ULBRA CENTRO UNIVERSITÁRIO LUTERANO DE PALMAS
COMUNIDADE EVANGÉLICA LUTERANA "SÃO PAULO"
Recredenciado pela Portaria Ministerial nº 3.607 - D.O.U. nº 202 de 20/10/2005

Márcio Fernandes Coelho

COMUNICAÇÃO VOIP ENTRE DOIS SERVIDORES ASTERISK USANDO O PROXY SIP

Palmas - TO

2012

Márcio Fernandes Coelho

COMUNICAÇÃO VOIP ENTRE DOIS SERVIDORES ASTERISK USANDO O PROXY SIP

Trabalho apresentado como requisito parcial da disciplina Trabalho de Conclusão de Curso (TCC) do curso de Sistemas de Informação, orientado pela Professora Mestre Madianita Bogo Marioti.

Palmas - TO

2012

Márcio Fernandes Coelho

COMUNICAÇÃO VOIP ENTRE DOIS SERVIDORES ASTERISK USANDO O PROXY SIP

Trabalho apresentado como requisito parcial da disciplina Trabalho de Conclusão de Curso (TCC) do curso de Sistemas de Informação, orientado pela Profª M.Sc. Madianita Bogo Marioti

Aprovado em _____ de 2012.

BANCA EXAMINADORA

_____

Profª M.Sc. Madianita Bogo Marioti.

Centro Universitário Luterano de Palmas

_____

Prof. M.sc Cristina D'Ornellas Filipakis Souza

Centro Universitário Luterano de Palmas

_____

Prof. M.sC Jamal Hassan Ibrahim

Centro Universitário Luterano de Palmas

Palmas - TO

2012

DEDICATÓRIA

Agradeço a Deus, por estar presente em todos os momentos da minha vida e dedico esta monografia a minha família e amigos onde encontrei forças para a realização deste trabalho.

AGRADECIMENTOS

Agradeço primeiramente a Deus, que sempre nos acompanha e guia nossos passos, dando – nos força, sabedoria, e nos estimulando a seguir em frente.

Aos meus pais, Raimundo Fernandes e Elvina Fernandes, aos meus irmãos Lívia, Junior e Neila e aos sobrinhos Neto Jr, Lara, Wallife e Laiza, a minha querida e eterna vó Camélia que não se encontra mais no nosso meio, mais tenho certeza que estar feliz por mais essa conquista, pois foi minha incentivadora nos estudos e agradecer especialmente a minha esposa Simone Morais pela motivação, entusiasmo e compreensão.

Não poderia deixar de agradecer a todos meus amigos e aos demais familiares e em especial a família de minha esposa por ter contribuído e muito para minha formatura, a minha cunhada Silvia que cedeu uma kit net e assim evitasse de trancar mais uma vez a faculdade a minha segunda mãe e sogra Maria Morais, que sempre ficava esperando chegar da faculdade pra levar a janta quentinha, que fazia o primeiro beiju e levava antes que saísse para a faculdade, são pra essas pessoas que faço meus agradecimentos.

Gostaria de agradecer os amigos e colegas da faculdade, que sempre ajudaram nas dificuldades, em especial ao Jefferson Leite, quem ensinou a compactar e descompactar os primeiros arquivos, ao Danilo Cavalcante, quando tinha qualquer dificuldade no Linux era a quem recorria e ao Gleisson Martins (Robinho) que Deus tenha em um bom lugar, quantas noites e finais de semanas ficávamos estuda ou fazendo trabalhos da faculdade, se hoje estou formado foi com grande contribuição dessas pessoas.

A minha professora e orientadora Madianita Bogo, por sua dedicação constante, buscando sempre extrair todo nosso potencial. Com sua inteligência e carisma inigualáveis, esteve sempre ao meu lado, ligando quando percebia que estava desmotivado, ajudando nas dificuldades, e partilhando das minhas superações. Agradeço aos professores Andrés, Cristina, Fabiano, Fernando, Jackson, Ricardo, Parcilene, Thereza e Leal.

Agradeço a todos que de forma direta ou indiretamente contribuíram para mais esta realização. E sobre todas as coisas, agradeço a Deus, por mais essa vitória em minha vida.

“Por mais que a ciência evolua e que a tecnologia avance, jamais ela vai decifrar a mente humana, pois cada cabeça é um mundo e cada ser humano uma história, jamais caberá numa tese ou num fundamento. Isso faz da

humanidade e seu imaginário imensamente complexos e hierárquicos".

Afonso Allan

RESUMO

As Redes de Computadores ampliaram sua abrangência de atendimento para um público cada vez maior, exigente e atento às inovações do mercado. Nesse contexto, o VoIP (Voice *over Internet Protocol*) – voz sobre IP é a tecnologia que está revolucionando o mercado de telefonia, por dispor aos usuários a realização de chamadas telefônicas a custos bem mais reduzidos do que as chamadas tradicionais. Atualmente, devido aos elevados custos com a telefonia convencional, muitas organizações e instituições estão migrando para o VoIP, que se apresenta, como uma alternativa para reduzir os gastos com telefonia. Este trabalho teve por objetivo geral possibilitar a comunicação VoIP entre ramais de redes distintas. Para isso, foram configurados dois servidores Asterisk, usando protocolo SIP, para realizar a comunicação VoIP, sendo configurados com o GNU\Linux Debian, de forma a permitir a comunicação VoIP. Os resultados obtidos foram plenamente satisfatórios, já que durante os testes, os servidores possibilitaram a conexão entre os ramais de redes distintas e o atendimento automático funcionou normalmente.

Palavras-Chave: Asterisk, VoIP, SIP, PABX.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS

ARPANET - Advanced Research Projects Agency

ASN.1 – Abstract Syntax Notation 1

CODEC - Codificador/Decodificador

DDoS – Distributed Deny of Service

DoS – Denial of Service

Dialplan – Plano de Discagem

DTLS – Datagram Transport Layer Security

FTP - File Transfer Protocol

GTS - Generic Traffic Shaping

HTTP - Hypertext Transport Protocol

IP - Internet Protocol

ISO (instituto Internacional para padronização)

ITU-T – International Telecom Union

Kbps - Kilo bits por segundo

LAN - Local Area Network

LaRC - Laboratório de Redes de Computadores

MCU – Multipoint Control Unit

MOS – Mean Opinion Score

MTU - Maximum Transfer Unit

OSI – Open Systems Interconnection

PABX - Private Automatic Branch Exchange

PCM – Pulse Code Modulations

PSTN - Public Switched Telefone Network

QoS – Qualidade de Serviço

TCP - Real Time Control Protocol

RTP - Real Time Protocol

RTPC - Rede telefônica Comutada

RPTC - Rede Pública de Telefonia Comutada

SIP - Session Iniciation Protocol

SIPP - Simple Internet Protocol Plus

S/MIME – Secure/Multipurpose Internet Mail Extensions

SBM - Subnet Bandwidth Management

SMDS - Switched Multimegabit Data Service

SMTP - Simple Mail Transfer Protocol

SNMP - Simple Network Management Protocol

SSL - Secure Sockets Layer

TCP - Transmission Control Protocol

TLS – Transpot Layer Security

UAC – User Agent Client

UAS – User Agent Server

UDP - User Datagram Protocol

URA Unidade de Resposta Audível

VLSI – Integrated Circuit Very Large Scale Integration

VoIP - Voz sobre IP

WAN – World Area Network

WFQ - Weighted Fair Queueing

SUMÁRIO

1 INTRODUÇÃO

Nos últimos anos, as Redes de Computadores ampliaram sua abrangência de atendimento para um público cada vez maior, exigente e atento às inovações que diariamente chegam ao mercado consumidor. Dessa maneira, as Redes de Computadores atendem às organizações e aos indivíduos, ofertando amplas possibilidades de uso como compartilhamento de recursos físicos e informações, comunicação entre usuários, comércio eletrônico, entretenimento, dentre tanto outros.

Nesse contexto, o VoIP (*Voice over Internet Protocol*) – voz sobre IP, se destaca como uma tecnologia que revolucionou o mercado de telefonia, por dispor aos usuários a realização de chamadas telefônicas a custos bem mais reduzidos do que as chamadas tradicionais.

Na tecnologia VoIP, a voz é submetida a protocolos de codificação e decodificação – os codecs – os quais definem como os sinais de voz serão digitalizados. Após esse processo para a forma digital, a voz é migrada para pacotes de dados e transmitida por meio das redes IP (*Internet Protocol*), fazendo uso dos protocolos de transporte como o UDP e o RTP (*Real Time Transport Protocol*). Finalmente, na chegada ao seu destinatário, tais pacotes são reordenados e convertidos à forma analógica.

Atualmente, devido aos elevados custos com a telefonia convencional, muitas organizações e instituições estão migrando para o VoIP, que se apresenta, dentre outras vantagens, como uma alternativa para reduzir os gastos com telefonia.

Em função dessa realidade, tornou-se pertinente o estudo dessa temática para a realização deste trabalho, que teve por objetivo geral possibilitar a comunicação VoIP entre ramais de redes distintas. Para isso, foram configurados dois servidores Asterisk, usando protocolo SIP, para realizar a comunicação VoIP, sendo configurados com o GNU\Linux Debian, de forma a permitir a comunicação VoIP.

Este trabalho é composto por seis capítulos estruturados conforme segue:

- o primeiro capítulo apresenta a Introdução do trabalho, com a definição do tema e a problemática que serviu de base para este estudo;

- o segundo capítulo, o Referencial Teórico está distribuído em sete temáticas, que são os conceitos das Redes de Computadores, comutação, padrões de rede, protocolo IP, VoIP, Asterisk e vulnerabilidades;
- no terceiro capítulo, Materiais e Métodos, é apresentada a metodologia adotada para o desenvolvimento do trabalho, bem como o local, o período, e o *hardware* e *software* utilizados para a configuração dos servidores Asterisk.
- o quarto capítulo apresenta os Resultados e Discussão do trabalho desenvolvido;
- no quinto capítulo estão as considerações finais do estudo. Finalizando, são apresentadas as referências das obras consultadas.

2 REFERENCIAL TEÓRICO

2.1 Redes de Computadores

A temática redes de computadores envolve muitos e diferentes tipos de redes, desde as grandes até as pequenas, como também aquelas bastante conhecidas e as que são pouco conhecidas. Além disso, atualmente, as pessoas estão interessadas e constantemente conectadas as redes de computadores e, para cada uma delas, as redes dispõem de diversos tipos de serviços (visando atender a demanda).

Dessa maneira, as redes de computadores atendem aos usuários oferecendo várias possibilidades de uso, tais como: a) *aplicações comerciais*: compartilhamento de recursos físicos e informações, VoIP, comunicação entre usuários, comércio eletrônico etc.; b) *aplicações domésticas*: compartilhamento de recursos físicos e informações, comunicação entre usuários, entretenimento etc.; c) aplicações *móveis*: escritório portátil, aplicações militares etc.

Assim, cabe salientar que, de uma maneira geral, as redes possuem "diferentes escalas, objetivos e tecnologias" (TANENBAUM, 2003, p. 53). Nesse contexto, as redes podem ser classificadas de diferentes formas e tipologias, tornando-se essencial a sua padronização, visando assegurar que a comunicação nas redes, entre máquinas de diferentes fabricantes, possa de fato acontecer com eficiência e qualidade.

E para que a comunicação nas redes seja estabelecida com eficiência é muito importante que seja feita a alocação do canal de comunicação, para que cada estação utilize o meio físico na sua abertura de tempo, evitando o desperdício da capacidade do canal (largura da banda). Por isso, antes de se falar na padronização, a seção seguinte apresenta o processo de comutação, que é um conceito importante para a compreensão da comunicação entre as máquinas.

2.2 Comutação

Comutação é a alocação de recursos que é realizada em uma rede de comunicação de forma a possibilitar a transmissão de dados pelos diversos dispositivos que estão conectados a esta rede (SOARES, 1995). Nas redes de comunicação existem três tipos de comutação: a comutação de circuitos, a comutação de mensagens e a comutação de pacotes.

Para o desenvolvimento do presente trabalho, torna-se necessário compreender como ocorrem os processos de comutações de circuito e pacote, que são usadas pela telefonia convencional e VoIP, respectivamente.

2.2.1 Comutação de Circuitos

Na comutação de circuitos é estabelecido um caminho fim-a-fim, de forma que antes da comunicação é feita uma reserva dos recursos que serão necessários para a transferência dos dados (GOMES, 2005, p. 41). As redes baseadas em comutação por circuito fazem a reserva prévia de recursos, como largura de banda, que ficam dedicados durante a comunicação.

Durante esse processo são executados três procedimentos: o estabelecimento da conexão, a transmissão de dados e o encerramento da conexão. Inicialmente, é estabelecida uma rota fixa entre as estações envolvidas para que ocorra a comunicação. Na sequência, é feita a transmissão de dados, quando as estações envolvidas podem trocar informações entre si, transmitindo e recebendo dados através do circuito já estabelecido. E, na última etapa, o encerramento da conexão: todos os nós intermediários do circuito precisam estar livres de modo a serem reutilizados, caso necessário, para a formação de novos circuitos entre quaisquer outras estações da rede.

A tecnologia de comutação de circuitos é a utilizada nas redes telefônicas, de forma que, durante uma chamada telefônica é estabelecido um circuito da linha de quem telefona, por meio de uma central de comutação local, que passa por linhas do tronco, por uma central de comutação remota, até chegar ao destinatário da chamada, como mostra a Figura 1.

Enquanto um circuito estiver aberto, o equipamento telefônico testa o microfone por diversas vezes e converte os sinais para o sistema digital, transmitindo-os por meio do circuito para o receptor (COMER, 1998).

A Figura 1 mostra que os circuitos entre origem e destino ficam ocupados quando ocorrer uma ligação entre eles. Uma ligação tendo como origem o circuito **A** e destino o circuito **B**, todos os enlaces que envolvem essa chamada ficam ocupado mesmo, com isso pode ter uma excelente qualidade na conversa e uma baixa eficiência, pois mesmo não usando todo o circuito o mesmo permanece ocupado durante toda a ligação.

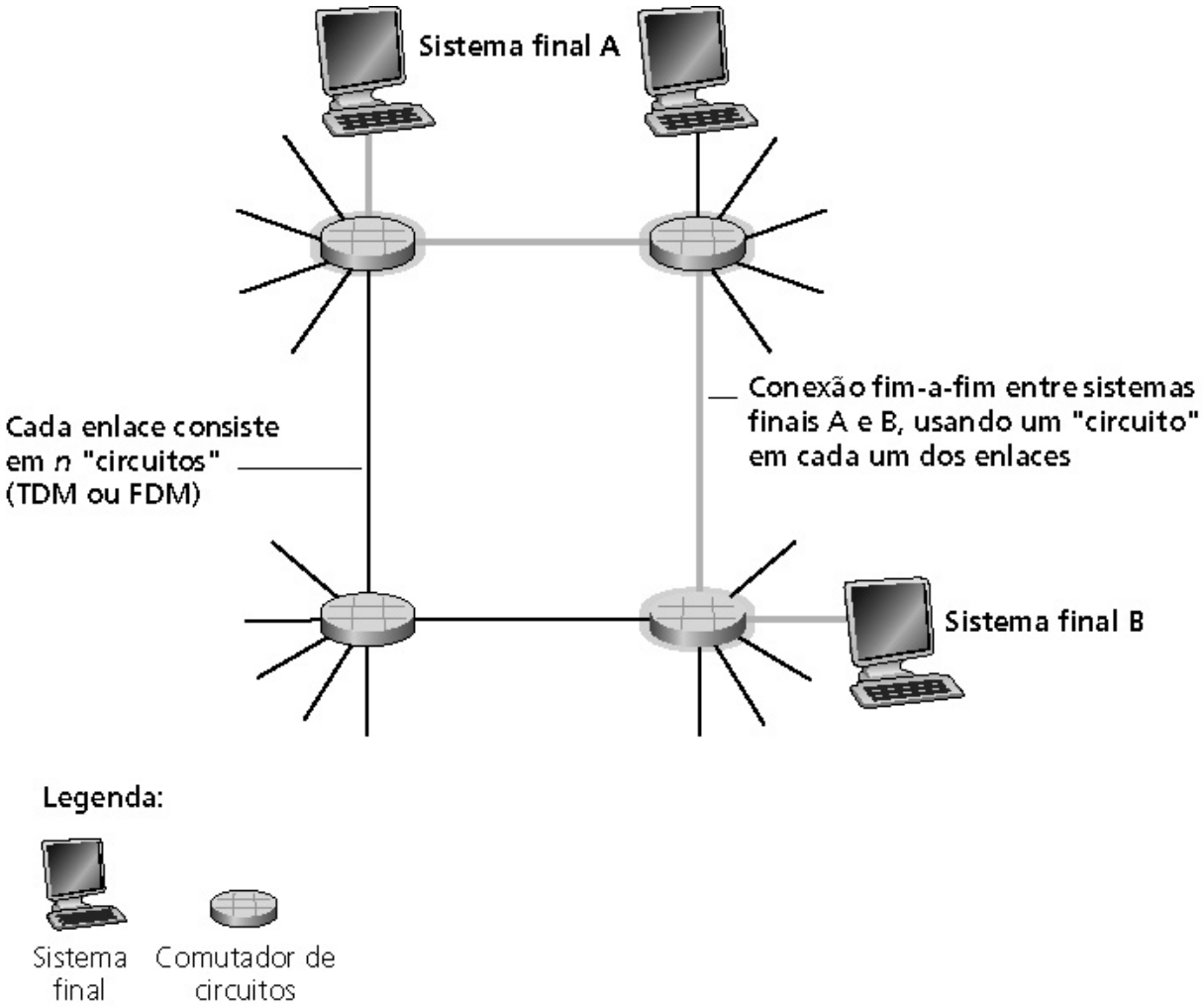

Figura 1: Comutação de Circuitos (KUROSE, 2003)

A principal vantagem da comutação de circuitos é que, uma vez estabelecido o circuito, nenhuma outra atividade de rede poderá reduzir a capacidade deste circuito, pois o percurso de dados é seguro. A principal desvantagem desse tipo de comutação é o seu alto custo, pois o preço é fixo é independe de sua utilização, por exemplo, o preço de uma ligação telefônica é o mesmo, ainda que as duas pontas não se comuniquem, já que o circuito conectado é dedicado e só será desfeito com o processo de desconexão.

2.2.2 Comutação de Pacotes

Nas redes de comutação por pacote a utilização da banda é feita de acordo com a necessidade, de forma que esta pode ser compartilhada para tráfego de mensagens de diversas origens e destinos, pois os caminhos não são dedicados (TANENBAUM, 2003, p. 395).

Nesse tipo de comutação, as mensagens trafegadas são divididas em pacotes. Cada pacote transporta uma identificação que capacita o *hardware* da rede a enviar as informações a um determinado destino e a montar os pacotes de forma a reconstruir a mensagem original. Exemplificando, durante a transmissão de uma mensagem entre dois equipamentos, é feita a divisão do arquivo em pacotes, são adicionados cabeçalhos com as informações necessárias para envio e remontagem, os pacotes são encaminhados à rede e, ao chegarem ao destino, são remontados em uma mensagem única.

A comunicação de voz e vídeo usa a mesma rede da comunicação de dados, assim essa comunicação é definida como comutação de pacotes, a Figura 2 mostra que a comunicação entre origem e destino é feita usando a mesma rede (internet), os pacotes enviados da origem ao destino podem seguir o mesmo caminho ou caminhos alternativos sem perder a qualidade da comunicação.

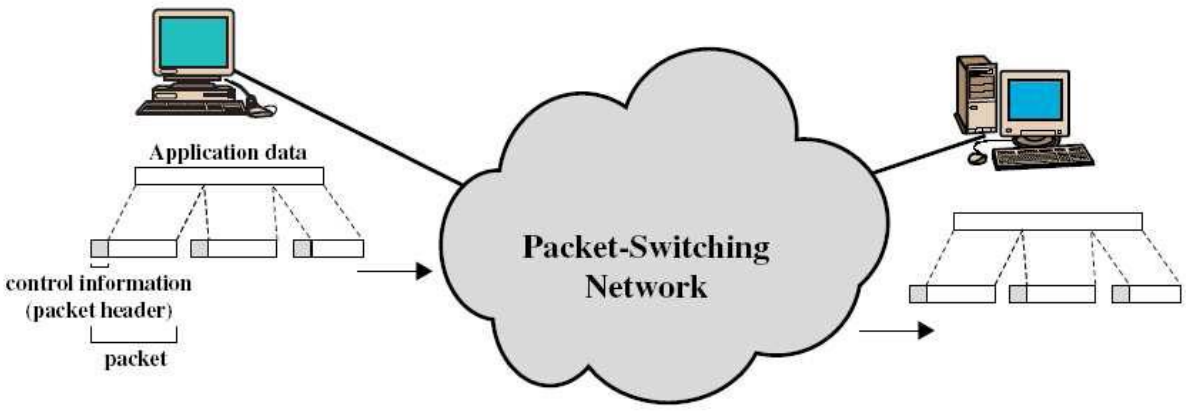

Figura 2: Comutação de Pacotes (STALLINGS, 2002)

Os comutadores de pacotes utilizam uma técnica chamada store-and-forward, na qual os pacotes passam por vários nós (roteadores) e em cada roteador é feita uma análise do pacote, com o intuito de descobrir o caminho até o destinatário, bem como descartar os pacotes que apresentarem problemas.

