VOIP: Um Estudo de Caso Utilizando o Servidor Stun

Fabrício José Rodrigues Costa[1], Luis Augusto Mattos Mendes[1]

[1]Departamento de Ciência da Computação – Universidade Presidente Antônio Carlos (UNIPAC)
Campus Magnus – Barbacena – MG – Brasil

fabjcosta@uol.com.br, luisaugustomendes@yahoo.com.br

Resumo. *A tecnologia VoIP, devido a sua crescente demanda no mercado, têm oferecido inúmeros benefícios a seus usuários em relação ao tradicional sistema de telefonia. Sendo assim, o presente artigo pretende mostrar algumas das vantagens deste recurso juntamente com uma ferramenta que auxiliará a interconectar redes distintas para utilizar um provedor VoIP, o servidor STUN.*

Palavras Chave: Rede, *Firewall*, *Stun*, SIP

1. Introdução

O constante avanço tecnológico, impulsionado pela ascensão da Internet e seus serviços agregados, tem feito com que cientistas não parem de pensar em novas tecnologias e melhorias para o mercado. Um desses, é o VoIP *(Voice over Internet Protocol)*, que mesmo estando a pouco tempo em pleno funcionamento, tem garantido novos benefícios à sociedade.

VoIP é uma tecnologia que utiliza redes IP para transmitir voz. O processo se dá por meio da conversão das amostras de voz em uma série de pacotes, gerenciáveis pela rede IP. [1]

As razões que motivam esforços para a integração de rede de dados e voz são várias. Entre essas, a necessidade de redução de custos em telecomunicações, o avanço da tecnologia digital e o desenvolvimento de protocolos que oferecem a qualidade de serviço, explicam tal motivação.

Apesar do serviço proporcionar grandes benefícios e ser eficiente, em certas redes pode apresentar problemas em seu funcionamento, tais como a dificuldade para ouvir, falar ou em ter um serviço de qualidade.

Atento a essas preocupações, este trabalho foi desenvolvido tendo como objetivo estudar a tecnologia VoIP, analisar seus problemas durante a comunicação e configurar a ferramenta STUN *(Simple Traversal of UDP[1] through NATs[2])* a fim de sanar alguns desses.

Dentro dessa configuração, alguns tópicos serão fundamentais para o perfeito entendimento, como: definição de comutação, os componentes básicos da comunicação de voz sobre IP, os possíveis problemas desse estudo e descrever minuciosamente o funcionamento do servidor STUN dentro de uma rede local; além de relatar sua contribuição para o meio acadêmico-científico.

[1] UDP – User Datagram Protocol
[2] NAT – Network Address Translation

2. Comutações

Comutação é o conjunto de operações para interligar circuitos que permitem a conexão entre dois ou mais assinantes. [2]

Dentro do atual sistema telefônico, existem dois tipos de comutação: comutação de circuitos e comutação de pacotes.

No sistema telefônico convencional, quando as chamadas são realizadas, um trajeto de fios de cobre é percorrido, do emissor ao receptor. Esse trajeto é desenvolvido pelo equipamento de comutação do sistema telefônico. Tal processo é denominado comutação de circuitos. [2]

Comutação de circuitos pelo fato de que dados só poderão ser enviados após estabelecido um caminho de um nó até o outro da rede. Essa é uma das vantagens dessa técnica, pois ao estabelecer a conexão por meio do caminho de cobre, o atraso estimado para a entrega dos dados é apenas o tempo de propagação de um sinal eletromagnético, cerca de 5 ms por 1000km. Uma outra vantagem está na questão de não haver congestionamentos na comunicação após esta estabelecida. O risco que se corre é congestionamento antes de estabelecer a conexão (sinal de ocupado) devido à capacidade do tronco. [2]

Já em outra extremidade do assunto, existe a comutação de pacotes. Técnica esta que impõem um limite máximo para o tamanho do pacote.

A comutação de pacotes não permite que usuários ocupem toda a rede para a transmissão de seus dados. Essas redes operam bem com a manipulação de tráfego interativo. Na maioria dos casos, as redes de computadores utilizam a comutação de pacotes. [2]

Uma das principais particularidades da comutação de circuitos em relação à de pacotes, é que ela consome totalmente a largura da banda antes de estabelecer a conexão. A comutação de pacotes permite que pacotes distintos sejam transmitidos, sem que parte da banda seja desperdiçada.

E uma última diferença muito significativa para desenvolvermos parte desse trabalho é entender como tais técnicas de comutações são tarifadas.

A comutação de circuitos baseia suas tarifas na distância e no tempo, e é indiferente quanto ao tráfego. Ao contrário, a comutação de pacotes está ligada ao número de bytes transmitidos e no tempo de conexão.

Abaixo, o Quadro 1 apresenta o comparativo dos dois tipos de comutação:

	Comutação de Circuitos	Comutação de Pacotes
Caminho de “cobre” dedicado	SIM	NÃO
Largura de Banda Disponível	FIXA	DINÂMICA
Largura de Banda potencialmente desperdiçada.	SIM	SIM
Transmissão store-and-forward	NÃO	SIM
Cada pacote segue a mesma rota	SIM	NÃO

Configuração de chamada	Necessária	Desnecessária
Quando pode haver congestionamento.	Durante a configuração	Em todos os pacotes
Tarifação	Por minuto	Por pacote

Quadro 1 - Comparativo entre Comutação de Circuitos e Comutação de Pacotes. [2]

3. VoIP

A tecnologia VoIP consiste na utilização de uma rede de computadores para a transmissão de voz. O sinal da voz é digitalizado para em seguida ser transmitido usando a infra-estrutura da LAN ou WAN. Ao chegar ao destino, o sinal é convertido em analógico. [3]

Nesses tipos de rede, os principais protocolos que atuam são o TCP (*Transmission Control Protocol* - Protocolo de Controle de Transporte), o UDP (*User Datagram Protocol* - Protocolo de Datagrama de Usuário) e o IP (*Internet Protocol* - Protocolo de Internet).

