REVISTA TECNOLÓGICA DA FATEC-PR

ISSN: 2179-3778

CURITIBA, V. 1, N. 4, JAN/DEZ 2013 – ISSN 2179-3778

REVISTA TECNOLÓGICA DA FATEC-PR

CURITIBA, V. 1, N. 4, JAN/DEZ 2013 – ISSN 2179-3778

FACULDADE DE TECNOLOGIA DE CURITIBA – FATEC-PR
Mantenedora: Escola Tecnológica de Curitiba S/C Ltda.
Rua Itacolomi, 450 – Portão
CEP: 81070-150 - Curitiba-Pr
Telefone: 3246-7722 - Fax: 3248-0246
http://www.fatecpr.edu.br

Dados Internacionais de Catalogação na Publicação (CIP)
(Biblioteca da FATEC-PR, PR Brasil)

Revista Tecnológica da FATEC-PR. Faculdade de Tecnologia de Curitiba. v. 1, n. 4, jan./dez. 2013. Curitiba (PR): FATEC-PR, 2013.

Periodicidade Anual.
Texto em português

ISSN 2179-3778

1 – Redes de Computadores. 2 – Telecomunicações. 3 – Eletroeletrônica Industrial. 4 – Administração. 5. Saúde.
I – Título.

CDD 004.6
- 658.

EXPEDIENTE
Revista Tecnológica da FATEC-PR
ISSN 2179-3778
É uma publicação Anual editada pela
Faculdade de Tecnologia de Curitiba – FATEC-PR
Rua Itacolomi, 450 – Portão
CEP: 81070-150 - Curitiba-Pr
Telefone: 3246-7722 - Fax: 3248-0246
e-mail: secretaria@fatecpr.edu.br
site : http://www.fatecpr.edu.br
ESCOLA TECNOLÓGICA DE CURITIBA S/C LTDA.
FACULDADE DE TECNOLOGIA DE CURITIBA – FATEC-PR

EDITORIAL

A Faculdade de Tecnologia de Curitiba - FATEC-PR, com sede na Rua Itacolomi, No. 450, Bairro Portão, Curitiba-PR, CEP: 81.070-150, é mantida pela ETC - Escola Tecnológica de Curitiba Ltda., pessoa jurídica de direito privado, com fins lucrativos e sede e foro em Curitiba, Estado do Paraná.

A IES foi credenciada pelo MEC através da Portaria No. 159, de 19 de janeiro de 2005, publicada no Diário Oficial da União do dia 20 de janeiro de 2005. A FATEC-PR iniciou suas atividades no ensino superior no ano de 2005, e atualmente, a IES conta com 4 (quatro) cursos, sendo 3 (três) cursos superiores de tecnologia e 1 (um) curso de bacharelado. Oferece atividades e Cursos de Extensão e Profissionalizantes, e Pós-graduação *Lato Sensu* em áreas tecnológicas dos cursos que oferta. O Curso de Tecnologia em Redes de Computadores, Autorizado na mesma portaria de credenciamento da IES e com o Curso de Tecnologia em Sistemas de Telecomunicações e Curso de Tecnologia em Eletrônica Industrial, Autorizados pelas Portarias No. 1.100 e 1.101, de 5 de abril de 2005, respectivamente, publicadas no DOU de 6 de abril de 2005.

O Curso de Tecnologia em Eletrônica Industrial foi reconhecido pela Portaria Ministerial Nº 471, de 22 de novembro de 2011, publicada no DOU de 24/11/2011. O Curso de Tecnologia em Sistemas de Telecomunicações foi reconhecido pela Portaria Ministerial Nº 298, de 27 de dezembro de 2012, publicada no DOU de 31/12/2012. O Curso de Tecnologia em Redes de Computadores foi reconhecido pela Portaria Ministerial Nº 302, de 27 de dezembro de 2012, publicada no DOU de 31/12/2012.

O Curso de Administração, bacharelado, foi Autorizado pela Portaria Nº 185 de 06/02/2009, publicada no DOU de 09/02/2009, foi avaliado pelo MEC e pelo CRA – Conselho Regional de Administração e reconhecido pela Portaria Nº 664, de 12/12/2013, publicada no D.O.U de 13/12/2013.

Todos os cursos de graduação superior funcionam no período noturno. Cada um dos cursos superiores têm Autorizadas 100 vagas anuais e todos são ofertados no regime semestral e período noturno. A IES apresenta um perfil acadêmico focado nas áreas de telecomunicações, eletrônica, redes de computadores e administração.

Até o final do 1º semestre de 2013, a Faculdade de Tecnologia de Curitiba - FATEC-PR fazia parte do Grupo ADAS onde participava a ETC - Escola Tecnológica de Curitiba S/C Ltda., a Faculdade de Tecnologia de Curitiba - FATEC-PR, o Colégio Técnico de Curitiba (reconhecido pela SEED-PR), a Daysoft, empresa desenvolvedora de *software*, que oferece oportunidade de trabalho aos alunos da faculdade, a Prime Saúde com sede em São Paulo a Fundação Natureza Pura que oferecia semestralmente bolsas de estudo de até 40%, beneficiando a comunidade local.

A partir do segundo semestre de 2013, a FATEC-PR e o CTC, instituições mantidas pela ETC, foram adquiridas por um grupo de educadores do Estado de São Paulo e que compreende 8 (oito) faculdades naquele Estado. A partir de então, a FATEC-PR compõe o grupo ao qual pertence a IERT – INSTITUIÇÕES DE ENSINO REUNIDAS DO TIÊTE, mantenedora sediada em Barra Bonita / SP ao qual pertence a Faculdade GRAN TIÊTE e a Faculdade GALILEU, instituições do grupo que ofertam cursos nas áreas de administração e engenharias.

A missão da FATEC-PR é:

"Promover educação superior que desenvolva no acadêmico suas potencialidades morais e intelectuais, proporcionando-lhe pleno exercício da cidadania e do serviço em prol da sociedade".

Nas mesmas instalações da FATEC-PR funciona o CTC - Colégio de Tecnologia de Curitiba, mantido pela ETC, onde são ofertados, no turno diurno e noturno, quatro cursos técnicos concomitantes e subsequentes ao nível do segundo grau (Técnico em Automação Industrial, Técnico em Informática para *Internet,* Técnico em Telecomunicações e Técnico em Eletrotécnica) e oferta o Curso de Ensino Médio Regular no período da manhã.

A FATEC-PR também tem tradição na realização de atividades e Cursos de Extensão e Profissionalizantes, em áreas tecnológicas dos cursos que oferta. Dentre estes cursos destacam-se: Comandos Industriais; Eletrônica Analógica (Eletrônica Básica); Eletrônica Digital; Instalação Elétrica Residencial e Predial; Microprocessadores e Microcontroladores PIC; Microcontrolador da Família 8051; NR 10; SEP; Informática Básica; Linguagem C++; Linguagem C; Linguagem Delphi; Linguagem Java; Linguagem Visual Basic; Programação Dot NET; Montagem e Manutenção de Computadores; Sistema Operacional *Linux*; Cabeamento Estruturado; Comunicações de Dados; Telefonia Básica e Telefonia Celular.

A FATEC-PR também oferta cursos de Pós-graduação *Lato Sensu*. Um dos fatos importantes e a atuação na responsabilidade social. Em 2013 a IES desenvolveu uma série de projetos extencionistas dentre os quais se destacaram a I FESTA JUNINA DA FATEC-PR – CTC – ALFA JUNIOR, o TROTE SOLIDÁRIO, e o PROJETO DE APOIO AO HOSPITAL DO TRABALHADOR.

Além disto, em 2013 também foram intensificadas as Visitas Técnicas com destaque para VISITA TÉCNICA À USINA HIDRELÉTRICA DE ITAIPU, a VISITA TÉCNICA À APPA – ADMINISTRAÇÃO DOS PORTOS DE PARANAGUÁ E ANTONINA, a VISITA TÉCNICA À REPAR e a VISITA TÉCNICA AO CINDACTA II.

Este quarto número da Revista Tecnológica da FATEC-PR fortalece a participação dos docentes com a publicação de artigos científicos e artigos de iniciação científica. Acadêmicos orientados por professores do corpo docente da instituição e de outras IES, em coautoria, encaminharam artigos para análise e publicação. Alguns destes artigos derivaram do TCC – Trabalho de Conclusão de Curso, como mais uma oportunidade da FATEC-PR para motivar a produção científica dos alunos de dos professores.

Outro ponto de destaque na Iniciação Científica da FATEC-PR foi a participação em 2013, a exemplo do que foi feito em 2012 e 2011, no CONIC – CONGRESSO NACIONAL DE INICIAÇÃO CIENTÍFICA. Neste ano foram inscritos e apresentados oito projetos de IC da FATEC-PR naquele congresso.

Cada um dos trabalhos apresentados contribui na área do conhecimento correspondente e as temáticas podem ser aprofundadas em estudos futuros. Deste modo, a Revista Tecnológica da FATEC-PR está, cada vez mais, se consolidando e se aperfeiçoando como mais uma referência para professores, pesquisadores e acadêmicos, disseminando a informação para a comunidade científica.

João Paulo Alves da Silva
Diretor Geral.

SUMÁRIO

IMPLEMENTAÇÃO DE VIRTUALIZAÇÃO EM *DATA CENTERS*

IMPLEMENTATION OF VIRTUALIZATION IN DATA CENTERS

Luiz Henrique Prado Cionek[1]
Fellipe Medeiros Veiga (Orientador)[2]

CIONEK, Luiz Henrique Prado; *VEIGA, Luiz Fellipe Medeiros (orientador).* **Implementação de Virtualização em *Data Centers***. *Revista Tecnológica da FATEC-PR, v.1, n.4, p. 8 -38, jan./dez., 2013.*

RESUMO:

Esta pesquisa apresenta o resultado do Trabalho de Conclusão de Curso de Tecnologia em Redes de Computadores, e tem como objetivo discorrer sobre a implementação da virtualização em *Data Centers* e analisar as vantagens e desvantagens de seu uso, além da realização de um estudo de caso, onde será aplicada a abordagem conhecida como consolidação de servidores, e serão realizados testes, analisando os seus resultados e comparando com o que foi visto na revisão bibliográfica. A importância desse trabalho é orientar às empresas sobre como o uso da virtualização pode trazer benefícios.

Palavras-chave: Virtualização. Máquinas Virtuais. Consolidação de Servidores. Sistemas Operacionais. Redução de Custos. *Data Center*.

ABSTRACT:

This work presents the proposal of completion of course work for the Technology in Computer Networks class. This paper aims to discuss the implementation of virtualization in Data Centers and analyze the advantages and disadvantages of their use, besides conducting a case study where the approach known as server consolidation will be applied, and tests will be conducted, analyzing and comparing the results with what was seen in the literature review. The importance of this work is to guide businesses on how the use of virtualization can bring benefits.

***Keywords**: Virtualization. Virtual Machines. Server Consolidation. Operating Systems. Cost Reduction. Data Centers.*

1 INTRODUÇÃO

Com o aumento do poder computacional dos servidores de grande porte, novas oportunidades se tornaram possíveis na área de tecnologia de informação, como a virtualização de servidores. A virtualização consiste em criar uma abstração

[1] Luiz Henrique Prado Cionek é graduado em Tecnologia em Redes de Computadores pela FATEC-PR (2013). Atua como profissional na área de Redes de Computadores.

[2] Fellipe Medeiros Veiga é Mestrando pela Universidade Tecnológica Federal do Paraná (UTFPR). Foi o orientador do Trabalho de Conclusão de Curso do acadêmico Luiz Henrique Prado Cionek. Graduado em Tecnologia em Processamento de Dados pela Faculdades Eseei (2007). Especialista em Teleinformática e Redes de Computadores pela UTFPR (2009). Atualmente é Professor da Faculdade de Tecnologia de Curitiba. Atua como Técnico Pleno de Redes de Computadores da Companhia de Informática do Estado do Paraná (CELEPAR) e é Professor da UTFPR.

dos recursos de hardware de um sistema computacional, permitindo o uso de vários sistemas operacionais em um único conjunto de hardware.

O uso da virtualização é uma tendência que vem aumentando nos últimos anos, e sua utilização pode gerar benefícios para as grandes empresas, pois pode gerar economia, ao reduzir despesas, e aproveitar melhor o hardware existente.

Esse trabalho consiste das seguintes etapas:

Através de análise bibliográfica, apresentar conceitos sobre a virtualização, suas vantagens e desvantagens existentes no seu uso em um ambiente de processamento de dados. Apresentar a abordagem conhecida como consolidação de servidores, que visa aproveitar o processamento ocioso dos computadores com a adição de sistemas operacionais virtualizados para melhor aproveitamento dos recursos de hardware. Tem também como objetivo realizar um levantamento com algumas das ferramentas usadas atualmente por grandes corporações, e um estudo de caso prático, onde será utilizada uma solução comercial de virtualização, para a implementação de um ambiente virtualizado para a consolidação de servidores. Após a implementação, serão realizados testes, comparando características da virtualização vistas na bibliografia com os resultados práticos.

Posteriormente, os resultados do estudo serão apresentados, bem como sua conclusão, e análise posterior.

1.1 OBJETIVO GERAL

O objetivo principal é o estudo das técnicas de virtualização, aplicadas ao ambiente de servidores, onde pode-se aproveitar de seus benefícios na consolidação de servidores e sistemas, melhorando o aproveitamento do hardware disponível, visando principalmente à redução de custos.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos são os seguintes:

a) Estudar as técnicas de virtualização existentes, juntamente com suas vantagens e desvantagens;

b) Analisar os benefícios que os ambientes virtualizados podem ter nas empresas;

c) Implementar uma arquitetura de consolidação de servidores, utilizando ferramentas de virtualização;

d) Estudar um caso real de implementação da virtualização;

e) Confrontar o estudo da teoria e a prática utilizada no caso de estudo;

f) Apresentar os resultados do estudo de caso proposto, juntamente com as considerações necessárias;

g) Mostrar as conclusões a que se chegaram.

2 JUSTIFICATIVA

A maioria das empresas possui hoje algum tipo de serviço na rede, e esses serviços requerem a existência de servidores. Para as grandes empresas, porém, devido a grande demanda por parte de seus clientes, torna-se necessária a utilização de servidores mais poderosos, com grande capacidade de processamento. O custo total de operação (adaptado do inglês TCO – *Total cost of ownership,* ou custo total de posse) desses servidores é muito alto, pois utilizam muita energia elétrica (alguns dos maiores *Data Centers* do mundo gastam tanta energia quanto uma cidade pequena), principalmente para resfriamento.

Segundo o *New York Times (2012)*, 90% da energia utilizada por esses *Data Centers* é desperdiçada, pois os equipamentos, não importando a demanda pelo serviço hospedado, estão sempre funcionando em sua capacidade máxima, sendo que a utilização real dos servidores é de 6 a 12% da energia fornecida a eles. Como medida contra falhas na energia, os *Data Centers* utilizam geradores à *diesel*, cujos resíduos geram poluição. É estimado que, mundialmente, seja gasto aproximadamente 30 bilhões de *watts* de eletricidade nesses ambientes. Existem estimativas de que em media, 90 por cento dos servidores Windows funcionam abaixo de 10% de sua capacidade total. (KAMOUN, 2009)

A virtualização hoje é uma tendência, e o seu uso com abordagens como a consolidação de servidores pode ajudar a reduzir esses custos, já que o objetivo dessa abordagem é centralizar vários servidores em um único servidor, que pode inclusive ser um sistema distribuído.

A importância desse trabalho é que ele pode ser usado como referência para gestores de *Data Centers*, ao apresentar as vantagens do uso da virtualização nesses ambientes, e as possíveis desvantagens que ainda existem nessa tecnologia, e assim, orientar quanto às quais tipos de serviço são mais vantajosos serem virtualizados.

3 METODOLOGIA

Seguindo o descrito em Marconi (2003), o trabalho foi desenvolvido como uma pesquisa bibliográfica e aplicada a um estudo e caso, ou seja, a aplicação de uma teoria na prática, seguindo os passos e como foram desenvolvidos conforme destacados a seguir.

a) Seleção e o estudo da bibliografia;

b) Levantamento de soluções de virtualização de uso empresarial, e algumas de suas características;

c) Uma análise bibliográfica sobre a virtualização, visando estudar sobre suas características, conceitos, vantagens do uso, bem como suas desvantagens e problemas a serem resolvidos para que essa tecnologia possa ser amplamente utilizada;

d) Estudo de um caso real prático;

e) Análise comparativa entre a teoria e a prática utilizada no caso de estudo;

f) Conclusões e considerações.

Cada uma das etapas está detalhada no item que trata sobre o desenvolvimento do trabalho, conforme a seguir.

4 REVISÃO BIBLIOGRÁFICA

A seguir estão apresentados os itens resultantes da pesquisa e estudos efetuados na literatura especializada.

4.1 SISTEMA OPERACIONAL

Sistema operacional é o *software* intermediário entre os aplicativos de usuário e o *hardware*, que cria uma abstração do *hardware* e fornece uma visão de alto nível aos programas, o que facilita criação dos mesmos, e também gerencia os recursos de *hardware,* como o processador, a memória, o dispositivo de armazenamento, os dispositivos de entrada e saída, entre outros. O sistema operacional recebe as solicitações dos programas do usuário e aloca os recursos de *hardware* para essas aplicações.

4.1.1 Núcleo (*Kernel*)

O sistema operacional conta com vários componentes, e a parte responsável por funcionar como um intermediário entre o *hardware* e os processos é o núcleo, ou *kernel*.

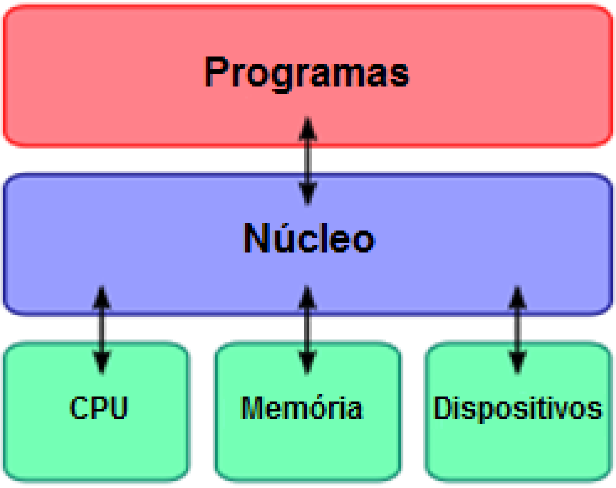


Figura 1: Representação do Kernel.
Fonte: Adaptado de *Wikimedia Commons* (2008).

Para a execução desses processos, o núcleo funciona em dois modos diferentes: o modo núcleo e o modo usuário.

4.1.1.1 Modo Núcleo (*System Kernel*)

O modo núcleo tem acesso completo ao hardware e pode executar qualquer instrução que possa ser executada pela máquina. O sistema operacional opera em modo núcleo, pois é ele que gerencia e aloca os recursos de *hardware* para os processos de usuário.

4.1.1.2 Modo Usuário (*User Kernel*)

Modo no qual apenas parte das instruções pode ser executada. Instruções que afetam o controle da máquina ou que realizam E/S (entrada/saída) não podem ser executadas nesse modo. Os processos do usuário normalmente são executados nesse modo.

4.1.2 Bibliotecas

Biblioteca é uma coleção de rotinas, escritas em linguagem de máquina, que oferece funções que simplificam a construção de um programa. O código de uma biblioteca é organizado de forma que possa ser usado por vários programas diferentes.

4.1.3 Aplicativos de Usuário

Também chamados de programas ou processos do usuário, são processos que executam sobre o sistema operacional e que executam diversas funções, como editor de texto, editor de imagem, navegador de internet, entre outros. Esses processos são normalmente executados pelo núcleo em modo usuário (*user kernel*), e quando necessitam de acesso ao *hardware,* realizam chamadas ao sistema.

4.1.4 Chamada ao Sistema

Por segurança, os processos do usuário não possuem acesso total ao conjunto de instruções do *hardware*. Quando um processo precisa executar uma instrução que necessita de acesso privilegiado ao *hardware*, ele requisita um serviço ao núcleo do sistema operacional. Esse mecanismo é denominado de chamada ao sistema.

4.2 ISA *(INSTRUCTION SET ARCHITECTURE*)

ISA é uma interface, que se constitui pelas instruções em linguagem de máquina aceitas pelo processador e as operações de acesso ao hardware.

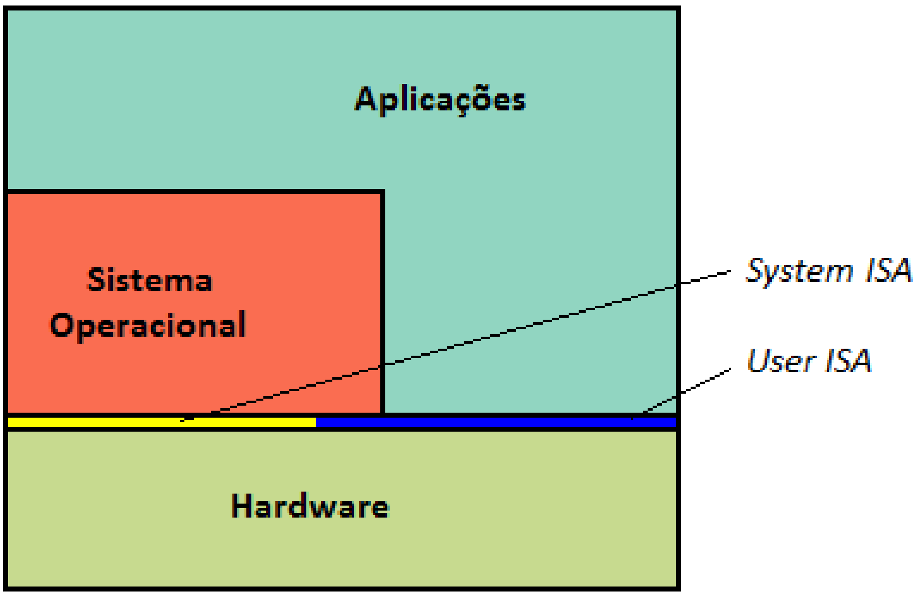


Figura 2: Representação da interface ISA.
Fonte: Autor.

Por segurança, o conjunto de instruções é dividido em duas partes, conforme descrito a seguir.

4.2.1 Instruções de Usuário (*User Isa*)

Instruções do hardware que podem ser acessadas pelos processos do usuário, que não tem acesso privilegiado ao hardware.

4.2.2 Instruções de Sistema (*System Isa*)

Instruções que são acessíveis somente ao núcleo do sistema operacional, que possui acesso completo ao hardware. Correspondem ao conjunto de instruções sensíveis do processador e demais itens de hardware (LAUREANO, MAZIERO, 2008), que segundo Tanenbaum (2003), são instruções que só podem ser executados em modo núcleo, como instruções de I/O, instruções de modificação nas configurações de MMU (*Memory Management Unit*), etc.

Isso torna necessário para processos de usuário o uso de chamadas ao sistema, pois os mesmos não possuem acesso privilegiado ao hardware.

4.2.3 Classificação do Conjunto de Instruções

Existem várias arquiteturas de hardware, com diferentes conjuntos de instruções. Os conjuntos de instruções são classificados em dois tipos: RISC e CISC.

4.2.3.1 CISC (*Complex Instruction Set Computer*)

Arquitetura que possui um número maior de instruções, de tamanho variável. Apesar das instruções CISC sejam mais curtas que as instruções RISC, a sua execução é mais demorada, exigindo mais ciclos de relógio, devido a sua complexidade. O número de ciclos necessários para a execução de instruções CISC é variável (NULL, LOBUR, 2010).

Um exemplo de arquitetura CISC é o x86.

4.2.3.2 Risc (*Reduced Instruction Set Computer*)

Arquitetura que tem um conjunto de instruções menor, quando comparado ao das máquinas CISC. O seu conjunto de instruções é menor, pois contém somente as instruções que realizam as operações usadas mais frequentemente, e emula as instruções que não possui através das instruções normais.

Arquiteturas RISC processam as operações em menor tempo, porém necessitam de mais memória, pois para "emular" as instruções não existentes na arquitetura RISC, é necessária a utilização de mais instruções (NULL, LOBUR, 2010).

O tempo de execução da arquitetura RISC tende a ser menor que a CISC, devido a suas instruções e tem um número de ciclos padronizado (normalmente um ciclo por instrução). Exemplos de arquiteturas RISC são: SPARC, PowerPC, entre outras.

4.3 VIRTUALIZAÇÃO

Uma camada de *software* que cria uma camada de abstração acima do hardware, permitindo que um único computador hospede múltiplas máquinas virtuais, cada uma com seu próprio sistema operacional e independente das outras.

Um dos principais motivos por trás da proposta da tecnologia de virtualização é a compatibilidade de interfaces, pois um programa só funciona sobre um sistema para o qual foi projetado, assim como um sistema operacional só funciona sobre a arquitetura para o qual foi projetado.

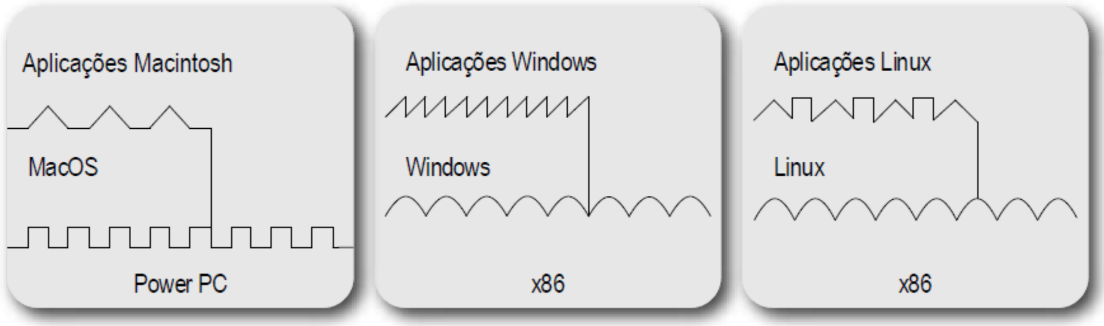


Figura 3: Representação de alguns sistemas operacionais, suas aplicações e arquiteturas sobre o qual executam.
Fonte: Laureano (2006).

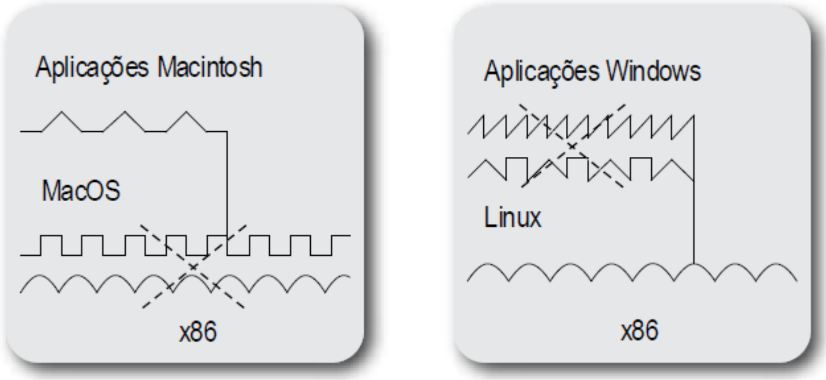


Figura 4: Incompatibilidade entre sistemas.
Fonte: Laureano (2006).

Isso dificulta a interoperabilidade entre sistemas diferentes, como um sistema para arquitetura x86 e um sistema SPARC.

O uso de virtualização torna possível solucionar esse problema, criando a interface necessária para o funcionamento do programa ou sistema, através de uma camada de *software*. Essa camada de *software* é chamada de hipervisor e a interface é chamada de máquina virtual.

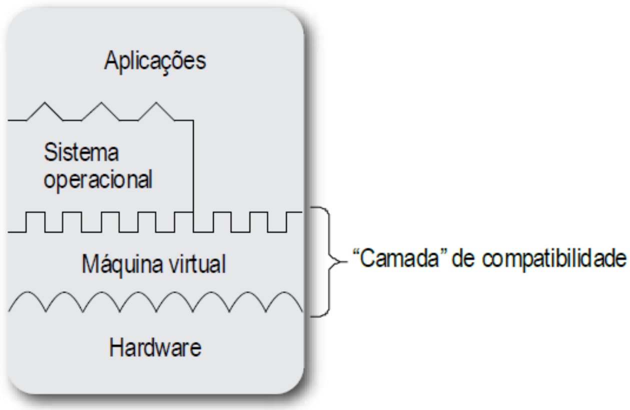


Figura 5: Representação da camada de *software*, que permite a compatibilidade entre um sistema operacional e uma arquitetura para o qual não foi construído.
Fonte: Laureano (2006).

4.3.1 Máquina Virtual

Máquina virtual é uma duplicata em *software* de uma máquina real, criada para executar um determinado programa ou sistema operacional.

Em 1974, os pesquisadores Gerald J. Popek, da Universidade da Califórnia, em Los Angeles e Robert P. Goldberg, da universidade de Harvard propuseram uma definição formal ao conceito de máquina virtual, que é “Uma duplicata eficiente e isolada de uma máquina real”.

A máquina virtual funciona da mesma maneira que uma máquina real, com seu processador, memória, armazenamento, etc., e, portanto possui sua própria *ISA*.

Se a máquina virtual possui um conjunto de instruções similar ao da máquina real, as instruções do processador virtualizado são capturadas pelo hipervisor, e simplesmente reenviadas ao processador sem nenhuma alteração.

Porém quando a arquitetura do conjunto é diferente, as instruções são capturadas, e traduzidas, para só então serem reenviadas ao processador, o que reduz um pouco a velocidade de processamento.

4.3.2 Sistema Hospedeiro (Host)

O computador que hospeda e executa máquinas virtuais é chamado de *host*, ou hospedeiro. Constitui o *hardware* base do sistema de virtualização, e caso o *VMM* seja do tipo 2, o hospedeiro será o sistema operacional que executa o mesmo.

4.3.3 Sistema Convidado (Guest)

Sistema que é executado por uma máquina real, através de um hipervisor. O sistema convidado “acredita” estar executando sobre um ambiente convencional com acesso direto ao *hardware*, ou seja, a máquina virtual trabalha como um computador completo.

4.3.4 Histórico da Virtualização

Na década de 60, a IBM desenvolveu um sistema operacional chamado M44/44X, um sistema *time-sharing* experimental, que simulava múltiplos computadores IBM 7044, através de particionamento lógico, o que permitia que o *mainframe* rodasse várias aplicações e processos ao mesmo tempo, como se fossem vários *mainframes* (POLLON *apud* CREASY, 1980).

A partir do sucesso inicial do M44/44x, a IBM continuou investindo em *mainframes* que utilizavam o conceito de virtualização, que até então ainda não estava formalizado, inclusive sendo usado para testes de viabilidade técnica de novos *mainframes*.

Na década de 70, os pesquisadores Gerald J. Popek e Robert P. Goldberg definiram formalmente vários conceitos relacionados à virtualização, como as condições necessárias para que um conjunto de hardware suportem virtualização.

O objetivo da virtualização nessa época era o fornecimento de um ambiente monousuário, com seu próprio sistema operacional e aplicações, isolado dos demais usuários.

Na década de 80, com o surgimento dos computadores pessoais e a queda no preço do *hardware*, a virtualização foi deixada de lado, pois era mais barato e simples cada usuário ter seu próprio computador do que manter um único mainframe executando múltiplos sistemas simultaneamente. Devido a essa mudança, as novas arquiteturas de computadores deixaram de ter suporte à virtualização.

A partir da década de 90 houve uma renovação no interesse pela virtualização, com o desempenho cada vez maior dos *PCs*. Porém, a arquitetura mais comum em *desktops*, a x86, não foi projetada para suportar virtualização.

Em 1999, a VMware lançou o *VMware Workstation*, um hipervisor hospedado para plataformas 32-*bit* de arquitetura x86. Após o lançamento do VMware *Workstation*, a virtualização novamente ganhou fôlego, pois a técnica utilizada pelo *VMware Workstation*, chamada de reescrita (ou tradução) de código, não necessita de que a arquitetura sobre o qual executa (no caso a arquitetura x86) tenha suporte nativo à virtualização.

Em 2005, a Intel introduziu em seus processadores a tecnologia Intel VT-x, que oferece suporte a virtualização em computadores de arquitetura x86.

No ano seguinte, os processadores da AMD também passaram a ter suporte à virtualização, devido à tecnologia desenvolvida pela AMD, que foi chamada inicialmente de AMD SVM (AMD *Secure Virtual Machine*), que depois foi abreviado para AMD-V.

Devido a essa popularização, surgiram inúmeras ferramentas, tanto para uso em computadores domésticos, como o *Oracle VirtualBox*, quanto para uso em servidores, como o *VMware Server*, ou o Xen. Hoje a virtualização se tornou uma tendência na área da tecnologia da informação, e um de seus principais usos por parte de empresas é para tentar reduzir custos, além do fornecimento de recursos computacionais para computação em nuvem.

4.4 HIPERVISOR

Hipervisor, ou monitor de máquina virtual (*VMM – Virtual Machine Monitor*), é o *software* que cria e executa máquinas virtuais. A função principal do hipervisor é virtualizar e alocar os recursos de *hardware*, de forma que cada máquina virtual veja o recurso alocado para ela como sendo um conjunto real de *hardware*, e se comporte como um computador real, com seu próprio sistema operacional.

Os hipervisores são classificados em dois tipos: o tipo 1, ou nativo, que executa diretamente no *hardware*, sem o intermédio de um sistema operacional, e o tipo 2, ou hospedado, que funciona sobre um sistema operacional.

Apesar dessa classificação em dois tipos, raramente são desenvolvidos hipervisores baseados em somente um dos tipos. Normalmente eles contam com características dos dois tipos, de forma que esses hipervisores podem ser chamados de híbridos.

4.4.1 Hipervisor Nativo

Segundo *National Instruments* (2011), o hipervisor de tipo 1, também chamado de nativo ou *bare metal*, executa diretamente no *hardware*, sem um sistema operacional abaixo. Esse é o modelo clássico de arquitetura de virtualização, desenvolvido pela IBM na década de 60.

Exemplos de hipervisores tipo I incluem os primeiros hipervisores criados pela IBM, como a ferramenta de testes SIMMON e o sistema operacional CP/CMS, e soluções modernas, como o *Xen*, *VMware ESX Server* e o *Microsoft Hyper-V*.

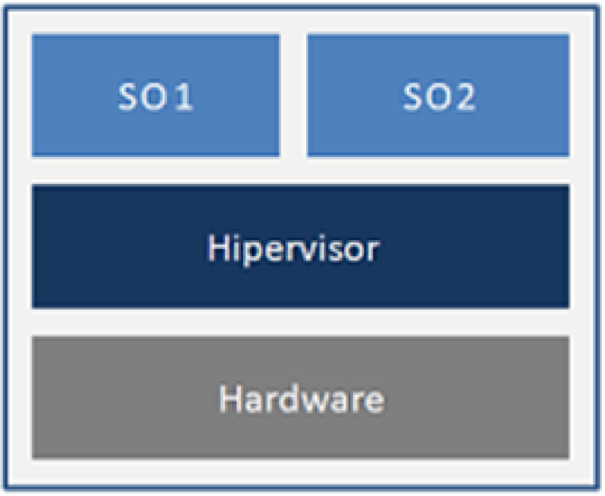


Figura 6: Arquitetura de um hipervisor tipo I.
Fonte: Adaptado de *National Instruments*, 2011.

4.4.2 Hipervisor Convidado

O hipervisor tipo 2, ou convidado, é executado com um processo sobre um sistema operacional nativo. O hipervisor usa os recursos oferecidos pelo sistema operacional nativo para oferecer recursos virtuais aos sistemas operacionais convidados.

Exemplos de hipervisores hospedados incluem o *Oracle VirtualBox, VMware Workstation* e o *QEMU*.

Hipervisores tipo 2 tem desempenho pior que os hipervisores nativos, pois só podem usar os recursos oferecidos pelo sistema operacional nativo, enquanto que os hipervisores tipo I podem acessar o *hardware* diretamente.

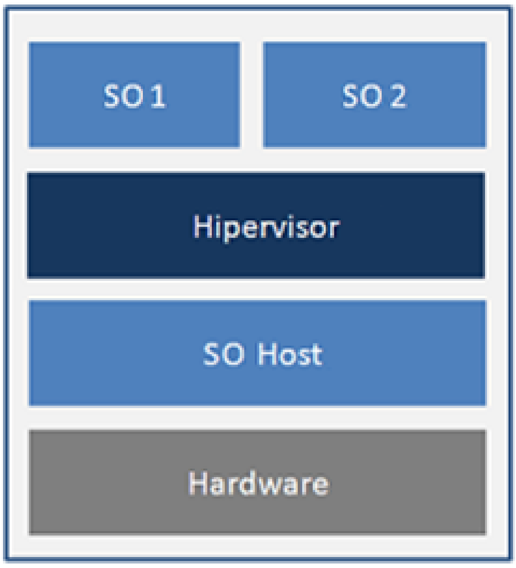


Figura 7: Arquitetura de um hipervisor tipo II.
Fonte: Adaptado de *National Instruments* (2011).

4.4.3 Hipervisor Híbrido

São hipervisores que aplicam conceitos dos dois tipos de hipervisores. Dificilmente os hipervisores, sejam eles classificados como tipo I ou II, são desenvolvidos inteiramente baseados em somente um dos conceitos. Hipervisores híbridos normalmente funcionam como um hipervisor convidado (tipo 2), mas podem acessar diretamente o *hardware* em operações de entrada e saída. Hipervisores de tipo 1 híbridos já tem acesso completo ao *hardware*, mas por serem integrados a um sistema operacional (Linux no KVM e Windows Server no Hyper-V) são considerados híbridos.

Muitos hipervisores hospedados atuais são híbridos, apesar de serem classificados como convidados, como o VMware *workstation*. Também existem hipervisores nativos que utilizam abordagens híbridas, como o KVM.

4.4.4 Características do Hipervisor

Em seu artigo *Formal Requirements for Virtualizable Third Generation Architectures*, Popek e Goldberg (1974) definiram algumas das características de um monitor de máquina virtual, como por exemplo:

O VMM providencia um ambiente para os programas que essencialmente idêntico ao da máquina original: o que significa que, um programa executando em uma máquina virtual deve executar da mesma maneira que executaria em uma máquina real, salvo as diferenças de recursos disponíveis.

Eficiência: significa que sempre que possível, a maioria das instruções do conjunto do processador virtual devem ser executadas diretamente pelo processador real, sem interferência do hipervisor. Isso permite que programas sendo executados na máquina virtual demonstrem somente pequenas reduções na velocidade de execução, quando comparados a uma máquina real.

Controle de recursos: o VMM deve ter acesso completo aos recursos de *hardware*, e o controle completo dos recursos de sistema disponíveis a ele.

4.5 TÉCNICAS DE VIRTUALIZAÇÃO

Existem diferentes técnicas e abordagens utilizadas pelos hipervisores para a execução de máquinas virtuais. As principais são virtualização total (*Full Virtualization*), tradução dinâmica de código (*Dynamic Translation*) e paravirtualização (*Paravirtualization*).

4.5.1 Virtualização Total

Método pelo qual todo o conjunto de *hardware* é virtualizado, como a memória, o processador e seu conjunto de instruções e os dispositivos de entrada e saída, de forma que o sistema convidado não precise ser alterado para executar na máquina virtual (LAUREANO, MAZIERO, 2008).

Porém esse método é mais lento, pois todo o acesso ao *hardware* é intermediado pelo hipervisor, que analisa todas as instruções do processador virtual, e caso seja necessário (como por exemplo, se o conjunto de instruções do sistema convidado seja diferente do conjunto do sistema hospedeiro, o que impossibilitaria o processador da máquina real de executar as instruções do sistema convidado), traduz as instruções executadas pela máquina virtual.

Devido a essa tradução de instruções, é possível fazer com que a máquina virtual tenha uma arquitetura de *hardware* diferente da máquina real, o que permite a execução de sistemas de arquitetura diferente da do sistema hospedeiro.

Um exemplo de hipervisor que utiliza virtualização total é o QEMU.

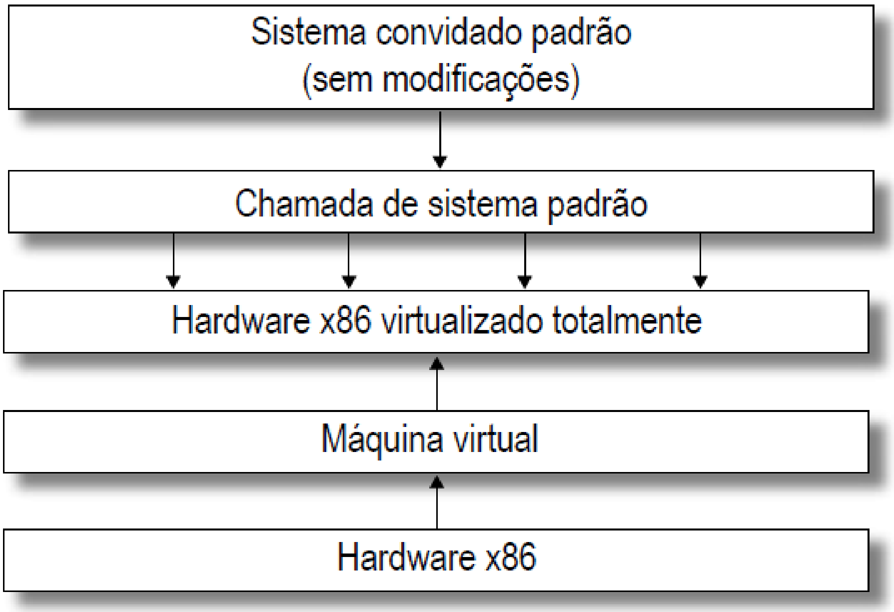


Figura 8: Representação da virtualização total.
Fonte: Laureano (2006).

4.5.2 Tradução Dinâmica de Código (*Dynamic Code Translation)*

Técnica utilizada por hipervisores na qual o hipervisor captura as instruções da interface ISA da VM e as traduz para instruções que o processador da máquina real compreenda, enquanto a máquina virtual está sendo executada.

O objetivo dessa técnica é o de garantir a execução do sistema convidado, ao traduzir as instruções da máquina virtual para instruções compatíveis com a máquina real.

Quando as instruções da máquina virtual podem ser executadas sem problemas pelo hospedeiro, as instruções não são traduzidas, mas simplesmente repassadas ao processador.

4.5.3 Paravirtualização

Paravirtualização é uma técnica em que parte do sistema convidado é modificada, para que sua interação com o hipervisor seja otimizada. Segundo Laureano e Maziero (2008):

> [...] Em meados dos anos 2000, alguns pesquisadores investigaram a possibilidade de modificar a interface entre o hipervisor e os sistemas convidados, oferecendo a estes um *hardware* virtual que é similar, mas não idêntico ao *hardware* real. Essa abordagem, denominada paravirtualização, permite um melhor acoplamento entre os sistemas convidados e o hipervisor, o que leva a um desempenho significativamente melhor das máquinas virtuais. As modificações na interface de sistema do *hardware* virtual (*system ISA*) exigem uma adaptação dos sistemas operacionais convidados, para que estes possam executar sobre a plataforma virtual. Todavia, a interface de usuário (*user ISA*) do *hardware* é preservada, permitindo que as aplicações convidadas executem sem necessidade de modificações. [...] (LAUREANO, MAZIERO, 2008)

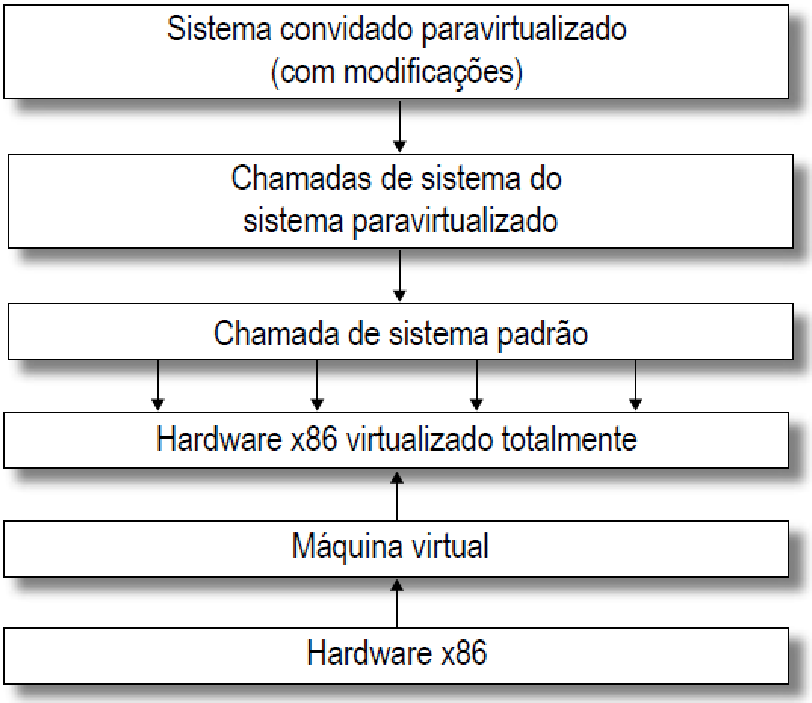


Figura 9: Representação da paravirtualização.
Fonte: Laureano (2006).

Ainda segundo os mesmos Autores:

> [...] Embora exija que o sistema convidado seja adaptado ao hipervisor, o que diminui sua portabilidade, a paravirtualização permite que o sistema convidado acesse alguns recursos do *hardware* diretamente, sem a intermediação ativa do hipervisor. Nesses casos, o acesso ao *hardware* é apenas monitorado pelo hipervisor, que informa ao sistema convidado seus limites, como as áreas de memória e de disco disponíveis. O acesso aos demais dispositivos, como mouse e teclado, também é direto: o hipervisor apenas gerencia a ordem de acessos, no caso de múltiplos sistemas convidados em execução simultânea. [...] (LAUREANO, MAZIERO, 2008).

Essa técnica é utilizada por hipervisores como o Xen, para prover recursos às máquinas virtuais.

4.5.4 Virtualização Aninhada (*Nested Virtualization*)

Virtualização aninhada é a técnica em que uma máquina virtual é criada e executada dentro de outra máquina virtual, ou um hipervisor é executado sobre outro hipervisor.

Essa técnica é útil para testar hipervisores, pois devido ao isolamento das máquinas virtuais, não afetará as outras máquinas, e também não será necessária a instalação do hipervisor a ser testado na máquina real, economizando tempo e esforço (SHIELDS, 2011).

Também pode ser usada para a migração de infraestruturas virtualizadas na computação em nuvem. O primeiro hipervisor a ter suporte à virtualização aninhada foi o KVM (JONES, 2012).

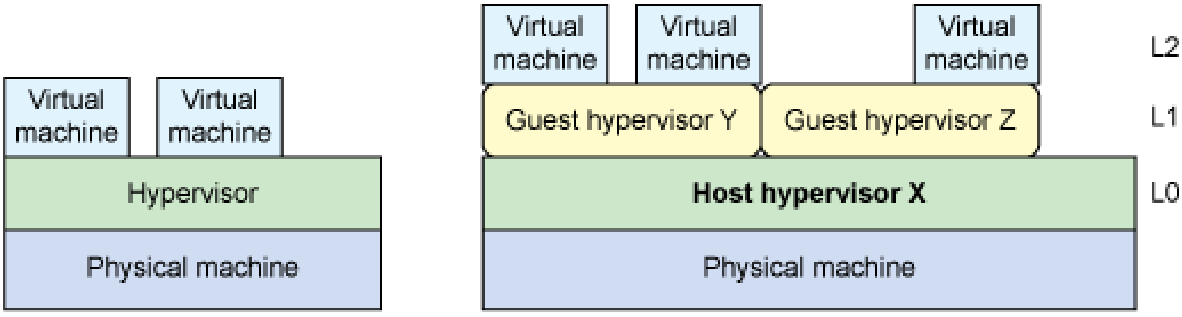


Figura 10: Comparação entre o modelo comum de virtualização e a virtualização aninhada.
Fonte: IBM, 2012.

4.6 VIRTUALIZAÇÃO EM PROCESSADORES X86

A virtualização na arquitetura x86 é um fato recente. Apesar da possibilidade de utilizar essa tecnologia já existir desde o final da década de 90 devido à hipervisores como o VMware, essa arquitetura só passou a ter suporte nativo à virtualização a partir da metade da última década, quando a Intel e a AMD, as duas principais fabricantes de processadores para computadores domésticos desenvolveram tecnologias em seus processadores, visando dar suporte à virtualização.

Essas tecnologias, que foram chamadas de extensões de virtualização, introduzem instruções extras no processador, feitas especificamente para a virtualização.

Com isso, o *overhead* da virtualização é reduzido, otimizando o desempenho. No caso da utilização da virtualização em um computador que não conta com essas tecnologias, utilizam-se técnicas de virtualização como a virtualização total ou tradução dinâmica.

4.6.1 Intel VT-X

Intel VT-x, ou *Intel Virtualization Technology*, é a tecnologia desenvolvida pela Intel para dar suporte nativo à virtualização em seus processadores. Apesar de ter sido lançada em novembro de 2005, ainda hoje alguns processadores da Intel não possuem essa tecnologia.

4.6.2 Amd V

Após a Intel lançar em seus processadores sua tecnologia para oferecer suporte a virtualização, a AMD também desenvolveu sua própria tecnologia para seus processadores, que foi chamada de AMD SVM (*Secure Virtual Machine*), que mais tarde foi renomeada como *AMD Virtualization*, que ficou abreviada como AMD V.

4.7 *DATA CENTER*

Data Center, ou centro de processamento de dados, é o local usado para armazenar equipamentos de processamento e armazenamento de dados, como computadores, sistemas de telecomunicações, etc.

4.8 CONSOLIDAÇÃO DE SERVIDORES

O uso de virtualização permite uma abordagem chamada de consolidação de servidores, que consiste no agrupamento de vários servidores, como *web, arquivos,* banco de dados, *e-mail*, entre outros, em um único servidor, ao invés de usar vários computadores isolados fisicamente. Essa técnica se torna muito útil em um ambiente onde existem muitos servidores, como um *Data Center* de uma grande empresa ou instituição de ensino, pois os benefícios decorrentes de seu uso são significativos.

Figura 11: Consolidação de servidores.
Fonte: MTI Tech Solutions (2012).

Essa abordagem é utilizada em ambientes de alta disponibilidade. E também é utilizada na computação em nuvem, para o fornecimento de recursos.

O objetivo da consolidação de servidores é a economia, tanto de recursos computacionais, ao agrupar sistemas que não utilizam totalmente a capacidade do *hardware* em um só computador, quanto economia de dinheiro, pois com menos máquinas reais funcionando, menos energia é necessário para que os serviços disponibilizados pela empresa se mantenham disponíveis.

Segundo a *VMware (2013)*, a média de servidores consolidados por máquina tem a proporção de 10/1 (taxa de 10 servidores por máquina), apesar de que é possível obter taxas ainda maiores de consolidação.

4.9 VANTAGENS DA CONSOLIDAÇÃO DE SERVIDORES

Podem-se obter muitos benefícios com o uso de virtualização. Entre esses benefícios podemos citar:

4.9.1 Melhor Utilização de *Hardware*

Um dos principais benefícios de um ambiente de servidor virtualizado é a possibilidade de consolidação de vários servidores subutilizados em uma única máquina real, o que permite um maior aproveitamento de *hardware*.

A média de utilização dos servidores, que em média é de 10 a 15%, pode ser elevada para 80% (*VMWARE, 2013*).

4.9.2 Agilidade de Implementação

Em um ambiente virtualizado, um disco rígido é representado por um conjunto de arquivos. Esses arquivos podem ser facilmente copiados e reutilizados na implementação de outra máquina virtual, o que agiliza a criação de servidores, e elimina a necessidade de *software, hardware* ou reconfigurações adicionais (KAMOUN, 2009).

Isso também facilita em testes de *software* e treinamento, pois o fornecimento rápido de um ambiente de testes idêntico ao original permite que sejam realizados testes sem comprometer o sistema original.

4.9.3 Redução do *TCO (Total Cost Of Ownership*)

Segundo Kamoun (2009), o uso de virtualização gera menos custos com investimento e manutenção do que vários servidores separados e, portanto, gera menos despesas com o *Data Center*. Isso resulta em uma vida útil maior dos servidores, ao prorrogar a compra de *hardware* novo.

Também gera uma redução no espaço necessário para o *Data Center*, pois com a consolidação dos servidores existem menos máquinas, além de menos gastos com manutenção, ventilação, cabeamento, entre outros.

Também há economia de energia, apesar de que com a centralização de vários servidores em uma única máquina, será necessário mais energia para a mesma, pois a maior utilização de *hardware* gera uma maior carga de processamento, e mais energia é necessária para o resfriamento da máquina.

4.9.4 Disponibilidade

Ainda segundo Kamoun (2009), apesar do fato de que a consolidação de várias máquinas virtuais em um único servidor físico pode levar a possibilidade de uma única falha afetar vários serviços, existem vários mecanismos de alta disponibilidade que podem evitar esse problema.

Por exemplo, é possível o uso de um cluster como hospedeiro para máquinas virtuais. Assim, caso um dos nós falhe, o cluster pode mover as *VMs* que estavam no nó que falhou para outros.

4.9.4.1 Migração

Migração é a transferência de uma máquina virtual de uma máquina física a outra distinta através da rede, sem a necessidade de desconectar o cliente ou a aplicação, e com um tempo *offline* mínimo.

Todas as características da máquina virtual são transferidas, como a memória, armazenamento e as conexões de rede. Em uma rede *Gigabit Ethernet,* esse processo pode levar menos de 2 segundos.

4.9.4.2 Facilidade de Recuperação

Como as máquinas virtuais funcionam de forma independente do *hardware* real, torna-se mais fácil a transferência da VM de um hospedeiro para outro, sem a necessidade do *hardware* ser igual ao original.

Também é possível salvar o estado da máquina virtual em um determinado ponto de sua execução (*snapshot*), para que, em caso de falha na máquina virtual, seja possível sua restauração em um momento anterior à falha (*rollback*).

4.9.5 Segurança

O uso de virtualização oferece algumas vantagens na área de segurança, como por exemplo:

4.9.5.1 Isolamento

Uma das principais características da virtualização é o isolamento entre as máquinas virtuais. Esse conceito está presente na definição formal de virtualização proposta pelos pesquisadores Popek e Goldberg, na década de 70.

O isolamento permite que, em caso de falha de software, invasão, ou qualquer outro problema que ocorra com uma máquina virtual, as outras máquinas virtuais que estejam sendo executadas não sejam afetadas.

Essa propriedade pode ser para a realização de testes, pois permite a criação de um ambiente em que possam ser testados os efeitos de programas suspeitos, sem a possibilidade de danificar a máquina virtual original ou outras máquinas virtuais executando no mesmo *host*.

4.9.5.2 Gerenciamento

Com a consolidação de servidores, os serviços tornam-se centralizados. Os hipervisores normalmente contam interfaces de gerenciamento, com consoles para a visualização das máquinas virtuais. Isso facilita o gerenciamento desses servidores, eliminando a necessidade de utilizar múltiplos terminais para o gerenciamento destes.

4.10 DESVANTAGENS (DESAFIOS E PROBLEMAS ATUAIS)

Apesar dessa tecnologia já ser bastante utilizada, a virtualização ainda apresenta alguns problemas, principalmente relacionados ao desempenho, que devem ser resolvidos ou amenizados antes de uma utilização mais ampla por parte das empresas. Estes desafios devem ser levados em conta na implementação da virtualização, pois podem afetar alguns serviços que necessitem de mais poder de processamento, ou que sejam serviços de missão crítica.

4.10.1 Desempenho

É inevitável a existência de *overhead* (tempo excessivo no processamento) no uso de máquinas virtuais, portanto a execução de várias máquinas virtuais simultaneamente em um único servidor pode afetar seu desempenho, e, portanto, o desempenho das próprias máquinas virtuais.

Por exemplo, operações de acesso ao *hardware*, como chamadas ao sistema, precisam primeiro ser capturadas pelo hipervisor, traduzidas caso seja necessário, e reenviadas para o processador, para só então serem executadas. Esse intermédio do hipervisor pode interferir em operações de entrada e saída, gerando lentidão nas mesmas.

4.10.1.1 Desempenho de Rede

Segundo Kamoun (2009), devido às máquinas virtuais compartilharem a mesma interface de rede, a largura de banda será dividida dinamicamente entre elas. Caso a demanda por banda exceder a capacidade da interface, cada VM só conseguirá uma fração da banda total.

A *CPU* do sistema hospedeiro precisa executar códigos adicionais para emular a interface de rede das VMs, o que gera um tempo adicional de processamento, que pode diminuir os recursos disponíveis para as próprias VMs.

4.10.1.2 Armazenamento

Várias VMs rodando em um mesmo dispositivo de armazenamento pode gerar concorrência de acesso ao disco, o que pode gerar lentidão, caso o servidor não possua velocidade de acesso ao disco ou de processamento suficiente para emular o acesso ao disco.

4.10.2 Segurança

Um ambiente virtualizado, principalmente os que utilizam hipervisores convidados, tem uma vulnerabilidade em potencial, que é a segurança do sistema hospedeiro. Caso a segurança do sistema hospedeiro seja quebrada, a segurança de todas as máquinas virtuais é comprometida, abrindo caminho para que as máquinas virtuais sejam invadidas por terceiros, infectadas por software malicioso, etc.

4.10.3 Disponibilidade

Devido à centralização gerada pela consolidação, se o servidor hospedeiro deixar de funcionar, e não existir nenhum mecanismo de alta disponibilidade, como um cluster executando o hipervisor, ou uma redundância de servidor, todos os serviços deixarão de funcionar.

4.11 PRINCIPAIS FERRAMENTAS DE VIRTUALIZAÇÃO

Existem várias soluções de virtualização existentes no mercado. Este item fala sobre algumas das principais ferramentas usadas pelas empresas.

4.11.1 Vmware Esx Server

VMware ESX Server é um hipervisor *bare metal* de nível empresarial (para grandes corporações) da VMware.

Segundo a VMware (2009), o VMware ESX conta com um sistema operacional Linux, chamado de console de serviço, para desempenhar funções de gerenciamento, como a execução de scripts e a instalação de agentes de terceiros para monitoramento de hardware, backup ou gerenciamento de sistemas.

