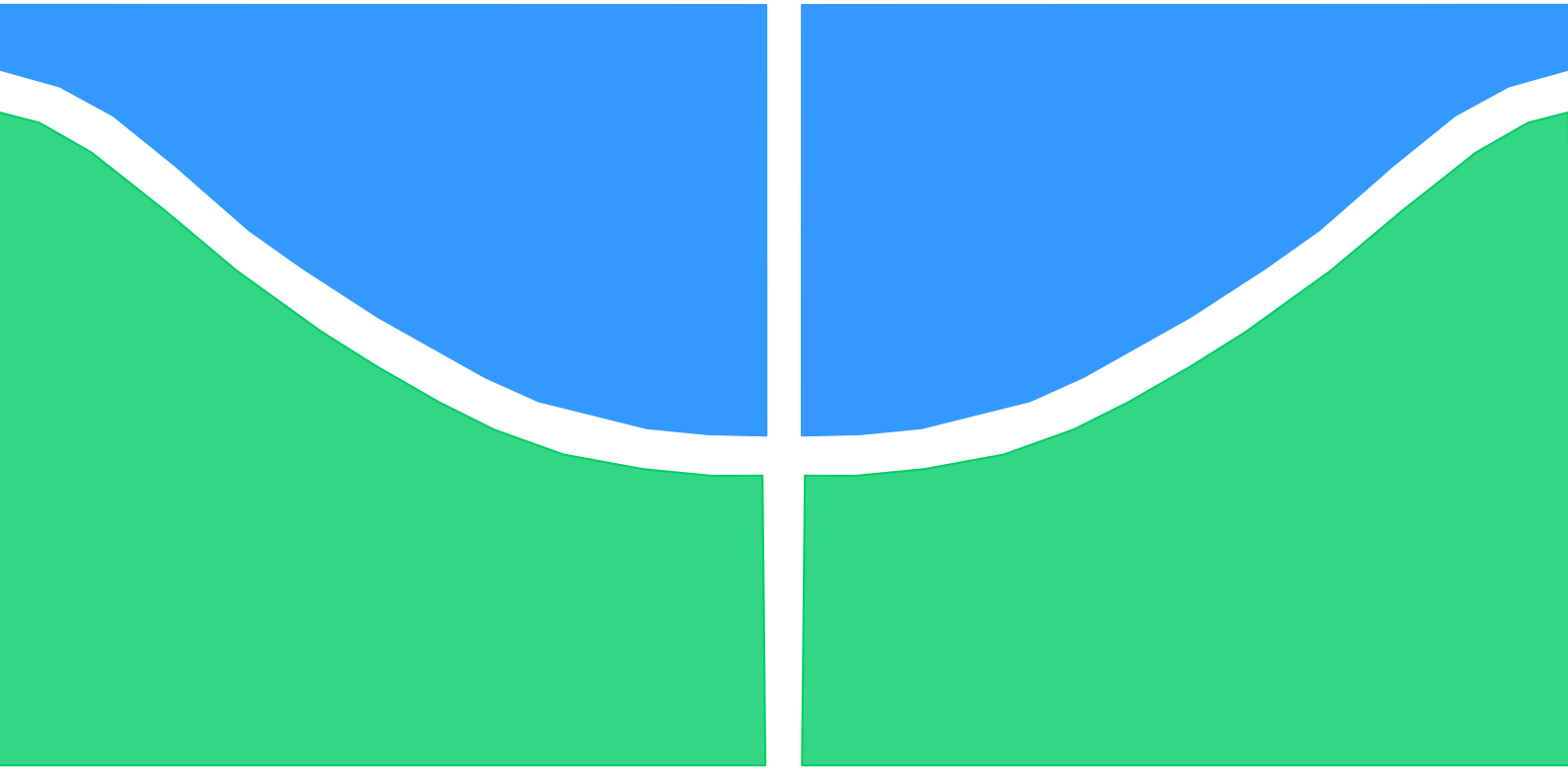


TRABALHO DE GRADUAÇÃO

ANÁLISE DOS ASPECTOS DE SEGURANÇA DA INFORMAÇÃO EM UM AMBIENTE DE COMUNICAÇÕES UNIFICADAS

Fernando de Britto e Silva
Silvio Mário Cândido de Jesus Júnior

Brasília, abril de 2013

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

TRABALHO DE GRADUAÇÃO

ANÁLISE DOS ASPECTOS DE SEGURANÇA DA INFORMAÇÃO EM UM AMBIENTE DE COMUNICAÇÕES UNIFICADAS

Fernando de Britto e Silva
Silvio Mário Cândido de Jesus Júnior

Relatório submetido como requisito parcial para obtenção
do grau de Engenheiro de Redes de Comunicação

Banca Examinadora

Prof. Edgard Costa, UnB/ Dep. _____

Prof. José Edil Guimarães de Medeiros, UnB/ Dep. Engenharia Elétrica _____

Eng. Pedro Paulo Mendes, UnB _____

Dedicatórias

Dedico este trabalho primeiramente a Deus por sempre estar me dando forças em minha caminhada. Dedico também a toda minha família que é meu principal suporte, especialmente a minha mãe Mary, minha mais importante companheira e ao meu pai Silvio, que me ensinou muitos dos valores que tenho hoje. E por último, mas não menos importante, a minhas irmãs Susanne e Karoline, com as quais venho dividindo ano após ano todas as alegrias e angústias pelas as quais passei e aos mais novos integrantes da família, meus sobrinhos Tiago e Felipe – que também é meu afilhado – e a minha afilhada Júlia, que nasceram para iluminar ainda mais nosso lar.

Silvio Mário Cândido de Jesus Júnior

A todos os que participaram da minha formação como pessoa e como profissional, dedico este trabalho. Dentre todos que se envolveram nesse processo dedico especialmente aos meus amados pais, Orlange e Bartolomeu por serem sempre as pessoas que me guiaram e me ajudaram em todas as situações da minha vida e sempre serão meus maiores mestres. Dedico ainda à minha amada vó e aos meus irmãos Hugo e João pelo apoio que sempre me concederam, além dos meus outros irmãos Larissa, Fábio e Marcus e minha outra mãe Rogéria por me demonstrar apoio incondicional sempre que preciso.

Fernando de Britto e Silva

Agradecimentos

Agradeço a todos os professores que formaram a minha maneira de pensar e enxergar o mundo. Agradeço ao meu orientador pelos valiosos conselhos e direcionamentos, pela paciência, pela atenção, pelo suporte e ajuda no decorrer deste trabalho.

Fernando de Britto e Silva

Agradeço a todos os professores que contribuíram para minha formação acadêmica, de modo especial aqueles que ministraram matérias correlatas com o assunto deste trabalho de graduação e ao nosso orientador que foi fundamental para a concretização deste. Agradeço também aos envolvidos no laboratório da Cisco em Brasília, que foram extremamente pacientes e disponíveis no uso do seu ambiente.

Silvio Mário Cândido de Jesus Júnior

RESUMO

O presente texto apresenta um estudo dos aspectos de segurança da informação em comunicações unificadas. Como todo estudo técnico-científico deve ser conduzido, é necessário criar uma base teórica antes do estudo de um caso prático e isso é feito visando à explicação dos conceitos mais importantes tanto de segurança da informação e sua tríade – confidencialidade, integridade e disponibilidade – quanto de comunicações unificadas. São apresentadas as principais definições que regem todo o universo de comunicações unificadas, bem como os aspectos de segurança que servem de ferramenta para proteção de todo tipo de comunicação. Feita essa revisão de definições, é possível partir para um estudo mais focado. Esse foco é dado no ambiente abordado no estudo de caso e a análise é feita seguindo o Processo de Gestão de Riscos de Segurança da Informação presente na norma ABNT NBR 27002:2005. O estudo é guiado para encontrar uma zona de convergência entre todos os tópicos – segurança da informação, comunicações unificadas e gestão de riscos – identificando os pontos de vulnerabilidades e as possíveis ameaças que explorariam esses pontos e propondo um conjunto de métricas que sirvam como instrumento de proteção para a rede. Do ponto de vista técnico, o trabalho serve para os profissionais e gestores de risco em tecnologia da informação que necessitarem de uma análise na área de comunicações unificadas.

Palavras-chave: comunicações unificadas, telefonia IP, VoIP, segurança da informação, gestão de riscos

ABSTRACT

This paper presents a study of the information security aspects on unified communications. Like all technical and scientific studies should be conducted, it is necessary to create a theoretical basis before the study of a practical case and it is done in order to explain the most important concepts of both information security and its triad – confidentiality, integrity and availability – as unified communications. It presents the main definitions that govern the entire universe of unified communications, and security aspects that serve as tool for protection of all types of communication. Following this review of definitions, you can go for a more focused study. This focus is given to the environment addressed in the case study and analysis is done following the Risk Management Process Safety Information present in standard ISO/IEC 27002:2005. The study is guided to find a zone of convergence between all topics - information security, unified communications and risk management - identifying points of vulnerabilities and potential threats that exploit these points and proposes a set of metrics that serve as an instrument protection for the network. From a technical standpoint, the work serves for professionals and risk managers in information technology who require an analysis in the area of unified communications.

Keywords: unified communications, IP telephony, VoIP, information security, risk management

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ACK	*ACKnowledgement*
AH	*Authentication Header*
API	*Application Programming Interface*
ARP	*Address Resolution Protocol*
ASA	*Adaptative Security Appliance*
ATA	*Analog Telephone Adapter*
ATM	*Asynchronous Transfer Mode*
bps	*bits per seconds*
BYOD	*Bring Your Own Device*
CA	*Certificate Authority*
CAPF	*Certificate Authority Proxy Function*
CEBP	*Communications-Enable Business Process*
CIA	*Confidenciability, Integrity and Avaliability*
CID	Confidencialidade Integridade e Disponibilidade
CIPC	*Cisco IP Communicator*
CNAME	*Canonical Name*
CODEC	Codificador/Decodificador
CPA	Centrais de Programa Armazenado
CPE	*Customer Premises Equipment*
CSP	Código de Seleção de Prestadora
CT	Central Telefônica
CTL	*Certificate Trust List*
CUCM	*Cisco Unified Communications Manager*
CUPS	*Cisco Unified Presence Server*
DARPA	*Defense Advanced Research Projects Agency*
DDD	Discagem Direta a Distância
DDI	Discagem Direta Internacional
DG	Distribuidor Geral
DHCP	*Dynamic Host Configuration Protocol*
DiffServ	*Differentiated Services*
DNS	*Domain Name Server*
ESP	*Encapsulating Security Payload*
FDDI	*Fiber Distributed Data Interface*

FDM	*Frequency Division Multiplex*
FEC	*Forward Error Correction*
HTTP	*Hyper Text Transfer Protocol*
Hz	Hertz
IDS	*Intrusion Detection System*
IETF	*Internet Engineering Task Force*
IM	*Instant Message*
IMP	*Instant Message and Presence*
IntServ	*Integrated Services*
IP	*Internet Protocol*
IPC	*IP Communications*
IPDC	*Internet Device Control Protocol*
IPSec	*IP Security Protocol*
IPT	*Internet Protocol Telephony*
ISDN	*Integrated Service Digital Network*
ITC	*Information Technology and Communication*
ITU-T	*Telecommunication Standardization Sector of International Telecommunication Union*
IVR	*Interactive Voice Responce*
LAN	*Local Area Network*
LDC	*Local Dynamic Certificate*
LSC	*Local Session Controller*
MAC	*Media Access Control*
MCS	*Media Convergence Servers*
MCU	*Multi Control Unit*
MDS	*Multilayer Directors Switch*
MEGACO	*Media Gateway Control*
MGCP	*Media Gateway Control Protocol*
MOS	*Mean Opinion Score*
MS	*Microsoft*
NAT	*Network Address Translation*
NBR	Norma Brasileira
OSI	*Open Systems Interconnection*
PABX	*Private Automatic Branch eXchange*
PBX	*Private Branch eXchange*
PAT	*Port Address Translation*
PC	*Personal Computer*

PCM	*Pulse Code Modulation*
PD	Painel de distribuição
PDCA	*Plan – Do – Check – Act*
PIX	*Private Internet eXchange*
PLC	*Packet Loss Concealment*
PSTN	*Public Switched Telephony Network*
QoS	*Quality of Service*
RAS	*Registration, Admission and Status*
RDSI	Rede Digital de Serviços Integrados
RFC	*Request For Comments*
RMS	Rede Multiserviços
RR	*Receiver Report*
RSTP	*Rapid Spannig Tree Protocol*
RSVP	*Resource reSerVation Protocol*
RTCP	*Real Time Control Protocol*
RTFC	Rede de Telefonia Fixa Comutada
RTP	*Real Time Protocol*
RTPub	Rede de Telefonia Pública
SCCP	*Skinny Call Control Protocol*
SCN	*Switched Circuit Network*
SDP	*Session Description Protocol*
SGCP	*Simple Gateway Control Protocol*
SGSI	Sistema de Gestão de Segurança da Informação
SI	Segurança da Informação
SIP	*Session Initiate Protocol*
SMS	*Short Message Service*
SMTP	*Simple Mail Transfer Protocol*
SNMP	*Simple Network Management Protocol*
SPIT	*Spam over IP Telephony*
SRTP	*Secure Real Time Protocol*
SSL	*Secure Sockets Layer*
SYN	*SYNchronize*
TCP	*Transport Control Protocol*
TDM	*Time Division Multiplex*
TFTP	*Trivial File Transfer Protocol*
TLS	*Transport Layer Security*
TTel	Terminal Telefônico

TUP	Terminal de Uso Público
UA	*User Agent*
UAC	*User Agent Client*
UAS	*User Agent Server*
UC	*Unified Communications*
UCaaS	*Unified Communications as a Service*
UCC	*Unified Communication and Colaboration*
UDP	*User Datagram Protocol*
UM	*Unified Messaging*
URL	*Uniform Resource Locator*
VAD	*Voice Activity Detection*
VLAN	*Virtual Local Area Network*
VoATM	*Voice over ATM*
VoFR	*Voice over Frame Relay*
VoIP	Voice over Internet Protocol
VOMIT	*Voice over Misconfigured Internet Telephones*
VPN	*Virtual Private Network*
VRF	*Virtual Routing and Forwarding*
WAN	*Wide Area Networks*
wav	*Waveform Audio File Format*
XMPP	eXtensible Messaging and Presence Protocol

1 INTRODUÇÃO

Um capítulo introdutório se faz necessário para situar o leitor acerca do trabalho que conduzido, apontando assim os aspectos gerais do assunto, importância do mesmo, bem como o que se deseja alcançar com o trabalho de uma forma geral. A maneira com que foi conduzido o estudo também será mostrada neste capítulo através da metodologia.

1.1 ASPECTOS GERAIS

A crescente demanda por fluxos de informação e processos cada vez mais rápidos e complexos trazem constantes desafios para empresas e pesquisadores de Tecnologia da Informação. Desde seu surgimento, em meio a Guerra Fria, voltada inicialmente para a comunicação militar e acadêmica, até sua popularização a partir da década de 1990, a internet ganha cada vez mais importância para o mundo corporativo, tanto influenciando o modo como as pessoas se comunicam como sendo influenciada por essas demandas. O usuário, que no início da popularização da internet era apenas um consumidor do descentralizado conteúdo dos grandes portais, passou a ser o principal produtor de dados e a cada vez mais compartilhar informações e experiências na grande rede, resgatando o universo colaborativo dos primórdios da internet acadêmica.

Hoje, atividades do dia a dia já não são mais realizadas como tempos atrás, como por exemplo, pagar contas, alugar filmes etc. O tráfego de voz não foge a esse comportamento. As primeiras centrais telefônicas datam do fim do século XIX e desde então evoluíram bastante até chegar às centrais digitais atuais, que mesmo assim não conseguem suprir as necessidades de comunicação atual. O transporte de voz sobre uma rede de dados baseada em protocolo IP (*Internet Protocol*) é uma alternativa para o sistema de comutação de circuitos dessas centrais.

Dentro deste cenário, cabe-se definir alguns conceitos: VoIP, Telefonia IP e por fim o Comunicações Unificadas.

Voice over IP (VoIP) pode ser entendida como uma solução *toll-bypass*, em que centrais telefônicas convencionais podem ser conectadas através da rede IP, o que se torna particularmente atrativo sob o ponto de vista econômico para ligações do tipo DDD e DDI. Para este cenário faz-se necessária a adição de placas de voz aos roteadores existentes. Note-se aqui que a voz é simplesmente transportada sobre a rede IP e que as tarefas de codificação e compressão da voz são executadas pelos roteadores com placa de voz, que neste ambiente operam como *gateways* entre o mundo da telefonia tradicional, representado pelos PABXs, e o mundo IP, associado aos roteadores.

IP Telephony (IPT) ou simplesmente Telefonia IP refere-se ao transporte tanto de voz quanto de pacotes de controle sobre a infraestrutura de redes baseadas em IP. Esse transporte de informação em mais de uma forma, exige da rede elementos que sejam responsáveis pelas tarefas de processamento de chamadas e os telefones IP (*IP Phones*), que se apresentam como a principal interface do usuário com a rede convergente.

Juntamente com o advento da Telefonia IP, outras tecnologias e demandas foram introduzidas nas redes IP, fazendo com que estas estivessem sempre como alvo de grandes investimentos por parte das empresas, ampliando a infraestrutura para comunicação de dados baseada em IP como protocolo de camada 3, ou a chamada L3. Com a convergência dos tráfegos de dados, voz e vídeo em uma infraestrutura de rede única e o desprendimento da internet do *desktop* físico, seja pela mobilidade oferecida pelos *smartphones* e *tablets* ou mais recentemente pela introdução de nós de internet em praticamente tudo conhecido, a chamada *Internet of Everything* (ou, em português, a Internet de todas as coisas), que foi surgindo o conceito de Comunicações Unificadas (UC, *Unified Communications*).

A integração de vídeo, voz e dados em uma plataforma unificada e multisserviços depende da adoção de alguns parâmetros que possam garantir os requisitos mínimos para o funcionamento ótimo desses tipos de mídia, observando-se principalmente exigências específicas do tráfego de voz e streaming de

vídeo. Por exemplo, adotando medidas que visem a redução dos atrasos de propagação e manipulação e a garantia de uma largura de banda mínima, pode-se praticamente tornar indiferenciável, do ponto de vista do transporte, o tráfego de pacotes de dados comuns nas redes IP ou de voz.

A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente. Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. Quando se trata do transporte de algo tão valioso quanto a informação, seja ela na forma de pacotes de dados ou voz, é imprescindível que se pense no quão seguro será esse transporte. Aí entra um conceito muito abrangente, a Segurança da Informação (SI). No geral SI se estabelece sobre três pilares, a confidencialidade, a integridade e a disponibilidade. A confidencialidade é a garantia de que a informação é acessível somente por pessoas autorizadas. A disponibilidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário. Por fim a integridade é a salvaguarda da exatidão da informação e dos métodos de processamento.

Usando esses conceitos, é possível fazer uma metáfora bem simples para o caso da comunicação por voz. Por exemplo, os participantes de uma conversa particular importante – uma transmissão de informação importante – devem se preocupar com alguém escutando a conversa, pois o assunto só pode ser conhecido por quem está de fato participando da conversa (confidencialidade). Os envolvidos devem atentar para o fato de que sempre deve existir alguém que possa manter a comunicação, ou seja, conversar, caso contrário a mesma acaba (disponibilidade). Por último, mas não menos importante, o assunto que está em pauta não pode ser modificado uma vez que isso acarretaria em uma conversa errada onde os participantes se referem a assuntos completamente distintos (integridade).

Assim, propor um conjunto de práticas que norteiem uma implementação segura de comunicações unificadas é algo primordial para o estabelecimento dessa tecnologia.

1.2 OBJETIVOS

1.2.1 OBJETIVO GERAL

O objetivo geral do presente trabalho de conclusão de curso a elaboração de um estudo sobre como a Segurança da Informação pode ser aplicada à tecnologia de comunicações unificadas, principalmente Telefonia IP, de forma a garantir confidencialidade, integridade e disponibilidade a informação trafegada sem que haja perda de desempenho no canal de comunicação envolvido.

1.2.2 OBJETIVOS ESPECÍFICOS

- Conceituar Segurança da Informação e Comunicações Unificadas, ou mais especificamente, Telefonia IP;
- Analisar ameaças e vulnerabilidades inerentes ao tipo de comunicação em questão;
- Identificar essas ameaças e vulnerabilidades em um caso específico de aplicação em um ambiente de teste;
- Agregar os resultados obtidos de modo que se possa propor uma solução de Segurança da Informação para VoIP.

1.3 JUSTIFICATIVA

Partindo do princípio que garantir segurança a informação transportada em uma rede, a proposição de um estudo pautado neste aspecto tem fundamental justificativa. Levando-se em consideração cada um dos objetivos propostos, tem-se na conceituação dos tópicos envolvidos um primeiro passo para a

perfeita compreensão acerca de como este tipo de comunicação deve ser tratada para garantir a tríade CID (Confidencialidade, Integridade e Disponibilidade). Assim, deve-se conceituar tanto o que é Segurança da Informação, seus desdobramentos em ameaças e vulnerabilidades entre outros, como também a tecnologia analisada. Nesse contexto, faz-se necessária um pequeno levantamento histórico e evolutivo de como o mercado tecnológico migrou do sistema de comunicação analógico único e exclusivamente de telefonia para o modelo de comunicações unificadas que se tem hoje.

Ainda nesta abordagem, é importante fazer um levantamento, com base nas normas de SI vigentes, de como este tipo de ambiente pode estar relacionado com os aspectos de Segurança da Informação, identificando as principais vulnerabilidades e ameaças as quais estão sujeitas e de que forma estas estão presentes quando lidamos com um caso específico de estudo.

Para finalizar o estudo, tem-se a necessidade de propor medidas que garantam confidencialidade, integridade e disponibilidade aos ativos envolvidos em comunicações unificadas.

1.4 METODOLOGIA

Pode-se dividir a metodologia aplicada em três fases: levantamento das referências bibliográficas, análise e proposição da solução.

1.4.1 PESQUISA BIBLIOGRÁFICA

Manter-se informado em meio a uma abundância de fontes de informação vem se tornando, paradoxalmente, cada vez mais problemático. A quantidade de informação desnecessária, e muitas vezes incorreta, que está ao alcance das mãos nos leva a tratar o processo de levantamento de referências bibliográficas ainda com mais importância. É preciso, portanto, garantir que em meio ao crescente quantitativo de fontes observadas tenha-se o cuidado de triá-las de modo a garantir a qualidade da pesquisa, cuidando para que estas fontes lhes agreguem algum valor.

A pesquisa foi desenvolvida com foco nas normas da ABNT para SI e em monografias e outros estudos científicos sobre os temas decorridos. Porém, outras fontes de informação também foram utilizadas, mesmo que de modo mais cauteloso para garantir a qualidade da pesquisa, observando-se principalmente o currículo dos autores dos artigos.

1.4.2 ANÁLISE

Levantamento bibliográfico feito, é hora de interligar os conceitos e fazer a análise descrita nos objetivos do presente trabalho. A análise será feita tanto com base no material obtido com a pesquisa como na análise subjetiva do caso de uso adotado.

