UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
CURSO DE ESPECIALIZAÇÃO EM TECNOLOGIAS, GERÊNCIA E SEGURANÇA
DE REDES DE COMPUTADORES

SIMONE HARFF

Requisitos e Proposta para Implantação de um Servidor VoIP

Trabalho de Conclusão apresentado como requisito parcial para a obtenção de grau de Especialista

Prof. Dr. João César Netto
Orientador

Prof. Dr. Sérgio Luis Cechin
Prof. Dr. Luciano Paschoal Gaspary
Coordenadores do Curso

Porto Alegre, outubro de 2008.

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS

ACELP	Algebraic Code Excited Linear Prediction
ACM	Automatic Channel Mapping
ADPCM	Adaptative Diferencial PCM
AES	Advanced Encryption Standard
AH	Authentication Header
ALG	Application Layer Gateway
AS	Assured Forwarding
ATA	Adaptador para Telefone Analógico
ATM	Asynchronous Transfer Mode
CAR	Commited Access Rate
CODEC	Codificador / Decodificador
CS-ACELP	Conjugate Structure ACELP
DiffServ	Differentiated Services
DSCP	Differentiated Service Code Point
DSP	Digital Signal Processor
EF	Expedited Forwarding
ESP	Encapsulating Security Payload
IETF	Internet Engineering Task Force
IntServ	Integrated Services
IP	Internet Protocol
ITU	International Telecommunications Union
ITU-T	ITU Telecom Standardization Sector
LDAP	Lightweight Directory Access Protocol
LD-CELP	Low-Delay Code Excited Linear Prediction

MC	Controlador Multiponto
MCU	Unidade de Controle Multiponto
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MIKEY	Multimídia Internet Keying
MIME	Multipurpouse Internet Mail Extensions
MKI	Master Key Identifier
MOS	Mean Option Scores
MP	Processador Multiponto
MP-MLQ	Multi-Pulse Multi-Level Quantization
MPLS	MultiProtocol Label Switching
NAT	Network Address Translation
PBX	Private Branch Exchange
PCM	Pulse Code Modulation
PHB	Per Hop Behaviours
QoS	Quality of Service
RSVP	Resource ReSerVation Protocol
RTCP	Real Time Control Protocol
RTP	Real Time Transport Protocol
RTPC	Rede Telefônica Pública Comutada
RTSP	Real Time Streaming Protocol
SBADPCM	Sub-band Adaptive Diferencial PCM
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLS	Service Level Specification
SRTCP	Secure RTP Control Protocol
SRTP	Secure Real-Time Transport Protocol
SSL	Secure Sockets Layer
STUN	Simple Traversal of UDP Trought NAT
TCP	Transfer Control Protocol

TCS	Traffic Conditioning Specification
TOS	Type of Service
TRIP	Telephony Routing Over IP
TURN	Traversal Using Relay NAT
UA	User Agent
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
VoIP	Voice Over Internet Protocol

LISTA DE FIGURAS

LISTA DE TABELAS

RESUMO

Este trabalho apresenta um estudo sobre os diversos aspectos envolvidos na implementação de um servidor VoIP. Protocolos de sinalização e transporte, CODECs, travessia de NAT e firewall, QoS, softwares VoIP são analisados e para cada item são apresentadas diferentes soluções.

Considerando uma empresa e sua atual estrutura de rede, o trabalho propõe ainda uma solução de implantação, atendendo necessidades como integração com a central telefônica tradicional e ampliação do número de ramais, sem deixar de considerar a viabilidade técnica e financeira da mesma.

Palavras-chave: VoIP, NAT, firewall e QoS.

Requirements and Proposal of VoIP Server Implementation

ABSTRACT

This monograph presents the study of various features involved in a VoIP implementation. Signaling protocols, transport protocols, CODECs, NAT traversal and firewall, QoS, VoIP softwares are analysed and, for each case, we present different solutions.

Regarding a company and its real network, this monograph suggest a solution of implementation, considering the necessary integration with the PBX, the increasing of extensions lines, the technical viability and the cost of that.

Keywords: VoIP, NAT, firewall and QoS.

1 INTRODUÇÃO

A tecnologia VoIP vem sendo largamente utilizada nas corporações, buscando a expansão da rede telefônica existente, fugir da dependência da telefonia tradicional ou diminuir os custos, é cada vez maior o número de empresas que adotam esta tecnologia, utilizando a estrutura física já existente para dispor de novos serviços.

Este trabalho tem por objetivo levantar e analisar os requisitos necessários para implantação de um servidor VoIP, buscando a inclusão deste numa rede já existente e também sua integração com o sistema de telefonia convencional.

O trabalho está dividido em sete capítulos sendo que o segundo abordará um pouco da história da telefonia, sua evolução até os dias atuais, a tecnologia VoIP, seus desafios e tendências para o futuro.

O terceiro capítulo definirá os diferentes cenários de comunicação VoIP, entre terminais IPs, entre terminal IP e telefone convencional e entre telefones convencionais utilizando a rede IP. Além disso, fará uma comparação entre os protocolos de sinalização H.323 e SIP e apresentará os protocolos de transporte RTP/RTCP.

O quarto capítulo discorrerá sobre a importância da utilização dos CODECs, fará uma breve descrição dos mais utilizados e um comparativo considerando os modelos MOS e E.

O quinto capítulo tratará sobre a importância e os diversos aspectos que precisam ser considerados para utilização de um servidor VoIP ultrapassando NAT e firewall, diversas técnicas são abordadas com o intuito de permitir a comunicação visando ao não comprometimento da segurança da rede. Serão levantados também alguns aspectos referentes à privacidade e autenticidade, requisitos necessários em qualquer comunicação.

O sexto capítulo abordará a QOS em comunicações VoIP, requisito extremamente importante quando se busca qualidade nas conversações. Serão analisadas as métricas que devem ser consideradas para obtenção da qualidade, vazão, atraso, jitter e perdas, os parâmetros necessários para elaboração de uma SLA e os mecanismos e arquiteturas que podem ser implementados buscando a melhor qualidade.

O sétimo capítulo fará um estudo sobre o Asterisk, software livre que possui as funcionalidades de um PBX completo, definindo sua arquitetura, interfaces e fazendo uma comparação com o OpenSer, software que atua como um SIP Proxy.

O oitavo capítulo apresentará uma proposta de implementação considerando uma rede previamente existente, abordando as necessidades de mudanças físicas e demais aspectos analisados nos capítulos anteriores. Esta proposta se baseia num escopo definido no início do oitavo capítulo, considerando as necessidades de integração com os serviços existentes, como por exemplo, a central telefônica convencional.

Espera-se com o exposto acima, atingir todos os pontos que devem ser considerados na implementação de um servidor VoIP e apresentar também diferentes alternativas para cada necessidade.

2 VoIP: UMA VISÃO GERAL

Desde 1876, quando Alexander Graham Bell patenteou o primeiro aparelho telefônico, que utilizava o eletromagnetismo para a transmissão de voz à distância, até os dias de hoje, a telefonia vem se desenvolvendo continuamente.

Passando pela criação da primeira central telefônica (1877); utilização da primeira central telefônica automática (1892); utilização da primeira central digital e sistema de discagem direta à distância (1958); utilização de fibra ótica, multiplicando a capacidade de tráfego de sinais telefônicos (1970); telefonia celular (1983), chegamos, em 1995, ao advento do VoIP (Voice Over Internet Protocol).

A tecnologia VoIP surgiu neste ano em Israel, quando um grupo desenvolveu um sistema que permitia utilizar os recursos multimídia de um PC doméstico para iniciar conversas de voz pela Internet. Apesar da qualidade não ser muito boa, este foi o primeiro passo para que outros pesquisadores se interessassem pelo assunto.

Neste mesmo ano, a empresa Vocaltec Inc lançou o primeiro software dedicado à comunicação VoIP, este software fazia a compressão do sinal de voz, tradução em pacotes de dados e o envio pela rede. Chamado Internet Phone Software, foi o precursor de softwares como Skype e Messenger, utilizados atualmente.

Em 1998 algumas companhias passam a oferecer serviço VoIP com certa qualidade, interligando-o ao serviço de telefonia convencional.

Portanto, VoIP é uma tecnologia que permite a comunicação telefônica utilizando a rede de dados como meio de transmissão da voz, como representado na figura abaixo:

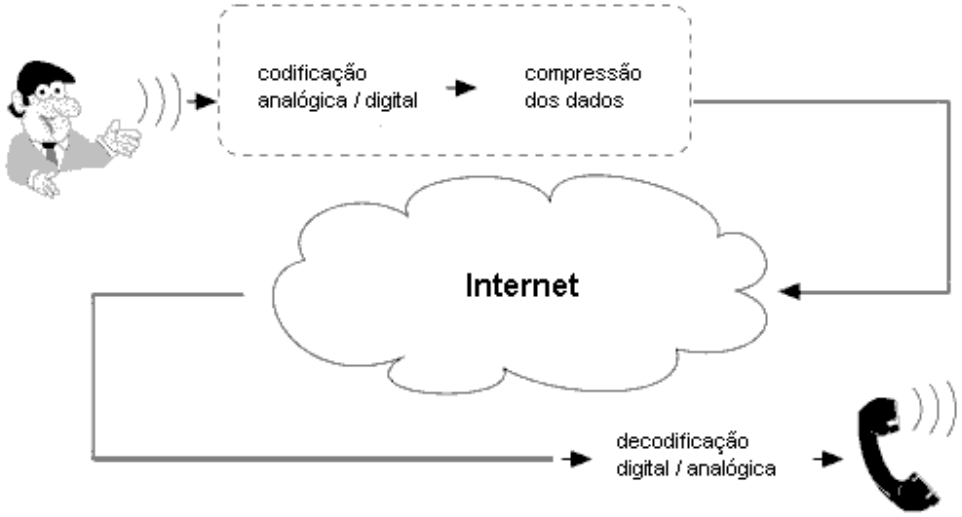

Figura 2.1: Comunicação VoIP (IZU et al., 2008)

Em 1998 surgiram os primeiros gateways, equipamentos capazes de interligar aparelhos telefônicos convencionais ou centrais telefônicas à rede de dados, para a comunicação entre estes sistemas utilizando VoIP.

Em seguida, surgiram gateways especializados e dispositivos chamados ATA (Adaptador para Telefone Analógico) para interligar dois sistemas convencionais e/ou centrais, utilizando como meio de transmissão a rede IP.

Com a utilização de VoIP e os equipamentos desenvolvidos é possível atualmente fazer a interligação entre centrais telefônicas e redes de dados, permitindo que sejam feitas ligações para telefones convencionais utilizando o computador e vice-versa. Da mesma forma, o aumento das taxas de transmissão permitiu que usuários domésticos também passassem a usufruir desta tecnologia.

VoIP é uma tecnologia que digitaliza, comprime e converte sinais de voz (analógico) em pacotes de dados e os transmite utilizando qualquer rede TCP/IP. Assim que estes pacotes são recebidos no destino, são convertidos em sinal analógico novamente, utilizando qualquer meio no qual seja possível reproduzir o som.

Protocolos de sinalização são utilizados para estabelecer, desconectar chamadas e transportar informações necessárias para localizar usuários e negociar funcionalidades. Esquemas de compressão (CODECs), habilitados nas extremidades das conexões, assim como protocolos de transporte (RTP e RTCP) também são necessários.

O grande desafio do VoIP é estabelecer a mesma qualidade e confiabilidade encontrada na telefonia convencional. Problemas como latência, jitter, congestionamento, firewalls, NATs e segurança são desafios técnicos a serem superados. Padrões de QoS, por

exemplo, podem ser negociados quando utilizamos uma rede privada, onde se tem total controle, porém, ao utilizarmos a Internet não temos este mesmo controle, o que pode tornar uma aplicação de voz em tempo real de baixa qualidade.

Nos próximos anos, a tecnologia VoIP deve se tornar um dos principais setores de crescimento no mercado de telecomunicações. Muitas empresas vêm utilizando a tecnologia VoIP em PBX (Private Branch Exchange), diminuindo desta forma os gastos com centrais telefônicas e fazendo uma melhor utilização da infra-estrutura de rede existente. Várias ligações podem ser executadas simultaneamente, nos períodos de inatividade de uma conexão a banda pode ser utilizada por outra aplicação, diferentemente da comutação por circuitos onde o meio de transmissão permanece ocupado durante todo o período da ligação. Além disso, a utilização do VoIP nos oferece mobilidade, permitindo ao usuário atender uma ligação em qualquer lugar que esteja.

A tecnologia VoIP e o oferecimento de novos serviços que englobam diversos tipos de informação vêm se mostrando um atrativo para as empresas de telecomunicações e também para toda a indústria ligada à computação. Percebe-se que as tecnologias utilizadas nos sistemas telefônicos e nas redes de computadores convergem para um ponto em comum.

Apesar de poucos ambientes utilizarem uma infra-estrutura puramente de telefonia IP, há um aumento gradual nesta utilização. Alguns analistas de mercado sugerem que o avanço do VoIP ocasionará a extinção por completo do modelo atual de ligações de longa distância pela RTPC (rede telefônica pública comutada) ou até a erradicação dos sistemas convencionais de telefonia.

3 CENÁRIOS DE COMUNICAÇÃO VoIP, PROTOCOLOS DE SINALIZAÇÃO E TRANSPORTE

3.1 Cenários de Comunicação VoIP

Em pouco tempo, diversas tecnologias de comunicação de voz sobre redes IP surgiram como solução para integração dos serviços de telefonia convencionais e as redes comutadas por pacotes. Novos equipamentos, protocolos e serviços são oferecidos visando a esta integração, sempre utilizando o protocolo IP como foco. Neste tópico, apresentamos os diversos cenários de comunicação VoIP, evidenciando suas diferenças e o que cada um necessita para seu funcionamento.

3.1.1 VoIP de Terminal IP para Terminal IP

Na comunicação entre terminais IPs é necessário que os interlocutores utilizem telefones IP, algum software no computador, os chamados softphones, ou adaptadores de telefones analógicos (ATAs). Estes softwares e equipamentos são denominados terminais ou agentes de usuários.

Os telefones IPs têm a capacidade de codificar e decodificar sinais de voz em fluxo de áudio digital e também enviá-los ou recebê-los através de uma rede IP. Os softwares utilizam APIs de captura e reprodução de áudio e de comunicação via IP providas pelo sistema operacional para transmitir e receber as amostras de áudio digitalizadas empacotadas em datagrama IP.

Os adaptadores de telefones analógicos permitem conectar um telefone convencional ao PC, efetuando a conversão analógico-digital.

Os equipamentos utilizados possuem CODECs de áudio e uma interface de rede conectada a uma rede IP para que a conversação seja estabelecida.

Uma comunicação deste tipo necessita apenas do protocolo de transporte RTP/RTCP para que seja feita a sincronização das amostras que trafegam na rede IP entre os agentes. Porém, se forem utilizados serviços como redirecionamento de conversações é

necessário a utilização de protocolos de sinalização que estabeleçam chamadas ou sessões entre os terminais, como H.323 ou SIP.

Além disso, caso se deseje que algumas funções estejam disponíveis mesmo quando os agentes não estão operando, como se espera numa central telefônica convencional, utiliza-se um gateway de gerência que centraliza as seguintes funções:

- Controle de acesso: controla o estabelecimento de novas chamadas, verificando o limite de chamadas simultâneas e os privilégios de cada agente, assim como também mantém informações sobre bilhetagem;
- Gerência de banda passante: controla a utilização da banda passante, limita o número de chamadas simultâneas, restringindo o número de chamadas quando necessário, utilizando mecanismos de QoS;
- Roteamento de chamadas: efetua o roteamento de chamadas com base na disponibilidade de banda passante.

A figura a seguir apresenta os elementos necessários para a comunicação entre terminais IPs:

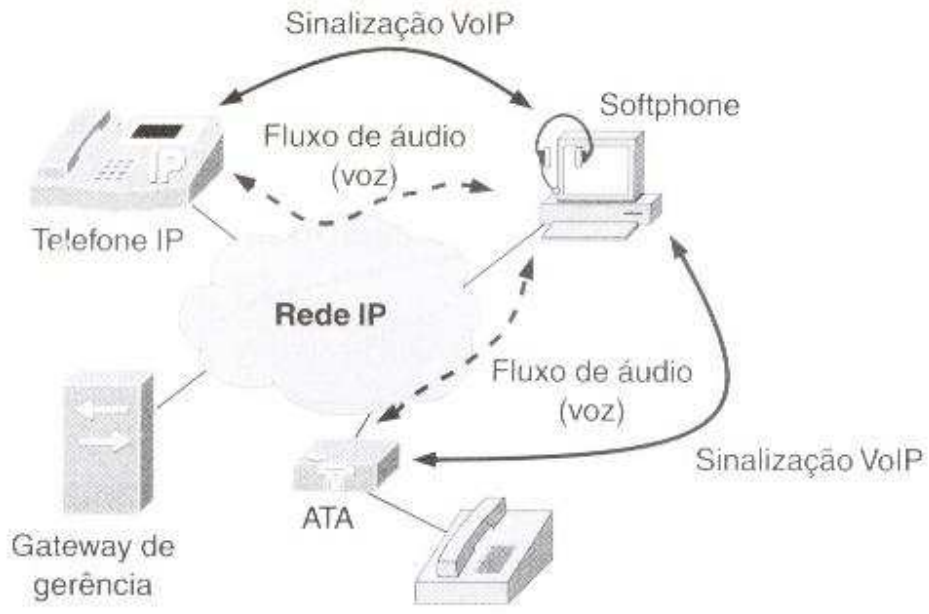

Figura 3.1: Comunicação de voz de terminal IP para terminal IP (COLCHER et al., 2005)

3.1.2 VoIP de Terminal IP para Telefone

Para que a comunicação entre um terminal IP e um telefone convencional se estabeleça são necessários, além dos mesmos elementos utilizados na comunicação entre terminais IPs, o uso do gateway de voz e do gateway de sinalização.

O gateway de voz, também chamado gateway de mídia, é responsável pela transmissão dos fluxos de áudio entre a rede IP e a RTPC. O gateway de voz tem as seguintes funções:

- Codificação e decodificação digital da voz, quando a RTPC é analógica;
- Transcodificação entre formatos digitais, quando a codificação utilizada na rede IP difere daquela utilizada na RTPC;
- Terminação de chamadas telefônicas na RTPC; e
- Transmissão e recepção de amostras de áudio digital encapsulados em datagramas IP.

Os terminais de rede IP vêem o gateway de voz como mais um terminal.

Já as centrais telefônicas vêem o gateway de voz da seguinte forma:

- Gateway residencial: interligação com interfaces analógicas tradicionais;
- Gateway de acesso: interligação com centrais privadas de comutação telefônica analógica ou digital;
- Gateway de trunking: interligação com grande número de troncos analógicos ou digitais da RTPC;
- Gateways de voz sobre ATM (Asynchronous Transfer Mode): interligação com redes de voz sobre redes ATM.

O gateway de sinalização, também chamado controlador de gateway de mídia (MGCs), controla os pedidos de estabelecimento de chamada que partem tanto da RTPC para a rede IP como o inverso.

O gateway de sinalização executa as seguintes funções:

- Conversão de sinalização: traduz as mensagens ou tons utilizados na RTPC para a sinalização VoIP;
- Controle de gateway de mídia: efetua o controle da lógica de funcionamento dos gateways de mídia, requisita a geração de sinais nas linhas telefônicas ou é notificado a respeito dos eventos iniciados na mesma.