4.11.1.1 *Vmware Esxi Server*

A VMware desenvolveu outra versão do VMware ESX, chamada de VMware ESXi server. A única diferença entre as duas versões é o espaço em disco ocupado pelo hipervisor, pois no VMware ESXi o console de serviço foi removido, de forma que o gerenciamento do servidor agora é feito totalmente através de ferramentas de gerenciamento remoto.

4.11.1.2 Licença

O VMware ESX é vendido em conjunto com a plataforma de virtualização vSphere, e seu preço de sua licença do está incluso no preço do vSphere.

O preço da licença do pacote VMware *vSphere Enterprise* é de US$ 2,875 por CPU, que pode ser somado ao preço do suporte básico, que é de US$ 604 por ano. Para o gerenciamento do servidor, é necessário o uso do *software* de gerenciamento da VMware, o *vCenter Server*, cuja licença pela edição *Standard* custa US$ 6,044.

Capability	ESX	ESXi 5.x
Service Console	Present	Removed
Admin/config CLIs	COS + vCLI	PowerCLI + vCLI (enhanced)
Advanced Troubleshooting	COS	ESXi Shell
Scripted Installation	Supported	Supported
Boot from SAN	Supported	Supported
SNMP	Supported	Supported
Active Directory	Integrated	Integrated
HW Monitoring	Third-party agents in COS	CIM providers
Serial Port Connectivity	Supported	Supported
Jumbo Frames	Supported	Supported
Rapid deployment and central management of hosts via Auto Deploy	Not Supported	Supported
Custom image creation and management	Not Supported	Supported
Secure syslog	Not Supported	Supported
Management interface firewall	Supported	Supported

Figura 12: Quadro comparativo entre o VMware ESX e o VMware ESXI.
Fonte: VMware (2013).

4.11.2 Xen

Xen é uma plataforma de virtualização de código livre para arquitetura x86, que foi desenvolvido inicialmente pela Xensource, e hoje pertence à Citrix. É um hipervisor do tipo *host* (tipo 1 ou nativo) e, portanto, executa diretamente sobre o *hardware*.

O Xen está sob a Licença GPL v2, sob o nome de *Xen Project*. É possível instalar o Xen em algumas distribuições Linux, como o Debian, Suse, Fedora, entre outros.

Para prover recursos às máquinas virtuais, o Xen utiliza paravirtualização (vista na seção/capítulo 4.5.2), modificando o sistema convidado para uma maior compatibilidade com o hardware virtual providenciado pelo hipervisor. Por esse motivo, o Xen tem uma lista limitada de sistemas operacionais que pode virtualizar.

O Xen é usado pela *Amazon*, como base dos seus serviços de computação em nuvem, o Amazon Elastic Compute Cloud (EC2).

4.11.2.1 Xenserver

O XenServer é uma solução pertencente a Citrix, que utiliza o Xen e funciona sobre um Linux modificado, com o Xen habilitado no *Kernel* do sistema, para que o hipervisor tenha acesso ao *hardware* e o controle do mesmo. Por funcionar de forma diferente do Xen puro, o XenServer possui uma lista de compatibilidade de sistemas operacionais diferente do Xen, além de recursos diferentes.

Antes de a Citrix tornar o XenServer *open-source,* haviam diferentes versões do XenServer disponíveis, cada uma com recursos diferentes. Porém, após a abertura do código, só existe uma única versão, que é gratuita. A Citrix oferece suporte ao XenServer com a compra de uma licença. A licença anual custa 500 dólares, e a licença vitalícia custa US$ 1,250.

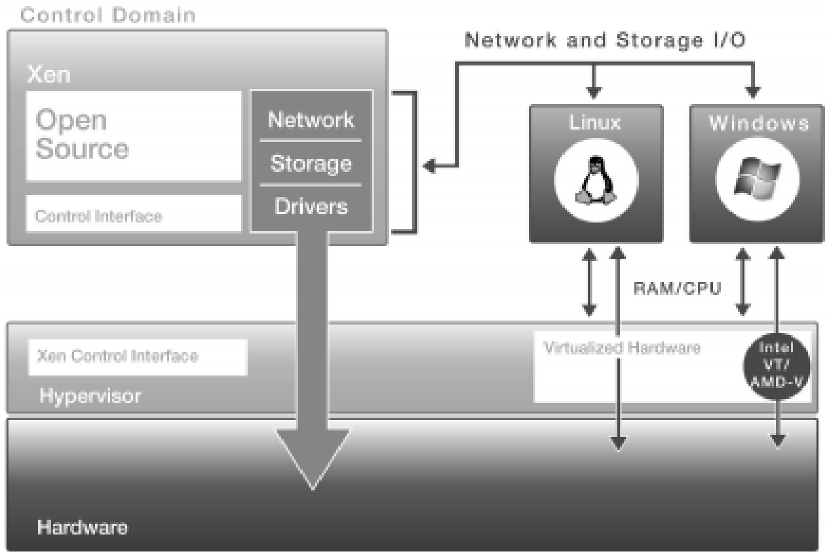


Figura 13: Arquitetura do XenServer.
Fonte: Citrix (2009).

4.11.2.1.1 Requisitos Mínimos de Instalação

O XenServer tem como requisitos mínimos para a instalação:

1. Um ou mais processadores x86 64-bit, com *clock* mínimo de 1.5 GHz. Para a virtualização de sistemas *Windows*, é necessário que o processador tenha tecnologia Intel VT ou AMD-V;
2. Pelo menos 1 GB de memória RAM;
3. Disco local com no mínimo 16 GB;
4. Placa de rede 10/100 Mbit/s ou mais.

4.11.3 Kvm

KVM (*Kernel Based Virtual Machine*) é uma ferramenta de virtualização de código aberto para Linux em arquiteturas x86, que utiliza extensões de virtualização, o que significa que o KVM só funciona em processadores que já contem com suporte a virtualização (Intel VT ou AMD-V).

O KVM utiliza a técnica de virtualização total, e necessita da instalação de uma versão modificada do QEMU para a execução das máquinas virtuais.

O KVM consiste de um módulo do *kernel* do Linux, kvm.ko, e um módulo específico do processador (kvm-intel.ko ou kvm-amd.ko). esse módulo já está incluído no *kernel* do Linux a partir da versão 2.6.20, o que significa que distribuições Linux com o *kernel* atualizado já podem usar essa ferramenta.

As máquinas virtuais do KVM executam como processos no sistema, e como o KVM faz parte do *kernel* do Linux, isso faz do KVM um hipervisor de nível 1 (*bare metal*), apesar de que sua integração com um sistema operacional permita que o mesmo seja classificado como híbrido.

5 DESENVOLVIMENTO

Cada uma das etapas previstas na metodologia para o desenvolvimento do trabalho foi desenvolvida conforme descrito a seguir.

5.1 SELEÇÃO E O ESTUDO DA BIBLIOGRAFIA

Para o desenvolvimento do trabalho foi selecionado e realizado o estudo da bibliografia pertinente ao assunto, buscando as referências em sites de literatura especializada, de organizações internacionais e governo, na biblioteca da instituição, nas anotações e materiais de aula.

Os resultados do estudo e pesquisa estão descritos no item 5 e seus subitens acima.

5.2 ESTUDO DE UM CASO REAL PRÁTICO

No desenvolvimento do trabalho foi realizada a implementação de um ambiente virtualizado, utilizando a ferramenta Citrix XenServer (vista no capítulo 4.11.2.1.1), instalando a mesma em um computador *Desktop*.

Foram criadas máquinas virtuais para serem utilizadas como servidores, e realizados testes, avaliando resultados obtidos, e comparando com as vantagens e desvantagens vistas durante a revisão bibliográfica. A realização do estudo de caso foi descrita a seguir.

5.2.1 Cenário Proposto para o Estudo de Caso

O cenário proposto para o estudo de caso é de um ambiente virtualizado, que contém 3 máquinas virtuais, sendo que 2 que serão utilizadas como servidores, disponibilizando serviços de web e banco de dados, respectivamente. A máquina virtual restante será utilizada como terminal de gerenciamento dos servidores.

5.2.2 Ferramentas de Apoio

Para o estudo de caso, serão usadas algumas ferramentas além do hipervisor escolhido, que serão usadas para auxiliar com os testes propostos, além de ferramentas necessárias para o gerenciamento apropriado do servidor hospedeiro.

As ferramentas de apoio utilizadas são Citrix XenCenter e *Backtrack*.

5.2.2.1 Citrix XenCenter

O XenCenter é uma ferramenta com interface gráfica utilizada para o gerenciamento do XenServer. O XenCenter é executado como um programa do Windows. É através desse programa que é realizada a instalação, o gerenciamento, e a configuração das máquinas virtuais.

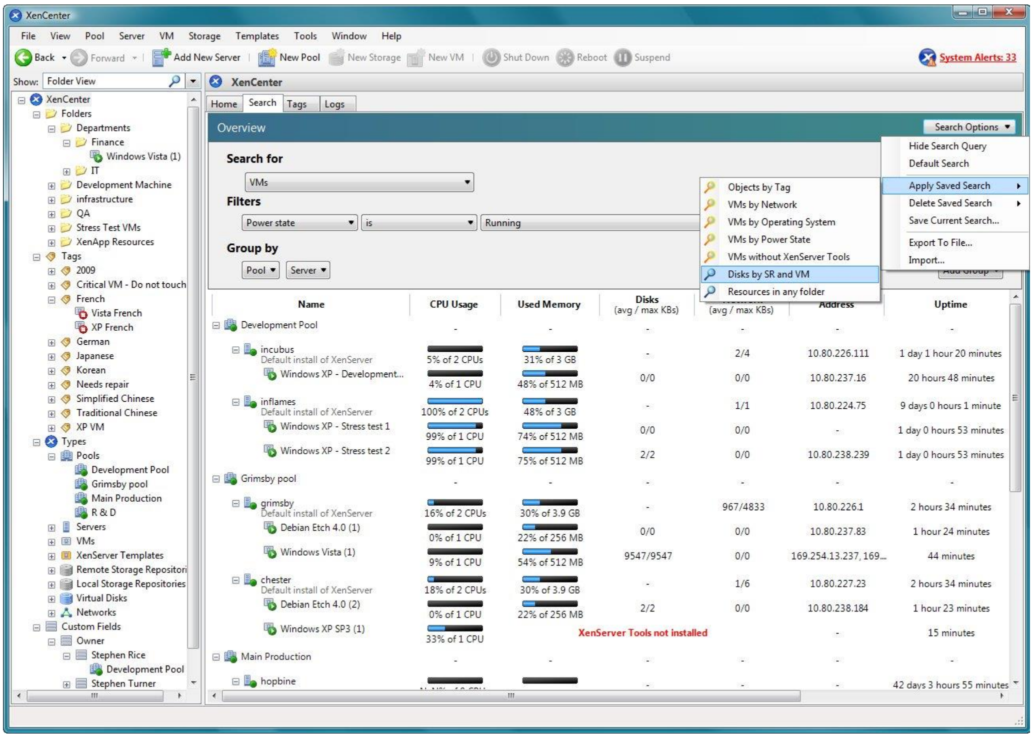


Figura 14: Tela de gerenciamento do XenCenter.
Fonte: Software Informer (2013).

5.2.2.1.1 Recursos do XenCenter

Segundo o site *Software Informer* (2013), os principais recursos do XenCenter são:

– Gerenciamento completo do servidor, incluindo a instalação e configuração de máquinas virtuais;

– Acesso aos consoles das máquinas virtuais, utilizando VNC para a instalação, XVNC para interfaces gráficas no Linux, e *Remote Desktop* para sistemas Windows;

– Gerenciamento dinâmico de memória;

– Gerenciamento de *pool* de recursos;

– Gerenciamento de VLANs e redes internas;

– Gerenciamento de *snapshots* e rollback das VMs.

5.2.2.2 Backtrack Linux

O BackTrack é uma distribuição Linux focada em testes de segurança, como simulações de invasões, ataques, etc., e por isso conta com centenas de ferramentas para vários tipos de ataques, como testes de *stress*, coleta de informações, ataque de senhas, entre outros.

O Backtrack pode ser executado de um *live CD,* o que permite que possa ser executado de qualquer lugar.

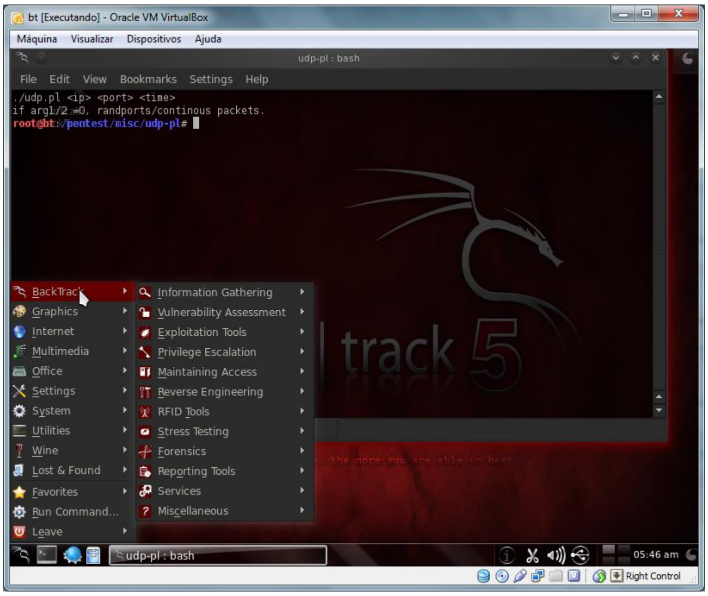


Figura 15: Captura de tela do BackTrack, que mostra os tipos de ferramentas que o sistema possui.
Fonte: Autor.

Essa ferramenta será utilizada no estudo de caso, para o teste de isolamento das máquinas virtuais.

5.2.3 Arquitetura Proposta

Para o estudo de caso, a arquitetura proposta é a de um ambiente virtualizado, utilizando a versão gratuita do Citrix XenServer para a instalação de três máquinas virtuais, como visto abaixo:

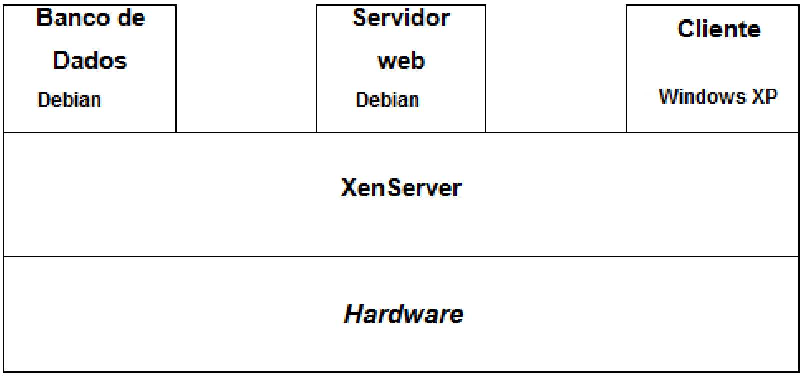


Figura 16: Representação da arquitetura do ambiente virtualizado.
Fonte: Autor.

Nessa arquitetura, que é voltada para os testes a serem realizados, as duas máquinas Debian serão utilizadas como servidor de dados e servidor *web*, respectivamente. A máquina restante, com um sistema Windows, será utilizada para acessar o servidor web, através do qual gerenciará o banco de dados.

O motivo dessa abordagem é o de tornar possível que no momento em que a máquina virtual executando o banco de dados sofrer o ataque DoS, no teste descrito no item 5.2.5.2, as duas outras máquinas percebam que a máquina atacada está *offline*.

5.2.3.1 Computador Utilizado para os Testes

O computador utilizado para o estudo de caso conta com as seguintes especificações:

- Processador Intel Core 2 Duo E8200 2.66 GHz;
- 4 gb de memória ram;
- Disco rígido de 128 GB;
- 2 placas de rede Fast Ethernet (10/100 Mbits).

5.2.4 Procedimentos de Instalação

Nesse capítulo serão descritos os procedimentos de instalação das ferramentas utilizadas no estudo de caso.

5.2.4.1 Instalação do Xenserver

Para o desenvolvimento do estudo, foi realizada a instalação do Hipervisor XenServer.

Figura 17: Tela inicial da instalação do Citrix XenServer.
Fonte: Autor.

A instalação do XenServer em si é muito simples, similar à instalação de uma distribuição Linux, como o Debian ou o Ubuntu. O que é justificado, pois o XenServer é basicamente um Linux customizado, com o Xen habilitado no seu kernel.

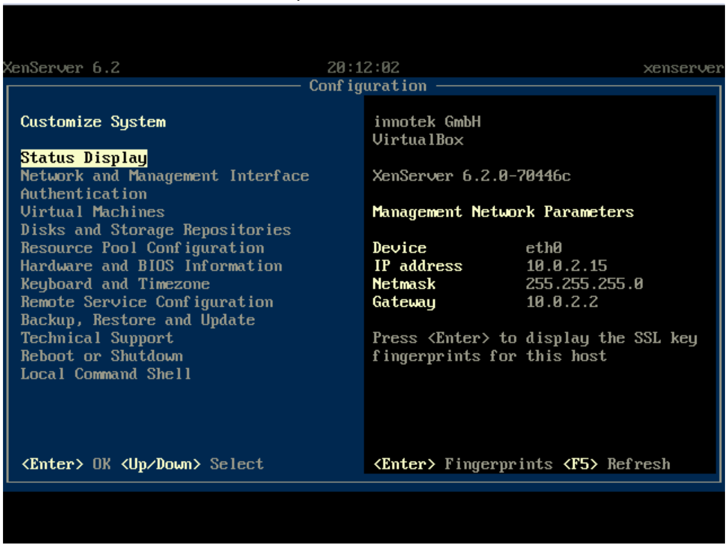


Figura 18: Tela inicial do XenServer, após o termino da instalação.
Fonte: Autor.

5.2.4.2 Instalação do XenCenter

A instalação do XenCenter, devido ao mesmo ser um aplicativo Windows, é bem direta, e portanto não será apresentada nesse trabalho.

5.2.4.3 Instalação das Máquinas Virtuais

Para que seja possível realizar a instalação de máquinas virtuais no XenServer, é necessário o uso do software Citrix XenCenter. Seguindo o padrão visto até agora nas instalações realizadas, a criação de máquinas virtuais também é simplificada.

A instalação das máquinas virtuais no XenServer pode ser feita tanto em um servidor local, quanto em um *pool* de recursos, que é um conjunto de recursos oferecidos por vários servidores existentes na rede que executam o XenServer. O *pool* de recursos pode ser configurado pelo XenCenter.

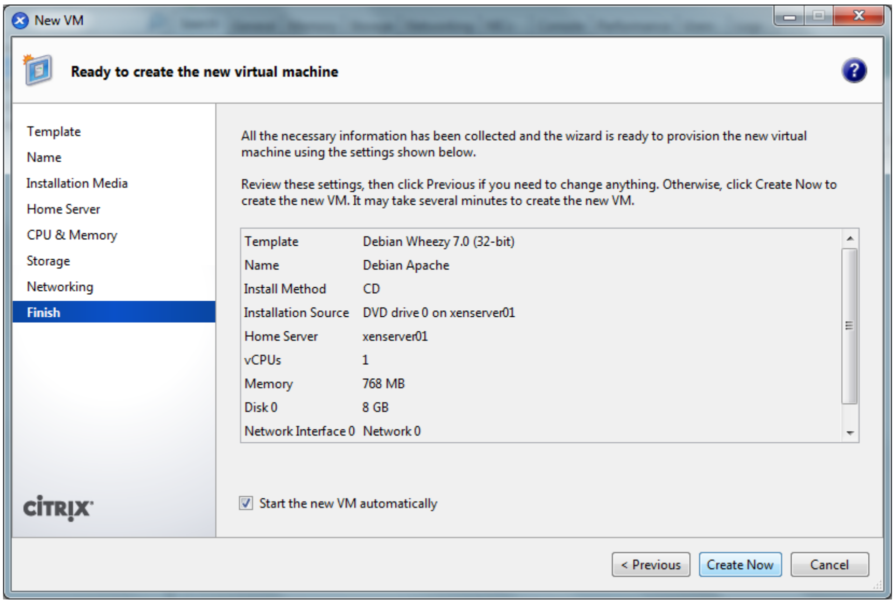


Figura 19: Tela final da criação da máquina virtual.
Fonte: Autor.

A criação da máquina virtual segue um roteiro, que começa pela escolha do *template* (modelo pré-configurado) do sistema a ser instalado, em seguida o nome da máquina virtual, o método de instalação (a instalação pode ser realizada com uma mídia física, como um CD ou DVD, ou através de uma biblioteca de imagens ISO), o servidor no qual será instalado (podem existir vários servidores em um *pool* de recursos), o número de CPUs da máquina virtual e a quantidade de memória RAM, o disco virtual a ser utilizado, e por fim, a interface de rede a ser utilizada pela VM.

Após todas as informações serem fornecidas ao XenCenter, é feita a criação da máquina virtual.

Após a criação da máquina virtual, a instalação de um sistema operacional na mesma segue da mesma maneira em que seria uma máquina real.

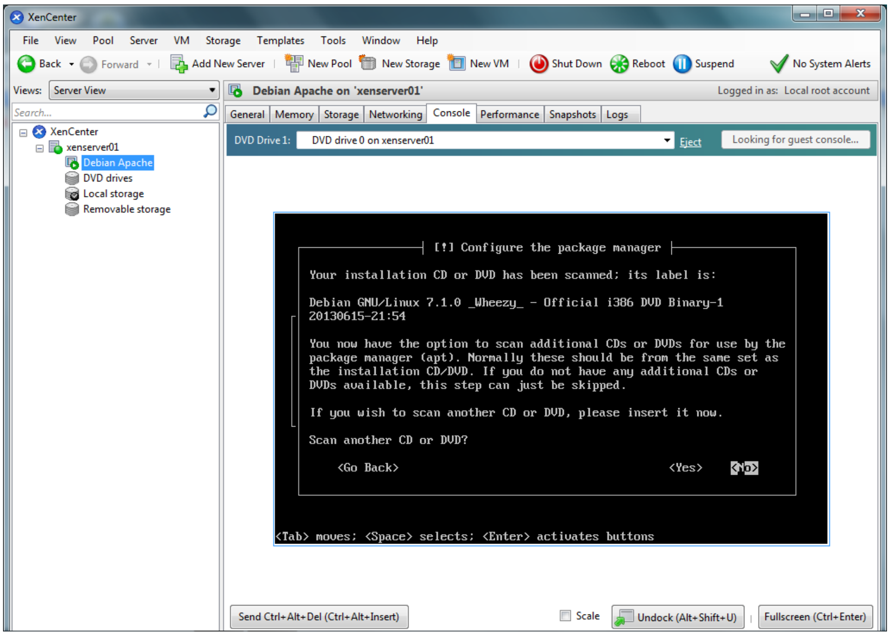


Figura 20: Console do XenCenter, enquanto é realizada a instalação do sistema operacional Debian 7 em uma máquina virtual.
Fonte: Autor.

5.2.5 Testes Realizados

Para o desenvolvimento do estudo de caso, foram realizados testes com as máquinas virtuais, com o objetivo de comprovar a veracidade de algumas das vantagens e características vistas na revisão bibliográfica. Esses testes foram descritos abaixo.

5.2.5.1 Quanto aos Testes

O objetivo do item 5.2.5 é o de realizar testes com as máquinas virtuais. Porém, algumas das características e vantagens do uso da virtualização foram percebidas sem a realização de nenhum teste, como o gerenciamento, a facilidade de criação de novas máquinas virtuais, e também de providenciar novas através da clonagem de máquinas virtuais.

Infelizmente não foi possível realizar de testes de características como latência de entrada e saída, *benchmarks* de desempenho, ou outros testes similares, pois faltariam as ferramentas e o conhecimento necessário para isso.

5.2.5.2 Teste de Isolamento

Para esse teste foi utilizada uma ferramenta chamada *Backtrack*, que é uma distribuição Linux que conta com várias ferramentas de invasão, ataques, *hacking,* entre outras, que nesse estudo de caso será utilizada para a realização do teste de isolamento entre as máquinas virtuais.

O objetivo desse teste é o de atacar uma das máquinas virtuais, e ao mesmo tempo em que essa máquina é atacada, analisar se as outras duas máquinas, que estarão acessando a máquina que será atacada via rede serão afetadas pelo ataque, já que as três máquinas virtuais compartilham a mesma interface de rede.

Segundo a teoria vista na revisão bibliográfica, a propriedade de isolamento das máquinas virtuais impede que haja qualquer alteração nas outras máquinas, tanto no desempenho quanto na segurança das mesmas. Esse teste pretende colocar essa afirmação à prova.

5.2.5.1.1 Método Utilizado

Para o teste o método de ataque que será utilizado é um ataque DoS (*Denial of Service*), que irá sobrecarregar a interface de rede da máquina virtual, impedindo ela de responder às requisições das outras máquinas.

As duas máquinas virtuais que não foram atacadas estavam conectadas à máquina alvo através da seguinte maneira: a máquina a ser atacada é um banco de dados, cujas tabelas são sendo acessadas pelo servidor web, pois uma de suas páginas funcionará como gerenciamento do banco para a máquina restante, que será um terminal de usuário.

Quando o ataque for realizado, o banco de dados deixará de responder às requisições do servidor web, que por sua vez deixará de exibir os dados do banco para o usuário.

5.2.5.1.2 Ataque Dos (*Denial Of Service*)

Para o ataque DoS, foi utilizado um script *perl* no Backtrack, chamado *slowloris*.pl, que envia requisições incompletas ao servidor, impedindo que o servidor responda às requisições de outros clientes.

O *slowloris* tem uma característica incomum em scripts de ataque DoS, que é a de não sobrecarregar o servidor, afetando somente o serviço que está sendo atacado.

A sintaxe para o uso do *slowloris* é *./slowloris.pl –dns "endereço alvo" –opções.*

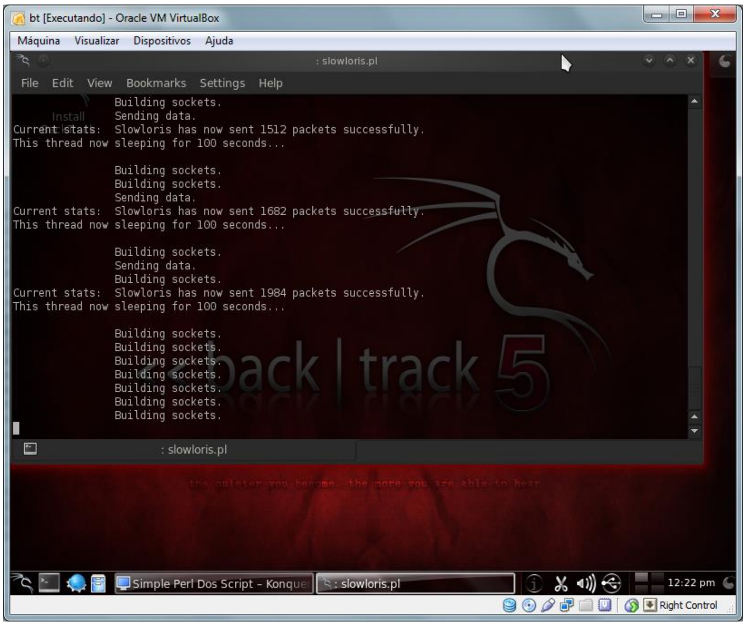


Figura 21: Slowloris.pl sendo executado.
Fonte: Autor.

Inicialmente o ataque não funcionou, não afetando a máquina alvo. Porém, em outra tentativa, O ataque obteve sucesso, impedindo a máquina alvo indisponível de responder aos pedidos das outras máquinas. As duas máquinas virtuais que não foram atacadas continuaram se comunicando normalmente, sem perda de desempenho aparente.

5.2.5.1.3 Resultado do Teste

O resultado do teste está mostrado na figura a seguir.

Figura 22: Captura de tela da máquina virtual Windows, mostrando que o banco de dados está inacessível.
Fonte: Autor.

Apesar da ocorrência de falhas durante o ataque DoS, o teste atingiu seu objetivo, ao realizar um ataque a uma máquina virtual da rede sem afetar as outras, pois nesse caso um ataque DoS deveria afetar a interface de rede todas as máquinas virtuais, mas devido ao isolamento criado pelo hipervisor, somente a fração alocada à máquina virtual atacada foi afetada.

O resultado do teste, portanto, comprovou a propriedade de isolamento das máquinas virtuais.

5.3 ANÁLISE COMPARATIVA ENTRE A TEORIA E A PRÁTICA UTILIZADA NO ESTUDO DE CASO

Os resultados do estudo de caso foram satisfatórios, apresentando uma facilidade inesperada em alguns fatores, como o gerenciamento, a instalação, a configuração das máquinas virtuais, entre outros. O desempenho das máquinas virtuais também estava dentro do previsto, considerando a escala do estudo de caso e a máquina utilizada para o mesmo.

As vantagens vistas na bibliografia se confirmaram no estudo, como o isolamento, a facilidade de criação de novas máquinas virtuais através da clonagem de VMs, a centralização do gerenciamento, entre outras. Também ficou claro quanto às desvantagens que se apresentam com o uso da virtualização, que normalmente não são tão proeminentes devido à infraestrutura dos *Data Centers* e servidores utilizados para abordagens utilizando essa tecnologia.

Apesar do desempenho das máquinas virtuais com Linux terem sido satisfatórios, a máquina virtual que foi instalado o SO Windows XP apresentou travamentos em alguns momentos, mas como já foi mencionado, isso se deve à escassez de recursos para que fossem realizadas várias instalações de máquinas virtuais, que ao final da instalação das três máquinas instaladas, sobrou menos de 500 MB de memória RAM livre para uso no XenServer.

6 CONCLUSÕES E RECOMENDAÇÕES

Com base nestes resultados dos trabalhos realizados, conclui-se o seguinte:

a) O trabalho permitiu que fosse realizado um estudo sobre a virtualização, conceitos relacionados, e as características dessa tecnologia;

b) A virtualização é uma grande tendência na área da tecnologia da informação, e deve continuar crescendo, pois com um *hardware* apropriado, pode-se utilizar da mesma para a realização de grandes projetos, como por exemplo o *Data Center* da Amazon, que utiliza o Xen para providenciar recursos de *cloud computing*

c) A virtualização ainda apresenta alguns problemas quanto à viabilidade de seu uso com computadores que não tem tantos recursos de hardware, por isso é necessário que, caso uma empresa resolva utilizar essa tecnologia em seus servidores, talvez deva fazer alguns investimentos em máquinas poderosas o suficiente para contornar os problemas em seu desempenho.

d) O estudo de caso seguiu as expectativas, ao ser confrontado com a teoria, porque ao mesmo tempo em que suas vantagens foram visíveis ao longo do estudo, suas desvantagens também foram perceptíveis, atingindo os objetivos propostos inicialmente, que eram analisar as vantagens e desvantagens do uso da virtualização e comprovar a veracidade das afirmações realizadas pelos artigos, sites, e livros pesquisados na revisão bibliográfica.

Por fim o trabalho foi importante tendo atingido os objetivos inicialmente propostos com destaque para a facilidade de instalação do hipervisor Citrix XenServer, cuja instalação e configuração foram tão simples quanto a de um sistema operacional doméstico.

BIBLIOGRAFIA CONSULTADA E/OU REFERENCIADA

BUGNION, EDOUARD; DEVINE, SCOTT; ROSENBLUM, JEREMY; WANG, EDWARD Y.; MENDEL; SUGERMAN. **Bringing Virtualization to the x86 Architecture with the Original VMware Workstation**. ACM Transactions on Computer Systems, Vol. 30, No. 4, 2012.

CITRIX. **White Paper: Technical and Commercial Comparison of Citrix XenServer and VMware vSphere.** Disponível em http://i.dell.com/sites/doccontent/business/smb/sb360/en/Documents/wp-comparison-citrixxen-vsphere.pdf. Acesso em 05/12/2013 às 10h31min.

CITRIX. **XenServer ® 6.2.0 Virtual Machine User's Guide**. 2013. Disponível em http://support.citrix.com/article/CTX137830. http://citrix-xencenter.software.informer.com/6.1/. Acesso em 02/12/2013 às 19h18min.

JONES , M. Tim. **Nested virtualization for the next-generation cloud.** Disponível em http://www.ibm.com/developerworks/cloud/library/cl-nestedvirtualization/. Acesso em 02/12/2013 às 13h25min

KAMOUN, Faouzi. ***Virtualizing the Data Center without Compromising Server Performance***, ACM Ubiquity, Volume10, Edição 9, 2009

KVM. **KVM Main Page**. Disponível em http://www.linux-kvm.org/page/Main_Page . Acesso em 03/12/2013 às 20h15min.

LAUREANO, Marcos. **Máquinas Virtuais e Emuladores - Conceitos, Técnicas e**

Aplicações. Editora Novatec, 2006.

CHEN, M. Peter; BRIAN, D. Noble. ***When Virtual Is Better Than Real***, 2001.
National Instruments. **NI Real-Time Hypervisor Architecture and Performance Details**. Disponível em http://www.ni.com/white-paper/9629/en/. Acesso em 15/11/2013 às 16h42min.

NULL, Linda; LOBUR, Julia. **Princípios básicos de arquitetura e organização de computadores segunda edição**. Editora Bookman, 2010.

OKLOBDZIJA, Vojin G. ***REDUCED INSTRUCTION SET COMPUTERS***. Disponível em http://www.ece.ucdavis.edu/~vojin/CLASSES/EEC180B/Fall99/Writings/RISC-Chaptr.PDF. Acesso em 05/11/2013 às 23h29min.

LAUREANO, Pchek; MAZIERO, Marcos Aurelio; ALBERTO, Carlos. **Virtualização: Conceitos e Aplicações em Segurança**, 2008. Disponível em http://www.dainf.ct.utfpr.edu.br/~maziero/lib/exe/fetch.php/research:2008-sbseg-mc.pdf. Acesso em 20/09/2013 às 13h43min.

POLLON, Vanderlei**. Virtualização de Servidores em Ambientes Heterogêneos e distribuídos: estudo de caso**. Disponível em http://www.lume.ufrgs.br/bitstream/handle/10183/15988/000695318.pdf.

Popek, Gerald J.; Goldberg, Robert P. ***Formal requirements for Virtualizable third generation architectures.*** *1974*.

Que raios é Hypervisor?. Disponível em http://www.vmworld.com.br/br/index.php/principal/50-virtualizacao/75-que-raios-e-hypervisor.html. Acesso em 29/09/2013 às 15h14min

QUINTILIANO DOS SANTOS, Douglas. **Conhecendo a origem da virtualização.** Disponível em: http://www.douglas.wiki.br/doku.php?id=conhecendo_a_origem_da_virtualizacao. Acesso em 10/11/2013 às 18h42min.

SHIELDS, Greg. ***What is Nested Virtualization?*** Disponível em http://windowsitpro.com/virtualization/q-what-nested-virtualization. Acesso em 02/12/2013 às 13h19min

SOFTWARE INFORMER. **Citrix XenCenter.** Disponível em:

TANENBAUM, Andrew S. **Sistemas operacionais modernos 3ª edição.** Editora Pearson. 2010.

THE NEW YORK TIMES. ***Data Centers Waste Vast Amounts of Energy, Belying Industry Image.*** Disponível em: http://www.nytimes.com/2012/09/23/technology/data-centers-waste-vast-amounts-of-energy-belying-industry-image.html?_r=0. Acesso em 20/11/2013 às 20h47min.

VMWARE BRASIL*.* **Virtualização e consolidação de servidor da VMware para**

pequenas empresas. Disponível em http://www.vmware.com/br/smb/server-consolidation.html. Acesso em 09/12/2013 às 14h47min.

VMWARE. **Compare VMware ESXi and ESX Hypervisors for Simplified Virtualization Management.** Disponível em: http://www.vmware.com/br/products/esxi-and-esx/compare.html. Acesso em 02/12/2013 às 16h42min.

VMWARE. **VMware ESX e VMware ESXi.** Disponível em http://www.vmware.com/files/br/pdf/products/VMW_09Q1_BRO_ESX_ESXi_BR_A4_P6_R2.pdf. Acesso em 02/12/2013 às 16h25min.

VMWARE. **vSphere ESX and ESXi Info Center**. Disponível em http://www.vmware.com/br/products/esxi-and-esx/overview.html. Acesso em 02/12/2013 às 16h36min.

WIKI Locaweb. **Como conectar a um banco MySQL através de script PHP**. Disponível em: http://wiki.locaweb.com/pt-br/Como_conectar_a_um_banco_MySQL_atrav%C3%A9s_de_script_PHP. Acesso em 04/12/2013 às 13h22min.

WIKIPEDIA. **Kernel Layout.svg**. Disponível em http://en.wikipedia.org/wiki/File:Kernel_Layout.svg. Acesso em 19/11/2013 às 13h25min.

XENSOURCE Documentation. ***Chapter 2. System Requirements***. Disponível em: http://docs.vmd.citrix.com/XenServer/4.0.1/installation/ch02.html. Acesso em 20/11/2013 às 23h30min.

APRESENTAÇÃO DE UMA SOLUÇÃO DE VOZ DISPONIBILIZANDO APLICAÇÕES EM PROTOCOLO SIP EM UMA REDE MPLS

PRESENTATION OF A SOLUTION OF VOICE APPLICATIONS PROVIDING SIP PROTOCOL ON A MPLS NETWORK

Ricardo Faustino da Silva[3]
Claudemir de Arruda Prado (Orientador)[4]

SILVA, Ricardo Faustino da; PRADO, Claudemir de Arruda (orientador). **Apresentação de uma solução de voz disponibilizando aplicações em Protocolo SIP em uma Rede MPLS**. *Revista Tecnológica da FATEC-PR, v.1, n.4, p. 39 -77, jan./dez., 2013.*

RESUMO:

O objetivo da pesquisa é uma apresentação de uma solução de voz, disponibilizando aplicações baseadas em protocolo SIP em uma rede MPLS. Demonstrar a solução de voz consiste na implantação de serviços VoIP na rede MPLS. Através da infraestrutura da rede, serão conectados servidores e terminais (SIP). No desenvolvimento apresentar um projeto para implantação do serviço VoIP na rede MPLS em uma rede coorporativa, baseado em estudo bibliográfico. Demonstrar as tecnologias que podem ser implementadas e suas vantagens e desvantagens.

Palavras-chave: *VoIP. SIP. MPLS. Protocolos de Comunicações.*

ABSTRACT:

The goal is a presentation of a voice solution, providing applications based on SIP protocol in an MPLS network. Demonstrate voice solution consists in deploying VoIP services in MPLS network. Through the network infrastructure, servers and terminals (SIP) will be connected .Submit a project in development for deployment of VoIP service in MPLS network in a corporate network, based on literature research. Demonstrate technologies that can be deployed and their advantages and disadvantages in this deployment.

Keywords: *VoIP SIP. MPLS.Comunication Protocol.*

1 INTRODUÇÃO

Houve uma época em que a voz era a melhor (e única) maneira de transmitir uma mensagem. Agora, a voz faz parte de um coral de canais de comunicação que incluem vídeo, redes sociais e muitos outros. Mas toda conversa precisa de uma voz

[3] Ricardo Faustino da Silva é graduado em Tecnologia em Redes de Computadores pela FATEC-PR (2013). Atua como profissional na área de Redes de Computadores.
[4] Claudemir de Arruda Prado foi o Orientador do acadêmico. Possui graduação em Engenharia Elétrica pela Universidade Federal de Itajubá (1991). Pós-graduado em Engenharia de Redes e Sistemas de Telecomunicações pelo INATEL - Instituto Nacional de Telecomunicações. Atualmente é professor nas disciplinas Redes de Longa Distância, Comunicações sem Fios I, Sistemas Digitais, Protocolos de Comunicação e Redes de Telecomunicações na Faculdade de Tecnologia de Curitiba (FATEC-PR). Tem experiência na área de Engenharia Elétrica, com ênfase em Telecomunicações. Experiência em Gerência de Rede, Projetos e Vendas de Sistemas Multiplex Ópticos, Gerência de Rede (instalação e operação de sistemas de Gerência de Rede - TMN).

forte e clara.

À medida que mais opções são disponibilizadas para realização dos negócios, fica mais fácil esquecer que a voz humana ainda é a ferramenta mais básica da comunicação nos negócios. É um aplicativo essencial.

Apresentar comunicações unificadas que funcionam com os recursos de TecnoIogia da Informação e voz.

Apresentar uma alternativa de solução de comunicação para empresa coorporativa, reduzindo custos e agilidade na comunicação este é o tema da pesquisa.

1.1 OBJETIVOS GERAIS

Demonstração para solução de aplicações e voz empresarial. Apresentar suporte às comunicações unificadas e colaboração – mobilidade, conferência, presença, serviço de número único, mensagens unificadas.

Apresentar uma solução de sobreposição para um sistema de telefonia existente para fornecer um gerenciamento de sessão SIP centralizado. Simplifica a administração, reduz custos de ligação, fazer interligação de vários sites e facilita a migração para as comunicações IP baseadas em software.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos são os seguintes:

a) Conhecer uma rede MPLS, funcionamento da rede e quais suas vantagens e desvantagens;

b) Demonstrar o protocolo SIP, implementação do protocolo SIP na solução de voz;

c) Apresentar um cenário com descritivo dos equipamentos para funcionamento de aplicações e voz;

d) Desenvolvimento do cenário;

e) Mostrar as conclusões e vantagens e desvantagens desta solução.

2 JUSTIFICATIVA

Objetivo da telefonia em redes IP é prover uma forma alternativa aos sistemas tradicionais, mantendo as mesmas funcionalidades e qualidade aproximada da rede pública telefônica mas permitindo novas aplicações com integração de processamento de dados e melhor aproveitamento dos recursos das redes de transporte.

Possibilidade de integrar as aplicações de transporte de sinais de voz e dados e eventualmente vídeo por um mesmo meio de acesso.

Disponibilizar preços de utilização de serviços de voz com independência de tempo e distância, com a confiabilidade e disponibilidade das redes de voz.

Demonstrar softwares que são utilizados hoje em grandes empresas que funcionam com comunicações unificadas com seus recursos de TI, voz e aplicativo.

Apresentar que o alto custo para implantar um sistema unificado é alto, porém o resultado vem logo com economia dos recursos durante longo tempo.

3 METODOLOGIA UTILIZADA NO DESENVOLVIMENTO

O trabalho foi desenvolvido como uma pesquisa bibliográfica, ou seja, a aplicação de uma teoria para demonstração, seguindo os passos e como foram desenvolvidos conforme destacados a seguir.

a) Seleção e o estudo da bibliografia;
b) Levantamento de ferramentas para apoiar na apresentação e na escolha das aplicações;
c) Análise da teoria e a prática utilizada na apresentação do desenvolvimento;
d) Conclusões e considerações.

Cada uma das etapas está detalhada no item que trata sobre o desenvolvimento do trabalho.

4 REVISÃO BIBLIOGRÁFICA

A seguir estão apresentados os itens resultantes da pesquisa e estudos efetuados na literatura especializada.

4.1 PROTOCOLO

Conforme Falbriard (2002) o protocolo é o método utilizado em redes de comunicação que definem conjuntos de regras que coordenam e asseguram o transporte das informações úteis entre dois ou mais dispositivos. Estabelecem os formatos, as regras e os métodos e negociam e concordam sobre o uso de parâmetros.

Os protocolos tratam de questões básicas como, quais são os sinais que podem ser enviados, como fazer um endereçamento de uma mensagem, quando pode ocorrer o envio de uma mensagem, quais são as mensagens que podem ser enviadas e como estabelecer uma conexão.

4.2 TCP/IP

Conforme Soares (2002) o IP é responsável pelo encaminhamento dos pacotes pela rede, entre as diversas sub-redes, desde a origem até o destino. TCP/IP se incube do transporte fim a fim confiável das mensagens de dados entre dois sistemas.

O IP é um protocolo não orientado a conexão, do tipo data grama e o TCP/IP é um protocolo orientado a conexão. Transporte oferecido pelo serviço TCP/IP é da alta confiabilidade, para redes que exigem qualidade de serviço. Quando essa qualidade não é importante, utiliza-se como protocolo de camada 4 o UDP, que não é orientado a conexão.

Os protocolos TCP/IP podem ser utilizados sobre qualquer estrutura de rede, simples ou complexa, ponto a ponto ou ponto a multiponto.

4.2.1 Aspectos básicos do TCP/IP

Protocolo IP provê a capacidade de comunicação entre cada elemento componente da rede para permitir o transporte de uma mensagem de origem até um destino. Funções realizadas por este protocolo estão à atribuição de um esquema de endereçamento independente do endereçamento da rede utilizada abaixo e independente da própria topologia da rede utilizada.

O quadro a seguir mostra a camada OSI e TCP/IP.

OSI	***TCP/IP***					
Aplicação	***FTP***	***TELNET***	***FINGER***	***NFS***	***SMTP***	***SNMP***
Apresentação						
Sessão						
Transporte	***TCP,UDP***					
Rede	***IP***					
Enlace	***Frame Relay, ATM***					
Física	***Enlace de WAN***					

Quadro 2 – OSI/TCP.
Fonte: Autor.

4.2.2 Protocolos de Transportes do TCP/IP

Os principais protocolos de aplicação TCP/IP são:

- FTP (*File Transfer Protocol*), usado para transferência de arquivos, trabalhas com as portas TCP 20 e 21;
- TELNET, protocolo que permite a criação de um terminal remoto de uma estação, trabalha sobre o TCP na porta 23;
- SNMP, protocolo usado para gerência de redes, trabalha sobre o UDP na porta 161 e a estação de gerência sobre o TCP na porta 162;
- HTTP, protocolo usado para páginas web, trabalha sobre o TCP na porta 80;
- DNS-–(Domain Name System), protocolo usado para resolução de nomes na Internet, trabalha sobre o protocolo UDP na porta 53.

4.3 MPLS (*Multiprotocol Label Switching)*

À medida que a Internet crescia, adquira-se a consciência de que ela se transformava na fundação de uma nova base para economia.

Segundo Tronco (2006) o MPLS aparece no cenário de redes como uma arquitetura emergente, que através do modelo de encaminhamento de pacotes baseados em rótulos, é possível a interoperabilidade e compatibilidade com diversas tecnologias de rede utilizadas pelos principais *backbones* ao redor do mundo.

A tecnologia que se apresenta mais promissora na tentativa de melhorar o desempenho das redes é o MPLS, por ser flexível e por permitir seu mapeamento em várias tecnologias de rede. As suas melhores perspectivas se apresentam no uso conjunto com a tecnologia IP, adicionando a esta o paradigma de circuito virtual e a possibilidade de aplicar conceitos como a engenharia de tráfego e a garantia de QoS, sem haver a necessidade de alterar totalmente a estrutura já existente nas redes de comunicação atuais.

Essa perspectiva suscitou o aparecimento de soluções que visavam melhorar o desempenho e QoS de um roteador IP, simplificando o complexo modelo de sobreposição do IP ao ATM.

Todas essas características citadas anteriormente nos fazem crer que o MPLS será capaz de melhorar a qualidade das transmissões de voz e vídeo (através do QoS), a segurança e também a velocidade e planejamento nas transmissões de dados (através da engenharia de tráfego) (TRONCO, 2006).

4.3.1 Rótulo do MPLS

O MPLS define uma arquitetura e um conjunto de protocolos para encapsular o tráfego IP em um novo cabeçalho de roteamento.

O rótulo MPLS tem um comprimento (32bits) fixo que funciona como representação curta do cabeçalho dos pacotes IP. Os 32 bits do cabeçalho do MPLS contêm os seguintes campos:

Label (20bits), que transporta o valor efetivo do rótulo.

CoS (3bits), utilizado para classificar a prioridade dos pacotes em até oito níveis.

Stack (1bit) indica o inicio/fim de uma pilha de rótulos hierárquicos, pois se pode ter uma sequência de rótulos contíguos entre o cabeçalho de camada 2 e camada 3. O fim a pilha, que é o primeiro rótulo a ser atribuído, é indicado pelo valor 1 desse bit.

TTL (8bits) provê a mesma funcionalidade que o TTL do IP convencional, duração de vida permitida ao pacote para trafegar na rede.

4.3.2 Elementos principais da arquitetura do MPLS

A seguir estão apresentados os elementos principais da arquitetura MPLS.

LER (*Label Edge Router*): equipamento que atribui o primeiro rótulo no pacote a ser transmitido, com base no endereço de destino e na qualidade de serviço requerida.

LSR (*Label Switching Router*): equipamento que faz a troca de rótulos, retira os rótulos dos pacotes que chegam às portas de entrada, coloca novos rótulos neles e envia-os para as portas de saída. Faz parte do núcleo da rede e encaminha os pacotes de um LSR a outro até o destino, pelo caminho definido nas tabelas de encaminhamento.

FEC (*Fowarding Equivalence Class*): representa um serviço ou conjunto de serviços cuja qualidade é equivalente. Serviços com a mesma FEC percorrem a mesma rota na rede.

LSP (*Label Switched Path*): é o caminho virtual fim a fim que os pacotes de uma dada aplicação percorrem pela rede, comutando enlace a enlace pela troca de rótulos, quando alocados a uma FEC.

FIB (*Foward Information Base*): base de dados dos equipamentos MPLS que contém a tabela de encaminhamento com os valores de rótulo/porta de entrada e a respectiva atribuição para rótulo/porta de saída.

LIB (*Label Information Base*): base de dados os equipamentos MPLS contém a informação cruzada do tipo de rótulo a ser utilizado para se obter uma determinada qualidade de serviço na rota.

LDP (*Label Distribution Protocol*):protocolo que distribui automaticamente os rótulos na rede, configurando as bases de dados (FIB e LIB) os equipamentos MPLS.

RVSP-TE (*Resources reSerVation Protocol – Traffic Engineering*): protocolo de sinalização utilizado para solicitar conexões MPLS (LSPs) e fazer a reserva dos recursos na rede.

CR-LDP (*Constraint-based Routing Label Distribution Protocol*): é um protocolo alternativo ao RVSP-TE também para sinalização e possui capacidade de estabelecer LSPs do tipo *strict* ou *loose*, em que as *stricts* são orientadas a conexão e as *loose* são não orientadas a conexão.

4.3.3 Dinâmica do protocolo MPLS

Na entrada de rede MPLS, um rótulo é agregado a cada pacote IP pelo equipamento LER. Esse rótulo contém informações sobre o próximo roteador MPLS (LSR) pertence ao caminho predefinido para o pacote, o LSP. Em todos os equipamentos LSRs subseqüentes, o rótulo é utilizado para as decisões de encaminhamento.

Quando o pacote chega a um LSR, ele examina e o utiliza como um índice na tabela de encaminhamento, a FIB. Com base nessa tabela, o rótulo é redefinido e trocado (*swapped*) e o pacote propaga pelo caminho correspondente à classe de serviço (FEC) a que foi atribuído. Pacote deixa rede MPLS, o rótulo é retirado e o pacote IP original é recuperado.

4.3.4 Funcionalidade de roteamento

Procedimento de estabelecimento de conexões, o roteamento é realizado uma única vez na entrada de rede pelo LER e o encaminhamento dos pacotes é baseado nos rótulos e executado pelos LSRs, que são os roteadores do núcleo de rede.

Parte do controle é implementada em software, para melhorar a eficiência da rede e a parte do encaminhamento é implementada pelo hardware (TRONCO, 2006).

4.3.5 LDP e tráfego

O LDP utiliza o algoritmo de *Djsktra* (algoritmo que toma decisão que parece ótimo no momento) para calcular as métricas e em seguida atribuir e distribuir os rótulos para os LSRs.

Desta forma compõe-se uma base de dados, a LIB, que possui informações sobre a topologia e estado de enlaces.

O RSVP-TE e/ou o CR-LDP que cria uma LSP com reserva de banda e de acordo com os parâmetros especificados nas mensagens de sinalização.

O cômputo de uma LSP com TE, é efetuado pelo algoritmo de *Djkstra* modificado, designado por *Constrained Shortest Path First* – CSPF, que contém atributos associados com o estado dos recursos da rede, como largura de banda total do enlace, largura de banda reservada no enlace, largura de banda média do enlace e outros.

4.3.6 Atributos do MPLS

O atributos do MPLS são os seguintes:

- MPLS é a maneira mais efetiva de integrar IP e as redes ATM numa rede única;
- MPLS reduz o processamento dos roteadores, melhorando a eficiência no encaminhamento dos pacotes;
- MPLS provê QoS às redes IP;
- MPLS elimina *overheads*, não é necessária a utilização do ATM como camada 2;

- Facilita a operação e o projeto da rede única;
- Opera sobre qualquer tecnologia de camada 2 (desde Ethernet até a óptica);
- Aceita qualquer protocolo da camada 3.

4.4 *QUALITY OF SERVICE* (*QoS*)

De acordo com Bernal (2007), o QoS é um requisito para as aplicações em que é necessário que certos parâmetros (como atraso, perdas, variação de atraso, largura de banda) estejam dentro de limites bem definidos (com um valor mínimo ou valor máximo estabelecido).

Aplicações que incluam voz e vídeo com alta taxa de utilização de largura de banda estão aumentando cada vez mais nos dias de hoje. As redes devem fornecer serviços que sejam seguros, previsíveis que possam garantir a qualidade dessas aplicações.

Os protocolos de qualidade de serviço(RSVP, DiffServ, MPLS, SBM) e mecanismos de priorização (ToS, CoS) garantem o serviço de sua estrutura tecnológica para o transporte de voz.

Assim, a utilização do MPLS ajuda a alcançar a qualidade de serviço exigida de ponta a ponta, ao mesmo tempo mantendo a simplicidade, escalabilidade e gerenciabilidade.

As principais características dos dispositivos que executam a QoS são:

- Nos pontos significativos de troca de velocidades e pontos de agregação;
- Nos dispositivos que possuem buffers de transmissão, que são memórias temporárias com a tendência de manterem-se sempre preenchidas quase integralmente, pelo mecanismo TCP, que permite alternar o tráfego cursado por diversos terminais da rede;
- Nos dispositivos que executam *buffering* para reduzir as perdas e introduzir normalização nos atrasos de transmissão, atenuando *jitter*, que é a variação do atraso dos pacotes na rede;
- Nos dispositivos que permitem a priorização do tráfego que é mais sensível às perdas e atrasos, como é o caso do VoIP.

4.5 VOIP

Convergência é um termo usado para combinação de computadores pessoais, telecomunicações e vídeo acessível a qualquer um. Podemos definir convergência da rede como um termo geral para a integração de voz, vídeo e rede de dados.

VoIP é um termo usado para telefonia IP, um conjunto de facilidades que permite gerenciar o envio de voz digitalizada sobre pacotes IP. Informação de voz e vídeo é transmitida por pacotes discretos na forma digital, em vez das técnicas tradicionais de comutação de circuitos da rede telefônica (BERNAL, 2007).

Atualmente VoIP é uma das tecnologias que mais crescem no mercado mundial. As empresas buscam constantemente a redução de custos, como custo com telecomunicações, as redes com voz sobre IP é cada vez maior, representando uma redução substancial nos custos das chamadas.

4.6 *CODECS*

Um *codec* de áudio é um dispositivo de hardware ou um programa de computador que codifica/decodifica dados de áudio digital de acordo com um determinado tipo de arquivo de áudio ou áudio "*streaming*". O termo *codec* é uma combinação de coder-decoder ("compressor/descompressor"). O objeto do algoritmo de um *codec* é representar os sinais de alta fidelidade do áudio com a quantidade mínima de bits, preservando ao mesmo tempo a qualidade. Isto pode efetivamente reduzir o espaço de armazenamento e a largura de banda exigidos para transmissão do arquivo de áudio armazenado.

O aspectos que envolvem o *CODECS* estão apresentados a seguir.

4.6.1 Digitalização de voz

Para que a voz seja transmitida em um sistema de comunicação digital, deve sofrer um processo de digitalização pelo qual a voz é transformada inicialmente em amostragens do sinal original, e posteriormente cada amostragem é processada e convertida em um conjunto de bits codificados a serem transmitidos até o destino (BERNAL, 2007).

4.6.2 Empacotamento de voz em protocolo IP

No VoIP a voz deve ser digitalizada e transportada pelo empacotamento em protocolo IP.

O ingresso da voz no sistema de digitalização e empacotamento é feito por um ou mais quadros de voz encapsulados em segmentos do protocolo RTP, dentro de segmentos UDP, envolvidos por um pacote IP e transmitidos pela rede de roteadores.

Na saída da rede, é necessário tratar do atraso de propagação e da sua variação (*jitter*). Controle da perda de pacotes e em seguida os pacotes IP são abertos, seguidos pelo tratamento dos segmentos UDP e RTP. Ao final se processa a decodificação e a recuperação do sinal de voz.

Processamento de codificação de voz causa um atraso no empacotamento da voz nos protocolos IP/UDP/RTP e no enquadramento e enfileiramento dos pacotes, decorrente dos processos de conversação do sinal analógico em digital e em virtude de outros mecanismos adicionais, como criptografia do conteúdo dos pacotes para preservar a segurança e a privacidade.

Esses processos são executados na transmissão e na recepção dos pacotes, geram atrasos em ambos os casos (BERNAL, 2007).

O esquema de compressão definido pela RFC 2508 é apropriado para o uso de VoIP. Ele comprime o cabeçalho do conjunto de protocolos IP/UDP/RTP, o que resulta maior eficiência do que compactar cada cabeçalho individualmente.