1.4.3 PROPOSIÇÃO DA SOLUÇÃO

Como resultado da análise feita anteriormente, tem-se uma série de insumos que serão agregados de modo a formar um conjunto conciso de boas práticas recomendáveis quando queremos garantir a tríade CID em um ambiente como o estudado.

2 REVISÃO DA LITERATURA

Encontra-se neste capítulo uma descrição geral do histórico das redes de telefonia mostrando desde onde surgiram e as tecnologias que utilizavam até a atual situação das comunicações unificadas. Um apanhado geral do TCP/IP se faz necessário para se entender o transporte de voz sobre IP e será abordado também neste capítulo. Por fim, como este é um trabalho que busca elucidar os aspectos de Segurança da Informação dentro da área de UC, primeiro serão mostradas as principais definições de segurança da informação para que no próximo capítulo se possa realizar um estudo mais detalhado da relação entre segurança da informação e as comunicações unificadas.

2.1 REDE DE TELEFONIA FIXA COMUTADA

Com o surgimento de sistemas móveis de comunicação, celulares, por exemplo, o termo "telefonia fixa" passou a identificar os sistemas telefônicos que não apresentam mobilidade para seus terminais.

A rede de telefonia fixa pode ser definida como uma rede pública comutada de telecomunicações que serve de suporte à transferência entre pontos terminais da rede em locais fixos, de voz e de informação de áudio com largura de banda de 3,1 kHz (300 Hz – 3400 Hz).

Uma rede de telefonia fixa comutada (também chamada de RTFC) é composta por alguns elementos básicos:

- Terminal telefônico: aparelho utilizado pelo assinante do serviço. Da ótica do assinante, pode existir um sistema telefônico privado (como um PABX) para atender uma empresa ou um único terminal. O terminal é associado na maioria das vezes a um assinante do sistema telefônico, mas existem ainda os chamados Terminais de Uso Público (TUP's) ou "orelhões".
- Central telefônica: é o subsistema mais importante da rede de telefonia e tem a função de gerência, concentração, tarifação das chamadas pelos assinantes e distribuição.
- Rede de acesso: é responsável pela conexão entre os assinantes e as centrais. É formada pelo conjunto de cabos de assinantes e cabos troncos que atendem um local, assim como dutos, ferragens, postes etc.

2.1.1 CENTRAL TELEFÔNICA

A finalidade da central telefônica (CT) é fazer a comutação, ou seja, interconexão ou chaveamento de um assinante com outro. Em uma central digital, todo esse processo de comutação é realizado automaticamente através de processamento computadorizado. Uma CT tem algumas funções principais, tais como atendimento, recepção da informação, processamento da informação, teste de ocupação, interconexão, alerta, supervisão e envio de informação. Na década de 1980 surgiram as centrais de comutação totalmente eletrônicas, onde as funções lógicas de comando, controle e conexão são executadas por dispositivos eletrônicos. Essas centrais são conhecidas como Centrais de Programa Armazenado (CPA's) e possuem algumas vantagens:

- Flexibilidade: permite alterações e reconfigurações sem que a central seja desligada.
- Facilidades para os assinantes: discagem abreviada, identificação de chamadas, restrição de chamadas.
- Facilidades administrativas: mudanças de roteamento, relatórios detalhados, estatísticas.

- Facilidade de manutenção: menor índice de falhas.
- Qualidade de conexão: não são produzidos ruídos de comutação mecânica que afetam a qualidade.
- Custo menor: com um índice de manutenção mais baixo e uma maior eficiência em termos de serviços as CPA's oferecem uma ótima relação custo/benefício.

Quanto à aplicação, as centrais telefônicas podem ser classificadas em públicas ou privadas. As centrais privadas são utilizadas em empresas e outros setores nos quais existe uma demanda de alto tráfego de voz. Os aparelhos telefônicos ligados a uma central privada são chamados de ramais e os enlaces com a central pública local são chamados troncos. As centrais públicas por sua vez são classificadas de acordo com a abrangência e os tipos de ligações que efetuam:

- Central Local: atende os assinantes de uma determinada região. Cada central local possui um prefixo comum e quando o número de assinantes extrapola sua capacidade, novas centrais são criadas e interligadas através de um cabo tronco.
- Central Tandem: principal função é proporcionar o trânsito entre centrais locais ou interurbanas.
- Central Mista: possui a função local e a função tandem ao mesmo tempo.
- Central Trânsito: interliga dois ou mais sistemas locais, interurbanos ou sistemas de comutação com outros países.
- Sistema PBX (*Private Branch eXchange*): é um sistema de ramais telefônicos comutados dentro de uma rede local que permite um número limitado de usuários que compartilham as linhas externas da operadora de telefonia. A proposta desse sistema é economizar na compra linhas telefônicas para uma empresa. Esses sistemas são compostos por múltiplas linhas (tronco telefônico), linhas internas, um console de operação e um aparelho de gerência da comutação dentro do PBX e para fora.
- Sistema PABX (*Private Automatic Branch eXchange*): pode ser chamado de evolução do sistema anterior pois faz automaticamente a comutação telefônica em uma rede privada. Este sistema possui busca automática, conexão central com a rede pública, acesso à rede digital de serviços integrados, interface para rede de dados e acesso a discagem direta a ramal.

2.1.2 COMUTAÇÃO

Importante, também é saber como é feita a comutação dentro da RTFC. As Centrais Telefônicas utilizam a comutação de circuitos, diferente das redes de computadores, com uma taxa de transmissão de 64 Kbps em uma topologia em estrela com o elemento comutador no centro dessa estrela. Esse tipo de comutação na RTFC exige o estabelecimento prévio de conexão, o que implica em um tempo adicional que atrasa a transmissão. Um problema da comutação de circuitos é o de caso não se consiga estabelecer uma linha física para ser utilizada na transmissão, não há como garantir uma transmissão confiável, assim a transmissão de dados dentro de uma rede com comutação de circuitos é feita com taxas de transmissão menores.

2.1.3 SERVIÇO LOCAL DE TELEFONIA

O serviço local é prestado pela operadora que possui a Central Local e a rede de acesso que se conecta com o terminal do assinante. Se dois terminais fixos estão dentro de uma área geográfica contínua de prestação de serviços, esta é definida como área local e o serviço é considerado local. Se existirem duas operadoras que prestam serviços dentro da mesma área local, deverá necessariamente haver interconexão entre as redes para que seja possível a ligação local entre os assinantes das duas operadoras.

2.1.4 SERVIÇO DE LONGA DISTÂNCIA

É o serviço destinado à comunicação entre dois terminais fixos localizados em áreas locais diferentes dentro do território nacional ou localizados em países diferentes. Normalmente uma chamada de longa de distância envolve três operadoras, a que presta serviço local ao assinante que origina a chamada, a que presta serviço local ao assinante que recebe a chamada e a operadora de longa distância. A operadora de longa distância é selecionada chamada a chamada pelo assinante através do código de seleção de prestadora (CSP).

Após estas definições, pode-se criar um esquemático bem simples e ilustrativo de uma RTFC comum:

Figura 1 - Estrutura da RTFC (PALHARES NETO, 2010).

2.2 PROTOCOLO TCP/IP

O TCP/IP é a sigla de *Transfer Control Protocol* / *Internet Protocol* e se refere ao conjunto de protocolos utilizados na rede mundial de computadores. Inclui uma série de padrões que especificam como os computadores se comunicarão, ou seja, um protocolo, e cria convenções para interconectar redes e para o roteamento por meio dessas conexões. De uma forma simples, mesmo conectados à mesma rede, dois computadores não iriam se comunicar se não "falassem" a mesma língua.

O TCP/IP é resultado de um projeto da DARPA (*Defense Advanced Research Projects Agency* - Agência de Projetos de Pesquisa Avançada de Defesa) sobre a conectividade entre redes, no final dos anos 70. O TCP/IP é uma excelente plataforma cliente-servidor. O TCP está definido nos RCF's 793, 1122, 1323, 2018 e 2581.

A principal função do IP é transportar os datagramas de uma rede a outra na Internet. Por não ser um protocolo orientado a conexão, não possui mecanismos de retransmissão e nem dá garantia de uma transmissão ordenada e sem falhas de integridade da mensagem. De maneira simples, ele descarta um datagrama caso não tenha sido entregue ou se passar muito tempo "perambulando" pela Internet. É um protocolo vital para o funcionamento da Internet, pois utiliza os ditos "endereços IP" como base para o direcionamento dos datagramas. Cada computador ligado à Internet possui um ou mais números IP's, sendo que cada IP é exclusivo, o que evita o envio de um datagrama para o lugar errado.

Os endereços IP são compostos em 4 *bytes*, separados por pontos e se dividem em endereço de rede e endereço local. O endereço de rede se refere à rede principal e às subnets e é representado pelos três primeiros *bytes* do IP. A dificuldade em se tratar apenas com números, exigiu a criação de um mecanismo que facilitasse esse processo. Foi criado então o DNS (*Domain Name Server*), que associa um nome a cada número IP. A hierarquia comum do DNS é país – organização – máquina.

Segundo Kurose e Ross (2006), diferentemente do IP, dito um protocolo não-orientado a conexão, o TCP antes do processo de uma aplicação começar a enviar dados a outro, faz com que ambos antes "apresentem-se" (enviar segmentos prévios entre eles para que ambos possam estabelecer os parâmetros que serão utilizados para a transmissão de dados em questão). O TCP é responsável pelo controle dos procedimentos da transferência segura de dados. Essa "conexão" TCP não é como a conexão de uma rede de comutação de circuitos que normalmente utiliza um TDM (*Time Division Multiplex*) ou FDM (*Frequency Division Multiplex*) fim-a-fim. Essa conexão é ponto a ponto, isto é

entre um único remetente e um único destinatário. A transmissão *multicast* (de um remetente para vários destinatários em uma única operação de envio) não é possível com o TCP. A confiabilidade das transmissões via TCP é baseada no seu trabalho com números de reconhecimento sequenciais e positivos. O *host* origem transfere os dados na forma de octetos e cada octeto recebe um número em sequência. O *host* destino analisa esses números para garantir a ordem e integridade da mensagem.

Outro serviço importante que o TCP faz é o de controle de fluxo, que cria uma janela de transmissão ao *host* de origem e faz com que essa janela limite o número de bytes que é transmitido por vez. A possibilidade de atribuir valores diferentes para o tamanho da janela faz o controle de fluxo em si.

Como o TCP roda apenas nos sistemas finais, e não nos elementos intermediários, os roteadores e comutadores da camada de enlace não enxergam conexões, e sim datagramas. O TCP provê um serviço *full-duplex*, ou seja, para uma conexão estabelecida entre dois processos, os dados da camada de aplicação podem ir do *host* A para o B ao mesmo tempo em que os dados podem ir de B para A.

As ditas camadas da pilha de protocolos buscam fornecer uma abstração aos protocolos e serviços da estrutura de dados. O modelo TCP/IP não é o único existente, mas é um dos mais práticos e didáticos. O modelo OSI é o modelo padrão de rede, fazendo a divisão em sete camadas da pilha de protocolos, sendo elas: aplicação, apresentação, sessão, transporte, rede, enlace e física. O modelo TCP/IP de camadas divide a pilha de protocolos em quatro camadas, sendo elas: aplicação, transporte, inter-rede e interface de rede (física). É nítida a semelhança entre os dois modelos, mas é importante ressaltar suas diferenças. Na camada de rede do modelo OSI existe suporte tanto a comunicação orientada a conexão quanto a não orientada a conexão, diferentemente da camada de rede do TCP/IP que apenas suporta o modo orientado a conexão. Observando a camada de transporte, no caso OSI, apenas existe a opção de comunicação orientada à conexão, enquanto o TCP/IP suporta ambos os modos. O TCP/IP combina os aspectos das camadas de apresentação e de sessão dentro da sua camada de aplicação e combina as camadas físicas e de enlace do OSI em uma única camada (COMER e STEVENS, 1998).

A Figura (2) abaixo mostra o comparativo entre os modelos OSI e TCP/IP.

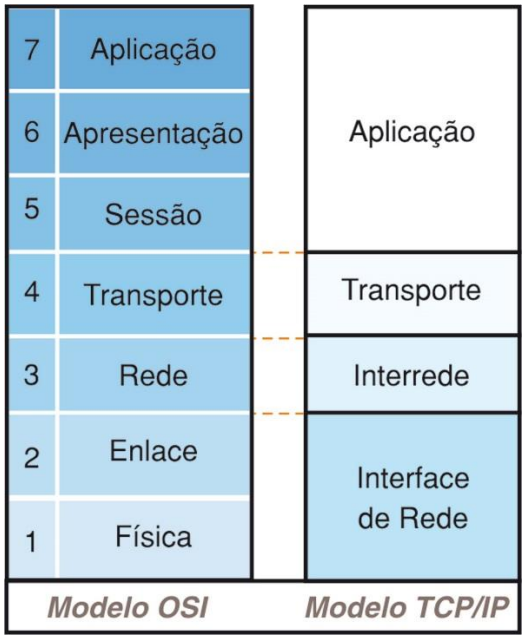


Figura 2 – Comparativo entre os modelos OSI e TCP/IP[1]

2.2.1 IPSEC

De acordo com a definição de Barbieri, Bruschi e Rosti (2002), o *IPsec* é um protocolo que fornece serviços de segurança para o tráfego IP, permitindo que um *host* configure um canal seguro IP com

[1] Figura modificada das apresentadas por Comer e Stevens (1998) para os modelos OSI e TCP/IP

qualquer par que deseja se conectar. Dependendo do nível de segurança exigido, os serviços fornecidos pelo *IPsec* são baseada em dois outros protocolos: um protocolo de autenticação (AH) e um combinado de criptografia e de autenticação (ESP). O primeiro protocolo fornece serviços tais como a integridade e autenticação de remetente, enquanto o segundo protocolo é encarregado da confidencialidade, entre outros serviços.

Para executar qualquer um desses algoritmos, os pares envolvidos na comunicação tem a necessidade de trocar um par de chaves secretas simétricas para poderem trocar mensagens e algoritmos criptográfico. O *IPsec* codifica a informação necessária para realizar AH e serviços ESP em dois cabeçalhos adicionais nos pacotes, chamados de cabeçalhos AH e ESP, respectivamente.

O *IPsec* pode operar de duas maneiras diferentes. Caso a comunicação segura for entre dois pontos diretamente conectados, o *IPsec* opera em modo de transporte e para o caso da comunicação ser entre dois gateways intermediários, em modo túnel.

Para aplicações de voz, confidencialidade é algo essencial e a autenticação *'in band'* se torna cara. Em sistemas VoIP, outra característica chave é que geralmente os *endpoint* são os pontos finais de criptografia. Portanto, a melhor escolha para proteger o tráfego de voz é usar o cabeçalho ESP em modo túnel.

2.3 VOZ SOBRE IP

O mundo corporativo atual faz o mercado pressionar as organizações e gerar uma necessidade de atualização baseada em novas ofertas de soluções ou até mesmo novos modelos de negócios. O mercado de telecomunicações, especificamente o caso das comunicações por voz, se insere nesse cenário, onde há constantemente o advento de novas soluções para todos os tipos de necessidades. Estas soluções trazem consigo um novo cenário onde sistemas de comunicação unificada, focados principalmente em conferências e vídeo, tem ganhado destaque. Ou seja, é o surgimento de uma tecnologia que possa transportar voz, vídeos e pacotes de dados pelo mesmo canal de comunicação, com diferentes dispositivos de acessos e a partir de qualquer localização geográfica.

Essa nova forma de comunicação é denominada *Voice over IP*, ou simplesmente pelo acrônimo VoIP, cujo aparecimento é totalmente justificado, uma vez que, com expressivo crescimento da internet, é natural que as mais diversas formas de comunicação sejam encapsuladas sob seu principal protocolo, o IP.

Alguns protocolos já utilizavam *Frame Relay* e/ou *ATM* para a transmissão de voz sobre redes de dados, porém somente na década de noventa é que o IP passou a ser utilizado para tal fim. Pode-se então, de forma simplificada, definir VoIP como sendo o processo de digitalização do áudio, seu consequente fracionamento em pequenas partes para a transmissão por uma rede IP e remontagem dos pacotes no destino, estabelecendo assim comunicação entre dois pontos de áudio. (PALHARES NETO, 2010)

O uso do VoIP vem sendo uma das grandes metas de investimentos por fornecedores de soluções e usuários de telecomunicações nos últimos anos. Esta tecnologia abre um novo horizonte para as possíveis aplicações integrando-se voz e dados num mesmo equipamento terminal de usuário, aproximando pessoas geograficamente distantes, aumentando a interatividade de aplicativos e diminuindo os custos de comunicação quando comparada às convencionais ligações telefônicas interurbanas.

2.3.1 CODECs

A transmissão de voz sobre redes de dados exigem alguns requisitos de banda de modo a minimizar principalmente atraso e perda de pacotes. Para isto, faz-se necessário adotar mecanismos de digitalização e compactação. São os chamados *CODECs*, que podem ser entendidos como um programa ou dispositivo com algoritmos capazes de converter o som (ou vídeo) analógico em sinais digitais e depois comprimi-los para diminuir seu tamanho, resultando em um arquivo que pode ser considerado um *trade off* entre qualidade, requisitos de banda e *delay*, cabendo ao administrador da rede escolher o *CODEC* a ser utilizado de acordo com esses requisitos. (ARAÚJO e BRAGA, 2009)

A primeira aplicação civil da codificação de um sinal de voz, ou seja, da digitalização de um sinal de modo a aperfeiçoar seu armazenamento e transmissão, data da década de 1970, onde as redes telefônicas utilizavam codificação PCM (*Pulse Code Modulation* – Modulação por Codificação de Pulsos), que consiste em 8.000 amostragens do sinal de voz contínuo, por segundo, representando o valor discreto amostrado em 8 bits, implicando na necessidade de um canal digital de 64 Kbps para transmissão de cada canal de voz. Este tipo de codificação procura reproduzir o sinal amostra por amostra, mantendo atraso e complexidade baixos, porém requerendo taxas de transmissão elevadas.

Com o passar dos anos esse processo de compressão da informação presente nas amostras do som foi sendo melhorado, de forma a explorar os modelos de produção da voz. Estas novas técnicas fazem a segmentação do sinal analógico em intervalos periódicos, para formação de quadros após a digitalização, diminuindo assim as taxas de transmissão.

Vários tipos de *CODECs* existem para diferentes tipos de aplicações. Aqueles que são voltados para VoIP, são otimizados à comprimir voz, com significativa redução de taxa de transmissão utilizada, comparado a transmissão de voz não comprimida. O som captado é comprimido e dividido em pequenas partes, que são coletadas e distribuídas em pacotes IP. O ITU-T (*Telecommunication Standardization Sector of International Telecommunication Union*) padronizou várias codificações ao longo dos anos. A Tabela (1) abaixo enumera os principais tipos de *CODECs*, e traz algumas informações relevantes a cerca deles.

Tabela 1 – Principais CODECs de áudio[2]

Padrão	Algoritmo	Taxa (kbps)	Largura de Banda (Hz)	MOS	Delay (ms)	Aplicação
G.711	PCM	48, 56, 64	300 – 3,4K	4,1	0,75	Telefonia Convencional
G.722	Dual band-ADPCM	48, 56, 64	50 – 7K	4,5	<2	Banda larga de voz, videoconferência tradicional e VoIP
G.722.1	MLT	24, 32	50 – 7K	3,8	<2	Videoconferência e VoIP
G.723.1	ACELP MPC-MLQ	5.3, 6.3	300 – 3,4K	3,9	30	videoconferência H.324 e VoIP
G.728	LD-CELP	16	300 – 3,4K	3,61	3 – 5	Ambiente com restrição de banda
G.729	CS-ACELP	8	300 – 3,4K	3.,92	10	Aplicações VoIP

Ainda de acordo com a tabela acima, podemos perceber a presença de uma coluna intitulada MOS (*Mean Opinion Score*) que atribui uma nota a cada um dos *CODEC* de acordo com seu desempenho. Este teste varia de 1 (ruim) até 5 (excelente), onde o nível 4 corresponde ao de uma linha telefônica analógica convencional. Testes MOS são feitos com um grupo de ouvintes e eles dão a cada amostra de voz uma classificação, de onde é retirada uma média para cada um deles.

Ao trafegar sobre redes IP, os pacotes estão sujeitos a se perderem durante a transmissão, fazendo-se necessária a adoção de mecanismos de compensamento das perdas através do preenchimento das lacunas com áudio perceptível aos ouvidos humanos. Este processo é chamado de *Packet-Loss Concealment* (PLC). Outro método para endereçar perda de pacotes é conhecido como *Forward Error*

[2] Tabela com base em FLORÊNCIO (2009) e ARAÚJO e BRAGA (2009).

Correction (FEC), que inclui algumas informações de pacotes previamente transmitidos nos pacotes subsequentes.

Outro ponto importante na evolução dos *CODECs* de áudio está no aproveitamento da banda disponível. Em média, apenas 40% do tempo de uma conversa telefônica é gasto com o canal ativo, ou seja, com o usuário falando. O *Voice Activity Detection* (VAD) e usado para identificar o silêncio e removê-lo do sinal, economizando assim banda.

De uma maneira geral a comunicação de voz sobre redes IP, pode ser descrita pela Fig. (3).

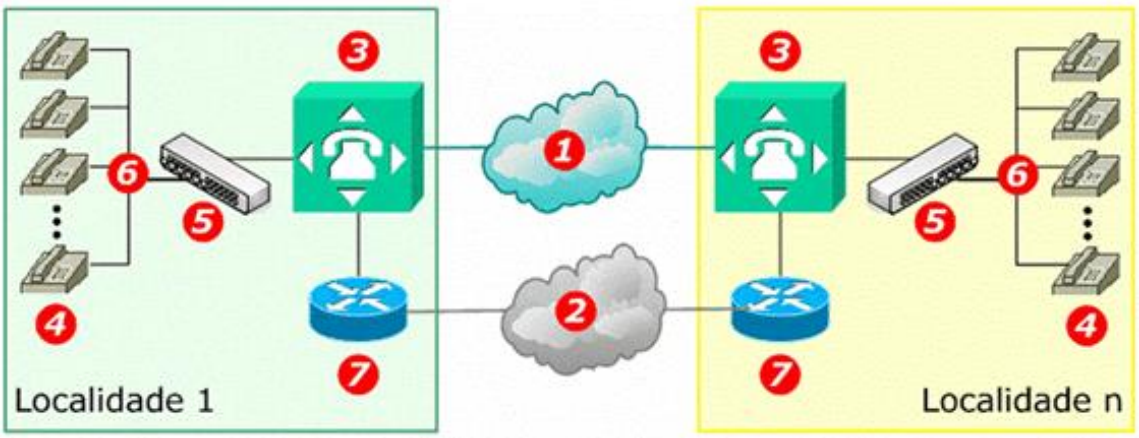


Figura 3 - Comunicação tradicional por voz (BRAGA, 2005).