Já os protocolos do serviço VoIP são fragmentados de acordo com a funcionalidade de cada um deles: Protocolos de Sinalização, Protocolos de Controle de *Gateway* e Protocolos de Transporte. As sessões a seguir tratam todos esses com maiores detalhes.

3.1 Protocolos de sinalização

Um protocolo de sinalização deve especificar a codificação da voz, a configuração das chamadas, o modo de autenticação, o transporte de dados e a sintaxe da mensagem. Tratando da tecnologia VoIP, dois protocolos gerenciam o serviço, o H.323 e o SIP. [4]

3.1.1 Protocolo H.323

É um protocolo para redes comutadas por pacotes. O H.323 suporta aplicações multimídias, porém não proporcionam qualidade no serviço (*QoS*). A interoperabilidade é garantida pela implantação de métodos e elementos de rede no fluxo de dados multimídia, além de serem estabelecidos meios para a codificação e decodificação das mensagens.

Os principais benefícios relacionados nesse protocolo são a independência da rede e plataforma, segurança, suporte *multcasting* e suporte a gerenciamento de largura de banda.

Trata-se de um padrão transparente à rede, já que pode ser aplicado tanto em redes *Ethernet*, *Fast Ethernet*, FDDI, *TokenRing*, sendo possível inclusive operar em redes *wireless*.

Os componentes principais em uma rede H.323 são os terminais, os *Gatekeepers*, as Unidades de Controle Multiponto e os *Gateways*. [4]

Terminais são os pontos finais da comunicação, os usuários comunicando em tempo real. Como exemplo, os computadores pessoais com recursos multimídias.

Os *Gatekeepers* desempenham o papel de uma central, ou seja, gerencia todas as chamadas de sua região.

Os *Gateways*, opcionais, têm a função de realizar a integração entre diversos terminais.

E por fim, as Unidades de Controle Multiponto, desempenham o papel de realizar conferências, ou seja, tratam as negociações entre todos os terminais de modo que possa determinar capacidades comuns no processamento multimídia.

A Figura 1 ilustra uma rede utilizando o protocolo H.323 e seus componentes, onde diversos dispositivos conseguem efetuar a comunicação simultaneamente. Aplicações multimídias, comunicação VoIP e integração com a com a PSTN (*Public Switched Telephone Network* - Rede Telefônica Comutada Pública) são algumas das funcionalidades que o protocolo proporciona. É a independência de topologia que permite essa integração.

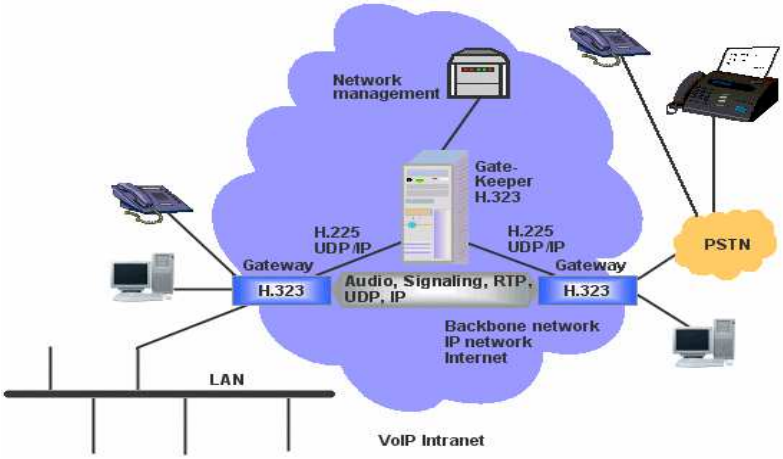

Figura 1 – Componentes de uma Rede H.323 [4]

3.1.2 Protocolo SIP

O SIP foi desenvolvido a fim de facilitar a implementação dos aspectos básicos de uma sessão, que é um processo nada trivial. Hoje é utilizado em escala mundial e é também um forte "concorrente" do H.323. [4]

SIP é um protocolo que sinaliza sessões cliente-servidor destacando presença e mobilidade, tendo como primitivas inicialização, modificação e finalização de sessões. [5]

Juntamente com RTP (*Real-time Transport Protocol)* , RTSP *(Real Time Streaming Protocol)*, SDP *(Session Description Protocol)*, o SIP estabelece uma arquitetura multimídia completa provendo serviços completos ao usuário. Os aspectos de segurança do SIP fornecem particularidades que incluem prevenção de negação do serviço, autenticação, integridade e serviços privados e encriptação.

A Figura 2 mostra uma rede com ambiente SIP, onde diferentes tipos de clientes têm acesso a esse protocolo, como: um telefone com suporte a protocolo SIP, um telefone sem fio com suporte ao SIP e também um computador convencional que possui um software de comunicação VoIP com suporte ao SIP.

