



UNIVERSIDADE DO SUL DE SANTA CATARINA
ALEX ADELINO VIEIRA

DESENVOLVIMENTO DE SOFTWARE DE ROTEAMENTO PARA PABX IP

Palhoça
2013

ALEX ADELINO VIEIRA

DESENVOLVIMENTO DE SOFTWARE DE ROTEAMENTO PARA PABX IP

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Sistemas de Informação da Universidade do Sul de Santa Catarina, como requisito parcial à obtenção do título de Bacharel em Sistemas de Informação.

Orientador: Prof. Paulo Ricardo Cechelero Villa, M.Eng.

Palhoça


2013

ALEX ADELINO VIEIRA

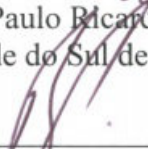
DESENVOLVIMENTO DE SOFTWARE DE ROTEAMENTO PARA PABX IP

Este Trabalho de Conclusão de Curso foi julgado adequado à obtenção do título de Bacharel em Sistemas de Informação e aprovado em sua forma final pelo Curso de Graduação em Sistemas de Informação da Universidade do Sul de Santa Catarina.

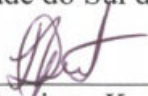
Palhoça, 20 de novembro de 2013.



Professor e orientador Paulo Ricardo Cechelero Villa, M.Eng.
Universidade do Sul de Santa Catarina



Prof. Robinson Pizzio, M.Eng.
Universidade do Sul de Santa Catarina



Prof. Luciano Kogut, M.Eng..
Universidade do Sul de Santa Catarina

AGRADECIMENTOS

Agradeço primeiramente a Deus, pois sem ele não alcançaria todos os meus objetivos como ser humano.

Agradeço muito a minha família pelo apoio durante todo meu período acadêmico.

Agradeço muito também a minha namorada pelo apoio e compreensão nos momentos em que não estive presente.

Agradeço a todo o corpo docente do curso de graduação Sistemas de Informação por compartilharem os seus conhecimentos.

Agradeço aos meus orientadores Robinson Pizzio e Paulo Ricardo Cechelero Villa pela intensa dedicação para que os objetivos do projeto fossem alcançados.

RESUMO

Devido vivência profissional do autor na implantação de Servidores Asterisk e a necessidade de configurar rotas no Dialplan de forma manual, surge a ideia de automatizar o processo de inserção de rotas através do compartilhamento de rotas entre Servidores Asterisk que estiverem interligados através de uma Rede Local utilizando a análise do enlace entre Servidores. Para a atualização de rotas e análise do enlace utilizou-se como referência teórica a proposta do protocolo de roteamento OSPF. Como etapas metodológicas: definiu-se nestas a revisão literária através de pesquisas bibliográficas sobre Telefonia IP, protocolo SIP, protocolos de roteamento e softPBX Asterisk; modelagem do sistema através da linguagem de notação UML; desenvolvimento do sistema, validação e testes. No desenvolvimento do sistema para que se proporcione os objetivos alcançados, utilizou-se a linguagem de programação *Shell Script Bash* devido esta possuir interação direta com comandos *shell* na execução do sistema proporcionando melhor desempenho deste. A validação e realização de testes do sistema foi realizada utilizando a instalação de três Servidores Asterisk em um ambiente virtualizado e endereçados em uma rede local.

Palavras-chave: SIP, VoIP, Telefonia, PABX, roteamento, Asterisk.

ABSTRACT

Because the author's professional experience in deploying Asterisk Servers and the need to configure routes in Dialplan manually, appears the idea of automating the process of inserting routes through the rout sharing between Asterisk servers that are interconnected through a LAN analyzing the link layer between servers. To update routes and linkage analysis was used as the theoretical framework proposed in the OSPF routing protocol. As methodological steps: we defined these literary review through literature research on IP Telephony, SIP protocol, and routing protocols softPBX Asterisk; system modeling through the language of UML notation; system development, validation and testing. In designing the system so that it provides the objectives achieved, we used the programming language Bash Shell Script because this has direct interaction with shell commands in the system execution providing better performance. Validation and testing of the system was performed using the installation of three Asterisk servers in a virtualized environment addressed on a local network.

Keywords: SIP, VoIP, Telephony, PBX, routing, Asterisk.

LISTA DE ILUSTRAÇÕES

| | |
|----------------------------------------------------------------------------------|----|
| Figura 1 - Amostras de um sinal analógico..... | 19 |
| Figura 2 - Diagrama em blocos da modulação PAM..... | 19 |
| Figura 3 - Função degrau usada no estágio de quantização | 20 |
| Figura 4 - Exemplo de um byte obtido do codificador | 21 |
| Figura 5 - Diagrama em blocos de um rádio digital | 22 |
| Figura 6 - Diagrama em blocos de um circuito digital via fio | 23 |
| Figura 7 - Formatos de endereços IP | 27 |
| Figura 8 - O uso de um Proxy e de servidores de redirecionamento com o SIP | 33 |
| Figura 9 - Fluxograma com as etapas metodológicas..... | 47 |
| Figura 10 - Desenho da solução | 48 |
| Figura 11 - Diagrama de Negócios Atual | 51 |
| Figura 12 - Diagrama de Negócios Novo | 52 |
| Figura 13 - Requisitos Funcionais | 53 |
| Figura 14 - Diagrama de Caso de Uso do Sistema | 56 |
| Figura 15 - Ícone da ferramenta VMware..... | 58 |
| Figura 16 - Ícone da distribuição Linux Ubuntu | 60 |
| Figura 17 - Ícone da ferramenta Asterisk..... | 61 |
| Figura 18 - Dialplan original | 64 |
| Figura 19 - Dialplan atualizado | 65 |
| Figura 20 - Cenário de testes..... | 66 |
| Figura 21 - Trace do protocolo SSH..... | 66 |
| Figura 22 - Trace do protocolo ICMP..... | 67 |
| Figura 23 - Trace do protocolo SIP na primeira chamada | 68 |
| Figura 24 - Trace do protocolo SIP na segunda chamada..... | 69 |

SUMÁRIO

| | | |
|-----------|------------------------------------------------------------------|-----------|
| 1 | INTRODUÇÃO | 11 |
| 1.1 | PROBLEMÁTICA | 12 |
| 1.2 | OBJETIVOS | 13 |
| 1.2.1 | Objetivo Geral..... | 13 |
| 1.2.2 | Objetivos Específicos | 14 |
| 1.3 | JUSTIFICATIVA | 14 |
| 1.4 | ESTRUTURA DA MONOGRAFIA | 15 |
| 2 | REVISÃO BIBLIOGRÁFICA..... | 16 |
| 2.1 | TELEFONIA ANALÓGICA..... | 16 |
| 2.2 | TELEFONIA DIGITAL | 17 |
| 2.2.1 | Conversão do sinal analógico em digital (A/D) | 17 |
| 2.2.1.1 | PCM – Pulse Code Modulation | 18 |
| 2.2.1.1.1 | Amostragem | 18 |
| 2.2.1.1.2 | Quantização | 19 |
| 2.2.1.1.3 | Codificação | 20 |
| 2.2.1.1.4 | Compressão | 20 |
| 2.2.2 | Conversão do sinal digital em analógico (D/A) do sinal PCM | 21 |
| 2.2.3 | Enlaces digitais..... | 21 |
| 2.2.3.1 | Canal rádio digital com fonte analógica..... | 22 |
| 2.2.3.2 | Comunicações digitais via fio | 22 |
| 2.2.4 | Protocolos de sinalização digital..... | 23 |
| 2.2.4.1 | Sinalização por canal associado (CAS)..... | 23 |
| 2.2.4.2 | Sinalização por canal comum (CCS) | 24 |
| 2.3 | CONVERGÊNCIA | 24 |
| 2.4 | ARQUITETURA TCP/IP | 25 |
| 2.4.1 | Camada de aplicação | 25 |
| 2.4.2 | Camada de transporte | 26 |
| 2.4.3 | Camada de sub-rede | 26 |
| 2.4.4 | Camada de inter-rede | 27 |
| 2.4.4.1 | Endereçamento IP | 27 |
| 2.5 | TELEFONIA IP E VOIP | 28 |
| 2.5.1 | VoIP e cenários de aplicação..... | 29 |
| 2.5.1.1 | VoIP de terminal IP para terminal IP..... | 29 |
| 2.5.1.1.1 | Gateway de gerência..... | 29 |
| 2.5.1.2 | VoIP de terminal IP para telefone convencional..... | 30 |
| 2.5.1.2.1 | Gateway de voz..... | 30 |
| 2.5.1.2.2 | Gateway de sinalização | 30 |
| 2.5.1.3 | VoIP de telefone convencional para telefone convencional..... | 31 |
| 2.6 | SIP (SESSION INITIATION PROTOCOL)..... | 31 |
| 2.6.1 | Definição do SIP | 32 |
| 2.6.2 | Funcionamento do SIP | 32 |
| 2.6.3 | Trapezóide SIP | 33 |
| 2.6.4 | Componentes de uma rede SIP | 34 |
| 2.6.5 | Processo de Registro do SIP | 34 |
| 2.6.6 | Mensagens Básicas | 35 |
| 2.7 | ASTERISK | 35 |
| 2.7.1 | Definição do Asterisk..... | 36 |

| | | |
|--------------|---------------------------------------------------------|-----------|
| 2.7.2 | Funcionamento do Asterisk | 36 |
| 2.7.2.1 | Sintaxe do Dialplan | 36 |
| 2.7.2.1.1 | Contextos | 36 |
| 2.7.2.1.2 | Extensões | 37 |
| 2.7.2.1.3 | Prioridades | 37 |
| 2.7.2.1.4 | Aplicações | 37 |
| 2.8 | FUNDAMENTOS DE ROTEAMENTO | 38 |
| 2.9 | RIP (<i>ROUTING INFORMATION PROTOCOL</i>) | 38 |
| 2.10 | OSPF (<i>OPEN SPF</i>) | 39 |
| 2.11 | SSH (<i>SECURE SHELL</i>) | 41 |
| 2.12 | SCP (<i>SECURE COPY PROTOCOL</i>) | 41 |
| 2.13 | ICMP (<i>INTERNET CONTROL MESSAGE PROTOCOL</i>) | 42 |
| 3 | MÉTODO | 44 |
| 3.1 | CARACTERIZAÇÃO DA PESQUISA | 44 |
| 3.1.1 | Classificação | 44 |
| 3.2 | ETAPAS METODOLÓGICAS | 46 |
| 3.3 | DESENHO DA SOLUÇÃO | 48 |
| 3.4 | DELIMITAÇÕES | 49 |
| 4 | MODELAGEM | 50 |
| 4.1 | ATORES | 50 |
| 4.2 | MODELAGEM DE NEGÓCIOS | 51 |
| 4.2.1 | Modelagem de negócios atual | 51 |
| 4.2.2 | Modelagem de negócios nova | 52 |
| 4.3 | REQUISITOS FUNCIONAIS | 52 |
| 4.4 | REQUISITOS NÃO FUNCIONAIS | 53 |
| 4.4.1 | Requisitos de produto | 54 |
| 4.4.2 | Requisitos organizacionais | 54 |
| 4.4.3 | Requisitos externos | 54 |
| 4.5 | REGRAS DE NEGÓCIOS | 55 |
| 4.6 | DIAGRAMA DE CASO DE USO | 55 |
| 4.6.1 | Descrição dos casos de uso | 56 |
| 4.6.1.1 | Caso de uso 1 – Inserção de extensões em Dialplan | 56 |
| 4.6.1.2 | Caso de uso 2 – Réplica de extensões | 57 |
| 4.6.1.3 | Caso de uso 3 – Definição da melhor rota | 57 |
| 5 | DESENVOLVIMENTO | 58 |
| 5.1 | FERRAMENTAS TECNOLÓGICAS | 58 |
| 5.1.1 | VMware | 58 |
| 5.1.2 | Ubuntu | 59 |
| 5.1.3 | Asterisk | 60 |
| 5.1.4 | Shell Scripting Bash | 61 |
| 5.1.5 | Wireshark | 62 |
| 5.2 | HISTÓRICO DE DESENVOLVIMENTO | 62 |
| 5.3 | PROBLEMAS E SOLUÇÕES | 63 |
| 5.4 | APRESENTAÇÃO DO SISTEMA | 64 |
| 5.5 | VALIDAÇÃO DO SISTEMA | 65 |
| 6 | CONCLUSÃO E TRABALHOS FUTUROS | 70 |
| 6.1 | OBJETIVOS ALCANÇADOS | 70 |
| 6.2 | RESULTADOS | 70 |
| 6.3 | TRABALHOS FUTUROS | 71 |
| | REFERÊNCIAS | 72 |
| | APÊNDICES | 74 |

| | |
|-----------------------------------------------------------|----|
| APÊNDICE A – CRONOGRAMA..... | 75 |
| APÊNDICE B – CÓDIGO DO ARQUIVO “ATUALIZAR_ROTAS.SH” | 76 |
| APÊNDICE C – CÓDIGO DO ARQUIVO “DEFINIR_ROTA.SH”..... | 80 |

1 INTRODUÇÃO

Segundo Chowdhury (2002, p.257) “não há dúvida de que voz sobre IP (VoIP, *voice over IP*) atualmente é um dos tópicos mais quentes no setor de telecomunicações. O equipamento para empacotar ligações de voz está disponível e, para os provedores de serviços, a economia do VoIP pode ser muito atraente.”

Conforme descrição de Chowdhury (2002, p.280)

Nos últimos anos, a telefonia pela Internet gerou muito entusiasmo no setor, a respeito da capacidade de usar uma rede IP para transportar o tráfego telefônico tradicional. A telefonia pela Internet foi desenvolvida originalmente para oferecer um meio de comunicação por voz de um sistema telefônico baseado em componente (por exemplo) para outro através da Internet. Nesse serviço, os usuários em uma extremidade podem falar com outros usuários em qualquer parte do mundo, desde que estejam conectados via Internet. Naturalmente, esse tipo de comunicação por voz não seria nítido para os usuários finais, mas foi bom o suficiente para a troca de informações.

Segundo Chowdhury (2002, p.280), uma das vantagens para o setor de telecomunicações ao utilizar telefonia através da Internet é a extinção de tarifas proporcionadas pelas Operadoras para comunicação de longa distância entre os usuários desta comunicação.

“Um roteador é capaz de selecionar um caminho ideal para o destino, a partir de vários caminhos existentes, usando um algoritmo de roteamento” (CHOWDHURY, 2002, p.88). Conforme descreve Colcher et. al (2005, p.152) “Em um cenário de integração com um grande número de gateways de voz, selecionar o gateway correto pode se tornar um problema complexo”.

“A implementação VoIP nos roteadores pode variar: alguns podem implementar somente uma parte dos dados e alguns podem implementar dados e PSTN (*Public Switched Telephone Network*)” (CHOWDHURY, 2002, p.88).

De acordo com Chowdhury (2002, p.88)

O roteamento em uma rede envolve uma coleção complexa de algoritmos, que trabalham de forma mais ou menos independente e ainda oferecem suporte um ao outro, trocando serviços ou informações. Um exemplo de tal configuração é a implementação de RIP e OSPF em uma intranet. A complexidade em um roteador é herdada de várias fontes. Primeiro, o roteamento exige coordenação entre todos os nós de uma sub-rede, em vez de simplesmente um par de módulos, como os protocolos de enlace e de rede.

Segundo COMER (1998, p.256)

De modo geral, o estabelecimento de rotas envolve inicialização e atualização. Ao começar, cada roteador deve estabelecer um conjunto inicial de rotas e atualizar as tabelas à medida que as rotas mudam (ou seja, quando uma interface de rede falha). A inicialização depende do sistema operacional. [...] Uma vez construída uma tabela de roteamento inicial, o roteador deve adaptar as mudanças de rotas. Em interligações de redes pequenas que mudam lentamente, os administradores podem estabelecer e modificar as rotas manualmente. Em ambientes de grande porte nas quais existem mudanças rápidas, todavia, é impossível uma atualização manual lenta. São necessários métodos automáticos.

1.1 PROBLEMÁTICA

A criação manual de rotas em Dialplans em PABX IP desenvolvidos através de SoftPBX Asterisk – software desenvolvido para convergência em Telefonia (MEGGELN, SMITH, MADSON, 2005, p. 9) - acaba sendo uma atividade exaustiva. Tendo em vista que em cenários onde há interconexão entre vários PABX IP Filiais e seu PABX IP Matriz resultando em uma topologia de telefonia IP robusta, a criação manual e a atualização de rotas pode ser uma atividade que exija total dedicação do técnico mantenedor das rotas.

O crescimento de uma estrutura de telefonia pode ser comparado ao crescimento de uma estrutura de Internet e seus roteadores, tendo como problemática numa topologia telefônica com seus PABX IP a não atualização automática de rotas entre estes elementos.

O grande dilema da telefonia convencional é a busca pela qualidade de voz na comunicação entre seus usuários. Este dilema ainda persiste na atual telefonia VoIP sendo ainda mais crítica nesta devido a dependência de recursos disponíveis através da Internet, rede hoje que acumula serviços variados como voz, dados e vídeo. Este dilema leva estudiosos a pensarem em estabelecer Qualidade de Serviço (QoS) para o tráfego de voz na Internet.

Segundo Chowdhury (2002, p.345)

A implementação atual do VoIP está lutando para oferecer uma qualidade de serviço comparável para PSTN. As tecnologias de VoIP tornaram a manutenção da VQ (*Voice Quality*) mais complexa, incluindo compressão não-linear e a necessidade da remessa de pacotes oportuna para redes não configuradas originalmente para essas condições. As condições de transmissão que impõem pouca ameaça para o tráfego

de voz com pacotes em tempo real podem introduzir diversos problemas para o tráfego de voz com pacotes em tempo real.

Pode-se citar dois problemas importantes que prejudicam a qualidade de voz em cenários com tecnologia VoIP que são eles:

- Perda de pacotes onde, segundo Chowdhury (2002, p.346), “é óbvio que pode haver alguma perda de pacotes; a rede de dados compensa isso com o uso da retransmissão TCP (*Transmission Control Protocol*). Como a rede VoIP utiliza UDP (*User Datagram Protocol*), não existe garantia de pacote. [...] perda de pacotes significa informações de voz perdidas”.
- Retardo: “O retardo é o fator principal para a transmissão de voz. A recomendação G. 114 da ITU-T sugere que um “retardo de transmissão unidirecional” de até 400ms é aceitável” (CHOWDHURY, 2002, p.346).