Neste tipo de implementação, onde a rede IP tradicionalmente utilizada para pacotes de dados é utilizada por elementos de comunicação por voz, algum equipamentos e elementos de rede devem ser identificados:

1. Rede de Telefonia Pública (RTPub) – incluem tanto as redes públicas de serviços de telefonia fixa comutada, como as redes públicas de telefonia celular;
2. Rede Multiserviços (RMS) – são os outros serviços que as empresas de telecomunicações oferecem para prédios de uma empresa. Os mais ofertados são canais de TDM convencionais, *Frame Relay*, e até mesmo canais ATM;
3. PABX – interliga-se com redes de telefonia pública e também pode interligar-se com outros PABX em outras instalações prediais de empresa;
4. Terminal Telefônico (TTel) – é uma interface entre o usuário e os serviços VoIP. Em conjunto com os demais equipamentos podem oferecer serviços adicionais de VoIP;
5. Painel de Distribuição (PD) – conhecido como Distribuidor Geral (DG) a estrutura que interliga os terminais telefônicos ao PABX;
6. Cabeamentos – são os cabos que interligam os terminais e os PABX;
7. CPE (*Customer Premises Equipment*) – Precisa se de um equipamento que seja interface entre a rede multiserviços de uma empresa corporativa com qualquer.

2.3.2 QUALIDADE DE SERVIÇO

Uma aplicação de dados tradicional, como e-mail, pode aceitar uma pequena intermitência no serviço, que geralmente é baseado no *best effort*, o que não acontece para comunicações por voz. A maioria dos usuário de VoIP quer que suas chamadas sejam completadas assim que terminem de discar o destino e que durante a chamada não haja demora ou falhas na comunicação. Em relação às operadoras de telefonia, as mesmas precisam oferecer telefonia IP, com qualidade equivalente aos serviços

existentes na rede convencional e assegurar um eficiente acoplamento com os equipamentos destas redes existentes.

Palhares Neto (2010) define QoS (*Quality of Service*) em redes IP como:

> *"A capacidade de prover garantias de transmissão segura e eficiente para que os serviços a serem executados sejam realizados da melhor maneira possível, independente das anormalidades que a rede possua, ou seja, é a garantia do melhor acesso de um ou mais serviços à rede a partir de políticas de prioridades, dando ênfase àquelas que necessitam de uma reservada largura de banda na rede"*

Vários institutos e pessoas tem se mobilizado para estudar as melhores formas de prover qualidade de serviço em uma rede IP. Hoje, a demanda de QoS se fundamenta em um conjunto de requisitos considerados essenciais, como a minimização do atraso e da taxa de perda de pacotes. Esses requisito entre outros é detalhado a seguir.

a) LATÊNCIA

A latência é caracterizada com o atraso fim a fim na comunicação, ou seja, é o tempo gasto por um pacote para ir da origem ao seu destino. Sobre voz, significa dizer que é o tempo que a voz leva do momento que é pronunciada até o momento em que chega ao ouvido de quem está escutando (VOLTAN JÚNIOR, 2005).

Os principais fatores que influenciam a latência na rede são:

- Atraso de propagação - tempo necessário para a propagação do sinal elétrico, rádio frequência, ou propagação do sinal óptico no meio que está sendo utilizado e é um parâmetro imutável;
- Atraso de processamento - referente ao processamento realizado nos equipamentos, incluindo o atraso para a formação do pacote;
- Atraso de fila – causado devido ao congestionamento na rede.

b) JITTER

Jitter é a variação do atraso da transmissão das informações e é causado pelas variações no tráfego e alterações no roteamento, que mudam ao longo do tempo.

Na transmissão de voz sobre IP os datagramas podem tomar caminhos diferentes ou sofrer atrasos devido a congestionamentos, o que pode resultar em diferentes tempos de propagação. Com o intuito de contornar essa limitação, *buffers* são utilizados na entrada do equipamentos decodificadores, garantindo que, mesmo que alguns pacotes sofram uma demora maior que a normal para chegada, os pacotes nos *buffers* sejam enviados para o decodificador da maneira mais constante possível.

c) ECO E SOBREPOSIÇÃO DO LOCUTOR

O eco é um fenômeno físico que se realiza através da repetição dum som, cuja causa é atribuída ao atraso fim a fim maior que 25ms, que é o tempo que o ser humano suporta ouvir sua própria voz, sem que esta cause desconforto a ele.

Nas redes de telefonia tradicionais o eco ocorre devido a um decasamento de impedância nas híbridas utilizadas para conversão dos quatro fios do nó de comutação para os dois fios do cabo telefônico tradicional.

Outra consequência do atraso é a sobreposição do locutor, que ocorre quando um locutor fala algo para a outra ponta da comunicação e sua mensagem leva muito tempo para chegar ao destino, fazendo com que o outro locutor – que ainda não sabe que há uma mensagem em transito - envie uma mensagem para o primeiro locutor, sobrepondo a mensagem inicial.

d) PERDA DE PACOTES

A perda de pacotes acontece quando um pacote enviado não conseguiu atingir seu destino – o que é bem comum para pacotes de dados - e isto implica na perda de qualidade para a aplicação. Essa perda de pacote não deve ultrapassar 5%, já que, com menos que isso, os CODECs passam a utilizar alguns recursos para lidar com esse problema, como repetir o pacote anterior ou fazer uma interpolação (PALHARES NETO, 2010).

Outra solução seria a utilização de protocolos de transporte confiáveis como, por exemplo, o TCP, no entanto os atrasos gerados pelo seu uso tornam-no inutilizável para este tipo de aplicação, o que faz da perda de pacotes um dos maiores desafios para implementação de QoS em redes VoIP.

e) LIMITAÇÕES DE BANDA

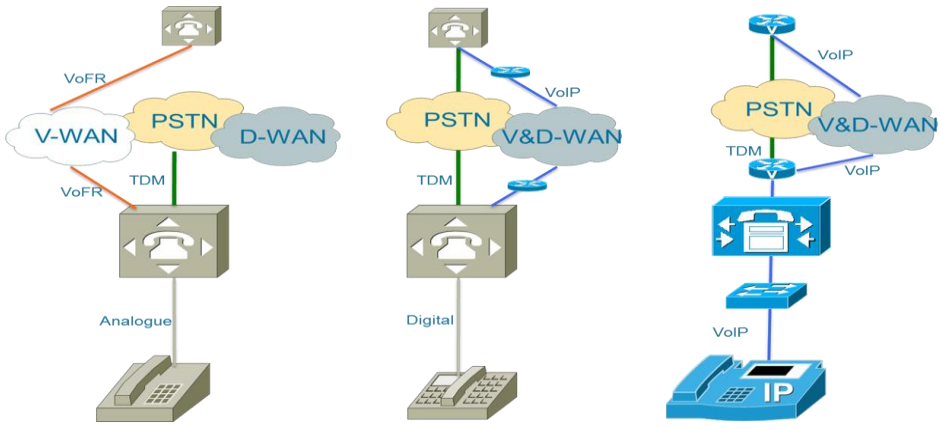
A largura de banda é a medida de capacidade de transmissão de dados, normalmente expressa em *kilobits* por segundo (Kbps) ou *megabits* (Mbps). Palhares Neto (2010) define a largura de banda como a capacidade máxima de transmissão teórica de uma conexão.

A fim de minimizar o requisito de banda, diversas técnicas são empregadas. A supressão de silêncio é uma delas, e consiste em se aproveitar que ao longo de uma conversação existem vários períodos de silêncio e suprimir estes períodos. Com isso o codificador de voz pode reduzir a banda consumida por cada canal podendo chegar a aproximadamente 25% de redução de banda, no caso do padrão G.729 por exemplo (FERNANDES, 2000).

Na rede IP atual, diferentes protocolos e tipos de tráfego compartilham a mesma infraestrutura, fazendo com que um *burst* de dados interajam com o outro de maneira que afetem o desempenho de suas aplicações. Uma implementação de QoS para a rede IP devem incluir, portanto, tecnologias como filas, *Integrated Services* (*IntServ* – QoS realizado por fluxo de dados) e *Differentiated Services* (DiffServ – que divide o tráfego de dados em classes distintas) (PALHARES NETO, 2010).

2.3.3 TELEFONIA IP

A tendência natural da telefonia é a migração total para o mundo IP. Atualmente, grande parte das implementações de telefonia sobre redes IP ainda mantem o legado das centrais telefônicas convencionais, implementando uma espécie de sistema híbrido, onde o PABX convencional e o PABX IP coexistem.



(a) PABX tradicional (b) PABX híbrido (c) Telefonia IP

Figura 4 – Evolução dos sistemas de comunicação por Voz

A Figura (4) acima mostra parte dessa evolução. À esquerda (Fig. 4a) temos esquematizado o sistema de redes telefônicas convencional, onde todo o trafego de voz é lançado sobre a PSTN (*Public Switched Telephone Network* ou Rede Pública de Telefonia Comutada) através do PABX. Inicialmente o trafego de voz também poderia ser transportados sobre redes *Frame Relay* através de WAN de voz totalmente segregada da rede de dados.

Com a introdução da tecnologia VoIP, houve uma integração das redes de voz e dados em uma mesma WAN sobre protocolo IP, mantendo-se ainda os terminais e centrais telefônicas convencionais na topologia, como pode ser visto ao centro (Fig. 4b). Na direita (Fig. 4c) temos o cenário de migração total onde o PABX convencional é totalmente substituído pelo PABX IP, também conhecido como *Softswitch* e os terminais telefônicos pelos *IP Phones* ou, durante a migração, conectados à rede utilizando-se um adaptador ATA (*Analog Telephone Adapter)*. Neste cenário toda a comunicação, deste o terminal telefônico IP de origem ao de destino é feito sobre redes IP (MATHIES, 2010).

Contudo, a diferença de preço entre o terminal telefônico convencional e um equipamento para uso de VoIP (seja um equipamento próprio ou um microcomputador) ainda é um forte fator limitante para uso desta última solução em larga escala. Além disso, a alta disponibilidade das redes telefônicas convencionais aliada à falta de garantia de qualidade de serviço originalmente herdada do IP, são aspectos de peso na comparação entre os ambientes legado e totalmente VoIP.

Não se pode precisar exatamente quando, mas é esperada a mudança do cenário de comunicação de voz e dados atual para uma realidade integrada em larga escala, onde os meios de transmissão deverão servir aos dois "mundos", de forma transparente ao usuário, podendo este utilizar o ponto de rede local que serve a um microcomputador equipado com a capacidade de comunicação de voz para ligação de um telefone IP.

Enquanto não se tenha a completa substituição do legado de telefonia, independente de tratar-se de um longo período de transição obrigatório, dado o volume de equipamentos envolvidos no mundo inteiro, ou por simples opção para maturação tecnológica de novas propostas, é possível a comunicação entre terminais de VoIP e aparelhos da rede telefônica convencional, RDSI (Rede Digital de Serviços Integrados ou ISDN) ou de telefonia móvel, através de *gateways* apropriados e já disponíveis no mercado.

2.3.4 GATEWAYS E GATEKEEPERS

Gateways são elemento da rede que realizam a conversão (tradução de protocolo) entre terminais distintos, permitindo a interoperabilidade entre sistemas. Também realizam serviços de compressão e empacotamento, transformando basicamente a voz do usuário em pacotes de dados e vice-versa (VOLTAN JÚNIOR, 2005).

Os gateways H.323 oferecem serviços para clientes H.323, de modo que possam se comunicar com interfaces não H.323. O tipo mais comum de gateway H.323 permite comunicações entre terminais H.323 e telefones na rede de comutação de circuitos (SCN – *Switched Circuit Network*), como é mostrado na Fig. (5). O gateway precisa oferecer traduções entre diferentes formatos de transmissão de áudio, vídeo e dados, assim como dos sistemas de comunicação e protocolos. Isso inclui o estabelecimento e finalização de chamadas nas redes IP e SCN.

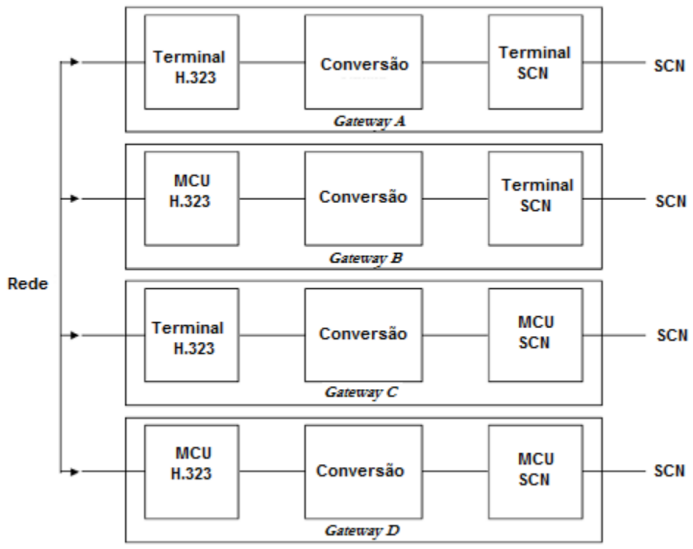


Figura 5 – Gateway H.323 (PALHARES NETO, 2010)

Já o *gatekeeper* é considerado o componente mais complexo da estrutura da recomendação H.323. Ele fornece serviços de pré-controle e controle e tem como principais funções a tradução de endereços que é usado para se encontrar um *alias*; sinalização; controle de chamadas o qual verifica a disponibilidade de recursos da rede; controle de admissão tanto à rede como a terminais, *gateways* e MCU. Enfim resume-se *gatekeeper* como sendo um servidor que provê serviços multimídia para as entidades da rede e ainda gerencia toda a conferência.

2.3.5 MCU

A Unidade de Controle de Multiponto (MCU – *Multi Control Unit*) é uma extremidade na rede cuja função é verificar o direito de acesso aos recursos e que oferece a capacidade para três ou mais terminais ou *gateways* participarem em uma conferência multiponto. Ela também pode conectar dois terminais em uma configuração ponto a ponto, que mais tarde pode se desenvolver para uma configuração multiponto.

Segundo Fernandes (2000), a MCU pode funcionar em três modos distintos:

- Modo Centralizado – a comunicação entre a MCU e os terminais ou gateway é *unicast*. Dados, áudio, vídeo e controle passam obrigatoriamente pela MCU;
- Modo Descentralizado – os terminais trocam informações de controle, e opcionalmente de dados, de forma centralizada com a MCU, mas trocam áudio e vídeo entre si por *multicast*;
- Modo Híbrido – a comunicação de dados e controle sempre se dá de forma centralizada com a MCU. Contudo, podemos ter áudio também centralizado e *multicast* de vídeo ou vice-versa

2.3.6 PRINCIPAIS PROTOCOLOS

Os protocolos de transporte não foram originalmente concebidos para transportar fluxos de mídia em tempo real, ou seja, fazer com que a informação chegue ao destino com *delay* máximo de 150ms. Esta é uma dos entraves de se implementar o tráfego de voz sobre redes IP. Outro ponto que dificulta a utilização dos protocolos usualmente empregados no transporte de pacotes de dados no transporte de voz é que em uma típica conversa de áudio o mecanismo pode não funcionar com a qualidade desejada, uma vez que para dados é tolerado o reenvio e a perda dos pacotes e para conversas deste tipo isso significaria uma dificuldade de estabelecer a comunicação.

As redes ISDN foram projetadas especificamente para a transmissão de voz e são perfeitamente adequadas para esta tarefa do ponto de vista técnico, porém não possuem a flexibilidade que uma rede VoIP pode oferecer, integrando a transmissão de voz aos protocolos que fazem parte da rede de pacotes. A seguir são apresentados os principais pacotes envolvidos na comunicação por voz.

a) H.323

O protocolo H.323 é um padrão que faz parte da ITU-T H.32x que pertence à série H da ITU-T, relacionados nos "Sistemas Audiovisuais e Multimídia". O padrão H.323 foi originalmente concebido para fornecer um mecanismo de transporte IP para videoconferências e pode ser dividido em três áreas principais de controle:

- Sinalização de registro, admissão e status (RAS) – fornece o controle pré-chamada em redes H.323 baseadas em *gatekeepers*;
- Sinalização de controle de chamadas (H.225) – usada para conectar, manter e desconectar chamadas entre pontos terminais;
- Controle e transporte de mídia – fornece o canal confiável H.245 que transporta mensagens de controle de mídia.

O H.323 trata o sistema de comunicação multimídia sem garantias de qualidade QoS, especificando o padrão de interoperabilidade de codificação e decodificação de áudio e vídeo e opera independentemente dos aspectos relacionados à rede, podendo ser utilizada qualquer tecnologia de enlace (*Ethernet*, *FastEthernet*, FDDI, ou *Token Ring*) ou topologia de rede.

Braga (2005) mostra uma série de benefícios da aplicação do padrão H.323:

- Independência da rede – as redes IP são projetadas para transporte de pacotes assim como o padrão H.323 é especificado, tornando fácil trabalhar com a aplicação multimídia pela rede, e conforme vai evoluindo a tecnologia de enlace evolui em proporção;
- Interoperabilidade de equipamentos e aplicações – os grandes fornecedores como Intel, Microsoft, Cisco e IBM investem em linhas de produtos H.323, permitindo a interoperabilidade entre as aplicações e dispositivos;
- Independência de plataforma – o padrão H.323 pode atuar em diversos mercados específicos, que vão desde softwares de videoconferência executados em PCs a telefones IP, televisões a cabo, devido a independência de hardware ou sistema operacional a ser usado;
- Representação padronizada de mídia – os métodos de compressão e descompressão de sinais de áudio e vídeo são padronizados;
- Flexibilidade nas aplicações clientes – o padrão H.323 permite que terminais com uma aplicação apenas para áudio participem de conferências com terminais que tenham suporte adicional para vídeo e/ou dados;
- Interoperabilidade entre redes – conexões entre uma rede LAN e redes como a rede telefônica pública ou ISDN através de um *gateway*;
- Gerenciamento de largura de banda – o padrão H.323 provê mecanismos de gerenciamento de controle de banda, delimitando a quantidade de conferências simultâneas, e também podendo até contabilizar o uso dos recursos da rede que podem ser usadas para fins de cobrança, através da utilização do *gatekeeper*;
- Conferências multiponto – o H.323 possui suporte a conferências multiponto.

b) SIP

O SIP (*Session Initiation Protocol* – Protocolo de Inicialização de Sessão) é um protocolo do nível de aplicação baseado em texto que permite o estabelecimento, gerenciamento e encerramento de sessões multimídia, como, por exemplo, chamadas telefônicas através da rede IP, através do uso de um modelo requisição-resposta para tal fim.

Este protocolo surgiu em meados da década de 1990[3]. Por ser um protocolo relativamente simples e de sintaxe semelhante a outros protocolos mais familiarizados no ambiente da comutação de pacotes, como o HTTP e SMTP, seu emprego tornou amplamente comum para sistemas de telefonia IP.

O SIP oferece serviços como transferência, redirecionamento, identificação e autenticação de chamadas, conferência etc., usando pacotes UDP como o suporte para suas mensagens. Ele trabalha em conjunto com outros protocolos, tais como MGCP, MEGACO, SDP, RSTP, RTP e RTCP e possui dois tipos de agentes, os agentes usuários (UA – *User Agent*) e os servidores.

O *SIP User Agent* é o terminal SIP ou o software de estação final e pode ser dividido em agentes usuários clientes (UAC – *User Agent Client*, responsáveis por originar a chamada SIP) e agentes usuários servidores (UAS – *User Agent Server*, respondendo a ligação de outro terminal). O UA armazena e gerencia situações de chamada, e pode aceitar e receber chamadas de outro UA sem requerer nenhum componente adicional do SIP. *IP Phones*, *softphones* e *gateways* são exemplos de UAC. Os servidores SIP podem ser:

- *SIP Proxy Server* – é um servidor intermediário do SIP, passando requisições adiante do UAC para o próximo servidor SIP, garantido assim que o IP do UAC não seja inidentificável a outros clientes. É também o responsável por reter informações objetivando a contabilidade e faturamento;

[3] RFC 2543 (IETF, 1999) atualizada para RFC 3621 (IETF, 2002).

- *SIP Redirect Server* – é outro tipo de servidor intermediário do SIP, cuja função é fornecer a resolução de nome e locação do usuário. Responde ao pedido do UA fornecendo informações sobre o endereço do servidor para que o cliente possa contata-lo diretamente;
- *SIP Register Server* – o registrador SIP fornece um serviço de informação de localidades; o UA solicita autenticação e ele armazena essa informação de registro, retransmitindo posteriormente esse pedido para o próximo *SIP Proxy Server*;
- *SIP Database Server* – é o local onde são armazenadas as informação de identificação dos clientes, como *login*, senha, ramal, endereço IP.

A arquitetura do SIP fixa o endereço do usuário SIP remoto, porém ao invés de permanecer amarrado a um endereço estático, ele se comporta como um endereço dinâmico que reflete o endereço de locação atual da pessoa remota. A combinação dos servidores de *proxy* e redirecionamento dá ao SIP grande flexibilidade de arquitetura, mesmo quando o usuário remoto é móvel. O protocolo SIP suporta o transporte de qualquer tipo de carga em seus pacotes, e é projetado no HTTP, funcionando como cliente/servidor sendo este o motivo da necessidade de requisições e respostas.

Os métodos de requisição do SIP são os seguintes: *INVITE*, *ACK*, *OPTIONS*, *BYE*, *CANCEL*, e *REGISTER*.

O comportamento destes métodos, como descrito em Almeida (2008), são descritos abaixo:

- *INVITE* – indica que o utilizador está a ser convidado para participar de uma sessão multimídia. O corpo da mensagem pode conter uma descrição da sessão, utilizando-se o protocolo de descrição de sessão SDP (*Session Description Protocol*).
- *ACK* – Mensagem recebida como resposta a um *INVITE*. A requisição *ACK* pode conter o SDP de descrição de sessão negociada entre ambos os clientes. Se não contiver o SDP, o utilizador chamado pode assumir a descrição dada pelo primeiro *INVITE*, se houver.
- *OPTIONS* – Faz uma pergunta sobre quais métodos e extensões suportados pelo servidor e pelo utilizador descrito no campo de cabeçalho "*To*:". O servidor pode responder a esta pergunta com o conjunto de métodos e extensões suportado pelo utilizador e por ele próprio.
- *BYE* – Usado para libertar os recursos associados a uma ligação e forçar a desconexão da mesma.
- *CANCEL* – Cancela uma requisição que ainda esteja pendente, ou seja, em andamento. Uma requisição é considerada pendente, se e somente se, não foi atendida com uma resposta ao *REGISTER*. Um cliente usa este método para registar o *alias* (apelido) do seu endereço em algum servidor SIP

Em relação ao H.323, algumas funcionalidades do SIP podem ser destacadas:

- Velocidade – enquanto o H.323 precisa enviar cerca de cinco mensagens para certa tarefa, o SIP o faz em apenas uma, aumento a rapidez da troca de sinalização. Além disso, o SIP pode usar o UDP, ao passo que o H.323 precisa usar o TCP;
- Uso de URLs – aparentemente um alias de e-mail H.323 (nome@dominio.com.br) e uma URL SIP (sip:nome@dominio.com.br) não possuem diferenças. Mas na verdade, um alias de e-mail H.323 considera que o protocolo usado seja o H.323, ao passo que o SIP especifica ele mesmo o protocolo na URL. Por causa disso, um servidor SIP pode redirecionar uma chamada para servidores não SIP de maneira bem flexível;
- Codificação de texto – a codificação de texto utilizada pelo SIP é mais simples e fácil de depurar usando-se analisadores de protocolo, fazendo com que problemas de interoperabilidade sejam facilmente detectáveis.