Figura 2 – Ambiente SIP [6]

Alguns fatores viabilizam o destaque desse protocolo na comunicação IP. A modularidade, simplicidade, escalabilidade, e a integração de transporte tanto em TCP ou UDP são exemplos desse mérito ao SIP. [4]

De uma maneira geral, quando um ambiente está operando em modo SIP, existem 5 componentes principais:

- SIP *User Agent*: o ponto final da comunicação multimídia;
- SIP *Proxy Server*: servidor de redirecionamento de requisições e respostas SIP passa a realizar a sinalização como se fosse a origem da chamada, e quando a resposta lhe é enviada, ela é redirecionada para a origem real.
- SIP *Redirect Server*: redireciona requisições e respostas, enviando uma mensagem para os clientes com o novo endereço SIP procurado, e não fazendo o papel de continuar a chamada.
- SIP *Register Server*: servidor SIP que suporta as requisições usadas para registrar informações de usuários em algum Servidor de Localização.
- Servidor de Localização: na RFC (*Request for Comments)* do SIP, apenas as funcionalidades de armazenamento e consulta de registros de usuários SIP neste servidor são descritas, ficando a critério da solução SIP que se quer implementar a escolha da melhor tecnologia para esta finalidade.

3.2 Protocolos de controle de Gateway

São protocolos responsáveis pela interoperabilidade entre a rede VoIP e a rede telefônica pública. Executa a conversão de mídia em tempo real (Voz analógica x Voz digital comprimida) e a conversão de sinalização para as chamadas telefônicas que entram e saem da rede VoIP.

3.3 Protocolos de Transporte

Protocolo de transporte, em redes de computadores, é o protocolo da camada de transporte de dados do modelo OSI. Os dois protocolos mais utilizados nesta camada são: TCP *(Transmission Control Protocol)* e UDP *(User Datagram Protocol)*. [4]

O protocolo TCP é orientado à conexão. Nesse caso, a conexão estaria solucionando os problemas de erros que não foram solucionados ao nível de IP. Dessa forma, o TCP tem a missão de recuperar pacotes, ou avaliar se há duplicidade nos mesmos, ou seja, assegurar a integridade dos dados.

O protocolo “fornece” um número seqüencial para cada pacote, garantindo que os mesmos sejam entregues na mesma ordem de postagem em seu destino.

Protocolos trabalham com conceitos de portas, o que permite que vários programas estejam em funcionamento, sem que um interrompa o outro, trocando pacotes com um ou mais serviços.

O protocolo UDP é um padrão TCP/IP, e é utilizado em algumas aplicações em vez do TCP para o transporte rápido de dados. Uma das principais diferenças entre o TCP e o UDP é o fato de que o UDP é um protocolo não orientado à conexão, e que também não faz a verificação dos dados.

A definição de portas UDP é idêntica ao conceito de portas TCP, porém a maneira de como as portas são utilizadas é que se difere.

Devido a essas características, se um *host* necessita de uma comunicação confiável, ele certamente deverá usar o TCP em um aplicativo que ofereça seus próprios serviços de confirmação e seqüênciamento. [4]

3.4 Redes de acesso

Na telefonia IP, a rede é plana, não hierárquica, especializada no roteamento e transporte de pacotes de dados, e pode oferecer vários tipos de serviços. Os terminais são inteligentes, seu endereçamento independe de sua localização geográfica, e o processamento e a realização das chamadas ocorrem em vários equipamentos que podem estar localizados em qualquer parte da rede. [4]

No caso específico de VoIP, o acesso pode ser obtido através de um serviço IP ligando computadores ou IP *phone*, e ainda por uma herança analógica, *handsets* através de um *gateway*.

3.4.1 Arquitetura PC-A-PC

Conforme apresentado na Figura 3, nessa arquitetura dois computadores, dotados de recursos multimídia ligados por uma rede local ou Internet, se comunicam para a troca de sinais de voz. Entre essa conexão são realizados três processos de tratamento do sinal de voz para que se tenha uma comunicação perfeita, são eles: amostragem, compressão e empacotamento.

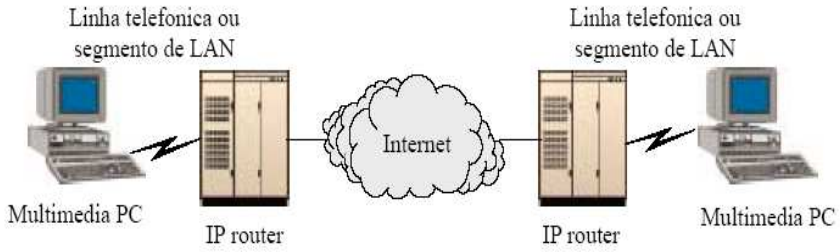

Figura 3 – Arquitetura PC-a-PC [7]

3.4.2 Arquitetura com Gateway

Na arquitetura com *Gateway*, um telefone específico (tipo VoIP com reconhecimento do SIP) é utilizado para realizar e receber chamadas da Internet. O usuário faz a conexão para seu *gateway* mais próximo, e esse tem a função de reconhecer e validar o

número telefônico do usuário de origem. Após esses passos, é realizada a autenticação e a solicitação do número do usuário de destino, conforme ilustrado na Figura 4.