1.2 OBJETIVOS

Os objetivos estão dispostos entre:

- Objetivo geral
- Objetivos específicos

1.2.1 Objetivo Geral

Desenvolver software para roteamento entre PABX IP para automatizar a criação de rotas em PABX IP e definir a melhor rota para entroncamentos IP.

1.2.2 Objetivos Específicos

Os objetivos específicos englobam:

- Definir a mais adequada Linguagem de Programação para desenvolvimento de Software;
- Definir uma topologia do cenário utilizado para testes de software;
- Definir o protocolo a ser utilizado na análise dos enlaces de comunicação;
- Aprofundar os conhecimentos em Sistema Operacional Linux;
- Aprofundar os conhecimentos em Protocolo SIP (*Session Initiation Protocol*);
- Definir SoftPBX a ser utilizado em cenários de testes;
- Aprofundar conhecimentos em Protocolos de Roteamento.

1.3 JUSTIFICATIVA

Durante experiência conquistada pelo auto em Análise Técnica de Ocorrências voltadas aos problemas relacionados à Qualidade de Voz em ambientes que utilizam a solução VoIP para telefonia. Pretende-se com o Projeto definir o enlace de comunicação entre usuários da telefonia IP através da análise de estado do enlace.

Deparando-se com a exaustiva definição de rotas de forma manual em Dialplans no SoftPBX Asterisk, pretende-se com o Projeto otimizar e automatizar a inclusão de rotas para Dialplans em SoftPBX beneficiando o técnico mantenedor do SoftPBX.

Além das vantagens que a solução VoIP já proporciona como redução de custos em Telefonia, convergência com as Redes de Dados e a não limitação geográfica na comunicação entre os usuários, pretende-se com este Projeto acrescentar a automatização no roteamento entre os PABX IP.

1.4 ESTRUTURA DA MONOGRAFIA

O capítulo atual descreve a introdução de forma genérica o assunto abordado, o objetivo geral e os objetivos específicos abordando também a justificativa.

Na revisão bibliográfica, em capítulo subsequente, serão disseminados os conceitos relacionados aos assuntos abordados e relacionados às tecnologias e protocolos que serão utilizados durante o desenvolvimento do Projeto proposto.

No capítulo 3, descreve-se o método que será utilizado para alcançar objetivos propostos.

2 REVISÃO BIBLIOGRÁFICA

Este capítulo terá como objetivo disseminar os conceitos relacionados aos protocolos e tecnologias que serão utilizados no decorrer do desenvolvimento do software para roteamento em PABX IP. Conceituando o novo mundo de convergência entre Telefonia e a *Internet*.

2.1 TELEFONIA ANALÓGICA

Segundo Meggelen, Smith, Madson (2005, p. 95) “a finalidade da Rede Pública de Telefonia Chaveada (PSTN) é estabelecer e manter conexões de áudio entre dois terminais”.

De acordo com Meggelen, Smith, Madson (2005, p.95) os humanos podem perceber vibrações sonoras na faixa de 20 a 20000Hertz e podem gerar sons vocálicos entre as frequências de 250 e 3000Hertz, tendo a telefonia o objetivo de transmitir estes sons, definiu-se uma largura de banda entre 300 a 3500Hertz.

“Um telefone analógico é composto de cinco partes: a campainha, o bloco de discagem, o híbrido (ou rede) e a chave de gancho e o fone manual (ambos são considerados partes do híbrido). A campainha, o bloco de discagem e o híbrido podem operar completamente independentes uns dos outros” (MEGGELEN, SMITH, MADSON, 2005, p.95).

Segundo Medeiros (2007, p. 22) “os equipamentos terminais da ponta da linha são telefones dos assinantes e o equipamento de comutação, responsável pelos enlaces é uma central telefônica. Os telefones são ligados à central por fios e cabos telefônicos”.

“As modernas centrais telefônicas são do tipo CPA (Central de Programa Armazenado), um equipamento de comutação da eletrônica digital, dotado de microprocessadores - μ P (Unidade Central de Processamento), que comandam e controlam as operações da central” (MEDEIROS, 2007, p.22).

“A CPA disponibiliza inúmeros serviços, tais como: conferência telefônica, siga-me, chamada em espera, chamada programada, identificação da chamada (bina), conferência telefônica, etc.” (MEDEIROS, 2007, p.22).

“Uma central telefônica pode ser pública ou privada” (MEDEIROS, 2007, p.22).

Segundo Medeiros (2007, p.22) a central pública provê enlaces entre ramais assinantes para uma determinada região tendo comunicação entre estas centrais de outros bairros, cidades, países e sistemas. A central privada é particular a uma organização (PABX – *Private Automatic Branch Exchange*).

“Os sinais elétricos das comunicações entre os telefones convencionais e a central telefônica ainda são analógicos. Quando o sistema é digital, por exemplo, em ISDN (*Integrated Services Digital Network*) o aparelho telefônico é específico” (MEDEIROS, 2007, p.23).

2.2 TELEFONIA DIGITAL

Segundo Meggelen, Smith, Madson (2005, p. 104) a centenas de anos, as redes de telefonia eram compostas somente de circuito chaveado. E a cada ligação telefônica realiza-se uma conexão dedicada efetuada entre os terminais. Se tornando uma rede custosa e este custo proporcional a distância entre os locutores.

2.2.1 Conversão do sinal analógico em digital (A/D)

De acordo com Medeiros (2007, p.62) “hoje, vencidas as dificuldades técnicas, a tecnologia digital desponta e é usada em larga escala. Muitas das comunicações com sinais analógicos migraram ou estão migrando para as comunicações digitais”.

“Ao contrário dos sinais analógicos, que são obtidos “naturalmente” de transdutores, os sinais digitais ou bits da informação digital são “sinais artificiais”,

codificados, gerados em circuitos da eletrônica digital como de um computador” (MEDEIROS, 2007, p.62).

Segundo Medeiros (2007, p.62) a conversão dos sinais analógicos em sinais digitais ocorre no conversor A/D e a operação inversa ocorre em conversor D/A (digital/analógico).

2.2.1.1 PCM – *Pulse Code Modulation*

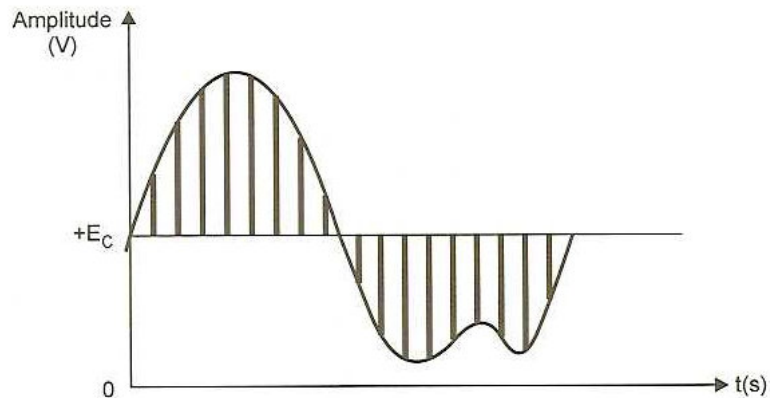
“Um dos processos de conversão do sinal analógico em digital é o PCM – modulação por código de pulso. A conversão compreende quatro estágios: amostragem, quantização, codificação e compressão” (MEDEIROS, 2007, p.70).

2.2.1.1.1 *Amostragem*

Segundo Medeiros (2007, p.70) amostrar (*sampler*) o sinal analógico consiste em entrecortar eletronicamente o sinal, a intervalos de tempo iguais, para obter estreitos pulsos nos valores de tensão do sinal, conforme a figura 1.

“Antes de ser amostrado, o sinal precisa passar por um filtro passa-faixa para limitação de banda e é colocado sobre um patamar de tensão contínua + E_c . O objetivo final é codificar, com 8bits, as amostras de diferentes amplitudes (valores positivos e negativos)” (MEDEIROS, 2007, p.70).

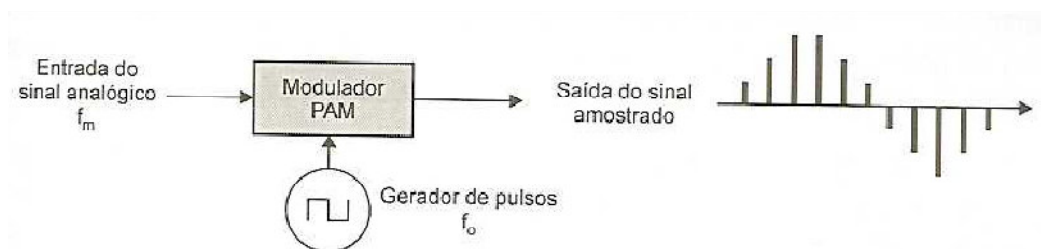
Figura 1 – Amostras de um sinal analógico



Fonte: Medeiros (2007, p.70)

A operação de amostragem do sinal pode ser realizada pelo circuito modulador PAM, mostrado na figura 2. Praticamente, o modulador PAM realiza a operação de “fatiar” o sinal analógico (MEDEIROS, 2007, p.71).

Figura 2 - Diagrama em blocos da modulação PAM



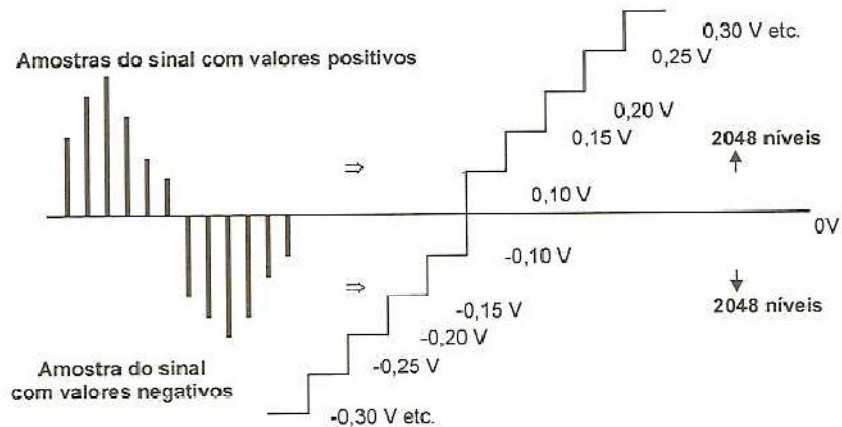
Fonte: Medeiros (2007, p. 71)

2.2.1.1.2 Quantização

De acordo com Medeiros (2007, p.72) quantizar consiste em “medir” eletronicamente as alturas dos pulsos recebidos do estágio amostrador, em “n” níveis fixados. A intenção é obter de cada altura medida 13bits, sendo 1 da paridade do sistema e 12 derivados da amostra.

Um quantizador, representado no gráfico da figura 3, função degrau, é o responsável pela medição das alturas das amostras do sinal analógico da informação (MEDEIROS, 2007, p.72).

Figura 3 - Função degrau usada no estágio de quantização



Fonte: Medeiros (2007, p.72)

2.2.1.1.3 Codificação

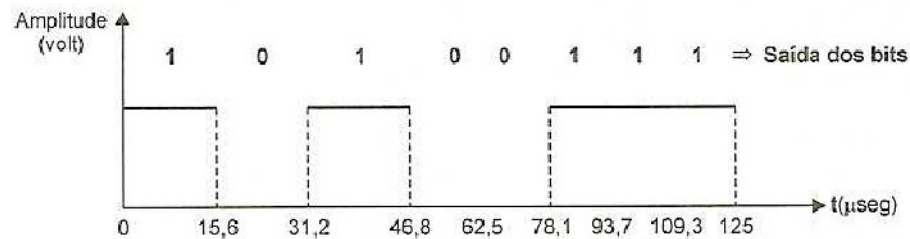
“O circuito codificador tem por função gerar 13bits por amostra quantizada num certo código preestabelecido. Repetindo o que já foi comentado, posteriormente os 13bits serão reduzidos para apenas 8 no estágio de compressão digital” (MEDEIROS, 2007, p.72).

2.2.1.1.4 Compressão

Segundo Medeiros (2007, p.72) a compressão digital consiste na redução dos 13bits codificados em apenas 8bits obedecendo a criteriosa aplicação de uma das leis de

compressão digital: lei A e lei μ de modo a não haver distorção no sinal analógico recuperado na recepção.

Figura 4 - Exemplo de um byte obtido do codificador



Fonte: Medeiros (2007, p.73)

2.2.2 Conversão do sinal digital em analógico (D/A) do sinal PCM

Conforme Medeiros (2007, p.74)

A recuperação do sinal digital deve trazer de volta os sinais da informação na forma analógica, com a menor distorção possível, de acordo com os padrões do sistema e de aceitação pelo usuário. A conversão D/A consiste em três etapas:

- 1.Regeneração: é o estágio em que os pulsos recebidos são limpos e refeitos pela eliminação do ruído superposto ao sinal e a distorção do formato do pulso.
- 2.Decodificação: é a operação inversa à codificação, na qual cada sequência de oito bits reproduz uma amostra na tensão correspondente ao sinal analógico original. Entretanto, antes da decodificação é feita uma operação de expansão dos bits, em oposição à de compressão, realizada por ocasião da conversão A/D.
- 3.Filtragem: pode ser feita por um simples circuito RC ou por um filtro passa-baixas (LPF) mais sofisticado. A partir da filtragem o sinal analógico está recuperado, pronto para ser amplificado e reproduzido pelo transdutor.

2.2.3 Enlaces digitais

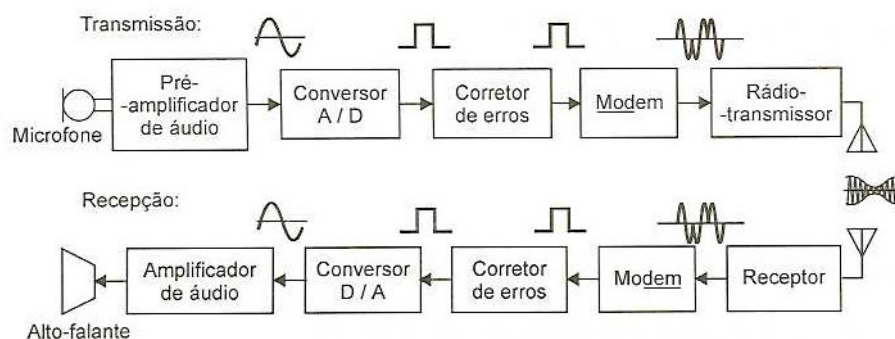
“Os enlaces digitais podem ser efetivados a partir de duas fontes singelas de informação de sinais analógicos e de dados (sinais digitais)” (MEDEIROS, 2007, p.263).

De acordo com Medeiros (2007, p.263) “nesta oportunidade serão apresentados, em diagramas, os enlaces rádio e fio com fontes de sinais analógicos, pela necessidade da conversão A/D na transmissão e D/A na recepção”.

2.2.3.1 Canal rádio digital com fonte analógica

Segundo Medeiros (2007, p.263) o diagrama em blocos da figura 5 mostra as partes integrantes de um sistema digital básico, via rádio, com fonte de informações de sinal analógico, como de voz.

Figura 5 - Diagrama em blocos de um rádio digital

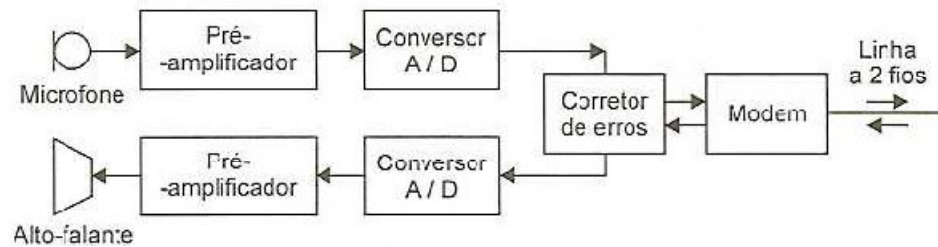


Fonte: Medeiros (2007, p.263)

2.2.3.2 Comunicações digitais via fio

A figura 6 mostra o diagrama em blocos de um sistema digital básico de comunicações via fio com sinal de entrada analógico (MEDEIROS, 2007, p.264).

Figura 6 - Diagrama em blocos de um circuito digital via fio



Fonte: Medeiros (2007, p.264)

2.2.4 Protocolos de sinalização digital

Segundo Meggelen, Smith, Madson (2005, p.105), não basta somente que os circuitos utilizados pela PSTN sejam portadores de dados (voz) entre terminais. Devem existir mecanismos como sinalizações para passar informações relacionadas ao estado do canal para cada terminal.

2.2.4.1 Sinalização por canal associado (CAS)

Conforme Colcher et al. (2005, p.96) “trata-se de um método em que a sinalização é transmitida no próprio canal da informação ou em um canal de sinalização permanentemente associado a ele”.

Segundo Colcher et al.(2005, p.96) na sinalização R2, um multiquadro com uma sequencia de 16 frames E1, no segmento 16 é utilizado para sinalização de dois canais. No primeiro frame, a sinalização é dos canais 1 e 17. E no segundo frame, a sinalização é nos canais 2 e 18.

De acordo com Meggelen (2005, p.105) “a sinalização CAS funciona roubando bits do fluxo de áudio para finalidades de sinalização. Apesar do efeito na qualidade de áudio não ser perceptível, a falta de um canal de sinalização potente limita a sua flexibilidade”.

2.2.4.2 Sinalização por canal comum (CCS)

“Na Sinalização por Canal Comum (*Commum Channel Signaling*), as informações de sinalização relativas a vários canais passam a poder ser transportadas em um único canal (comum) por meio de mensagens endereçadas e identificadas” (COLCHER et al., 2005, p.97).

Após abordagem histórica relacionada a telefonia, em próxima seção será abordado o surgimento de convergência entre a telefonia convencional e a Internet.

2.3 CONVERGÊNCIA

Segundo Tanenbaum (2005, p.516) o número de bits de dados transferidos igualou o número de bits de voz devido codificação PCM nos troncos. E o volume do tráfego de dados era dez vezes maior que o volume do tráfego de voz, fazendo com que operadores de rede de dados se interessassem em transportar nestas redes voz.

A tecnologia da informação avança cada vez mais em relação a comunicação através da grande rede internacional de computadores – a *Internet*, proporcionando uma comunicação geograficamente ilimitada entre seus usuários. Esta evolução se dá nos recursos utilizados para esta comunicação, sendo estes recursos os protocolos e tecnologias.

Ao passo que se dá na evolução tecnológica, o acesso a tecnologia da informação através da *Internet* chega a um número maior de usuários como ocorreu com as redes telefônicas.