A figura abaixo demonstrar o processo de empacotamento de voz:

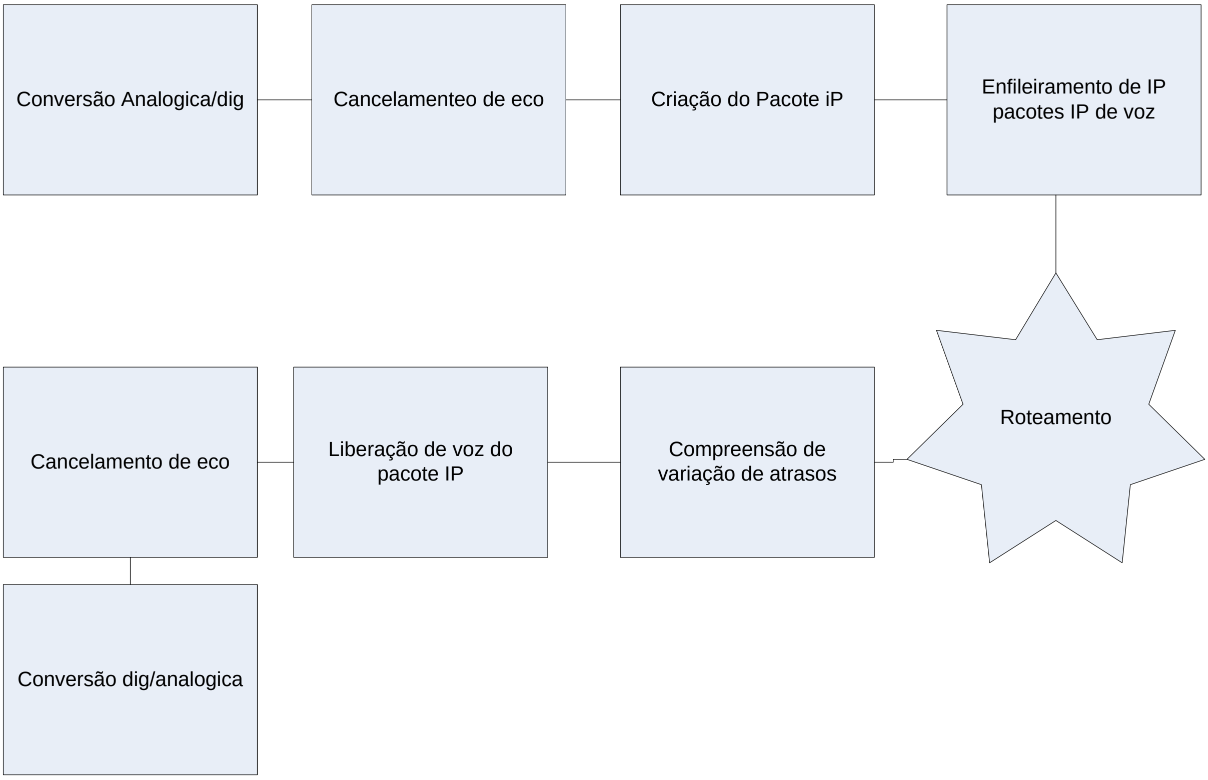


Figura 01 – Empacotamento de voz.
Fonte: Autor.

4.6.2.1 RFC 2508

Este documento (RFC 2508 – *Request For Coments – Number 2508*) está publicada para a informação da comunidade mundial da área.

A compactação de IP / UDP / RTP Cabeçalhos em fevereiro de 1999.

Cabeçalho tamanho pode ser reduzido à compressão através de técnicas como tem sido feito com grande sucesso para a TCP [2]. Neste caso, poderá compressão ser aplicada à RTP cabeçalho sozinho, com um fim-de-final, ou para o combinação de IP, UDP e RTP cabeçalhos em um *link-by-Link* base.

Comprimir os 40 bytes de cabeçalhos combinadas em conjunto proporciona substancialmente mais do que ganhar comprimir 12 *bytes* de cabeçalho RTP sozinho porque o resultado é aproximadamente o mesmo tamanho (2-4 bytes) em noutro caso. Comprimindo-a com um elo com base também fornece melhor desempenho, porque o atraso e a taxa de perda são mais baixos.

Portanto, aqui é definido o método combinado para a compressão de IP, UDP e RTP cabeçalhos em um *link-by-Link* base.

O presente documento estabelece um regime de compressão que pode ser utilizado com IPv4, IPv6 ou pacotes encapsulados com mais de um cabeçalho IP, embora o foco inicial seja sobre IPv4.

4.6.3 Eficiência do empacotamento

A quantidade de voz colocada em cada pacote tem influência direta na eficiência do tráfego de pacotes pela rede. O transporte VoIP é ineficiente para pouca quantidade de voz por pacote, portanto cria pacotes pequenos.

As diferenças do atraso de propagação de um pacote VoIP em relação ao próximo provocam aparecimento do *jitter*. O uso de memórias intermediárias (*buffers*) elásticas na recepção dos pacotes VoIP neutraliza esse efeito, uniformiza o atraso entre a chegada de um pacote e do próximo. A variação máxima do atraso (*jitter*) tolerável é entre 20 e 50ms.

*Jitte*r é uma variação estatística do atraso na entrega de dados em uma rede, ou seja, pode ser definida como a medida de variação do atraso entre os pacotes sucessivos de dados. Observa-se ainda que uma variação de atraso elevada produzisse uma recepção não regular dos pacotes.

Logo, uma das formas de minimizar os efeitos da variação de atraso é a utilização de buffer, o qual armazena os dados à medida que eles chegam até que os pacotes enviados pela origem da comunicação sejam recebidos no destino final desta comunicação, então os pacotes são ordenados de acordo com a ordem de envio e os encaminha para a aplicação seguindo a mesma cadência.

4.6.4 Eco e cancelamento

Outro efeito indesejado que deve ser tratado nos sistemas que convertem sinais de voz em VoIP é o eco.

O eco é devido à alimentação do canal de recepção pelo sinal do emissor e pelo efeito de realimentação nos transformadores híbridos que convertem os dois canais (emissor e recepção) na entrada do par metálico telefônico em outros distintos; na saída à conversão é inversa.

4.6.5 Perdas de pacotes em sistema VoIP

Sistemas VoIP podem sofrer perdas de pacotes durante a operação normal, o que degrada a qualidade da comunicação de voz ou causa a sensação de vazio por desconexão.

O uso de esquemas de correção de erros associados aos protocolos IP/UDP/RTP pode melhorar o desempenho. Uma alternativa para a correção de erro pela perda de pacotes é inserção de pacotes com conteúdo de silêncio no lugar dos pacotes perdidos.

4.7 SIP

O SIP ou *Session Initiation Protocol* é um protocolo padrão IETF (*Internet Engineering Task Force*) usado para iniciar sessões de usuário multimídia, podendo ser usado para vídeo, voz, chat, jogos e realidade virtual.

SIP trabalha na camada de aplicação, como HTTP, FTP e Telnet. A partir do SIP podemos iniciar uma chamada telefônica na rede IP, monitorar ou terminar, além disso, o SIP trabalha também com sessões *unicast* e *multicast*, possibilitando recursos de conferência de voz.

De acordo com Moraes (2009), SIP é baseado em um modelo cliente/Servidor e usa maior parte dos cabeçalhos do HTTP. É um protocolo confiável, independente do TCP.

Os serviços do SIP para o estabelecimento e o encerramento de sessões multimídia incluem:

Localização do usuário: um usuário pode ser movimenta por toda rede e este procedimento determina a localização do usuário e se o mesmo pode ser usado para comunicação;

Capacidades do usuário: este procedimento é utilizado para determinar as capacidades de mídia dos usuários envolvidos na comunicação e para determinar os parâmetros da mídia a serem usados;

Disponibilidade do usuário: após um usuário ser localizado é preciso saber se ele esta disponível para comunicação e determinar se o usuário possui recursos disponíveis para iniciar uma nova comunicação;

Configuração da chamada: é o processo de definição dos parâmetros que serão utilizados para o estabelecimento da chamada;

Controle da chamada: processo de gerenciamento da chamada, incluindo processos de transferência de ligações e encerramento da chamada.

4.7.1 Arquitetura

A arquitetura SIP é composta de dois elementos de rede: os terminais e os servidores.

Os Terminais: iniciam os pedidos de conexão e usualmente são telefones IP, PCs ou *gateways*.

Os Servidores: os servidores SIP localizam usuários, mapeiam nomes em endereços IP, encaminham mensagens de sinalização e solicitam encaminhamento de chamadas entre terminais.

Existem três tipos de servidores:

1) Servidores de registro: recebem as atualizações a respeito da localização dos usuários. Monitoram os terminais dentro do seu domínio de rede;
2) Servidores Proxy: encaminham pedidos e respostas SIP, é o ponto de contato do terminal para envio/recebimento das mensagens de sinalização. O SIP define vários tipos de servidores Proxy:
   - *Call-Stateful*: localizado na borda da rede. Monitora o estado da chamada;
   - *Transaction-Stateful*: fica próximo ao núcleo da rede. Monitora as solicitações e respostas, mas não tem conhecimento do estado da chamada;
   - *Stateless*: localizado no núcleo da rede, recebe as solicitações de chamada e as encaminhada. São servidores mais rápidos;
3) Servidores de Redirecionamento: recebem pedidos e então retornam a localização de outro terminal ou servidor em que o usuário pode ser encontrado.

4.7.2 Processo de estabelecimento de chamadas SIP

A Figura 02 mostra o estabelecimento de uma sessão RTP (*Real-Time Transport Protocol*) em tempo real com uma transação SIP.

Figura 02 – Estabelecimento de uma chamada SIP.
Fonte: Microsoft (2013).

A figura 03 ilustra uma interação SIP que estabelece uma sessão RTP entre duas UA (Unidade de Atendimento) em domínios separados.

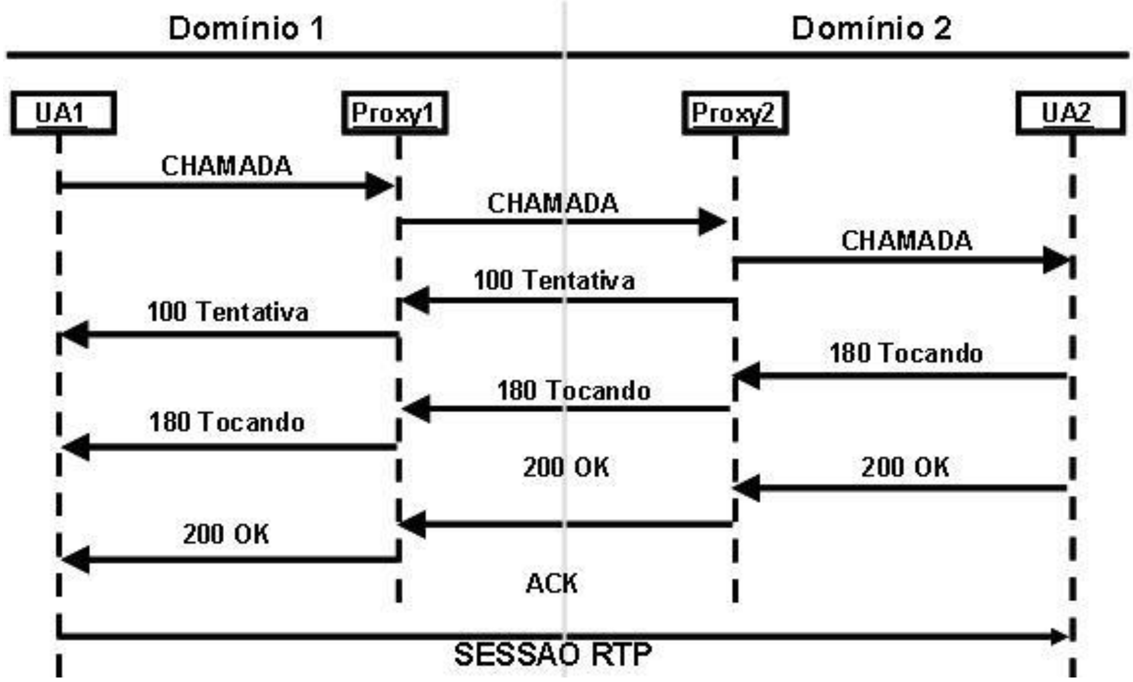


Figura 03 – Chamada SIP entre 2 domínios.
Fonte:Microsoft (2013).

4.7.3 Mensagens SIP

As mensagens SIP utilizam o HTML (*Hyper Text Markup Language*), as quais são baseadas no (HTTP). As mensagens consistem em uma linha inicial que especifica o protocolo, seguida das propriedades da chamada e informações de serviço, e um campo opcional que pode conter uma descrição da seção.

O quadro 3 mostra os métodos básicos e solicitação de conexão para iniciar uma conexão, que são enviados pelas trocas de mensagens do protocolo SIP.

Método	Significado	Finalidade
INVITE	CONVIDAR	Estabelece uma sessão
ACK	CONFIRMAR	Confirmar o comando convida
BYE	ATÉ LOGO	Finaliza uma sessão
CANCEL	CANCELAR	Cancela a sessão ainda não respondida
REGISTER	REGISTRO	Informa a localização do usuário, o nome do usuário e o endereço IP
OPTIONS	OPÇÕES	Informar a capacidade e disponibilidade dos telefones de chamada de recebimento SIP

Quadro 3 – Métodos básicos conexão SIP.
Fonte: Adaptado de Bernal (2007).

O quadro 4 mostra os requerimentos dos métodos básicos de respostas às solicitações de conexão SIP acionam respostas que constam seis classes.

1xx = respostas de informações	100 Tentando	180 Chamando	181 Chamada sendo encaminhada	182 Fila de espera	
2xx = respostas de confirmação	200 OK	202 Aceito, usado para referencias			
3xx = respostas de redirecionamento	300 Múltiplas escolhas	301 Movido permanente	302 Movido temporariamente	305 User proxy	380 Serviço Alternativo
4xx = comandos não realizados	400 Requerimento errado	401 Não Autorizado: Restrito aos usuários registrados. Proxys devem ser usar Proxy Autorização 407	402 Necessita pagamento (reservado para uso futuro)	403 Proibido	404 Não encontrado: Usuário não encontrado
4xx = comandos não realizados	407 Necessária autenticação do proxy	408 Timeout pedido: não foi possível localizar o usuário a tempo	410 Saiu: o usário, mas não está mais disponível	413 Pedido de dados muito longo	414 Pedido-URL muito longo
4xx = comandos não realizados	420 Extensão ruim: erro na extensão utilizada do protocolo SIP, não compreendida pelo Servidor	421 Extensão necessária	423 Intervalo muito breve	480 Temporariamente não disponível	481 Chamada/transação não existente
4xx = comandos não realizados	484 Endereço incompleto	485 Ambíguo	486 Ocupado aqui	487 Pedido concluído	488 Não aceito aqui
5xx = erros do servidor	500 Erro interno do servidor	501 Não implementado: o método de pedido SIP não está	502 *Gateway* ruim	503 Serviço não disponível	504 Servidor em time-out

		sendo implementa do aqui			
6xx = erros globais	600 Ocupado em todo lugar	603 Rejeitar	604 Não existe em nenhum lugar	606 Não aceito	

Quadro 4 – Métodos básicos de respostas SIP.
Fonte: Adaptado de Bernal (2007).

4.8 RTP

O RTP (*Real-Time Transport Protocol*) é um protocolo padrão Internet usada para gerenciar e transmitir dados em multimídia na modalidade *unicast* e *multicast*, protocolo para suportar vídeo conferência entre participantes dispersos, é muito utilizado em aplicações de telefonia Internet (MORAES, 2009).

O RTP roda sobre UDP (*User Datagram Protocol*), e o SIP usam o RTP.

O pacote RTP inclui número de sequência que é usado para detectar pacotes perdidos na rede, identificação do *payload* que descreve o tipo de mídia que está sendo transmitida, indicação do Frame que marca o início do frame, identificação da origem e sincronização.

O RTPC controla também parâmetros de QoS, que incluem a quantidade de pacotes perdidos e assim as pontas podem ajustar as taxas de transmissão de acordo com o controle da sessão, usando pacotes RTCP BYE para que os participantes deixem a sessão.

RTP comprimido, também chamado de CRTP, foi criado para reduzir o tamanho do cabeçalho IP, UDP e RTP, o protocolo comprime essas informações de modo que o pacote possa ser transmitido com um atraso menor.

4.9 DHCP (*DYNAMIC HOST CONFIGURATION PROTOCOL*)

De acordo com Chiozzoto (1999), o DHCP é um protocolo de serviço TCP/IP que oferece configuração dinâmica de terminais, com concessão de endereços IP de host e outros parâmetros de configuração para clientes de rede.

O DHCP usa um modelo cliente-servidor, no qual o servidor DHCP mantém o gerenciamento centralizado dos endereços IP usados na rede.

4.10 NTP (*NETWORK TIME PROTOCOL*)

O NTP é um protocolo para sincronização dos relógios dos computadores, ele define um jeito para um grupo de computadores conversarem entre si e acertar seus relógios, baseados em alguma fonte confiável de tempo (CHIOZZOTO, 1999).

4.11 CSTA (*COMPUTER SUPPORTED TELECOMUNICATIONS APLICATIONS*)

Conforme *Unify* (2013), CSTA é um conjunto de recursos completo e um modelo de chamada abrangente.

O CSTA suporta, com modelo de chamada mesmo, Voz e interações não voz (e-mail, bate papo, mensagens instantâneas e muito mais) e complementa SIP protocolo, permitindo que os desenvolvedores de aplicativos para fornecer recursos avançados.

CSTA é uma camada de abstração para aplicação de telecomunicações, independente dos protocolos de sinalização, SIP, ISDN e etc.

Independente de dispositivos é utilizado para apoio pessoal telefone, controle de telefone, *soft-phone*, conferência e colaboração, presença, disponibilidade contexto de dispositivo.

O *Session Initiation Protoco*l (SIP) é um protocolo de controle (sinalização) para criar, modificar e terminar sessões com um ou mais participantes. Estas sessões incluem chamadas telefônicas de Internet, distribuição de multimídia e conferências multimídia. CSTA padroniza um conjunto muito poderoso e flexível de serviços de aplicação para observar e controlar a mídia não-voz de voz e chamadas, bem como o controle e observar não-recursos de chamadas.

O Relatório Técnico Ecma descreve como CSTA pode ser usado para fornecer um subconjunto de funcionalidades de controlo de chamadas CSTA, chamado primeiro controle de chamadas partido, para os agentes de usuário SIP. O CSTA prazo (para o agente de usuário CSTA) refere-se ao transporte de ECMA-323 mensagens (CSTA XML) em uma sessão SIP.

CSTA aproveita SIP mecanismos para fornecer um conjunto altamente robusto e extensível de recursos para suportar aplicações no ambiente corporativo.

4.12 SOAP (*SIMPLE OBJECT ACCESS PROTOCOL*)

É um protocolo de especificação para troca de informações estruturadas na implementação de serviços da Web em redes de computadores. Ele se baseia em *XML Information Set* para seu formato de mensagem, e, geralmente, depende de outras *Application Layer* protocolos, principalmente *Hypertext Transfer Protocol* (HTTP) ou *Simple Mail Transfer Protocol* (SMTP), para negociação e transmissão de mensagens.

SOAP pode formar a camada base de uma pilha de protocolos de serviços web , oferecendo uma estrutura de mensagens básica sobre a qual os serviços web podem ser construídos. Este protocolo baseado em XML consiste em três partes: um envelope, que define o que está na mensagem e como processá-la, um conjunto de regras de codificação para expressar instâncias de tipos de dados definidos pelo aplicativo, e uma convenção para representar chamadas de procedimentos e respostas. Tem três características principais: extensibilidade (segurança e WS-roteamento estão entre as extensões em desenvolvimento), neutralidade (SOAP pode ser usado sobre qualquer protocolo de transporte, tais como HTTP , SMTP , TCP , ou JMS) e independência (permite qualquer modelo de programação).

Como um exemplo de como os procedimentos de SOAP pode ser usado, uma mensagem SOAP pode ser enviado para um site que tem serviços web habilitado, como um banco de dados de preços de imóveis, com os parâmetros necessários para uma pesquisa. O site, então, retornar um documento formatado em XML com os dados resultantes, por exemplo, preços, localização, características. Com os dados que estão sendo retornados em um formato de máquina parsable padronizado, ele pode ser integrado diretamente em um site ou aplicativo de terceiros.

4.13 XMPP (*EXTENSIBLE MESSAGING AND PRESENCE PROTOCOL*)

Extensible Messaging and Presence Protocol (XMPP) é um protocolo de comunicação para a mensagem-oriented *middleware* baseado em XML (*Extensible Markup Language*).

O protocolo foi originalmente chamado *Jabber,* e foi desenvolvido pela comunidade de código aberto *Jabber* em 1999, para quase em tempo real, de mensagens instantâneas (IM), informações de presença e lista de contatos de manutenção. Projetado para ser extensível, o protocolo também tem sido usado para publicar-se inscrever sistemas de sinalização para VoIP, vídeo, transferência de arquivos, jogos e serviços de redes sociais .

Diferentemente da maioria dos protocolos de mensagens instantâneas, XMPP é definido em um padrão aberto e usa um sistema aberto abordagem de desenvolvimento e aplicação, pelo qual qualquer pessoa pode implementar um serviço de XMPP e inter operar com implementações de outras organizações.

Sendo o XMPP um protocolo aberto, as implementações podem ser desenvolvidos usando qualquer licença de software, embora muitos de servidor, cliente e biblioteca implementações são distribuídos como software livre e de código aberto, muitos de freeware e software comercial implementações também existem.

4.14 MGCP/*MEGACO (MEDIA GATEWAY CONTROLLER PROTOCOL)*

Os protocolos MGCP e *Megaco* atuam como uma interface entre um controlador de *gateway* de mídia e um *gateway* de mídia. Baseiam-se numa arquitetura centralizada, na qual os dispositivos da banda da rede (os telefones) possuem uma capacidade limitada, tornando-os mais baratos e simples de serem construídos (TRONCO, 2006).

4.14.1 MGCP (*Media gateway controller protocol*)

O protocolo de Controle de *Media Gateway* (MGCP) é definido pela recomendação RFC 2705 do IETF, e usado para controlar as conexões (chamadas) nos *gateways* presentes nos sistemas VOIP. O MGCP implementa uma interface de controle através de um conjunto de transações do tipo comando (resposta que cria, controla e audita as chamadas nos GW's). Estas mensagens usam como suporte os pacotes UDP da rede IP, e são trocadas entre os GC's e GW's para o estabelecimento, acompanhamento e finalização de chamadas.

O sistema é composto por um *Call Agent*, pelo menos um media *gateway* (MG), responsável pela conversão dos sinais entre circuitos e pacotes, e pelo menos um *signaling gateway* (SG), quando conectado a um PSTN. Trabalha basicamente como mestre/escravo, onde os *gateways* devem executar os comandos pelo agente de chamadas.

O quadro abaixo mostra mensagens do MGCP e o seu significado.

Mensagem	Significado
MG –Media Gateway:	Processa a conversão dos dados do formato da rede de circuito para o formato da rede de pacotes.
MGC –Media Gateway:	Gerenciar as conexões nas redes de pacotes, através dos agentes de chamada.
SG –Signalling Gateways:	Interface para a rede de sinalização SS7 da rede de telefonia comutada (RTPC).
MCU–Multipoint Conference Unit:	Gerencia as chamadas *multicast* (conferência).

Quadro 5 – Mensagens do MGCP.
Fonte: Autor.

4.14.1.1 RFC 2705

Este documento (RFC2705) está sendo publicado para a informação da comunidade. Ele descreve um protocolo que está sendo implantado num certo número de produtos. Implementadores devem estar cientes de desenvolvimentos na *Megaco* Grupo de Trabalho IETF e ITF-T SG16 que são atualmente trabalhando em um sucessor potencial para esse protocolo.

Abstrato: Descreve uma interface de programação de aplicativo e um protocolo correspondente (MGCP) para o controle de voz sobre IP (VoIP).

Gateways de elementos de controle de chamada externa. MGCP assume uma chamada arquitetura de controle onde o controle de "inteligência" chamada está fora os *gateways* e manipulados por elementos de controle de chamada externa.

O documento está estruturado em seis seções principais:

1. A introdução apresenta os pressupostos básicos e a relação para outros protocolos como o H.323, RTSP, SAP ou SIP;
2. A seção interface apresenta uma visão conceitual do MGCP, apresentando as convenções de nomenclatura, o uso da sessão descrição do protocolo SDP, e os procedimentos que compõem MGCP: notificações requisita, notificação, criar conexão, modificar conexão, excluir conexão, *auditendpoint, auditconnection* e *restartInprogress*;
3. A seção de descrição do protocolo apresenta as codificações MGCP, que são baseados em formatos de texto simples, e a transmissão procedimento sobre UDP;
4. A seção de segurança apresenta a exigência de MGCP segurança, e seu uso dos serviços de segurança IP (IPSec);
5. A seção de pacotes evento fornece uma definição inicial de embalagens e nomes de eventos;
6. A descrição das alterações feitas na combinação SGCP 1.1 e IPDC para criar o MGCP 1.0.

4.14.2 *Megaco*

O protocolo *Megaco* é resultado de um esforço conjunto do IETF e do ITU-T. Este protocolo foi concebido para ser utilizado para controlar GW’s monolíticos (um único equipamento) ou distribuídos (vários equipamentos). Sua plataforma aplica-se a *gateway* (GW), controlador multiponto (MCU) e unidade interativa de resposta audível (IVR). Possui também interface de sinalização para diversos sistemas de telefonia, tanto fixa como móvel (TRONCO, 2006).

A estrutura de comandos do MEGACO é simples e flexíveis são somente 8 comandos.

Os comandos são agrupados em transações, usando as regras flexíveis de construção e reduzindo de modo significativo o *overhead* de mensagens.

4.15 VLAN (Virtual LAN)

De acordo com Tronco (2006), vlan é um mecanismo para criar domínios de broadcast e definir as estações que pertecem a cada domínio, independente da localização física, é virtual. Defenida como uma coleção de estações que se comunicam no mesmo domínio de broadcast.

VLANs são utilizadas para controlar o tráfego e prover segurança, uma vez que somente as estações Autorizadas podem se comunicar dentro de cada domínio. Por serem virtuais, facilitam as mudanças, alterações de localidade de usuários.

5 DESENVOLVIMENTO

Para cada uma das etapas previstas na metodologia o desenvolvimento do trabalho foi efetuado conforme descrito a seguir.

5.1 SELEÇÕES E O ESTUDO DA BIBLIOGRAFIA

O estudo da bibliografia pertinente ao assunto foi feito buscando as referências em sites de literatura especializada, de organizações internacionais, na biblioteca da instituição e nas anotações e materiais de aula.

Os resultados do estudo e pesquisa estão descritos no item 4 e seus subitens acima.

5.2 APRESENTAÇÕES DA VISÃO GERAL DA SOLUÇÃO

O *OpenScape Voice* é uma pedra fundamental da estratégia *Open Communications* da Siemens e é parte central do *OpenScape Unified* Communications Server. Oferece uma ampla variedade de vantagens tecnológicas e comerciais e possuem alguns diferenciais fundamentais de outras soluções de comunicação empresarial que tornam a implantação de comunicações unificadas mais flexível, confiável e econômica.

A solução proposta é baseada na solução *OpenScape Unified Communication* distribuída através de duas localidades.

A solução a ser implantada será composta pelos componentes:

- *OpenScape Voice & OS UC Application Simplex;*
- *OpenScape Branch 50;*
- *OpenScape Branch 50i DP14e;*
- *OpenScape Xpressions;*
- *Openscape WebCollaboration;*
- *Gateway SIP Celular;*
- Aparelho SIP;
- *Softphone.*

5.3 ELEMENTOS DA SOLUÇÃO

Em termos de definição, os elementos da solução podem ser dispositivos de hardware ou aplicações de software do catalogo de produtos Siemens ou qualquer dispositivo de terceiro que esteja contemplado no projeto.

A solução *OpenScape* consiste de um número de elementos core e componentes remotos.

A lista dos componentes está sumarizada na tabela abaixo:

Aplicação	Modelo de distribuição
OSV & UC	Servidor
OpenScape Branch 50i DP14e	*End Point*
OpenScape Xpressions	Servidor

Quadro 6 - Elementos da solução.
Fonte: Autor.

5.4 REQUISITOS OBRIGATÓRIOS PARA INSTALAÇÃO E INTEGRAÇÃO

As informações nessa sessão explicam e detalham as tarefas necessárias acordadas a serem concluídas para que a solução seja sucedida no ambiente.

5.4.1 Checklist do ambiente

O quadro a seguir especifica os itens que precisam ser confirmados ou precisam existir na área/sala ou espaço em que a solução será instalada.

Lista de Preparação do Ambiente
Provisão de Racks
Aterramento do rack está disponível
Energia do rack está disponível
Existem tomadas de alimentação suficiente nos racks para todos os servidores
Um No Break está disponível nas localidades
O cabeamento do rack disponível (ligações de Patch)
Ligações de Patch para telefones disponíveis
Cabos *link* E1 disponíveis
Patch Panel / DG para equipamentos novos
Bandejas de rack para equipamentos novos
Unidades de KVM com portas suficientes disponíveis para todos os servidores
Cabos de KVM disponíveis
Atender aos requisitos de rede
Atender aos requisitos de virtualização

Quadro 7 - Checklist do Ambiente.
Fonte: Autor.

5.4.2 *Checklist* de preparação da rede

A tabela abaixo resume a configuração do ambiente de rede que precisa ser estabelecida antes de realizar qualquer atividade de integração e implantação.

Lista de preparação da rede
Acesso remoto no local
Fornecer portas de switch que são configuradas
Portas de *uplink* no equipamento da rede do cliente foram configuradas
Sub-redes designadas da solução, Vlans e RTP Vlans são capazes de rotear o tráfego entre si
Configurações de DHCP
Configurações de DNS
As sub-redes para os PCs do cliente ou laptops roteiam para as sub-redes da solução

Quadro 8 - *Checklist* de Integração de Rede.
Fonte: Autor.

5.4.3 Cabeamento de rede

Os aspectos que envolvem o cabeamento das redes estáo consideradas conforme os itens a seguir.

5.4.3.1 UTP (*Unshielded Twisted Pair*)

Cabeamento geralmente utilizado para conexão entre dispositivos na LAN (Local Área Network), pois tem bom rendimento em redes corporativas onde a distância entre equipamentos não ultrapasse 100 metros. A seguir estão listadas as categorias mais utilizadas nas redes corporativas.

Categoria Cat 5e – É uma melhoria das características dos materiais utilizados na categoria 5, que permite um melhor desempenho, podendo ser fabricado com freqüências de 100Mhz a 155Mhz.

Categoria Cat 6 – Características para desempenho especificado até 250Mhz e velocidades de 1Gbps até 10Gbps, com limitação de 55 metros.

Categoria Cat 6a – Melhoria da categoria 6 para que o freqüência de 250Mhz seja mantida até 100 metros.

5.4.3.2 Fibra óptica

As fibras ópticas podem ser usadas na LAN e na WAN, ao utilizar uma fibra óptica deve se considerar a distância entre os dispositivos a serem conectados e a função dessa conexão.

Mono Modo – Possui um núcleo que restringe o trafego das informações para um único sentido, é aconselhável para grandes distâncias (dezenas de km).

Multimodo – Possui múltiplos núcleos que permitem que o haja trafego de informações em ambos os sentidos, é aconselhável para distancias curtas (até 2 km).

5.5 DISPONIBILIDADES VOIP

Para que a tecnologia VoIP seja implantada é necessário que a rede corporativa atenda os requisitos mínimos de *Jitter*, *delay* e perda de pacote com os seguintes parâmetros.

5.5.1 J*itter*

Também conhecido como variação do *Delay* (atraso), indica as diferenças do tempo de chegada de datagramas de voz durante uma chamada de voz sobre IP. O Buffer de *Jitter* pode ser configurado através dos *gateways* e telefones IP, tendo um valor ideal inferior a 30ms. Se o *Jitter* for muito alto, superior a 40 ms, isso acarretará em um aumento excessivo do *delay* ou perda de pacotes.

5.5.2 *Delay*

Caracteriza-se pelo tempo que um pacote leva para percorrer toda a rede entre dois pontos de conversação. O *delay* (atraso) recomendável para uma comunicação de boa qualidade é inferior a 150ms (milissegundos), tolerável até 250ms. Este é o tempo máximo que o pacote IP deve demorar a alcançar seu destino (incluindo tempo de empacotamento dos *codecs*, *jitter* e propagação na rede).

5.6 PERDAS DE PACOTE

A perda de pacotes não deve ultrapassar 1%, sendo tolerável um valor até 3%. Com perdas acima deste valor, podem ocorrer problemas na qualidade de voz, como por exemplo, o Eco.

5.7 *NOBREAK*

Deve possuir rede elétrica estabilizada e mantida por sistemas de NoBreak na localidade de principal.

Para outra localidade é necessário 1 *NoBreak* e banco de baterias.

5.8 TOPOLOGIA E ARQUITETURA

Na sequência está descrita a topologia e a arquitetura da solução proposta.

5.8.1 Visão geral da arquitetura da solução

Em uma visão geral, a solução proposta apresenta os componentes das Aplicações Unificadas (UC) que agrupa o *OpenScape* Voice, o *OpenScape Expressions*, o *OpenFire*, o *OpenScape Web Colaboration* e o *OpenScape Vídeo*, que todos estes aplicativos disponíveis ao usuário final

Com este grupo se comunica com o Media Server , Interface Celular e *OpenScape Branch* que é interligado com a rede MPLS e a rede pública.

Com a rede MPLS se faz o tráfego interno de ramais, que é controlado pelo *OpenScapeVoice*, que gerenciar as ligações. A rede MPLS se comunica com vários protocolos.

Rede MPLS se interliga com vários sites.

O *Openscape Branch* e a interface celular se faz a interligação com a rede PSTN (Pública) é a interface que se comunicar a rede PSTN com a rede interna.

OpenScape Voice funciona como servidor SIP

Terminal de usuário onde todos os aplicativos estão disponíveis.

5.8.2 Diagrama geral

A figura a seguir mostra o Diagrama Geral da solução proposta explicada acima.

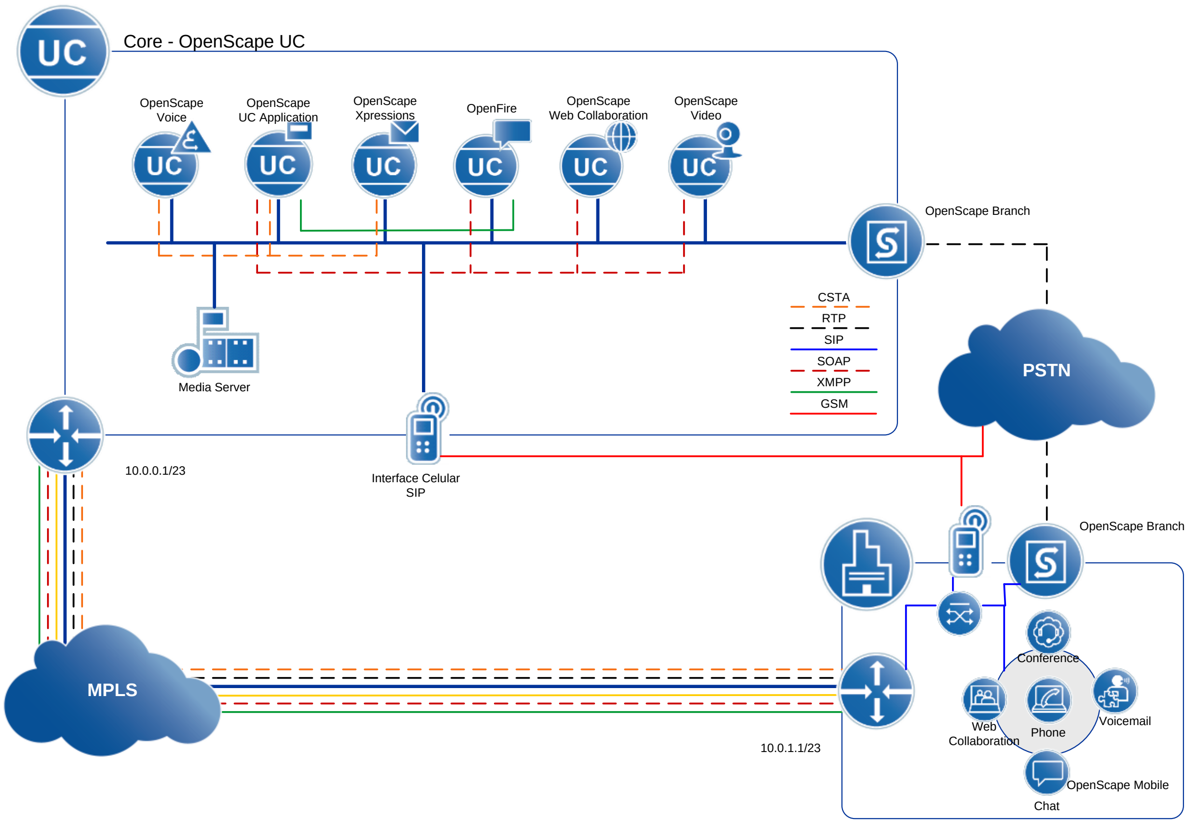


Figura 04 – Topologia da Solução Proposta.
Fonte: Autor.

5.8.3 Versões planejadas

A seguir serão apresentados cada componente da solução.

5.8.3.1 Aplicativos

Os aplicativos que compõe a solução e que estão agrupados são:

- *OpenScape Voice;*
- *OpenScape UC Application;*
- *OpenScape WEB Collaboration.*

5.8.3.2 Pontos de extremidade suportados

Os dispositivos utilizados pelos usuários finais são:

- Aparelhos SIP;
- *Softphone.*

5.8.3.3 Provedor de anúncios de conferencia

Quem faz os anúncios de voz, ramal ocupado ou disponível é o *Media Server.*

5.8.3.4 *Gateway* PSTN

O *Gateway* é formado pelos componentes:

- *OpenScape Branch;*
- *Interface Celular SIP.*

5.8.3.5 Sistema de *voice mail*

O Servidor de Correio de Voz é gerenciado pelo *OpenScape Xpressions*.

5.8.3.6 SIP *proxy*

Quem controla as passagens *é o OpenScape Branch.*

5.9 OPENSCAPE UC

OpenScape UC Application é altamente aberto solução de comunicações unificadas para empresas que precisa de uma solução extremamente flexível que pode integrar diversas TI e ambientes de telefonia, e existente *Microsoft, IBM*, Google ou aplicações. Além disso, para as empresas que buscam a eficiência do processo de transformação de processos de negócios de comunicações embutidas, este é o aplicativo que se integra com outros negócios aplicações e ferramentas de mídia social.

5.10 OPENSCAPE WEB COLABORATION

OpenScape Web Collaboration ajuda empresas a reduzir custos em viagens de negócios e serviços de conferência web, permitindo aos parceiros e clientes a compartilhar mais idéias e informações a qualquer momento, e em uma fração do custo. Ele fornece uma forma rentável e eficiente para reuniões com até mil participantes por sessão para treinamentos, reuniões de projetos, reuniões de vendas, demonstrações de produtos, e suprote remoto básico suporte aos clientes e usuários finais.

O.*OpenScape Web Collaboration* fornece simples e rápido acesso aos recursos, incluindo ambiente de trabalho e compartilhamento de aplicativos, compartilhamento de arquivos, bate papo. Permite aos participantes fazer a transição fácil de uma mídia (chat, web e vídeo) para outra com um único clique.

A solução é mantida em segurança por meio de criptografia que usa 256 bits de uma ponta para outra. Os usuários móveis com o iPhone , iPad , Android ou qualquer aparelho Smartphone podem facilmente participar de uma sessão de conferência web de qualquer lugar utilizando o *Web OpenScape Colaboration Mobile Client*.

Os principais recursos do *OpenScape Web Collaboration* são intuitivos e tem uma interface flexível com o usuário e permite *switching* entre várias telas. O usuário decide se quer ver uma ou todas elas.

5.11 RESILIÊNCIA DA SOLUÇÃO

Os itens a seguir descrevem os componentes de redundância da plataforma de comunicação de voz e sistema de comunicações integradas.

5.11.1 Redundância provida pelo *Openscape Voice*

A solução que compõe a plataforma de *Softswitch* é composta por 01 (um) *OpenScape Voice* que será instalado no site principal. Por se tratar de uma arquitetura simplex a redundância está no servidor, uma vez que tem redundância nas fontes, processadores, *côolers, e HDs* em *Raid*-1.

Para uma redundância consistente, cada uma das fontes do servidor *OpenScapeVoice* deve ser ligada em circuito elétrico distinto, que deve estar ligado a um *Nobreak* com estabilizador exclusivo.

5.11.2 Redundância provida pelo *Openscape Branch*

O *OpenScape Branch* é utilizado no projeto para prover a solução de *Proxy Server* e oferecer um método de sobrevivência aos telefones das localidades. Isto significa que os telefones da localidade se comunicam somente com o *Proxy Server* e este se comunica com o *OpenScape Voice.*

Nos casos onde houver interrupção nos serviços providos pelo *OpenScape Voice*, o *Proxy Server* irá assumir o controle da sinalização SIP e entrará em "Sobrevivência". Neste momento, uma mensagem SIP será enviada aos telefones registrados passando-os para "Modo Limitado Temporário".

O recurso DNS SRV é um pré-requisito para este modelo de solução, pois, todos os telefones da localidade irão se comunicar com o *OpenScape Branch* e se este ficar indisponível, os telefones deverão se comunicar diretamente com o *OpenScape Voice*.

Os detalhes específicos da configuração do DNS-SRV podem ser encontrados no tópico referente ao DNS.

5.12 PROTOCOLOS, *CODECS* E INTERFACES

Os protocolos envolvidos, *codecs* e interfaces estão mostrados no quadro a seguir.

Dispositivos	Protocolos utilizados	Protocolos suportados	Trafego
IP Phones	**SIP**	**H323 e SIP**	**Interno**
OpenScape Branch	**SIP, MFCR2**	**SIP MFCR2, ISDN, MGCP**	**SIP (Interno), MFCR2 (Externo)**
Xpressions	**SIP**	**SIP, LDAP, SMTP, POP, IMAP**	**Interno**
UC Application	**SIP, CSTA, LDAP, SMTP**	**SIP, CSTA, LDAP, SMTP**	**Interno**
WebCollaboration	**http, https**	**HTTP, https**	**Interno**
Media Server	**MGCP**	**MGCP**	**Interno**

Quadro 9 – Protocolos que são utilizados na proposta da solução.
Fonte: Autor.

O quadro abaixo mostra os *Codecs* utilizados na solução proposta.

Dispositivos	*Codecs* utilizados	*Codecs* Suportados	Aplicação
IP Phones	**G.729**	**G.711,G.722 E G.729**	**VOZ**
Gateways	**G.729, T.38**	**G.711, T.38 E G.729**	**VOZ**

Quadro 10 – *Codecs.*
Fonte: Autor.

5.12.1 Interfaces

As interfaces utilizadas estão explicadas a seguir.

CSTA - O sistema dispõe de uma Interface CSTA, dedicada para aplicações (ver explicação na revisão bibliográfica).

SOAP - O Gerenciamento do sistema é realizado sob a aplicação CMP (*Common Manager Portal*). O acesso a esta ferramenta é realizado via SOAP, o que possibilita a manutenção do sistema via *Web Browser* (ver explicação na revisão bibliográfica).

5.13 GERENCIAMENTOS DA SOLUÇÃO *OPENSCAPE VOICE*

A seguir está mostrado como é feito o gerenciamento da solução pelo *OpenScape Voice*.

5.13.1 Gerenciamento do *Openscape Voice*

O gerenciamento e administração da plataforma *OpenScape Voice* é realizada das seguintes formas:

– *Common Management Portal* – CMP Aplicação em execução no servidor do *UC Application*, que proporciona um ambiente gerenciamento do sistema;

– *Secure Shell* – SSH - Aplicativo de gerenciamento utilizado para executar comandos em uma unidade remota em uma segura e criptografada.

5.13.2 Gerenciamento de terminais

O Gerenciamento dos ramais será realizado através da ferramenta CMP.

5.14 INFRAESTRUTURA DA REDE DE DADOS

A seguir está mostrada a infraestrutura para a solução.

5.14.1 Arquitetura

A rede de dados faz parte da solução e será utilizada para transporte do tráfego das aplicações de voz, conforme descrito no item 6.8.1.

5.14.2 *Links* entre as localidades

É necessário que duas ou mais localidades sejam interligadas através de *link* MPLS. Também é preciso definir a banda disponível no *link* WAN entre estas localidades. Será utilizado o DSCP EF para priorizar os tráfegos de *Payload* de voz e sinalização em relação aos demais tráfegos na rede. Os sites são interligados por fibra óptica.

Os *codecs* G.711 e G.729 serão utilizados conforme especificação a seguir.

O *codec* G.711 será utilizado para chamadas SIP na mesma localidade (LAN), ele não é comprimido e garante uma ótima qualidade nas chamadas SIP.

O *codec* G.729 será utilizado para chamadas SIP em localidades diferentes, é um *codec* comprimido para utilizar menos banda na WAN e garante uma boa qualidade de voz.

Para efeitos de cálculo de chamadas entre sites deve-se considerar que o *codec* G.729A utiliza aproximadamente 36 Kbps por chamada.

O quadro abaixo demonstra os dados fornecidos. Para implantação da solução será utilizado o *Code* G.729 entre as localidades. Deverá ajustar a reserva de banda para VoIP, conforme a sua necessidade.

Localidade	Serviço	Marcação	*Link* (Kbps)	Reserva da banda	Qtda de Chamadas na banda atual
Site 1	RTP	EF	XMb	XKb	xx
	SIP	EF			
Site 2	RTP	EF	XMb	XKb	xx
	SIP	EF			

Quadro 11 – Reserva da banda.
Fonte: Autor.

5.14.3 Endereçamento IP

O quadro abaixo ilustra as localidades e seus respectivos intervalos de endereço IP.

Localidade	VLAN'S	DESCRIÇÃO	TAG	Rede
Site 1	Vlan 9	Telefones e *gateways*	9	10.0.0.1/23
Site 1	Vlan 17	*OpenScape* Administração	17	10.0.10.0/26
Site 1	Vlan 18	*OpenScape* Sinalização	18	10.0.10.64/26
Site 1	Vlan 19	*OpenScape* Servidores	19	10.0.10.128/26
Site 2	Vlan 10	Telefones e *gateways*	10	10.0.1.1/24

Quadro 12 – Endereçamento IP.
Fonte: Autor.

Especificação das VLANs para o Site 1.

Segue abaixo a especificação das VLANs que deverão se configuradas para suportar a solução *OpenScape Voice*.

VLAN *Administration* (*openscape*_adm): A rede de administração é responsável pelo gerenciamento do sistema *OpenScape Voice*, podendo ser feito através de CLI via SSH ou SOAP via HTTP.

Esta VLAN deve ser configurada com o VLAN ID 17 e máscara de rede /26.

VLAN Sinalização (*openscape_sig*): A rede de sinalização é responsável por processar toda a sinalização SIP.

Esta VLAN deve ser configurada com o VLAN ID 18 e máscara de rede /26.

VLAN Servidores (*openscape_srv*): Será utilizada para hospedar todos os servidores adicionais que compõem a solução de UC Application e servidores responsáveis por serviços periféricos.

Esta VLAN já está em produção e responde pelo VLAN ID 19 e máscara de rede /26.

VLAN Telefones (telefones): A rede telefones é responsável por hospedar todos os endpoints. Esta VLAN deve ser criada com VLAN ID 9 e máscara de rede /23.

Especificação das VLANs para o Site 2

VLAN Telefones (telefones): A rede telefones é responsável por hospedar todos os *gateways* e endpoints. Esta VLAN deve ser criada com VLAN ID 10 e máscara de rede /24, sendo que a faixa reservada para utilização dos *gateways* é de 10.0.1.10 até 10.0.1.254.

O quadro a seguir resume as configurações necessárias.

Rede	Máscara	*Gateway*	VLAN ID	Nome VLAN	Descrição
10.0.1.0	/24	10.0.1.1	10	Telefones	Telefones e *gateways*

Quadro 13 – Endereçamento IP Site 2.
Fonte: Autor.

5.14.4 Endereços IP fixos dos servidores, *gateways* e *endpoints*

O quadro abaixo apresenta os IP fixo dos servidores dos Sites 1 e 2:

Aplicação	Nome VLAN	VLAN ID	IP	Máscara	*Gateway*
OpenScape Voice	*openscape_adm*	17	10.0.10.5	/26	.1
OpenScape Voice	*openscape_sig*	18	10.0.10.70	/26	.65
OpenScape Voice	*openscape_srv*	19	10.0.10.130	/26	.129
OpenScape WEB Collaboration	*openscape srv*	19	10.0.10.131	/24	.129
OpenScape Xpressions	*openscape srv*	19	10.0.10.132	/26	.129
OpenScape Branch Site 1	*endpoint sip1*	9	10.0.0.4	/23	.1
OpenScape Branch Site 2	*endpoint sip 2*	10	10.0.1.4	/24	1
Endpoint SIP Celular Site 1	*endpoint sip1*	9	10.0.0.5	/23	.1
Endpoint SIP Celular Site 2	*endpoint sip 2*	10	10.0.1.5	/24	.1
Telefones SIP Site 1	*endpoint sip1*	9	10.0.0.10-XXX	/23	.1
Telefones SIP Site 2	*endpoint sip 2*	10	10.0.1.10-254	/24	.1

Quadro 14 – Endereçamento IP dos Servidores.
Fonte: Autor.

5.15 DNS

O quadro 15 informa os servidores de DNS que deverão ser utilizados no projeto.

Localidade	Servidor	IP
Site 1	DNS primário	*10.0.0.1*
	DNS secundário	-
Site 2	DNS primário	*10.0.1.2*
	DNS secundário	-

Quadro 15 – Servidores DNS.
Fonte: Autor.

Faz-se necessário que haja a replicação da base de dados entre os servidores de DNS e a replicação pode ser manual ou automática.

5.15.1 Configuração do DNS e entradas de DNS para o domínio padrão

Para todas as localidades, faz-se necessário realizar a configuração do serviço DNS-SRV para viabilizar a sobrevivência dos ramais, caso ocorra a interrupção dos serviços do *OpenScape Branch*.

O serviço DNS-SRV é uma tecnologia especificada pela RFC 2782 que permite a um host de rede (Ex.: *Endpoint*) pesquisar por um nome de rede, por exemplo: yyy.xxxxx.com.br e receber como resposta, dois ou mais endereços IP.

A aplicação do DNS-SRV ocorrerá na comunicação entre os *endpoints* e o *OpenScape Branch* e ou *OpenScape Voice*. Sempre que o *endpoint* realizar uma consulta ao servidor de DNS, receberá como reposta duas opções, sendo a primeira o endereço IP do *OpenScape Branch* e a segunda o endereço IP do *OpenScape Voice.*

Em condições normais de funcionamento os *endpoints* irão sempre se comunicar com a primeira opção e no caso de interrupção nos serviços do *OpenScape Branch*, os *endpoints* seguirão automaticamente para a segunda opção sem que haja a interrupções dos serviços, que não dependam exclusivamente do *OpenScape Branch.*

5.16 CONFIGURAÇÕES DO SUBDOMÍNIO SRV

No domínio existente "sites.ad", será criado um subdmínio chamado "voip".

No domínio "sites.ad" será criado um subdomínio para cada localidade que irá ter *OpenScape Branch*.

5.16.1 Configuração das entradas SRV no subdomínio

O quadro a seguir informa as entradas SRV que deverão ser configuradas no domínio "voip.sites.ad".

Subdomínio	Sinalização	Prioridade	Port	Serviço	Transporte	Hostname
Site 1	UDP	10	5060	_sip	_udp	mtntelosb01.site1.ad
		20	5060	_sip	_udp	mtntelosv02.site2.ad
	TCP	10	5060	_sip	_tcp	mtntelosb01.site1.ad
		20	5060	_sip	_tcp	mtntelosv02.site2.ad
	TLS	10	5061	_sips	_tcp	mtntelosb01.site1.ad
		20	5061	_sips	_tcp	mtntelosv02.site2.ad
Site 2	UDP	10	5060	_sip	_udp	imatelosb01.site1.ad
		20	5060	_sip	_udp	mtntelosv02.site2.ad
	TCP	10	5060	_sip	_tcp	imatelosb01.site1.ad

Subdomínio	Sinalização	Prioridade	Port	Serviço	Transporte	Hostname
		20	5060	_sip	_tcp	mtntelosv02.site2.ad
	TLS	10	5061	_sips	_tcp	imatelosb01.site1.ad
		20	5061	_sips	_tcp	mtntelosv02.site2.ad

Quadro 16 – SRV.
Fonte: Autor.

5.17 CONFIGURAÇÕES PARA OS TELEFONES IP

As figuras a seguir indicam o modelo de configuração para os *endpoints* a ser seguido a fim de viabilizar a o modelo de sobrevivência.

Para simplificar as informações, serão especificados apenas os parâmetros diferentes do padrão.

O endereço "*Sip server address*" deverá ser configurado com o IP "10.0.10.5".

O endereço "*Sip registrar address*" deverá ser configurado com o IP "10.0.10.5".

O endereço "*Sip gateway address*" deverá ser configurado com o FQDN "<sigla_da_localidade>voip.sites.ad".

A figura a seguir demonstrar como configurar o registro do aparelho SIP:

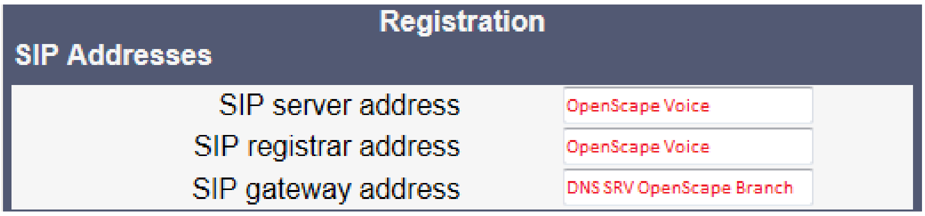


Figura 05 - Terminal SIP – *SIP Gateway*.
Fonte: Autor.

O parâmetro *"Outbound proxy*" deverá ser marcado.

O parâmetro "*SIP transport*" deverá ser configurado como "UDP", como demonstrar a figura abaixo:

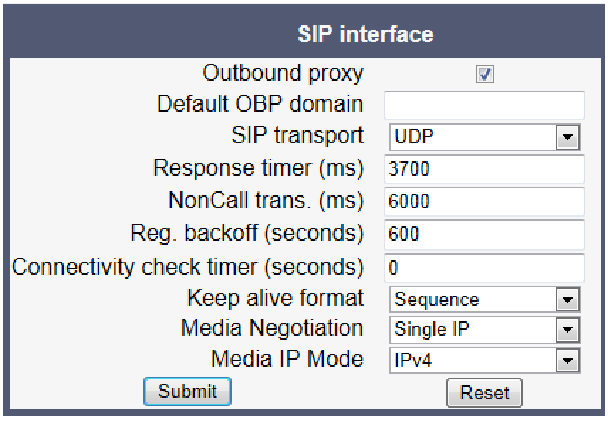


Figura 06 - Terminal SIP – SIP Interface.
Fonte: Autor.

O parâmetro “SIP *gateway*” deverá ser configurado como “0”(zero), conforme a figura abaixo:

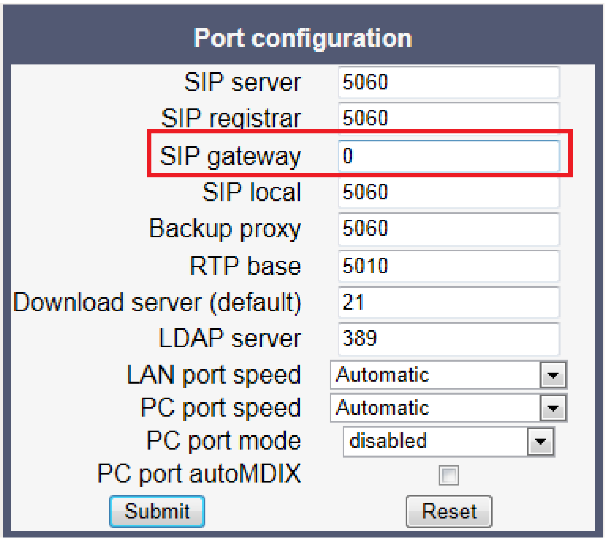


Figura 07 - Terminal SIP – *Port Configuration.*
Fonte: Autor.

5.18 NTP

A rede utiliza os seguintes servidores para sincronização de horário, de acordo com a localidade, garantir o perfeito sincronismo entre os mesmos.

Todos os servidores, *gateways* e *endpoints* deverão se configurados com os servidores, respeitando a respectiva localidade. O endereço IP dos servidores de NTP deve ser fornecido através do escopo de DHCP.

Caso o servidor de NTP seja baseado na plataforma Microsoft Windows, o mesmo deverá ser configurado para sincronizar com uma fonte de *clock* segura (GPS) ou fonte externa via internet. O não atendimento a esses pré-requisitos irá ocasionar no mau funcionamento dos telefones IP.

5.19 *VOIP CODECS*

A escolha do *CODEC* de voz a ser utilizado no projeto VoIP é muito importante para o correto dimensionamento da banda a ser ocupada na rede. Na rede LAN geralmente a banda não é um fator decisivo para o projeto, porém o mesmo não ocorre quando falamos de WAN.

Todos os *Codecs* possuem um valor de ocupação de banda, porém, quanto menor a banda ocupada por um *CODEC* menor será a qualidade de voz.

Abaixo seguem os *Codecs* mais utilizados em projetos de Voz.

CODEC	**Frames por Segundo**	**Bytes por Payload**	**Bytes Total**	**BANDA (bps)**
G.729	50	20	90	36000
G.711	33.33	240	310	82667

Quadro 17 - Lista de *Codecs*.
Fonte: Autor.

A rede de voz do configurada para funcionar com o *CODEC* G.711 na LAN e o *CODEC* G.729 na WAN. Todos os roteadores da rede corporativa que farão parte da rede VoIP deverão estar com as políticas de QoS aplicadas tanto na interface LAN quanto na WAN.

5.20 GERENCIAMENTO VIA SNMP

A seguir será apresentada a relação dos componentes da solução que suportam SNMP.

Aplicativos: *OpenScape Voice*, *OpenScape Application e OpenScape WEB Collaboration.*

Pontos de Extremidade suportados: Aparelhos SIP e *Softphone*.

Sistema de *Voice Mail: Openscape Xpressions.*

Sip Proxy: OpenScape Branch.

5.21 ESPECIFICAÇÕES OPENSCAPE VOICE

A seguir está apresentada as especificações do OpenScape Voice.

5.21.1 Faixa ddr / ramais

Site1 tem faixas de ramais que coincide com a faixa DDR.

Site2 tem faixas de ramais que coincide com a faixa DDR.

O quadro abaixo demonstra a faixa de ramais dos sites das localidades:

Localidade	Tipo	N Chave / N linhas	Faixa DDR	Faixa Ramais
Site1	E1 – MFCR2 – SIP Trunk	55 (xx) xxxx-1400	1400 a 1599	1400 a 1599
Site2	E1 – MFCR2 – SIP Trunk	55 (xx) xxxx-3300	3300 a 3399	3300 a 3399

Quadro 18 - Faixa DDR das localidades.
Fonte: Autor.