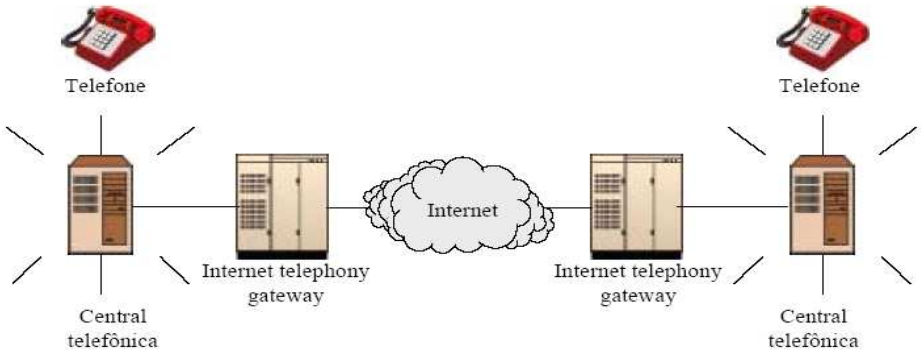

Figura 4 – Arquitetura com Gateway [7]

Assim, após *gateways* de entrada e saída serem reconhecidos, inicia-se a transmissão dos pacotes fim-a-fim. O processo de codificação do sinal e seu respectivo empacotamento são realizados no próprio *gateway* de origem enquanto o inverso é realizado no destino. A digitalização do sinal pode ser feita tanto no *gateway*, quanto na central e ainda no telefone.

3.4.3 Arquiteturas híbridas

Ilustrado na Figura 5, nessa arquitetura o usuário de um telefone analógico (convencional) realiza (ou recebe) uma ligação de um usuário de PC ou telefone IP. Em tais aplicações deve haver um sistema de translação de endereços IP em números telefônicos. Para tal feito podem ser empregadas quatro variações: PC-a-PC, PC-a-*Gateway*, *Gateway-a-Gateway*, *Gateway-a-PC*.

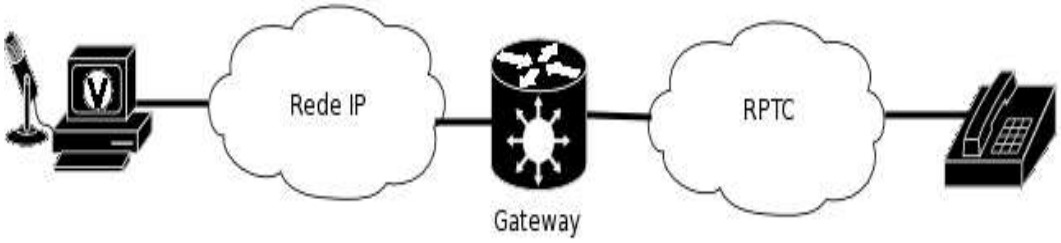

Figura 5 – Arquitetura Híbrida

Numa rede o tráfego de voz exige muito mais largura de banda do que a comunicação de dados, uma vez que para garantir a qualidade, a transmissão deve ser feita em tempo real e a perda de um pacote pode causar a degradação do sinal.

4. Ferramentas

Para que se possa comprovar a funcionalidade do assunto abordado, algumas ferramentas são necessárias. Esta sessão as descrevem com algumas de suas características principais.

4.1 Servidor STUN

O STUN (*Simple Traversal of User Datagram Protocol* (UDP), por meio da *Network Address Translators (*NATs)), é um servidor que permite que clientes NAT (ex.: computadores protegidos por *firewall*) realizem chamadas telefônicas a um provedor VoIP que se encontre fora da rede local. [8]

O servidor STUN permite que os clientes descubram seu endereço público, o tipo de NAT utilizado, e o lado da porta da Internet associada à NAT com uma porta local específica. Essas informações são usadas para permitir a comunicação UDP entre o cliente e o provedor VoIP, e então, estabelecer a chamada. O protocolo STUN é definido pela RFC *(Request for Comments)* 3489. [9]

O servidor STUN está ligado à porta UDP 3478. No entanto, o servidor irá sugerir aos clientes que realizem testes em IPs e números de portas alternativos. O RFC determina que tanto portas como IPs podem ser usados de acordo com a preferência do cliente.

Dentro desse trabalho, o STUN será instalado e configurado juntamente com o servidor VoIP. O STUN, uma ferramenta que executada no sistema operacional Linux, proporcionará ao cliente VoIP, sua conexão com o servidor.

4.2 Ferramenta Networkactiv PIAFCTM V 2.2.1 – Análise de Tráfego na Rede.

NetworkActiv PIAFCTM permite capturar e analisar pacotes IP, pesquisa de palavras e definir diferentes filtros para limitar a captura de pacotes. Além disso, permite capturar e armazenar arquivos completos HTTP (Web - páginas, fotos, downloads etc), que passam por seu computador através de sua rede. É uma ferramenta de fácil utilização para a rede TCP / IP, ideal para administradores e profissionais de segurança.

4.3 X-Lite

O X-Lite é um programa para realizar ligações através de um computador, que pode ser utilizado com um headset ou com microfone e caixas de som.

É importante frizar, que é um aplicativo bem fácil de instalar e simples de utilizá-lo. É a ferramenta que irá fazer a conexão com o servidor VoIP**.**

5. Metodologia

A metodologia utilizada para a coleta de dados constitui de pesquisa bibliográfica e estudo de caso. Para isso, a configuração das redes neste trabalho foi baseada nos estudos das redes de computadores e do serviço VoIP *(Voice over Internet Protocol)*.

