/utilizadores criados

Como referido anteriormente, as contas dos utilizadores são configuradas nos servidores com os respetivos números e senhas, que servem de autenticação para a utilização das mesmas contas. A Figura 4.1 mostra as contas de utilizadores criadas no servidor Matriz, e a Figura 4.2 mostra as contas de utilizadores no servidor Filial

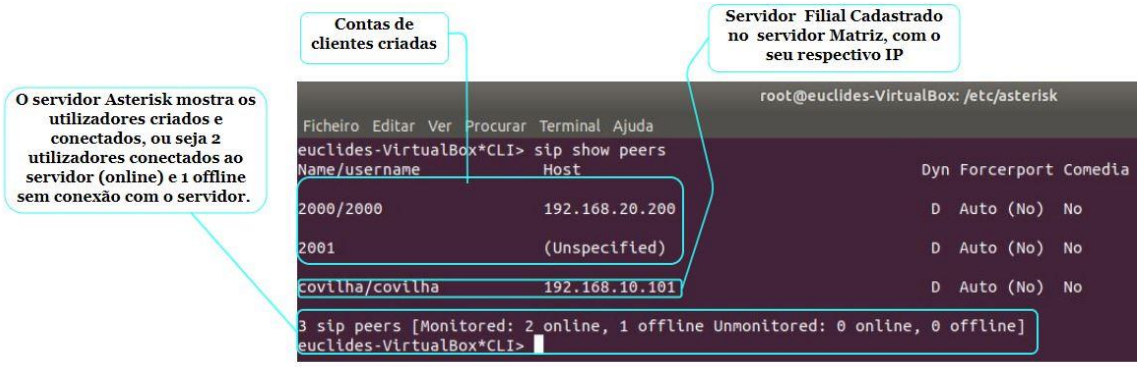

Figura 4.1: Visualização dos utilizadores criados no Servidor Filial.

Figura 4.2: Visualização dos utilizadores criados no Servidor Matriz.

Para a que haja comunicação entre as distintas redes é preciso que os servidores se comuniquem, a Figura 4.3 apresenta o servidor Filial a identificar o registo do servidor Matriz.

```
root@eg-VirtualBox:/home/eg# asterisk -r cvv
No ethernet interface found for seeding global EID. You will have to set it manually.
Asterisk 13.17.2~dfsg-1ubuntu1, Copyright (C) 1999 - 2014, Digium, Inc. and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=========================================================================
Connected to Asterisk 13.17.2~dfsg-1ubuntu1 currently running on eg-VirtualBox (pid = 922)
[May 29 22:25:41] WARNING[1152]: acl.c:939 ast_ouraddrfor: Cannot connect to 192.168.20.201: Network is unreachab
[May 29 22:25:41] WARNING[1152]: chan_sip.c:3785 __sip_xmit: sip_xmit of 0x7f746c01b460 (len 416) to 192.168.20.2
[May 29 22:25:41] ERROR[1152]: chan_sip.c:4274 __sip_reliable_xmit: Serious Network Trouble; __sip_xmit returns e
[May 29 22:25:41] NOTICE[1152]: chan_sip.c:15875 sip_reg_timeout:    -- Registration for 'covilha@192.168.20.201'
[May 29 22:25:41] WARNING[1152]: acl.c:939 ast_ouraddrfor: Cannot connect to 192.168.20.201: Network is unreachab
[May 29 22:25:41] WARNING[1152]: chan_sip.c:3785 __sip_xmit: sip_xmit of 0x7f746c00d8f0 (len 418) to 192.168.20.2
[May 29 22:25:41] ERROR[1152]: chan_sip.c:4274 __sip_reliable_xmit: Serious Network Trouble; __sip_xmit returns e
[May 29 22:25:41] NOTICE[1152]: chan_sip.c:15875 sip_reg_timeout:    -- Registration for 'covilha@192.168.20.201'
eg-VirtualBox*CLI>
```

Figura 4.3: Comunicação entre os Servidores.

Também para os utilizadores (Softphones), o servidor reporta se a autenticação foi bem-sucedida, estando esse cliente pronto para fazer chamadas entre os demais clientes na rede, como mostra a Figura 4.4.