5.21.2 Global – *home directory numbers*

O *Home Directory Numbers* é uma tabela onde inserirmos o número de todos os ramais SIP que irão se registrar no *OpenScape Voice*. Posteriormente esses números serão utilizados na seção de numeração para criar os *Subscribers* (Ramais SIP).

5.21.3 Plano de numeração

O plano de numeração é o módulo responsável por toda a estrutura de roteamento de voz do *OpenScape Voice*. Nele determinamos as regras de roteamento para chamadas internas e externas, bem como regras customizadas.

5.22 *MEDIA SERVER*

A aplicação Media Server é a responsável por toda a parte de anúncios e suporte a salas de conferência da solução *OpenScape Voice* e suporte aos portais de voz e conferência da solução UC Application. Os recursos de *Media Server* necessários ao UC Application serão suportados pelo *Media Server* central, contudo, a configuração do sistema será realizada de modo a permitir a instalação de novos *Media Servers*.

O quadro abaixo demonstra a aplicação e função do media *Server*:

Aplicação	Função	*Routing Areas*	*Media Server*
UC Application	Portal de voz	Todos	Central
UC Application	Portal de conferência	Todos	Central
OpenScape Voice	MLHG utilizados pelo OSCC	Todos	Central
OpenScape Voice	Anúncios / *Large Conference*	Site1	Central
OpenScape Voice	Anúncios / *Large Conference*	Site2	Central

Quadro 19 - Media Server.
Fonte: Autor.

5.23 LISTAS DE PORTAS

A seguir serão apresentados as portas, protocolos e sentido das informações dos aplicativos utilizados na solução:

O quadro de portas TELEFONES IP / *SOFTPHONE* é o seguinte.

Gerência	UDP	TCP	Sentido	Coorporativa	UDP	TCP	Aplicação	Observação
5060	x	x	↔	5060	x	x	sip	*SIP Signaling*
5061		x	↔	5061		x	sip	*SIP Signaling*
-			→	20		x	ftp	FTP para atualização do telefone
-			→	21		x	ftp	FTP para atualização e controle dos telefones
-			→	443		x	https	*Endpoint Webaccess configuration* https://
162	x		←	-			snmp	SNMP Traps
-			→	161	x		snmp	SNMP get

Quadro 20 - Portas utilizadas por Telefones SIP/*Softphone.*
Fonte: Autor.

Segue o quadro de portas *Xpressions*:

Gerência	UDP	TCP	Sentido	Coorporativo	UDP	TCP	Aplicação	Observação
-			↔	5060	x	x	sip	SIP Signaling
-			→	25			SMTPAPL	SMTP server
-			→	80			WEBAPL	HTTP server

Quadro 21 - Portas utilizadas pelo *Xpressions.*
Fonte: Autor.

Na sequência está o quadro de portas *OpenScape Voice*:

OpenScape Voice								
Gerência	**UDP**	**TCP**	**Sentido**	**Coorporat ivo**	**UDP**	**TCP**	**Aplicação**	**Observaç ão**
5060	x	x	↔	5060	x	x	sip	SIP Signaling
5061		x	↔	5061		x	sip	SIP Signaling
162	x		←	-			snmp	SNMP Traps
-			→	161	x		snmp	SNMP get
-			→	4000-4199	x		Media Server	Media Server Tones and announces

Quadro 22 - Portas utilizadas pelo *OpenScape Voice.*
Fonte: Autor.

A seguir está mostrado o quadro de portas *Web Collaboration:*

Gerência	**UDP**	**TCP**	**Sentido**	**Coorporativo**	**UDP**	**TCP**	**Aplicação**	**Observação**
80		x	←	Any		x	http	HTTP
443		x	←	Any		x	https	HTTPS
1434	x		←	Any	x		Microsoft	*Proprietary Microsoft protocol for the communication from the nth Web Collaboration server computer to the first Web Collaboration server computer*
1500		x	←	Any		x	Microsoft	*Proprietary Microsoft protocol for the communication from the Nth Web Collaboration server computer to the first Web Collaboration server computer*
5000[3]		x	←	Any		x	Fast Viewer	*Proprietary FastViewer protocol*
5004		x	←	Any		x	XML-RPC	XML-RPC
Any	x		→	1434	x		Microsoft	*Proprietary Microsoft protocol for the communication from the Nth Web Collaboration server computer to the first Web Collaboration server computer*
Any		x	→	1500		x	Microsoft	*Proprietary Microsoft protocol for the communication from the Nth Web Collaboration server computer to the first Web Collaboration server computer*

Quadro 23 - Portas utilizadas pelo *Web Colaboration.*
Fonte: Autor.

5.24 *OPENSCAPE XPRESSIONS*

OpenScape Xpressions PhoneMail é um sistema de *voicemail* para o acesso às mensagens na sua caixa postal *OpenScape Xpressions* através do telefone, que pode ser utilizado como sistema independente ou incorporado a um ambiente de *Unified Messaging*, para permitir o acesso à caixa postal. Desta forma, o usuário é capaz de administrar todas as mensagens entregues em sua caixa postal *OpenScape Xpressions* quase que exclusivamente por telefone.

5.24.1 Topologia

O *OpenScape Xpressions* para atender os ramais do *OpenScape Voice*, como *voicemail.*

5.24.2 Números de acesso

Direct Access é utilizado para efetuar login no servidor com o seu número de telefone e um PIN.

Guest / Foward Access as chamadas para um ramal serão desviadas para a caixa postal. As pessoas que chamam podem depositar aí as suas mensagens. Assim, você pode usar a caixa postal como uma secretária eletrônica.

Callback Access, através dele tem um acesso rápido à caixa postal. Além disso, pode consultar à caixa postal com a tecla correspondente no telefone, caso existam novas mensagens.

O acesso com este número corresponde ao Direct Access, com a diferença que não é mais necessário digitar o próprio número, uma vez que é aplicado o número do equipamento usado. Isto também significa que este tipo de acesso só pode ser utilizado a partir de um terminal telefônico específico.

Transfer Access utilizado para transferir para as caixas postais chamadas dirigidas ao ramal. Pode conectar a pessoa que chama com uma caixa postal específica.

5.25 INTERFACE CELULAR

Interface Celular com funções *gateway* VoIP baseado em IP e rede sem fio GSM, que fornece uma configuração flexível de rede.

Interface Celular SEP suporta o padrão RJ45 com 10 ou 100 Mbps rede. Seção sem fio, inserir o cartão SIM diretamente no canal GSM.

6.25.1 SIP configuration

O quadro abaixo mostra os campos que configuram uma Interface Celular SIP:

SIP Configuration	Usado para configurar canal VoIP, SIP add Plataforma de Registro e SIP locais *Channel*, e configurar o protocolo SIP e outras informações relacionadas.
SIP Server Address	Usado para configurar o endereço do servidor SIP e *Channel*, o endereço IP pode ser endereço, também pode ser um nome de domínio (DNS deve ser capaz de resolução), os detalhes, o prestador de serviços de consultoria.
SIP Proxy Port	Configuração padrão da porta é 5060. Para mais detalhes, consulte o provedor de serviços.
Outbound Proxy Address	Proxy de saída, é usado principalmente em ambiente de *firewall* / NAT. Que fazem a sinalização e mídia fluxos são capazes de

	penetrar o firewall, os detalhes por favor, o prestador de serviços de consultoria.
Outbound Proxy Port	Número da porta proxy de saída, os detalhes, o prestador de serviços de consultoria.
Use Randon Port	Defina o local, monitor de porta SIP (fixo ou aleatório), é aleatória cada vez que você iniciar o dispositivo aleatório Selecione um livre SIP Monitor de porta.
Is Register	Padrão definido sim, se você quiser que o dispositivo pode fazer uma chamada sem registro, definido Não, permitir também a opção "Permitir envio de chamadas sem Registro" e "Permitir chamadas sem função Registration ".
Register Interval	Significa quantas vezes o equipamento registrará uma vez para o servidor / proxy SIP.

Quadro 24 - Descrição da configuração do SIP.
Fonte: Autor.

5.26 TERMINAIS SIP

Aparelhos com *Session Initiation Protocol* (SIP) normalmente são telefones que foram projetados para melhorar as comunicações, reduzindo os custos de atendimento, simplificando a administração e melhorando a funcionalidade.

Softphone é um aplicativo multimídia, que trabalha associado com a tecnologia VoIP/telefone IP permitindo fazer chamadas diretamente do PC ou *laptop*.

O *softphone* transforma o computador em um telefone multimídia, com capacidade de voz, dados e imagem.

As exigências incluem um PC (*Personal Computer*) que esteja conectado a rede coorporativa, preferivelmente a cabo ou sem fio, um microfone, alto-falantes e o *softphone*.

Primeiramente se deve fazer o *download* do *software,* e depois que devidamente instalado basta estar com o microfone e alto-falantes, ou *headset*, ligados para poder utilizar o *softphone*.

Esses programas são, geralmente, bem simples e fáceis de usar. Possuem interface intuitiva e de fácil compreensão, e possuem também um teclado virtual muito parecido com o de um telefone convencional.

5.26.1 Configurações dos terminais SIP na solução

O quadro abaixo demonstra os campos a ser configurados:

Terminal SIP							
Número ramal terminal	**UDP**	**VLAN**	**Mascara**	**IP Terminal**	***Gateway***	**IP de registro SIP Server**	**SIP *Gateway* address**
XXXX	x	XX	X.X.X.X	X.X.X.X	X.X.X.X	X.X.X.X	DNS SRVOpenScape

Quadro 25 - Terminal SIP.
Fonte: Autor.

A figura abaixo demonstra uma interface do UC utilizada na solução:

Figura 08 - Terminal Softphone.
Fonte: Unify (2013).

5.27 VANTAGENS DA SOLUÇÃO

Comunicações unificadas são recursos de TI, voz e aplicativo. Apresenta *OpenScape UC*, a plataforma de software de comunicações unificadas mais aberta, escalonável e flexível.

Apresenta aprimoramento dos processos estratégicos voltados para o cliente por meio da integração das comunicações para aplicativos empresariais.

Demonstra que aumenta a capacidade de resposta, oferecendo aos funcionários um meio conveniente de colaborar em tempo real, possibilitando uma melhor e mais rápida tomada de decisões em tempo real. Permite que os usuários estejam altamente móveis e em *home office* com as comunicações em tempo real e baseadas em presença. Aumenta a produtividade das equipes. Provê economia nos custos de comunicação, viagens de negócios e uso de espaço físico.

Permite serviço de números únicos. Os funcionários publicam somente um número que pode, depois, ser acessado pela rede mais barata, em qualquer lugar, qualquer hora, e no dispositivo de sua preferência. Define o “dispositivo preferencial” (telefone comercial, telefone residencial, celular, *laptop*, etc.).

Apresentar economia em investimentos em telefonia, TI e aplicativos.

Possibilita economias com tarifas e custos de serviços públicos de telecomunicações.

Permite o gerenciamento das ferramentas e rede.

Possibilita que a equipe compartilha os documentos, vídeos e outras mídias;

Consolida uma infraestrutura única.

5.28 DESVANTAGENS DA SOLUÇÃO

A confiabilidade/estabilidade das redes IP não é equivalente atualmente à da rede telefônica.

A qualidade de reprodução de voz em sistemas VoiP também não é atualmente equivalente à da telefonia.

Novos cuidados com a segurança são necessários.

Alto custo para implantar esta solução.

7 CONCLUSÕES E RECOMENDAÇÕES

O SIP é um protocolo usado para estabelecimento, controle e desconexão de chamada VoIP e que permite:

– Demonstrar os benefícios da implantação de redes VoIP inclui diversas facilidades e funcionalidades que garantem mobilidade, pois há um único sistema de telefone distribuído por múltiplos escritórios, permitindo que os colaboradores se movam entre escritórios sem requerer instalações fixas.

– Apresentar a tecnologia que tem mobilidade e a virtualidade das redes de roteamento IP que permitem aos empregados de uma empresa trabalhar em casa e acessarem as aplicações do escritório, como os sistemas de comunicação VoIP e seus correios de voz.

Conclui-se que diversas tecnologias e protocolos foram desenvolvidos para suportar o VoIP através da rede Internet pública.

Como recomendações sugere-se para trabalhos futuros ou complementares, desenvolver a parte de segurança para esta solução de voz.

Também foi possível desenvolver um estudo de caso, implementando esta solução no caso real.

Outra recomendação é fazer as implementações para mais aplicações com foco na mobilidade, utilizando esta solução de voz.

BIBLIOGRAFIA REFERENCIADA E CONSULTADA

BERNAL, Paulo Sergio. **Voz sobre Protocolo IP**. 1º ed., Editora Érica, São Paulo, 2007.

CHIOZZOTO, Mauro;SILVA, Luis Antonio Pinto da. **TCP/IP – Tecnologia e Implementação**. 2º ed., Editora Érica, São Paulo, 1999.

CSTA. Informações disponíveis em http://translate.google.com/translate?hl=ptBR&sl=en&u=http://wiki.unify.com/wiki/CSTA&prev=/search%3Fq%3Dcsta%2Bsiemens%26sa%3DX%26biw%3D1280%26bih%3D668 Acessado em 11/11/2013 as 19:00

CSTA. Informações disponíveis em http://www.ecmainternational.org/activities/Communications/TG11/cstaIII.htm. Acessado em 11/11/2013a as 19:00

FALBRIARD, Claude. **Protocolos e aplicações para redes de computadores**. Editora Érica, São Paulo, 2002.

MICROSOFT. Informações disponíveis em http://www.microsoft.com/brasil/msdn/arquitetura Acessado em 12/11/2031 as 20:00

MORAES, Alexandre Fernandes de. **Redes de Computadores Fundamentos**. 6º ed., Editora Érica, São Paulo,2009 .

OPENSCAPE ***UC***. Informações disponíveis em http://www.siemens-enterprise.com/br/products-services/unifiedcommunications/openscape-uc-application.aspx . Acessado em 05/9/2013 as 10:00.

OPENSCAPE ***UC***. Informações disponíveis em http://www.siemensenterprise.com/br//br/~/media/internet%202010/Documents/Datasheets/OpenScapeUC-Application_V7_%20DataSheet_%20Issue_2.pdf . Acessado em 05/9/2013 as 10:00.

OPENSCAPE ***Voice.*** Informações disponíveis em http://www.siemens-enterprise.com/br/products-services/voice-solutions/openscape-voice.aspx. Acessado em 05/9/2013 as 10:00

OPENSCAPE ***Voice.*** Informações disponíveis em http://www.siemensenterprise.com/br//br/~/media/internet%202010/Documents/Datasheets/OpenScape-Voice_V7_Data_Sheet_2.pdf . Acessado em 05/9/2013 as 10:00

OPENSCAPE ***Voice***. Informações disponíveis em http://www.siemensenterprise.com/br//br/~/media/internet%202010/Documents/Datasheets/OpenScapePE.pdf . Acessado em 04/10/2013 as 17:00.

OPENSCAPE ***Xpressions***. Informações disponíveis em http://www.siemens-enterprise.com/br/products-services/unified-communications/openscape-xpressions.aspx. Acessado em 05/9/2013 as 10:00.

OPENSCAPE ***Xpressions***. Informações disponíveis em http://www.siemensenterprise.com/br//br/~/media/internet%202010/Documents/Datasheets/Openscape-Xpressions_DB_v7_e.pdf . Acessado em 05/9/2013 as 10:00.

RFC 2508. ***Request for Coments***, Disponível em http://www.normes-internet.com/normes.php?rfc=rfc2508&lang=pt Acessado em 11/11/2013 as 19:00.

RFC 2705**.** ***Request for Coments***. Disponível em http://www.ietf.org/rfc/rfc2705.txt&prev=/search%3Fq%3DRFC%2B2705%2Bdo%2BIETF%26biw%3D1242%26bih%3D442. Acessado em 11/11/2013 as 19:00

SIP**.** Informações disponíveis em http://www.microsoft.com/brasil/msdn/arquitetura/20080428/Comunicacao_como_Servico.mspx. Acessado em 11/11/2013 as 19:00

SOAP. Informações disponíveis em http://translate.google.com.br/translate?hl=ptBR&sl=en&u=http://en.wikipedia.org/wiki/SOAP&prev=/search%3Fq%3Dinterface%2Bsoap%26biw%3D1280%26bih%3D696 Acessado em 11/11/2013 as 20:00

SOARES, Lilian Campos;Freire, Victor Araujo. **Redes Convergentes.** Editora Alta Books Ltda., Rio de Janeiro, 2002.

SOUZA, Linderberg de. **Redes de computadores dados, voz e imagem**. 4º ed., Editora Érica, São Paulo1999.

TANENBAUN, Andrew S. **Redes de Computadores.** Tradução por Insight Serviços de informática. 3º ed., Rio de Janeiro, 1997. Tradução de: Computer Networks.

TRONCO, Tânia Regina. **Redes de Nova Geração**. 1º ed.,- Editora Érica, São

Paulo, 2006 .

WEB COLABORATION. Informações disponíveis em http://www.siemens-enterprise.com/br/products-services/unified-communications/openscape-web-collaboration.aspx . Acessado em 05/9/2013 as 10:00.

WEB COLABORATION. Informações disponíveis em http://www.siemensenterprise.com/br//br/~/media/internet%202010/Documents/Brochures/UK/OpenScapeWebCollaboration_V7_Brochure.pdf. Acessado em 05/9/2013 as 10:00.

XMPP. Informações disponíveis em http://translate.google.com/translate?hl=ptBR&sl=en&u=http://en.wikipedia.org/wiki/XMPP&prev=/search%3Fq%3Dxmpp%26biw%3D1280%26bih%3D668. Acessado em 11/11/2013 as 19:00

VANTAGENS DA IMPLEMENTAÇÃO DA ARQUITETURA IMS EM REDES LEGADAS DE TELECOMUNICAÇÕES

ADVANTAGES OF IMPLEMENTATION OF IMS ARCHITECTURE IN TELECOMMUNICATION NETWORKS LEGACY

Antonio Marcos Moreira[5]
Marcelo Sorente Calixto[6]
Marcelo Takashi Uemura (Orientador)[7]

MOREIRA, Antonio Marcos; CALIXTO, Marcelo Sorente; UEMURA, Marcelo Takaschi (orientador). **Vantagens da implementação da Arquitetura IMS em Redes Legadas de Telecomunicações**. *Revista Tecnológica da FATEC-PR, v.1, n.4, p. 77 -128, jan./dez., 2013.*

RESUMO:

Este trabalho decorre de um estudo de caso comparativo focado na abordagem da arquitetura IMS (IP *Multimedia Subsystem*) e visa o apontamento das vantagens de implementação desse padrão sobre as redes legadas. A convergência das redes de telecomunicações é algo mandatório diante a evolução dos padrões de consumo e aos investimentos necessários relativos à operação e desenvolvimento das redes instaladas, *CAPEX/OPEX* (*Capital Expenditure / Operational Expenditure*). Tal cenário é uma realidade através do modelo NGN (*Next Generation Network*), que tem base na rede IP (*Internet Protocol*), cuja principal vantagem é o fornecimento de serviços diferenciados aos usuários e redução dos custos de operação. Órgãos de padronização estão em constante estudo objetivando o desenvolvimento de novos padrões e tecnologias para que tal convergência seja a mais produtiva possível, tanto com relação à disponibilização de novos serviços aos usuários, quanto ao atendimento das demandas das operadoras por redes mais eficientes e rentáveis. Um dos modelos de arquitetura de redes convergentes mais promissores é o IMS que entre suas principais premissas estão à integração de novos serviços, tarifação diferenciada, provisão de qualidade de serviço dentre outros pontos que serão expostos mais adiante. Será apresentado um estudo sobre as vantagens da implementação da arquitetura IMS com relação às redes legadas TDM *(Time-Division Multiplexing)* e NGN, trazendo motivações e razões que levam tal arquitetura a ser considerada altamente promissora e que vem sendo apontada por especialistas como uma melhoria significativa para serviços oferecidos pela rede IP.

Palavras-chaves: Arquitetura IMS. Redes Convergentes. NGN. Telecomunicações.

---

[5] Antonio Marcos Moreira é graduado em Tecnologia em Sistemas de Telecomunicações pela FATEC-PR (2013). Atua como profissional em empresa de grande porte na área de Telecomunicações.
[6] Marcelo Sorente Calixto é graduado em Tecnologia em Sistemas de Telecomunicações pela FATEC-PR (2013). Atua como profissional em empresa de grande porte na área de Telecomunicações.
[7] Marcelo Takashi Uemura foi o Orientador dos acadêmicos. Possui graduação em Engenharia Industrial Elétrica pela UTFPR - Universidade Tecnológica Federal do Paraná (1998). Especialização em Métodos em Engenharia de Software pela UTFPR (2002). Especialização em Teleinformática e Redes de Multiserviços pela Universidade Federal de Pernambuco (2001). Atualmente é Gerente de Projetos do Positivo Informática S/A. Tem experiência na área de Engenharia Elétrica , com ênfase em Eletrônica Industrial, Sistemas e Controles Eletrônicos.

ABSTRACT:

This work is a comparative case study focused on the IMS (IP Multimedia Subsystem) architecture and intends to point its implementation advantages on legacy networks. The convergence of telecommunications networks is something mandatory against the evolution of consumption and investment models, necessary for the operation and development of installed networks - Capital Expenditure / Operational Expenditure (CAPEX / OPEX). Such a scenario is already a reality through the NGN (Next Generation Network) model, which is based on IP network, whose main advantage is to provide differentiated services to users and reducing operating costs. Standardization sectors are constantly aiming to study the development of new standards and technologies, in order that such convergence is as productive as possible, both in relation to provisioning new services to users and to meet the demands of operators for a more efficient and profitable network. One of the most promising model of convergent network architecture is the IMS (IP Multimedia Subsystem), which among its premises are the integration of new services, differentiated pricing, quality of service provision, among other points that will be detailed furthermore. It will be presented the study on the benefits of the IMS architecture implementation with respect to Legacy TDM and NGN networks, bringing motivations and reasons about why such an architecture is considered highly promising and has been identified by experts as a significant improvement to services offered by the IP network.

Keywords*: IMS architecture. Converged Networks. NGN. Telecommunications.*

1 INTRODUÇÃO

Atualmente as operadoras de telecomunicações estão passando por um período de grande evolução tecnológica na área das telecomunicações, cujas redes estão cada vez mais evoluindo para uma arquitetura centralizada. Ou seja, uma plataforma única que forneça uma vasta gama de serviços, além de reduzir os custos tanto operacionais quanto de desenvolvimento futuro. Um dos grandes motivos para esse cenário está no aumento exponencial de usuários de *Internet*.

Segundo Barcellos (2013), “Diversos estudos apontam projeções de que o mercado global em 2020 terá mais de 2,5 bilhões de pessoas ligadas em rede e cerca de 50 bilhões de dispositivos conectados [...]”.

Os serviços de *Internet* aparecem a cada dia e, nesse contexto, as operadoras fornecem apenas o caminho para a *Internet*, deixando de fomentar esse nicho promissor de mercado através de novos serviços.

Existe uma grande expectativa por parte dos usuários com relação a novos serviços, mobilidade e inclusive integração desses serviços em uma única operadora. Atender a demanda dos usuários agregando novas experiências e ao mesmo tempo controlar a cadeia de lucro passa a ser o objetivo central das operadoras.

A grande dificuldade das operadoras está na estrutura vertical da sua rede legada em que ocorre sobreposição na parte de *hardware,* serviços e base de dados, dificultando, assim, a redução do *CAPEX/OPEX* (*Capital Expenditure/ Operational Expenditure)* além de fornecer novos serviços com muita dificuldade devido à falta de uma arquitetura mais aberta e convergente.

Essa demanda somente poderá ser atendida por uma arquitetura de rede que possibilite uma convergência mais completa e efetiva para as redes legadas implantadas. Órgãos como o ETSI (*European Telecommunications Standards Institute*) e o 3GPP *(3rd Generation Partnership Project)* vêm estudando o subsistema IMS ao qual é visto como uma solução promissora por vários especialistas.

O IP *Multimedia Subsystem* (IMS) tem como função integrar todos os serviços multimídia, inclusive a rede legada já existente, pois conta com uma arquitetura funcional dividida em pontos de referência com funções específicas.

Esta arquitetura permite ampliar o número de serviços oferecidos, dar mobilidade, potencializar a rede já implantada, além de evitar sobreposição de custos com novas infraestruturas independentes.

O IMS foi idealizado no ano 2000, com a finalidade de proporcionar aos provedores de acesso sem fio, principalmente as operadoras de serviço móvel pessoal (SMP), uma forma mais eficiente no gerenciamento das chamadas em redes baseadas em IP (*Internet Protocol).*

O propósito deste projeto é apresentar a funcionalidade desta arquitetura, diferenças e vantagens com relação à rede legada bem como, dados atuais de implementação e possibilidade de serviços que o IMS pode prover.

Outro norteador desse trabalho é clarificar a arquitetura IMS e sua potencialidade, de forma a facilitar tomadas de decisão com relação à implementação do padrão, além de alertar a comunidade acadêmica para um assunto atual.

1.1 OBJETIVO GERAL

Abordar a arquitetura IMS comparando-a com a rede legada TDM/NGN, de forma a evidenciar suas vantagens de implementação. Busca-se também proporcionar material sobre o assunto que colabore com a comunidade acadêmica tendo em vista a visível falta de conhecimento sobre este novo padrão, além de servir de apoio à decisão de operadoras de telefonia sobre qual direção devem seguir suas redes.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos podem ser resumidos na relação abaixo:

a) Abordar a arquitetura IMS e seus principais protocolos, trazendo transparência com relação ao comportamento da estrutura;
b) Demonstrar as vantagens da arquitetura IMS sobre as redes legadas;
c) Apresentar alguns novos serviços que podem ser oferecidos com essa nova arquitetura;
d) Apresentar um assunto atual cuja disseminação de conhecimento é restrita até o momento, tornando-o aberto ao público de interesse.

2 JUSTIFICATIVA

Com a evolução das telecomunicações, focando o atendimento às novas tendências de mercado, tornou-se necessário o desenvolvimento de uma rede unificada a qual dê suporte a diferentes serviços e que estes estejam acessíveis pelos mais diversos tipos de terminais.

Buscando atender tais requisitos e outras tantas exigências do cliente atual, vários órgãos estão se dedicando à pesquisa buscando um padrão que consiga atender a essas necessidades, mantendo o padrão de qualidade e disponibilidade já impresso pelas redes em operação.

Nesse cenário, surge o IMS, apontado pelos especialistas como uma arquitetura promissora. Muitas operadoras de telecomunicações ainda estão receosas e indecisas pelos novos gastos em recursos a serem investidos nessa nova arquitetura. Algumas operadoras já iniciaram investimentos nesse sentido, visando o pioneirismo e a conquista de novos mercados, alavancando seus rendimentos.

Diante disso, muitas especulações e dúvidas existem ao redor dessa arquitetura, que vem a cada dia, tornando-se uma realidade na vida de operadoras e clientes de telecomunicações. Tornar clara tal arquitetura, assim como seus potenciais benefícios, auxiliará em possíveis dúvidas de implementação, assim como, fornecerá maiores informações à sociedade acadêmica sobre um tema atual e que merece destaque.

3 METODOLOGIA

A metodologia adotada refere-se a uma pesquisa bibliográfica e constitui-se das seguintes etapas:

- Levantamento das bibliografias necessárias e pertinente ao projeto;
- Definição e delimitação dos tópicos a serem abordados para o desenvolvimento focado na arquitetura IMS e suas vantagens;
- Desenvolvimento, explicitação e fundamentação dos critérios a partir do qual é possível evidenciar as vantagens da arquitetura IMS frente às redes legadas;
- Elaborar as conclusões e recomendações a respeito do assunto e estudo realizado.

4 REVISÃO BIBLIOGRÁFICA

Neste tópico estão descritos os itens necessários para a compreensão da temática abordada no trabalho, elaborados de acordo com o estudo da bibliografia.

4.1 AMBIENTE PRÉ-CONVERGÊNCIA

Segundo Alberti (2009), com o desenvolvimento das telecomunicações, vários novos serviços começaram a ser oferecidos aos clientes pelas operadoras de telefonia fixa e móvel, nas quais se destacam TV a cabo, *Internet*, entre outros serviços que passaram a fazer parte do cotidiano das pessoas. Contudo, era necessária uma rede própria e especializada para cada novo serviço.

Cada operadora era especializada em alguns serviços que podiam ser atendidos em suas redes. O usuário precisava contratar diversas operadoras além de receber diversas contas. Para acessar cada uma dessas redes os usuários precisavam de terminais especializados: TV, telefone, computador, etc.

Como consequência dessa segmentação tecnológica cada serviço foi regulamentado também de forma especializada.

A figura abaixo demonstra de forma clara a separação das redes.

Figura 23: Separação das redes e serviços.
Fonte: Encontro Telesintese (2012.)

Essa heterogeneidade de tecnologias e regulamentações trouxe grandes desafios, principalmente nos cenários de interconexão de soluções, criando verdadeiras ilhas tecnológicas além de dificultar a oferta de novos serviços.

4.2 PONTOS IMPACTANTES: CENÁRIOS PRÉ-CONVERGENTES

Conforme Braga (2011), para a maioria das redes especializadas era necessário um meio próprio para sua transmissão. Ou seja, se a operadora desejasse ofertar mais de um serviço precisaria investir em uma nova infraestrutura.

A cada novo serviço, uma nova plataforma era adquirida, e consequentemente novos investimentos eram demandados até mesmo na operação e manutenção elevando os custos, investimentos em equipamentos e serviços tornaram-se pontos importantes nas decisões das operadoras.

Tornou-se necessária a contratação de profissionais especializados em infraestrutura, uma vez que esta, por ser muito especializada e fragmentada, não estava apta a oferecer um único padrão.

Devido à diversidade de infraestruturas observou-se uma grande dificuldade em oferecer novos serviços, os quais se tornaram limitados.

Outro ponto operacional impactante era a necessidade de diferentes terminais para uso das diferentes redes, elevando consideravelmente os investimentos por parte dos usuários além de restringir a mobilidade e disponibilidade dos serviços.

Todos esses fatores e restrições fizeram com que a necessidade de integração dessas redes fosse vista como uma das saídas, embora a grande diversidade de tecnologias e o uso de *interfaces* proprietárias dificultassem e elevassem os custos dessa integração.

Apesar de essas interconexões apresentarem uma saída para esse problema, à manutenção de redes muito específicas acabou se tornando inviável.

Em vista disso, começou-se a desenvolver um conceito de redes que poderiam oferecer mais de um tipo de serviço, sendo que os primeiros estudos foram feitos com os serviços de voz e dados haja vista a popularização da *Internet* e a necessidade da telefonia.

4.3 MOTIVAÇÕES PARA CONVERGÊNCIA DE REDES E SERVIÇOS

Segundo Amado (2009), diante das dificuldades operacionais e financeiras já relatadas, esforços para desenvolver uma plataforma mais convergente começaram a serem empreendidos por vários órgãos de regulamentação. Vários foram os motivos para essa nova visão e concepção de rede.

A manutenção de infraestruturas especializadas de difícil interconexão possui um custo muito alto, pois cada infraestrutura possui demandas particularizadas que elevam os custos.

Uma rede convergente permite usar da melhor forma possível os recursos disponíveis, pois todo um leque de serviços e aplicações compartilham a infraestrutura disponível.

A existência de uma infraestrutura convergente permite que as operadoras melhor administrem seus negócios, realizando também a convergência de produtos e serviços.

A convergência dos produtos e serviços seria benéfica para as operadoras, pois facilitaria a criação de pacotes de serviços com custos reduzidos (Combo) além de proporcionar ao cliente melhores tarifas e mais satisfação.

Com uma rede única, o controle de tráfego seria facilitado, haveria uma melhor gerência facilitando o suporte e controle de qualidade dos serviços ofertados, além de apresentar um bom custo benefício para a operadora.

Por todas as motivações acima, se chegou à conclusão que a convergência das redes era a melhor opção para o fornecimento de novos serviços e redução dos custos operacionais no mercado de telecomunicações.

4.4 EFEITOS DA CONVERGÊNCIA

O efeito da convergência sobre os usuários é menos tecnológico e mais prático. A percepção deste, ao longo do processo, é o aumento da oferta de serviços de forma integrada, de fácil acesso e a preços mais baixos.

De certa forma, em algum momento, cada usuário poderá lidar com um único provedor (de sua preferência), mover-se com seus equipamentos ou dispositivos para qualquer lugar e, ainda assim, utiliza-los normalmente, recebendo ao final do mês, apenas uma única cobrança consolidada que discrimina todos os serviços utilizados.

Essa é a necessidade e o sonho de consumo de muitos clientes. Em termos tecnológicos e mercadológicos, é o que se denomina redes de próxima geração, NGN (COLCHER, 2005). A figura a seguir mostra os motivos da preferência dos usuários pelos serviços integrados.

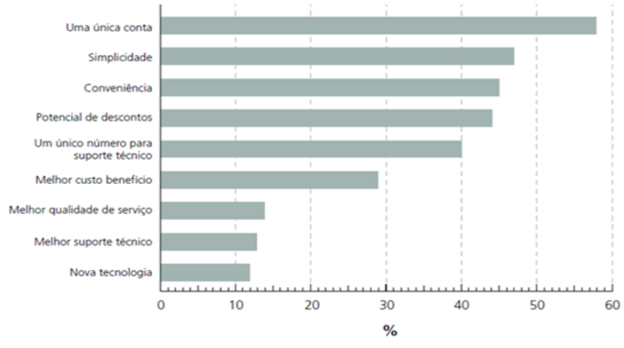


Figura 24: Motivos da preferência pelo serviço integrado
Fonte: PROMON (2007)

4.5 DEFINIÇÃO E PREMISSAS - REDES CONVERGENTES (NGN)

A norma regulamentada informa:

> A NGN é uma rede baseada em pacotes capaz de fornecer serviços de telecomunicações e de fazer uso de múltiplas tecnologias de transporte *broadband* e com *QoS* habilitado. As funções relacionadas a serviço são independentes das camadas inferiores relacionadas às tecnologias de transporte. Esta permite acesso irrestrito para os usuários de redes e prestadores de serviços concorrentes e/ou serviços de sua escolha. Suporta a mobilidade generalizada que permite a provisão consistente e ubíqua dos serviços aos usuários [...]. (ITU-T, 2001)

Outro conceito de NGN aceito pela GSC *(Global Standard Collaboration)* é a definição ETSI *(European Telecommunications Standards Institute)*.

> NGN é um conceito para definição e utilização de redes, que devido à separação formal em diferentes camadas e uso de *interfaces* abertas, disponibilizam para os provedores de serviços e operadoras uma plataforma capaz de criar, oferecer e gerenciar serviços inovadores [...]. (CASTRO, 2011)

Algumas premissas intrínsecas à NGN são:

- Modelo de arquitetura funcional padronizado e aberto com suporte às redes legadas;
- Assegura qualidade de serviço fim-a-fim;
- Plataformas de serviço com provisionamento e controle para múltiplas redes;
- Segurança adequando protocolos e API's (*Application Programming Interfaces*);
- Mobilidade generalizada, garantindo a interconectividade e o *roaming* ao usuário.

A primeira versão do padrão NGN (*Release* 1 ou apenas Rel-1) foi concluída em Dezembro de 2005 pelo TISPAN (*Telecommunications and Internet converged Services and Protocols for Advanced Networking*), onde provê o primeiro conjunto de especificações para implementação da NGN.

4.5.1 Início da separação dos elementos de rede

Segundo Tronco (2006), a separação dos elementos de rede teve início com o advento da RI (Rede Inteligente). Nas centrais de comutação telefônicas tradicionais, as funções de controle de rotas, encaminhamento das informações e criação de serviços são integradas no mesmo elemento (estrutura monolítica).

Na RI iniciou-se o processo de separação da camada de aplicação das demais camadas de rede. A sequência evolutiva continuou com a separação da camada de controle das camadas de comutação e acesso.

A camada de acesso e comutação passou a ser denominada MG *(Media Gateway)* e a camada de controle de MGC *(Media Gateway Controller).*

A padronização entre MGC e MG favoreceu a livre escolha entre diferentes fabricantes de equipamentos.

A figura a seguir mostra as camadas e aplicações em uma configuração

MGC e comutadores e nos da uma base de como se iniciou o processo de segmentação da estrutura monolítica.

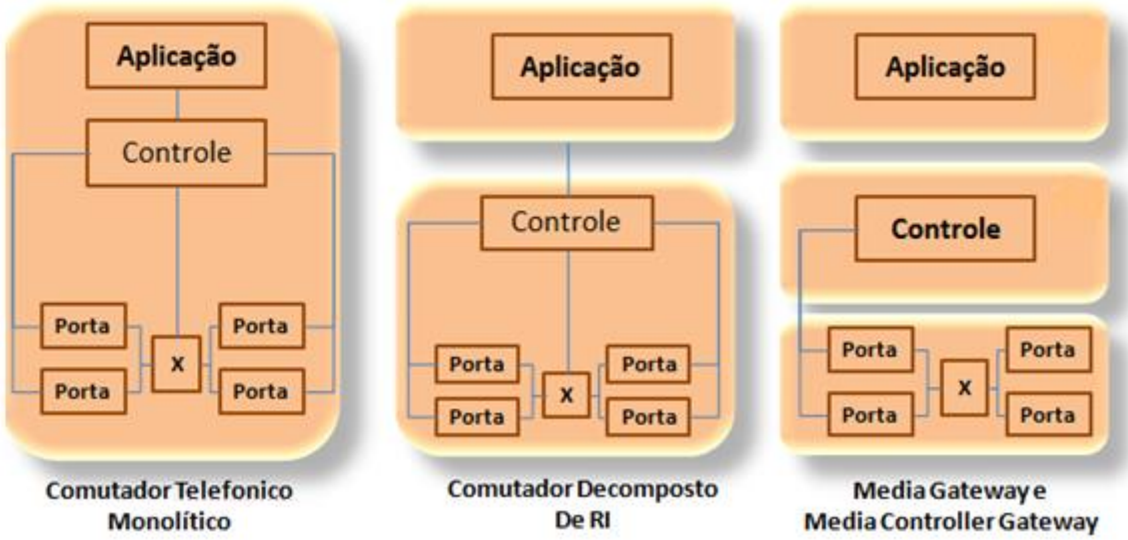


Figura 25: Decomposição da estrutura monolítica
Fonte: MSF (2013) (*Multiservice Switching Forum*).

Ainda, de acordo com Tronco (2006), o foco da NGN *(Next Generation Network)* é separar o *hardware* do *software* dos equipamentos de telecomunicações, através de *interfaces* padronizadas, criando um ambiente multifornecedor tanto para *hardware* quanto para *software*, além de tornar possível a distribuição dessas partes para locais mais apropriados (arquitetura distribuída), mais próximos do assinante ou mais próximos do núcleo da rede.

4.6 CONCEITOS IMS – IP *MULTIMEDIA SUBSYSTEM*

Segundo Camarillo (2004), antes de surgir o conceito IMS, a situação na qual os operadores se encontravam não era muito encorajadora. Se por um lado, o mercado baseado em voz sobre comutação de circuitos acomodou-se, tornando complicado para os operadores obterem apenas receitas fornecendo e tarifando chamadas de voz, por outro, serviços sobre comutação de pacotes ainda não tinham grande penetração no mercado, não obtendo os operadores ainda grandes receitas com a sua utilização.

Os operadores precisavam de uma forma de fornecer serviços sobre pacotes de uma forma mais atrativa.

Deste modo, conforme Camarillo (2004), o IMS foi criado, tendo como objetivos:

- Combinar as últimas tendências da tecnologia;
- Permitir a interligação e mobilidade na *Internet;*
- Criar uma plataforma comum para desenvolver serviços multimídia diversificados;
- Criar um mecanismo que permitisse aumentar o desempenho da utilização da rede devido ao uso excessivo da rede de comutação de pacotes.

Conforme Colcher (2005), o IP *Multimidia Subsystem* (IMS) foi concebido como ideia no ano de 2000, com a finalidade de proporcionar aos provedores de acesso sem fio, principalmente as operadoras de serviço móvel pessoal (SMP), uma forma mais eficiente no gerenciamento de chamadas em redes baseadas em IP (*Internet Protocol*).

O IMS foi concebido para unir o mundo celular com o mundo da *Internet*, sendo que sua arquitetura de controle de serviço foi projetada para proporcionar o *QoS (Quality of Service*) desejado, controle de tarifação e customização de serviços que não eram possíveis na *Internet* (AL-BEGAIN, 2009).

O IMS foi criado inicialmente como um padrão para redes sem fio. No entanto, as operadoras de telefonia fixa, na busca por um padrão para unificação das redes, notaram o potencial da arquitetura, cogitando a utilização em uma rede independente e de maior abrangência (AGBINYA; JOHNSON, 2010).

O IMS é uma nova estrutura para distribuir multimídia, que está desvinculada do dispositivo (telefone móvel ou fixo, computador, *palmtop*, etc.) ou do meio de acesso (*Wi-Fi*[8] *(Wireless Fidelity)*, rede celular, banda larga, etc.), o que tornará o mundo cada vez mais digital (AGBINYA; JOHNSON, 2010).

5 DESENVOLVIMENTO

Cada uma das etapas, previstas na metodologia para o desenvolvimento do trabalho, foi desenvolvida conforme descrito a seguir.

5.1 *OVERVIEW* DA EVOLUÇÃO

Desde a invenção do telefone no século19 até o século atual passamos por várias transformações tecnológicas, as quais nos permitiram um desenvolvimento contínuo rumo a inovações nunca antes imaginadas.

De acordo com Colcher (2005), até a década de 1950 a rede telefônica era totalmente baseada em tecnologia analógica, sendo que somente após a invenção do transistor em 1948 e sua evolução até a produção do primeiro circuito integrado em 1958 permitiram a criação das primeiras centrais digitais em 1960. Um pouco antes disso, em 1946, surgiu o primeiro computador digital.

As digitalizações nos sistemas telefônicos, em paralelo ao avanço que a tecnologia digital estava proporcionando aos sistemas computacionais motivaram o desenvolvimento das CPAs (Centrais de Programa Armazenados) oferecendo uma série de vantagens em termos de operação, manutenção e provisão de serviços.

Segundo Braga (2011), o desenvolvimento da eletrônica digital possibilitou a digitalização completa das informações tratadas internamente nas centrais. A informação analógica passou a ser convertida para digital logo na *interface* de entrada da central e todo tratamento posterior dentro do sistema, incluindo a comutação, é feita digitalmente.

Temos um exemplo da evolução na figura abaixo:

[8] *Wi-Fi* (pronúncia em inglês /ˈwaɪfaɪ/) é uma marca registrada da *Wi-Fi Alliance*. É utilizada por produtos certificados que pertencem à classe de dispositivos de rede local sem fios baseados no padrão IEEE 802.11.

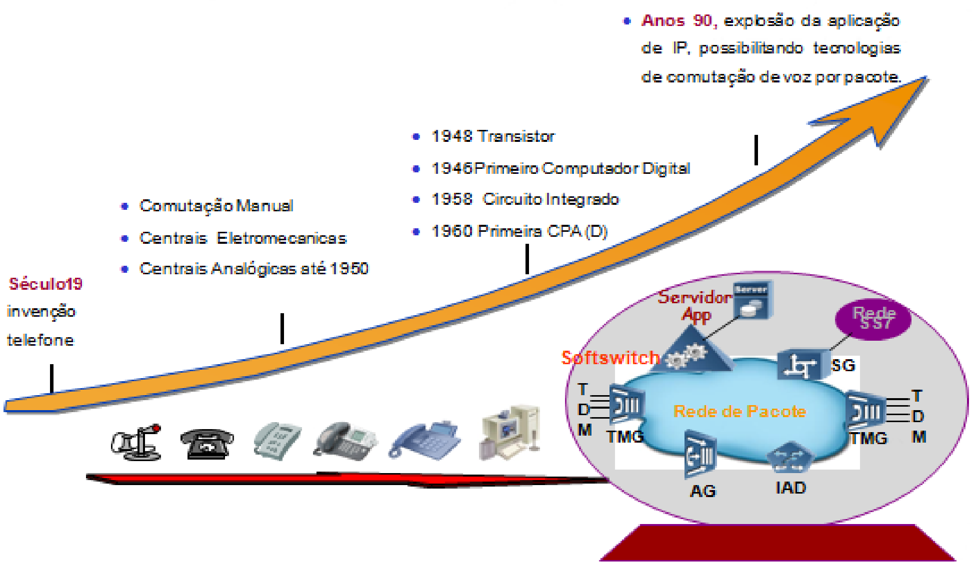


Figura 26: Evolução das telecomunicações.
Fonte: Elaborado pelo Autor, com base na apostila Huawei (2002).

Isso permitiu um melhor desempenho na parte de processamento de chamadas, redução de tamanho físico e redução de consumo de energia. Surgiu então à tecnologia TDM (*Time Divison Multiplexing*), sistema baseado no conceito de modulação PCM (*Pulse Code Modulation*) que converte o sinal analógico em um sinal binário para ser transmitido digitalmente.

A figura abaixo demonstra o sistema de modulação:

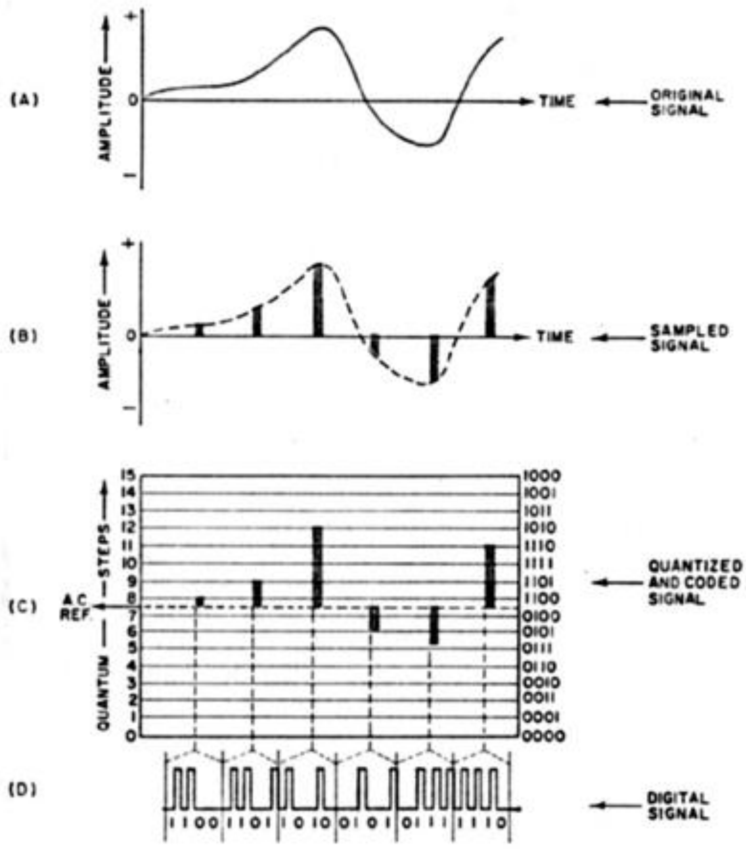


Figura 27: Modulação do sinal analógico em digital.
Fonte: Ecured (2013).

Esse sistema trouxe algumas melhorias, dentre elas a possibilidade de várias chamadas simultâneas, a regeneração do sinal sem elevação da taxa de ruído e a criação de níveis hierárquicos que conseguem transportar grandes volumes de canais de conversação. A partir desse ponto a evolução das redes de telefonia seguem em direção ao sistema NGN.

Com todas essas evoluções, novos serviços podiam ser oferecidos aos usuários pelas operadoras. Novas redes, produtos e inovações surgiram. Novas perspectivas de receitas poderiam ser geradas. Porém, a diferente característica dos tráfegos (texto, áudio, imagem, vídeo, etc.) apontou para o desenvolvimento do sistema de comunicação especificamente projetado para atender a determinado tipo de mídia.

O resultado foi o surgimento de várias redes específicas para o transporte dos diferentes tipos de informação, todas estas projetadas para atender aplicações específicas, adaptando-se mal a outros tipos de serviço.

Para as operadoras, novos nichos de mercado, embora os custos excessivos de operação e manutenção de tais estruturas eram vistos como fatores preocupantes.

Aos poucos ficou evidente que era necessário a unificação das plataformas como forma de oferecer mais serviços com menos custos. Em paralelo com esse cenário um fenômeno muito importante estava ocorrendo, a massificação do uso da *Internet* e dos serviços por ela oferecidos.

Com a popularização da *Internet* e o aumento das taxas de transmissão, o serviço de voz começou a entrar em decadência, devido aos novos serviços que surgiram, como o *VoIP* (*Voice over Internet Protocol*). Demais serviços poderiam ao longo do tempo ser incorporados e fornecidos também, tornando ainda mais complexo esse contexto.

As operadoras preocupadas com esse cenário precisavam de uma alternativa para manter seus antigos clientes, e continuar conquistando novos, assegurando a sua sobrevivência no competitivo mercado.

A solução encontrada foi à migração para uma infraestrutura única que pudesse integrar os serviços e mantendo a rede tradicional: a NGN. Esta se baseia no oferecimento de serviço *triple play*, ou seja, é capaz de fornecer serviços de voz, vídeo e dados encapsulando as informações e transmitindo através do protocolo IP na rede de dados já existente.

Esta arquitetura possibilitaria a introdução de novos serviços de forma ágil, flexível, eficiente, evoluindo das redes telefônicas tradicionais, baseadas em comutação de circuito, para redes convergentes baseada em comutação de pacotes com *interfaces* abertas e padronizadas.

Dessa forma, as operadoras deixariam de ser somente o caminho para a *Internet*, tonando-se fornecedores de aplicações e serviços customizados, além de preservarem os investimentos já aplicados na rede legada.

Tal investimento se justificaria tanto do ponto de vista econômico-financeiro não apenas pelas perspectivas de novas receitas, mas também pela redução dos custos operacionais obtidos pelas convergências das infraestruturas de transporte e gerenciamento.

Uma das principais dificuldades na implementação dessa evolução é a mudança significativa na topologia de rede, sendo que a mesma deve ser implementada de forma gradual possibilitando assim que a camada de transporte (*Backbone* IP) cresça gradativamente à medida que o processo de evolução caminhe.

Abaixo segue gráfico comparativo de implementação das redes com relação a custos.

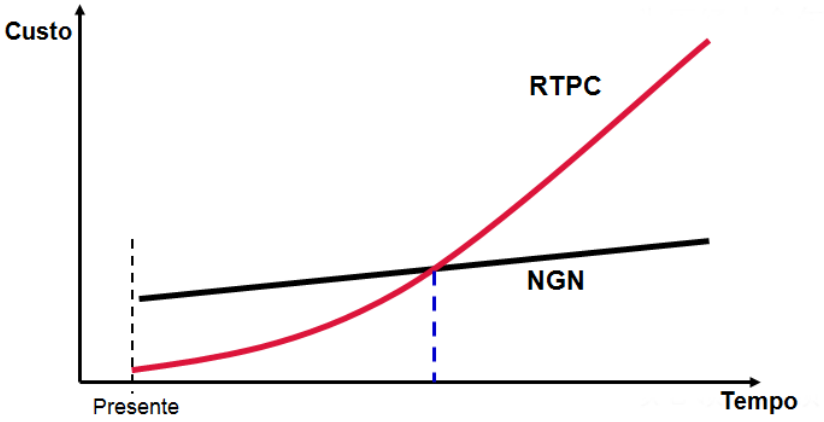


Figura 28: Comparativo investimento de implementação das redes.
Fonte: Huawei (2002).

5.1.1 Comutações de circuitos (PSTN) e pacotes (NGN)

Fato importante a se dizer é que, antes da NGN, as centrais de telefonia *Public Switched Telephone Network* (PSTN) utilizavam a tecnologia de comutação de circuito, que pressupõe o estabelecimento de um caminho dedicado durante todo o período da comunicação entre as centrais envolvidas.

Nesse caso, o estabelecimento de uma chamada é realizado em três etapas: estabelecimento do circuito, transferência de informação e ao fim desconexão do circuito. Neste tipo de comutação o meio alocado permanece dedicado durante todo o período da comunicação de forma exclusiva, mesmo que nenhuma informação seja transmitida. Este tipo de comutação se faz interessante para tipos de tráfegos constantes e contínuo caso contrário o meio físico será desperdiçado ou subutilizado. Uma das vantagens desse método é a garantia da disponibilidade do meio, uma vez que ele se torna exclusivo após o estabelecimento, garantindo uma qualidade constante. Mas, nem todos os tipos de tráfegos em uma rede são contínuos, com taxas constantes.

Vídeo comprimido, texto e gráficos em geral geram tráfego com taxas de bits variáveis. A utilização de redes comutadas por circuito para transmissão de tráfegos com taxas variáveis ou em rajada causa um desperdício da rede, pois os recursos passarão por períodos de ociosidade.

Por outro lado, a NGN, trabalha com comutação de pacotes, onde o meio é utilizado de forma dinâmica e compartilhada, otimizando a rede de transporte. Nesse tipo de comutação, as informações são digitalizadas, quebradas em tamanhos menores compatíveis ao *payload* do protocolo que a transportará, sendo que em alguns casos pode haver compressão, otimizando os recursos de transmissão pela utilização de *codecs* (codificador/decodificador) com reduzida taxa de bits, utilização de técnicas de supressão de silêncio e multiplexação estatística.

Outro ponto importante a ser lembrado é que, as redes de telefonia convencionais (PSTN), são conhecidas pela sua qualidade de serviço e confiabilidade do sistema. Já na comutação por pacote, estes são entregues a rede e utilizam a técnica *Best effort*[9], roteando os pacotes de informações com base no estado da rede daquele momento e não garantindo a entrega. O uso de priorização pode ser empregado para implementar níveis de *Qos.*

A tecnologia de comutação de pacotes tem evoluído a fim de obter a mesma qualidade de serviço das redes de telefonia tradicionais. É exatamente por essa qualidade que o legado de telefonia ainda continua em operação. Trata-se de um sistema já consolidado há muitos anos, por isso, sua migração para a convergência tende a ser lenta.

Abaixo figura de uma estrutura monolítica que utiliza comutação por circuito em comparação com uma estrutura horizontal que utiliza comutação de pacote.

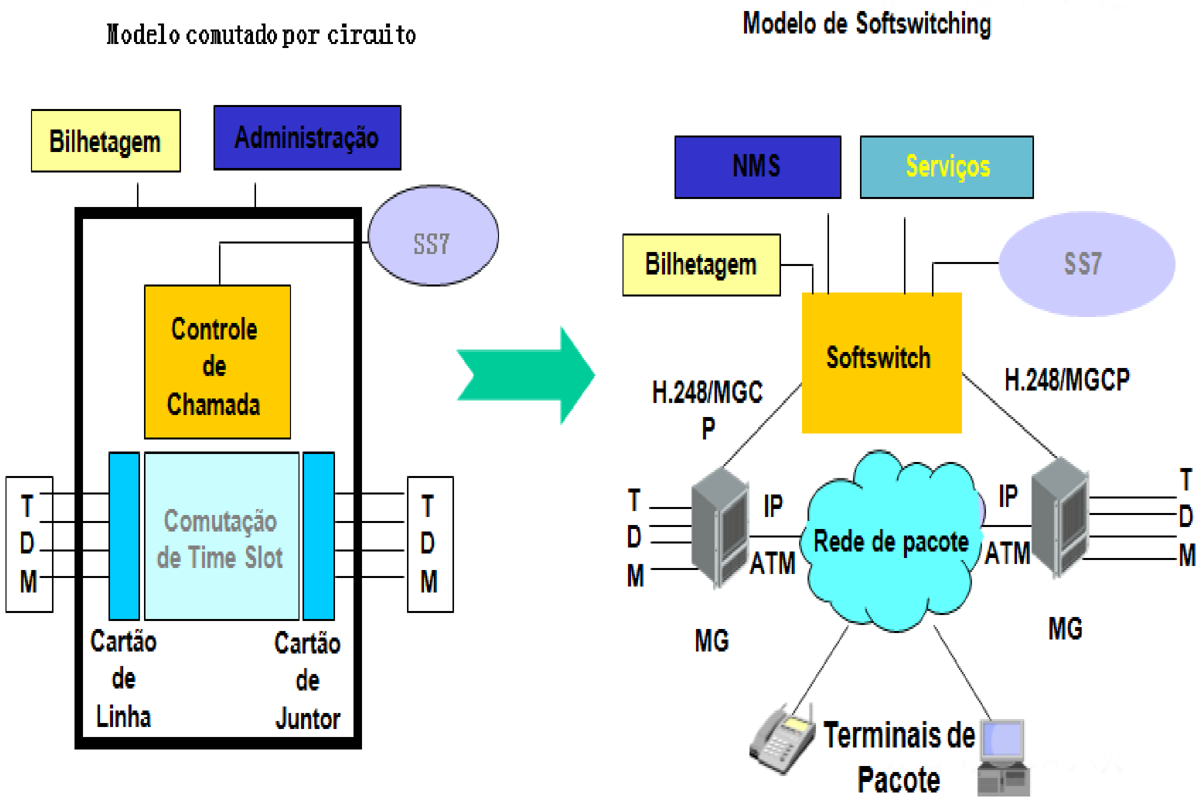


Figura 29: Comutação de circuito versus comutação de pacotes.
Fonte: Huawei (2002).

5.1.2 NGN – *Next Generation Network*

Diante do cenário exposto a solução que melhor se apresentou para este dilema foi à convergência dos serviços em redes conhecidas como redes de próxima geração (NGN).

O conceito NGN está relacionado a uma ideia bastante simples: transportar toda a informação que corre pela rede em pacotes digitais que utilizam o protocolo IP (*Internet Protocol*). Tais pacotes seriam capazes de transportar conversas telefônicas, vídeo, arquivos, *e-mails*, dentre outros.

Outro conceito de NGN aceito pela GSC (*Global Standard Collaboration*) é a

[9] O *Best-Effort* é um modelo de serviço atualmente usado na *Internet*. Consiste num utilizador que envia um fluxo de dados, ao mesmo tempo em que a largura de banda é partilhada com todos os fluxos de dados enviados por outros utilizadores, ou seja, estas transmissões são concorrentes entre si.

definição ETSI (*European Telecommunications Standards Institute*): NGN é um conceito para definição e utilização de redes, que devido à separação formal em diferentes camadas e uso de *interfaces* abertas, disponibilizam para os provedores de serviços e operadoras uma plataforma capaz de criar, oferecer e gerenciar serviços inovadores.

