

CENTRO UNIVERSITÁRIO SENAC

Rodrigo Morim Martins

OUTROS TRABALHOS EM:

www.projetoderedes.com.br

SEGURANÇA EM SISTEMAS VOZ SOBRE IP

São Paulo
2007

Rodrigo Morim Martins

Segurança em Sistemas Voz sobre IP

Trabalho de conclusão de curso
apresentado ao Centro Universitário
Senac como exigência para
obtenção da Pós Graduação em
Segurança de Redes e Sistemas.

Orientador Prof. Marcelo Lau

São Paulo
2007

Martins, Rodrigo Morim

Segurança em Sistemas Voz Sobre IP /

Rodrigo Morim Martins – São Paulo, 2006

113 f.

Trabalho de Conclusão de Curso – Centro Universitário

Senac – Lapa – Pós Graduação em Segurança de Redes e Sistemas.

Orientador: Prof. Marcelo Lau

1. Voz Sobre IP 2.Segurança

Aluno: Rodrigo Morim Martins

Titulo: Segurança em Sistemas Voz sobre IP.

Trabalho de conclusão de curso
apresentado ao Centro Universitário
Senac como exigência para
obtenção da Pós Graduação em
Segurança de Redes e Sistemas.

Orientador Prof. Marcelo Lau

A banca examinadora dos Trabalhos de Conclusão em
sessão pública realizada em __/__/____, considerou o(a)
candidato(a):

- 1) Examinador(a)

- 2) Examinador(a)

- 3) Presidente

São Paulo
2007

Dedico esse trabalho aos meus pais, minha namorada,
pela dedicação e apoio durante todos os
momentos da minha vida.

AGRADECIMENTOS

Ao Centro Universitário Senac, agradeço a oportunidade que me foi dada de ser aluno do curso de Pós Graduação desta instituição.

Ao Prof. Marcelo Lau, por suas orientações que foram fundamentais para a consecução deste trabalho.

“Um homem não entra duas vezes no mesmo rio; da segunda vez não é o mesmo homem nem o mesmo rio.”

(Heráclito de Éfeso)

RESUMO

O presente trabalho, intitulado "Segurança em Sistemas Voz sobre IP" propicia o estudo da segurança em redes Voz sobre IP, onde apresentaremos a infra-estrutura da rede de dados para trafegar voz, a comparação de diferentes tipos de protocolos utilizados para sinalização e troca de informações, as principais ameaças dentro de um ambiente corporativo e os tipos de ataques que afetam a segurança em Voz sobre IP. Este trabalho traz também o histórico do desenvolvimento desta solução, bem como o uso de diversas topologias seguras para evitar ameaças e corrigir possíveis vulnerabilidades.

A segurança em sistemas Voz sobre IP é aplicada para evitar que um invasor possa obter informações que tornarão possíveis a obtenção de lucros de forma indevida, realize uma escuta telefônica, coleta de dados ou falsificação de identificação à utilização do serviço de forma indevida. Cada vez mais as empresas estão habilitando soluções Voz sobre IP, com isso as demandas de desenvolvimento de aplicações seguras em ambientes corporativos se tornam necessárias.

Palavras-chave: Voz Sobre IP, segurança, protocolos.

ABSTRACT

The current document, entitled "Voice over IP Security", propitiates the study of network security, where the internet network is used to transmit voice traffic. We analyzed the development history of this solution by comparing different protocols used for data exchange and signaling, main threats at the company environment, types of threats, as well the utilization of different secure topologies in order to avoid threats and to solve vulnerabilities.

The security on voice over IP systems is applied for avoiding a hacker to obtain important information and takes benefits on it, eavesdrop on VOIP calls, and collect data, ID falsification and improper service utilization. Companies are applying systems voice over IP more and more, therefore development of secure applications for corporation environments become necessary.

Keywords: Voice over IP, secure, protocols.

LISTA DE ILUSTRAÇÕES

Figura 1 – Mercado de Voz sobre IP.	15
Figura 2 – Evolução do mercado Voz sobre IP.	15
Figura 3 – Evolução de vendas.	16
Figura 4 – Arquitetura telefonia IP.	18
Figura 5 – Elementos fundamentais do terminal H.323.	19
Figura 6 – Fluxos de mídia H.323 com uso de gatekeeper.	20
Figura 7 – Zona H.323.	23
Figura 8 – Estabelecendo uma chamada.	24
Figura 9 – Sinalização RAS: uso de LRQ's.	29
Figura 10 – Arquitetura micro a micro.	32
Figura 11 – Arquitetura gateway a gateway.	33
Figura 12 – Sinalização entre dois terminais SIP.	37
Figura 13 – Arquitetura H.248/Megaco.	38
Figura 14 – Arquitetura básica de uma rede SIP.	48
Figura 15 – Topologia na LAN.	68
Figura 16 – Topologia na WAN.	76

LISTA DE TABELAS

Tabela 1 – Recomendações H.323.....	40
Tabela 2 – Formatos de mídia reconhecidos na arquitetura H.323.....	41
Tabela 3 – Classificação de ameaças - Parte I.....	58
Tabela 4 – Classificação de ameaças - Parte II.....	59
Tabela 5 – Classificação de ameaças - Parte III.....	60
Tabela 6 – Ameaças e medidas de contenção a ataques – Parte I.....	79
Tabela 7 – Ameaças e medidas de contenção a ataques – Parte II.....	80
Tabela 8 – Ameaças e medidas de contenção a ataques – Parte III.....	81
Tabela 9 – Ameaças e medidas de contenção a ataques – Parte IV.....	82

SUMÁRIO

1. INTRODUÇÃO	1
1.1 Conceitos	2
1.1.1 Voz sobre IP	2
1.1.2 Segurança	3
1.1.3 Sistema	3
1.2 Justificativa	4
1.3 Metodologia da pesquisa	4
1.4 Objetivo	5
1.5 Estrutura do trabalho	5
2. VOZ ATRAVÉS DE REDES DE COMUNICAÇÃO	7
2.1 História	7
2.2 Mercado de VOIP no Brasil e no mundo e suas tendências	13
2.3 Terminologia do ambiente Voz sobre IP	17
2.3.1 Terminais H.323	18
2.3.2 Gateways	21
2.3.3 Gatekeepers	22
2.3.4 Multipoint Control Units (MCU)	29
2.4 Arquiteturas	31
2.4.1 Arquitetura micro a micro	31
2.4.2 Arquitetura gateway	32
2.4.3 Arquitetura híbrida	34
2.5 Sinalização	34
2.6 Recomendação H.323	40
3. SEGURANÇA DA INFORMAÇÃO	43
3.1 Conceitos de Segurança da Informação	43
3.1.1 Ativo	44
3.1.2 Vulnerabilidade	44
3.1.3 Ameaça	44
3.1.4 Risco	45
3.1.5 Disponibilidade	45
3.1.6 Autenticidade	46
4. AMEAÇAS DE SEGURANÇA NO AMBIENTE VOZ SOBRE IP	47
4.1 Principais ameaças	49
4.1.1 Ataques à Disponibilidade	51
4.1.1.1 DoS (<i>Denial of service attack</i>)	51
4.1.1.2 DDoS (<i>Distributed denial of service attack</i>)	51
4.1.2 Ataques à Privacidade e Confidencialidade	52

4.1.2.1	<i>EAVESDROPPING</i> (Escuta telefônica).....	52
4.1.2.2	<i>Spam over IP Telephony</i> (SPIT)	52
4.1.3	Ataques à Integridade	53
4.1.3.1	<i>Man in the Middle</i> ou MITM (Homem no meio)	53
4.1.3.2	<i>Call Fraud</i> (Fraude nas chamadas).....	53
4.1.3.3	<i>Call Hijack</i> (Seqüestro de chamada).....	54
4.1.3.4	Falsificação de identidade do usuário	54
4.1.3.5	<i>Phishing</i>	54
4.1.3.6	<i>Malware</i>	55
4.1.3.7	Riscos relacionados ao Sistema Operacional	56
5.	MELHORES PRÁTICAS DE SEGURANÇA EM VOZ SOBRE IP	61
5.1	Protocolos de Segurança	61
5.1.1	<i>SIP Digest</i>	61
5.1.2	TLS Transport Layer Security.....	61
5.1.3	IPSec <i>IP Security</i>	62
5.1.4	SRTP Secure Real-Time Protocol.....	63
5.1.5	<i>AIB Authenticated Identity Body</i>	63
5.1.6	<i>IHF Identity Header Field</i>	64
5.2	Requisitos de segurança em projetos envolvendo voz sobre IP	64
5.2.1	<i>Firewalls</i> Voz sobre IP	65
5.2.2	IPS Voz sobre IP	65
5.2.3	Segurança nas estações de trabalho	66
5.2.4	Zonas Militarizadas	66
5.2.5	<i>Resilience</i>	67
5.2.6	Monitoração.....	67
5.3	Segurança na LAN	68
5.3.1	Segmentação do tráfego de voz e dados.....	69
5.3.2	Segmentação de Servidor DHCP	70
5.3.3	<i>Appliance</i> Multifuncional.....	70
5.3.4	Configurar os telefones IP com endereços IP associados ao <i>mac</i>	71
5.3.5	Usar endereços IP privativos e inválidos nos telefones IP	72
5.3.6	<i>Personal firewall</i>	72
5.3.7	Utilização de senha	73
5.3.8	Restringir o acesso físico	74
5.3.9	Auditar os recursos Voz sobre IP	75
5.4	Segurança na WAN.....	76
5.4.1	Virtual Private Network (VPN)	76
5.4.2	Internet com VPN	78
5.4.3	Segurança em acessos remotos	78
5.5	Resumo das melhores práticas em segurança no Ambiente VOIP	79
6.	CONSIDERAÇÕES FINAIS	84
6.1	Trabalhos Futuros	84
6.2	Conclusão	85

REFERÊNCIAS BIBLIOGRÁFICAS.....	87
--	-----------

1. INTRODUÇÃO

É crescente a demanda para a migração de redes tradicionais¹ para redes convergentes² através de Voz sobre IP³. Isto ocorre principalmente devido à redução de custos operacionais, proporcionando retorno de investimento (*ROI*), mobilidade para os usuários, provendo acesso à comunicação e às aplicações de qualquer ponto da rede e compartilhamento de recursos entre diversas unidades, tais como aplicações de correio de voz, *contact center*⁴, gravação digital, telefonista, entre outros.

Para implementar uma rede Voz sobre IP é necessário planejamento e aquisição de recursos adicionais que diferem dos recursos necessários utilizados na telefonia tradicional. Em virtude desta nova infra-estrutura, a segurança e a disponibilidade devem receber atenção especial tanto na implementação quanto na manutenção do ambiente, pois novas ameaças surgem nesta infra-estrutura que não se apresentam no ambiente de telefonia tradicional.

¹ Redes tradicionais no mundo de telecomunicações e informática são plataformas de comunicação totalmente independentes, onde temos uma infra-estrutura dedicada para os elementos de redes, que compõem a rede de dados, e uma infra-estrutura dedicada para os elementos de telefonia, que compõem a rede de telefonia.

² Redes convergentes: é a união dos mundos de voz, dados e imagem. O termo convergência tem sido amplamente empregado pelo setor de tecnologia. Sua aplicação designa a união dos mundos de voz, dados e imagem para uma mesma plataforma de comunicação, com todos os recursos e facilidades.

³ Pesquisa de Mercado realizada pela empresa Siemens. Disponibilizada através de um *Whitepaper* nomeado: "Segurança em Redes Convergentes Versão 1.0" do mês de agosto de 2006.

⁴ *Contact Center*: Aplicação preparada para oferecer atendimento por diversos meios de comunicação, como o telefone e e-mail. Os *contact centers* podem utilizar mecanismos que possibilitam o contato direto entre o chamador e os operadores automatizando o atendimento.

Em virtude deste novo cenário este trabalho apresenta sua contribuição apresentado como foco principal a segurança no ambiente Voz sobre IP.

1.1 Conceitos

Para que o leitor obtenha melhor entendimento é importante conceituar alguns termos que fazem parte deste trabalho. A seguir apresentaremos os conceitos dos seguintes termos: Voz sobre IP, segurança e sistema.

1.1.1 Voz sobre IP

Voz sobre IP (*Voice over IP*) é a tecnologia que permite a transmissão de voz por uma rede de dados. Isso pode significar todo um sistema de telefonia trafegando pela Internet.

A voz, através de equipamentos e *softwares* específicos, é transformada em pacotes de dados e, em vez de seguir por ramais telefônicos, se vale das infra-estruturas existentes de banda larga, antes usada apenas para finalidades como e-mail ou acesso à internet. Quando transmitidas por esses canais, essas ligações são novamente convertidas em voz quando chegam ao seu destino. [1]

1.1.2 Segurança

O conceito de segurança nos remete a termos como garantia, firmeza, certeza, confiança, convicção. Portanto segurança é a qualidade, condição daquilo que é confiável, indubitável e indevassável.

Segurança da informação importa em adotar critérios e medidas protetores da informação consistida em qualquer tipo de suporte e linguagem documental. [1]

Desta forma a segurança é um dos fatores mais importantes para garantir a confiabilidade, integridade e disponibilidade das chamadas telefônicas transmitidas através da rede de dados nos sistemas Voz sobre IP.

1.1.3 Sistema

O conceito de sistema é uma das mais simples de se escrever, um dos mais abrangentes de se aplicar, bem como um dos mais difíceis de compreender plenamente.

Um sistema pode ser definido como um conjunto de elementos inter-relacionados que interagem no desempenho de uma função.

Em sistemas Voz sobre IP, sistemas são conjuntos de elementos inter-relacionados (chamados de componentes), e que podemos identificar alguma função desempenhada pelo sistema como um todo. Alguns componentes tais como, terminais, *gateways* e *gatekeepers* fazem parte de um sistema Voz

sobre IP, maiores informações sobre estes componentes serão ilustradas no decorrer deste trabalho. [1]

Os demais termos não apresentados apresentam-se disponíveis no glossário.

1.2 Justificativa

Este trabalho tem o propósito de apresentar e demonstrar os sistemas Voz sobre IP, buscando identificar suas características, no ponto de vista de segurança e no ambiente operacional onde o sistema está operando.

Através do mapeamento de falhas e de vulnerabilidades, é possível identificar neste trabalho a aplicação segura de sistemas Voz sobre IP, dependendo de topologias e elementos de redes capazes de tornar o ambiente seguro.

1.3 Metodologia da pesquisa

Para alcançar os objetivos deste trabalho, foi utilizada como base de estudos e pesquisa uma extensa bibliografia, onde o assunto principal é a segurança em sistemas Voz sobre IP, para composição dos tópicos contidos neste trabalho. Como existe um vasto material sobre segurança em sistemas Voz sobre IP disponível na Internet, a qual foi a principal fonte para obter informações sobre este assunto, houve a preocupação em selecionar artigos e publicações de fontes confiáveis, tais como documentos publicados por

empresas ligadas ao desenvolvimento de sistemas Voz sobre IP, bem como organismos que, apesar de não estar relacionados especificamente ao assunto segurança em Voz sobre IP, fazem referência à Voz sobre IP como forma de garantir a segurança destes sistemas.

1.4 Objetivo

Demonstraremos a evolução dos sistemas Voz sobre IP, terminologias aplicáveis no ambiente, protocolos de comunicação utilizados para o tráfego de voz, os possíveis impactos de segurança causados pelas novas aplicações sobre as redes e analisar o nível de criticidade de ameaças sobre as aplicações e serviços oferecidos pela Voz sobre IP.

Este trabalho tem objetivo de mostrar que a convergência dos sistemas tradicionais para Voz sobre IP permitiu o surgimento de novas vulnerabilidades para redes de computadores afetando a segurança e sigilo das informações.

1.5 Estrutura do trabalho

Com a finalidade de consecução dos objetivos deste trabalho, a estrutura deste trabalho foi organizada da seguinte forma:

O capítulo dois introduz os conceitos básicos sobre segurança em sistemas Voz sobre IP, bem como trata e apresenta suas origens, relacionando os primeiros sistemas que se tem conhecimento sobre uso da Voz sobre IP,

traçando uma linha no tempo até os dias atuais, no mundo e também da evolução de sistemas Voz sobre IP no Brasil.

No capítulo três são abordados conceitos relacionados à segurança da informação, tais como confidencialidade, integridade e disponibilidade. Dentro deste contexto, é feita uma descrição dos processos de confidencialidade, integridade e disponibilidade no ambiente Voz sobre IP.

O capítulo quatro apresenta uma avaliação das principais ameaças nos sistemas Voz sobre IP.

O capítulo cinco apresenta melhores práticas de segurança em Voz sobre IP, demonstrando diversas soluções desenhadas e desenvolvidas para infra-estruturas convergentes, protocolos de segurança e requisitos de segurança em projetos envolvendo Voz sobre IP.

Na parte final do trabalho é apresentada a conclusão, bem como algumas indicações de futuros trabalhos acadêmicos que poderão ser elaborados, de modo a complementar um tema tão abrangente, como é segurança em sistemas Voz sobre IP.

2. VOZ ATRAVÉS DE REDES DE COMUNICAÇÃO

2.1 História

Nos anos 70, universitários pesquisadores que já trabalhavam com a transmissão de dados e texto na *Arpanet*, rede de computadores de algumas universidades entre elas a Universidade da Califórnia em Los Angeles, decidiram tentar trafegar voz em uma rede de dados existente. Alguns destes experimentos mostravam que conferências de voz eram possíveis utilizando a tecnologia de comutação de pacotes⁵, entretanto, nenhuma ferramenta foi desenvolvida para que pudessem ser amplamente utilizados estes recursos.

No fim dos anos 80 e início dos anos 90, o crescimento do poder computacional fez com que máquinas convencionais realizassem conferências de voz entre usuários conectados à Internet. Diversos experimentos realizados utilizando *multicast*⁶ geraram ferramentas que permitiam a conferência de voz. Entretanto, era pouco freqüente a utilização destas ferramentas, visto que poucas pessoas na Internet tinham acesso a máquinas com o sistema operacional UNIX e estas ferramentas, além de instáveis, eram difíceis de serem utilizadas. Na época a banda disponível era limitada nas conexões que formavam o *backbone*⁷ da Internet, por isso a obtenção de qualidade de som

⁵ Em sistemas que utilizam comutação por circuito, dois circuitos são necessários para efetuar a comunicação entre dois pontos do início ao fim da chamada. Na comutação por pacotes, um número maior de comunicações pode estar em curso no mesmo circuito. Para maior detalhamento, consulte o tutorial disponível em: <<http://www.techguide.com>>.

⁶ *Multicast* é uma tecnologia de conservação de banda que permite que um fluxo de dados seja enviado para múltiplos destinos simultaneamente.

⁷ *Backbone* são linhas base de conexão de alta velocidade dentro de uma rede, que, por sua vez, se conectam às linhas de menor velocidade. Num nível de rede local, como o de uma empresa, por exemplo, o *backbone* é uma linha ou um conjunto de linhas com a qual uma rede local se conecta a uma rede maior, como a Internet, por exemplo. Na Internet, *backbone* é um

era praticamente impossível. Apesar de não ser necessário ter muita banda de comunicação, diversos fatores são importantes para a qualidade do som sendo susceptíveis a perda de pacotes e atrasos, demora no recebimento.

A partir de 1995, o avanço na infra-estrutura das redes, na codificação da voz e no poder computacional dos elementos de *hardware* permitiu a proliferação dos sistemas Voz sobre IP. Nestes anos, diversos produtos comerciais foram lançados para aplicações Voz sobre IP.

A empresa Vocaltec (israelense) em 1995 fez o lançamento do *Internet Phone*⁸, programa de computador que trafega voz sobre a rede da internet, este foi o primeiro produto utilizado comercialmente em grande numero. Este produto mostrava que uma chamada VOIP (Voz sobre IP) não era muito diferente de uma chamada realizada por uma linha telefônica. [2]

Com o lançamento de soluções que possuem a característica de prover a comunicação entre dois computadores, não era possível uma linha convencional⁹ se comunicar com estes computadores, exemplo uma conexão com a Internet através de uma linha telefônica residencial. Então surgiram os equipamentos com função de converter a comunicação entre a Internet, e a rede de Telefonia, convertendo os sinais de voz analógico do telefone, em pacotes IP que trafeguem na Internet, esses equipamentos são denominados “*Gateways de Voz*”.

conjunto de caminhos pelos quais as redes menores se unem para efetuar uma conexão de longa distância.

⁸ Programa de computador que emula funções de um aparelho telefônico. Exemplo de ferramentas atuais: Microsoft *NetMeeting* <http://www.microsoft.com/netmeeting/>, *Skype* entre outros. Para maior detalhamento sobre o *Internet Phone*, consulte o site do fabricante, disponível em: <<http://www.vocaltec.com>>.

⁹ Linha convencional, linha telefônica residencial utilizada para prover solução de telefonia fixa.

No início de 1996, surgiu a “*Free World Dialup*”¹⁰ uma associação de pessoas que desenvolveram um projeto de um *software* que permitia que usuários conectados a Internet ligassem para telefones convencionais que, apesar de suas restrições, mostrou que a Internet não era limitada apenas às máquinas conectadas.