O estudo de caso faz-se necessário devido a necessidade de comprovar que é possível utilizar-se de comunicação VOIP em uma rede de computadores sem que para isso seja necessário abrir mão do quesito segurança, ou ainda, colocando o mesmo em situação de fragilidade.

5.1 Ambiente de testes

Serão configuradas duas redes locais distintas, a fim de comprovar a funcionalidade do STUN, ambas com a mesma configuração. E fora dessas, será configurado o provedor VOIP, onde também será instalado este servidor.

A seguir, a descrição detalhada dessas redes e a configuração do servidor STUN:

5.1.1 REDES :

a) Configuração de cada Servidor/Roteador:

- Sistema Operacional: Suse Linux 9.3
- *Firewall Iptables*;
- Acesso à Internet Banda Larga;
- Duas placas de Rede (IP Falso (Rede Local) e IP Verdadeiro (Rede Pública))

b) Configuração de cada Cliente:

- *Desktop* com Processador Celeron® de 2.5 GHz;
- 512 de Memória RAM;
- 40 Gb de capacidade de disco rígido;
- Kit multimídia com caixas de som e microfone;
- Sistema Operacional Windows XP Professional;
- Software Fone X-Lite da Counter Path – Ferramenta para a comunicação VOIP;

5.1.2 SERVIDOR VOIP COM A CONFIGURAÇÃO DO SERVIDOR STUN

a) Servidor:

- Sistema Operacional: Suse Linux 9.3
- *Firewall Iptables*;
- Acesso à Internet Banda Larga;
- Software Asterisk (Aplicação Sip) – Provedor Voip
- Configuração do Servidor STUN;

5.2 Estudo de Caso

O presente estudo relata o funcionamento de um serviço VoIP juntamente com uma rede privada, onde encontra-se computadores, *gateways*, roteadores e inclusive um *firewall* configurado. O que ocorre é que em determinadas redes, as restrições são tantas que são capazes até de impedir ou prejudicar o funcionamento de alguns serviços.

A problematização levantada nesse trabalho é de que clientes de redes privadas não consigam acessar o serviço VoIP em uma rede pública, devido à segurança imposta pelo *firewall*. Nas redes privadas, cada computador recebe um número de “IP falso”, que só é válido para aquela rede. Determinados tipos de protocolos não conseguem funcionar com os “IP´s falsos”, o que torna necessário que haja uma translação para “IP ´s válidos”. Esse processo é feito por uma técnica chamada NAT (*Network Andress Translation* – Translação de Endereço de Rede). Apesar da técnica ser eficiente e muito utilizada, as regras de alguns *firewalls* chegam a ser tão rígidas que mesmo assim o serviço não funciona como o usuário deseja.

A cada dia milhares de novos computadores são conectados à Internet. Devido ao crescimento dessa rede, os especialistas têm cada vez mais preocupação com a segurança das informações que trafegam entre esses computadores.

Quando uma rede é criada, e interconectada a outras, milhares de pacotes transitam pelos mais variados percursos. Pelo fato de quase nunca ser possível saber por onde esses pacotes passam, e quem pode estar "acessando-os" é que ferramentas de segurança são implantadas em redes privadas. Apesar de todo esse cuidado, nem sempre há proteção total dos dados.

Uma ferramenta muito utilizada na criação e proteção de redes é o chamado *Firewall*. *Firewall* é um dispositivo que pode ser tanto físico quanto lógico e que irá determinar regras de acesso dentro de uma rede. O mesmo permite ou bloqueia o acesso às portas, protocolos, a programas ou a outros tipos de dados.

Para sanar a situação de endereços privados que não conseguem acessos a endereços públicos sem que se prejudique o nível de segurança da rede, foi configurada a ferramenta chamada STUN *(Simple Traversal of UDP NATs)* . Servidor STUN é um dispositivo que, mesmo com o *firewall* ativo e suas regras rígidas, ele proporcionará a clientes internos acessos à rede pública.

O STUN será configurado juntamente com o provedor VOIP, caracterizado pelo software ASTERISK.

Um dispositivo na rede pública reconhecerá o endereço externo do dispositivo atrás do NAT.

Sendo assim, pretende-se com a instalação e configuração do STUN que clientes de redes privadas distintas tenham acesso à um provedor VoIP que se encontra na rede pública.

Clientes de duas redes distintas foram configurados para acessar o serviço oferecido pelo servidor VoIP, este que se encontrava em um rede pública, por meio da ferramenta X-Lite. O X-Lite é um software que possui suporte ao protocolo SIP e ainda têm a funcionalidade de suportar servidores STUN.

A Figura 6 apresenta a interface do Software X-Lite. Conforme ilustrado, tem características semelhantes à de um telefone convencional:

Figura 6 – Interface X-Lite

Ainda no X-Lite, nas Figuras 7 e 8, é ilustrada a configuração do Software para a comunicação com o servidor VoIP.