A NGN proporciona um caminho para a migração da rede tradicional para uma rede baseada em IP, mantendo os serviços existentes e sua implementação traz os seguintes resultados:

- Reduz custos (*CAPEX e OPEX*);
- Aumenta o ROI (*Return On Investment*);
- Provê uma base comum para serviços fixos, móveis e corporativos;
- Permite a rápida criação e distribuição de serviços inovadores e convergentes sob demanda;
- Possibilita o dimensionamento flexível, de fácil escalabilidade e a centralização do controle da rede para bilhetagem e atividades de operação e manutenção;
- Atrai serviços providos por terceiros sem que se perca o controle da rede;
- Garante o uso de *interfaces* abertas e de diferentes fornecedores, o que permite a escolha do melhor equipamento para cada camada da rede.

A ideia geral da NGN é ter uma única rede capaz de transportar todos os tipos de informações, serviços e mídias. Esta rede é construída sob o protocolo IP com o princípio da estruturação e divisão dos planos funcionais em: acesso, transporte *e switching,* controle, inteligência e serviço (SULTAN, 2002).

Em suma, a NGN veio para concretizar o velho sonho das telecomunicações e áreas afins disponibilizando uma plataforma de transporte comum para vídeo, voz, dados, permitindo aplicações do tipo telefonia IP, acesso a *web* através de telefones móveis, e outras aplicações bastante interessantes.

5.1.3 Arquitetura NGN

De acordo com Davidson (2000), uma visão bastante empregada na literatura para clarificar a arquitetura modela as redes convergentes em três camadas, sendo essas compostas por *interfaces* de comunicação abertas e padronizadas proporcionando interoperabilidade e flexibilidade na integração com os diversos fornecedores.

Segundo Funicelli (2007), outro detalhe é que as camadas são independentes e podem ser modificadas, substituídas ou atualizadas sem afetar os outros níveis funcionais.

Segue figura mostrando a divisão de camadas da arquitetura NGN.

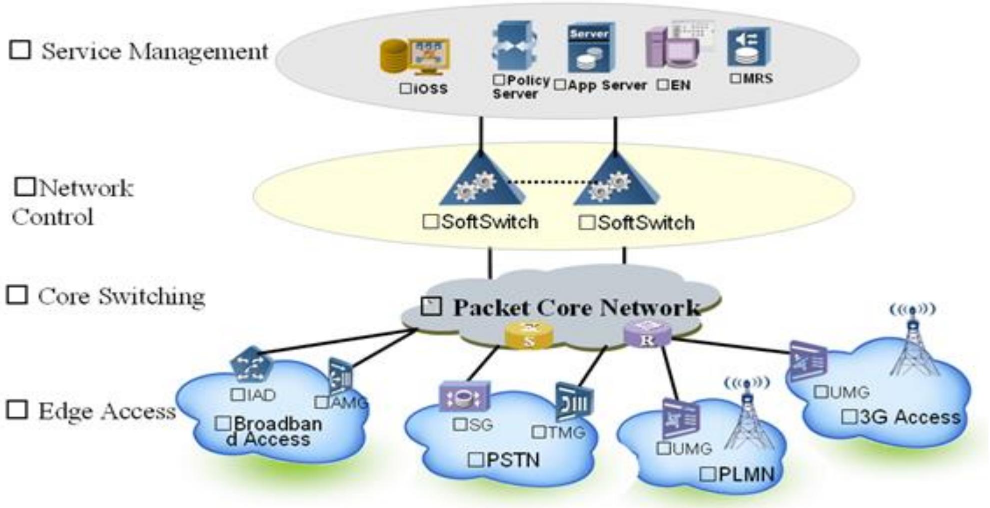


Figura 30: Camadas da arquitetura NGN.
Fonte: Huawei (2003).

Antes da NGN o modelo de serviço era de estruturas verticais com tecnologias dedicadas a cada tipo de acesso, incorrendo na duplicação de funcionalidades entre os vários sistemas isolados. Mas agora a NGN propõe a simplificação deste modelo de serviço, estruturando horizontalmente as camadas e unificando as funcionalidades para oferecer os serviços e conteúdos a todos os meios de acesso.

A figura a seguir compara as modificações nas estruturas antes e depois da NGN simplificando as funcionalidades.

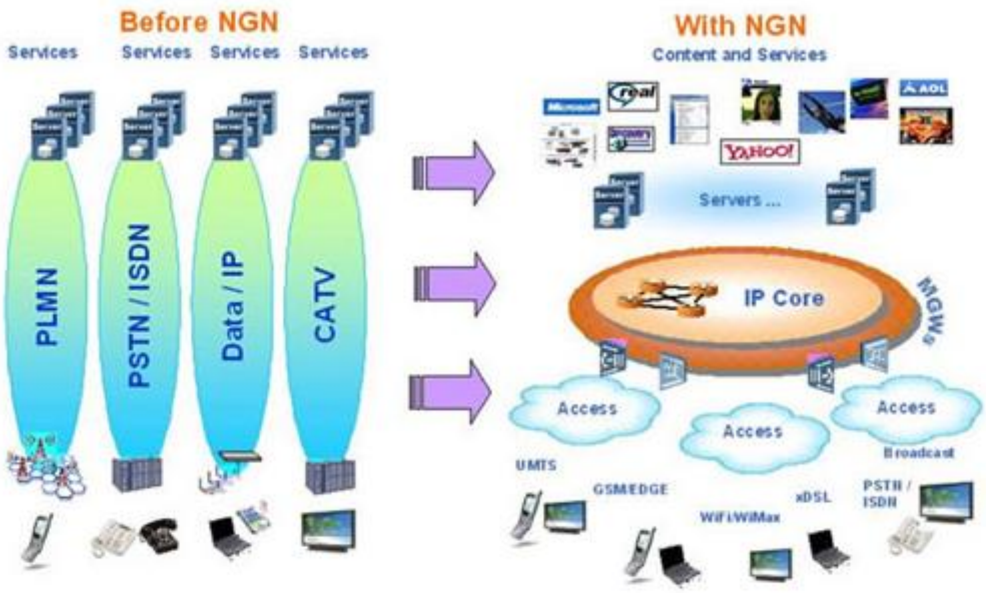


Figura 31: Comparação da arquitetura antes e depois da NGN.
Fonte: Teleco (2013).

5.1.4 Camada de acesso

Segundo Peters (2000), nessa camada encontram-se as unidades de acesso de assinante, como os telefones IPs e *Access Gateways*, além de comutadores, roteadores e *Media Gateways* (que transformam a voz em pacotes), responsáveis por prover as *interfaces* de acesso à rede convergente e pela codificação e empacotamento dos sinais multimídia.

As principais funções dessa camada são:

- Processamento da voz (compressão, descompressão e empacotamento);
- Transporte da sinalização para a camada de controle.

É nessa camada que os *codecs* atuam sobre a informação a ser tratada.

Outro elemento importante que reside nessa camada são os servidores de mídia (*Media Servers*) que são responsáveis por fazer todo o processamento de mídia, gravação, reprodução de mensagens, reconhecimento de fala.

Os *media gateways* são frequentemente classificados como:

– ***Residential gateways***, que são os equipamentos que provêm à *interface* da rede convergente com aparelhos telefônicos convencionais através de *interfaces* analógicas a dois fios;
– ***Enterprise gateways***, que são os equipamentos que provêm à *interface* da rede convergente com o PABX (*Private Automatic Branch eXchange*) digital através de enlaces E1[10], utilizando principalmente sinalização R2 digital;
– ***Trunking gateways***, que são os equipamentos que provêm à *interface* da rede convergente com a RTPC ou (Rede de Telefonia Pública Comutada) através de enlaces E1, utilizando principalmente sinalização por canal comum SS7 (*Signaling System* 7*)*;
– ***Signaling gateways***, que convertem a sinalização de chamada telefônica, denominada *Commom Channel Signaling System 7 (SS7)*, para sinalização de chamada para a rede IP. Na SS7, as mensagens de sinalização são trocadas entre as centrais de comutação telefônica através de um canal dedicado de *64Kbit/s* por onde trafega a sinalização de todos os canais telefônicos simultaneamente.

Para a comunicação com a camada de controle são utilizados protocolos entre os elementos, como o MGCP (*Media Gateway Control Protocol*), ou posteriormente o H.248[11], protocolo mais atual e com maior aplicação.

Tais protocolos serão abordados com maior ênfase na sequência do trabalho.

5.1.5 Camada de controle

A camada de controle de chamadas é responsável pelo estabelecimento, tarifação, supervisão e liberação de todas as chamadas que trafegam pela rede convergente, por meio do controle dos *media gateways* via protocolos padronizados.

É uma parte estratégica da rede onde fica o equipamento chamado *Media Gateway Controller* (MGC) ou *softswitch* que é a inteligência da rede. O *softswitch* tem a função de interpretar os números discados pelo assinante, acompanhar e controlar o estabelecimento da chamada, além de deter tarefas relacionadas à tarifação.

Como principais características do MGC/s*oftswitch* destacam-se:

– *Interface* com os protocolos de sinalização como: ISUP (ISDN *Iuser Part)*,

[10] E1 é um padrão de linha telefônica digital europeu criado pela ITU-TS e o nome determinado pela Conferência Europeia Postal de Telecomunicação (CEPT), sendo o padrão usado no Brasil e na Europa; é o equivalente ao sistema *T-carrier* norte-americano, embora o sistema T norte-americano utilize taxas de transmissão diferentes.

[11] H.248, também conhecido como protocolo Megaco, é um padrão desenvolvido cooperativamente entre o ITU (*International Telecommunications Union*) e a IETF (*Internet Engineering Task Force*) para permitir que um *Media Gateway Controller* (MGC) desempenhe seu papel em um *media gateway* (MG).

INAP (*Intelligent Network Application Protocol*), H.323[12], SIP (*Session Initiation Protocol*), MGCP, H.248 entre outros;
- Separação do controle de chamada da parte de serviço e transporte;
- Inteligência centralizada facilitando a rápida introdução de novos serviços convergentes;
- Confiabilidade e segurança na tarifação, medição de desempenho e controle de recursos.

Tanto a parte de controle quanto a de sinalização é feita através dos protocolos, desde aqueles utilizados para aplicações em tempo real RTP (*Real-time Transport Protocol*) ou mesmo protocolos de sinalização e controle (SIP). Tais protocolos serão detalhados mais adiante na explanação do IMS.

5.1.6 Camada de serviços

A camada de serviços é constituída por servidores e bases de dados que controlam a lógica de execução dos serviços oferecidos aos usuários atendidos pela rede convergente. O desenvolvimento de novos serviços segundo esse modelo se resume à introdução de novas aplicações nesses servidores. Por isso, a implantação de novos serviços nessas redes é considerada mais ágil, flexível e abrangente do que nas redes telefônicas convencionais.

Os modos mais comuns para oferecimento de serviços são através do modelo de rede inteligente INAP *(Intelligent Network Application Protocol)* e pelo protocolo H.323 ou SIP.

Dentre os serviços mais oferecidos pelas operadoras na atualidade estão *voice-mail*, serviços pré-pagos, *unified messaging, voice browser* entre outros.

Na figura a seguir temos uma demonstração dos elementos, protocolos e conectividade da rede NGN.

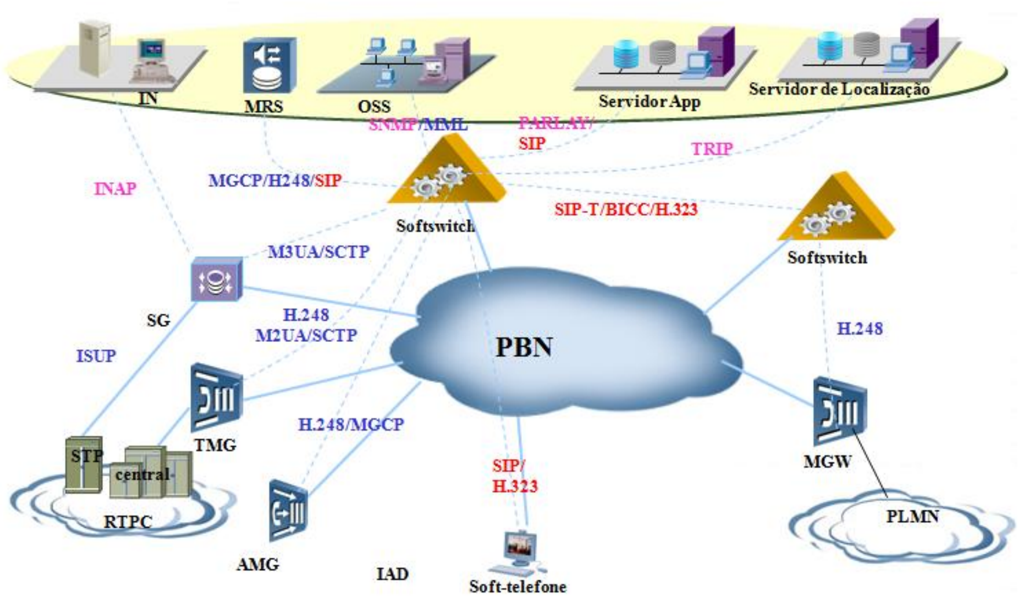


Figura 32: Elementos da rede NGN, protocolos e conectividade.
Fonte: Huawei (2003).

[12] O padrão H.323 é parte de recomendações ITU-T (*International Telecommunication Union Telecommunication Standardization sector*) e que trata de "Sistemas Audiovisuais e Multimídia". A recomendação H.323 tem o objetivo de especificar sistemas de comunicação multimídia em redes baseadas em pacotes e que não provêm uma Qualidade de Serviço (*QoS*) garantida.

5.1.7 Tecnologias de uma rede NGN

Segundo Ibe (2003), é praticamente impossível introduzir uma rede NGN sem considerar as seguintes tecnologias:

- **Processamento digital de sinais:** o processamento dos sinais digitais é a tecnologia chave para a integração do tráfego de voz e dados. A vantagem é a facilidade de compressão de voz e a sua conversão para pacotes de dados;
- **Roteamento dos pacotes:** os recentes protocolos de roteamento permitem priorizar as filas e os pacotes das aplicações que exijam qualidade de serviço (*QoS*);
- **Redes ópticas:** as redes ópticas aumentam, substancialmente, a banda de transmissão que está disponível pelos provedores de telecomunicações e dos usuários. As vantagens da multiplexação por onda de luz e o roteamento por comprimento de onda deverá consolidar o roteamento nas redes ópticas;
- **Protocolos avançados:** o TCP/IP (*Transmission Control Protocol/Internet Protocol*) tornou-se um protocolo estratégico, muitos esforços estão sendo feitos para conceber novas funções e aumentar seu desempenho. As redes baseadas em IP em breve deverão ser capazes de prover a mesma qualidade de serviço encontradas nas redes ATM (*Asynchronous Transfer Mode*) atualmente. Recentes avanços incluem o protocolo RTP (*Realtime Transfer Procotocol*), o MPLS (*Multi-Protocol Label Switching*), o SS7-to-IP um protocolo de sinalização de telefonia SS7 para rede IP e o modelo de serviços diferenciados (*DiffServ*). O tráfego convergente tem trazido considerável interesse para os administradores de rede e tem levado os provedores de serviços de rede a introduzir soluções que vão ao encontro aos requerimentos dos clientes. Nem os tradicionais serviços de telefonia nem os novos provedores de NGN serão competitivos apenas reduzindo os custos de transmissão, entretanto, o ponto chave é a *QoS*, características como desempenho, disponibilidade, flexibilidade e adaptabilidade, serão padrões de mercado.

5.2 PADRONIZAÇÃO

Os principais órgãos envolvidos na padronização da NGN são o TISPAN (*Telecommunications and Internet converged Services and Protocols for Advanced Networking*), um grupo de trabalho do ETSI (*European Telecomunication Standards Institute*), o FGNGN (*Focus Group on NGN*), o NGN-GSI (*NGN-Global Standard Initiative*), ambos os grupos pertencem ao ITU-T (*Internetional Telecommunication Union Telecommunication Standardization Sector*).

A primeira versão de padronização NGN foi feita pelo TISPAN em dezembro de 2005 e estabeleceu as primeiras especificações para implementação da NGN.

Entre as principais resoluções estavam à substituição da PSTN, mantendo o fornecimento da mesma, a introdução de serviços multimídia, novos serviços baseados no protocolo IP, arquitetura, subsistemas e forma de operação dos mesmos.

A segunda versão chamada REL-2, foi finalizada no início de 2008 levando em consideração outros aspectos:

- Análise de exigências do FMC (*Fixed Mobile Convergence*) e do FMCA (*Fixed Mobile Convergence Aliance*);
- Análise das capacidades da rede de suportar o IPTV (*Internet Protocol Television*);
- Integração do IPTV utilizando IMS.

Nessa versão já houve sincronismo entre o TISPAN e o 3GPP a fim de verificar o alinhamento dos padrões para a *interface* móvel também.

A padronização da NGN iniciou-se separadamente e em vários órgãos que focavam em pesquisar e desenvolver novos serviços direcionados as suas áreas de atuação, ou seja, seguindo o modelo vertical habitual.

Mas com a nova tendência de integração e convergência de serviços exigida pelos usuários e as necessidades de redução de custos, o conceito logo mudou e então passaram a compartilhar as pesquisas e unir forças para chegarem à padronização de protocolos, *interfaces* e arquiteturas comuns e que interoperem com todas as demais já existentes para proporcionar a maior flexibilidade possível.

Na figura abaixo visualizamos a integração dos órgãos de padronização.

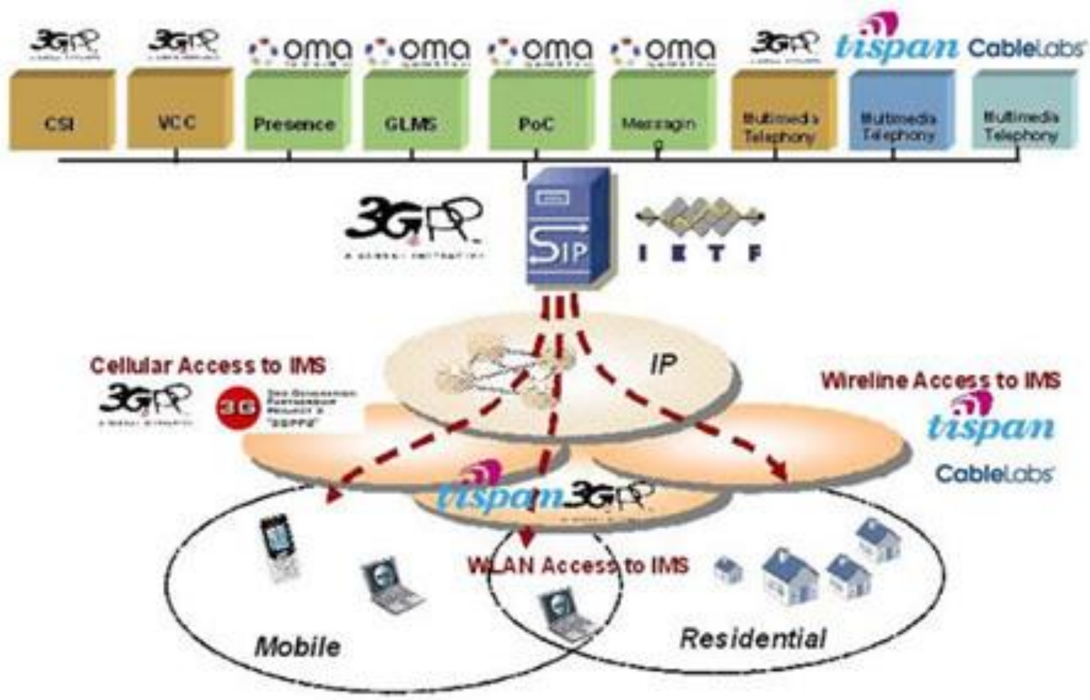


Figura 33: Integração dos órgãos de padronização.
Fonte: Teleco (2013).

Observou-se que para controlar e possibilitar a entrega de diversos conteúdos e serviços a qualquer tipo de acesso fazia-se necessário um *core* bem definido e estruturado. Assim surgiu o IMS (IP *Multimídia Subsystem*) com o propósito de prover a integração completa das redes e serviços, cuja centralização esta representada na figura a seguir.

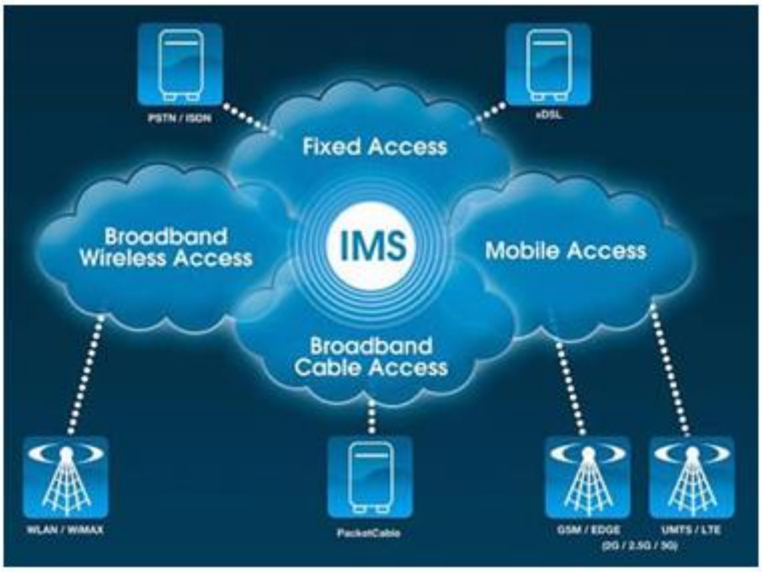


Figura 34: Arquitetura IMS centralizando o controle das redes.
Fonte: Teleco (2013).

5.3 IMS – IP *MULTIMIDIA SUBSYSTEM*

O IMS é uma arquitetura de referência que visa à entrega de serviços multimídia através da rede IP. É uma maneira completamente nova de distribuir multimídia (voz, vídeo, dados, etc.) independente do dispositivo (telefone móvel ou fixo, cabo, *Internet,* etc.) ou do meio de acesso (celular, *Wi-Fi*, banda larga, linha telefônica, etc.) e que mudará o modo como todos nós nos relacionamos com o mundo cada vez mais digital.

O IMS é considerado uma plataforma única, que será capaz de oferecer serviços completos, inclusive para as redes sem fio com a vantagem da mobilidade e da possibilidade de combinação de serviços.

Segue figura detalhando e comparando os serviços cobertos pela NGN em relação ao IMS.

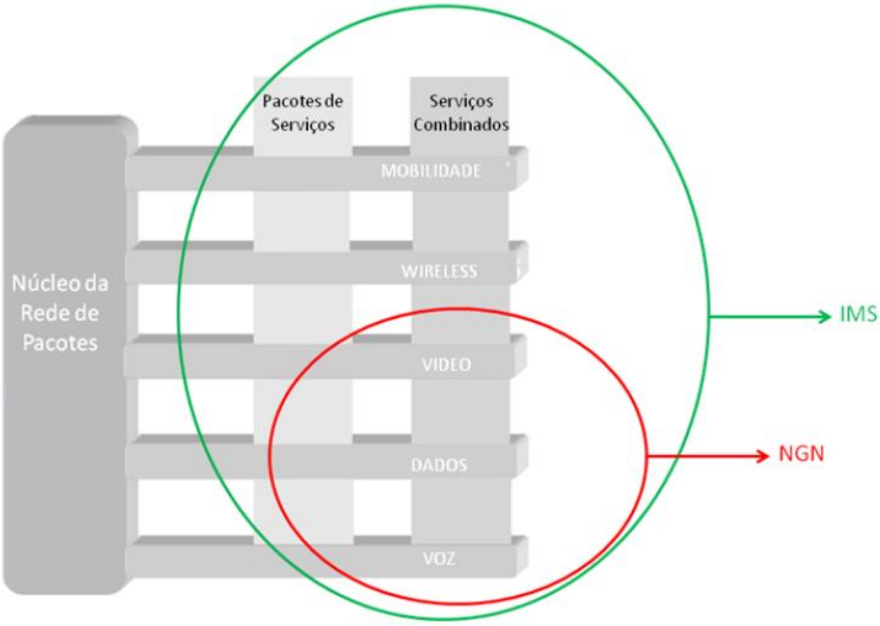


Figura 35: Abrangência arquitetura NGN e IMS.
Fonte: Braga (2011).

Segundo Salchow (2008), um exemplo prático de serviço do IMS seria um usuário utilizando um dispositivo móvel, realizando uma chamada pela rede de telefonia celular, ao entrar numa rede *Wi-Fi,* uma rede sem fio doméstica, por exemplo, a chamada seria movida dinamicamente, e de forma transparente, para a rede *Wi-Fi* válida, obtendo diversas vantagens, como por exemplo, maior largura de banda.

Esta mesma chamada poderia ser transferida para um *softphone VoIP* no *notebook* ou para um telefone fixo. Estas trocas seriam feitas entre provedores de serviços sem que a chamada fosse interrompida.

5.3.1 História do IMS

De acordo com Al-Begain (2009), antigamente a telefonia celular só oferecia serviços de voz 1G (Primeira Geração), mas a partir da 2G (Segunda Geração), com a entrada da era digital nas comunicações celulares, e principalmente na 3G (Terceira Geração), onde as taxas de transmissão de dados aumentaram bastante, passamos a ter a telefonia celular como um meio de acesso à *Internet*.

As redes 3G já possuem nativamente a comutação de pacotes, tornando a comunicação de dados mais rápida e eficiente, comparada com dispositivos 2G, que fazem uso de comutação de circuitos.

A idealização do IMS foi motivada pelo sucesso da *Internet,* o qual os serviços multimídia sobre a tecnologia de redes de pacotes estavam experimentando um sucesso satisfatório. Isso instigou as operadoras de telefonia celular a introduzir serviços multimídia em suas redes centradas em voz.

As redes de acesso celular tinham evoluído de uma tecnologia puramente de comutação de circuitos para a terceira geração (3G), redes sem fio que poderiam suportar altas velocidades de dados, voz e serviços multimídia utilizando comutação por pacotes (IP).

O *core* da rede estava dividido em domínio de comutação (CS) baseado no GSM (*Global System for Mobile Comunication*) e domínio de comutação de pacotes baseado no GPRS (*General Packet Radio Services*).

O domínio GPRS permitia o usuário acessar serviços multimídia e aplicações *Internet* usando o protocolo IP, muito embora a largura de banda das redes de acesso 3G ainda era muito escassa para apoiar serviço de multimídia em tempo real, além dos desafios advindos da mobilidade relativos entre os usuários em *roaming* entre diferentes redes de acesso e domínios administrativos.

Outro detalhe, não menos importante refere-se ao suporte fim-a-fim do *Qos* em redes 3G, sendo essa uma complexa tarefa. Apesar da terceira geração já ser comutada por pacote, o que permite que os usuários tenham uma transmissão de dados mais rápida e uma maior largura de banda, a rede IP não oferece nenhuma garantia sobre qualidade de serviço, ou seja, não garante uma largura de banda suficiente para manter um serviço de vídeo conferência, por exemplo. É dentro desse contexto que surge o IMS!

O IMS foi introduzido como parte das especificações 3GPP no estágio R5 (Subsistema do domínio PS) pelas operadoras móveis a fim de oferecer acesso a serviços de multimídia para redes móveis e sem fio com garantia de *QoS,* customização de serviços, controle de tarifação e outros serviços não disponibilizados pela *Internet*.

O IMS foi concebido para unir o mundo celular com o mundo da *Internet.*

A figura a seguir indica a evolução e a entrada do IMS na rede.

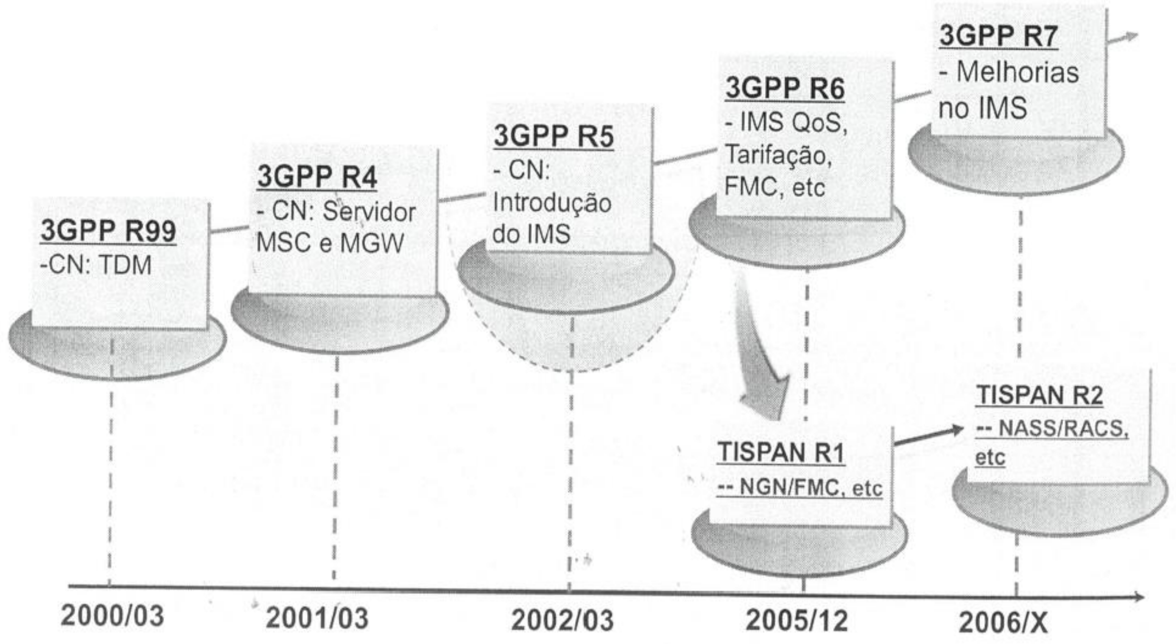


Figura 36: Evoluções da rede móvel e entrada do IMS.
Fonte: Huawei (2010).

5.3.2 Arquitetura da rede IMS

A arquitetura da rede IMS é composta por camadas bem definidas, cujos nós presentes nessas possuem uma ou mais funções.

O 3GPP não padroniza os elementos físicos da arquitetura IMS, mas sim as funcionalidades e *interfaces* entre os elementos. Isto significa que a arquitetura IMS é um conjunto de funcionalidades interligadas por *interfaces* padronizadas. Os fabricantes têm a possibilidade de combinar diferentes funcionalidades num único elemento da arquitetura (isto é, num único elemento físico). Similarmente, os fabricantes poderão separar uma única funcionalidade em dois ou mais elementos.

Segundo Silva (2009), outro ponto importante a se referir é que a arquitetura IMS definiu inicialmente o uso exclusivo de IPv6 (*Internet Protocol Version 6*) nas suas redes. Porém, durante os últimos anos, o progresso na migração de IPv4 (*Internet Protocol Version 4*) para IPv6 por parte das operadoras não foi muito significativo. Desta forma, para permitir a integração das redes IPv4 tradicionais foi necessário definir dois novos elementos, o *Application Layer Gateway* (ALG) e o *Transition Gateway* (TrGW).

O primeiro realiza a interoperabilidade entre IPv4 e IPv6 no plano da sinalização (mensagens SIP (*Session Initiation Protocol)* e SDP (*Session Description Protocol)*, enquanto o ultimo processa o tráfego do MG, por exemplo, RTP (*Real-time Transport Protocol)*).

A arquitetura IMS pode ser dividida em camadas semelhantes ao modelo apresentado pela NGN: camada de acesso / controle de portadora, camada de controle e camada de serviço.

A figura abaixo mostra a divisão das camadas IMS.

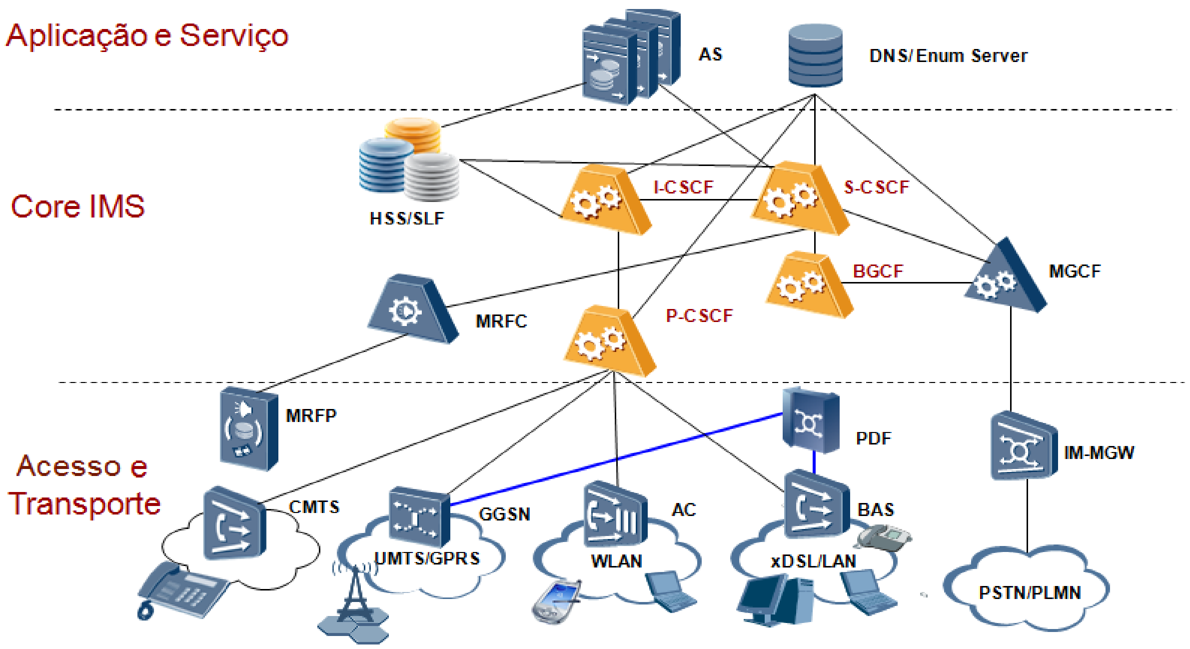


Figura 37: Camadas da rede IMS.
Fonte: Huawei (2010).

5.3.3 Camada de acesso / Controle de portadora

A primeira camada é a de acesso e controle de portadora. Faz a abstração das redes de acesso ao IMS, ou seja, independente se temos UMTS (*Universal Mobile Telecommunication System*) ou *Wi-Fi* como meio de acesso, para o IMS isso é transparente.

Em essência, essa camada age como um ponto de junção entre as camadas de acesso e a rede IP acima dela. Ela é responsável pelo provisionamento IP inicial (atribuição de endereços de IP e *gateway* padrão por DHCP (*Dynamic Host Configuration Protocol*), bem como facilitar o registro de dispositivos nas camadas superiores).

É importante lembrar que, em geral, tudo que há acima dessa camada (as camadas de controle e serviço) é baseado em IP, enquanto a camada de acesso abaixo pode não ser de fato baseada em IP.

5.3.4 Camada de Controle

A segunda camada é a de controle de sessões, ela controla a autenticação, roteamento e distribuição do tráfego IMS entre a camada de transporte e a camada de serviço. A maior parte do tráfego nessa camada é baseada no protocolo SIP.

Além de rotear mensagens SIP para seus serviços apropriados, a camada de controle também pode oferecer interação entre a camada de serviços e outros serviços.

O componente principal na camada de controle é o *Call Session Control Function* (CSCF), que facilita a interação correta entre os servidores de aplicativos, de mídia e o *Home Subscriber Service* (HSS) que é o repositório centralizado para todas as informações de contas de assinantes. Essa também é a camada responsável pela combinação de serviços, ou seja, oferecendo a capacidade de combinar voz (que agora é composta apenas de pacotes IP), dados e vídeo. Isso permite que os dispositivos IMS recebam múltiplos serviços quase que simultaneamente em uma única sessão.

Segundo Salchow (2010), um exemplo seria um serviço *pay-per-download* onde os clientes adquirem tons de celular ou vídeo. A operadora precisa não somente ser capaz de distribuir esses produtos para o usuário, mas também tem de interagir com serviços de faturamento, autenticação (para determinar privilégios de usuário) e até com serviços *QoS* para garantir uma distribuição e processamento adequados do conteúdo adquirido. Grande parte desses processos é executada por essa camada.

5.3.5 Camada de serviço / aplicação

A camada de serviços é aquela em que os serviços residem. Isso inclui serviços tradicionais de voz (como correio de voz, anúncios, resposta de voz interativa, etc.), bem como novos aplicativos que expandem a arquitetura IMS. Pode fornecer aplicações desenvolvidas por um terceiro confiável tais como: central de jogos, centro de conferência, aplicações empresariais, etc.

Essa é a camada final de abstração que dá à arquitetura IMS a força e flexibilidade para implementar rapidamente os novos serviços, conforme demonstrado na figura a seguir:

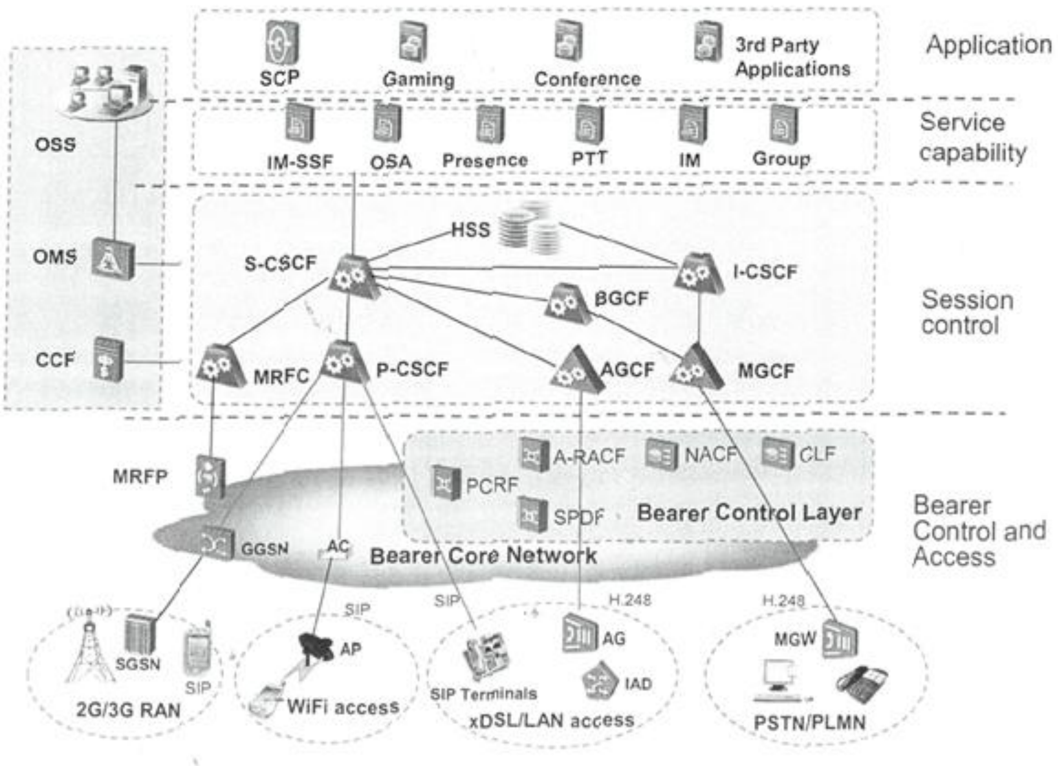


Figura 38: Camadas e elementos da arquitetura IMS.
Fonte: Huawei (2010).

5.3.6 Características IMS

Separações importantes são realizadas na arquitetura IMS:

– Implementação do serviço separado do controle da chamada, comparado com a rede pré-NGN, o serviço é completamente separado do controle

da sessão na rede IMS, tornando a camada de serviço mais flexível e aberta para atualização e emprego do serviço;
- Controle de chamada separado da portadora de mídia.

Outro ponto fundamental é que a mesma esta em acordo com as tendências para o desenvolvimento de rede:

- FMC (*Fixed and Mobile Convergence*) e *ALL* IP;
- Redes baseadas em *software* (vantagens de mercado funcionais para vendedores qualificados em *software*);
- Plataforma de serviço aberta e compartilhada: (adota ao máximo o protocolo de *Internet* como o SIP (*Session Initiation Protocol*), projeto e emprego mais simples de novo serviços);
- Segmentação das funcionalidades (arquitetura da rede torna-se favorável pela separação de função).

A figura abaixo ilustra a evolução da separação de funcionalidades.

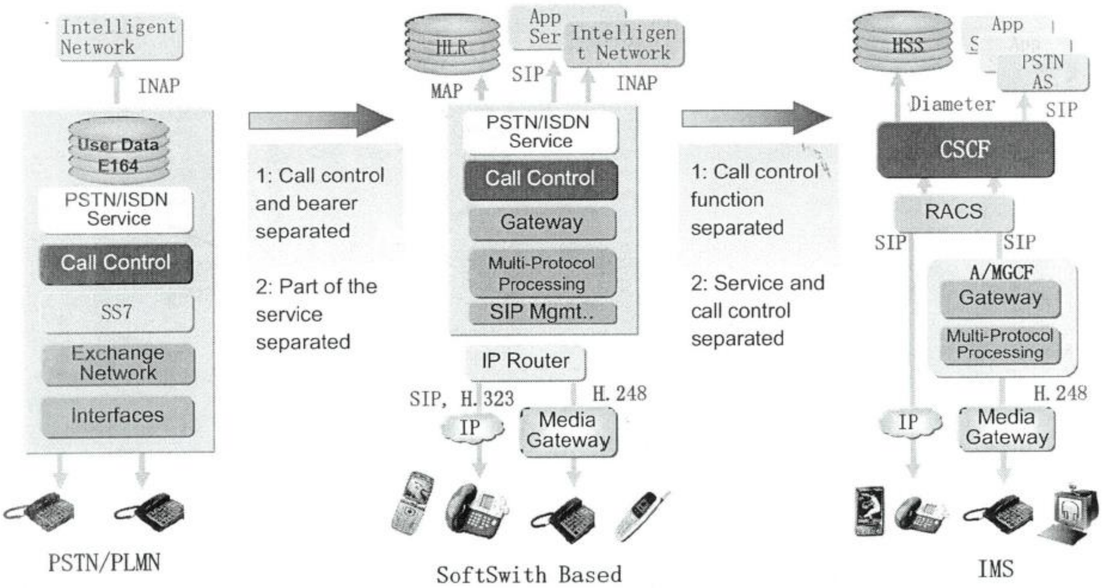


Figura 39: Tendências das redes.
Fonte: Huawei (2010).

5.3.7 Elementos IMS

O IMS é dividido em *core* e elementos que o integram para poder fornecer uma completa gama de serviços que atendam todas as características de uma rede tradicional.

Dentro do *core* temos o S-CSCF (*Serving-Call Session Control Function*), I-CSCF (*Interrogating-Call Session Control Function*), P-CSCF (*Proxy-Call Session Control Function*) e BGCF (*Breakout Gateway Control Function*) os quais desempenham funções centrais dentro do *core* IMS (ETSI TS 182 012 V1. 1.1 2006-04[13]).

Figura demonstrativa dos elementos da arquitetura IMS

[13] *(European Telecommunications Standards Institute (ETSI) que revisou as especificações técnicas do 3rd Generation Partneship Project)* 3GPP e 3GPP2 e adequou como parte das especificações do *Telecoms & Internet converged Services & Protocols for Advanced Networks* (TISPAN).

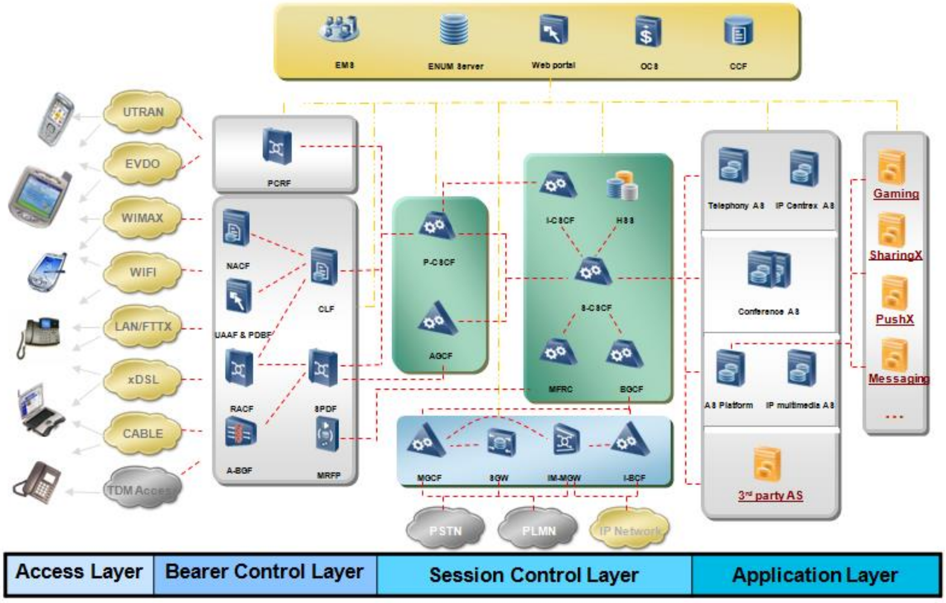


Figura 40: Elementos da arquitetura IMS
Fonte: HUAWEI (2010)

Segmentando os elementos de rede por função temos o seguinte:

- Controle de chamada: P-CSCF, I-CSCF e S-CSCF;
- Gerenciamento de usuário: HSS e SLF (*Subscriber Location Function*);
- Interconexão de rede: MGCF (*Media Gateway Control Function)*, IM-MGW e BGCF;
- Recursos de mídia: MRFC (*Multimedia Resource Function Controller*) e MRFP (*Multimedia Resource Function Processor*).

Seguem as principais características de cada elemento de rede a ser executada por um ou mais nós:

5.3.7.1 P-CSCF (*Proxy*)

Destaca-se com:

- Primeiro ponto de contato para a rede IMS no domínio local ou no domínio visitado;
- Consulta de endereço do I-CSCF no DNS (*Domain Name System*), se necessário;
- Controle da rede de acesso;
- Controle de *QoS,* controle de NAT (*Network Address Translation*) e controle de segurança;
- Envio da mensagem de registro para o I-CSCF;
- Quando a transação é finalizada, envio de dados de tarifação;
- Compressão de sinalização;
- Suporte para registros implícitos, que indica que um único usuário IMS tem a habilidade de registrar um conjunto de identidades públicas de usuário, utilizando um registro único;
- Para cada transação SIP, aplicação da política SDP, se definida;
- Envio de mensagem SIP para o próximo nó IMS.

6.3.7.1.1 I-CSCF (*Interrogating*)

Procede da seguinte forma:
- Solicitação ao HSS do S-CSCF a ser utilizada, esta solicitação é realizada utilizando o protocolo *Diameter*;
- Consulta ao DNS se necessário;
- Envio da mensagem SIP *register* para o S-CSCF;
- Quando a transação é finalizada, envio de dados de tarifação;
- Primeira entrada para a rede IMS de uma operadora;
- Designa S-CSCF e roteamento da sessão para sessão;
- Ocultar topologia.

6.3.7.1.2 S-CSCF (*Serving*)

Executa as seguintes funções:
- Autenticação de registro de usuário;
- Controle de roteamento de sessão (normal, interconexão, chamada de emergência);
- Disparo de serviço;
- Para uma nova transação SIP, aplicação dos critérios de filtragem, definidos no perfil do usuário;
- Opcionalmente, consulta do DNS para localização do próximo nó IMS;
- Envio da mensagem SIP para os nós SIP especificados pelos critérios de filtragem;
- Quando a transação é finalizada, envio de dados de tarifação. Este sendo obrigatório;
- Suporte da utilização e/ou bloqueio seletivo nômade, este sendo opcional.

Ainda dentro do *core* IMS podemos verificar que existem além dos CSCF´s outros blocos como o *Media Gateway Control Function* (MGCF), o *Multimídia Resource Function Controller* (MRFC) e o *Breakout Gateway Control Function* (BGCF) que tem funções específicas principalmente para auxiliar na integração com a rede legada e outras redes (ETSI ES 282 007 V1. 1.1 2006-06).

5.3.7.1.3 BGCF – *Breakout Gateway Control Function*

Procede da seguinte forma:
- Seleciona um MGCF apropriado para a interconexão com o domínio PSTN/CS;
- Opcionalmente consulta do DNS;
- Envio da mensagem SIP ao nó IMS selecionado.

O BGCF lida exclusivamente com a função de rotear chamadas quando um dispositivo IMS tenta se comunicar com um aparelho telefônico que está em uma rede comutada por circuito fixa ou móvel determinando qual será o *gateway* de mídia mais adequado (ETSI ES 282 007 V1. 1.1 2006-06).

5.3.7.1.4 MGCF - *Media Gateway Control Function*

Executa as seguintes funções:
- Controla o IMS-MGW para estabelecer/modificar/apagar canais de mídia;

- Seleciona o I-CSCF para chamadas de entrada da PSTN/CS;
- Realiza conversão do protocolo entre ISUP e SIP.

O MGCF tem como funções fornecer a capacidade de controlar troncos de mídia o que inclui alocações e deslocações de recursos de mídia e também a modificação do uso destes recursos.

O MGCF realiza comunicações com o CSCF, com o BGCF e com redes de comutação de circuitos. Também realiza conversão de protocolos entre o ISDN *User Part* (ISUP) e SIP, suportando interfuncionamento de chamadas não relacionadas com a sinalização de canal comum número 7 (SS7). No caso de chamadas que são originadas na rede legada, o MGCF irá determinar os próximos saltos IP dependendo das informações que foram recebidas na sinalização, podendo também realizar a função de roteamento de tráfego de trânsito (ETSI ES 282 007 V1. 1.1 2006-06).

Figura representando o MGCF e sua função.

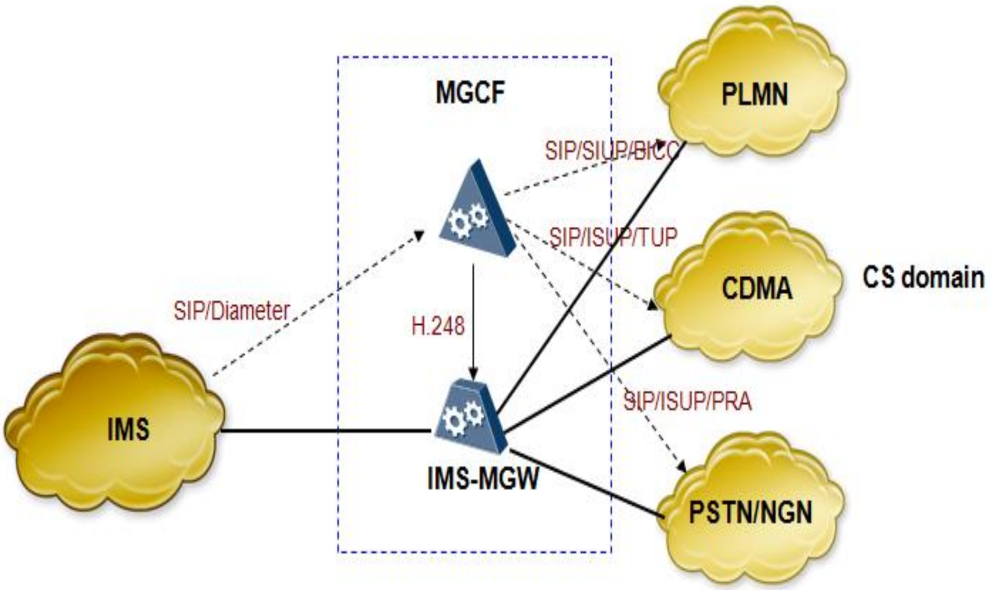


Figura 41: Função do elemento MGCF.
Fonte: Huawei (2010).

5.3.7.1.5 MRFC – *Multimedia Resource Function Controller*

Executa as seguintes funções:

- Controla os recursos de fluxo de mídia no MRFP;
- Interpreta informações vindas de um AS e S-CSCF e controla o MRFP adequadamente.

O MRFC em conjunto com um MRFP (*Multimedia Resource Function Protocol)* que está localizado na camada de transporte irá fornecer um conjunto de recursos de mídia para serviços de apoio, por exemplo, anúncios de número inexistente, bloqueios, ativações e desativações de serviços suplementares.

5.3.7.1.6 MRFP – *Multimedia Resource Function Processor*

Executa as seguintes funções:

- Fornece os recursos a serem controlados pelo MRFC;
- Mistura fluxos de mídia entrantes (conferência);

– Processa fluxos de mídia (codificação de áudio, análise de mídia).

5.3.7.1.7 IM-MGW – *IMS Media Gateway Function*

Efetua a terminação de canais portadores da rede de comutação de circuitos e fluxos de mídia de uma rede de pacotes. Faz adaptação do tráfego das redes legadas para a camada de transporte IP.

5.3.7.1.8 HSS – *Home Subscriber Server*

Procede da seguinte forma:

- Identificação de usuário, informação de numeração e endereçamento;
- Informação de controle de acesso de rede para autenticação e Autorização;
- Informação de localização do usuário em sistemas móveis;
- Informação de perfil de usuário (IFC).

Uma das grandes vantagens do HSS é a centralização dos dados. Além disso, o HSS é capaz de gerenciar múltiplas identidades para um mesmo assinante.

6.3.7.1.9 SLF – *Subscription Locator Function*

Quando um operador tem mais de um HSS o SLF é usado para selecionar o HSS correspondente, normalmente o SLF é combinado com o HSS. Uma consulta ao SLF recebe o endereço de usuário como entrada e retorna em qual HSS estão às informações daquele usuário como saídas.

Existem também outros elementos de rede que atuam na camada de acesso e portadora, cujas funções estão descritas abaixo:

- Controle de recursos: PCRF (*Policy and Charging Rules Function*) e SPDF (*Service Based Policy Decision Function*), também conhecidos como RACS (*Resource and Admission Control Subsystem*);
- Controle de acesso: NACF (*Network Access Control Function*) e CLF (*Conectivity Location and repostory Function*), também conhecido como NASS (*Network Attachment Subsystem*);
- *SBC (Session Border controler)*: ABGF (*Access Border Gateway Function).*

5.3.7.2 PCRF/SPDF

Realiza a função de controle de *QoS* na rede IMS.

Segundo Bea (2006), tais elementos Autorizam e fazem a gerência dos recursos de qualidade e serviço, sobre os planos de mídia e meios de comunicação.

O SPDF pode ser integrado com o P-CSCF ou pode ser implementado como uma unidade separada. O SPDF controla e monitora os pacotes do tráfego IP da rede. Ele mede a capacidade e faz os ajustes necessários para aumentar a taxa de transmissão, diminuir os atrasos e os erros. Com isso, os usuários podem ter diferentes níveis de *QoS* para diferentes tipos de serviços.

5.3.7.2.1 NACF/CLF

Atua como DHCP (*Dynamic Host Configuration Protocol*) e função de servidor AAA (*Authentication, Authorization and Accounting)* para acesso a usuário da rede fixa.

5.3.7.2.2 DNS/ENUM (*Electronic Numbering*)

DNS (Domain *Name System*) é responsável por traduzir URL (*Uniform Resource Locator*) para endereço IP para roteamento da sessão.

ENUM (E. 164 *Number* URI *Mapping*) é usado para traduzir o telefone URI para SIP URI.

5.3.7.2.3 SBC – *Session Border Controller*

Procede as seguintes ações:

- Realiza funções tais como: NAT transversal; segurança; conversão IPv4/IPv6;
- *Proxy* de mídia, controle de *QoS* na rede fixa e segurança.

Por fim, outro elemento também importante na arquitetura é o CCF (*Charging Collection Function),* cuja função é receber informação de tarifação das chamadas de vários elementos, uni-las e disponibiliza-las à medição.

5.3.7.2.4 Pontos de referência da rede IMS

A figura abaixo fornece uma visão geral das entidades funcionais que compõe o IMS assim como os pontos de referência entre elas. Tais pontos são considerados *interfaces* lógicas que especificam o protocolo e relação de conectividade entre os elementos. Através dessa especificação, por exemplo, podemos restringir a coleta de mensagens entre determinados elementos para efeito de análise de falha. Por exemplo, o ponto de referência CX relaciona a conexão entre o I-CSCF e S-CSCF ao HSS, e o protocolo utilizado nessa comunicação é o *Diameter*.

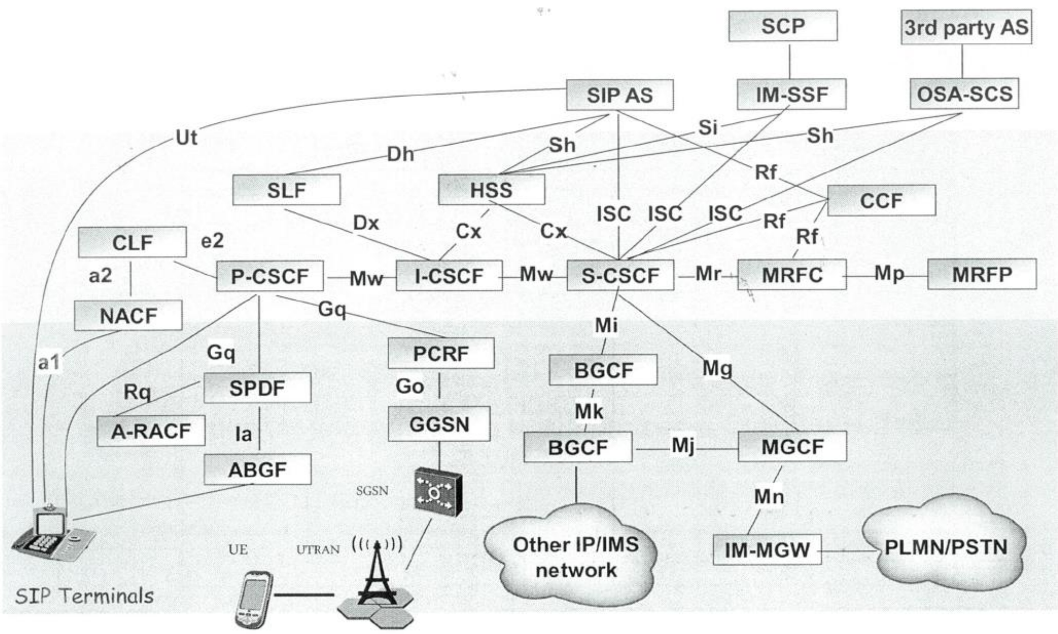


Figura 42: Pontos de referência entre elementos da arquitetura IMS.
Fonte: Huawei (2010).

