Uma proposta de implementação de telefonia VoIP na UPE-POLI

Trabalho de Conclusão de Curso

Engenharia da Computação

Raphael Fonseca Dantas
Orientador: Prof. Sérgio Campello Oliveira

Universidade de Pernambuco
Escola Politécnica de Pernambuco
Graduação em Engenharia de Computação

Raphael Fonseca Dantas

Uma proposta de implementação de telefonia VoIP na UPE-POLI

Monografia apresentada como requisito parcial para obtenção do diploma de Bacharel em Engenharia de Computação pela Escola Politécnica de Pernambuco – Universidade de Pernambuco.

Recife, Outubro de 2016.

POLI
ESCOLA POLITÉCNICA
DE PERNAMBUCO

MONOGRAFIA DE FINAL DE CURSO

Avaliação Final (para o presidente da banca)*

No dia 16 de 12 de 2016, ás 10:00 horas, reuniu-se para deliberar a defesa da monografia de conclusão de curso do discente **Raphael Fonseca Dantas**, orientado pelo professor **Sérgio Campello Oliveira**, sob título **Uma proposta de implementação de telefonia VoIP na UPE-POLI**, a banca composta pelos professores:

Edison de Queiroz Albuquerque
Sérgio Campello Oliveira

Após a apresentação da monografia e discussão entre os membros da Banca, a mesma foi considerada:

☑ Aprovada ☐ Aprovada com Restrições* ☐ Reprovada

e foi-lhe atribuída nota: 7,5 (Sete e Meio)

*(Obrigatório o preenchimento do campo abaixo com comentários para o autor)

O discente terá 07 dias para entrega da versão final da monografia a contar da data deste documento.

Edison de Queiroz Albuquerque

EDISON DE QUEIROZ ALBUQUERQUE

S. Campello Oliveira

SÉRGIO CAMPELLO OLIVEIRA

Dedico este projeto ao meu falecido pai: Edison Dantas.

Agradecimentos

Agradeço, primeiramente, a ajuda imprescindível de minha maior incentivadora e namorada, Arine Pedrosa. Agradeço a meus falecidos pai e minha mãe por terem me dado total condições, desde iniciada a vida estudantil até esta etapa da minha vida. Agradeço ainda aos amigos Rômulo Marques, Vânia Vanderlei, Maria Eugênia e de minha tia Célia Fonseca por terem, de alguma forma, contribuído para a conclusão deste projeto. E por fim, agradeço aos conselhos e instruções do meu professor orientador Sérgio Campello.

Resumo

Este trabalho tem como principal objetivo propor uma solução de baixo custo para o sistema de comunicação da UPE-POLI, através da implantação da Tecnologia VoIP (Voz sobre IP). Para que tal tecnologia seja implantada, o projeto apresenta as características dos protocolos VoIP H.323 e SIP (Protocolo de iniciação de sessão). Também foi realizada uma análise da QoS (Qualidade de Serviço) da rede para definir que passos devem ser seguidos, evitando erros e implantações mal sucedidas da solução e suas especificações. Também é abordada a estrutura física de telefonia atual da POLI e é comparada com a nova topologia apresentada neste projeto, utilizando VoIP, e apresentadas as vantagens desta última sobre a primeira. Por fim são listados os equipamentos necessários para esta implementação, explicando como ocorre a conexão das redes operantes e são sugeridos trabalhos futuros que poderão vir a complementar este projeto.

Abstract

This paper aims to propose a low-cost solution to the communication system of the UPE-POLI, through the deployment of VoIP (Voice over IP) technology. For such technology to be deployed, the project brings the characteristics of VoIP protocols H.323 and SIP (Session Initiation Protocol). QoS (Quality of Service) analysis of the network and its specifications also were held to define which steps must be followed, preventing errors of badly succeeded implementations of the solution. Also is discussed the current telephony physical structure of POLI and it is compared with the new topology presented in this project, using VoIP, and presented the advantages of the latter one over the first one. Finally, it is listed the necessary equipment for this implementation, explaining how does the connection of operant networks and future work is suggested that may complement this project.

Sumário

Índice de Figuras

Índice de Tabelas

Tabela de Símbolos e Siglas

ASCII	American Standard Code for Information Interchange	Código Padrão Americano para o Intercâmbio de Informação
ATA	Analog Telephone Adapter	Adaptador de telefone analógico
ATM	Asynchronous Transfer Mode	Modo assíncrono de transferência
DDD		Discagem Direta a Distância
DDI		Discagem Direta Internacional
DDoS	Distributed Denial of Service	Negação de serviço distribuída
DoS	Denial of Service	Negação de serviço
DHCP	Dynamic Host Configuration Protocol	Protocolo de configuração dinâmica de *Host*
DSP	Digital signal processor	Processador digital de sinal
GSM	Global System for Mobile Communications	Sistema global para comunicações móveis
HTTP	Hypertext Transfer Protocol	Protocolo de transferência de Hipertexto
ID	Identifier	Identificador
IDS	Intrusion Detection System	Sistema de detecção de intrusos
IEEE	Institute of Electrical and Electronics Engineers	Instituto de engenheiros eletricistas e eletrônicos
IETF	Internet Engineering Task Force	Grupo de trabalho de engenharia da I*nternet*

IP	Internet Protocol	Protocolo de *internet*
IPTEL	Internet Protocol Telephony	Telefonia de protocolo de *internet*
ITU-T	International Telecommunication Union Standardization Sector	Setor de normatização das telecomunicações
LAN	Local Area Network	Rede de área local
MAC	Media Access Control	Controle de acesso de mídia
MAN	Metropolitan Area Network	Rede de área metropolitana
MCU	Multipoint Control Unit	Unidade de controle multiponto
MP	Multipoint Processor	Processador multiponto
PABX	Private Automatic Branch Exchange	Troca automática de ramais privados
PBX	Private Branch Exchange	Troca de ramais privados
PC	Personal Computer	Computador pessoal
PIN	Personal Identification Number	Número de identificação pessoal
PINT	PSTN and Internet Interworking	Interfuncionamento da PSTN e *internet*
POLI		Escola Politécnica de Pernambuco
PRTG	Paessler Router Traffic Grapher	Gráfico do tráfego do roteador desenvolvido pela Paessler
PSTN	Public Switched Telephone Network	Rede pública de telefonia comutada

QoS	Quality of Service	Qualidade de serviço
RFC	Request for Comments	Solicitação de comentários
RTCP	RTP Control Protocol	Protocolo de controle do RTP
RTP	Real-time Transport Protocol	Protocolo de transporte em tempo real
RTT	Round-trip Time	Tempo de ida e volta
SCTP	Stream Control Transmission Protocol	Protocolo de transmissão de controle de fluxo
SIP	Session Initiation Protocol	Protocolo de iniciação de sessão
SLA	Service Level Agreement	Acordo de nível de serviço
SMTP	Simple Mail Transfer Protocol	Protocolo de transferência de correio simples
SNMP	Simple Network Management Protocol	Protocolo simples de gerência de rede
SRTP	Secure Real-time Transport Protocol	Protocolo seguro de transporte em tempo real
TCP	Transmission Control Protocol	Protocolo de controle de transmissão
TLS	Transport Layer Security	Segurança de camada de transporte
UDP	User Datagram Protocol	Protocolo datagrama de usuário
UPE		Universidade de Pernambuco

URL	Uniform Resource Locator	Localizador uniforme de recursos
VLAN	Virtual Local Area Network	Rede local virtual
VoIP	Voice Over Internet Protocol	Voz sobre protocolo de *internet*
VOMIT	Voice Over Misconfigured Internet Telephones	Voz sobre telefones de *internet* mal configurados
VPN	Virtual Private Network	Rede privada virtual
WAN	Wide Area Network	Rede de longa distância

Capítulo 1

Introdução

Este capítulo tem como intuito: apresentar a motivação para este trabalho, através da Seção 1.1, os objetivos deste projeto definidos na Seção 1.2, a metodologia empregada para o desenvolvimento deste trabalho (Seção 1.3), e finalmente um descritivo da estrutura do documento para um melhor entendimento geral deste documento (Seção 1.4).

1.1 Motivação

A *Internet* está cada vez mais presente nos ambientes corporativos e educacionais, como também a qualquer pessoa que possua um computador e uma conexão de rede. A necessidade de comunicação entre pessoas de diferentes locais torna-se cada vez mais alta, devido principalmente a uma economia globalizada, que integra fornecedores e clientes em uma ampla rede mundial.

É cada vez maior o número de usuários que utilizam o serviço de VoIP no mundo e este número está aumentando em grandes proporções se compararmos ao número de provedores (empresas que fornecem serviço de VoIP) [1].

A necessidade de redução de custos corporativos aponta para soluções de racionalização de recursos, e existe a tendência de supressão da infraestrutura de telefonia convencional, e consequentemente dos seus custos de instalação e manutenção. Também se faz necessária a utilização da rede de dados para suportar um novo sistema, com a implementação de serviços de voz sobre IP (*Internet Protocol*).

Com a utilização da tecnologia VoIP, em ligações de longa distância nacionais e internacionais, tradicionalmente de alto custo, é possível conseguir uma redução mensal considerável nesses custos.

Foi constatada, por meio de pesquisas na Internet e na busca de materiais especializados sobre o assunto para o desenvolvimento deste projeto, a pouca quantidade de materiais em português sobre VoIP com a finalidade de efetuar a transição de sistemas antigos existentes para o novo sistema.

1.2 Objetivos

O objetivo geral do projeto é propor uma solução de comunicação de baixo custo para a UPE-POLI (Escola Politécnica da Universidade de Pernambuco), utilizando VoIP em telefonia IP, o qual inclui estudo da tecnologia, dos equipamentos necessários e o projeto da rede. Serão abordadas ainda as principais ameaças desse sistema, e também será apresentado um panorama das melhores práticas de segurança a fim de tornar essa tecnologia mais confiável e segura.

Este trabalho pode ainda servir como referência para implantação de outros projetos na área de VoIP, o qual será muito útil para empresas que estão iniciando o estudo de implantação de projetos nesta área, e não possuem familiaridade com esse sistema.

1.3 Metodologia

A metodologia empregada para a conclusão deste trabalho consta de:

- Pesquisas bibliográficas e pesquisas na *Internet* com o objetivo de formar a base teórica sobre ferramentas existentes e os trabalhos relacionados.
- Identificação de ferramentas e produtos disponíveis aos usuários.
- Avaliação de características típicas dos produtos VoIP.
- O estudo do sistema existente no centro de tecnologia da POLI, detalhando a configuração da atual rede e seus equipamentos existentes.

- Analisar as interações necessárias para transição da tecnologia atual para a proposta neste projeto

1.4 Estrutura do Documento

Após este capítulo introdutório, que basicamente visa contextualizar e apresentar a motivação, os objetivos e a metodologia deste projeto, o restante do trabalho será estruturado em cinco capítulos, conforme descrito a seguir:

Capítulo 2 – **Aplicações na Área de Telefonia** – Apresenta um referencial teórico sobre: conceitos VoIP e aspectos importantes para segurança da telefonia sobre IP, apresentando as principais ameaças e seus meios de proteção.

Capítulo 3 – **Os Protocolos VoIP** – É introduzido um estudo dos protocolos utilizados em tecnologia VoIP, focando nos protocolos de aplicação H.323 e SIP e nos protocolos de transporte RTP (*Real-time Transport Protocol*) e RTCP (*RTP Control Protocol*).

Capítulo 4 – **Qualidade de Serviço – QoS** – É realizado um estudo do QoS, com os parâmetros necessários para que uma ligação tenha qualidade.

Capítulo 5 – **O Projeto VoIP na UPE-POLI** – Traz uma visão geral do sistema telefônico existente na UPE-POLI, e é apresentada uma proposta de implementação de projeto que visa a efetuar a transição do atual sistema para a rede de Telefonia VoIP. Também são abordados os equipamentos e vantagens deste novo sistema.

Capítulo 6 – **Considerações Finais e Trabalhos Futuros** – Finalmente, no sexto capítulo, apresentam-se as conclusões e recomendações para trabalhos futuros, que reúne os comentários finais deste trabalho de pesquisa, fundamentados no referencial teórico e justificados pelas avaliações e análises desenvolvidas.

Capítulo 2

Aplicações na Área de Telefonia

Neste capítulo será exposto o conceito da tecnologia de Voz sobre IP, abordando suas vantagens e aplicações, como também será feito uma comparação com a rede de telefonia convencional. Uma seção sobre segurança envolvendo VoIP é descrita posteriormente, destacando-se as principais ameaças e soluções para combatê-las. Este tema é fortemente abordado atualmente.

2.1 Redes VoIP

VoIP é a tecnologia que viabiliza o estabelecimento de conversações telefônicas em uma Rede IP (na maior parte das vezes a *Internet*), tornando a transmissão de voz mais um dos serviços suportados pela rede de dados. Como a internet é uma rede global isso significa este tecnologia pode ser utilizada em qualquer lugar do mundo onde houver acesso [2].

Por utilizar a rede de computadores para transmissão de dados é necessário primeiro converter a voz em sinais digitais, sendo assim o primeiro passo é o *software* utilizado digitalizar a voz em pacotes de dados para que trafegue pela rede IP, após isso, quando o sinal chega no destino é novamente convertido em voz para o utilizador final.

A ligação VoIP pode ser feita através de um computador, utilizando programas de *SoftPhone*[1], com adaptadores ATA (*Analog Telephone Adapter*) ou por Telefone IP, que são vistos na Seção 5.2 desta monografia.

[1] Aplicativo multimídia, oferecido por operadoras VoIP, que trabalha associado com a tecnologia VoIP/telefone IP que dá a possibilidade de fazer chamadas diretamente do computador.

Existem diversas vantagens da tecnologia VoIP sobre a telefonia convencional, destacando-se a principal delas que é a redução de despesas, visto que a rede de dados (e consequentemente o VoIP) não está sujeita à mesma tarifação das ligações telefônicas convencionais, calculadas em função de distâncias geodésicas entre os pontos e horários de utilização estabelecidos pelas operadoras de telefonia. Outra grande vantagem da telefonia VoIP em relação à convencional é que esta última está baseada em comutação de circuitos, que podem ou não ser utilizados, enquanto a VoIP utiliza comutação por pacotes, que utiliza o aproveitamento dos recursos existentes de forma mais eficiente (circuitos físicos e largura de banda).