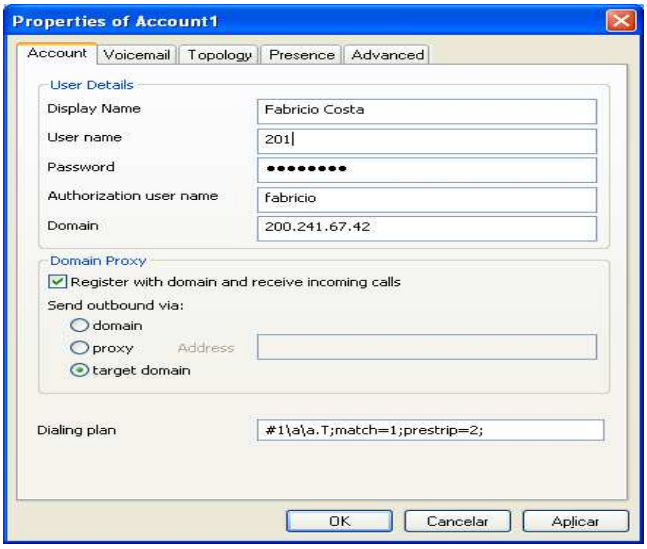

Figura 7 – Configuração X-Lite

A Figura 7 mostra, que cada usuário (*user name*) é identificado no servidor VoIP como se fosse um ramal(ex: 201), mas ainda assim existe um campo que identifica o nome do usuário com seu ramal (*Display Name*). O campo domínio (*Domain*) indica o endereço do servidor com a aplicação SIP (Servidor VoIP).

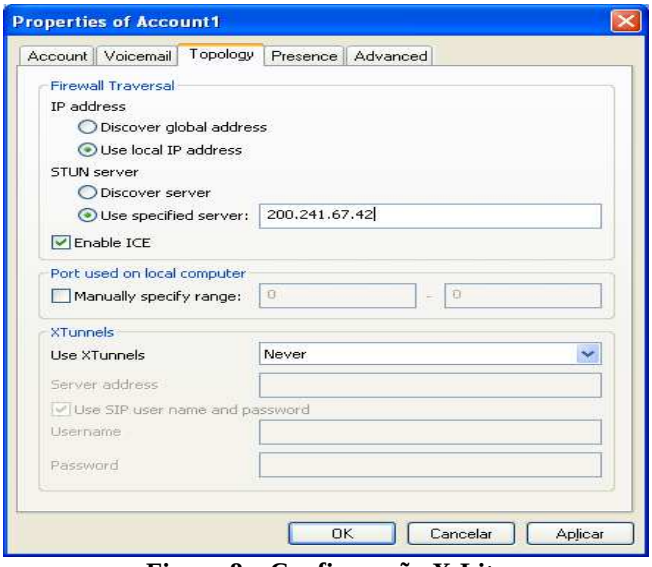

Figura 8 – Configuração X-Lite

Na Figura 8, encontra-se a especificação de endereço do servidor STUN. Comparando as duas figuras anteriores, observamos que o VoIP e o servidor STUN estão configurados no mesmo computador.

A Figura 9 ilustra como ficou estruturada as redes, com os clientes VoIP e o servidor STUN com a aplicação SIP (Servidor VoIP):