Segundo Colcher et al.(2005, p. 8) serviços tradicionalmente vinculados a redes específicas passaram a ser também oferecidos sobre redes IP (*Internet Protocol*). Fluxos para distribuição de áudio e vídeo (*streaming*) de emissoras de rádio e TV pela *Internet* são lugar-comum hoje, por exemplo.

Em próxima seção conceitualiza-se o protocolo TCP/IP para posteriormente realizar-se abordagem à tecnologia VoIP.

2.4 ARQUITETURA TCP/IP

Segundo Tanenbaum (2005, p. 45) quando foram criadas as redes de radio e satélite, começaram a surgir problemas com os protocolos existentes, o que forçou a criação do Modelo de Referência TCP/IP que se proporciona conexão de várias redes de maneira uniforme.

Com este propósito segundo Colcher et al. (2005, p. 66) “foram propostos os conhecidos protocolos TCP (*Transmission Control Protocol*) e IP (*Internet Protocol*). Considerando que a ênfase, principalmente do IP, era no aproveitamento de outras redes existentes para a interligação dos roteadores”.

Segundo Colcher et al.(2005, p.67) para interligar duas redes distintas é necessário conectar uma máquina a ambas as redes. Uma máquina que conecta duas ou mais redes é denominada *gateway* ou roteador. Os roteadores precisam conhecer alguma informação sobre a topologia da inter-rede.

“A arquitetura Internet TCP/IP é organizada em quatro camadas: Aplicação, Transporte, Inter-rede e Sub-rede” (COLCHER et al., 2005, p.67).

2.4.1 Camada de aplicação

Conforme descreve Tanenbaum (2005, p.45) acima da camada de transporte, encontramos a camada de aplicação. Ela contém todos os protocolos de nível mais alto. Dentre eles estão o protocolo de terminal virtual TELNET (*Terminal over Networks*), FTP (*File Transfer Protocol*) e o SMTP (*Simple Mail Transfer Protocol*).

“No nível de aplicação, os usuários usam programas de aplicação para acessar os serviços disponíveis na inter-rede. As aplicações interagem com o nível de transporte para enviar e receber dados” (COLCHER et al., 2005, p.68).

2.4.2 Camada de transporte

Segundo Torres (2001, p.66) no modelo TCP/IP a camada de transporte utiliza um esquema de multiplexação, onde é possível transmitir “simultaneamente” dados das mais diferentes aplicações.

De acordo com Tanenbaum (2005, p. 46) a finalidade dessa camada é permitir que as entidades pares dos hosts de origem e de destino mantenham uma conversação. Dois protocolos fim a fim foram definidos aqui. O TCP (*Transmission Control Protocol*) orientado a conexões e confiável e o UDP (*User Datagram Protocol*) não confiável.

“A arquitetura Internet permite que sejam utilizados dois tipos principais de protocolo em sua camada de transporte. O primeiro deles é o TCP, que opera no modo orientado à conexão fornecendo um serviço de transferência de dados confiável” (COLCHER et al., 2005, p.78).

“A outra opção é o UDP, que opera no modo sem conexão e fornece um serviço datagrama não confiável, sendo uma simples extensão do IP” (COLCHER et al., 2005, p.78).

2.4.3 Camada de sub-rede

De acordo Tanenbaum (2005, p.49) “abaixo da camada inter-redes, encontra-se um grande vácuo. O modelo de referencia TCP/IP não especifica muito bem o que acontece ali, exceto o fato de que o host tem de se conectar a rede utilizando algum protocolo para que seja possível enviar pacotes IP”.

Descreve Colcher et al. (2005, p. 69) que a ideia é que qualquer tecnologia, padronizada por qualquer outra entidade, ou mesmo proprietária, pode ser utilizada para compor a camada de sub-rede, bastando para isso que seja desenvolvida uma interface que compatibilize aquela tecnologia específica com o protocolo IP.

2.4.4 Camada de inter-rede

De acordo com Colcher et al. (2005, p.68) o nível inter-rede é o responsável pelo encaminhamento de dados através da sub-rede, desde a máquina de origem até a máquina de destino . Esse nível recebe pedidos para transmitir pacotes do nível de transporte.

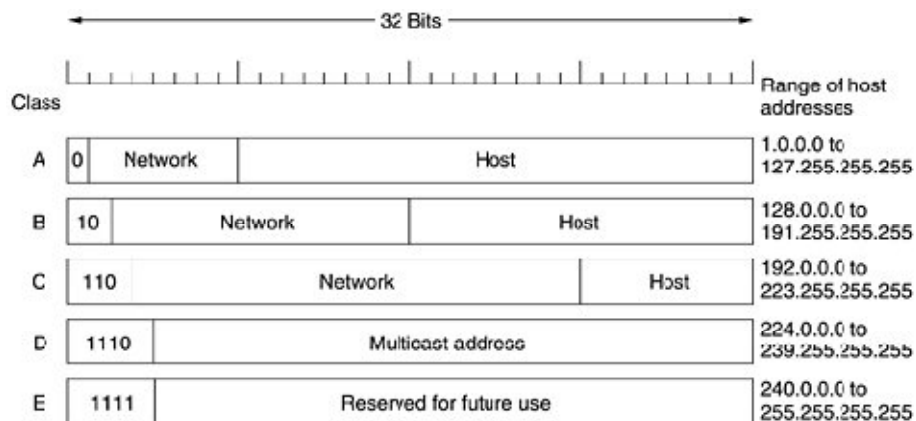
Tanenbaum (2005, p.46) descreve que a camada inter-redes define um formato de pacote oficial e um protocolo chamado IP (*Internet Protocol*). A tarefa da camada inter-redes é entregar pacotes IP onde eles são necessários. O roteamento de pacotes é de suma importância nessa camada, assim como a necessidade de evitar o congestionamento.

2.4.4.1 Endereçamento IP

Conforme Tanenbaum (2005, p. 337) “na Internet, cada host e cada roteador têm um endereço IP que codifica seu número de rede e seu numero de host. Todos os endereços IP tem 32bits e são usados nos campos *Source address* e *Destination address* dos pacotes IP”.

É importante observar que um endereço IP não se refere a um host e sim se refere a uma interface de rede; assim, se um host estiver em duas redes, ele precisará ter dois endereços IP (TANEBAUM, 2005, p. 337).

Figura 7 - Formatos de endereços IP



Fonte: Tanenbaum (2005, p. 334)

“É bastante comum, tanto na mídia quanto na indústria, o uso dos termos “VoIP” e telefonia IP (*Internet Protocol*) de modo diferenciado” (COLCHER et al., 2005, p. 9).

Conceitualização da Telefonia IP e descrição detalhada desta seguem em seção subsequente.

2.5 TELEFONIA IP E VOIP

Conforme descreve Mueller (2002, p.190) “Telefonia IP (*Internet Protocol*) é um termo vagamente definido. Basicamente, é um conjunto de tecnologias que suporta os serviços equivalentes (ou um fax razoável) de voz da rede de telefonia em redes de dados público e privados”.

Conceituando telefonia IP “o termo telefonia IP tem sido empregado para se referir á aplicação de tecnologias de VoIP na transmissão e na sinalização, com o oferecimento de um serviço de qualidade similar ao da telefonia convencional” (COLCHER et al., 2005 p. 9).

Segundo Colcher et al. (2005, p. 9) “telefonia IP é também frequentemente mencionada como a extensão do serviço de comunicação vocálica propiciada por tecnologias de VoIP até o equipamento do usuário final e sua consequente possibilidade de integração com outros serviços típicos da *Internet*.

De acordo com Meggelen, Smith, Madson (2005, p. 110) a premissa básica do VoIP é empacotamento de fluxos de áudio para transporte sobre redes baseadas em Protocolo da *Internet*.

“O VoIP mantém a promessa de incorporar comunicações de voz em todos os outros protocolos que nós temos em nossas redes, mas, devido ás demandas especiais da conversação de voz, conhecimentos especiais são necessários para projetar, montar e fazer manutenção dessas redes”(MEGGELLEN, SMITH, MADSON, 2005, p. 110).

Devido os cenários em que aplica-se VoIP serem projetados de formas distintas, na próxima seção serão abordados alguns dos cenários que utilizam VoIP (Voz sobre IP).

2.5.1 VoIP e cenários de aplicação

Apresenta-se nesta seção os principais cenários a serem implementados para o protocolo SIP (*Session Initiation Protocol*).

2.5.1.1 VoIP de terminal IP para terminal IP

Os interlocutores usam equipamentos dotados de *codecs* (Codificador/Decodificador) de áudio e interfaces ligadas a uma rede IP em suas conversações. Segue exemplos: o software *softphone*, equipamentos como telefones IP e os ATA (*Analog Telephone Adaptors*) (COLCHER et al., 2005, p.146).

2.5.1.1.1 Gateway de gerência

“Outro aspecto importante no estabelecimento de um serviço conversacional VoIP ao estilo do STFC (Serviço Telefônico Fixo Comutado) é o oferecimento de funções que precisam estar disponíveis mesmo quando terminais estão inoperantes” (COLCHER et al., 2005, p.147).

De acordo com Colcher et al. (2005, p.147)

Em VoIP, um componente opcional chamado gateway de gerência centraliza o oferecimento dessas funções. Dentre as funções oferecidas por um gateway de gerência, destacam-se:

- Controle de acesso: um gateway de gerência permite controlar o estabelecimento de novas chamadas com base em limitações no número de chamadas simultâneas ou nos privilégios dos participantes.
- Gerência de banda passante: administradores de rede podem controlar o uso de banda passante na rede pelo serviço de VoIP por intermédio do gateway de gerência, limitando o número de chamadas simultâneas, restringindo o estabelecimento de chamadas a certos horários ou usando mecanismos de provisão de QoS (*Quality over services*) específicos.

- Rerroteamento de chamadas: um gateway de gerência pode rerrotear uma chamada com base na disponibilidade de banda passante, por exemplo.

2.5.1.2 VoIP de terminal IP para telefone convencional

“A integração entre RTCCs (Redes Telefônicas Comutadas por Circuito) e serviços conversacionais de VoIP envolve o uso de dois componentes adicionais, chamados gateways de voz e gateways de sinalização” (COLCHER et al., 2005, p.148).

2.5.1.2.1 Gateway de voz

Descreve Colcher et al. (2005, p.149) que os gateways de voz são responsáveis pelo repasse de fluxos de áudio entre a RTCC e a rede IP. Suas principais funções são a codificação e decodificação digital da voz, a transcodificação entre formatos digitais, a terminação de chamadas telefônicas na RTCC e a transmissão e recepção de amostras de áudio digital encapsuladas em datagrama IP.

Segundo Colcher et al. (2005, p.149)

Do ponto de vista da RTCC, um gateway de voz pode se apresentar sob as mais diversas formas. Exemplos de gateways de voz incluem:

- Gateways residenciais: para interligação com interfaces analógicas tradicionais (RJ11) da RTPC (Rede Telefônica Pública Comutada).
- Gateways de acesso: para interligação com CPCTs (Centrais Privadas de Comutação Telefônica) analógicas ou digitais.
- Gateways de *trunking*: para interligação com um grande número de troncos analógicos ou digitais da RTPC.
- Gateways de voz sobre ATM (*Asynchronous Transfer Mode*): para interligação com redes de voz sobre redes ATM.

2.5.1.2.2 Gateway de sinalização

Descreve Colcher et al. (2005, p.150)

Os gateways de sinalização lidam fundamentalmente com o tratamento de pedidos de estabelecimento de chamadas partindo da RTCC e destinados a equipamentos na rede IP, e vice-versa. Entre as suas funções principais incluem-se:

- Conversação da sinalização: traduz mensagens ou tons especiais de sinalização usados na RTCC (DTMF (*Dual-tone Multifrequency*) e SS7 (Sistema de Sinalização Número 7), por exemplo) para a sinalização VoIP.
- Controle de gateways de mídia: efetua o controle da lógica de funcionamento dos gateways de mídia, requisitando a geração de sinais nas linhas telefônicas (tom de discagem, ocupado etc.) ou sendo notificado a respeito de eventos disparados nas mesmas (fonte fora de gancho, número discado etc.) por exemplo.

2.5.1.3 VoIP de telefone convencional para telefone convencional

“Este cenário se apresenta como um caso misto dos dois cenários anteriores, em que gateways de voz e de sinalização permitem que RTCCs distintas utilizem redes IP para se interligarem” (COLCHER et al., 2005, p.151).

Segundo Colcher et al.(2005, p.146) quando serviços de telefonia mais sofisticados são desejáveis, torna-se necessário que os terminais sejam dotados de protocolos de sinalização. Em geral, esses protocolos de sinalização estabelecem chamadas ou sessões entre os terminais, como por exemplo: o H.323 e o SIP (*Session Initiation Protocol*).

Sendo em próxima seção conceituado o protocolo de sinalização SIP.

2.6 SIP (*SESSION INITIATION PROTOCOL*)

Nesta seção serão abordados a definição do protocolo SIP, o seu funcionamento, o trapezóide do SIP, os componentes de uma rede SIP, o processo de registro no SIP e as mensagens básicas deste protocolo.

2.6.1 Definição do SIP

Segundo Chowdhury (2002, p.284) “SIP é um protocolo de sinalização leve que faz parte da arquitetura de controle de conferência da IETF (*Internet Engineering Task Force*). O protocolo de controle do nível de aplicação é usado para criar, modificar e terminar sessões com um ou mais participantes”.

De acordo com Tanenbaum (2005, p. 520) diferente do H.323, o SIP foi projetado para interoperar bem com aplicações da Internet existentes. Por exemplo, ele define números de telefones como URLs, de forma que as paginas da Web possam conter esses números, permitindo que um clique em um link inicie uma ligação telefônica.

De acordo com Chowdhury (2002, p.284) “o SIP não prescreve como uma configuração deve ser gerenciada; em vez disso, ele usa um servidor central para gerenciar o estado da conferência e do participante, distribuindo esse estado via *multicast*”.

“SIP permite mobilidade de usuário, através de Proxy e redirecionamento de requisições para o local atual do usuário. Os usuários desse protocolo são capazes de se comunicar uns com os outros através de *multicast* ou *unicast*, ou uma combinação de ambos” (CHOWDHURY, 2002, p.284).

2.6.2 Funcionamento do SIP

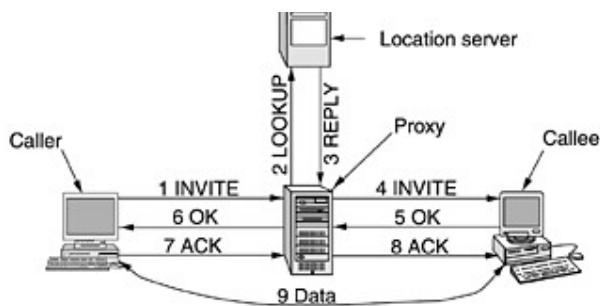
Segundo Tanenbaum (2005, p.559)

Para estabelecer uma sessão, o chamador cria uma conexão TCP com o chamado e envia uma mensagem INVITE sobre ela, ou então envia a mensagem INVITE em um pacote UDP. Se o chamado aceitar a ligação, ele responderá com um código de resposta do tipo HTTP (*Hyper Text Transfer Protocol*). A conexão é feita com o uso de um *handshake* de três vias, de forma que o chamador responde com uma mensagem ACK (*Acknowledged*) para finalizar o protocolo e confirmar o recebimento da mensagem 200. Para finalizar uma sessão gera-se a mensagem BYE. O método *OPTIONS* é usado para consultar uma máquina sobre seus próprios recursos e o método *REGISTER* localizar e conecta-se a um usuário que esta longe de casa.

Na figura 8, o usuário chamador gera uma mensagem de INVITE ao servidor Proxy para que seja ocultado o redirecionamento e o proxy procura o usuário a ser chamado e

envia um INVITE a este. Posteriormente a estes INVITES enviados, o servidor Proxy atuará como um relé para mensagens subsequentes em *handshake* de três vias (TANENBAUM, 2005, p.520).

Figura 8 - O uso de um Proxy e de servidores de redirecionamento com o SIP



Fonte: Tanenbaum (2005, p. 520)

2.6.3 Trapezóide SIP

De acordo com Gonçalves (2007, p.3) “Na arquitetura SIP, nós usamos agentes usuário e servidores. O SIP usa um modelo distribuído ponto-a-ponto usando um servidor de sinalização. O servidor gerencia apenas a sinalização, enquanto os agentes usuários e os agentes servidores manuseiam a sinalização e a mídia (áudio, vídeo, etc...)”.

No modelo SIP, o agente usuário de origem inicia a comunicação com o SIP Proxy, este na figura sendo o SIP Proxy de saída para que seja enviada uma mensagem de INVITE (convite).

O SIP Proxy de saída por sua vez checa se o INVITE será direcionado para um domínio externo iniciando uma consulta ao servidor DNS para determinar o domínio alvo e resolver o endereço IP. Então ele encaminha a chamada ao SIP Proxy responsável pelo domínio B.

O SIP Proxy de entrada efetua verificação em sua tabela de localização pelo endereço IP do agente usuário de destino e se este encontrar-se na tabela de localização de

usuários e o SIP Proxy puder localizar o endereço IP deste agente, será encaminhada a chamada ao agente usuário de destino.

Ao receber o INVITE gerado, o agente de destino terá todas as informações para estabelecer uma sessão RTP com o agente usuário de origem (GONÇALVES, 2007, p.3).

2.6.4 Componentes de uma rede SIP

Segundo Gonçalves (2007, p.4)

O SIP é um protocolo de sinalização de voz sobre IP que possui os seguintes componentes:

- UAC (*user agent client*) – cliente ou terminal que inicia a sinalização SIP.
- UAS (*user agent server*) – servidor que responde a sinalização SIP de um UAC.
- UA (*user agent*) – terminal de rede SIP (telefones SIP, ou gateway para outras redes), contém UAC e UAS.
- Servidor Proxy – recebe pedidos de conexão de um UA e transfere-o para outro servidor Proxy se a estação em particular não está em sua administração.
- Servidor de Redirecionamento – recebe pedidos de conexão e enviados de volta ao emissor incluindo os dados de destino ao invés de enviá-los diretamente à parte chamada.
- Servidor de localização – recebe pedidos de registro de um UA e atualiza a base de dados de terminais com eles.

2.6.5 Processo de Registro do SIP

No processo de registro há um servidor de localização que recebe pedidos através da mensagem REGISTER gerada pelos agentes usuários. Após o usuário iniciar uma sessão com outro usuário, o servidor de localização tem a tarefa de descobrir o *host* atual onde o usuário pode ser encontrado e determina para onde deve ser enviado o pedido baseando-se em uma tabela de localização por domínio (GONÇALVES, 2007, p5).