A principal vantagem da comutação de pacotes é a possibilidade da realização simultânea de várias comunicações entre computadores, compartilhando o mesmo meio físico. A desvantagem desse processo é que “um par de computadores conectados entre si recebe uma capacidade menor de rede”, (COMER, 1998, p. 21), pois, sempre que uma rede de comutação de pacotes estiver sobrecarregada, os computadores que estiverem conectados a ela terão que aguardar a sua vez de enviar pacotes adicionais.

Na comutação de circuito é estabelecido um caminho fim-a-fim e, com isso, fica mais fácil garantir qualidade de serviços (QoS), em contra partida, perde-se eficiência, já que o meio fica alocado, não permitindo seu uso por outra comunicação. As redes de comutação de pacotes são mais eficientes, pois não trabalham com reserva de banda, com isso é possível o tráfego de vários pacotes no mesmo canal de comunicação.

Apesar dessa desvantagem, a comutação de pacotes tornou-se bastante popular, pois, vários usuários podem compartilhar o *hardware* da rede e isso faz com que o número de conexões diminua, tornando o seu custo relativamente baixo (COMER, 1998), se comparada a comutação de circuitos. A redução dos custos é possível pelo compartilhamento de recursos na rede e não alocação de um caminho dedicado.

2.2.3 Comutação de Circuitos X Comutação de Pacotes

De acordo com o funcionamento apresentado na seção anterior, pode-se levantar várias características distintas entre a comutação de circuitos e a comutação de pacotes, como apresenta o Quadro 1.

Quadro 1: Comutação de Circuitos X Comutação de Pacotes

COMUTAÇÃO	
Comutação de Circuitos	**Comutação de Pacotes**
Vantagens • Garantia de recursos • Disputa pelo acesso somente na fase de conexão • Não há processamento nos nós intermediários • Menor tempo de transferência • Controle nas extremidades • Comunicação em três fases • Estabelecimento do circuito (conexão) • Não há congestionamento dos dados a serem enviados • Determinação e alocação de uma rota entre as estações • Alocação de um canal por enlace • Transferência de dados • Desconexão do circuito	**Vantagens** • Uso otimizado do meio compartilhado • Ideal para dados • Erros recuperados no enlace onde ocorreram • Nós intermediários (roteadores) encaminham os pacotes • Compartilhamento de enlaces ou partes de enlaces • Não há reserva de recursos • Não guarda informação de estado • Informações a serem enviadas são quebradas em pacotes • Pacotes contêm dados e cabeçalho (informação de controle) > *overhead* • Cabeçalho inclui informação para permitir escolha de uma rota (roteamento) para o pacote • Custo baixo
Desvantagens • Desperdício de banda durante períodos de silêncio • Problema para transmissão de dados • Ruim quando o tempo de conexão é da ordem do tempo da comunicação • Erros são recuperados fim a fim • Probabilidade de bloqueio • Circuitos ocupados em um instante • Alto Custo	**Desvantagens** • Sem garantias de banda, atraso e variação do atraso (*jitter*) • Por poder usar diferentes caminhos, atrasos podem ser diferentes • Variação do atraso • Ruim para algumas aplicações tipo voz e vídeo • Overhead de cabeçalho • Disputa nó-a-nó • Atrasos de enfileiramento e de processamento a cada nó

O Quadro 1 apresentou um paralelo entre a comutação de circuitos e a comutação de pacotes, destacando as principais vantagens e desvantagens existentes em cada uma das referidas comutações.

Nesta análise comparativa foi possível constatar que se por um lado a comutação de circuitos apresenta problemas durante a transmissão dos dados, a comutação de pacotes apresenta-se como favorável para tal transmissão, pois quando ocorrem erros, estes são recuperados no enlace onde ocorreram.

A seção seguinte apresenta os padrões de redes, que foram criados com o intuito de resolver os problemas de incompatibilidade e, com isso, tornam possível a troca de informações entre as redes de computadores.

2.3 Padrões de Rede

Existem diversos fabricantes e fornecedores de placas de redes, sendo que cada um deles possui "sua própria concepção de como tudo deve ser feito" (TANERBAUN, 2003. p. 76). Em função disso, verifica-se que se não existisse uma coordenação básica nas redes de computadores, evidentemente, haveria um caos completo, e os usuários não se comunicariam com outros computadores com placas de redes diferentes. Mediante este contexto, a alternativa mais viável encontrada pela indústria foi a criação de alguns padrões de rede.

Conforme explica Tanenbaun (2003, p. 76), a padronização das redes possibilita a comunicação entre diferentes computadores, além de ampliar o mercado para os produtos que aderem as suas regras. Dentre as vantagens pontuadas pelo autor está o fato de que "um mercado mais amplo estimula a produção em massa, proporciona uma economia no processo de produção".

Assim sendo, a literatura básica aponta que existem duas categorias de padrões de rede: de *facto* e de *jure*. Tais categorias são conceituadas respectivamente como padrões "de fato" e padrões "por lei". O primeiro, padrão de fato, não se aplica em um plano formal, pois são praticamente copiados. Estes padrões se aplicam em computadores pessoais, escritórios e casas, a exemplo da IBM PC.

No segundo caso, o padrão por lei, trata-se dos padrões legais e formais que são adotados por uma instituição de padronização autorizada. Geralmente, esses padrões seguem um critério de legalidade e autorização internacional, sendo divididos em duas classes: os tratados estabelecidos entre governos nacionais e organizações voluntárias. O modelo OSI e a Arquitetura TCP/IP são exemplos desses padrões, os quais são apresentados nas seções seguintes (TANERBAUN, 2003. p. 76).

2.3.1 Modelo OSI

O modelo de referência OSI (*Open Systems Interconnection*) é uma arquitetura de rede baseada em uma proposta desenvolvida pela Organização Internacional de Normalização – *a International Standards Organizacion* (ISO) –, criada no início dos anos 1980, para "facilitar o processo de padronização e obter interconectividade entre máquinas de diferentes

fabricantes, [...] definindo diretivas genéricas para a construção de redes de computadores independente da tecnologia de implementação" (PINHEIRO, 2004, *on line*).

Atualmente, embora os protocolos associados ao modelo OSI sejam raramente usados, o modelo em si ainda é válido em função das importantes características descritas em cada uma das camadas (DAY E ZIMMERMAN *apud* TANENBAUM, 2003, p. 40).

O modelo OSI possui sete camadas, como mostra a Figura 3, que seguem princípios de aplicação já estabelecidos, que vão do modelo mais simples – mais direcionado à informação – até ao mais complexo (TANENBAUM, 2003, p. 46).

Figura 3: Camadas do modelo de referência OSI

Em relação às sete camadas vale salientar alguns princípios que são utilizados para se chegar a todas elas:

> 1. Uma camada deve ser criada onde houver necessidade de um grau de abstração adicional. 2. Cada camada deve executar uma função bem definida. 3. A função de cada camada deve ser escolhida tendo em vista a definição de protocolos padronizados internacionalmente. 4. Os limites da camadas devem ser escolhidos para minimizar o fluxo de informações pelas interfaces. 5. O número de camadas deve ser grande o bastante para que funções distintas não precisem ser desnecessariamente colocadas na mesma camada e pequeno suficiente para que a arquitetura não se torne difícil de controlar (TANENBAUM, 2003, p. 41).

Nesse contexto, vale observar que o modelo OSI não constitui uma arquitetura de rede, haja vista, que não são especificados os serviços e os protocolos exatos que devem ser utilizados em cada uma das camadas, ou seja, apenas informa o que cada camada deve fazer (TANENBAUM, 2003, p. 41).

A seguir estão descritas as características e objetivos de cada uma das sete camadas do modelo de referência OSI:

1. **Camada física:** visa articular as partes mecânicas, elétricas e de sincronização, que estão diretamente relacionadas ao meio físico de transmissão. Trata-se, portanto, da transmissão de bytes brutos por um canal de comunicação. Dessa maneira, o projeto de rede deve assegurar que quando um lado enviar um byte 1, o outro lado o receberá como um byte 1 e não como um byte 0 (TANENBAUM, 2003, p. 42). Essa camada, conforme explica Ponce (2002), não inclui o meio no qual os dados trafegam, esta função é do cabo de rede.
2. **Camada de enlace de dados**: também denominada de *Link* de Dados ou Conexão de Dados, esta camada tem por função "transformar o canal de transmissão bruto em uma linha que pareça livre de erros de transmissão não detectados para a camada de rede" (TANENBAUN, 2003. p. 42). Em outras palavras, esta camada pega os pacotes de dados oriundos da camada de Rede e os transforma em quadros a serem trafegados pela rede. Durante este processo são adicionadas informações como endereço físico da placa de rede de origem e de destino, bem como dados de controle, dados em si, e os controles de erros. Na sequência, esse pacote de dados é enviado à camada física, que o converte em sinais elétricos enviados pelo cabo da rede (PONCE, 2002, p. 43).
3. **Camada de rede**: é responsável pelas rotas – seleção de caminhos e sua finalidade é controlar a operação da sub-rede, na qual a comunicação é feita por pares de roteadores cujas rotas baseiam-se em tabelas estáticas (de forma manual), ou altamente dinâmico (por protocolos de roteamento). Assim, a qualidade de serviços é definida pela dependência potencial de seu receptor. O exemplo clássico é a internet (TANENBAUN, 2003. p. 42).
4. **Camada de transporte:** é responsável pela qualidade e a confiabilidade dos serviços, sua função básica é a entrega e recebimento de dados, para as aplicações, garantindo o correto endereçamento. "É uma camada fim a fim que liga a origem ao destino" (TANENBAUN, 2003. p. 43).

5. **Camada de sessão:** permite que aplicações de diferentes máquinas estabeleçam sessões de comunicação entre elas. Nesta sessão, as aplicações definem como será feita a transmissão de dados e marcam os dados que estão sendo transmitidos. Tipos de serviços oferecidos: intercâmbio de dados, gerenciamento de diálogos (que mantém o controle de quem deve transmitir em cada momento), o gerenciamento de *token* (impedimento em que duas partes tentem executar a mesma operação crítica ao mesmo tempo), sincronização (verificação periódica de transmissões longas para permitir que elas continuem a partir do ponto em que estavam ao ocorrer uma falha), gerenciamento de atividades, relatório de exceções (PINHEIRO, 2004, *on line*).
6. **Camada de apresentação:** também denominada de Camada de Tradução porque esta camada faz com que as informações trocadas pelos usuários sejam compatíveis entre si, fornecendo ainda serviços de criptografia e compressão de dados. A compressão de dados pega os dados recebidos da camada sete e os comprime (como se fosse um compactador, como o *Zip*) e a camada 6 do dispositivo receptor fica responsável por descompactar esses dados. Esta camada gerencia essas estruturas de dados abstratos, permitindo a definição e o intercâmbio de estruturas de dados de nível mais alto, como é o caso dos registros bancários (TANEMBAUM, 2003).
7. **Camada de aplicação:** camada mais próxima do usuário. "A camada de aplicação faz a interface entre o protocolo de comunicação e o aplicativo que solicitou ou receberá a informação através da rede" (TORRES, 2001, p. 15). Um protocolo de aplicação bastante utilizado é o *HTTP* (*HyperText Transfer Protocol*), que constitui a base para a *World Wide Web*. Segundo Tanembaum (2003), quando um internauta deseja acessar uma página da Web, ele envia o nome desta página ao servidor, utilizando o HTTP e o servidor transmite a página de volta. Outros protocolos de aplicação são usados para transferir arquivos, *e-mails* e transmitir notícias pela rede.

No estudo realizado sobre as sete camadas do modelo de referência OSI, pôde-se constatar que tais camadas disponibilizam aos seus usuários de rede serviços conjugados, que se configuram como sendo um processo de comunicação estabelecido com outras máquinas pela correspondência plausível entre elas. Diante do exposto, verificou-se que a transmissão dos dados se dá por meio dos níveis subjacentes, os quais são ampliados para o nível adjacente.

Nesse contexto, vale ressaltar que os protocolos assumem, portanto, um papel decisivo no processo de comunicação entre as máquinas, já que está pautado em regras e formatos sequenciais.

Observa-se por fim, que as sete camadas podem ser categorizadas com as três mais baixas, atuando dessa maneira nos modelos de transmissão, a quarta na comunicação e as três camadas superiores atuam ao nível do usuário.

2.3.2 Arquitetura TCP/IP

O desenvolvimento da arquitetura TCP/IP se deu com o surgimento da rede ARPANET[1], uma "rede de pesquisa patrocinada pelo Departamento de Defesa dos Estados Unidos (DoD)" (TANENBAUM, 2003, p. 44).

Inicialmente, o principal objetivo dessa rede era o de compartilhar recursos para fins militares, ou seja, manter a comunicação, mesmo que em parte, com as instituições governamentais, na eventualidade da ocorrência de guerras ou catástrofes que afetassem os meios de comunicação daquele país.

Entretanto, aos poucos, várias universidades e repartições públicas foram conectadas, usando linhas telefônicas dedicadas. Foi nesse contexto, que a ARPANET surgiu, como a rede que permaneceria intacta caso um dos servidores perdesse a conexão (TANENBAUM, 2003, p. 42; COMER, 1998, p. 12).

Entretanto, os protocolos de comunicação da rede ARPANET não possuíam um conjunto de regras bem definidas, os serviços oferecidos eram limitados e não padronizados, dificultando seu crescimento e causando problemas de funcionamento. Por exemplo, com o crescimento da rede no início dos anos 1980, os militares precisavam de uma política de segurança, que atendesse as suas necessidades, o que era difícil de implementar nos protocolos existentes na época (COMER, 1998).

Em relação a esse processo, Tanenbaum (2003, p. 44) explica: "quando foram criadas as redes de rádio e satélites, começaram a surgir problemas com os protocolos existentes, o que forçou a criação de uma nova arquitetura de referência". Dessa maneira, o principal objetivo do projeto inicial foi o de desenvolver habilidades para conectar várias redes de maneira uniforme.

[1] Rede percussora de pesquisa do governo americano que objetivava compartilhar recursos tecnológicos para fins militares.

Em função dessa realidade, surgiram discussões sobre a possibilidade de um novo modelo de protocolo, que fosse menos limitado e tivesse menos falhas no recebimento e no envio de dados. Com isso, foi criada a Arquitetura TCP/IP, cuja implantação se deu a partir da necessidade de padronização do conjunto de protocolos, o que permitiu a interconexão de redes heterogêneas, tanto em relação ao Sistema Operacional, quanto ao fabricante de *hardware.* Posteriormente, devido aos seus dois principais protocolos, essa arquitetura TCP[2] (*Transmission Control Protocol*) e IP[3] (*Internet Protocol*) foram denominadas de Modelo de Referência (TANENBAUM, 2003; COMER, 1998).

Atualmente, a tecnologia de interligação em redes é reconhecida como sendo uma interconexão de sistema aberto porque, ao contrário de outros sistemas de comunicação patenteados, disponíveis por determinado fornecedor, as especificações estão disponíveis ao público. Assim sendo, qualquer pessoa está apta a desenvolver o *software* necessário para estabelecer a comunicação de interligação em redes (COMER, 1998, p. 8).

Segundo Comer (1998), um dos aspectos mais importantes da tecnologia de interligação em redes está no fato de que esta foi projetada para estimular a comunicação entre máquinas de arquitetura de *hardware* distinta, para utilizar qualquer *hardware* de comutação de pacotes e vários sistemas operacionais.

A arquitetura TCP/IP é formada por um conjunto de protocolos distribuídos em camadas, que dividem a tarefa da comunicação entre máquinas em rede. Os protocolos determinam todo o processo de comunicação, por exemplo, contêm os detalhes de formatos de mensagens, descrevem o que deve ser feito no recebimento de uma mensagem e especificam como o computador trata os erros ou outras condições anormais (COMER, 1998, p. 4). A Figura 4 apresenta a divisão em camadas da arquitetura TCP/IP.

---

[2] *Transmission Control Protocol* (TCP) – Protocolo de nível de transporte padrão de TCP/IP que fornece um serviço *full-duplex*, confiável, de transmissão de uma cadeia de bytes do qual muitos protocolos de aplicação dependem. O TCP permite que um processo em uma máquina envie uma cadeia de dados para um processo em outra (COMER, 1998, p. 646).

[3] Internet Protocol (IP) é um protocolo da camada de sessão do TCP/IP, que define o datagrama IP como a unidade de informação passada por meio de uma interligação em redes e fornece as base para o serviço sem conexão de entrega *Best-effort* de pacotes (COMER,1998, p. 631).

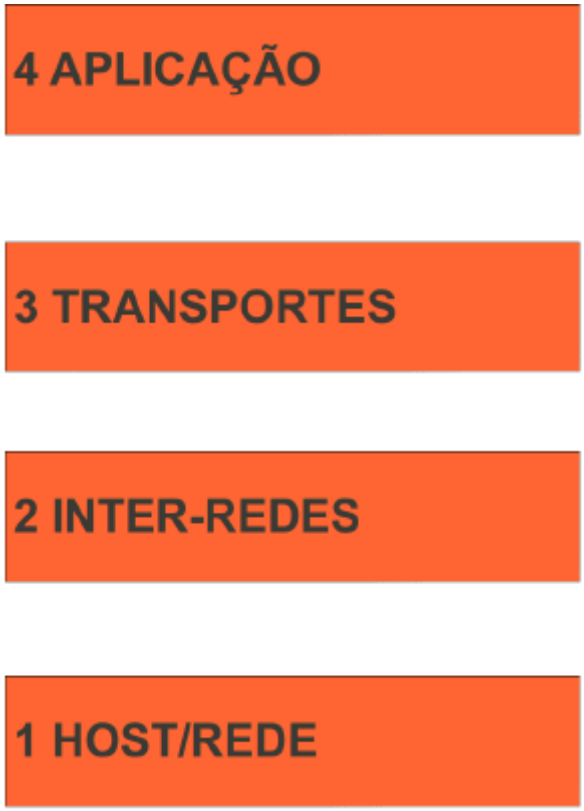

Figura 4: Arquitetura TCP/IP – Arquitetura em Camadas (TANENBAUM, 2003, p. 46)

Na divisão em camadas, cada camada é responsável por oferecer serviços às camadas superiores e utilizar os serviços das camadas inferiores, de forma que cada uma oferece seu serviço sem se preocupar com o comportamento das demais. Esse modelo faz com que a manutenção e a modificação dos protocolos de uma camada não interfiram nas demais, tornando o modelo flexível. A descrição das camadas é a seguinte:

1. **Camada da interface de rede:** segundo Comer (2003, p. 186), "a camada de interface de rede é responsável pela aceitação de datagramas IP e por sua transmissão através de uma rede específica". Durante o envio, é de responsabilidade da camada de interface receber os datagramas IP da camada de rede e transmitir independentemente do protocolo e do meio físico, até o destino. No recebimento, a camada de interface faz a transmissão dos datagramas recebidos para a camada de rede através de uma rede específica. O TCP/IP não define o funcionamento dessa camada. É o nível mais baixo do *software*.
2. **Camada rede ou internet:** as funções principais dessa camada são endereçamento e roteamento dos datagramas IP, sendo responsável por receber os pacotes enviados de diversos *hosts* e garantir que eles trafegarão até o destino (TANENBAUM, 2003, p.

45). O principal protocolo dessa camada é o IP, porém, existem outros como: ARP (*Address Resolution Protocol* – Protocolo de Resolução de Endereços), ICMP (*Internet Control Message Protocol* - Protocolo de Mensagem de Controle da Internet), RARP (*Reverse Address Resolution Protocol* - Protocolo de Resolução Reversa de Endereços), RIP (*Routing Information Protocol* - Protocolo de Roteamento de Informação), IGP (*Interior Gateway Protocols* – Protocolos de Roteamento Interno), OSPF (*Open Shortest Path First* – Protocolo de Gateway Interior da Internet). O roteamento tem papel imprescindível, para evitar congestionamentos de informações. A camada de rede da arquitetura TCP/IP é similar à camada de rede do modelo OSI.

3. **Camada de transporte:** situada acima da camada inter-redes, tem por finalidade manter a conversação dos *hosts* de origem e destino. A função principal dessa camada é garantir a comunicação fim a fim, visando à troca de informações entre dois aplicativos. Os protocolos da camada de transporte utilizam o conceito de portas para identificar os processos das aplicações (TANENBAUM, 2003, p. 46). Os principais protocolos dessa camada são: TCP (*Transport Control Protocol* - Protocolo de Controle de Transmissão) - orientado a conexão e confiável e UDP (*User Datagram Protocol* - Protocolo de Transmissão de Dados) - não orientado a conexão e não confiável.
4. **Camada de aplicação:** a função principal dessa camada é fornecer suporte às aplicações do usuário. O serviço oferecido não possui um padrão comum descrito na arquitetura TCP/IP, sendo de responsabilidade dos protocolos de aplicação e dos programas aplicativos determinar os detalhes de funcionamento. A camada de Aplicação faz a comunicação entre os aplicativos e o protocolo de transporte para enviar e receber dados. Alguns protocolos dessa camada são: HTTP (*Hypertext Transfere Protocol* - Protocolo para Transferência de Hypertexts), FTP (*File Transfere Protocol* - Protocolo de transferência de arquivos), DNS (*Domain Mame System* - Sistema de Nomes de Domínios), SNMP (*Simples Network Management Protocol* - Protocolo Simples de Gerência de Rede), entre outros.