A figura a seguir apresenta os elementos necessários para a comunicação entre terminais IP e telefone convencional:

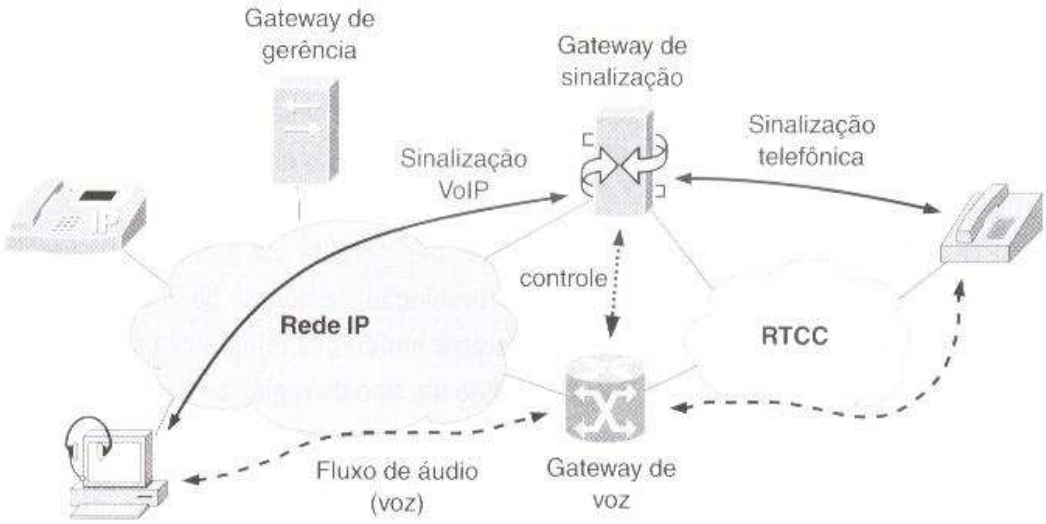

Figura 3.2: Comunicação de voz de terminal IP para telefone (COLCHER et al., 2005)

3.1.3 VoIP de Telefone para Telefone

A comunicação entre dois telefones convencionais se dá, normalmente, entre duas centrais telefônicas distintas. Neste caso, a utilização de gateways de sinalização permite que as centrais utilizem a rede IP para se interligarem. Pode ser utilizado um gateway de sinalização para cada central telefônica ou apenas um único gateway, o que elimina a necessidade de sinalização entre os gateways.

Os demais elementos presentes no cenário terminal IP para telefone também são necessários neste modelo.

A figura a seguir ilustra o cenário de comunicação de voz de telefone para telefone, utilizando um gateway de sinalização para cada central telefônica:

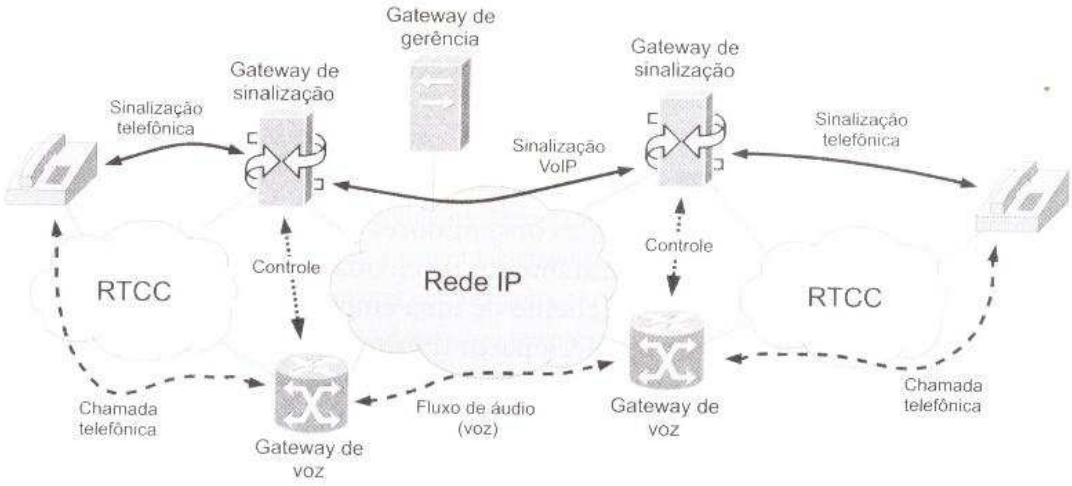

Figura 3.3: Comunicação de voz de telefone para telefone usando redes IP (COLCHER et al., 2005)

3.2 Protocolos de Sinalização

Protocolos de sinalização estabelecem as chamadas ou sessões entre os terminais. A força do H.323 está em sua interoperabilidade com a RTPC, enquanto que o SIP (Session Initiation Protocol) é um protocolo desenvolvido especificamente para a Internet, com grande escalabilidade e flexibilidade. Estes protocolos estão descritos a seguir:

3.2.1 H.323

O ITU-T (International Telecommunication Union – Telecommunication Standardization Sector) definiu a Recomendação H.323 com o objetivo principal de padronizar a transmissão de dados em sistemas de conferência audiovisual por meio de redes comutadas por pacotes, que não provêem garantia de QoS. (COLCHER et al., 2005)

Esta recomendação determina os padrões a serem utilizados para sinalização, estabelecimento de sessões, controle de chamadas, gerenciamento de largura de banda, controle de admissão, CODECs para transferência de áudio e vídeo e protocolos de transferência de dados.

Basicamente, num sistema baseado em H.323, são definidos quatro componentes:

- Terminais: São estações clientes da rede de onde são originados ou destinados os fluxos de informação em tempo real. O sistema H.323 especifica quais os padrões de codificação para captura e apresentação de mídias aos quais os terminais devem dar suporte;
- Gateways: São utilizados quando se quer estabelecer a comunicação entre terminais de diferentes tipos de rede, um gateway é, ao mesmo tempo, de voz e sinalização. O gateway efetua a conversão do formato de codificação de mídias

e a tradução dos procedimentos de estabelecimento e encerramento de chamadas. Eles garantem a interoperabilidade entre terminais H.323 e a rede telefônica comutada por circuitos;
- Gatekeepers: É um gateway de gerência, o componente mais importante de uma rede H.323. Permite o controle centralizado do sistema. Nele são registrados todos os pontos finais e é efetuado o controle de admissão de chamadas para as estações registradas, controle de largura de banda e a tradução de endereços dos apelidos dos terminais de rede e gateways para endereços IPs. O gatekeeper também pode efetuar o roteamento de mensagens de sinalização e controle;
- MCU (unidade de controle multiponto): Permite o estabelecimento de conferência entre três ou mais pontos finais. É formado por um controlador multiponto (MC) e processadores multiponto (MP). O MC centraliza o processo de estabelecimento de chamadas multiponto negociando parâmetros de comunicação entre os pontos finais. Já o MP é responsável pelo encaminhamento de fluxos de áudio, vídeo e dados textuais entre os pontos finais.

Terminais, gateways e MCUs administrados por um único gatekeeper formam uma zona de gerência H.323, existe apenas um gatekeeper ativo em cada zona de gerência.

Dentre os protocolos utilizados pelo H.323 estão os seguintes:

- RTP/RTPC: utilizados para o empacotamento de amostras de áudio e vídeo assim também como para transmissão e sincronismo de redes comutadas por pacotes;
- H.225: para sinalização de chamada;
- H.245: para controle de mídia; e
- H.225.0 RAS: para registro, controle de admissão e determinação de estado de chamadas, acontecem sempre dos terminais H.323 para o gatekeeper.

Mensagens de sinalização H.225.0 devem ser transportadas na rede comutada por pacotes por meio de um serviço de entrega fim a fim confiável.

O estabelecimento de uma chamada entre pontos finais é sempre necessário antes de qualquer comunicação quando se utiliza H.323.

Quando não se utiliza um gatekeeper as mensagens de estabelecimento de chamadas são trocadas diretamente entre os pontos finais.

Existem dois modos de operação entre os terminais H.323:

- Modo Direct Routed: O gatekeeper recebe a chamada e provê ao terminal H.323 o endereço IP do terminal chamado, neste ponto, a sinalização de estabelecimento de chamada prossegue entre os terminais H.323;
- Modo Gatekeeper Routed: O gatekeeper intermedia a sinalização de estabelecimento de chamada e de negociação de mídia como se fosse o terminal chamador.

3.2.2 SIP

Proposto pelo IETF (Internet Engineering Task Force) o SIP tem mobilizado muitos fabricantes da área de telefonia e dados, por causa de sua flexibilidade, integração a aplicações Internet e de arquitetura aberta.

SIP é um protocolo de sinalização de nível de aplicação. Ele negocia os termos e as condições de uma sessão. Estabelece, modifica e finaliza chamadas telefônicas, definindo os tipos de mídia, padrões de codificação utilizados, requisitos de largura de banda e auxiliando na localização dos participantes da sessão.

O protocolo SIP é baseado no HTTP e no SMTP, suportando o transporte de qualquer tipo de dados em seus pacotes, utilizando MIME-Types (multipurpose internet mail extensions), similar ao e-mail, que transporta qualquer tipo de dados em seus anexos. Por utilizar uma arquitetura cliente/servidor, suas operações envolvem apenas métodos de requisição e respostas, como ocorre também no HTTP.

Num sistema SIP, são definidos os seguintes componentes:

- User Agent (UA): o user agent é formado por uma parte cliente (UAC), capaz de iniciar requisições SIP e uma parte servidor (UAS), capaz de receber e responder requisições SIP. O UA faz chamadas a endereços parecidos com os utilizados em e-mail, como por exemplo SIP:user@proxysip.com.br. Agentes de usuários podem enviar e receber chamadas de outros agentes sem a necessidade de componentes adicionais do SIP;
- Servidos proxy: efetua requisições para outros clientes que não podem fazer requisições diretamente, o proxy passa adiante as requisições de um UA para outro servidor SIP, atua tanto como servidor como cliente. O servidor proxy também retém informações para faturamento;
- Servidor de redirecionamento: mapeia um endereço nos diversos endereços associados a um cliente, fornece informações ao UA sobre o endereço solicitado, possibilitando ao UA conectá-lo diretamente. Geralmente opera como um cliente de algum tipo de serviço de localização, normalmente um banco de dados que mantêm as informações necessárias;
- Servidor de registro (registrar): é um gateway de gerência, armazena informações sobre as UAs, para fornecer um serviço de localização e tradução de endereços do domínio que controla. Trabalha em conjunto com o servidor proxy e o servidor de redirecionamento.

Dentre os protocolos que o SIP utiliza estão os citados abaixo:

- RTP: para transportar os dados por uma rede comutada por pacotes;
- RTCP: para fornecer informações de controle e também QoS;
- RTSP (real time streaming protocol): para controlar a entrega de fluxos de distribuição de mídia;

- MGCP (media gateway control protocol) e Megaco/H248: para controlar gateways de mídia;
- SDP (session description protocol): para descrever sessões multimídia;
- DNS: para determinação do destinatário dos pedidos;
- LDAP: para o acesso direto à base de dados de um servidor de localização;
- TRIP (Telephony Routing Over IP): para troca de informações de encaminhamento entre domínios administrativos de telefonia;
- RSVP: para estabelecer a reserva de recursos.

O SIP opera das seguintes formas:

- Modo direto (peer to peer): permite um agente SIP enviar requisições diretamente a outro agente. Um UAC troca mensagens diretamente com um UAS, negociando parâmetros de sessão e estabelecendo comunicação de voz. Apesar de ser o modo mais simples para estabelecer uma sessão vários recursos e serviços podem não ser suportados;
- Modo indireto (via proxy): há a necessidade de outros servidores que integram a infra-estrutura baseada em SIP. Neste caso, o agente envia as mensagens de sinalização para o servidor proxy, responsável por encaminhá-las e controlar a entrada e saída de mensagens do sistema. O servidor proxy pode estar integrado ao servidor de registro e servidor de redirecionamento, evitando o acesso direto aos mesmos;
- Outbound proxy: o proxy recebe pedidos de um terminal, mesmo não sendo ele o destinatário. Esta configuração é utilizada quando existe um firewall, o UA é configurado para receber e enviar pedidos através deste servidor.

Quando utilizamos um servidor proxy, também podemos definir de que forma será feito o encaminhamento das mensagens:

- Stateless (sem estado): nenhuma informação sobre a mensagem é mantida pelo proxy;
- Stateful (com estado): informações sobre a mensagem encaminhada são mantidas pelo proxy, facilitando o encaminhamento de outras mensagens da mesma sessão.

3.2.3 Diferenças entre H.323 e SIP

Comparando os protocolos H.323 e SIP, podemos chegar as seguintes considerações:

- O H.323 tem sua abordagem voltada para os serviços terminais enquanto que a abordagem do SIP é voltada para os usuários de serviços integrados na Internet;
- Ambos os protocolos utilizam RTP/RTCP para o transporte e controle dos dados;
- O H.323 é muito mais extenso que o SIP, tornando-se mais complexa sua implementação, há a necessidade de um maior esforço do desenvolvedor para entendimento da especificação;

- As mensagens H.323 utilizam representação binária enquanto que o SIP utiliza texto para representação, tornando mais fácil o entendimento deste protocolo;
- O suporte a novos CODECs é livre no SIP, enquanto que no H.323 os CODECs devem ser padronizados pelo ITU, dificultando a inclusão de CODECs de terceiros;
- Os gateways SIP podem trabalhar tanto no modo stateful como no modo stateless, enquanto o H.323 trabalha apenas no modo stateful, mantendo sempre o controle da chamada. Isto pode acarretar perda de performance quando existir uma grande quantidade de chamadas simultâneas.

3.3 Protocolos de Transporte

Os protocolos de transporte RTP/RTCP são definidos pela RFC 3550 do IETF.

3.3.1 RTP

O protocolo RTP permite serviços de entrega fim a fim para a transmissão de dados em tempo real, como por exemplo, transmissão de áudio e vídeo, pode ser utilizado também em comunicações multicast, utiliza o protocolo UDP. O RTP não implementa soluções de QoS, mas permite a aplicação destes métodos, como IntServ e DiffServ que serão discutidos mais à frente.

Mesmo que façam parte de uma mesma comunicação, diferentes tipos de mídia, como áudio e vídeo, são enviados em sessões diferentes de RTP.

O protocolo oferece as seguintes funções:

- Padding: sinaliza a adição de octetos em preenchimento adicional ao conteúdo da carga (payload) sem fazer parte da mesma. Este preenchimento adicional é normalmente utilizado na transmissão de pequenos pacotes ou quando são utilizados algoritmos de encriptação que necessitam um tamanho fixo de blocos;
- Sequence number (número sequencial): esta numeração põe em ordem os diversos pacotes RTP. Este ordenamento serve para o receptor detectar os pacotes perdidos e também restaurar a sequência dos pacotes;
- Timestamp: indica o instante em que o primeiro octeto de dados foi gerado. Quando um pacote de fluxo de mídia chega ao destinatário, o número de sequência é analisado para determinar a sequência correta dos dados e também para registrar a fração de dados perdidos. O valor do timestamping é utilizado para determinar o espaçamento de tempo entre os pacotes. Com estas informações o receptor pode reproduzir o áudio, observando a taxa na qual o fluxo foi codificado;
- SSRC: identifica a fonte de sincronização. Cada participante de uma sessão RTP utiliza um identificador SSRC, este irá identificá-lo de forma única dentro da sessão;
- CSRC: identifica as fontes que contribuíram para a formação dos dados contidos no pacote. Aplica-se a pacotes gerados por mixers. O mixer é posicionado perto

de locais com banda passante reduzida. Ele resincroniza os pacotes que chegam neste ponto, gerando um único pacote, mantendo uma identificação das fontes que contribuíram para esta comunicação, deste modo, as informações são recebidas corretamente no destino.

3.3.2 RTCP

O RTPC é um protocolo de controle e monitoramento empregado nas conexões RTP. É baseada na transmissão periódica de pacotes de controle a todos os participantes da sessão, monitorando a qualidade do serviço e transportando informações dos participantes. (COLCHER et al., 2005)

O RTCP realiza as seguintes funções:

- Feedback sobre a qualidade do serviço: Os receptores indicam a qualidade da recepção relativa a cada emissor (número de pacotes perdidos, jitter e roud-trip delay), estas informações são utilizadas pelos emissores para ajustar parâmetros;
- Sincronização entre meios: pacotes de áudio e vídeo são transportados muitas vezes em streams separados e necessitam ser sincronizados no receptor;
- Identificação dos participantes da sessão: o RTCP é responsável por distribuir o nome canônico dos participantes (CNAME), este garantirá que diferentes mídias sejam reconhecidas como parte de uma única comunicação;
- Controle da sessão: o período entre pacotes RTCP deve ser ajustado dinamicamente à dimensão do grupo (participantes da sessão), procurando que o percentual de tráfego RTCP seja constante no tráfego total, evitando sobrecarregar a rede.

4 CODECs

Este capítulo apresenta os CODECs de voz que podem ser utilizados na comunicação VoIP, diferenciando-os e comparando-os em diversos aspectos.

> *"A palavra CODEC é uma contração de codificador e decodificador e significa um dispositivo que digitaliza sinais de voz ou vídeo para transmissão por serviços de dados digitais e os converte de volta na outra ponta." (CHOWDHURY, 2002, p.263)*

4.1 Codificação de Voz

Um CODEC converte sinais analógicos para digitais, esta conversão é feita por amostragem, desta forma, um fluxo contínuo de informações (analógico), é dividido em um conjunto de amostras (digital) que serão posteriormente transmitidas e decodificadas na outra extremidade.

Quanto mais amostras forem utilizadas no tempo, maior será a fidelidade da amostra reproduzida logo, quanto maior a amostra, melhor a reprodução. Para compensar, os CODECs normalmente efetuam a tarefa de compressão de voz, buscando otimizar a utilização da largura de banda, estes métodos de compressão permitem a reprodução com a mesma fidelidade. Os CODECs podem ser de alta ou baixa complexidade de acordo com o número de ciclos de CPU utilizados nos DSP (Digital Signal Processor).

Os codificadores de voz podem ser classificados da seguinte forma:

- Baseados na forma do sinal (waveform codecs):
  - Recuperam o sinal de entrada sem modelar o processo que gerou o sinal;
  - Podem replicar o som gerado para qualquer tipo de fonte;
  - Não estão otimizados para baixas taxas de bit nem para determinados tipos de fonte sonora;
  - Qualidade de sinal elevada;
  - Largura de banda utilizada elevada;
  - Delay do algoritmo muito baixo.

- Baseados na fonte do sinal (vocoders):

  - O sinal é assumido como sendo unicamente voz e não qualquer forma de onda possível;
  - Codificam apenas o suficiente para inteligibilidade e identificação do interlocutor;
  - Tentam reproduzir o sinal de acordo com modelos matemáticos;
  - Usam um modelo do aparelho de voz humano para imitar o sinal de origem;
  - Transmitem os parâmetros utilizados no modelo, ao invés do sinal amostrado;
  - Utilizam pouca largura de banda;
  - Qualidade de voz baixa;
  - Voz reproduzida parece sintética.

- Híbridos:
  - Utilizam uma combinação de análise da forma do sinal e modelagem da fonte;
  - Boa qualidade;
  - Baixa largura de banda;
  - Mais complexos.

Os algoritmos de codificação/digitalização são padronizados pelo ITU-T, através de recomendações da série G.7XX. Cada um destes algoritmos possui características de desempenho que devem ser consideradas na escolha de um CODEC:

- Qualidade de voz: é medida utilizando uma metodologia chamada MOS (Mean Option Scores), o MOS varia de uma escala de 1 (qualidade ruim) a 5 (qualidade excelente);
- Compensação: também conhecida como ocultação à perda de pacotes. CODECs que possuem esta característica conseguem compensar a perda de algum pacote de voz, fazendo com que o usuário não a perceba;
- Silêncio e ruído: alguns CODECs detectam silêncio ou intervalo sem presença de voz, não o transmitindo, gerando economia de banda;
- Atraso de compressão de voz: tempo necessário para compressão da voz;
- Taxa de produção de amostras digitais: medida em kbit/s.

O ITU-T especificou padrões recomendados para a codificação de voz. A tabela a seguir demonstra a utilização em ambientes de teste, não considerando jitter, atraso, perda de pacotes ou pacotes desordenados.