As primeiras soluções Voz sobre IP conectadas a centrais telefônicas se basearam em conexão através de ATM por meio da recomendação (ITU-T I.363.1) que especifica a camada de adaptação (AAL-1)¹¹, onde são definidos serviços que disponibilizam o desenvolvimento de aplicações que tenham como requisitos a transferência de dados a uma taxa constante de bits e o suporte ao sincronismo entre destino e origem. Com a definição desta camada possibilitou o desenvolvimento de aplicações para emulação de circuitos *multiplexing* de divisão do tempo (TDM), que permitiram instalar o serviço de voz sobre ATM (*Voice over ATM*), voz trafegando sobre redes de *multiplexing*¹² de tempo. Diversos projetos foram realizados na época utilizando estes recursos, tais como a da rede de pesquisa da Austrália (AARnet – *Australian Academic and Research Network*). Neste projeto¹³ os PBX (*Private Branch Exchange*) ou centrais telefônicas, foram interligados utilizando PVC's (*Permanent Virtual Circuit*), circuitos virtuais permanentes, que emulavam circuitos TDM E1 (N x 64 Kbps). O que restringia a utilização do serviço era que todas as localidades deveriam estar interligadas a Internet através de redes ATM. [3]

¹⁰ Maiores detalhes sobre projetos desenvolvidos por essa empresa. Consulte o site, disponível em: <<http://www.freeworlddialup.com>>.

¹¹ Especificações detalhadas sobre a camada de adaptação, tal como as recomendação ITU-T 363.1 e o protocolo ATM . Consulte o documento, disponível em: <<http://ieeexplore.ieee.org/iel5/50/29736/01353395.pdf>>.

¹² *Multiplexing* de tempo é um sistema assíncrono de divisão de tempo, onde os *time slots* são atribuídos dinamicamente aos utilizadores conforme solicitado.

¹³ Rede de Pesquisas, *Australian Academic and Research Network*. Consulte o site, disponível em: <<http://old.www.aarnet.edu.au>>.

Quando os primeiros *gateways* de Voz sobre IP surgiram, em função de sua facilidade de conexão e abrangência, a Internet se tornou o meio ideal para a implementação do serviço de telefonia. Com esses equipamentos se tornou possível implementar o conceito de telefone IP, onde *PBX's* em localidades distintas eram conectados utilizando a rede IP como transporte. Esta aplicação tornou possível a conectividade telefônica entre as localidades remotas sem a necessidade de utilizar a rede de telefonia pública.

Como o *gateway* é um dispositivo de grande importância no processo de comunicação de Voz sobre IP, consideramos importante uma breve conceituação deste equipamento, o *gateway* é um equipamento que converte o sinal do PBX em pacotes IP, estes pacotes são transmitidos pela Internet até o *gateway* remoto, onde são convertidos para a rede de telefonia e então transmitidos para o telefone remoto. Outra possível aplicação é a utilização dos *gateways* interligados diretamente na rede pública, possibilitando que ligações de longa distância sejam efetuadas sem a utilização do serviço das operadoras de telefonia pública. Temos as seguintes vantagens quando utilizamos os serviços de telefonia sobre IP:

- Convergência das redes de telefonia e de dados para uma única estrutura e;
- Já que será utilizada a mesma equipe para cuidar da solução teremos redução de custos com a operação e quando uma corporação possui diversas localidades remotas, pois não existe a necessidade de utilização de linhas independentes para dados e telefonia e independência do custo em relação a distância.

O detalhamento aprofundado sobre *gateways* pode ser visto no item 2.3 deste trabalho.

A partir do final da década de 90, a padronização dos protocolos de sinalização e de transporte de mídia na rede IP relacionados com a crescente oferta de *gateways* de voz e vantagens oferecidas pelos serviços de telefonia IP, tornou-se mais simples a implementação e manutenção dos sistemas, e incentivou a criação de diversos projetos para a instalação deste serviço. [4] Maiores detalhes no capítulo de sinalização adiante neste trabalho.

Na área acadêmica, na década de 90 alguns trabalhos merecem destaques tais como o realizado nas redes nacionais de pesquisa da Alemanha, República Tcheca, Austrália, nas quais foram utilizadas o protocolo H.323 para fins de sinalização, (tendo em vista o uso do protocolo SIP). Este trabalho tem como finalidade demonstrar a utilização do protocolo H.323 desenvolvido por especialistas que atuam na área de telecomunicações e o protocolo SIP que foi desenvolvido por especialistas que atuam na área de informática, bem como suas aplicações.

A pesquisa do projeto Voz sobre IP da rede Nacional da Alemanha iniciou em 2000 tendo como objetivo testar a interoperabilidade dos dispositivos e a qualidade necessária para a transmissão de voz. No fim de 2002, aproximadamente 20 centros universitários e alguns centros de pesquisa participavam do projeto. [4]

A pesquisa do projeto¹⁴ da rede da República Tcheca (*CESNET – Czech Education and Scientific Network*) teve início em 1999 com o objetivo de interligar os PBX's de diversas localidades e conectar a estrutura à rede de telefonia pública. O projeto envolve 12 localidades conectadas através de 10 *gateways* de voz. Este projeto tem como objetivo testar a interoperabilidade

¹⁴ Projeto completo da “*Australian Academic and Research Network*”. Disponível na internet em: <<http://www.aarnet.edu.au/rd/voip/index.html.aarnet.edu.au>>.

dos produtos de diferentes fabricantes, o desenvolvimento de novas ferramentas e componentes visando o uso de tecnologia. [5]

O grupo de trabalho da RNP (Rede Nacional de Pesquisa), no Brasil, desenvolve experimentos de telefonia IP associados a VOIP, sendo responsável pela implementação de um serviço experimental no *backbone*, permitindo às organizações usuárias utilizar suas redes para estabelecer comunicação de voz a partir de seus *PBX's*, telefones IP e/ou estações de trabalhos. No projeto implementado em 2004, foram utilizados *gateways PSTN/H323* (centrais convencionais / centrais Voz sobre IP), que possibilitam a interligação da Internet com os *PBX's* e o uso de transparência de facilidades de telefonia IP para o usuário final, e a implementação de *gatekeepers* que facilitaram a utilização da telefonia IP diretamente às estações de trabalho. [6]

A partir de 2004 as soluções de telefonia IP também passaram a ter um custo um pouco mais acessível, e se tornaram também cada vez mais robustas e dependendo do tipo de solução Voz sobre IP, o valor do investimento se paga em curto espaço de tempo.

Tendo diversos tipos de fabricantes disponíveis no mercado aliados a grande evolução do poder computacional, tornou-se necessário a adoção de padrões para a comparação da qualidade do serviço prestado pelo serviço de voz. Um destes parâmetros é a disponibilidade, definida como a probabilidade de uma chamada ser estabelecida com sucesso na primeira tentativa em que é realizado, não considerando fatores como telefone ocupado e linhas não atendidas. Considerando que as chamadas realizadas com sucesso ocorrem enquanto o serviço está operacional, a disponibilidade do serviço pode ser calculada como proposto por *Jiang e Shulzrinne*: [4]

Disponibilidade = $\frac{\text{número de chamadas realizadas com sucesso}}{\text{número de chamadas realizadas (Primeira Tentativa)}}$

Objetivando a medição da disponibilidade de um serviço VOIP atuando na Internet, estes pesquisadores obtiveram um índice de 98% de disponibilidade em testes envolvendo medições ativas, longe dos 59% da telefonia celular, mas aceitável se comparada à da telefonia tradicional, normalmente entre 97% e 99%.

2.2 Mercado de VOIP no Brasil e no mundo e suas tendências

O mercado de equipamentos que provém soluções Voz sobre IP, mais do que dobrará entre 2006 a 2009: passará de 6,0 bilhões de reais para 13,8 bilhões de reais. As vendas desse tipo de equipamento e serviço crescerão 26% ano após ano, segundo o estudo divulgado pela *Infonetics Research*. [7]

De acordo com a pesquisa, o mercado das empresas prestadoras de serviços Voz sobre IP é robusto e aponta para um ciclo de investimentos sustentáveis, já que não tem as extravagâncias que resultaram na quebra do setor de telecomunicações entre 2000 e 2002.

Ainda segundo a *Infonetics*, todos os segmentos exceto o *softphone*, que são terminais no formato de *software* para instalação no PC do usuário, mostraram crescimento no quarto trimestre de 2006. O estudo também destaca que o segmento de *gateway* crescerá 11% por trimestre e 45% ano após ano e o número de assinantes VOIP residenciais e de pequenos escritórios vai aproximadamente dobrar entre 2006 e 2007 e chegará a 87 milhões de reais.

Em relação à previsão de vendas, a *Infonetics* destaca que a Cisco tem um grande trimestre de vendas pela frente, crescendo em até 22%.

Diversas empresas que comercializam servidores de comunicação compõem um ambiente extremamente competitivo no mercado de Voz sobre IP. Essas empresas estão divididas da seguinte maneira de acordo com pesquisa de mercado divulgada pela empresa Siemens: [8]

- **Serviços IT:** São empresas integradoras de sistemas de informática ingressando no mercado com soluções Voz sobre IP. IBM, Accenture e EDS são exemplos de empresas serviços IT;
- **Aplicações IT:** São empresas que estão expandindo suas ofertas em aplicações Voz sobre IP. Microsoft e SAP são exemplos de empresas aplicações IT;
- **Operadoras Fixas:** São empresas que oferecem serviços de *Data Center*¹⁵ (Voz e Dados) para clientes, muitas vezes essas empresas fornecem desde a infra-estrutura até a equipe que fará o operacional. Telemar e Telefônica são exemplos de empresas operadoras fixas.
- **Redes de Dados:** São empresas que oferecem soluções para redes corporativas. Essas empresas entram de forma agressiva no mercado Voz sobre IP. A Cisco é um exemplo de empresa redes de dados e;
- **Central Telefônica Convencional:** São empresas tradicionais fornecedoras de centrais telefônicas tradicionais migrando sua base instalada para Voz sobre IP.

¹⁵ *Data Center* é uma modalidade de serviço de valor agregado que oferece recursos de processamento e armazenamento de dados em larga escala para que organizações de qualquer porte e mesmo profissionais liberais possam ter ao seu alcance uma estrutura de grande capacidade e flexibilidade, alta segurança, e igualmente capacitada do ponto de vista de *hardware* e *software* para processar e armazenar informações.

A figura 1 ilustra as informações apresentadas.



Figura 1 – Mercado de Voz sobre IP. ¹⁶

A figura 2 ilustra a evolução dos sistemas Voz sobre IP, onde através de uma linha do tempo (de 2004 até 2011) mostramos a evolução dos sistemas tradicionais para sistemas Voz sobre IP.

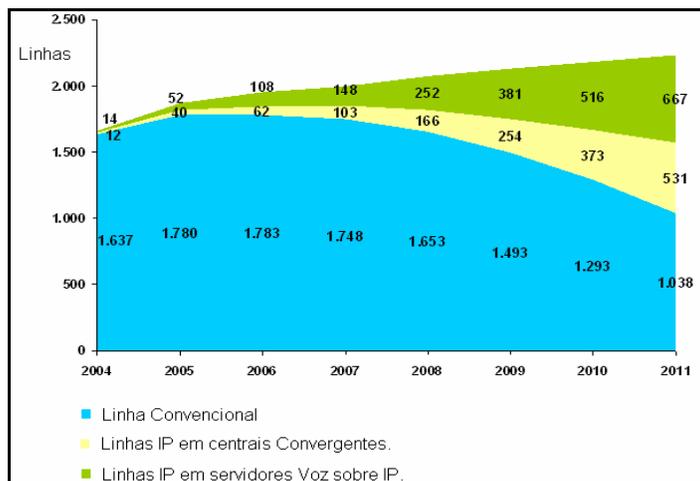


Figura 2 – Evolução do mercado Voz sobre IP. ¹⁷

¹⁶ Fonte: Siemens Enterprise Network, Strategic and Marketing Share Planning VOIP 2006 - 2011. Whitepaper Siemens Communications Mercosur. Divulgado em Dez 2006.

¹⁷ Fonte: Siemens Enterprise Network, Strategic and Marketing Share Planning VOIP 2006 - 2011. Whitepaper Siemens Communications Mercosur. Divulgado em Dez 2006.

Analisando a figura 2 podemos concluir que de acordo com a tendência de mercado, o comprador opta por sistemas de comunicação que utilizam soluções IP em centrais tradicionais e soluções totalmente Voz sobre IP, que são servidores exclusivos para o tráfego de Voz sobre IP. O mercado da telefonia tradicional diminuirá significativamente a quantidade de implementação em numero de linhas.

A figura 3 ilustra a evolução das empresas fornecedoras de servidores de comunicação no mercado Voz sobre IP.

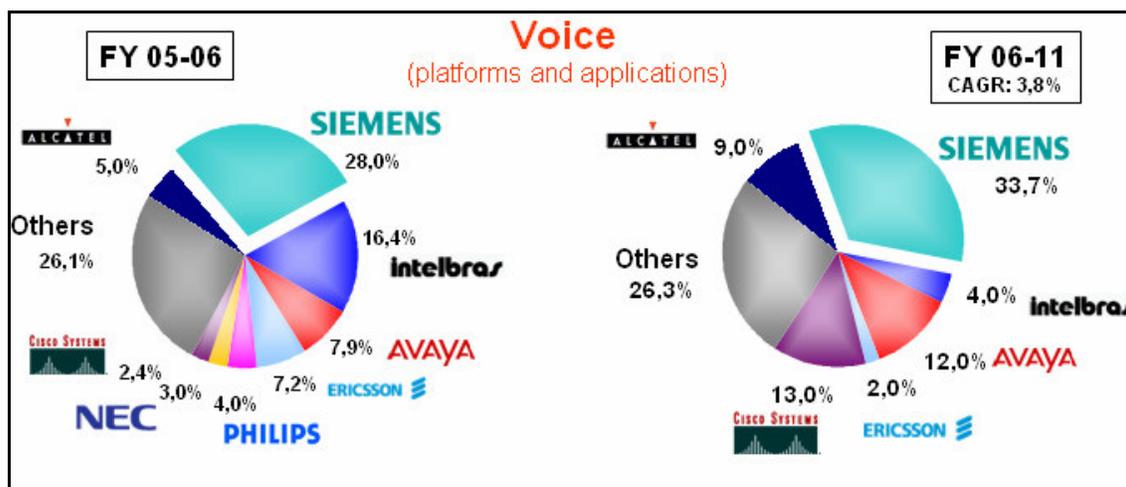


Figura 3 – Evolução de vendas.¹⁸

Podemos observar que ao lado esquerdo da figura 3 temos a análise da evolução de vendas no período de 2005 até abril 2006 e ao lado direito temos uma projeção de vendas do início de maio de 2006 até 2011. A grande evolução ocorrerá com a empresa Cisco que no mercado de servidores de comunicação, não comercializa servidores de comunicação tradicional, apenas comercializa servidores que disponibilizam plataformas IP, servidores convergentes.

¹⁸ Fonte: *Siemens Enterprise Network, Strategic and Marketing Share Planning VOIP 2006 - 2011*. Whitepaper Siemens Communications Mercosur. Divulgado em Dez 2006.

Essas informações foram coletadas de uma pesquisa de mercado elaborada pela empresa Siemens. [8]

A seguir veremos os componentes e algumas terminologias e que compõem os sistemas Voz sobre IP.

2.3 Terminologia do ambiente Voz sobre IP

Os seguintes elementos compõem a solução de sistemas Voz sobre IP:

- **Terminais:** São equipamentos que se comunicam através do padrão H.323, pode ser um *desktop* executando uma aplicação multimídia, um telefone IP, entre outros;
- **Gateways:** Conecta duas redes dissimilares, efetuando uma conversão de protocolos;
- **Gatekeeper:** É o principal elemento na arquitetura H.323, onde regula que dispositivos podem iniciar ou receber chamadas. Possui as seguintes funções: Endereçamento, autorização e autenticação de terminais e *gateways*, gerenciamento de banda, tarifação, cobrança e roteamento de chamadas;
- **MCU Multipoint Control Unit:** Permite a conferência entre três ou mais terminais.

A figura 4 apresenta uma arquitetura típica de uma rede de telefonia IP.

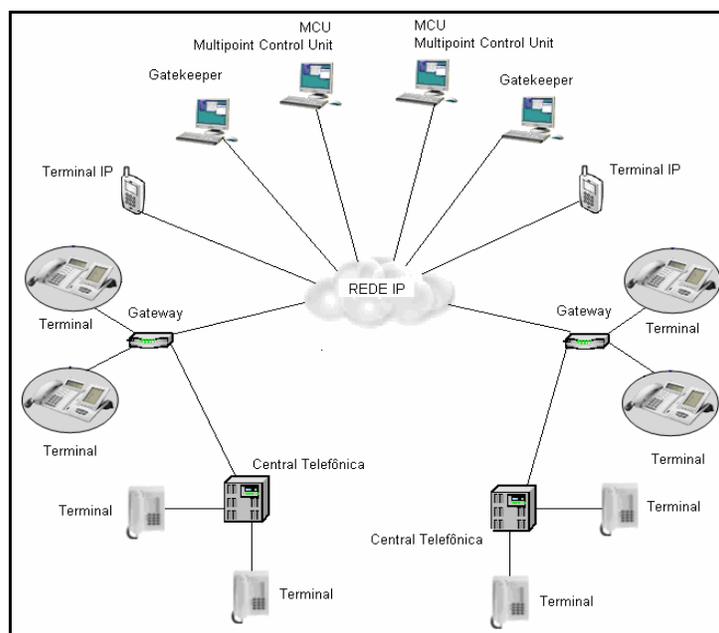


Figura 4 – Arquitetura telefonia IP. ¹⁹

A seguir detalharemos cada um destes elementos.

2.3.1 Terminais H.323

O terminal H.323 equivale a um aparelho telefônico com funções adicionais, que embute obrigatoriamente recursos para a transmissão de áudio e, opcionalmente, pode incluir recursos para a transmissão de vídeo e o compartilhamento de dados. Os terminais são configurados com uma interface de rede e são operados diretamente pelo usuário. [9]

¹⁹ Fonte: VoIP UFSC, Uso de Voz sobre IP na Universidade. Disponível em: <http://voip.npd.ufsc.br/docs/artigo_voip.pdf>.

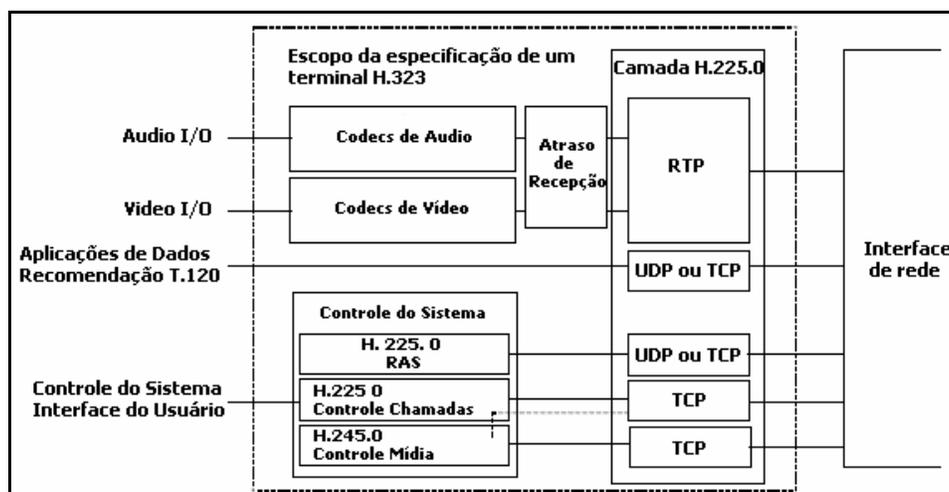


Figura 5 – Elementos fundamentais do terminal H.323. ²⁰

A figura 5 apresenta os elementos funcionais de um terminal H.323. A camada H.225.0, ilustrada no item controle do sistema, formata os fluxos de vídeo, áudio, dados e de controle em mensagens recebidas da rede. Esta camada é responsável pelo enquadramento, pelo seqüenciamento de mensagens e pela detecção de erros na transmissão e recepção de fluxos de mídia e de controle. Em redes Voz sobre IP, estas funções são realizadas pelos protocolos IP (*Internet Protocol*) /UDP (*User Data Protocol*) /RTP (*Real Time Protocol*) para a transmissão do áudio e pelos protocolos IP (*Internet Protocol*) /TCP (*Transmission Control Protocol*) na transmissão dos fluxos de controle.

Todos os terminais H.323 precisam implementar o protocolo H.225, que define um conjunto de mensagens para a sinalização das chamadas e para a comunicação com o *gatekeeper*. A sinalização é utilizada para o estabelecimento, término e controle de chamadas. Outro componente necessário é o protocolo H.245, utilizado na sinalização dos canais de mídia, onde são negociadas as capacidades suportadas pelos dois dispositivos H.323

²⁰ Fonte: Rhyshaden - *The H.323 terminal is designed mainly for audio communication and it can interact with other multimedia terminals.* Disponível em: <<http://www.rhyshaden.com/voice.htm>>.

e iniciados os canais lógicos por onde serão transmitidos os fluxos de mídia (figura 6).