Ao analisar as camadas que compõem a arquitetura TCP/IP, constata-se que esta não possui camadas de sessão e de apresentação. Baseando-se na literatura pesquisada, infere-se que tal fato se justifica pelo pouco uso constatado na maioria das aplicações, incluindo-as nos protocolos mais altos.

2.3.3 Modelo OSI X Arquitetura TCP/IP

Ao se fazer uma análise comparativa sobre o modelo OSI e arquitetura TCP/IP é possível constatar muitas semelhanças. Na avaliação de Tanenbaum (2003, p. 47), esses se baseiam no conceito de uma "pilha de protocolos independentes" e suas camadas exercem praticamente as mesmas funções. Conforme explicação do mesmo autor, tanto no modelo OSI como na arquitetura TCP/IP "estão presentes as camadas que englobam até a camada de transporte para oferecer um serviço de transporte fim a fim independente da rede a processos que desejam se comunicar".

No entanto, embora o modelo de referência OSI e a arquitetura TCP/IP apresentem semelhanças fundamentais, também existem diferenças, conforme destacadas no quadro demonstrativo a seguir (Quadro 2).

Quadro 2: Modelos de Referência OSI e TCP/IP

MODELOS DE REFERNCIA OSI E TCP/IP	SEMELHANÇAS	DIFERENÇAS
	Os dois possuem camadas;	O número de camadas se diferencia: OSI - 7 camadas, TCP/IP - 4 camadas;
	Existem camadas idênticas, tanto na nomenclatura quanto em sua funcionalidade.	Existe uma simplificação da camada de aplicação do TCP/IP, a qual agrega a funcionalidade das camadas de apresentação e sessão do modelo OSI;
	As camadas de transporte são semelhantes no fornecimento dos serviços de rede de fim a fim.	Modelo de referência OSI criado antes do estabelecimento de protocolos (é genérico) e o TCP/IP parte da organização de protocolos sistematizados modelo aberto
	As camadas inferiores fornecem serviços as superiores	Modelo OSI é mais detalhado facilita a relação com o objeto (ensino e aprendizagem)
	Tanto no OSI quanto no TCP/IP, apresentam um conjunto serviços definidos por sua semântica por meio de métodos;	Modelo OSI suporta dois tipos de comunicação (sem comunicação e orientado à comunicação) e a TCP/IP suporta somente um modo na camada de rede.
	Todos os projetistas precisam conhecer o modelo OSI e arquitetura TCP/IP	A arquitetura TCP/IP opera em ambos os modos de comunicação na camada de transporte

Nesse contexto, vale salientar que o modelo OSI possui três conceitos fundamentais que são: serviços, interfaces e protocolos.

Na concepção de Tanenbaum (2003, p. 41), a grande contribuição do modelo OSI é distinguir tais conceitos. Já que, cada camada executa alguns serviços para a camada acima dela. Dessa maneira, tem-se que a definição do serviço informa o que a camada faz, e não a forma como as entidades acima dela o acessam ou mesmo como se dá o seu funcionamento. E

a interface de uma camada informa como os processos acima dela podem acessá-la. Além disso, os protocolos utilizados em uma camada são de responsabilidade exclusiva dessa mesma camada.

Em relação à arquitetura TCP/IP, verifica-se que originalmente este não distinguia com clareza a diferença entre serviço, interface e protocolo, muito embora se saiba que os seus criadores tenham feito tentativas no sentido de adaptá-lo ao modelo OSI (TANENBAUM, 2003, p. 40).

Segundo Tanenbaum (2003), os protocolos do modelo OSI são melhores encapsulados que os da arquitetura TCP/IP, podendo, portanto, em função dos avanços tecnológicos, serem facilmente substituídos.

Na sequência desse estudo, estão algumas considerações sobre o Protocolo IP, incluindo-se o IPv4 e a nova versão – o IPv6 – que surge em função da rápida expansão da rede mundial de computadores. Conhecer melhor tais conceitos e processos torna-se essencial para o objeto do estudo em foco, desenvolvimento e instalação de um servidor *Asterisk*, usando o *Proxy Asterisk* e o *Goteway Asterisk*.

2.4 Protocolo IP

O *Internet Protocol* (IP) é um protocolo da camada de rede, responsável pelo encaminhamento dos dados entre as redes. Para isso, realiza diversos serviços, tais como: interconexão, endereçamento, fragmentação e roteamento. Esse protocolo constitui a base da arquitetura Internet, sendo usado por todos os serviços de aplicação, já que tudo que trafega pela rede é transformado em pacote IP (BEZERRA, 2008,p. 3).

Para a comunicação entre as aplicações, o IP adota um sistema de endereçamento semelhante aos de números de telefone, visando à identificação única do computador na internet (BEZERRA, 2008, p. 3). Assim, cada computador conectado a Internet dispõe de um número específico, denominado de endereço IP ou número IP. De forma que, quando uma aplicação se comunica com outra será necessário apenas que as mensagens sejam endereçadas ao endereço IP do computador no qual está instalada aplicação destino.

As aplicações podem estar em redes distintas, interconectadas por roteadores, podendo inclusive existir vários roteadores com caminhos alternativos. Dessa forma, os roteadores coletam, descobrem e agregam informações sobre as rotas de comunicação que podem ser usadas pelos computadores e demais equipamentos no momento do envio dos pacotes de

dados. Essa tarefa é gerenciada e executada pelos protocolos de roteamento, que funcionam internamente ao roteador.

Nesse contexto, o protocolo IP oferece o serviço de roteamento, que é o processo de encaminhar pacotes entre redes conectadas, ou seja, é a escolha do caminho onde os datagramas irão trafegar. Para redes baseadas em TCP/IP, o roteamento faz parte do protocolo IP e é usado em combinação com outros serviços de protocolo de rede para fornecer recursos de encaminhamento entre *hosts* localizados em segmentos de rede diferentes em uma rede maior baseada em TCP/IP (COMER, 1998, p. 99).

No protocolo IP, a reserva de recurso do meio físico é feita utilizando à comutação de pacotes, assim, as mensagens são divididas em pacotes, nos quais é adicionado um cabeçalho IP com todas as informações necessárias para que se alcance o destino. Esses pacotes são remontados no destino. O processo de dividir em pacotes é chamado de fragmentação e o de reconstrução é chamado de remontagem de pacotes.

O protocolo IP não limita datagramas a um tamanho pequeno, nem garante que datagramas grandes serão entregues sem fragmentação. A origem pode escolher qualquer tamanho de datagrama que julgar apropriado; a fragmentação e remontagem ocorrem automaticamente, sem qualquer ação específica por parte da origem (PINHEIRO, 2005, *on line*).

Atualmente, existem duas versões do protocolo IP, que são o IPv4 e o IPv6. Essas versões serão comentadas na próxima seção.

2.4.1 Versões do protocolo IP: IPv4 e IPv6

Até os anos 90 a comunicação em rede era realizada somente com o IPv4, mas, devido ao grande aumento de usuários de Internet, pesquisadores e engenheiros da área começaram a discutir a possibilidade de escassez de endereços e a pensar em uma nova versão – o IPv6.

As duas versões do IP – IPv4 e o IPv6 – fornecem os serviços básicos da camada de rede, apresentados na seção anterior. Porém, na nova versão, que foi projetada para evitar o esgotamento dos endereços IP, foram elaboradas algumas modificações e incrementos nos serviços, visando melhorar pontos fracos do IPv4.

O Quadro 3 apresenta um paralelo entre as duas versões do protocolo IP.

Quadro 3: Quadro Comparativo do Protocolo IPv4 – IPv6

PROTOCOLO IP	
IPv4	**IPv6**
• Endereçamento de 32 bits: o espaço é limitado	• Quadruplica de 32 para 128 bits: expansão da capacidade de endereçamento, não pode ser consumida em futuro previsível
• Possibilidade de 4.294.967.296 endereços distintos: atende as necessidades de redes de diferentes tamanhos;	• Possibilidade de 340.282.366.920.938.463.463.374.607.431.768211.45340.282.366.920.938.463.463.374.607.431.768.211.456 endereços distintos: permite diferenciação de tráfego e mecanismos de prioridade;
• Possui endereço *broadcast*	• Não possui endereço de *broadcast*
• Formato do Cabeçalho de datagrama é fixo	• Formato do Cabeçalho de datagrama é flexível
• Não possui capacidade de extensão	• Capacidade de extensão do protocolo, que permite recursos adicionais
• Fragmentação é feita por vários roteadores ao longo do caminho	• Fragmentação é feita na origem
• Sem suporte a segurança	• Suporte a segurança
• Sem suporte a qualidade de serviços (QoS)	• Suporte a qualidade de serviços (QoS)

A seguir é apresentada uma breve explicação sobre as características citadas no quadro 3:

- *Endereçamento*: a principal diferença do IPv6 em relação ao IPv4 é a capacidade de armazenamento, que passou de 32 bits da versão IPv4 para 128 bits na versão IPv6. Esse aumento permite identificar um número maior de dispositivos conectado na rede. (NIC.BR, 2012, *on line*).

- *Broadcast:* no IPv4 o endereço *broadcast* é usado para enviar um pacote para todas as interfaces da rede, ou seja, comunicação de um para todos. No IPv6 esse serviço é executado pelo endereço *multicast*. O IPv4 oferece *broadcast* e *multicast.* O *multicast* é uma forma especial de difusão, que parte de um remetente para um grupo de endereços, ou seja, “o destino é um conjunto de

computadores, possivelmente em diversos locais. Uma cópia do datagrama será entregue a cada membro do grupo usando *hardware multicast* ou *broadcast*, conforme o caso" (COMER, 1998, p. 560).

- *Cabeçalho:* o IPv6 mudou comple*tamente* o formato do datagrama, alguns campos do cabeçalho IPv4 foram removidos ou tiveram seus nomes alterados e posicionamento modificados (NIC.BR, 2010, *on line). Essa*s mudanças foram feitas para aprimorar o funcionamento do protocolo e, com isso, torná-lo mais simples, flexível e eficiente. As opções e alguns campos fixos presentes no cabeçalho IPv4 foram armazenadas em cabeçalhos de extensão do IPv6, para melhorar o desempenho dos roteadores.

- *Roteamento:* no IPv4, o roteamento é feito ao longo do caminho e em cada roteador, já "o IPv6 inclui extensões de roteamento simplificadas que suportam novas funcionalidades de roteamento" que é obtida criando sequências de endereços IPv6 e usando a opção r*outing*. "Essa opção é usada por um equipamento de origem para listar um ou mais nós intermediários (ou grupos de nós) a serem visitados no caminho de destino de um pacote do protocolo" (TELECO, 2012, *on line*).

- *Fragmentação:* em redes IPv4 um pacote pode ser fragmentado por vários roteadores ao longo do caminho, isso ocorre quando o MTU[4] da próxima rede é menor que o pacote a ser transmitido. No IPv6, a fragmentação é feita apenas na origem. Antes de enviar o pacote a origem faz um cálculo para identificar a rede com o menor MTU ao longo do caminho até o destino. No IPv4, "todos os roteadores podem fragmentar os pacotes que sejam maiores que o MTU do próximo enlace. Dependendo do desenho da rede, um pacote IPv4 pode ser fragmentado mais de uma vez durante seu trajeto (NIC.BR, 2012, *on line*).
- *Segurança: o* IPv4 não oferece suporte a segurança, já no protocolo IPv6 várias ferramentas de segurança foram implementadas tais como: "IPSec, *Secure Neighbor Discovery (SEND*), Estrutura dos Endereços, *Cryptographically Generated Address* (CGA), Extensões de Privacidade e

[4] *Maximum Transfer Unit*. É o maior volume de dados que pode ser transferido em determinada rede física. A MTU é determinada pelo hardware da rede (COMER, 1998, p. 634).

ULA". O protocolo IPv6 alia-se à segurança do protocolo IPSec e, com isso, permite maior confiabilidade, autenticidade e integridade dos dados (MOREIRAS, 2012; NIC.BR, 2012, *on line*).

- *Suporte a qualidade de serviços (QoS)*: conjunto de padrões e mecanismos que garante a qualidade da transmissão de dados em programas que possuam o QoS. O protocolo IPv6 oferece suporte a QoS através de um campo no cabeçalho, cuja tarefa é oferecer um melhor serviço na transferência dos dados, evitando atraso ou perda de pacotes (NIC.BR, 2012, *on line*).

Apesar das diferenças verificadas nas duas versões – IPv4 e IPv6 - o funcionamento básico e os principais serviços oferecidos pelo protocolo IP são os mesmos nas duas.

Essa seção apresentou uma visão geral do Protocolo IP, na próxima seção será feita uma descrição do VoIP, que será usado para fazer a comunicação entre os servidores Asterisk.

2.5 VoIP (Voz sobre IP)

Desde a primeira transmissão de voz realizada por Alexander Graham Bell, em 1876, por meio de uma conexão física com fios entre dois dispositivos e sem discagem de números, circuito direto (DAVIDSON *et al*, 2008, p. 31), até os dias de hoje, houve uma verdadeira quebra de paradigma no mundo das telecomunicações. A começar pela criação da Rede Pública de Telefonia Comutada (RPTC), para viabilizar a operação em rede, pois tudo o que se escuta, incluindo-se a voz humana, está na forma analógica.

Entretanto, conforme explica Davidson *et al* (2008, p. 33), "embora a comunicação analógica seja ideal para a interação humana, não é nem robusta nem eficiente" no que diz respeito a eliminação de ruídos, já que estes podem distorcer a forma de onda analógica e causar uma recepção errada.

Tal problemática fez surgir às redes digitais, aonde o ruído de linha não chega a se constituir um problema, já que os diversos repetidores além de amplificar o sinal, também, o regenera a condição original. Comprovados os benefícios dessa representação digital, a rede telefônica migrou para a modulação por código de pulso (PCM – *Pulse Code Modulations*) (DAVIDSON *et al*, 2008, p. 35).

Na velocidade da revolução tecnológica, a operação em rede avançou para o surgimento do VoIP, tecnologia que, na concepção de vários estudiosos, apresenta-se com amplas vantagens de uso, principalmente, no que se refere a redução substancial dos custos com telefonia.

VoIP, ou *Voice over IP* em inglês, significa Voz sobre o Protocolo de Internet. Trata-se de uma tecnologia que permite que a voz, normalmente transmitida pela rede de telefonia, seja digitalizada e codificada ao empacotamento de dados IP, para transmissão de voz sobre as redes de dados interligadas pelo protocolo IP (COLCHER apud CRISTOFOLI *et al*, 2006, p. 55; KELLER, 2009; TELECO, 2012, *on line*).

A tecnologia VoIP permite a realização de chamadas telefônicas por meio de uma rede de dados, substituindo os serviços telefônicos tradicionais. Para Balbinot *et al* (2003), "a voz é submetida a protocolos de codificação e decodificação (codecs) que definem como os sinais de voz são digitalizados" (apud CRISTOFOLI *et al*, 2006, p. 56) . Na utilização da Internet para realização de chamadas locais e/ou de longas distâncias, a tecnologia VoIP tem-se apresentado como uma solução economicamente viável às organizações públicas e privadas que visam o aperfeiçoamento de suas comunicações.

Conforme explica Keller (2009, p. 23), para que a voz saia de uma origem e chegue ao seu destinatário de maneira audível, o protocolo VoIP estabelece normas de implementação, para que, assim, a voz seja codificada, dividida em pacotes e transportada pela rede IP.

Assim, a plataforma VoIP transforma os sinais de voz analógicos em digitais, para serem transmitidos tanto pela Internet como também via Intranet (CRISTOFOLI *et al*, 2006, p. 56). Nesse processo, são utilizados protocolos de transporte tais como o UDP (*User Datagram Protocol*) e o RTP (*Real Time Transport Protocol*). Chegando ao destinatário, os pacotes são reordenados e convertidos à forma analógica.

No entanto, para que aconteça de forma satisfatória, a transmissão de voz exige certas características da rede "como baixa latência (atraso) origem-destino, baixa variação da latência, taxas de perdas de pacotes e ainda erros de bits baixa" (CRISTOFOLI *et al*, 2006, p. 56).

Nesse contexto, vale lembrar que, embora a transmissão em rede seja um dos grandes avanços tecnológicos da atualidade, a Internet apresenta problemas como a perda e o atraso de dados em curtos intervalos de tempo, o que geralmente acaba por congestionar a rede e causar a interrupção do fluxo de dados, o que na plataforma VoIP refere-se ao fluxo da reprodução da voz, que acaba por gerar prejuízos a comunicação.

Assim, embora se verifique amplas vantagens no uso do VoIP, há que se reconhecer os problemas que esta tecnologia apresenta, mas que podem ser minimizados e até resolvidos com a utilização dos protocolos e padrões existentes, e que visam fazer com que a comunicação VoIP seja além de aceitável a melhor solução para os problemas atuais da comunicação em rede.

No estudo sobre VoIP, ficarem caracterizadas as transformações que esta tecnologia está causando ao sistema de comunicação em redes, com o uso da Internet para substituir os serviços telefônicos tradicionais. Na sequência serão apresentadas algumas motivações que justificam o uso de VoIP.

2.5.1 Motivações

Embora a RPTC (Rede Pública de Telefonia Comutada) seja eficiente ao comutar chamadas de voz, atualmente, muitas oportunidades de negócio demandam a migração desta para uma nova rede, onde a voz é operada sobre redes construídas com uma aproximação focada para dados. Assim sendo, verifica-se que os serviços de dados são operados sobre redes que foram construídas para transportar voz de maneira eficiente, mas estes dados possuem características diferentes, como por exemplo, um uso variável da largura de banda e uma necessidade mais alta de largura da banda (DAVIDSON *et al*, 2008, p. 46).

Conforme Davidson *et al*, (2008, p.47), a RPTC não pode criar e entregar os serviços com a rapidez da demanda. Além disso, os Dados/Voz/Vídeo (D/V/V) não podem convergir na RPTC como a mesma se encontra hoje. A justificativa para tal fato decorre de que "somente com uma linha analógica, na maior parte das casas, você não pode ter acesso de dados (acesso à Internet), acesso telefônico e acesso a vídeo "(DAVIDSON *et al*, 2008, p. 47).

Além disso, a arquitetura construída para voz não é flexível o suficiente, para realizar o transporte dos dados, já que chamadas comutadas por circuitos demandam um circuito de 64 kbps permanente entre dois telefones. Assim, independentemente de quem estiver falando, a pessoa que fez ou a que recebeu a chamada, a conexão de 64 kbps não pode ser utilizada por outra fonte. Entretanto, a rede de dados, que usa a comutação de pacotes, tem a capacidade de usar a banda disponível somente quando necessário. E embora essa diferença seja pequena, esta é uma das maiores vantagens de redes de voz baseadas em pacotes (DAVIDSON *et al*, 2008, p. 47).

Mediante tais considerações, a integração Dados/Voz/Vídeo (D/V/V) constitui-se em mais que uma mudança na infraestrutura, já que a D/V/V permite desenvolver novas facilidades mais rapidamente, além de abrir o desenvolvimento de aplicações para milhares ISVs (*Independent Software Vendors*).

Muito se tem falado sobre as vantagens de VoIP, no entanto, a maioria dos comentários se referem a redução dos custos de chamadas telefônicas, principalmente em empresas que possuem filiais em outro local e costumam fazer ligações constantes para estas. Vale ressaltar outros benefícios da comunicação de voz por meio do protocolo IP, que são:

- *Infraestrutura única*: os serviços passam a ser convergentes, e a voz é transmitida pela rede de dados, dispensando a necessidade de se manter uma rede de dados e outra de telefonia na mesma empresa;
- *Mobilidade*: a telefonia IP pode utilizar a Internet como meio de comunicação e, com uma conexão banda larga, o usuário tem seu ramal em um equipamento no qual poderá se autenticar e não uma localização física do mesmo;
- *Controle do sistema de telefonia*: a empresa passa a controlar seu sistema interno de telefonia. A partir da comunicação VoIP, a empresa tem o controle das ligações feitas ou recebidas por cada setor, assim como pode fazer auditorias, implementar novas funcionalidades e etc.

Para se alcançar tais benefícios e para que a comunicação seja realizada sem falhas, por ocasião da implantação do VoIP, faz-se necessário atender a todas as exigências do *software*, observando as seguintes métricas:

- *Atraso*: tempo que um pacote gasta para fazer o percurso de uma origem até o seu destino e que pode ser reduzido com a priorização dos pacotes nos nós de comutação da rede (OLIVEIRA FILHO, 2006).
- *Variação do atraso (jitter):* variação do tempo e/ou sequência da entrega de pacotes. Este problema pode ser solucionado com o uso de atraso de reprodução (KUROSE, 2006, p. 35).
- *Largura de banda*: especifica a quantidade de dados demandados por uma aplicação em uma unidade de tempo (SILVA, 2004, p. 38). Deve-se especificar

uma largura de banda mínima para cada aplicação de tal forma que o fluxo de dados demandado possa ser atendido.

- *Perda de pacotes*: pacotes de dados que na saída de sua origem são perdidos e por algum motivo não chegam ao seu destino.

Após conhecer os benefícios que a telefonia IP oferece ao usuário do sistema, na sequência deste estudo serão abordados os serviços disponibilizados com a implantação da plataforma VoIP.

2.5.2 VoIP: Serviços Disponibilizados

A disponibilidade de uma infraestrutura VoIP demanda equipamentos básicos e específicos, tanto no que se refere a conversão analógico/digital, como para compressão da voz, segurança, integração entre TDM ou móveis, dentre outros.