A Figura (6) abaixo mostra as trocas de mensagens durante uma chamada SIP.

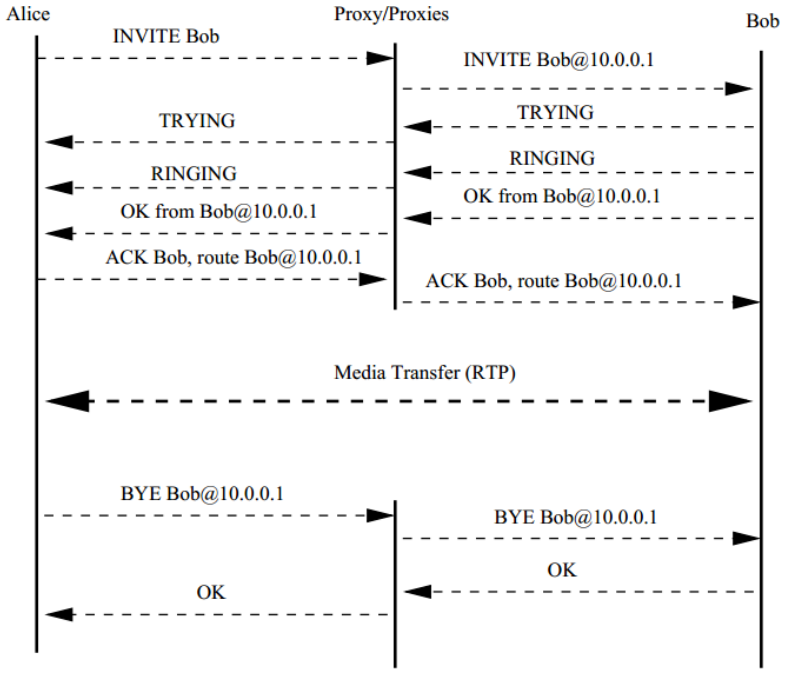


Figura 6 – Troca de mensagens durante uma ligação baseada em SIP (KEROMYTIS, 2009).

Na o diagrama (Fig. 6), Alice envia uma mensagem *INVITE* para o servidor *proxy*, que no caso é o *Call Manager*, opcionalmente contendo informações de sessão codificada dentro de SDP. Caso Alice e Bob estejam em um mesmo domínio, o *proxy* envia esta mensagem diretamente para Bob. Se Bob é registrado em um domínio diferente de Alice, a mensagem será retransmitida ao *proxy* sob o qual Bob está registrado, e de lá para ele. Enquanto Bob não aceita a chamada, mensagens de zumbido (mensagens *RINGING*) são enviadas de volta para Alice. Uma vez que a chamada tenha sido aceita, uma mensagem de OK é enviado para Alice, contendo os parâmetros preferidos codificados dentro SDP. Alice responde com uma mensagem de ACK, que caso já não tenha sido enviado, contém seus parâmetros (uma vez que o no INVITE, o envio destes via SDP é opcional).

Após isso, o tráfego de mídia é estabelecido, transportando voz, vídeo ou outro conteúdo (negociado), utilizando um protocolo de transporte de mídia, normalmente RTP. Enquanto a sinalização SIP pode ser retransmitida por um certo número de *SIP proxies*, o tráfego de mídia é trocado diretamente entre os dois pontos terminais da comunicação. Quando o trafego trafega, por exemplo, pela PSTN, *gateways* de mídia podem perturbar a natureza fim a fim da transferência de mídia, uma vez que podem ter que traduzir o conteúdo (por exemplo, áudio) entre os formatos que são suportados pelas diferentes redes (KEROMYTIS, 2009).

c) RTP, RTCP e SRTP

O RTP (*Real Time Protocol*) é um protocolo utilizado para o transporte de mídias contínuas de tempo real em uma conexão ponto-a-ponto, projetado para permitir que os receptores compensem o *jitter* e a perda de sequência dos pacotes introduzidos pelas redes IP, por meio do controle de buffer e sequenciamento apropriado. Pode ser usado também em uma comunicação multidestinatária utilizando um endereço IP da faixa reservada para grupos *multicast* e para qualquer fluxo de dados em tempo real, como voz e vídeo. O RTP define um modo de formatar pacotes IP que carregam dados e inclui informações sobre o tipo de dado transportado, *timestamps* e números de sequência.

Este protocolo não reserva recursos nem garante qualidade de serviço (QoS), porém é frequentemente utilizado em paralelo com o RTCP (*RTP Control Protocol*), viabilizando uma certa monitoração da comunicação (quantidade de *jitter*, perda média de pacotes, etc) e o transporte de algumas informações a respeito da identidade dos participantes.

O RTCP é o protocolo responsável no envio de pacotes de controle a todos os participantes da conexão (chamada), usando o mesmo da mídia (voz), só que em tempo real usando o suporte UDP

(para a voz e controle) da rede IP. O uso de UDP é apropriado, uma vez que o esquema de retransmissão do TCP não é adaptado para dados que precisam ser transportados com uma latência muito baixa, como no caso de comunicações interativas. Nesse caso, o RTP é tradicionalmente associado a uma porta UDP de número par e o RTCP, a próxima porta UDP de número ímpar.

Cabe ao RTCP também transmitir o nome canônico (CNAME) de cada participante. Se houver conflito no identificador de das fontes de sincronização, este pode se alterar para que não haja conflito. Porém, não pode haver conflito para os CNAMEs. É Função do CNAME é garantir o reconhecimento dos diferentes tipos de mídias como parte de uma única comunicação daquele participante.

RTP e RTCP são utilizados paralelamente, mas os pacotes de cada protocolo são transmitidos de forma independente e não tem qualquer influência sobre o comportamento da rede IP, sendo inertes ao controle de qualidade de serviço. A rede pode perder, inserir atraso ou perder a sequência de um pacote RTP da mesma maneira que qualquer outro pacote IP.

Já SRTP é um perfil de segurança para a RTP que agrega confidencialidade, autenticação de mensagens e proteção para *replay* para esse protocolo e para o RTCP. SRTP é ideal para proteger o tráfego *Voice over IP*, porque pode ser utilizado em conjunto com a compressão de cabeçalho e não tem nenhum efeito sobre a qualidade de serviço IP. Estes fatos fornecem vantagens significativas, principalmente para o tráfego de voz utilizando CODEC como o G.729.

d) MGCP e MEGACO

O MGCP (M*edia Gateway and Control Protocol*) é um protocolo utilizado para controlar gateway de mídia sobre redes IP. É o resultado da combinação de outros dois protocolos para controle de gateways: o SGCP (*Simple Gateway Control Protocol*, desenvolvido pela *Telcordia Bellcore e Cisco Systems*) e o IPDC (*Internet Device Control Protocol*, desenvolvido pela *Level 3 Communications*).

O MGCP é um protocolo de sinalização e controle de chamadas usado dentro da rede VoIP, que que normalmente interoperam com a rede telefónica pública comutada (PSTN), implementando um modelo *PSTN-over-IP*. Outra implementação da arquitetura de protocolos de controle de gateway de mídia existente é o protocolo H.248/MEGACO (RFC[4] 3015 e posteriormente RFC 3025, que é uma colaboração da IETF e da ITU-T.

Ambos os protocolos podem seguir as diretrizes da *Media API Gateway Control Protocol*, porém os protocolos são incompatíveis devido a diferenças na sintaxe de protocolo e modelo de ligação subjacente.

O MEGACO Foi concebido para ser utilizado para controlar *gateways* monolíticos (um único equipamento) ou distribuídos (vários equipamentos). Sua plataforma aplica-se a *gateway*, controlador multiponto (MCU) e unidade interativa de resposta audível (IVR).

Possui também interface de sinalização para diversos sistemas de telefonia, tanto fixa como móvel.

2.4 COMUNICAÇÕES UNIFICADAS

A convergência das mais variadas formas de comunicação sob protocolo IP e plataformas de software-livre está permitindo que surja um novo paradigma para as comunicações, mudando a forma como os indivíduos, grupos e organizações se comunicam e colaboram. Surge então, nesse contexto, o conceito de comunicações unificadas, que visam melhorar significativamente as tradicionais formas de interagir e executar. *Unified Communications*, ou simplesmente, UC é o processo no qual todos os meios e dispositivos de comunicação e mídia estão integrados permitindo que os usuários se comuniquem em tempo real com qualquer pessoa em qualquer lugar e a partir de qualquer dispositivo, representando uma unificação de tecnologias implementadas independentes, como telefonia IP, videoconferência (salas, *desktop* e *web*), serviços de mensagens instantâneas e serviços de presença.

De forma simples, UC pode ser definida como:

[4] *Request for Comments* (RFC) é um documento que descreve os padrões de cada protocolo da Internet.

> *"UC é a convergência de todas as formas de áudio, vídeo, web e comunicações, sobre uma infraestrutura de rede de dados que derruba as barreiras de distância, tempo e tipo de comunicação. Isto faz com que as pessoas se comuniquem entre si a qualquer momento, em qualquer lugar, independente do meio ou do dispositivo usado" (PEREIRA, 2011)*

Pereira (2010) ainda faz uma ressalva ao uso correto do termo *Unified Communications*, alertando para o fato que muitas vezes o termo 'unificado' é utilizado juntamente com diversos produtos de seu portfolio, mas não são capazes de interoperar com produtos de terceiros, sendo usados apenas em configuração isoladas de modo não integrado.

O mercado de comunicações unificadas está crescendo no ambiente corporativo. Segundo dados da *ABI Research*, empresa de consultoria e pesquisa em TIC, o segmento de UC, composto de telefonia IP, conferências, colaboração e outras formas integradas de comunicações, deve chegar a 4,2 bilhões de dólares em 2014, ante os 302 milhões de dólares em 2008. A Gartner, outra empresa de consultoria em TIC, define como produtos de comunicações unificadas aqueles produtos (equipamentos, softwares e serviços) que facilitam o uso de métodos de comunicação empresariais múltiplos. Isso pode incluir o controle, gestão e integração desses métodos. Produtos de UC integram canais de comunicação (mídia), redes e sistemas, bem como aplicações de negócios de tecnologia da informação e comunicação e, em alguns casos, aplicações e dispositivos dos consumidores. (GARTNER, 2012)

Estes produtos podem ser compostos de um único fornecedor (*stand-alone suite*) ou os clientes podem implantar um portfólio de aplicações integradas e plataformas, abrangendo vários fornecedores. Produtos de UC são usados pelas pessoas para facilitar as comunicações pessoais e pelas empresas para suporte de comunicações de grupos de trabalho e de colaboração. Alguns produtos de UC pode estender UC fora dos limites da empresa para melhorar a comunicação entre as organizações, para apoiar as interações entre as grandes comunidades públicas ou para comunicações pessoais. Aplicações de UC são cada vez mais integrados ou oferecidos em conjunto com aplicativos de colaboração para formar comunicações unificadas e colaboração (*Unified Communications and Colaboration* - UCC).

Os requisitos básicos de UC, implícitos em sua definição, exigem que três pontos relevantes sejam observados:

- Disponibilidade – as aplicações devem estar disponíveis sob demanda, não importando em qual espaço/tempo os usuários estejam, ou seja, a aplicação deve permitir interação em tempo real aos usuários independente de sua localização física e permitir que se tenha acesso a esses recursos envolvidos para posterior acesso e compartilhamento;
- Simplicidade – O uso das tecnologias deve ser o mais simples e intuitivo possível, uma vez que a forma como usamos determinadas ferramentas é cultural e mudanças nesses hábitos devem estar muito bem fundamentadas. A solução, portanto, deve ser amigável para que toda a empresa perceba seus benefícios;
- Interoperabilidade – Fazer com que soluções de diferentes fabricantes interajam entre si é uma ponto chave, pois é desejo de todos que exista uma solução convergente unificada tanto do ponto de vista dos recursos providos como do ponto de vista dos fabricantes envolvidos no processo.

É útil para dividir UC em seis grandes áreas:

- Voz e Telefonia - Esta área inclui telefonia fixa, móvel e suave, bem como a evolução dos PBXs e PBXs IP. Ele também inclui comunicações ao vivo, como a telefonia de vídeo;
- Conferência - Esta área inclui conferências de voz, videoconferência e recursos de conferência *Web*, como várias formas de recursos de conferência unificada;
- Mensagens - Esta área inclui e-mail, que se tornou uma ferramenta de negócios indispensável, correio de voz e várias abordagens para *Unified Messaging* (UM);
- Presença e IM - Estes irão desempenhar um papel cada vez mais central na próxima geração de comunicações. Serviços de presença, em particular, estão a expandir para permitir a

agregação e publicação de presença e de informação de localização entre (a partir de e para) de múltiplas fontes;

- Clientes - clientes unificados permitem o acesso a várias funções de comunicação a partir de uma interface consistente. Estes podem ter diferentes formas, incluindo clientes de *desktop*, de navegadores e de dispositivos móveis, como *smartphones* e *tablets*, além de clientes especializados embutidas dentro de aplicações de negócios;
- Aplicativos habilitados para UC - Este grupo de aplicações tem funcionalidades de UC integradas. As principais áreas de aplicação incluem aplicativos de colaboração, de *contact center*, de notificação e de gestão consolidada, com ferramentas de análise e/ou elaboração de relatórios. Quando as aplicações de negócios são integradas com aplicativos de comunicação para melhorar as operações, a Gartner os chama de processos negócios habilitados para comunicação (*Communications-Enabled Business Processes*, CEBPs).

Na formação de seu *Magic Quadrant*, a Gartner (2012) define quatro características de *Unified Communications* que vão ter um efeito importante sobre o sucesso de um produto UC e a satisfação dos usuários:

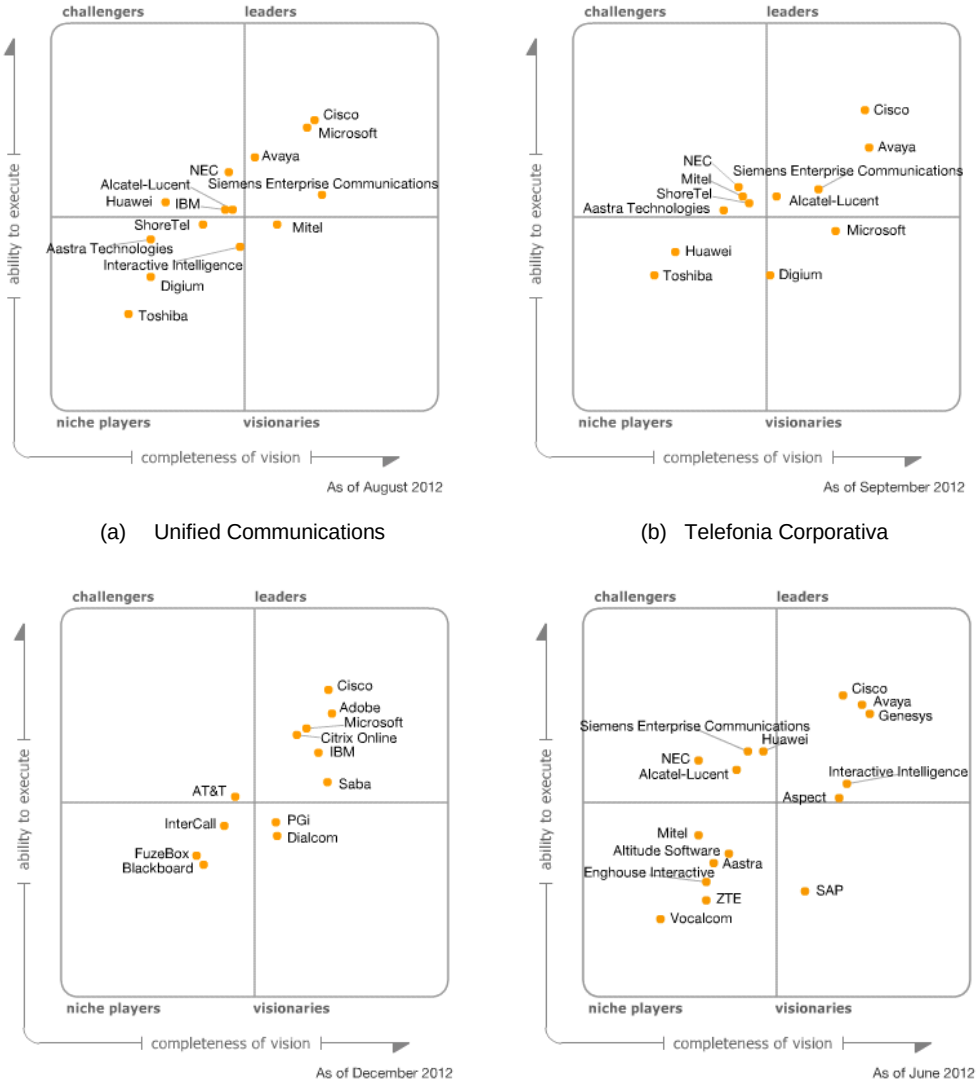
- Mobilidade – Funcionalidades UC completas em dispositivos móveis. Usuários esperam cada vez mais funcionalidades UC completas em todas as plataformas móveis e sistemas operacionais;
- Abertura - Empresas querem evitar "jardins fechados" e fraco suporte para padrões definidos, de modo a garantir a escolha e controle da solução. Oferecer suporte para padrões é uma consideração crítica, pois possibilita que as empresas integrem suas soluções de UC com parceiros de negócios, clientes, aplicativos de negócios e de produtos de terceiros. Em particular, as empresas esperam de boa qualidade suporte para SIP, XMPP e integrações H.323, bem como um compromisso de longo prazo claro para interoperabilidade e federação;
- *Cloud* - Integração de UC no local com a nuvem e serviços híbridos de UC irão desempenhar um papel importante para que uma solução *de Unified Communications as a Service* (UcaaS) torne-se mais amplamente aceito;
- Solução abrangente – Casos de sucesso de soluções de UC dependem de quão amplo e diversificado é o público de tomadores de decisão da empresa. O sucesso exigirá avançar em um conjunto completo de recursos de UC dentro das empresas oferecendo os requerimentos para os tão diversos grupos, como telecomunicações, comunicação de dados, áudio e vídeo, bem como oferecer os requisitos mínimos de mobilidade para usuários de negócios que trazem seu próprio dispositivo (*Bring Your Own Device* - BYOD) para o ambiente corporativo.

Abaixo (Fig. 7) está mostrado como está o posicionamento em UC segundo o Gartner (2012). Dividido em quatros grandes áreas (*Unified Communications*, Telefonia Corporativa, Conferência Web e Centrais de Atendimento) esses quadrantes conseguem mostrar como está o *Market Share* de comunicações unificadas.

Percebe-se que há dois grupos de empresas, as que tentam diversificar o seu portfolio de produtos e buscam a liderança nos quatro quesitos, como a Cisco e a Siemens, e as que se especializam em um deles para se destacarem, como a Genesys, focada principalmente em soluções de Centrais de Atendimento.

Bailey (2008), mostra os benefícios da implantação de um sistema de *IP Communications* (IPC), onde três temas gerais caracterizam os resultados encontrados:

- Aplicações de UC levam a comunicação a um nível mais efetivo e inteligente;
- *Unified Communications* proporciona tanto economia de tempo e redução de custos;
- O nível de benefícios da aplicação de Comunicações Unificadas aumenta conforme o número de diferentes aplicações disponíveis aumenta.



(a) Unified Communications

(b) Telefonia Corporativa

(c) Conferência Web

(d) Contrais de Atendimento

Figura 7 – *Magic Quadrants for Unified Communications* (GARTNER, 2012)

A Figura (8) a seguir mostra a ampla gama de áreas operacionais onde as Comunicações Unificadas podem atuar, para melhorar a produtividade em ambientes corporativos. Por exemplo, organizações que usam *Mobile Unified Communications* e *Unified Messaging* apresentam melhorias na produtividade dos funcionários remotos, através da melhoria dos processos de gerenciamento e economia de tempo. UC permite às empresas se adaptar a dispersão natural provocada pela globalização sem que este distanciamento físico entre sedes e funcionários acarretem em uma separação também da visão da empresa.

As comunicações unificadas são, portanto, uma importante ferramenta para solucionar as complexidades inseridas com uso difundido de vídeo e a sobrecarga de informações na rede, conectando pessoas, informações e equipes, ajudando a capacitar experiências de colaboração abrangentes e eficazes. Com as Comunicações Unificadas, uma empresa pode:

- Conectar colegas, parceiros, fornecedores e clientes com as informações e especializações de que eles precisam;
- Acessar e compartilhar vídeo no desktop, em trânsito e sob demanda, com a mesma facilidade com que faz uma chamada telefônica;

- Facilitar melhores interações de equipe, reunindo dinamicamente os indivíduos, grupos de trabalho virtuais e equipes;
- Tornar os ramais dos dispositivos móveis da rede corporativa tão móveis que os funcionários podem ser produtivos em qualquer lugar;
- Inovar em toda a cadeia de valores, integrando colaboração e comunicação em aplicações e processos corporativos;

Além disso, uma implementação de UC fornece uma experiência de alta qualidade e altamente segura em todo o espaço de trabalho, proporcionando a reduzir os ciclos de vendas e atendimento aos clientes e do tempo até a colocação do produto no mercado, além de favorecer a inovação e a adaptação as mudanças do mercado.

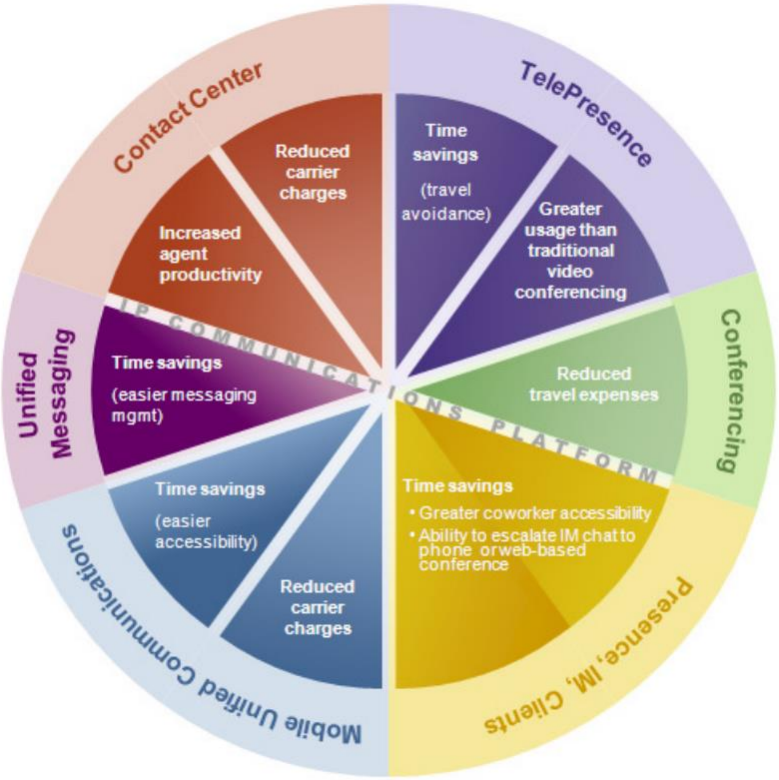


Figura 8 - Benefícios de Comunicações Unificadas: além de implantação básica

2.5 SEGURANÇA DA INFORMAÇÃO

2.5.1 CONCEITO

A norma NBR 27002 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT, 2005), que trata sobre tecnologia da informação e técnicas de segurança, define SI como:

> *"A proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio."*

A Segurança da Informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto às informações corporativas quanto às pessoais. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

2.5.2 PRINCÍPIOS DA SEGURANÇA

A tríade CID - Confidencialidade, Integridade e Disponibilidade - representa os principais atributos que, atualmente, orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger. Com a evolução do comércio eletrônico e da sociedade da informação, a privacidade é também uma grande preocupação.