Esta característica também traz outra vantagem à VoIP, que é a capacidade dos pacotes de voz serem transmitidos pelo melhor caminho entre dois pontos, tendo sempre mais rota disponível e, portanto, com maiores opções de contingência.

Resumidamente, a tecnologia VoIP é um meio eficaz, econômico e dependendo do canal de transmissão torna-se bastante eficiente, essa tecnologia transforma sinais analógicos de áudio em sinais digitais de forma bidirecional que são transmitidos através da *Internet*. [3]. A Tabela 1 lista as características principais dos sistemas VoIP e convencional para telefonia.

Característica	Telefonia Convencional	Telefonia VoIP
Conexão na casa do usuário	Cabo de cobre (par trançado)	Banda larga de Internet
Falta de Energia Elétrica	Continua funcional	Para de funcionar
Mobilidade	Limitada a casa do usuário	Acesso em qualquer lugar do mundo, desde que conectado a *Internet*
Número Telefônico	Associado ao domicílio do usuário	Associado à área local do número contratado
Chamadas locais	Área local do domicílio do usuário	Área local do número contratado

Tabela 1. Telefonia Convencional x Telefonia VoIP.

Equivocadamente, a tecnologia VoIP é tratada em algumas ocasiões como o mesmo que Telefonia IP, embora sejam conceitos diferentes. VoIP é a tecnologia

que transforma a voz do modo convencional em pacotes IP para ser transmitida por uma rede de dados, enquanto a Telefonia IP, que utiliza VoIP, possui uma série de serviços agregados e carrega outras aplicações que não somente VoIP.

2.2 Segurança VoIP

Atualmente, ainda são poucos os ataques documentados especificamente em redes VoIP, talvez pela ainda não familiarização dos invasores com os protocolos desta tecnologia.

Todavia, já é de conhecimento que, em breve, esse cenário sofrerá mudanças, devido a vários fatores, um deles é o valor das informações que trafegam pelas redes VoIP, e que em mãos erradas poderão causar grandes prejuízos e lucros a diversas pessoas.

Vale ressaltar que na convergência das redes de voz com as redes de dados baseadas em TCP/IP (*Transmission Control Protocol over Internet Protocol*), houve também a convergência das vulnerabilidades inerentes às duas tecnologias [4].

Isto é, agora, um computador com telefone IP compatível precisa ser protegido tanto das ameaças relacionadas aos computadores quanto das ameaças relacionadas com a telefonia. Por exemplo, um telefone IP instalado em uma estação de trabalho com o sistema operacional *Windows* está suscetível às vulnerabilidades do *Windows* [5].

2.2.1 Ameaças

Em meio às várias ameaças à telefonia VoIP e às redes IP, podemos citar as principais delas:

- **Captura de tráfego e acesso indevido a informações**

Nas Redes transmissoras de voz sobre IP, a voz é transportada juntamente com as informações da rede de dados, encapsulado em pacotes IP, e a captura destes pacotes em uma rede IP através de analisadores de pacote (*Sniffers*) é

relativamente trivial [6]. Atualmente, já podemos contar com algumas ferramentas que facilitam este trabalho para o usuário, por exemplo, o VOMIT (*Voice Over Misconfigured Internet Telephones*), que utiliza a ferramenta *tcpdump* do Unix para capturar pacotes de uma conversa telefônica, que está trafegando na rede de dados e consegue remontá-los e convertê-los em um formato comum de áudio (*.wav). Melhor dizendo, trata-se de uma espécie de "grampo telefônico" em plena rede de dados. Apesar desta ferramenta não ter sido criada para este fim, usuários mal intencionados estão aproveitando-se da sua funcionalidade. Esta ferramenta está disponível gratuitamente em [7]. Fazendo uma analogia à telefonia convencional, seria o mesmo que realizar uma escuta telefônica e gravá-la.

Existem outras técnicas, mais ou menos complexas, que fraudulentamente podem ser utilizadas pelos atacantes para obtenção de acesso indevido às informações que trafegam pela rede. Outro exemplo seria o ataque denominado *Caller Identity Spoofing. Nesse tipo de ataque,* o atacante induz um usuário remoto a pensar que ele está conversando com uma pessoa diferente, ou seja, passa-se por outra pessoa para obter informações sigilosas. Este tipo de ataque requer apenas que o atacante obtenha acesso físico à rede e consiga instalar um telefone IP não autorizado.

Políticas preventivas empresariais podem ser uma solução satisfatória quando se pretende evitar ataques deste tipo. A integridade da rede será ainda maior se for possível combinar as políticas com uma boa administração da mesma, por exemplo, sempre obtendo controle de pontos de rede ativos, mas não utilizados.

O preparo dos usuários, bem como o treinamento dos funcionários envolvidos com este tipo de rede, dificultarão a ação dos atacantes em se aplicar engenharia social [6], assim seria mais difícil de induzir alguém acreditar ser o atacante quem ele não é [5].

- **Código Malicioso**

Conforme já visto anteriormente, a tecnologia VoIP está presente nas redes convergentes, ou seja, em redes que trafegam tanto dados, como voz no mesmo

meio físico. Desta forma, a tecnologia VoIP também está susceptível às vulnerabilidades da rede de dados.

Exemplos dessas vulnerabilidades que também podem afetar as redes de voz são os conhecidos vírus, *Trojans* e outros tipos de códigos maliciosos que podem vir a infectar e danificar os sistemas de telefonia IP baseados em PCs (*Personal Computer*), os *Gateways* e outros componentes críticos estruturais. Sendo assim, pode-se concluir que até mesmo ataques e códigos que não surgiram para afetar as redes VoIP, podem causar a paralisação do mesmo [5].

- **Fraude financeira, uso indevido de recursos corporativos**

Outra grande ameaça às redes VoIP é a chamada *Toll Fraud*, ilustrada na Figura 1. Esta ameaça consiste no uso não autorizado dos serviços de telefonia IP ou métodos de fraude para iludir os mecanismos de bilhetagem e cobrança das ligações realizadas.

Existem vários métodos para se aplicar esta técnica. Um deles pode ser o sequestro de um serviço de telefone para realização de chamadas de longa distância que sejam contabilizadas como tendo sido originadas pelo endereço do telefone IP de alguma outra pessoa, a qual seria então responsável até o momento pelos gastos.

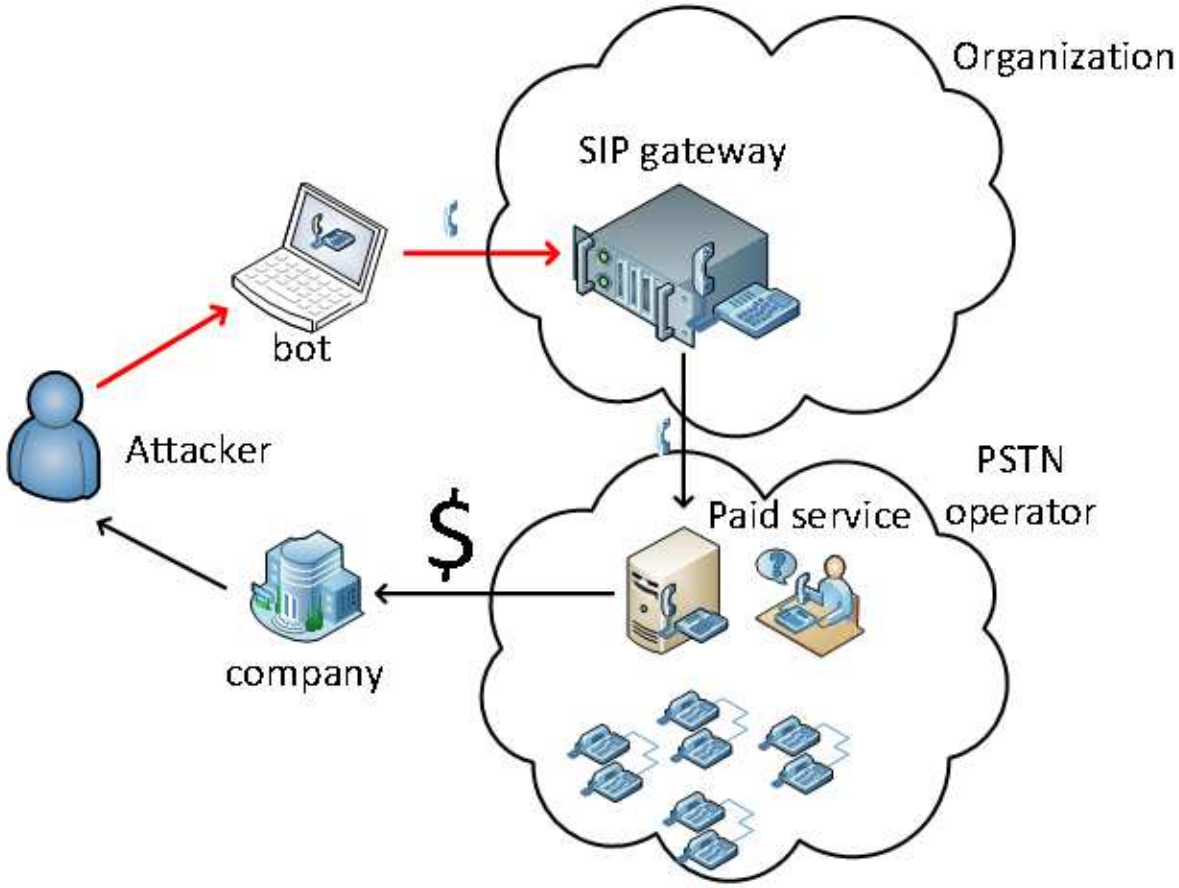

Figura 1. Exemplo de *Toll Fraud.*

- **Indisponibilidade de Serviços**

Em razão do uso de rede de dados para se transportar voz, esta também se torna vulnerável aos ataques não só destinados à própria rede, como também aos destinados à rede TCP/IP. Um exemplo ao qual ela torna-se vulnerável é ao ataque de DoS (*Denial of Service*) ou DDoS (*Distributed Denial of Service*), ilustrado na Figura 2, os quais causam a paralisação dos serviços em redes TCP/IP, sendo assim esta paralisação afetará também os serviços de voz, fax e vídeo atrelados a esse transporte.

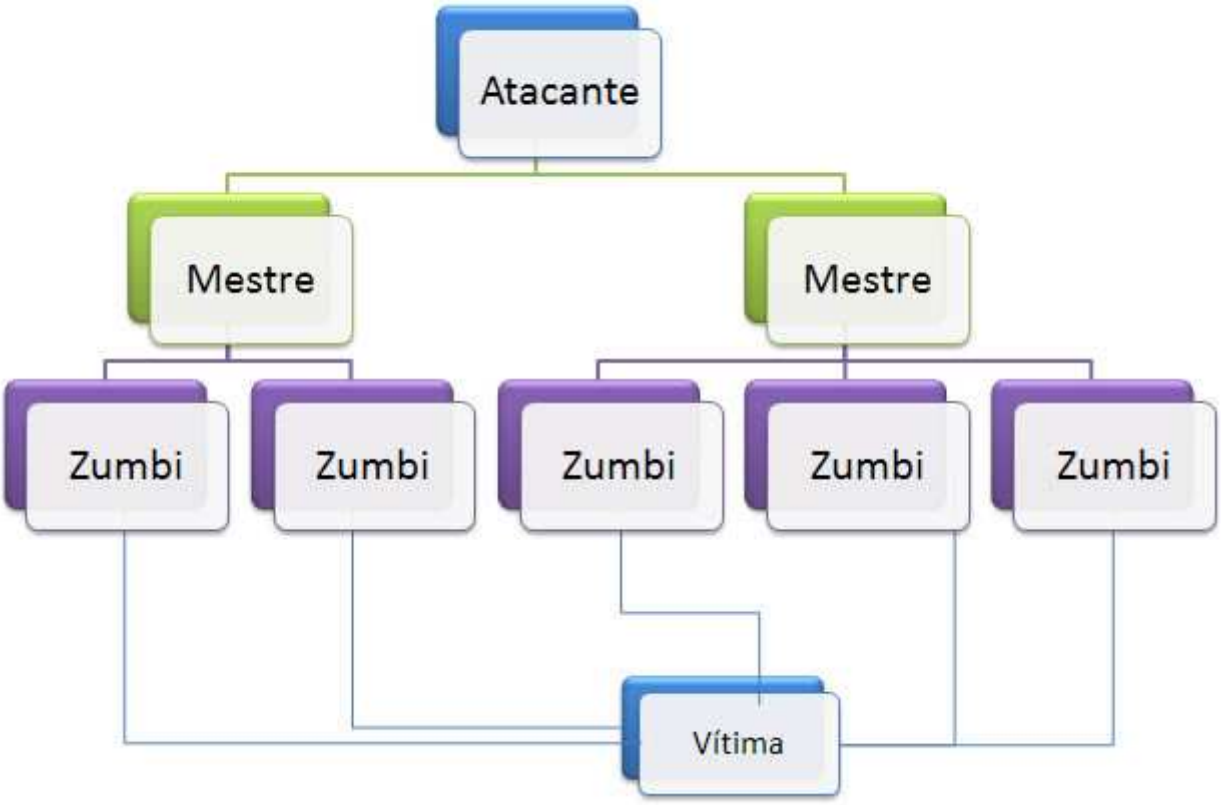

Figura 2. Como funciona um ataque DDoS.

Existem vários os tipos ataques que podem causar negação de serviço em redes TCP/IP, entre eles podemos citar o *TCP SYN Flood[8]*[2] e suas variações, e também a exploração de falhas nas pilhas de protocolo dos sistemas operacionais, como no *Ping of Death[8]*[3], *LAND[8]*[4], *Teardrop[8]*[5], dentre outros ataques que podem ocasionar paralisação dos serviços do VoIP.

[2] Ataque de negação de serviço em que um invasor envia uma sucessão de solicitações SYN para o sistema de destino.

[3] Tipo de ataque que envolve o envio de um grande pacote de *ping* para uma máquina destino.