O terminal H.323 deve dar suporte ainda aos protocolos RTP e RTCP utilizados para a transmissão da mídia e para o monitoramento da qualidade da chamada, respectivamente.

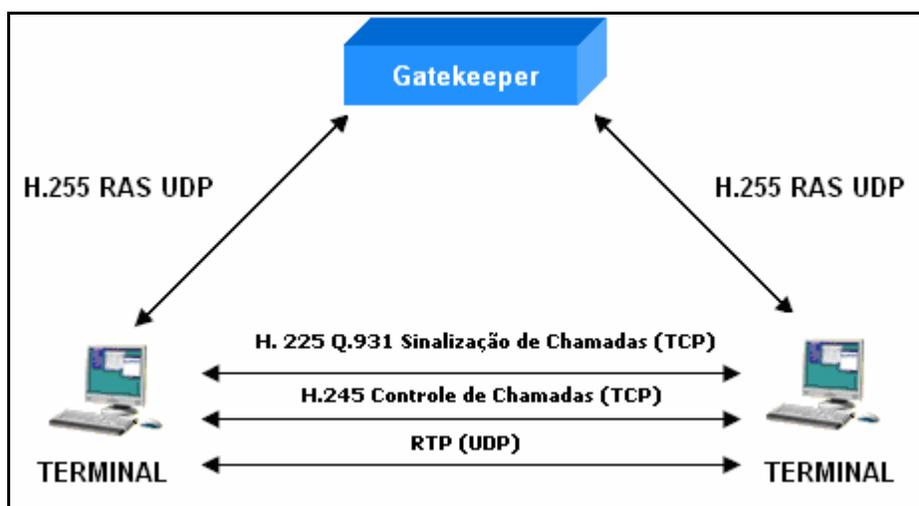


Figura 6 – Fluxos de mídia H.323 com uso de *gatekeeper*.²¹

Os fluxos RTP podem ser bidirecionais ou unidirecionais, depende como for negociado na sinalização. De qualquer forma, sempre existem dois canais de mídia, um para cada sentido da conversação. Em cada sentido há uma conexão RTCP associada, através da qual a estação receptora do fluxo de mídia reporta diversas informações associadas à QOS (qualidade de serviço) do fluxo RTP recebido. Analisando essas informações é possível avaliar a perda de pacotes, o atraso e a variação do atraso associado a cada um dos fluxos. Como as condições da rede podem ser diferentes nos dois sentidos, pode haver problemas em um sentido e no sentido contrario não existir

²¹ Fonte: Rhyshaden - *The H.323 terminal is designed mainly for audio communication and it can interact with other multimedia terminals.* Disponível em: <<http://www.rhyshaden.com/voice.htm>>.

qualquer alteração. A avaliação da qualidade das chamadas pode ser realizada analisando estas informações.

2.3.2 Gateways

A função principal do *gateway* é prover a interconexão entre redes que não utilizam o protocolo H.323, tais como redes RDSI²² (rede digital de serviços integrados) que utilizam o protocolo H.320 para a realização de conferências multimídia e a rede de telefonia convencional. [4]

O *gateway* realiza funções como a tradução da sinalização utilizada para o estabelecimento e término de chamadas e a conversão do formato da mídia de uma rede para a outra.

Este equipamento é tratado na rede H.323 como mais um dispositivo H.323, implementando os protocolos para a sinalização de chamadas (H.225), sinalização de canais de mídia (H.245) e transmissão da mídia em chamadas realizadas com outros *gateways*, terminais ou MCUs.

Em redes VOIP, os *gateways* são configurados com porta de voz para conexão a PBXS e comutadores de telefonia. Varias alternativas de conexão são possíveis, variando conforme o tipo de porta disponível no PBX e no *gateway*.

O *gateway* também deve ter informações suficientes do plano de numeração em uso na rede VOIP, para que possa encaminhar as chamadas

²² RDSI Rede Digital de Serviços Integrado é um serviço de dados digital de alta velocidade. O RDSI permite transmitir grandes volumes de dados, sinais de vídeo e áudio sobre uma única linha telefônica a alta velocidade e baixo custo.

com base no número discado pelo usuário que iniciou a chamada. As chamadas recebidas são encaminhadas de acordo com o número recebido através da sinalização da chamada (*setup H.225*), no caso do VOIP; ou do endereço discado, no caso da telefonia. As chamadas podem ser destinadas a telefones tradicionais ou a dispositivos H.323, o *gateway* deve saber como encaminhá-las. A arquitetura H.323 pressupõe a existência de um *gatekeeper*, elemento que auxilia na localização do destino.

2.3.3 Gatekeepers

O *gatekeeper* é o principal elemento na arquitetura H.323, onde regula que dispositivos podem iniciar ou receber chamadas. Uma das principais diferenças do H.323 em relação ao protocolo SIP, é que no SIP não existe um dispositivo definido explicitamente para controle de acesso aos recursos da rede. [4]

O padrão H.323 especifica os componentes, protocolos e procedimentos que provêm serviços de multimídia (áudio, vídeo e dados) sobre redes de dados.

O SIP (*Session Initiation Protocol*), padrão proposto pelo IETF (RFC 2543), é um protocolo baseado em texto que possui elementos comuns a Internet, tais como: o formato HTTP, DNS e estilo de endereçamento de e-mail. Os padrões H.323 e SIP serão descritos detalhadamente adiante neste trabalho.

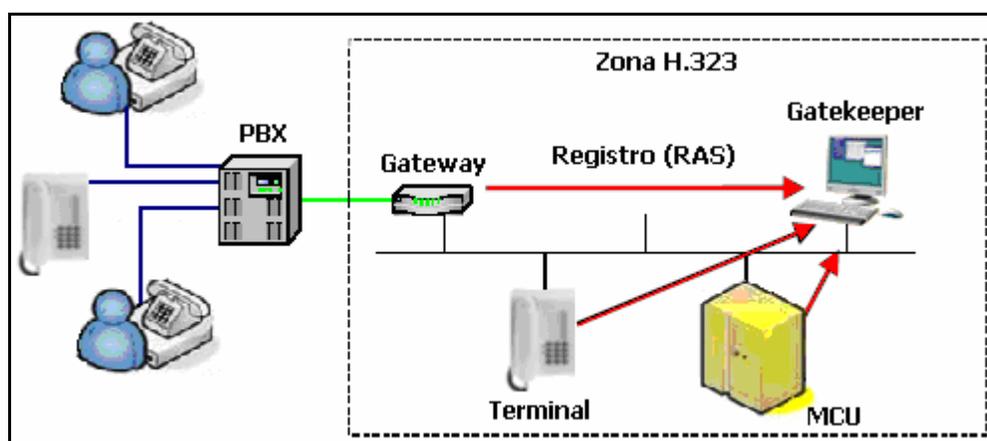


Figura 7 – Zona H.323.²³

A arquitetura H.323 utiliza o conceito de “zona”, que compreende um *gatekeeper* e todos os dispositivos H.323 que controlam conforme ilustrado na Figura 7.

Os dispositivos H.323 utilizam o protocolo RAS²⁴ (*registration, admission and status*) para se registrar no *gatekeeper*, através da mensagem RRQ (*registration request*). Recebem como resposta uma mensagem positiva com um RCG (*registration confirm*) confirmando o recebimento, ou não, com um RRJ (*registration reject*). Segue figura 8 exemplificando uma chamada.

²³ Fonte: Ericsson. H.323. Multimedia sobre redes IP. Disponível em: <<http://www.coit.es/publicac/publbit/bit109/quees.htm>>.

²⁴ RAS *Registration, Admission and Status* é um componente do protocolo de rede que envolve a adição (ou a recusa a adicionar) de usuários autorizados novos, a admissão dos usuários autorizados baseados na largura de faixa disponível, e seguir do *status* de todos os usuários. Formalmente, RAS é parte do protocolo H.225 para redes de comunicações H.323, projetado para suportar larguras de faixa dos multimídia. RAS é um componente de sinalização importante nas redes usando a Voz sobre IP, suportando larguras de faixa de multimídia.

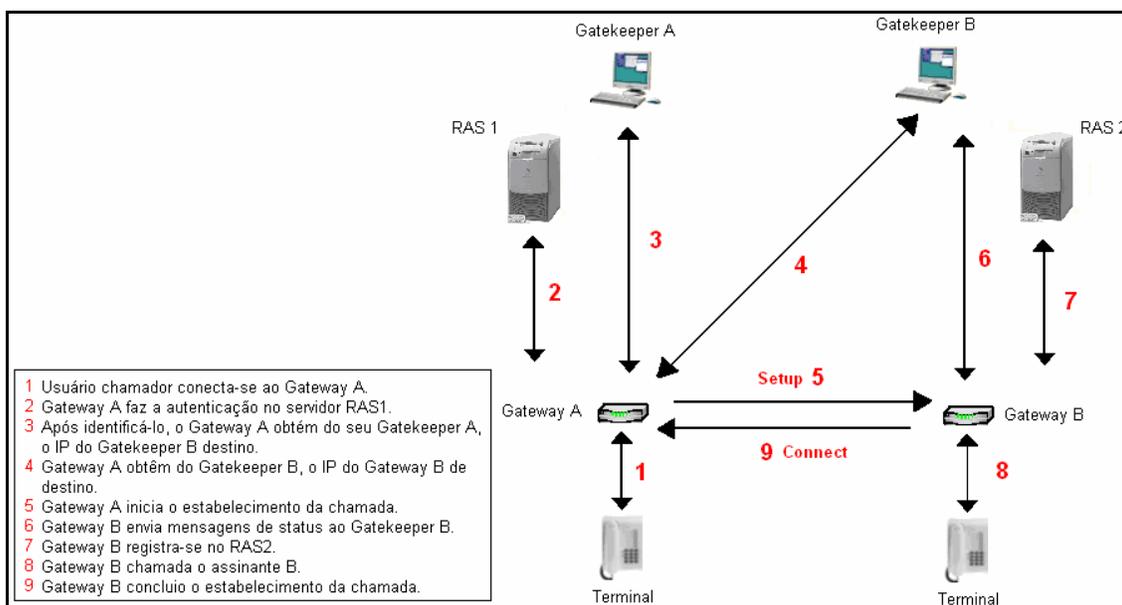


Figura 8 – Estabelecendo uma chamada.²⁵

O *gatekeeper* também deve prover a todos os dispositivos registrados, os serviços de controle de admissão e tradução de endereços. O padrão ITU-T E.164²⁶ define a numeração empregada em redes públicas de telefonia e controle de largura de banda²⁷. [10]

Qualquer chamada realizada a partir de terminais e *gateways* devem ser autorizadas pelo *gatekeeper*. Antes de iniciar qualquer chamada, o dispositivo H.323 utiliza o protocolo RAS para solicitar autorização ao *gatekeeper* para realizar a chamada. São usadas para este fim, as mensagens ARQ (*admission request*), e ACF (*admission confirm*) e ARJ (*admission reject*). Os critérios que

²⁵ Fonte: Monografia Voz sobre IP - Marcel Barbosa de Oliveira. Disponível em: <<http://www.midiacom.uff.br/~debora/fsmm/trab-2003-2/apres-voip.pdf>>.

²⁶ O Padrão ITU-T E.164, define a numeração empregada em redes públicas de telefonia.

²⁷ Largura de banda é a medida da faixa de frequência, em *hertz*, de um sistema ou sinal. A largura de banda é um conceito central em diversos campos de conhecimento, incluindo teoria da informação, rádio comunicação, processamento de sinais, eletrônica e espectroscopia. Em radio comunicação, ela corresponde a faixa de frequência ocupada pelo sinal modulado. Em eletrônica normalmente corresponde a faixa de frequência na qual um sistema tem uma resposta em frequência aproximadamente plana (com variação inferior a 3 dB).

devem ser utilizados pelo *gatekeeper* para autorizar uma chamada não são especificados no H.323, ficando a critério da implementação. Pode ser utilizado, por exemplo, um sistema pré-pago, em que as chamadas só são autorizadas se o usuário ainda tiver crédito disponível. Restrições para determinadas faixas de telefones também podem ser adotadas como, por exemplo, permitir ligações para celulares somente a usuários específicos.

As conexões entre dispositivos H.323 são realizadas com base no endereço de rede e no identificador TSAP²⁸ (*transport service access point*). Em redes IP, o endereço de rede, o endereço IP e o identificador TSAP é um número de porta TCP ou UDP. O uso de apelidos facilita a identificação de dispositivos H.323 para os usuários do serviço. Estes podem ser identificados H.323 (H.323-ID), representados por uma seqüência qualquer de caracteres, ou endereço E.164, numeração adotada na telefonia.

No momento em que solicita o registro no *gatekeeper*, o dispositivo informa os apelidos e o endereço que o identificam. Ao iniciar uma chamada, o terminal envia no pedido de admissão o apelido do terminal que está sendo chamado. Com base nas informações que dispõe, o *gatekeeper* traduz o *alias* (apelido) para um endereço IP e número de porta TCP, que serão utilizados para alcançar o terminal destino. A partir desta informação, pode ser iniciada a sinalização H.225 para estabelecer a chamada. Os *gateways* registram no *gatekeeper*, informações sobre os prefixos associados ao PBX em que estão conectados, de forma que todas as chamadas direcionadas a ramais utilizando o prefixo registrado sejam direcionadas ao *gateway*.

²⁸ A numeração é feita pelo hospedeiro começando em 256 que identifica os *saps* locais da conexão TCP. A porta, mais o endereço IP do hospedeiro, formam o identificador TSAP (*Transport SAP*) único de 48 bits. Os dois números juntos dos *sockets* de *Source* e *Destination Port* formam o identificador de conexão.

O *gatekeeper* deve estar preparado para controlar a banda alocada a uma chamada. Por exemplo, havendo uma mudança do *codec*²⁹ utilizado, pode haver uma mudança que deve ser solicitada ao *gatekeeper* através do protocolo RAS. Havendo limitação na largura de banda alocada ao serviço Voz sobre IP, o pedido pode ser aceito, ou não. Opcionalmente, o *gatekeeper* pode realizar o gerenciamento da largura de banda alocada ao serviço, onde novas chamadas somente serão admitidas se existir banda disponível. Caso não haja, as chamadas serão rejeitadas ou direcionadas para *gatekeepers* alternativos. Desta forma, é possível implementar o serviço VOIP sem causar prejuízos às outras aplicações na rede. O uso de *gatekeepers* alternativos pode ocorrer também no caso de sobrecarga provocada por um número muito grande de chamadas. Esta facilidade garante o uso do serviço H.323 em rede de grande porte.

O *gatekeeper* pode manter uma lista das chamadas ativas, de forma que possam ser identificados os terminais ocupados e para prover informações necessárias ao gerenciamento da largura de banda.

A sinalização de chamadas (H.225), o controle de canais associados à mídia (H.245) e os próprios canais de mídia (RTP/RTCP) são normalmente estabelecidos diretamente entre o dispositivo que realiza a chamada e o que é chamado após receber a confirmação do pedido de admissão do *gatekeeper*. Este modo de operação é chamado de sinal direto de chamada. Alternativamente, o *gatekeeper* pode intermediar a sinalização entre os dispositivos envolvidos quando opera no modo *gatekeeper* sinalizador de

²⁹ *Codec* Codificadores/Decodificadores, são mecanismos de compressão de voz que visam a otimização da utilização da largura de banda para a sua transmissão. Estes mecanismos executados pelos *codec* nada mais são do que circuitos integrados especializados (DSP – *digital signal processor*) e dedicados para o processamento dos sinais de voz com sua conversão analógica para digital.

roteamento de chamada. Neste modo, a sinalização H.225 passa a ser estabelecida entre o dispositivo que inicia a chamada e o *gatekeeper*, que a repassa ao dispositivo chamado, ou ao *gatekeeper* onde dispositivo chamado está registrado. Este procedimento facilita a implementação de mecanismos de segurança na rede, já que apenas o *gatekeeper* precisará ter visibilidade direta da Internet.

O *gatekeeper* é um dispositivo que também tem controle sobre as chamadas realizadas ou recebidas pelos dispositivos na “zona” sob sua responsabilidade, sendo uma importante fonte de informações que podem ser utilizadas para fins de contabilização de chamadas e bilhetagem. Apesar de dois dispositivos poderem estabelecer chamadas entre si sem o uso de *gatekeeper*, esta opção deve ser evitada para não afetar o gerenciamento do serviço, principalmente ao se usar *gateways*.

A política de segurança normalmente adotada nas redes corporativas, gera problemas para o uso do protocolo H.323. As máquinas internas normalmente não são visíveis a partir da Internet, portanto o estabelecimento de uma conexão TCP só ocorre quando iniciada a partir das máquinas internas (máquinas fisicamente conectadas a uma rede local). Outro problema está relacionado aos canais de mídia, que utilizam portas TCP diferentes a cada chamada realizada. A solução para facilitar o uso de H.323 através da Internet e a configuração dos *firewalls*, é o emprego do *gatekeeper* como *proxy* para o tráfego RTP. Com esta configuração, todo o tráfego de mídia da rede interna para a internet, e vice-versa, é realizado através do *gatekeeper*. Na realidade, o *gatekeeper* estabelece duas chamadas, uma com a máquina interna e outra com a externa, intermediando todo o tráfego entre as duas e realizando as

adaptações necessárias na sinalização. Desta forma, o *firewall*³⁰ é configurado para permitir o tráfego associado à mídia das máquinas internas somente com o *gatekeeper* partindo deste ponto para qualquer máquina na internet.

Quando o destino da chamada é um dispositivo em outra “zona” o *gatekeeper* remoto deve ser localizado para que possam ser obtidas informações sobre este dispositivo. Dois métodos podem ser utilizados com este objetivo: para apelidos tipo H323 ID, deve ser utilizado o serviço DNS³¹, e para endereços E.164, mensagens RAS (LRQ – *location request*).

O uso de DNS para a localização do *gatekeeper* remoto requer que o H323 ID associado ao destino esteja no formato *usuário@domínio*. Nas informações associadas ao domínio no serviço DNS, deve haver um registro dos tipos SRV ou TXT no DNS indicando o endereço IP do *gatekeeper* associado ao domínio.

Ao utilizar endereço E.164 como apelidos, devem ser definidos os prefixos que são atendidos por cada “zona”. No caso de *gateways* conectados à rede de telefonia, estes devem indicar no registro os prefixos associados ao telefones atendidos por esta conexão. Desta forma, as chamadas destinadas a estes telefones serão encaminhadas para o *gateway*. Na comunicação entre zonas, os *gatekeepers* devem ter uma configuração estática dos prefixos

³⁰ O *firewall* é um mecanismo utilizado para proteger uma rede interna (confiável) de uma outra rede externa (não confiável). Um *firewall* assegura que não há possibilidades de acesso à rede externa (por exemplo, internet) a partir da rede interna, nem vice-versa, a não ser que se passe por esse ponto. Ele verifica e filtra todas as conexões vindas da rede externa para a rede interna e vice-versa através de um único ponto de acesso seguro.

³¹ DNS *Domain Name System*, sistema de nomes de domínio, este é o protocolo que torna possível que qualquer computador encontre qualquer outro dentro da internet.

atendidos por cada *gatekeeper* conhecido. Desta forma, ao receber um pedido de admissão, o prefixo é extraído do apelido do destino. A partir do prefixo é identificado o endereço do *gatekeeper* remoto, para onde é enviada uma mensagem RAS (LRQ – *location request*), como apresentada na Figura 9.

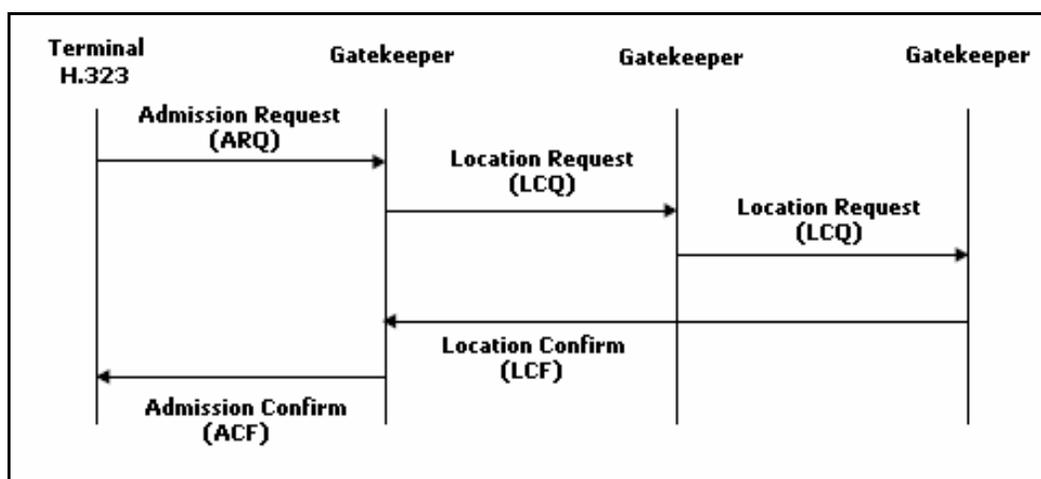


Figura 9 – Sinalização RAS: uso de LRQ's.³²

Ao receber a mensagem LRQ é verificado se o destino está registrado. Em caso afirmativo, e não havendo restrições, será enviada uma confirmação de localização que indicará os parâmetros necessários para estabelecer o canal de sinalização das chamadas.