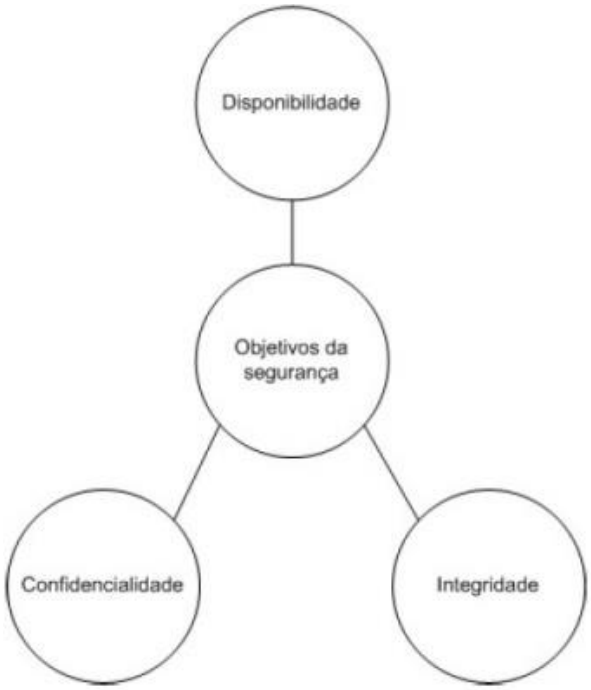


Figura 9 – Tríade CID (Confidencialidade, Integridade e Disponibilidade) (ANTONIAZZI, 2008)

Segundo Antoniazzi (2008), a triade de SI pode ser definida como:

- Confidencialidade - propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação. É o que assegura a proteção da informação contra o acesso e divulgação não autorizados, esteja ela armazenada, em processamento ou em trânsito.
- Integridade - propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição). Princípio que trata da legitimidade e consistência da informação que se refere às permissões para modificação de seu conteúdo as quais são definidas pelo proprietário da informação e devem ser garantidas durante todo o seu ciclo de vida. Pode-se definir a autenticidade como uma sub-propriedade da integridade e trata da legitimidade da informação.
- Disponibilidade - propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação. É a probabilidade de um sistema estar em funcionamento e pronto para uso em um determinado instante de tempo.

Ainda no campo das definições, a norma 27002 determina uma diferença clara entre vulnerabilidades e ameaças e ainda uma definição de gestão de riscos:

> *"Ameaça – causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.*
> *Vulnerabilidade – fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.*

Gestão de riscos – atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos e geralmente inclui análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos".
(ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT, 2005)

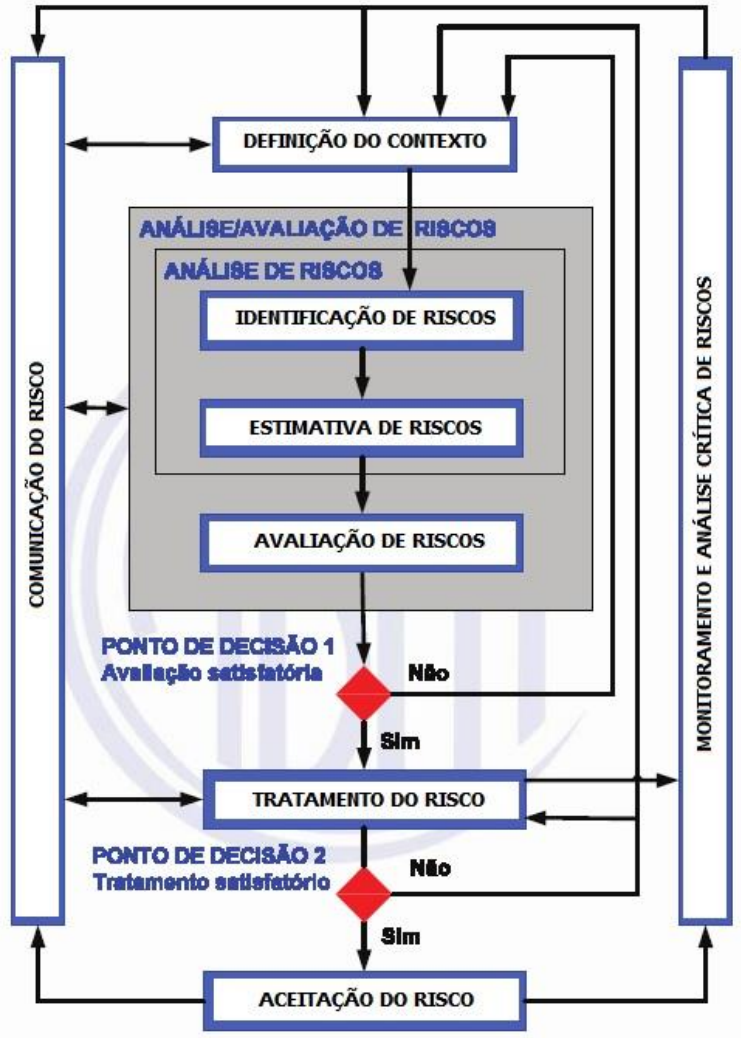


Figura 10 – Processo de Gestão de Riscos de Segurança da Informação[5]

De uma maneira mais simples, a vulnerabilidade está contida dentro do ativo, ou seja, é independente do ambiente, enquanto as ameaças são externas. Outra definição simples e que evita confusões é sobre o risco, que segundo a norma NBR 31000 é efeito da incerteza nos objetivos (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT, 2009).

2.5.3 ATIVOS

Segundo Gonçalves (2010), existem diversos tipos de ativos, que podem ser organizados e classificados por meio de propriedades conforme exemplo das Tab. (2) e (3)[6]. Tais propriedades muitas vezes classificam os ativos em grupos com características semelhantes no que diz respeito às necessidades de especialização (ativos tangíveis e intangíveis), e a responsabilidade pela segurança de

[5] Reconstruída. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT, 2008)

[6] Tabelas (2) e (3) tem fonte: *Secure Officer– Módulo Education Center* (*apud* GONÇALVES, 2010)

uma organização (lógico, físico e humano), o que em geral, acaba sendo normalmente dividida entre uma ou mais áreas.

Tabela 2 – Exemplo de classificação de ativos

Categorias de Ativos	Exemplos
Tangíveis	Informações impressas ou digitais
	Impressoras
	Móveis de escritório
Intangíveis	Imagem da empresa
	Confiabilidade de um órgão federal
	Marca de um produto

Tabela 3 – Exemplo de classificação de ativos

Categorias de Ativos	Exemplos
Lógicos	Dados armazenados em um servidor
	Sistemas
	Rede dados
	VoIP
Físicos	Estação de trabalho
	Sistema de ar-condicionado
	NoBreak
	Gerador
	Equipamentos
Humanos	Colaboradores
	Prestadores de Serviço
	Estagiários

Da mesma forma que os ativos possuem características específicas, utilizam-se abordagens especializadas para atender às demandas de segurança, que são chamadas de medidas de proteção. Essa proteção pode ser física, lógica ou administrativa, ou ainda de acordo com a ação e o momento em que ela ocorre, pode-se classificar as proteções em preventiva, desencorajadora, limitadora, monitorada, detectora, reativa, corretiva e recuperadora.

2.5.4 MECANISMOS DE SEGURANÇA

Segundo Ferreira (2005), o suporte para as recomendações de segurança pode ser encontrado principalmente em controle físicos e lógicos. Os controles físicos são barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura (que garante a existência da informação) que a suporta. Existem mecanismos de segurança que apoiam os controles físicos, como portas, trancas, paredes, blindagem, guardas entre outros. Já os controles lógicos são barreiras que impedem ou limitam o acesso a informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal intencionado. Alguns mecanismos de segurança apoiam os controles lógicos:

- Mecanismos de criptografia – permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros. Utiliza-se para tal, algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados. A operação inversa é a decifração.
- Assinatura digital – um conjunto de dados criptografados, associados a um documento do qual são função, garantindo a integridade do documento associado, mas não a sua confidencialidade.
- Mecanismos de garantia da integridade da informação – usando funções de *hashing* ou de checagem, consistindo na adição.
- Mecanismos de controle de acesso – palavras-chave, sistemas biométricos, firewalls, cartões inteligentes.
- Mecanismos de certificação - atestam a validade de um documento.
- Integridade – medida em que um serviço/informação é genuíno, isto é, está protegido contra a personificação por intrusos.

2.5.5 CICLO PDCA

A norma NBR 27002 sugere a implantação do Sistema de Gestão da Segurança da Informação (SGSI) através do ciclo contínuo de aprimoramento do sistema. Esse ciclo, conhecido como PDCA (*Plan – Do – Check – Act*) é implementado da seguinte maneira (PROMON LOGICALIS, 2005):

- PLAN – Esta etapa visa o estabelecimento de um SGSI, através da definição de uma diretriz para a segurança da informação em consonância com os objetivos de negócio da corporação; da realização de um levantamento de todos os ativos de informação contidos na empresa; da atribuição de um valor para cada ativo, analisando suas vulnerabilidades e ameaças e o impacto associado a cada ameaça; e da definição, de acordo com as práticas da norma, quais controles devem ser introduzidos para reduzir o risco existente;
- DO – Nessa fase, tem-se a imlementação e operação do SGSI, através da definição de planos de tratamento de riscos, que podem incluir a instalação de ferramentas, treinamentos, campanhas de conscientização, criação de procedimentos de trabalho, ou transferir o risco para terceiros (contratação de seguros).
- CHECK – Nessa etapa é feito o monitoramento e revisão do Sistema de Gestão da Segurança da Informação, verificando se, no tratamento dos riscos identificados, os planos delineados foram adequados e se o Sistema está atingindo os objetivos esperados.
- ACT – Etapa onde a manutenção e o melhoramento do Sistema de Gestão da Segurança da Informação é pratica constante. As ações a serem tomadas nessa fase são a verificação da adequação do Sistema de Gestão da Segurança da Informação em relação aos objetivos iniciais; a proposição de melhorias ao Sistema e a definição de novos objetivos de segurança.

3 SEGURANÇA DA INFORMAÇÃO EM COMUNICAÇÕES POR VOZ

Este é o capítulo que une os princípios da Segurança da Informação com os aspectos nos quais as Comunicações por Voz se dão e busca mostrar quais são os ataques possíveis de se fazer em comunicações por voz e como se proteger dos mesmos.

3.1 ASPECTOS GERAIS

Com o desenvolvimento das novas tecnologias, tornou-se possível a evolução dos sistemas de transmissão, o que viabilizou a criação de redes de pacotes muito mais velozes. Todo este desenvolvimento tem permitido a evolução das redes convergentes, que são redes capazes de transportar pacotes de dados e voz digitalizados. Hoje contamos com vários tipos de redes que são capazes de transportar pacotes de dados e voz, por exemplo, redes baseadas em ATM, *Frame Relay* e TCP/IP. Destas apenas o *Frame Relay* e o TCP/IP são utilizados com mais frequência, embora o ATM tenha sido projetado para tal finalidade. O transporte através da tecnologia *Frame Relay* e TCP/IP são conhecidos como VoFR e o VoIP.

A diferença entre a utilização de tais redes é referente ao seu custo/benefício. As redes IP, estão associadas à camada 3 do modelo OSI, o que lhe dá muitas vantagens, entre elas o baixo custo e capacidade de operação em redes heterogêneas, em contrapartida recebe como desvantagens a qualidade de serviço e questões relacionadas com a segurança. Já as redes VoFR e VoATM, estão associadas com acamada 2 do modelo OSI, que então apresentam como vantagem, maior qualidade de serviço pois requerem redes homogêneas para o tráfego de informações, e como desvantagem, um custo elevado. (GALVÃO e ZATTAR, 2003)

A TiSafe, empresa brasileira de TIC, identifica vários equipamentos passíveis de receberem ataques em redes VoIP, a Fig. (11) abaixo demonstra de forma simples e didática estes locais com vulnerabilidades.

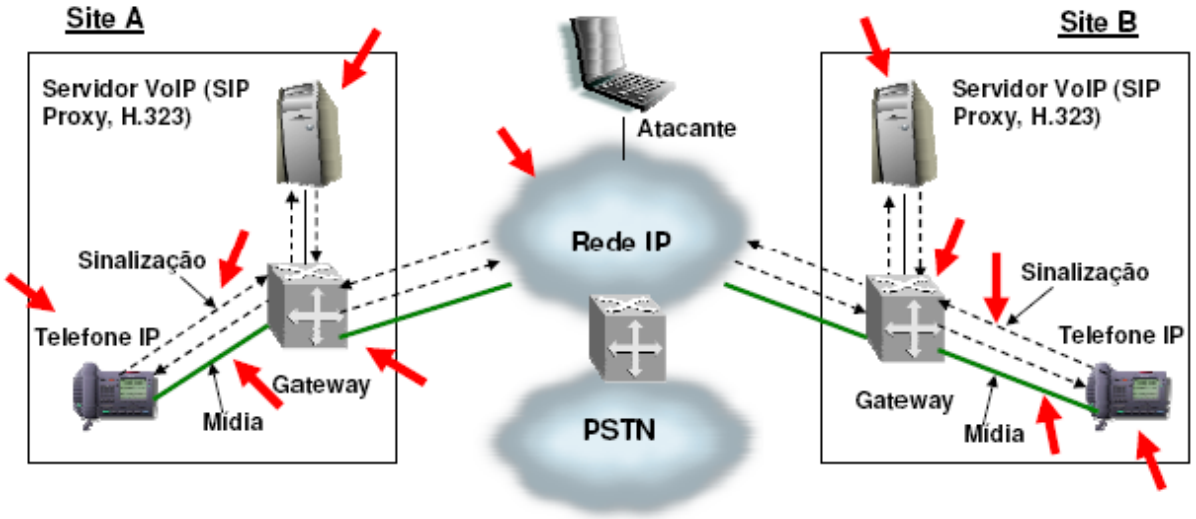


Figura 11 – Alvos de ataques em redes VoIP (TI SAFE - SEGURANÇA DA INFORMAÇÃO, 2010)

3.2 VULNERABILIDADES

As vulnerabilidades do VoIP abrangem não só as falhas inerentes ao aplicativo de VoIP em si, mas também nos sistemas operacionais subjacentes. A complexidade de VoIP cria um grande número de vulnerabilidades que afetam as três áreas clássicas da segurança da informação: confidencialidade, integridade e disponibilidade. Abaixo, na Tab. (4), McGann e Sicker (2005) apresenta uma descrição das principais vulnerabilidades identificadas em seu estudo, separando-as de acordo com o modelo de camadas TCP/IP, embora muitas dessas vulnerabilidades possam atravessar camadas.

Tabela 4 – Vulnerabilidades VoIP por camadas

Camada	Vetor de Ataque	Confidencialidade	Integridade	Disponibilidade
Interface de Rede	*Físico*	x		X
	ARP Cache	x	x	X
	ARP Flood			X
	MAC Spoofing	x	x	X
Interrede	*IP Spoofing*			
	Dispositivo	x	x	X
	Redirecinamento via IP Spoofing	x	x	X
	Pacotes mal formados	x	x	X
	Fragmentação de IP	x	x	X
	Jolt			X
Transporte	*TCP/UDP flood*			X
	TCP/UDP replay	x	x	
Aplicação	*Inserção de TFTP Server*		x	
	Inserção de DHCP Server		x	
	Anulação de DHCP			X
	ICMP flood			X
	SIP			
	Sequestro de registro	x	x	X
	Sequestro MGCP	x	x	X
	Modificação de mensagens	x	x	
	Inserção de RTP			
	Spoofing via cabeçalho	x	x	X

Tabela 4 – Vulnerabilidades VoIP por camadas (continuação)

Camada	Vetor de Ataque	Confidencialidade	Integridade	Disponibilidade
Aplicação	*Falso Cancel / bye*			x
	Método mal formado			x
	Método de redirecionamento	x		x
	RTP			
	Redirecionamento SDP			x
	RTP payload			x
	Adulteração de RTP	x	x	x
	Criptografia	x	x	x
	Configuração padrão	x	x	x
	Serviços desnecessários	x	x	x
	Buffer Overflow	x	x	x
	Redes Legado	x	x	x
	Disponibilidade de DNS			x

Uma observação importante, é que a Tab. (4) não traz ainda aspectos de segurança física, que são um grande problema em todos os sistemas de informação.

3.3 ALGUNS ATAQUES

Hoje, ainda são mínimos os ataques documentados em cima de redes VoIP, talvez pela ainda não familiarização dos "invasores" com os protocolos desta tecnologia. No entanto já é sabido que em um curto espaço de tempo, esta realidade tomará rumos diferentes, isto se deve a vários motivos, um deles é pelo valor das informações que trafegam pelas redes VoIP, e que em mãos erradas poderão causar grandes prejuízos e lucros a diversas pessoas.

Segundo Galvão e Zattar (2003), é importante ressaltar que na convergência das redes de voz com as redes de dados baseadas em TCP/IP, houve também a convergência das vulnerabilidades inerentes as duas tecnologias. Ou seja, agora, um computador com telefone IP compatível precisa ser protegido tanto das ameaças relacionadas aos computadores quanto das ameaças relacionadas com a telefonia. Por exemplo, um telefone IP instalado em uma estação de trabalho com o sistema operacional MS *Windows* está suscetível às vulnerabilidades do *Windows*.

3.3.1 CAPTURA DE TRÁFEGO E ACESSO INDEVIDO A INFORMAÇÕES

Nas Redes que trafegam voz sobre IP, a voz é transportada juntamente com as informações da rede de dados, encapsulado em pacotes IP, e a captura destes pacotes em uma rede IP através de técnicas de "*Sniffing*" é relativamente trivial. Hoje já podemos contar com algumas ferramentas que facilitam este

trabalho para o usuário, por exemplo, o VOMIT ("V*oice Over Misconfigured Internet Telephones"),* que utiliza a ferramenta tcpdump do Unix para capturar pacotes de uma conversa telefônica, que está trafegando na rede de dados e consegue remontá-los e convertê-los em um formato comum de áudio (*.wav). Ou seja, trata-se de uma espécie de "grampo telefônico" em plena rede de dados. No entanto estas ferramentas estão começando a surgir agora na internet e ainda encontram-se limitadas a alguns padrões existentes, por exemplo, o CODEC G.711 utilizado pela *Cisco*. Devemos ressaltar que é questão de tempo para que ferramentas mais poderosas se adentrem a internet, já que os mecanismos de transporte de voz, por enquanto, não utilizam criptografia, deixando assim os pacotes vulneráveis a qualquer destas ferramentas existentes.

3.3.2 *CALLER IDENTITY SPOOFING*

Várias outras técnicas que podem ser ou não mais complexas podem ser utilizadas pelos atacantes para obtenção de acesso indevido às informações que trafegam pela infraestrutura onde se localiza a rede VoIP. Por exemplo, no ataque de "*Caller Identity Spoofing*" (algo como "falsificação da identidade do usuário que iniciou a chamada"), o atacante induz um usuário remoto a pensar que ele está conversando com alguma outra pessoa, ou seja, finge ser alguém que não é para obter informações sigilosas. Este tipo de ataque requer apenas que o atacante obtenha acesso físico à rede e consiga instalar um telefone IP não autorizado. Outra técnica que pode ser utilizada é a de ("*MAC Spoofing*"), o atacante deverá conseguir que seu telefone IP assuma a "identidade" de um telefone IP válido da rede empresa.

Boas políticas aplicadas nas empresas podem ser uma boa solução quando se pretende evitar estes tipos de ataques, a integridade da rede aumentará ainda mais se for possível combinar as políticas com uma boa administração da rede, por exemplo, sempre obtendo controle de pontos de rede ativos que não estão sendo utilizados. O treinamento e a boa orientação dos usuários destes tipos de rede, culminarão na dificuldade dos atacantes em se aplicar engenharia social, assim seria mais difícil de se induzir alguém que o atacante é quem ele não é. (GALVÃO e ZATTAR, 2003)

3.3.3 CÓDIGO MALICIOSO

Como já foi visto anteriormente, a tecnologia VoIP está presente nas redes convergentes, ou seja, aquelas redes que trafegam dados e voz no mesmo meio físico. Portanto a tecnologia VoIP também esta susceptível às vulnerabilidades da rede de dados. Algumas das vulnerabilidades que também podem afetar as redes de voz, são os conhecidos vírus, "*Trojan Horses*" e outros tipos de códigos maliciosos que podem vir a infectar os sistemas de telefonia IP baseados em PCs, os "*Gateways*" e outros componentes críticos da infraestrutura. Sendo assim, podemos concluir que até mesmo "técnicas" que não surgiram para afetar as redes VoIP, podem causar a paralisação deste serviço.

3.3.4 FRAUDE FINANCEIRA, USO INDEVIDO DE RECURSOS CORPORATIVOS

Uma das ameaças às redes VoIP é a ameaça de "*Toll Fraud*". Esta ameaça consiste no uso não autorizado dos serviços de telefonia IP ou métodos de fraude para iludir os mecanismos de bilhetagem e cobrança das ligações realizadas. Existem vários métodos para se aplicar esta técnica. Um deles pode ser o uso indevido de um telefone IP 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.

Um método mais sofisticado envolveria a instalação de um "*Voice Gateway*" (ponto de convergência entre as redes) falsificado pelo atacante, pois é neste Gateway que passam todas as ligações. Caso o "*Voice Gateway*" principal não seja comprometido, o atacante deverá tentar instalar na rede um segundo "*Gateway*" e tentar redirecionar para ele o tráfego destinado ao "*host*" original. Desta forma, é possível bloquear, desviar e até mesmo escutar ligações. (GALVÃO e ZATTAR, 2003)

3.3.5 REPÚDIO

Repúdio em relação à tecnologia VoIP tem a ver com a negação, por parte de um usuário que utilizou os serviços de telefonia IP para fazer uma ligação, de que ele tenha realmente feito tal ligação. Isto só

poderá ser comprovado com a implantação de algum mecanismo eficiente para autenticação, do contrário, não será possível identificar os usuários dos serviços, nem discriminar quem executou quais chamadas a partir de quais telefones IP.

3.3.6 INDISPONIBILIDADE DE SERVIÇOS

Devido à utilização da rede de dados para se transportar voz, esta também torna-se vulnerável aos ataques não só destinados à ela como também aos destinados à rede TCP/IP. Um exemplo ao qual ela torna-se vulnerável é ao ataque de DoS ("*Denial of Service*"), os quais causam a paralisação dos serviços em redes TCP/ IP, sendo assim esta paralisação afetará "por tabela" os serviços de voz, fax e vídeo que dependam deste transporte.

São vários os ataques que podem causar negação se serviço em redes TCP/IP, entre eles podemos citar o "*TCP SYN Flood*" e suas variações, e também a exploração de falhas nas pilhas de protocolo dos sistemas operacionais, como no "*Ping of Death*", "*Teardrop*" e vários outros ataques que podem tornar os serviços do VoIP indisponíveis.