[4] Ataque de negação de serviço que consiste em enviar um pacote falso para um computador, fazendo com que ele se comporte de forma indesejada.

[5] Envolve o envio de fragmentos IP com cargas superdimensionadas e sobrepostas para o computador de destino.

Nas redes VoIP, os equipamentos de PABX (*Private Automatic Branch Exchange*) [9] tradicionais são trocados por aplicações PABX IP-compatíveis que são executadas, por exemplo, em servidores *Windows* 10. Estas aplicações de *Call Management* são críticas para a infraestrutura de VoIP, e, no entanto estão sujeitas aos ataques que exploram vulnerabilidades não só das próprias aplicações como também do sistema operacional [5].

2.2.2 Formas de Proteção

A seguir são apresentadas algumas práticas para implantação de uma estrutura VoIP segura a fim de evitar problemas, como os descritos na Subseção 2.2.1:

- **Dividir o tráfego de voz e dados**

O fracionamento do tráfego de voz e dados pode ser feito utilizando *Switches*. Um exemplo de *Switch* usado como proposta para desenvolvimento de uma rede VoIP deste projeto será mostrado no Capítulo 5 deste trabalho. Estas segmentações contribuem para obtenção de uma melhor qualidade de serviço (QoS) e servem para reencaminhar pacotes entre os diversos nós da rede, além de facilitar a gerência da rede de voz e simplificar sua manutenção. Ainda podemos com isso evitar que a segmentação da voz seja alvo de ataques de captura não autorizada do tráfego de conversas telefônicas que trafegam nas redes encapsuladas em pacotes IP (*eavesdropping*), realizados com técnicas de *sniffer* com o uso, por exemplo, do VOMIT e outras ferramentas semelhantes, conforme abordados na Subseção 2.2.1.

Com a implementação desta segmentação, outros ataques ficam impossibilitados para a rede de voz, como por exemplo, os ataques baseados em TCP/IP (como o ataque DDoS, visto na Subseção 2.2.1) que, mesmo destinados a outros alvos não relacionados diretamente com a infraestrutura de VoIP, podem tornar estes serviços indisponíveis caso todo o tráfego esteja no mesmo segmento.

Para um aprimoramento em vários aspectos citados da rede de voz, recomenda-se a separação dos segmentos de rede de voz e dados em redes locais virtuais (VLANs) distintas. Na proposta deste projeto, por tratar-se de uma instalação

de pequeno porte, uma VLAN dedicada ao tráfego de voz seria suficiente, onde seriam instalados os equipamentos responsáveis pelo gerenciamento de chamadas (*Call Manager*) e os telefones IP. Outros componentes como estações de gerenciamento e sistemas de *Voice/Mail* podem residir no segmento de dados. Já para empresas e estabelecimentos de grande porte, várias VLANs podem ser criadas, tanto para voz quanto para dados. Por exemplo, os serviços de *Voice/Mail* podem ocupar uma VLAN dedicada [5]. No Capítulo 5, serão apresentados os equipamentos necessários para a proposta deste projeto.

- **Controlar os acessos com um *firewall* especializado**

O uso de um *firewall* especializado servirá para controlar o acesso ao segmento de rede onde está instalado o *Call Manager.* Este tem como objetivo, filtrar todo o tipo de tráfego que seja endereçado à rede de voz e não seja necessário para o funcionamento destes serviços. O *firewall* irá proteger o *Call Manager* de acessos indevidos por parte de telefones IP não autorizados que sejam instalados em outros segmentos.

Portanto, as portas e protocolos que serão configuradas para liberação ou bloqueio no *firewall* irão depender do tipo de solução/fabricante dos equipamentos VoIP usados.

- **Utilizar preferencialmente telefones IP que suportem VLAN.**

Não é aconselhável a utilização de *softwares* que fazem simulações de telefones (*SoftPhones)*, convém utilizar telefones IP que suportem VLANs, uma vez que os *SoftPhones* estão sujeitos a um maior número de ataques que os aparelhos de telefonia IP baseados em *hardware*.

Além da possibilidade de falhas em seu próprio código, as aplicações de telefone IP para PCs estão sujeitas às vulnerabilidades do sistema operacional e também de outras aplicações residentes no computador onde estão instaladas, como vírus e outros códigos maliciosos.

Já os telefones IP executam sistemas operacionais próprios com serviços limitados, sendo assim, menos vulneráveis. Além disso, os *SoftPhones* precisam

residir no segmento de dados da rede, portanto eles estão expostos a ataques de negação de serviços, como *floods* baseados em UDP (*User Datagram Protocol*) ou TCP, que sejam destinados ao segmento como um todo, e não apenas ao computador em que estão instalados [5].

- **Usar endereços IP privativos e inválidos nos telefones IP**

Nos telefones IP é preferível utilizar endereços IP inválidos. Esta medida servirá para reduzir a possibilidade de que o tráfego de voz possa ser monitorado de fora da rede interna e para evitar que os atacantes consigam mapear o segmento de voz em busca de vulnerabilidades. Além disto, o uso de IPs inválidos acarretará em menores custos.

- **Configurar os telefones IP com endereços IP estáticos, associados ao endereço MAC (*Media Access Control*).**

A utilização do endereço MAC permite a autenticação dos telefones IP, ou seja, quando um telefone IP tenta obter configurações da rede do *Call Manager*, seu endereço Mac pode ser verificado em uma lista de controle de acesso. Caso o endereço seja desconhecido, o dispositivo não será aceito e não receberá a configuração solicitada.

Se possível, preferencial, deve-se aplicar endereços IP estáticos para os telefones IP, e associa-los ao endereço MAC do dispositivo. Sendo assim, cada telefone IP terá sempre o mesmo endereço IP associado ao endereço MAC. Desta forma, para conseguir instalar um telefone IP não autorizado na rede, um atacante teria que forjar tanto um endereço IP válido para o segmento de voz quanto o endereço MAC a ele associado, dificultando assim a sua ação.

Alguns aspectos devem ser considerados antes de tal aplicação, pois, dependendo das características do ambiente da implantação, a associação entre endereço IP estático e endereço MAC nos telefones IP pode ser de difícil gerenciamento [5]. A estrutura do endereço MAC é ilustrada na Figura 3.

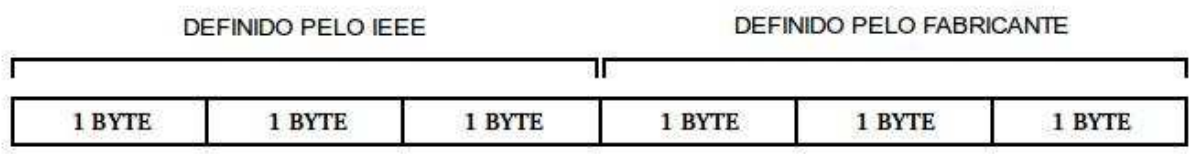

Figura 3. Estrutura do Endereço MAC [10].

Existe uma padronização dos endereços MAC administrada pela IEEE (*Institute of Electrical and Electronics Engineers*) que define que os três primeiros *bytes, conforme* Figura 3, e são destinados à identificação do fabricante. Eles são fornecidos pela própria IEEE. Os três últimos bytes são definidos pelo fabricante, sendo este responsável pelo controle da numeração de cada placa que produz. Apesar de ser único e gravado em *hardware*, o endereço MAC pode ser alterado através de técnicas específicas. [10]

- **Usar servidores DHCP (*Dynamic Host Configuration Protocol*) distintos para Voz e Dados.**

É aconselhado, utilizar servidores DHCP distintos para os segmentos de voz e dados. Sendo assim, os ataques de negação de serviços, como por exemplo, os ataques DDoS, e outros lançados contra o servidor DHCP em na parte de dados não irão influenciar com a alocação de endereços IP para os telefones no segmento de voz, e vice-versa, o que aumenta a estabilidade da rede [5].

- **Criar mecanismos que permitam a autenticação dos usuários**

Convém implementar os recursos de autenticação dos usuários dos telefones IP, além de autenticar apenas os dispositivos através de seus endereços MAC.

Atualmente, existem diversos modelos de telefones com tecnologia VoIP que exigem *login* por parte do usuário e uma senha ou PIN (*Personal Identification Number*) válidos para que possam utilizar o dispositivo e ter acesso ao sistema. Este tipo de autenticação reduz os riscos de uso indevido dos recursos da rede de voz, e permite maior rastreabilidade no uso dos serviços, além de certo nível de não repúdio [5].

- **Implementar um sistema de detecção de intrusão**

Detecção de assinaturas envolve a procura em trafego de rede de *bytes* ou sequencias de pacotes conhecidos como maliciosos. Uma vantagem chave desse método é que assinaturas são fáceis de serem desenvolvidas e entendidas se sabida o comportamento da rede que se esta tentando identificar. Os eventos gerados por um IDS (*Intrusion Detection System*) baseado em assinaturas podem comunicar o que causou o alerta. [11]

Desta forma, convém que uma aplicação de IDS seja instalada no segmento onde estiver instalado o *Call Manager*, visando à detecção de ataques originados principalmente no segmento de dados, onde estão localizadas as estações de trabalho dos usuários [5].

- **Fazer o *hardening* do local onde está instalado o *call manager***

Hardening é um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas, com foco na infraestrutura e objetivo principal de torná-la preparada para enfrentar tentativas de ataque. [12]

Normalmente, o processo inclui remover ou desabilitar nomes ou *logins* de usuários que não estejam mais em uso, além de serviços desnecessários.

Outras providências que um processo de *hardening* pode incluir: limitar o *software* instalado àquele que se destina à função desejada do sistema; aplicar e manter os *patches* atualizados, tanto de sistema operacional quanto de aplicações; revisar e modificar as permissões dos sistemas de arquivos, em especial no que diz respeito à escrita e execução; reforçar a segurança do *login*, impondo uma política de senhas fortes, dentre outras.

Quem ataca a rede, costuma explorar as vulnerabilidades do *Call Manager* da infraestrutura de VoIP, devido ao grande quantidade de serviços que podem estar sendo oferecidos por estas aplicações.

O *Call Manager*, por exemplo, costuma disponibilizar aplicações para controle de chamadas, permite a configuração via *Web*, dá suporte a serviços de localização

de telefones (*IP Phone browsing*), conferência e gerenciamento remoto por SNMP(*Simple Network Management Protocol*).

Por este motivo, convém que sejam implementados procedimentos para a configuração segura (*Hardening*) do servidor onde está localizado o *Call Manager*. [5]

- **Monitorar o desempenho e status dos servidores de VoIP**

O objetivo deste controle é permitir a monitoração periódica, se possível em tempo real, de diversos fatores tais como perda de pacote, tempo de viagem ida e volta (RTT), e variação de atraso de pacotes que possam comprometer o desempenho ou disponibilidade dos serviços. A monitoração pode ser feita através de soluções proprietárias disponibilizadas pelos próprios fabricantes dos equipamentos (Cisco, etc), ou de soluções de mercado como o PRTG (*Paessler Router Traffic Grapher*) [5] [13].

- **Restringir o acesso físico a rede**

O acesso físico à rede deve ser restrito, isto devido à possibilidade de alguém mal intencionado conseguir acesso físico indevido a rede e conseguir tirar proveitos disto. Com acesso à rede física o atacante pode, por exemplo, instalar um telefone IP não autorizado e utilizar técnicas de *MAC Spoofing* [14] e *Caller Identity Spoofing* [15] para mascarar os pacotes IP e enganar os usuários, fazendo-os pensar que estão conversando com alguma outra pessoa, quando na verdade estão conversando com o invasor. Desta forma informações sigilosas poderão ser obtidas através de engenharia social. Um exemplo de *Spoofing* é ilustrado na Figura 4.

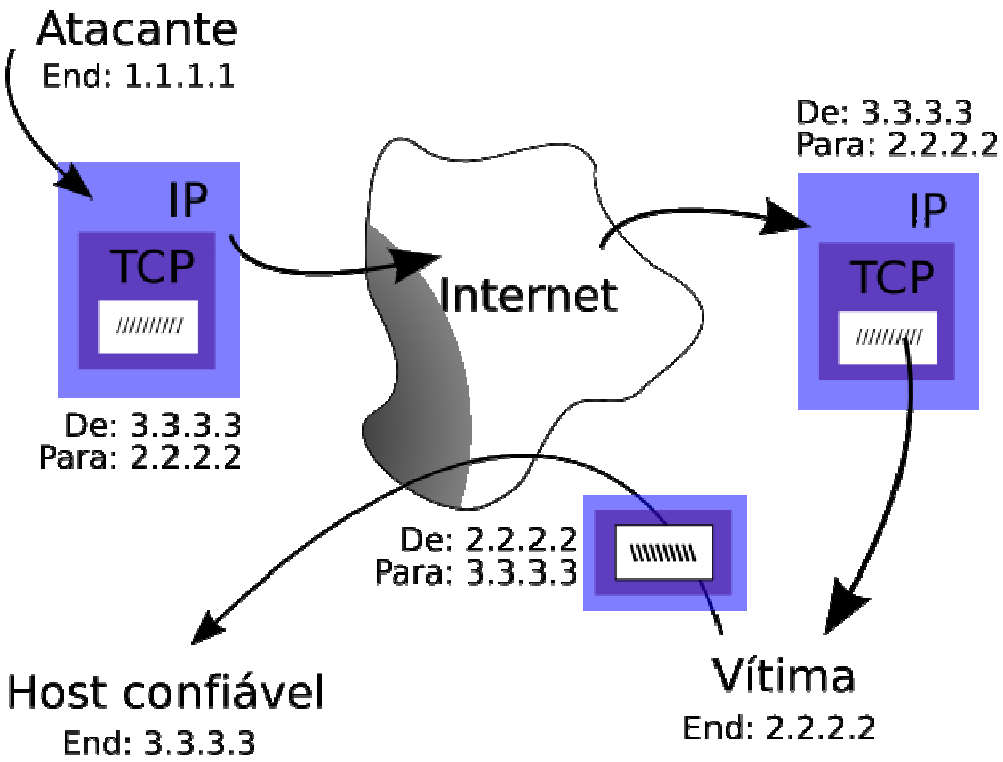

Figura 4. Falsificação de um pacote (*Spoofing*).