A autenticação dos clientes na rede é importante, porque faz partes dos requisitos de segurança da rede VoIP. Como exemplo, supomos que alguém tem acesso a rede e que existem contas criadas, e que essas contas foram configuradas sem senhas. O elemento conectado a rede pode fazer um pedido ao servidor para ser associado a umas das contas existentes basta que esteja conectado a rede e saiba o nome da conta. Mas com uma conta protegida por uma senha a autenticação só é possível caso ele conheça essa senha, na Figura 4.5 mostra a falha na autenticação.

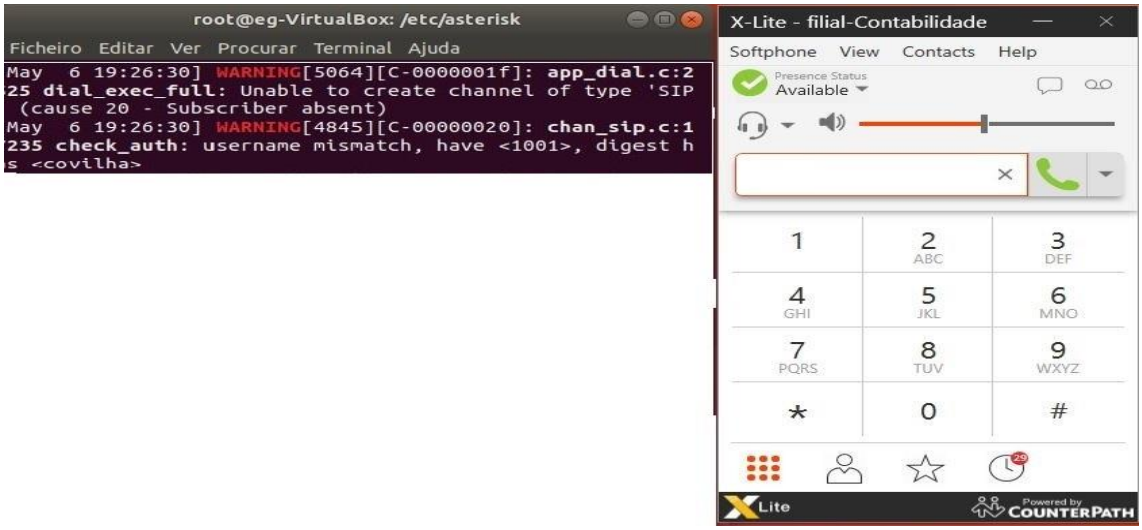

Figura 4.4: Comunicação entre o Softphone e o Servidor.