Nas redes VoIP, os equipamentos de PBX tradicionais são substituídos por aplicações PBXs IP compatíveis que são executadas, por exemplo, em servidores MS *Windows* NT. Estas aplicações de "*Call Management*" são críticas para a infraestrutura de VoIP, e no entanto estão sujeitas aos ataques que exploram vulnerabilidades não só das próprias aplicações como também do sistema operacional.

3.4 MEIOS DE PROTEÇÃO

3.4.1 SEGMENTAÇÃO DO TRÁFEGO DE VOZ E DADOS

As segmentações do tráfego de voz e dados podem ser feitas utilizando *switches*. Esta segmentação contribui para obtenção de um 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.

Galvão e Zattar (2003) mostra que 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 VoIP, 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 baseado em "*UDP Flood*" no segmento de dados poderia afetar também os serviços de voz se as 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 VLANs distintas. Como por exemplo, em uma instalação de pequeno porte, uma VLAN dedicada ao tráfego de voz seria suficiente, onde seriam instalados o "*Call Manager*" e os telefones IP. Outros componentes como estações de gerenciamento e sistemas de "*Voicemail*" podem residir no segmento de dados. Já em instalações de grande porte, várias VLANs podem ser criadas, tanto para voz quanto para dados. Por exemplo, os serviços de "*Voicemail*" podem ocupar uma VLAN dedicada.

3.4.2 CONTROLE DO ACESSO AO SEGMENTO DE VOZ

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

em outros segmentos. Logo, as portas e protocolos que serão configuradas no firewall irão depender do tipo de solução/fabricante de solução VoIP em uso.

Um aspecto importante ao qual se deve estar atento é ao de que o firewall deve ser compatível com o protocolo H.323. Isto se deve ao fato de que este protocolo aloca portas de forma dinâmica para canais de áudio, vídeo e dados. Alguns fabricantes oferecem "*aplliances*" de *firewall/VPN* customizados para suas tecnologias, como por exemplo, o "*Contivity Secure IP Services Gateway*" da Nortel[7].

3.4.3 NÃO USO DE *PC-BASED PHONES*

Galvão e Zattar (2003) recomenda que a utilização de *softPhones*, ou seja, aplicações de telefonia que rodam sobre arquitetura de computadores, deve ser evitada, sendo uma boa prática a utilização de telefones IP que suportem VLANs, já que os *softPhones* estão sujeitos a um maior número de ataques que os aparelhos de telefonia IP baseados em hardware. Além do risco de falhas em seu próprio código, as aplicações de telefone IP para PCs estão sujeitas às vulnerabilidades do sistema operacional e também de outras aplicações que residem no computador onde estão instaladas, bem como vírus, *worms* e outros códigos maliciosos. Já os telefones IP executam sistemas operacionais proprietários com serviços limitados (e portanto menos vulneráveis). Além disso, como as aplicações de telefone IP para PC precisam residir no segmento de dados da rede, elas são susceptíveis a ataques de negação de serviços (como "*floods*" baseados em UDP ou TCP) que sejam destinados ao segmento como um todo, e não apenas ao computador em que estão instalados.

3.4.4 USO DE ENDEREÇOS PRIVATIVOS NOS TELEFONES IP

Nos telefones IP devem ser utilizados endereços IP privativos. Esta medida servirá para reduzir a possibilidade de que o tráfego de voz possa ser monitorado de fora da rede interna e para evitar que os atacantes consigam mapear o segmento de voz em busca de vulnerabilidades. Além disto o uso de IP's 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*"). (GALVÃO e ZATTAR, 2003)

3.4.5 ASSOCIAÇÃO ENTRE ENDEREÇOS IP ESTÁTICOS E *MAC ADDRESSES*

A utilização do *MAC Address* permite a autenticação dos telefones IP ou seja quando um telefone IP tenta obter configurações da rede do "*Call Manager*", 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 associa-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 da implantação, a associação entre endereço IP estático e "*Mac Address*" nos telefones IP pode ser de difícil gerenciamento.

3.4.6 UTILIZAÇÃO DE SERVIDORES DHCP SEPARADOS PARA VOZ E DADOS

Preferencialmente deve-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.

[7] Nortel – uma das grandes fabricantes de equipamentos de redes de computadores

3.4.7 MONITORAMENTO DE ENDEREÇOS MAC NO SEGMENTO DE VOZ

A utilização de ferramentas como, por exemplo, o *Arpwatch* para monitorar os "*MAC Addresses"* de todos os dispositivos instalados no segmento de voz trará mais segurança à rede. O *Arpwatch* é capaz de registrar alterações não autorizadas na associação entre endereço IP e endereço MAC, através de requisições ARP.

3.4.8 AUTENTICAÇÃO DE USUÁRIOS

Se a tecnologia em uso atualmente suportar, convém implementar os recursos de autenticação dos usuários dos telefones IP, além de autenticar apenas os dispositivos através de seus endereços MAC. Hoje já podemos encontrar com certa facilidade, alguns modelos de telefones IP que exigem do usuário um "*login*" e uma senha ou número de identificação (PIN) válidos para que possam utilizar o dispositivo. Este tipo de autenticação reduz os riscos de uso indevido dos recursos da rede de voz, e permite maior rastreabilidade no uso dos serviços, além de certo nível de não repúdio.

Algumas aplicações de telefone IP para a plataforma MS *Windows* suportam autenticação integrada ao sistema operacional, enquanto outros modelos utilizam uma combinação de nome de usuário/PIN. Em qualquer caso, as senhas utilizadas devem ser trocadas periodicamente e devem ser de difícil dedução.

3.4.9 IMPLEMENTAÇÃO DE UM SISTEMA IDS

É sabido que os sistemas atuais de detecção de intrusão (IDS) ainda não são compostos pelas assinaturas específicas de ataques para os protocolos de VoIP, no entanto eles podem ser úteis para monitorar ataques baseados em UDP e HTTP que podem ser executados contra os componentes da infra-estrutura. Por este motivo, convém que uma aplicação ou *aplliance* de IDS seja instalado no segmento onde estiver instalado o "*Call Manager*", visando a detecção de ataques originados principalmente no segmento de dados, onde estão localizadas as estações de trabalho dos usuários. Naturalmente, é necessário fazer o *tunning* do IDS para maximizar sua eficiência. Esta operação é dependente do tipo de tecnologia e protocolos de VoIP em uso. De qualquer forma, se tiverem sido separados os segmentos de voz e dados como recomendado, o tráfego esperado no segmento de voz estará obrigatoriamente associado a um número limitado de protocolos e portas, o que facilita a configuração do IDS e reduz o número de falsos positivos. Qualquer tráfego TCP/ IP que não esteja relacionado aos protocolos utilizados pela tecnologia VoIP em uso deve gerar alarmes no sistema IDS.

Preferencialmente os atacantes tentam explorar as vulnerabilidades do *Call Manager* da infra-estrutura de VoIP, devido ao grande número de serviços que podem estar sendo oferecidos por estas aplicações. O *Call Manager*, por exemplo, normalmente disponibiliza aplicações para controle de chamadas, permite a configuração via *Web*, dá suporte a serviços de localização de telefones (*IP Phone browsing*), serviços de conferência, e gerenciamento remoto por SNMP. Por este motivo, convém que sejam implementados procedimentos para a configuração segura ("*Hardening*") do servidor onde o *Call Manager* está instalado. Como recomendações genéricas, convém desabilitar todos os serviços desnecessários, instalar os patches do sistema operacional e um bom antivírus. Os serviços inicializados pelo *Call Manager* devem utilizar contas de baixo privilégio, e o acesso físico ao servidor deve ser restrito a usuários autorizados. (GALVÃO e ZATTAR, 2003)

3.4.10 MONITORAMENTO DE PERFOMANCE E STATUS DOS SERVIÇOS VOIP

O objetivo deste controle é permitir a monitoração periódica, se possível em tempo real, do desempenho da rede de voz, e detectar instabilidades, atrasos e latências que possam comprometer a performance ou disponibilidade dos serviços. A monitoração pode ser feita através de soluções proprietárias disponibilizadas pelos fabricantes (Cisco etc.), ou de soluções de mercado como o *VoIP Manager da Net IQ* ou o *VoIP Test Suite da Brix Networks*.

3.4.11 ESTRUTURA DE SUPORTE EM VOIP

Apenas uma boa implantação da estrutura VoIP não é suficiente para garantir sua perfeita funcionalidade durante o decorrer do tempo, devemos aplicar métodos que ajudaram a manter esta implantação em perfeito funcionamento durante sua existência no ambiente. Para isso deveremos, se

possível, ter presente no ambiente que foi implantando a estrutura VoIP uma equipe treinada para realizar configurações necessárias nos equipamentos (*Switches*, Roteadores e etc.) e aplicações utilizados pela rede de voz além de prestar suporte técnico para os usuários. Também é conveniente manter um contrato de Suporte Técnico com algum integrador qualificado, ou com o próprio fabricante dos equipamentos adquiridos.

3.4.12 ACESSO FÍSICO RESTRITO

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, instalar um telefone IP não autorizado e utilizar técnicas de "*MAC Spoofing*" e "*Caller Identity Spoofing*" 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 infraestrutura de VoIP a 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, *Call Manager*, *Firewalls* etc.), seja restrito apenas a usuários autorizados.

3.4.13 AUDITAMENTO DO USO DOS RECURSOS

A verificação da qualidade de serviço prestada pelos equipamentos VoIP 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 etc.) além de informações relacionadas ao QoS (latência, perda de pacotes, uso de banda etc.). A auditoria pode ser implementada através de aplicações especializadas.

Para um auditoria mais precisa, recomendamos que os usuários utilizem algum tipo de autenticação quando utilizarem os serviços da rede de voz.

3.4.14 CRIPTOGRAFIA DO TRÁFEGO VOIP

Recomendamos a criptografia de todo o tráfego passante entre o telefone IP e o "*Call Manager*". Esta medida tem como objetivo impedir o uso de ferramentas como o VOMIT para violação da confidencialidade das conversações.

Um exemplo de criptografia que pode ser utilizada para tal ambiente seria a implantação de um túnel IPSec entre as estações com telefones IP e o "*Call Manager*". Para as comunicações externas (matriz com filiais, por exemplo), deve-se considerar a implementação de uma VPN ("*Virtual Private Network*") para criptografar o tráfego de VoIP.

Tendo em mente o que foi dito neste capítulo, podemos entender os riscos (telefones IP, roteadores, *Switches*, *Gateways*, sistemas de "*Voicemail*", *Firewalls* e outros) e problemas (*delay*, *jitter*, perda de pacotes, "*Toll Fraud*" (fraudes de pagamento), *IP Phone Spoofing* etc.) inerentes pelos quais as redes de voz estão vulneráveis. Compreendemos ainda que estes riscos e problemas aumentam caso a estrutura da rede de voz esteja na mesma estrutura da rede de dados, pois assim a rede de voz herdará todos os perigos das redes de dados (mapeamentos, TCP/IP *Denial of Service*, exploração das vulnerabilidades dos sistemas operacionais, engenharia social, roubo de identidade e *spoofin* etc.), isto porque a convergência das redes traz também a convergência das ameaças. É óbvio que um bom sistema de autenticação não só dos dispositivos (telefone IP e etc) como também do usuário é muito importante para um controle mais preciso do ambiente da rede de voz, evitando assim que ferramentas como o VOMIT possam vir a comprometer a confidencialidade das conversas telefônicas, permitindo acesso indevido a informações sigilosas, além de outros problemas como repúdio, etc.

3.4.15 TRATAMENTO DIFERENCIADO PARA TRÁFEGO DE MÍDIA NO FIREWALL

Ao fazer uma inspeção avançada dos protocolos de telefonia deve ser observada a forma com que os protocolos de sinalização de Telefonia IP (que podem usar transporte TCP ou UDP) negociam as portas UDP destinadas aos canais de mídia (RTP/RTCP). Moraes (2012), enumera algumas dessas práticas:

- Se os firewalls inseridos entre os elementos de sinalização não entenderem perfeitamente a natureza do protocolo em uso (SCCP, SIP, H.323 ou MGCP), não serão capazes de criar corretamente as conexões RTP/RTCP.
- As conexões devem ser dinamicamente terminadas para liberação de recursos. Para materializar tal possibilidade é importante que o firewall suporte *timeouts* diferenciados para as sessões de controle e mídia.
- Os protocolos de sinalização de voz tipicamente incluem o endereço IP em seu *payload* (camada de aplicação). Desta forma, caso as comunicações se estabeleçam em ambientes com NAT ou PAT, é fundamental que o firewall tenha consciência de tais características para que possa efetuar as traduções de endereços IP nas camadas 3 e 7 simultaneamente.
- A Telefonia IP tem a capacidade de prover confidencialidade para a voz transportada, usando, por exemplo, sinalização sobre TLS (*Transport Layer Security*) para então derivar os canais *Secure RTP* (SRTP) para mídia Em termos práticos, esse atrativo pode significar deixar de implementar criptografia de voz, uma vez que o firewall não consegue entender a sinalização cifrada e teria, portanto, que deixar um grande número de portas UDP (associadas ao SRTP) abertas.

4 ESTUDO DE CASO

Este capítulo apresenta o estudo de caso da análise de Gestão de Riscos feita em um laboratório a fim de identificar as vulnerabilidades existentes e as ameaças que possam por ventura se aproveitar dessas vulnerabilidades.

4.1 CONTEXTUALIZAÇÃO DO AMBIENTE

O presente trabalho tem como um dos objetivos a análise de um ambiente de comunicações unificadas sob o ponto de vista da tríade de SI – confidencialidade, integridade e disponibilidade. O ambiente em questão está baseado no escritório da multinacional estadunidense do ramo de redes de computadores, Cisco Systems Inc, em Brasília-DF.

Intitulado "*Security UC Lab*", este laboratório é focado em demonstrar principalmente a integração entre o *appliance* de segurança e o *Call Manager* da Cisco, ou seja, a integração ASA (*Adptative Security Appliance*) / CUCM (*Cisco Unified Communications Manager*), mostrando as diversas opções de criptografia de chamadas sob a ótica dos elementos terminais da rede (IP Phones), do servidor (CUCM) e do *firewall* (Cisco ASA). Além disso, o laboratório foca em como o ASA lida com pacotes de outras formas de comunicação, como vídeo, conferência, *Instant Message* e presença.

4.1.1 TOPOLOGIA

A Figura (12) a seguir ilustra o cenário analisado:

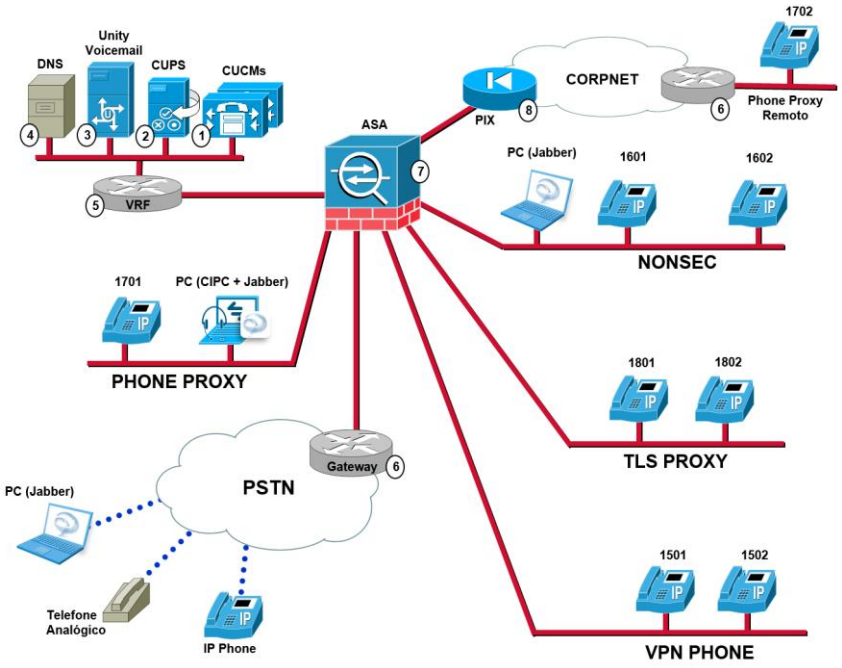


Figura 12 – Topologia básica do ambiente

Na topologia acima, pode-se identificar os seguintes elementos:

1. Cisco *Unified Communications Manager* 8.6 (*Publisher e Subscriber*) - *Call Manager*
2. Cisco *Unified Presence Server* 8.6 (Servidor de *Instant Message and Presence*)

3. Cisco *Unity Express* 8.6 (Servidor de *Voicemail*)
4. Servidor de DNS – *Windows Server* 2008
5. *Virtual Routing and Forwarding* (VRF)
6. Cisco *Router* 2911
7. Cisco *Adaptative Security Appliances* – ASA 5500
8. Cisco PIX

   IP Phones (8), sendo:

   - dois *Cisco IP Phone* 9971 na rede *VPN Phone*;
   - um *Cisco IP Phone* 9951 na rede *TLS Proxy*;
   - um *Cisco IP Phone* 7942 na rede *TLS Proxy*;
   - dois *Cisco IP Phone* 7962 na rede *Phone Proxy*;
   - dois *Cisco IP Phone* 7960 na rede *NONSEC.*

   Notebooks, sendo

   - um com *Cisco Jabber for Windows* e *Cisco IP Communicator* instalados;
   - um somente com o *Cisco Jabber* instalado.

Como análise da imagem (Fig. 12), percebe-se que o ASA é o ponto de interligação da rede, centralizando todos os fluxo de pacotes sobre ele, podendo atuar de modo participativo ou transparente a depender da solução adotada e do tipo de tráfego. Observando a implementação, é notável a presença de 5 importantes subredes envolvidas, sendo uma de servidores e as outras quatro para a telefonia:

- Rede dos Servidores;
- Rede NONSEC
- Rede TLS Proxy
- Rede Phone Proxy
- Rede VPN Phone

Essas redes se conectam com a PSTN através de um *gateway* de voz e com a própria rede corporativa da Cisco, onde o tráfego entrante ainda passa por outro elemento de *firewall*, o PIX. Na rede dos servidores é onde se encontra o *Call Manager*, *Unity* (*voicemail*) e o CUPS (*Presence*), além de serviços adicionais primordiais para um bom funcionamento de uma rede de comunicação, como DNS.

Para cada um das redes o *firewall* identifica claramente as portas associadas ao áudio, porém é necessário criar regras que permitam o uso de serviços auxiliares:

- TFTP – neste caso, as atribuições principais do servidor TFTP são a transferência de arquivos de *firmware* e configuração para os telefones
- Resolução DNS do nome do CUCM (e eventuais serviços complementares).
- DHCP é a escolha tradicional para endereçamento dos IP *Phones*. A opção DHCP 150 informa os telefones sobre o endereço IP do servidor TFTP. Tal funcionalidade pode ser habilitada por interface no próprio Cisco ASA.

Há ainda, na comunicação integrada com as redes tradicionais de telefonia, tarefas adicionais de complexo tratamento no *firewall* para garantir o tráfego seguro. É necessário enfatizar que o *firewall* deve analisar a sinalização da conexão, interferindo o mínimo possível na transmissão de voz para o usuário e que este, por possuir diversas interfaces, pode fazer com que IP *Phones* e servidores estejam e rede distintas, o que inevitavelmente acarretaria na inspeção de mensagens de controle envolvendo os gateways das redes.

Cada uma das redes onde estão os telefones IP tem características próprias de acordo com a tecnologia de segurança implementada. A rede intitulada *NONSEC*, como a tradução da abreviação para o ‘português deixa claro, é a rede onde não há nenhum mecanismo de segurança adicional para registro dos telefones e para chamadas. Essa é a rede inicial para configuração em cada um dos telefones da topologia, pois um boot do telefone nela garante que ele esteja livre de qualquer erro de configuração (por configuração antiga) ou autenticação. Para fins de análise, essa rede foi considerada como uma solução de implementação sem segurança independente a título de comparação.

O ASA é o responsável por proporcionar a segurança para a solução de comunicação unificadas da Cisco, tendo duas funções de transporte chave: *TLS Proxy* e *Phone Proxy*.

O *TLS* (*Transport Layer Security*) *Proxy* fornece a interoperabilidade entre as chamadas de voz criptografadas e o firewall, que provê uma série de serviços para proteger as aplicações de UC e os servidores, inspecionando também a sinalização entre o CUCM e os telefones IP.

A Figura (13) abaixo ajuda a descrever este processo de sinalização:

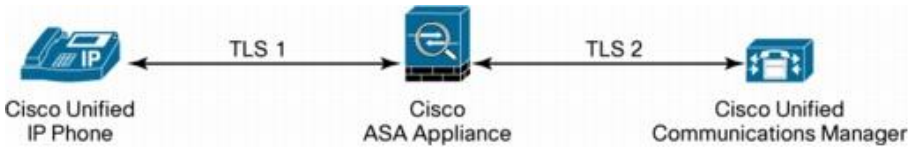


Figura 13 – Conexões TLS utilizadas em uma solução Cisco ASA TLS Proxy (CISCO SYSTEMS INC, 2008)

O ASA intermedia a sinalização entre o telefone e o CUCM, onde funcionar como um *proxy* para os envolvidos, fingindo ser o *Call Manager* para o *IP Phone* e o *IP Phone* para o *Call Manager*. Este tipo de solução não é desenhada para prover criptografia em acessos remotos ou segurança para softphones (como o CIPC – *Cisco IP Communicator* – ou o Cisco *Jabber*).

Neste cenário, após a sinalização, o telefone IP tenta estabelecer um canal SRTP com o destino. Estando numa mesma interface do ASA, esse canal é trivialmente constituído, porém para interfaces distintas, requisitos adicionais de configuração no ASA se fazem necessários.

Um ponto a ser destacado é a relação de confiança que o ASA exerce, tanto com o IP *Phone* quanto com o *Call Manager* ao se inserir entre eles. A Fig. (14) descreve o processo de autenticação TLS.

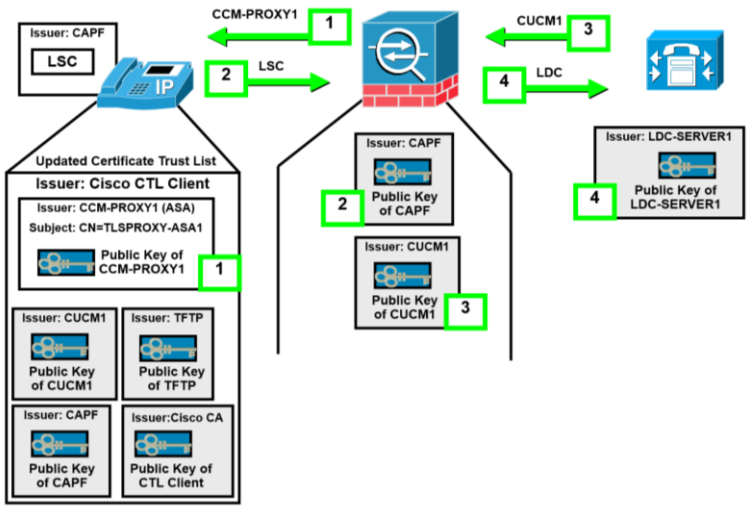


Figura 14 – Relação de confiança da Cisco ASA TLS Proxy (MORAES, 2011)

De acordo com a imagem acima, essa relação é estabelecida da seguinte forma:

1. O ASA apresenta seu certificado ao IP *Phone*, atualizando seu CTL *Client;*
2. Assumindo o uso de LSC, o ASA autentica o LSC apresentado pelo IP Phone, formando um CAPF *trustpoint;*
3. Outro CAPF *trustpoint* é criado no ASA, para autenticar o CUCM (ou outro servidor como o CUPS ou o *Unity Express*);
4. Uma CA conhecida como LDC *(Local Dynamic Certificates*) é criada no ASA para gerar os certificados dos IP *Phones* e para enviar esses certificados ao CUCM.