Consequentemente, o acesso físico indevido também expõe os componentes da infraestrutura de VoIP a ameaças como fraudes, roubo, sabotagem ou dano acidental ou proposital dos equipamentos, podendo causar a indisponibilidade dos serviços. Por estes motivos, convém que o acesso físico aos dispositivos mais críticos da rede (*Switches*, Roteadores, *Call Manager*, *Firewalls*, etc), seja restrito apenas a usuários autorizados [5].

- **Auditar o uso de recursos**

Convém auditar regularmente a verificação da qualidade de serviço prestada pelos equipamentos VoIP, bem como sua utilização pelos usuários da rede. Para isso devem-se manter registros das informações sobre as sessões (data e horário do início e término, duração, origem, destino, etc) além de informações relacionadas à QoS (latência, perda de pacotes, uso de banda, etc). A auditoria pode ser implementada através de aplicações especializadas. Algumas dessas aplicações podem ser encontradas em [16].

Para uma auditoria mais precisa, é recomendado que os usuários do sistema utilizem algum tipo de autenticação ao utilizar os serviços da rede de voz [5].

- **Criptografar o tráfego de VoIP**

É aconselhada a criptografia de todo o tráfego de pacotes entre o telefone IP e o *Call Manager*. Esta medida tem como objetivo impedir o uso de ferramentas como o VOMIT que pode ser utilizados para violar a confidencialidade das conversações. Um exemplo de criptografia que pode ser utilizada para tal ambiente seria a implantação de um túnel IPSec[6] entre as estações com telefones IP e o *Call Manager*. Para as comunicações externas (matriz com outras filiais, por exemplo), deve-se considerar a implementação de uma VPN (*Virtual Private Network*) para criptografar o tráfego de VoIP [5].

A criptografia pode ser feita através de *Softwares* específicos. No entanto, para que uma chamada seja garantida, tanto os clientes de envio, quanto os de recebimento devem ter o *software* instalado. Também poderá ser feito o uso de procolos de segurança nas chamadas, como o TLS (Transport Layer Security), ou o SRTP (*Secure Real-time Transport Protocol*), que já possuem criptografia interna.

2.2.3 Resumo do Capítulo

Conforme visto anteriormente, a tecnologia VoIP tem uma série de benefícios quando comparada à tecnologia convencional de telefonia. O fato de esta tecnologia trabalhar com comutação de pacotes, ao invés de comutação de circuitos, traz uma série de benefícios. Foi verificado também neste capítulo que a segurança para os serviços VoIP é motivo de preocupação. Foram mostradas as ameaças existentes e as melhores práticas para contê-las.

[6] Extensão do protocolo IP que visa ao fornecimento de privacidade ao usuário.

Capítulo 3

Os Protocolos VoIP

3.1 Estrutura do VoIP

O uso da tecnologia VoIP proporciona uma série de possibilidades para os usuários do serviço, conforme Figura 5:

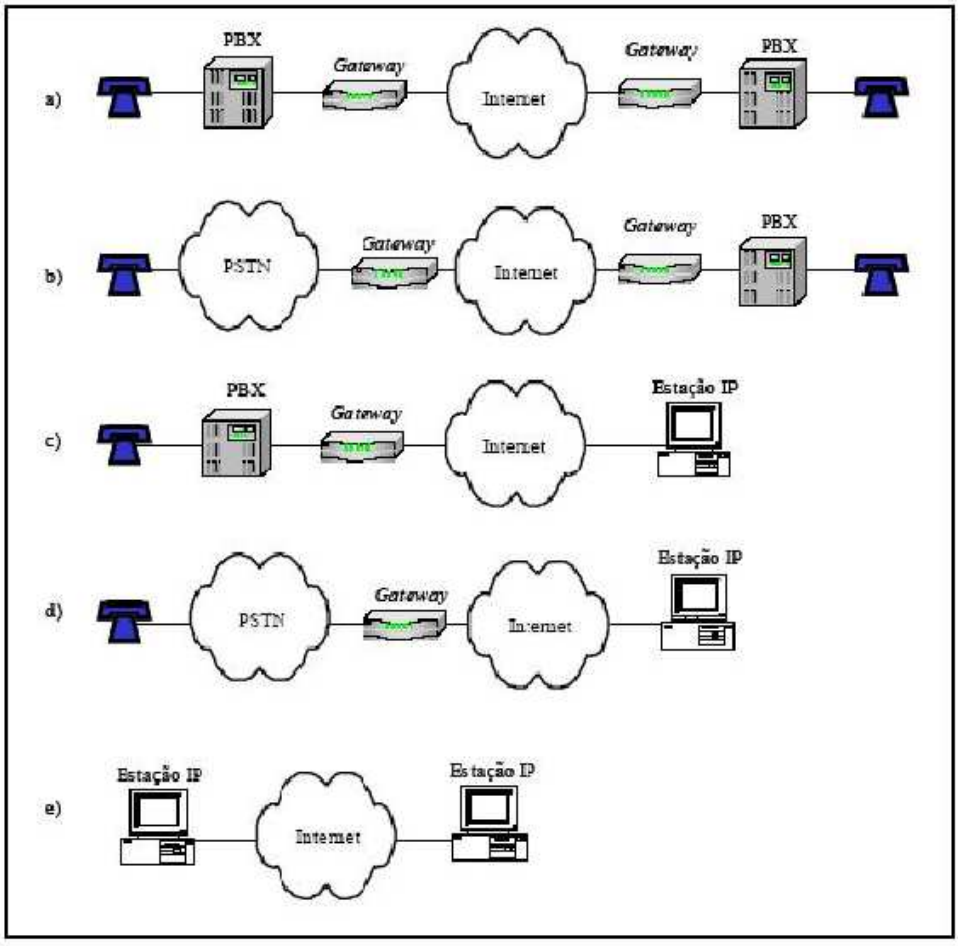

Figura 5. Cenários do serviço VoIP.

VoIP é uma arquitetura em quatro níveis, definida por várias organizações em seus respectivos padrões, que identifica as interfaces que existem entre cada nível:

- Nível de Aspecto de Serviço – A responsabilidade desse nível envolve todos os aspectos do serviço VoIP, que inclui a segurança da cobrança e a codificação da fala em pacotes digitais.
- Nível de Sessão – Esse nível ajuda o VoIP a estabelecer uma chamada e realizar o registro quando o terminal é conectado à rede no início de uma ligação.
- Nível de Transporte – Responsável pela remessa de mensagens de ponta a ponta.
- Nível de Rede – Nível em que os serviços de roteamento são executados, por exemplo, a transferência do pacote IP.

A tecnologia VoIP utiliza o protocolo IP para a transmissão de dados através de pacotes em redes IP. Assim, o VoIP consegue alcançar redes *Internet*, *Intranets* e *Lans*. O sinal de voz (analógico) é digitalizado, sofre compressão e é transformado em pacotes IP que são transmitidos na Rede. Para que esse processo aconteça, são utilizados diversos padrões sendo os mais destacados o H.323 e o SIP, que veremos com mais detalhes nas seções seguintes deste trabalho. Na Figura 6 é possível analisar detalhadamente os níveis do VoIP.

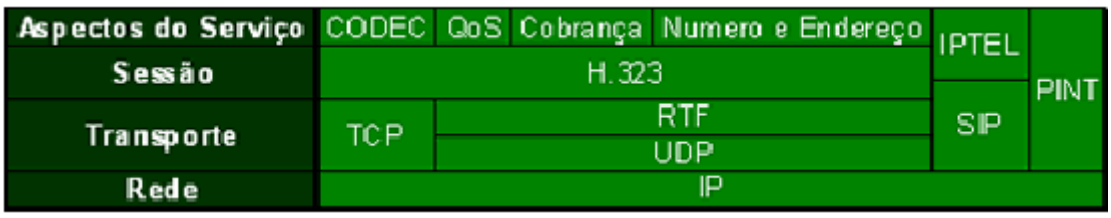

Figura 6. Arquitetura dos níveis do VoIP.

3.2 Protocolo H.323

H.323 é o conjunto de protocolos e especificações elaborados pela ITU-T (União Internacional de Telecomunicações – Setor de Padronização), pertencente à série H que trata da comunicação em tempo real de áudio, vídeo e dados sobre a rede IP, criada em 1996, pode ser visualizado em [17]. As recomendações H.323 têm como objetivo especificar um sistema de comunicações multimídia em redes baseadas em pacotes, porém não objetivam uma Qualidade de Serviço (QoS). Também estabelece padrões de codificação e decodificação no fluxo de dados audiovisuais que se baseiam no padrão H.323. Na Tabela 2 é descrito os principais protocolos deste padrão.

Protocolo	Descrição
H.323	Responsável pelas especificações do sistema.
H.225.0	Exerce funções de controle de chamada (RAS), estabelecimento de chamada e sincronização dos dados.
H.235	Protocolo de segurança (autenticação, integridade, privacidade, etc.).
H.245	Responsável pela comunicação das capacidades dos terminais.
H.450	Responsável por serviços suplementares (p. ex. chamada em espera, transferência de chamadas, etc.).

Tabela 2. Principais Protocolos do modelo H.323.

Esse modelo usa conceitos de ambos os protocolos, tanto o tradicional PSTN (*Public Switched Telephone Network*) quanto as normas relacionadas com a *Internet*. Tratando tanto de comutação de circuitos quanto de comutação de pacotes e padrões de protocolo, o H.323 é capaz de se integrar harmoniosamente com o PSTN, que são responsáveis por prover o serviço de telefonia convencional, enquanto ao mesmo tempo envia comunicações multimídia sobre meios como a *Internet* (VoIP).

O H.323 pode ser utilizado em qualquer tipo de rede (*ethernet*, *fast ethernet*, dentre outras) ou em qualquer topologia (ponto a ponto ou redes interconectadas).

Apesar de especificar padrões de vídeo e dados em comunicações multimídia, apenas o suporte a áudio é obrigatório. Isso quer dizer que, quando utilizado, o Padrão H.323 cria pacotes envolvendo somente áudio (telefonia IP), áudio e vídeo (videoconferência), áudio e dados ou os três tipos de comunicações.

Os benefícios da adoção do padrão H.323 são:

- Independência da Rede – O protocolo H.323 permite a utilização de aplicações de áudio sem alterações na estrutura da rede. Assim, à medida que os limites de velocidade na *Internet* evoluem, os benefícios da utilização destas aplicações são imediatamente incorporados.

- Interoperabilidade de Equipamentos e Aplicações – Permite interoperabilidade entre os mais diversos fabricantes e as diversas aplicações.

- Independência de Plataforma – Não especifica o Sistema Operacional utilizado podendo abranger diversos segmentos como: videoconferência em PCs, telefones IP, televisão a Cabo, entre outros.

- Representação Padronizada de Mídia – O protocolo H.323 estabelece codificações para compressão e descompressão dos sinais de áudio e vídeo normalmente executadas pelo sistema.

As desvantagens são: o Protocolo H.323 é muito complexo sendo de difícil configuração; utiliza representação binária para mensagens, tornando configurações mais difíceis. Possui centenas de elementos.

Conforme visto em [18], os componentes especificados pelo padrão H.323 são destacados a seguir e ilustrados na Figura 7. É importante ressaltar que, em uma implementação prática do H.323, todos esses componentes podem coexistir em um mesmo equipamento.

- Terminais – são os dispositivos com os quais os usuários interagem na comunicação (Telefones, *softphones*, etc.).

- *Gateways* – É um elemento opcional na intraestrutura da rede sobre IP que tem a função de negociar a sinalização e o transporte da mídia, servindo como interface entre terminais e outros tipos de rede. Para isso, um *gateway* provê uma série de funções, dentre as quais se destaca a conversão do formato de codificação de mídias e a tradução dos procedimentos de estabelecimento e encerramento de chamadas.

- *MultiPoint Control Units* (MCUs) – Controla a conferência entre três ou mais terminais. Manipula as negociações entre os mesmos para determinar capacidades comuns de processamento de áudio e vídeo.

- *Multipoint Processors* (MPs) – Os MPs têm a capacidade de mesclar, chavear e processar os bits de áudio, vídeos e/ou dados.

- *Gatekeepers* – Sua principal função é traduzir os endereços dos nomes simbólicos em endereços IP na infraestrutura da rede do H.323. Adicionalmente gerencia serviços e recursos da rede prestados aos terminais (Controle de banda, gerenciamento da zona de controle de admissão do H.323) É ao mesmo tempo um equipamento de mídia e de sinalização.

- Elementos de borda – frequentemente são colocados juntos a um *gatekeeper* trocando informação de endereçamento e participam na autorização da chamada entre domínios administrativos. Podem agregar a informação de endereço para reduzir o volume de informação de roteamento trafegado na rede. Os elementos da borda podem ajudar na autorização ou autenticação da chamada diretamente entre dois domínios administrativos.

Figura 7. Componentes do H.323.

Os padrões para protocolos referenciados na recomendação H.323 constituem uma pilha organizada, como é mostrada na Figura 8:

<table>
<tr><td>Vídeo</td><td>Audio</td><td colspan="4">Controle</td><td>Dados</td></tr>
<tr><td>H.26x</td><td>G.7xx</td><td rowspan="2">RTPC</td><td rowspan="2">H.225.0
(RAS)</td><td rowspan="2">H.225.0 - Q.931
(Sinalização de
Chamadas)</td><td rowspan="2">H.245
(Controle de
Chamadas)</td><td rowspan="2">T.120</td></tr>
<tr><td colspan="2">RTP</td></tr>
<tr><td colspan="4">UDP</td><td colspan="3">TCP</td></tr>
<tr><td colspan="7">IP</td></tr>
<tr><td colspan="7">Protocolo da camada física</td></tr>
</table>

Figura 8. Pilha de protocolos H.323.

O H.323 já foi um importante protocolo para telefonia IP, porém, vem perdendo espaço para o protocolo SIP que é mais moderno e menos complexo, que será descrito na Seção 3.3.