Para que um terminal como um telefone IP possa receber chamadas, este necessita registrar-se em uma base de localização e neste o nome é associado ao endereço IP onde o telefone encontra-se (GONÇALVES, 2007, p5).

2.6.6 Mensagens Básicas

As mensagens básicas enviadas em um ambiente SIP são:

Quadro 1 – Mensagens Básicas

| Método | Descrição | Referência |
|-----------|--------------------------------------------------------|------------|
| ACK | Confirmação do INVITE | RFC3261 |
| BYE | Término de uma sessão | RFC3261 |
| CANCEL | Término de uma sessão não estabelecida | RFC3261 |
| INFO | Transporta sinalização no meio de uma chamada | RFC2976 |
| INVITE | Estabelece uma sessão | RFC3261 |
| MESSAGE | Transporta uma mensagem instantânea | RFC3428 |
| NOTIFY | Entrega informações após o SUBSCRIBE | RFC3265 |
| OPTIONS | Pede quais recursos estão disponíveis ao UA ou Proxy | RFC3261 |
| PRACK | Confirma uma resposta provisória | RFC3262 |
| PUBLISH | Atualiza as informações de status no servidor | RFC3903 |
| REGISTER | Registra o usuário e mantém a tabela de localização | RFC3261 |
| REFER | Pede que outro UA atue sobre um URI | RFC3515 |
| SUBSCRIBE | Estabelece uma sessão pra receber futuras atualizações | RFC3265 |
| UPDATE | Atualiza as informações de status de um servidor | RFC3311 |

Fonte: Gonçalves (2007, p.7)

Em próxima seção será conceitualizada uma das ferramentas utilizadas para criação de SIP *Server*, o Asterisk.

2.7 ASTERISK

Nesta seção serão apresentados a definição do software Asterisk, o seu funcionamento e as características de Dialplan.

2.7.1 Definição do Asterisk

Conforme Meggelen, Smith, Madson (2005, p. 9) o Asterisk é uma plataforma de telefonia convergida, em código aberto, que é projetada para rodar em Linux, proporcionando aplicações tais como correio de voz, conferência, ordenamento de chamadas e agentes, música e chamadas em espera implementadas em software.

De acordo com Meggelen, Smith, Madson (2005, p.17) a partir do surgimento do Asterisk inicia-se uma nova evolução numa área da tecnologia que esteve parada no tempo não limitando a integração de sistemas antigos ao próprio Asterisk.

2.7.2 Funcionamento do Asterisk

Conforme Meggelen, Smith, Madson (2005, p.77) o Dialplan é o coração de qualquer sistema Asterisk, já que ele define como o Asterisk manipula os telefonemas que chegam e que são enviados. Em resumo, ele consiste de uma lista de instruções ou passos que o Asterisk irá seguir.

2.7.2.1 Sintaxe do Dialplan

“O Dialplan do Asterisk é especificado no arquivo de configuração chamado de *extensions.conf*. O Dialplan é composto de quatro partes principais: contextos, extensões, prioridades e aplicações” (MEGGELEN, SMITH, MADSON, 2005, p.77).

2.7.2.1.1 Contextos

“Os Diaplans são divididos em seções chamadas contextos. Os contextos são chamados grupos de extensões. Posto simplesmente, eles evitam que partes diferentes do dialplan interajam umas com as outras” (MEGGELEN, SMITH, MADSON, 2005, p.78).

Segundo Meggelen, Smith, Madson (2005, p.78) “Os contextos são denotados pela colocação do nome do contexto dentro de colchetes ([]). O nome pode ser formado com letras de A a Z (maiúsculas ou minúsculas), os algarismos de 0 a 9, o hífen e o sublinhado” .

2.7.2.1.2 Extensões

“Uma extensão é uma instrução que o Asterisk irá seguir, acionada por uma chamada de entrada ou por dígitos sendo discados num canal. As extensões especificam o que acontece às chamadas enquanto elas seguem seu caminho pelo dialplan” (MEGGELEN, SMITH, MADSON, 2005, p.78).

2.7.2.1.3 Prioridades

“Cada extensão pode ter vários passos, chamados de prioridades. Cada prioridade é numerada sequencialmente, começando por 1. Cada prioridade executa uma aplicação específica” (MEGGELEN, SMITH, MADSON, 2005, p.79).

2.7.2.1.4 Aplicações

De acordo com Meggelen, Smith, Madson (2005, p.79) “as aplicações são os cavalos de batalha do Dialplan. Cada aplicação executa uma ação específica no canal em questão, tal como emitir um som, aceitar uma entrada toque-tom ou desligar a chamada”.

Pode-se relacionar o Dialplan em Asterisk com uma forma de rotear uma requisição solicitada por uma origem qualquer. Em seção subsequente será descrito alguns conceitos relacionados a roteamento.

2.8 FUNDAMENTOS DE ROTEAMENTO

Segundo Torres (2001, p.356) os roteadores possuem uma tabela interna que lista as redes conhecidas por ele, chamada tabela de roteamento. Essa tabela possui ainda uma entrada informando o que fazer quando chegar um datagrama com um endereço desconhecido.

De acordo com Torres (2001, p.356) na conexão de redes autônomas, criar e manter tabelas de roteamento nos roteadores é uma tarefa simples sendo o maior trabalho configurá-las pela primeira vez denominando-se como tabela de roteamento estática.

O problema ocorre quando se conecta a rede Internet e as redes são removidas e adicionadas de tempos em tempos tendo a necessidade de se utilizar uma tabela de roteamento dinâmica onde os roteadores atualizam suas rotas através da comunicação entre estes (TORRES, 2001, p.356).

De acordo com Torres (2001, p. 356) a protocolo de roteamento pode operar de duas formas: informando o menor caminho para atingir uma rede ou então informando o melhor caminho. Protocolos que operam dessa forma são classificados como sendo baseados no estado do link.

Em próximas seções será descrito o protocolo RIP baseado na distância e o protocolo OSPF baseado no estado do link.

2.9 RIP (*ROUTING INFORMATION PROTOCOL*)

Segundo Comer (1998, p.298) “RIP (*Routing Information Protocol*), também conhecido pelo nome do programa que o implementa: *routed*. A implementação do *routed* foi

originalmente criada na Universidade da Califórnia, Berkeley, para fornecer informações consistentes sobre o roteamento e a acessibilidade de suas redes locais”.

O RIP divide os participantes em máquinas ativas e passivas. Os roteadores ativos anunciam suas rotas aos demais; as máquinas passivas entendem e atualizam suas rotas baseadas em anúncios, mas não anunciam (COMER, 1998, p.299).

No protocolo RIP, os roteadores encaminham suas tabelas de roteamento para outros roteadores que conseguirem acessar diretamente de 30 em 30 segundos. A tabela de roteamento inclui também a distância entre as redes e a distância é calculada através da quantidade de roteadores que o datagrama necessita trafegar (TORRES, 2001, p.357).

Uma desvantagem do RIP é que este define o caminho a ser percorrido para alcançar as redes baseando-se na distância não considerando o desempenho. Por exemplo, uma comunicação que percorra três roteadores passando por três redes Ethernet de 100Mbps (mega bits por segundo) sendo esta comunicação mais rápida do que a comunicação que percorra dois roteadores que trafeguem entre uma lenta conexão via satélite. Conclui-se que com a menor distância, não significa o melhor caminho. Outra desvantagem do RIP é que este não leva em consideração a possibilidade do caminho encontrar-se congestionado ou fora do ar (TORRES, 2001, p.359).

2.10 OSPF (*OPEN* SPF)

Segundo Comer (1998, p.309) “um grupo de trabalho da IETF criou um protocolo de gateway interno que usa o algoritmo do SPF. Denominado *Open* SPF (OSPF), o novo protocolo aborda várias metas ambiciosas”.

O OSPF tem sua especificação publicada em literatura sendo um padrão aberto para que desenvolvedores possam implementá-lo sem que haja a necessidade de pagar taxas de licenciamento.

Este protocolo possui um roteamento por tipo de serviço em que o administrador poderá definir várias rotas para um único destino, uma rota para cada tipo de serviço. No roteamento de um datagrama, um roteador na execução do OSPF utiliza os campos de endereço de destino e tipo de serviço do cabeçalho IP para determinar a rota a ser utilizada.

Outro recurso disponível no OSPF é o balanceamento de carga em que o administrador determina várias rotas para um determinado destino ao mesmo custo e o OSPF terá a função de distribuir o tráfego para todas as rotas igualmente (COMER, 1998, p.309).

Para permitir o crescimento e fazer com que as redes de um site sejam fáceis de gerenciar, o OSPF permite que um site particione suas redes e roteadores em subconjuntos chamados áreas. O conhecimento de topologia permanece oculto e exclusivo a cada área, com isso os grupos dentro de cada site cooperam com o uso do OSPF (COMER, 1998, p.309).

O OSPF promove recurso de segurança através da autenticação necessária na comunicação entre os roteadores com o objetivo de assegurar que somente roteadores confiáveis poderão divulgar as informações pertinentes ao roteamento (COMER, 1998, p.309).

Segundo Tanenbaum (2005, p.350) o OSPF é compatível com três tipos de conexões e redes: 1. Linhas ponto a ponto entre dois roteadores; 2. Redes de multiacesso com difusão; 3. Redes de multiacesso sem difusão.

“O OSPF funciona transformando o conjunto de redes, roteadores e linhas reais em um grafo orientado, no qual se atribui um custo (distância, retardo etc.) a cada arco. Em seguida, o OSPF calcula o caminho mais curto com base nos pesos dos arcos” (TANENBAUM, 2005, p.350).

De acordo com Tanenbaum (2005, p.350) o OSPF distingue quatro classes de roteadores: 1. Os roteadores internos, que ficam inteiramente em uma área; 2. Os roteadores de borda de área, que conectam duas ou mais áreas; 3. Os roteadores de *backbone*; e 4. Os roteadores de fronteira do SA (Sistema Autônomo).

Segue quadro que descreve as mensagens do OSPF:

Quadro 2 – Mensagens do OSPF

| Tipo de mensagem | Descrição |
|-------------------------|--------------------------------------------------|
| Hello | Usada para descobrir quem são os vizinhos |
| Link state update | Fornece os custos do transmissor a seus vizinhos |
| Link state ack | Confirma a atualização do estado do enlace |
| Database description | Anuncia quais são as atualizações do transmissor |
| Link state request | Solicita informações do parceiro |

Fonte: Tanenbaum (2005, p.353)

Em próxima seção será abordado o protocolo de autenticação SSH (*Secure Shell*) utilizado nos cenários em que se deseja executar aplicações em outras entidades da rede de forma segura.

2.11 SSH (*SECURE SHELL*)

De acordo com Dwivedi (2004, p.3) Secure Shell (SSH) é um programa utilizado para proteger a comunicação entre duas entidades. SSH usa arquitetura cliente/servidor, disponível em todas as versões do Windows, diferentes versões de Unix, e vários sistemas operacionais Macintosh. Pode-se conectar a servidores SSH os sistemas operacionais como Sun Solaris ou Microsoft Windows ou dispositivos como um roteador Cisco.

Em seu sentido mais simples, o SSH é usado para executar comandos remotos com segurança em outra entidade. Frequentemente é utilizado como um substituto para a Berkeley Telnet e "R" protocolos como o *Shell remoto* (RSH) e *Login remoto* (rlogin). Além de execução de comandos remotos, SSH é usado como uma garantia a cópia remota, substituindo protocolos tradicionais, como o *File Transfer Protocol* (FTP) e *Remote Copy Protocol* (RCP). Apesar do nome *Secure Shell*, SSH não é um *shell* em tudo. Ao contrário de outros *shells* tradicionais encontrados em diversas versões de Unix, como o Bash, KORN, e C, o SSH fornece criptografia entre as entidades e não uma interface de *Shell* entre estas.

Na próxima seção descreve-se o protocolo SCP (*Secure Copy Protocol*) utilizado para a troca de arquivos entre entidades.

2.12 SCP (*SECURE COPY PROTOCOL*)

De acordo com Parziale et. al (2006, p.533) *Secure Copy Protocol* (SCP) e *Secure Shell File Transfer Protocol* (SFTP) são dois métodos para implementação de transferência segura de arquivos a partir de um hospedeiro para outro. Nenhum protocolo foi projetado para realizar a autenticação, sendo necessário confiar no protocolo SSH subjacente em que foram

construídos. Isto não só simplifica a implementação do protocolo, mas evita as armadilhas do tradicional FTP (*File Transfer Protocol*), criptografando todos os dados que passa entre os dois *hosts*.

Segundo Parziale et. al (2006, p.533) as funções SCP são parecidas com o comando de cópia (cp) em sistemas baseados em UNIX, e assume o seguinte formato:

scp flags sourceFile destinationFile

Tanto o ID de utilizador é necessário para ter acesso ao computador remoto quanto o local do *host* remoto são especificados como parte do nome do arquivo. Por exemplo, suponha que um utilizador quer copiar um arquivo do *host* remoto ao *host* local. O arquivo está no diretório /tmp e é nomeado *yourdata*. Além disso, este usuário tem um ID de usuário no *host* de *myId* e quer copiar o arquivo para o diretório /localfolder como “meusdados”. A fim de alcançar o objetivo usando SCP, o usuário emite o seguinte comando: “scp myId@hostremoto:/tmp/yourdata/localfolder/meusdados”.

Da mesma forma, este usuário pode fazer *upload* de uma cópia do “meusdados” para o *remotehost*, usando o seguinte comando: “scp /localfolder/meusdados myId@remote.hos:/tmp/yourdata”.

Em próxima seção descreve-se o protocolo ICMP (*Internet Control Message Protocol*) e suas principais mensagens.

2.13 ICMP (INTERNET CONTROL MESSAGE PROTOCOL)

Conforme Tanenbaum (2005, p.346) “a operação da Internet é monitorada rigorosamente pelos roteadores. Quando ocorre algo inesperado, o evento é reportado pelo ICMP (*Internet Control Message Protocol*), que também é usado para testar a Internet. Existe aproximadamente uma dezena de tipos de mensagens ICMP definidos”.

As mensagens mais importantes estão descritos abaixo de acordo com Tanenbaum (2005, p.346):

- A mensagem DESTINATION UNREACHABLE é usada quando a sub-rede ou um roteador não consegue localizar o destino, ou quando um pacote

com o bit DF não pode ser entregue, porque há uma rede de "pacotes pequenos" no caminho.

- A mensagem TIME EXCEEDED é enviada quando um pacote é descartado porque seu contador chegou a zero. Esse evento é um sintoma de que os pacotes estão entrando em loop, de que há um enorme congestionamento ou de que estão sendo definidos valores muito baixos para o timer.
- A mensagem PARAMETER PROBLEM indica que um valor inválido foi detectado em um campo de cabeçalho. Esse problema indica a existência de um *bug* no software IP do *host* transmissor ou, possivelmente, no software de um roteador pelo qual o pacote transitou.
- Antes, a mensagem SOURCE QUENCH era usada para ajustar os *hosts* que estivessem enviando pacotes demais. Quando recebia essa mensagem, um *host* devia desacelerar sua operação.
- A mensagem REDIRECT é usada quando um roteador percebe que o pacote pode ter sido roteado incorretamente. Ela é usada pelo roteador para informar ao *host* transmissor o provável erro.
- As mensagens ECHO e ECHO REPLY são usadas para verificar se um determinado destino está ativo e acessível. Ao receber a mensagem ECHO, o destino deve enviar de volta uma mensagem ECHO REPLY.
- As mensagens TIMESTAMP REQUEST e TIMESTAMP REPLY são semelhantes, exceto pelo fato de o tempo de chegada da mensagem e o tempo de saída da resposta serem registrados na mensagem de resposta. Esse recurso é usado para medir o desempenho da rede.

3 MÉTODO

Aborda-se neste capítulo o método que será utilizado para alcançar os objetivos propostos.

3.1 CARACTERIZAÇÃO DA PESQUISA

Segundo Silva e Menezes (2001, p.20) “pesquisa é um conjunto de ações, propostas para encontrar a solução para um problema, que têm por base procedimentos racionais e sistemáticos. A pesquisa é realizada quando se tem um problema e não se tem informações para solucioná-lo”.

A pesquisa é desenvolvida mediante o concurso dos conhecimentos disponíveis e a utilização cuidadosa de métodos, técnicas e outros procedimentos científicos. A pesquisa desenvolve-se ao longo de um processo que envolve inúmeras fases, desde a formulação do problema até a apresentação dos resultados (GIL, 2002, p.17).

Conforme Demo (2004, p.33) “na condição de princípio científico, pesquisa apresenta-se como a instrumentação teórico-metodológica para construir conhecimento”.

“Como princípio educativo, pesquisa perfaz um dos esteios essenciais da educação emancipatórias, que é o questionamento sistemático crítico e criativo” (DEMO, 2004, p.33).

3.1.1 Classificação

A pesquisa pode ser classificada conforme as definições citadas abaixo.

Conforme Silva e Menezes (2001, p.20) a pesquisa pode ser classificada conforme sua natureza sendo dividida entre básica e aplicada. A pesquisa básica tem o objetivo de gerar

novos conhecimentos úteis sem aplicação prática e a pesquisa aplicada tem o objetivo de gerar conhecimentos para aplicação prática.

O projeto utiliza pesquisa classificada como aplicada decorrente objetivar-se o desenvolvimento de software aplicado ao roteamento entre PABX-IP.

Do ponto de vista da forma de abordagem a pesquisa pode ser classificada como quantitativa que considera que tudo pode ser quantificável, traduzindo em números informações e opiniões. E pode ser também classificada como qualitativa (SILVA E MENEZES, 2001, p.20).

Segundo Tozoni-Reis (2009, p.10) “a pesquisa qualitativa defende a idéia de que, na produção de conhecimentos sobre fenômenos humanos e sociais, interessa muito mais compreender e interpretar seus conteúdos que descrevê-los”.

Conforme Marques et al. (2006, p.36) “abordagem qualitativa: é aquela cujos dados não são passíveis de serem matematizados”.

A pesquisa abordada neste projeto será classificada em relação a forma de abordagem como qualitativa devido objetivar-se o desenvolvimento de software para aperfeiçoar o roteamento entre PABX-IP.

Com base em seus objetivos gerais, pode-se classificar as pesquisas em três grandes grupos: exploratórias, descritivas e explicativas. Pesquisas exploratórias têm como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a constituir hipóteses (GIL, 2002, p.42).