Já o *Phone Proxy* utiliza o recurso de criptografia nativo dos telefones IP da Cisco para se comunicarem seguramente através da internet ou externamente a LAN.

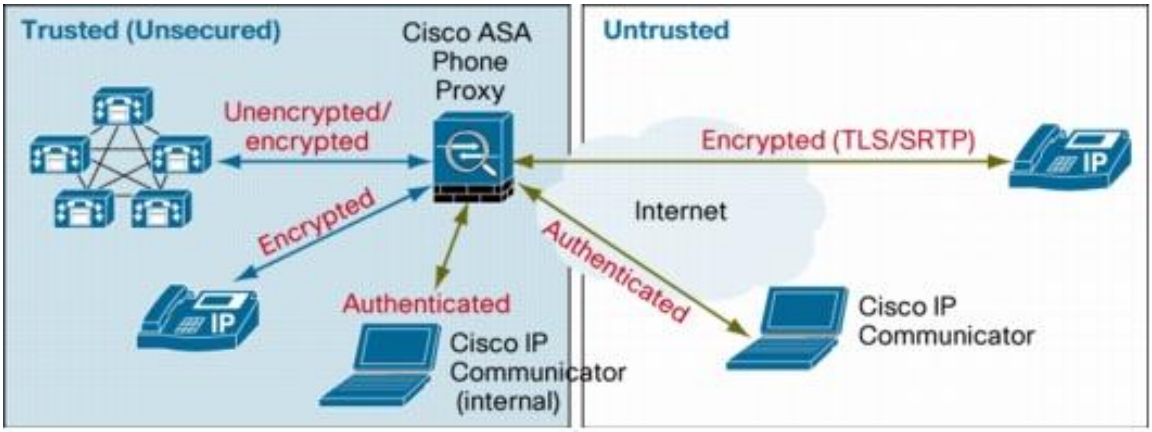


Figura 15 – Implementação da solução Cisco ASA Phone Proxy (CISCO SYSTEMS INC, 2008)

A Figura (15) acima mostra o nível de comunicação permitido com o *Phone Proxy*. IP *Phones* externos a rede segura podem utilizar a criptografia nativa para garantir confidencialidade e integridade ao se conectar remotamente ao cluster CUCM, sem que haja a necessidade da adição de elementos de segurança no site remoto.

Outro ponto de distanciamento entre o *Phone Proxy* e o *TLS Proxy* é o fato de que o primeiro permite que a conexão entre o ASA e o CUCM não seja necessariamente criptografada. Somado a isso, o ASA *Phone Proxy* resolve o desafio de prover a segurança entre VLANs, o chamado *Secure VLAN Traversal Challenge*, possibilitando a comunicação autenticada entre *softphones* (no caso o *Cisco IP Communicator*). Segundo Moraes (2011), essa capacidade é garantida habilitando-se o ASA *Phone Proxy* na interface de dados da rede, para que o ASA faça com que haja a autenticação e criptografia do *softphones* antes de permitir a comunicação através da *Voice VLAN*.

Da mesma forma que acontece para IP *Phones*, a comunicação com o uso de *softphones* permite que se tenha na topologia um computador remoto com um software desenvolvido para fazer chamadas telefônicas pela a internet comunicando-se com um terminal de mídia local a rede de maneira autenticada, conforme pode ser visto na Fig. (15).

O *ASA Phone Proxy* faz uma inspeção na sinalização de estabelecimento da chamada, de modo a garantir que o canal de mídia seja roteada passando pelo ASA *Appliance.* Ou seja, o ASA provê, dentre uma série de atribuições, funções de *proxy* e de criptografia tanto para o processo de sinalização das chamadas quanto para o tráfego de mídia propriamente dito. No caso da solução Cisco ASA *Phone Proxy*, este tráfego é do tipo SRTP (*Secure Real Time Protocol)*, que implementa mecanismos de segurança ao tradicional RTP.

A Tabela (5) abaixo mostra algumas funcionalidades da solução *Cisco ASA Phone Proxy*:

Tabela 5 – Funcionalidades do Phone Proxy[8]

Funcionalidades	Cisco ASA Phone Proxy
Suporte para SCCP (Skinny Client Control Protocol – Protocolo de sinalização proprietário Cisco para redes VoIP)	Sim
Suporte para SIP	Sim
Suporte para Soft Phones	Sim (no modo não seguro)
Autenticação de dispositivos	Sim
Suporte para mais de um dispositivo de acesso remoto	Sim
Criptografia para o CUCM em modo seguro	Sim
Criptografia para o CUCM em modo não seguro	Sim
Suporte para Cluster CUCM	Sim
Escalabilidade	10.000 sessões proxy UC no Cisco ASA 5580 *appliance*

Por fim, temos a opção de arquitetura de redes de comunicações unificadas com o emprego de VPN (*Virtual Private Network*) em contrapartida as solução de criptográfica chave naturalmente implementáveis no CUCM/ASA. Soluções VPN geralmente são independentes e plataforma, provendo confidencialidade como um serviço, utilizando-se de uma única arquitetura para prover criptografia tanto para voz quanto para dados em geral. Geralmente, essa solução não é parte integrante da implementação do *Call Manager*, sendo necessária sua configuração nos roteadores da rede e no firewall. Telefones mais novos (como o Cisco *IP Phone* 9971 utilizado em parte da topologia) possuem um cliente VPN nativo que se integra perfeitamente nesse cenário.

Quando fala-se de VPNs, basicamente a segurança da comunicação é garantida através do estabelecimento de um túnel seguro entre as origem e destino do tráfego, o que estende os benefícios da VPN, normalmente pensada para pacotes de dados, a todo o tráfego do túnel, incluído o tráfego IP que a infraestrutura de comunicações por voz demanda, como presença, SMS e IM (*Instant Message*). Em contraposição a estes benefícios, protocolos VPN (como IPSec e SSL) podem introduzir um *delay* extra no tráfego de voz, o que, dependendo dos níveis, por comprometer significativamente a comunicação. Este acréscimo de *delay* é resultado principalmente pelo fato destes protocolos trabalharem sobre TCP, que é um protocolo de transporte orientado a conexão.

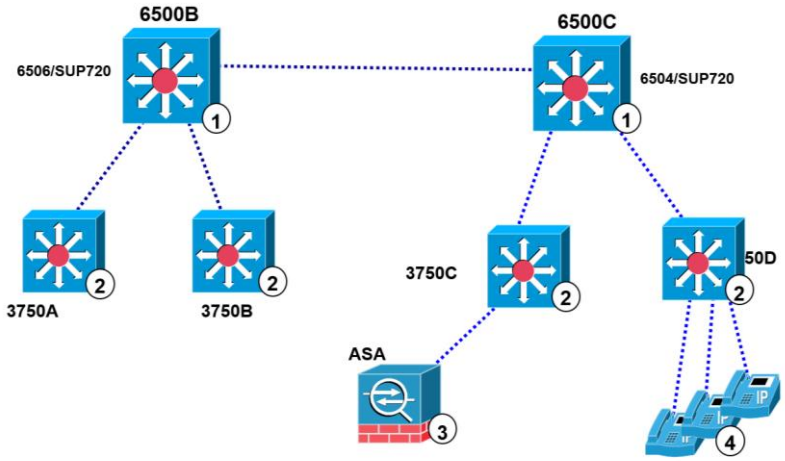


Figura 16 – Core da rede do laboratório do estudo de caso

[8] Tabela extraída de Cisco Systems (2008)

Voltando ao caso de estudo (Fig. 16), a topologia física dos switches de acesso ao laboratório de UC da Cisco é arquitetada. Os equipamentos do core da rede podem ser identificados como:

1. *Cisco Catalyst Switch* 6500 *Series*
2. *Cisco Catalyst Switch* 3750 *Series*
3. *Cisco Adaptative Security Appliances* – ASA 5500
4. *Cisco IP Phones*

Por ela, pode-se perceber que todos os telefones internos estão plugados no *switch* denominado 3750D – excetuando-se o *IP Phone* remoto da rede *Phone Proxy* que está conectado em um ponto da rede corporativa, como pode ser visto na Fig. (12). Já conexão com os servidores é feita através do 6500B, utilizando um esquema de servidores virtuais, conforme é mostrado abaixo (Fig.17):

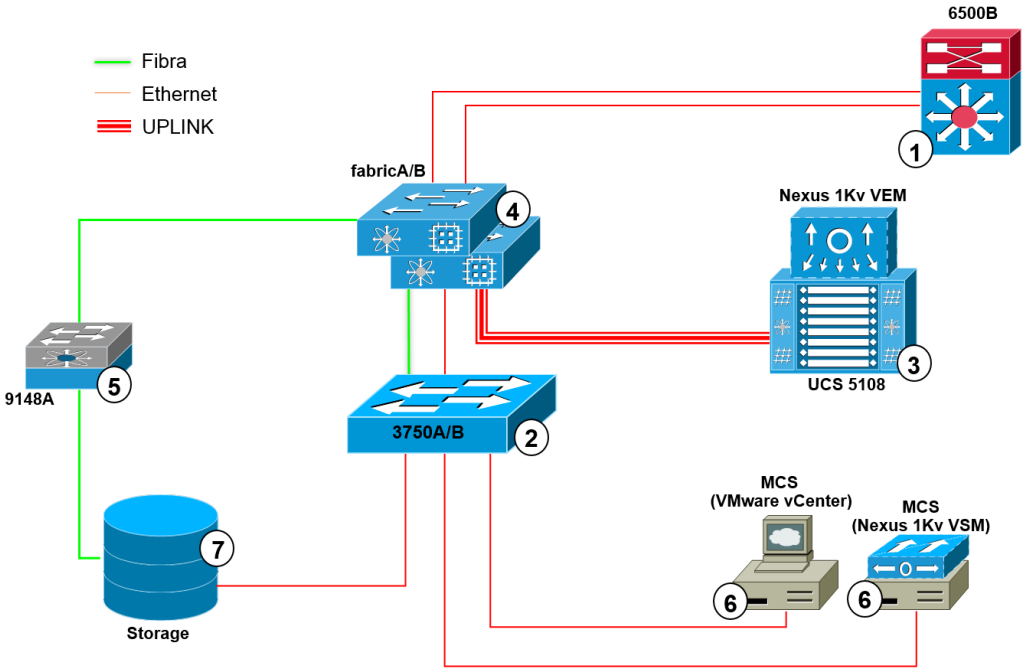


Figura 17 – Acesso ao UCS e ao *storage* do laboratório do estudo de caso

Os seguintes elementos podem ser identificados no acesso ao laboratório:

1. *Cisco Catalyst* 6500 *Series*
2. *Cisco Catalyst* 3750 *Series*
3. *Cisco UCS* 5108 *B-Series*
4. *Cisco Fabric Interconnect* (redundantes)
5. *Cisco MDS* 9148
6. *Cisco MCS*
7. *Nexan Storage SataBeast*

Tendo como base as três figuras acima (Fig. 12, 16 e 17), pode-se ter uma base de como é estruturada a topologia. Os servidores utilizados estão virtualizados sob ESX 5 da *VMware* instalado no UCS e armazenado no *storage*. A interconexão deste servidor virtualizado e a rede é feita no *Fabric Interconnect* A/B e o gerenciamento através do *vMware vCenter* instalado sobre uma máquina independente (MCS).

O distanciamento físico entre telefones e servidores feito adotando um esquema de LAN virtuais estendidas e roteáveis de acordo com as necessidades da rede. Por fim, tem-se os *gateways*, que são o

elo de comunicação com a PSTN e com a CORPNET (rede corporativa), que ainda conta com uma segurança adicional fornecida pelo PIX.

4.1.2 POLÍTICAS DE SEGURANÇA E USUÁRIOS

O acesso físico ao laboratório é permitido somente para alguns dos funcionários da Cisco mediante autorização do responsável pelo laboratório. Este acesso é garantido via cartão de acesso magnético.

O acesso lógico a rede do laboratório em questão é feito via rede corporativa mundial da Cisco, de uso exclusivo de seus funcionários e pessoas devidamente autorizadas. Em cada um dos computadores, servidores e equipamentos de rede do ambiente há ainda senha própria cujo conhecimento é restrito aos responsáveis pelo ambiente descrito e por outros ambientes de simulação que compartilhem ativos físicos e/ou de software com este.

Este ambiente possui como usuários, os próprios responsáveis por sua configuração e manutenção e pessoas envolvidas na demonstração deste laboratório.

4.2 PONTOS DE VULNERABILIDADES ENCONTRADOS

Observando a topologia utilizada para este laboratório, podem-se destacar alguns pontos de interesse do ponto de vista da Segurança da Informação. A imagem abaixo (Fig. 18), analogamente a Fig. (11), que mostra para uma solução geral os principais pontos de ameaças e vulnerabilidades presentes neste tipo de ambiente, tem a função de fornecer estes mesmos insumos para o caso específico utilizado.

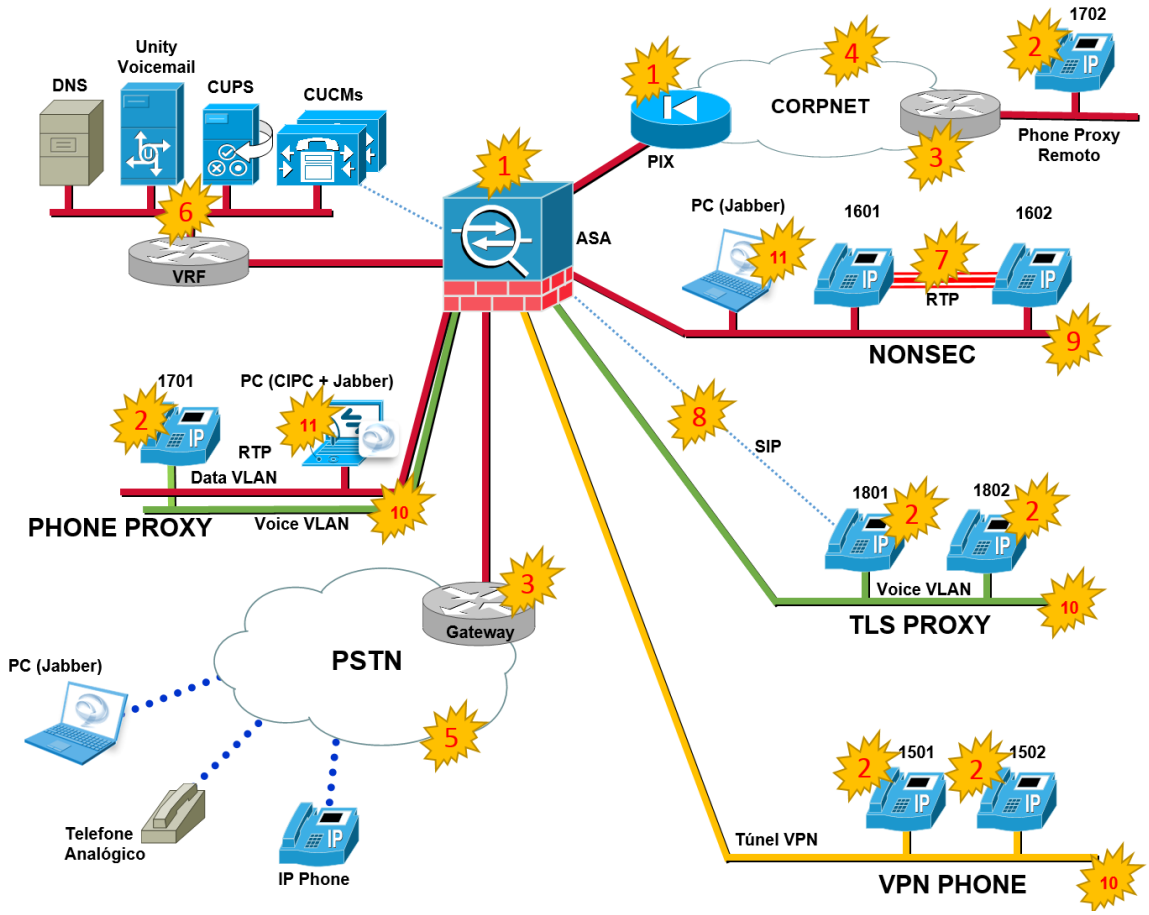


Figura 18 – Pontos de vulnerabilidades do ambiente

Da figura acima (Fig. 18), pode-se identificar em que ponto, de uma maneira geral, a rede pode estar vulnerável a um ataque. Essa identificação feita independe da solução posteriormente analisada, já que seu intuito é basear a própria análise. Na topologia em questão, tem-se portanto, os seguintes ataques:

1. Ataque diretamente aos elementos de *firewall* (ASA e PIX);
2. Ataques diretamente aos IP *Phones;*
3. Ataques diretamente nos *gateways;*
4. Ataques oriundos da rede corporativa;
5. Ataques oriundos da rede PSTN;
6. Ataques diretamente nos servidores;
7. Ataque no fluxo de mídia;
8. Ataque na sinalização;
9. Ataque na VLAN compartilhada;
10. Ataques nas redes dos telefones (intercomunicação com os switches de acesso);
11. Ataques aos *notebooks*

Tendo esses pontos em mãos, pode-se analisar a topologia para buscar que tipo de ameaças podem se aproveitar deles a fim de prejudicar a rede. Porém, antes de prosseguir com análise, cabe restringi-la somente para a comunicação de cada uma das redes com a PSTN, uma vez que o tráfego entre as 5 redes da topologia (servidores + redes de telefones) e o tráfego pela rede corporativa são regidos pelos elementos de firewall do laboratório, atuando o PIX como um controlador de entrada dos pacotes da CORPNET e o ASA como o elemento centralizador de segurança interno ao ambiente. Nesse sentido, o trafego internos a cada uma das redes propostas, entre elas e em relação a rede corporativa não objeto de análise deste trabalho.

5 RESULTADOS

A ideia do capítulo é apresentar a partir da teoria geral e do estudo de caso, ou seja, dos capítulos 3 e 4, um conjunto de recomendações que busque diminuir as possíveis vulnerabilidades de uma comunicação por voz que seja feita sobre IP.

5.1 AMEAÇAS PRESENTES NA TOPOLOGIA

As vulnerabilidades identificadas no capítulo anterior são bases para a análise da forma como ameaças podem explorar a topologia. Sabendo que o estudo de caso em questão trata da demonstração de soluções de segurança (criptografia, principalmente) sob a ótica de três visões de implementação (*TLS Proxy*, *Phone Proxy* e *VPN Phone*), a análise foi feita restringindo, para cada caso, a comunicação entre a implementação de segurança na rede (e para o caso *NONSEC*) com a rede PSTN, como pode ser visto nas tabelas (Tab. 6, 7, 8 e 9) abaixo.

Tabela 6 – Ameaças encontradas para o caso *NONSEC*

Tipos de Ameaças	Ameaças
Confidencialidade	Escuta clandestina de chamadas
	Acesso não autorizado (físico)
	Gravação de ligações
Disponibilidade	Buffer overflow
	Worms e Vírus
	DoS de infraestrutura física, de sinalização e de fluxo de mídia
Autenticidade	Falsificação do identificador de chamada
	Sequestro de sessão
	Redirecionamento de tráfego
	Injeção de tráfego
Crimes	Roubo de serviços na parte do cobrador
	Roubo de dados
SPIT[9]	Chamadas não solicitadas
	Sobrecarga no voicemail

A Tabela (6) é referente a implementação de UC em uma rede sem segurança dita *NONSEC*. A comunicação analisada neste caso é uma ligação de um IP Phone para um telefone (IP ou não) através da PSTN. A Fig. (19) ilustra este cenário específico.

[9] SPIT é conhecido como sendo o "spam over IP Telephony", em outras palavras, spit são as mensagens não solicitadas que chegam por meio de Voz sobre IP (VoIP) aos usuários da tecnologia (VOLTAN JÚNIOR, 2005).

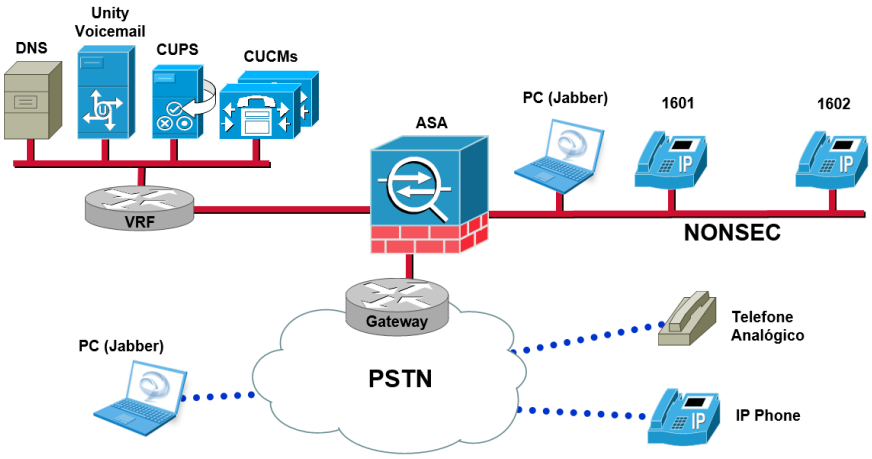


Figura 19 – Implantação da solução sem segurança (NONSEC)

Neste caso, praticamente todas as ameaças existentes em redes VoIP tem um ponto de vulnerabilidade na rede para explorar. Por padrão, a solução de telefonia IP da Cisco possui alguns aspectos de segurança que minimizam algumas ameaças, mais ainda sim uma rede totalmente desprotegida é um convite para atacantes. Com uma configuração simples no CUCM é possível habilitar a criptografia nativa do Cisco *IP Phone*, que adota um sistema de certificados visando garantir o tráfego seguro entre o CUCM e o telefone, independente do uso de um *firewall*. No ambiente analisado, este tipo de configuração não foi adotado, o que nos leva a analisar o ambiente intitulado *NONSEC* como descrito na Tab. (6) acima.

Para o caso específico da comunicação entre o *Cisco Jabber* – em modo *softphone* – e um dispositivo na rede PSTN, não existe diferenças quanto aos níveis de segurança da informação quando comparado com a comunicação entre um *IP Phone* e essa rede, pois a rede *NONSEC* não possui divisão de VLANs de dados e voz, consequentemente o tráfego é único. Essa característica traz perigo à segurança da comunicação.