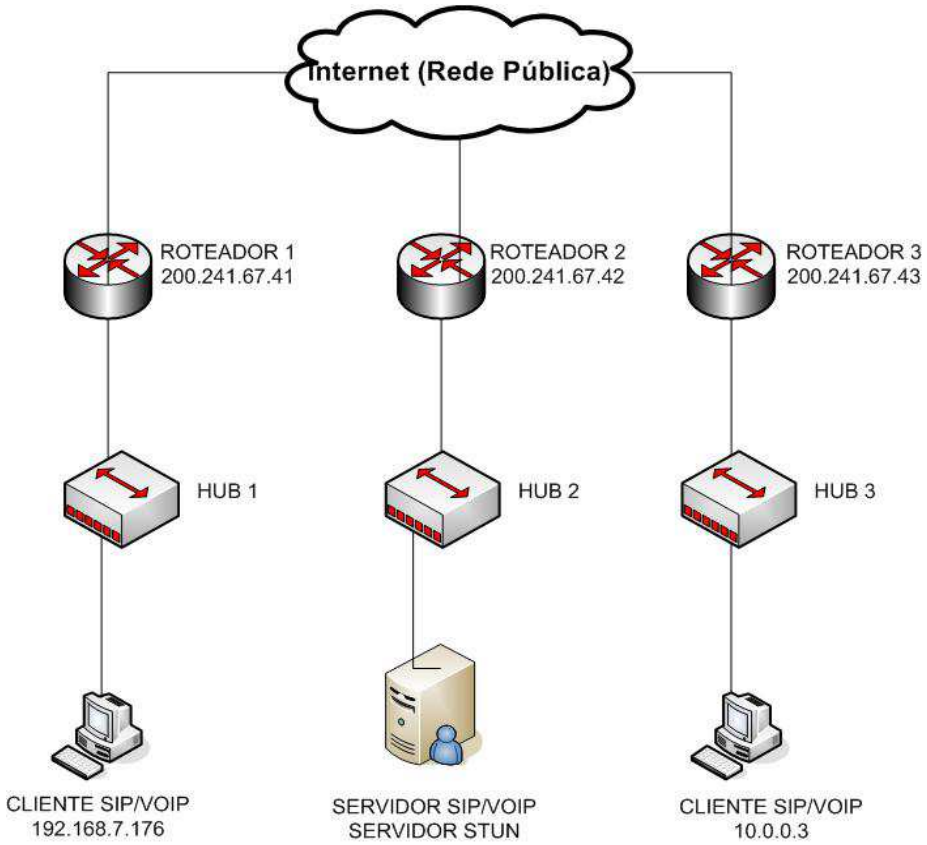

Figura 9 – Ambiente configurado para a Análise de Dados

5.3 Análise dos Dados

Dentro das redes foi instalada a ferramenta Networkactiv PIAFCTM V 2.2.1 que analisa o tráfego de pacotes em redes locais. Em um primeiro momento, a Figura 10 mostra as características dos pacotes coletados na rede durante a utilização do serviço VoIP. Na linha destacada, tem-se a captura de um pacote tentando realizar a comunicação UDP entre cliente e servidor pela porta 5060, que é a porta do protocolo SIP(Servidor VoIP), porém o aplicativo não consegue especificar esse pacote, pois o mesmo é barrado pelo *firewall* da rede e o STUN ainda não encontra-se ativo. A restrição estabelecida pelo *firewall* se faz bem rígida, estabelecendo acesso somente a alguns sites e algumas conexões remotas (conforme a configuração estabelecida). Como se pode notar não existe a especificação do pacote no local indicado pela ferramenta Networkactiv PIAFCTM V 2.2.1. Abaixo, a Figura 10 apresenta as determinações de origem, destino e autenticação dos pacotes da comunicação VoIP.

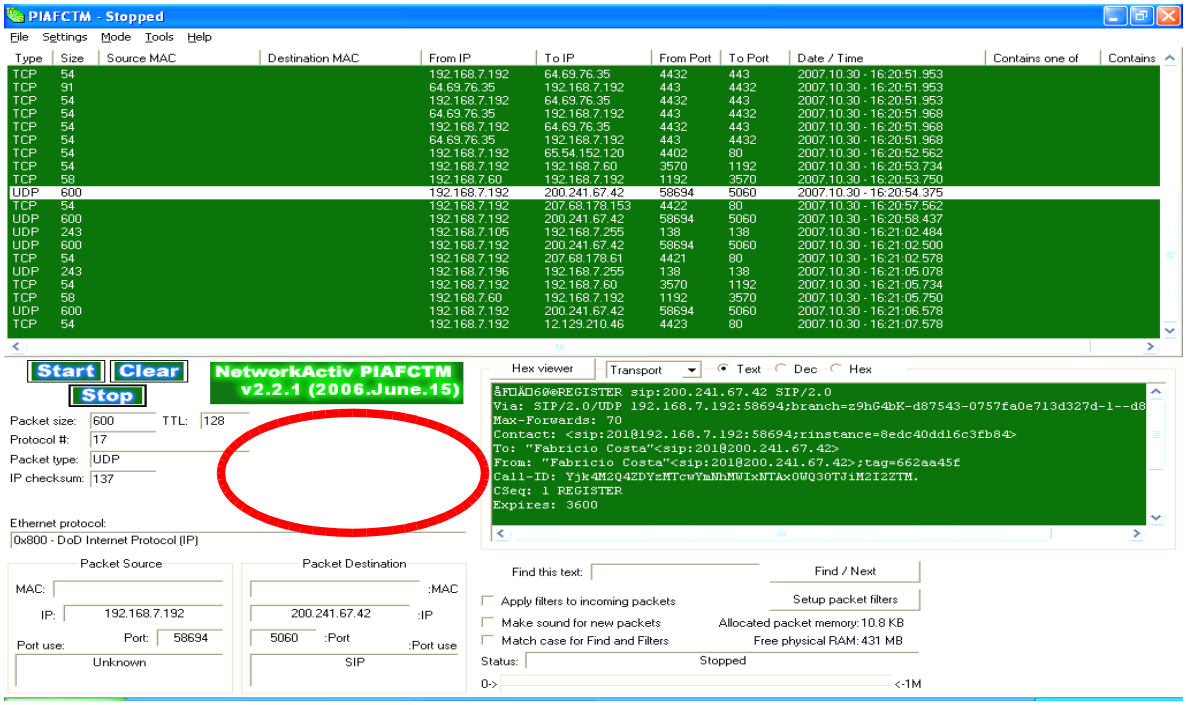

Figura 10 – Análise de Pacotes com o STUN inativo

A fim de estabelecer a referida comunicação sem que se viole as regras de segurança na rede, o servidor STUN foi ativado onde se encontra também configurada a aplicação SIP (Servidor VoIP).