Tabela 4.1: Comparativo entre CODECs

Padrão	Algoritmo	Taxa de Compressão (Kbps)	Recursos de Processamento Necessário	Qualidade de Voz	Atraso Adicionado	MOS Estimado
G.711	PCM	48, 56, 64 (sem compressão)	Nenhum	Excelente	Nenhum	4,2
G.722	SBC/DPCM	64	Moderado	Excelente	Alto	-
G.723.1	MP-MLQ ou ACELP	5.3, 6.4	Moderado	Boa (6.4) Moderada (5.3)	Alto	3,9 (6.4) 3,7 (5.3)
G.726	ADDPCM	16, 24, 32, 40	Baixo	Boa (40) Moderada (24)	Muito Baixo	4,3
G.728	LD-CELP	16	Muito Alto	Boa	Baixo	4,3
G.729	CS-ACELP	8	Alto	Boa	Baixo	4

Fonte: ITU-T

Em comparação com o modelo MOS, podemos também utilizar o Modelo E. Este modelo computacional complexo avalia e quantifica a degradação da qualidade das ligações, para tal, considera:

- Taxa de transmissão;
- Relação básica sinal-ruído;
- Fator degenerativo simultâneo;
- Fator degenerativo de atraso;
- Fator degenerativo de equipamentos;
- Fator de expectativa.

O E-model resulta em um número chamado de fator R, derivado de atrasos e fatores de deteriorização causados pelos equipamentos. O fator R medido pode ser mapeado por um MOS estimado, varia de 100 (excelente) a 0 (não recomendado). Este modelo é recomendado para avaliação da qualidade das chamadas VoIP.

Para que uma rede possibilite uma boa qualidade da chamada VoIP é recomendado que o atraso fim-a-fim seja menor que 150 ms, um limite máximo de 50 ms para a variação do atraso e taxa de perda limitada a 3%. O não respeito a estes limites gera degradações de qualidade de voz perceptíveis ao usuário.

A seguir, a tabela comparativa entre MOS e Modelo E:

Tabela 4.2: Relação entre Fator R e MOS

Fator R	MOS	Satisfação
$90 \leq R \leq 100$	4,3 – 4,5	Ótima
$80 \leq R \leq 90$	4 – 4,3	Boa
$70 \leq R \leq 80$	3,6 – 4	Mediana
$60 \leq R \leq 70$	3,1 – 3,6	Pobre
$50 \leq R \leq 60$	2,6 – 3,10	Ruim
$00 \leq R \leq 50$	1 – 2,6	Péssima

Fonte: ITU-T

As soluções disponíveis no mercado permitem a utilização de diferentes CODECs de acordo com a rede em questão ou até mesmo alteração do CODEC depois de estabelecida a comunicação.

4.2 G.711

O CODEC G.711 é a escolha natural para redes locais. Baseado em forma de onda, segundo HERSENT, 2002, utiliza uma escala semi-logarítmica chamado de PCM (Pulse Code Modulation), aumentando desta forma os sinais de baixa amplitude enquanto que os de alta amplitude são tratados de forma proporcional, operando de forma análoga ao ouvido humano. Existem dois métodos de compactação para codificar um sinal PCM: *μ-law* e *A-law*. Como exemplo, temos um sinal analógico de 4000 Hz (voz) que é amostrado, quantizado e codificado, gerando um fluxo digital com 8000 amostras por segundo, com 8 bits cada, consumindo 64 kbit/s. O espectro acima de 4000 Hz é cortado na utilização do G.711.

4.3 G.722

O CODEC G.722 oferece uma ótima qualidade de áudio e necessita pouco esforço de processamento, porém, ainda é pouco sensível a erros de transmissão, também baseado em forma de onda. Permite a codificação de 7000 Hz do espectro de voz, consumindo 48, 56 ou 64 kbit/s, utilizando o método de compressão SBADPCM (Sub-band Adaptive Diferencial Pulse Code Modulation).

4.4 G.732.1

Baseado em vocoders, este CODEC pode apresentar problemas de sincronismo caso haja perda de pacotes, podendo necessitar de quadros extras para o reestabelecimento do sincronismo. Possui detecção de presença de voz, transmissão descontinuada e geração de ruído de conforto. Utiliza comprimento de quadro de 30 ms e necessita de 7,5 ms de previsão. Utiliza-se de dois métodos de compressão: MP-MLQ (Multi-Pulse, Multi-Level Quantization), operando a 64 kbit/s ou ACELP (Algebraic Code Excited Linear Prediction), operando a 5,3 kbit/s.

4.5 G.726

Este CODEC, também baseado em forma de onda, utiliza o método de compressão ADPCM (Adaptative Diferencial Pulse Code Modulation) para codificar um fluxo G.711 em palavras de 2, 3 ou 4 bits, resultando em taxas de 16, 24 e 32 kbit/s. Quando utilizado a 32 Kbps atinge a pontuação MOS de 4.3, sendo utilizado como referência para qualidade telefônica.

4.6 G.728

Utilizando o método de compressão LD-CELP (Low-Delay Code Excited Linear Prediction), é um codificador otimizado para voz, baseado em vocoders. Sua pontuação MOS é de 4.3 com uma taxa de apenas 16 kbit/s. Este CODEC modela especificamente sons de voz e funciona comparando a forma da onda a ser codificada com um conjunto de modelos de forma de onda e busca aquele que seja mais parecido. Faz-se então necessário a transmissão apenas do índice da onda mais parecida, da freqüência fundamental da voz e mais alguns parâmetros. A utilização de modems de baixa velocidade obteve bons resultados com a utilização deste CODEC.

4.7 G.729

O CODEC G.729 utiliza o método de compressão CS-ACELP (Conjugate-Structure Algebraic Code-Excited Linear Prediction), produzindo quadros de 80 bits codificando 10 ms de fala a uma taxa de 8 Kbps, exigindo um esquema de previsão de 5 ms. Este CODEC, baseado em vocoders, é bastante popular em aplicações que utilizam voz sobre frame-relay. Permite o envio de ruído de conforto evitando o envio de pacotes normais contendo apenas silêncio.

5 NAT/Firewall e Privacidade/Autenticidade em VoIP

Segurança e eficiência são muitas vezes requisitos conflitantes. Apesar de haver áreas na Internet onde o impacto desses mecanismos de segurança é menor, as aplicações em tempo real como VoIP podem ser seriamente afetadas. A introdução de uma outra camada para garantir a segurança, pode tornar mais lentas as transmissões de pacotes, muitas vezes não sendo aceitáveis para transmissões em tempo real, como alguns mecanismos de criptografia. Logo, vários aspectos devem ser analisados quando se tenta transmitir esses tipos de mídia através de canais seguros. (PASSITO et al., apud BARBIERI, 2002)

Este capítulo irá abordar alguns aspectos de extrema importância e que muito afetarão a implementação proposta mais adiante, como prover a segurança e permitir a comunicação VoIP em redes distintas que utilizam NAT e firewall e também como garantir a privacidade e autenticidade dos dados quando necessário. Verificaremos os problemas que esta estrutura apresenta e possíveis soluções para a mesma.

5.1 NATs e Firewalls em VoIP

Com a utilização de aplicações VoIP, encontramos vários problemas para ultrapassar NATs e firewalls visto que a operação normal destes é baseada em tráfego que pode ser determinado por um conjunto de regras estáticas, o que não ocorre com os protocolos utilizados em VoIP.

O NAT faz a tradução de endereços IPs e portas da rede local, inválidos, para endereços válidos utilizados na Internet. Ou seja, um pacote enviado ou a ser recebido por uma estação de trabalho da rede local passa por um servidor que o traduz num endereço válido quando enviado para a Internet e no endereço correto da rede interna quando este está sendo encaminhado da Internet para uma estação de trabalho.

Como os principais protocolos de transporte (TCP e UDP) utilizam o conceito de multiplexação através de portas de origem e destino, podemos utilizar apenas um endereço IP público para traduzir vários endereços privados, utilizando portas diferentes e armazenando estas informações em uma tabela de conexões.

Apesar de efetuar esta tradução de endereços e permitir a comunicação da rede interna com a Internet, o NAT apresenta os seguintes problemas:

- Não é possível efetuar a tradução de endereços para chamadas iniciadas de fora da rede, não solicitadas. Mesmo que o usuário tenha conhecimento do endereço a que deseja chamar, este não é roteável na rede pública;
- Mensasgens SIP fim-a fim entre clientes também não são roteáveis. As mensagens SIP contêm o endereço IP e porta originais, que serão utilizados pelos fluxos de mídia logo, a comunicação fim-a-fim entre os clientes falha porque estes endereços não são roteáveis na Internet;
- Após algum tempo, o NAT encerra qualquer conexão UDP caso nenhum pacote esteja sendo transmitido, se um dos lados está apenas ouvindo e não transmite nenhum pacote, esta conexão será encerrada, considerada pelo NAT uma conexão inativa.

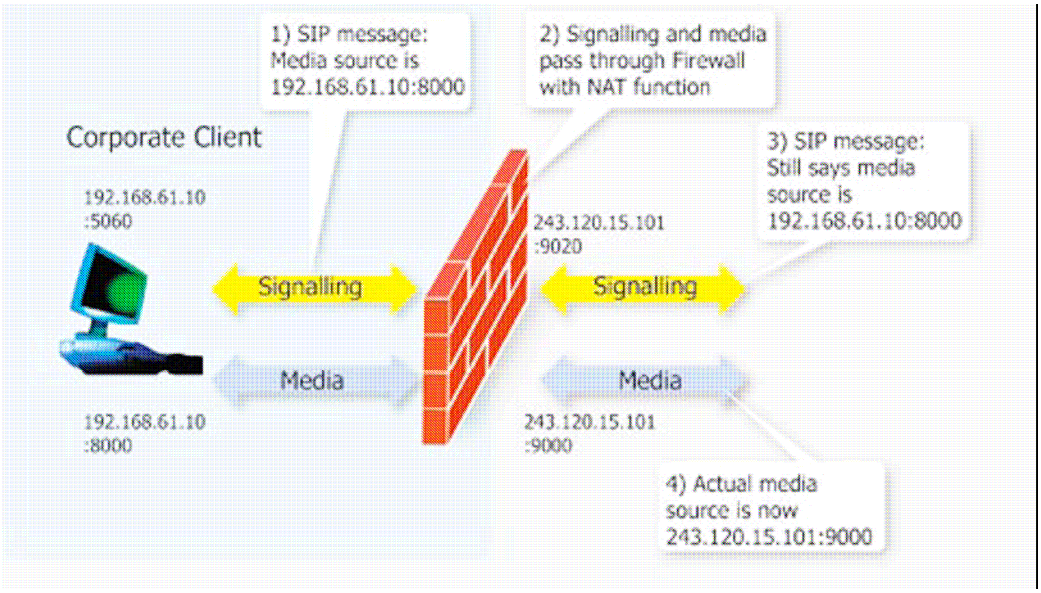

Figura 5.1: NAT bloqueia fluxo de mídia fim-a-fim (Newport Networks, 2006)

O firewall tem como objetivo proteger a rede privada de ser acessada por fontes não autorizadas. Este controle é feito através do bloqueio de tráfego baseado em três parâmetros: fonte, destino e tipo de tráfego. Basicamente, o firewall permite que pacotes vindos da rede privada alcancem a rede pública e controla os pacotes vindos da rede pública, permitindo normalmente a passagem de pacotes associados a uma conexão iniciada internamente.

Enquanto que um firewall é capaz de abrir e fechar portas dinamicamente, como a sinalização VoIP requer, ela fica sem efeito para fluxos de mídia que chegam de redes externas.

Muitos administradores são relutantes em modificar esta política, permitindo comunicação irrestrita nos dois sentidos, devido a sérios riscos criados. Qualquer solução

deve fornecer segurança na comunicação em ambos os sentidos, sem afetar em grandes modificações nas regras e sem reduzir o nível de segurança existente.

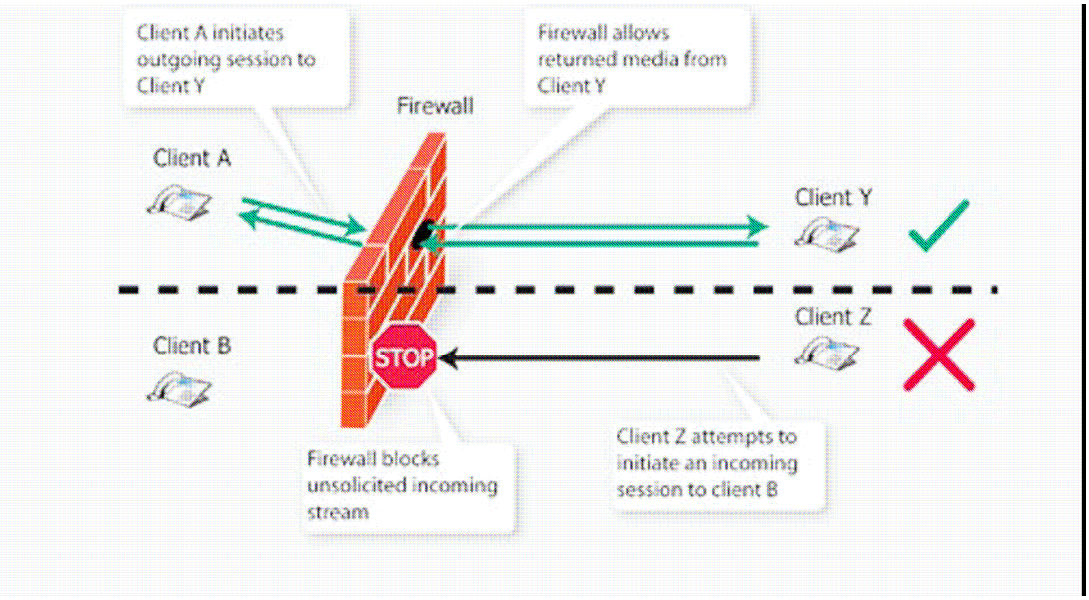

Figura 5.2: O problema do firewall (Newport Networks, 2006)

Qualquer abordagem para solucionar os problemas anteriormente listados, deve permitir uma comunicação segura nos dois caminhos, incluindo chamadas não solicitadas e também minimizar dependências na atualização de NATs e firewalls.

As aplicações VoIP precisam descobrir e utilizar o endereço e porta externo que é selecionado pelo NAT na sinalização. O cliente VoIP, de posse dessas informações pode colocá-los dentro da sinalização para estabelecer a chamada, assegurando a conectividade fim-a-fim, porém, precisa encontrar um meio de utilizá-lo também na transmissão dos fluxos de mídia.

Serão descritos a seguir alguns mecanismos para resolver estes problemas.

5.1.1 Universal Plug and Play (UPnP)

Esta tecnologia foi desenvolvida para pequenos usuários de escritórios e domésticos.

Ela foi projetada para tratar várias questões, não apenas VoIP. UPnP permite que aplicações cliente descubram e configurem componentes de rede, mapeando portas internas para portas externas.

Um cliente pode perguntar ao NAT um endereço particular IP e porta, que o NAT selecionou para sinalização e transmissão, através do protocolo chamado UPnP. Obtendo

esta informação, o cliente VoIP pode utilizá-la na sinalização e estabelecer a chamada, utilizando endereços e portas públicas roteáveis, efetuando assim conexões fim-afim.

No entanto, esta abordagem não resolve o problema de segurança de forma satisfatória, existe um pequeno número de fabricantes comprometidos em usar UPnP, muitos User Agents e NATs não o suportam.

É um método que pode ser implementado em pequenas redes.

5.1.2 Simple Traversal of UDP Trought Network Address Translators (STUN)

Este protocolo permite que o cliente descubra se está atrás de um NAT e determine o tipo de NAT que a rede possui.

A proposta deste protocolo define um servidor especial para informar o cliente SIP STUN-enabled, na rede privada, qual o endereço utilizado na rede pública para cada sessão, este endereço será utilizado na mensagem de estabelecimento da chamada.

O servidor STUN efetua este processo examinando as mensagens que chegam ao servidor, mas não se preocupa com sinalização ou transmissão de dados.

O STUN confia que uma vez mapeada a porta pelo servidor STUN, qualquer tráfego de entrada ou saída será capaz de usar o mapeamento na direção reversa e atingir a porta de recepção do cliente. Com isso, o NAT fica susceptível a ataques e cria problemas de segurança, introduzindo riscos adicionais ao firewall.

O STUN recebeu uma atenção, como uma técnica, pelo IETF, porém, alguns problemas foram identificados. O STUN não funciona com NAT simétrico, que é o tipo de configuração mais comum encontrado nas corporações e também não trata a necessidade de suportar dispositivos SIP baseados em TCP.

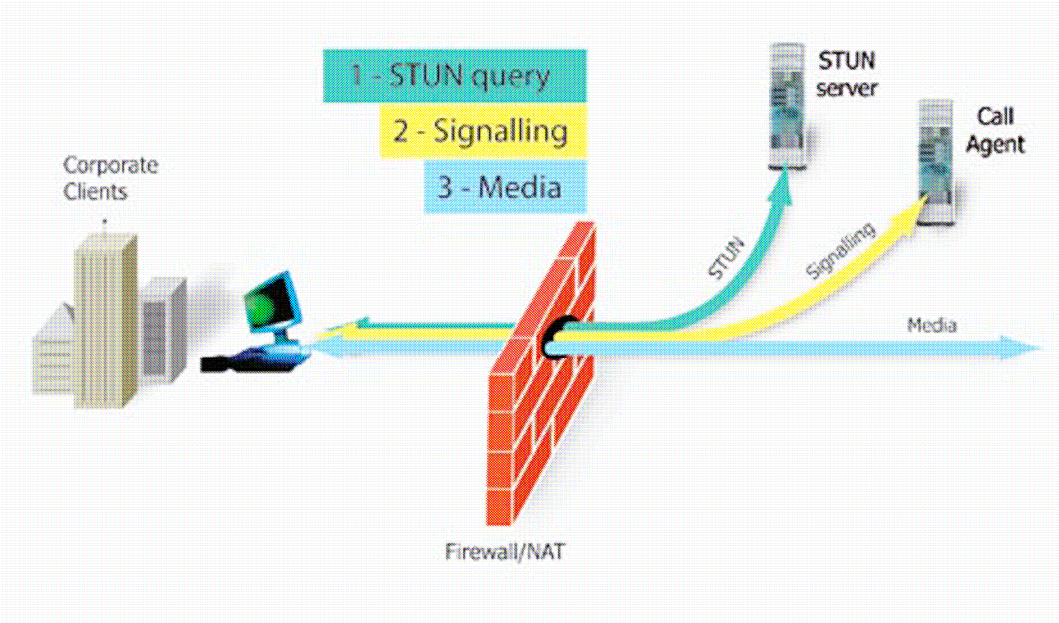

Figura 5.3: STUN (Newport Networks, 2006)

5.1.3 Traversal Using Relay NAT (TURN)

O IETF propôs um mecanismos adicional, TURN, com o objetivo de resolver o problema de NATs simétricos, problema este não resolvido pelo STUN.

O TURN se baseia num servidor que é inserido no caminho da sinalização e mídia, localizado na DMZ ou no provedor de serviços de rede, este provê um endereço externo que atua como relay e garante que o tráfego alcançará o endereço interno, ele atua como um intermediário entre o endereço origem e destino.

O cliente SIP TURN-enabled envia um pacote exploratório para o servidor TURN, que responde informando o IP e porta pública utilizada pelo NAT, utilizando-se desta informação no estabelecimento da chamada SIP e na transferência de dados. Neste caso, não há como o NAT ver o endereço de destino, podendo então ser utilizado o NAT simétrico. Além disso, alguns itens de segurança foram associados ao TURN, aumentando sua aceitação.

O TURN aumenta o consumo de banda uma vez que os dados são transmitidos duas vezes, da origem ao servidor TURN e do servidor TURN ao destino.

Este método adiciona uma complexidade, logo, requer que os softphones dos clientes sejam atualizados pelos desenvolvedores para suporta-los, o que gera sempre uma relutância na utilização.