5.3.7.2.5 Processo de registro em uma rede IMS

Para o registro do usuário IMS é necessário à descoberta do *proxy* ao qual será enviada a solicitação, sendo que essa descoberta pode ser feita por modos:

- Procedimento GPRS (terminais móveis): através desse procedimento o IP do *proxy* é descoberto via GGSN (*Gateway GPRS Support Node*);
- DHCP/DNS: através desse procedimento o servidor DHCP pode fornecer IP/nome de domínio do *proxy* enquanto designa IPs dinâmicos;
- Ajuste de configuração estática no terminal do usuário.

O usuário somente pode efetuar qualquer solicitação de serviço após estar registrado, com exceção de chamadas de emergência. A autenticação é um método usado para identificar um usuário e garantir a validade do mesmo.

De forma resumida, o processo de registro inicia-se com o envio de uma mensagem SIP (*Register*) ao *proxy*, este por sua vez encaminha ao elemento I-CSCF que consulta o HSS sobre qual S-CSCF poderá atender a requisição.

De posse da informação consultada ao HSS o I-CSCF encaminha a solicitação de registro ao S-CSCF designado que consulta o HSS com relação aos dados de autenticação do usuário em questão.

De posse dos dados de autenticação do usuário, o S-CSCF roda um algoritmo e armazena a resposta e na sequência retorna uma mensagem SIP 401 ao originador da requisição.

O originador, após receber tal resposta, utiliza os dados de autenticação recebidos, roda também um algoritmo e gera uma nova mensagem SIP (*register*), ao qual será recebida pelo S-CSCF e comparada ao dado armazenado, caso seja semelhante o usuário é registrado. Esse processo de registro garante confiabilidade ao processo de acesso do IMS.

Segue figura mostrando o processo de requisição inicial e a segunda mensagem contendo os dados codificados para comparação.

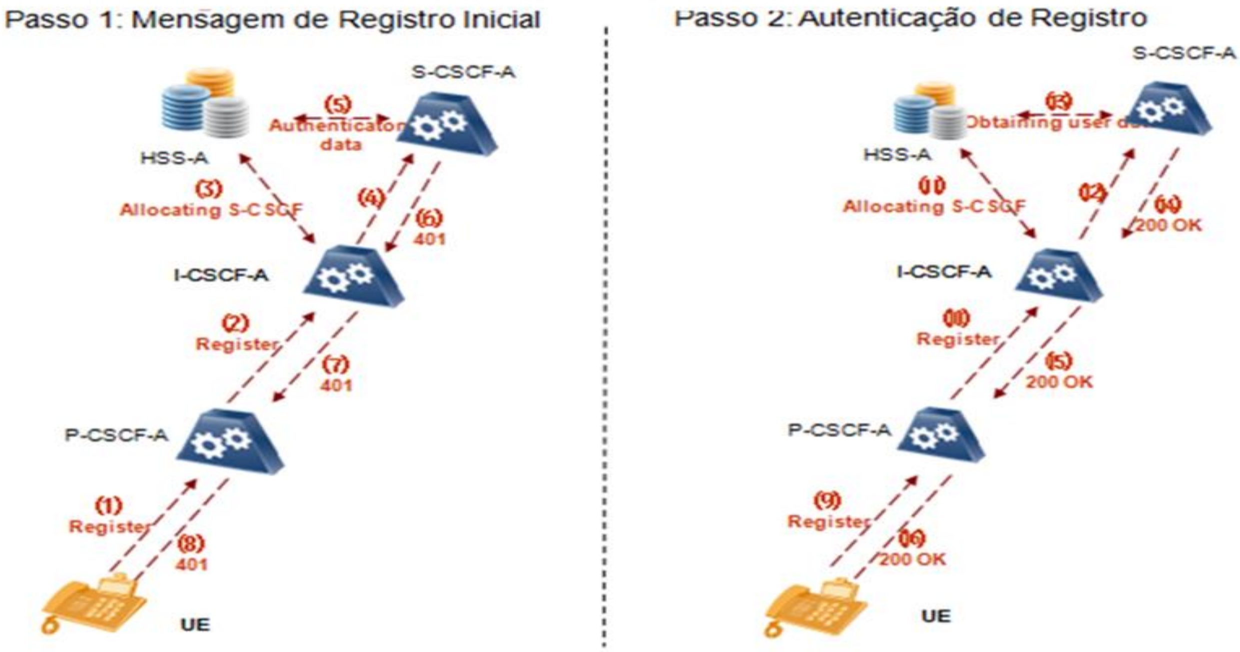


Figura 43: Processo de registro de usuário IMS.
Fonte: Huawei (2010).

5.3.7.2.6 Processo de estabelecimento de sessão IMS-MS

1 - Usuário (UE) obtém o endereço do *proxy* via procedimento de descoberta do P-CSCF;

2 - Após descoberta do *proxy* é enviado uma mensagem de registro (*Register*) com destino ao mesmo, este encaminha para o I-CSCF que interroga o HSS para descobrir qual S-CSCF tratará a requisição;

3 - Após designação do S-CSCF, o I-CSCF encaminha a solicitação de registro ao mesmo que efetua nova consulta ao HSS, sendo que essa se refere à check dos dados de autenticação;

4 - O HSS consulta os dados encaminhados em sua base e retorna as informações ao S-CSCF que roda um algoritmo sobre a mesma, armazena o resultado e encaminha os dados originais recebidos do HSS numa reposta SIP 401 enviada ao originador;

5 - O originador ao receber a resposta SIP 401, roda um algoritmo na informação de autenticação recebida e encaminha uma nova mensagem *register*. Os dados dessa são comparados ao chegar no S-CSCF com os dados armazenados inicialmente, caso haja semelhança o usuário é registrado;

6 - Após o registro o S-CSCF baixa os dados de assinatura do usuário e dispara o registro em outros servidores de aplicações, caso necessário;

7 - A partir desse momento o usuário esta apto a usar os serviços da rede IMS;

8 - Caso a sessão seja de usuário IMS para outro usuário da mesma rede ou de outra rede IMS (IMS-IMS), uma mensagem *invite* é encaminhada ao P-CSCF já descoberto. O P-CSCF encaminha esta requisição ao S-CSCF obtido no processo de registro;

9 - O S-CSCF analisa os dados de B em conjunto com outros elementos (AS/ENUM) e valida se o usuário de destino pertence a uma rede IMS ou a PSTN, neste caso considera-se que o usuário B pertence à outra rede IMS;

10 - Depois de validado que o usuário B é de outra rede IMS a requisição *invite* é enviada ao I-CSCF da outra rede, que consulta do HSS de sua rede para descoberta do S-CSCF;

11 - Após descoberto o S-CSCF, o I-CSCF encaminha a requisição ao mesmo. De posse da requisição o S-CSCF a encaminha ao P-CSCF, sendo que este envia a mesma ao chamador;

12 - A partir do recebimento do *invite* pelo usuário de destino tem-se a troca de mensagens SIP passando por esses mesmos elementos mencionados até que o usuário A e B estejam trocando mídia entre eles.

Abaixo segue figura para melhorar ilustrar os passos citados acima.

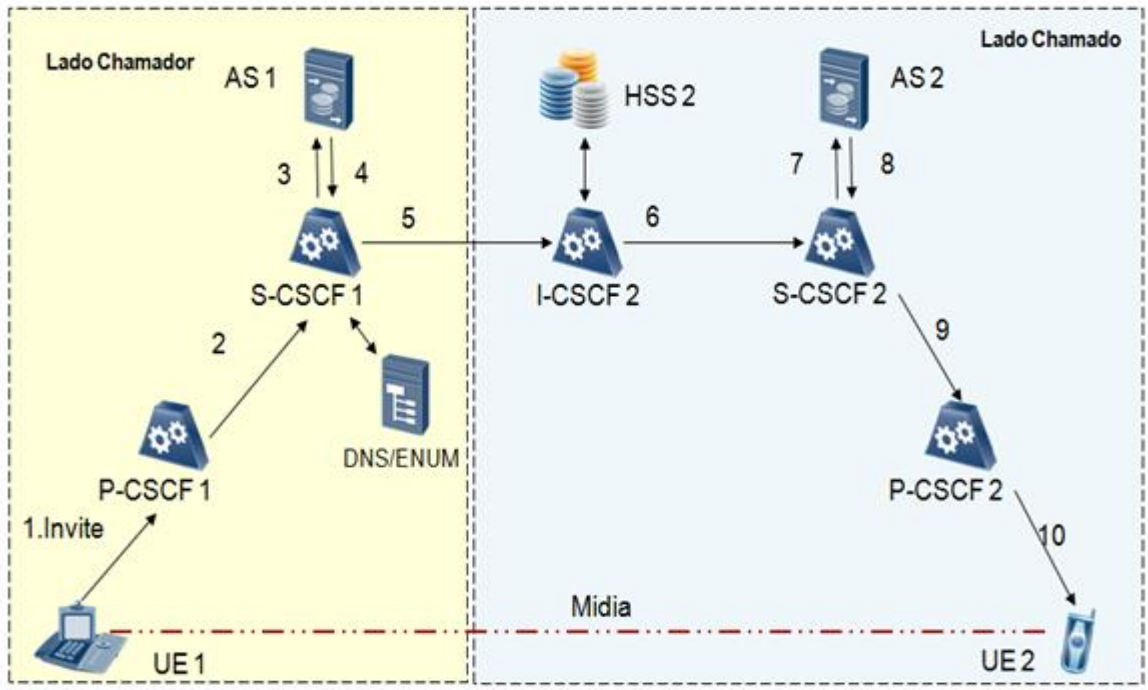


Figura 44: Processamento de chamadas IMS-IMS.
Fonte: Huawei (2010).

6.3.7.2.7 Processo de estabelecimento de sessão IMS-PSTN

1 - Caso a chamada tivesse destino um usuário da rede PSTN, a diferença se iniciaria a partir do passo 8 citado mais acima;

2 - Nesse caso, após o *invite* chegar ao S-CSCF, o numero de B seria normatizado, verificado junto ao ENUM, e em caso de resposta negativa o S-CSCF seria notificado com resposta de erro encaminhando o *invite* para o BGCF;

3 - O BGCF analisaria para qual MGCF a requisição seria enviada. Após a análise o BGCF encaminha o *invite* ao MGCF correspondente que controlará o *media gateway* que fará a interconexão com a rede comutada (PSTN);

4 - O MGCF também enviará mensagens SS7 à rede PSTN para solicitar reserva de recurso e desconexão de circuito;

5 - Após recebimento das mensagens SS7 a PSTN sinaliza o usuário B para completamento da chamada;

6 - Após o completamento da chamada um circuito é reservado entre a PSTN e o *media gateway*, sendo que por este ocorrerá um fluxo TDM. Já entre o *media gateway* e a origem ocorrera um fluxo de pacotes. A função do *media gateway* e fazer essa ponte entre a rede de pacotes e a rede de circuito, efetuando a conversão da mídia, aplicação de *codecs,* supressão de silêncio e cancelamento de eco quando necessário.

A figura a seguir ilustra os passos citados acima:

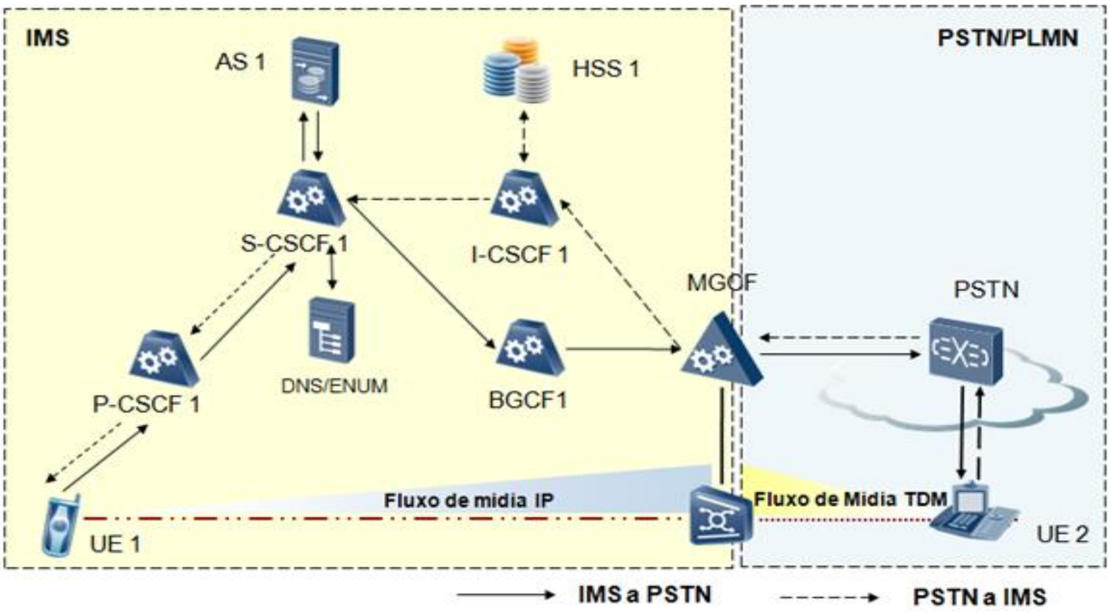


Figura 45: Processamento de chamada IMS-PSTN e PSTN-IMS
Fonte: Huawei (2010).

5.3.7.2.8 Implementação de *QoS* no IMS

O IETF definiu duas abordagens bem conhecidas para a solução de *QoS* na camada IP, o modelo de integração de serviços *(IntServ*) e o modelo de serviços diferenciados (*DiffServ*), além do que recentemente foi proposto um novo modelo que permite o uso de *intserv* sobre domínios *diffserv*.

Segundo Nobôa (2012), duas estratégias são consideradas para providenciar um bom nível da *QoS* em redes de pacotes, o primeiro envolve evitar o congestionamento.

Isso pode ser feito através da implementação do CAC (*Connection Admission Control*), reservando recursos ou simplesmente superdimensionado a rede (*over-provisioning*), um exemplo da *QoS* baseado na reserva de recursos é a integração de serviços (*IntServ*).

O segundo método seria o gerenciamento de congestionamento. A diferenciação para providenciar melhor *QoS* seria simplesmente conceder o melhor serviço para os fluxos mais importantes, um dos padrões mais conhecidos usando esse método seria o *diffserv.*

Com relação ao gerenciamento da *QoS* podemos destacar dois tipos, o primeiro focado no provisionamento garantido da *QoS* enquanto o outro é focado em *QoS* relativo.

No garantido com *delay* ou perda de taxas pode ser providenciado pelo esquema de reserva de recursos, na *QoS* relativo pode ser implementado por diferenciação de tráfego.

As redes IMS suportam ambos o controle de admissão e diferenciação da *QoS.*

5.4 PROTOCOLOS

O IMS é baseado em protocolos da *Internet,* que são basicamente o SIP, *diameter* e o RTP, separando de forma clara o transporte de dados, o controle de sessão e as aplicações lógicas. O COPS (*Common Open Policy Service*) e o H.248 também fazem parte da arquitetura. O IMS utiliza o protocolo SIP para o controle e sinalização das sessões (relacionados na arquitetura como CSCFs).

As relações de autenticação, Autorização e contabilidade são baseadas no protocolo *diameter* do IETF e é executado no HSS.

O RTP é outro protocolo importante nas aplicações multimídias, este protocolo ira prover a entrega fim-a-fim de dados em tempo real.

Além disso, o IMS utiliza o IPv6 como protocolo de rede, mas mantém compatibilidade com o IPv4.

Exibiremos a seguir as principais características de cada um desses protocolos, fundamentais a operação da rede.

5.4.1 RTP - *Real-time Transport Protocol*

O protocolo de tempo real RTP (*Real Time Trasport Protocol*), é definido na RFC 3550, usando outro protocolo para controle, o RTCP *(Real Time Control Protocol),* também definido na mesma RFC e ambos rodam comumente sobre o UDP *(User Datagram Protocol).*

O RTP anexa campos de cabeçalhos às informações de áudio/vídeo antes de repassá-las ao destinatário, isso porque muitas aplicações utilizam uma numeração de sequência e também marcas de tempo, além de outras informações que podem ser úteis, principalmente para sincronizar os dados na recepção.

Segundo Kurose (2006), basicamente, o RTP encapsula uma parte da mídia, som ou vídeo, por exemplo, dentro de um pacote RTP, isso no lado do remetente, e depois encapsula outra vez, só que dentro de um *socket* de *interface* UDP, onde é encaminhado para o IP.

Do lado do destinatário, o pacote RTP é extraído do pacote UDP e depois a parte da mídia é extraída do pacote RTP, sendo então encaminhada para a aplicação para ser decodificada e apresentada.

Como o RTP trabalha com UDP (*User Datagram Protocol*), com a explicação simples mostrada acima, pode-se deduzir que o RTP não garante nenhuma entrega de pacotes, ordem na entrega (*Sequencial Number*), e muito menos oferece mecanismos para isso. Além disto, não fornece garantias de qualidade de serviço *(QoS).*

Além disso, os pacotes RTP não são limitados às aplicações ponto-a-ponto (*unicast)*, podendo ser de um-para-muitos ou de muitos-para-muitos, estabelecendo assim uma sessão *multicast.*

Dentre os cabeçalhos do RTP, podemos destacar quatro:

- Campo de carga útil com 7 bits de comprimento pode ser usado para indicar o tipo de codificação da mídia, áudio ou vídeo, por exemplo;
- Campo do número de sequência tem comprimento de 16 bits, cada pacote enviado pelo remetente é incrementado de uma unidade. Este campo é utilizado para sincronizar os pacotes recebidos pelo destinatário;
- Campo de marca de tempo - possui um comprimento de 32 bits. O relógio de marca de tempo é incrementado em uma unidade de acordo com o período de amostragem da mídia, e pode ser usado para amenizar o atraso ocasionado pela rede e melhorar a sincronização;
- Identificador de sincronização da fonte com 32 bits identifica a fonte da corrente através de um número aleatório, geralmente cada fonte de uma

sessão RTP possui seu próprio identificador (KUROSE, 2006).

5.4.1.1 SIP - *Session Initiation Protocol*

O protocolo de inicialização de sessão SIP (*Session Initiation Protocol*), definido no RFC 3261, é um protocolo de controle da camada de aplicação, que cria, modifica e encerra uma sessão com um ou mais participantes, os quais podem entrar e sair de sessões existentes.

Conforme o IETF (RFC 3261), as sessões incluem chamadas telefônicas na *Internet*, distribuição de multimídia e conferências multimídia. O SIP tem cinco funções de sessão, que são configuração, gerenciamento, finalização, localização e capacidade.

O SIP basicamente:

- Oferece os mecanismos necessários para que seja estabelecida a comunicação entre dois agentes em uma rede IP, ou seja, permite que um interlocutor chame o outro, que por sinal pode aceitar ou não a chamada, e permite que ambos possam finalizar a sessão;
- Permite que os participantes da sessão concordem com a codificação da mídia;
- Provê mecanismo para o requisitante determinar o IP do requisitado, pois os usuários normalmente não têm um IP fixo, e sim dinâmico, usando DHCP;
- Oferece mecanismos para gerenciar chamadas, como por exemplo, adicionar novos recursos, novos participantes, alterar a codificação da mídia e transferir chamadas, sem que a mesma seja perdida, ou seja, numa mesma chamada.

O SIP em si não oferece serviços, é um componente que pode ser integrado com outros protocolos para prover uma arquitetura completa de multimídia. Tais protocolos podem ser o RTP, H.248 ou o SDP.

O SIP deve ser usado em conjunto com outros protocolos para oferecer um serviço completo para o usuário, mas sua funcionalidade não depende de nenhum desses protocolos.

O Protocolo SIP possui um conjunto de métodos (mensagens de sinalização), que permitem iniciar ações (convidar um usuário para uma chamada registrar-se, entre outros). As trocas de mensagens SIP utilizadas para registrar um usuário ou para iniciar, terminar ou modificar uma sessão são designadas por transações.

Uma sessão SIP corresponde à chamada tradicional entre dois usuários.

Uma transação SIP é constituída por um pedido seguido de uma ou mais respostas informativas, e por uma ou mais respostas finais. Para estabelecer uma sessão SIP é necessário enviar um método específico (*invite*) ao destinatário. O pedido pode ter que passar por um *proxy server* que encaminha o pedido para o destinatário caso a mesma pertença ao seu domínio ou para outro SIP *server* caso o destinatário seja de um domínio diferente.

O *Proxy server* responde imediatamente ao emissor com o envio de uma resposta informativa (*TRYING*), somente quando o usuário atender, o dispositivo envia um sinal indicando o estabelecimento de chamada (*OK*), esta passa pelo caminho inverso ao do método *invite*.

Para finalizar a transação de estabelecimento de chamada, a origem envia um *ACK* que será encaminhado pelo mesmo caminho que o do *invite*.

O transporte das mensagens SIP pode ser feito quer através do protocolo *Transmission Control Protocol* (TCP) ou *User Datagram Protocol* (UDP).

Caso seja utilizado o protocolo UDP existe um comportamento adicional de forma a garantir a recepção das mensagens no destino, sendo necessário repetir o envio das mensagens até chegar uma resposta de recepção.

As respostas informativas também podem ser confirmadas pelo receptor, e será usada para isso a mensagem de (*PRACK)*, esta mensagem é enviada quando a mensagem de resposta informativa transporta explicitamente o pedido de confirmação.

Uma alternativa para o SIP é o H.323, que é um padrão para áudio e videoconferência entre sistemas finais na *Internet*.

O H.323 é um protocolo completo, que é integrado com outros protocolos, já o SIP aborda apenas sinalização e gerenciamento de sessão, é um componente separado, que não precisa de nenhum outro protocolo para funcionar.

Além disso, o H.323 vem da ITU (*International Telecommunication Union*) (telefonia), enquanto que o SIP vem da IETF *(Internet Engineering Task Force) (Internet)*.

A figura abaixo mostra um exemplo típico de troca de mensagens SIP entre dois usuários, Bob e Alice. Bob envia um convite e uma mensagem M (que contém um conjunto de parâmetros necessário para estabelecer a comunicação, como o endereço, cabeçalhos e tipo de mídia) para Alice, que aceita a chamada e envia sua resposta, quando Bob recebe a resposta de Alice, envia um *ACK* e a sessão é estabelecida. Após um período de transferências, Alice envia uma requisição para finalizar a sessão, Bob recebe e encerra a sessão.

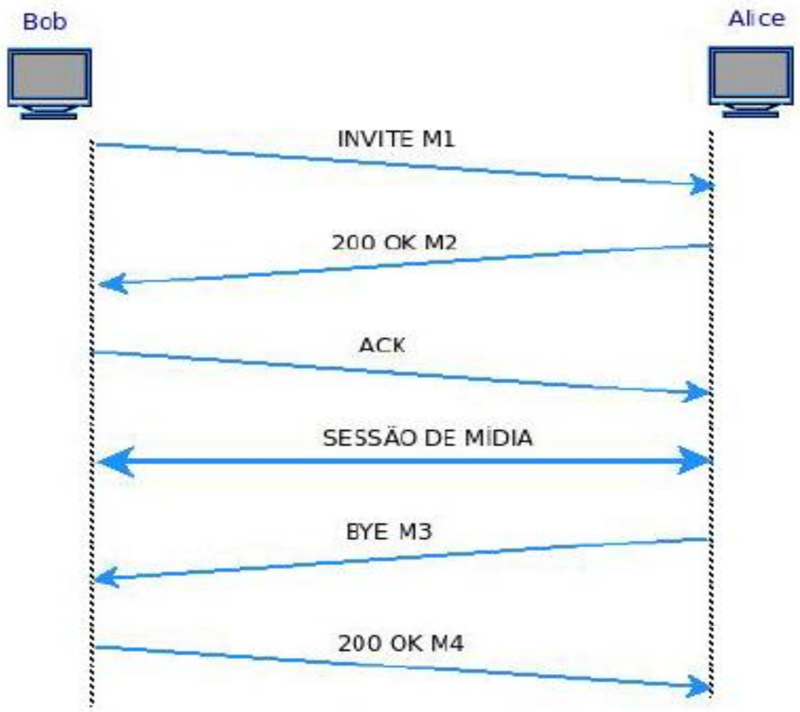


Figura 46: Troca de mensagens SIP.
Fonte: Macapuna (2008).

A troca de mensagens da figura anterior é uma visão simplificada da inicialização de uma sessão, onde poderão existir mais componentes envolvidos dentro da estrutura da rede SIP. Esses componentes são os servidores *proxy*, *redirect*, registrar e *location server*.

5.4.1.2 Componentes SIP

User Agent (UA) – Corresponde ao equipamento terminal SIP do usuário e integra como componente SIP o *User Agent* (UA) que inicia ou aceita as chamadas.

Recebe e envia pedidos de forma a estabelecer sessões, ou seja, comporta-se como um *User Agent Server* (UAS) ou como um *User Agent Client* (UAC), respectivamente.

Proxy Server – O *proxy server* recebe os pedidos dos UAC e encaminha-os de acordo com o *request* URI (URI contido no cabeçalho do método SIP), e alguns outros cabeçalhos. O *proxy server* encaminha o pedido SIP para o domínio a que pertence o utilizador chamado.

Redirect Server – Um *redirect server* recebe o pedido, mas não emite nenhum pedido. Sempre que recebe um pedido responde com uma mensagem 3xx.

Esta mensagem contém uma ou mais localizações do usuário destinatário.

Location Server – O *location server* é usado pelo *registration server* para localizar o usuário chamado, bem como guardar informação dos usuários registrados.

Registration Server (SIP REGISTRAR) – O *location server* é atualizado através do *registration server*. Quando um usuário fica ativo num terminal envia para o servidor *registration server* uma mensagem de registro onde é transportada a informação da sua localização atual e do respectivo período de validade. Este servidor autentica o usuário e registra a sua localização e período de validade do registo no *location server*. São os procedimentos de registo que permitem a mobilidade dos usuários na rede SIP.

Back 2 *Back User Agent* (B2BUA) – Um B2BUA é uma entidade lógica que recebe pedido, processa-os como um UAS, com o objetivo de determinar como um pedido deve ser respondido, atua como um UAC e gera pedido.

Um B2BUA tem de manter estado das chamadas e participar ativamente no envio de pedidos e respostas a diálogos nos quais se encontra envolvido (um diálogo representa uma relação ponto-a-ponto entre dois *user agents* que se mantém por algum tempo).

Um B2BUA possui maior controle sobre uma chamada que um *proxy*, e pode, por exemplo, desligar uma sessão sem a intervenção dos usuários.

5.4.1.3 Mensagens SIP

O funcionamento do protocolo SIP baseia-se em métodos (mensagens de sinalização), que iniciam modificam e terminam sessões.

O quadro abaixo específica com mais detalhes esses métodos e suas ações.

INVITE	Inicia uma sessão, ou muda os parâmetros de uma sessão já existente (re-INVITE).
ACK	Enviado como confirmação a uma resposta final de um INVITE.
BYE	Terminação da sessão.
CANCEL	Cancelamento da sessão em estabelecimento.
REGISTER	Efetua o registro, ou deregistro do usuário.
OPTIONS	Indicação das capacidades disponibilizadas nos UA.
INFO	Envia informação durante uma sessão que não modifica o estado da sessão (por exemplo, dígitos DTMF gerados durante uma sessão).
PRACK	Confirmação de respostas provisórias
UPDATE	Permite o update de parâmetros de sessão não tendo impacto no estado do diálogo. Semelhante ao re-INVITE mas ao contrário do re-INVITE pode ser enviado sem que o INVITE inicial receba uma resposta final.
REFER	Este método indica ao receptor que tem de contactar uma terceira entidade usando a informação enviada neste pedido (usada na implementação de serviços suplementares conferência e transferência de chamadas).
SUBSCRIBE	Pedido de notificação de um evento (ex: recepção de e-mail, estado de presença)
NOTIFY	Notificação de um evento.
PUBLISH	Usado para publicar um estado. Similar ao REGISTER pois permite que o usuário crie, modifique e remova estados numa entidade que gere esses estados pelo mesmo.
MESSAGE	Usado para envio de conteúdo sobre a forma de texto no corpo da mensagem.

Quadro 1: Descritivo dos métodos utilizados pelo SIP.

Para cada método recebido, o destinatário pode responder com respostas pertencentes a um conjunto de seis classes. A resposta é identificada por um identificador da mensagem de três dígitos, onde o dígito das centenas identifica a classe.

O quadro abaixo relaciona as classes de respostas que podem ser enviadas e seu significado.

1xx	Provisória	Pedido recebido, continuando a processar o pedido. Ex: 100 Trying
2xx	Sucesso	O pedido foi recebido, identificado e aceito com sucesso. Ex: 200 OK
3xx	Redireccionamento	É necessária a realização de outras ações para processar completamente o pedido. Ex: 302 Moved Temporarily
4xx	Erro do Cliente	O pedido contem sintaxe errada ou não pode ser completamente atendido por este servidor. Ex: 404 Not Found.
5xx	Erro do Servidor	O servidor falhou ao servir um pedido aparentemente válido. Ex: 504 Server Time-out
6xx	Falha Global	O pedido não pode ser processado em nenhum servidor. Ex: 603 Decline

Quadro 2: Classes de respostas SIP.

5.4.1.4 H.248 – Megaco

O protocolo de controle de *gateways* GCP *(Gateway Control Protocol)* desenvolvido em parceria entre a ITU-T - ITU *Telecommunication Standardization*

Sector (com a designação de H.248) e o IETF (com a designação de Megaco) são usados entre o *softswitch* MGC (*Media Gateway Controller)* e o MG (*Media Gateway*), ou seja, é usado para controlar os recursos de voz, vídeo e multimídia num meio de comunicação fim-a-fim.

O MG converte diferentes formatos de mídias de diferentes tipos de redes, por exemplo, entre uma mídia de uma rede comutada por circuitos e uma mídia de uma rede comutada por pacotes (por exemplo, o RTP). Além disso, o MG é capaz de processar áudio, vídeo ou qualquer combinação *full duplex* (transmissão simultânea), como vídeo conferência, além de outras funções. O MGC (também conhecido como *Call Agent* (Agente de chamada)) controla as partes do estado da chamada que pertençam ao controle de conexão dos canais em uma mídia MG.

Segue exemplos de MG:

- *Trunking gateways, voice over ATM gateways, residential gateways*;
- *Access gateways, business gateways, network access server*.

Conforme o IETF (RFC 3425), algumas de suas características são:

- É um padrão aberto;
- É um protocolo mestre/escravo (*master/slave*), difere do SIP e do H.323, que são protocolos *peer-to-peer*;
- Apresenta interoperação com SIP e o H.323;
- Provê vantagens como redução de *overhead* das mensagens;
- É aplicável para todo tipo de rede de pacotes.

5.4.1.5 *Diameter protocol*

O *diameter* é um protocolo desenvolvido inicialmente pela IETF, padronizado na RFC 3588, e prove autenticação, Autorização e contabilidade AAA (*Authentication, Authorization and Accounting*) para uma gama de serviços na *Internet*, como acesso remoto, VPN (*Virtual Private Network*), *VoIP* e IP móvel.

Desenvolvido como alternativa para o Radius *(Remote Authentication Dial In User Service),* que não suporta de forma eficiente mobilidade e serviços *QoS.*

Além disso, oferece melhorias nas áreas de confiabilidade, segurança, escalabilidade e flexibilidade.

Segundo IETF RFC 3588, O *diameter* oferece as seguintes facilidades e vantagens:

- Confiável na camada de transporte (TCP ou SCTP);
- Camada de rede e transporte seguros (IP sec. ou TLS);
- Gestão de conexão e sessão;
- Autenticação de usuários e capacidade de negociação;
- Contabilidade de serviços básicos;
- Entrega confiável de AVP (*Attribute Value Pairs*) atributo de valor par;
- Extensibilidade, através de novos comandos AVPs.

O protocolo *diameter* consiste na troca de comandos AVPs entre clientes e servidores. Alguns comandos são utilizados no próprio protocolo, e outros são utilizados para dar suporte (oferecer dados associados) das aplicações que utilizam o *diameter* (IETF RFC 3588).

5.5 VANTAGENS REDE IMS

Podemos citar inúmeras vantagens da arquitetura IMS com relação às arquiteturas de redes legadas, tais como:

- Unificação da base de dados, toda a base de dados de todos os tipos de redes pode ser centralizada em um único elemento reduzindo custos adicionais e sobreposição de *hardware.* O IMS permite o compartilhamento de bases de dados de assinantes, autenticação, faturamento (tudo centralizado) e até os serviços de outros aplicativos. Consequentemente, isso vai incentivar e acelerar o desenvolvimento de aplicativos inovadores, além de reduzir os custos operacional e capital da distribuição de aplicativos. A rede legada apresenta baixa eficiência na administração de bases de dados. Frequentemente, cada plataforma de serviços requer sua própria base de dados de assinantes para provisionamento;
- Segregação bem definida entre a camada de controle e a camada de aplicação. Isso permite que novas aplicações sejam criadas de forma mais rápida e descomplicada;
- Com a arquitetura horizontal do IMS, as operadoras podem se afastar da tradicional implementação vertical de serviços que com sua funcionalidade específica de cobrança, presença, gestão de grupos e listas, roteamento e provisionamento, são muito caros e complexos para construir e manter. As implementações separadas de cada camada devem ser construídas para cada serviço das redes legadas, e a estrutura é replicada na rede inteira, a partir do terminal até o terminal do outro usuário, através da rede *core.* Em oposição a isso, o IMS oferece várias funções comuns com estrutura e implementações genéricas que podem ser reutilizadas por praticamente todos os serviços da rede;
- Uso de *interfaces* abertas e protocolos bem sucedidos. Protocolos como o SIP e o *diameter* garantem maior agilidade, flexibilidade e cobertura de novos cenários. Por exemplo, o SIP exige uma quantidade bem menor de mensagens para completar uma sinalização comparada ao H.323, isso o torna mais ágil e menos oneroso com relação à ocupação de banda. Outro ponto positivo do SIP é que ele possui campos que podem ser manipulados de acordo com a necessidade, garantindo flexibilidade em novas implementações. Outro ponto importante a citar é que devido à utilização de protocolos abertos o desenvolvimento de novas aplicações tornou-se menos complexo, ao contrário das redes legadas que utilizavam protocolos proprietários complexos como o CAP/INAP limitando e dificultando a implementação de novos serviços;
- Arquitetura de acordo com as tendências de desenvolvimento de rede, cuja rede é baseada em *software*, aplicada a convergência das redes fixas e moveis (FMC) e destinada à convergência gradual para *ALL*-IP.
- A maioria dos elementos que compõe a arquitetura são aplicações carregadas em *hardware* que atuam em modo *loadsharing* ou ativo/*standby*. Normalmente a redundância ou elemento que divide carga reside em *hardware* distinto, em caso de falha de um elemento o tráfego é comutado ou redistribuído permitindo assim que o serviço não seja afetado. Isso permite que se tenha um maior segurança operacional assim como facilita a implementação de uma redundância geográfica que garanta uma proteção ainda maior. Por exemplo, caso ocorra falha no HSS e esse não retorne uma consulta, o HSS da redundância geográfica pode ser consultado em segunda prioridade;

- Acesso independente: a camada de transporte faz a abstração das redes de acesso ao IMS, ou seja, independente se temos UMTS ou *Wi-Fi* como meio de acesso, para o IMS isso é transparente. Todos os dispositivos IMS poderão acessar os aplicativos IMS da mesma forma, não meras "traduções" ou "emulações" deles, que poderiam variar de um dispositivo para outro. Seja a partir de um telefone doméstico, terminal sem fio ou dispositivo móvel, o acesso e a operação dos aplicativos serão idênticos;
- Garantia de *QoS*, melhor controle de tarifação e facilidade de implementação de serviços inovadores, permitindo as operadoras oferecerem serviço de qualidade, identificação do tipo de serviço para uma tarifação mais adequada além da capacidade de provisão de serviços customizados. Por exemplo, uma das vantagens da IMS são as informações a respeito do tipo de serviço invocado pelo usuário. Com essa informação, a operadora pode determinar como cobrar seus usuários baseado no tipo de serviço (ou seja, podem optar por cobrar o usuário pelo numero de bits transmitidos, pela duração da sessão ou qualquer outro novo tipo de cobrança);
- Oferecimento de serviços *quadruple-play* (voz, dados, vídeo e mobilidade);
- Permite agregar novas experiências aos usuários e controlar a cadeia de lucro. As operadoras deixam se der apenas o caminho e passam a prover conteúdos diversificados;
- Novas tecnologias como o GPON (*Gigabit-capable Passive Optical Networks*) e o LTE (*Long Term Evolution*) permitem que as novas aplicações a serem oferecidas pelo IMS possam ser mais complexas, tornando o mundo digital mais atraente e empolgante. O usuário pode desfrutar de serviços convergentes melhorados;
- Conforme a Ericsson (2004), o IMS fornece um conjunto de funções comuns chamados *service enablers* que podem ser usadas por diversos serviços (por exemplo, grupo/lista de gerenciamento, presença, provisionamento, operação e gestão, faturamento...). Os *service enablers* reduzem os riscos associados com a criação dos novos aplicativos necessários para atrair e manter clientes. Isso faz com que a implementação do serviço seja muito mais fácil e mais rápida. Além disso, permite uma interação direta entre diversos serviços. Este é um considerável avanço em relação à maioria das arquiteturas utilizadas atualmente de característica vertical na implementação do serviço. A rede legada apresenta baixa interação entre plataformas de serviços;
- Disponibilização dos serviços em *roaming*. A arquitetura IMS permite que todos os serviços estejam disponíveis independentes da localização do usuário. Um dos maiores problemas das tecnologias celulares atuais é que alguns serviços não estão disponíveis quando os usuários estão em *roaming*. O IMS usa tecnologias e protocolos da *Internet* para permitir *roaming* dos usuários que continuam, dessa forma, podendo executar serviços que executariam em suas redes locais;
- Os custos com a rede de transporte sofrerão uma redução significativa com a migração de canais de comutação de circuitos para comutação de pacotes (infraestrutura IP);
- Além destas vantagens, as redes IMS podem trazer as operadoras um aumento da simplicidade de operação e manutenção das redes dado que

os sistemas de gestão, provisionamento e tarifação são comuns a todas as redes.

Abaixo figura comparando a arquitetura legada com a rede IMS

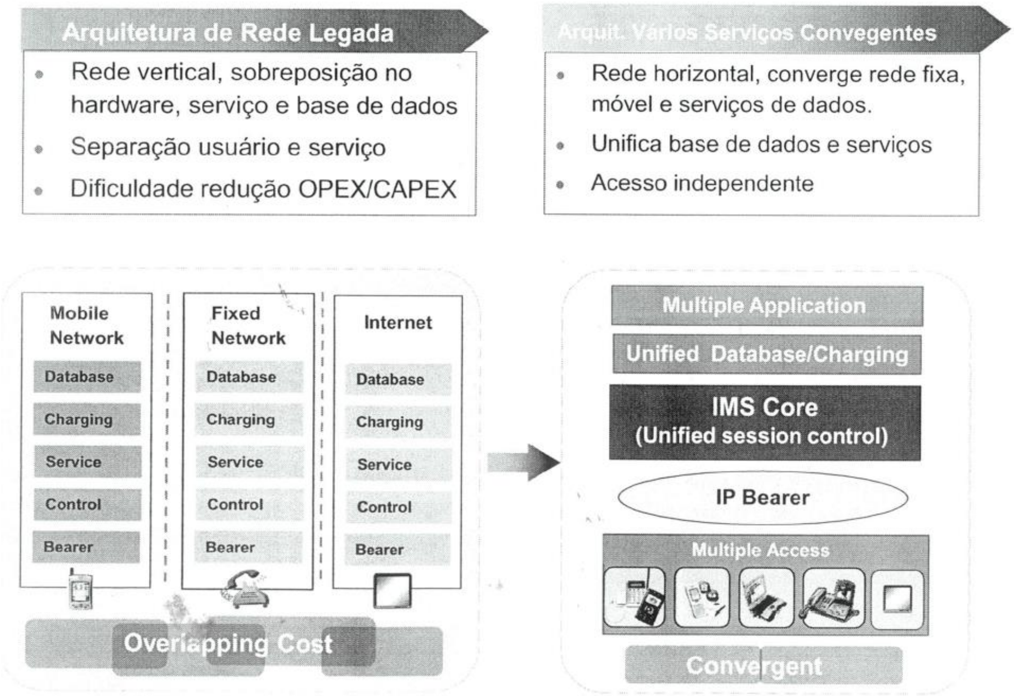


Figura 47: Comparativos das arquiteturas: rede legada X IMS.
Fonte: Huawei (2010).

A figura seguinte nos mostra a clara sobreposição de recursos nas redes estruturadas verticalmente. Cada rede possui sua base de dados, camada de controle e tarifação, serviços independentes e sem nenhum compartilhamento de dados, acessos exclusivos entre outros pontos que tornam esse modelo inviável.

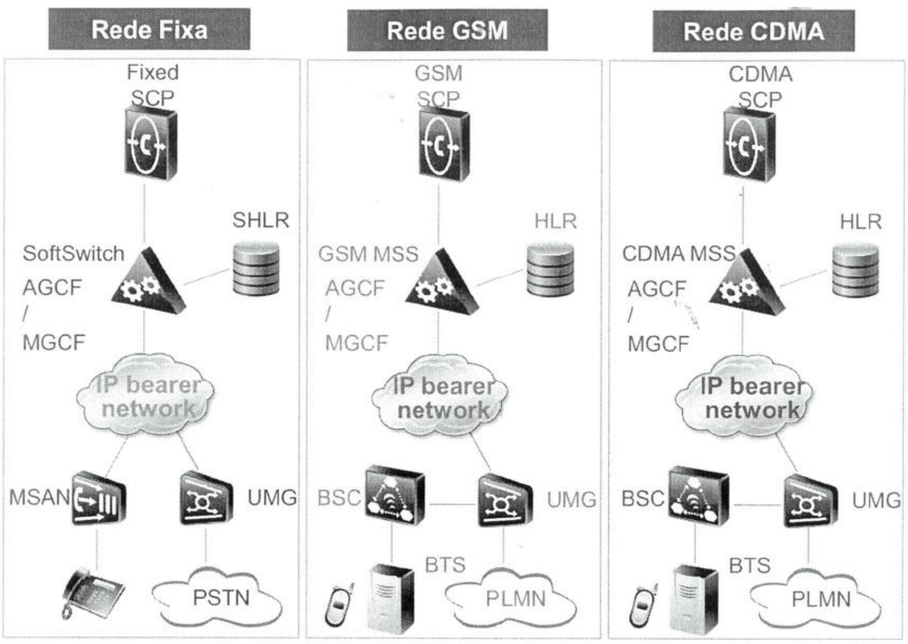


Figura 48: Sobreposição de funções nas arquiteturas de redes verticais.
Fonte: Huawei (2010).

Outro ponto a se observar na figura acima é a segmentação da camada de controle da camada de serviço via SCP. O SCP utiliza protocolo CAP/INAP, sendo os mesmos tão complexos que os provedores de serviço são limitados e um novo serviço é difícil de implementar.

A figura a seguir mostra as redes verticais da figura anterior sendo convergida para a arquitetura IMS. Percebe-se um controle único, compartilhamento de serviços e de dados utilizados pelo mesmo além da independência do acesso.

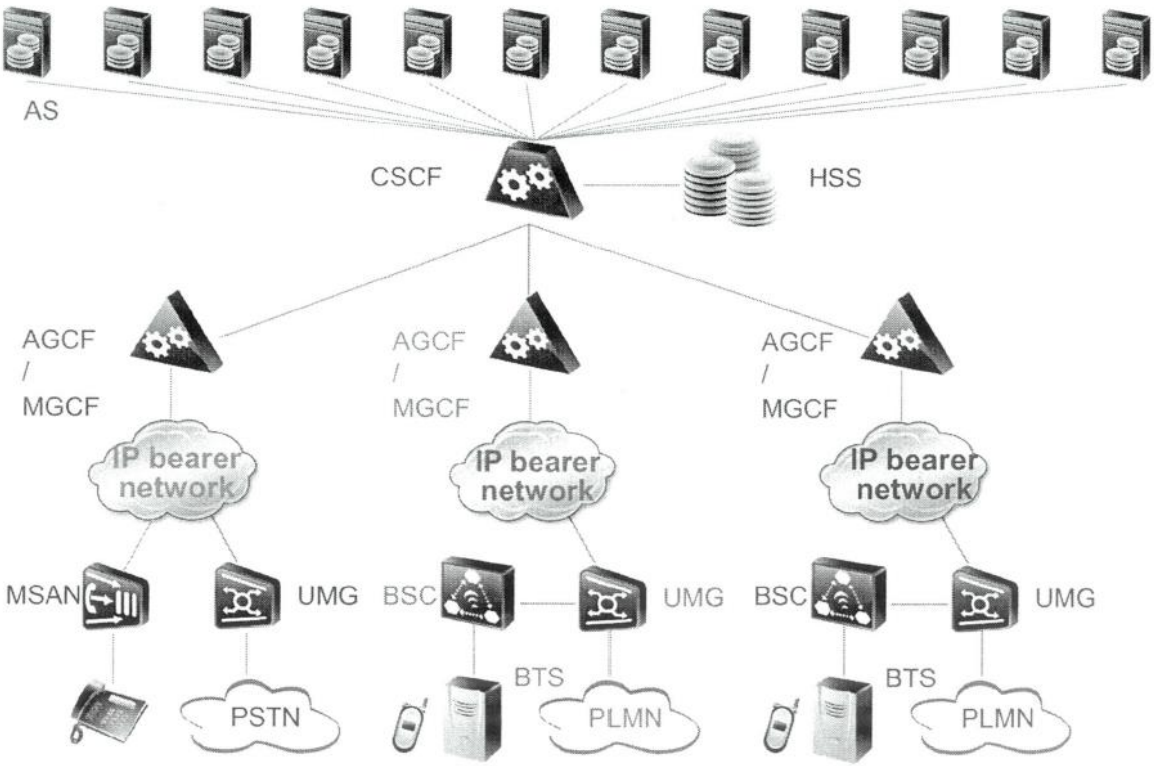


Figura 49: Arquitetura IMS convergindo redes verticais legadas.
Fonte: Huawei (2010).

5.6 BENEFÍCIOS DO IMS

Com a implementação do IMS é esperado vários benefícios, tanto para as operadoras quanto para os clientes finais, sendo estes a motivação para a implantação dessa nova arquitetura.

Segundo Livingston (2004), "[...] a IMS traz múltiplos benefícios para operadoras de redes e o usuário final com novos aplicativos e uma experiência melhor [...]", disse Chris Pearson, Presidente da 3G Américas.

> As operadoras que adotam a IMS nessa etapa inicial devem ganhar vantagens competitivas. Além de reduzir os custos operacionais, a IMS permite que as operadoras escolham os melhores componentes de vendas para as suas necessidades específicas. A infraestrutura de IMS também oferece *interfaces* abertas e padronizadas para o desenvolvimento de aplicativos de terceiros, no intuito de criar conjuntos atrativos e sofisticados de serviços de multimídia [...]. (LIVINGSTON, 2004).

Em linhas gerais podemos apontar os benefícios para operadoras e clientes da seguinte forma:

Para as operadoras:

- Os principais benefícios obtidos pelas operadoras com a implantação de redes IMS é o aumento da receita obtida através de novos serviços e redução do *CAPEX/OPEX*. A criação de novos serviços multimídia poderão ser desenvolvidas e entregues em um curto espaço de tempo, reduzindo drasticamente o custo de suporte e desenvolvimento das aplicações. O IMS permite a criação de novos serviços que não eram possíveis anteriormente, ou poderiam ter sido muito caro e complexo de implementar;
- Novos serviços poderão ser desenvolvidos para uma única plataforma estando estes disponíveis através de múltiplas redes de acesso. Isso permitirá aumentar a fidelidade dos clientes, aumentar a base instalada e reduzir o *churn* (migração). O IMS permite misturar e combinar diferentes serviços para chegar a um novo serviço, otimizando o uso das informações;
- Ao implantar uma arquitetura de rede IMS, as operadoras podem reduzir a necessidade de construir várias redes ao ter que adicionar novos serviços, reduzindo os custos associados com a compra de novos equipamentos. Em longo prazo o IMS reduzirá os custos e complexidades de gerenciamento de vários elementos reduzindo as despesas operacionais.

Para os usuários finais:

- Com IMS, os usuários finais terão acesso a uma nova realidade digital, novos recursos aos quais estes nunca poderiam ter pensado. Tais benefícios incluem experiências multimídias mais ricas, possibilidade de *roaming*, novos serviços baseados em IP, gerenciamento de identidade simplificada, customização de facilidades, segurança e integração móvel-fixo-*Internet*.

5.7 APLICAÇÕES IMS

Muitas são as novas aplicações possíveis sobre a arquitetura IMS. De certa forma esse é um dos pontos forte da arquitetura, fornecimento de serviços inovadores que além de atender as necessidades dos usuários surpreendam os mesmos com uma nova realidade digital, além de é claro, fidelizar o mesmo e alavancar a cadeia de lucro das operadoras.

Segundo Braga (2011), a seguir estão listadas algumas aplicações suportadas pelo IMS:

- Atendimento de chamadas do aparelho fixo no móvel;
- Suporte a TV (mensagens na TV ou ligações via TV);
- TV interativa: assistir um programa na TV, com interatividade, convidar outros usuários para assistir o mesmo programa (via *chat*), fazer conferência (voz, vídeo), *instant messaging*, etc;
- Transferência de conteúdo entre dispositivo: assistir vídeo no celular (comprar / baixar) e transferir para a TV o que foi comprado ao chegar à residência;
- Compra de conteúdo (com pedido de Autorização);
- Presença: utilização de um livro de endereços ativos (com status e localização), voz e vídeo chamadas;

- Videoconferências;
- Receber ligações no *desktop*: recebimento de ligações no *desktop* e depois transferi-la para o celular e vice-versa;
- Regra para encaminhamento: criar regras para encaminhamento de chamadas quando em reunião, almoço, praticando esportes, etc.;
- *Push-to-Talk* over celular (sistema de celular via rádio).

A figura abaixo aponta algumas das aplicações citadas anteriormente.

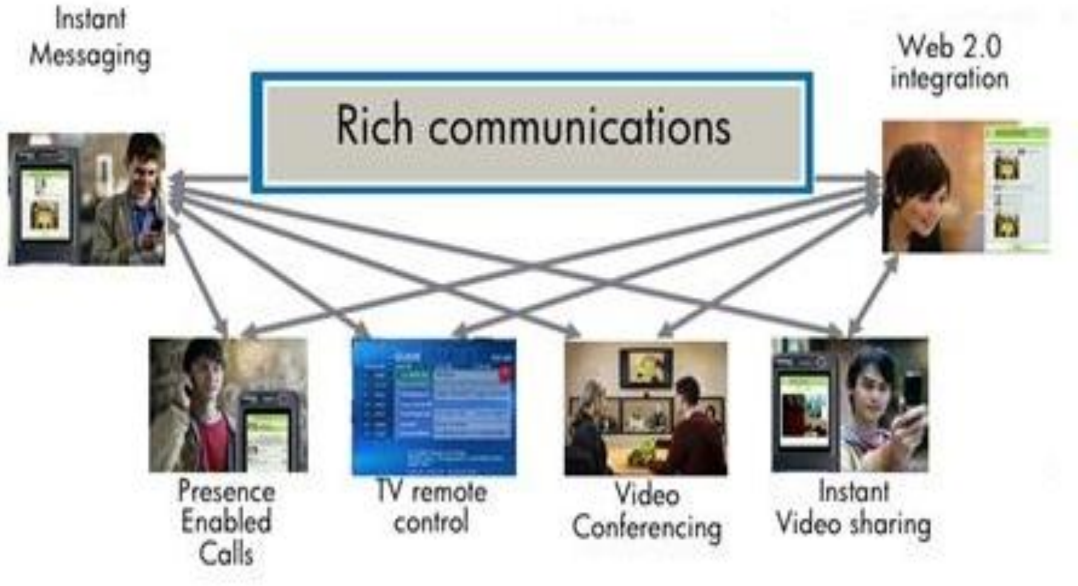


Figura 50: Exemplo de aplicações IMS.
Fonte: slideshare.net (2013).

5.8 OPERADORAS E FORNECEDORES PARA SOLUÇÃO IMS

Para que um sistema seja implantado com sucesso é necessário que as operadoras estejam dispostas a adquirir esta tecnologia e precisam conhecer fornecedores e produtos para a solução IMS.

5.8.1 Operadoras que aderiram ao IMS

Atualmente no Brasil tem-se informação que as operadoras GVT (*Global Village Telecom*), Brasil Telecom e Oi estão aderindo à nova arquitetura em suas redes.

Segundo (Huawei Telecom), em agosto de 2012, a China Telecom Fujian estreou seu serviço *SkyEye,* sobre sua rede IP *Multimedia Subsystem* (IMS) para monitoramento de vídeo móvel, por meio de sua linha de saída principal. Com a funcionalidade *plug-and-play*, nos dois sentidos porteiro, alarme do telefone, e reprodução de vídeo, este produto inovador estabelece uma base sólida para novos empreendimentos para a *Internet*.

Em 2011, o operador provincial começou o IMS *rollout,* uma migração de cerca de três milhões de assinantes TDM existentes para esta nova plataforma.

5.8.2 Fornecedores

Alguns fornecedores que disponibilizam a solução IMS podem ser vistos na sequência.

Segundo (McGarvey 2010), os 5 maiores fornecedores da solução IMS são:

- Alcatel-Lucent;
- Ericsson;
- Huawei;
- NSN and ZTE;
- Nokia Siemens Networks;

Nem todos podem fornecer a solução completa, visto que a mesma é composta por vários elementos. O único fabricante que informa possuir a solução completa é a Huawei (Huawei *Tecnologies Co.Ltd*).

A figura aponta alguns dos principais fornecedores de solução IMS.

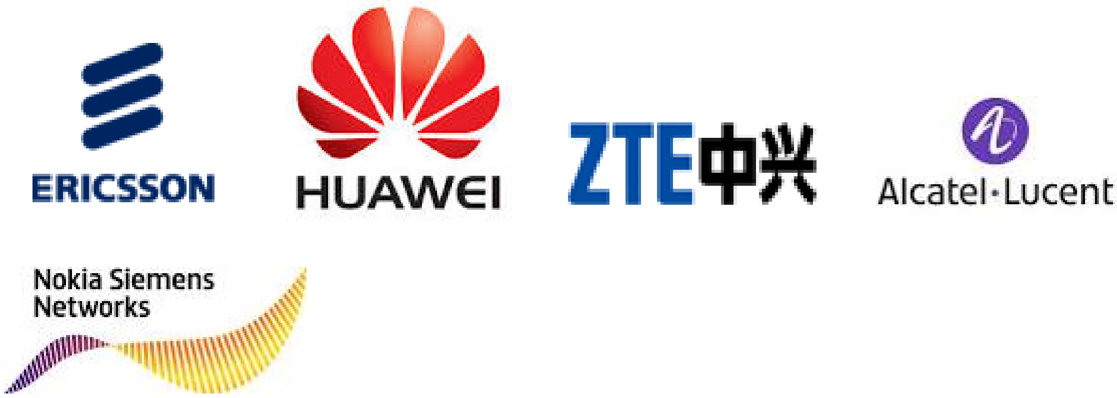


Figura 51: Fornecedores que comercializam elementos da solução IMS.
Fonte: Autor.

7 CONCLUSÕES E RECOMENDAÇÕES

As evoluções tecnológicas ao qual temos passado ao longo dos anos aliada as novas demandas dos usuários finais levaram ao desenvolvimento e disponibilização de vários serviços aos quais as operadoras poderiam aumentar sua base de assinantes assim como impulsionar seus rendimentos.

No entanto, devido às diferentes características de tráfego de cada serviço, foram criadas redes independentes para cada novo serviço oferecido.

Ao longo do tempo notou-se que essa diversidade de redes e padronizações seria inviável e tornavam complicada a redução dos custos de operação e manutenção assim como oferecimento de serviços com melhor custo-benefício, gerando ao invés ilhas tecnológicas de difícil interoperabilidade.

Outro fator importante de ser citado foi à massificação e popularização do acesso a *Internet*. Este fato instigou os operadores a almejarem a junção desses dois mundos, *Internet* e telecomunicações, de forma a não mais somente serem o caminho aos serviços, mais também fornecedores de serviços e soluções customizadas a fim de estarem mais inseridos dentro da cadeia de lucro.

Nesse mesmo sentido, melhorias como o desenvolvimento de *codecs* e protocolos mais simples e adaptativos tornou o *VoIP* uma opção válida, impactando no provimento de serviço via circuito comutado.

Diante de tais fatos evidenciou-se a necessidade de uma plataforma ao qual convergissem todos os serviços e permitisse a operação e o fornecimento de novos serviços de forma viável e descomplicada.

Para a mudança desse paradigma, deveriam iniciar um processo de adaptação de suas redes baseadas quase que exclusivamente em comutação de circuitos para uma rede baseada em comutação de pacotes. Tal processo se iniciou com a introdução de uma nova arquitetura de rede conhecida como NGN (*Next Generation Network*), que atenderia a uma série de novos requisitos além de permitir o tráfego *triple play* (voz, vídeo e dados) através de uma rede baseada em comutação de pacotes numa única plataforma, com a premissa de manter todo o investimento da rede legada.

O processo de implementação da NGN pelas operadoras iniciou-se antes mesmo que a padronização em desenvolvimento pelo TISPAN (NGN REL 1) estivesse concluída. Isso fez com que muitos fabricantes oferecessem equipamentos e soluções distintas que muitas vezes apresentavam problemas de interoperabilidade. A partir do *release* inicial, novas *releases* foram surgindo para cobertura de outras necessidades, como por exemplo, FMC e a inclusão do IPTV.