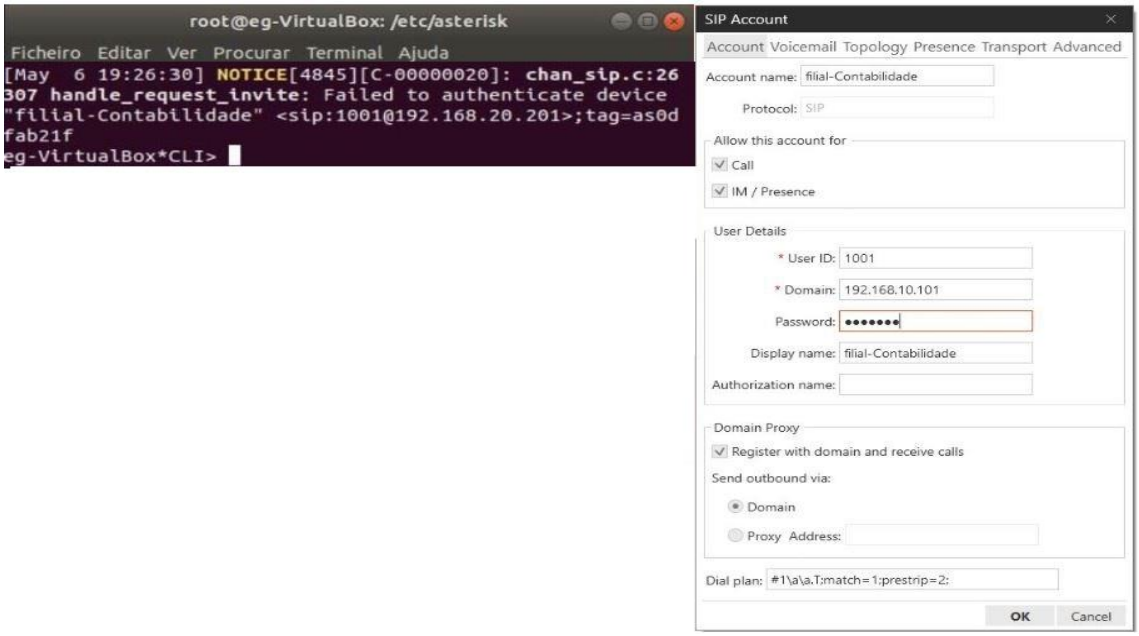

Figura 4.5: Falha na Autenticação pelo Softphone.

Testes de Chamadas

De acordo com a solução proposta para essa dissertação, onde foram definidas as duas redes, essas redes foram configuradas de maneiras a existir uma comunicação local e uma comunicação externa, assim sendo serão apresentados os testes de chamadas localmente e externas tanto para a Matriz como para a Filial.

- **Chamada local**

A Figura 4.6 mostra uma chamada local na rede Mariz entre o telefone IP Matriz-Contabilidade com o número 2001 e endereço IP 192.168.20.200, e a Matriz-RH (com o número 2000 e endereço IP 192.168.20.202), a Figura 4.7 mostra uma chamada local na rede Filial entre Filial-Contabilidade (com o número 1000 e endereço IP 192.168.10.100), e Filial-RH (com o número 1001 e endereço IP 192.168.10.102)

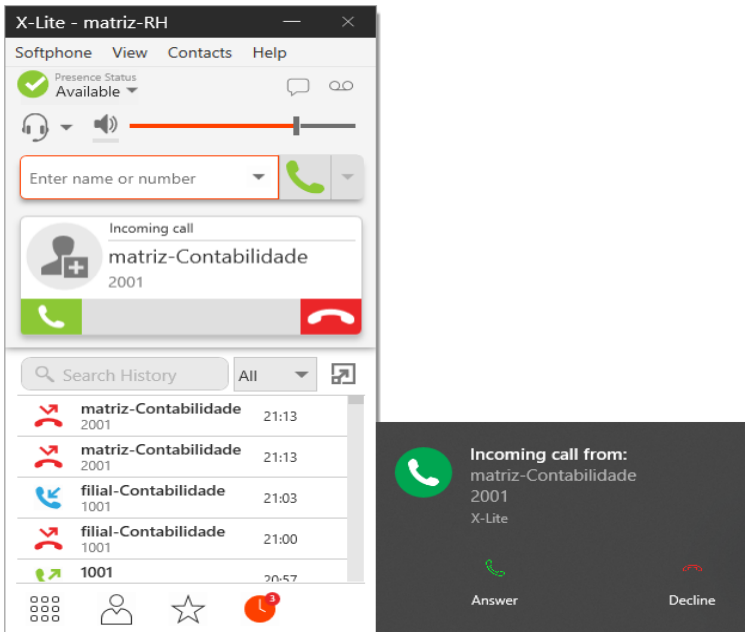

Figura 4.6: Teste de Chamada Local na Rede Matriz.

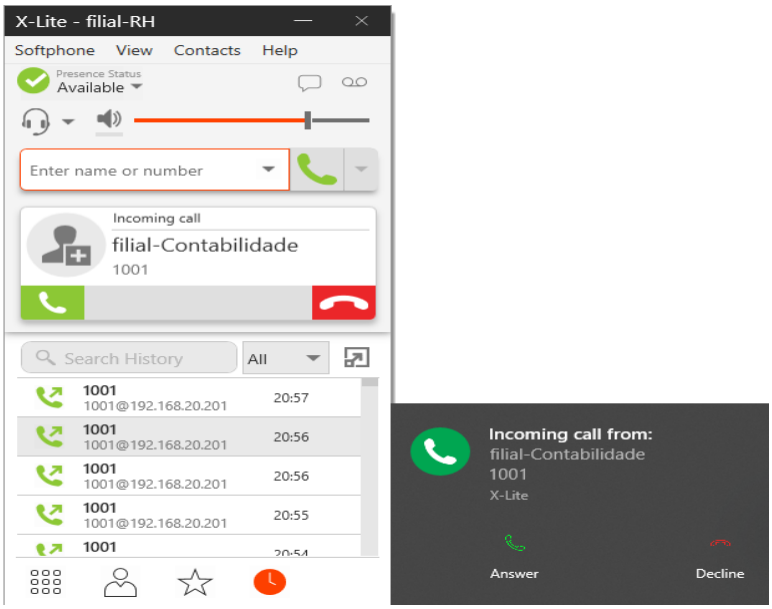

Figura 4.7: Teste de Chamada Local na Rede Filial.