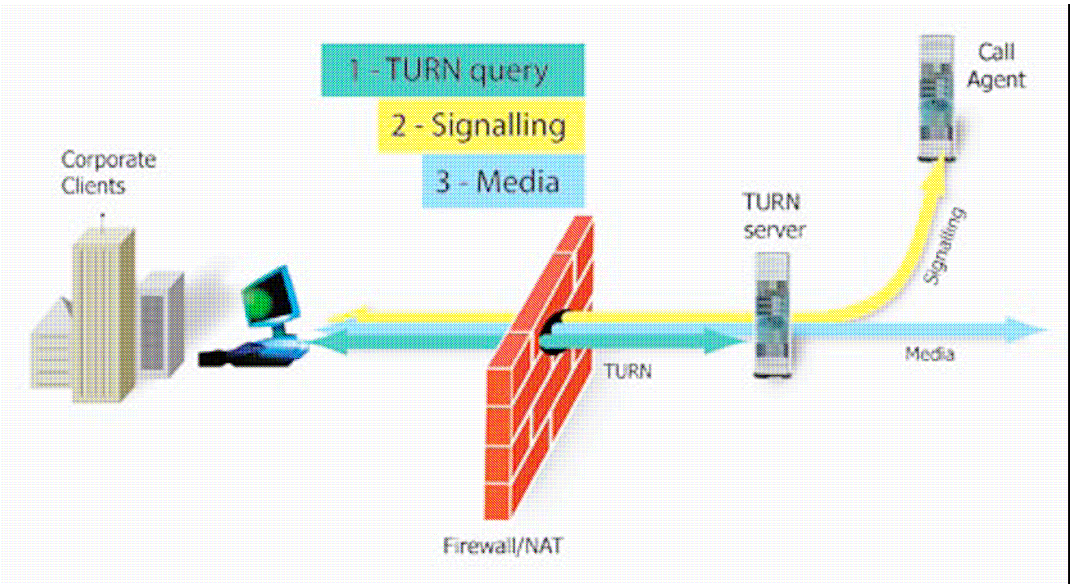

Figura 5.4: TURN (Newport Networks, 2006)

5.1.4 Application Layer Gateway (ALG)

Esta técnica se baseia na instalação de um novo NAT/firewall, chamado ALG que entende as mensagens de sinalização SIP e as altera para permitir a comunicação VoIP fim-a-fim.

Esta técnica processa a sinalização e o tráfego, alterando a sinalização de forma a refletir o endereço IP e porta pública utilizados para a sinalização e posterior tráfego de mídia. ALG tem a vantagem de ser transparente para User Agents e servidores VoIP.

Como dito anteriormente, esta técnica requer a substituição do NAT/firewall, alternativamente, alguns fabricantes provêm atualizações de software para suportar as funcionalidades do ALG.

O ALG requer prática para configurações e administração de NAT e firewall, indicando que upgrades ou atualizações não são simples. ALG deve ser implementado de forma cautelosa em grandes corporações que possuam suporte adequado.

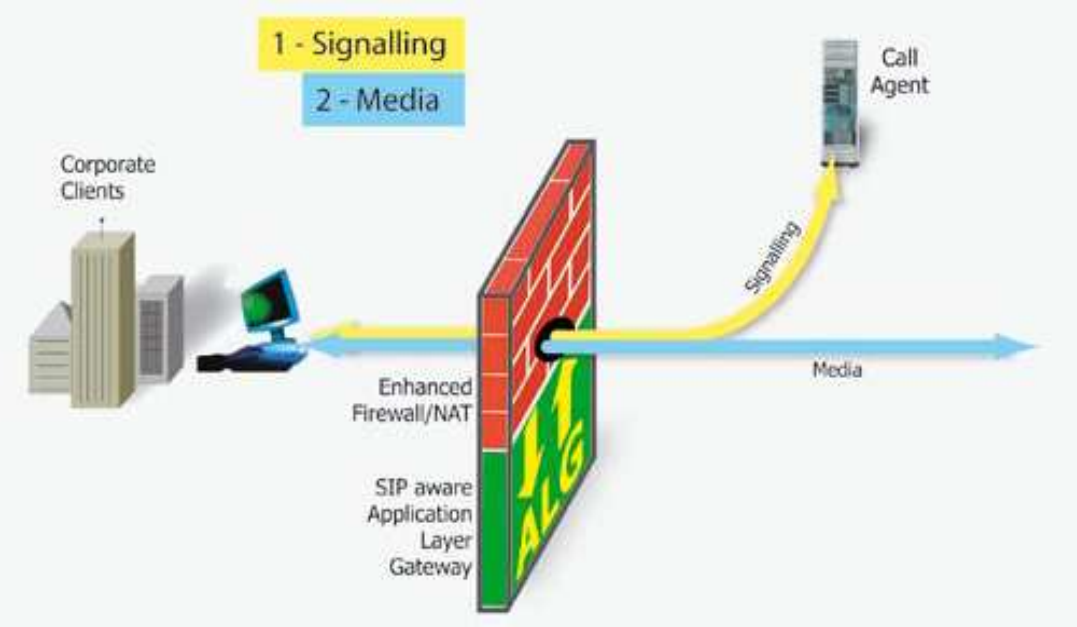

Figura 5.5: ALG (Newport Networks, 2006)

5.1.5 Configuração Manual

Esta técnica é recomendada apenas para pequenas redes, em virtude de ser manual e necessitar configurações fixas.

O cliente neste caso é configurado com detalhes de endereço IP e porta pública que o NAT utilizará para sinalização e tráfego de mídia e também terá IP e porta fixo para receber as mesmas informações.

O NAT também é configurado manualmente com mapeamento estático para cada cliente.

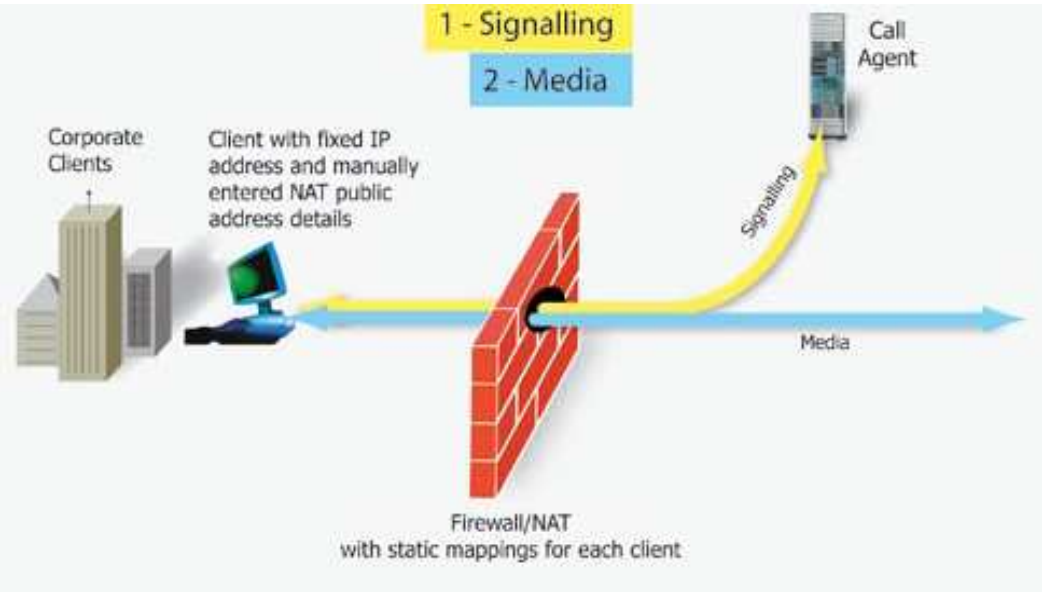

Figura 5.6: Configuração Manual (Newport Networks, 2006)

5.1.6 Técnicas de Tunelamento

Este método utiliza tunelamento para atravessar NAT e firewall. Ele requer a existência de um servidor dentro da rede privada e outro na rede pública, criando um túnel não criptografado entre eles, transportando todo o tráfego SIP por um firewall reconfigurado. Este método pode ocasionar atrasos, reduzindo desta forma a qualidade da voz.

O servidor externo modifica o sinal para refletir a porta de saída permitindo ao sistema VoIP efetuar e receber chamadas.

Este método produz pequenas mudanças nas políticas de segurança, mas pode criar riscos adicionais por possuir um servidor externo, vulnerável e que pode ser utilizado para acessar a rede interna.

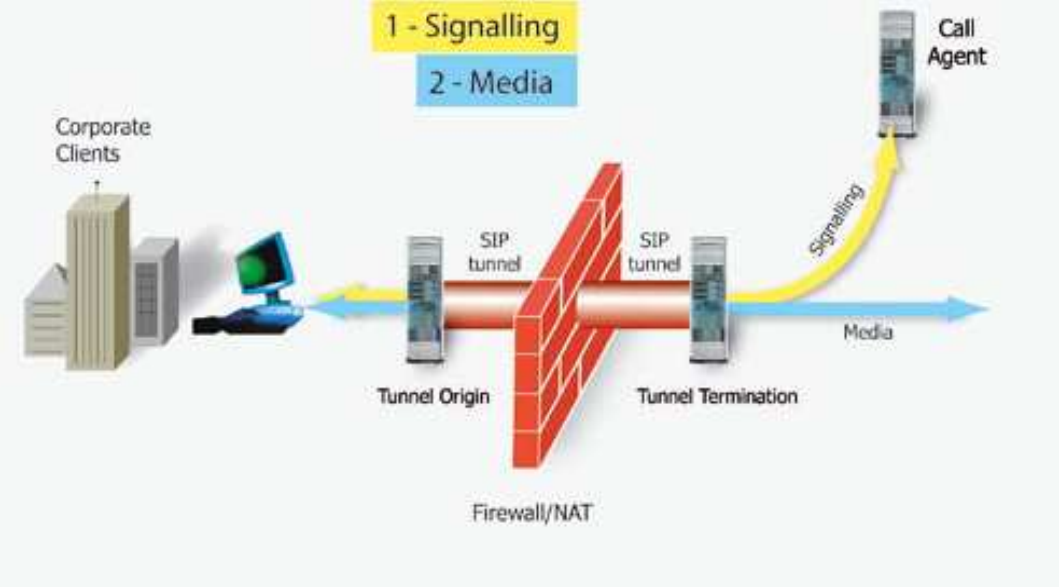

Figura 5.7: Tunneling (Newport Networks, 2006)

5.1.7 Automatic Channel Mapping (ACM)

O Newport Networks 1460 session border controller, equipado com a aplicação ACM é especificamente desenvolvido para resolver problemas de NAT e firewall, sem necessitar alterações nas regras de segurança. Ele habilita traduções de endereços de rede (NAT) e firewall para acesso seguro à rede.

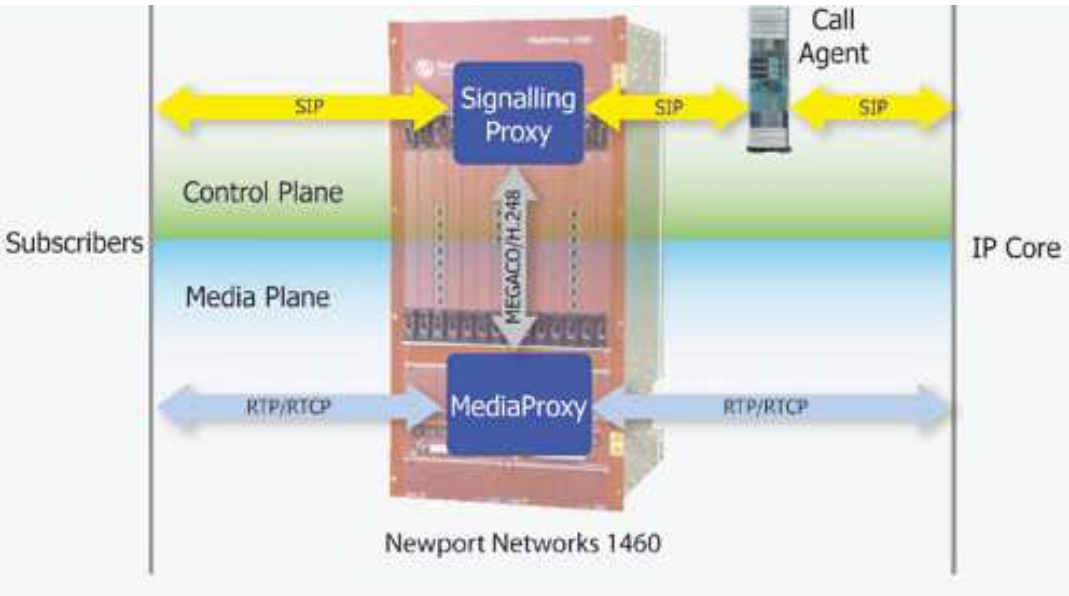

Figura 5.8: Newport Networks 1460 session border controller (Newport Networks, 2006)

Para resolver o problema de tradução de endereços são utilizados os seguintes componentes: Signalling Proxy e Media Proxy.

O signalling proxy tem como função fazer com que endereços não roteáveis da rede privada sejam repassados à rede pública. O signalling proxy age como um B2BUA (back to back user agent) de alta performance. Este proxy é configurado como um ponto de transição para mensagens de sinalização SIP entre o cliente e o servidor, garantindo que todas as mensagens passem por ele.

As mensagens de sinalização SIP destinadas ao signalling proxy deixam a rede privada utilizando IP e porta alocados pelo NAT. Quando o signalling proxy recebe a mensagem inicial (User Agent) , um endereço de origem no signalling proxy é alocado para as mensagens de sinalização deste cliente. Uma mensagem de registro modificado é encaminhada para o Call Agent, indicando o signalling proxy como origem.

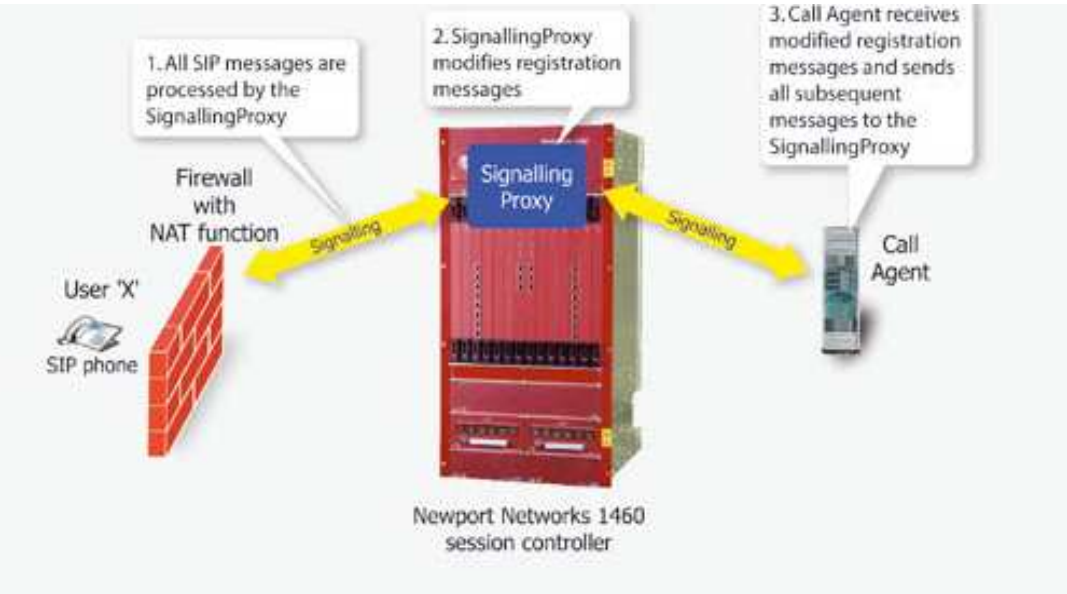

Figura 5.9: Signalling Proxy (Newport Networks, 2006)

O media proxy opera por baixo do controle do signalling proxy para prover um ponto de trânsito para streams RTP e RTCP entre agentes.

Para garantir que o provedor de serviço tenha total visibilidade e controle do stream de mídia, garantindo qualidade de serviço, toda a mídia é direcionada para o media proxy.

O media proxy usa NAT dinâmico para esconder detalhes da rede, ajudando a prover proteção contra DoS, negação de serviço.

Na utilização de NAT as portas alocadas para fluxos de mídia para cada cliente são imprevisíveis. Utilizando o Newport Network o signalling proxy manipula as mensagens de sinalização, garantindo desta forma que os streams de mídia sejam direcionados para portas alocadas dinamicamente no media proxy.

O signalling proxy e o media proxy utilizam o protocolo interno MEGACO/H.248 para troca de informações.

Quando o User Agent inicia uma chamada, o signalling proxy recebe uma mensagem e se comunica com o media proxy para obter informações do NAT. O IP de origem e o campo SDP são então modificados, definindo o signalling proxy como caminho de retorno para sinalização e o media proxy como caminho de retorno da mídia.

O endereço IP e porta utilizados pelo NAT são facilmente determinados lendo-se os detalhes do stream de mídia. Logo, todos os fluxos de sinalização passam pelo signalling proxy enquanto que todos os fluxos de mídia passam pelo media proxy, permitindo ao provedor de serviço todo o controle da conexão.

Resolver o problema do firewall significa prover segurança na entrada de mídias não solicitadas, IPs e portas desconhecidas.

No Newport Network, o media proxy age como um ponto de transição entre as sessões de mídias, que são sempre iniciadas dentro do firewall, enviadas por IP e porta do media proxy dinamicamente alocados para a sessão. O media proxy aprende então o endereço público de origem, retornando o stream de entrada para o mesmo endereço e porta.

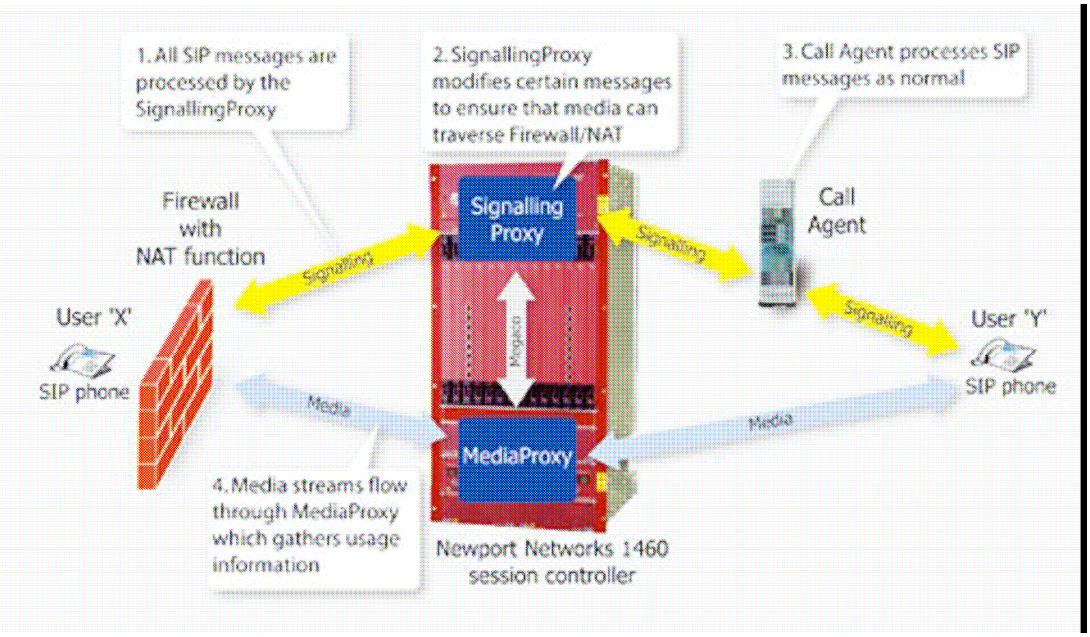

Figura 5.10: Garantindo o fluxo de mídia fim-a-fim (Newport Networks, 2006)

5.2 Privacidade/Autenticidade em VoIP

Além dos problemas mencionados nas sessões anteriores, nos deparamos muitas vezes também com a necessidade de prover privacidade e/ou autenticidade dos dados.

Confidencialidade ou privacidade é a garantia que a informação não estará disponível a pessoas não autorizadas, normalmente este processo é feito com utilização de criptografia.

Já a autenticidade é a garantia da origem da informação e juntamente com a integridade garantem que a mesma também não sofreu alterações.

A seguir, serão descritas quatro formas de prover privacidade e autenticidade em VoIP. É importante salientar que, exceto em VoIP sobre SSL, os demais protocolos provêem apenas segurança de mídia e não na sinalização.