Diante de todas as novas exigências ficou clara a necessidade de uma rede capaz de controlar e prover diversos tipos de serviços, com um melhor controle de tarifação, capacidade de garantir *QoS* ao qual o usuário poderia acessar através de qualquer rede e dispositivo.

O 3GPP, através de estudos para melhoria das redes móveis nos quesitos controle de tarifação, controle de *QoS* e disponibilização de novos serviços desenvolveu o subsistema IMS. Tal subsistema após ser melhor estudado passou a ser visto não como apenas uma melhoria da rede móvel, mas como uma arquitetura independente e utilizável em redes de maior abrangência.

A partir desse ponto, o TISPAN adotou a arquitetura do 3GPP *release* 5, efetuando a implementação de novos elementos (NASS / RACS), especialmente para acesso de rede fixa e controle de *QoS.* Notadamente a partir desse ponto os órgãos de padronização passaram a trabalhar em conjunto para um melhor desempenho, fato que não ocorreu no desenvolvimento inicial da NGN. O IMS passou a ser visto pelos especialistas como uma plataforma potencial e promissora, que permitiria resolver a maioria das questões implícitas nas novas *releases* da NGN.

Algumas operadoras já estão implementado a arquitetura IMS em suas redes mesmo que de forma prematura, visando reduzir seus custos, minimizar o *churn* e principalmente aumentar seus rendimentos através de serviços inovadores.

Conforme mencionado no corpo do trabalho muitas são as vantagens de implementação do IMS em relação às redes legadas, sendo estas o propulsor para todas as mudanças e investimentos necessários.

Os operadores visualizam no IMS a possibilidade de uma rede com menores custos de operação e manutenção ao qual pode prover serviços inovadores com qualidade e mobilidade, atingindo o máximo retorno financeiro possível.

A busca por uma estratégia de oferta baseada em *multiple play* (*dual, triple, quadruple* etc.) é um fenômeno sem volta na indústria de telecomunicações. Mas, ao mesmo tempo em que impõe enormes desafios às operadoras, particularmente nas perspectivas de seleção de plataformas tecnológicas, empacotamento e precificação, controle e bilhetagem e de regulamentação, abre-se um enorme horizonte de possibilidades tanto para a dimensão de oferta como para a dimensão de demanda.

O IMS eleva as operadoras de rede a uma condição de competição com desenvolvedores do mundo da *Internet*.

A decisão de implantar o IMS é estratégica, as operadoras de rede podem escolher uma implantação antecipada, a fim de aproveitar os preços mais elevados cobrados inicialmente por estarem mais “à vontade” no mercado.

Nesta estratégia pioneira abriria vantagem sobre os seus concorrentes e assumiria riscos significativos, alternativamente, poderá esperar, a fim de reduzir os custos de investimento, aprendendo com as falhas de seus concorrentes.

Como conclusão, a decisão de implantar IMS é mais uma decisão estratégica do que uma decisão tecnológica.

Apesar da imaturidade do IMS verificou-se com o trabalho realizado, que já é possível criar e disponibilizar serviços rapidamente. Com esta nova realidade e com os mecanismos adequados de tarifação as operadoras têm a possibilidade de obter as receitas que tanto anseiam e recuperarem as perdas para as tecnologias tipo *VoIP* e *Internet*.

Atualmente seu modelo de arquitetura está sendo bem aceito, sendo assim desenvolvidos muitos equipamentos baseados em seus conceitos.

Com a popularização dos serviços 3G, os quais o IMS foi especialmente desenvolvido, o padrão provavelmente durará por algum tempo.

O LTE, também conhecido como 4G (Quarta Geração), já apresenta a solução com a presença do núcleo IMS. No entanto como a evolução da área das telecomunicações ocorre num ritmo muito acelerado, poderão surgir outras soluções melhores e de maior confiabilidade.

BIBLIOGRAFIA REFERENCIADA E CONSULTADA

AL-BEGAIN, Khalid. *et al.* **IMS: *a development and deployment perspective***.(Agbinya, Johnson I, 2010) *IP communications and services for NGN / author*, Johnson I. Agbinya.

ALBERTI, A. M. **Convergência Digital em Telecomunicações**: Das Redes Especializadas à Internet do Futuro, Inatel, 2009.

BARCELLOS, Marco: Disponível em: http://canaltech.com.br/coluna/internet/Internet-de-Todas-as-Coisas-uma-nova-internet-para-uma-nova-era/#ixzz2fBWHjjU0 (visitado em: 17/09/2013).

BEA Systems, Inc, **BEA WebLogic *Communications Platform and IP Multimedia.*** Disponível em: http://www.ucstrategies.com/uploadedFiles/UC_Information /White_Papers/BEA_IMS_wp.pdf (acessado em: 28/10/2013 às 16h15minhs)

BRAGA, Leticia Azevedo Genovez de Mesquita. **Estudo de convergência de Redes, Next Generation *Network e IP Multimedia Subsystem.*** Monografia de Especialização. Escola de Eng. São Carlos / SP, 2011.

CAMARILLO, Gonzalo. ***The 3G IP Multimedia Subsystem*.** 1st Ed. *West Sussex*: John Wiley & Sons Ltd, 2004.

COLCHER, Sérgio *et al.* **VoIP Voz sobre IP**. Rio de Janeiro: Elsevier, 2005 – 3ª Reimpressão.

COMUTAÇÃO de circuito versus comutação de pacotes. Disponível em Huawei 2002 - Apostila Huawei – NGN *Concepts and Applications.*

DECOMPOSIÇÃO da estrutura monolítica MSF 2013 - (*Multiservise Switching Forum).* Disponível em: htpp://msforum.org/. Acesso em 23/11/2013.

ERICSSON. **IMS - *The value of using the IMS architecture.*** Ericsson, Tech. Rep., 2004.

EXEMPLO de aplicações IMS. Disponível em http://www.slideshare.net/cflorin/ims-applications-case-studies. Acesso 23/11/2013.

FUNICELLI, V. B. **NGN e IMS I**: **Redes Legadas e Redes Convergentes**. Teleco 2007. Disponível em: http://repositorio.unb.br/bitstream/10482/9841 /5/2011_Marco Ant%C3%B4niodeCastro.pdf. Acesso em 19/09/013 as 12h04min.

HUAWEI. Apostila Huawei. **Camadas da rede IMS**. Disponível em HUAWEI 2010 - Apostila IMS *Overview Training.*

HUAWEI. ***Architecture and Principle:*** Camadas da arquitetura NGN. Disponível em HUAWEI 2003 - Apostila Huawei NGN.

HUAWEI. **China Telecom: *Telco exposure through* IMS**. Disponível em: http://www.huawei.com/en/about-huawei/publications/communicate/hw-267884.htm. Acesso em 29/10/2013 às 15h25min.

IETF RFC 3261. **SIP: *Session Initiation Protocol***. Disponível em http://www.ietf.org /rfc/rfc3261.txt.2002. Acesso em: 29/10/2013.

IETF RFC 3435. ***Media gateway control protocol* (MGCP)**. Disponível em: http://www.ietf.org/rfc/rfc3435.txt, 2003. Acessado em 25/10/2013.

IETF RFC 3588. ***Diameter Base Protocol***. Disponível em: http://www.ietf.org /rfc/rfc3588.txt, 2003. Acesso em 31/10/2013.

ITU-T Recommendation Y.2001: ***Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks: Next Generation Networks – Frameworks and functional architecture models*.** Genebra, 2004.

ITU-T's. ***Definition of* NGN.** Disponível em http://www.itu.int/en/ITU-T/gsi/ngn/Pages/definition.aspx. Acesso em 22/09/2013.

KUROSE, J. F.; ROSS, W. **Redes de Computadores e a *Internet***: Uma abordagem *Topdown.* trad. 3 ed. ed. São Paulo: Addison Wesley, 2006.

LIVINGSTON, Vicki. ***3G Americas Divulga White Paper de IMS.*** Bellevue, WA: 3G, Jul 2004. Disponível em http://www.4gamericas.org/index.cfm?fuseaction= pressreleasedisplay&pressreleaseid=1923. Acesso em 04/11/2013.

MACAPUNA. **Troca de mensagens SIP**. Disponível em http://www.macapuna.com.br/index/index.php?option=com_phocadownload&view=file&id=10%3Aims&Itemid=56&lang=en. Acesso em 23/11/2013.

MCGARVEY,Joe. **Principal Analyst, IP Services Infrastructure.** Disponível em: http://www.currentanalysis.com/f/2010/ims/. Acesso em 29/10/2013 as 15h00min.

MODULAÇÃO do sinal analógico em digital. Disponível em: http://www.ecured.cu/index.php/Modulaci%C3%B3n_por_codificaci%C3%B3n_de_pulsos_PCM. Acesso em 23/11/2013.

MOTIVOS da preferência pelo serviço integrado. Disponível em: http://www.promon.com.br/portugues/noticias/download/Triple play_10.pdf. Acesso em 15/11/2013.

NOBÔA, Francisco José Viudes. **Análise do mecanismo de segurança da arquitetura IMS.** Campinas, SP: [s.n.], 2012. Disponível em: http://www.bibliotecadigital.unicamp.br/document/?view=000868190. Acesso em 04/11/2013 às 17h42min.

RIBEIRO, Amado; GARCIA, Janaína P. Candeias. ***Network Eletronic Media*** **– Uma Visão para o Futuro das Redes de Comunicação.** Monografia de Especialização, INATEL, 2009.

SILVA, Luis Filipe Carvalho da. **Plataformas de Serviços em Redes de próxima Geração (IMS)**; Dissertação de Mestrado apresentada na Universidade de Aveiro. Disponível em http://ria.ua.pt/bitstream/10773/1999/1/2009000834.pdf. Acesso em: 29/10/2013.

TELECO. **Integração dos órgãos de padronização**. Disponível em: http://www.teleco.com.br/tutoriais/tutorialngnims1/pagina_2.asp. Acesso em 23/11/2013.

TRONCO, Tania Regina. **Redes de Nova Geração**. – 1.ed. – São Paulo: Érica, 2006.

WIRELESSBRASIL. **Separação das redes e serviços**. Disponível em http://www.wirelessbrasil.org/flavia_lefevre/2012/Cons_Consultivo_%20Apres_Jarbas_Valente_%2025%20mai%202012.pdf. Acesso em 23/11/2013.

CONECTIVIDADE IPV6 EM AMBIENTE DE REDE VIRTUALIZADO

IPV6 CONNECTIVITY IN VIRTUALIZED NETWORK ENVIRONMENT

Marco Antonio Ferreira[14]
Marcelo Takashi Uemura (Orientador)[15]

FERREIRA, Marco Antonio; UEMURA, Marcelo Takaschi (orientador). **Conectividade IPv6 em ambiente de rede virtualizado**. *Revista Tecnológica da FATEC-PR, v.1, n.4, p. 129 -160, jan./dez., 2013.*

RESUMO:

O trabalho visa examinar o cenário atual das redes *Internet Protocol version* 4 (IPv4), no qual o espaço de endereçamento está se esgotando, e apresentar a nova versão, *Internet Protocol version 6* (IPv6), descrevendo a sua importância e características, bem como algumas técnicas de conectividade que podem ser utilizadas durante o período de transição, em que redes IPv4 e IPv6 estarão operando simultaneamente, tendo em vista que a migração está sendo realizada em escala mundial de forma gradual. Será apresentado um cenário virtualizado no qual é possível acessar um endereço IPv6 utilizando um *link* exclusivamente IPv4 através da técnica de tunelamento Teredo, capaz de prover conectividade IPv6 em ambientes de redes locais, atentando-se não somente para a conectividade proporcionada, como também para as questões de segurança que acarretam de sua utilização.

Palavras-chave: *Protocolo. Conectividade. Tunelamento. Migração. Redes de Computadores.*

ABSTRACT:

The paper aims to examine the current situation of networks that use Internet Protocol version 4 (IPv4), in which the address space is running out, and present the new version, Internet Protocol version 6 (IPv6), describing its importance and characteristics, as well some connectivity techniques that can be used during the transition period in which IPv4 and IPv6 networks will be operating simultaneously, in order that migration is being performed worldwide gradually. It will be presented a virtualized scenario in which is possible to access an IPv6 address using IPv4 link through the Teredo tunneling technique, capable to provide IPv6 connectivity in environments of local networks, observing not only the connectivity provided, as well the safety issues that result from its use.

Keywords*: Protocol. Connectivity. Tunneling. Migration. Computer Networks.*

[14] Marco Antonio Ferreira é graduado em Tecnologia em Redes de Computadores pela FATEC-PR (2013). Atua como profissional em empresa de grande porte na área de Informática.

[15] Marcelo Takashi Uemura foi o Orientador do acadêmico. Possui graduação em Engenharia Industrial Elétrica pela UTFPR - Universidade Tecnológica Federal do Paraná (1998). Especialização em Métodos em Engenharia de Software pela UTFPR (2002). Especialização em Teleinformática e Redes de Multiserviços pela Universidade Federal de Pernambuco (2001). Atualmente é Gerente de Projetos do Positivo Informática S/A. Tem experiência na área de Engenharia Elétrica , com ênfase em Eletrônica Industrial, Sistemas e Controles Eletrônicos.

1 INTRODUÇÃO

Em 1982, a suíte de protocolos *Transmission Control Protocol / Internet Protocol* (TCP/IP) tornou-se o padrão adotado pela agência do governo americano *Advanced Research Projects Agency Network* (ARPANET) levando às primeiras definições de “Internet” como sendo um conjunto de redes interconectadas por TCP/IP. Naquela época, os cerca de 4 bilhões e 300 milhões de endereços únicos proporcionados pelo protocolo IPv4 pareciam ser mais do que suficientes, já que os *hosts* existentes não passavam de algumas centenas.

A situação mudaria em 1991, com a criação da *World Wide Web* (WWW), a Internet que existe atualmente. Rapidamente, a quantidade de endereços que outrora parecia inesgotável, começou a dar sinais de que, em algum momento, poderia atingir seu fim, afinal, o IPv4 não fora projetado para a crescente demanda por conectividade. Apenas um ano depois, a rede mundial alcançava a marca de 1 milhão de *hosts* conectados, fato que veio a confirmar que medidas deveriam ser tomadas para dar condições ao vertiginoso crescimento que se anunciava.

O *Internet Engineering Task Force* (IETF) já vinha trabalhando no sucessor do IPv4 desde o começo dos anos 1990 e, em 1994, formou um grupo de trabalho chamado *IP Next Generation*, para estabelecer os padrões do novo protocolo, já que, pelas projeções feitas pelo próprio IETF, o espaço de endereçamento provido pelo protocolo IPv4, acabaria entre 2005 e 2011.

A figura 1 mostra o acentuado crescimento das tabelas de roteamento da Internet a partir de meados de 1993, segundo Graziani (2012).

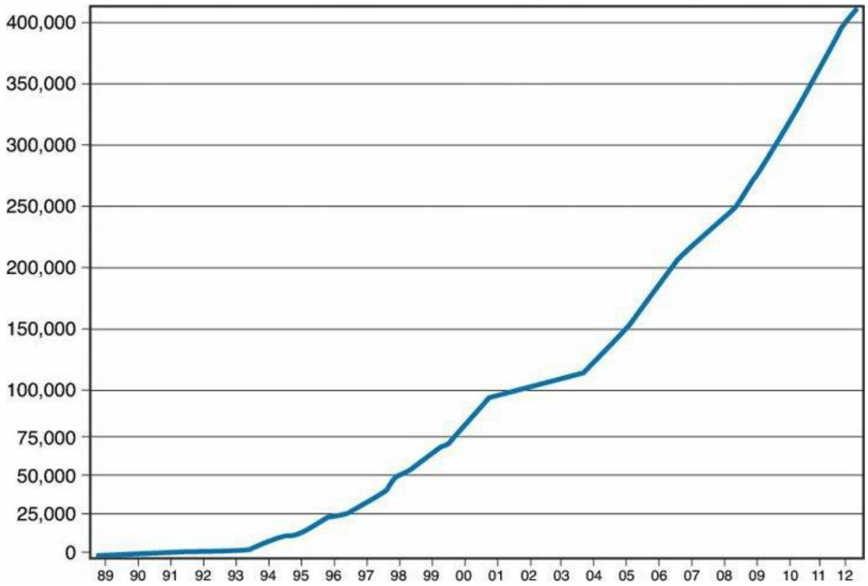


Figura 52 - Crescimento do número de redes na tabela de roteamento da Internet entre 1989 e 2012.
Fonte: Graziani (2012).

Além de oferecer uma nova estrutura de endereçamento, o protocolo IPv6 deveria também sanar algumas deficiências do protocolo anterior, provendo mais eficiência e flexibilidade.

Entre os principais objetivos do IPv6 pode-se destacar:

- Prover endereçamento de 128 *bits* em contraste aos 32 *bits* do IPv4, possibilitando um espaço de endereçamento gigantesco;
- Eliminar broadcasts utilizando técnicas para resolução de endereços mais eficientes, fazendo uso mais inteligente da banda ao aplicar *multicast*;

- Oferecer ferramentas para a coexistência entre os protocolos durante a migração, quando redes IPv4 e IPv6 estiverem operando simultaneamente.

1.1 OBJETIVO GERAL

O propósito principal deste trabalho é apresentar um estudo do protocolo IPv6 destacando suas características e diferenças em relação ao protocolo IPv4, focando ainda em algumas técnicas a serem utilizadas durante a fase de transição entre os protocolos.

1.2 OBJETIVOS ESPECÍFICOS

Destacam-se os seguintes objetivos específicos:

a) Apresentar a atual situação da alocação de endereços IPv4;
b) Destacar as inovações do novo protocolo que permitem solucionar a contento o problema de esgotamento de endereços do protocolo utilizado atualmente e outras características interessantes;
c) Demonstrar que, embora não serem diretamente compatíveis, o IPv4 e o IPv6 podem funcionar nos mesmos equipamentos de forma simultânea e interoperar através de técnicas auxiliares;
d) Apresentar as técnicas mais utilizadas que permitem a interoperabilidade;
e) Apresentar um cenário virtualizado no qual ambos os protocolos coexistem e a conectividade IPv6 utilizando um *link* IPv4 é provida através de uma dessas técnicas;
f) Analisar aspectos de segurança inerente a utilização da técnica empregada no ambiente virtual.

2 JUSTIFICATIVA

A realização deste trabalho foi motivada pela real necessidade de migração para o protocolo IPv6, uma vez que a *Internet Assigned Numbers Authority* (IANA) não possui mais endereços IPv4 para serem distribuídos para as *Regional Internet Registry* (RIR), organizações responsáveis pela alocação de endereços regionalmente e, no âmbito regional, Ásia e Europa já distribuíram seus últimos endereços (BRITO, 2013).

A migração já está ocorrendo, mas tende a acelerar nos próximos anos. Durante algum tempo os dois protocolos estarão operando simultaneamente e, por este motivo, é de suma importância compreender o cenário atual e as técnicas que permitem este funcionamento, bem como aprender sobre o IPv6 para implementá-lo num futuro próximo.

3 METODOLOGIA

Para a compreensão da necessidade da implementação do protocolo IPv6, foi realizado um estudo de pesquisa bibliográfica sobre a estrutura e as características do novo protocolo e a situação de esgotamento do protocolo atual e ainda, uma aplicação prática de conectividade IPv6 em um ambiente virtualizado.

Para o ambiente virtual apresentado neste trabalho foram utilizados programas amplamente difundidos e consolidados, os quais possuem farto material de estudo, fato que possibilitou a correta configuração da rede de testes.

Além da bibliografia, foram consultados, *sites* considerados Autoridade no assunto e as respectivas *Request For Comments* (RFC) das tecnologias citadas, conforme os passos a seguir:

a) Seleção e estudo da bibliografia;
b) Apresentação da situação do endereçamento IPv4;
c) Estudo das características do protocolo IPv6 em comparação ao IPv4;
d) Análise das tecnologias de conectividade que permitem a operação entre os protocolos;
e) Levantamento das ferramentas necessárias para a criação de um laboratório virtual para testes práticos de conectividade IPv6;
f) Exemplo de configuração de *firewall* para evitar conectividade indesejada e prevenir brechas de segurança;
g) Conclusões e considerações.

Cada uma das etapas está detalhada no item que trata sobre o desenvolvimento do trabalho, conforme a seguir.

4 REVISÃO BIBLIOGRÁFICA

A seguir estão apresentados os itens resultantes da pesquisa e estudos efetuados na literatura especializada.

4.1 O ESGOTAMENTO DE ENDEREÇOS IPv4

Como apresentado por Tanenbaum (2003), ainda que técnicas como *Classless Inter-Domain Routing* (CIDR) e *Network Address Translation* (NAT) tenham algum efeito, o esgotamento total de endereços IP versão 4 é inevitável.

Quando o protocolo IPv4 foi implementado, a Internet era utilizada apenas por universidades, empresas de tecnologia e alguns setores do governo americano. Numa época em que os *hosts* da rede não chegavam a mil, os cerca de 4 bilhões e 300 milhões de endereços pareciam ser mais do que suficientes. Entretanto, a versão 4 do protocolo não foi projetada para a demanda por conectividade que se tem atualmente.

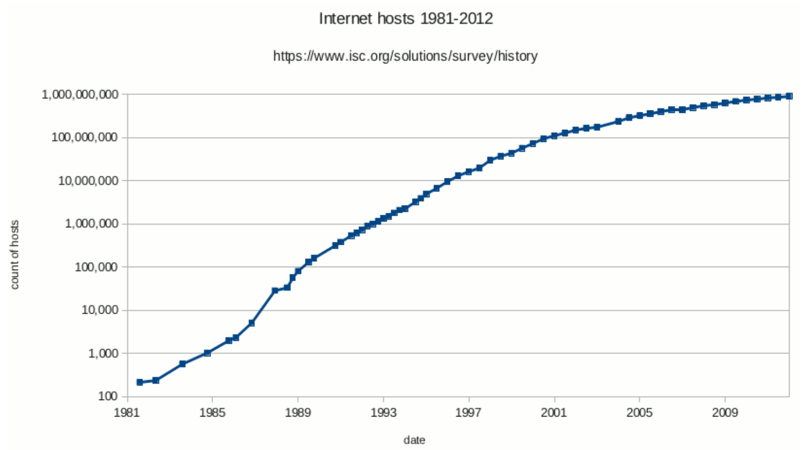


Figura 53 - Número de *hosts* na Internet de 1981 à 2012.
Fonte: Ke4roh (2012).

Mesmo assim, pode-se concluir que, em seus trinta anos, o protocolo IPv4 cumpriu seu dever muito bem. Para Comer (2008), o protocolo foi bem-sucedido pois, em sua existência, conseguiu lidar com redes heterogêneas, mudanças extremas nas tecnologias de *hardware* e um crescimento em escala global.

A Internet atual é muito mais do que páginas, *e-mails* e transferências de arquivos.

Segundo Graziani (2012), a convergência das redes de informação, comunicação e entretenimento e a explosão de crescimento dos dispositivos móveis, somados aos dispositivos que tradicionalmente não requeriam conexão, trouxeram o conceito de Internet das Coisas (*Internet of Things*), no qual uma infinidade de dispositivos pode se conectar à rede utilizando uma conexão IP, fazendo ainda mais pressão na desgastada estrutura de endereçamento IPv4.

4.2 IPv5

No final da década de 1970, um protocolo chamado *Stream Protocol* (ST) foi criado para a transmissão experimental de voz e vídeo sob demanda. Duas décadas mais tarde, este protocolo foi revisto para a versão *Stream Protocol version 2* (ST2) e começou a ser implementada em alguns projetos por empresas como IBM, Apple, NeXT e Sun. A ideia era que aplicações multimídia utilizassem o IPv4 em conjunto com o ST2 para o tráfego que necessitasse de entrega de dados em tempo real. Para este arranjo, foi reservada a nomenclatura IPv5. Posteriormente, o ST2 foi considerado apenas um complemento do IPv4 e utilizado somente em nível experimental. Contudo, a designação IPv5 já havia sido utilizada (GRAZIANI, 2012).

4.3 MIGRAÇÃO PARA O IPv6

Diferentemente da migração entre o protocolo *Network Control Program* (NCP) para o IPv4, que ocorreu no dia 1º de janeiro de 1983, a migração para a versão 6 está sendo feita gradualmente pois, devido ao tamanho e à complexidade da Internet atual, é impensável estabelecer uma data limite para a adoção completa do novo protocolo (KUROSE, 2012). Abaixo, é apresentada uma tabela com a porcentagem de usuários com acesso IPv6, por país, em junho de 2013.

Posição em 2013	**País**	**Porcentagem de usuários IPv6**	**Número de usuários IPv6**
1	Romênia	10.84%	1.053.237
2	Suíça	10.72%	700.777
3	Luxemburgo	6.96%	32.535
4	França	5.46%	2.824.465
5	Bélgica	4.17%	339.651
6	Japão	4.13%	4137.476
7	Alemanha	3.24%	2.212.062
8	Estados Unidos	2.72%	6.768.264
9	Peru	2.42%	273.370
10	República Tcheca	2.12%	157.203
11	Cingapura	1.58%	54.060
12	Noruega	1.21%	53.677
13	Eslovênia	0.92%	13.230
14	China	0.90%	4.651.953
15	Grécia	0.78%	44.572
16	Portugal	0.76%	45.408

Posição em 2013	País	Porcentagem de usuários IPv6	Número de usuários IPv6
17	Taiwan	0.72%	120.180
18	Holanda	0.70%	109.425
19	Austrália	0.69%	121.256
20	Eslováquia	0.52%	21.169

Quadro 1 - Ranking de países por porcentagem de usuários com acesso IPv6 em junho de 2013.
Fonte: Huston (2013).

A *Internet Society* (ISOC) organiza datas para o *World IPv6 Day*, cujo propósito é acelerar a migração para o IPv6 através de eventos nos quais são estabelecidas metas a serem alcançadas. No primeiro, em junho de 2011, grandes provedores puderam testar suas implementações em IPv6. Em junho do ano seguinte, aconteceu o segundo *World IPv6 Day* e, a partir desta data, estes mesmos provedores tiveram que disponibilizar definitivamente acesso IPv6 aos seus serviços (GRAZIANI, 2012).

Muito se especula sobre os endereços quando os endereços IPv4 se esgotarão completamente, mas o fato é que a necessidade de implementação do IPv6 é urgente. Em algumas regiões, os endereços já esgotaram e as previsões mais otimistas indicam que até 2018 não haverá mais endereços disponíveis.

Em fevereiro de 2011, a IANA distribuiu o último bloco regional disponível. Regionalmente, Ásia e Europa já não possuem mais endereços para distribuir para os provedores (KUROSE, 2012).

No gráfico abaixo pode-se observar a situação de cada região mundial

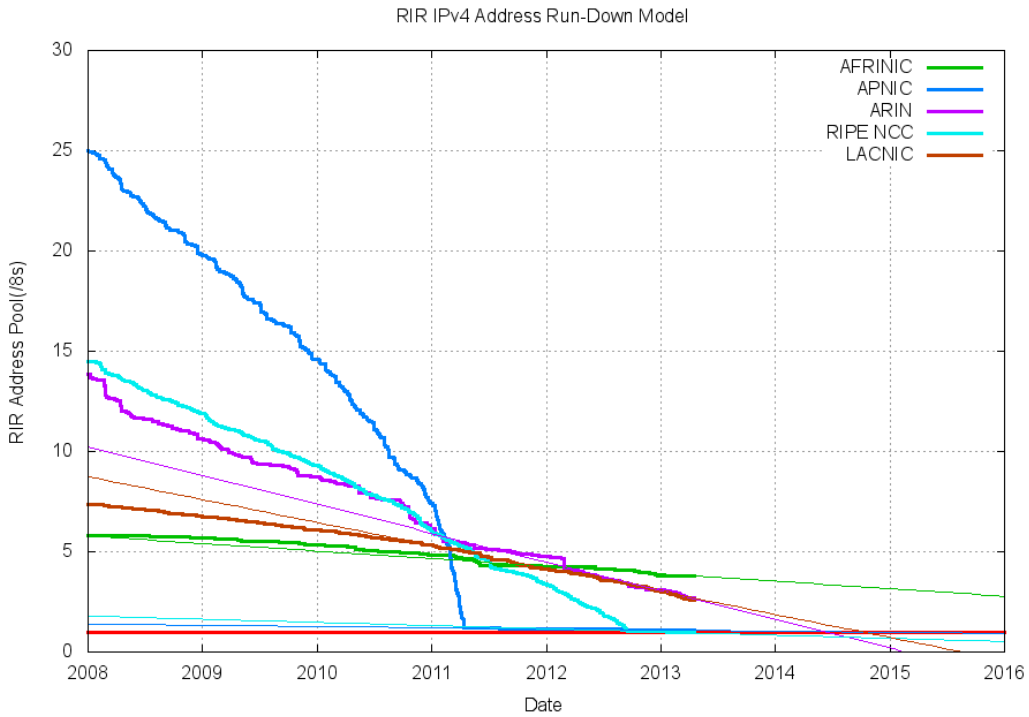


Figura 54 - Esgotamento de endereços IPv4 por região.
Fonte: Huston (2013).

Como dito anteriormente, *Réseaux IP Européens Network Coordination Centre* (RIPE NCC) e *Asia-Pacific Network Information Centre* (APNIC), as RIR responsáveis pela distribuição na Europa e no bloco Ásia-Pacífico, respectivamente, já esgotaram seus endereços. Pelas previsões, os últimos endereços da *Latin*

America and Caribbean Network Information Centre (LACNIC) da América Latina e Caribe e da *American Registry for Internet Numbers* (ARIN) devem ser distribuídos entre 2015 e 2016. Somente a *African Network Information Centre* (AfriNIC) tem mais algum tempo de vida, mesmo assim, é esperado que a RIR africana termine seus endereços IPv4 até 2018.

Segundo Davies (2012), apesar dos avanços tecnológicos óbvios, a implantação de IPv6 nativo numa infraestrutura de rede envolve planejamento e estratégias de manutenção e instalação de hardware e software, bem como treinamento de pessoal e precisa ser justificado da perspectiva de negócios. A migração necessita de tempo e recursos significativos, sendo assim, pode ser adiada frente a outras iniciativas de maior visibilidade ou melhores benefícios de curto prazo.

Deve-se considerar, entretanto, que a Internet é atualmente um meio de comunicação indispensável e parte integrante da economia global e, para continuar crescendo, provedores de acesso, órgãos governamentais e empresas devem substituir o protocolo atual o quanto antes, para se beneficiarem dos novos recursos do IPv6.

4.4 O PROTOCOLO IPv6

A preocupação com espaço de endereçamento do IPv4 surgiu no início da década de 1990, quando a taxa de nós conectados à Internet começou a crescer expressivamente. Assim, o IETF iniciou o desenvolvimento do IPv6, cujo principal objetivo principal era ampliar a quantidade de endereços providos pelos 32 *bits* do protocolo IPv4. Entretanto, os projetistas do IPv6 aproveitaram a oportunidade para corrigir algumas deficiências e inserir novas funcionalidades baseadas nos anos de experiência com a versão 4.

Segundo Tanenbaum (2012), antevendo outros problemas no horizonte, além de ser capaz de prover uma quantidade imensa de endereços, o IETF desenvolveu a nova versão do IP para ser mais flexível e eficiente.

Seus principais objetivos foram:

1) Suporte a uma quantidade de *hosts* quase inesgotável;
2) Redução do tamanho das tabelas de roteamento;
3) Simplificar o processamento de pacotes pelos roteadores;
4) Suporte à segurança (autenticação e privacidade);
5) Priorizar o tipo de serviço, especialmente para dados em tempo real;
6) Suporte a *multicast*, permitindo a especificação de escopos;
7) Tornar possível a locomoção sem mudança de endereço;
8) Permitir que o protocolo evolua no futuro;
9) Fornecer meios para a coexistência dos antigos e novos protocolos.

De um modo geral, o IPv6 mantém as características básicas do protocolo corrente, como não ser orientado a conexão (*connectionless*), permitindo que cada pacote seja roteado independentemente, ou ainda, como serão aplicadas as regras para o descarte de um pacote, além de outras facilidades (COMER, 2008).

Para Tanenbaum (2012), apesar de ser um padrão da Internet desde 1998 e de prover uma estrutura capaz de atender a atual demanda da convergência de redes de computadores, comunicação e entretenimento, o IPv6 ainda é utilizado por uma pequena fração da Internet (pouco mais de 1%). A implementação do novo protocolo não é trivial e, apesar das similaridades com o antecessor, os dois protocolos não interoperam tornando a migração mais complexa.

Entretanto, a vigente falta de endereços e real possibilidade de telefones, televisões e outros dispositivos se tornarem nós de rede, intensificam cada vez mais a necessidade da rápida implementação do IPv6.

4.5 CARACTERÍSTICAS DO PROTOCOLO IPv6

Segundo Davies (2012), as principais características do protocolo IPv6 podem ser sumarizadas em:

- Novo formato de cabeçalho;
- Espaço de endereçamento de 128 *bits*;
- Suporte obrigatório ao *Internet Protocol Security* (IPsec);
- Suporte melhorado a priorização de tráfego;
- Interação entre nós vizinhos através de protocolo;
- Extensibilidade.

4.5.1 Novo Formato de Cabeçalho

Com menos campos, o cabeçalho IPv6 foi projetado para minimizar o seu processamento. Isso foi possibilitado pela remoção de campos não-essenciais do cabeçalho IPv4 que agora são supridos pelos cabeçalhos de extensão do IPv6, quando há necessidade.

4.5.2 Espaço de Endereçamento de 128 *Bits*

O espaço de endereçamento do IPv6 passa a ter 128 *bits* e permite o endereçamento de 340.282.366.920.938.463.374.607.431.768.211.456 (340 undecilhões) de endereços únicos na Internet. Comparado a estrutura de 32 *bits* do IPv4, que provê 4.294.967.296 de endereços, tem-se uma estrutura 79 octilhões de vezes maior, capaz de prover aproximadamente 56 octilhões de endereços para cada habitante do planeta, solucionando definitivamente o problema de escassez de endereços que existe atualmente.

4.5.3 Suporte Obrigatório a IPsec

Diferentemente do IPv4, no qual a utilização do IPsec é opcional, no IPv6, o IPsec passa a ser um componente do protocolo tornando-o potencialmente mais seguro que o IPv4. Isso não significa que qualquer pacote IPv6 está automaticamente mais seguro, mas sim que o protocolo possui mecanismos nativos capazes de prover soluções de segurança como autenticação e criptografia, em dispositivos que o suportem, bastando apenas configurá-lo corretamente.

4.5.4 Suporte Melhorado à Priorização de Tráfego

No IPv6 foram implementados campos no cabeçalho que permitem a um roteador identificar a prioridade de um pacote permitindo a sua manipulação de maneira mais eficiente. O campo *Traffic Class* identifica a prioridade do pacote e o campo *Flow Label* classifica os pacotes de um fluxo específico durante toda a transmissão, simplificando assim o fornecimento de serviços que necessitem de Qualidade de Serviço.

4.5.5 Interação Entre Nós Vizinhos Através de Protocolo

Assim como seu antecessor, o IPv6 utiliza o *Internet Control Message Protocol version 6* (ICMPv6) que, entre as novas funcionalidades, destaca-se o *Neighbor Discovery Protocol* (NDP), uma série de mensagens que gerencia a interação entre nós vizinhos, substituindo a combinação do protocolo *Address Resolution Protocol* (ARP) e mensagens ICMPv4, minimizando o *broadcast* e fazendo uso mais eficiente da banda ao utilizar *multicast* e *unicast* para a autoconfiguração da rede.

4.5.6 Extensibilidade

O IPv6 não inclui um campo fixo de opções em seu cabeçalho como no protocolo IPv4. Para incluir funcionalidades adicionais, o IPv6 utiliza-se de cabeçalhos de extensão separados do cabeçalho principal. Essa abordagem permite diminuir a carga de processamento nos roteadores intermediários, que não utilizam as informações opcionais, mantendo no cabeçalho principal apenas as funções realmente básicas, otimizando o desempenho da rede.

4.6 COMPARAÇÃO ENTRE IPv4 E IPv6

A seguir, é apresentado um comparativo entre as características de cada protocolo.

IPv4	IPv6
Espaço de endereçamento de 32 *bits* (4 *bytes*).	Espaço de endereçamento de 128 *bits* (16 *bytes*).
Suporte a IPsec é opcional.	Suporte a IPsec é obrigatório.
Não faz a identificação de fluxo de pacotes para tráfego priorizado.	Possui campo de identificação de fluxo de pacotes no cabeçalho para tráfego priorizado.
A fragmentação de pacotes é executada pelo *host* emissor e pelos roteadores, diminuindo a performance,	A fragmentação de pacotes é executada apenas pelo *host* emissor.
Cabeçalho inclui a checagem de erros.	Cabeçalho não possui campo de checagem de erros.
O cabeçalho inclui campo opções de tamanho fixo.	Opções foram movidas para cabeçalhos de extensão.
O ARP envia quadros de requisições em *broadcast* para resolver endereços.	O ARP foi substituído pelo NDP que envia solicitações via *multicast* para resolver endereços.
Endereços de *broadcast* são utilizados para enviar tráfego para todos os nós de uma sub-rede.	Para alcançar todos os nós de um mesmo enlace, o IPv6 utiliza endereços especiais (*multicast-all-nodes*).
Deve ser configurado manualmente ou automaticamente através de servidor.	Possui funcionalidades de autoconfiguração.

Quadro 2 - Comparação entre os cabeçalhos IPv4 e IPv6.
Fonte: Davies (2012).

4.7 CABEÇALHO IPv6

O cabeçalho IPv6 tem tamanho fixo de 40 *bytes*, o dobro do cabeçalho IPv4 (tamanho variável de 20 a 60 *bytes*), entretanto agora possui apenas oito campos, removendo ou tornando opcionais alguns dos doze campos do cabeçalho da versão 4. Essas mudanças resultaram no processamento mais rápido dos datagramas nos roteadores (KUROSE, 2012).

Segundo Brito (2013), o tamanho fixo é o principal diferencial, pois agora os equipamentos não precisam mais analisar previamente o extinto campo *Internet Header Length* (IHL), responsável por determinar o tamanho do cabeçalho, antes de analisar as informações de controle. Outras modificações notáveis são a ausência do campo de verificação de erros, executada em outras camadas, tornando o processo redundante e desnecessário e o campo de opções, que agora faz parte dos cabeçalhos de extensão.

A figura 4 compara a estrutura do cabeçalho dos dois protocolos e mostra quais campos foram removidos ou tiveram seus nomes alterados, e também o campo de identificação de fluxo, o único campo criado no cabeçalho do IPv6.

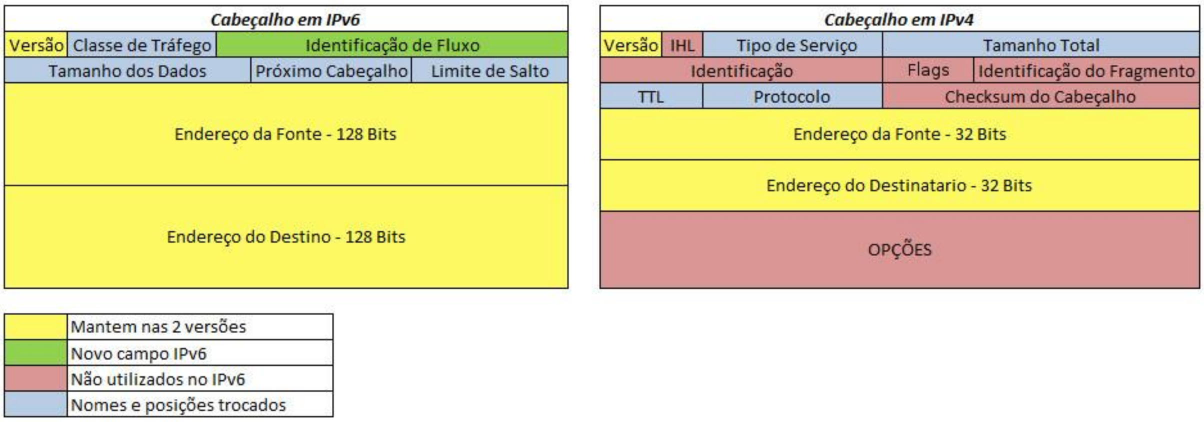


Figura 55- Diferenças entre os cabeçalhos IPv4 e IPv6.
Fonte: Avila (2011).

Entre os campos renomeados, vale destacar o campo *Time to Live* (TTL), tempo de vida, para *Hop Limit*, quantidade de saltos, que determina após quantos saltos um pacote deve ser descartado, e que também funcionava desta forma no cabeçalho IPv4 e, portanto, recebeu um nome mais apropriado.

O campo protocolo do IPv4, que apontava para o protocolo de camada superior, passou a se chamar próximo cabeçalho, pois pode apontar para um cabeçalho de camada superior ou para um cabeçalho de extensão como pode ser observado a seguir.

4.7.1 Cabeçalhos de Extensão

O projetistas do IPv6 focaram principalmente na simplicidade. O objetivo era manter o datagrama tão simples quanto possível, fixando o tamanho do cabeçalho em 40 *bytes*. A principal razão para esta decisão era maximizar o desempenho de processamento.

O formato do cabeçalho IPv4 contém, além de uma maior quantidade de campos, um campo de opções de tamanho variável para conter informações que, às vezes, podem nem existir. O IPv6 mostra uma abordagem diferente, na qual somente os campos essenciais estão presentes. Todo o resto foi deslocado para os novos cabeçalhos de extensão, que são acionados por demanda e não precisam ser verificados pelos roteadores intermediários, diminuindo a carga de processamento e otimizando o desempenho da rede.

Um ou mais cabeçalhos de extensão podem ser acrescentados após o cabeçalho principal do pacote através de um mecanismo denominado encadeamento de cabeçalho que é implementado utilizando-se o campo próximo cabeçalho. Este campo, substitui o campo “protocolo” do cabeçalho IPv4 que aponta para o protocolo da camada de transporte. No IPv6, além desta função, o campo pode apontar para um cabeçalho de extensão, que também possui o campo próximo cabeçalho, viabilizando a operação.

Desta forma podem-se acrescentar as funcionalidades necessárias até, finalmente, o último cabeçalho apontar para a camada superior (BRITO, 2013).

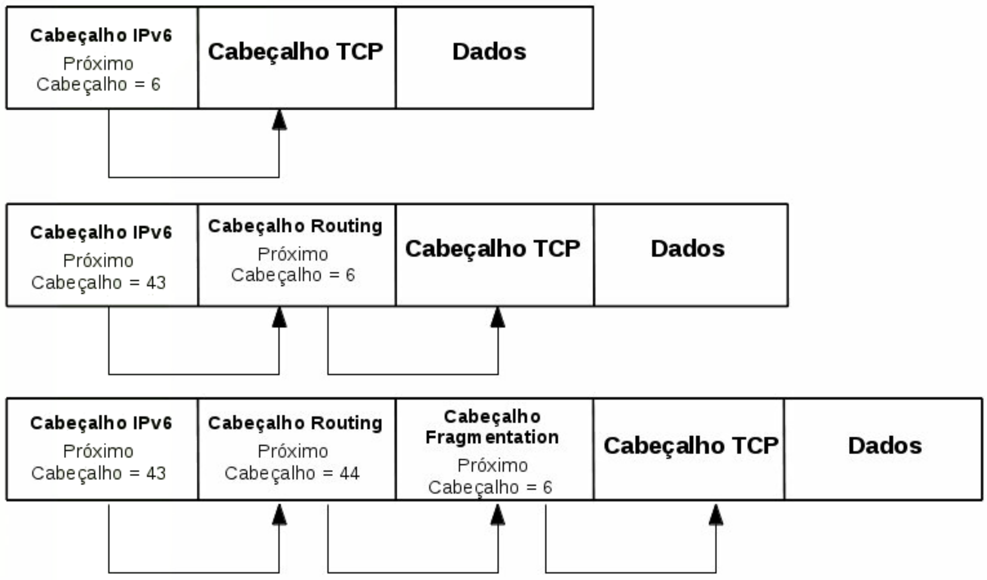


Figura 56 - Mecanismo de encadeamento de cabeçalhos IPv6.
Fonte: Moreiras (2012).

Outra vantagem desta abordagem é permitir testar funcionalidades, já que apenas as pontas precisam entender o conteúdo do cabeçalho de extensão. Assim, uma vez que uma característica experimental mostre-se útil, pode ser facilmente implementada (COMER, 2008).

4.8 CONCEITOS BÁSICOS DO ENDEREÇAMENTO IPv6

O comprimento do endereço, certamente, está entre as mudanças mais notáveis, pois foi aumentado significativamente para expandir o espaço de endereço disponível. O endereço IPv6 é formado por 128 *bits* (ou 16 *bytes*) de comprimento, quatro vezes mais longo que seu antecessor. Isto não significa dizer que pode existir uma quantidade de endereços quatro vezes maior com o IPv6. O crescimento é exponencial, e cada bit de comprimento endereço adicionado dobra o número de endereços disponíveis, resultando num espaço de endereçamento realmente enorme, que permite resolver o problema de escassez de endereços na Internet e trazer de volta o modelo de comunicação fim-a-fim, dispensando a utilização do NAT (BRITO, 2013).

Definido na RFC 4291, os 128 *bits* dos endereços IPv6 são escritos no formato hexadecimal. Nesta notação, cada 4 *bits* equivalem a um único dígito hexadecimal, formando um total de 32 dígitos, separados pelo caracter “:” em oito grupos de quatro dígitos.

Semelhante ao IPv4, o IPv6 mantém o princípio hierárquico onde existe um prefixo de rede e um sufixo de *host* dentro desta rede. O que muda na arquitetura

IPv6 é a representação dos prefixos, pois deixa de existir a máscara de rede tornando a notação CIDR a única opção (GRAZIANI, 2012).

Exemplo de endereço IPv6: 2001:5db8:cafe:0001::/64

Como mencionado, uma das características mais marcantes do IPv6 é a capacidade autoconfiguração de endereços, mesmo sem a presença de um servidor Dynamic Host Control Protocol (DHCP) na rede. Resumidamente, neste cenário, um host IPv6 “aprende” o prefixo da rede e determina o sufixo a partir do endereço físico da interface de rede com a aplicação de um algoritmo que preenche os 64 bits restantes, uma vez que um endereço físico é formado por apenas 48 bits. Esse é o comportamento padrão dos sistemas operacionais Linux e MacOS. No Windows, a Microsoft optou por gerá-los aleatoriamente porque entende que é um risco de segurança incorporar os endereços físicos das interfaces de rede no próprio IPv6.

Salientando que esse é o comportamento padrão de cada sistema operacional, sendo possível configurar o Linux para gerar os endereços aleatoriamente ou o Windows para utilizar o algoritmo automaticamente.

4.8.1 Tipos de Endereços IPv6

De acordo com HUGHES (2010), no IPv6 existem três tipos de endereços: *Unicast* (um para um), *multicast* (um para muitos) e *anycast* (um para um de muitos). Comparando com o IPv4, pode-se notar a ausência dos endereços de *broadcast* (um para todos) que eram especificados no último endereço de cada sub-rede, entretanto, ainda é possível enviar uma mensagem para todos os nós de uma rede através de endereços especiais *multicast all nodes*. Essa abordagem permite fazer uso mais eficiente da banda disponível ao eliminar as mensagens periódicas de broadcast.

Tipo	Propósito
***Global* (*Unicast*)**	Globalmente roteável. Identifica uma interface de forma única na rede possibilitando a volta do modelo ponto-a-ponto na Internet.
***Global Link-Local* (*Unicast*)**	Endereços reservados exclusivamente para comunicação local. Pacotes com esses endereços não são encaminhados para outras redes. Todas as interfaces são obrigadas a ter pelo menos um endereço *Link-Local* que são automaticamente configurados.
***Global Unique-Local* (*Unicast*)**	Similar aos endereços privados do IPv4. Ou seja, endereços roteáveis apenas localmente. A recomendação é que sempre sejam utilizados endereços do tipo Global mas, em algumas situações, sua utilização pode ser necessária.
Multicast	Utiliza o mesmo conceito do IPv4 mas no IPv6 é parte essencial do funcionamento, permitindo a autoconfiguração de endereços, por exemplo. Um pacote enviado é recebido por todos os membros do grupo *multicast*.
Anycast	A ideia básica por trás do *anycast* é que

Tipo	Propósito
	existe um grupo de nós IPv6 fornecendo o mesmo serviço. Se você usar um endereço *anycast* para identificar este grupo, o pedido será entregue ao seu membro mais próximo.

Quadro 3- Tipos de endereço IPv6.
Fonte: Do Autor.

Baseado nas informações da RFC 4291, no IPv6, endereços são atribuídos às interfaces e não aos nós. Obrigatoriamente, ao menos um endereço do tipo *Link-Local* é atribuído a todas as interfaces e cada interface pode ter mais de um endereço IPv6 de qualquer tipo (*Unicast, multicast* ou *anycast*).

4.9 COEXISTÊNCIA E TRANSIÇÃO

Apesar das vantagens oferecidas pelo protocolo IPv6 e da necessidade de implementação, a migração se dará lenta e gradualmente, pois, devido ao grau de disseminação do IPv4 nas redes das organizações e na própria Internet, a transição não será um processo trivial.

Eventualmente, todos os protocolos e aplicativos serão migrados, num processo que pode durar mais de uma década. Enquanto isso, os dois protocolos deverão coexistir de maneira transparente ao usuário, permitindo acesso total ao conteúdo da Internet. Para que essa coexistência aconteça, métodos de transição foram criados para viabilizar a comunicação entre as duas versões do protocolo. Estes métodos foram projetados como parte do próprio IPv6, uma vez que esse cenário de transição já era previsto (BRITO, 2013).

Os mecanismos que tornam possível a complexa interoperabilidade entre IPv4 e IPv6 podem ser classificados nas três categorias que podem ser observadas a seguir.

4.9.1 Pilha-dupla

Segundo BRITO (2013), esta técnica consiste em que todos os nós e equipamentos de infraestrutura tenham suporte a ambos os protocolos. A pilha-dupla é uma estratégia evolucionista, pois possibilita que o IPv6 seja inserido na rede gradativamente até se tornar totalmente operacional, permitindo o desligamento definitivo do IPv4.

Por se tratar de um mecanismo de transição, não se deve implementá-lo sem planejamento ou utilizá-lo por um tempo muito prolongado. Manter os dois protocolos em funcionamento traz complexidade à rede, que passa a ter planos de endereçamento, tabelas de roteamento e regramentos de firewall distintos, dificultando o gerenciamento.

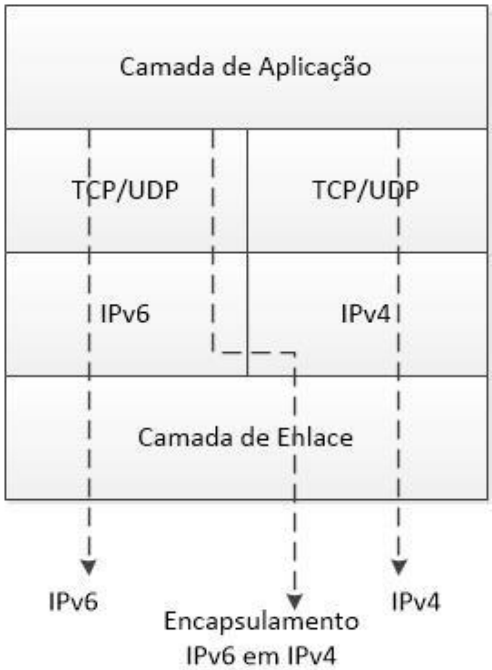


Figura 57 - Arquitetura de pilha-dupla.
Fonte: Do Autor.

4.9.2 Tunelamento

Também chamado de encapsulamento, o tunelamento, é a técnica na qual a informação de um protocolo é encapsulada como *payload* de dados no interior do pacote de outro protocolo. Este mecanismo pode ser usado quando dois nós ou redes que utilizam o mesmo protocolo desejam se comunicar através de uma rede que utiliza um protocolo distinto.

Figura 58 - Encapsulamento de pacote IPv6 em IPv4.
Fonte: Do Autor.

Este método é utilizado quando a estrutura completa, ou partes dela, ainda não é capaz de oferecer funcionalidade IPv6 nativa e é frequentemente escolhido como o primeiro passo em direção à adoção do novo protocolo e iniciar testes de integração com o IPv6.

Existem várias técnicas de tunelamento que podem ser configuradas manualmente ou automaticamente entre roteadores, entre hosts, de host para roteador ou de roteador para host. Entre as mais utilizadas atualmente, existem:

Tunnel broker, *6to4*, *6over4*, *Intra-Site Automatic Tunnel Addressing Protocol* (ISATAP) e Teredo (HUGHES, 2010).

4.9.3 Tradução

Dentre os mecanismos de transição, a tradução é, certamente, o mais complexo, trazendo consigo as limitações operacionais do NAT acrescidas da complexidade da conversão entre endereços IPv4 e IPv6.

Como uma tendência natural do cenário de migração, à medida que avançarmos em direção ao IPv6, principalmente nos ISP, o modelo pilha-dupla gerará nós somente IPv6 que, de alguma forma terão que se comunicar com as redes IPv4 legadas, fazendo necessária a presença de *gateways* de tradução na comunicação.

Para GRAZIANI (2012), a tradução oferece duas vantagens sobre o tunelamento:

- A tradução provê um mecanismo de mudança gradual e contínuo para o IPv6;
- Permite aos provedores de conteúdo fornecer serviços de forma transparente para os usuários da Internet IPv6.

5 DESENVOLVIMENTO

Cada uma das etapas previstas na metodologia para o desenvolvimento do trabalho foi desenvolvida conforme descrito a seguir.

5.1 SELEÇÃO E O ESTUDO DA BIBLIOGRAFIA

O estudo da bibliografia pertinente ao assunto foi efetuado tendo como referenciais *sites* de literatura especializada, materiais de aula e as RFC das técnicas estudadas e const ado item anterior.

5.2 LEVANTAMENTO DAS TÉCNICAS DE TUNELAMENTO E ESCOLHA DE *SOFTWARE*

Em seguida foram identificadas algumas técnicas de tunelamento a serem consideradas para obter conectividade IPv6 utilizando um *link* IPv4, a escolha dos sistemas operacionais dos hosts da rede e do *software* de *firewall*, e ainda, o *software* analisador a ser utilizado na captura dos pacotes IPv6, para a criação de um ambiente de rede local virtualizado que simula um cenário que pode ser encontrado em algumas empresas e instituições.

Para a criação da rede virtual, o trabalho baseou-se na utilização do *software* de virtualização VirtualBox, executado no sistema operacional Windows 8. Após testes com outras distribuições especializadas em *firewall* como Endian (Linux), Ipfire (Linux) e M0n0wall (FreeBSD), o *firewall* pfSense (FreeBSD) foi selecionado para simular um ambiente de rede local protegido e duas instâncias baseadas em Linux (Ubuntu e Debian), simulam os clientes dessa rede, na qual foram efetuados os testes de conectividade IPv6. Em ambos os clientes da rede, foram instalados o pacote miredo, que permite a utilização da técnica Teredo em ambientes Linux e BSD (*Berkeley Software Distribution*) e ainda, o analisador de pacotes *Wireshark*, para a verificação do tráfego de rede.

Foram instalados também os seguintes programas para testes de conectividade IPv6 local: *Secure Shell* (SSH) para acesso remoto, *Very Secure FTP Daemon* (VSFTPD) - servidor *File Transfer Protocol* (FTP), filezilla (cliente FTP) e nmap (varredura de portas). Em todos os casos, o *host* Debian foi configurado como servidor.

5.3 TUNELAMENTO TEREDO

Após algumas tentativas de implementação da técnica 6-to-4, foi verificado que a mesma funciona somente em interfaces de rede configuradas com endereços públicos, tornando-se inadequada para a utilização no cenário proposto. Por isso, foi escolhida a técnica de tunelamento Teredo para o desenvolvimento do trabalho que, devido às características que serão descritas a seguir, se revelaram mais adequadas para a implementação em ambiente virtualizado.

Teredo é uma tecnologia de tunelamento automática criada pela Microsoft e descrita na RFC 4380 que provê conectividade IPv6 ponto-a-ponto através da Internet IPv4. Diferente de outras tecnologias que dependem da contratação de serviços ou requerem endereços públicos para efetuar o encapsulamento, como na tecnologia 6-to-4, o Teredo provê conectividade IPv6 num tipo de ambiente muito comum em ambientes *small office / home office* (SOHO), no qual a conectividade dos clientes da rede com a Internet é configurada com a utilização de NAT.

O NAT, especificado na RFC 2663, foi a técnica que teve o maior impacto na sobrevida do IPv4. Com o seu emprego, é possível que através de um único endereço público, vários *hosts* de uma rede privada obtenham acesso à Internet. A proposta consiste na implementação de um roteador de borda (*gateway*) conectado simultaneamente à rede local é à Internet, responsável por executar a tradução de endereços, público e privado, permitindo assim, o compartilhamento da conexão.

E é justamente o NAT que adiciona complexidade ao funcionamento das tecnologias de tunelamento, deixando o Teredo como uma das únicas alternativas.

O Teredo funciona com NAT do tipo *Cone Full* e Restrito, entretanto, não possui suporte ao NAT simétrico. Portanto, clientes Teredo que fazem parte de uma rede local configurada com este tipo de NAT, não conseguem conectividade IPv6 utilizando esta técnica.

O método de encapsulamento do Teredo é um pouco mais complexo, pois todos os pacotes IPv6 são compostos por um cabeçalho de pacote IPv4, um cabeçalho de transporte UDP, seguido pelo pacote IPv6 como *payload*.

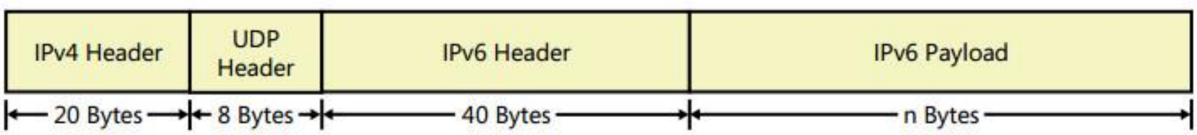


Figura 59 - Encapsulamento do pacote Teredo
Fonte: Davies (2012).

Para prover a conectividade IPV6, a infraestrutura Teredo é formada pelos seguintes componentes: Clientes Teredo, servidores Teredo e relays Teredo. O servidor Teredo fica “ouvindo” a porta *User Datagram Protocol* (UDP) 3544 aguardando requisições dos clientes Teredo para iniciar a comunicação que acontece conforme a figura a seguir.