Nessa sessão, serão apresentadas as possibilidades de arquitetura e de serviços que podem ser somados aos sistemas de voz em IP, que segundo Bianchini (2008, p. 9) são as seguintes:

a) Integração de sistemas com tecnologia VoIP à rede pública de telefonia PSTN;
b) Todas as funcionalidades de um PABX;
c) *Call Center* e Voice Mail;
d) Sistemas de autoatendimento;
e) Integração com outras aplicações;
f) Sistemas de teleconferência;
g) Sistemas de chamadas de longa distância.

Com a disponibilidade desses serviços, o uso da tecnologia VoIP torna-se mais atraente, pois por meio do uso de *softwares* livres (servidores, banco de dados, *softphones*), permite a configuração para disponibilização dos serviços de VoIP, contribuindo para a redução nos custos (BIANCHINI, 2008, p. 17).

Para utilizar a tecnologia VoIP é necessário que se tenha uma rede de telecomunicações, móvel ou fixa, dando suporte a esse conjunto de tecnologias, conforme demonstrado na Figura 5.

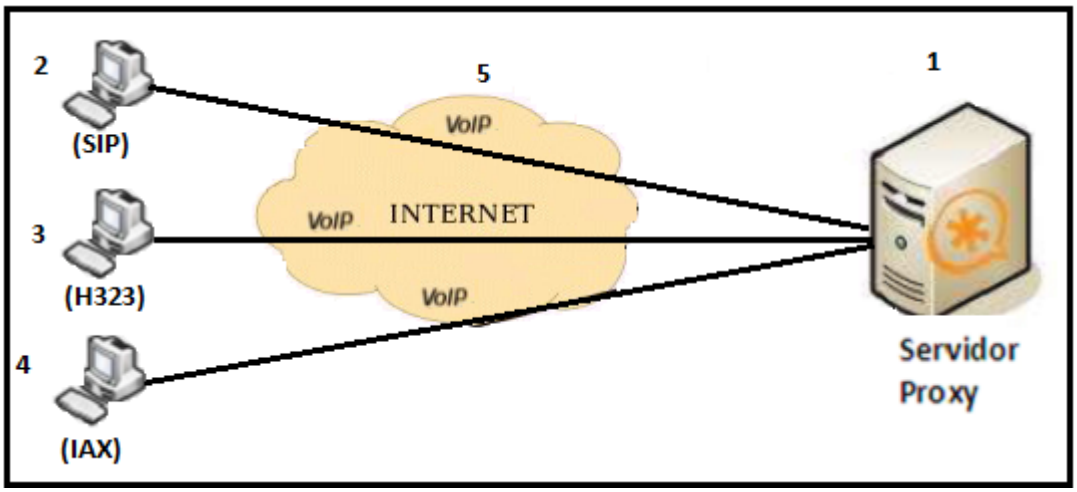

Figura 5: Central Asterisk interligada com os protocolos VoIP

A Figura 5 apresenta os usuários 2, 3, e 4 conectados a central Asterisk (1) via VoIP utilizando a internet (5) como meio de comunicação, os protocolos VoIP usados para essa comunicação são SIP, H323 e IAX respectivamente. A escolha de cada protocolo fica a critério de cada empresa ou usuário, observando as características de cada um.

Assim, o Asterisk fornece um grupo de aplicações que implementam as funcionalidades oferecidas. Exemplificando tem-se: Dial() – conecta dois canais de comunicação; Hangup() – encerra uma chamada; Voicemail – correio de voz; dentre outras. O processamento do Asterisk é baseado em planos de discagem, ou seja, com organização das regras de discagem, usando um conjunto de aplicações.

2.5.3 Codecs (Codificador/Decodificador) de voz

Os codecs, codificador/decodificador, são interpretados como modelos matemáticos utilizados para digitalizar informações analógicas de áudio, ou seja, converter o áudio de analógico para digital (KELLER, 2009, p. 20).

A função principal dos Codecs (COder/DECoder) é codificar a voz em um formato específico para transporte em uma rede digital, compactar os dados e colocar resistência a latência da perda de pacotes.

Os programas que fazem uso do VoIP têm no mínimo um codec, que deverá ser previamente configurado, tanto na origem como no destino, para que a comunicação seja estabelecida. Existem vários tipos de codecs, com necessidades específicas.

Os codecs têm como principais características a taxa de bits – quantidade de bits por segundo necessária para a entrega de um pacote de voz; e o MOS (*Mean Opinion Score*) – padrão do ITU-T, que visa medir a qualidade do áudio na visão do usuário. A medição do MOS é realizada de maneira subjetiva, exemplificando, um grupo de pessoas ouve um determinado codec e atribui uma nota de 1 a 5, sendo que a nota 1 equivalente a péssimo e 5 a excelente (AMORIM, 2010, p. 15). Quando a qualidade do áudio é inferior a 3,5, o áudio é considerado como não aceitável. Os principais codecs de áudio são: G.711, G.729A, GSM e iLBC. Na tabela 1 estão relacionados os principais codecs de áudio (DAVIDSON, 2008, p. 168).

Tabela 1: Principais Codecs

Codec	Taxa de bits (Kbps)	Licença Livre?	MOS	Comentários
G.711	64	Sim	4,3	Baixo uso da CPU (baixa compressão)
G.729A	8	Não	3,7	Ótimo uso da Banda e qualidade de voz (alta compressão)
GSM	13	Sim	3,8	Mesma codificação do celular/ baixo uso da banda (compressão baixa/média)
iLBC	13.33/15	Sim	4,14	Resistente a perda de pacotes (compressão baixa/média)

Fonte: Amorim (2010)

G.711

O codec G.711 é o padrão da telefonia convencional e possui excelente qualidade na reprodução da voz. No entanto, para realizar as transmissões requer uma largura de banda maior. O G.711 é muito usado em aparelhos de fax para enviar e receber chamadas.

G.729A

O codec G.729A usa a mesma codificação da telefonia móvel, utilizando uma pequena largura de banda oferece excelente qualidade de áudio. Embora o G.729A seja um modelo bastante popular e utilizado por muitos sistemas de telefonia, a sua utilização demanda uma licença paga (MATIAS & FERNANDES, 2009, p. 32).

Nesse CODEC os dados que são muito comprimidos, assim, para que o G.729A atinja sua taxa de compressão necessita de uma grande quantidade de processamento de CPU. Num

sistema VoiP como o Asterisk, por exemplo, seu uso não é vantajoso devido "ao fato de que rapidamente sobrecarregaria a CPU" (MATIAS & FERNANDES, 2009, p. 32).

Outro aspecto a ser ressaltado sobre este codec é que utiliza uma largura de banda muito pequena, apenas 8 Kbps de banda, já que os dados são bastante comprimidos.

GSM

A utilização do GSM é livre e não necessita de licença para seu uso, tornando-se assim o mais utilizado em sistemas Asterisk. Além disso, é um codec que apresenta excelente desempenho no que se refere ao uso da CPU, pois não demanda muito processamento. A principal característica do codec GSM é o modelo matemático que modela o sistema vocal humano, utilizando o método de compressão LPC (*Linear Predictive Code*). O LPC é um método de compressão digital que foi projetado especificamente para voz e que adapta o sinal de voz por um modelo matemático para transmissão, e depois decodifica, gerando uma voz sintética similar a original (MATIAS & FERNANDES, 2009, p. 33).

iLBC

Este codec, mesmo tendo um baixo uso de largura de banda, é especialmente adequado para os *links* de rede atenuadores, pois utiliza 13,3 quadros de 30 ms ou 15,2 quadros de 20 ms. Atualmente, embora este modelo seja suportado pelo Asterisk, ele não é tão popular quanto os outros codecs. Por isso, o iLBC pode não ser compatível com alguns telefones IP comuns e sistemas comerciais VOIP. Além disso, como o iLBC utiliza algoritmos complexos de compressão, acaba gerando um grande custo para a CPU no Asterisk. E embora o seu uso não implique no pagamento de direitos autorais, faz-se necessário assinar uma cópia da licença para envio aos seus criadores (MATIAS & FERNANDES, 2009, p. 33).

2.5.4 Protocolos de Sinalização

Para se estabelecer uma conexão eficiente é necessário um protocolo de sinalização para: estabelecer as conexões, determinar o ponto de destino e, ainda, a sinalização de telefonia. (MONTARGIL, 2007).

Os protocolos utilizados e já padronizados para uma comunicação de áudio em tempo real são: SIP, H.323, MGCP e H.248/MEGACO. Entretanto, os principais protocolos usando redes baseadas no protocolo IP são o SIP e o H.323, protocolos esses, específicos para a tecnologia de VoIP (BIACHINI, 2006, p. 23). Além desses dois, nesse trabalho será apresentado o IAX2, que é o protocolo próprio do Asterisk, apesar dessa aplicação permitir os demais.

Na sequência são apresentadas informações sobre protocolos SIP, H.323 e IAX2.

SIP

O SIP (*Session Initiation Protocol*) é um protocolo de sinalização que faz o controle da inicialização, modificação e terminação de sessões interativas multimídia. Essas sessões podem ser diversas como, por exemplo, as chamadas de áudio e vídeo que podem ser realizadas entre dois ou mais interlocutores. O SIP é um protocolo *Peer to Peer*, ou seja, "as capacidades de rede, a exemplo de roteamento de chamadas e funções de gerenciamento de sessão, são distribuídas por todos os nós (incluindo terminais e servidores de rede) dentro da rede SIP" (DAVIDSON et al, 2008, p. 271).

O SIP (Session Initiation Protocol) é um protocolo de controle da camada de aplicação, que faz uso do protocolo de transporte TCP (*Transmission Control Protocol*) ou UDP (*User Datagram Protocol*) (porta 5060). Geralmente, o UDP tem a preferência de uso pelo fato de ser mais rápido, aceitar *multicast* e possuir alguns mecanismos de confiabilidade (OLIVEIRA, 2001, apud BIANCHINI, 2006).

Dentre as funcionalidades do SIP descritas por Davidson et al (2008) está a sua capacidade de criar e controlar sessões multimídia, tais como: localização, capacidades e disponibilidades do usuário, além da conFiguração e manipulação de sessão (conjunto de fluxos de mídia, onde cada fluxo pode ser de áudio, vídeo, etc.) com um ou mais usuários (participantes).

Nestas sessões estão inclusas as conferências multimídia e as chamadas de telefone para Internet. Dessa maneira, os participantes de uma sessão podem se comunicar via *multicast* (enviar uma única cópia da informação para um grupo de endereços) ou *unicast*

(envio de uma cópia separada da mesma informação para cada pessoa), por meio de uma combinação mútua (BIANCHINI, 2006, *online*; DAVIDSON, 2008, p. 272).

Na configuração da sessão, o SIP permite o estabelecimento de parâmetros de sessão para as partes envolvidas nesta. Assim, a mudança ou término é independente do tipo de mídia ou aplicação a ser usada na chamada, podendo utilizar diferentes tipos de dados, áudio, vídeo e muitos outros formatos.

O protocolo SIP possui diversos componentes, entre eles, os agentes usuários e servidores de rede. Os agentes usuários são denominados como *User Agente* (um agente de usuário), UAC (*User Agent Client* – agente usuário cliente), UAS (*User Agent Server*) e o Proxy (DAVIDSON et al, 2008).

O UAC é o agente usuário cliente, que inicia a sinalização SIP. Os agentes usuários podem ser Softphones, Telefones IP, Gateways, entre outros, e podem exercer as funções de UAC e UAS.

O UAS é o agente usuário servidor, que responde à sinalização gerada por um UAC. Os servidores de rede SIP são:

a) Servidor Proxy: entidade intermediária na rede SIP responsável para prosseguir às requisições SIP ao UAS alvo ou para outro Proxy, em favor de um UAC. Assim, um proxy faz um roteamento dentro da rede SIP, ou seja, recebe pedidos de conexão de um agente usuário cliente (UAC) encaminhando-a para um usuário agente servidor (UAS), ou para outro servidor proxy, não estando o agente usuário servidor sob sua administração. Dessa forma, o usuário cliente não estabelece uma conexão direta com o usuário servidor, podendo ser utilizado para garantir a segurança dos envolvidos na comunicação. Ele pode prover funções como autenticação, controles de acesso, segurança e roteamento (SILVA, 2006; DAVIDSON et al, 2008).

b) Servidor de Redirecionamento ou redirect: trata-se de um UAS que gera mensagens de resposta SIP da classe 300 para as requisições recebidas direcionando o UAC para contactar um conjunto alternativo, ou seja, recebe os pedidos de conexão do usuário cliente e os reenvia-os ao solicitante com informações do usuário servidor. Neste caso, o usuário cliente fica como responsável por todo o gerenciamento da chamada (SILVA, 2006; DAVIDSON et al, 2008).

c) Servidor de registro: um UAS aceita as requisições SIP REGISTER e atualiza as informações de localização em uma base de dados (DAVIDSON et al, 2008, p. 278).

H.323

O H.323 é um protocolo desenvolvido e mantido pelo ITU (MEGGELEN, 2005, p. 112). Entre os protocolos de sinalização VoIP, é o mais complexo no que tange a especificação. Esse protocolo usa portas TCP (*Transport Control Protocol*) e UDP (*User Datagram Protocol*) para iniciar e manter as comunicações de voz, vídeo. Comparando com o SIP, o H.323 possui melhor suporte a videoconferências com transmissão de dados, porém, o SIP tem um maior suporte a segurança.

O padrão H.323 utiliza canais lógicos para separar os dois tipos de mídias que podem ser enviados ou recebidos em uma chamada. Por meio dos canais lógicos é definido qual a capacidade e o tipo de mídia a serem utilizadas durante a chamada (BIANCHINI, 2006, *on line*). Em relação às mensagens, verifica-se que o H.323 trabalha com codificação binária, assim sendo, todas as mensagens são codificadas em conformidade com o Q.931 para o subconjunto de mensagens H.225. Assim, as demais mensagens são codificadas usando-se regras de codificação de pacotes PER *(Packet Encoding Rules)* e ASN.1 *(Abstract Syntax Notation 1).* Devido a essas características, o H.323 torna-se um sistema complexo, já que misturam dois métodos de codificação com regras totalmente diferentes, o que resulta em grandes esforços de programação por parte das empresas (HERSENT, apud BIANCHINI, 2006).

As revisões recentemente realizadas sobre o padrão H.323 pontuaram alguns problemas como, por exemplo, os longos intervalos para o estabelecimento de chamadas, o que resulta em sobrecarga de um protocolo de conferência cheio de facilidades, com muitas funções demandadas em cada *gatekeeper*, além de preocupações com expansibilidade para as implementações de roteamento via *gatekeeper*.

Além desses quesitos, Davidson et al (2008) ressalta que para conFigurações com terminais inteligentes, o SIP pode resolver alguns dos problemas encontrados no H.323, uma alternativa em muitas redes. No entanto, quando se refere ao mercado de provedores, o H.323 continua no comando das implantações VoIP.

Atualmente, as organizações de padrões já estão trabalhando com uma interoperabilidade SIP H.323, com a possibilidade dessa interação ocorrer em um período de transição razoável.

IAX2

O IAX Protocolo criado pela empresa mantenedora do *software* de PABX Asterisk, o qual possui o tratamento de fluxos de dados muito parecido com o SIP (MEGGELEN, 2005). O IAX foi criado para fazer comunicação entre servidores Asterisk e passou a ser utilizado para interligação de clientes. O IAX é um protocolo aberto, porém, ainda não é um padrão mantido por um órgão de padronização o que não tem impedido o seu crescimento.

2.5.5 Protocolos de Transporte

Para que ocorra a comunicação VoIP, é essencial o uso de um protocolo de transporte, como o *Transmission Control Protocol* (TCP) ou o *User Datagram Protocol* (UDP). Por ser orientado a conexão, a escolha natural para o VoIP seria o TCP, por assegurar o caminho dos dados e prover um transporte seguro, mas há um problema, o TCP reenvia pacotes descartados, causando atrasos na transmissão da voz. O UDP seria então a melhor escolha, já que não há o problema do reenvio dos pacotes, mas o mapeamento da rede se torna mais difícil (GORALSKI; KOLON, 2000).

Para resolver esse problema e realizar a comunicação fim-a-fim do áudio e/ou vídeo em tempo real, alguns protocolos de camadas superiores foram criados, dentre eles o RTP (*Real-Time Transport Protocol)* e o RTCP (*Real-Time Transport Control Protocol*).

RTP

O RTP é um protocolo de transporte de dados em tempo real usado em voz e vídeo na comunicação VoIP. O RTP trabalha em conjunto com o protocolo UDP, o qual, não garante que os pacotes enviados pela a origem serão entregues ao destinatário.

O RTP define como deve ser feita a fragmentação do fluxo de dados de voz e vídeo, adicionando em cada pacote informações como ordem de envio e tempo de entrega. Caso algum pacote seja perdido ao longo do caminho ou chegue atrasado ao destino o RTC não envia um novo pacote. Para complementar o serviços oferecidos pelo RTP foi desenvolvido o RTCP.

RTCP

O RTCP oferece mecanismos de monitoramento dos pacotes, como: número de pacotes enviados, número de pacotes perdidos, *jitter* etc. Através do RTCP é possível controlar a sessão através do uso de pacotes do tipo BYE, que indica o fim da sessão e obter informações dos usuários da sessão como e-mail, nome e número de telefone (ARORA, 2000, *on-line*).

Segundo Arora (2000, *on-line*), as principais funções do protocolo RTCP são:

- Sequenciamento dos pacotes: os pacotes são numerados em sequência de forma a detectar a perda de pacotes.
- Identificação de payload: a internet é uma rede heterogenia, eventualmente é preciso que a transmissão se ajuste a mudanças de banda disponível.
- Indicação do quadro: um bit é usado para indicar o início e o fim do quadro.
- Identificação da fonte: cada fonte, em uma transmissão multicast, recebe um identificador para determinar o originador do quadro.
- Sincronização Intramedia: O RTP fornece indicação de tempo nos pacotes para compensar a variação no atraso dos pacotes.

Essa seção apresentou os protocolos da camada de transporte que auxiliam o TCP e UDP na transmissão de voz via rede IP. A próxima seção fará uma abordagem sobre o Asterisk, usado para configurar a central PABX.

2.6 Asterisk

O Asterisk é um *software* PBX baseado em código livre, criado por Mark Spencer, da Digium Inc., atualmente, a principal desenvolvedora e fabricante de placas de telefonia para Asterisk (MONTARGIL, 2007). Este *software* fornece todas as funcionalidades de uma central telefônica convencional (PABX) e opera tanto em uma plataforma Linux como em outras plataformas como Unix e Windows, com ou sem *hardware* conectado à rede pública de telefonia.

Como o Asterisk é um s*oftware* livre, e, portanto de código aberto, implementa em *software* os recursos encontrados em um PABX convencional, utilizando a tecnologia de

VoIP (SMITH, 2005). Assim, as aplicações e os recursos que o Asterisk disponibiliza como projeto de código aberto aos seus usuários, são de grande relevância para a comunicação em rede, pois é possível realizar conferências, correio de voz, música em espera, e até as chamadas em espera

Conforme explica Gonçalves (2008, *on-line*), o Asterisk é o primeiro PABX de código aberto da indústria, sendo que:

> Metade do desenvolvimento é feito pela empresa e metade pela comunidade. Quando usado em conjunto com as placas de telefonia PCI, ele oferece excelente relação custo/benefício para o transporte de voz e dados sobre arquiteturas TDM, comutadas e redes baseadas no protocolo IP.

Por ser um *software* que apresenta custos bastante reduzidos, pode ser interessante para as empresas implantar a comunicação com o VoIP, substituindo as centrais telefônicas convencionais pelo Asterisk, o qual permite conectividade entre os ramais da empresa e, destes, com rede pública de telefonia.

Atualmente, a Digium Inc. é a principal patrocinadora do Asterisk e uma das líderes na indústria de PABX em código aberto, oferecendo o Asterisk, em três tipos de licenciamentos, que são:

1) ***Asterisk GPL***: a utilização deste modelo permite que o código seja alterado desde que toda e qualquer modificação e/ou implementação no código seja dividida com todos (DIGIUM, 2012; GONÇALVES, 2008).

2) ***Asterisk Business Edition***: este é destinado ao agente usuário, que deseja modificar e/ou implementar o código, mas não quer divulgá-lo, e ainda para aqueles que não querem ou não podem utilizar a versão GPL. A licença GPL não tem diferença de código para o *Business Edition* (DIGIUM, 2012; GONÇALVES, 2008).

3) ***Asterisk OEM***: esta versão é destinada aos que não desejam que terceiros saibam que utilizam Asterisk em suas centrais (DIGIUM, 2012; GONÇALVES, 2008).

Como o Asterisk é um *software* gratuito, não existem estatísticas de vendas de PABX IP. Entretanto, anualmente são realizados um milhão de *downloads* e mais de 300.000 sistemas instalados.

Assim, o Asterisk, por meio da comunicação por IP, permite a construção de centrais PABX IP de vários portes, sendo que as suas funcionalidades são configuradas em planos de discagem, tema a ser abordado na seção seguinte.

2.6.1 Plano de discagem e funcionalidades

O plano de discagem (*Dialplan*) do Asterisk é a mola propulsora do *software*, que define como as chamadas serão gerenciadas pelo Asterisk (GONÇALVES, 2008), no qual são definidas como as chamadas de entrada e saídas serão programadas, determinando, por exemplo, em qual tronco a ligação vai sair. É possível desenvolver um plano de discagem simples para que todas as chamadas de entradas sejam direcionadas a um único ramal ou mesmo a montagem de uma URA (Unidade de Resposta Audível), que realiza atendimento automático e encaminha o usuário para o ramal desejado.