5.2.1 IP Security

O protocolo IPSec é amplamente utilizado para prover segurança em ambientes corporativos, uma vez que o protocolo IP não possui nenhuma característica de segurança.

O IPSec introduziu criptografia, autenticação, validação de integridade e anti-replay. Pode ser utilizado para proteger uma comunicação fim-a-fim ou entre dois sistemas intermediários, chamados gateways de segurança, conectados aos sistemas finais.

O IPSec oferece criptografia e autenticidade, sendo necessário a utilização do mesmo algoritmo e chaves criptográficas pelas partes comunicantes. O IPSec utiliza uma associação segura (AS) para gerenciar as particularidades da sessão.

O IPSec utiliza os seguintes protocolos:

- Authentication Header (AH): provê autenticação da origem, checagem de integridade da mensagem e anti-replay. O payload não é encriptado, apenas há modificação no cabeçalho;
- Encapsulating Security Payload (ESP): provê checagem da integridade da mensagem, confidencialidade dos dados, anti-replay e autenticação.

E também possui dois modos de conexão:

- Modo túnel (TS 33.210 – interconexão e núcleo): este modo é utilizado para interconexão de redes, o tráfego é capturado por um gateway de segurança e criptografado;
- Modo transporte (TS 33.203 – acesso): este modo é utilizado para garantir segurança em comunicações fim-a-fim, somente o segmento da camada de transporte é criptografado e autenticado.

No modo transporte AH, o payload e o cabeçalho IP são protegidos com a inserção de um novo cabeçalho entre o original e o payload. No modo túnel, todo o pacote IP é encapsulado dentro do AH e de um novo cabeçalho IP, contendo, por exemplo, o endereço do gateway de segurança.

O cabeçalho AH permite a detecção de pacotes fora de seqüência, autenticação do remetente e também protege a integridade do cabeçalho e do payload. Ao receber o pacote, o destinatário recalcula o hash e verificando diferenças, descarta o pacote.

Desta forma, IPSec AH é incompatível com NAT, já que o NAT altera o cabeçalho do pacote e o destinatário, verificando esta alteração, descartará o pacote.

Já no modo de conexão ESP em modo transporte e túnel os dados são encapsulados e anexados ao cabeçalho IP original. No modo transporte apenas o payload do pacote TCP ou UDP é encapsulado, enquanto que no modo túnel todo o pacote é encapsulado. Neste caso, não é checado se a parte criptografada está de acordo com a parte não criptografada, permitindo assim atravessar o NAT.

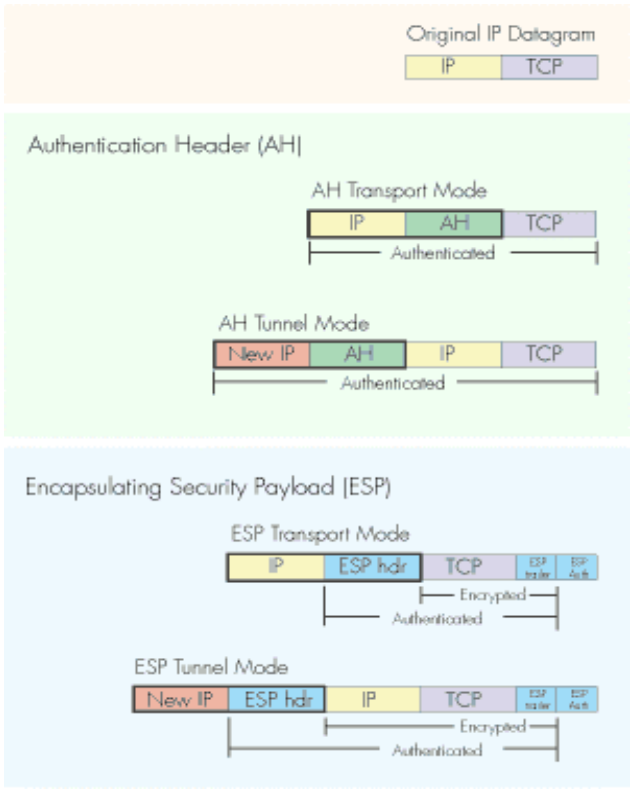

Figura 5.11: Protocolo IPSec (Newport Networks, 2006)

O ESP com autenticação provê a segurança necessária para prover um caminho seguro para aplicações de sinalização VoIP.

O problema na utilização do NAT com IPSec consiste em que NATs são utilizados para mapear vários dispositivos numa rede privada, alterando o protocolo de transporte TCP e UDP. Ocorre que quando o NAT encontra um pacote IPSec ESP ele irá traduzir o IP privado para um IP público. O problema ocorre quando vários IPSec precisam se comunicar com o mesmo servidor, pois o IPSec encapsula e esconde a informação da porta que o NAT necessita para criar ligações únicas, ocasionando que várias conexões tentarão acessar o mesmo servidor, utilizando o mesmo IP e porta, desta forma, não há como retornar o tráfego para o telefone correto.

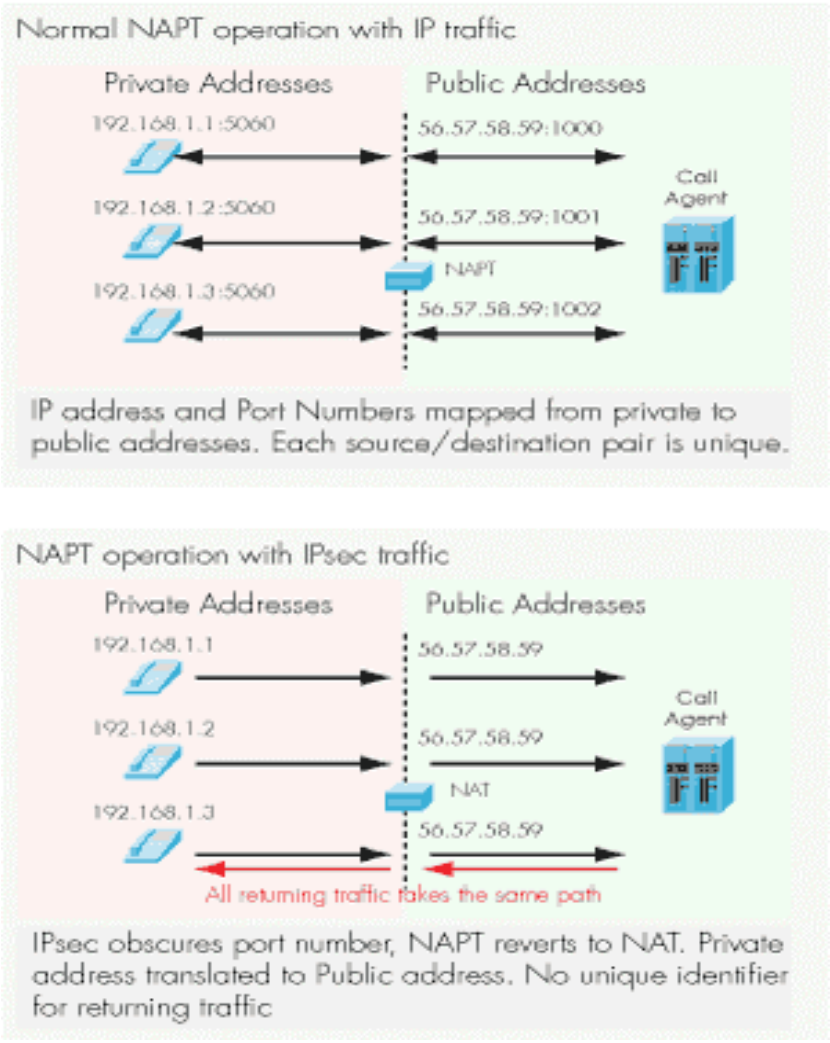

Figura: 5.12: Operação de NAT com IP e IPSec (Newport Networks, 2006)

O TISPAN (Telecoms & Internet Converged Services & Protocols for Advanced Networks) oferece uma solução alternativa para garantir segurança na sinalização do telefone ao servidor numa rede. Ele reconhece que transpor o NAT não é possível com as soluções de segurança do IMS security framework (TS 33.203) e propõe a utilização de UDP encapsulando IPSec, de acordo com a RFC 3948.

Este encapsulamento ocorre em dois estágios, primeiro, a mensagem original é encapsulada utilizando IPSec ESP, que é encapsulado em outro cabeçalho UDP. Esta mensagem é então enviada utilizando-se a porta 4500. O NAT pode trocar o IP de origem e a porta sem afetar o payload do IPSec. O processo inverso é chamado de De-encapsulamento.

Desta forma, o NAT pode ser ultrapassado, efetuando a tradução de endereço e porta de forma normal. Sendo uma extensão do IMS security framework, outros mecanismos, como troca de chaves, permanecem inalterados.

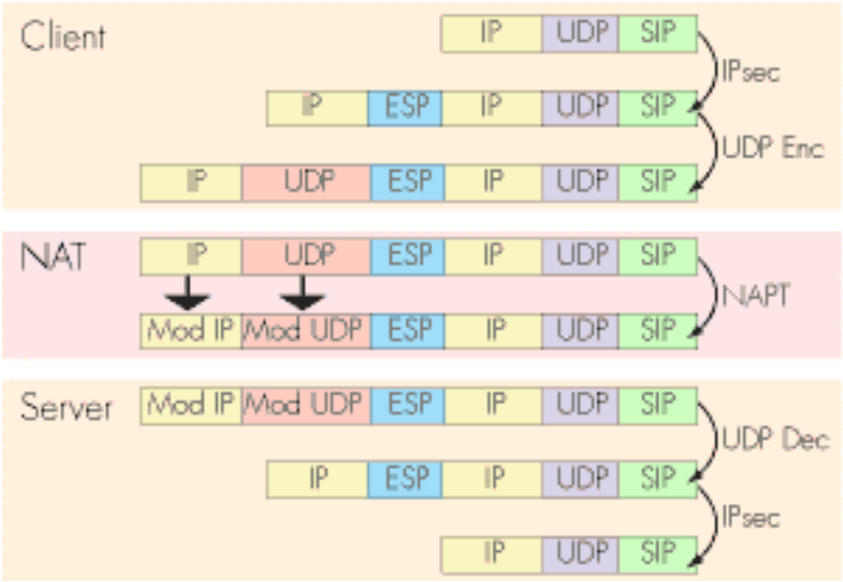

Figura 5.13: UDP encapsulando IPSec (Newport Networks, 2006)

Além das questões expostas acima, o IPSEC necessita introduzir novos cabeçalhos no datagrama IP para oferecer os serviços de segurança, aumentando consideravelmente o tamanho do datagrama. (HERSENT, 2002)

Uma conseqüência desse aumento é que a taxa do tamanho atual do payload em relação ao tamanho total do pacote se degrada, diminuindo a carga útil transportada na banda. Esse aumento do pacote não reflete negativamente apenas na banda, mas também impacta nos atrasos de transmissão, roteadores, enfileiramentos, enfim, no atraso total dos pacotes. (PASSITO et al., apud BARBIERI, 2002)

5.2.2 SRTP

Com a ausência de definição de meios para implantar segurança em RTP/RTCP, o IETF elaborou a RFC 3711, de março de 2004, que definiu os protocolos SRTP (Secure Real-Time Transport Protocol) e o SRTCP (Secure RTP Control Protocol).

O SRTP oferece confidencialidade, autenticidade e proteção contra replays dos pacotes RTP, prevenindo desta forma ataques como escuta do RTP, manipulação do SSRC (Synchronization Source) e manipulação do CODEC. Assim como o RTP, o RTCP possui também um protocolo para prover segurança, o SRTCP, que possui as mesmas características de segurança do SRTP.

Para evitar a manipulação dos protocolos de sinalização e também a utilização do tráfego de áudio por terceiros, faz-se necessário a utilização de criptografia, desta forma, mesmo capturados por terceiros, os dados serão inúteis, não sendo possível ouvir a conversa.

O SRTP utiliza o protocolo Multimídia Internet Keying (MIKEY) para gerenciamento das chaves, este utiliza um sistema de chaves pré-compartilhadas, infra-estrutura de chave pública e o algoritmo Diffie-Hellman para troca das chaves.

A RFC define a utilização do algoritmo AES (Advanced Encryption Standard), de 128 bits, de chave simétrica para criptografia de mídia, proporcionando um nível de segurança elevado para o tráfego de áudio e define a utilização do HMAC-SHA1 para autenticação e integridade.

O payload do RTP é encriptado e encapsulado em um pacote SRTP, este se baseia em uma chave de encriptação, uma função hash para autenticação da mensagem e no número seqüencial do RTP, não efetuando nenhuma alteração no cabeçalho do RTP. O SRTP inclui no cabeçalho um campo adicional chamado Authentication Tag, que possui dados de autenticação da mensagem e um campo chamado MKI (Master Key Identifier), ambos opcionais.

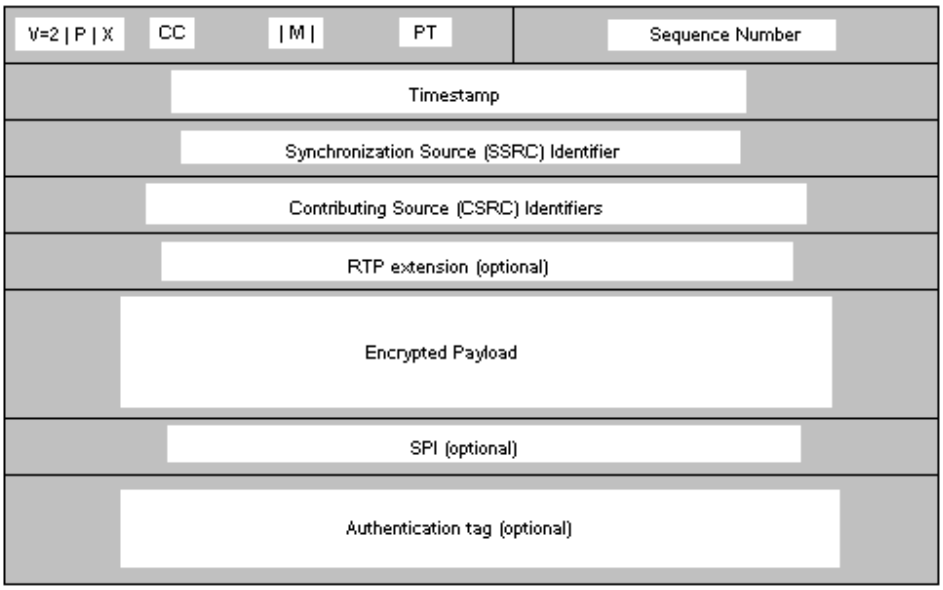

Figura 5.14: SRTP Header (Snom VoIP Phones, 2006)

Acima está representado o cabeçalho do pacote SRTP, desta forma é garantido confidencialidade ao payload e integridade para todo pacote RTP.

Apesar da implantação da segurança, o SRTP provê uma alta vazão com pouco overhead adicional nos pacotes dos fluxos de dados, sendo desta forma adequado para ambientes heterogêneos.

5.2.3 zRTP

O zRTP é um protocolo para criptografia de áudio que utiliza o algoritmo Diffie-Hellman para troca de chaves seguras, ele provê confidencialidade e proteção contra ataques Man in the Middle.

Este protocolo gera um segredo compartilhado que será utilizado posteriormente para gerar as chaves, passando assim para uma sessão SRTP. Este procedimento é efetuado durante a chamada e é transportado na mesma porta utilizada pelo stream de mídia RTP, esta sessão é estabelecida normalmente por um protocolo de sinalização, por exemplo, SIP. (Zfone Project, 2008)

O protocolo não requer um segredo compartilhado anteriormente, infra-estrutura de chave pública ou autoridades certificadoras, as chaves Diffie-Hellman são geradas no estabelecimento de cada sessão. (Zfone Project, 2008)

O algoritmo Diffie-Hellman sozinho não provê segurança contra ataques Man in the Middle, para autenticar a troca de chaves o zRTP utiliza o Short Authentication String (SAS), que é um hash de dois valores Diffie-Hellman. Este valor é distribuído para os dois

pontos finais da chamada e conferido durante a conexão para garantir autenticação. A alteração deste valor indica ataque Man in the Middle e a não alteração indica uma alta probabilidade do ataque não ter ocorrido. (STALLINGS, 2003)

O zRTP provê um segundo nível de autenticação contra ataques Man in the Middle utilizando um hash da chamada anterior juntamente com o segredo compartilhado da próxima chamada, portanto, se não há ataque na primeira chamada, este também não deverá ocorrer nas subseqüentes.

O IETF pretende adicionar ainda proteção de integridade nas informações da sessão SIP e esta proteção utilizará a infra-estrutura de chave pública, adicionando assim mais proteção contra ataques Man in the Middle.

5.2.4 VoIP sobre SSL

O SSL (Secure Sockets Layer) é um protocolo que visa estabelecer uma comunicação segura entre dois pontos na Internet, provendo autenticidade, integridade e confidencialidade dos dados. O SSL ajuda a prevenir que intermediários tenham acesso indevido ou alterem os dados que estão sendo transmitidos.

O protocolo é composto de três fases:

- Handshake: estabelecimento da conexão;
- Cálculo de chaves: autenticação
- Transferência de dados: utilizando criptografia.

SSL necessita de certificados, emitidos por autoridades certificadoras, que possuem informações como o nome da entidade que o forneceu e o time stamp. Além do certificado, dois tipos de chaves são utilizadas pelo protocolo, chaves privadas são utilizadas pelos servidores e nunca são distribuídas e chaves públicas são distribuídas para os clientes. Dados criptografados com a chave pública só podem ser decriptografados com a chave privada.

Chamadas VoIP normalmente não são criptografadas, a utilização do protocolo SSL pode ser utilizado quando a confidencialidade se faz necessária. Desenvolvedores VoIP podem integrar o protocolo SSL em suas aplicações, o mais fácil é utilizar o SSL nos protocolos de sinalização.

6 QoS EM VoIP

Este capítulo irá tratar dos problemas e dos mecanismos necessários para se obter a qualidade de serviço desejada nas aplicações VoIP. Serão verificados os parâmetros que devem ser considerados para obtenção de qualidade, os mecanismos utilizados para obtenção de QoS e como as principais arquiteturas, IntServ e DiffServ, provêm QoS e buscam um melhor desempenho no encaminhamento de pacotes em uma rede IP.

É preciso definir claramente os parâmetros de vazão, atraso, jitter e perda quando se espera a obtenção de qualidade de serviço (QoS) em uma aplicação VoIP.

O desafio é construir um sistema de comunicação genérico que dê suporte às diversas mídias e às características de tráfego por elas impostas, de acordo com os níveis de qualidade almejados pelas aplicações. (COLCHER et al., 2005)

6.1 Métricas de QoS

Para que obtenhamos QoS é necessário considerar os seguintes parâmetros:

- Vazão: é o parâmetro básico de QoS, qualquer aplicação necessita de banda para operar adequadamente;
- Atraso: é a soma dos atrasos impostos pela rede e equipamentos utilizados na comunicação, este atraso ou latência implica em um tempo de resposta da aplicação. Os principais fatores que influenciam na latência da rede são o atraso de propagação, velocidade de transmissão e processamento nos equipamentos.
- Jitter: é a variação no atraso, pode se dar em função da variação do tempo ou até da sequência de entrega de pacotes, em aplicações VoIP é necessário que as informações sejam processadas em períodos de tempo bem definidos e que os pacotes sejam entregues na ordem correta;
- Perdas: as perdas de pacotes ocorrem por erro e congestionamento (descarte), em aplicações VoIP é preciso garantir limites razoáveis de perda para que a voz digitalizada tenha uma qualidade aceitável.

A garantia de QoS implica na atuação em todos os equipamentos envolvidos na comunicação fim-a-fim, garantindo a entrega da informação do host de origem até o host de destino. Quando tratamos de QoS em VoIP, precisamos considerar principalmente atraso, jitter e perda de pacotes.

6.2 Provisão de QoS

A solicitação de QoS da aplicação é expressa e solicitada por um contrato de serviço chamado de SLA, Service Level Agreement. Ela é garantida pela rede, seus componentes e equipamentos. A SLA deve definir claramente os requisitos necessários para obtenção da qualidade.