3.3 Protocolo SIP

O SIP, como o H.323, também é um protocolo de padronização de videoconferência, telefonia e mensagens instantâneas. O protocolo foi criado em 1999, e foi desenvolvido para ser mais simples que seus antecessores e vem ganhando espaço em aplicativos que utilizam Voz sobre IP. O SIP foi desenvolvido como parte da *Internet Multimedia Conferencing Architecture,* pela IETF (*Internet Engineering Task Force*) definido no RFC (*Request for Comments*) 3261, que pode ser visto em [19], e foi projetado para oferecer suporte para outros protocolos da Internet como TCP, UDP, TLS, SCTP (*Stream Control Transmission Protocol*), dentre outros. Por esse motivo oferece grande estabilidade e flexibilidade e assemelha-se muito com o conhecido protocolo HTTP (*Hypertext Transfer Protocol*). Por ter representação textual (vantajoso em relação à representação binária do protocolo H.323), tem sido visto como protocolo predominante na tecnologia VoIP. Um exemplo de seu funcionamento é ilustrado na Figura 9.

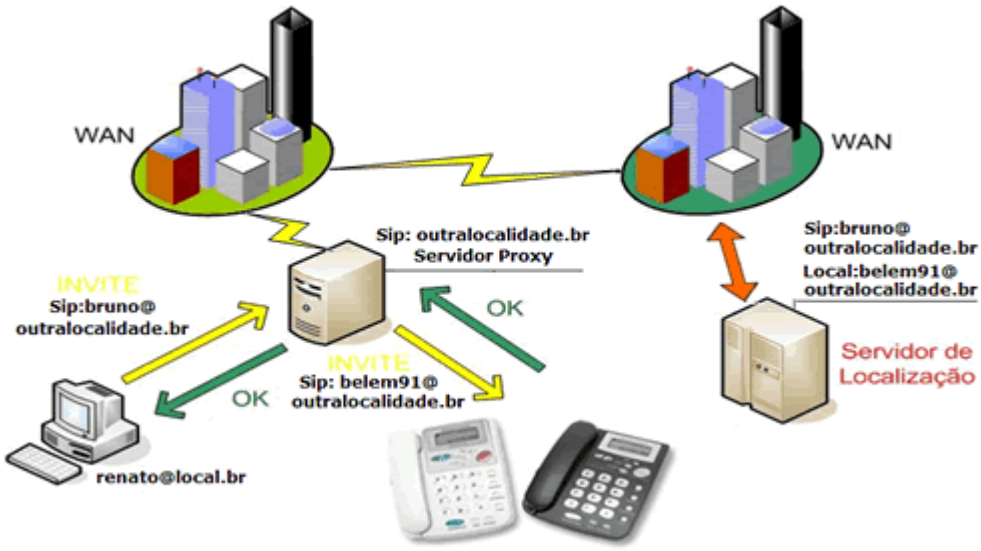

Figura 9. Funcionamento do protocolo SIP [20].

Algumas das características da aplicação SIP são:

- Oferece recursos de controle de chamada, como: espera, encaminhamento, transferência, mudanças de mídia etc.
- Aceita infraestrutura da *Web*, por exemplo, segurança, cookies.

- É orientado para *Web* e independe do protocolo de rede.
- Pode oferecer notificação de evento e "listas de companheiros".
- Pode envolver diversos servidores e clientes.
- Utiliza como suporte para as suas mensagens os pacotes UDP da rede IP

A especificação do SIP define os componentes da arquitetura de sinalização como clientes e servidores:

- Agente usuário – Formado por uma parte cliente com a finalidade de iniciar requisições SIP, e a outra parte como servidor, com a finalidade de receber e responder as requisições. Pode está integrado a um terminal IP ou um s*oftphone*.
- Servidores Proxy – Servidor de procuração é uma entidade intermediária que atua tanto como servidor ou cliente. No modo cliente, tem o propósito de fazer as requisições por outros clientes. o modo servidor, um *proxy* tem como função principal o roteamento, fazendo com que a requisição seja enviada para outra entidade mais próxima do dispositivo final. Os servidores *proxy* também servem, por exemplo, para verificar se determinado usuário tem direitos de estabelecer uma chamada, ou ainda, pode reescrever partes específicas da mensagem de requisição antes de repassá-la adiante.
- Servidor de redirecionamento – mapeia um endereço em zero ou mais novos endereços associados a um cliente e redireciona as requisições SIP para um usuário que está fora do seu domínio.
- Servidor de registro – Servidor encarregado por fazer autenticação e registro dos usuários conectados, trabalhando em conjunto com o servidor de redirecionamento e o servidor proxy. Neste servidor fica armazenado o ID (identificador) do usuário e os dispositivos utilizados na comunicação.

- Servidor de Localização – Mantém um banco de dados com o registro dos usuários e suas localizações e é utilizado por outros servidores para obter informações sobre a possível localização do destino requisitado.

O SIP não descreve como uma configuração deve ser gerenciada, ao invés disso, ele usa um servidor central para gerenciar o estado da conferência e do participante. Ele pode convidar usuários para conferências, transportando as informações necessárias.

Como visto anteriormente, o SIP vem ganhando espaço sobre H.323 na telefonia IP. Apesar de terem finalidades parecidas, o protocolo H.323 é um protocolo robusto que foi inicialmente desenvolvido para aplicações multimídias em LANs (*Local Area Network*), diferentemente do SIP, que é um protocolo simples e eficiente, baseado nos protocolos HTTP e SMTP (*Simple Mail Transfer Protocol*) da *Internet*. Na Tabela 3 é apresentado um breve comparativo entre os dois protocolos:

Assunto	H.323	SIP
Desenvolvedores	ITU-T	IETF
Compatibilidade com RTCP	Grande	Maior
Compatibilidade com Internet	Não	Sim
Sinalização	Sim	Sim
Formato mensagem	Binário	ASCII
Transporte de mídia	RTP/RTCP	RTP/RTCP
Conferências multimídia	Sim	Não
Chamadas multiparticipante	Sim	Sim
Endereçamento	Máquina ou nº. do telefone	URL
Terminação da chamada	Explicita ou por terminação TCP	Explicita ou por timeout
Criptografia	Sim	Sim
Rede no mundo	Disponível Universalmente	Em expansão

Tabela 3. Comparação dos protocolos H.323 e SIP.

Resumindo, o H.323 é um padrão muito poderoso, porém complexo demais para ser utilizado em telefonia IP. Uma vez que a tecnologia VoIP visa uma redução

dos custos, o H.323 torna-se uma solução mais complicada, pois exige um grande esforço de implementação, diferente do SIP que é um protocolo simples, confiável e desenvolvido para a *Internet*, ideal para telefonia IP. O fator decisivo para o SIP substituir o H.323 não está na qualidade e sim na simplicidade.

3.4 Protocolos de Transporte

Aplicações usuais de Internet usam TCP/IP, enquanto VoIP usa RTP/UDP/IP. O TCP é um protocolo confiável que utiliza confirmações e retransmissões para assegurar que os pacotes foram recebidos. O TCP tem a característica de ajustar a taxa de transmissão, que aumenta quando a rede está descongestionada, mas diminui rapidamente quando o host originador não recebe uma confirmação positiva do host destino. Logo o TCP não é um protocolo adaptável a aplicações em tempo real como a transmissão de voz, porque a necessidade de confirmação e retransmissão leva a um atraso excessivo. O UDP provê um serviço de entrega não confiável utilizando o IP para transportar suas mensagens entre dois pontos na Internet.

Por não ser um protocolo completamente confiável, a tecnologia VoIP faz uso de algumas técnicas de QoS, como por exemplo, as que serão exploradas no Capítulo 4 deste trabalho, a fim de minimizar os seus problemas.

3.4.1 RTP

O RTP é um protocolo de transporte, da camada de aplicação, que tem como objetivo transportar informações multimídias, que ficam contidas em seus cabeçalhos, para o receptor.

O RTP roda comumente sobre o UDP. O lado remetente encapsula uma porção de mídia dentro de um pacote RTP, em seguida, encapsula um pacote em um segmento UDP, e então passa o segmento para o IP. O lado receptor extrai o pacote RTP do segmento UDP, em seguida extrai a porção de mídia do pacote RTP e então passa a porção para o transdutor para decodificação e apresentação. [21]

Este protocolo está sendo altamente utilizado, e isto permite uma maior interoperabilidade entre as aplicações multimídias.

O RTP não reserva recursos de rede e nem garante qualidade de serviço para tempo real. O transporte dos dados é incrementado através do RTCP (protocolo de controle) que monitora a entrega dos dados e provê funções mínimas de controle e identificação.

3.4.2 RTCP

O RTCP, também desenvolvido pelo IETF, pode ser usado em conjunto com o RTP, porém eles diferem um do outro pelo uso de diferentes números de portas.

Sua principal função é transmitir periodicamente pacotes de controle, contendo informações estatísticas, para os participantes com o objetivo de monitorar a qualidade de serviço e transportar informações úteis de tais participantes. Os pacotes RTCP contêm informações que representam estatísticas que podem ser úteis para a aplicação. Estas estatísticas incluem o número de pacotes perdidos e o *jitter*.

O RTCP executa as seguintes funções:

- Provê o *feedback* da qualidade da distribuição de dados;
- Controla a taxa para que o RTP seja escalável para um grande número de participantes;
- Transporta o mínimo de informações de controle de sessão.

A Figura 10 demonstra o encapsulamento dos pacotes UDP pelo cabeçalho RTP. Ao serem transmitidos pela rede estes pacotes chegam até seu destino. A partir de então algumas informações de controle podem ser enviadas para o receptor através do protocolo RTCP.

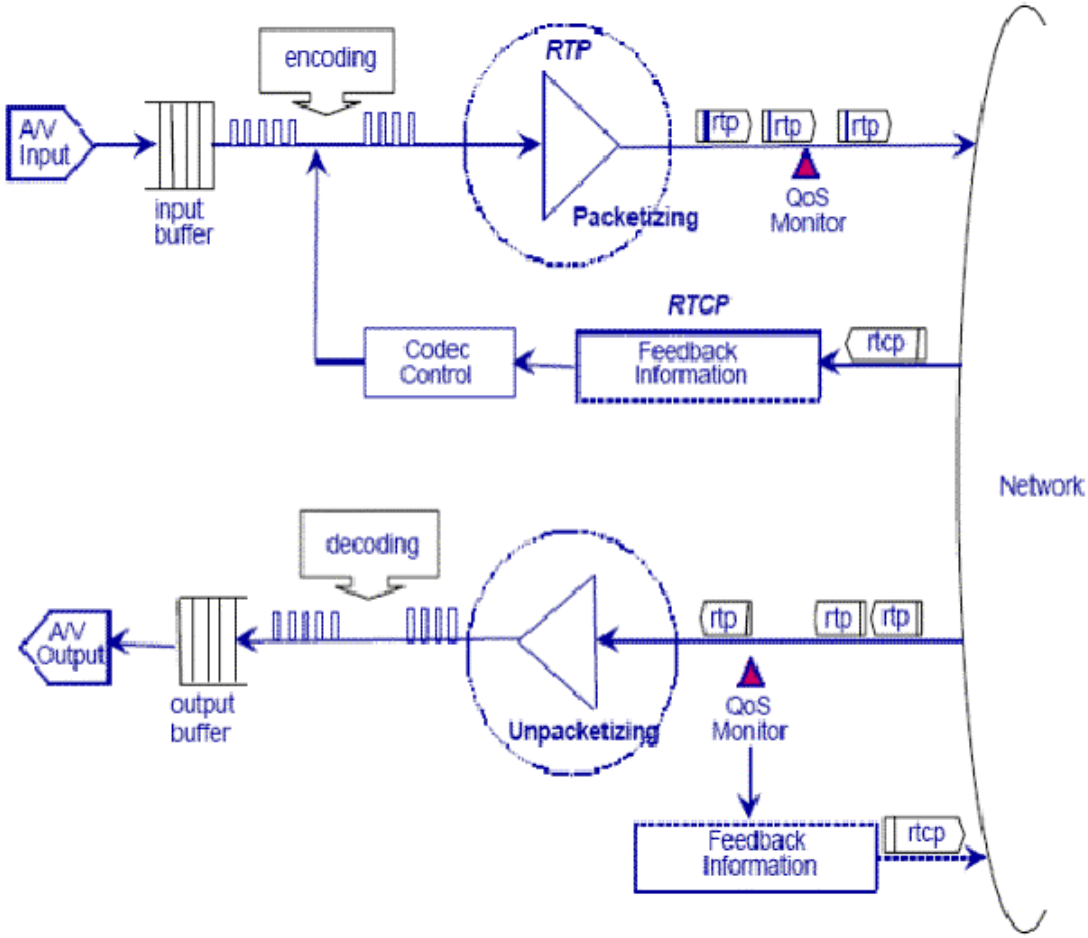

Figura 10. Encapsulação dos pacotes UDP [22].

Capítulo 4
Qualidade de Serviço – QoS

4.1 Definição

Segundo Monks [23], QoS (Qualidade de Serviço) é uma medida coletiva de nível de serviço apresentado ao usuário. Pode ser considerado como sendo o nível de confiança na rede por determinada aplicação para atingir os requisitos necessários para o seu funcionamento. O uso de QoS para serviços VoIP é um fator fundamental para garantia de qualidade dos dados.

A condução de dados VoIP, utilizando como base a *rede Internet* comercial, nos mostra com o conhecimento, que os pacotes IP com os dados de voz, ao incidirem por diversos domínios e roteadores, comumente não têm mais condições de apresentar uma qualidade de voz admissível no destino. Uma das razões é que os parâmetros de QoS estabelecidos para este serviço, relativos ao atraso e à variação deste atraso, não podem ser garantidos pela *Internet* comercial. O volume de dados produzidos por uma aplicação VoIP é outro desafio para a rede TCP/IP, fazendo com que a sua aplicação, muitas vezes, se reduza a redes corporativas privadas, nas quais é relativamente simples e pouco dispendiosa a disponibilização de amplos recursos em termos de banda passante.

O objetivo ao se utilizar metodologias de QoS é oferecer uma boa garantia de performance no fluxo de dados (incluindo voz), mesmo em períodos que a rede esteja em condições desfavoráveis. Redes que estejam passando por ameaças, como as descritas no Capítulo 2 deste documento, podem, ainda assim apresentar uma excelente qualidade no fluxo de dados, se utilizados artifícios de QoS apropriados.