O plano de discagem consiste em uma lista de instruções que o Asterisk deve seguir. Tais instruções são disparadas a partir dos dígitos recebidos de um canal ou aplicação (GONÇALVES, 2008).

Cada instrução é ordenada por prioridades, a instrução com maior prioridade é disparada primeiro, prosseguindo para uma com prioridade menor, sequencialmente, ou de forma imposta por uma aplicação. Essas instruções são chamadas de Extensões (*Extensions*), e seguem uma formatação pré-definida, formadas por um identificador, uma prioridade e uma aplicação a ser executada.

As listas de instruções são divididas em blocos, denominados de contexto (*Context*), o qual permite que as instruções de um contexto sejam totalmente isoladas das instruções de outro contexto.

Dessa maneira, são os contextos que definem como as ligações de entrada ou saída serão tratadas, já que cada interface tem um contexto definido. Assim sendo, as interações entre os contextos poderão acontecer se estiverem sido especificadas.

Existem várias aplicações disponíveis para o plano de discagem, elas incluem acesso a banco, gerenciamento de ligações, controle das extensões, manipulação de *string*, entre outras. A partir delas é possível criar menus de voz, acesso ao *voicemail*, conferência e vários outros serviços comuns à telefonia.

O plano de discagem é criado no arquivo ***extensions.conf***, no qual são criados contextos, extensões, prioridades e aplicações, os quais estão definidos a seguir:

- ***Contextos***: local em que são realizadas as identificações do *dialplan*, *com suas* especificidades e para qual fim serão destinadas as extensões que são inclusas dentro deste. No contexto, é possível separar as extensões de acordo com os departamentos da corporação, implementando a segurança, no que se refere ao

controle de chamadas interurbanas, pois como o Asterisk faz a autenticação do usuário, ele pode restringir as chamadas (GONÇALVES, 2008).

- ***Extensões***: trata-se das linhas que serão interpretadas pelo Asterisk durante sua execução. As extensões são numéricas e podem conter símbolos como aqueles caracteres que são encontrados no teclado telefônico. Os caracteres que são restritos, pois representam extensões padrão do Asterisk como o s (*start*), t (*time-out*), h (*hangup*) (GONÇALVES, 2008).
- ***Prioridades***: são definidas pela quantidade de linhas encontradas na extensão ou pelo usuário, principalmente em casos que existam exceções para atender, por exemplo. No *dialplan*, elas são encontradas após o número da extensão e sempre separados os campos através de vírgulas como por exemplo: *exten=>123,1,Answer()*. As exceções têm como padrão não seguir a sequência da numeração, mas acrescentar 100 (cem) juntamente com o início da sequência da numeração. Por exemplo: *exten=>123,101,Playback(demo-thanks).* (GONÇALVES, 2008).
- ***Aplicações***: também chamadas de funções. Executam tarefas como atender a chamada, desligar e fazer discagem, ou seja, funções rotineiras de um PBX analógico. Desta forma pode-se trabalhar com tecnologia digital em funções analógicas. Tem-se como exemplo: Answer(), Hangup(), Dial().(GONÇALVES, 2008).

O Asterisk oferece várias aplicações, sendo as mais utilizadas:

- ***Answer*()**: é usada para responder a um canal que está chamando (ARTHUR, 2009, p. 3).
- ***Playback*()**: utilizada para tocar um arquivo de som previamente gravado sobre um canal (ARTHUR, 2009, p. 3).
- ***Hangup*()**: desliga o canal ativo e quem está chamando recebe uma indicação de que a chamada foi desligada. Essa aplicação deve ser usada ao final do contexto, quando quiser terminar a atual ligação para assegurar que o *dialplan* não continuará sendo usado (ARTHUR, 2009, p. 3).
- ***Background*()**: funciona da mesma forma que o *playback*(), mas na *background*() quando o chamador pressionar uma tecla, ou uma série de teclas,

em seu telefone, ela interrompe a música ou outro som qualquer como o menu de voz e vai para a extensão que corresponder ao dígito pressionado. Assim, se o chamador pressionar a tecla 5, ela vai parar de tocar o arquivo de som e enviar o controle da chamada para a primeira prioridade de extensão 5. A utilização mais comum da *background*() é criar menu de vozes, também denominada de auto-atendentes (ARTHUR, 2009, p. 3).

- ***Goto*()**: usada para enviar a chamada para outro contexto, extensão ou prioridade. Por meio desta aplicação torna-se fácil mover programaticamente uma chamada entre duas partes diferentes do *dialplan* (ARTHUR, 2009, p. 4).

O Asterisk pode ser utilizado como um servidor de aplicações para um PABX existente ou conectado diretamente à rede pública. Neste caso, ver Figura 6, ele desempenha a função de correio de voz, recepção de fax, gravação de chamadas, URA conectada a um banco de dados ou mesmo um servidor de áudio conferência. Caso, o Asterisk seja integrado ao *e-mail* tem-se então, um sistema de mensagens unificado. Na avaliação de Gonçalves (2008, p. 4), tal situação em outras plataformas torna-se "uma solução muito dispendiosa. Para estas aplicações, o Asterisk é uma excelente opção com um custo relativamente pequeno".

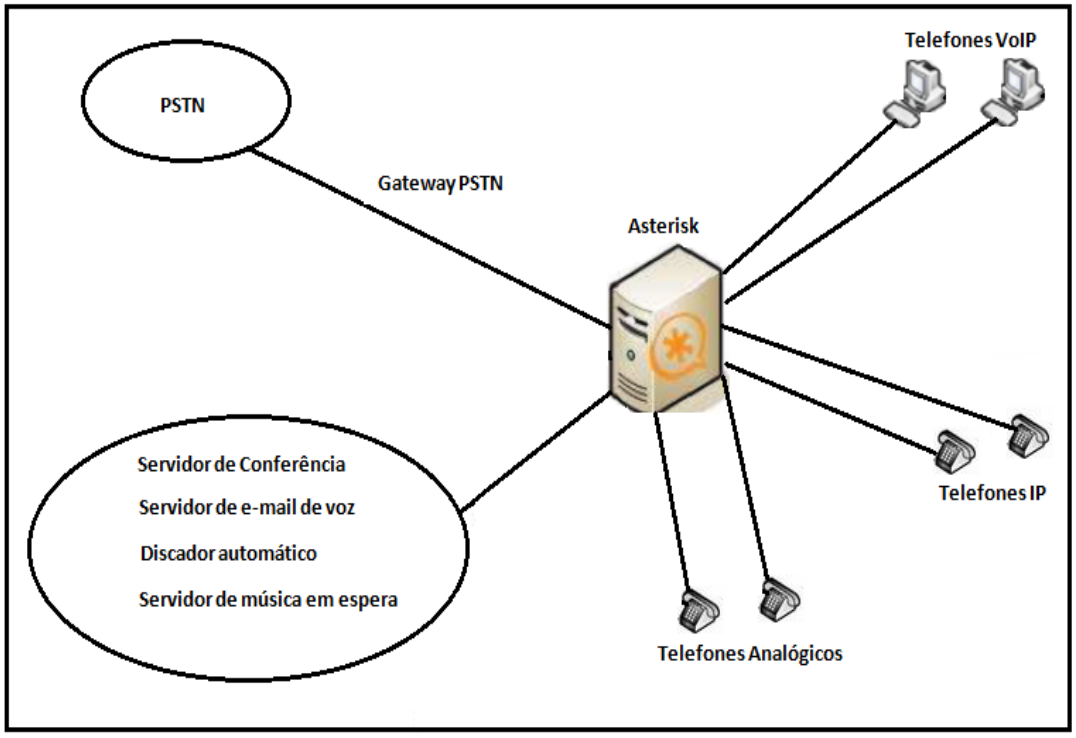

Figura 6: Central PABX com vários serviços

A Figura 6 apresenta a integração de vários serviços no Asterisk, ligados a uma central PABX utilizando a tecnologia VoIP, e a partir dessa central é possível realizar ligações para vários telefones IP's, Analógicos ou VoIP, além de oferecer serviços como URA e permitir a conexão com a rede PSTN.

A URA pode fornecer várias serviços, como correio de voz, sala de conferência, discador automático, servidor de música em espera, sistema de mensagens unificadas, distribuidor automático de chamadas e fila de atendimento.

2.6.2 Vantagem X Desvantagem

O Quadro 4 apresenta um resumo das vantagens e desvantagens do Asterisk.

Quadro 4: Vantagens x Desvantagens do Asterisk

ASTERISK	
Vantagens	**Desvantagens**
• Softwares livres – dão maior poder ao usuário; • Não há limite para a quantidade de ramais instalados; • Redução dos custos com equipamentos e contas de telefonia; • Permite o uso de telefones convencionais evitando novos gastos na requisição de aparelhos IP; • AsteriskNOW - instalação e a operação são fáceis (CD) • Total liberdade de conFiguração e personalização; • Autonomia para controle do sistema de telefonia; • Não há dependência da espera de um técnico para conFigurar o PABX do proprietário; • Flexibilidade permite mudanças de funcionalidades facilmente implementadas; • Melhoria no atendimento com recursos de correio de voz e registro de chamadas perdidas; • Facilidade e rapidez no ambiente de desenvolvimento; • Recursos amplos e abrangentes; • Provisão de conteúdo dinâmico por telefone; • Plano de discagem flexível e poderoso; • Roda no Linux e é em código aberto - comunidade de software livre	• Por ser um software gratuito a participação de mercado do Asterisk é muito pequena; • Algumas empresas são resistentes ao uso de *software* livre; • Uso da CPU do PC para processar o áudio é condenável; • Falta de alimentação elétrica; • Vulnerável a quaisquer tipos de ataques interno e externo; • A voz consome muito mais tráfego do que uma comunicação de dados (como email, navegação na Internet, etc.); • Críticas sobre eventuais falhas do servidor; • Dificuldades de se encontrar suporte técnico; • Não faz retransmissão da voz, ou seja, a perda de algum pacote de dados causará uma degradação na qualidade da voz.

Apesar das desvantagens apresentadas no Quadro 4, estudiosos e profissionais da área como Flávio Gonçalves (2008) defendem amplamente o uso do Asterisk. Na sequência deste estudo está uma breve abordagem acerca das Redes Asterisk.

2.6.3 Redes Asterisk

A maioria dos provedores de voz sobre IP usam um SIP proxy para fazer o registro, localização e autenticação dos usuários. De qualquer forma a ligação tem de ser encaminhada na maioria das vezes para a rede pública de telefonia. Isto pode ser feito diretamente através

de um gateway PSTN[5] usando interfaces E1[6] ou analógicas. Em muitos casos, no entanto, é preciso encontrar com um provedor de terminações usando conexões SIP ou H.323. O Asterisk pode atuar nesta arquitetura como um media gateway, traduzindo protocolos de sinalização e codecs, sendo que, o seu custo chega a ser uma ordem de grandeza menor que as soluções proprietárias de outras empresas (GONÇALVES, 2008, on-line).

A comunicação VoIP pode ocorrer entre vários servidores, bem como entre um servidor e vários clientes. A Figura 7 apresenta a comunicação de um servidor com vários clientes.

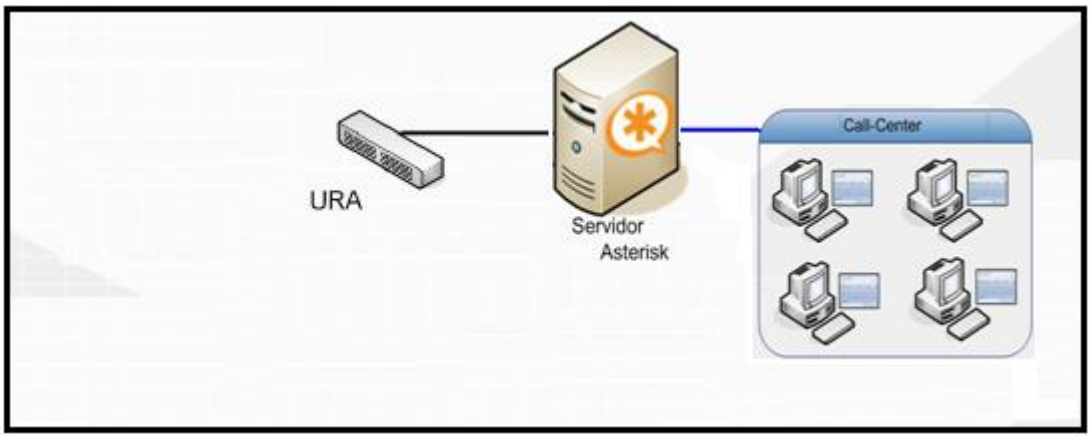

Figura 7: Ambiente de um servidor Asterisk e vários clientes

A Figura 7 apresenta o ambiente de comunicação de um servidor Asterisk e vários clientes. O servidor Asterisk, além das funções básicas de um PABX, possui a implantação de um *Call-Center* representado por quatro computadores, cada qual com sua respectiva estação de trabalho, de forma que, ao ligar para o serviço de *Call-Center* a ligação é encaminhada no primeiro instante para a URA, responsável por filtrar e encaminhar as ligações para cada setor da empresa, representado aqui pelas estações de trabalho.

A maior parte das empresas que usam Asterisk tem a necessidade de interligar redes distintas de forma que os ramais entre matriz e filial se comuniquem sem gerar nenhum custo

[5] Rede Pública de Telefonia Comutada ou RTPC (do inglês *Public Switched Telephone Network* ou PSTN) trata-se da rede telefônica mundial comutada por circuitos destinada ao serviço telefônico, e que é administrada pelas operadoras de telefonia. Inicialmente foi projetada como uma rede de linhas fixas e analógicas, mas atualmente é digital, incluindo ainda dispositivos móveis como os telefones celulares (RONCAGLIA, 2009). Disponível em: <http://mestreasterisk.com.br/artigos-mestre-asterisk/pstn-rede-publica/> Acesso em: 11/jun./2012.

[6] O Asterisk é interligado a uma rede de dados por meio de uma porta Ethernet de 100 Mbps, "com a possibilidade de ativar um *firewall* e fazer o controle de banda para os telefones IPs, caso seja necessário". Para interligar-se com o PBX Analógico ou STFC, o Asterisk possui vários tipos de modelos de placas, com interfaces FXS, FXO, E1, T1 e PRI (ALIGERA, 2012). Disponível em: <http://www.aligera.com.br/o-que-e-asterisk>

adicional as empresas. A Figura 8 apresenta a comunicação entre matriz e filial em redes distintas.

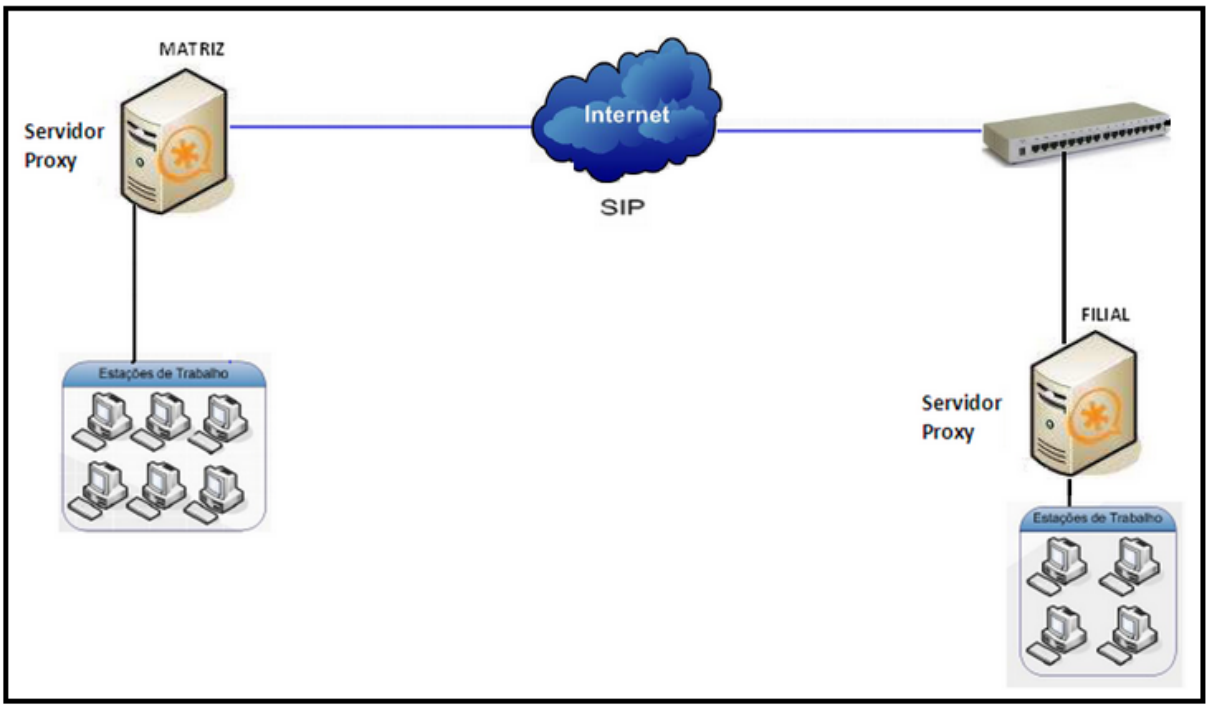

Figura 8: Ambiente em implantação matriz e filial

A Figura 8 representa o ambiente de dois servidores Asterisk, sendo um ligado na rede da matriz e o outro na rede da filial. O Asterisk não limita a quantidade de ramais para cada servidor e sim a quantidade de ligações simultânea em cada um deles. A fim de tornar mais fácil a entendimento da comunicação entre matriz e filial, vamos representar a matriz como sendo a ULBRA Canoas e a filial como a ULBRA Palmas.

Todos os ramais existentes na ULBRA Canoas estão configurados em um PABX representado pela matriz, assim como todos os ramais da ULBRA Palmas estão configurados em um PABX representado pela filial, para que a comunicação venha acontecer entre a matriz e a filial ou vice-versa é necessário um link de internet. A comunicação entre os servidores Asterisk tanto da matriz quanto da filial foi feita através de um servidor *proxy*, que faz a ligação entre a origem e o destino. O servidor *proxy* pode ser configurado usando qualquer protocolo de sinalização.

2.7 Vulnerabilidade

Atualmente, tem sido cada vez mais frequente as ocorrências de ataques a computadores que ficam conectados a Internet. Na maioria das vezes, esses ataques ocorrem devido à vulnerabilidade deste computador, ou seja, um computador conectado a Internet explora a vulnerabilidade de outro computador, para acessá-lo sem autorização.

A vulnerabilidade é explicada na Cartilha de Segurança para Internet (CERT.br, 2012, *on line*), como sendo "uma falha no projeto, implementação ou configuração de um *software* ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador".

Esses ataques tem sido notificados e acompanhados periodicamente pelo CERT.br/Nic.br, com posterior análise dos incidentes que diariamente lhe são reportados. Dentre as principais notificações de incidentes destacam-se as tentativas de fraude, ataques a servidores *Web*, computadores comprometidos, varreduras e propagação de códigos maliciosos (CERT.br, 2012, *on line*).

As categorias de incidentes mais comuns, notificados pelo CERT.br (*on line*) são:

> ***Worm***: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede. ***Dos*** (DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede. **Invasão**: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede. ***Web***: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desFigurações de páginas na Internet. **Scan**: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador. **Fraude**: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem **[grifo nosso]**. (CERT.br, 2012, *on line*).

Assim, as notificações de incidentes demonstram o quanto são vulneráveis. Os principais ataques que ocorrem nos sistemas são: *buffer overflow*, *denial of service* e *cross-site scripting*. O ataque *denial of service* tem como objetivo evitar que usuários legítimos do sistema tenham acesso aos serviços. Isto é obtido através do envio de grandes volumes de dados ao sistema, consumindo de forma deliberada todos os seus recursos (FORRISTAL, 2001).

O ataque *cross-site scripting* tem como objetivo o browser do usuário. É a habilidade de inserir *scripts* maliciosos dentro de páginas Web. Os *scripts* são disfarçados como dados legítimos e executados no browser do usuário resultando no comprometimento de informações confidenciais (FORRISTAL, 2001).

Todos estes ataques ocorrem devido a vulnerabilidades existentes nas aplicações. De acordo com Vilela (2002), vulnerabilidade de segurança é definida como um problema técnico, manifestado em um defeito no *software*, que possibilita o uso ou acesso não autorizado a recursos do sistema. A vulnerabilidade só se constitui como tal se existir uma relação direta entre o problema técnico e o uso ou acesso não autorizado e se houver relato de pelo menos uma exploração em particular.

Existem disponíveis vários pacotes de *software* contendo ferramentas fáceis de usar e utilizadas pelos *hackers* para explorar as vulnerabilidades de um sistema, tornando o ataque mais efetivo. Estes pacotes contêm ferramentas do tipo *password cracking tools*, *packet sniffers*, ferramentas que modificam os arquivos *log* do sistema e os arquivos de conFiguração.

Diante disso, vale ressaltar que da mesma maneira que uma rede de computadores precisa de mecanismos de segurança para se proteger dos ataques originados das mais diferentes fontes, a tecnologia VoIP também está vulnerável a essas ameaças, necessitando portanto de segurança.