- **Chamada externa**

A Figura 4.8 mostra uma chamada externa entre as distintas redes Mariz e Filial, essa chamada é feita entre o telefone IP Matriz-Contabilidade (com o número 2001 e endereço IP 192.168.20.200), e telefone IP Filial-Contabilidade (com o número 1001 e endereço IP 192.168.10.100).

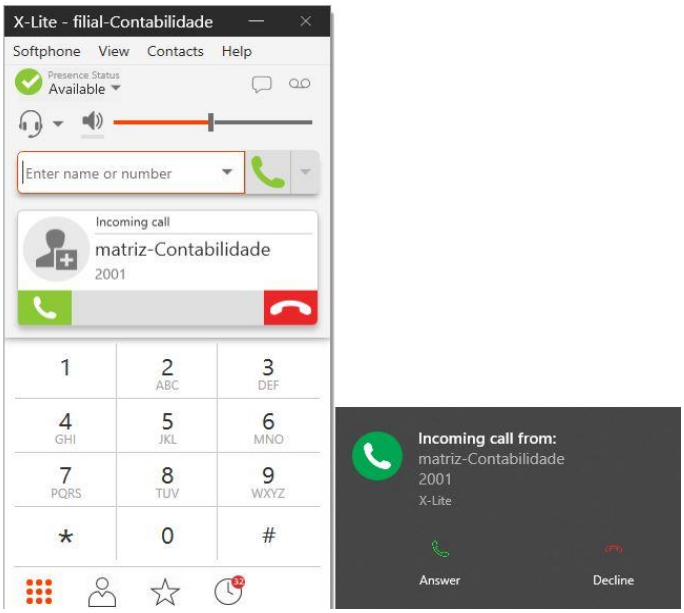

Figura 4.8: Chamada entre as duas redes (Filial e Matriz)

- **Rejeição de Chamada**

Quando existe rejeição de chamadas o servidor envia uma mensagem a notificar essa rejeição. A rejeição de chamadas pode ser vista de duas maneiras, uma é quando essas rejeições de chamadas são configuradas, definindo restrições de chamadas entre os utilizadores. A outra é quando o utilizador faz um pedido ao servidor (chamada), e o servidor verifica se existe esse utilizador na rede ou se está *online* , se existir faz o encaminhamento, e rejeição caso não exista ou não esteja online, a Figura 4.9 ilustra um dos tipos de rejeição de chamada.