Desde que a procura pelos serviços de telefonia IP aumentou, os fabricantes de equipamentos começaram uma corrida para desenvolver protocolos que avalizassem uma melhor qualidade destes serviços.

A disposição básica do QoS apresenta as três fundamentais características para a sua prática:

- Identificação e marcação de técnicas de QoS para a coordenação de ponta a ponta entre elementos da rede;
- QoS dentro de um único elemento de rede;
- Políticas de QoS, administração, contabilidade e funções para controlar e administrar o tráfego da rede;

A Figura 11 ilustra um exemplo de implementação de QoS.

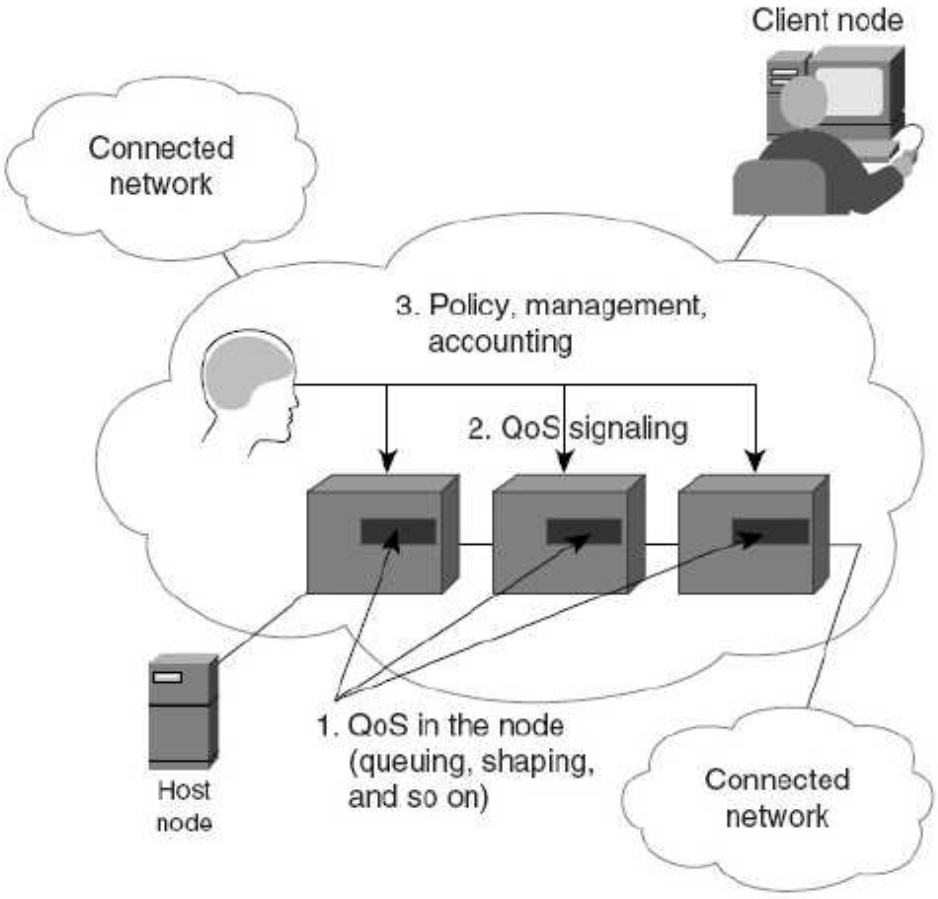

Figura 11. Implementação básica de QoS [24].

A QoS designa fornecer um serviço com qualidade, ou seja, atender as perspectivas de tempo e resposta do serviço fornecido, garantindo um nível

admissível de perdas de pacotes de acordo com o que foi determinado em contrato que é denominado como SLA (*Service Level Agreement*), que é uma espécie de acordo comercial que deverá ser negociado entre os contratos de serviços.

A SLA deve definir declaradamente quais condições devem ser garantidos para que as aplicações possam ser executadas com qualidade.

Na especificação das SLAs são determinados os parâmetros de qualidade de serviço e alguns dos mais usualmente utilizados são descritos no transcorrer deste capítulo.

4.2 Vazão

A vazão (banda) é o parâmetro mais fundamental de QoS. Consiste, basicamente, na taxa de transferência de informações entre dois nós da rede e é indispensável para a operação apropriada de qualquer aplicação. [25]

Em termos objetivos, as aplicações provocam vazões que devem ser supridas pela rede. A Tabela 4 ilustra a vazão peculiar de algumas aplicações:

Aplicação	Vazão (típica)
Aplicações Transacionais	1 Kbps a 50 Kbps
Quadro Branco (*Whiteboard*)	10 Kbps a 100 Kbps
Voz	10 Kbps a 120 Kbps
Aplicações Web	10 Kbps a 500 Kbps
Transferência de Arquivos (Grandes)	10 Kbps a 1 Mbps
Vídeo (*Streaming*)	100 Kbps a 1 Mbps

Tabela 4. Vazão típica de algumas aplicações.

4.3 Latência e Atraso

A latência e o atraso são parâmetros fundamentais para a qualidade de serviço das aplicações. Ambos podem ser empregados na especificação de QoS, apesar do termo "latência" ser convencionalmente mais empregado para equipamentos e o termo "atraso" seja mais empregado para as transferências de dados.

O atraso ou latência, ilustrado na Figura 12, é o tempo que um determinado pacote leva para ser enviado do transmissor para o receptor, através de uma rede.

Os atrasos fixos causam incômodo na conversação e as variáveis atrapalham a cadência na transmissão da voz. Nascem, então, dois problemas para o tráfego de voz quando o atraso é elevado: o eco e a sobreposição de conversação. [26]

Os principais fatores que fazem influência na latência de uma rede são: o atraso de propagação, a velocidade de transmissão e o processamento nos equipamentos.

O atraso de propagação é o tempo necessário para a difusão do sinal no meio que esteja sendo utilizado (fibras ópticas, satélite, cabo coaxial, etc) e é um parâmetro inalterável, onde o administrador de rede não tem qualquer influência.

A velocidade de transmissão é um parâmetro controlado pelo administrador tendo em vista, normalmente, à adaptação da rede à qualidade de serviço requerida. Em se tratando de redes locais, as velocidades de transmissão são normalmente bastante altas e geralmente superiores a 10 Mbps para cada usuário, como por exemplo, no caso de redes utilizando LAN *Switches*. Além disso, vale salientar também que, em um panorama de redes locais, têm-se apenas custos de investimentos iniciais, pois, nelas não se tem, pelo menos em termos de equipamentos, gastos operacionais mensais.

Em se tratando de redes de longo alcance, as velocidades de transmissão variam de acordo com a escolha de tecnologia de rede WAN (*Wide Area Network*), como Linhas privadas, *Frame Relay*, satélite, ATM (*Asynchronous Transfer Mode*). Embora haja a possibilidade de escolha da velocidade apropriada para garantia da

qualidade de serviço, observam-se neste caso ressalvas e/ ou restrições nas velocidades utilizadas, tipicamente devidas às despesas mensais envolvidas na operação da rede. Além disso, observam-se também algumas ressalvas quanto à disponibilidade tanto da tecnologia quanto da velocidade de transmissão almejada. Em termos práticos, trabalha-se em WAN tipicamente com vazões da ordem de alguns *megabits* por segundo para grupos de usuários. [23]

O resultado das exposições discutidas é que a garantia de QoS é seguramente mais difícil em redes MAN (*Metropolitan Area Network*) e WAN, pela soma de dois fatores, ambos negativos: o trabalho com vazão mais baixa e a atrasos muito maiores quando comparados às LANs.

O terceiro fator que colabora para a latência da rede é a contribuição do atraso alusivo ao processamento realizado nos equipamentos. Como forma de exemplo, numa rede IP os pacotes são processados ao longo do percurso entre origem e destino por:

- Roteadores
- LAN *Switches*
- Servidores de Acesso Remoto
- *Firewalls*

Como a latência é um parâmetro ponto a ponto, os equipamentos finais (*hosts*) igualmente têm sua quantia de contribuição para o atraso. No caso dos *hosts*, este depende de uma série de fatores, tais como, a capacidade de processamento do processador, a disponibilidade de memória, os mecanismos de *cache* e o processamento nas categorias de nível mais alto da rede. [23]

Em resumo, nota-se que os *hosts* são também um fator importante para a qualidade de serviço e, em alguns casos, pode ser um ponto crucial na garantia de QoS. Esta consideração é válida para equipamentos servidores (*Servers*) que têm a tarefa de receber solicitações simultâneas de clientes em rede.

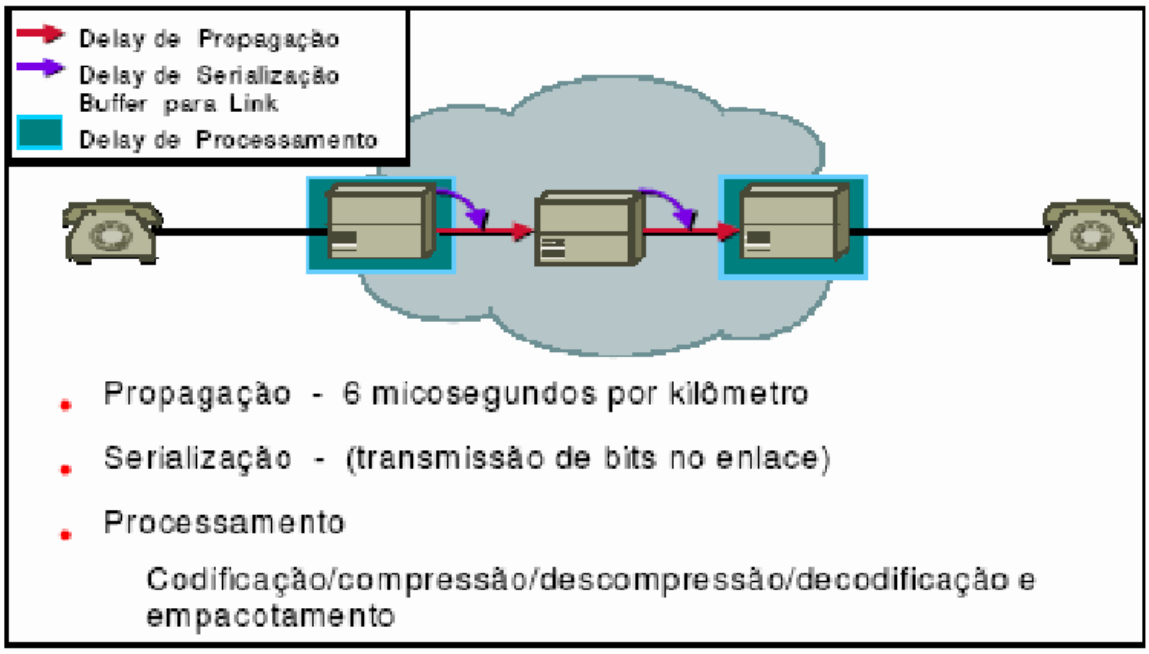

Figura 12. Atraso na rede.

4.4 *Jitter*

O *jitter* é outro parâmetro fundamental para a qualidade de serviço. No caso, o *jitter* é importante para as aplicações destacadas em rede cuja operação apropriada depende da garantia de que os pacotes devem ser processados em intervalos de tempo bem definidos. Este é o caso, por exemplo, de aplicações VoIP, aplicações de tempo real, etc.

Do ponto de vista de uma rede de computadores, o *jitter* é a variação estatística do atraso de entrega dos pacotes em uma rede, ou seja, é a medida da variação do tempo de entrega dos dados recebidos por um nó.

Uma variação de atraso alta significa que os pacotes estão chegando em intervalos aleatórios de tempo, o que acaba tornando complicada a conversação através da rede.

Para evitar problemas deste tipo deve ser criado um *buffer*, onde os dados são guardados antes de serem emitidos para a aplicação, com isso, mantendo constante a taxa de apresentação dos pacotes. [26]

Conforme vistos anteriormente, a rede e seus equipamentos impõem um atraso à informação e este atraso é mutável devido a uma série de fatores, como o tempo de processamento distinto nos equipamentos intermediários (roteadores, *switches*, etc), tempos de arquivamento diferentes estabelecidos pelas redes públicas (*Frame relay*, ATM, IP, etc) e outros fatores atrelados à operação da rede.

A Figura 13 mostra o efeito do *jitter* entre a criação de pacotes na origem e o seu processamento no destino. Observe que o jitter causa, não somente uma entrega com periodicidade variável, como também a entrega de pacotes fora de ordem.

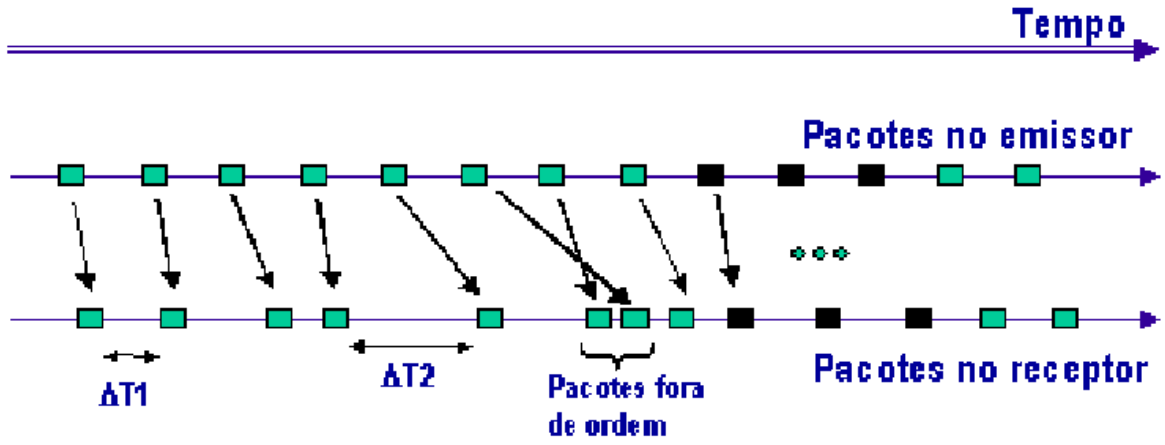

Figura 13. Efeito do jitter para as Aplicações.