“As pesquisas descritivas tem como objetivo primordial a descrição das características de determinada população ou fenômeno ou, então, o estabelecimento de relações entre variáveis” (GIL, 2002, p.42).

As pesquisas explicativas têm como preocupação central identificar os fatores que determinam ou que contribuem para a ocorrência dos fenômenos (GIL, 2002, p.42).

O projeto efetuará uma pesquisa explicativa devido explorar conceitos tecnológicos de protocolos existentes para roteamento no desenvolvimento do software para PABX-IP.

Com relação aos procedimentos técnicos, a pesquisa poderá ser classificada como bibliográfica quando elaborada a partir de material já publicado, como documental quando elaborada a partir de material que não sofreu tratamento analítico, como experimental quando se determina um objeto de estudo, selecionam-se as variáveis que seriam capazes de influenciá-lo, definem-se as formas de controle e de observação dos efeitos que a variável produz no objeto. A pesquisa ainda pode ser classificada como levantamento quando a

pesquisa envolve a interrogação direta á pessoas. Como estudo de caso quando envolve o estudo profundo de um ou poucos objetos. Classificada como *expost-facto* quando o experimento é realizado após ocorrência dos fatos, como *pesquisa-ação* quando concebida e realizada em estreita associação com uma ação. E classifica como participante quando se desenvolve a partir da interação com os pesquisadores (SILVA E MENEZES apud GIL, 2001, p.22).

Este projeto utilizará a pesquisa experimental decorrente do desenvolvimento de software para roteamento entre PABX-IP tendo em vista obter-se informações conclusivas relacionadas à implementação deste software em cenário a ser definido.

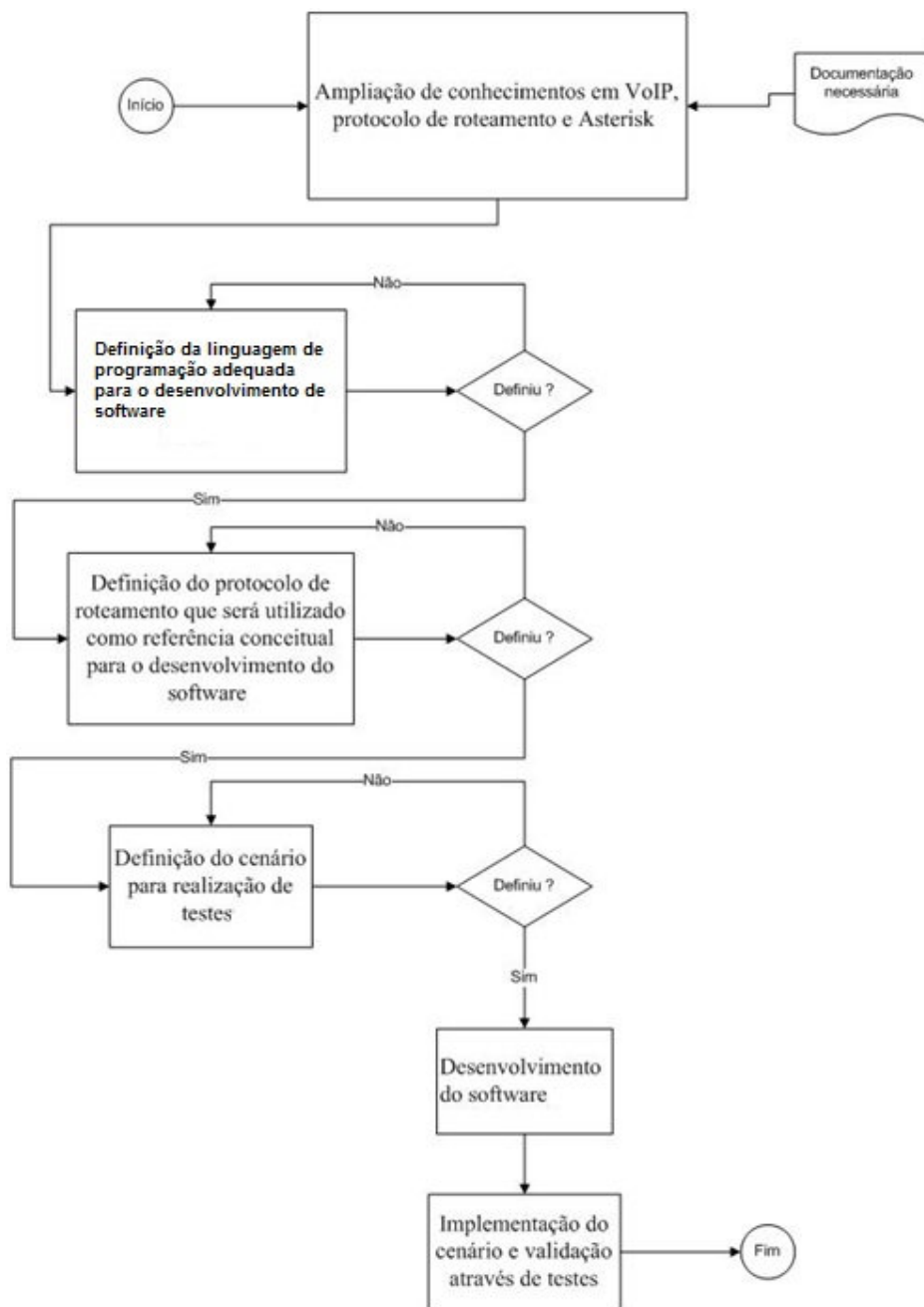
3.2 ETAPAS METODOLÓGICAS

As etapas metodológicas deste projeto segue descritas abaixo :

- Ampliação de conhecimentos em VoIP, protocolo de roteamento e Asterisk;
- Definição da linguagem de programação adequada para o desenvolvimento de software;
- Definição do protocolo de roteamento que será utilizado como referência conceitual para o desenvolvimento do software;
- Definição do cenário para realização de testes;
- Desenvolvimento do software;
- Implementação do cenário e validação através de testes.

Segue abaixo fluxograma através da Figura 9 que apresenta as etapas metodológicas.

Figura 9 - Fluxograma com as etapas metodológicas

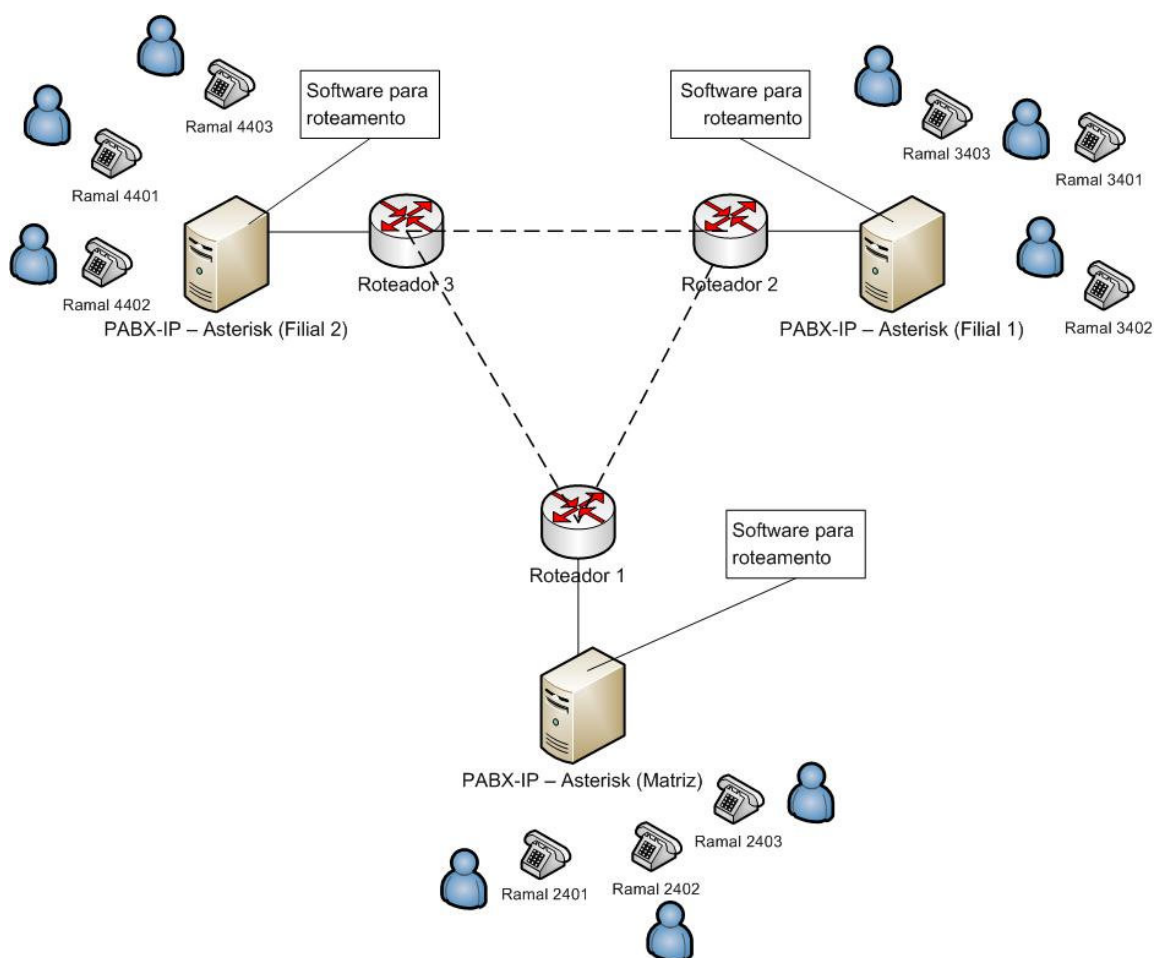


Fonte: Elaborada pelo autor

3.3 DESENHO DA SOLUÇÃO

O projeto tem a proposta de desenvolver um software que aperfeiçoe o roteamento entre PABX-IP das organizações numa topologia de matriz e filiais de acordo com o desenho topológico da solução expressado na Figura 10.

Figura 10 - Desenho da solução



Fonte: Elaborada pelo autor

3.4 DELIMITAÇÕES

A finalidade deste projeto é otimizar o roteamento entre os PABXs-IP para a comunicação entre os usuários destes, proporcionando para a comunicação o enlace disponível, porém o projeto apresentará algumas delimitações citadas abaixo :

- O software de roteamento estará utilizando recursos da camada de aplicação e da camada de rede do Modelo OSI;
- O cenário a ser implementado não estará efetuando conexão através da Rede Internet;
- Os usuários somente utilizarão *Softphones* para a comunicação;
- Limitação de três usuários;
- Limitação de três PABX-IP;

4 MODELAGEM

Neste capítulo será descrito a modelagem do software a ser desenvolvido e apresentados os diagramas gerados pela modelagem.

4.1 ATORES

Segundo Silva e Videira (2001, p.155) “um *actor* é o conceito que representa, em geral, um papel que um utilizador desempenha relativamente ao sistema em análise”.

Os atores do sistema a ser desenvolvido são o Analista de Telecomunicações e o Usuário de Telefonia.

O Analista de Telecomunicações têm a responsabilidade de efetuar as configurações do PABX-IP e realizar a manutenção das funcionalidades do PABX-IP. Deve possuir um conhecimento avançado em informática, possuir nível de escolaridade superior completo ou incompleto no curso de Sistemas de Informação, Ciências da Computação, Engenharia de Telecomunicações ou Engenharia Elétrica e deve possuir acesso a todas as funcionalidades do sistema. A sua frequência de uso do sistema é diária.

O Usuário de Telefonia têm a responsabilidade de realizar chamadas saintes e efetuar o atendimento de chamadas entrantes através das funcionalidades do PABX-IP. Deve possuir um conhecimento médio em informática, possuir nível de escolaridade médio completo e deve possuir acesso médio as funcionalidades do sistema. A sua frequência de uso do sistema é diária.

4.2 MODELAGEM DE NEGÓCIOS

4.2.1 Modelagem de negócios atual

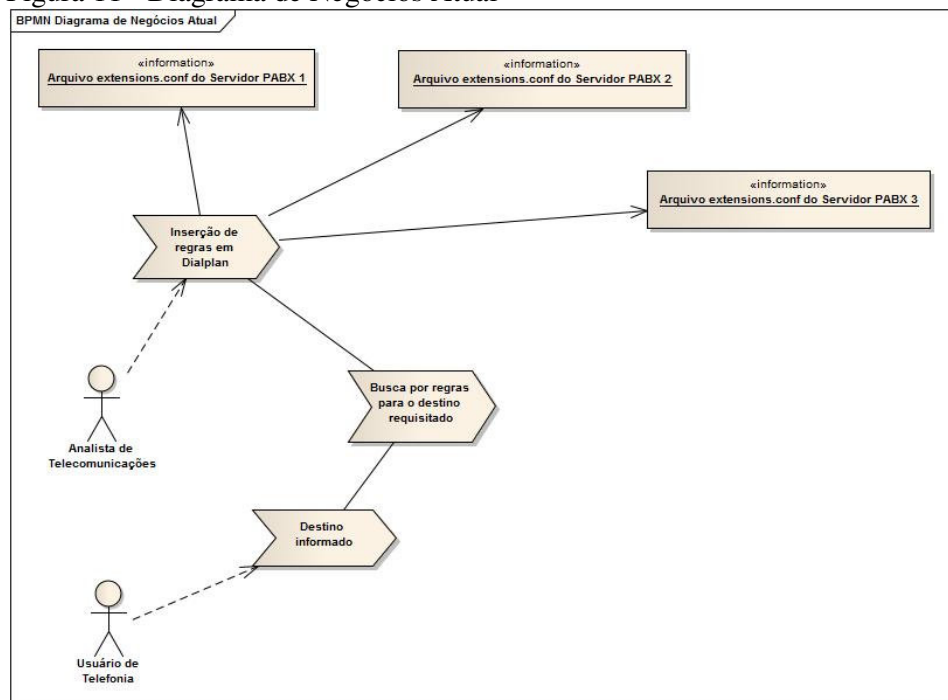
Atualmente o Analista de Telecomunicações ao configurar o PABX-IP, o mesmo efetua a inclusão manualmente das extensões em arquivo de dialplan (/etc/asterisk/extensions.conf) que servirão como rotas a serem seguidas em requisições geradas pelo Usuário de Telefonia para chamadas saintes.

As extensões criadas também servirão para tratamento de chamadas entrantes e encaminhamento destas chamadas ao Usuário de Telefonia para realização de atendimento.

No cenário atual, o Analista de Telecomunicações efetua a criação manual de novas extensões em Dialplan em novos PABX-IP's que serão instalados em novas filiais.

O sistema não efetua a checagem de rotas disponíveis a serem utilizadas para a realização de chamadas saintes com o objetivo de buscar a melhor rota a ser utilizada. Na figura 11 descreve o Diagrama de negócios atual.

Figura 11 - Diagrama de Negócios Atual



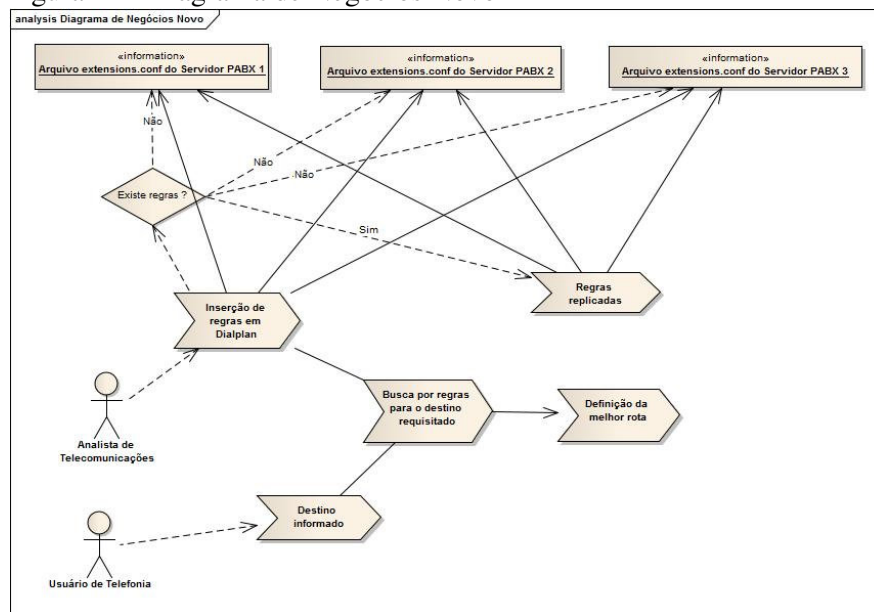
Fonte: Elaborada pelo autor

4.2.2 Modelagem de negócios nova

Na nova modelagem de negócios o Analista de Telecomunicações efetuará somente uma única vez a inclusão de extensões em arquivo de Dialplan tendo o sistema a funcionalidade de compartilhamento de extensões entre os PABX-IP efetuando-se a verificação de extensões já existentes ou não.

Também nesta modelagem, há uma nova funcionalidade em que o sistema efetua a avaliação do enlace entre estes PABX-IP com o objetivo de se utilizar o enlace disponível para a comunicação. Na figura 12 descreve o Diagrama de negócios atual.

Figura 12 - Diagrama de Negócios Novo



Fonte: Elaborada pelo autor

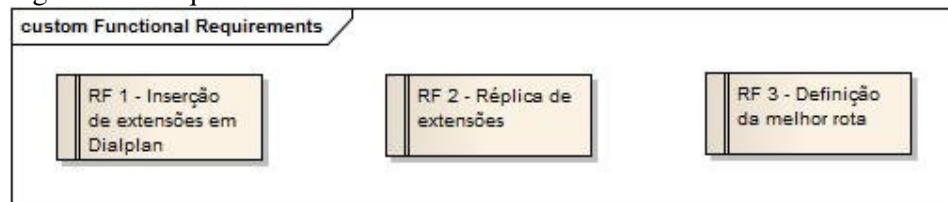
4.3 REQUISITOS FUNCIONAIS

De acordo com Sommerville (2003, p.89) “os requisitos funcionais de um sistema descrevem o que o sistema deve fazer. Esses requisitos dependem do tipo de software que está

sendo desenvolvido, dos usuários a que o software se destina e da abordagem geral considerada pela organização ao redigir os requisitos”.

A seguir é apresentado os Requisitos Funcionais através da Figura 13.