2.3.4 Multipoint Control Units (MCU)

O *Multipoint Control Units* (MCU) é um equipamento que dá o suporte necessário a conferências envolvendo mais de dois dispositivos em redes

³² Fonte: Monografia Voz sobre IP, Tecnologias e Aplicações. - José Marcos Câmara Brito. Disponível em: <http://cict.inatel.br/nova2/docentes/brito/Voz_sobre_IP.html>.

H.323. O MCU consiste de um *Multipoint Controller* (MC)³³ e de dois ou mais *Multipoint Processors* (MP)³⁴. O *Multipoint Controller* manipula a negociação H.245 com todos os dispositivos que vão participar de uma conferência, identificando as capacidades de áudio e vídeo comuns a todos, determinando assim o modo de comunicação a ser adotado. O Protocolo H.245 é utilizado ainda para verificar se os dispositivos envolvidos suportam comunicação *multicast*. Cada conferência estabelecida é associada somente a um MC. Cada dispositivo H.323 estabelece uma sessão bidirecional com o MC. [4]

O *multipoint Processors* é responsável por converter a mídia para diferentes formatos, por exemplo, de G.711³⁵ para G.723³⁶, ou por combinar o áudio proveniente de várias fontes, transmitindo o fluxo combinado para todos os dispositivos. [11]

As conferências H.323 podem ser descentralizadas ou centralizadas. As descentralizadas dependem do suporte à transmissão *multicast* nos dispositivos envolvidos, já que os fluxos de mídia para os dispositivos associados à conferência serão transmitidos utilizando-se este tipo de endereçamento. Nas conferências centralizadas, todos os fluxos de mídia são

³³ Controlador Multiponto (MC - *multipoint controller*), responsável pela sinalização das chamadas.

³⁴ Processador Multiponto (MP - *multipoint processor*), responsável pelo processamento dos pacotes de dados dos sinais de Voz dos terminais envolvidos na conferência.

³⁵ G.711: Padrão de codificação dos pacotes de voz para o transporte pela rede IP. O áudio G.711 possui qualidade de telefonia (banda estreita, 3 Khz) e consome 48-64 Kbps de largura de banda.

³⁶ G.723: Algoritmo utilizado para compressão de voz e supressão de silêncio de um sinal digital cuja variante mais conhecida é o G-723. 1, que consegue converter um sinal PCM de entrada de 64 kbps em uma saída que pode variar de 5,3 a 6,4 kbps.

transmitidos para o MCU que, por sua vez, os retransmite para todos os dispositivos que participam da conferência.

2.4 Arquiteturas

Podemos definir três arquiteturas de implementação no ambiente Voz sobre IP: arquitetura micro a micro, arquitetura *gateway* e arquitetura híbrida. [11] Dentre as arquiteturas veremos alguns componentes tais como: terminais, *gatekeepers*, *gateways*, *multipoint control units*, já apresentados neste trabalho.

2.4.1 Arquitetura micro a micro

A arquitetura micro a micro é utilizada quando dois usuários desejam se comunicar através de Voz sobre IP, este modelo de implementação é composto por dois computadores com recursos de multimídia, conectados a uma rede local ou, através da rede de telefonia pública, a um provedor de serviços internet, se comunicando para trocar sinais de voz. Todo tratamento do sinal de voz, amostragem, compressão e empacotamento é realizado nos computadores, sendo a chamada de voz estabelecida baseada no endereço IP do receptor. Este modelo de implementação, está ilustrado na figura 10.

A arquitetura micro a micro possui uma variante onde o computador é substituído por um telefone IP que possui a capacidade de codificar voz, conhecido como *hard phone*, que é um aparelho telefônico com funções Voz sobre IP.

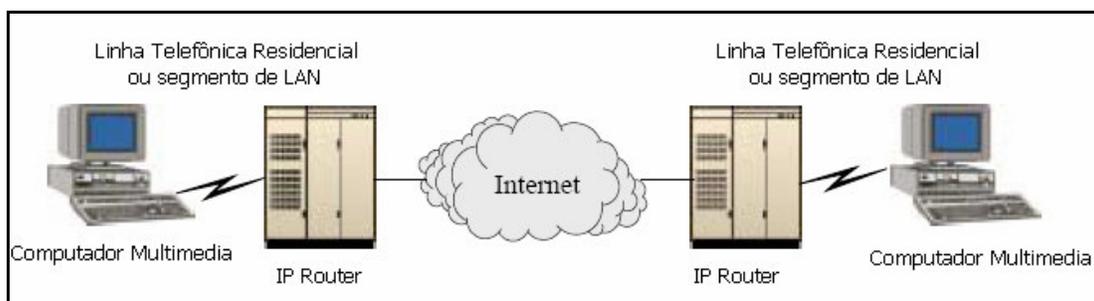


Figura 10 – Arquitetura micro a micro.³⁷

Esta arquitetura é utilizada para comunicação de dois computadores multimídia dentro de uma rede. Neste exemplo temos um computador multimídia que pode estar conectado a uma linha telefônica residencial ou a um segmento de local que utiliza a rede da internet para se comunicar com o outro computador multimídia. Este tipo de arquitetura também é utilizado quando dois computadores conectados na mesma rede utilizam a solução Voz sobre IP.

2.4.2 Arquitetura *gateway*

Este modelo de implementação, ilustrado na figura 11, utiliza um aparelho telefônico padrão para gerar e receber chamadas telefônicas no ambiente internet. O usuário chamador discar para o *gateway* de telefonia IP mais próximo de sua central telefônica local. Este *gateway* valida o número telefônico do usuário chamador (para autenticar e tarifar) solicitando a este o número do usuário de destino.

³⁷ Fonte: Monografia Implementação e Gerência de uma Arquitetura de Voz sobre IP. - José Carlos Peixoto de Almeida. Disponível em: <http://www1.capes.gov.br/estudos/dados/2003/31001017/002/2003_002_31001017110P8_Teses.pdf>.

O *gateway* de entrada identifica o *gateway* de saída mais próximo e inicia uma sessão para transmissão de pacotes. O *gateway* de saída realiza a chamada ao telefone receptor e, após a chamada ser atendida, a comunicação fim-a-fim tem início, com o sinal de voz sendo enviado através de datagramas IP entre os *gateways*. A codificação e empacotamento do sinal de voz são feitos no *gateway* originador da chamada, enquanto a decodificação e o desempacotamento são feitos no *gateway* de destino. A digitalização do sinal de voz pode ser feita na central, no *gateway*, ou mesmo no telefone.

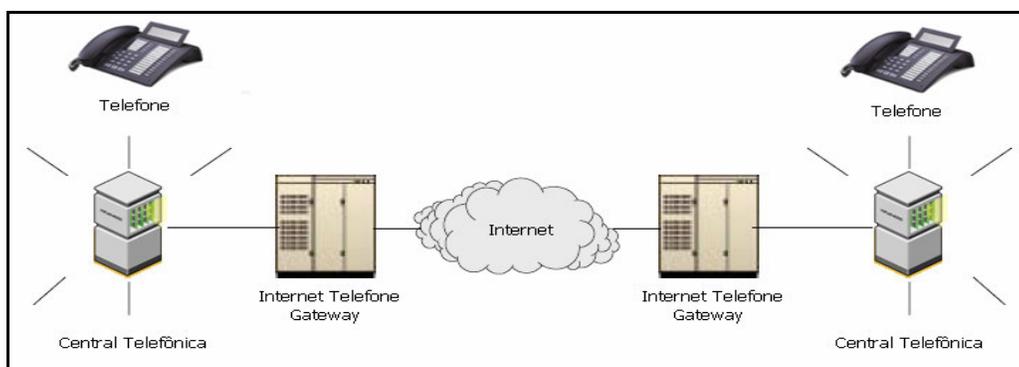


Figura 11 – Arquitetura *gateway a gateway*.³⁸

Esta arquitetura é utilizada para comunicação de dois computadores multimídia dentro de uma rede. Neste exemplo temos um computador multimídia que pode estar conectado a uma linha telefônica residencial ou a um segmento de local que utiliza a rede da internet para se comunicar com o outro computador multimídia. Este tipo de arquitetura também é utilizado quando dois computadores conectados na mesma rede utilizam a solução voz sobre IP.

³⁸ Fonte: Monografia Implementação e Gerência de uma Arquitetura de Voz sobre IP. - José Carlos Peixoto de Almeida. Disponível em: <http://www1.capes.gov.br/estudos/dados/2003/31001017/002/2003_002_31001017110P8_Teses.pdf>.

2.4.3 Arquitetura híbrida

Naturalmente, esquemas híbridos das duas arquiteturas anteriores são possíveis e necessários para conexão entre localidades remotas. Nestas estruturas um usuário de telefone padrão recebe ou origina uma chamada para um usuário de computador ou de telefone IP. Em tais situações, deve haver um serviço de mapeamento ou tradução de endereços IP em números telefônicos. Existem alguns caminhos: Micro a micro, *gateway* a *gateway*, micro a *gateway* e *gateway* a micro. Em todas as arquiteturas os pontos terminais sejam eles micro ou *gateway* devem empregar o mesmo esquema de codificação de voz.

Embora as arquiteturas mostradas até então ilustrem o transporte de voz sobre a internet existem as aplicações locais onde utilizamos centrais telefônicas totalmente IP. Em termos de segurança, devemos complementar a segurança as melhores práticas nas configurações dos elementos de rede. Podemos mencionar como exemplo a arquitetura *gateway* a *gateway* onde devemos utilizar uma VPN (*Virtual Private Network*) para garantir a segurança no tráfego das informações. Neste mesmo exemplo, ainda podem-se usar roteadores para completar a solução, adicionando uma camada extra na segurança da comunicação entre os sites.

2.5 Sinalização

Quando um usuário disca um número de telefone, ou faz uso de um nome associado a um destino (*alias*), é necessária uma sinalização que determine inicialmente o estado do dispositivo remoto a ser chamado (*called*

party), indicando se o mesmo está ocupado ou disponível. Caso esteja disponível, a sinalização será responsável por estabelecer a chamada. Quando um dos usuários desliga, a sinalização será utilizada para terminar a chamada e liberar os recursos associados.

Três padrões são utilizados na sinalização em redes VOIP: a recomendação H.323 do ITU-T (*Internacional Telecommunication Union – Telecom Standardization*), o protocolo SIP (*Session Initiation Protocol*) do IETF (*Internet Engineering Task Force*) e a recomendação H.248 do ITU-T.

A recomendação H.323 compreende um conjunto de protocolos utilizados para a realização de conferências multimídia utilizando vídeo, voz e dados em rede de pacotes, onde não há garantia em relação à qualidade de serviço. A primeira especificação do H.323 foi aprovada em 1996, mas os primeiros artigos da série H.323 foram aprovados no início dos anos 90. A segunda versão, aprovada em janeiro de 1998, além das correções de problemas relativos à primeira especificação, trouxe novas funcionalidades que permitem o uso do H.323 em rede WAN. Podemos ainda destacar o suporte à segurança, à QOS (*quality of service*) e à disponibilidade. Novas versões de H.323 foram aprovadas desde então, agregando novas funcionalidades.

Os equipamentos utilizados em redes H323 incluem terminais, *gateways*, *multipoint control units* (MCU) e *gatekeepers*. Os três primeiros podem iniciar e receber chamadas H.323.

A recomendação H.323 define um conjunto de protocolos que são utilizados para fins de sinalização de chamadas e controle dos canais de

mídia. O tráfego associado à mídia é transportado utilizando o protocolo *real time protocol* (RTP)³⁹.

O protocolo SIP foi desenvolvido inicialmente dentro do grupo de trabalho MMUSIC (*Multiparty Multimedia Session Control*) do IETF. Posteriormente, um grupo de trabalho específico em SIP acabou sendo formado. SIP é um protocolo de aplicação baseado em texto, que utiliza o modelo “requisição-resposta”, similar ao *http*⁴⁰, para iniciar seções de comunicação interativa entre usuários. Na figura 12, pode ser visto um exemplo da sinalização estabelecida entre dois terminais SIP. Tais sessões incluem voz, vídeos, mensagens instantâneas, jogos interativos e realidade virtual. A descrição das características da sessão, tais como os *codec's*⁴¹ utilizados e endereços associados aos fluxos de mídia, é realizado pelo protocolo SDP (*session description protocol*). [12]

O protocolo SIP é especificado na RFC 2543, que passou ao estado de padrão proposto (*proposed standard*) em março de 1999.

O protocolo SIP segue uma arquitetura cliente/servidor. Os dois terminais envolvidos são chamados de *user agents*⁴², responsáveis em originar ou terminar requisições SIP, atuando como clientes ou servidores SIP,

³⁹ RTP *Real Time Protocol* é um protocolo de redes utilizado em aplicações de tempo real como, por exemplo, entrega de dados áudio ponto-a-ponto, como Voz sobre IP.

⁴⁰ HTTP *Hypertext Transport Protocol* é o protocolo que define como é que dois programas/servidores devem interagir, de maneira a transferirem entre si comandos ou informações relativos ao www.

⁴¹ *Codec* (Codificadores/Decodificadores), são mecanismos de compressão de voz que visam a otimização da utilização da largura de banda para a sua transmissão. Estes mecanismos executados pelos codec (Codificadores/Decodificadores), que nada mais são do que circuitos integrados especializados (DSP – *digitals signal processor*) e dedicados para o processamento dos sinais de voz com sua conversão analógica para digital.

⁴² *User Agent* é o *software* que está na parte final do sistema, funcionando como *software* cliente num PC, num dispositivo móvel, ou como *firmware* num Telefone IP.

respectivamente. Opcionalmente, além dos agentes podem ser utilizados servidores procuradores, atuando como intermediários no encaminhamento de mensagens SIP e dos fluxos de mídias entre dois agentes. Esse tem funções adicionais associadas à autenticação e autorização de uso do serviço que são essenciais quando é necessária a contabilização das chamadas. Outros componentes podem ser utilizados para facilitar o encaminhamento de chamadas e a localização de usuários. [13]

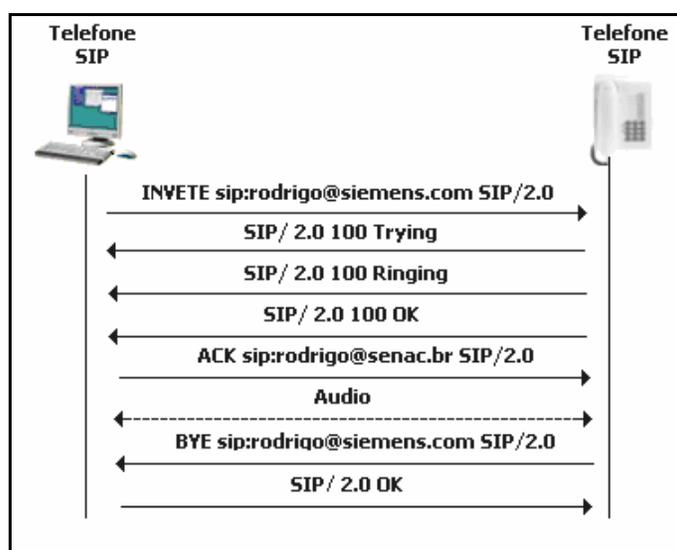


Figura 12 – Sinalização entre dois terminais SIP. ⁴³

Protocolo MGCP (*Media Gateway Control Protocol*) foi proposto pelo grupo de trabalho *Megaco (Media Gateway Control)* do IETF, objetivando uma integração da arquitetura, adotada em redes de sinalização na telefonia tradicional, com redes IP, *Frame Relay* e ATM. Em uma evolução do MGCP, o trabalho cooperativo de grupo do ITU-T e do IETF resultou na recomendação H.248, definida também como protocolo Megaco (IETF), através da RFC3015. [14]

⁴³ Fonte: Série SIP Sinalização Voz sobre IP - Wireless BR. Disponível em: <http://www.wirelessbrasil.org/.../serie_voip_055.html>.

Media Gateways (MG) convertem a mídia entre os vários tipos de rede a que podem estar conectados. Enquanto no H.323 o *gateway* passa a ser realizada pelo MGC (*Media Gateway Controller*). Este equipamento pode controlar vários MG's. O principal objetivo do MGCP era a decomposição da arquitetura H323 para que de forma semelhante às redes, haja uma rede de pacotes empregada exclusivamente para o transporte da sinalização a qual será utilizada para controlar os comutadores por onde trafega a voz. O H. 248 é um protocolo “*master/slave*”, onde o MGC tem um controle total sobre os elementos da rede e o MG apenas executa os comandos recebidos, como apresentado na figura 13. Ele contrasta com o H.323 e com o SIP, protocolos “*peer-to-peer*”, ponto a ponto, onde os clientes podem estabelecer sessões diretamente com outros clientes.

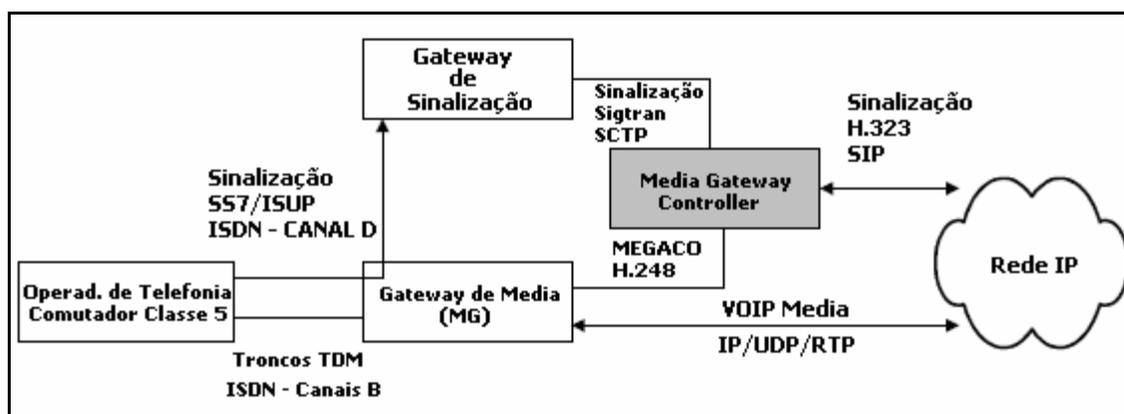


Figura 13 – Arquitetura H.248/Megaco. ⁴⁴

O protocolo H.245 é considerado complementar ao H.323 e ao SIP. Nele um MGC irá controlar um MG usando H.248, mas irá se comunicar com outros utilizando H.323 ou SIP. A comunicação entre MGC's não é definida no H.248/Megaco. Na figura 13 pode ser vista a arquitetura do Megaco. Além dos MG's e dos MGC's, é utilizado um *gateway* que tem a responsabilidade

⁴⁴ Fonte: Série SIP Sinalização Voz sobre IP - Wireless BR. Disponível em: <http://www.wirelessbrasil.org/.../serie_voip_055.html>.

de terminar a sinalização proveniente da rede de telefonia e transportá-la para o MGC.

Estes três protocolos têm similaridades, uma vez que têm o objetivo comum de prover uma comunicação VOIP. Eles diferem somente na localização da “inteligência”, ou seja, onde é realizado o processamento: no H.323, a inteligência é distribuída por todos os elementos que compõem a rede (terminais, *gateways*, *gatekeepers* e *MCU's*) no SIP, a inteligência fica restrita aos dispositivos terminais das chamadas; e no H.248, a inteligência fica na rede (MGC's), não sendo feito qualquer processamento nos *gateways* (MG's).

O protocolo H.248/Megaco é indicado para redes com grandes quantidades de *gateways*, operando com grandes quantidades de portas, e onde haja a necessidade de integração com redes locais. Em redes de menor porte e onde haja a necessidade de comunicação *peer-to-peer*, os protocolos H.323 e SIP são os indicados. O Protocolo SIP, por ter sido definido pela comunidade IP, apresenta características que o adaptam facilmente para novas aplicações na internet. O H.323, por ter sido desenvolvido pela comunidade de telecomunicações, tem uma melhor interação com a telefonia convencional. O H.323 foi definido com o objetivo de prover um sistema unificado que permitisse em relação aos componentes e à sinalização. O H.323 apresenta também procedimentos definidos para um melhor gerenciamento do serviço e recuperação em caso de falhas. O SIP especifica um protocolo de sinalização aberto. Conseqüentemente, as implementações podem variar, não sendo totalmente compatíveis.

Na prática, um grande número de rede Voz sobre IP utilizam o protocolo H.323 devido à grande disponibilidade de produtos H.323 no mercado, ao maior número e estabilidade de implementações, ao foco na integração com

a rede de telefonia e às facilidades associadas ao gerenciamento do serviço e das chamadas. Entretanto, vem sendo ampliado o número de produtos e aplicações que utilizam o SIP. A seguir veremos as recomendações do protocolo H.323.