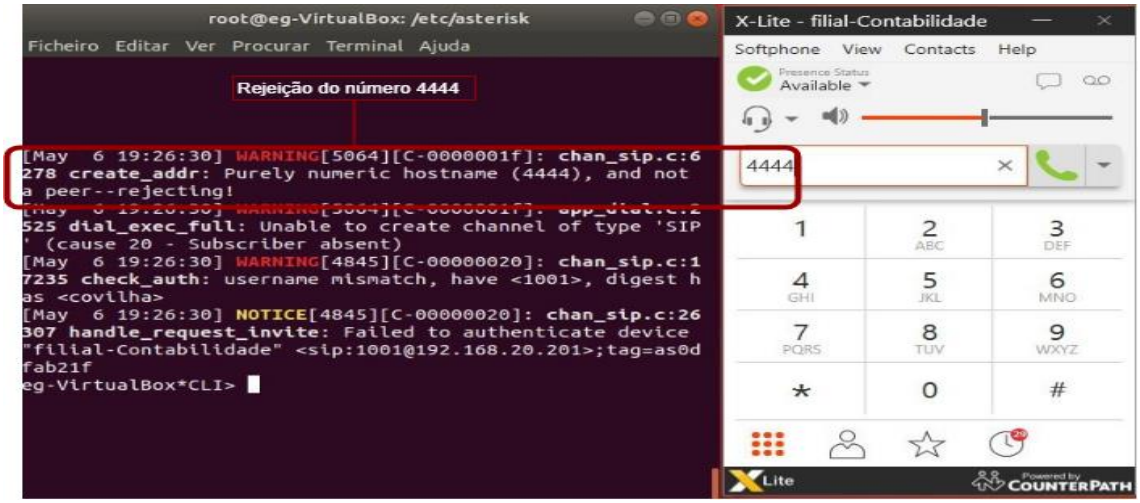

Figura 4.9: Notificação do servidor rejeitando a ligação do número 4444

Capítulo 5

5 Conclusão e Trabalho Futuro

Esta dissertação tem como objetivo principal o desenho e implementação de uma solução VoIP.

Para tal, foram analisados e comparados os elementos que compõem uma solução VoIP desde os sistemas para a montagem de um servidor VoIP (PBX IP), onde se verificou que os serviços fornecidos são em muitos casos semelhantes. Para garantir o desempenho de uma solução VoIP primeiro deve ser definida a infraestrutura de rede que essa solução vai utilizar, sendo o Asterisk e outros sistemas baseados no Asterisk uns dos mais utilizados, por serem *open source* e podem ser instalados como um servidor independente ou como parte de uma distribuição pré configurada que inclui o sistema operativo, também são de simples adaptação nas arquiteturas de redes existentes ou criadas, dando a liberdade de configuração ao administrador da rede.

A seguir devem ser levadas em conta questões importantes como o número máximo de chamadas simultâneas, gravação de voz e os CODECs a serem utilizados, sendo estes os processos que mais exigem do servidor. Para comunicação no VoIP podem ser utilizados vários CODECs, estes apresentam características diferentes como bit *rate*, *Mean Opinion Score* (MOS) e atraso de compressão.

Outro argumento de escolha é ainda o facto de que alguns deles são livres e outros exigem licenciamento. As suas características são de extrema importância pois só assim é possível escolher o CODEC ideal para a comunicação dependendo da largura de banda, porque a largura de banda e os requisitos do processador definem qual CODEC a ser utilizado. Os CODECs que fornecem a melhor qualidade consomem a maior parte da largura de banda. De acordo com as pesquisas feitas para a escrita desta dissertação o CODEC G.711 é o mais recomendável quando se tem alta largura de banda

pois fornece qualidade de voz não compactada, assim sendo, consome mais largura de banda (2.5 Mb/s). Com um servidor equipado com um processador Intel Dual Xeon 3.0 Ghz, 4 GB de RAM é possível fazer até 120 chamadas simultâneas com o CODEC 711 e G729.

Os equipamentos utilizados numa rede têm um impacto significativo na qualidade de chamada de voz, por isso a escolha de equipamentos também é um dos requisitos a considerar na implementação de uma solução VoIP. Para a escolha de um ATA ou router devem ser levados em conta fatores como técnicas de compactação (CODECs) suportadas, cancelamento de eco (mecanismo para diminuição de eco) e suporte de firewall. Também a escolha de telefones IP porque a frequência de telefones IP pode causar interferência nos outros equipamentos.

A Tecnologia VoIP funciona na infraestrutura das redes de dados, o que possibilita ter numa única rede dados e voz. Garantir a segurança e o bom funcionamento dos mesmos é preciso fazer a segmentação da rede, ou seja, separar o tráfego de dados e voz, o que facilita a detenção de problemas separadamente e como consequência as técnicas ou ferramentas para a resolução destes problemas, algumas ferramentas utilizadas para segurança de tráfego dados podem não proteger o tráfego de voz.

Ainda sobre segurança sobre, configurar os equipamentos VoIP na rede com IP estáticos e associar estes IP ao MAC *Address*, isso assegura que só os dispositivos configurados com o MAC *Address* podem funcionar na rede.

5.1 Sugestões de trabalhos futuros

Para trabalhos futuros, propõe-se a implementação das seguintes tarefas:

- Implementar e comparar os métodos abordados de redução de *jitter*, *delay* e perda de pacotes em soluções VoIP, na perspetiva de obter o mais eficiente entre eles;
- Com o estudo feito implementar uma solução de VoIP mista, com Asterisk e Cisco CallManager express.