A infraestrutura do VoIP pode sofrer ataques como o do *Deny of Service* (DoS), que visa interromper ou degradar o serviço de VoIP oferecido. Dessa maneira existem "ataques de negação de serviço típicos de uma rede IP e os ataques de negação de serviço específicos destinados aos protocolos e aos atributos particulares de VoIP". (TELECO, 2012, p.1). Os ataques mais comuns detectados com o VoIP são:

- *Distributed Deny of Service* (*DDoS*): faz uso de programas maliciosos como vírus e *worms*, que são capazes de afetar o funcionamento dos equipamentos de VoIP. (TELECO, 2012).
- SIP *Flooding* – Inundação SIP: esse ataque se caracteriza por realizar a inundação de envio de mensagens INVITE do protocolo SIP ao destino, degradando o desempenho de servidores proxy SIP, impossibilitando que os terminais façam ligações. (TELECO, 2012).
- SIP *Sinalling Loop* – Repetição de Sinalizações SIP: nesta situação, são registrados dois usuários em domínio distintos, de uma maneira que quando o

servidor proxy SIP receber mensagens INVITE provenientes desse ataque, ocorrerá a duplicação das mensagens nos domínios, comprometendo o sistema SIP. (TELECO, 2012).

- VoIP *Packet Replay Attack* – Ataque de Resposta de Pacotes VoIP: é a captura e reenvio de pacotes de voz fora da sequência, gerando atraso e degradação na qualidade das chamadas. (TELECO, 2012).
- *QoS Modification Attack* – Ataque de Modificação de QoS: neste tipo de ataque, os campos de marcação dos pacotes de tempo real são modificados, necessitandode prioridade no tráfego da rede anulando o mecanismo de QoS. (TELECO, 2012).
- *VoIP Packet Injection* – Injeção de Pacotes VoIP: são inseridos na rede pacotes VoIP falsificados, com falas, ruídos e lacunas nas chamadas ativas. (TELECO, 2012).
- *Faked Call Teardown Message* – Fraude de Mensagem de Término de Chamada: esse ataque finaliza uma sessão SIP precocemente. Durante a sessão SIP, o agente do usuário recebe uma mensagem BYE para terminar a comunicação. No caso de um atacante conseguir enviar a mensagem SIP BYE, a comunicação será encerrada prematuramente. Esse ataque também pode ser direcionado ao *gateway* de sinalização, que gerencia as chamadas telefônicas, caso o *gateway* receba mensagens BYE todo o tempo, o usuário terá o serviço negado. (TELECO, 2012, p. 1).

Nas aplicações VoIP, a violação do acesso também pode acontecer por causa das vulnerabilidades dos sistemas envolvidos. Exemplificando tal situação destaca-se “a não mudança de conFigurações padrões dos dispositivos, como senha e contas que não são modificadas”. (TELECO, 2012, p. 1). Outras possibilidades de violação de acesso ao VoIP são:

1) O ataque *Man in the middle* - homem-do-meio: este ataque é realizado a partir da interceptação da sessão ativa com o invasor se apropriando dela após autenticação. No âmbito da tecnologia VoIP este ataque é denominado de sequestro de chamadas. (TELECO, 2012).

2) Ataque de dicionário de autenticação SIP: tem por objetivo adquirir credenciais de um usuário no sistema SIP, realizando o método da força bruta e que consiste no envio de

inúmeras mensagens *REGISTER* com userids e senha provenientes de um arquivo de dicionário. Assim, descobrindo a senha, o atacante pode então acessar o serviço.

Além disso, como os métodos de escuta e análise de tráfego da tecnologia VoIP afetam a confidencialidade do serviço, atualmente, buscam-se cada vez mais informações para aperfeiçoar ataques futuros, os quais acontecem quando a sinalização e o tráfego de dados não estão criptografados. Dentre estes métodos destaca-se:

- ARP *Poisoning* ou ARP *Spoofing* - Envenenamento ARP: este é um ataque que acontece no nível de enlace de rede. O atacante tenta publicar um endereço MAC (físico) para o mapeamento com um endereço IP (lógico) na tabela ARP, para interceptar uma comunicação (TELECO, 2012).
- VLAN *Hopping*: escuta de tráfego entre segmentos de rede distintas. O ataque ocorre em função da má conFiguração dos *switches* de rede (TELECO, 2012).
- Ataque ao protocolo MGCP: consiste no envio de mensagens de sinalização do protocolo ao gateway onde o atacante manipula as conexões ativas e desvia o fluxo de dados para um equipamento intermediário, antes que os dados cheguem ao verdadeiro destino.

Após conhecer os principais ataques que podem comprometer o desempenho do VoIP, o próximo item deste estudo apresenta as soluções de segurança direcionadas especificamente ao VoIP.

2.8 Soluções de Segurança para o VoIP

Inicialmente a tecnologia de VoIP chegou ao mercado ofertando redução de custos com telecomunicações e melhor aproveitamento dos benefícios da convergência. Entretanto, após o sucesso do VoIP, hoje, o foco das organizações é a segurança do serviço, principalmente no que se refere "à disponibilidade e ao sigilo das comunicações baseadas em VoIP" (CPqD, 2012, p. 1).

Para atender aos implementadores da tecnologia VoIP em relação aos seus aspectos de segurança existe a organização *Voice over Internet Protocol Security Alliance* (*VOIPSA*), que busca conduzir "a adoção de VoIP promovendo a pesquisa de segurança, a conscientização do uso das metodologias e ferramentas de testes da tecnologia" (TELECO, 2012, p. 1).

Tais ações são decorrentes das vulnerabilidades, ameaças e ataques que tanto uma rede IP como um serviço de VoIP pode sofrer, fazendo-se portanto, necessária a implementação de métodos de segurança para preservar o pleno funcionamento da comunicação das chamadas telefônicas na rede. Nesse contexto, é de grande importância que o processo de implantação e desenvolvimento de VoIP seja bem fundamentado e estruturado, com atenção redobrada nos aspectos de segurança, além do uso de ferramentas adequadas e seguras, pois esta é a melhor arma que se tem contra os prejuízos resultantes das falhas de segurança do *softwar*e.

Pois, conforme Albuquerque (2002) nenhum processo garantirá a eliminação de todos os defeitos de desenvolvimento e nem a produção de um *software* totalmente seguro. Mas, existem vários aspectos de segurança a serem considerados no desenvolvimento de sistemas. Os mais importantes são: a *confidencialidade*, a *integridade* e a *disponibilidade da informação*.

O aspecto de segurança da *confidencialidade* é a capacidade que um sistema deve ter para impedir que usuários não autorizados vejam determinada informação. Quanto ao aspecto da *integridade* da informação é a capacidade do sistema para detectar ou impedir que uma informação seja alterada sem autorização. E por fim, o aspecto referente à *disponibilidade da informação*, que é a capacidade do sistema para impedir que uma informação seja apagada ou se torne inacessível a usuários autorizados.

Em relação à questão da segurança, vale ressaltar que esta se constitui em um importante mecanismo preventivo de proteção dos dados e processos importantes em uma organização, pois ao definir a política de segurança é definido o padrão de segurança a ser seguido pelos funcionários da instituição. Pois, as políticas de segurança tal como as leis, são regras que estabelecem princípios de como proteger, controlar e monitorar as informações manipuladas pelos sistemas computacionais e redes de computadores. (DIAS, 2000).

Além disso, ao se adotar políticas de segurança, são atribuídos direitos e responsabilidades para todos aqueles que lidam com os recursos computacionais de uma organização e com as informações armazenados. É por meio da política de segurança, que também se definem as atribuições de cada funcionário em relação à segurança dos recursos com os quais trabalham, bem como as penalidades à quais estão sujeitos aqueles que não a cumprirem. (CERT.BR, 2007).

Além destes três aspectos, existem outros tais como: *autenticação, não repúdio e auditoria*. A *autenticação* representa a capacidade de garantir que um usuário, sistema ou informação é mesmo quem alega ser. O *não repúdio* é a capacidade do sistema de provar que

um usuário executou determinada ação no sistema e *auditoria* é a capacidade do sistema de analisar todas as tarefas realizadas pelos usuários, detectando fraudes ou tentativas de ataque.

Na concepção de Laureano (2005, p. 20), a autenticação é definida como sendo:

> [...] o meio para obter a certeza de que o usuário ou objeto remoto é realmente quem está afirmando ser. É um serviço essencial de segurança, pois uma autenticação confiável assegura o controle de acesso, determina quem está autorizado a ter acesso à informação, permite trilhas de auditoria e assegura a legitimidade do acesso.

Problemas de segurança são ocasionados pela perda de qualquer um destes aspectos que são de grande importância para o sistema. Ataque ao sistema é um tipo de problema de segurança grave e bastante sério, pois geralmente o atacante objetiva obter algum retorno, podendo assim, provocar grandes danos.

Existem três preocupações que são fundamentais e complementares, em relação à segurança, que são:

- Segurança do ambiente de desenvolvimento: manter os códigos-fonte seguros evitando que sejam roubados (ALBUQUERQUE, 2002).
- Segurança da aplicação desenvolvida: desenvolver uma aplicação que seja segura, seguindo corretamente a especificação de segurança e que não contenha acessos ocultos (*backdoors*), pelos procedimentos usuais, códigos maliciosos ou falhas que comprometam a segurança. O *backdoors* é um ponto dentro de um programa que permite alguém ganhar acesso ao sistema sem ter que passar (ALBUQUERQUE, 2002).
- Garantia de segurança da aplicação desenvolvida: garantir a segurança da aplicação em desenvolvimento através de testes de garantia de segurança (ALBUQUERQUE, 2002).

Dessa maneira, um sistema que consegue se proteger de um grande número de ataques, provavelmente dificultará uma série de outros, pois geralmente a maioria utiliza o mesmo mecanismo de invasão. Tais princípios devem ser observados também com VoIP, que pode dispor dos seguintes métodos de segurança:

1 *VLAN*: com a utilização deste método ocorre a segmentação lógica da rede, que separa o tráfego de voz do tráfego de dados, minimizando o efeito de ataques

de negação de serviço. Este recurso deve ser devidamente configurado, para não resultar na vulnerabilidade da VLAN *hopping* (TELECO, 2012).

2 *Virtual Private Network (VPN)*: permissão de uso de uma rede pública, Internet, para a conexão de redes privadas com alto grau de privacidade para os dados por meio de criptografia. Ao utilizar um recurso de VPN, a comunicação VoIP faz com que a ligação telefônica ocorra de modo seguro, mesmo trafegando pela Internet (TELECO, 2012).

3 *Firewall*: tem por objetivo bloquear todo tráfego proveniente de fora da rede de acordo com as políticas e regras de acessos definidas. Esse bloqueio é realizado pela técnica do filtro de pacotes, que analisa as informações contidas nos pacotes IP que transportam dados de voz, para identificar se eles são legítimos ou não (TELECO, 2012).

4 *Intrusion Detection System (IDS) e Intrusion Prevention System (IPS):* sistemas que detectam pacotes maliciosos mesmo após terem passado pelo firewall. O IDS analisa o comportamento da rede, buscando indícios de anomalias do funcionamento, gerando alarmes e eventos ao administrador de rede. Já o IPS é proativo, tratando os alertas e realizando ações de bloqueio (TELECO, 2012).

5 *Autenticação SIP*: fornece segurança no processo da requisição da sessão SIP (mensagens INVITE) e no registro dos terminais (mensagens REGISTER). A autenticação consiste em mensagens de desafio, onde a requisição e o registro não são realizados de imediato, mas com a solicitação de novas mensagens INVITE eREGISTER com MD5 digest, para que o terminal seja devidamente autenticado (TELECO, 2012).

6 *IP Security (IPSec)*: é a extensão do protocolo IP com mecanismos de segurança no tráfego de seus pacotes. O IPSec pode operar de duas maneiras: modo transporte, onde somente a carga útil do pacote (dados de sinalização ou voz) são protegidos, ou modo túnel, em que o pacote todo é protegido por criptografia (TELECO, 2012).

7 *Transpot Layer Security (TLS)*: protocolo usado para criptografar mensagens de sinalização dos protocolos VoIP, como uma URL SIP, que recebendo o mecanismo do TLS passa a ser “sips:”. Mas o TLS não é apropriado para a segurança de mensagens que utilizam o UDP na camada de transporte. Para o tráfego de mídia, é necessário o uso do DTLS (TELECO, 2012).

8 *Datagram Transport Layer Security (DTLS)*: protocolo que limita as limitações do TLS relacionadas ao protocolo UDP. Em muitos aspectos é semelhante ao TLS, tendo como diferencial o tratamento de perda de pacotes baseado em um temporizador para retransmissão. Inclui cookies nas respostas do servidor e verificando se as requisições recebidas são de um cliente legítimo ou não.

9 *Secure/Multipurpose Internet Mail Extensions (S/MIME)*: "criptografa mensagens do SIP que utilizam o SDP para definir o tipo de informação a ser transmitida (voz, dados ou vídeo)" (TELECO, 2012, p. 1).

Neste estudo sobre as vulnerabilidades das redes de comunicação constata-se que a implementação da segurança para a tecnologia VoIP, embora seja uma questão bastante complexa, é de fundamental importância a sua efetivação. Pois, embora o VoIP seja uma tecnologia recente, já se apresenta provida de soluções de segurança, qualidade de serviço, aplicações e protocolos padronizados a sua utilização.

3 MATERIAIS E MÉTODOS

Nesta seção é apresentado o local e período no qual foi configurado os servidores utilizados para realizações dos testes propostos, o *hardware* e os *softwares*, e os métodos utilizados para desenvolvimento deste trabalho.

3.1 Local e Período

Para a realização das configurações e testes propostos neste trabalho foi utilizado o Laboratório de Redes de Computadores (LaRC), do Complexo de Informática do Centro Universitário Luterano de Palmas (CEULP/ULBRA). Este trabalho foi desenvolvido como requisito parcial para as disciplinas de "Trabalho de Conclusão de Curso em Sistemas de Informação I (TCCI)" e "Trabalho de Conclusão de Curso em Sistemas de Informação II (TCCII)", no decorrer do primeiro semestre do ano de 2012.

3.2 Material

Os recursos de *hardware* e *software* utilizados para a elaboração do trabalho foram disponibilizados pelo Centro Universitário Luterano de Palmas (CEULP/ULBRA) ou adquiridos gratuitamente pela internet.

3.3 *Hardware*

Os recursos de *hardware* utilizados para a implantação do trabalho foram dois computadores, sendo um (*Desktop*) e outro *notebook*. A configuração dos computadores foi padronizada segundo a necessidade de utilização de cada um na rede.

O computador *Desktop* foi configurado como servidor Asterisk filial e o *notebook* como o servidor Asterisk matriz, os dois computadores utilizarão o sistema operacional GNU/Linux Debian.

Os servidores foram configurados como central PABX, para o envio e o recebimento de chamadas reais de áudio e atendimento automático (URA).

Também, foi utilizado um *switch* com 16 portas para a realização de testes de um terceiro computador (*Desktop*).

3.4 *Software*

Os *softwares* utilizados para realização deste trabalho estão sobre uma licença de livre distribuição como a GPL (*General Public Licença* - Licença de Pública Geral) e estão listados nesta seção.

- Linux Debian V: é um sistema operacional com distribuição livre e que possui código fonte aberto. O Debian pode ser executado em quase todos os computadores, incluindo os mais antigos, e funciona a partir do kernel do Linux. Para fazer a instalação do Debian pode-se usar uma imagem de cd ISO ou, se preferir, pode fazer a instalação via rede.

- *Zoiper*: o zoiper foi utilizado para a realização das chamadas entre os servidores Asterisk, já que este oferece as mesmas funcionalidades de um telefone convencional, seu funcionamento se dar a partir da tecnologia VoIP, tornando possível a comunicação entre os ramais conFigurados a partir de um desktop, notebook, laptop entre outros. Para realizar ou receber chamadas no *zoiper*, basta ligar de um ramal conFigurado na matriz para um ramal conFigurado na filial. Com isso o Asterisk transforma o computador em um telefone multimídia, para receber a comunicação em voz.

3.5 Métodos

Para o desenvolvimento do presente trabalho de conclusão de curso, o primeiro passo a ser realizado foi um levantamento teórico através de pesquisas e estudos com o objetivo de obter embasamento suficiente para a elaboração do trabalho. Os conceitos abordados nesta fase são relacionados à comunicação VoIP a partir de uma central PABX Asterisk.

Concluída a fase de estudos sobre comunicações VoIP e temas relacionados, o próximo passo foi fazer a delimitação do que seria necessário para a configuração de uma central PABX experimental que atendesse aos requisitos para a realização do trabalho. A partir da pesquisa, fez-se a definição do *software* e *hardware*, bem como dos serviços que seriam implantados e de como os testes seriam realizados.

Foi escrita uma revisão de literatura na qual são apresentadas as definições de conceitos relacionados à comunicação VoIP, bem como a descrição do Asterisk. Em comunicações VoIP foram observados os principais serviços disponibilizados e os componentes necessários requeridos por estes.

Com os estudos dos serviços disponíveis em um ambiente de comunicações VoIP, constatou-se que as chamadas de áudio necessitam de um tratamento diferenciado em uma rede IP para que haja uma comunicação com qualidade. O Asterisk, foi escolhido para ser implementado no ambiente de comunicações, por atender as necessidades do ambiente implementado. Depois, foi definida a implantação do ambiente de comunicações VoIP e os testes com foco nos serviços de áudio utilizando o *codec* GSM.

Após a definição com base na revisão bibliográfica do ambiente a ser implantado, o *hardware* necessário foi configurado para a realização dos testes, no LaRC/CEULP.

O ambiente de comunicações VoIP foi configurado da seguinte forma: primeiro foi configurado o notebook sendo o servidor Asterisk matriz, após a configuração do servidor matriz foi preciso a realização de alguns testes locais, para testar o funcionamento do Asterisk e corrigir eventuais erros. Após a realização dos testes, foi necessário configurar o segundo servidor Asterisk filial, para testar a comunicação via rede IP. Nos dois computadores foi instalado o zoiper, e com isso transformou os dois computadores em telefones multimídia, e assim receber a comunicação VoIP.

Para que os computadores pudessem se comunicar foram configurados um ramal tanto na matriz quanto na filial para utilização dos testes via VoIP. Após a configuração básica dos servidores foi feita a configuração para realização dos testes, que foram feitos em dois cenários:

- **cenário 1:** foi realizada uma ligação de um ramal da matriz para um ramal da filial de forma direta.
- **Cenário 2:** foi realizada uma ligação de um ramal da matriz para o serviço URA, que a partir das opções do menu foi redirecionada para o ramal da filial.

As descrições dos resultados tanto no cenário 1, quanto no cenário 2 serão descritos na seção de resultados.

4 RESULTADOS E DISCUSSÃO

O objetivo deste trabalho foi a configuração de dois servidores Asterisk que utilizam o protocolo SIP para realizar a comunicação VoIP entre os ramais de uma mesma rede e entre ramais de redes distintas. Esta seção tem a finalidade de apresentar a estrutura do ambiente criado nos servidores, detalhes de configuração, os resultados dos testes práticos que demonstram o funcionamento da central PABX e algumas considerações sobre esse tipo de ambiente.

Foram criados dois cenários de testes, no primeiro foi feita uma ligação de um ramal da matriz para o ramal da filial de forma direta, para testar o funcionamento do proxy SIP. No segundo cenário, foi feita uma ligação do ramal da matriz para um ramal configurado utilizando a URA, para testar o funcionamento do atendimento automático.

4.1 Ambiente Implantado

O ambiente implantado nesse trabalho simula um ambiente de uma rede corporativa, sendo composto por uma rede local da matriz, que possui um servidor Asterisk e os clientes (ramais) , assim como possui uma rede local da filial, com a mesma composição da matriz. Os dois ambientes VoIP local se comunicam através do Proxy SIP.

O ambiente de rede construído para o desenvolvimento deste trabalho foi configurado no Laboratório de Rede de Computadores (LaRC) do Centro Universitário Luterano de Palmas (CEULP/ULBRA), utilizando como plataforma o Sistema Operacional Linux Debian. Esse ambiente, mostrado na Figura 9, é formado por:

- LAN 1 – rede local da matriz: rede 10.243.0.0/24
- LAN 2 – rede local da filial: rede 10.242.0.0/24
- LAN entre os servidores – rede 10.241.0.0/16

O ambiente implantado para o desenvolvimento deste trabalho pode ser visto na Figura 9.