A provisão de QoS é efetuada em diferentes fases do ciclo de vida de um serviço:

- Solicitação do serviço: caracterização do tráfego e especificação da QoS a ser aplicada, implica na alteração do estado interno da rede;
- Estabelecimento de contratos de serviços: aplicação gera fluxos em conformidade com o que foi especificado na solicitação do serviço;
- Manutenção do contrato de serviço: a rede deve empregar mecanismos apropriados de forma a manter o nível de QoS solicitado pela aplicação;
- Término do contrato de serviço: aplicação informa à rede a intenção de finalizar o controle estabelecido, liberando os recursos.

6.3 Mecanismos de QoS

Uma vez identificadas as métricas para obtenção de QoS, verificaremos os mecanismos, algoritmos e protocolos utilizados na implementação da qualidade de serviço. Numa rede IP, a garantia de QoS consiste num mecanismo fim-a-fim, atuando em todos os equipamentos envolvidos e garantido a entrega da informação. Os mecanismos que serão implementados nos equipamentos devem atuar de forma integrada e cabe ao gerente de TI a escolha e implementação dos mecanismos adequados.

6.3.1 Tratamento de Filas

Para que haja controle de admissão e escalonamento dos pacotes é necessário que o tráfego seja classificado conforme algum critério, possibilitando um tratamento diferenciado nas demais etapas. A classificação deve ser efetuada o mais próximo possível da origem.

Algoritmos de prioridade são mecanismos utilizados pelo equipamento de rede para garantia de QoS, tipicamente implementados em roteadores. A definição de prioridades prevê diferentes tempos de espera para o processamento de informações.

A priorização de pacotes em aplicações VoIP provê largura de banda, evitando ou diminuindo atraso, jitter ou perda de pacotes. Um problema deste mecanismo é que pacotes de baixa prioridade podem ter muito atraso ou nunca serem processados.

O tratamento das filas se dá baseado na classificação feita anteriormente, que pode ser das seguintes formas:

- IP Precedence:

A priorização de pacotes se dá com a utilização do campo TOS (type of service) do cabeçalho IP, especificando desta forma, uma classe de serviço para cada pacote. São utilizados três bits para marcar um pacote com a classe desejada, quando este entra na rede. O tratamento é associado à classe identificada, para cada tipo de tráfego é definido um valor específico.

Os roteadores que suportam este mecanismo devem utilizá-lo em qualquer ponto cujo processamento esteja relacionado com a alocação de recursos finitos como buffers.

- Priority Queueing:

A priorização dos pacotes é feita de forma rígida, o pacote de maior prioridade sempre será enviado primeiro. O mecanismo permite atribuir níveis diferentes de prioridade para tráfego com diferentes importâncias.

Existem quatro filas neste mecanismo, alta, média, normal e baixa sendo que pacotes não classificados são colocados na fila normal.

Tráfego de voz, devido à baixa tolerância a perda de pacotes e atrasos devem ser colocados em uma PQ. É preciso ter cuidado pois, em casos extremos, se o fluxo prioritário ocupar toda a banda, o tráfego de menor prioridade pode sofrer um grande atraso ou nunca ser atendido.

6.3.2 Controle de Admissão

Para que não ocorram congestionamentos, deve-ser considerado também o descarte de pacotes quando necessário, proporcionando a igualdade na distribuição de banda e processamento.

Os mecanismos de controle de admissão determinam se um novo fluxo de dados será aceito ou não, procurando não comprometer os fluxos previamente aceitos. Congestionamentos ocorrem normalmente por falta de buffer em algum ponto da rede. Estes mecanismos não agem de forma pró-ativa e podem ser parte integrante dos mecanismos de escalonamento.

Os controles são implementados com a utilização de métodos como Token Bucket e suas demais variações.

6.3.3 Escalonamento de Filas

Este mecanismo é utilizado para que a banda e o processamento sejam distribuídos de forma justa entre os fluxos, procurando garantir que cada stream obtenha os recursos que lhe foi alocado.

A função básica do escalonamento é implementar uma política para servir os pacotes na fila de saída.

Abaixo estão descritos alguns dos algoritmos de escalonamento:

- FIFO (First In First Out):

Este algoritmo é apenas um mecanismo de armazenamento e repasse (store and forward), não implementando nenhum tipo de QoS. Tratamento default nos roteadores, pacotes são enviados estritamente na ordem em que são recebidos.

- RR (Round Robin):

Este algoritmo atende ciclicamente cada fila, transferindo um pacote por vez, não utilizando pesos para tal.

- WRR (Weighted Round Robin):

Este algoritmo utiliza como parâmetro de prioridade o peso das filas. Este peso é utilizado quando ocorre congestionamento, neste mecanismo é atribuído um peso alto para o tráfego prioritário, porém, sem esquecer o tráfego de baixa prioridade. Quando há largura de banda suficiente e não há congestionamento todas as filas são atendidas da mesma forma. Este mecanismo pode ser utilizado em VoIP, de preferência com um número pequeno de filas com buffers maiores.

- GPS (Generalized Processor Sharing):

Este algorítmo utiliza pesos atribuídos a cada conexão, existe uma fila para cada fluxo.

A implementação deste método torna-se inviável pois, assume-se que a capacidade do enlace pode ser dividida infinitamente.

- CBQ (Class Based Queueing):

Os pacotes são enquadrados em diversas classes, organizando de forma a criar um esquema de prioridades entre os fluxos de saída.

- FQ (Fair Queueing):

O tráfego é ordenado em sessões e para cada uma das sessões é alocado um canal. Este algoritmo provê uma alocação mais justa entre os fluxos de dados.

- WFQ (Weighted Fair Queueing):

Este algoritmo distribui pesos aos fluxos de saída, possibilitando ponderar determinados tipos de fluxos. O algoritmo escalona o tráfego prioritário (interativo) para frente da fila e compartilha o restante da banda de forma justa entre os demais fluxos. O WFQ é dinâmico e se adapta automaticamente às mudanças das condições de tráfego.

6.3.4 Controle de Congestionamento

Este mecanismo provê a inibição dos fluxos sempre que houver congestionamento, fazendo com que os geradores de fluxo reduzam a carga sobre a rede e, conseqüentemente, o congestionamento.

Abaixo são apresentados três mecanismos para controle de congestionamento:

- RED (Random Early Detection):

Mecanismo de prevenção e inibição de congestionamento, efetua o descarte randômico quando o congestionamento é detectado.

A idéia central de funcionamento do algoritmo é, ao invés de esperar que uma fila FIFO encha para começar a descartar pacotes, e talvez descartar pacotes importantes, que se inicie o descarte sempre que a fila exceda um determinado nível. (REZENDE, 1999)

O mecanismo descarta pacotes aleatoriamente indicando para a fonte que esta deve diminuir a taxa de transmissão, porém, sempre que um determinado nível é alcançado o pacote é descartado. A probabilidade de que um pacote seja descartado é proporcional a parcela de banda alocada para aquele fluxo.

- WRED (Weighted Random Early Detection):

Este mecanismo combina as funcionalidades do RED com a classificação dos pacotes por precedência IP. O WRED descarta pacotes de forma seletiva, levando em conta as informações de prioridade do campo TOS do pacote IP, descartando inicialmente os pacotes de menor prioridade.

É utilizado geralmente em roteadores centrais de backbones (core routers).

- ECN (Explicit Congestion Notification):

Este método permite a notificação fim-a-fim de congestionamento na rede sem o descarte de pacotes. É apenas utilizado quando as duas pontas sinalizam a necessidade de sua utilização.

Quando há congestionamento um bit é setado no cabeçalho IP ao invés do pacote ser descartado, indicando desta forma o início do congestionamento. Ao receber o pacote sinalizado, um aviso é enviado à origem para que seja tomada uma atitude antes que pacotes passem a ser descartados.

6.3.5 Conformação de Tráfego

A conformação provê mecanismos para controle de tráfego utilizando filtros conhecidos como tocken bucket, limitando o tráfego de saída a uma determinada taxa.

A conformação de tráfego limita o tráfego de rajada, não prejudicando desta forma o tráfego prioritário.

Existem dois métodos utilizados para a conformação de tráfego:

- Leak Bucket (balde vazado):

Neste modelo o tráfego que chega de uma fila é depositado em um balde de capacidade B, que possui um ourifício, permitindo o tráfego fluir a uma taxa de vazamento r.

O tráfego que chega a uma taxa menor que r é diretamente encaminhado e o que chega a uma taxa maior que r irá sendo acumulado no balde.

Caso a taxa de chegada seja muito maior que r, o baldo irá enchendo até que pacotes sejam descartados.

Este modelo suaviza o tráfego de rajadas que é distribuído na rede.

- Token Bucket (balde com fichas):

Este modelo define uma taxa de transmissão variável com atraso limitado.

Consiste em um balde de capacidade B que representa a capacidade de armazenar fichas (tockens), estas fichas são repostas através de uma taxa constante de reposição R.

Quando um pacote chega, verifica-se se há ficha no balde, se existir, o pacote é marcado como *in* e uma ficha é consumida, caso contrário, é marcado como *out*.

Este método possui um parâmetro chamado TSPEC que especifica o tráfego (taxa e profundidade do balde) e outro chamado RSPEC que especifica as garantias que o tráfego necessita.

Este modelo permite à aplicação vazar rajadas para a rede até a profundidade do balde, enquanto limita a taxa média em r.

6.3.6 Policiamento de tráfego

O método Committed Access Rate (CAR) é utilizado para controle e policiamento de tráfego IP, ele gerencia a banda com limitação de taxa de acesso, controlando a taxa máxima de recepção ou transmissão dos dados.

Os pacotes são classificados através de precedência IP ou grupos de QoS e podem ser descartados ou reclassificados sempre que os limites determinados são excedidos.

O mecanismo tocken bucket também é utilizado no CAR, o tráfego é examinado, comparado com os parâmetros do tocken bucket e a partir destes uma ação é tomada em relação ao pacote. Neste método é possível limitar o tráfego por aplicação, priorizando, por exemplo, o tráfego VoIP.

6.4 Arquiteturas de QoS

6.4.1 IntServ

A qualidade de serviço nesta arquitetura é garantida através de mecanismos de reserva na rede, a aplicação reserva os recursos necessários antes de iniciar o envio dos dados.

Esta arquitetura acrescenta ao serviço de melhor esforço, categorias de serviços com diferentes graus de comprometimento de recursos (banda passante e buffer) e com diferentes níveis de QoS para fluxos de transporte distintos na rede IP. (COLCHER et al., 2005)

É preciso definir como as aplicações fazem suas solicitações e como os elementos da rede devem proceder para garantir o QoS.

Cada fluxo é identificado por IP e porta de origem e IP e porta de destino, permitindo que os recursos para fluxo de transporte sejam alocados individualmente.

As solicitações de QoS são feitas através do protocolo de sinalização RSVP, este atua sobre o tráfego de pacotes.

Os principais componentes deste modelo são:

- Controle de admissão: determina se um novo fluxo pode ser admitido sem interferir nos fluxos admitidos anteriormente;
- Escalonador de pacotes: gerencia os buffers das filas de saída dos roteadores e estações, utiliza alguma política de atendimento para tal;
- Classificador: reconhece e mapeia os pacotes dos fluxos nas diferentes categorias de serviços, notifica a função de policiamento e os coloca no buffer da fila de saída;
- Policiamento: determina se os pacotes notificados pelo classificador estão em conformidade com os parâmetros de tráfego e QoS negociados para o fluxo.

Na arquitetura IntServ três categorias de serviço são definidas pelo IETF:

- Best Effort: esta é a categoria tradicional, utiliza as rotas de menor atraso, trocando informações entre os roteadores. Os pacotes passam a ser descartados quando os buffers estão cheios, este descarte é detectado pelo TCP, reduzindo assim a taxa de transmissão. Na verdade, nesta categoria, não há QoS;
- Serviço de Carga Controlada: esta categoria de serviço aproxima-se do best effort sob condições de baixa carga. Não fornece limite máximo para o atraso de pacotes de um fluxo, porém, garante que grande parte dos pacotes tenha um atraso mínimo. Não há garantias contra perdas por descarte devido a enfileiramento de pacotes. Reserva uma parcela dos recursos disponíveis na rede aos fluxos que usam este serviço e limita o número de serviços no controle de

admissão. Os serviços compartilham entre si essa parcela de recursos da rede. Há uma alta taxa de entrega, baixíssima perda nas filas;
- Serviço Garantido: nível de comprometimento garantido de banda passante para fluxo de transporte. Impede o descarte de pacotes nesses fluxos por falta de espaço no buffer do roteador, porém, podem ocorrer perdas devido à falha na rede ou alterações de rota. Os fluxos devem estar em conformidade com os parâmetros de QoS indicados pela aplicação, durante o controle de admissão. Além disso, fornece um limite máximo para o retardo de transferência dos pacotes. Se uma aplicação indica com precisão as características de tráfego do seu fluxo, a QoS almejada por ela pode ser mantido na rede.

A solicitação destes serviços normalmente emprega procedimentos dinâmicos e estes dependem de protocolos de sinalização específicos. Através de APIs, a aplicação informa ao protocolo de sinalização a categoria de serviço desejada e a estrutura flowspec, esta descreve os parâmetros de QoS de serviços integrados (Tspec – traffic specification e Rspec – request specification).

Uma SLA IntServ define os aspectos técnicos que caracterizam um serviço, como nível de garantia desejado, a descrição do fluxo e os parâmetros de QoS.

Nesta arquitetura há pouca escalabilidade, para cada sessão RSVP conhecida pelo roteador, este tem que manter informações de estado de reserva sobre ela, estas são atualizadas periodicamente, tornando difícil a gerência de todas as reservas.

6.4.2 DiffServ

A qualidade de serviço nesta arquitetura é garantida através de mecanismos de priorização de pacotes na rede.

Esta arquitetura não utiliza nenhum mecanismo de reserva de recursos, os pacotes são classificados, marcados e processados de acordo com seu rótulo (DSCP).

A arquitetura DiffServ não padroniza serviços, apenas especifica comportamentos de encaminhamento, chamados Per Hop Behaviors (PHB), eles descrevem o comportamento de cada classe em cada roteador. São definidas poucas classes de serviços, classes essas definidas em função da QoS especificada para cada fluxo, reduzindo o nível de processamento necessário nos roteadores. (COLCHER et al., 2005)

Na arquitetura DiffServ duas categorias de serviço são definidas pelo IETF:

- Expedited Forwarding (EF): esta classe provê o maior nível de QoS. A idéia é emular uma linha dedicada convencional minimizando atraso, perda e jitter para os pacotes, há garantia de banda. EF utiliza mecanismos de traffic shaping, buferização e priorização de filas;
- Assured Forwarding (AF): esta classe emula um comportamento semelhante a uma classe com pouca carga mesmo durante a ocorrência de congestionamento. Há garantia de banda, porém, não há garantia de atraso ou jitter. Pode ocorrer

perda de pacotes. Esta categoria define quatro classes de prioridade de tráfego (ouro, prata, bronze e best effort), cada classe possui três níveis de precedência de descarte. AF utiliza mecanismos de traffic shaping e o algoritmo RED.

Esta arquitetura especifica comportamentos de encaminhamento, ela não padroniza serviços e desta forma, também não os limita.

Uma SLA DiffServ define características como forma de tarifação, penalidades em caso de interrupção e o SLS (Service Level Specification), que especifica a parte técnica.

Um SLS define:

- Disponibilidade do serviço;
- Mecanismos de autenticação e criptografia;
- Restrições de rotas;
- Monitoração e auditoria de QoS;
- TCS (Traffic Conditioning Specification):
  - Caracterização do tráfego;
  - Ações de policiamento;
  - Parâmetros de QoS;
  - Escopo do serviço.

Uma vantagem desta arquitetura é que a classificação dos pacotes é realizada nos limites da nuvem DiffServ, possibilitando aos demais roteadores operarem normalmente, sem a preocupação das complexidades de contabilização dos pagamentos e imposição dos acordos realizados.

7 ASTERISK

Desenvolvido inicialmente pela Digium, o Asterisk é um software de PBX-IP completo, possuindo todas as características de uma central telefônica de grande porte. Permite a adição de vários componentes de telefonia, tanto hardware e software, possibilitando ao usuário modelar seu PBX da forma que preferir. (SPENCER et al., 2003)

A seguir, são descritas as características mais importantes do Asterisk e feitas também algumas comparações com outro software.

7.1 PBX-IP

Um PBX-IP baseia-se num sistema de comunicação de voz sobre IP e funciona com um software específico capaz de gerenciar toda a comunicação de voz, substituindo dessa forma um sistema de telefonia tradicional.

Um PBX-IP oferece uma série de vantagens em relação a uma central convencional:

- Mobilidade: o ramal pode estar disponível em qualquer lugar;
- Flexibilidade: o ramal pode ser conectado em qualquer ponto de rede desde que haja acesso à Internet;
- Escalabilidade: o número de ramais pode ser expandido sem a necessidade de hardware adicional;
- Redução de custos com ligações;
- Integração com centrais convencionais.

A seguir é feita uma comparação entre uma central telefônica convencional e um PBX-IP:

Tabela 7.1: Comparação entre PBX Convencional e PBX-IP

	PBX Convencional	PBX-IP
Tipo	Comutação de circuito	Comutação de pacotes
Arquitetura	Centralizada	Distribuída
Instalação Elétrica	Cada ponto (telefone) necessita de um par de fios	Cada ponto (telefone) necessita estar ligado a Internet – TCP/IP
Capacidade	Depende do hardware	Depende da velocidade do link

Escalabilidade	Complexo (depende do equipamento)	Simples
Convergência	Voz e dados são duas redes	Tudo via TCP/IP
Flexibilidade	Pouca, adicionar ou mover ramais requer mudança física	Grande, um ramal funciona em qualquer ponto de rede e via Internet
Limitação (aplicação)	Limitado aos recursos tradicionais de voz	Aplicações baseadas em software
Novas aplicações	Necessita de interfaces ou placas adicionais	Fácil expansão, baseado em software e link
Redundância	Não existe, necessário outro PBX	Backup de software ou reinstalação
Configuração	Complicada	Simples
Interligação	Não suporta interligação com outro PBX	Interligação simples via Internet
Integração com PCs	Pequena ou inexistente	Ligados via rede ou Internet

Fonte: Interlize

7.2 Funcionalidades

O Asterisk é licenciado através de uma licença do tipo GPL – Gnu Public License e roda sobre Linux e outras plataformas Unix, possuindo as seguintes funcionalidades:

- Gateway VoIP;
- Gateway de mídia: entre a rede IP e a RTPC, traduz protocolos de sinalização e CODECs;
- Private Branch eXchange (PBX): efetua controle de encaminhamento de chamadas intra e inter-terminais;
- Servidor URA: toca mensagens pré-programadas;
- Softswitch: computadores que comutam circuitos de hardware na forma de interfaces padrões de telefonia;
- Discador automático;
- Correio de voz: semelhante a uma secretária eletrônica ou caixa de mensagem do celular;
- Sistema de mensagens unificadas: todas as mensagens de um mesmo usuário são direcionadas para um mesmo local, como uma caixa de mensagens;
- Distribuidor automático de chamadas e fila de atendimento;
- Registro detalhado de chamadas: para integração com sistemas de tarifação;
- Servidor de música em espera: para clientes esperando na fila, com suporte a streaming de media, bem como música em formato MP3;
- Servidor de conferência.