References

[1] M. Yamac, “Malicious Users Discrimination in Organized Attacks Using Structured Sparsity,” pp. 276–280, 2017.

[2] S. Paulsen, T. Uhl, and K. Nowicki, “Influence of the jitter buffer on the quality of service VoIP,” *2011 3rd Int. Congr. Ultra Mod. Telecommun. Control Syst. Work.*, no. January 2011, pp. 1–5, 2011.

[3] W. Zhang, Y. Chang, Y. Liu, and Y. Tian, “Perceived QoS assessment for Voip networks,” *Int. Conf. Commun. Technol. Proceedings, ICCT*, pp. 707–711, 2013.

[4] S. Phithakkitnukoon, R. Dantu, and E. A. Baatarjav, “Voip security — attacks and solutions,” *Inf. Secur. J.*, vol. 17, no. 3, pp. 114–123, 2008.

[5] A. Aburumman, W. J. Seo, C. Esposito, A. Castiglione, R. Islam, and K. K. R. Choo, “A secure and resilient cross-domain SIP solution for MANETs using dynamic clustering and joint spatial and temporal redundancy,” *Concurr. Comput.* , vol. 29, no. 23, pp. 1–16, 2017.

[6] C. N. Lin, T. L. Lin, J. Chen, and W. J. Chen, “VoIP Communication Quality and Flow Volume Preference — A SIP and Red5 Example,” no. Icsai, pp. 782–786, 2016.

[7] U. U. Rehman and A. G. Abbasi, “Security Analysis of VoIP Architecture for Identifying SIP Vulnerabilities,” no. i, pp. 87–93, 2014.

[8] M. Alshamrani and G. Ansa, “SIP Signaling Implementations and Performance Enhancement over MANET : A Survey,” vol. 7, no. 5, pp. 191–204, 2016.

[9] A. Khiat, M. El Khaili, J. Bakkoury, and A. Bahnasse, “Study And Evaluation Of Voice Over IP Signaling Protocols Performances On MIPv6 Protocol In Mobile 802.11 Network SIP And H.323,” 2017.

[10] I. Savvius, “VoIP Technology and Glossary.” [Online]. Available: https://www.savvius.com/networking-glossary/voip.

[11] I. (d. b. a. R. C. Sonus Networks and O. Company)(“Ribbon”), “What is Media Gateway Control Protocol (MGCP)?” [Online]. Available: https://ribboncommunications.com/company/get-

help/glossary/media-gateway-control-protocol.

[12] R. Arora, “Voice over IP : Protocols and Standards.”

[13] G. Vennila and M. S. K. Manikandan, “A Scalable Detection Technique for Real-time Transport Protocol (RTP) Flooding Attacks in VoIP Network,” *Procedia Comput. Sci.*, vol. 93, no. September, pp. 893–901, 2016.

[14] K. Mohamed, O. Mohamed, M. Hamoudi, and M. Masmoudi, “QoS evaluation in VoIP software with and without Blowfish encryption module,” *3rd Int. Conf. Control. Eng. Inf. Technol. CEIT 2015*, 2015.

[15] H. P. Singh, S. Singh, J. Singh, and S. A. Khan, “VoIP: State of art for global connectivity - A critical review,” *J. Netw. Comput. Appl.*, vol. 37, no. 1, pp. 365–379, 2014.

[16] S. Dhar, “A STUDY OF VOIP CODECS PERFORMANCE,” no. June 2003, pp. 23–24, 2017.

[17] C. Olariu, M. Zuber, and C. Thorpe, “Delay-based priority queueing for VoIP over Software Defined Networks,” *Proc. IM 2017 - 2017 IFIP/IEEE Int. Symp. Integr. Netw. Serv. Manag.*, pp. 652–655, 2017.

[18] S. E. I. Brak, M. Bouhorma, and A. Boudhir, “Voice over V ANETs (Vo V AN): QoS Performance Analysis of Different Voice CODECs in Urban V ANET Scenarios,” *Ieee 2012*, pp. 0–5, 2012.