4.5 Perdas

As perdas são definidas como o porcentual de pacotes que não chegam ao seu destino. Estas podem ser um problema sério, a depender da rede de pacotes que está sendo empregada. Como redes IP não garantem QoS, elas normalmente possuem uma perda de pacotes de voz mais elevada que uma rede ATM, por exemplo. Nas redes IP atuais, todos os pacotes de voz são tratados como pacotes de dados. Diante de circunstâncias de congestionamento e de alta carga, os pacotes de voz são rejeitados da mesma forma que os pacotes de dados. Contudo, os pacotes de dados não são sensíveis à temporização, e sua perda pode ser corrigida

por retransmissões. Já os pacotes de voz perdidos não podem ter o mesmo tratamento, então convém utilizar métodos alternativos. [23]

O primeiro destes métodos é chamado de interpolação. Nele repete-se o último pacote recebido durante o espaço de tempo destinado ao pacote perdido. Este método funciona muito bem quando a quantidade de perdas é baixa.

O segundo artifício seria enviar dupla informação à custa de um consumo maior de banda da rede. No modelo duplica-se e o n- ésimo pacote de voz é enviado junto com a (n+1)-ésima cópia do pacote. Este método poderá ser capaz de corrigir o pacote perdido, entretanto além de utilizar uma maior banda, também gera maior atraso.

O terceiro método utiliza uma codificação de voz de banda bem menor para prover informação repetida junto com o (n+1)-ésimo pacote. Isto diminui os problemas causados pelo consumo de banda extra, mas não resolve o problema do atraso.

Apesar das inevitáveis variâncias no desempenho da rede, a manutenção dos graus de qualidade de voz aceitáveis, é obtida através de técnicas como: compressão, bufferização, supressão de silêncio e cancelamento de eco. [23]

O desenvolvimento de equipamentos como os DSP (*Digital signal processor*) permitiu melhorias notáveis nas práticas de voz sobre a rede de dados. Com baixo custo e alto desempenho, os DSPs podem processar através de algoritmos competentes a compressão e o cancelamento de eco.

4.6 Disponibilidade

A disponibilidade é um aspecto da qualidade de serviço abordada geralmente na etapa de projetos da rede.

Em síntese, a disponibilidade é uma medida da garantia de implemento da aplicação ao longo do tempo e está amarrada a alguns fatores, como a

disponibilidade da rede pública ou disponibilidade de equipamentos em caso de rede proprietária.

As empresas são dependentes cada vez mais de redes de computadores para a viabilização de seus negócios (Comércio eletrônico, *home banking*, atendimento online, etc), que torna a disponibilidade um requisito bastante rígido. Requisitos de disponibilidade acima de 99% do tempo são corriqueiros para a QoS de aplicações WEB, aplicações cliente/servidor e aplicações de grande interação com o público, dentre outras.

Capítulo 5

O Projeto VoIP na UPE-POLI

Devido à sua disposição tecnológica fechada, com inteligência e funcionalidades reunidas nas centrais telefônicas, efetuar melhorias em funcionalidades já existentes ou incluir novos serviços de valor agregado ao sistema é muitas vezes um processo caro, lento e complexo. Este capítulo irá apresentar os equipamentos necessários para a implantação de uma melhor tecnologia no sistema já existente da unidade de ensino.

Os equipamentos sugeridos na Seção 5.2 deste projeto são fornecidos pela fabricante Cisco *Systems* [27] (referência no fornecimento de soluções para redes e comunicações). A empresa oferece instalação e suporte para seus equipamentos.

5.1 O Sistema Atual de Telefonia da UPE-POLI

A Escola Politécnica de Pernambuco adotou em 2010 um novo sistema de ramais digitais que estão ativos até hoje. Com o novo sistema, a unidade implementou novos pontos de voz e conectou-se com a rede de comunicação do Governo do Estado de Pernambuco (PE-Conectado).

5.1.1 Equipamentos do Sistema

No Sistema atual a POLI utiliza os equipamentos e componentes listados e ilustrados na Figura 14 e 15 a seguir:

- **Siemens Hipath 3000 (PABX digital):**

É a central telefônica da POLI aonde chegam as linhas da rede pública e saem os ramais para os usuários dos terminais internos conectados a ela. São configurados pelo *software* Hipath 3000 *Manager,* cujo manual pode ser acessado em [28], que efetua controle dos usuários, podendo gerenciar permissões de uso individuais ou por grupo.

O equipamento permite efetuar ligações entre telefones internos, de forma gratuita, sem intervenção manual, através dos ramais ou ainda efetuar e receber chamadas da rede externa, através do Digitronco (Tronco E1[7] da operadora OI, atual operadora de telefonia da POLI). Neste caso, as ligações externas estão sujeitas a tarifação pela OI.

Figura 14. Siemens Hipath 3000.

- **Siemens 3005:**

Terminais telefônicos que são conectados a central PABX para ter acesso à rede telefônica, com o fim de efetuar ou receber chamadas. Estes aparelhos têm as seguintes funcionalidades extras: Ligação direta a outro terminal, conferências,

[7] Cabos de par de fio trançado por onde trafegam os sinais telefônicos e seguem o padrão de linha telefônica digital europeu criado pela ITU-T.

chamada em espera, efetuar rechamadas, desvio de chamadas para outro terminal e captura de chamadas de outros terminais.

Figura 15. Siemens 3005.

- **Outros componentes:**

Além do *software manager* da Siemens e do tronco E1 da OI, já relatados anteriormente, o sistema utiliza também cabos de par trançado para fazer a conexões dos terminais ao PABX.

A disposição final da central e seus terminais estão ilustrados na Figura 16:

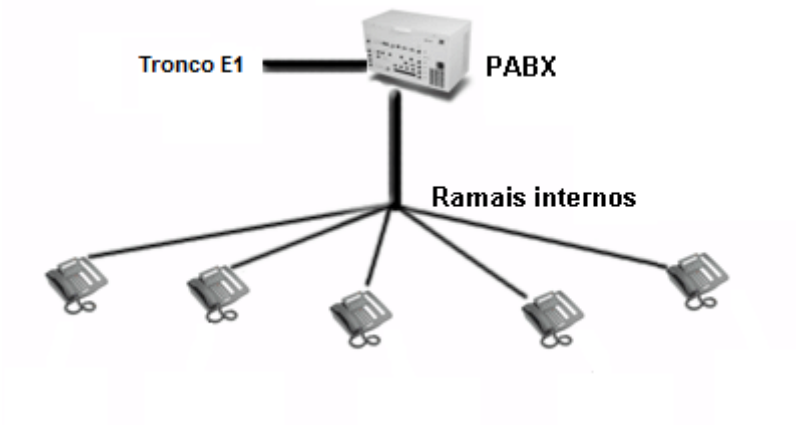

Figura 16. Estrutura física do atual sistema de telefonia da UPE-POLI.

5.2 Topologia e Equipamentos Necessários para a Rede VoIP

Conforme ilustrado na Figura 17, a topologia de rede da empresa será formada por um roteador central interligado à rede da operadora existente que fará a ligação com a rede pública de telefonia. A esse roteador estarão interligados todos os terminais, passando anteriormente por um *Switch*, que poderá também servir como uma forma alternativa de receber energia para os terminais.

Como alternativa, as ligações poderão ser entregues via *internet* para uma operadora digital (como o Skype, dentr outros). Neste caso, esta operadora também através da *internet*, será responsável por entregar as ligações na rede, transformando o sistema 100% digital.

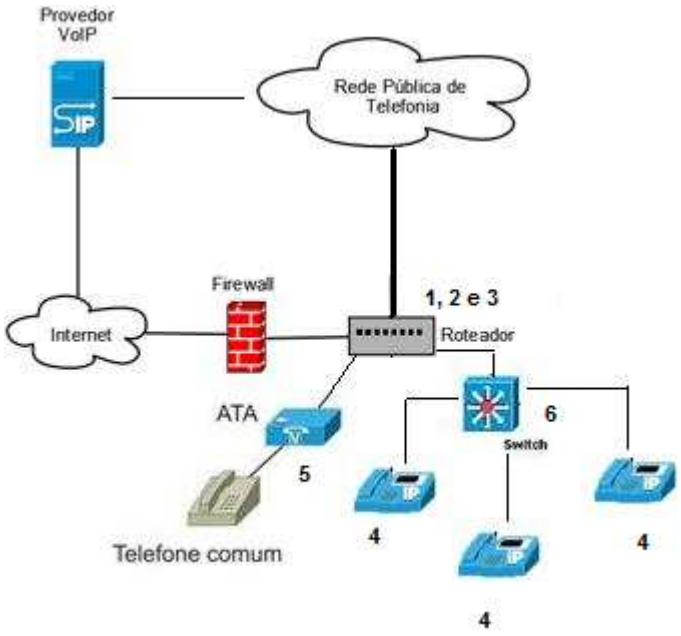

Figura 17. Topologia da rede VoIP na POLI [29]

Em seguida serão listados os equipamentos e componentes necessários para a viabilidade do projeto de telefonia VoIP. Estes equipamentos estão ilustrados da Figura 18 a 23.

Os valores apresentados a seguir são valores médios para uma unidade. Comprando em quantidades maiores, o preço por unidade tende a reduzir.

1. Cisco *Unified Communications Manager Express* (Call Manager):

Software que irá rodar no sistema operacional do roteador da Cisco e irá controlar os telefones da rede, assim como realizar o controle das rotas de telefonia.

Preço médio para licença de até 72 usuários: R$ 5.500,00 (valores para diferente número de usuários podem ser consultados em [30]).

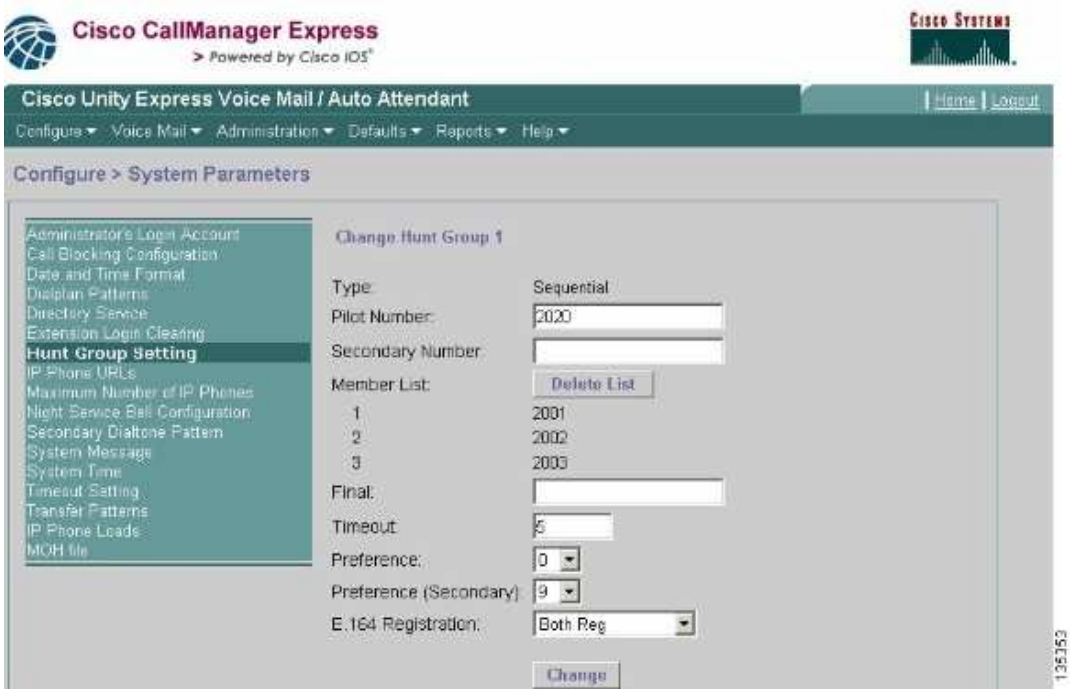

Figura 18. Interface do *Cisco Unified Communications Manager Express* [31].

2. Roteador Cisco 2921 (Gateway):

Hardware que irá executar o item 1 e tem capacidade para até 100 telefones/ramais.

Preço médio unitário: R$ 2.400,00

Figura 19. Cisco 2921 [32].

3. Cisco *Dual Port T1/E1 Multiflex Voice/WAN Interface Card*:

Placa que deve ser encaixada na parte de trás do item 2 e é responsável por receber o tronco E1 (interface), fornecido pela operadora de telefonia.

Preço médio unitário: R$ 70,00

Figura 20. *Cisco Dual Port T1/E1 Multiflex Voice/WAN Interface Card* [33].

4. Telefones IP Cisco 7942G:

O telefone IP é um aparelho criado para a telefonia IP contendo características exclusivas para lidar com a tecnologia VoIP.

Preço médio unitário: R$ 300,00

Figura 21. Cisco 7942G [34].

5. Cisco ATA 187 *Analog Telephone Adaptor*:

Os ATAs são dispositivos que permitem a comunicação em VoIP por meio dos aparelhos telefônicos comuns. Esse tipo de dispositivo faz a conversão dos sinais digitais e analógicos da voz durante a comunicação.

Preço médio unitário: R$ 480,00

Figura 22. Cisco ATA 187 [35].

6. Cisco *Catalyst 2960 48 Power over Ethernet (PoE) Switch*:

É um dispositivo utilizado para reencaminhar pacotes entre os diversos nós. Neste projeto ele será responsável por alimentar os telefones com energia, através dos cabeamentos da rede.

Preço médio unitário: R$ 6.250,00

Figura 23. Cisco Catalyst 2960 [36].

5.3 Funcionamento do Sistema

Tratando-se de uma rede pequena, destinada, a priori, para apenas uma unidade da UPE que é a Escola Politécnica de Pernambuco, que conta com 98 ramais, a rede deverá ter a seguinte estrutura física, baseada nos equipamentos descritos na Seção 5.2 deste projeto:

O *software call manager express* (item 1.) irá controlar os telefones da rede e as chamadas. Esse sistema roda dentro do roteador (item 2) e é necessária prévia configuração e licenças para cada terminal conectado a ele. O roteador, através do *call manager,* será responsável por identificar ligações internas ou externas da rede e encaminhar para os destinos solicitados e fará todo o gerenciamento telefônico, através de prévia configuração. Na parte de trás do roteador deve-se encaixar a placa de adaptação (item 3) de forma a receber o cabo (tronco E1) da operadora já existente na central PABX digital atual, com a finalidade de receber e efetuar ligações externas.