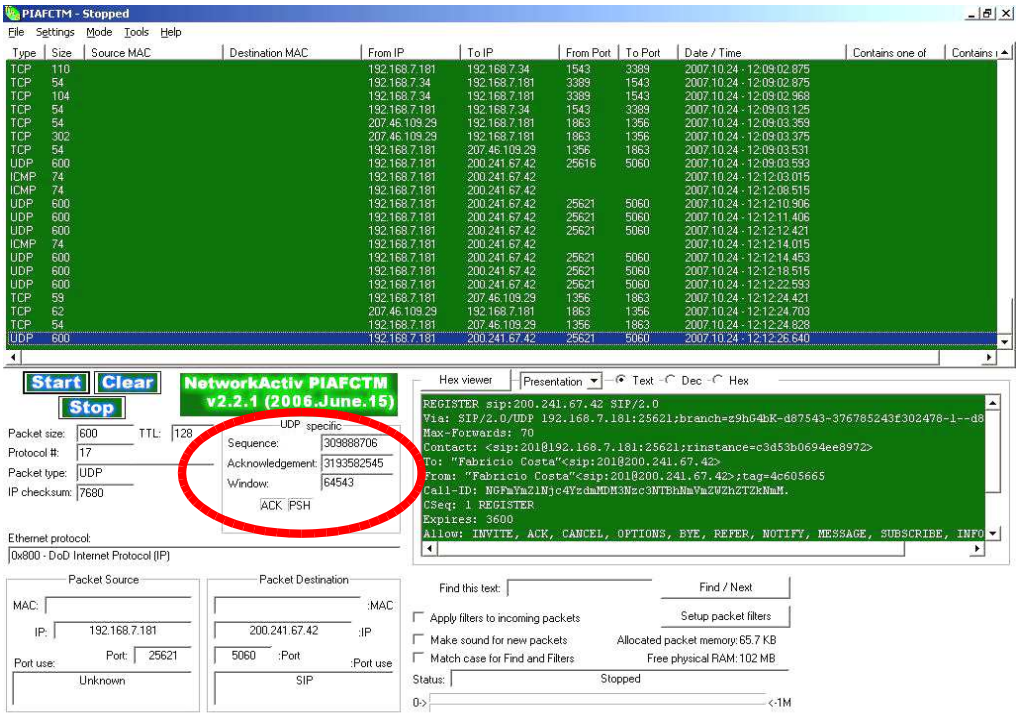

Figura 11 – Análise de Pacotes com o STUN ativo

Feito isso, novamente tentou-se realizar a comunicação com o software X-Lite obtendo êxito, conforme mostra a ferramenta Networkactiv PIAFCTM na Figura 11. Observe que na linha destacada acima, encontra-se informações da conta/usuário SIP e também as configurações de autenticação no servidor VoIP. Na área destacada é

possível identificar a especificação do pacote, ao contrário da situação obtida na Figura 10.

Mediante tais considerações, conclui-se que a configuração do STUN permite que clientes de redes locais tenham acesso ao servidor VoIP sem que se alterem políticas de segurança das organizações.

6. Considerações Finais

O tema abordado nesse trabalho, é mais um passo da tecnologia da informação, onde basicamente compartilha-se pacotes de dados e voz em tempo real em uma mesma estrutura física.

No decorrer dessa pesquisa, tornou-se necessário ressaltar algumas considerações. Inicialmente, tinha-se a proposta com apenas alguns dos fundamentos que seriam utilizados. Após a coleta bibliográfica, pôde-se estruturar como o trabalho seria desenvolvido, incluindo definição de conceitos, que tipo e quais ferramentas seriam utilizadas e a criação do ambiente de testes. Após o cumprimento desta etapa, partiu-se para a aplicação prática, realizando configurações, testes e análises.

Através do estudo de caso observou-se que a utilização da comunicação através da tecnologia VoIP é possível sem que para isso seja necessário abrir mão da segurança. Desta forma, com a correta configuração do servidor STUN torna-se possível efetuar ligações VoIP passando pelo *firewall* sem qualquer tipo de problema.

A partir desse estudo pode-se identificar novas alternativas para a comunicação comprovando suas funcionalidades no ambiente de testes instaurado. Com as ferramentas apresentadas, foi configurada uma solução de comunicação de baixo custo, e que ainda deixa um leque para aprimoramentos em estudos futuros.

O mercado tecnológico, dentro do contexto atual, pode acompanhar as tendências trazendo ao usuário final soluções que aproveitem ao máximo o hardware já existente e que ainda tenham a facilidade de se configurá-las ou implementá-las, como foi o caso desse instrumento.

Para trabalhos futuros, fica a idéia de se estudar a viabilidade de comunicação VoIP com a redução gradativa da segurança do *firewall* considerando o servidor STUN inativo. Com essa hipótese, pode-se ter a idéia da necessidade de segurança nas redes. Outro fator que também pode ser validado, é a necessidade de largura de banda para que se estabeleça essa comunicação de forma eficaz.

7. Referências Bibliográficas

[1] CENTRAL TELEFÔNICA 3CX IP. Definição de VoIP. Disponível em http://www.3cx.com.br/voip-sip/voip-definition.php. Acesso em 19 out. 07.

[2] TANENBAUM, Andrew S. A Camada Física. Cap. 2 In: Redes de Computadores. São Paulo: Campus,(1990). p: 87- 193.

[3] INFO WESTER. Tecnologia VOIP. Disponível em http://www.infowester.com/voip.php. Acesso em 03 mai.07.

[4] BARBOSA, Camila Soares. Voz sobre IP em Redes Locais sem Fio. CEFET – Centro Federal de Educação Tecnológica de Goiás. Goiânia, (2006).

[5] SIP. Definindo o que é um protocolo de sinalização. Disponível em http://www.gta.ufrj.br/grad/06_1/sip/Definindooqueumprotocolodesinalizao.html. Acesso em 03 mai.07.

[6] SANTOS, Rafael Moraes. Telefonia IP: Estudo dos Protocolos SIP e H.323. CEFET Centro Federal de Educação Tecnológica de Goiás. Goiânia, (2006)

[7] CEFET – RIO. VoIP. Disponível em www.cefetrio.hpg.ig.com.br. Acesso em 19 out. 07.

[8] NEWPORT NETWORKS. Solving the Firewall and NAT Traversal Issues for Multimedia over IP Services. Disponível em http://www.newport-networks.com/whitepapers/nat-traversal3.html . Acesso em 28 mar.2007.

[9] RFC 3489 - STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs). Disponível em http://www.faqs.org/rfcs/rfc3489.html . Acesso em 15 de out. 2007

[10] TELECO. Banda Larga e VOIP. Disponível em http://www.teleco.com.br/tecvoip.asp. Acesso em 08 jun.07.