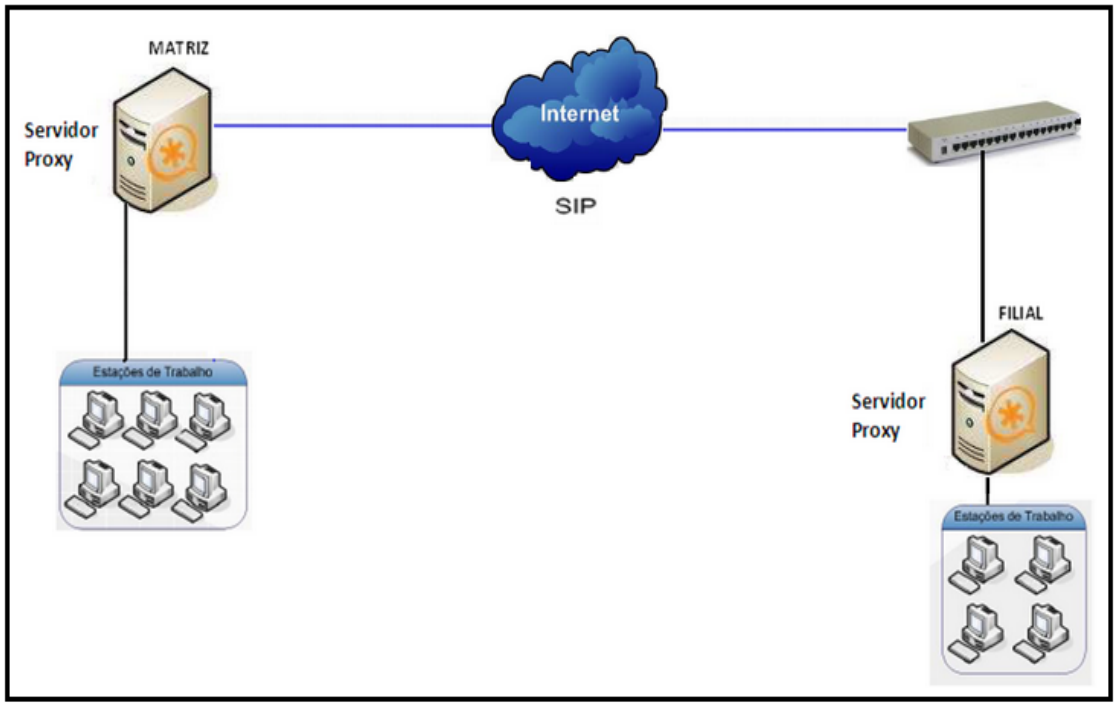

Figura 9: Ambiente Implantado

Como pode ser visto na Figura 9, no ambiente de rede implantado os dois servidores foram configurados como Proxy SIP para possibilitar a comunicação VoIP entre os ramais de redes locais distintas.

Na prática, os servidores matriz e filial estão configurados na mesma rede, porém, o funcionamento seria semelhante se estivessem configurados em rede distintas, de modo que foram criadas na mesma rede no intuito de facilitar a configuração e realização dos testes.

A próxima seção apresenta em detalhes a configuração do ambiente implantado, representado na Figura 9.

4.2 Configuração do Ambiente

Essa seção apresenta uma visão geral dos arquivos de configuração do Asterisk, que foram alterados para a configuração do ambiente. As configurações apresentadas nessa seção são as realizadas no servidor Proxy SIP da matriz, sendo que as configurações do servidor Proxy SIP da filial são realizados de forma similar, as únicas alterações são os nomes das

seções e o endereço IP. Assim, não foi descrita a configuração da filial nessa seção, sendo que os arquivos foram disponibilizados nos.

4.2.1 Configuração do Servidor Proxy SIP da Matriz

Os arquivos de configuração do Asterisk ficam dentro do diretório padrão **/etc/asterisk**, de forma que as configurações, atualizações ou modificações de cada servidor Asterisk podem ser feitas por manipulação dos arquivos existente ou pela criação de novos arquivos. Para o desenvolvimento do presente trabalho foram utilizados os arquivos de configurações ***sip.conf*** e ***extensions.conf***, que serão apresentados a seguir.

Sip.conf

O arquivo sip.conf é o arquivo responsável pela configuração de modo geral do funcionamento do servidor Asterisk com o protocolo SIP. É nesse arquivo que são configurados todos os ramais que irão se comunicar com servidor, assim como são configurados vários parâmetros como senhas, codecs utilizados, endereço IP, entre outros.

Esse arquivo é formado por uma seção geral [general], na qual as configurações valerão para todos os canais (*peers*) especificados nas outras seções do arquivo, e pelas seções de definição dos canais de comunicação, uma para cada canal/peer (Keller, 2009). A Figura 10 apresenta o conteúdo do arquivo **sip.conf** configurado no servidor da Matriz.

```
1  ;; CRIAÇÃO DA SEÇÃO DA MATRIZ;;
2
3  [matriz]
4  type = friend
5  username = matriz
6  secret = matriz
7  host = 192.168.254.137
8  qualify = yes
9  context = matriz
10 disallow = all
11 allow = alaw,ulaw,gsm
12 language = pt_BR
13
14 ;; CRIAÇÃO DO RAMAL DA MATRIZ;;
15
16 [100]
17 type = friend
18 username = 100
19 secret = 123
20 context = usuarios
21 qualify = yes
22
23 ;; CRIAÇÃO DO RAMAL EXTERNO;;
24
25 [300]
26 type = friend
27 username = 300
28 secret = 123
29 context = usuarios
30 qualify = yes
31 host = dynamic
```

Figura 10: Arquivo sip.conf do servidor matriz

No trecho da linha 3 até a linha 12 é configurada a seção geral [general], na qual são configuradas as opções do SIP. O nome da seção (linha 3) fica a critério de cada usuário, sendo que nesse trabalho foi definido o nome **matriz**. As demais configurações são:

- type: define o tipo de cliente. Existem três tipos de clientes: ***peer*** permite que o usuário apenas receba chamada, ***user*** permite que o usuário apenas faça chamadas e ***friend*** permite que o usuário passa fazer e receber ligações.
- username: define o nome do usuário
- *secret*: define a senha do usuário

- *host*: configura o endereço IP ou nome do cliente, com quem irá estabelecer comunicação. Se usar a opção *dynamic*, registra um endereço dinâmico, definido pelo DHCP da rede IP.
- *context*: define o contexto de cada peer. O Asterisk permite adicionar mais de um contexto para cada canal, desde que crie em linhas diferentes.
- *dissallow*: desabilita a utilização de todos os codecs.
- *allow*: habilita a utilização de um ou mais codecs. Para a configuração deste trabalho foram habilitados os codecs alaw, ulaw e GSM.

As linhas 16 a 31 apresentam as configurações dos ramais (*peers*) que ligam ou recebem ligações utilizando o servidor da matriz. O primeiro ramal foi configurado da seguinte forma: na linha 16 foi atribuído o número 100 para o ramal; a linha 17 determina que esse ramal pode fazer e receber ligações; na linha 18 definiu-se o nome do ramal como 100; na linha 19 definiu-se a senha como 123; na linha 20 associou o ramal ao contexto usuários, que foi configurado no plano de discagem (arquivo ***extenesions.conf***); e, por fim, a linha 21 apresenta o parâmetro ***qualify***, determinando que a todo instante será verificado se um ramal pode ser alcançado ou não. Das linhas 25 a 31 foi criado um segundo ramal com o número 300, que tem configurações semelhantes as do ramal 100, diferenciando-se por apenas receber ligações, pois seu tipo foi definido como ***peer*** (linha 20) e aceitar ligação de qualquer outro servidor SIP, já que o host foi configurado como ***dynamic***.

Extensions.conf

O arquivo *extensions.conf* é o arquivo responsável pela configuração do plano de discagem (dialplans), que determina como as chamadas de entrada e saída deverão ser tratadas. É nesse arquivo que são configuradas as aplicações existentes na central PABX, de forma que sem configurar esse arquivo, ou se a configuração estiver incorreta, torna-se impossível o funcionamento da central. Esse arquivo é dividido em seções, da seguinte forma (KELLER, 2009, p. 54):

- **Contextos**: agrupam as regras de discagem. O nome do contexto não pode ser superior a 79 caracteres e pode conter apenas os caracteres 0 a 9, de A a Z (maiúsculas ou minúsculas) e os caracteres hífem e sublinhado.
- **Extensões**: são as entradas, sequência de caracteres, recebidas pelo Asterisk. Tudo para o Asterisk é tratado como texto.
- **Prioridades**: especificam a ordem de interpretação das regras de discagem e consequentemente de execução das aplicações. Devem seguir uma ordem sequencial, sempre iniciando com a prioridade 1.
- **Aplicações**: ação ou comando a ser executado. O Asterisk possui aproximadamente 170 aplicações. Para obter a forma de funcionamento e de uso de cada uma delas, basta digitar core show application <*aplicação*> na console (CLI) do Asterisk.

A Figura 11 apresenta o conteúdo do arquivo ***extensions.conf*** configurado no servidor da Matriz.

```
 1  [usuarios]
 2
 3  exten => _1XX,1,Answer()
 4  exten => _1XX,n,Dial(SIP/${EXTEN},15,rTt)
 5  exten => _1XX,n,Hangup()
 6
 7  exten => _2XX,1,Answer()
 8  exten => _2XX,n,Dial(SIP/filial/${EXTEN},15,rTt)
 9  exten => _2XX,n,Hangup()
10
11  ;;NUMERO ATENDIMENTO DA URA
12
13  exten => 1000,2,GoTo(ura,s,1)
14
15  ;; CRIAÇÃO DA URA ;;
16
17  [ura]
18
19  exten => s,1,Answer()
20  exten => s,n(ura),BackGround(mensagemtcc)
21  exten => s,n,WaitExten(5)
22
23  exten => 1,1,PlayBack(administrativo)
24  exten => 1,2,Hangup()
25
26  exten => 2,1,Dial(SIP/filial/200,15,rTt)
27  exten => 2,2,Hangup()
28
29  exten => 3,1,PlayBack(gerencia)
30  exten => 3,2,Hangup();
31
32  ;; ENTRADA INVALIDA
33  exten => i,1,PlayBack(opcaoinvalida)
34  exten => i,n,Goto(ura,s,1)
35
36  ;; TEMPO ESGOTADO
37  exten => t,1,PlayBack(tempoesgotado)
38  exten => t,n,Hangup
```

Figura 11: Arquivo *extensions.conf* do servidor matriz

No trecho da linha 1 até a linha 9 é configurado o contexto que oferece serviços aos ramais configurados no **sip.conf**. O nome do contexto (linha 1) fica a critério de cada usuário, sendo que nesse trabalho foi definido o nome **usuários**.

As linhas compreendidas de 3 a 5 estão configuradas de forma para especificar como atender qualquer ligação dos ramais compreendidos entre 100 e 199 (_1XX), de modo que: a linha 3, na prioridade 1 é indicada a aplicação ***Answer***, que atende a chamada e sincroniza o canal de áudio, das chamadas originadas dos ramais compreendidos entre 100 e 199; a linha 4, na prioridade n, a aplicação ***Dial*** encaminha as chamadas recebidas pelos ramais entre 100 e 199 para o destinatário, utilizando o protocolo SIP; a linha 5, prioridade **n**, a aplicação ***Hangup*** encerra a chamada, fechando todos os canais de comunicação A linha 13 determina que se o ramal 1000 receber uma ligação, o atendimento será encaminhado para o contexto [ura], que determina as configurações do atendimento automático.

A linha 13 determina que se o ramal 1000 receber uma ligação, o atendimento será encaminhado para o contexto **ura**, configurado a partir da linha 17, que determina as configurações do atendimento automático.

Das linhas 19 até 38 foi realizada a configuração da URA, para realizar atendimentos automáticos, em um contexto chamado [ura]. A configuração desta foi realizada da seguinte forma:

- na linha17 foi criado o contexto da URA com o nome **ura**.
- das linhas 19 a 21 foi configurada a mensagem de atendimento automático com as opções de menu, sendo que essa mensagem é gravada em um arquivo de áudio que será reproduzido automaticamente ao usuário que originou a chamada. Na linha 19, prioridade 1, é determinado o atendimento da chamada e a sincronização do canal de áudio; na linha 20 a aplicação ***Background*** reproduz o arquivo de som configurado e armazenado no diretório ***/var/lib/asterisk/sounds***, esse arquivo informa ao usuário as opções de atendimento da URA e com isso permite a interação do usuário com o sistema.
- nas linhas 23 e 24 foi configurado o atendimento para setor administrativo, quando o usuário escolher a opção 1 no menu de atendimento automático. A linha 23, prioridade 1, determina que será reproduzida ao usuário uma mensagem gravada em um arquivo de áudio chamado **administrativo**; a linha 24 encerra a chamada após o usuário ouvir a mensagem.
- nas linhas 26 e 27 foi configurado o que ocorre quando o usuário escolher a opção 2 no menu de atendimento automático. A linha 26, prioridade 1, determina o encaminhamento da chamada do usuário para o ramal 200 da filial,; a linha 27 espera por 15 segundos para que o usuário da filial atenda a chamada, se não for atendida durante esse tempo a chamada é encerrada.
- nas linhas 29 e 30 foi configurado como é feito o atendimento para setor de gerência, quando o usuário escolher a opção 3 no menu de atendimento automático. A linha 29, prioridade 1, reproduz ao usuário uma mensagem gravada no arquivo de áudio chamado **gerência**; a linha 30 encerra a chamada após o usuário ouvir a mensagem.

- nas linhas 33 e 34 foi configurado que uma mensagem de aviso será apresentada ao usuário, sempre que mesmo escolher uma opção que não esteja configurada no menu de atendimento automático; a linha 33, prioridade 1, determina a execução do arquivo de áudio **opção inválida**, que contém a mensagem de aviso ; a linha 34 retorna a ligação para o menu de atendimento automático através da aplicação **Goto**, para que o usuário escute a mensagem de atendimento novamente.nas linhas 37 e 38 foi configurado que se esgotar o tempo de espera para que o usuário escolha uma opção do menu de atendimento automático, será executado o arquivo de áudio chamado **tempo esgotado.** A linha 37 determina que a espera máxima é 30 segundos após o usuário ouvir as opções do menu de atendimento automático; a linha 38 encerra a chamada após o usuário escutar a mensagem.

O contexto da URA funciona da seguinte forma: quando o usuário liga para o ramal 1000 a ligação será encaminhada para a [ura], a URA pode oferecer inúmeros serviços dependendo da necessidade de cada empresa ou pessoa. Alguns serviços oferecidos são: fila de espera, conferência, *voicemail*, *menu* de atendimento automático, entre outros. Como ambiente de teste foi configurado para o presente trabalho o *menu* de atendimento automático.

4.3 Descrição dos Testes

Para a realização dos testes da comunicação VoIP entre os servidores, foram criados dois cenários, o primeiro para testar a comunicação do servidor matriz para o servidor filial, a partir de uma ligação direta e o segundo cenário foi usado para testar a mesma comunicação entre os servidores, só que usando os serviços da URA. Os testes foram realizados utilizando chamada real com áudio entre matriz e filial. Esses testes foram feitos em dois cenários, descritos nas seções a seguir.

4.3.1 Cenário 1 – Ligação direta

No cenário 1 foram realizados testes no ambiente de comunicações VoIP fazendo ligações diretas, sem usar os serviços da URA. As ligações foram feitas a partir do ramal 100, configurado no servidor matriz, destinadas ao ramal 200, configurado no servidor filial.

A chamada realizada utilizando o servidor de comunicações VoIP, apresentou as seguintes características: o ramal da matriz se comunicou normalmente com o ramal da filial, o que comprova o funcionamento do proxy SIP, que redirecionou a chamada para os ramais localizados em redes distintas; o áudio apresentou boa qualidade; e o som não apresentou distorções e nem atraso.

A comunicação foi feita utilizando o codec GSM, que é um dos aceitos pelos servidores (configuração na linha 11 da Figura 10). A Figura 12 mostra uma imagem capturada durante os testes no cenário 1.

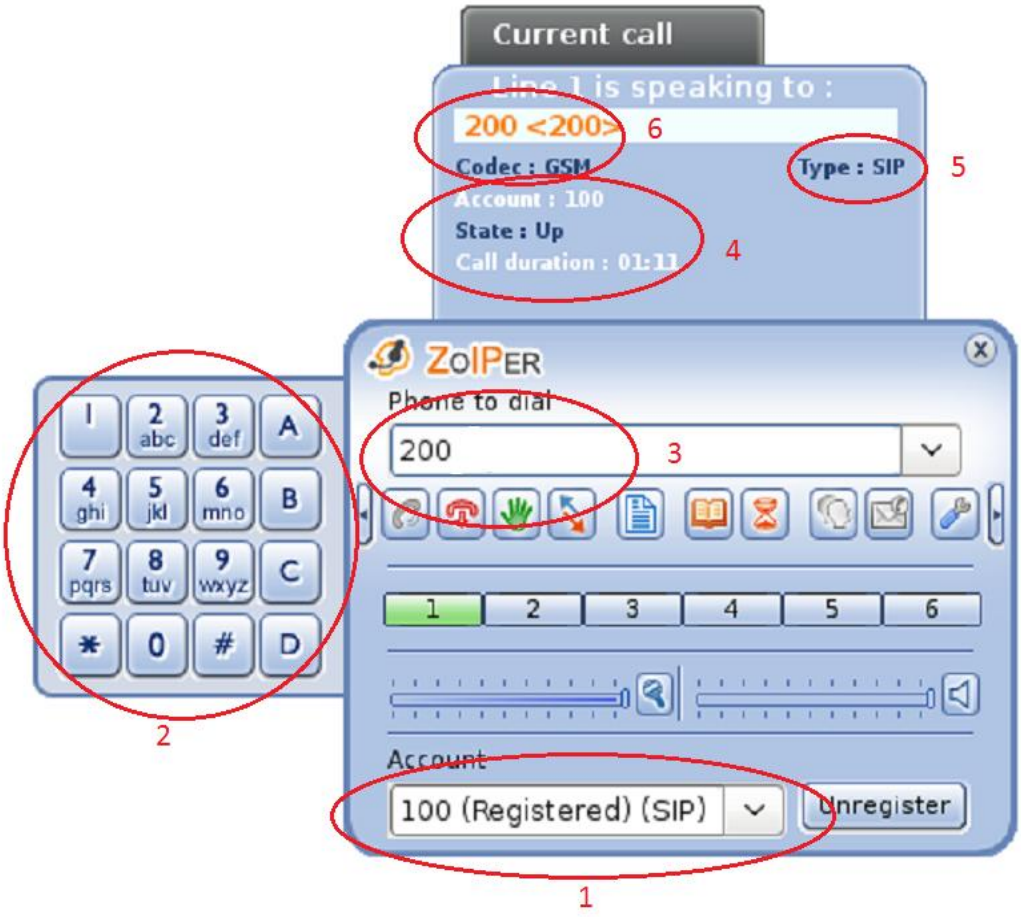

Figura 12: Ligação direta do ramal 100 da matriz para o ramal 200 da filial

A Figura 12 apresenta a tela acessada pelo usuário que utilizou o ramal 100, do servidor da matriz, para realizar uma ligação direta para o ramal 200, do servidor filial:

- a marcação 1 mostra que o ramal 100 da matriz foi registrado no protocolo SIP e foi o ramal de origem;

- a marcação 2 apresenta o teclado numérico do zoiper;
- a marcação 3 indica o local usado pelo usuário para digitar o ramal destinatário, representado aqui neste cenário pelo ramal 200;
- a marcação 4 mostra a conta (ramal) que originou a chamada, que neste caso foi o ramal 100 da matriz, assim como mostra o tempo de duração da chamada que foi de 01:11;
- a marcação 5 mostra que o protocolo utilizado na comunicação entre o ramal da matriz e da filial foi o SIP;
- a marcação 6 mostra o ramal 200 da filial como sendo o ramal destinatário da chamada, assim como mostra que o codec GSM foi o responsável pela transmissão da voz via rede IP.

A Figura 13 mostra a tela acessada pelo usuário do ramal 200, da filial, para receber a chamada originada do ramal 100, da matriz.

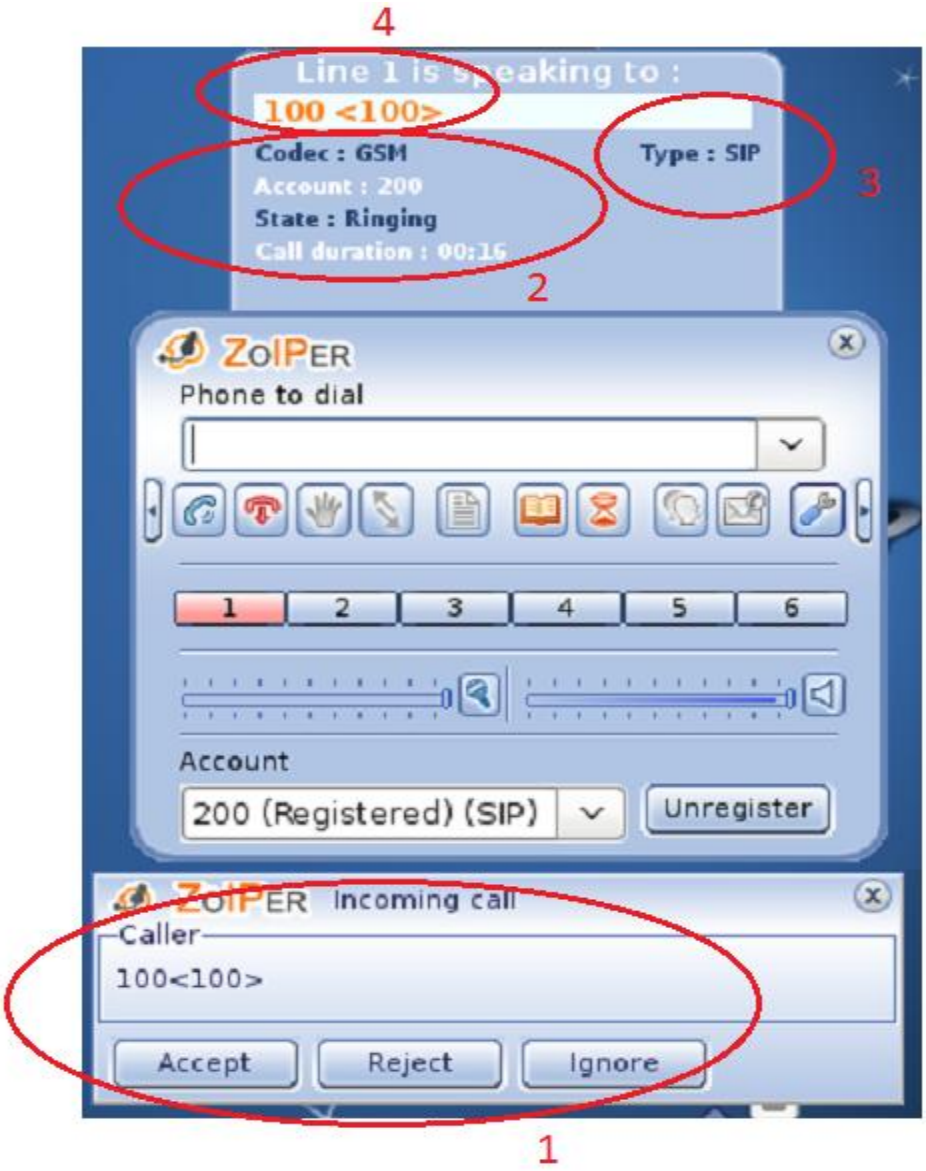

Figura 13: Ligação do ramal 200 da filial para o ramal 100 da matriz

A Figura 13 mostra a tela aberta para o usuário do ramal 200, no momento que a central PABX Asterisk recebe a chamada do ramal.