Através de configuração os telefones IP (item 4) irão se registrar e serão controlados pelo roteador e também poderão efetuar ligações na rede interna de forma gratuita.

Os telefones podem ser alimentados com energia através de uma fonte de alimentação ou através do cabeamento de rede, nesse segundo caso o *switch* (item 6) fornecerá energia para os terminais.

Em seu horário de maior movimentação (horário comercial), a rede proposta neste projeto suprirá as necessidades dos 98 ramais existentes, mesmo que em ligações simultâneas.

5.3.1 Casos Específicos

Caberá à POLI, através de análise e estudo internos, definir quais as suas exigências para o sistema. A seguir serão definidos alguns casos específicos que poderão ser requeridos pela unidade:

- **Ligações internacionais:**

Para ligações DDD (Discagem Direta a Distância) que estejam fora da rede VoIP, como por exemplo, telefones convencionais não conectados à *internet*, a operadora atual disponibiliza ligações com custos fixos e cobrados apenas uma vez, já cobertas pelo plano de tarifação da mesma.

Mas, caso sejam realizadas muitas ligações DDI (Discagem Direta Internacional) e os terminais de destino são telefones convencionais que não fazem parte da rede VoIP, convém utilizar outra operadora para efetuar estas ligações. Neste caso, ao invés de se conectar o tronco E1 no roteador, deverá ser fornecido acesso à *internet* ao mesmo, e ser formado um tronco digital via protocolo SIP com uma operadora digital, como o Skype[37], que oferece diversas vantagens e tarifas bem mais baixas. Desta forma o projeto passará ser todo digital e terá custos bem menores, mas ficará sujeito a quedas de conexão ou instabilidade da *internet*.

- **Aumento do número de terminais integrados a central:**

O projeto atual sugere licença para 72 usuários no sistema, mas o número de usuários dependerá das necessidades da unidade. Caso sejam necessários novos terminais conectados, será necessário contratar novas licenças para cada terminal adicional conectado. O roteador usado neste projeto e ilustrado na Figura 19 oferece

suporte para até 100 ramais simultâneos. Caso sejam necessários mais ramais, pode ser consultado em [31] um modelo de roteador com maior capacidade.

- **Utilização de *Softphones*:**

Há ainda a possibilidade de conectar computadores diretamente ao roteador e utilizá-los como terminais virtuais, fazendo uso de *Softphones*, que são disponibilizados gratuitamente na *internet*.

Neste caso, é necessário precaver-se dos riscos existentes, conforme demonstrado no Capítulo 2 desse projeto.

- **Manutenção de telefones convencionais:**

Se for necessário manter os telefones convencionais atuais, podem-se utilizar conversores ATA (item 5 da Seção 5.2), para adaptar telefones comuns à rede VoIP.

Se, por exemplo, o projeto da for usado o VoIP apenas como uma alternativa à telefonia convencional, é mais útil considerar o uso do ATA.

5.3.2 Vantagens do Sistema em relação ao atual

Após a atualização do sistema para a o uso de telefonia VoIP, a rede apresentará diversas vantagens, dentre as quais se destacam:

1. Redução nos custos de ligações internacionais, interurbanas e intra-empresa, pois possibilita comunicação a custo zero quando feitas totalmente por meio do VoIP;

2. Possibilidade de integrar nas estações de trabalho, voz e dados, tornando a infraestrutura de comunicação convergente. Desta forma, compartilham-se equipamentos e recursos humanos para diferentes tarefas;

3. Amplia as opções de comunicação de voz da empresa, fora da capacidade já existente em PABX's;

4. Permitir um melhor gerenciamento online das informações estratégicas de custeio e de despesas;

5. Identificador de chamadas mostradas na tela do termina, incluindo o seu local de origem.

6. Normalmente, 64 kbps por ligação, são o suficiente para uma boa qualidade VoIP no seu melhor *Codec* (G.711). Fazendo com que o consumo de banda seja relativamente pequeno para uma rede simples e com poucos ramais. Em redes corporativas com maior número de ramais, pode-se usar o *Codec* G.729 que possui uma maior compressão de dados e demanda uma taxa de transferência de 8 kbps por ligação. A Tabela 5 ilustra uma lista de *Codecs* mais usados no VoIP atualmente:

Codec	Bit Rate (kbps)	Atraso Fim-a-Fim (ms)	Qualidade de voz
G.711	48;56;64	<<1	Excelente
G.722	48;56;64	<<2	Boa
G.723.1	5.36.3	67-97	Razoável
G.726	16;24;32;40	60	Boa (40) Razoável (24)
G.727	16;24;32;40	60	Boa (40) Razoável (24)
G.728	16	<<2	Boa
G.729	8	25-35	Boa

Tabela 5. Lista de Codecs VoIP

Capítulo 6
Considerações Finais e Trabalhos Futuros

6.1 Considerações Finais

As tecnologias VoIP já estão em funcionamento em várias empresas e instituições ao redor do mundo e vêm se difundindo dia a dia. Empresas como a Cisco, abordada nesse projeto, já possuem linhas completas de produtos capazes de executar em redes de produção a arquitetura VoIP integrada ao ambiente de rede atual. Vastos são os campos de pesquisas e cenários onde o conceito pode ser aplicado. O profissional de redes precisa se manter atualizado sobre as mais modernas tecnologias de transmissão que otimizem sua atividade, de forma a definir qual melhor se adéqua a seu projeto ou ambiente, baseado na comunidade de pesquisa, empresas e fabricantes de equipamentos VoIP.

Apresentando as suas vantagens, este projeto tem por objetivo fornecer uma proposta de implementação da tecnologia VoIP e as funcionalidades da Tecnologia IP, substituindo, total ou parcialmente, o sistema existente atualmente na Escola Politécnica de Pernambuco, a fim de atender a demanda reprimida existente e criando possibilidades de novas expansões futuras sem grandes investimentos novos.

Busca também ser um modelo a ser usado nas necessárias expansões de centrais telefônicas localizadas em outros centros da Universidade ou expansões para a própria unidade.

Apresentou-se, então, o embasamento teórico-prático de uma solução viável, incluindo custos aproximados dos equipamentos a serem utilizados, para um problema concreto vivido pela unidade.

6.2 Trabalhos Futuros

O conceito de telefonia VoIP abre um leque extenso para vários campos de pesquisa. Cada tecnologia de rede é um potencial usuário da arquitetura.

Propõe-se a criação de um projeto, por exemplo, para baratear os custos de ligações para celular, valendo-se de *Gateways* GSM (*Global System for Mobile Communications*) [38], que em paralelo com o *Call Manager*, encaminha ligações, com ajuda da *internet*, para os chips respectivos de cada operadora de telefonia do celular de destino.

Outra proposta seria: apresentar um projeto que busque incorporar outras unidades da UPE à mesma rede apresentada neste trabalho, utilizando *Gatekeepers*.

Bibliografia

[1] Fernandes, A. e Simonini, L. C. S. **Desenvolvimento de uma camada de gerenciamento para interoperação de ilhas VoIP**. Disponível em: http://www.ceel.eletrica.ufu.br/artigos2011/IX_CEEL_102.pdf. Acesso em 11/12/2016.

[2] Colcher, S. **Voz sobre IP**. Rio de Janeiro, Elsevier, 2005.

[3] VALDES, R. **Como Funciona o VoIP**. 2004. Disponível em: http://informatica.hsw.uol.com.br/VoIP.htm. Acessado em: 11/10/2016.

[4] Antoniazzi, A. S. **Segurança VoIP: Ameaças, Vulnerabilidades e as Melhores Práticas**. UFRS, Porto Alegre, TCC, 2008.

[5] GALVÃO, M e ZATTAR, A. **Aspectos de segurança em rede voz sobre IP**. Mslab, 2003, 13p.

[6] Nakamura, E. T. e Licio, P. **Segurança em redes cooperativos**. São Paulo, Novatec, 2007, 1 ed.

[7] **VOMIT**, http://vomit.xtdnet.nl/. Acesso em 11/10/2016.

[8] Endler, D. e Collier, M. **Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions**. McGraw-Hill, 2007.

[9] **Pabx**. Disponível em: http://pabx.telecomunicacoes.org/. Acesso em: 11/10/2016.

[10] Maia, L. P. **Arquitetura de Redes de Computadores.** Rio de Janeiro, LTC, 2009.

[11] Maestrelli, R. IDS - **Sistemas de Detecção de Intrusos**. Disponível em: http://www.gta.ufrj.br/grad/07_2/rodrigo_leobons/assinaturas.html. Aceso em: 11/10/2016.

[12] Reis, F. A. e Pagani, E. **Hardening em Sistemas Operacionais GNU/LINUX**. 2010. Disponível em: http://re.granbery.edu.br/artigos/Mzk3.pdf. Acesso em: 11/10/2016.

[13] **PRTG**, https://www.br.paessler.com/prtg. Acesso em: 11/10/2016

[14] Cardenas, E. D. **MAC Spoofing - An Introduction**. GIAC Security Essentials Certification, SANS Institute, 2013.

[15] Schneier, B. **Caller ID Spoofing**. Disponível em: http://schneier.com. Acesso em: 16/01/2011.

[16] Teruel, E. C. **Principais ferramentas utilizadas na auditoria de sistemas e suas características**. São Paulo, UNINOVE. Disponível em: http://www.cps.sp.gov.br/pos-graduacao/workshop-de-pos-graduacao-e-pesquisa/anais/2010/trabalhos/gestao-e-desenvolvimento-de-tecnologias-da-informacao-aplicadas/trabalhos-completos/teruel-evandro-carlos.pdf. Acesso em: 11/10/2016.

[17] **H.323,** ITU-T. Disponível em: http://www.itu.int/rec/T-REC-H.323/en/. Acesso em: 12/12/2016.

[18] Aguiar, G. Protocolos para VoIP. **Tutoriais Banda Larga.** Disponível em http://www.teleco.com.br/tutoriais/tutorialvoipindoor1/pagina_2.asp. Acesso em: 11/10/2016.

[19] **SIP: Session Initiation Protocol.** Disponível em: https://datatracker.ietf.org/doc/rfc3261/. Acesso em 11/10/2016.

[20] Lima, B. e Moraes, R. Session Initiation Protocol (SIP). **Tutorial Banda larga VoIP**. Disponível em: http://www.teleco.com.br/tutoriais/tutorialtelip2/pagina_3.asp. Acesso em: 11/10/2016.

[21] Kurose, F.J. e Ross, **W.K. Redes de computadores e a Internet.** Vol. 3, São Paulo, 2006, p. 465

[22] Moura, N. T. **Voice Over Internet Protocol – VoIP**. Disponível em: http://www.ic.uff.br/~celio/classes/mmnets/projetos/Nilmax/Voip_Survey.html. Acesso em 11/10/2016.

[23] Monks, E. M. **Planejamento de Capacidade em Redes Corporativas para implementação de Serviços VoIP**. UFRGS, Porto Alegre, Dissertação de Mestrado, 2006.

[24] Interworking Technology Handbook. **Quality of Service (QoS) – Cisco Systems.** Disponível em: http://www.cisco.com/en/US/docs/internetworking/technology/handbook/QoS.html. Acesso em: 15/01/2010.

[25] Almeida, A. B. **Medição de qualidade de voz em Wireless utilizando Codecs G711, G729, G723 e GSM**. PUC Campinas, dissertação de mestrado, 2008.

[26] Bernal, P. S. M. **Voz sobre Protocolo IP- A Nova Realidade da Telefonia**. São Paulo, Érica, Ed. 1, 2007.

[27] **Cisco Systems**, http://www.cisco.com. Acesso em: 11/10/2016.

[28] **Siemens Hipath 3000 Manual**. Disponível em: http://www.cpatelecom.com.br/download/Manual_HP3000.pdf. Acesso em: 12/12/2016.

[29] Stallings, W. **Redes e Sistemas de Comunicação de Dados: teoria e aplicações corporativas**. 5. ed. Rio de Janeiro: Elsevier, 2005

[30] **Cisco CallManager Express Feature Licenses**. Disponível em: http://www.globalpricelists.com/globalpricelistcisco.php?groopa=775. Acesso em: 11/10/2016.

[31] **Cisco Unified Communications Manager Express**. Disponível em: http://www.cisco.com/c/en/us/products/collateral/unified-communications/unified-communications-manager-express/datasheet-c78-737647.html. Acesso em: 11/10/2016.

[32] **Cisco 2900 Series Integrated Services Routers**. Disponível em: http://www.cisco.com/c/en/us/products/collateral/routers/2900-series-integrated-services-routers-isr/data_sheet_c78_553896.html. Acesso em: 11/10/2016.

[33] **Cisco One and Two Port T1/E1 Multiflex Voice/WAN Interface Card**. Disponível em: http://www.cisco.com/c/en/us/products/collateral/routers/3600-series-multiservice-platforms/product_data_sheet09186a0080091b9c.html. Acesso em: 11/10/2016.

[34] **Cisco Unified IP Phone 7942G.** Disponível em: http://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/unified-ip-phone-7942g/product_data_sheet0900aecd8069bb68.html. Acesso em: 11/10/2016.

[35] **Cisco ATA 187 Analog Telephone Adaptor**. Disponível em: http://www.cisco.com/c/en/us/products/collateral/unified-communications/ata-187-analog-telephone-adaptor/data_sheet_c78-608596.html. Acesso em: 11/10/2016.

[36] **Cisco Catalyst 2960 48 Power over Ethernet (PoE) Switch**. Disponível em: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-series-switches/product_bulletin_c25-512173.html. Acesso em: 11/10/2016.

[37] **Skype**. https://www.skype.com/. Acesso em: 11/10/2016.

[38] Silva, L. A. **O que é um gateway GSM e o que a sua empresa tem a ganhar com ele**. Disponível em: http://www.canaltelecom.com.br/blog/gateway-gsm/. Acesso em: 11/10/2016.