2.6 Recomendação H.323

A recomendação H.323 define uma arquitetura para estabelecer uma comunicação multimídia em redes de pacotes que não tenham suporte à qualidade de serviço (QOS). O H.323⁴⁵ é um documento base que faz referência a um conjunto de protocolos e formatos de mensagens definidos em outros documentos, e explica como os vários protocolos interagem com os vários elementos que compõem a arquitetura. Na tabela 1 são apresentadas recomendações do ITU-T definidas para dar suporte à sinalização H.323. [11]

Recomendação	Título
H.225.0	<i>Call Signaling Protocols and Media Stream Packetization for Packet Based Multimedia Communication Systems</i>
H. 235	<i>Security and Encryption for H-Series Multimedia Terminals</i>
H. 245	<i>Control Protocol for Multimedia Communication</i>
H. 350.x	<i>Directory Services Architecture for Multimedia Conferencing</i>
Série T.120	<i>Data Protocols for Multimedia Conferencing</i>

Tabela 1 – Recomendações H.323.

Na tabela 1 estão descritos as recomendações que dão suporte a sinalização H.323 onde a coluna recomendação contém o número da recomendação e no título a base para pesquisa. O item T.120 governa a

⁴⁵ ITU-T Rec. H.323. Visual Telephone Systems and Equipment for Are Networks which Provide a Non-Guaranteed Quality of Service.

porção áudio gráfica das séries H.320, H.323 e H.324 e opera também com elas ou sozinha. O conjunto de recomendações T.120 consiste em uma série, as quais estão resumidas na tabela 1. Estas recomendações, bem como outras referências relacionadas à T.120, são objetos de constantes revisões. O usuário deve procurar consultar a lista de Recomendações ITU-T atualizada, publicada regularmente, para obter normas válidas para o momento atual. [20]

Além das funções de sinalização, a arquitetura H.323 incorpora vários formatos associados à mídia transmitida em fluxos específicos, como apresentado na tabela 2. Em redes Voz sobre IP, os fluxos associados à transmissão do áudio são encaminhados utilizando-se o protocolo RTP.

Mídia	Formatos
Áudio	G.711, G.722, G.723, G.728, G.729, GSM, ISSO/IEC 11172-3
Vídeo	H.261, H.262, H.263
Dados	Série de recomendações T.120

Tabela 2 – Formatos de mídia reconhecidos na arquitetura H.323.

O primeiro segmento do mercado a adotar o padrão T.120 foi a comunidade de teleconferências, em virtude do amplo alcance dessa tecnologia, que permite seu uso, efetivamente, por um grande número de vendedores de *softwares* aplicativos e provedores de equipamentos. [11]

O paradigma da computação está se estendendo rapidamente do passado para os modelos de produtividades atuais. Vendedores de *software* independentes já adotaram o T.120 como um meio de incorporar capacidades de colaboração em tempo-real em aplicativos comuns, como por exemplo, em processadores de texto e apresentações gráficas.

A arquitetura H.323 especifica quatro componentes básicos: terminais, *gatekeepers*, *gateways* e *multipoint control units*, já apresentados anteriormente neste trabalho.

A seguir apresentaremos aspectos gerais da segurança da informação no ambiente Voz sobre IP.

3. SEGURANÇA DA INFORMAÇÃO

Este capítulo tem como objetivo apresentar aspectos gerais da segurança da informação. Analisando nosso presente momento histórico, nos encontramos com um complexo e, de certo modo, eficiente mundo de soluções Voz sobre IP. Em virtude de sua complexidade, estas tecnologias mostram-se, também inseguras em virtude da incapacidade da evolução da segurança face à evolução de dispositivos e equipamentos tecnológicos, pois assim como algumas destas novas tecnologias que são inseridas em redes de comunicação não apresentam implementações contra vulnerabilidade que apenas são descobertas após o uso da solução por diversas empresas, portanto as preocupações com segurança da informação tornam-se cada vez mais primordiais, levando empresas, executivos e inclusive pessoas físicas a obterem conhecimentos no mínimo de conceitos básicos de segurança da informação. [15]

3.1 Conceitos de Segurança da Informação

Dentro da área de segurança da informação lidamos com um conteúdo altamente técnico e conceitual, havendo assim a necessidade do conhecimento de diversas áreas e assuntos para uma compreensão e sucesso profissional aceitável. [16] A seguir detalharemos os seguintes conceitos:

3.1.1 Ativo

Qualquer coisa que manipule direta ou indiretamente uma informação. Em termos de segurança em ambiente Voz sobre IP, um ativo pode ser um terminal, um *gateway*, um próprio usuário, onde a informação tem um grande valor e se torna diferencial competitivo. [16]

3.1.2 Vulnerabilidade

Ponto pelo qual alguém pode ser atacado, molestado ou ter suas informações corrompidas. Podemos citar como exemplo, uma análise de ambiente em uma sala de servidores de Voz sobre IP com a seguinte descrição: A sala de servidores não possui controle de acesso físico, senhas de acesso padrão, entre outros. [16]

3.1.3 Ameaça

Algo que possa provocar danos ao ambiente Voz sobre IP, prejudicar as ações de comunicação da empresa e sua sustentação no negócio, mediante a exploração de uma determinada vulnerabilidade. Seguindo o exemplo da sala dos servidores, poderíamos identificar a ameaça da seguinte forma em ambiente Voz sobre IP: Fraudes, utilização não devida dos terminais, paralisação dos serviços, entre outras ameaças. [16]

3.1.4 Risco

É medido pela probabilidade de uma ameaça acontecer e o dano potencial à empresa. Existem algumas maneiras de se classificar o grau de risco no mercado de segurança, mas de uma forma simples, poderíamos tratar como alto, médio e baixo risco. Os principais riscos no ambiente Voz sobre IP, são nas conexões com a rede externa da empresa, como por exemplo, um elemento que faça a interligação entre duas localidades (roteador) esta ameaça pode ser classificada como de alto risco. [16]

3.1.5 Disponibilidade

É a propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação. Este conceito tem despertado maior interesse depois do avanço das instalações de sistemas Voz sobre IP, a telefonia passou a depender mais da informática para estar disponível ao usuário final. Afinal, de nada adiantará uma completa infra-estrutura tecnológica, com recursos que garantam a integridade e confidencialidade dos sistemas Voz sobre IP, se quando o usuário for utilizá-la, a mesma não estiver disponível. [17]

A disponibilidade das comunicações em tempo real depende diretamente da disponibilidade da rede. Portanto, requisitos de alta disponibilidade são fatores indispensáveis nos sistemas Voz sobre IP.

3.1.6 Autenticidade

Defini-se pela veracidade do emissor e receptor de informações trocadas. No ambiente Voz sobre IP existem algumas tecnologias que permitem identificar os emissores e receptores de forma confiável. [18] No capítulo Protocolos de Segurança iremos detalhar este item.

O tema segurança da informação encontra-se altamente relacionada com os sistemas Voz sobre IP, pois além da segurança da rede de dados convencional é necessário prever as ameaças e vulnerabilidades apresentadas nos sistemas Voz sobre IP, que serão detalhadas no próximo capítulo.

Além a gestão e planejamento da informação, além de dispositivos sociais e tecnológicos, chegando inclusive ao âmbito da legislação.

Assim como qualquer nova aplicação na rede, Voz sobre IP representa um potencial vetor para ataques. Novas ameaças, além das já conhecidas, são introduzidas devido às vulnerabilidades inerentes aos protocolos específicos de telefonia IP, por exemplo, H.323 e SIP.

A seguir detalharemos as ameaças de segurança em ambiente Voz sobre IP.

4. AMEAÇAS DE SEGURANÇA NO AMBIENTE VOZ SOBRE IP

Cada vez é maior a preocupação dos usuários e prestadores de serviço de Voz sobre IP com relação às ameaças e aos riscos vinculados a este tipo de serviço. A grande preocupação advém do fato da Voz sobre IP integrar os serviços de comunicação de voz, antes restritos a uma rede planejada e dedicada para este fim, pois a infra-estrutura de dados é razoavelmente exposta a uma série de ameaças, independente das ameaças específicas do ambiente Voz sobre IP.

Essa integração acaba trazendo para a telefonia os riscos de segurança hoje existentes apenas nas redes de computadores. A preocupação com os riscos é agravada pela expectativa, não negociável, de manter os mesmos níveis de serviço hoje ofertados pelo serviço telefônico, tais como ligações simultâneas, conferências, interligações entre filiais entre outros.

Define-se segurança como o estado de estar livre de perigo ou ameaça, tanto do ponto de vista do usuário (seja residencial ou corporativo) como do ponto de vista do prestador do serviço.

A seguir veremos algumas considerações de segurança dos serviços Voz sobre IP que são realizadas com base na arquitetura do protocolo SIP, já que este tem sido o padrão de fato para serviços de Voz sobre IP orientados ao usuário final. Mesmo assim, muitas das considerações sendo realizadas são válidas também para o protocolo H.323.

A arquitetura SIP é composta por agentes de usuário (*user agents*) capazes de iniciar ou terminar sessões. Os *user agents* podem ser terminais IP, telefones IP, *softphones*⁴⁶, *gateways*, servidores de mídia entre outros. Estes *user agents* são gerenciados por *proxies*⁴⁷, *registrars*⁴⁸ e *redirect servers*⁴⁹, veja figura 14, que se encarregam de transmitir ou orientar os *user agents* quanto à transmissão de suas mensagens e de manter seu estado e regras de localização.

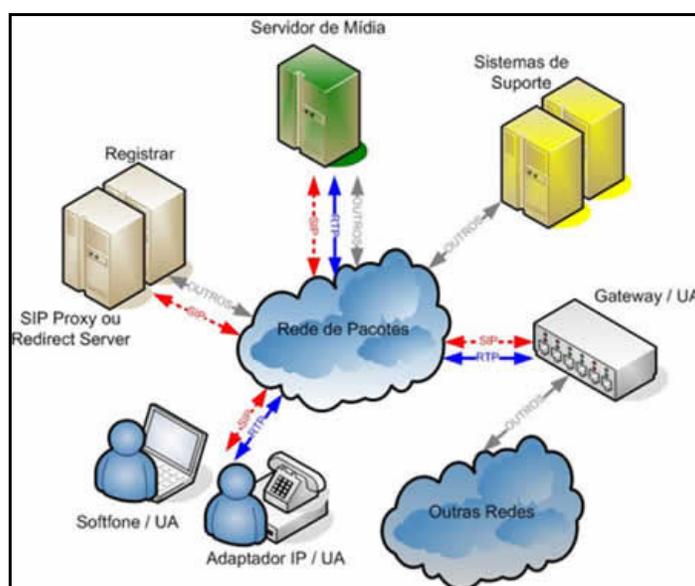


Figura 14 – Arquitetura básica de uma rede SIP.⁵⁰

⁴⁶ *Softphones*: São terminais no formato de *software* para instalação no PC do usuário. Este *software* trará todas as facilidades de telefonia para o controle e comunicação pelo PC.

⁴⁷ *Proxies*: O servidor *proxy* é o único ponto de contato que os *User Agents* (UA) têm para a troca de mensagens de sinalização.

⁴⁸ *Registrars* é usado para executar registro, controle de admissão, mudanças de largura de banda e status.

⁴⁹ *Redirect Servers*: O servidor deixa o *user agent* (UA) chamador (A) saber a localização do *user agent* chamado (B) e então as mensagens de sinalização subsequentes são trocadas diretamente entre os *users agents*.

⁵⁰ Fonte: Conceitos de Sistemas Voz sobre IP - Enciclopédia livre Wikipédia. Disponível em: <http://pt.wikipedia.org/wiki/Seguran%3%A7a_da_informa%C3%A7%C3%A3o>.

Compõe ainda esta infra-estrutura os serviços de suporte como DNS, sistemas de bilhetagem⁵¹, sistemas de monitoramento⁵², entre outros, indispensáveis para a operação e gerência de serviços Voz sobre IP.

O protocolo SIP estabelece um conjunto de mensagens que permite estabelecer, modificar e terminar vários tipos de sessões, inclusive sessões de voz. Depois que uma determinada sessão é estabelecida entre um originador e um terminador a voz é digitalizada utilizando um codificador/decodificador (*codec*) negociado durante o estabelecimento dessa sessão.

A partir deste ponto a voz digitalizada trafega através do protocolo RTP (*Real Time Protocol*) que conta com o RTCP (*Real Time Control Protocol*) para auxiliá-lo no controle dos dados trafegados. [19]

4.1 Principais ameaças

Assim como qualquer nova aplicação na rede, Voz sobre IP representa um potencial vetor para ataques. Novas ameaças, além das já conhecidas, são introduzidas devido às vulnerabilidades inerentes aos protocolos específicos de telefonia IP, por exemplo, H.323 e SIP. Devemos considerar que:

⁵¹ Sistemas de Bilhetagem responsáveis pela tarifação das chamadas telefônicas. Aloca o custo de acordo com as tarifas pré-fixadas.

⁵² Sistemas de monitoramento responsáveis pela escuta, gravação e monitoração das chamadas telefônicas. Existem gravadores próprios para gravar Voz sobre IP. Maiores informações consulte o site: <<http://www.wittel.com>>.

- Uma vez que muitas vulnerabilidades e ameaças já são conhecidas, as recomendações de segurança também devem ser aplicadas para comunicações em tempo real e;

- Quando a mesma rede suporta o tráfego de voz e dados, torna-se mais simples o acesso e a interceptação de pacotes. Isso não ocorre numa rede TDM, onde é necessário o acesso físico ao distribuidor geral⁵³ ou a central para interceptar comunicações entre dois pontos e a disponibilidade das comunicações em tempo real depende diretamente da disponibilidade da rede. Portanto, requisitos de alta disponibilidade e *resilience*⁵⁴ são fatores indispensáveis em ambiente Voz sobre IP.

É importante saber que existem novas vulnerabilidades devido a Voz sobre IP, porém o mais importante é ter conhecimento de como as mesmas podem ser minimizadas através de técnicas específicas.

Os ataques aos sistemas Voz sobre IP podem ser divididos em quatro categorias segundo o tipo principal de impacto: disponibilidade, integridade, confidencialidade e privacidade. [21]

⁵³ Distribuidor Geral é o local em uma instalação telefônica onde são feitas as interligações entre os diversos cabos que compõem o sistema telefônico.

⁵⁴ *Resilience* é a habilidade de recuperação rápida de um problema ou mal-funcionamento. A propriedade de um material de voltar ao seu formato ou posição original após ter sido deformado, comprimido, estragado. Aplicado às Telecomunicações, significa manter os equipamentos sempre com alternativas de operação no caso de falhas de componentes ou infra-estrutura pela qual se comunica.

4.1.1 Ataques à Disponibilidade

Os ataques à disponibilidade podem causar perda de receita, de produtividade e incremento dos custos (normalmente decorrentes de manutenções não previstas) pela indisponibilidade ou degradação do serviço. Dentro dessa categoria incluem-se ataques como o *DoS (Denial of Service Attack)* e *DDoS (Distributed Denial of Service Attack)*.

4.1.1.1 DoS (*Denial of service attack*) Ataque por negação de serviço

Dispositivos como telefones IP, *softphones* e *gateways* de Voz sobre IP, assim como qualquer outro dispositivo de rede, podem sofrer ataques com pacotes SYN ou ICMP em uma tentativa de congestionar e indisponibilizar o sistema de comunicação. Esse tipo de ataque normalmente é executado através do consumo dos recursos, alteração nas configurações ou interrupção do funcionamento de componentes da rede. [22]

4.1.1.2 DDoS (*Distributed denial of service attack*) Ataque distribuído

É basicamente um *DoS* (ataque por negação de serviço) originado simultaneamente por vários telefones IP, *softphones* distribuídos. O atacante consegue isso comprometendo vários equipamentos ao mesmo tempo e o seu objetivo final é aumentar o impacto do ataque sendo realizado. [22]

4.1.2 Ataques à Privacidade e Confidencialidade

Os ataques à privacidade e confidencialidade podem expor informações confidenciais de determinado negócio, operação ou pessoa física, exemplos de ataque à privacidade e confidencialidade consistem na escuta (*eavesdropping*), podendo evoluir para um ataque à integridade, assim como o SPIT (*Spam over IP Telephony*) onde mensagens não autorizadas são recebidas, violando a privacidade dos usuários do serviço. [19]

4.1.2.1 *EAVESDROPPING* (Escuta telefônica)

Interceptação dos pacotes de voz por usuário não autorizado através da LAN ou da Internet com objetivo de convertê-los em formato de áudio. Também conhecido com *eavesdropping* (*escuta telefônica*). Ferramentas como *VOMIT*⁵⁵ permitem a captura e conversão destes pacotes. [23]

4.1.2.2 *Spam over IP Telephony* (SPIT)

É o envio de mensagens de voz não autorizadas ou indesejadas, normalmente com fins comerciais. O SPIT se refere ao “*Spam over IP Telephony*”, ou seja, mensagens não solicitadas que chegam por meio de Voz sobre IP. [24]

⁵⁵ *Vomit Voice Over Misconfigured Internet Telephones*, técnica para captura de pacotes de voz e conversão para um formato de áudio conhecido. Permite o ataque através do grampo IP.

4.1.3 Ataques à Integridade

Os ataques à integridade tentam comprometer os serviços Voz sobre IP através de troca de identidade e outras atividades fraudulentas. Ataques deste tipo podem ter impacto financeiro, prejudicar a reputação, deixar vaziar informação sensível e causar perda de produtividade. Dentro dessa categoria podemos incluir *Man in the Middle*(MITM), *Call Hijack*, *Spoofing*, *Call Fraud*, *Phishing* e *Malware*. [25]

4.1.3.1 *Man in the Middle* ou MITM (Homem no meio)

É um ataque onde o invasor consegue se colocar entre o emissor e o receptor sendo capaz de ler, inserir e modificar mensagens, sem que nenhum dos lados saiba que a sessão entre eles está comprometida. Em sistemas Voz Sobre IP o atacante, consegue escutar perfeitamente a conversa entre o chamador e o receptor. [25]

4.1.3.2 *Call Fraud* (Fraude nas chamadas)

É o uso ilícito da rede de telefonia ou da rede Voz sobre IP para realizar chamadas telefônicas. Onde o invasor utiliza o sistema Voz sobre IP de maneira não autorizada obtendo acesso a recursos de maneira indevida para realização de chamadas que sejam contabilizadas como tendo sido originadas pelo endereço do telefone IP de alguma outra pessoa, a qual seria então responsável até o momento pelos gastos. [26]

4.1.3.3 *Call Hijack* (Seqüestro de chamada)

É um tipo de ataque onde o atacante consegue se fazer passar por um dos agentes de usuário (*user agents*) da chamada. Esse tipo de ataque normalmente acaba evoluindo para um ataque do tipo MITM. [25]

4.1.3.4 Falsificação de identidade do usuário

Captura e alteração de pacotes de sinalização das chamadas. Isso permite que o hacker assuma a identidade de outro usuário para obtenção de informações confidenciais ou realização de chamadas sem ônus. Também conhecido como *Caller Identity Spoofing*. Ataques mais complexos, podem ser feitos diretamente aos servidores de tarifação. [26]

4.1.3.5 *Phishing*

Termo que evoluiu to verbo *fish* (pescar) em inglês, e é utilizado para categorizar aqueles ataques realizados através de técnicas de engenharia social (*social engineering*). [27] Exemplos desse tipo de método são e-mails simulando correspondência de bancos ou da receita federal, telefonemas simulando fiscalização ou até acesso a dados confidenciais jogados no lixo, onde o atacante consegue acesso a informações privilegiadas como número do cartão de crédito, senhas entre outras.

4.1.3.6 *Malware*

É um *software* desenhado para se infiltrar e causar dano a sistemas de computação. São vários os tipos de *malware*: vírus de computador, *trojan horses*, *spyware* entre outros. [28]

O *vishing* usa números de VOIP falsos para incitar a vítima a fornecer dados bancários. Um novo tipo de roubo de identidade, por meio de números obtidos em sistemas de Voz sobre IP, está começando a aparecer.

Relacionado com *phishing*, o novo esquema usa números de VOIP obtidos por cartões de crédito ou serviços telefônicos financeiros falsos. Nos golpes de *phishing scam*, os ladrões de identidade enviam e-mails com vírus que aparentemente seriam mensagens de bancos, empresas de cartões de crédito ou de serviços de pagamento on-line.

Normalmente, o e-mail diz que a conta do usuário está comprometida de alguma maneira, e contém um link que pode captar as informações da conta.

O e-mail estimula a vítima a ligar para um número conectado ao VOIP, facilmente obtido por serviços como *Skype*. Em um dos casos de '*vishing*', os alvos foram os usuários de *Paypal*, um serviço de pagamento via internet, que receberam um número de telefone no e-mail. Em outro caso, foi desenvolvido um discador automático, que dizia, por meio de uma gravação, que o cartão de crédito da vítima havia sido fraudado. Detalhe, a gravação ainda incitava a vítima a ligar para um número e fornecer seus dados bancários.

Os números de VOIP são muito fáceis de obter. No entanto, o maior problema é a facilidade com que se consegue o número das contas da vítima pela internet ou pelo telefone.