Figura 13 - Requisitos Funcionais



Fonte: Elaborada pelo autor

A seguir é apresentada a descrição para cada Requisito Funcional:

- RF 1 – Inserção de extensões em Dialplan: o Analista de telecomunicações efetua a inserção de regras no arquivo de Dialplan para cada PABX-IP.
- RF 2 – Réplica de extensões: o sistema efetua a validação em cada arquivo de Dialplan checando se estes possuem as extensões já criadas em cada PABX-IP que encontra-se na topologia de telefonia.
- RF 3 – Definição da melhor rota: o sistema efetua a avaliação através de *ping* nos enlaces disponíveis para estabelecimento da chamada telefônica requisitada e define o enlace a ser utilizado.

4.4 REQUISITOS NÃO FUNCIONAIS

Segundo Silva e Videira (2001, p.143) “Requisitos não funcionais têm a ver com aspectos gerais do sistema tais como: desempenho, robustez, fiabilidade, distribuição, segurança, integração com a Internet, abertura, ou suporte de *standards*”.

Conforme descreve Sommerville (2003, p.83) os requisitos não funcionais podem ser classificados em: requisitos de produto, requisitos organizacionais e requisitos externos.

4.4.1 Requisitos de produto

Estes requisitos especificam o comportamento do produto. Entre os exemplos estão requisitos de desempenho quanto à rapidez com que o sistema deve operar e quanto de memória ele requer e requisitos de confiabilidade, de portabilidade e de usabilidade (SOMMERVILLE, 2003).

Descrição dos requisitos de produto:

- RNF 1 – confiabilidade: será permitido somente a replicação de extensões não existentes nos arquivos de Dialplan.
- RNF 2 – desempenho: a definição da rota com resposta a 5 pacotes enviados.

4.4.2 Requisitos organizacionais

Descrição dos requisitos organizacionais:

- RNF 3 – Será utilizada a linguagem de programação *Shell Scripting Bash*.
- RNF 4 – O sistema operacional a ser utilizado será Linux.

4.4.3 Requisitos externos

RNF 5 – segurança: o Usuário de telefonia deverá estar autenticado em sua conta VoIP para requisição de chamadas.

4.5 REGRAS DE NEGÓCIOS

Apresentação das regras de negócios do sistema através do Quadro 3:

Quadro 3 – Regras de negócio do Sistema

| Regras de negócio do Sistema | |
|-------------------------------------|------------------------------------------------------------------------------------------------|
| RN 1 | O sistema não permitirá a replicação de extensões já existentes em arquivo de Dialplan. |
| RN 2 | O Usuário de telefonia deverá estar autenticado em sua conta VoIP para requisitar uma chamada. |
| RN 3 | O sistema deverá retornar um enlace válido para estabelecimento da chamada. |

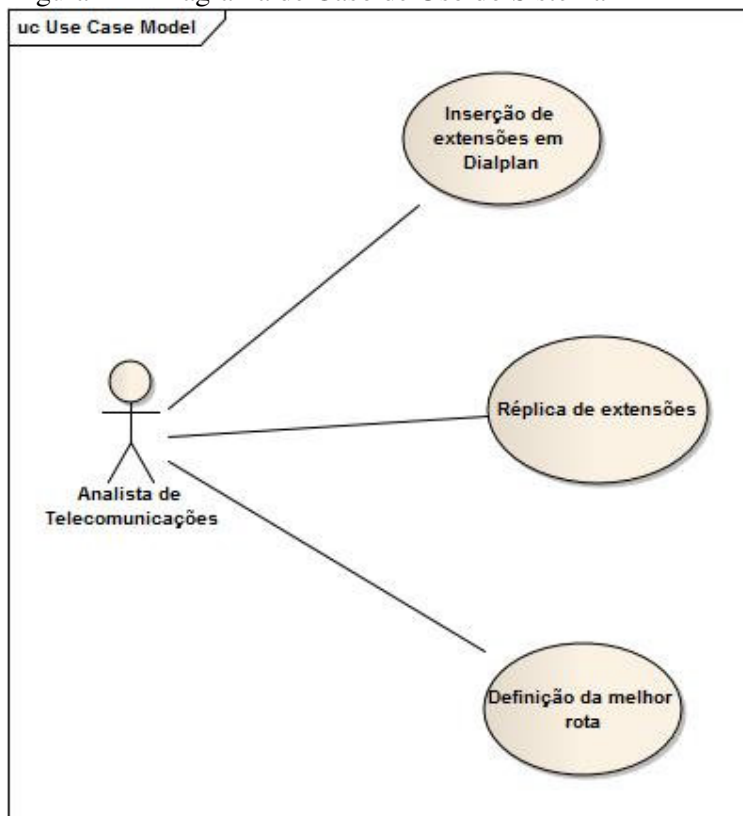
Fonte: Elaborada pelo autor

4.6 DIAGRAMA DE CASO DE USO

Conforme Silva e Videira (2001, p.124) um diagrama de casos de utilização descreve a relação entre atores e casos de utilização de um dado sistema. Este é um diagrama que permite dar uma visão global e de alto nível do sistema, sendo fundamental a definição correta da sua fronteira.

A seguir é apresentado o Diagrama de Caso de Uso do Sistema através da Figura 14.

Figura 14 - Diagrama de Caso de Uso do Sistema



Fonte: Elaborada pelo autor

4.6.1 Descrição dos casos de uso

4.6.1.1 Caso de uso 1 – Inserção de extensões em Dialplan

Quadro 4 – Caso de uso 1 – Inserção de extensões em Dialplan

| |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Caso de uso 1 – Inserção de extensões em Dialplan |
| Descrição: Este caso de uso descreve a inserção de extensões em arquivo de Dialplan |
| Ator: Analista de telecomunicações |
| Fluxo de eventos: <ol style="list-style-type: none"> 1. Analista de telecomunicações edita as extensões. 2. Sistema efetua a inserção em arquivo de Dialplan. |

Fonte: Elaborado pelo autor

4.6.1.2 Caso de uso 2 – Réplica de extensões

Quadro 5 – Caso de uso 2 – Réplica de extensões

| |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Caso de uso 2 – Réplica de extensões |
| Descrição: Este caso de uso descreve a realização de replicação de extensões em arquivo de Dialplan |
| Ator: Gestor do sistema |
| Fluxo de eventos: <ol style="list-style-type: none"> 1. Sistema efetua a validação de extensões em arquivo de Dialplan. 2. Sistema efetua a cópia de extensões em arquivo de Dialplan. 3. Sistema efetua a replicação de extensões copiadas para arquivos de Dialplan de outros PABX-IP's. |

Fonte: Elaborado pelo autor

4.6.1.3 Caso de uso 3 – Definição da melhor rota

Quadro 6 – Caso de uso 3 – Definição da melhor rota

| |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Caso de uso 3 – Definição da melhor rota |
| Descrição: Este caso de uso descreve a avaliação dos enlaces disponível para realização de chamadas |
| Ator: Gestor do sistema |
| Fluxo de eventos: <ol style="list-style-type: none"> 1. Sistema válido a existência de enlaces para realização de chamada. 2. Sistema efetua a análise dos enlaces. 3. Sistema definiu o melhor enlace. |

Fonte: Elaborado pelo autor

5 DESENVOLVIMENTO

Descrevem-se neste capítulo as ferramentas tecnológicas utilizadas no desenvolvimento do projeto, o histórico de desenvolvimento, um detalhamento dos problemas encontrados na implantação bem como as soluções tomadas, o sistema desenvolvido e os métodos utilizados para a validação do sistema.

5.1 FERRAMENTAS TECNOLÓGICAS

Nesta seção serão destacadas as ferramentas tecnológicas utilizadas para o desenvolvimento do projeto e uma descrição destas.

5.1.1 VMware

Antecipadamente a realização da codificação do sistema, se fez necessário a implementação do cenário de solução em ambiente virtualizado utilizando-se a ferramenta VMware. Na figura 15 é apresentado o ícone da ferramenta. A solução disponibilizada em versão a caráter de homologação durante 30 dias. O ambiente de virtualização foi implementado em conjunto com a distribuição Linux Ubuntu.

Figura 15 - Ícone da ferramenta VMware



Fonte: VMWARE Workstation (2013)

Segundo Veras (2011, p.87) a virtualização pode ser conceituada de duas principais formas: em primeira instância conceitua-se virtualização como o particionamento

de um servidor físico em vários servidores lógicos. Em segunda conceitualização, a virtualização é uma camada de abstração entre o hardware e o software que protege o acesso direto do software aos recursos físicos do hardware.

O intuito de se utilizar ambiente virtualizado é se beneficiar de apenas um hardware para a utilização de um ou mais sistemas operacionais.

5.1.2 Ubuntu

De acordo com Thomas, Channelle, Sicam (2009, p.31) Linux aplica uma filosofia alternativa para a computação que gira em torno da partilha não só de software, mas também de conhecimento. Ao utilizar-se o Linux tornar-se parte de uma grande comunidade global de pessoas que se agarraram a um fenômeno que está mudando o mundo.

O Ubuntu é um projeto fundado pelo empresário Mark Shuttleworth, com a intenção de trazer um sistema livremente disponível, operacional de alta qualidade para o mundo (THOMAS, CHANNELLE, SICAM, p.31, 2009).

A decisão pela utilização do sistema operacional Linux e distribuição Ubuntu se fez necessária devido o software PBX (*Private Branch Exchange*) Asterisk, que é implementado no projeto como um SIP Server e na grande maioria dos SIP Servers em cenário produtivos são instalados em distribuições Linux. Deu-se preferência pela distribuição Ubuntu devido ser uma distribuição de fácil instalação e devido esta disponibilizar por padrão ferramentas utilizadas para desenvolvimento bem como boa documentação e suporte pela comunidade. Segue abaixo o ícone da distribuição Ubuntu apresentado através da figura 16.

Figura 16 - Ícone da distribuição Linux Ubuntu



Fonte: UBUNTU to run on tablets, smartphones and TVs, canonical founder says (2013)

5.1.3 Asterisk

Conforme Meggelen, Smith, Madsen (2005, p. 9) o Asterisk é uma plataforma de telefonia convergida, open source, que é projetada para rodar em Linux, proporcionando aplicações tais como correio de voz, conferência, ordenamento de chamadas e agentes, música e chamadas em espera implementadas em software.

A utilização do SIP Server Asterisk se deu pela familiaridade com a ferramenta em experiência profissional do autor, a disponibilidade de arquivos textuais para configuração de rotas e contas SIP viabilizando a edição destes arquivos através de Shell Scripting. Segue abaixo apresentação do ícone relacionado ao Asterisk através da figura 17.

Figura 17 - Ícone da ferramenta Asterisk



Fonte: IPBX com Asterisk (2013)

5.1.4 Shell Scripting Bash

A linguagem de programação utilizada para o desenvolvimento do sistema é a linguagem Shell Scripting Bash disponibilizada por padrão através do sistema operacional Linux.

Conforme Burtch (2004, p.2) o *shell* é um programa que executa comandos no sistema operacional, sendo a linguagem *Shell Scripting Bash* um conjunto de instruções *shell* com a adição de recursos para tomadas de decisões e laços.

“O primeiro *shell* Unix foi o desenvolvido por Steven R. Bourne em 1974 para a sétima Edição do Unix. Chamado de shell Bourne (ou *sh*) em homenagem ao seu criador, que estabeleceu o padrão para *shells* de Unix , incluindo o cifrão default (\$)” (BURTCH, 2004, p.2).

De acordo com Burtch (2004, p.4) a Shell Scripting Bash é padrão na maioria das distribuições Linux. No entanto, existem outros shells do Linux disponíveis e não há exigência de que o Bash deva estar presente em qualquer distribuição particular. O Bash é um software de código aberto lançado sob a licença pública GNU (*General Public License*) (GPL).

A linguagem Shell Scripting Bash é adequada para o desenvolvimento do sistema proposto, pois é necessária a execução de aplicações para edição de arquivos, transporte de arquivos e gerenciamento de rede, disponibilizadas pelo sistema operacional.

5.1.5 Wireshark

De acordo com Morimoto (2008, p.501) Wireshark, antigo Ethereal, mudou de nome em Junho de 2006. Ele é um *sniffer*, que permite capturar o tráfego da rede, fornecendo uma ferramenta para analisar, detectar problemas e entender melhor o funcionamento de cada protocolo.

Conforme Morimoto (2008, p.502) o Wireshark pode ser usado tanto para proteger seu sistema quanto para roubar dados dos vizinhos. Devido a isso, ele é às vezes visto como uma "ferramenta hacker", quando na verdade o objetivo do programa é dar a você o controle sobre o que entra e sai da sua máquina e a possibilidade de detectar rapidamente qualquer tipo de *trojan*, *spyware* ou acesso não autorizado.

5.2 HISTÓRICO DE DESENVOLVIMENTO

Em primeira instância identificou-se no processo de implementação de rotas em arquivo do Dialplan (localizado no S.O. Ubuntu em “/etc/asterisk/extensions.conf”) em Servidores Asterisk durante experiência profissional do autor, a necessidade de se automatizar a atualização de rotas em uma rede local entre Servidores Asterisk e de se definir a melhor rota para a comunicação entre estes.

Posteriormente a apresentação dos objetivos e justificativas no capítulo 1, efetuou-se no capítulo 2 um levantamento teórico de protocolos de roteamento dinâmicos que possivelmente poderiam ser utilizados como base no desenvolvimento do sistema proposto. Definiu-se utilizar os conceitos do protocolo de roteamento dinâmico OSPF devido este basear-se no estado de enlace para definir o melhor caminho a ser utilizado.

O cenário da solução foi determinado, juntamente com as etapas metodológicas e as delimitações da proposta sendo apresentados no capítulo 3. Apresenta-se no capítulo 4 a modelagem do sistema que consiste da Modelagem de Negócios atual e nova, do Diagrama de Caso de Uso e dos Requisitos Funcionais e não Funcionais.

O processo de desenvolvimento iniciou-se através da criação de dois arquivos Bash com extensões *sh* chamados *atualizar_rotas.sh* e *definir_rota.sh*. Tendo o script

atualizar_rotas.sh, os objetivos de efetuar a leitura dos Endereços IP utilizados para autenticação nos troncos SIP cadastrados no arquivo “/etc/asterisk/sip.conf”, trocar entre os SIP Servers arquivo de dialplan “/etc/asterisk/extensions.conf” e incrementar extensões relacionadas as rotas distintas encontradas na comparação entre arquivos.

O script definir_rota.sh possui o objetivo de executar aplicação do sistema operacional para gerenciar o estado da comunicação entre os Endereços IP de cada Servidor Asterisk e posteriormente definir o melhor enlace a ser utilizado para estabelecimento de chamadas VoIP.

5.3 PROBLEMAS E SOLUÇÕES

Encontrou-se durante o início da codificação do sistema através da linguagem de programação Java EE, a complexidade de se requisitar a execução de aplicações em *shell* através do sistema operacional Linux.

Avaliando-se as linguagens de programação disponibilizadas pelo sistema operacional Linux, decidiu-se em utilizar para a codificação do sistema a linguagem Shell Scripting Bash que em código proporciona a utilização de comandos *shell* para execução de aplicações do sistema operacional.

No entanto, se fez necessário a realização de estudo para se assimilar a utilização das sintaxes disponibilizadas para a codificação através de Shell Scripting Bash.

Outro problema encontrado foi a necessidade de se utilizar dois servidores físicos conectados dentro de uma rede local endereçada para a realização de testes durante a codificação do sistema. E para a solução deste, realizou-se a implementação de máquinas virtuais através do ambiente virtualizado disponibilizado pela ferramenta VMware.

5.4 APRESENTAÇÃO DO SISTEMA

O sistema desenvolvido possui interação somente entre os agentes criados nos Servidores Asterisk apresentado no apêndice B, que demonstra o código do arquivo “atualizar_rotas.sh”. Esse script realiza a atualização de rotas mediante a comparação entre os arquivos de Dialplan compartilhados através da utilização do protocolo SCP (*Secure Copy Protocol*) de forma segura através do protocolo SSH (*Secure Shell*) entre os Servidores Asterisk.

A figura 18 mostra o arquivo de Dialplan “/etc/asterisk/extensions.conf” originado de forma manual antecipadamente a execução do script “atualizar_rotas.sh”. O arquivo possui rotas para comunicação interna entre ramais SIP.

Figura 18 - Dialplan original

```
[general]
static=yes
writeprotect=no
clearglobalvars=no

[globals]
CONSOLE=Console/dsp
IAXINFO=guest
TRUNK=DAHDI/G2
TRUNKMSD=1

[sip]
exten => _2XXX,1,Dial(SIP/${EXTEN},,)
exten => _2XXX,n,Hangup()
```

Fonte: Elaborada pelo autor

Na figura 19 é apresentando o arquivo de Dialplan “/etc/asterisk/extensions.conf” atualizado após a execução do script “atualizar_rotas.sh”. O arquivo “/etc/asterisk/extensions.conf”, posteriormente a atualização, possui as rotas utilizadas pelo segundo PABX IP e pelo terceiro PABX IP no cenário da solução proposta.

Figura 19 - Dialplan atualizado

```

[general]
static=yes
writeprotect=no
clearglobalvars=no

[globals]
CONSOLE=Console/dsp
IAXINFO=quest
TRUNK=DAHDI/G2
TRUNKMSD=1

[sip]
exten => _2XXX,1,Dial(SIP/${EXTEN},,)
exten => _2XXX,n,Hangup()
exten => _3XXX,1,Dial(SIP/${EXTEN}@192.168.92.130,,)
exten => _3XXX,n,Hangup()
exten => _4XXX,1,Dial(SIP/${EXTEN}@192.168.92.132,,)
exten => _4XXX,n,Hangup()

```

Fonte: Elaborada pelo autor

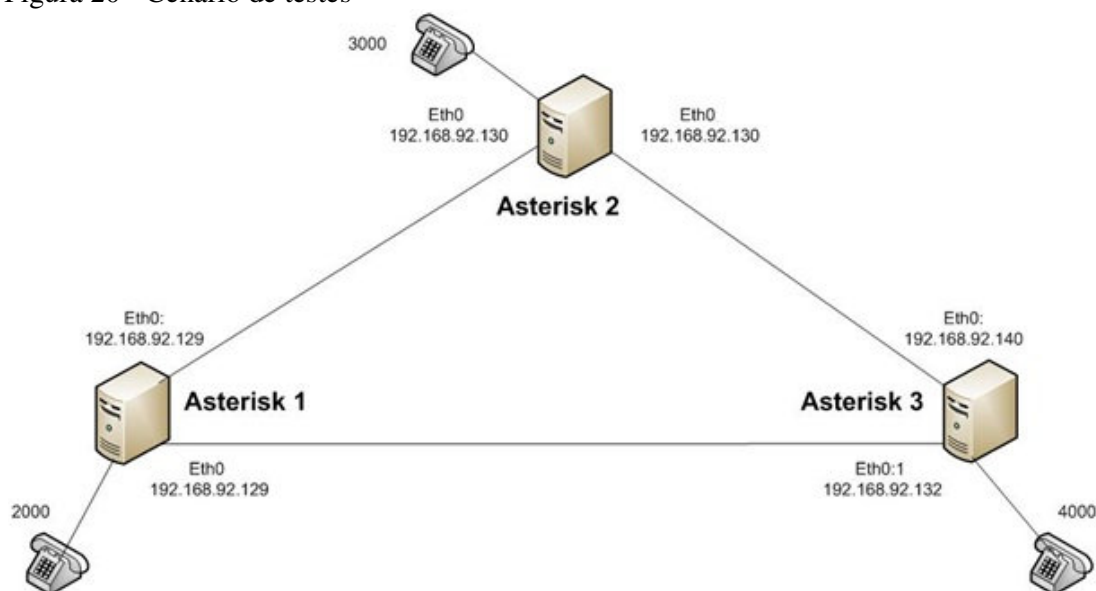
O apêndice C demonstra o código “definir_rota.sh” que possui o objetivo de realizar através do protocolo ICMP (*Internet Control Message Protocol*) gerenciando a resposta após geração de cinco pacotes com destino aos Endereços IP utilizados por cada Servidor Asterisk.