7.3 Arquitetura

O Asterisk possui uma arquitetura simples, conectando tecnologias de telefonia no nível mais baixo até softwares de telefonia no nível mais alto, criando um ambiente consistente para construir um ambiente misto de telefonia. (SPENCER et al., 2003)

Os componentes básicos da arquitetura do Asterisk são:

- Canais: São equivalentes à linha telefônica do sistema comutado na forma de um circuito digital de voz. Um canal pode ser uma conexão a um telefone analógico tradicional, ou a uma linha telefônica PSTN, ou uma chamada lógica, como uma chamada via Internet. Não há distinção se é um telefone ou uma linha telefônica, tudo é visto como CANAL. Cada chamada é originada ou recebida em um canal distinto;
- CODECS: São responsáveis pela conversão da voz analógica para sinal digital e seu transporte pela rede. Permite a execução de várias chamadas telefônicas em uma mesma rede, a quantidade de chamadas depende do CODEC implementado. O Asterisk possui também tradutores de CODECs, o que permite que canais que utilizem diferentes CODECs, com diferentes taxas de compressão de dados possam se comunicar. (SPENCER et al., 2003)
  O capítulo 4 trata especificamente sobre este assunto;
- Protocolos: São responsáveis pela sinalização das chamadas, estabelecendo sessões entre os terminais e também pelo transporte, efetuando entrega fim-a-fim de dados em tempo real, o capítulo 3 trata sobre protocolos de sinalização e transporte;
- Aplicações: São as funcionalidades encontradas no Asterisk, como servidor URA, correio de voz e conferências, descritas na seção 7.2.

A figura a seguir mostra a arquitetura básica do Asterisk:

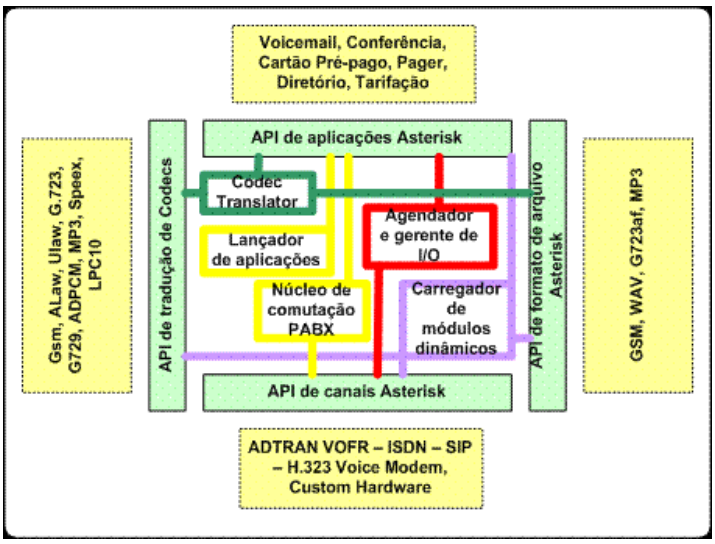

Figura 7.1: Arquitetura do Asterisk (Gonçalves, 2007)

7.4 Componentes do Asterisk

Os componentes do Asterisk podem ser divididos em interfaces de hardware e software, abaixo estão descritas ambas interfaces.

7.4.1 Interfaces de Hardware

Para a conexão física com o Asterisk podemos utilizar várias interfaces, entre elas podemos citar:

- Interfaces analógicas (linha de telefone e telefone analógico);
- Circuitos digitais (linhas T1 e E1);
- Protocolos VoIP (SIP, H.323, MGCP, etc).

Abaixo um exemplo de como o Asterisk pode ser implementado, utilizando as interfaces de hardware descritas acima:

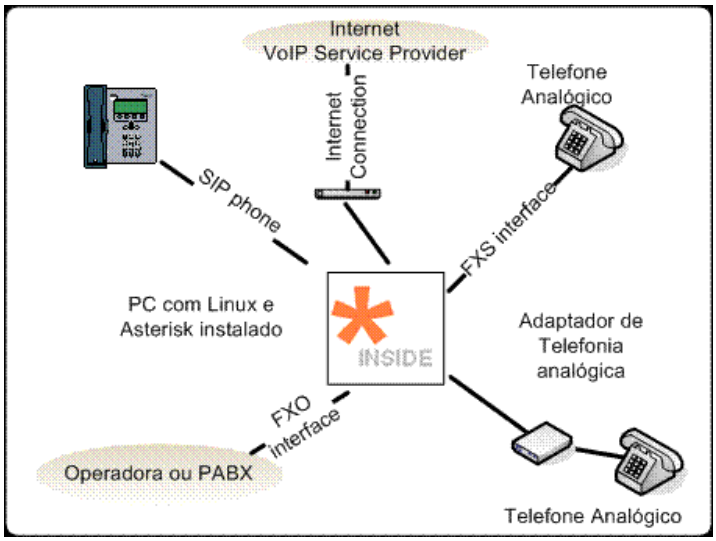

Figura 7.2: Interfaces do Asterisk (Gonçalves, 2007)

O Asterisk pode ser conectado utilizando softphones sem a necessidade de uma interface de hardware adicional, através de telefones IP, ou, simplesmente roteando as chamadas pela Internet para um provedor de serviços de telefonia.

A forma mais simples de criar um PBX é utilizando placas FXO e FXS. As placas FXO permitem a conexão a uma linha de telefone analógico e não geram tom de discagem, apenas aceitam. Já as placas FXS permitem a conexão a um telefone analógico, fornecem o tom de discagem e também sinalizam quando uma ligação é recebida.

Embora a porta FXO não gere tom de discagem, ambas as interfaces fornecem comunicação bidirecional.

Um dos cenários mais comuns para aplicações VoIP é o exposto na figura apresentada a seguir, onde procura-se aproveitar a estrutura já existente, habilitando uma central antiga para chamadas VoIP.

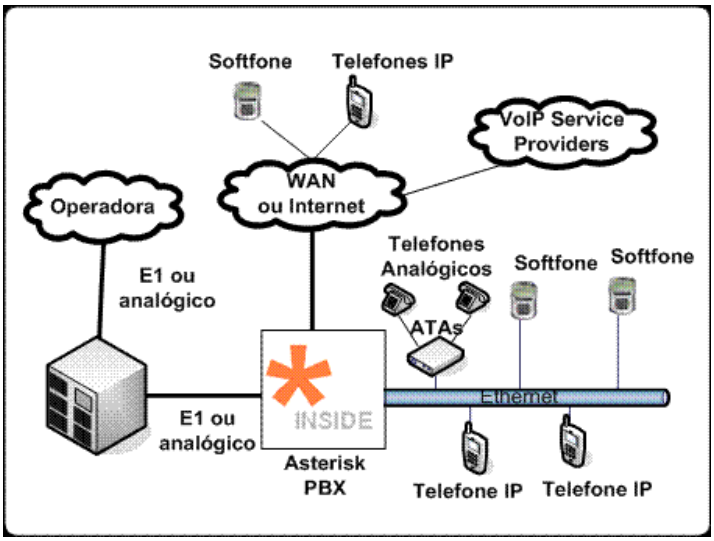

Figura 7.3: Integração com PBX existente (Gonçalves, 2007)

É preciso verificar as necessidades de integração com outras centrais e o número de canais que serão utilizados para especificar o hardware que será utilizado.

O Asterisk faz o processamento dos canais de voz, utilizando de forma intensiva o processador e não requer muito espaço em disco, aproximadamente 100 Mb.

Caso apenas VoIP seja utilizado, nenhum hardware adicional se faz necessário.

7.4.2 Interfaces de Software

As diversas tecnologias e interfaces suportadas pelo Asterisk são divididas em três grupos. (SPENCER et al., 2003)

As seguintes interfaces de software podem ser adicionadas ao Asterisk:

- Interface Pseudo TDM Zaptel: Permite a integração com o sistema digital e analógico e possui suporte à Pseudo-TDM switching, permitindo a realização de vídeo conferência. O pseudo-tdm simula o processamento TDM feito em hardware, o suporte a TDM é adicionado ao Asterisk, deixando o processamento de vídeo conferência e outras aplicações para o software;
- Interface não Zaptel: Também permite a integração com o sistema digital e analógico, porém, não permite a realização de vídeo conferência;
- Protocolos de pacotes de voz: São os protocolos padrões para comunicação VoIP e não necessitam de hardware adicional.

7.5 Asterisk X OpenSER

A seguir, será feita uma comparação entre o Asterisk e o OpenSER, SIP Proxy licenciado pela licença GNU como software livre.

Um SIP Proxy efetua requisições para agentes que não podem fazê-las diretamente, efetuando a comunicação com outro servidor SIP e retendo informações que podem ser usadas posteriormente, como informações de faturamento.

O OpenSER não é exatamente um concorrente do Asterisk, ele pode ser utilizado como um provedor VoIP, como solução para travessia de NAT e também para balanceamento de carga.

A travessia de NAT é mais fácil no Open SER, a mídia pode ser enviada diretamente do cliente ao provedor, a não ser que NAT não simétrico esteja sendo utilizado.

Enquanto que a arquitetura do Asterisk é um B2BUA, back to back user agent, o Open SER, sendo apenas um SIP Proxy, possui uma arquitetura mais leve, apresentando um melhor desempenho na implementação, considerando vazão ou número de canais atendidos. (GONÇALVES, 2008)

Em compensação, a arquitetura do Asterisk, embora mais pesada, gerencia a mídia e possui diversos recursos não encontrados num SIP Proxy, como por exemplo, tradução de CODECs e URA. (GONÇALVES, 2008)

Enquanto que o Asterisk possui uma série de funcionalidades listadas anteriormente, o OpenSER não é capaz de efetuar nenhum serviço relacionado à mídia, é necessário integrar a ele um servidor de mídia.

O OpenSER necessita de um gateway para se comunicar com a rede pública, enquanto que o Asterisk pode ser utilizado como gateway, efetuando ele próprio a comunicação com a rede pública. (GONÇALVES, 2008)

Considerando os aspectos citados acima, podemos concluir que os dois softwares podem ser utilizados em conjunto, o OpenSER atuando como SIP Proxy, mais robusto, e o Asterisk efetuando uma série de outras funcionalidades necessárias a um PBX-IP, aproveitando, desta forma, o que cada um tem de melhor.

É importante salientar, porém, que o Asterisk é mais simples de configurar e gerencia volumes pequenos a moderados, enquanto que o OpenSER é mais robusto, capaz de gerenciar um grande volume de chamadas.

Portanto, cabe ao gerente de TI analisar suas necessidades e os aspectos citados acima para determinar a necessidade ou não de recursos adicionais.

8 PROPOSTA DE IMPLEMENTAÇÃO

Baseado na estrutura de rede existente numa empresa e todas as conexões com suas filiais, este capítulo tem por finalidade elaborar uma proposta de implementação VoIP considerando todos os aspectos estudados nos capítulos anteriores.

8.1 Escopo

Permitir a comunicação telefônica utilizando a rede de dados, atingindo os seguintes objetivos:

- Comunicação VoIP entre a matriz e as filiais;
- Interligação da central telefônica tradicional existente com o sistema VoIP;
- Aumento do número de ramais existentes na matriz;
- Qualidade e confiabilidade semelhantes à telefonia convencional;
- Privacidade dos dados;
- Implementação dos seguintes serviços: servidor URA, correio de voz, registro e transferência de chamadas e vídeo conferência.

8.2 Estrutura da Rede

A rede atual da matriz possui as seguintes características que devem ser consideradas:

- Existem duas formas de acesso à rede interna, pela Internet ou através de uma rede MPLS (voz e dados), esta conecta todas as filiais e utiliza H.323 para garantir a interoperabilidade com a central telefônica;
- O firewall e NAT estão configurados no roteador que dá acesso à Internet;
- A estrutura possui uma DMZ, os equipamentos da DMZ estão separados da rede interna por um switch nível 3;
- A estrutura possui também uma central telefônica, conectada através de um canal E1 ao roteador que dá acesso à rede MPLS.

A figura a seguir representa a estrutura atual da rede:

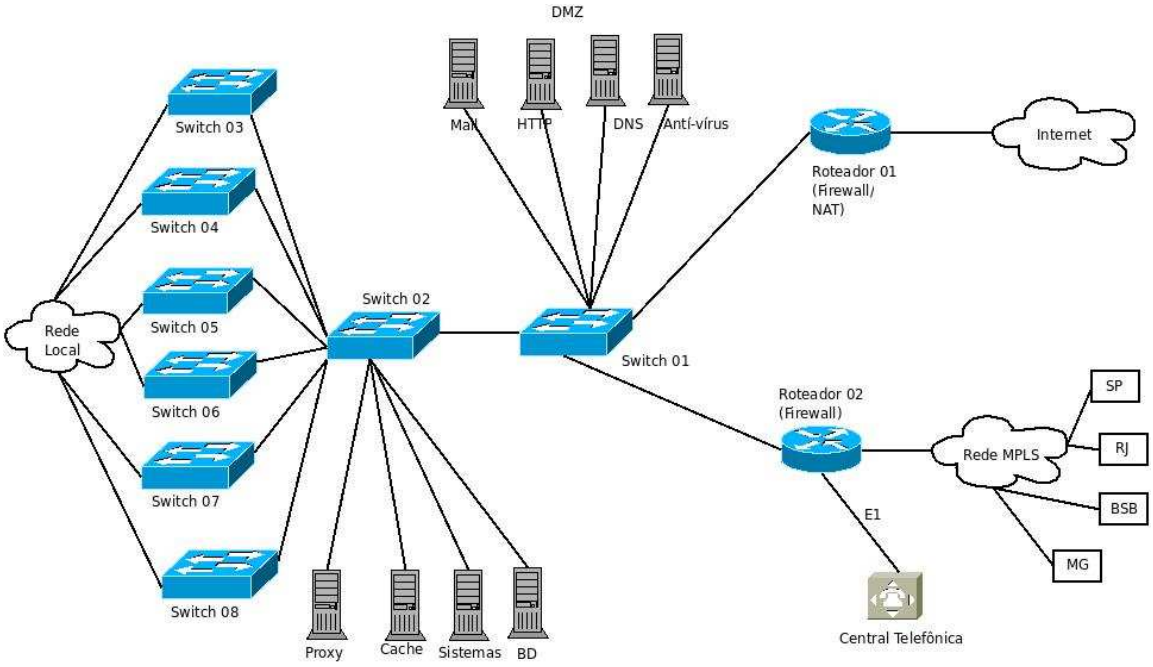

Figura 8.1: Estrutura atual da rede (o Autor)

Baseado na estrutura existente e no que se deseja implementar, as seguintes modificações devem ser efetuadas:

- Configuração do NAT e firewall no switch 01, possibilitando a colocação de um servidor para ultrapassar o NAT na DMZ e aumentando a segurança, atualmente não existe um firewall isolando a rede local da DMZ, tornando-a vulnerável;
- Inclusão de um servidor Asterisk na DMZ, com um canal E1 fazendo a ligação entre ele e a central telefônica existente, possibilitando a ligação de ramais do Asterisk (SIP) para a central telefônica (H.323) e vice-versa. As funções de gateway de mídia, gerência e proxy serão executadas pelo Asterisk. Não há a necessidade de nenhuma configuração especial para a rede MPLS, sendo a mesma tranparente para este tipo de aplicação;
- Inclusão de um segundo servidor na DMZ, utilizando Transversal Using Relay NAT (TURN) para ultrapassar o NAT, existe também a possibilidades da utilização de tunelamento, mas isto acarretaria na inclusão de mais um servidor;
- Utilização do roteador 01 como um segundo firewall, protegendo a DMZ;
- Inclusão de adaptadores ATA, telefones IP e softphones na rede local de acordo com a necessidade.

A figura a seguir representa a estrutura da rede com as modificações propostas anteriormente:

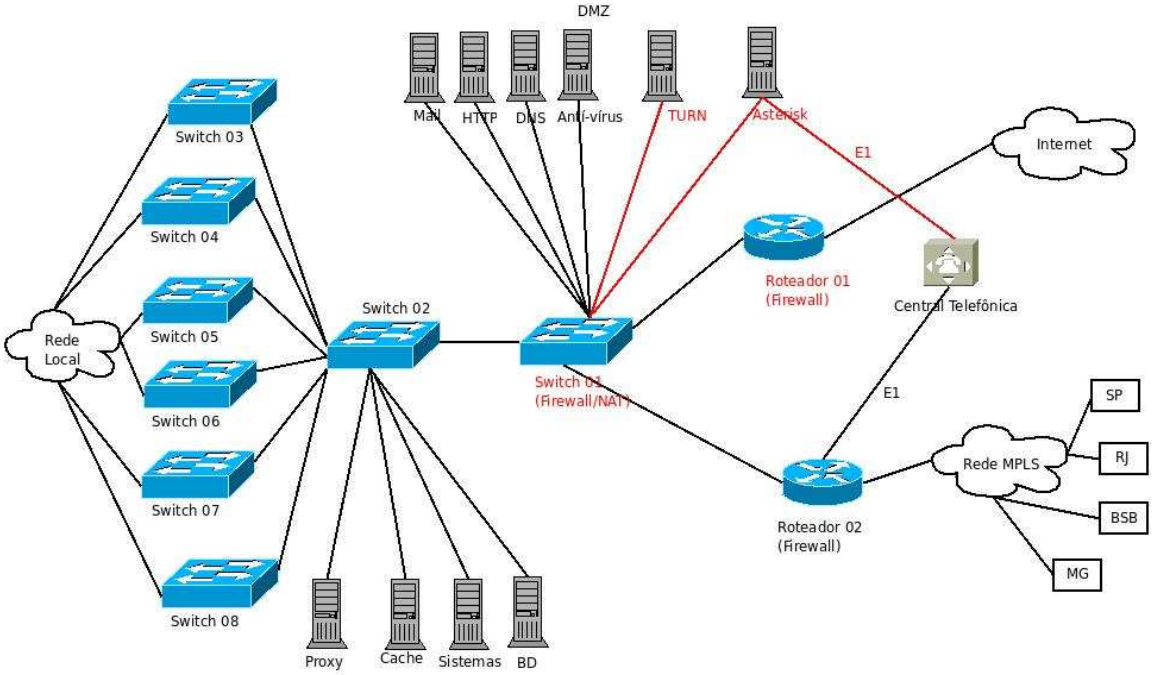

Figura 8.2: Estrutura Proposta (o Autor)

8.3 Implementação

Baseado na nova estrutura proposta e no escopo que se pretende atingir, será necessária a implementação do que segue.

8.3.1 Protocolos de Sinalização e Transporte

Para estabelecimento das sessões entre os terminais deverá ser utilizado o protocolo de sinalização SIP, em virtude de que ele foi desenvolvido especificamente para a Internet, possuindo grande escalabilidade e flexibilidade. O protocolo possui suporte a novos CODECs o que facilita alterações futura caso um CODEC mais apropriado seja desenvolvido.

Embora a central telefônica opere com o protocolo de sinalização H.323, não exiete problema na utilização dos dois protocolos simultaneamente, cabendo ao gateway de sinalização a conversão de um para outro quando necessário.

O modo de operação a ser utilizado deverá ser o modo indireto, obrigando o agente ao envio de mensagens de sinalização através do proxy e possibilitando a manutenção destas informações, o tipo de encaminhamento deverá ser statefull, facilitando desta forma o envio de outras mensagens da mesma sessão.

Os protocolos RTP e RTCP deverão ser utilizados em conjunto, permitindo o serviço de entrega fim-a-fim e monitoramento das conexões, efetuando a sincronização das amostras que trafegam na rede.

Embora o RTP não implemente QoS, ele permite que métodos como IntServ e DiffServ sejam aplicados, o que será tratado mais adiante.

8.3.2 CODECs

Para a conversão de sinais analógicos para digitais, considerando os modelos MOS e modelo E e também as características de cada CODEC, deverá ser utilizado o CODEC G.711 ou, como segunda opção o CODEC G.726.

Segundo o modelo E, a satisfação obtida pelo G.726 se enquadraria como ótima, enquanto que o G.711 se enquadra como boa.

Apesar do G.711 possuir um MOS estimado de 4,2, abaixo do valor estimado para o G.726 que é de 4,3, ele é considerado a opção natural para redes locais, possui excelente qualidade de voz, não necessita recursos de processamento e também não adiciona nenhum atraso na compressão de voz.

Já o G.726 possui uma qualidade de voz que varia entre moderada a boa, necessita poucos recursos de processamento e adiciona pouco atraso na compressão de voz.

8.3.3 NAT/ Firewall

Considerando os aspectos abordados no capítulo 5, dois mecanismos seriam indicados para ultrapassar NAT/firewall, Traversal Using Relay NAT (TURN) ou Tunelamento.

Em virtude do método de tunelamento necessitar um servidor adicional, o que aumentaria os custos de implantação, deverá ser utilizado o método TURN para resolver os problemas de NAT e firewall.