Os consumidores já se acostumaram a obter crédito pela internet, ou com a discagem automática oferecida por alguns sites de serviços bancários. Se para conseguir crédito fosse necessária a presença física da pessoa, não existiria este tipo de ameaça.

4.1.3.7 Riscos relacionados ao Sistema Operacional

Os servidores de aplicações e algumas estações de usuário utilizam sistemas operacionais de mercado. As vulnerabilidades e riscos intrínsecos a estes sistemas afetam diretamente a segurança de toda a rede convergente.
[25]

As ameaças relacionadas ao sistema operacional trazem diretamente riscos aos sistemas Voz sobre IP e podem causar indisponibilidade na solução. Por exemplo, no ambiente Voz sobre IP temos diversos servidores distribuídos, onde cada um tem sua função específica. Neste exemplo utilizaremos um servidor de licença responsável pelo licenciamento dos terminais, que sofreu um ataque de DoS por não estar com o sistema operacional atualizado, este ataque ocorreu, pois o fabricante do sistema operacional divulgou as correções de segurança a serem instaladas no ambiente, porém o administrador do sistema Voz sobre IP não o fez, com isso uma ameaça conhecida, foi utilizada por um atacante para paralisar o sistema Voz sobre IP. Este é um dos casos onde os riscos e ameaças aos sistemas operacionais podem prejudicar a

solução Voz sobre IP assim como qualquer outra aplicação que esteja sendo executada sobre um sistema operacional.

Ao utilizar soluções Voz sobre IP estamos codificando a nossa voz em pacotes que são transmitidos estatisticamente através de uma rede computadores, na maior parte das vezes a Internet, na qual trafega dados das mais variadas fontes, para os mais variados destinos, rede esta cuja propriedade e controle, é bastante fragmentado. É praticamente impossível para qualquer empresa garantir a segurança dos elementos de rede intermediários, que estejam fora do controle da própria empresa.

Considerando que Voz sobre IP na maior parte das vezes é implementada através da própria Internet, os terminais e servidores necessários para a sua implementação ficam acessíveis a milhões de computadores distribuídos pelo mundo todo.

A sensibilidade dos sistemas Voz sobre IP, as questões de desempenho e a acessibilidade que permeia o conceito da própria Internet, abrem margem para uma vasta gama de possibilidades de ataque do tipo *DoS (denial of service)*, seja um ataque genérico, realizado no nível de rede, seja um ataque realizado no nível da aplicação Voz sobre IP.

Outro elemento que impacta a efetividade do ataque é a expectativa do usuário com relação ao serviço. Acostumado com o nível de serviço oferecido pelo sistema de telefonia tradicional, o usuário espera uma disponibilidade de 99,999%. Isso significa no máximo 5 minutos de indisponibilidade por ano, ou seja, no caso de um ataque a infra-estrutura, a abordagem de segurança deve ser rápida o suficiente para dar uma resposta imediata ao problema.

Finalmente é importante notar que a tecnologia Voz sobre IP ainda está amadurecendo, a ausência de um padrão de segurança bem definido e aceito pela indústria e a existência de problemas de compatibilidade também tem um impacto significativo sobre o modelo de segurança. O efeito dessas limitações é acentuado quando considerada a fragmentação de fornecedores de equipamento, *software* e terminadores existentes e a força que a liberdade de escolha tem sobre a oferta do serviço Voz sobre IP. [22]

Essa característica da indústria dificulta o estabelecimento de padrão de segurança fim-a-fim sob pena de limitação do leque de alternativas existentes e perda das vantagens econômicas que tal conjunto de alternativas propicia. Na medida em que riscos e ameaças começam a se concretizar e seu impacto seja efetivamente mensurado, políticas e padrões poderão ser mais bem estabelecidos. A seguir apresentaremos tabelas com a classificação das ameaças.

Ameaça	Categoria	Característica
DoS <i>Denial of Service Attack</i>	Disponibilidade	Causa a indisponibilidade ou a degradação de serviço para os usuários do sistema Voz sobre IP.
DDoS <i>Distributed Denial of Service attack</i>	Disponibilidade	É basicamente um DoS, originado por vários computadores distribuídos, e tem o objetivo de causar a indisponibilidade ou a degradação de serviço para os usuários do sistema Voz sobre IP.
Eavesdropping	Privacidade e Confidencialidade	É a interceptação de mensagens e conversações por receptor não autorizado. Esta ameaça pode causar a perda da privacidade do usuário do sistema Voz sobre IP e da confidencialidade da comunicação.

Tabela 3 – Classificação de ameaças - Parte I.

Ameaça	Categoria	Característica
MITM <i>Man in the Middle</i>	Integridade	É uma ameaça onde o invasor consegue se colocar entre o emissor e o receptor sendo capaz de ler, inserir e modificar mensagens, sem que nenhum dos lados saiba que a sessão entre eles está comprometida, perdendo então a integridade na comunicação Voz sobre IP.
Call Fraud	Integridade	É o uso ilícito da rede de telefonia ou rede VOIP para fazer chamadas telefônicas. Esta ameaça compromete a integridade do sistema Voz sobre IP.
Call Hijack	Integridade	É um tipo de ataque onde o atacante consegue se fazer passar por um dos <i>user agents</i> da chamada. Esse tipo de ataque normalmente acaba evoluindo para um ataque do tipo MITM, comprometendo a integridade na comunicação Voz sobre IP.
Phishing	Integridade	É utilizado para categorizar aqueles ataques realizados através de técnicas de engenharia social. Exemplos desse tipo de método são e-mails simulando correspondência de bancos ou da receita federal, telefonemas simulando fiscalização, onde o atacante consegue acesso a informações privilegiadas como número do cartão de crédito, senhas entre outras, comprometendo a integridade na comunicação Voz sobre IP, pois utilizam a rede VOIP para trafegar esse tipo de ameaça.

Tabela 4 – Classificação de ameaças - Parte II.

Ameaça	Categoria	Característica
Malware	Integridade	É um <i>software</i> desenhado para se infiltrar e causar dano a sistemas Voz sobre IP. São vários os tipos de <i>malware</i> : vírus de computador, <i>trojan horses</i> , <i>spyware</i> entre outros. Esse tipo de software ameaça a integridade das informações geradas através dos <i>softphones</i> utilizados pelos sistemas Voz sobre IP.
Riscos Relacionados ao Sistema Operacional	Integridade	As vulnerabilidades e riscos intrínsecos aos sistemas operacionais afetam diretamente a integridade de toda a rede Voz sobre IP.

Tabela 5 – Classificação de ameaças - Parte III.

As ameaças das redes de computadores tradicionais trazem para a tecnologia Voz sobre IP os riscos de segurança hoje existentes apenas nas redes de computadores além de novas ameaças que surgiram com a criação das soluções Voz sobre IP, porém diversos mecanismos de segurança, aliados à utilização de melhores práticas podem ser implementados para minimizar os riscos e as ameaças nos sistemas Voz sobre IP.

A seguir demonstraremos mecanismos de segurança para proteger ambientes Voz sobre IP.

5. MELHORES PRÁTICAS DE SEGURANÇA EM VOZ SOBRE IP

A seguir serão apresentados mecanismos de segurança e melhores práticas para implementação de uma estrutura Voz sobre IP segura.

5.1 Protocolos de Segurança

Neste grupo incluem-se mecanismos como o *SIP Digest*, *Network Asserted Identity*, *Authenticated Identity Body (AIB)*, *Identity Header Field* e protocolos como *TLS*, *IPSec* e *SRTP* que serão detalhados a seguir.

5.1.1 SIP Digest

O *SIP Digest* é um mecanismo de autenticação básico, trazido do *HTTP*, que deve ser suportado por qualquer agente usuário (*user agent SIP*). É uma forma simples de servidor e cliente verificarem se efetivamente tem um segredo compartilhado sem que a senha trafegue abertamente. [29]

5.1.2 TLS Transport Layer Security

O *TLS (Transport Layer Security)*, já está na sua versão 1.1 e é uma evolução do *SSL (Secure Socket Layers)*. O *TLS* é um protocolo que pode ser utilizado para prevenir a escuta, modificações em mensagens ou o envio de

mensagens falsas da sinalização VOIP. O TLS também pode servir para prevenir ataques do tipo DoS.

Em contrapartida agrava os ataques DoS na medida em que, nesse caso, pode haver um consumo significativo da capacidade de processamento do sistema para a descryptografia das mensagens do ataque.

O uso do TLS é feito *hop-by-hop* (nodo-a-nodo) o que obriga a todos os elementos da rede VOIP que encaminham sinalização, suportem o protocolo TLS para que a sinalização esteja 100% protegida. [30]

Considerando a diversidade de fornecedores de terminais e interconexões que hoje são agregados para implementar o VOIP, tal abordagem limita bastante o número as alternativas disponíveis no mercado. O TLS envolve ainda a manutenção e gerência de uma entidade certificadora que permita verificar se os certificados são válidos e cancelar certificados já sem validade.

5.1.3 IPSec IP Security

O *IPSec* ou *IP Security* provê criptografia no nível de rede e pode ser utilizado para garantir a autenticidade, a integridade e a confidencialidade tanto fim-a-fim como nodo-a-nodo. O *IPSec* funciona autenticando e criptografando os pacotes IP e precisa de um protocolo adicional para a troca de chaves: o IKE (*Internet Key Exchange*).

O *IPSec* tem problemas graves ao ser utilizado em redes que fazem uso de NAT (*Network Address Translation*), uma situação bastante comum nas

rede IP de hoje em dia, e precisa dispor de uma infra-estrutura pública para troca e validação das chaves, infra-estrutura que hoje não existe. [31]

5.1.4 SRTP Secure Real-Time Protocol

O SRTP ou *Secure Real-Time Protocol* e o SRTCP ou *Secure Real-Time Control Protocol* oferece confidencialidade, autenticação e proteção contra retransmissão fraudulenta dos pacotes RTP e RTCP prevenindo ataques como escuta do RTP, manipulações do SSRC, manipulações do CODEC e inserções RTCP.

O *Network Asserted Identity* é um mecanismo bastante específico para a troca de identidade entre elementos de rede que já possuem relacionamento confiável utilizando algum outro mecanismo ou política de segurança. [32]

A utilidade desse tipo de mecanismo é, por exemplo, permitir que um usuário, depois de autenticado, faça chamadas anônimas sem que para isso a rede perca a possibilidade de rastrear a chamada realizada, preservando assim a privacidade do originador.

5.1.5 AIB Authenticated Identity Body

O *Authenticated Identity Body* (AIB) é um mecanismo que utiliza corpos de mensagens e certificados S/MIME para assinar parte do cabeçalho das mensagens de forma a autenticar o *user agent*, dessa forma evitando ataques do tipo *spoofing*. [33]

5.1.6 IHF *Identity Header Field*

Finalmente o *Identity Header Field* é outro mecanismo que também permite assinar parte dos cabeçalhos da mensagem. A diferença é que este mecanismo utiliza cabeçalhos-padrão específicos para a assinatura e para o acesso ao certificado, o que resolve alguns dos problemas relacionados à utilização do padrão S/MIME. [34]

Os mecanismos *SIP Digest*, *Network Asserted Identity*, *Authenticated Identity Body (AIB)*, *Identity Header Field* e protocolos como TLS, IPSec e SRTP podem ser utilizados para garantir a questão de disponibilidade, integridade, confidencialidade e privacidade.

A seguir demonstraremos os requisitos de segurança em projetos envolvendo Voz sobre IP a serem utilizados em conjunto com os mecanismos e protocolos de segurança para garantir a segurança nos sistemas Voz sobre IP.

5.2 Requisitos de segurança em projetos envolvendo voz sobre IP

Não há convergência segura se não houver segurança no perímetro. Diversos mecanismos devem ser utilizados para garantir a disponibilidade, integridade, confidencialidade e privacidade das comunicações entre componentes e aplicações da rede.

É necessário garantirmos que o tráfego de voz, dados e multimídia estejam protegidos. Para isso, diversas soluções desenhadas e desenvolvidas

para infra-estruturas convergentes são indicadas para cada caso. Algumas delas são:

5.2.1 Firewalls Voz sobre IP

Firewalls Voz sobre IP são sistemas desenvolvidos para prevenir acessos não autorizados à rede Voz sobre IP, através de filtros de pacotes. Pode ser implementado em *hardware*, ou *software* ou em combinação de ambos.

No ambiente Voz sobre IP, a filtragem de um *firewall* é necessária para gerir os protocolos de rede. Os *firewalls* tradicionais possuem filtros de pacotes que não conseguem lidar com protocolos Voz sobre IP complexos tais como H.323 e SIP, que utilizam diversas portas UDP e TCP e complicados esquemas de inicialização. Existem *firewalls* especialmente desenhados para lidar com o tráfego de Voz sobre IP, ou seja, inspecionar profundamente os pacotes de H.323 e SIP. Trabalham com uma quantidade grande de pequenos pacotes UDP, e a capacidade de controlar a abertura e fechamento de portas dinâmicas, entre outras características. [35]

5.2.2 IPS Voz sobre IP

Intrusion Prevention System Voice over IP, são sistemas de prevenção de intrusão em soluções Voz sobre IP. O IPS é um aplicativo usado para detectar intrusões dentro da rede e responder prontamente contra as vulnerabilidades subjacentes dos protocolos Voz sobre IP, preservando a integridade dos aplicativos e da qualidade de voz da telefonia IP. Algumas

ferramentas de IPS já estão aptas a lidar com ataques específicos de VOIP, como o VOMIT e o Grampo IP. [36]

5.2.3 Segurança nas estações de trabalho

Além dos itens apresentados acima, é importante que cuidemos de estações de trabalho e *notebooks* corporativos, evitando a entrada de vírus e ataques polimórficos na rede. A maior parte das empresas protege as estações de trabalho através de *firewalls* e soluções de antivírus baseadas em assinaturas. Infelizmente, muitas ameaças atuais não podem ser travadas por estas soluções tradicionais.

Novos e desconhecidos ataques ocorrem todas as semanas e podem causar danos significativos antes de o seu padrão ser conhecido. Para fazer em face de tais ataques, as empresas necessitam de *software* de prevenção de intrusões residentes no *host*. Trata-se de agentes que residem em cada *desktop* ou servidor e podem ser administrados para fazer cumprir políticas que diminuem ou eliminem ataques conhecidos e desconhecidos, através de monitoração e limitando o que um dado *host* pode ou não fazer. Proteção de intrusão no *host* é especialmente desejável numa rede Voz sobre IP porque detém ataques que, se deixados descontrolados, poderiam abater a estrutura da rede e prejudicar o serviço de voz. [37]

5.2.4 Zonas Militarizadas

Os serviços e aplicações Voz sobre IP tornam-se complexos, quando introduzimos aplicações como *unified messaging*, *contact center* e *presence*, é

bastante recomendável a criação de uma “zona militarizada”. A função dela é segmentar a rede, com dispositivos multifuncionais que controlam o tráfego passante, evitando inclusive ataques internos.

A zona militarizada, conhecida também como rede de perímetro, seria a exposição de determinada área da rede interna para publicar determinados serviços Voz sobre IP. Para configurar uma rede de perímetro precisamos do auxílio de *firewall* para que somente as portas e/ou protocolos que interessam sejam desbloqueados e assim diminuir ao máximo a exposição para a internet. [39]

5.2.5 Resilience

Pode ser definido como a capacidade de uma rede de manter-se operante em situações adversas. Deve ser feito através da utilização de mecanismos que garantam alta disponibilidade e redundância de todos os seus componentes, além de uma rápida recuperação em caso de desastre. Diversos componentes contribuem para a criação de uma rede convergente resiliente. [40]

5.2.6 Monitoração

A monitoração da rede convergente é necessária para garantir alta disponibilidade e rápida recuperação de todo o sistema em caso de falhas. Sistemas de gerenciamento permitem ações pró-ativas, indicando alarmes através do padrão SNMP, gerenciando falhas de plataformas convergentes, aplicações e terminais. [41]

Os requisitos de segurança em projetos Voz sobre IP devem ser utilizados para garantir a disponibilidade, integridade, confidencialidade e privacidade das comunicações entre componentes e aplicações da rede.

A seguir demonstraremos a utilização de melhores práticas no ambiente LAN (*Local area network*) e WAN (*Wide area network*).

5.3 Segurança na LAN

Neste primeiro cenário, ilustramos a utilização de telefones IP, *softphones* e aplicações na LAN.

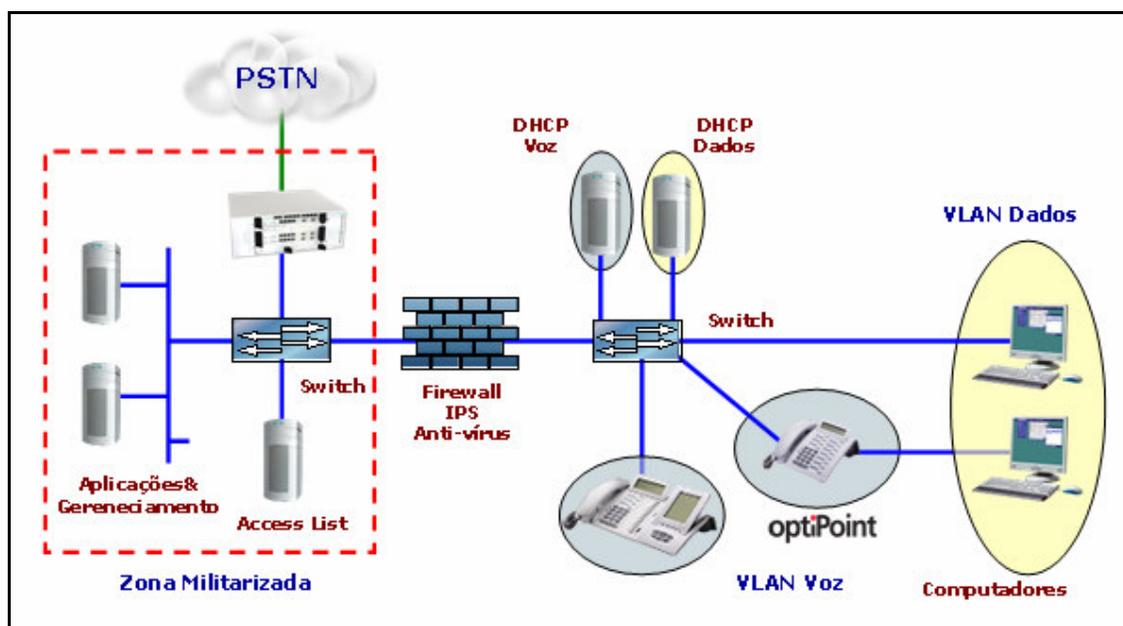


Figura 15 – Topologia na LAN. ⁵⁶

⁵⁶ Fonte: Série VOIP - Dimensionamento VOIP - Parte 01. Disponível em: <http://www.wirelessbrasil.org/wirelessbr/colaboradores/jose_smolka/voip/artigo_04/serie_voip_041.htm>.

Neste caso, são recomendadas as seguintes ações para aumentar a segurança da rede convergente:

5.3.1 Segmentação do tráfego de voz e dados

As segmentações do tráfego de voz e dados podem ser feitas através de *switches*. O *switch* é um equipamento que filtra e envia pacotes entre segmentos LAN, operando na camada 2, e as vezes camada 3, do modelo OSI de referência.

Esta segmentação contribui para obtenção de uma melhor QoS além de facilitar a gerência da rede de voz e simplificar sua manutenção. Ainda podemos com isso evitar que o segmento de voz seja alvo de ataques de “*eavesdropping*” (captura não autorizada do tráfego de conversas telefônicas que trafegam na rede encapsuladas em pacotes IP) realizados com o VOMIT e outras ferramentas semelhantes descritas anteriormente.

Com a implementação da segmentação, vários outros ataques deixam de existir para a rede de voz, como por exemplo, os ataques baseados em TCP/IP que, mesmo destinados a outros alvos que não estejam diretamente relacionados com a infra-estrutura de Voz sobre IP, podem tornar estes serviços indisponíveis caso todo o tráfego esteja no mesmo segmento. Por exemplo, os telefones IP normalmente utilizam o protocolo UDP com portas acima de 16384 para sua comunicação. Sendo assim, um ataque de negação de serviços no segmento de dados poderia afetar também os serviços de voz se redes não estiverem adequadamente segmentadas.

Para que se possa melhorar ainda mais os vários aspectos citados da rede de voz, recomenda-se a separação dos segmentos de rede de voz e

dados em VLAN's distintas. Como por exemplo, em uma instalação de pequeno porte, uma VLAN dedicada ao tráfego de voz seria suficiente, onde seriam instalados os servidores Voz sobre IP e os telefones IP. Outros componentes como estações de gerenciamento e sistemas de correio de voz podem residir no segmento de dados. Já em instalações de grande porte, várias VLAN's podem ser criadas, tanto para voz quanto para dados. [38]

5.3.2 Segmentação de Servidor DHCP

Preferencialmente devem-se utilizar servidores DHCP separados para os segmentos de voz e dados. Sendo assim, os ataques de negação de serviços (DoS) e outros lançados contra o servidor DHCP no segmento de dados não vão interferir com a alocação de endereços IP para os telefones no segmento de voz, e vice-versa, o que aumenta a tolerância da rede, isto também aumenta a proteção contra ataques como falsificação de identidade do usuário, escuta telefônica (grampo IP) ou DoS (*denial of service*) ou ataques gerados por *worms* e vírus polimórficos. [42]

5.3.3 *Appliance* Multifuncional

O *appliance* multifuncional dentro do ambiente Voz sobre IP inclui a utilização de um *firewall* e um IPS em conjunto, permitindo que usuários com *softphone* no computador acessem somente a VLAN de voz e que o tráfego de pacotes deste computador seja unicamente de pacotes de voz. O IPS descarta os pacotes através de assinaturas não válidas ou por anomalias de pacotes que queiram atingir a VLAN de voz indevidamente.