[19] Z. Li, S. Zhao, S. Bruhn, J. Wang, and J. Kuang, “Comparison and optimization of packet loss recovery methods based on AMR-WB for VoIP,” *Speech Communication*, vol. 54. pp. 957–974, 2012.

[20] 2 Benedikt Machens1, Olaf Gebauer2 and Diederich Wermser1, “Fraud Attacks in VoIP-Based Communications Systems Risk Analysis, Prevention, Protection, Detection,” *1IANT - Int. Appl. NGN Technol. GmbH, Salzdahlumer Str. 46/48, D-38302, Wolfenbüttel, Ger. 2Research Gr. IP-Based Commun. Syst. Ostfalia Univ. Appl. Sci. Salzdahlumer Str. 46/48, D-38302, Wolfenbüttel, Ger.*, no. March, pp. 1–8, 2017.

[21] © TransNexus 1997 - 2018, “Introduction to VoIP Fraud,” 2018. [Online]. Available: transnexus.com/resources/telecom-industry-

topics/fraud/introduction-to-voip-fraud.
[22] Certicom, “Securing VoIP Networks,” no. January, 2006.
[23] I. Digium, “Asterisk,” 2017. [Online]. Available: https://www.asterisk.org.
[24] CISCO, “Cisco Unified Communications Manager (CallManager).” [Online]. Available: https://www.cisco.com. [Accessed: 22-Jan-2018].
[25] C. Li, H. Li, K. Wang, and K. Nan, “Research and Implementation of Unified Communications System based on Elastix,” pp. 1–4, 2011.
[26] Telzio Inc, “Telzio.” [Online]. Available: https://telzio.com.
[27] “3CX.” [Online]. Available: https://www.3cx.com.
[28] I. M. P. Doyle, G. Dale, H. Choi, and B. City, “(12) UnIted States Patent,” vol. 2, no. 12, 2012.
[29] VOIP-Info.org LLC, “Softphones VoIP.” [Online]. Available: https://www.voip-info.org.
[30] VBUZZER™, “VBUZZER.” [Online]. Available: https://www.vbuzzer.com.
[31] P. Phusamchot and P. Wuttidittachotti, “Comparison of Skype VoIP Quality over 3G with Mobility : A Case Study of Fair Usage Policy Effects,” pp. 0–4, 2015.
[32] © Microsoft, “Skype features,” 2018. [Online]. Available: www.skype.com/en/features/.
[33] Mizutech S.R.L., “WINDOWS SOFTPHONE -SHORT DESCRIPTION,” 2017. [Online]. Available: https://www.mizu-voip.com.
[34] © CALLCENTRIC, “WHAT IS CALLCENTRIC?” [Online]. Available: www.callcentric.com/how.
[35] “Devices.” [Online]. Available: https://wiki.voip.ms.
[36] VoIPstudio, “How Does A VoIP Adapter Work.” [Online]. Available: https://voipstudio.com.
[37] NFON AG, “IP phone.” [Online]. Available: https://www.nfon.com.
[38] VoIPSUPPLY, “Types of VoIP Phones.” [Online]. Available: https://www.voipsupply.com.
[39] NFON AG, “Conference Phones.” [Online]. Available:

https://www.nfon.com.

[40] D. D. David Malllory, Ken Salhof, *Cisco Voice Gateways and Gatekeepers*. 2004.

[41] VoIP Supply, “VoIP Gateway Overview.” [Online]. Available: https://www.voipsupply.com/overview-of-voip-gateways.

[42] CISCO, “Understanding H.323 Gatekeepers.” [Online]. Available: https://www.cisco.com/c/en/us/support/docs/voice/h323/5244-understand-gatekeepers.html#gatekeeperdef.

[43] N. Unuth, “Which VoIP Provider to Choose?” [Online]. Available: www.lifewire.com/voip-providers-which-voip-providers-to-choose-3426565.

[44] © CounterPath, “What Is A VoIP Service Provider?,” 2016. [Online]. Available: https://help.bria-x.com/hc/en-us/articles/218764318-What-is-a-VoIP-Service-Provider-.

[45] QuinStreet Inc, “VoIP service provider,” 2018. [Online]. Available: https://www.webopedia.com/TERM/V/voip_service_provider.html.