5.5 VALIDAÇÃO DO SISTEMA

Para validação do sistema proposto efetuou-se a implementação do cenário de testes de acordo com a figura 20, constando três Servidores Asterisk com o sistema operacional Linux, estando estes servidores inseridos em uma Rede Local endereçada. Os servidores encontram-se implementados em ambiente virtualizado através da aplicação Vmware.

Realizou-se em testes a execução do script “atualizar_rotas.sh” no Servidor Asterisk 1 com endereçamento IP “192.168.92.129” e este o script requisita os arquivos de Dialplan do Servidores Asterisk 2 com endereçamento IP “192.168.92.130” e Asterisk 3 com os endereçamentos IP “192.168.92.140” e “192.168.92.132”. Posteriormente a recepção dos arquivos de Dialplan e comparação entre estes e o arquivo de Dialplan já configurado no Servidor Asterisk 1, verificou-se a inserção automatizada das rotas distintas às rotas já criadas de forma manual.

Figura 20 - Cenário de testes



Fonte: Elaborada pelo autor

Na figura 21, apresenta-se o trace administrado pela aplicação Wireshark do protocolo SSH (*Secure Shell*) utilizado para proporcionar autenticação durante o compartilhamento dos arquivos de Dialplan entre os Servidores Asterisk 1 e Asterisk 2.

Figura 21 - Trace do protocolo SSH

| logssh.pcap [Wireshark 1.10.3 (SVN Rev 53022 from /trunk-1.10)] | | | | | | |
|---------------------------------------------------------------------------------------------------------|-----------|----------------|----------------|----------|--------|------------------------------------------------------------|
| File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help | | | | | | |
| Filter: ssh Expression... Clear Apply Save | | | | | | |
| No. | Time | Source | Destination | Protocol | Length | Info |
| 21 | 5.092898 | 192.168.92.129 | 192.168.92.130 | SSHv2 | 107 | Client Protocol: SSH-2.0-openssh_5.9p1 Debian-5ubuntu1.1\r |
| 23 | 5.098063 | 192.168.92.130 | 192.168.92.129 | SSHv2 | 1050 | Server: Key Exchange Init |
| 24 | 5.103231 | 192.168.92.129 | 192.168.92.130 | SSHv2 | 1338 | Client: Key Exchange Init |
| 28 | 5.143423 | 192.168.92.129 | 192.168.92.130 | SSHv2 | 146 | Client: Diffie-Hellman Key Exchange Init |
| 30 | 5.153993 | 192.168.92.130 | 192.168.92.129 | SSHv2 | 378 | Server: New Keys |
| 31 | 5.178996 | 192.168.92.129 | 192.168.92.130 | SSHv2 | 82 | Client: New Keys |
| 33 | 5.218365 | 192.168.92.129 | 192.168.92.130 | SSHv2 | 114 | Encrypted request packet len=48 |
| 35 | 5.219254 | 192.168.92.130 | 192.168.92.129 | SSHv2 | 114 | Encrypted response packet len=48 |
| 36 | 5.219619 | 192.168.92.129 | 192.168.92.130 | SSHv2 | 130 | Encrypted request packet len=64 |
| 65 | 15.231539 | 192.168.92.130 | 192.168.92.129 | SSHv2 | 130 | Encrypted response packet len=64 |
| 66 | 15.233386 | 192.168.92.129 | 192.168.92.130 | SSHv2 | 210 | Encrypted request packet len=144 |
| 68 | 15.238798 | 192.168.92.130 | 192.168.92.129 | SSHv2 | 98 | Encrypted response packet len=32 |
| 69 | 15.275259 | 192.168.92.129 | 192.168.92.130 | SSHv2 | 194 | Encrypted request packet len=128 |
| 71 | 15.349805 | 192.168.92.130 | 192.168.92.129 | SSHv2 | 114 | Encrypted response packet len=48 |
| 72 | 15.350285 | 192.168.92.129 | 192.168.92.130 | SSHv2 | 226 | Encrypted request packet len=160 |
| 74 | 15.353231 | 192.168.92.130 | 192.168.92.129 | SSHv2 | 146 | Encrypted response packet len=80 |
| 75 | 15.353622 | 192.168.92.130 | 192.168.92.129 | SSHv2 | 114 | Encrypted request packet len=48 |
| Frame 21: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) | | | | | | |
| Ethernet II, Src: Vmware_04:be:6b (00:0c:29:04:be:6b), Dst: Vmware_d4:b4:f7 (00:0c:29:d4:b4:f7) | | | | | | |
| Internet Protocol Version 4, Src: 192.168.92.129 (192.168.92.129), Dst: 192.168.92.130 (192.168.92.130) | | | | | | |
| Transmission Control Protocol, Src Port: 41241 (41241), Dst Port: ssh (22), Seq: 1, Ack: 42, Len: 41 | | | | | | |
| SSH Protocol | | | | | | |

Fonte: Elaborada pelo autor

Na figura 22, apresenta-se o trace administrado pela aplicação Wireshark do protocolo ICMP utilizado durante a execução do script “definir_rota.sh” efetuando-se a verificação de resposta ao se encaminhar cinco pacotes aos endereços IP do Servidor Asterisk 2 e Asterisk 3 e como originador dos pacotes o Servidor Asterisk 1.

Simula-se antecipadamente a execução do script “definir_rota.sh” a queda da interface de rede do Servidor Asterisk 2 endereçado com o endereço IP “192.168.92.130” e o script utiliza para as rotas a serem requisitadas para os ramais de 3000 a 3999 o endereço IP “192.168.92.140” disposto ao Servidor Asterisk 3.

Figura 22 - Trace do protocolo ICMP

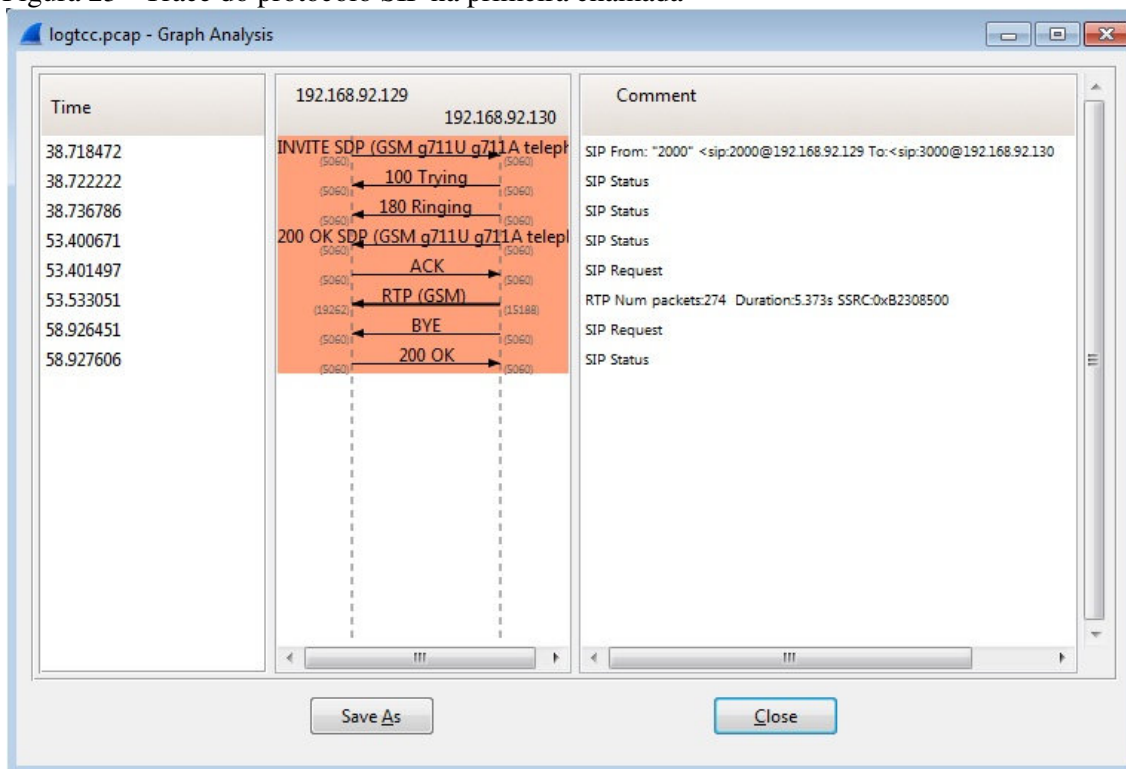
| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|----------------|----------|--------|------------------------------------------------------------------|
| 101 | 26.718213 | 192.168.92.129 | 192.168.92.140 | ICMP | 98 | Echo (ping) request id=0x0e9b, seq=1/256, ttl=64 (reply in 102) |
| 102 | 26.718853 | 192.168.92.140 | 192.168.92.129 | ICMP | 98 | Echo (ping) reply id=0x0e9b, seq=1/256, ttl=64 (request in 101) |
| 103 | 27.721487 | 192.168.92.129 | 192.168.92.140 | ICMP | 98 | Echo (ping) request id=0x0e9b, seq=2/512, ttl=64 (reply in 104) |
| 104 | 27.722008 | 192.168.92.140 | 192.168.92.129 | ICMP | 98 | Echo (ping) reply id=0x0e9b, seq=2/512, ttl=64 (request in 103) |
| 112 | 28.721506 | 192.168.92.129 | 192.168.92.140 | ICMP | 98 | Echo (ping) request id=0x0e9b, seq=3/768, ttl=64 (reply in 113) |
| 113 | 28.721974 | 192.168.92.140 | 192.168.92.129 | ICMP | 98 | Echo (ping) reply id=0x0e9b, seq=3/768, ttl=64 (request in 112) |
| 117 | 29.721559 | 192.168.92.129 | 192.168.92.140 | ICMP | 98 | Echo (ping) request id=0x0e9b, seq=4/1024, ttl=64 (reply in 118) |
| 118 | 29.722329 | 192.168.92.140 | 192.168.92.129 | ICMP | 98 | Echo (ping) reply id=0x0e9b, seq=4/1024, ttl=64 (request in 117) |
| 122 | 30.723986 | 192.168.92.129 | 192.168.92.140 | ICMP | 98 | Echo (ping) request id=0x0e9b, seq=5/1280, ttl=64 (reply in 123) |
| 123 | 30.724451 | 192.168.92.140 | 192.168.92.129 | ICMP | 98 | Echo (ping) reply id=0x0e9b, seq=5/1280, ttl=64 (request in 122) |
| 124 | 30.870070 | 192.168.92.129 | 192.168.92.140 | ICMP | 98 | Echo (ping) request id=0x0eaa, seq=1/256, ttl=64 (reply in 125) |
| 125 | 30.870725 | 192.168.92.140 | 192.168.92.129 | ICMP | 98 | Echo (ping) reply id=0x0eaa, seq=1/256, ttl=64 (request in 124) |
| 126 | 31.871752 | 192.168.92.129 | 192.168.92.140 | ICMP | 98 | Echo (ping) request id=0x0eaa, seq=2/512, ttl=64 (reply in 127) |
| 127 | 31.872873 | 192.168.92.140 | 192.168.92.129 | ICMP | 98 | Echo (ping) reply id=0x0eaa, seq=2/512, ttl=64 (request in 126) |
| 135 | 32.873642 | 192.168.92.129 | 192.168.92.140 | ICMP | 98 | Echo (ping) request id=0x0eaa, seq=3/768, ttl=64 (reply in 136) |
| 136 | 32.874106 | 192.168.92.140 | 192.168.92.129 | ICMP | 98 | Echo (ping) reply id=0x0eaa, seq=3/768, ttl=64 (request in 135) |
| 140 | 33.872643 | 192.168.92.129 | 192.168.92.140 | ICMP | 98 | Echo (ping) request id=0x0eaa, seq=4/1024, ttl=64 (reply in 141) |
| 141 | 33.873155 | 192.168.92.140 | 192.168.92.129 | ICMP | 98 | Echo (ping) reply id=0x0eaa, seq=4/1024, ttl=64 (request in 140) |
| 145 | 34.874411 | 192.168.92.129 | 192.168.92.140 | ICMP | 98 | Echo (ping) request id=0x0eaa, seq=5/1280, ttl=64 (reply in 146) |
| 146 | 34.875255 | 192.168.92.140 | 192.168.92.129 | ICMP | 98 | Echo (ping) reply id=0x0eaa, seq=5/1280, ttl=64 (request in 145) |

| | |
|---------------------------------------------------------------------------------------------------------|--|
| Frame 101: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) | |
| Ethernet II, Src: Vmware_04:be:6b (00:0c:29:04:be:6b), Dst: Vmware_df:1e:e6 (00:0c:29:df:1e:e6) | |
| Internet Protocol Version 4, Src: 192.168.92.129 (192.168.92.129), Dst: 192.168.92.140 (192.168.92.140) | |
| Internet Control Message Protocol | |

Fonte: Elaborada pelo autor

Efetuuou-se em testes, posteriormente a atualização de rotas a realização de chamada originada no ramal 2000 cadastrado e autenticado no Servidor Asterisk 1 tendo-se como destino desta chamada o ramal 3000 cadastrado e autenticado no Servidor Asterisk 2. A figura 23 apresenta o trace do protocolo SIP administrado pela aplicação Wireshark para a chamada realizada entre o ramal 2000 e o ramal 3000.

Figura 23 - Trace do protocolo SIP na primeira chamada

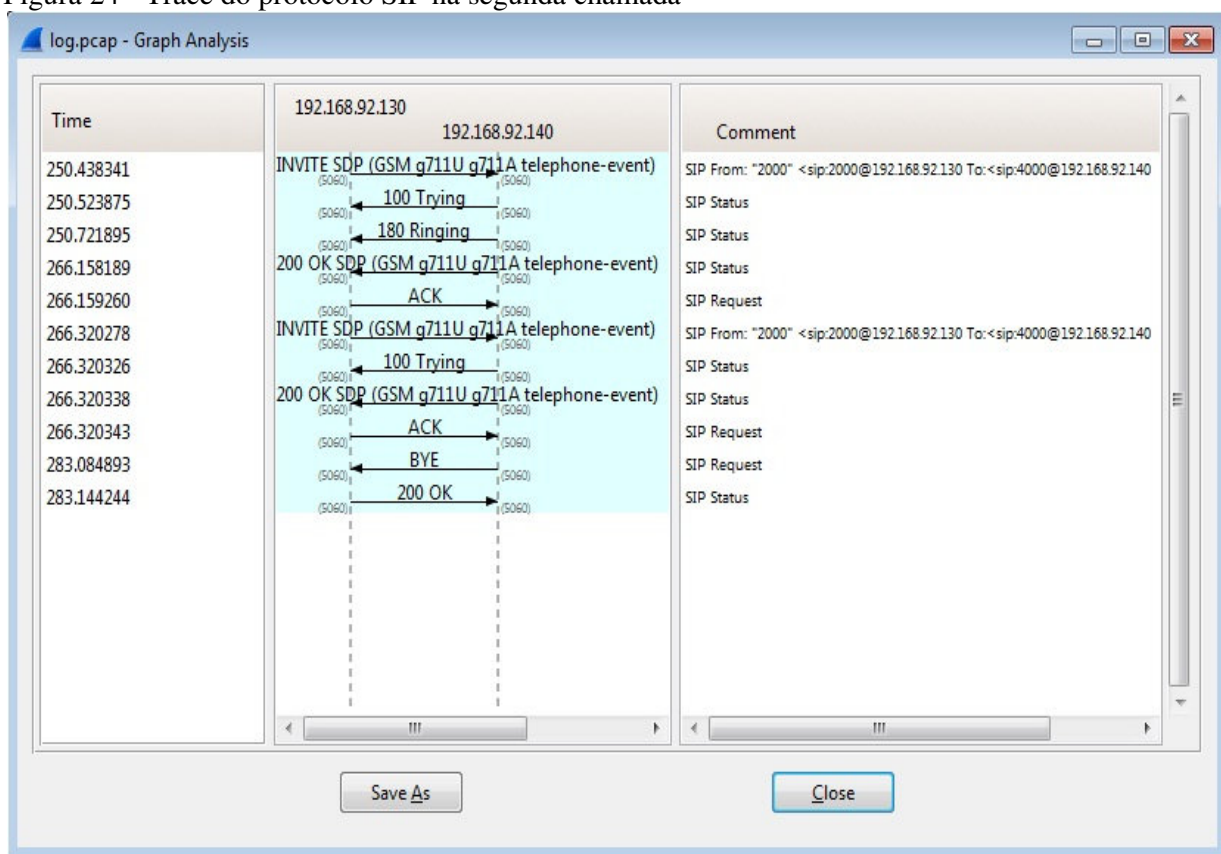


Fonte: Elaborada pelo autor

Executou-se o script "definir_rota.sh", simulando-se a queda da segunda interface de rede do Servidor Asterisk 3 utilizada para registro SIP entre o Servidor Asterisk 1 e o Servidor Asterisk 3.

Realizou-se uma chamada do ramal 2000 cadastrado e autenticado no Servidor Asterisk 1 para o ramal 4000 cadastrado e autenticado no Servidor Asterisk 3. A figura 24 apresenta o trace do protocolo SIP administrado pela aplicação Wireshark para a chamada realizada entre o ramal 2000 e o ramal 4000, porém utilizando-se o registro SIP entre o Servidor Asterisk 1 e o Servidor Asterisk 2.