Os *softphones* que são instalados em estações de trabalho e que conseqüentemente pertencem a VLAN de dados precisam de acesso à rede Voz sobre IP. Portanto, teremos conexões de dados dentro VLAN de voz. Para minimizarmos este risco, é sugerido incluir um *firewall* e um IPS, que compõem a solução *Appliance* Multifuncional.

Para melhorar o desempenho do *firewall* / IPS, é recomendável a utilização de um servidor de lista de acessos, definindo os usuários que podem ou não acessar o *gateway* através de autenticação e senha individual. [42]

5.3.4 Configurar os telefones IP com endereços IP associados ao *mac*

A utilização do *mac address* permite a autenticação dos telefones IP, ou seja, quando um telefone IP tenta obter configurações da rede do servidor Voz sobre IP, seu *mac address* pode ser verificado em uma lista de controle de acesso. Caso o endereço seja desconhecido, o dispositivo não receberá a configuração.

Caso seja possível, devem-se aplicar endereços IP estáticos para os telefones IP, e associá-los ao *mac address* do dispositivo. Sendo assim, cada telefone IP terá sempre o mesmo endereço IP associado ao endereço MAC. Desta forma, para conseguir instalar um telefone IP não autorizado na rede, um atacante teria que forjar tanto um endereço IP válido para o segmento de voz quanto o endereço MAC a ele associado.

Alguns aspectos devem ser considerados antes de tal aplicação, pois dependendo das características do ambiente de implementação, a associação

entre endereço IP estático e *mac address* nos telefones IP pode ser de difícil gerenciamento. [43]

5.3.5 Usar endereços IP privativos e inválidos nos telefones IP

Para reduzir a possibilidade de que o tráfego de voz possa ser monitorado de fora da rede interna e para evitar que os atacantes consigam mapear o segmento de voz em busca de vulnerabilidades, nos telefones IP devem ser utilizados endereços IP inválidos, compatíveis com a RFC 1918.

Além disto, o uso de endereços IP inválidos sucumbirá em menores custos. A utilização de endereços IP privativos e principalmente de classes diferentes nos segmentos de voz e dados, de acordo com a orientação do RFC 1918 (*Address Allocation for Private Intranets*), servirá para facilitar a configuração de filtros e a monitoração. As conexões com redes externas devem utilizar endereços IP válidos fornecidos por um *firewall*, através do serviço NAT (*Network Address Translation*). [44]

5.3.6 Personal firewall

O *personal firewall* é um sistema desenvolvido para prevenir acessos não autorizados, controle de acesso, detecção de ataques, controle de aplicações e monitoramento de desempenho. Como os *softphones* são instalados em computadores, em qualquer topologia de rede será necessária instalação de um *personal firewall*, para evitar que ataques que tenham como objetivo a rede de dados ou voz atinjam a estação de trabalho e

conseqüentemente o sistema de Voz sobre IP, deixando-o fora de operação. O *personal firewall* é uma ferramenta muito importante para garantir a disponibilidade do *softphone*. [37]

5.3.7 Utilização de senha

É possível atribuir uma senha PIN (*personal identification number*) de autenticação pessoal para cada usuário. Isto restringe ainda mais o acesso indevido à rede convergente. Em caso de reinicializar ou para administrar o telefone IP, é necessária uma senha de administrador evitando acesso indevido.

Dentre as políticas utilizadas pelas grandes corporações a composição da senha é a que gera mais controversa, por um lado profissionais com dificuldade de memorizar varias senhas de acesso, por outro, funcionários displicentes que anotam a senha sob o teclado no fundo das gavetas, em casos mais graves o colaborador anota a senha no monitor.

Recomenda-se a adoção das seguintes regras para minimizar o problema, mas a regra fundamental é a conscientização dos colaboradores quanto ao uso e manutenção das senhas.

- Senha com data para expiração;
- Adotar um padrão definido onde a senha tem prazo de validade, obrigando o colaborador ou usuário a renovar sua senha;
- Inibir a repetição;
- Adotar através de regras predefinidas que uma senha uma vez utilizada não poderá ter mais que 60% dos caracteres repetidos, p. ex: senha

anterior “123senha” nova senha deve ter 60% dos caracteres diferentes como “456seuze”, neste caso foram repetidos somente os caracteres “s” “e” os demais diferentes;

- Obrigar a composição com número mínimo de caracteres numéricos e alfabéticos;
- Definir obrigatoriedade de 4 caracteres alfabéticos e 4 caracteres numéricos, por exemplo: 1s4e3u2s ou posicional os 4 primeiros caracteres devem ser numéricos e os 4 subseqüentes alfabéticos por exemplo: 1432seuz, e;
- Criar um conjunto de possíveis senhas que não podem ser utilizadas Monta-se uma base de dados com formatos conhecidos de senhas e proibir o seu uso, como por exemplo, o usuário chama-se Jose da Silva, logo sua senha não deve conter partes do nome como 1221jose ou 1212silv entre outros, os formatos DDMMAAAA ou 19XX, 1883emc ou l2B3M4 entre outras. [45]

5.3.8 Restringir o acesso físico

O acesso físico à rede em si deve ser restrito, isto devido à possibilidade de algum atacante conseguir acesso físico indevido na rede e através dessa vulnerabilidade conseguir tirar proveitos. Com acesso à rede física o atacante pode, por exemplo, acessar um console fisicamente, instalar um telefone IP não autorizado e utilizar técnicas de ataque para enganar os usuários, fazendo-os pensar que estão conversando com alguma outra pessoa, quando na verdade estão conversando com o atacante. Desta forma, informações sigilosas poderão ser obtidas através de engenharia social.

Naturalmente, o acesso físico indevido também expõe os componentes da infra-estrutura dos sistemas Voz sobre IP, ameaças como fraudes, roubo, sabotagem ou danificação acidental ou proposital dos equipamentos, podendo causar a indisponibilidade dos serviços. Por estes motivos, convém que o acesso físico aos dispositivos mais críticos da rede (*switches*, roteadores, servidores Voz sobre IP, *firewalls*, entre outros), seja restrito apenas a usuários autorizados. [46]

5.3.9 Auditar os recursos Voz sobre IP

A verificação da qualidade de serviço prestado pelos equipamentos Voz sobre IP, bem como sua utilização pelos usuários deve ser auditada periodicamente. Para isso devemos manter registros das informações sobre as sessões (data e horário do início e término, duração, origem, destino, entre outros) além de informações relacionadas à qualidade de serviço. A auditoria pode ser implementada através de aplicações especializadas, e devem monitorar principalmente os terminais e os *gateways* de voz.

Para uma auditoria mais precisa, recomendamos que os usuários utilizem algum tipo de autenticação (descritos anteriormente neste trabalho) quando utilizarem os serviços da rede de voz. [47]

A utilização de melhores práticas no ambiente LAN (*Local area Network*) devem ser implementada para garantir a segurança no sistema Voz sobre IP. A seguir demonstraremos a utilização de melhores práticas no ambiente WAN (*wide area network*).

5.4 Segurança na WAN

A topologia apresentada abaixo indica a interligação através da WAN entre duas localidades que utilizam telefones IP, *softphones* e aplicações:

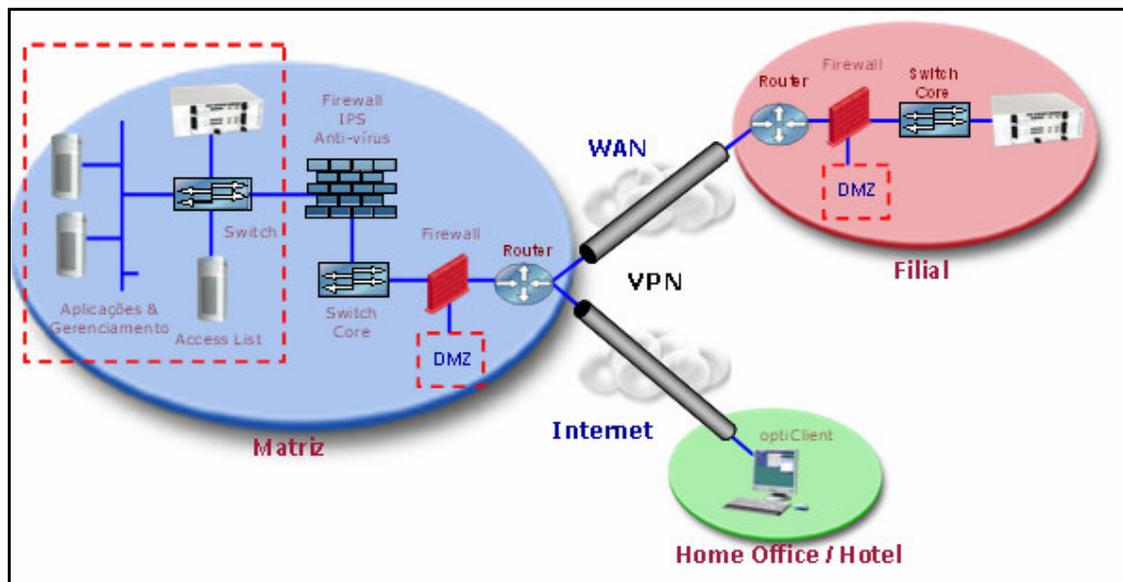


Figura 16 – Topologia na WAN. ⁵⁷

5.4.1 Virtual Private Network (VPN)

O conceito de VPN (*Virtual Private Network*) surgiu da necessidade de se utilizar redes de comunicação não confiáveis para trafegar informações de forma segura.

As redes públicas são consideradas não confiáveis, tendo em vista que os dados que nelas trafegam estão sujeitos a interceptação e captura. Em

⁵⁷ Fonte: Série VOIP - Dimensionamento VOIP - Parte 02. Disponível em: <http://www.wirelessbrasil.org/wirelessbr/colaboradores/jose_smolka/voip/artigo_04/serie_voip_042.htm>.

contrapartida, estas tendem a ter um custo de utilização inferior aos necessários para o estabelecimento de redes proprietárias, envolvendo a contratação de circuitos exclusivos e independentes.

Com o explosivo crescimento das soluções de Voz sobre IP, o constante aumento de sua área de abrangência, e a expectativa de uma rápida melhoria na qualidade dos meios de comunicação associado a um grande aumento nas velocidades de acesso e *backbone*, esta passou a ser vista como um meio conveniente para as comunicações corporativas entre as localidades interligadas. No entanto, a passagem de dados sensíveis pela Internet somente se torna possível com o uso de alguma tecnologia que torne esse meio altamente inseguro em um meio confiável.

Os ataques de um *hacker* com acesso a WAN utilizando principalmente um grampo pode ser solucionado programando VPN (*Virtual Private Network*) entre os roteadores das localidades que utilizam a telefonia IP.

Desenvolvida para uma transmissão de dados segura a VPN tem como função a criptografia de dados. Estes dados trafegam na WAN num túnel de segurança virtual de um ponto a outro, restringindo o acesso remoto dos computadores que não estejam dentro deste domínio.

As medidas de segurança recomendadas para os riscos de dentro da LAN, para as topologias com telefones IP, e com telefones IP expostas anteriormente são aplicáveis também a este caso dentro da LAN. [48]

5.4.2 Internet com VPN

Neste cenário, acrescentamos um usuário remoto que quer realizar uma chamada telefônica utilizando o *softphone* através da Internet. Este usuário se expõe a todos os problemas de utilizar um serviço de pouca confiabilidade, como é o caso da Internet.

Para este tipo de utilização é recomendável instalar VPN, no computador remoto com *softphone*. Desta forma iremos garantir que não haja escuta telefônica através de captura de pacotes na Internet, ataques de DoS e autenticação de um usuário indevido no sistema Voz sobre IP. [48]

5.4.3 Segurança em acessos remotos

Sistemas Voz sobre IP que são gerenciados remotamente não poderão maximizar os seus níveis de produtividade se não tiverem acesso completo aos recursos de que necessitam. Esse acesso, todavia, deve ser seguro para garantir a integridade da informação. Ligações seguras entre localizações remotas podem ser conseguidas utilizando tecnologias de segurança de rede tais como VPN para voz e vídeo (V3PN). V3PN integra segurança de conectividade com razoabilidade de custos através de VPN com IPSec, produzindo convergência de redes de dados, voz e vídeo sobre IP, conforme detalhado anteriormente neste trabalho. [49]

As medidas de segurança aplicadas na WAN, LAN devido a serem semelhantes podem ser aplicadas também neste caso.

5.5 Resumo das melhores práticas em segurança no Ambiente VOIP

As melhores práticas em segurança no ambiente Voz sobre IP devem ser implementadas com bastante cuidado, tendo em vista as ameaças que podem prejudicar o ambiente Voz sobre IP.

Cuidados no desenho da arquitetura de rede e implementação dos procedimentos que serão utilizados para prover e gerenciar os serviços de Voz sobre IP, são itens chave para maior garantia de segurança.

A possibilidade de separar física e logicamente os serviços de voz dos serviços de dados em redes diferentes, com blocos de endereços separados e serviços de suporte DHCP dedicados dificulta a escuta e facilita a definição das regras de acesso, simplificando a configuração e o controle.

A seguir apresentaremos tabelas com recomendações e melhores práticas mencionadas neste capítulo, para os seguintes tipos de ameaças.

Ameaça	Categoria	Medidas de Segurança
DoS <i>Denial of Service Attack</i>	Disponibilidade	O TLS é uma evolução do SSL e pode servir para prevenir ataques do tipo DoS. A Segmentação dos Servidores DHCP e a implementação de VPN entre as localidades é uma pratica recomendável para evitar o DoS. Implementação de <i>firewall</i> auxiliam na prevenção de acessos não autorizados.

Tabela 6 – Ameaças e medidas de contenção a ataques – Parte I.

Ameaça	Categoria	Medidas de Segurança
DDoS <i>Distributed Denial of Service attack</i>	Disponibilidade	O TLS é uma evolução do SSL e pode servir para prevenir ataques do tipo DDoS. A Segmentação dos Servidores DHCP e a implementação de VPN entre as localidades é uma prática recomendável para evitar o DDoS. Implementação de <i>firewall</i> auxiliam na prevenção de acessos não autorizados.
Eavesdropping	Privacidade e Confidencialidade	O SRTP e o SRTCP oferecerem confidencialidade e privacidade para proteção contra retransmissão fraudulenta dos pacotes RTP e RTCP prevenindo ataques como <i>eavesdropping</i> . O TLS é uma evolução do SSL e pode servir para prevenir ataques do tipo <i>eavesdropping</i> . Segmentação do tráfego de voz e dados pode evitar que o segmento de voz seja alvo de ataques de <i>eavesdropping</i> .
SPAM <i>Spam over IP Telephony</i>	Privacidade e Confidencialidade	O SRTP e o SRTCP oferecerem confidencialidade e privacidade para proteção contra retransmissão fraudulenta dos pacotes RTP e RTCP prevenindo ataques como SPAM. IHF <i>Identity Header Field</i> permite assinar parte dos cabeçalhos da mensagem IPSec IP Security. O IPSec ou IP Security provê criptografia no nível de rede e pode ser utilizado para garantir a autenticidade, a integridade e a confidencialidade tanto fim-a-fim como nodo-a-nodo. Importante garantirmos a segurança nas estações de trabalho.

Tabela 7 – Ameaças e medidas de contenção a ataques – Parte II.

Ameaça	Categoria	Medidas de Segurança
MITM <i>Man in the Middle</i>	Integridade	O IPSec provê criptografia no nível de rede e pode ser utilizado para garantir a autenticidade, a integridade e a confidencialidade tanto fim-a-fim como nodo-a-nodo. Implementação de uma VPN criando um túnel seguro. Segurança física aos equipamentos e segurança no acesso remoto. Podemos utilizar o SIP <i>Disgest</i> como mecanismo de autenticação. Utilização de um IPS na monitoração do sistema pode auxiliar na segurança.
Call Fraud	Integridade	O IPSec provê criptografia no nível de rede e pode ser utilizado para garantir a autenticidade, a integridade e a confidencialidade tanto fim-a-fim como nodo-a-nodo. A Implementação de uma VPN criando um túnel seguro. Segurança física aos equipamentos e segurança no acesso remoto.
Call Hijack	Integridade	O TLS é uma evolução do SSL e pode servir para prevenir ataques do tipo <i>Call Hijack</i> . O IPSec ou IP Security provê criptografia no nível de rede e pode ser utilizado para garantir a autenticidade, a integridade e a confidencialidade tanto fim-a-fim como nodo-a-nodo. Podemos utilizar o AIB como mecanismo de segurança.

Tabela 8 – Ameaças e medidas de contenção a ataques – Parte III.

Ameaça	Categoria	Medidas de Segurança
<i>Phishing</i>	Integridade	O TLS (<i>Transport Layer Security</i>) é uma evolução do SSL (<i>Secure Socket Layers</i>) e pode servir para prevenir ataques do tipo <i>Phishing</i> . O IPSec ou IP Security provê criptografia no nível de rede e pode ser utilizado para garantir a autenticidade, a integridade e a confidencialidade tanto fim-a-fim como nodo-a-nodo.
<i>Malware</i>	Integridade	O TLS (<i>Transport Layer Security</i>) é uma evolução do SSL (<i>Secure Socket Layers</i>) e pode servir para prevenir ataques do tipo <i>Malware</i> . O IPSec ou IP Security provê criptografia no nível de rede e pode ser utilizado para garantir a autenticidade, a integridade e a confidencialidade tanto fim-a-fim como nodo-a-nodo. Atualizações automáticas do sistema operacional e utilização de mecanismos como <i>firewall</i> e antivírus.
Riscos Relacionados ao Sistema Operacional	Integridade	Atualizações automáticas do sistema operacional e utilização de mecanismos como <i>firewall</i> e antivírus. Importante garantirmos a segurança nas estações de trabalho.

Tabela 9 – Ameaças e medidas de contenção a ataques – Parte IV.

Um repositório dos eventos de chamada pode ter uma política de segurança mais orientada à preservação da integridade enquanto para um servidor Voz sobre IP pode ter uma política cujo enfoque seja no requisito disponibilidade.

A padronização da configuração dos componentes de rede, eliminando todos os serviços não necessários e o estabelecimento do IPSec ou do *secure shell* (SSH) para gerência remota são políticas importantes para redução das portas de entrada e prevenção contra o acesso não autorizado.

O uso de redundância em todos os níveis: físico, de enlace, de rede, de transporte e de aplicação são vitais para fornecer garantias de continuidade frente a eventuais ataques e fatores não previstos. Essa redundância deve também estar presente no planejamento da rede elétrica (redundância esta que precisa ser testada e calibrada periodicamente), de forma a garantir a continuidade nos casos de falta de força.

As verificações dos componentes de *software* da infra-estrutura VOIP com relação aos requisitos de segurança e uma política de gerência de *patches* (correções de *software*) é vital na garantia do nível de qualidade, já que a segurança deve estar presente em cada um dos sistemas existentes e não somente através de sistemas especializados.

6. CONSIDERAÇÕES FINAIS

6.1 Trabalhos Futuros

Visando complementar o tema que foi abordado neste trabalho, alguns assuntos, que não foram explorados ou apenas citados aqui, poderão ser desenvolvidos em futuras linhas de pesquisas e estão relacionados a seguir:

- Técnicas, Anti Análise Forense

Este estudo permitirá analisar as necessidades investigativas por profissionais na área de informática e área jurídica permitindo reconstituir fatos imprescindíveis necessários a situações de litígio, trazendo informações importantes sobre as técnicas utilizadas por fraudadores e criminosos permitindo a eliminação de rastros na recomposição destes fatos e prevenindo aos administradores de sistemas Voz sobre IP, além dos administradores de segurança a prevenção contra esta ameaça.

- Segurança em Redes sem Fio

Este tema trata sobre a utilização de sistemas Voz sobre IP através de redes de comunicação sem fio. Um desenvolvimento de técnicas e análise de vulnerabilidades em redes sem fio, com tráfego de Voz sobre IP assim como o detalhamento de suas correções e melhores práticas de implementação.

- Legislação

Questões legais são muito importantes, já que os sistemas Voz sobre IP envolvem ou manipulam informações confidenciais e que devem ser mantidas íntegras. Seria interessante uma pesquisa complementar com uma análise de como estas questões são tratadas pela lei no exterior, e se há alguma legislação vigente ou projeto de lei que trata deste assunto no Brasil.