- a marcação 1 mostra que o ramal 100 da matriz é o ramal que tem como destino a ligação que partiu do ramal 200 da filial, essa ligação três opções ao destinatário: na primeira opção, ***Accept,*** o usuário poderá aceitar a chamada e iniciar a conversa; na segunda, ***Reject***, o usuário poderá rejeitar e a chamada será encerrada; e na terceira opção, ***Ignore***, o usuário pode ignorar e a chamada ficará tocando em modo silencioso, da mesma forma que acontece com um celular;

- a marcação 2 mostra a conta (ramal) que originou a chamada, que neste caso foi o ramal 200 da filial, assim como mostra o tempo de duração da chamada que foi de 00:16;
- a marcação 3 mostra que o protocolo utilizado na comunicação entre o ramal da matriz e da filial foi o SIP;
- a marcação 4 mostra o ramal 100 da matriz como sendo o ramal destinatário da chamada, assim como mostra que o codec GSM foi o responsável pela transmissão da voz via rede IP.

Considerando essas possibilidades, foram feitos dois testes:

- a chamada não foi atendida: nesse caso, após 15 segundos a chamada foi encerrada automaticamente, o que foi definido no arquivo **extensions.conf**, como explicado na seção anterior
- a chamada foi atendida: nesse caso, foi possível conversar normalmente.

Os testes realizados no cenário 1 demonstram que o servidor proxy SIP está funcionando normalmente, pois, um ramal da filial conseguiu se comunicar com um ramal da matriz, mesmo estando em redes distintas e tendo sido configurados em servidores distintos.

4.3.2 Cenário 2 – Usando os serviços da URA

No cenário 2 foram realizados testes no ambiente de comunicações VoIP fazendo ligações para o ramal de atendimento automático da URA, esse ramal foi configurado com o número 1000, como mostra a Figura 11, linha 13. Os testes feitos no cenário 2 foram idênticos aos realizados no cenário 1, as Figuras 13 e 14 representam os mesmos parâmetros usados nas chamadas entre os ramais dos servidores matriz e filial.

O que altera de um cenário para outro é o percurso da chamada entre origem e destino. Já que no cenário 1 a ligação foi feita de forma direta e para o cenário 2 será usado o ramal de atendimento automático da URA. O primeiro teste realizado no cenário 2 foi ligar do ramal 100 da matriz para o ramal 1000 configurado na URA, quando o ramal 1000 recebe uma ligação, o atendimento será encaminhado para o contexto **ura**, configurado a partir da linha 17, da Figura 11, e a partir daí o usuário entrará no atendimento automático da URA.

Os serviços oferecidos pela URA são serviços de *Call-Center*, semelhante aos serviços oferecidos ao usuário quando liga na central de atendimento do seu cartão de débito, crédito entre outros. A URA pode oferecer inúmeros serviços, como: fila de espera, conferência, *voicemail*, menu de atendimento automático entre outros. Para testar a comunicação no cenário 2 foi feita uma ligação do ramal 100 da matriz para o ramal 1000 ura, com isso foi apresentado ao usuário um menu com ramais de atendimento da URA.

O ambiente implantado oferece três opções de atendimento para o usuário, que são:

- se o usuário escolher a opção 1 a ligação será encaminhada para o setor administrativo como mostra a Figura 11, linha 26, nesse momento o usuário ouvirá uma mensagem e a ligação será encerrada;
- se o usuário escolher a opção 2 a ligação será encaminhada para o ramal 200 da filial, como mostra a Figura 11, linha 23. O ramal 200 foi configurado na ura como atendimento de suporte.
- se o usuário escolher a opção 3 a ligação será encaminhada para o setor de gerencia como mostra a Figura 11, linha 29, nesse momento o usuário ouvirá uma mensagem e a ligação será encerrada;

As chamadas realizadas a partir dos servidores de comunicações VoIP, apresentou as seguintes características: o áudio ficou normal, e com isso permitiu uma ligação telefônica, sem cortes, já que a voz foi transmitida e recebida normalmente, sem a verificação de falhas ou atraso na execução da mesma.

A partir dos testes realizado mostrou-se que é possível a comunicação entre redes distintas com o VoIP usando a mesma rede de dados. Os resultados nos dois cenários foram iguais, atendendo as necessidades de tráfegos e realizando uma comunicação com qualidade.

4.4 Considerações sobre uso de VoIP e do PBX Asterik

Essa seção apresenta algumas considerações sobre o uso do VoIP e do Asterisk, tecnologias estas que vem sendo adotadas por muitas organizações e instituições em função das amplas vantagens de uso, principalmente, no que se refere a redução substancial dos custos com telefonia.

Coforme já apresentado no referencial teórico existem várias motivações para se usar VoIP nas empresas tais como:

- integração de sistemas com tecnologia VoIP à rede pública de telefonia PSTN;
- apresenta todas as funcionalidades de um PABX;

Entre outras apresentadas na seção 2.5.1

No entanto, apesar das motivações que justificam o uso de VoIP, também existem pontos críticos que devem ser levados em consideração no momento de sua implantação, para que não ocorram problemas no ambiente VoIP. Algumas considerações se referem a:

- questões de segurança: podem acontecer ataques e violação do acesso por causa das vulnerabilidades dos sistemas envolvidos.
- características das redes: é necessário que se tenha uma rede de telecomunicações, móvel ou fixa, dando suporte a tecnologia VoIP;
- qualidade da rede: VoIP exige condições favoráveis de rede como boa largura de banda, por exemplo.

Em relação ao Asterisk, vale ressaltar que se trata de um *software* robusto, gratuito e de fácil configuração, que fornece todas as funcionalidades de uma central telefônica convencional (PABX), operando em várias plataformas (Linux, Unix, Windows), com ou sem *hardware* conectado à rede pública de telefonia.

Porém, devido às características que o Asterisk requer para sua implantação, tais como equipamentos adequados, profissional qualificado e condições favoráveis de rede, as organizações tem optado por contratar empresas especializadas em serviços VoIP em vez de configurar servidores próprios.

Além disso, há que se ressaltar que a implantação do sistema Asterisk e VoIP em uma organização deve ser planejada com a observância dos investimentos financeiros necessários a sua efetivação, tais como os preços dos equipamentos, gastos com a contratação de pessoal de suporte, (salário, Fundo de Garantia Por Tempo de Serviço – FGTS, férias, 13º salário), dentre outros. Pois, dependendo da infraestrutura da empresa, principalmente para as de pequeno e médio porte, tal implantação pode não ser vantajosa e se tornar mais onerosa. Assim sendo, a tecnologia VoIP poderá apresentar desvantagem, pois pode ser que a relação custo/benefício não comporte o investimento necessário a adoção da tecnologia VoIP.

Quanto as empresas de grande porte, os benefícios gerados com a adoção da tecnologia VoIP e Asterisk são grandes, principalmente no que se refere a redução dos custos com telefonia, bem como a integração de sistemas da tecnologia VoIP à rede pública de telefonia PSTN; apresentar todas as funcionalidades de um PABX; *Call Center* e *Voice Mail*;

sistemas de autoatendimento; integração com outras aplicações; sistemas de teleconferência; e de chamadas de longa distância

5 CONSIDERAÇÕES FINAIS

Este trabalho teve por objetivo geral possibilitar a comunicação VoIP entre ramais de duas redes distintas. Para isso, foram configurados dois servidores Proxy Asterisk, usando protocolo SIP, para realizar a comunicação VoIP. Durante este processo, os servidores Asterisk foram configurados com o GNU\Linux Debian, de forma a permitir a comunicação VoIP. Os testes foram feitos com chamadas de áudio entre os dois servidores Asterisk matriz e filial e para realizar as chamadas foi utilizado o zoiper.

Após a configuração do ambiente, foram criados dois cenários para a realização dos testes, sendo que no primeiro foi feita uma ligação de um ramal da matriz para o ramal da filial de forma direta e no segundo cenário foi feita uma ligação do ramal da matriz para um ramal configurado na URA, para testar o funcionamento do atendimento automático. Durante os testes, o servidor Proxy SIP realizou a comunicação da forma desejada, ou seja, os servidores possibilitaram a conexão entre os ramais de redes distintas e o atendimento automático funcionou normalmente.

Na realização do presente trabalho, a maior dificuldade foi encontrar material para auxiliar a configuração entre os dois servidores locais usando o Proxy SIP. Esse tema é muito abordado em artigos científicos, trabalhos acadêmicos e livros, mas estes não apresentam a configuração da comunicação entre os servidores. O problema foi resolvida após fazer o cadastro na comunidade do Asterisk no Brasil e compartilhar o problema com os membros dessa comunidade, a partir daí muitas pessoas postaram suas ideias e após vários testes foi possível realizar a comunicação entre os servidores usando o Proxy SIP.

Na finalização deste trabalho, fica como sugestão para trabalhos futuros a realização de estudos mais aprofundados sobre a tecnologia VoIP, tanto nos aspectos relacionados a segurança desta tecnologia, como principalmente no que diz respeito a QoS. Pois, mediante a observância dos aspectos pontuados por este estudo sobre os benefícios do VoIP, a implementação dos serviços de voz sobre IP tendo como matriz ULBRA/Canoas e filial ULBRA/Palmas poderia gerar ganhos ainda mais significativos para a instituição.

Outro aspecto que poderia ser bastante interessante poderia ser a implantação de um sistema semelhante de forma a ligar toda a rede ULBRA com o mundo, ou seja, expandindo para as ligações externas.

REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, Julio Cesar. **Utilização de Voip através do Asterisk.** Monografia (Especialização Latu Sensu) Universidade Federal de Lavras. Lavras: 2007. 111f.
Disponível em: <http://www.ginux.ufla.br/files/mono-JulioAbreu.pdf> Acesso em: 23/mar/2012.

ALBUQUERQUE, Fernando. **TCP/IP Internet**: Protocolos e tecnologias. Departamento de Ciência da Computação da Universidade de Brasília – UnB. 3ª ed. Brasília: Axcel Books, 2001.

ALBUQUERQUE, Ricardo. **Segurança no desenvolvimento de software**. Rio de Janeiro: Campus, 2002.

ALIGERA. **O que é Asterisk? Funcionamento do Asterisk**. Disponível em: <http://www.aligera.com.br/o-que-e-asterisk> Acesso em: 11/jun./2012.

ANATEL – Agência Nacional de Telecomunicações. **Serviços de Voz sobre IP**. Disponível em: <http://www.anatel.gov.br/Portal/exibirPortalPaginaEspecial.do?acao=&codItemCanal=1216 Acesso em: 12/mar/2012.

ARTHUR, Luiz. **Redes VoIP Asterisk *Dial Plan***. Publicado em 21/junho/2009. Disponível em: <http://www.slideshare.net/luiz_arthur/redes-voip-asterisk-dial-plan> Acesso em: 26/mai/2012

ASSIS, Alexandre Urtado de; ALVES JR, Nilton. **Implementação do protocolo IPv6 na Rede Rio**. NIC.BR. Núcleo de Informação e Coordenação do Ponto BR. Comitê Gestor da Internet no Brasil. Disponível em: <http://www.ipv6.br/IPV6/ArtigoImplementacaoRedeRioParte02> Acesso em: 17/maio/2012.

BALBINOT R. *et al.* Voz Sobre IP: Tecnologias e Tendências. In: **Simpósio Brasileiro de Redes de Computadores**. Anais. Natal: UFRN, 2003.

BESERRA, Danilo Huberto et al. **Asterisk – o futuro da telefonia**. Administração de Redes I. Faculdade Maurício de Nassau. Ensino Superior Bureau Jurídico. Recife (PE): 2008. Disponível em: <www.madeira.eng.br/liberty/download_file.php?attachment_id=145> Acesso em: 26/abril/2012.

BEZERRA, Romildo Martins. **Redes de Computadores II**. A camada de rede. Disponível em: <http://www.ifba.edu.br/professores/romildo/downloads/ifba/rede.pdf>
Acesso em: 18/jan/2012.

BIANCHINI, Renato Luiz. **Implantação de Sistema VoIP** na Universidade Federal de Lavras Utilizando Softwares Livres. Monografia (Graduação) Universidade Federal de Lavras Departamento de Ciência da Computação. Lavras, (MG): 2006. 80 p. Disponível em: <http://www.bcc.ufla.br/monografias/2005/Implantacao_de_sistema_VoIP_na_UniverUniver_Federal_de_Lavras_utilizando_softwares_livres.pdf> Acesso em: 4/abril/2012.

CANTÚ, Evandro. **Rede de Computadores e Internet**. Curso de Telecomunicações. CEFET – SC. Unidade de São José. Disponível em: <http://www.das.ufsc.br/~montez/Disciplinas/materialRedes/ApostilaCantu.pdf> Acesso em: 18/jan/2012.

CAVEDINI, Ricardo. **O padrão SS7 e o SS7 sobre IP nas redes de telecomunicações**. Monografia (Especialização). Universidade Federal do Rio Grande do Sul – UFRS. Porto Alegre, 2007. Disponível em: <http://www.lume.ufrgs.br/bitstream/handle/10183/14329/000664873.pdf?sequence=1> Acesso em 7/mar/2012.

CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de Segurança para Internet**. 2ª ed. São Paulo: Editora Comitê Gestor da Internet no Brasil, 2012. Disponível em: <http://cartilha.cert.br/seguranca/> Acesso em: 08/jun./2012.

COMER, Douglas E. **Interligação em Redes com TCP/IP**. Volume I. Princípios, protocolos e arquitetura. 3ª ed. Tradução de ARX Publicações. Rio de Janeiro: Campus, 1998.

CPqD. **Segurança em VoIP**. Disponível em: <www.cpqd.com.br> Acesso em: 4/abril/2012.

CRISTOFOLI, Fulvio et al. **Benefícios do Uso do VoIP**: Um estudo de caso na GM. Artigo. RBGN, São Paulo, Vol. 8, n.21, p. 55-69, mai. / ago.2006.

DIAS, Claudia. **Segurança e Auditoria da Tecnologia da Informação**. Rio de Janeiro: Axcel Books do Brasil, 2000.

DIGIUM. Disponível em: <http://www.digium.com> Acesso em: 4/abril/2012.

FORRISTAL, Jeff ; TRAXLER, Julie. **Site Seguro**: Aplicações *Web*. Alta Books, 2002.

GONÇALVES, Flavio E. **Como construir e configurar um PABX com *software* livre**. Abordando a versão 1.4. Quarta Geração. eBook Asterisk Guia de ConFiguração. 1ª ed./dezembro/2008 - rev. 9. Florianópolis (SC): 2006. Disponível em: <http://www.voipexperts.com.br/FreeChapters/Portugues/FreeChapters123pt.html#_Toc216419810> Acesso em: 4/abril/2012.

GOMES, Anderson Ferreira. **Qualidade de serviços em VoIP** (Voz sobre IP). 60 f. Monografia (Trabalho de Conclusão de Sistemas de Informação) – UNIMONTES. Universidade Estadual de Montes Claros. Montes Claro, 2005. Disponível em: <http://www.ccet.unimontes.br/arquivos/monografias/66.pdf> Acesso em: 29/março/2012.

KELLER, Alexandre. **Asterix na prática**. São Paulo: Novatec Editora, 2009.

KUROSE, James F. **Redes de Computadores e a Internet**. São Paulo: Addison Wesley, 2003.

LAUREANO, Marcos Aurelio Pchek. **Gestão de Segurança da Informação**. 2005

MADEIRA, Frederico Tiago Tavares. **Segurança em redes de voz sobre IP**. Monografia (Pós-Graduação Segurança em Redes de Computadores). Associação de Ensino Superior de Olinda (AESO). Olinda (PE), 2007. Disponível em: <http://www.madeira.eng.br/wiki/index.php?page=A+Tecnologia+VoIP> Acesso em: 4/abril/2012.

MATIAS, Camila Verônica Alves; FERNANDES, Pedro Augusto Domiciano. **Asterisk uma solução em PABX IP**. Monografia (Graduação em Engenharia de Computação). Universidade Católica de Goiás. Goiânia (GO), 2009. Disponível em: <aldeia3.computacao.net/greenstone/collect/trabalho/index/.../doc.pdf> Acesso em: 26/abril/2012.

MEGGELEN, J. V. Asterisk. **O Futuro da Telefonia**. 1ª ed. Rio de Janeiro: Alta Books, 2005.

MICROSOFT TECHNET. Biblioteca do TechNet. **Roteamento IP**. Disponível em: <http://technet.microsoft.com/pt-br/library/cc785246(v=ws.10).aspx> Acesso em: 15/mar/2012.

MICHALET, Charles-Abert. **O que é mundialização?** São Paulo: Edições Loyola, 2003.

MONTARGIL, André. **PABX Digital utilizando Asterisk rodando em Linux**. Dissertação (Especialização em Redes de Computadores e Comunicação de Dados). Universidade Estadual de Londrina – UEL. Londrina (PR), 2007.
Disponível em: <http://www2.dc.uel.br/nourau/document/?view=543> Acesso em: 26/abril/2012.

MOREIRAS, Antonio M. **Segurança e IPv6. Aspectos teóricos e práticos**. NIC.BR. Núcleo de Informação e Coordenação do Ponto BR. Comitê Gestor da Internet no Brasil. 2009. Disponível em: <http://www.ceptro.br/pub/CEPTRO/PalestrasPublicacoes/FISL10-Seguranca-v6.pdf> Acesso em: 17/maio/2012.

OLIVEIRA FILHO, Jorge Lima de. **Tecnologia DIFFSERV** como suporte para qualidade de serviços de aplicações multimídia - Aspectos de configuração e integração. 112 f. Dissertação de Mestrado – Universidade Salvador, Salvador, 2006.

ONG IDEPAC. **Apostila de *hardware***. Disponível em: <http://www.idepac.org.br/apostilas/apostilaHardware.pdf>. Acesso em: 10/mar/2012

PINHEIRO, José Maurício Santos. **O modelo OSI**. Artigo publicado em 22/11/2004. Disponível em: <http://www.projetoderedes.com.br/artigos/artigo_modelo_osi.php> Acesso em 7/mar/2012.

_____. **Por Falar em Roteadores**. Artigo publicado em 23/02/2005. Disponível em:<http://www.projetoderedes.com.br/artigos/artigo_por_falar_em_roteadores.php> Acesso em 4/mai/2012.

PONCE, Alexandre. **Redes de Computadores**. Apostila. Disponível em: <http://www.micropic.com.br/paginadecliente/noronha/Informatica/REDES/gerenciamento.pdf> Acesso em: 05/mar./2012.

RONCAGLIA, Adriano. **PSTN – Rede Pública de Telefonia Comutada**. Artigo publicado em 6/outubro/2009. Disponível em: <http://mestreasterisk.com.br/artigos-mestre-asterisk/pstn-rede-publica/> Acesso em: 11/jun./2012.

SMITH, J. Et. Al. 2005 – Asterisk the Future of Telephony

SOARES. L. F, G. Lemos, e S. Colcher. **Redes de Computadores** - Das LANs, MANs e WANs as Redes ATM. 3ª ed. Rio de Janeiro: Campus, 1995.

STALLINGS, Willian. Arquitetura e Organização de Computadores: Projeto para o Desempenho. São Paulo: Prentice Hall, 2002.

TANENBAUM. Andrew S. **Redes de Computadores**. Tradução de Vandenberg D. de Souza. 4ª ed. Rio de Janeiro: Elsevier/Campus, 2003.

TELECO, **Conceitos de VOIP/Telefonia IP e Regulamentação aplicável**, Disponível em: <http://www.teleco.com.br/tutoriais/tutorialvoip/pagina_1.asp>. Acesso em: 29/março/2012.

_____. Seção: Tutoriais Banda Larga. **IPv6: Endereço e Roteamento**. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialipv6/pagina_3.asp> Acesso em: 18/maio/2012.

_____. Inteligência em Telecomunicações. **Modelo OSI para VoIP Peering**. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialvoippeering/pagina_3.asp> Acesso em: 6/abril/2012.

_____. Seção: Tutoriais VoIP. **Segurança VoIP:** Soluções. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialvoipconv2/pagina_3.asp> Acesso em: 10/mai/2012.

TORRES, Gabriel. **Redes de Computadores** - Curso Completo. São Paulo: Axcel Books, 2001.