Tabela 7 – Ameaças encontradas para o caso *TLS Proxy*

Tipos de Ameaças	Ameaças
Confidencialidade	Acesso não autorizado (físico) Gravação de ligações
Disponibilidade	DoS de infraestrutura física, de sinalização e de fluxo de mídia
Autenticidade	Injeção de tráfego
Crimes	Roubo de serviços na parte do cobrador Roubo de dados

A análise do cenário descrito na Fig. (20) é mostrada na Tab. (7). O emprego da solução *TLS Proxy* garante segurança à sinalização das chamadas, já que este tipo de tráfego é direcionado ao ASA que faz a mediação entre o *IP Phone* e o *Call Manager*. O tráfego de mídia é feito sobre SRTP (*Secure RTP*), porém ainda é suscetível a ataques de *flood* quando a comunicação com a PSTN é feita, isso por que, para este tráfego é estabelecido um canal somente entres os *endpoints* envolvidos na conversação sem que o ASA participe do caminho escolhido.

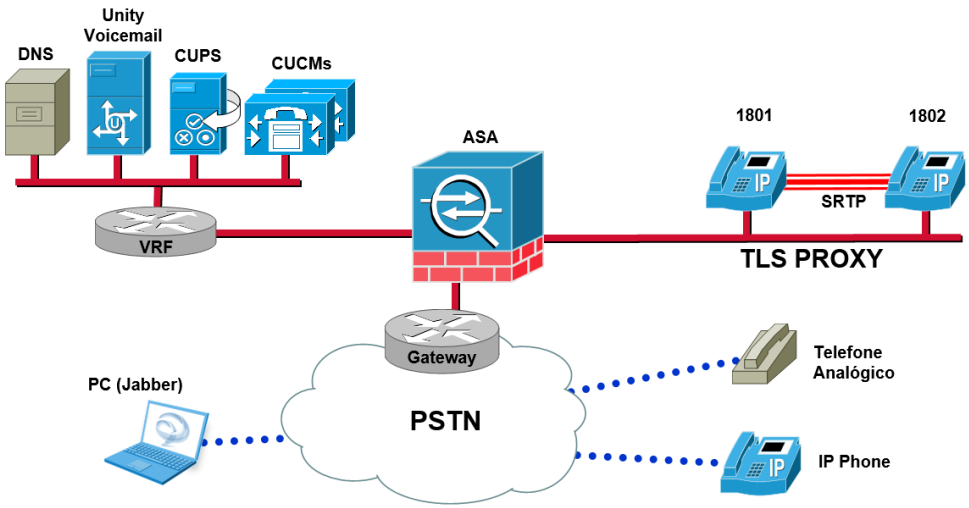


Figura 20 – Implantação da solução *TLS Proxy*

A comunicação externa com a rede de servidores é controlada pelo ASA, porém a medida que o canal SRTP é formado com o *Voicemail* (sem o *firewall* no meio) este também pode estar sob influências dessas ameaças.

Tabela 8 – Ameaças encontradas para o caso *Phone Proxy*

Tipos de Ameaças	Ameaças
Confidencialidade	Acesso não autorizado (físico)
Disponibilidade	DoS de infraestrutura física, de sinalização e de fluxo de mídia

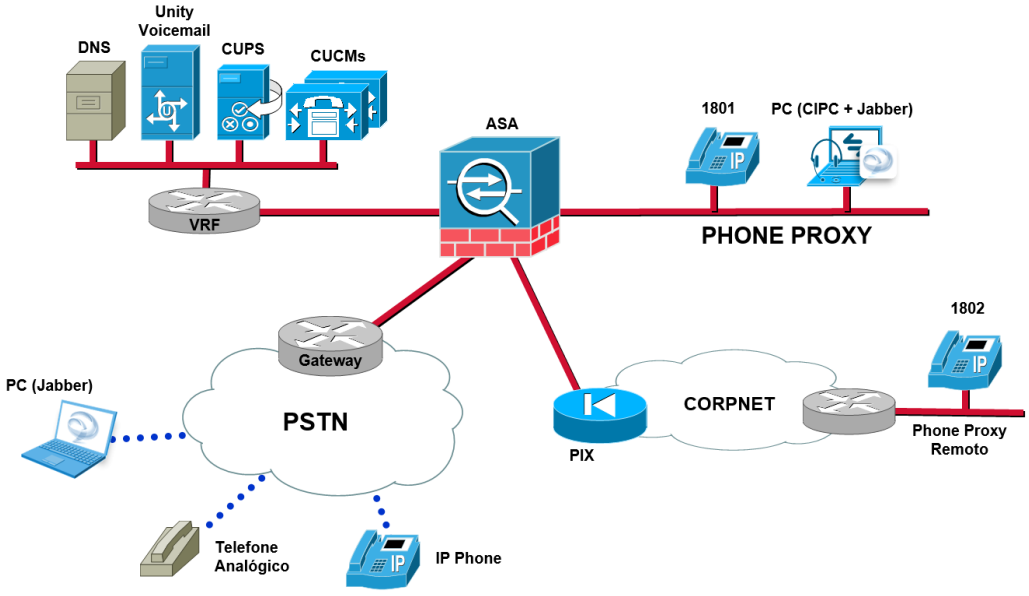


Figura 21 – Implantação da solução *Phone Proxy*

A terceira tabela (Tab. 8) é a análise da implementação do *Cisco ASA Phone Proxy* (Fig. 21). Este tipo de rede é ainda mais completo do ponto de vista de segurança da informação, ao fazer com que o tráfego de mídia também seja direcionado ao ASA. Neste tipo de rede, assim como nas anteriores, o acesso físico aos equipamentos é uma vulnerabilidade que independe da tecnologia de segurança adotada. Como foi dito no item 4.1.2 este acesso é totalmente controlado no ambiente de laboratório e no escritório.

De acordo com a implementação do *Phone Proxy* o tráfego de voz e dados é separado pelo emprego de VLANs distintas. Neste caso, quando há comunicação entre os *Softphones* (CIPC e *Cisco Jabber*) e a PSTN o tráfego segue na VLAN apropriada, ou seja, o tráfego de voz na *Voice VLAN* e os pacotes oriundos do computador seguem na *Data VLAN*. Essa divisão de camada dois proporciona uma proteção quanto a ataques entre VLANs, dificultando o ataque ao tráfego de voz através da VLAN de dados.

Tabela 9 – Ameaças encontradas para o caso *VPN Phone*

Tipos de Ameaças	Ameaças
Disponibilidade	DoS de infraestrutura física, de sinalização e de fluxo de mídia

Redes VPN, como se pode perceber na Tab. (9) acima, eliminam praticamente os pontos de vulnerabilidades. A segurança de todo o tráfego, inclusive o tráfego de mídia, entre os pontos envolvidos na comunicação é garantida estabelecendo-se o túnel seguro – a Fig.(22) mostra esta implementação de forma isolada. Como o túnel é uma entidade virtual, a ameaça de confidencialidade decorrente do acesso não autorizado é eliminada. A única ressalva feita a esta implementação, assim como a qualquer outra, é que ainda é possível a realização de ataques *DoS* de infraestrutura física, que somente pode ser mitigado através de políticas de segurança que foquem na gestão de ambiente e pessoas, o que independe da tecnologia aplicada.

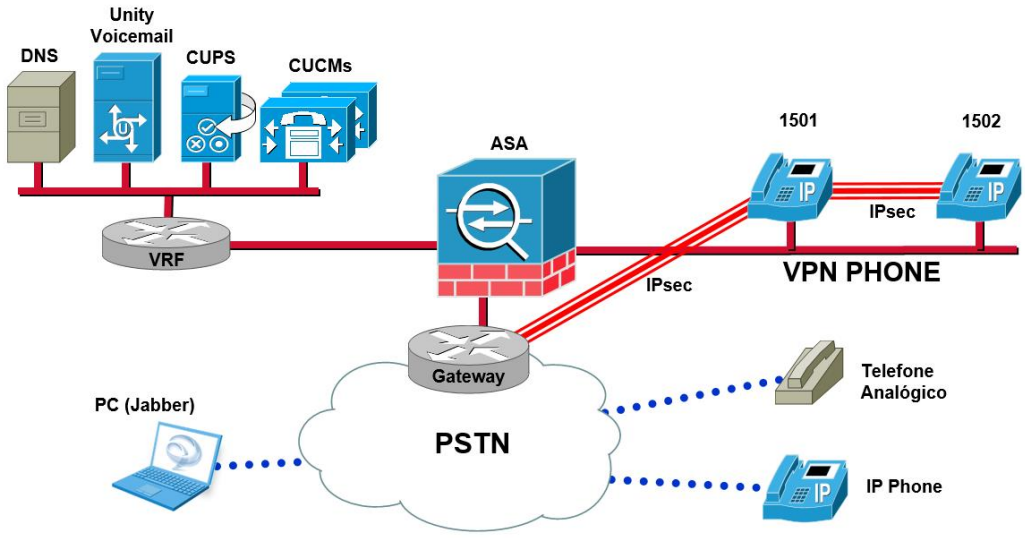


Figura 22 – Implantação da solução *VPN Phone*

Ainda existe um ponto a ser analisado da topologia: a comunicação entre os dispositivos de *Instant Message and Presence* (*Cisco Jabber for Windows*), seja internos à topologia ou com algum outro que esteja situado na PSTN.

A Figura (23) abaixo foca nesses elementos:

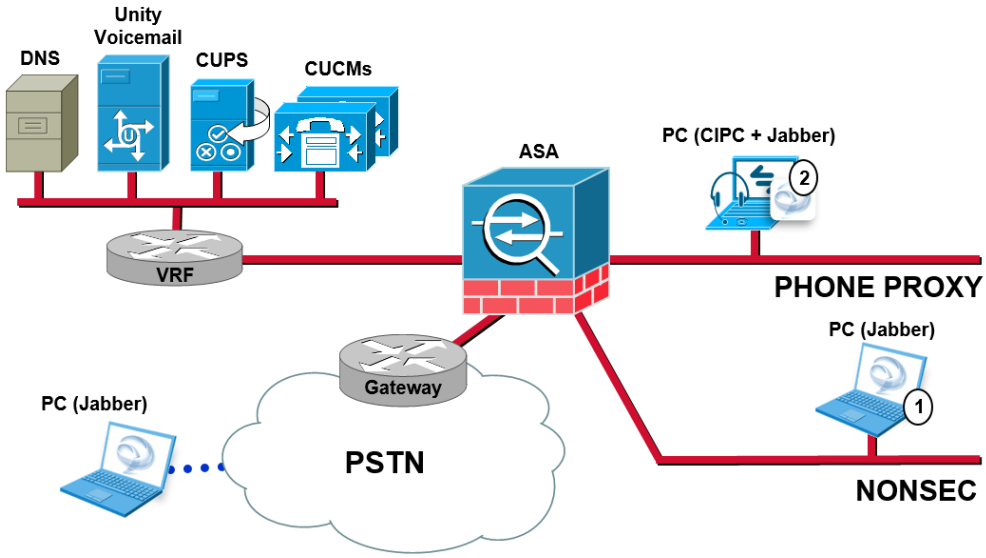


Figura 23 – Implantação da solução de IMP (*Cisco Jabber*)

No caso de ambos os dispositivos estarem dentro do ambiente seguro, o ASA garante a proteção à comunicação, desde que as portas apropriadas para este tipo de comunicação tenham o tratamento adequado.

Quando o tráfego é destinado ou oriundo da PSTN a análise quanto a segurança é análoga ao caso do NONSEC para o elemento 1 da figura acima (Fig. 23) e análogo ao *Phone Proxy* para o elemento 2 da mesma figura.

5.2 *BEST PRACTICES*

A análise da seção anterior permite propor uma série de recomendações para cada uma das abordagens utilizadas na metodologia. A referência para essas proposições é dada no Capítulo 3 deste trabalho.

5.2.1 NONSEC

Como visto anteriormente essa rede não possui proteção adicional, o que implica na necessidade de boas políticas de segurança da informação desde gerência de pessoas e ambientes até a proteções em nível de configuração. A primeira recomendação para esta rede é a segmentação do tráfego de voz e dados em VLANs distintas, que dificulta o aproveitamento do tráfego de dados como degrau para o tráfego de voz e faz com que o uso de s*oftphones* não seja tão prejudicial à segurança da rede.

Outra boa prática é a adoção de IPs privados para os *IP Phones*, *softphones* e servidores. Essa ação garante o acesso a esses dispositivos exclusivamente quando provenientes de dentro da rede. É aconselhável que a atribuição de um endereço IP seja estática, porém, quando a atribuição for dinâmica, deve-se usar um servidor DHCP diferente para cada uma das VLANs. O PABX IP deve ter uma base de dados referente aos *MAC Adressess* – como já está presente nesta implementação – e aos seus IPs de cada um dos dispositivos configurados.

As recomendações acima proporcionam um nível de segurança mínimo mas que não elimina as vulnerabilidades inerentes a um sistema VoIP. Esse nível pode ser incrementado com o uso de dispositivos de segurança de redes, como o *firewall* e o IDS. Esses equipamentos garantem a proteção da rede através do controle do acesso tanto de usuários comuns quanto de possíveis atacantes, agem como um gerenciador de certificado garantindo que a criptografia do tráfego de voz e de sinalização

na rede tenha sua confidencialidade protegida e possibilitam o controle da entrada de pacotes na rede, o que em grande quantidade poderia ocasionar um *DoS*.

Obviamente essas recomendações de nada valem sem uma boa política de controle de acesso físico aos equipamentos bem como o monitoramento constante da rede e de seus recursos e a disponibilidade de uma equipe de suporte técnico qualificada.

5.2.2 TLS PROXY, PHONE PROXY E VPN PHONE

A presença do firewall (ASA) como intermediador do tráfego nessas redes traz consigo toda a proteção descrita na Seção anterior. A diferença se dá de acordo com os níveis de profundidade com que o ASA age em cada uma das redes. Para o *TLS Proxy* o tráfego de mídia propriamente dito ainda é vulnerável a ameaças, pois a função do ASA é restrita à sinalização. Para diminuir este tipo de vulnerabilidade presente na rede, é aconselhável que se faça a criptografia tanto da sinalização quanto do tráfego de mídia. A rede que utiliza *Phone Proxy* faz esse tratamento com relação à comunicação entre os *endpoints*, protegendo de forma mais abrangente a rede. Esta implementação traz ainda uma alternativa de segurança para o uso de *Softphones* e garante a criptografia da sessão entre dispositivos remotamente conectados e o *cluster* a partir do uso da criptografia nativa do próprio dispositivo.

Em uma implementação que necessite de um nível avançado de segurança de dados, inclusive UC, a adoção de redes virtuais privadas (VPN) é uma alternativa recomendável ao retirar da rede as vulnerabilidades físicas da rede quanto a possibilidade de intrusão de um atacante.

Não se pode esquecer que o controle de acesso físico, monitoramento da rede e estrutura de suporte técnico são indispensáveis para as premissas de segurança da informação: confidencialidade, integridade e disponibilidade.

6 CONCLUSÃO

Este capítulo faz um condensado das observações encontradas no estudo feito por este trabalho de conclusão de curso.

As comunicações unificadas elevam o tráfego de informação a níveis jamais vistos, tendo como fonte as mais variadas origens (localização, dispositivo etc.) e os mais variados intuitos (vídeo, voz, dados etc.). Voz e dados quando tratados com igualdade, guardadas as devidas diferenças inerentes a cada tipo de comunicação, necessitam de muito mais cuidado ao serem transportados pela rede IP. Esse tipo de abordagem introduz vulnerabilidades que não estavam presentes no sistema de telefonia convencional. Embora já tenha se firmado como uma tecnologia de comunicação alternativa aos sistemas convencionais baseados em redes de circuitos comutados, em termos de segurança as comunicações unificadas tem ainda mais desafios, pois além dos já comumente lidados na telefonia convencional, herdam as vulnerabilidades das redes de dados.

Após conduzir um estudo mais aprimorado de UC e seus aspectos de segurança da informação fica evidente a importância do presente trabalho como síntese das diretrizes da gestão de riscos de SI aplicadas aos ambientes de comunicações unificadas. O trabalho em questão então pode ser considerado com uma fonte qualificada para o tema, que ainda não dispõe de muitas publicações científicas, sobretudo em português. Propor um estudo como esse, além do ganho pessoal proporcionado com o desenvolvimento de conceitos não tão vistos durante a graduação que são de grande valia para a formação profissional, faz com que futuras pesquisas na area de segurança da informação para comunicações unificadas sejam desenvolvidas de forma mais simples, uma vez que a partir da conceituação feita neste trabalho, tem-se a base necessária para o desenvolvimento de analises mais completas.

A presente análise foi importante para entender de forma prática as implicações das normas de SI mostrando as vulnerabilidades presentes em um ambiente VoIP e como algum atacante pode ameaçar a rede explorando as mesmas. No caso específico analisado, essas vulnerabilidades foram independentemente tratadas de acordo com cada tipo de implementação presente e através dessa análise pôde ser descrito um conjunto de boas práticas que diminuem os riscos inerentes à rede, principalmente no caso da telefonia IP.

Mesmo o estudo do caso prático sendo norteado em uma solução proprietária, as práticas recomendadas se aplicam à tecnologia VoIP em geral podendo ser utilizadas como ferramenta para um melhor entendimento de como os aspectos de confidencialidade, integridade e disponibilidade devem ser tratados em problemas similares ao analisado, ajudando e servindo de suporte aos profissionais que trabalhem com gestão de risco e segurança da informação no tratamento de problemas que apareçam no dia a dia.

7 REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, C. G. **SIP Web Client: Comunicações Convergentes**. Dissertação (Mestrado em Engenharia Informática e Computação), Universidade do Porto. Porto. 2008.

ANTONIAZZI, A. S. **Segurança em VoIP: Ameaças, Vulnerabilidades e as suas Melhoes Práticas de Segurança**. Trabalho de Conclusão (Especialização em Tecnologias, Gerência e Segurança de Redes de Computadores), Universidade Federal do Rio Grande do Sul. Porto Alegre. 2008.

ARAÚJO, F.; BRAGA, C. **Convergência e Interoperabilidade entre a Rede de Telefonia Fixa Comutada e a Rede IP**. Trabalho de Graduação (Graduação em Engenharia de Redes de Comunicação), Universidade de Brasília. Brasília. 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. **NBR ISO 27002 - Tecnologia da Informação - Técnicas de Segurança - Código de Práticas para a Gestão de Segurança da Informação**. Rio de Janeiro: ABNT, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. **NBR ISO 27005 - Tecnologia da Informação - Técnicas de Segurança - Gestão de Riscos de Segurança da Informação**. Rio de Janeiro: ABNT, 2008.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. **NBR ISO 31000 - Gestão de Riscos - Princípios e Diretrizes**. Rio de Janeiro: ABNT, 2009.

BAILEY, C. M. **Unified Communications Applications: Uses and Benefits**, Boston, Julho 2008.

BARBIERI, R.; BRUSCHI, D.; ROSTI, E. **Voice over IPsec: Analysis and Solutions**, In: 18th Annual Computer Security Applications Conference (ACAC), Las Vegas, Dezembro 2002.

BRAGA, E. S. **VoIP: Telefonia IP, Arquitetura, Protocolos e Soluções Corporativas**. Trabalho de Conclusão (Especialização em Redes de Computadores e Comunicação de Dados), Universidade Estadual de Londrina. Londrina. 2005.

CISCO SYSTEMS INC. **TLS Proxy vs. Phone Proxy**, 2008. Disponivel em: <http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns165/ns391/white_paper_c11-493584.pdf>. Acesso em: 21 Fevereiro 2013.

COMER, D.; STEVENS, D. **Interligação em Rede com TCP/IP:** Princípios Protocolos e Arquiterura. 2. ed. Rio de Janeiro: Campus, v. 1, 1998.

FERNANDES, N. L. **Voz sobre IP:** uma Visão Geral, Rio de Janeiro, 2000. Disponivel em: <http://professores.unisanta.br/santana/downloads%5CTelecom%5CCom_Digitais%5CAulas%202o.%20Bimestre%5Cnelson_voip.pdf>. Acesso em: 06 Dezembro 2012.

FERREIRA, M. **O que vem a ser Segurança da Informação**, 2005. Disponivel em: <http://www.apinfo.com/artigo81.htm>. Acesso em: 21 Janeiro 2013.

FLORÊNCIO, A. **Tecnologias para Comunicação Colabotaiva em Direção à Melhoria da Experiência e Integração de Plataformas**. Dissertação (Mestrado em Engenharia Elétrica), Universidade de Brasília. Brasília. 2009.

GALVÃO, M.; ZATTAR, A. **Aspectos de segurança em redes voz sobre IP**, MSLAB (Módulo Security Lab), 2003.

GARTNER. **Magic Quadrant for Unified Communications**, 2012. Disponivel em: <http://www.gartner.com/technology/reprints.do?id=1-1BUWTHV&ct=120828&st=sb>. Acesso em: 2013 Fevereiro 2013.

GONÇALVES, J. **Segurança da Informação e Necessidade de Capacitação do Profissional de Segurança da Informação**, Curitiba, 2010.

INTERNET ENGINEERING TASK FORCE - IETF. **RFC 2543 - SIP: Session Initiation Protocol**, IETF, Março 1999.

INTERNET ENGINEERING TASK FORCE - IETF. **RFC 3621 - SIP: Session Initiation Protocol**, IETF, Junho 2002.

KEROMYTIS, A. **Voice over IP: Risks, Threats and Vulnerabilities**, In: Cyber Infrastructure Protection (CIP) Conference, New York, Julho 2009.

KUROSE, J.; ROSS, K. **Redes de computadores e a internet:** uma abordagem top-down. 3. ed. São Paulo: Pearson Addison Wesley, 2006.

MATHIES, B. **Comparativo de Soluções para Comunicação Unificada**. Pontífica Universidade Católica do Paraná. Curitiba. 2010.

MCGANN, S.; SICKER, D. **An Analysis of Security Threats and Tools in SIP-based VoIP Systems**, In: 2nd Annual Workshop VoIP Security, Washington, Junho 2005.

MORAES, A. **Cisco Firewalls - Concepts, Design and Deployment for Cisco Stateful Firewall Solutions**. 1. ed. Indianapolis: Cisco Press, 2011.

MORAES, A. **Segurança para Comunicações Unificadas:** o que Esperar do seu Firewall?, 2012. Disponivel em: <http://alexandremspmoraes.wordpress.com/2012/07/09/1064/>. Acesso em: 24 Janeiro 2013.

PALHARES NETO, M. **Implantação da Rede de Telefonia IP para Enlace de Baixa Velocidade**. Trabalho de Graduação (Graduação em Engenharia Elétrica), Universidade Politécnica de Pernambuco. Recife. 2010.

PEREIRA, O. **Comunicação Unificada - Tecnologia e seu Impacto nos Negócios**, 2011. Disponivel em: <http://www.teleco.com.br/tutoriais/tutorialcomuni/pagina_1.asp>. Acesso em: 29 Agosto 2012.

PROMON LOGICALIS. **Segurança da Informação: um Diferencial Determinante na Competitividade das Corporaçoes**, 2005.

TI SAFE - SEGURANÇA DA INFORMAÇÃO. **Segurança em Redes de Voz sobre IP (VoIP)**, São Paulo, Março 2010.

VOLTAN JÚNIOR, G. **Voz sobre IP: Segurança de Transmissões**. Trabalho de Graduação (Bacharel em Ciência da Computação), Pontífica Universidade Católica do Goiás. Goiânia. 2005.