6.2 Conclusão

A tecnologia de sistemas Voz sobre IP já é uma realidade para muitas empresas no Brasil. A cada dia novas empresas implementam ou analisam projetos de sistemas Voz sobre IP para suas redes. A evidente redução de custos com telefonia, ganhos de mobilidade e compartilhamento de recursos ao longo da rede faz com que a convergência de redes seja a tecnologia com previsão de maior crescimento no mundo nos próximos anos.

Com a atenção das empresas voltadas para sistemas Voz sobre IP, invasores aproveitam a tecnologia emergente para tentar encontrar novas vulnerabilidades e maneiras de atacar redes e conseguir informações confidenciais. Isto faz com que, junto com o crescimento da adoção de sistemas Voz sobre IP, segurança seja outro potencial, de área que deve crescer.

Uma solução adequada contra ataques a redes com sistemas Voz sobre IP não pode ser obtida através de uma única tecnologia. Recursos de segurança dos sistemas Voz sobre IP são fundamentais, mas não são

suficientes. Premissas concretas do projeto de segurança, aliadas às melhores técnicas para garantir a continuidade dos negócios e disponibilidade dos serviços, complementam as soluções.

É importante notar que apesar do grande número de ameaças que podem afetar a disponibilidade, integridade e a privacidade e confidencialidade do serviço Voz sobre IP, eventualmente causando prejuízo a usuários e prestadores de serviço, a sua existência é apenas teórica. Ainda é muito difícil encontrar empresas que sofreram ataques a sistemas Voz sobre IP.

Na prática, ataques aos serviços Voz sobre IP ainda são muito difíceis de conduzir. Eventuais atacantes enfrentam uma barreira de conhecimento que aliada à baixa popularidade dos serviços Voz sobre IP não torna tal esforço compensador, porém diversos mecanismos de segurança são implementados para garantir a segurança no ambiente Voz sobre IP.

Projetar, implementar, e operar sistemas Voz sobre IP de forma segura é um esforço complexo que exige uma preparação cuidadosa, por esse motivo sugere-se que a análise das vulnerabilidades do serviço e a mensuração do custo-benefício das diferentes opções disponíveis antecedam todas as ações de melhorias de segurança planejadas para um serviço de voz sobre IP.

Por fim, concluímos que a implementação das melhores práticas e gerenciamento, podem resultar em redes Voz sobre IP seguras.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Claudio Brancher Kerber, **Glossário Tecnológico**. Disponível em <http://www.portaldigitro.com.br/glossario_digitro.php>. Acesso em: Jan. de 2007.

[2] Vocaltec Communications Ltda. Internet Phone, **A empresa Vocaltec fez o lançamento do Internet Phone**. Disponível em: <<http://www.vocaltec.com/engsite/home/default.asp>>. Acesso em: Nov. de 2006.

[3] *Australian Academic and Research Network VoIP Project*. Disponível em: <<http://www.aarnet.edu.au/rd/voip/index.html>>. Acesso em: Nov. 2006.

[4] José Marcos Câmara Brito, **Voz sobre IP, Tecnologias e Aplicações**. Monografia apresentada no curso de especialização “Engenharia de Comunicação de Dados” do Instituto Nacional de Telecomunicações em Dezembro de 2004.

[5] CESNET. **Voice services in the network**. Disponível em: <<http://www.ces.net/project/iptelephony/>>. Acesso em Jan de 2007.

[6] Rede Nacional de Pesquisa, Projeto **Piloto Voip Relatório Técnico P.5.1**. Disponível em: <<http://www.voip.nce.ufrj.br/publication/reports/gt-voip-p51.pdf>>. Acesso em: Out de 2004.

[7] Infonetics Research, **Estudo da Infonetics mostra ganhos no mercado de VOIP**. Disponível em:

<<http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=5512&sid=24&tpl=printerview>>. Acesso em: Jan 2007.

[8] Siemens Enterprise Network, **Strategic and Marketing Share Planning VOIP 2006 - 2011**. Whitepaper **Siemens Communications Mercosur**. Divulgado em: Dez. de 2006.

[9] Recomendação H.323 do ITU-T International Telecommunication Union – Telecom Standardization ITU-T Rec. H323. **Visual Telephone Systems and Equipment for Are Networks which Provide a Non-Guaranteed Quality of Service**. Disponível em: <<http://www.itu.int/rec/T-REC-H.323/e>>. Acesso em: Nov. de 2006.

[10] ITU-T E. 164, **The International public telecommunication numbering plain**. Disponível em: <<http://dret.net/biblio/reference/e164>>. Acesso em: Nov de 2006.

[11] José Carlos Peixoto de Almeida, **Implementação e Gerência de uma Arquitetura de Voz sobre IP**. Monografia apresentada no curso de graduação em “Matemática” do Instituto de Matemática do UFGR em Set de 2003.

[12] Avaya Custom Edition, **SIP Communications For Dummies®** Publicado em set de 2006, por Wiley Publishing.

[13] SINNREICH, Henry; et all. **SIP beyond VoIP**. Disponível em <<http://www.amazon.com/SIP-Beyond-VoIP-Communications-Revolution/dp/0974813001>>. Acesso em: Dez. de 2004.

[14] IETF RFC 3015, **Megaco Protocol Version 1.0**

Disponível em: <www.infres.enst.fr/~rigault/Multiprovider_services.pdf>.

Acesso em: Nov. 2004

[15] Gustavo Dobkowski Longo, Artigo **Científico - Segurança da Informação**. Artigo Científico apresentado no curso de graduação de Sistemas de Informação da Faculdade de Ciências de Bauru.

Disponível em: <<http://www.firewalls.com.br>> Acesso em: Jan. 2007.

[16] Modulo Security, Definições e **Conceitos sobre Segurança da Informação**. Disponível em:

<<http://www.modulo.com.br/empresa3/noticias/ibiznet-020502.htm>>. Acesso em Jan. de 2007.

[17] Enciclopédia livre Wikipédia, **Conceitos de Segurança da Informação**.

Disponível em:

<http://pt.wikipedia.org/wiki/Seguran%3%A7a_da_informa%C3%A7%C3%A3o>. Acesso em: Jan. de 2007

[18] Ibiznet, **Guia de Segurança do Ibiznet**. Disponível em:

<<http://www.ibiznet.com.br/secg/>>. Acesso em Jan. de 2007.

[19] KUHN, D. Richard, **Security Considerations for Voice Over IP Systems**, National Institute of Standards and Technology. Jan. de 2005.

[20] Series Standard, **A Primer on the T.120**. Documento Disponível em:

<<http://www.lotus.com/products/learnspace.nsf/95febc158ad081518525674c0065aa5f/cb3a67f9f86a93898525679900531dc7?OpenDocument>>. Acesso em: Out. de 2004.

[21] D. Richard Kuhn, Thomas J. Walsh, Steffen Fries, **Security Considerations for Voice over IP Systems** - NIST SP 800-58

Publicação: 800-58. Documento de abril de 2004.

[22] Cisco Systems, **Call Manager Denial of Service**. Disponível em: <http://www.cisco.com/en/US/products/products_security_advisory09186a00805e8a55.shtml>. Acesso em: Jan. de 2007.

[23] Security Focus, **Eavesdropping in VOIP**. Disponível em: <<http://www.securityfocus.com/print/infocus/1862>>. Acesso em: Jan. de 2007.

[24] Internet Security System, **Alerta para os Perigos do VOIP**. Disponível em: <http://www.iss.net/about/press_center/releases/pr_30868.html>. Acesso em: Jan. de 2007.

[25] Teleco Informática e Telecomunicações, **Segurança VoIP - Conceitos e Nomenclatura**. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialsegvoip/pagina_2.asp> Acesso em: Jan. de 2007.

[26] Dígito Tecnologia, **Glossário Tecnológico**. Disponível em: <http://www.portaldigitro.com.br/glossario_digitro.php>. Acesso em: Jan. de 2007.

[27] Revista Info, **Phishing por VOIP**. Disponível em: <http://info.abril.com.br/corporate/edicoes/38/conteudo_187750.shtml>. Acesso em Jan. de 2007.

[28] Asterisk VOIP News, **Security experts taps VOIP as new Malware Target**. Disponível em: <http://www.asteriskvoipnews.com/voip_security/security_expert_taps_voip_as_new_malware_target.html>. Acesso em Jan. de 2007.

[29] Planet Telephony, **SIP Digest Authentication (MD5)**. Disponível em: http://www.planet.com.es/index.php?option=com_content&task=view&id=99&lang=pt>. Acesso em Jan. de 2007.

[30] Attachmate, **Túneis Seguros**. Disponível em: <http://br.attachmate.com/pt-BR/TechTalks/Secure+Tunnels.htm>>. Acesso em: Jan de 2007.

[31] CliConnect Internet Telephony, **Análise de desempenho de tráfego VOIP utilizando o protocolo IP**. Disponível em: <http://www.clicconnect.com/br/Artigos/AnalDesempTrafego/AnalidesemptrafVolP5.html>>. Acesso em: Jan. de 2007.

[32] Vocal Technologies LTDA, **SRTP Secure Real-Time Transport Protocol**. Disponível em: <http://www.vocal.com/srtp.html>>. Acesso em: Jan. de 2007.

[33] IETF RFC 3893, **Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format**. Disponível em: <http://www.rfc-archive.org/getrfc.php?rfc=3893>>. Acesso em: Jan. de 2007.

[34] IETF RCF 3325, **Private Extensions to the Session Initiation**. Disponível em: <http://www.zvon.org/tmRFC/RFC3325/Output/chapter9.html>>. Acesso em: Jan. de 2007.

[35] D. Richard Kuhn, Thomas J. Walsh, Steffen Fries, Security Considerations for Voice Over IP Systems - **Recommendations of the National Institute of Standards and Technology**.

[36] McAfee Network Protection, **Appliances de IPS para Rede McAfee IntruShield**. Disponível em:

<http://www.mcafee.com/br/enterprise/products/network_intrusion_prevention/intrushield_network_appliances.html>. Acesso em: Jan. de 2007.

[37] Cisco Systems Whitepaper, **Securing Your Network for IP Telephony**

Disponível em:

<http://www.cisco.com/application/pdf/en/us/guest/netsol/ns391/c654/cdccont_0900aec801e6159.pdf>. Acesso em: Jan. de 2007.

[38] Computer World, Medidas **defensivas protegem servidores de voz**.

Disponível em:

<http://computerworld.uol.com.br/seguranca/2006/07/07/idgnoticia.2006-07-07.7352822093/IDGNoticia_view>. Acesso em: Jan. de 2007.

[39] Julio Battisti, **CONHECENDO O ISA SERVER 2000**. Disponível em:

<<http://www.juliobattisti.com.br/tutoriais/breinerqueiroz/isaserver2k001.asp>>. Acesso em Jan. de 2007.

[40] IBM Resilience, **Segurança nos Centros de Dados: Resilience, Novidades**. Disponível em:

<http://www-1.ibm.com/services/pt/its/ITSNewsletterMar_Abr2004Edicao.pdf>. Acesso em Jan. de 2007.

[41] IBM Educação, **Solução de redes convergentes**. Disponível em:

<http://www.ibm.com/br/industries/education/solution/networking_3.phtml>. Acesso em Jan. de 2007.

[42] Voip Center - **VoIP, Segmentação da Comunicação**. Disponível em:

<<http://www.voipcenter.com.br/modules/news/article.php?storyid=1788>>. Acesso em Jan. de 2007.

[43] Debian – **Configuração de Rede Endereços Ip / Mac Address**. Disponível em: <<http://www.debian.org/doc/manuals/reference/ch-gateway.pt-br.html>>. Acesso em Jan. de 2007.

[44] RFC-1918 **Address Allocation for Private Intranets**. Disponível em: <<http://www.gnutellaforums.com/archive/index.php/t-6124.html>>. Acesso em Jan. de 2007.

[45] Enciclopédia livre Wikipédia, **Definição de Senhas**. Disponível em: <http://pt.wikipedia.org/wiki/Seguran%C3%A7a_da_informa%C3%A7%C3%A3o>. Acesso em: Jan. de 2007

[46] Microsoft Technet Brasil, **Aviso de segurança de 5 minutos - Segurança física básica**. Disponível em: <<http://www.technetbrasil.com.br/Artigos/Seguranca/AvisoSeguranca/203.asp>>. Acesso em: Jan. de 2007.

[47] Convergência Digital – **Quanto custa o seu alô?**. Disponível em: <<http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?inford=5505&sid=26>>. Acesso em: Jan. de 2007.

[48] GPR, **Document Actions VPN Virtual Private Network**. Disponível em: <<http://www.gpr.com.br/cursos/vpn>>. Acesso em Jan. de 2007.

[49] Microsoft Technet Brasil, **Configurar Segurança de Acesso Remoto**. Disponível em: <<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/pt-br/library/ServerHelp/d12a01a4-1c3e-472b-901d-2d200816bb25.mspx?mfr=true>>. Acesso em: Jan. de 2007.

GLOSSÁRIO

Aplicações: Softwares que proporcionam recursos adicionais às plataformas de comunicação convergentes. Por exemplo, aplicações de *unified messaging* ou aplicações para soluções de *contact center*. As aplicações geralmente são instaladas em servidor que se comunica pela rede IP ou interface serial com a plataforma, trocando informações sobre as ligações nesta realizadas ou efetuando a inteligência de encaminhamento das chamadas.

ARP: *Address Resolution Protocol*. Protocolo utilizado para mapear um endereço IP para um endereço físico (endereço MAC) conhecido na LAN.

Contact center: Aplicação preparada para oferecer atendimento por diversos meios de comunicação, como o telefone e e-mail. Os *contact centers* podem utilizar mecanismos que possibilitam o contato direto entre o chamador e os agentes enquanto o usuário estiver conectado a Internet, chats (conversação on-line com agentes), e pedidos para contatos telefônicos posteriores disparados por meio de e-mail.

Caller Identity Spoofing: Termo utilizado para indicar a utilização indevida de um *login* de um usuário por um *hacker*, que faz-se passar por outra pessoa.

Criptografia: Processo de proteção de dados que o codifica (criptografando) num formato não compreensível através de algoritmos de *software* ou *hardware*. Somente quem possui a “chave” secreta pode decodificar a mensagem.

Contingência: Situação excepcional decorrente de um desastre.

Convergência: União dos mundos de voz, dados e imagem. O termo convergência tem sido amplamente empregado pelo setor de tecnologia. Sua aplicação designa a união dos mundos de voz, dados e imagem para uma mesma plataforma de comunicação, com todos os recursos e facilidades que a nova tendência possibilita.

CTI: *Computer, Telephony e Integration* - Integração Computador e Telefonia. Soluções que integram centrais telefônicas e sistemas de processamento de dados dentro de um mesmo sistema (usado principalmente em *call centers*).

DG: Distribuidor Geral - É o local em uma instalação telefônica onde são feitas as interligações entre os diversos cabos que compõem o sistema telefônico.

DHCP: *Dynamic Host Configuration Protocol* - Protocolo de configuração de *Host* Dinâmico. Atribui dinamicamente endereços IP para dispositivos de rede.

DoS: *Denial of service* - Negativa de serviço. Tipo de ataque que envia um grande número de pacotes a um dispositivo de rede com objetivo de retirá-lo de serviço.

Ethernet: Padrão de comunicação em redes locais que opera em par trançado ou cabo coaxial em velocidade de até 10 ou 100 Mbps.

Firewall: Sistema desenvolvido para prevenir acessos não autorizados na Internet ou para redes privadas. Pode ser implementado em *hardware* ou *software* ou em combinação de ambos.

Gateway: Equipamento ou ponto de entrada e saída de uma rede de comunicação. Trata-se de um nó de rede que traduz pacotes de informação

entre duas redes incompatíveis, permitindo, por exemplo, que componentes não-IP tenham acesso à rede IP.

Hash: Algoritmo usado para verificar a integridade das informações transmitidas. Analisa os dados enviados e cria uma chave associada. Na recepção é criada uma nova chave com base nos dados recebidos e compara com a chave gerada inicialmente.

ICMP: *Internet Control Message Protocol*. Trata-se de um protocolo para controle de mensagem e erros entre um servidor e um gateway para a internet.

IEEE: *Institute of Electrical and Electronics Engineers*, entidade internacional responsável pela definição de diversos padrões para comunicações entre redes.

IP: *Internet Protocol* - Protocolo de Internet. Pacote de protocolos de comunicação mais utilizado na internet, que permite endereçar um pacote e colocá-lo no sistema.

IPS: *Intrusion Prevention System* - Sistema de Prevenção de Intrusão. Aplicativo usado para detectar intrusões dentro da rede e responder prontamente a esses ataques.

IP-Trunking: Interligação de canais de voz entre plataformas através da tecnologia VOIP.

LAN: *Local area networks* - Conceito que define as interligações entre computadores que se encontram em um mesmo prédio. As tecnologias mais utilizadas para as LANs são: *Ethernet*, *Fast Ethernet*, FDDI e ATM.

Logon: É um processo para identificação em um sistema ou rede de computadores. Toda vez que você se conecta a algum sistema este processo se realiza, sendo geralmente composto de duas etapas: primeiro você fornece o nome através do qual você é conhecido na rede (*username*), e depois informa a sua senha (*password*).

MAC: *Media Access Control Address* – Número que identifica o dispositivo de rede.

NAT: *Network Address Translation*. Processo responsável pela tradução de endereços IP válidos e não válidos, estes usados dentro de redes corporativas.

Payload: Carga útil de um pacote de dados IP. Um pacote de dados IP é constituído de um cabeçalho com informações de transmissão e de *payload* com os dados que realmente quer-se transmitir ao destino.

PBX: *Private Branch Exchange* – Central Telefônica.

PSTN: *Public Switched Telephone Network*. Rede pública de telefonia, rede provida pelas Operadoras de Telefonia.

Resilience: É a habilidade de recuperação rápida de um problema ou malfuncionamento. A propriedade de um material de voltar ao seu formato ou posição original após ter sido deformado, comprimido, estragado. Aplicado às Telecomunicações, significa manter os equipamentos sempre com alternativas de operação no caso de falhas de componentes ou infra-estrutura pela qual se comunica.

Roteador: Dispositivo que encaminha pacote de dados pela rede. O roteador é conectado pelo menos a duas redes, comumente a duas LANs ou WANs. Estão localizados em lugares onde duas ou mais redes se conectam.

Sinalização: Troca de informações necessárias ao estabelecimento, controle e operação de conexões de uma rede de comunicação (por exemplo, a rede pública de telefonia).

Switch: dispositivo que filtra e envia pacotes entre segmentos LAN, operando na camada 2, e as vezes camada 3, do modelo OSI de referência.

SYN flooding: Método que permite o usuário de um *client* hostil conduzir um ataque DoS (*Denial of Service*) enviando repetidamente pacotes SYN (sincronismo) para todas as portas no servidor utilizado endereços IP falsos.

Softphone: São terminais no formato de *software* para instalação no PC do usuário. Este *software* trará todas as facilidades de telefonia para o controle e comunicação pelo PC.

SSL: *Secure Socket Layer*. Protocolo desenvolvido pela Netscape para transmissão de documentos privados pela Internet. SSL trabalha pelo uso de uma chave privada para encriptar dados que são transferidos sobre uma conexão SSL. Ambos Netscape *Navigator* e Internet Explorer suportam SSL e muitos *Web sites* usam o protocolo para obter informações confidenciais de usuários, tais como número de cartão de crédito. Por convenção, páginas web que requerem uma conexão SSL começam com https: no lugar de http:. Outro protocolo para transmissão de dados seguros pela www é o HTTP seguro (S-HTTP). Ao invés do SSL, que cria uma conexão segura entre um cliente e um servidor, sobre o qual qualquer quantidade de dados pode ser enviado seguramente, S-HTTP é projetado para enviar mensagens individuais

seguramente. SSL e S-HTTP podem ser tanto tecnologias complementares quanto competitivas. Ambos protocolos foram aprovados pelo Internet Engineering Task Force (IETF) como um padrão.

TDM: *Time Division Multiplexing* - Multiplicação por Divisão de Tempo. Técnica em que um mesmo canal é usado por vários usuários, um por vez. Em outras palavras, cada usuário tem ao seu dispor toda a largura de banda do canal, durante certo tempo. É a base tecnológica da atual rede pública de telefonia.

VLAN: *Virtual Local Area Network*. Padrão que permite a segmentação em LAN virtuais, ou seja, dispositivos conectados aos mesmos *switches*, porém sem acesso a dispositivos alocados em outras VLANs.

VOIP: *Voice over IP* - Voz sobre IP - Tecnologia que permite a transmissão de voz por uma rede IP. Isso pode significar todo um sistema de telefonia trafegando pela Internet.

Vomit: *Voice Over Misconfigured Internet Telephones*. Técnica para captura de pacotes de voz e conversão para um formato de áudio conhecido. Permite o ataque através do grampo IP.

VPN: *Virtual Private Network* - Rede privada virtual - Rede privada virtual para uso exclusivo dos usuários de uma empresa, para que se conectem a ela de qualquer parte do mundo. Funciona como uma rede privada, com a diferença de que trafega dados sobre a infra-estrutura da própria Internet ou de uma rede pública de dados.

WAN: *Wide Area network*.