Para que este método possa ser implementado, será incluído um servidor na DMZ para execução desta tarefa e as funções de NAT e firewall passarão a ser implementadas no switch 01.

A utilização do método TURN se justifica por este tratar NAT simétrico, ele provê um endereço externo que atuará como relay e servirá como um intermediário entre origem e destino.

Um inconveniente deste método é que ele aumenta o consumo de banda, pois os dados são transmitidos da origem ao servidor e do servidor ao destino.

É preciso utilizar softphones com suporte a TURN, caso contrário há a necessidade de um proxy.

A figura abaixo demonstra os fluxos de dados de um cliente da rede local, ultrapassando o NAT com a utilização do TURN, atingindo um cliente externo:

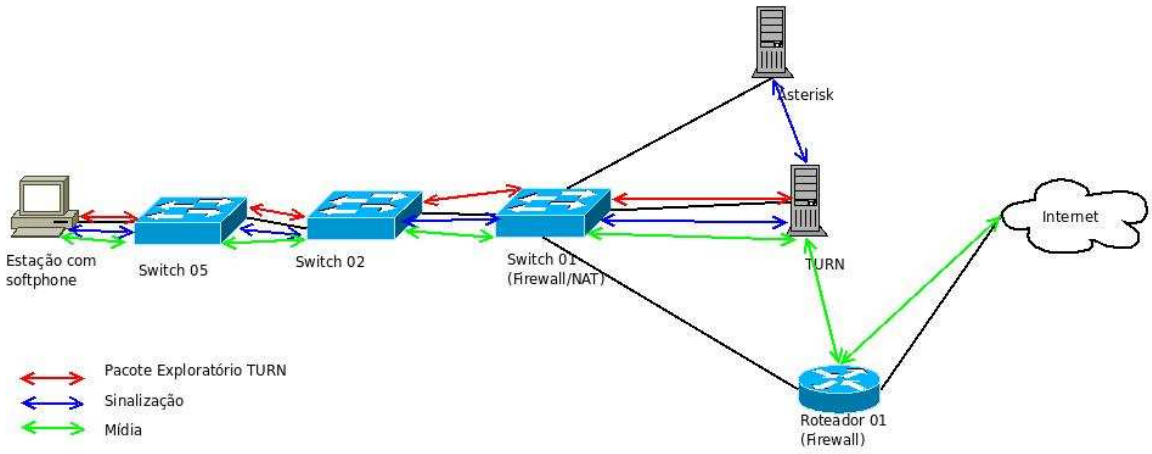

Figura 8.3: Fluxo de dados utilizando TURN (o Autor)

8.3.4 Privacidade e Autenticidade

Considerando que o escopo especificado anteriormente exige que haja privacidade dos dados que trafegam pela rede, faz se necessário que os protocolos RTP e RTCP sejam substituídos pelos protocolos SRTP e SRTCP.

Os protocolos SRTP/SRTCP oferecem confidencialidade, autenticidade e proteção contra replay.

Como descrito no capítulo 5, o SRTP utiliza criptografia, garantindo que mesmo que os dados sejam capturados, não será possível decifrá-los. A RFC 3711, que define o protocolo, define também que seja utilizado o algoritmo AES, de 128 bits, proporcionando desta forma um nível de segurança elevado para o tráfego de áudio e também a utilização de HMAC-SHA1 para autenticação e integridade.

Desta forma, embora não definido no escopo, pode-se garantir, além da privacidade, também a autenticidade dos dados.

8.3.5 QoS

A qualidade de serviço em redes IP é um aspecto fundamental para o desempenho fim-a-fim das aplicações VoIP, considerando os aspectos abordados no capítulo 6, será definido o que segue para obtenção de QoS.

A proposta consiste na utilização do modelo de rede DiffServ, garantindo a priorização de determinados pacotes na rede, sem no entanto utilizar mecanismos de reserva de recursos.

Nesta arquitetura, os pacotes serão marcados, campo DSCP, criando classes de pacotes que em conjunto com uma estratégia de encaminhamento, chamada PHB, cria classes de serviços com tratamento diferenciado. Devem ser definidas poucas classes de serviços na estrutura da rede reduzindo o nível de processamento nos roteadores.

Uma vez classificado o pacote, o tráfego deverá ser encaminhado utilizando a categoria de serviço AF, Assured Forwarding. Esta categoria provê banda, mas não garante atraso ou jitter, porém, oferece uma melhor utilização da mesma.

Como esta arquitetura baseia-se na priorização de pacotes, deverá ser utilizado o algoritmo Priority Queueing, priorizando de forma rígida o tráfego de voz em relação aos demais tráfegos, diminuindo atraso e perda de pacotes.

Em virtude da utilização desta arquitetura, também deverá ser utilizado o mecanismo de conformação de tráfego tocken bucket, especificando as garantias que o tráfego VoIP necessita, diminuindo a probabilidade de descarte, maior liberação de banda e menor tempo na fila.

O algoritmo RED deverá ser utilizado para controle de congestionamento, inibindo o fluxo de pacotes na origem quando necessário, evitando o descarte de pacotes de alta prioridade.

Para o escalonamento das filas nas interfaces de saída deverá ser utilizado o algoritmo WRR, atribuindo-se um peso alto para o tráfego VoIP. É recomendada a utilização de um número pequeno de filas com buffers maiores, conforme descrito na seção 6.3.3.

Conforme a recomendação G.114 do ITU-T, o atraso máximo não deve ser maior que 400 ms, sendo que entre 150 e 400 ms pode ocorrer impacto em algumas aplicações e até 150 ms é o atraso considerado ideal. Além disso, a taxa de perda não deve ser superior a 10% e recomenda-se uma técnica de buffering para que o jitter seja evitado.

A figura a seguir demonstra onde serão implementados os mecanismos de QoS:

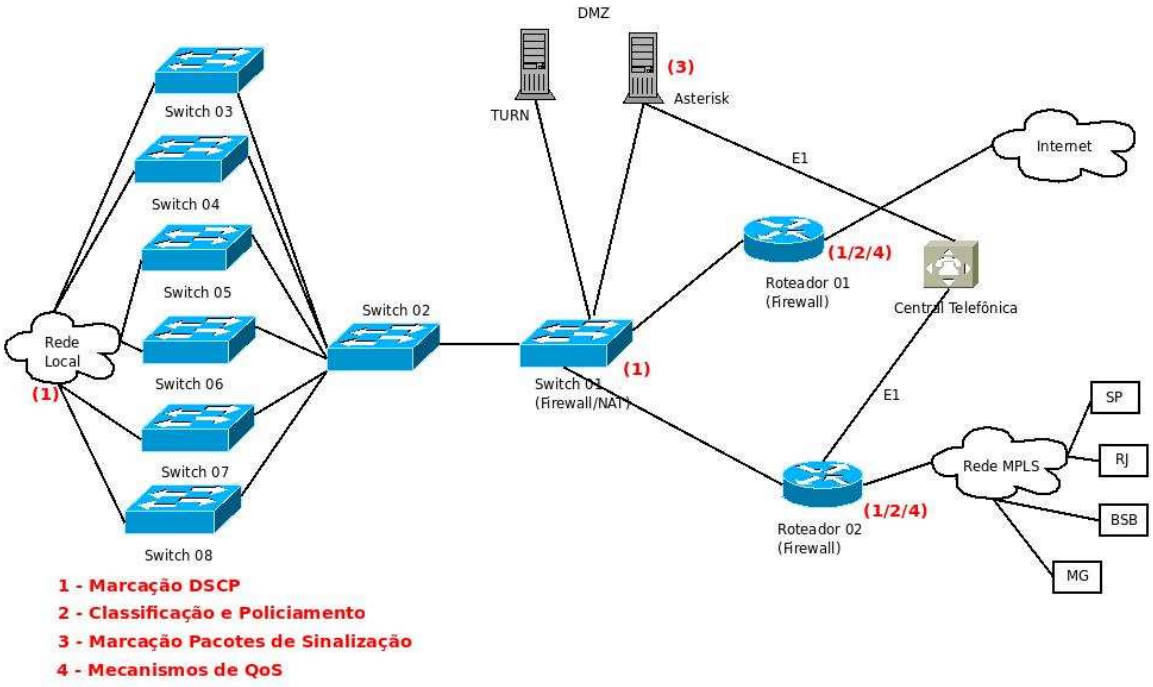

Figura 8.4: QoS na Estrutura da Rede (o Autor)

8.3.6 Asterisk

Para que se atinja os objetivos formulados no escopo, deverá ser instalado um servidor Asterisk na DMZ.

O servidor Asterisk utiliza a tecnologia VoIP com diversos protocolos, possibilita a integração com vários equipamentos de telefonia e a conexão com a rede pública, bem como a interligação entre a matriz e as filiais através da Internet, permitindo a comunicação direta a custo zero.

Este servidor será conectado ao switch 01 e terá também um canal E1 efetuando a ligação entre o mesmo e a central telefônica.

O Asterisk efetuará as seguintes funções:

- Gateway de gerência: efetuando a comunicação entre terminais IP, controlando o estabelecimento de novas chamadas, roteamento das mesmas e banda passante;
- Gateway de mídia: transmitindo fluxos de áudio entre a rede IP e a central telefônica, efetuando codificação e decodificação da voz e transcodificação entre formatos digitais diferentes;
- Gateway de sinalização: controlando os pedidos de chamada entre a rede IP e a central telefônica e efetuando a conversão de mensagens ou tons entre e rede IP e a central telefônica;
- Servidor URA: servidor de mensagens pré-programadas;

- Correio de voz;
- Plano de numeração de chamadas;
- Registro de chamadas;
- Vídeo conferência: é necessário que a interface Pseudo TDM Zaptel seja instalada para dar suporte à realização de vídeo conferência.

Com a definição dos serviços a serem executados pelo Asterisk, as modificações propostas na estrutura física e as implementações propostas acima, torna-se viável a utilização de VoIP para a comunicação entre matriz e filiais e interligação com a central telefônica existente, objetivo principal deste projeto.

8.3.7 Guia de Implementação

A tabela a seguir descreve, de forma sucinta, o que e como deverá ser implementado a proposta definida anteriormente, esta implementação está prevista para uma segunda etapa, posterior a este trabalho.

Tabela 8.1: Etapas para Implantação do Servidor VoIP

Etapas	Implementação	Descrição
Aquisições	Servidor Asterisk	Servidor com capacidade para rodar o Asterisk e ligação com a central telefônica utilizando um canal E1.
	Servidor TURN	Servidor com capacidade para rodar o TURN, possibilitando a travessia do NAT.
	Adaptadores ATA, telefones IP e headsets	De acordo com a necessidade, preferência para utilização de softphones com headsets.
Mudanças na Estrutura Atual	Configuração do NAT	Regras do roteador 01 implementadas no switch 01.
	Configuração do firewall	Inclusão de regras no switch 01.
Instalação Servidores	Asterisk	Execução de funções de gateway de mídia, gerência e proxy. Protocolo de sinalização: SIP Protocolo de transporte: SRTP/SRTCP CODEC: G.711 Instalação da interface Pseudo TDM Zaptel. Serviços: servidor URA, correio de voz, registro de chamadas, vídeo conferência e plano de numeração de ramais.
	TURN	Configuração do TURN fazendo ligação entre a rede interna e o Asterisk (sinalização) ou cliente (mídia).

Configuração de QoS	DiffServ	Definição de uma classe com prioridade sobre as demais. Marcação do campo DSCP dos pacotes de sinalização e transporte que provêm da Internet ou da rede MPLS, executadas nos roteadores 01 e 02 respectivamente, os roteadores devem verificar se há marcação e refazerem a mesma caso haja necessidade. Os roteadores 01 e 02 também devem efetuar a classificação e policiamento destes pacotes. Para os pacotes provenientes dos clientes da rede local a marcação deve ser efetuada pelo softphone ou, caso o software não suporte, pelo switch 01. O Asterisk deverá efetuar a marcação dos pacotes de sinalização, não necessariamente na classe de mais alta prioridade, mas numa classe que ofereça alguma garantia de vazão.
	Mecanismos	Os mecanismos de QoS deverão ser implementados nos roteadores de borda caso se necessite tratar QoS fora da rede local. Priorização de pacotes – PQ Conformação de tráfego – Tocken Bucket Controle de congestionamento – RED Escalonamento das filas – WRR

Fonte: o Autor

9 CONCLUSÃO

No decorrer deste trabalho, procurou-se levantar todos os aspectos pertinentes à implementação de um servidor VoIP. Foram apresentadas soluções para cada necessidade, protocolos de transporte, QoS, NAT entre outros, permitindo a análise e opção pela solução considerada mais viável.

Percebe-se que a implementação pode ser executada de diversas formas, utilizando um grande número de técnicas, protocolos, serviços e também diferentes combinações dos mesmos.

Com o intuito de definir uma única proposta, procurou-se indicar os protocolos, arquiteturas, técnicas e serviços que mais se adaptam à estrutura da rede existente e onde as alterações necessárias sejam viáveis, considerando aspectos técnicos e também a necessidade de aquisições.

Percebe-se ainda que a tarefa de implantação é trabalhosa, requer conhecimentos técnicos para execução e também um estudo sobre os impactos que as mudanças podem causar na estrutura da rede.

A tabela a seguir apresenta todos os passos necessário para a implantação do servidor VoIP:

Tabela 9.1: Etapas para Implantação do Servidor VoIP

Etapas	Implementação	Descrição
Aquisições	Servidor Asterisk	Servidor com capacidade para rodar o Asterisk e ligação com a central telefônica utilizando um canal E1.
	Servidor TURN	Servidor com capacidade para rodar o TURN, possibilitando a travessia do NAT.
	Adaptadores ATA, telefones IP e headsets	De acordo com a necessidade, preferência para utilização de softphones com headsets.
Mudanças na Estrutura Atual	Configuração do NAT	Regras do roteador 01 implementadas no switch 01.
	Configuração do firewall	Inclusão de regras no switch 01.

Instalação Servidores	Asterisk	Execução de funções de gateway de mídia, gerência e proxy. Protocolo de sinalização: SIP Protocolo de transporte: SRTP/SRTCP CODEC: G.711 Instalação da interface Pseudo TDM Zaptel. Serviços: servidor URA, correio de voz, registro de chamadas, vídeo conferência e plano de numeração de ramais.
	TURN	Configuração do TURN fazendo ligação entre a rede interna e o Asterisk (sinalização) ou cliente (mídia).
Configuração de QoS	DiffServ	Definição de uma classe com prioridade sobre as demais. Marcação do campo DSCP dos pacotes de sinalização e transporte que provêm da Internet ou da rede MPLS, executadas nos roteadores 01 e 02 respectivamente, os roteadores devem verificar se há marcação e refazerem a mesma caso haja necessidade. Os roteadores 01 e 02 também devem efetuar a classificação e policiamento destes pacotes. Para os pacotes provenientes dos clientes da rede local a marcação deve ser efetuada pelo softphone ou, caso o software não suporte, pelo switch 01. O Asterisk deverá efetuar a marcação dos pacotes de sinalização, não necessariamente na classe de mais alta prioridade, mas numa classe que ofereça alguma garantia de vazão.
	Mecanismos	Os mecanismos de QoS deverão ser implementados nos roteadores de borda caso se necessite tratar QoS fora da rede local. Priorização de pacotes – PQ Conformação de tráfego – Tocken Bucket Controle de congestionamento – RED Escalonamento das filas – WRR

Fonte: o Autor

Espera-se que o que foi levantado e estudado ao longo deste trabalho e com a proposta de implementação apresentada no capítulo anterior, seja possível, numa segunda etapa, implementar o servidor em sua totalidade.

REFERÊNCIAS

ARCOMANO, R. **VoIP How To.** [S. l.], 2002. Disponível em: <http://tldp.org/HOWTO/VoIP-HOWTO.html>. Acesso em: jan. 2008.

CHOWDHURY, D. D. **Projetos Avançados de Redes IP**. Rio de Janeiro: Campus, 2002. 380p.

COLCHER, S. et al. **VoIP**. Rio de Janeiro: Campus, 2005. 288p.

E-MODEL Tutorial. Disponível em: <http://itu.int/ITU-T/study/groups/com12/emodelv1/introduction.html>. Acesso em: mar. 2008.

GONÇALVES, F. **Comparing Asterisk and OpenSER.** [S. l.], 2008. Disponível em: < http://www.packtpub.com/article/comparing-asterisk-and-openser>. Acesso em: jul. 2008.

GONÇALVES, F. **Guia de Configuração para o Asterisk PBX** . Florianópolis: Título Independente, 2007. 358p.

HERSENT, O.; GUIDE, D.; PETIT, J. **Telefonia IP**. São Paulo: Prentice Hall, 2002. 451p.

IPSEC in VoIP Networks. [S.l.], 2006. Disponível em: <http://www.newport-networks.com/whitepapers/IPSec-1.html>. Acesso em: maio 2008.

IZU, A.; MAGUITA, W. **VoIP e a Revolução na Telefonia:** Segunda Parte. [S.l.], 2005. p.01-03. Disponível em: <http://conhecimento.incubadora.fapesp.br/portal/trabalhos/2005/VoIPEARevoluçaoNaTelefoniaSegundaParte/>. Acesso em: jan. 2008.

KHLIFI, H.; GRÉGOIRE, J.; PHILLIPS, J. VoIP and NAT/Firewalls: Issues, Traversal Techniques and a Real-World Solution. **IEEE Communications Magazine,** New York, v.44, p. 93-99, July 2006.

MEGGELEN, J. SMITH, J.;MADSEN, L. **Asterisk:** O Futuro da Telefonia. Rio de janeiro: Alta Books, 2005. 332p.

NAT Traversal for Multimidia Over IP. [S.l.], 2006. Disponível em: <http://www.newport-networks.com/whitepapers/nat-traversal.html>. Acesso em: maio 2008.

OpenSER - The Open Source SIP Server. [S.l.], 2005. Disponível em: < http://www.openser.org>. Acesso em: jul. 2008.

PABX Virtual. Rio de Janeiro, 2008. Disponível em: < http://www.interlize.com.br/?id_menu=19>. Acesso em: jul.2008.

PASSITO, A.et al. Análise de Desempenho de Tráfego VoIP Utilizando o Protocolo IP Security. In: BARBIERI, R. **Voice over IPsec:** Analysis and Solutions. Milano: Dipartimento di Scienze dell'Informazione: Università degli Studi di Milano, 2002.

PINHEIRO, C. E**specificação ITU H.323:** Tutorial**.** Porto Alegre, 2000. Disponível em: <http://penta2.ufrgs.br/h323/indice.htm>. Acesso em: fev. 2008.

REZENDE, J. F.; ZIVIANI A. **Tráfego de Voz em um ambiente de diferenciação de serviços na Internet**. Rio de Janeiro, 1999. Disponível em: <http://www.gta.ufrj.br>. Acesso em: jun. 2008.

SAADE, D. **Fundamentos de Sistemas Multimídia.** Disponível em: <http://www.midiacom.uff.br/~debora/fsmm/pdf/parte5.pdf>. Acesso em: mar. 2008.

SECURITY in VoIP Environments. [S.l.], 2006. Disponível em: < http://wiki.snom.com/Security_in_VoIP_environments#Media_Encryption_.28SRTP.29>. Acesso em: jun. 2008.

SILVA, A. **Qualidade de Serviço VoIP:** Parte I. 2000. Disponível em: <http://www.rnp.br/newsgen/0005/qos-voip1.html>. Acesso em: mar. 2008.

SPENCER, M.; ALLISON, M.; RHODES, C. **The Asterisk Handbook.** 2003. Disponível em: <http://www.digium.com/handbook-draft.pdf>. Acesso em: jul. 2008.

STALLINGS, W. **Cryptography and Network Security:** Principles and Practice. 3rd ed. [S.l.]: Prentice-Hall, 2003.

TANENBAUM, A. **Redes de Computadores**. Rio de Janeiro: Elsevier, 2003. 945p.

ZRTP: Media Path Key Agreement for Secure RTP. [S.l.], 2008. Disponível em: <http://zfoneproject.com/docs/ietf/draft-zimmermann-avt-zrtp-07.html>. Acesso em: jun. 2008.