[46] © VoipReview.org, “Compare Top Rated Residential VoIP Providers.” [Online]. Available: www.voipreview.org/residential-voip.

[47] © GetVoIP.com, “The Best Cloud Hosted PBX Providers of 2018,” 2018. [Online]. Available: getvoip.com/hosted-pbx.

[48] I. RingCentral, “4 Factors to Consider Before Choosing a VoIP Provider,” 2016. [Online]. Available: www.ringcentral.com/blog/2016/12/choosing-a-voip-provider.

[49] S. Khan and N. Sadiq, “Asterisk server and OPNET platform,” 2017.

[50] S. Jalendry and S. Verma, “A Detail Review on Voice over Internet Protocol (VoIP),” vol. 23, no. 4, pp. 161–166, 2015.

[51] S. Hofbauer, K. Beckers, G. Quirchmayr, and C. Sorge, “A lightweight privacy preserving approach for analyzing communication records to prevent voip attacks using toll fraud as an example,” *Proc. 11th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. - 11th IEEE Int. Conf. Ubiquitous Comput. Commun. IUCC-2012*, pp. 992–997, 2012.

[52] © 2018 Hummingbird Networks, “The Importance of VLAN

Segmentation for Voice and Data," 2015. [Online]. Available: https://info.hummingbirdnetworks.com/blog/importance-of-vlan-segmentation-voice-data.

[53] Inaani Pte. Ltd, "Things Must Know about VoIP Server," 2017. [Online]. Available: https://www.inaani.com/blog/things-must-know-voip-server/.

Apêndice A

A.1 Configuração do servidor Matriz ficheiro sip.conf

A.1.1 Configuração para a criação dos clientes (utilizadores)

```
[general]



[2000]

type=friend

host=dynamic

secret=123

context=test

qualify=yes



[2001]

type=friend

host=dynamic

secret=123

context=test

qualify=yes



[covilha]
```

```
type=friend

host=dynamic

username=covilha

secret=123

context=test

qualify=yes

insecure=invite
```

A.2 Configuração dos CODECs utilizados

```
disallow=all

allow=alaw

allow=gsm

allow=g729
```

A.3 Configuração do registo do servidor Lisboa no servidor Covilhã

```
register => lisboa:123@192.168.10.101/covilha
```

A.4 Configuração do servidor Matriz ficheiro extensions.conf

A.4.1 Plano de discagem

```
[general]

autofallthrough=yes

[test]

exten => _XXXX,1,Dial(SIP/${EXTEN},30,r)
```

```
exten => _XXXX,2,Dial(SIP/${EXTEN}@covilha,30,r)
```

A.5 Configuração do servidor Filial ficheiro sip.conf

A.5.1 Configuração para a criação dos clientes (utilizadores)

```
[1000] ; criação de um cliente(utilizador)

type=friend

host=dynamic

secret=123

context=test

qualify=yes

[1001]

type=friend

host=dynamic ; Quer dizer que podemos nos comunicar com qual endereço IP, diferente se fosse para um IP especifico,  no caso colocaríamos o IP

secret=123 ; definida a senha para autenticação do utilizador

context=test; definição do contexto

qualify=yes

[lisboa] ; configuração do servidor como cliente, para poder se comunicar com o servidor outro servidor

type=friend

host=dynamic
```

```
username=lisboa

secret=123

context=test

qualify=yes

insecure=invite
```

A.6 Configuração dos CODECs utilizados

```
disallow=all ; Primeiro são desabilitados todos os CODECs

allow=alaw ; Permite definir CODEC a nossa preferência

allow=gsm ; CODEC definido

allow=g729 ; CODEC definido
```

A.7 Configuração do registo do servidor Covilhã no servidor Lisboa

```
register => covilha:123@192.168.20.201/lisboa

register => covilha:123@192.168.20.201/2000
```

A.8 Configuração do servidor Filial ficheiro extensions.conf

A.8.1 Plano de discagem

```
[general]

autofalltrough=yes
```

```
[test]



; sip local

exten => _XXXX,1,Dial(SIP/${EXTEN},30,r)



;sip remoto, só procura no caso de falhar o local

exten => _XXXX,2,Dial(SIP/${EXTEN}@lisboa,30,r)
```