Figura 24 - Trace do protocolo SIP na segunda chamada



Fonte: Elaborada pelo autor

6 CONCLUSÃO E TRABALHOS FUTUROS

Este capítulo apresenta os resultados obtidos com a implementação do sistema para roteamento para PABX IP proposto para o cenário a ser solucionado. O sistema automatizou a atualização de rotas inseridas de forma manual em cada PABX IP presente no cenário e definir a rota disponível para comunicação.

6.1 OBJETIVOS ALCANÇADOS

Para se alcançar os objetivos do projeto houve a necessidade de ampliar os conhecimentos de protocolos de roteamento, de conceitos em Linguagem de programação *Shell Script Bash* e de conceitos relacionados ao protocolo SIP.

O desenvolvimento do desenho do cenário contribuiu para o desenvolvimento do sistema, pois norteou o traçado do desenvolvimento e delimitou o sistema proposto reduzindo o tempo para desenvolvimento.

A vivência profissional do autor também contribuiu imensamente para a criação da ideia do projeto e para elaboração da arquitetura do sistema. Porém o aperfeiçoamento do sistema dependeu da busca constante por conceitos relacionados a comandos *Shell* do sistema operacional Linux.

6.2 RESULTADOS

O resultado do trabalho obtido é o estudo sobre a utilização conceitual de protocolos de roteamento dinâmico, como o OSPF, para o desenvolvimento de um sistema que automatize a troca de rotas e se promova a análise do estado de enlace em um ambiente em que constitui-se de uma topologia em PABX IP ao invés de roteadores convencionais.

Com base na experiência profissional do autor em roteamento OSPF em redes LAN com roteadores convencionais e implantação de Servidores Asterisk contribuíram para o desenvolvimento do sistema e a realização dos testes para validação.

A principal vantagem do sistema é o desempenho, devido a ser desenvolvido em *Shell Script Bash* facilitando a interação entre o sistema desenvolvido e o sistema operacional Linux.

6.3 TRABALHOS FUTUROS

O sistema desenvolvido para o trabalho de conclusão de curso é um sistema diferenciado, portanto existe a possibilidade de se desenvolver novos módulos para que o sistema seja utilizado para diversos cenários, independente de sua topologia e quantidade de entidades inseridas.

O sistema atual efetua o gerenciamento do estado do enlace entre os Servidores Asterisk através do protocolo ICMP, porém não possui o gerenciamento da quantidade de nós presentes no enlace de comunicação.

A ideia de se automatizar a troca de rotas entre os Servidores Asterisk é uma ideia válida que pode ser colocada em desenvolvimento através de diversos métodos de desenvolvimento.

Outro trabalho futuro pode ser a proposta do manuseio na criação de rotas em arquivo de Dialplan através de um sistema *web* que interaja com o Analista de Telecomunicações.

Sugere-se para novos módulos a utilização conceitual de protocolos de roteamento que beneficiam redes WAN como a Internet para o desenvolvimento do sistema viabilizando a delimitação geográfica dos cenários.

REFERÊNCIAS

BURTCH, Ken O. **Linux Shell Scripting with Bash**. Indianapolis: Term Ling, 2004.

CHOWDHURY, DhimanDeb. **Projetos avançados de rede IP**: roteamento, qualidade serviço e voz sobre IP; tradução de Daniel Vieira. Rio de Janeiro: Campus, 2002.

COLCHER, Sérgio et al. **VoIP**: Voz sobre IP; Rio de Janeiro: Elsevier, 2005.

COMER, Douglas E. **Interligação em rede com TCP/IP**; tradução de ARX Publicações. Rio de Janeiro: Campus, 1998.

DEMO, Pedro. **Pesquisa e construção de conhecimento**: Metodologia científica no caminho de Habermas. 6. ed. Rio de Janeiro: Tempo Brasileiro, 2004.

DWIVEDI, Himanshu. **Implementing SSH**: Strategies for Optimizing the Secure Shell. Indianapolis: Wiley Composition Services, 2004.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Altas, 2002.

GONÇALVES, Flávio Eduardo de A. **Telefonia IP com SIP**: Abordando o SIP Express Router. Florianópolis: Título Independente, 2007.

IPBX com Asterisk: IPBX com Digium/Asterisk – TrixBox – Elastix. Disponível em: <<http://linuxplace.com.br/category/produtos/ipbx-com-asterisk>>. Acesso em: 16 out. 2013.

MARQUES, Heitor Romero et al. **Metodologia de Pesquisa e de Trabalho Científico**. 2. ed. Campo Grande: Ucdb (universidade Católica Dom Bosco), 2006.

MEDEIROS, Júlio Cesar de Oliveira. **Princípios de Telecomunicações**: Teoria e Prática. 2. ed. São Paulo: Érica, 2007.

MEGGELN, Jim Van; SMITH, Jared; MADSEN, Leif. **Asterisk**: O Futuro da Telefonia. Rio de Janeiro: Alta Books, 2005.

MORIMOTO, Carlos E. **Redes, guia prático**. 2. ed. São Paulo: Gdh Press e Sul Editores, 2008.

PARZIALE, Lydia et al. **TCP/IP Tutorial and Technical Overview**. New York: Ibm Redbooks, 2006.

SILVA, Alberto Manuel Rodrigues da; VIDEIRA, Carlos Alberto Escaleira. **UML, Metodologias e Ferramentas CASE: UML, Metodologias e Ferramentas CASE Linguagem de Modelação UML, Metodologias e Ferramentas CASE na Concepção e Desenvolvimento de Software**. Porto: Centro Atlântico, 2001.

SILVA, Edna Lúcia da; MENEZES, Eстера Muszkat. **Metodologia da pesquisa e elaboração de dissertação**. 3. ed. rev. atual. Florianópolis: Laboratório de Ensino a Distância da Ufsc, 2001.

SOMMERVILLE, Ian. **Engenharia de Software**. 8. ed. São Paulo: Pearson, 2003.

TANENBAUM, Andrew S.. **Rede de Computadores**; tradução de Vandenberg D. de Souza. 4. ed. Rio de Janeiro: Campus, 2005.

THOMAS, Keir; CHANNELLE, Andy; SICAM, Jaime. **Beginning Ubuntu Linux: From Novice to Professional, Fourth Edition**. New York: Apress, 2009.

TORRES, Gabriel. **Rede de Computadores: Curso Completo**. Rio de Janeiro: Axcel Books, 2001.

TOZONI-REIS, Marília Freitas de Campos. **Metodologia de Pesquisa**. 2. ed. Curitiba: Iesde Brasil, 2009.

UBUNTU to run on tablets, smartphones and TVs, canonical founder says: "Linux for human beings" to challenge Google, Apple and Microsoft. Disponível em: <<http://news.techworld.com/operating-systems/3314656/ubuntu-to-run-on-tablets-smartphones-and-tvs-canonical-founder-says/>>. Acesso em: 16 out. 2013.

VERAS, Manoel. **Virtualização: Componente Central do Datacenter**. Rio de Janeiro: Brasport, 2011.

VMWARE Workstation. Disponível em: <<http://www.vmware.com/br/products/workstation/>>. Acesso em: 16 out. 2013.

APÊNDICES

APÊNDICE A – Cronograma

| ATIVIDADES | AGOSTO | SETEMBRO | OUTUBRO | NOVEMBRO |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|----------|---------|----------|
| DEFINIÇÃO E ENTREGA DO CRONOGRAMA | | | | |
| ENTREGA DAS CORREÇÕES REALIZADAS DECORRENTES AS ALTERAÇÕES SUGERIDAS PELO AVALIADOR EXTERNO | | | | |
| AMPLIAÇÃO DE CONHECIMENTOS, DEFINIÇÃO DO PROTOCOLO DE ROTEAMENTO PARA REFERÊNCIA CONCEITUAL, DEFINIÇÃO DO CENÁRIO DE TESTES E DEFINIÇÃO DA INCLUSÃO DE PROGRAMAÇÃO | | | | |
| ENTREGA DO CAPÍTULO DE MODELAGEM | | | | |
| CODIFICAÇÃO INICIAL | | | | |
| ELABORAÇÃO DO CENÁRIO DE SIMULAÇÃO | | | | |
| TESTES INICIAIS | | | | |
| CONTROLE E VERIFICAÇÃO DO DESENVOLVIMENTO EM SALA DE AULA | | | | |
| APERFEIÇOAMENTO DO SOFTWARE | | | | |
| TESTES FINAIS | | | | |
| ELABORAÇÃO TEXTUAL DO CAPÍTULO DE DESENVOLVIMENTO | | | | |
| APRESENTAÇÃO E ENTREGA IMPRESSA DO CAPÍTULO DE DESENVOLVIMENTO | | | | |
| (17/10) DATA LIMITE PARA ENVIO DO ORIENTADOR DO TERMO DE ENCAMINHAMENTO PARA DEFESA PÚBLICA | | | | |
| DEFINIÇÃO DA BANCA EXAMINADORA E DEFINIÇÃO DE DATA DE DEFESA | | | | |
| ELABORAÇÃO DA APRESENTAÇÃO | | | | |
| (07/11) DATA LIMITE PARA ENTREGA DA MICROGRAFIA | | | | |
| SEMANA DE DEFESAS DO TRABALHO DE CONCLUSÃO DE CURSO | | | | |

APÊNDICE B – Código do arquivo “atualizar_rotas.sh”

```
#!/bin/bash
#-----
# -----|
# |      Atualizacao de rotas      ||
# -----|
#-----

contador=`grep -c 'register' /etc/asterisk/sip.conf`

for i in $(seq $contador);
do
cat /etc/asterisk/sip.conf | sed -n '/register/w register.txt'
cat register.txt | sed -n $i' p;' >> host.txt
host=`cat host.txt | cut -d@ -f2`

rm -rf host.txt
ip=`ifconfig eth0 | sed -n '/inet addr/{ s/.*addr:\([0-9.]\+\)
.\*/\1/p }'`

if [ "$ip" != "$host" ];
then
mkdir /tmp/$host
sshpass -p "alex" scp alex@$host:/etc/asterisk/extensions.conf
/tmp/$host/
sed -i 's/}}}}@'"$host"'/ /tmp/$host/extensions.conf
aux1=`grep -c '"$host"' /tmp/$host/extensions.conf`
```

```

fi

if [ "$aux1" -gt "1" ];
then
cat -n /tmp/$host/extensions.conf | sed -n /@"'$host'"'/p >>
teste.txt
sed -i '"$i"'d' teste.txt
cat teste.txt | cut -de -f1 >> linha.txt
rm -rf teste.txt
sed -i 's/^[ \t]*//' linha.txt
sed -i 's/[ \t]*$//' linha.txt
aux2=`cat linha.txt`
rm -rf linha.txt

sed -i '"$aux2"'s/@"'$host'"'/@/g' /tmp/$host/extensions.conf
diff /etc/asterisk/extensions.conf /tmp/$host/extensions.conf
| grep ^\> > /tmp/$host/linhas_acrescentadas.txt
cat /tmp/$host/linhas_acrescentadas.txt | sed 's/>/' >> /tmp/
$host/tratamento.txt
sed -i 's/^[ \t]*+/' /tmp/$host/tratamento.txt
cat /tmp/$host/tratamento.txt >> /etc/asterisk/extensions.conf
sed -i '"$ip"'d' /etc/asterisk/extensions.conf

asterisk -rx "dialplan reload"
rm -rf /tmp/$host

```

```

else
echo entro no else
diff /etc/asterisk/extensions.conf /tmp/$host/extensions.conf
| grep ^\> > /tmp/$host/linhas_acrescentadas.txt
cat /tmp/$host/linhas_acrescentadas.txt | sed 's/>/' >> /tmp/
$host/tratamento.txt
sed -i 's/^ \+/' /tmp/$host/tratamento.txt
cat /tmp/$host/tratamento.txt >> /etc/asterisk/extensions.conf
sed -i '/'"$sip"/d' /etc/asterisk/extensions.conf
asterisk -rx "dialplan reload"
rm -rf /tmp/$host
fi
done

aux3=`grep -c '@.*@' /etc/asterisk/extensions.conf`

if [ "$aux3" != 0 ];
then
cat /etc/asterisk/extensions.conf | awk '!( $0 in a) {a
[$0];print}' >> /etc/asterisk/extensions.conf.tmp
mv /etc/asterisk/extensions.conf.tmp
/etc/asterisk/extensions.conf
sed -i '/'"@.*@"/d' /etc/asterisk/extensions.conf
asterisk -rx "dialplan reload"
fi

```

```

cat /etc/asterisk/sip.conf | sed -n '/register/w reg.txt'
cat reg.txt | sed -n 2' p;' >> host.txt
host1=`cat host.txt | cut -d@ -f2`
rm -rf host.txt
rm -rf reg.txt

cat /etc/asterisk/extensions.conf | sed -n '/4XXX/p' >> aux0.txt
aux=`grep -cv '$=' aux0.txt`
if [ "$aux" != 0 ];
then
cat aux0.txt | sed -n '/@/p' >> aux1.txt
cat aux1.txt | cut -d@ -f2 >> aux2.txt
cat aux2.txt | cut -d, -f1 >> aux3.txt

host2=`cat aux3.txt | sed -n 1' p;`
host3=`cat aux3.txt | sed -n 2' p;`

rm -rf aux0.txt
rm -rf aux1.txt
rm -rf aux2.txt
rm -rf aux3.txt

if [ -z "$host2" ];
then
exit
elif [ "$host1" != "$host2" ];
then
sed -i '/'"$host2"'/d' /etc/asterisk/extensions.conf
fi

if [ -z "$host3" ];
then
exit
elif [ "$host1" != "$host3" ];
then
sed -i '/'"$host3"'/d' /etc/asterisk/extensions.conf
fi
asterisk -rx "dialplan reload"
fi

```

APÊNDICE C – Código do arquivo “definir_rota.sh”

```
#!/bin/bash
# Definicao da melhor rota
#

contador=`grep -c '@' /etc/asterisk/extensions.conf`

cat /etc/asterisk/sip.conf | sed -n '/register/w register.txt'
cat register.txt | sed -n 1' p;' >> host.txt
host3=`cat host.txt | cut -d@ -f2`
rm -rf register.txt
rm -rf host.txt

cat /etc/asterisk/sip.conf | sed -n '/register/w register.txt'
cat register.txt | sed -n 2' p;' >> host.txt
host4=`cat host.txt | cut -d@ -f2`
rm -rf register.txt
rm -rf host.txt

cat /etc/asterisk/extensions.conf | sed -n '/@/p' | cut -d@ -
f2 | cut -d, -f1 >> teste.txt

host1=
host2=

if [ "$contador" -gt "1" ];
then
host1=`sed -n 1' p;' teste.txt`
host2=`sed -n 2' p;' teste.txt`
else
host1=`sed -n 1' p;' teste.txt`
fi
```



```

rm -rf teste.txt

if [ "$host1" != "$host3" ];
then
host1=$host3
fi

if [ "$host2" != "$host4" ];
then
host2=$host4
fi

ip=`ifconfig eth0 | sed -n '/inet addr/{ s/.*addr:\([0-9.]\+\)
.\*/\1/p }'`
aux1=
aux2=

for i in $(seq $contador);
do

if [ "$i" != "2" ];
then
if [ "$ip" != "$host1" ];
then
ping -c 5 $host1 >> ping.txt
aux1=`grep -c '5 received' ping.txt`
rm -rf ping.txt
fi

if [ "$aux1" -gt "0" ];
then
cat -n /etc/asterisk/extensions.conf | sed -n '/@/{p;q}' >>

```

```

teste.txt
#sed -i '2d' teste.txt
cat teste.txt | cut -de -f1 >> aux.txt
sed -i 's/^[ \t]*$//' aux.txt
sed -i 's/[ \t]*$//' aux.txt
aux3=`cat aux.txt`
rm -rf teste.txt
rm -rf aux.txt

sed -i ''"$aux3"s/@.*,/@'"$host1"'',,/'
/etc/asterisk/extensions.conf
asterisk -rx "dialplan reload"

elif [ "$ip" != "$host2" ];
then
ping -c 5 $host2 >> ping.txt
aux2=`grep -c '5 received' ping.txt`
rm -rf ping.txt

if [ "$aux2" -gt "0" ];
then
cat -n /etc/asterisk/extensions.conf | sed -n '/@/{p;q}' >>
teste.txt
#sed -i '2d' teste.txt
cat teste.txt | cut -de -f1 >> aux.txt
sed -i 's/^[ \t]*$//' aux.txt
sed -i 's/[ \t]*$//' aux.txt
aux3=`cat aux.txt`
rm -rf teste.txt
rm -rf aux.txt

sed -i ''"$aux3"s/@.*,/@'"$host2"'',,/'

```

```

/etc/asterisk/extensions.conf
asterisk -rx "dialplan reload"

fi
fi
fi

if [ "$i" = 2 ];
then
if [ "$ip" != "$host2" ];
then
ping -c 5 $host2 >> ping.txt
aux1=`grep -c '5 received' ping.txt`
rm -rf ping.txt
fi

if [ "$aux1" -gt "0" ];
then
cat -n /etc/asterisk/extensions.conf | sed -n '/@/h;${x;p;}'
>> teste.txt
#sed -i '1d' teste.txt
cat teste.txt | cut -de -f1 >> aux.txt
sed -i 's/^[ \t]*$//' aux.txt
sed -i 's/[ \t]*$//' aux.txt
aux4=`cat aux.txt`
rm -rf teste.txt
rm -rf aux.txt

sed -i '$aux4's/@.*,/@"$host2"',,/'
/etc/asterisk/extensions.conf
asterisk -rx "dialplan reload"

```

```

elif [ "$ip" != "$host1" ];
then
ping -c 5 $host1 >> ping.txt
aux2=`grep -c '5 received' ping.txt`
rm -rf ping.txt

if [ "$aux2" -gt "0" ];
then

cat -n /etc/asterisk/extensions.conf | sed -n '/@/h;${x;p;}'
>> teste.txt
#sed -i 'ld' teste.txt
cat teste.txt | cut -de -f1 >> aux.txt
sed -i 's/^[ \t]*//' aux.txt
sed -i 's/[ \t]*$//' aux.txt
aux4=`cat aux.txt`
rm -rf teste.txt
rm -rf aux.txt

sed -i '"$aux4"'s/@.*,/@'"$host1"',,/'
/etc/asterisk/extensions.conf
asterisk -rx "dialplan reload"

fi
fi
fi
done

```