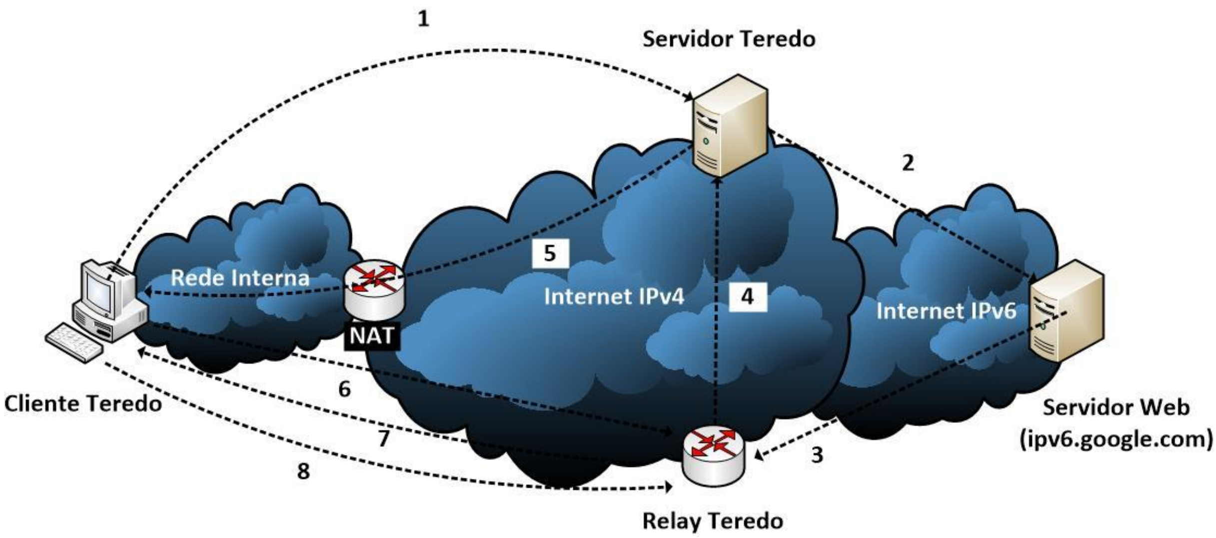


Figura 60 - Estabelecimento da comunicação por túnel Teredo.
Fonte: Do Autor.

Na comunicação inicial, cliente e servidor Teredo estabelecem uma conexão com a finalidade de identificar o tipo de NAT utilizado na rede do cliente. Esta etapa faz parte do funcionamento padrão da técnica de transição e pode causar um atraso na comunicação inicial, que pode ser menor ou maior, em função do tipo de NAT utilizado. Em seguida, após verificar a conectividade IPv6 do destino, um *relay* Teredo é utilizado para criar uma interface que irá prover a comunicação entre o cliente e o nó destino.

A comunicação é estabelecida conforme os passos a seguir:

1. Para iniciar a comunicação com o host IPv6, o cliente Teredo deve primeiro determinar o endereço IPv4 do *relay* Teredo que está mais próximo do *host* IPv6, ipv6.google.com, no exemplo;
2. O servidor Teredo recebe a requisição e encaminha para o *host* IPv6, através da Internet IPv6;
3. O host IPv6 responde com um pacote Teredo endereçado ao *relay* Teredo mais próximo;
4. O *relay* Teredo determina que o cliente Teredo está atrás de um NAT restrito através de campos específicos do pacote. Em seguida, envia um pacote de bolha (pacote Teredo sem *payload*) para o servidor Teredo através da Internet IPv4;
5. O servidor Teredo recebe o pacote de bolha do *relay* Teredo e o encaminha para o cliente Teredo, com um indicador de origem que contém o endereço IPv4 e o número da porta UDP do *relay* Teredo;
6. O cliente Teredo determina o endereço IPv4 do *relay* Teredo mais próximo do *host* IPv6 através do indicador de origem do pacote de bolha recebido. Para estabelecer um mapeamento específico o cliente Teredo envia um pacote de bolha para o *relay*;
7. O *relay* Teredo envia a mensagem de resposta para o cliente Teredo, determinando que o mapeamento NAT do cliente Teredo agora existe;
8. A comunicação inicial entre o cliente Teredo e o host IPv6 é estabelecida através do *relay* Teredo.

A situação descrita apresenta o cenário mais complexo, com o NAT de tipo restrito. No NAT de tipo cone, por uma questão de arquitetura, o procedimento de troca de *bubble packet,* não envolve o servidor, refletindo no desempenho do estabelecimento da conexão. Foge ao escopo do trabalho explicar em detalhes o funcionamento de cada tipo de NAT.

5.3.1 Segurança

A Microsoft desenvolveu o Teredo como alternativa ao tunelamento 6-to-4 para ser utilizado em ambientes configurados por NAT.

Por esta característica, o Teredo torna-se potencialmente perigoso, pois os túneis são capazes de receber conexões entrantes que contornam os mecanismos de segurança existentes, possibilitando que o tráfego indesejado obtenha acesso à rede interna “escondido” pelo encapsulamento IPv4. O risco aumenta, pois o Teredo vem habilitado de forma automática em algumas versões do Windows, sistema operacional amplamente utilizado nas empresas.

Uma alternativa para eliminar este risco é desabilitar o Teredo em todos os *hosts* que utilizam o Windows na rede. Entretanto, esta opção torna-se inviável numa rede com muitos *hosts*.

A forma mais eficiente de impedir o funcionamento do Teredo é bloquear todo o tráfego da porta UDP 3544, sendo liberado para hosts específicos conforme a necessidade.

5.3.2 *Teredo Sunset*

Considerado como uma tecnologia de último recurso pela própria Microsoft, o Teredo foi projetado como um mecanismo de transição de rápida implementação, com a sua utilização não sendo recomendada para uso prolongado.

Na RFC 4380, que trata do Teredo, pode ser verificado que a tecnologia passaria por um procedimento de desligamento (*Teredo Sunset*), no qual seriam anunciadas datas em que os servidores Teredo iriam parar de prover o serviço. Esta data dependeria diretamente do grau de implementação do IPv6 nativo ou da disponibilidade de *gateways* operando em pilha-dupla.

De 9 a 15 de julho de 2013, a Microsoft realizou o primeiro teste desativando o principal servidor Teredo (teredo.ipv6.microsoft.com), presente nas configurações padrão do Windows, para medir o impacto causado conectividade IPv6 atual. Como parte do experimento, a empresa divulgou um endereço de *backup* (test.ipv6.microsoft.com) e constatou que apenas 0,01% do tráfego global do Teredo foi configurado manualmente para este servidor durante o período, evidenciando a baixa utilização da tecnologia.

Isto não significa que o Teredo vai se tornar inoperante dentro de pouco tempo e muito menos que seu aprendizado não seja importante. Na verdade, não se sabe por quanto tempo outros servidores Teredo permanecerão disponibilizando o serviço e a própria Microsoft ainda não se manifestou sobre o desligamento definitivo de seus servidores e *relays*.

Os principais servidores Teredo são:

- teredo.ipv6.microsoft.com;
- teredo.remlab.net;
- teredo2.remlab.net;
- debian-miredo.progsoc.org;
- teredo.ginzado.ne.jp;
- teredo.iks-jen.de.

Salientando que outros servidores existem e que é possível criar novos servidores Teredo.

5.4 CONFIGURAÇÃO DO AMBIENTE VIRTUAL

O ambiente criado para os testes de conectividade IPv6 conta com três instâncias instaladas no software de virtualização VirtualBox, configurados conforme a descrição a seguir.

O *firewall* pfSense (baseado em FreeBSD) foi escolhido por se tratar de uma distribuição livre e amplamente utilizada e documentada, favorecendo a criação de um cenário que pode ser encontrado em redes de pequenas e médias empresas atualmente. Foram configuradas duas placas de rede, uma em modo bridge, que recebe um IP versão 4 para acesso à Internet via roteador fornecido pela operadora, e outra, em modo de rede interna, para simular a rede local “atrás” de NAT.

Figura 61 - Detalhe da configuração das interfaces de rede do *firewall*.
Fonte: Do Autor.

Os dois *hosts* da rede utilizaram distribuições Linux, Ubuntu e Debian, nas quais foram instaladas o pacote “miredo”, que provê conectividade IPv6 em ambientes Linux e BSD. O pacote encontra-se nos repositórios oficiais das duas distribuições e pode ser instalado através do comando: apt-get install miredo. Após instalado, o serviço é iniciado junto com o sistema.

Na figura abaixo, o ambiente virtual com acesso à Internet IPv4 e IPv6.

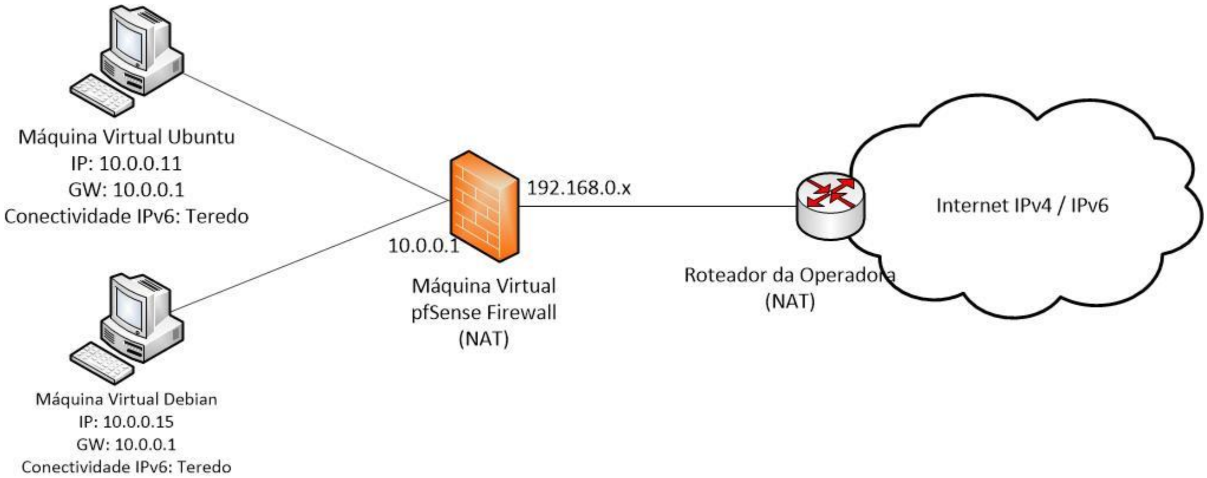
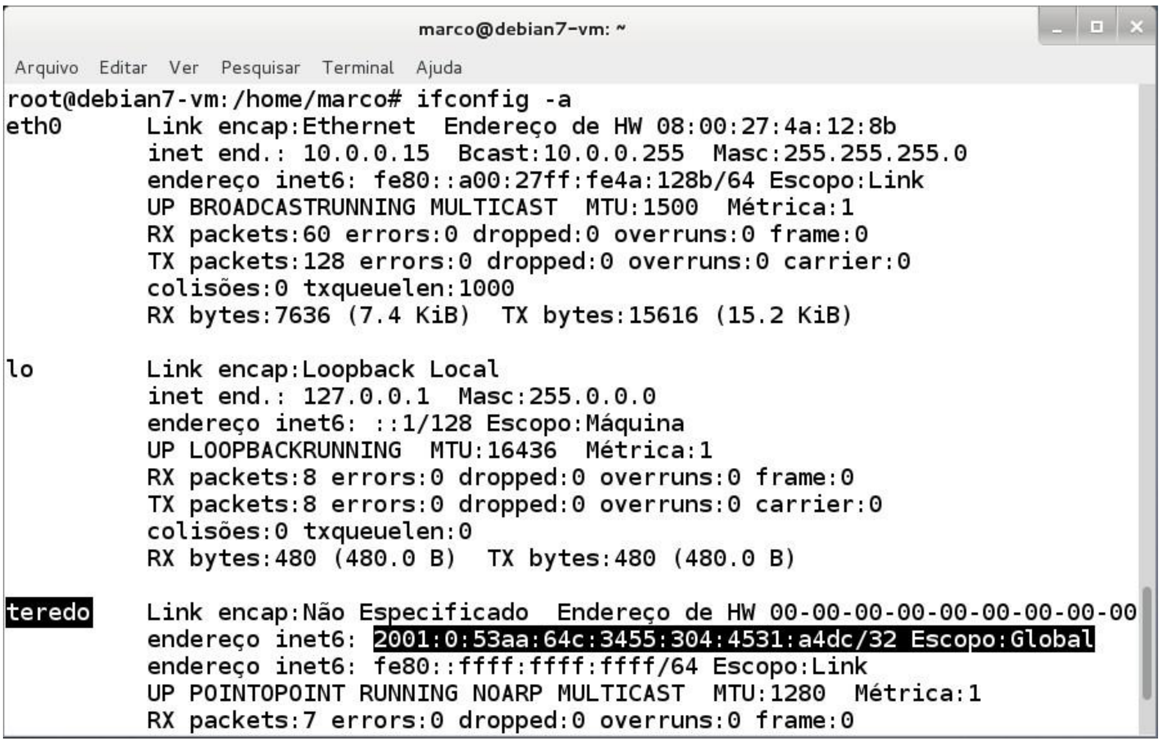


Figura 62 - Representação gráfica do ambiente virtual.
Fonte: Do Autor.

Ao iniciar os dois sistemas, foi observado, através do comando ifconfig, a criação de uma interface chamada teredo, provida pelo pacote instalado previamente. A interface já contava com um endereço IPv6 configurado, garantindo assim, a conectividade desejada.



```
marco@debian7-vm: ~
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
root@debian7-vm:/home/marco# ifconfig -a
eth0      Link encap:Ethernet  Endereço de HW 08:00:27:4a:12:8b
          inet end.: 10.0.0.15  Bcast:10.0.0.255  Masc:255.255.255.0
          endereço inet6: fe80::a00:27ff:fe4a:128b/64 Escopo:Link
          UP BROADCASTRUNNING MULTICAST  MTU:1500  Métrica:1
          RX packets:60 errors:0 dropped:0 overruns:0 frame:0
          TX packets:128 errors:0 dropped:0 overruns:0 carrier:0
          colisões:0 txqueuelen:1000
          RX bytes:7636 (7.4 KiB)  TX bytes:15616 (15.2 KiB)

lo        Link encap:Loopback Local
          inet end.: 127.0.0.1  Masc:255.0.0.0
          endereço inet6: ::1/128 Escopo:Máquina
          UP LOOPBACKRUNNING  MTU:16436  Métrica:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          colisões:0 txqueuelen:0
          RX bytes:480 (480.0 B)  TX bytes:480 (480.0 B)

teredo    Link encap:Não Especificado  Endereço de HW 00-00-00-00-00-00-00-00-00
          endereço inet6: 2001:0:53aa:64c:3455:304:4531:a4dc/32 Escopo:Global
          endereço inet6: fe80::ffff:ffff:ffff/64 Escopo:Link
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1280  Métrica:1
          RX packets:7 errors:0 dropped:0 overruns:0 frame:0
```

Figura 63 - Interface Teredo com endereço IPv6 configurado.
Fonte: Do Autor.

5.4.1 Testes de Conectividade Remota e Local

Efetuadas as instalações e configurações necessárias para o funcionamento do ambiente virtual, foram iniciados os testes de conectividade IPv6.

Com a utilização do comando ping (Packet Internet Groper), foi possível observar a resposta dos *sites* ipv6.google.com e www.v6.facebook.com. A sintaxe do comando ping no IP versão 6 difere um pouco da versão 4, ficando da seguinte forma: ping6 ipv6.google.com (ou ping -6 ipv6.google.com, em sistemas Windows).

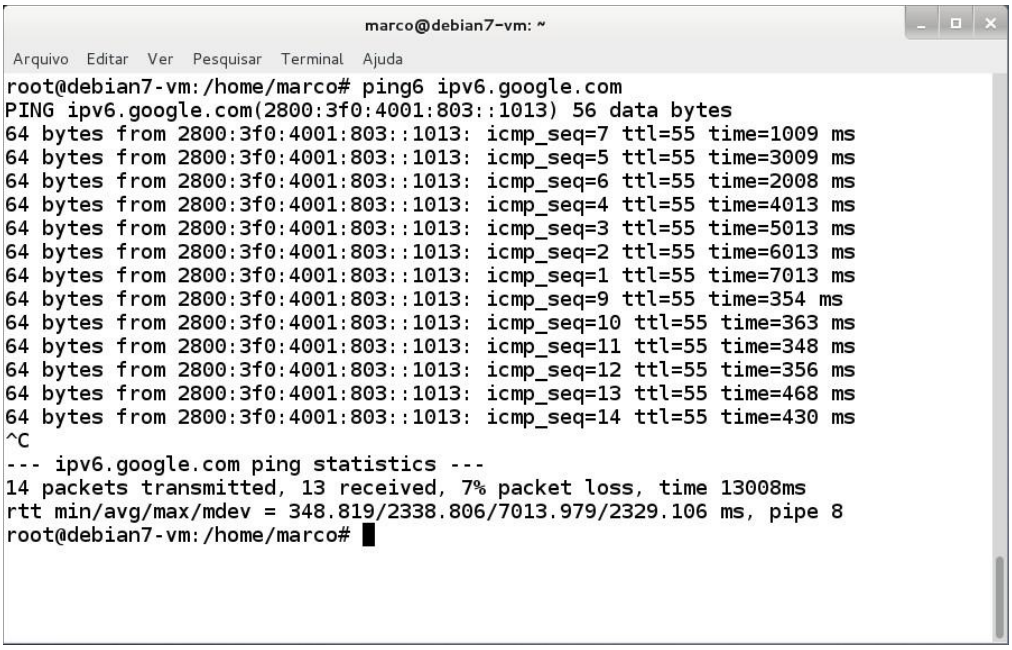


Figura 64 - Endereço IPv6 do Google respondendo ao comando ping.
Fonte: Do Autor.

Uma vez verificada a conectividade, foram efetuados testes bem-sucedidos de acesso via *browser* de ambos os sites.

Além do acesso IPv6 dos sites citados, foi efetuado um teste complementar ao acessar o site test-ipv6.com, muito utilizado para verificação de conectividade IPv6, que trouxe como resultado a identificação da técnica de acesso utilizada. O site pontua a conectividade com notas que vão de 0 à 10 e a diferença entre o acesso empregando ou não o mecanismo de transição Teredo pode ser vista na figura a seguir.

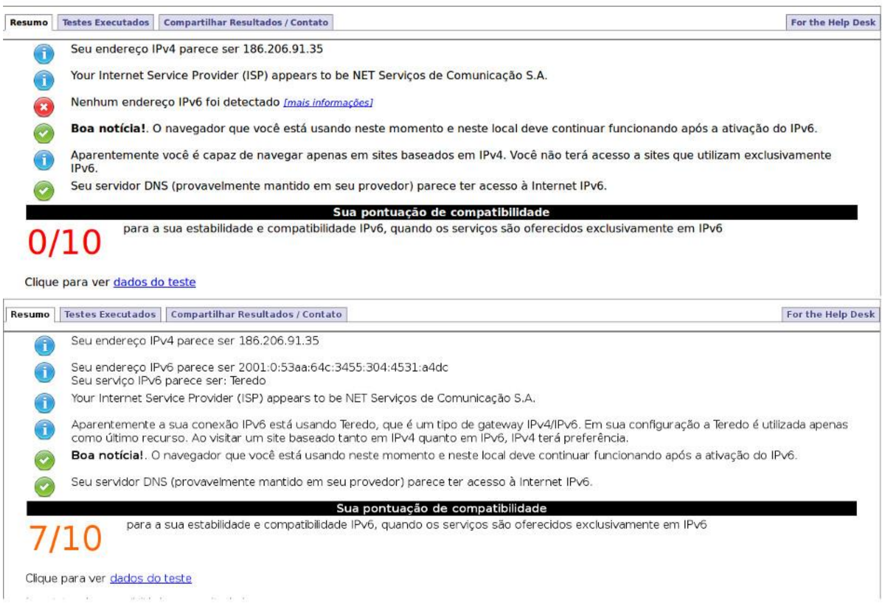


Figura 65 - Resultados da avaliação online de conectividade IPv6.
Fonte: Do Autor.

Adicionalmente, foram realizados testes de conectividade entre nós do mesmo enlace utilizando os endereços IPv6 do tipo *link-local*. Como já citado, nós do mesmo enlace se comunicam a nível de rede, utilizando endereços IPv6 específicos autoconfigurados, uma vez que, na versão 6 do IP, uma interface pode ter mais de um endereço.

Neste caso, é necessário adicionar o parâmetro -I e especificar a interface de saída do comando. Como no exemplo: ping6 -I eth0 fe80::a00:27ff:fe2a:128b

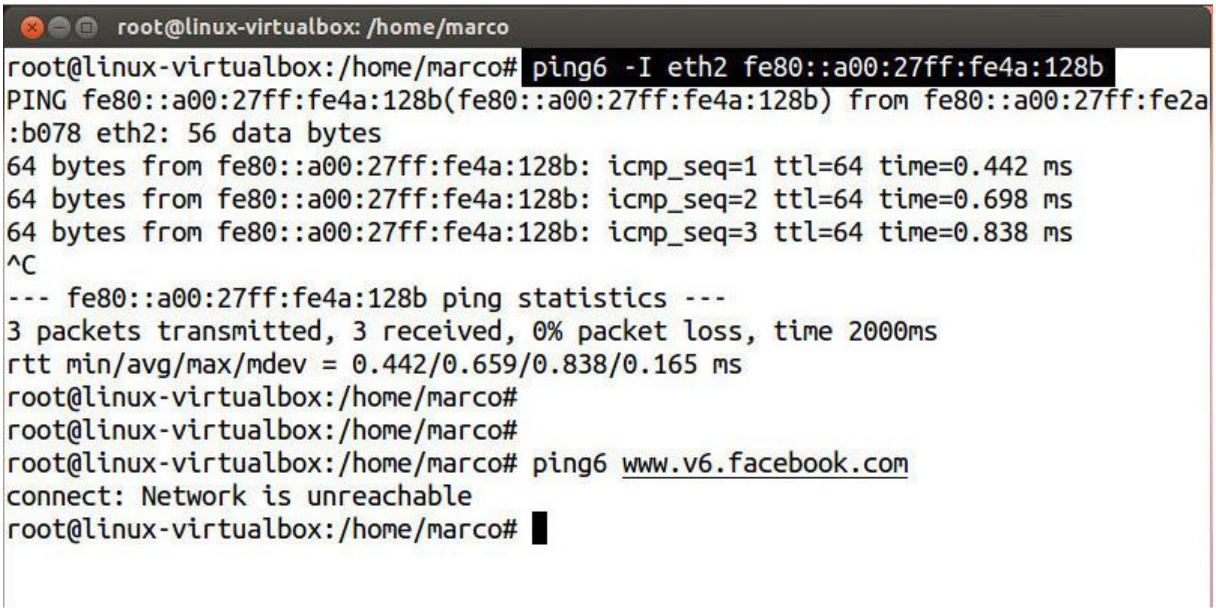


Figura 66 - Teste de conectividade IPv6 local.
Fonte: Do Autor.

Foram realizados ainda, outros testes de acesso no ambiente virtual utilizando programas e protocolos de uso comum em redes IPv4, através dos endereços IPv6 do tipo *link-local*.

O *software* de varredura de portas Nmap, muito utilizado para avaliar a segurança e descobrir serviços de uma rede de computadores, funciona em IPv6 com uma sintaxe um pouco diferente e ainda possui alguns parâmetros inoperantes em comparação com as varreduras efetuadas em IPv4. Entretanto, é possível fazer um escaneamento de portas simples utilizando endereços do tipo *link-local*.

Durante os testes, o *host* Ubuntu foi capaz de verificar as portas abertas por serviços do host Debian, utilizando a seguinte sintaxe: nmap -6 fe80::a00:27ff:fe2a:128b%eth2.

Figura 67 - Escaneamento de portas local com o programa Nmap em IPv6.
Fonte: Do Autor.

No teste seguinte, o *host* Debian foi configurado como servidor de arquivos com a instalação do *software* vsftpd.

Por padrão, o servidor vsftpd vem configurado para “ouvir” requisições IPv4, sendo necessária a configuração manual atender requisições IPv6, uma vez que, o *software* não é capaz de atendê-las simultaneamente. Para atender ambas, teriam que ser instaladas duas instâncias do vsftp. Uma para cada versão do IP.

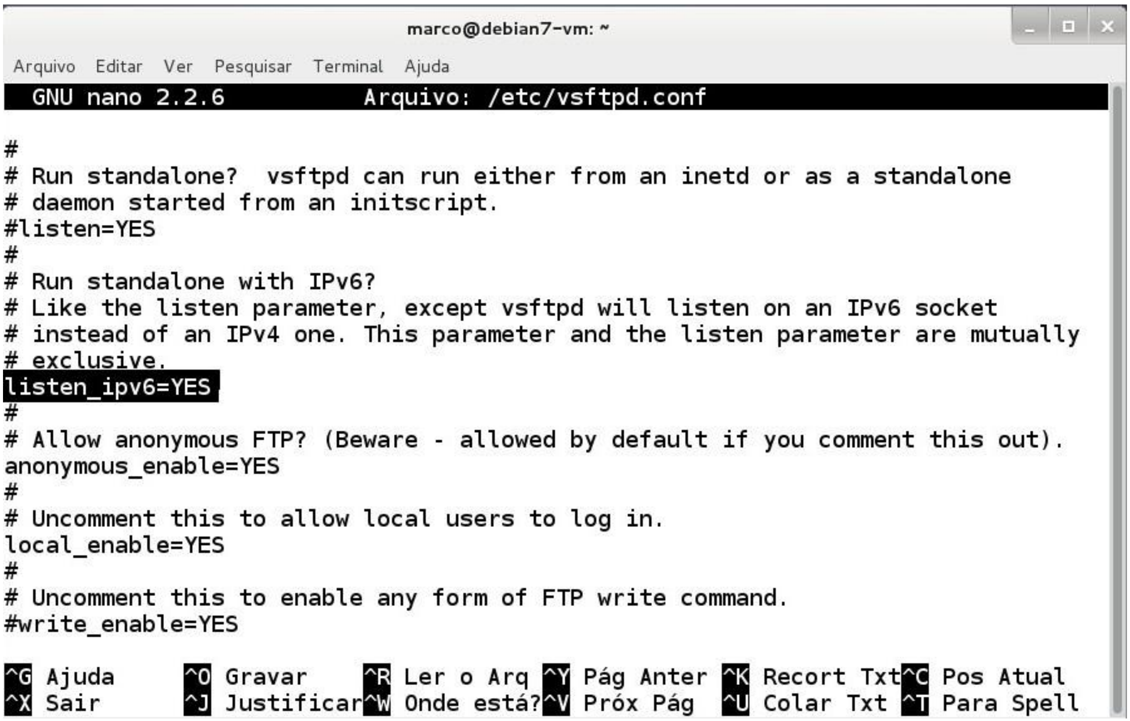


Figura 68 - Configuração do servidor FTP para atender requisições IPv6.
Fonte: Do Autor.

Configurado o servidor, foi instalado no *host* Ubuntu, o *software* cliente FTP Filezilla e efetuado um teste de acesso ao servidor Debian.

De forma diferente do IPv4, onde é inserido diretamente o endereço IP do servidor no campo “*Host*” do Filezilla, em IPv6, o endereço deve estar entre colchetes e seguido da informação da interface de acesso do cliente.

Exemplo: [fe80::a00:27ff:fe2a:128b%eth2].

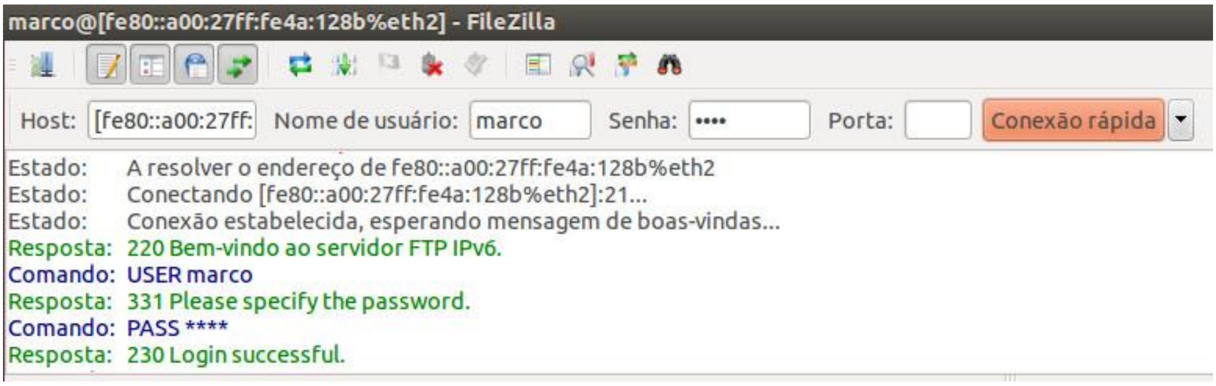


Figura 69 - Detalhe do cliente FTP acessando o servidor em IPv6.
Fonte: Do Autor.

Finalmente, foi efetuado um teste de acesso via SSH utilizando o endereço IPv6 *link-local*.

Neste teste foi observado que não é necessário parâmetro algum que indique a utilização do IPv6, a única mudança na sintaxe é, mais uma vez, a inclusão da interface de acesso do cliente.

Exemplo: ssh fe80::a00:27ff:fe2a:128b%eth2

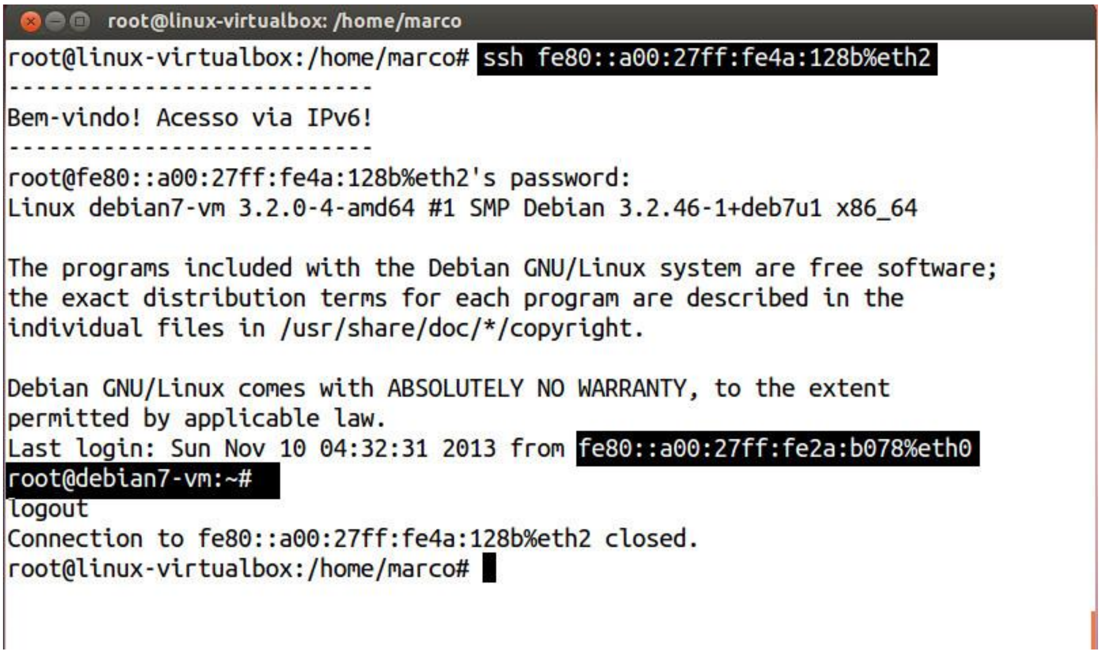


Figura 70 - Acesso SSH entre máquinas virtuais via IPv6.
Fonte: Do Autor.

5.4.2 Captura de Pacotes

Com a utilização do analisador de pacotes Wireshark foi possível fazer a identificação do tráfego IPv6 na interface conectada ao *firewall*.

O software permitiu identificar o tunelamento Teredo, bem como o protocolo de transporte UDP, a porta padrão 3544 da tecnologia de transição e o endereço

IPv6 do site que estava sendo acessado.

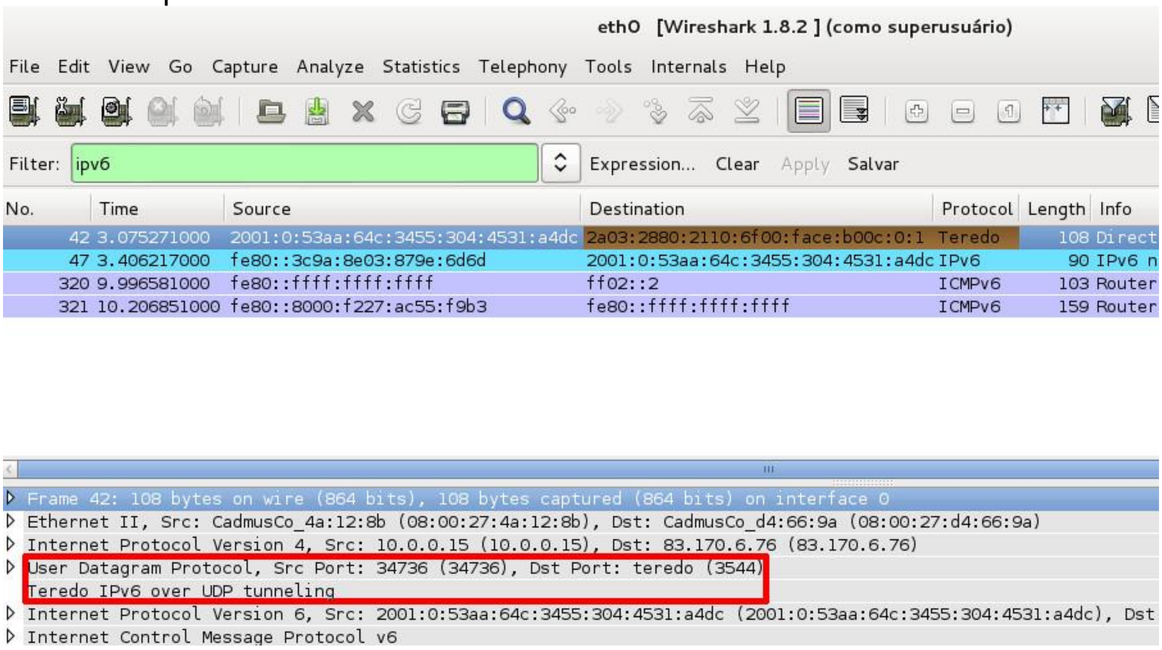


Figura 71 - Confirmação da utilização da tecnologia Teredo para acesso à Internet IPv6.
Fonte: Do Autor.

A próxima figura mostra o momento da troca de chaves do acesso remoto via SSH, destacando o algoritmo de criptografia Diffie-Hellman.

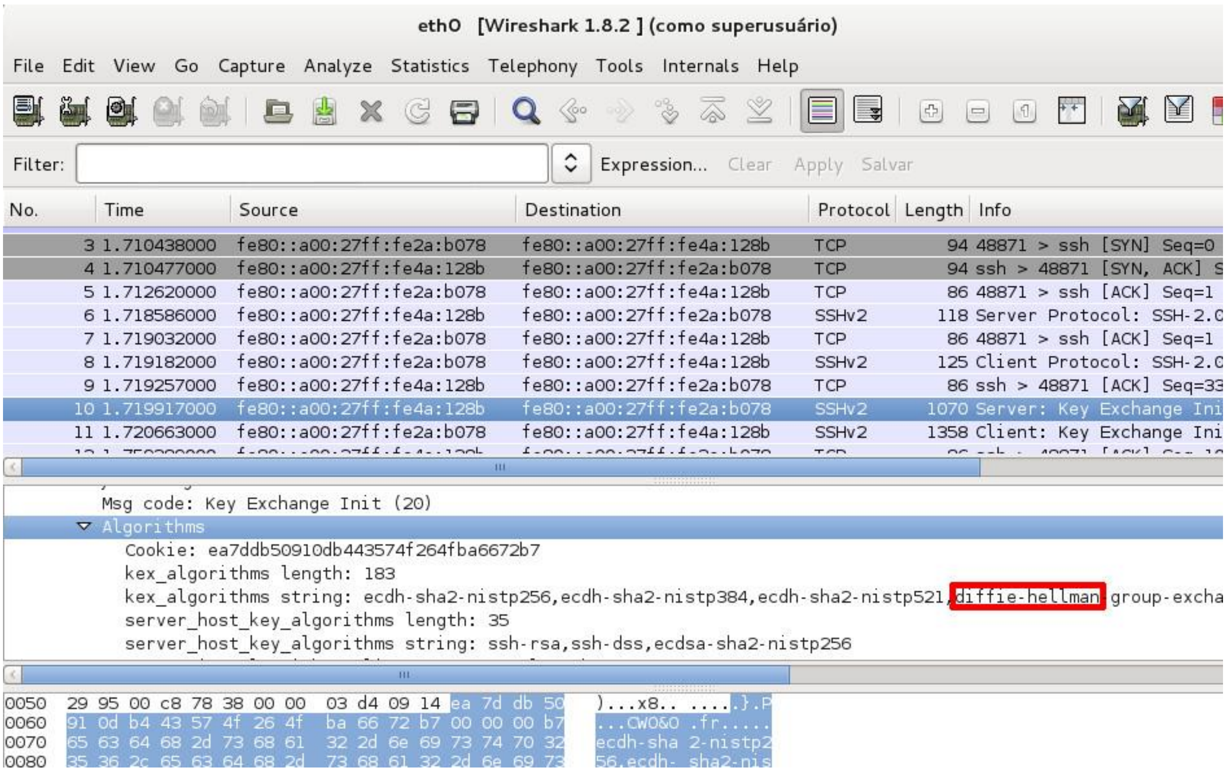


Figura 72 - Captura de pacotes do acesso SSH no momento da troca de chaves.
Fonte: Do Autor.

Durante a captura de pacotes do acesso ao servidor FTP foi possível visualizar a senha de acesso do usuário.

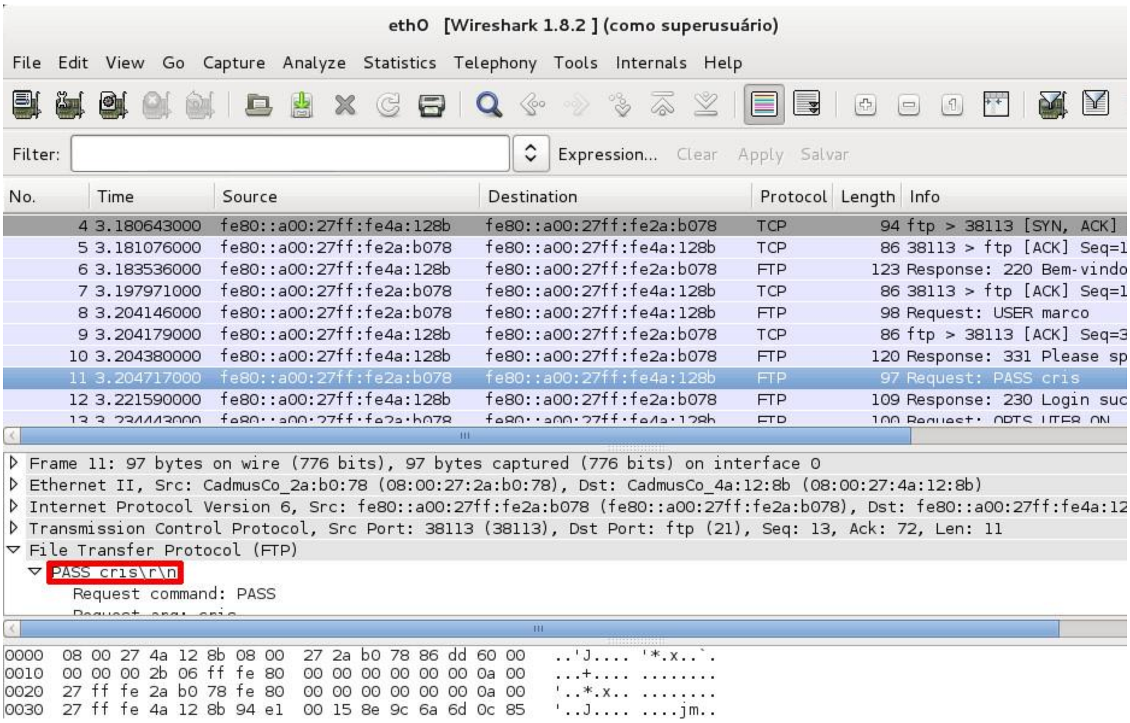


Figura 73 - Detalhe da captura da senha durante o acesso ao servidor FTP via IPv6.
Fonte: Do Autor.

5.4.3 Regras de *Firewall* no Ambiente Virtual

Num ambiente protegido por *firewall* é possível controlar o tráfego de entrada e saída com o objetivo de trazer segurança para a rede através da aplicação de regras.

Como mencionado, devido ao encapsulamento IPv4, tráfego IPv6 não solicitado pode acabar passando pelo *firewall* se as regras apropriadas não forem aplicadas.

Durante o estudo da bibliografia, constatou-se a necessidade da aplicação de regras no *firewall* relacionadas a conectividade proporcionada pelo método de funcionamento do tunelamento automático da tecnologia Teredo, que possibilita brechas de segurança.

No ambiente de rede virtualizado do trabalho, com o tráfego IPv4 liberado, foi possível trazer tráfego IPv6 para a rede interna de maneira relativamente fácil. Como exemplo, num dos *hosts* da rede foi aplicada a regra que bloqueia o tráfego IPv6 proporcionado pelo Teredo para demonstrar como utilizar a tecnologia para testes de maneira segura, liberando ou bloqueando o acesso para hosts específicos.

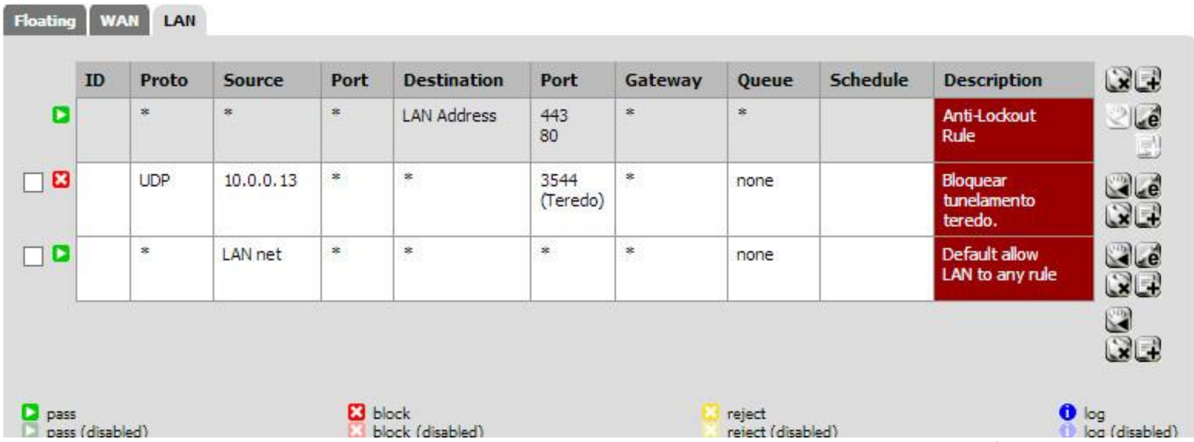


Figura 74 - Regra de firewall que bloqueia o tunelamento no *host* específico.
Fonte: Do Autor.

Após a configuração de bloqueio para o *host* Ubuntu, foi verificado que a Internet IPv6 tornou-se inacessível. Como pode ser confirmado na figura abaixo.

Figura 75 - Internet IPv6 inacessível após bloqueio no firewall.
Fonte: Do Autor.

O procedimento para liberar novamente o acesso a um *host* bloqueado requer dois passos, bastando desabilitar a regra do *firewall* que executa o bloqueio e reiniciar o tunelamento Teredo no respectivo *host* através do comando: service miredo restart. Após este procedimento, o *host* volta a ter conectividade IPv6.

Como pode ser observado na próxima figura, o servidor ipv6.google.com encontrava-se inatingível. Após a liberação no *firewall* e o reinício do serviço, o comando ifconfig apresenta um endereço IPv6 Teredo e o servidor volta a responder.

Figura 76 - Reinicialização do serviço de tunelamento.
Fonte: Do Autor.

Certamente, conhecer a porta UDP 3544, padrão do Teredo, é de suma importância para administradores de rede, uma vez que ele é instalado e habilitado por padrão a partir dos sistemas Windows Vista e 7, sistemas operacionais amplamente utilizados nas redes das empresas.

7 CONCLUSÕES E RECOMENDAÇÕES

O estudo permitiu a compreensão do cenário atual, no qual tem-se a escassez de endereços e a demanda por serviços nos quais o IPv4 já não é mais adequado, como o IPv6 foi projetado para suprir estas necessidades e como as tecnologias de transição vêm para auxiliar na migração gradual de um ambiente de rede.

Em seus trinta anos de uso, o IPv4 passou por uma série de refinamentos e cumpriu bem a sua função, mostrando suas qualidades e deficiências e servindo de base para o protocolo IPv6.

Os testes práticos na rede virtualizada, realizados neste trabalho, permitiram conhecer as características da técnica Teredo, com suas vantagens e limitações e o funcionamento da conectividade IPv6 em redes locais.

Adicionalmente, foi possível conhecer as questões de segurança inerente às tecnologias de tunelamento automático, especialmente o Teredo, e as soluções para a sua utilização de forma segura.

Com base nos estudos e testes efetuados no trabalho realizado, foram obtidas as seguintes conclusões:

a) O trabalho permitiu um estudo sobre a problemática da lenta implementação do IPv6 em contraste à urgente necessidade de endereços, uma vez que a Internet precisa continuar a crescer e os dispositivos utilizam cada vez mais o protocolo IP;
b) As técnicas de transição existentes são ferramentas que devem ser utilizadas para uma migração gradual e segura, pois possibilitam a execução de testes sem a necessidade de mudanças estruturais;
c) A operação simultânea dos protocolos IPv4 e IPv6 nas redes atuais, exige dos profissionais o conhecimento mais detalhado de ambos os protocolos e dos mecanismos de transição, pois possuem características e regras de firewall distintas;
d) A técnica de tunelamento Teredo levanta questões de eficiência e segurança a serem consideradas. Contudo, em alguns casos, pode ser a única alternativa disponível e a importância de seu conhecimento advém do fato de ser implementado automaticamente em algumas versões do Windows, o sistema operacional mais amplamente utilizado.

Desde 2011, o tráfego IPv6 monitorado pelo Google vive uma situação de pleno crescimento.

Figura 77 - Crescimento dos acessos ao Google por meio de IPv6.
Fonte: Huston.

A movimentação no *backbone* da Internet em direção ao IPv6 pode ser notada, dada a implementação do protocolo em dez, dos treze *root servers* da rede.

Internamente, Google e Facebook já iniciaram a utilização do IPv6 em larga escala.

O IPv6 tornou-se padrão de fato em junho de 2012 e, certamente, alguns ajustes serão necessários à medida que a grande massa de usuários iniciar a utilização mas não resta dúvidas sobre o seu crescimento nos próximos anos.

Nacionalmente, o Núcleo de Informação e Coordenação do Ponto BR (NIC.br), promove ações para fomentar a adoção do IPv6 no Brasil, através de cursos, palestras e congressos que visam disseminar a importância da implantação do protocolo.

Portanto, é chegada hora de parar de se referir ao IPv6 como o “novo protocolo” e, aos poucos, acostumar-se a chamar o IPv4 de “protocolo antigo”.

Por fim o trabalho foi importante tendo atingido os objetivos inicialmente propostos.

BIBLIOGRAFIA REFERENCIADA E CONSULTADA

BRITO, Samuel Henrique Bucke. **IPv6 – O novo protocolo da Internet**. 1ª ed., Editora Novatec, 2013.

COMER, Douglas. ***Computer Networks and Internets***. 5ª ed., Editora Prentice Hall, 2008.

CORDEIRO, Edwin. **Teredo Sunset – Mais um passo na transição para o IPv6**. Disponível em: http://ipv6.br/teredo-sunset-mais-um-passo-na-transicao-para-o-ipv6/. Acesso em 27/11/2013.

DAVIES, Joseph. ***Understanding IPv6***. 3ª ed., Microsoft Press, 2012.

DENIS-COURMONT, Rémi. ***Miredo : Teredo IPv6 tunneling for Linux and BSD***. Disponível em: http://www.remlab.net/miredo/intro.shtml. Acesso em 20/11/2013.

GOMES, Alexandre José, **Rede IP I:Melhores Práticas de Migração de Rede IPv4 para IPv6**. Disponível em: http://www.teleco.com.br/tutoriais/tutorialredeipmig1/default.asp. Acesso em 19/11/2013.

GRAZIANI, Rick. ***IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6***. 1ª ed., Cisco Press, 2012.

HUGHES, Lawrence E. ***The Second Internet - Reinventing Computer Networking with IPv6**.* 1ª ed, InfoWeapons, 2010.

HUSTON, Geoff. ***A Primer on IPv4, IPv6 Transition***. Disponível em http://www.potaroo.net/ispcol/2013-04/primer.html. Acesso em 19/11/2013.

HUSTON, Geoff. ***A Year in Life***. Disponível em http://www.potaroo.net/ispcol/2013-06/ipv6-365.html. Acesso em 19/11/2013.

HUSTON, Geoff. ***Testing Teredo***. Disponível em https://labs.ripe.net/Members/gih/testing-teredo. Acesso em 20/11/2013.

KUROSE, Jim; ROSS, Keith. ***Computer Networking – A Top-down Approach***. 6ª ed., Editora Pearson Education, 2013.

MOREIRAS, Antonio Marcos. **Transição.** Disponível em: http://ipv6.br/entenda/transicao/. Acesso em 20/11/2013.

MOTA FILHO, João Eriberto. **Descobrindo o Linux.** 3ª ed., Editora Novatec, 2012.

RFC 2460. ***Internet Protocol, Version 6 (IPv6) Specification***. Disponível em: http://tools.ietf.org/html/rfc2460. Acesso em 27/11/2013.

RFC 2663. ***IP Network Address Translator (NAT) Terminology and Considerations***. Disponível em: http://tools.ietf.org/html/rfc2663. Acesso em 27/11/2013.

RFC 4291. ***IP Version 6 Addressing Architecture***. Disponível em: http://tools.ietf.org/html/rfc4291. Acesso em 27/11/2013.

RFC 4380. ***Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)***. Disponível em: http://tools.ietf.org/html/rfc4380. Acesso em 27/11/2013.

TANENBAUM, Andrew S; WETHERALL, David J. ***Computer Networks***. 3ª ed. Editora Prentice Hall, 2011.

WILLIAMSON, Matt. ***pfSense 2 Cookbook***. 1ª ed., Editora Packt, 2011.

SISTEMA DE IRRIGAÇÃO CONTROLADO VIA CLP

IRRIGATION SYSTEM CONTROLLED BY CLP

Ivan de Oliveira[16]
Anderson José da Silva[17]
Tiago Manczak (Orientador)[18]

OLIVEIRA, Ivan de; SILVA, Anderson José da, MANCZAK, Tiago (orientador). **Sistema de Irrigação Controlado via CLP**. *Revista Tecnológica da FATEC-PR, v.1, n.4, p. 161 - 185, jan./dez., 2013.*

RESUMO:

O projeto consiste em controlar o fluxo de água utilizando para irrigação em gramados por intermédio de sensores conectados a um PLC devidamente programado. Os sensores serão utilizados para supervisão de temperatura e umidade relativa do ar com a finalidade de criar condições satisfatórias para a conservação de jardins. O CLP em questão envolve um sistema de supervisão, como indicação de alarmes em tempo real apresentados por um sistema supervisório com emissão de relatórios e controle de usuários. Uma replica de um gramado foi construída para a simulação do sistema em funcionamento

Palavras-chave: Eletricidade. Automação Industrial. Projeto de Automação.

ABSTRACT:

The project is a automated irrigation control system, that uses sensors connected to a properly programmed CLP. The sensors are used for monitoring temperature and relative humidity in order to create good conditions for the conservation of gardens. The programming of the chosen PLC involves a system of supervision with real time alarm signals presented by a supervisory system which has reporting and user management functionalities. A replica of a garden was built for the simulation of the system.

Keywords: *Electricity. Industrial Automation. Automation Project.*

1 INTRODUÇÃO

A irrigação está se tornando cada vez mais popular. Muito diferente do que quando surgiu, no hemisfério norte, no início do século, somente com o objetivo de suprir a falta d'água dos gramados e canteiros das cidades mais quentes e secas. Paulatinamente a automação vem sendo introduzida à irrigação para substituir os métodos manuais, tornando mais eficiente (CODESVASF, 2010).

---

[16] Ivan de Oliveira é graduado em Tecnologia em Eletrônica Industrial pela FATEC-PR (2013). Atua como profissional em empresa de grande porte na área de Eletrônica.

[17] Anderson José da Silva é graduado em Tecnologia em Eletrônica Industrial pela FATEC-PR (2013). Atua como profissional em empresa de grande porte na área de Eletrônica.

[18] Tiago Manczak foi o Orientador dos acadêmicos. Mestre em Engenharia Biomédica pela Universidade Tecnológica Federal do Paraná (UTFPR/2012). Especialização em Redes e Segurança de Sistemas. Graduado em Engenharia Elétrica (Eletrônica/Telecomunicaçõe) pela UTFPR. Tem experiência na área de Engenharia Eletrônica, com ênfase em Biomédica Lógicas e Semântica de Programas, atuando principalmente nos seguintes temas: automatização, eletrônica industrial, projeto de software e sistemas embarcados. Trabalha na COPEL, empresa do setor Elétrico como Engenheiro de Automação de Subestações de Transmissão.

Para uso em jardinagem, existem vários métodos práticos de irrigação: Aspersão estática, aspersão giratória, aspersão oscilantes, gotejamento simples, gotejamento automático entre outros que vamos explicar.

No mercado podem ser encontrados sistemas comerciais para automação de irrigação, como por exemplo, a GARDENA (Alemã) e a NUTRIJARD (GARDENA, 2011).

1.1 OBJETIVO GERAL

Implantar um sistema de irrigação utilizando um equipamento já existente no mercado, CLP (CMC-TC). Com o intuito de automatizar o sistema de irrigação, facilitando o dia-a-dia de usuários do sistema. Realizar a montagem de protótipo de um jardim, para simular a irrigação do mesmo através do CLP (CMC-TC)

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos do trabalho foram os seguintes:

- Desenvolver um projeto utilizando os seguintes componentes: CLP, sensor de temperatura, sensor de umidade, válvula solenoide, irrigador, temporizador, disjuntor e led;
- Estudar os tipos de irrigação existentes no mercado;
- Demonstrar e explicar o funcionamento de um CLP no sistema de irrigação.

2 JUSTIFICATIVA

Os sistemas de irrigação ocupam cada vez mais espaços em jardins residenciais, estágios de futebol, agricultura, estufas e outras aplicações em geral (UNESP, 2003).

Pensando nisso, foi desenvolvido um projeto de irrigação via CLP (CMC-TC), controlado por um sensor de temperatura (RITTAL 7320.580) e um sensor de umidade relativa do ar (RITTAL 7320.510), tendo como principal vantagem, a economia de água, visando o meio ambiente.

3 METODOLOGIA

Trata-se de uma pesquisa bibliográfica e aplicada, referente a sistema de irrigação com CLP. Prevê as seguintes fases / etapas:

a) Seleção e estudo da bibliografia;
b) Estudo de manuais disponíveis de fabricantes da RITTAL e ACECO TI;
c) Estudo de manuais do CLP (CMC-TC);
d) Levantamento dos componentes que serão necessários para a montagem do protótipo;
e) Montagem, testes e ajustes do protótipo;
f) Análise comparativa entre a teoria e a prática;
g) Apresentação das conclusões e considerações;
h) Elaboração do relatório final.

4 REVISÃO BIBLIOGRÁFICA

4.1 IRRIGAÇÃO

Até o Século 19 a irrigação ainda era realizada sem a utilização de equipamentos específicos e somente utilizava-se de métodos como o de inundação e através de sulco.

Um fato muito importante para a irrigação no mundo foi à criação do primeiro aspersor de impacto, criado por Orlan Englehart que foi um cultivador de citrus residente no sul da Califórnia no ano de 1933, desta forma (RAIN BIRD RJ, 2003) a revolucionou a história da produção de alimento e iniciou uma nova era na irrigação mundial.

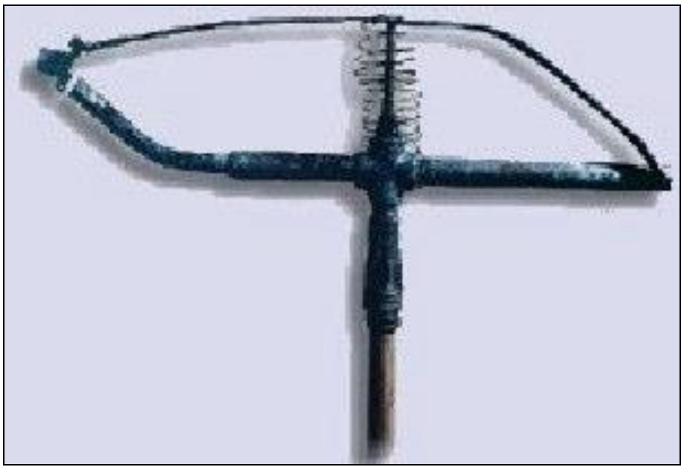


Figura 78 - Primeiro aspersor de impacto.
Fonte: RAIN BIRD RJ (2003, p. 2).

A Irrigação então começou a se dividir em métodos conforme as técnicas e a série de produtos utilizada. As principais técnicas são: irrigação por Aspersão, Irrigação Localizada (basicamente gotejamento e microaspersão) e a Irrigação por Superfície (sulcos e inundação, que são os mais antigos).

4.2 ASPERSÃO ESTÁTICA

Esta técnica consiste em uma base fixa que se encaixa na ponta de uma mangueira e, com a pressão, a água cai no terreno de forma semelhante à chuva.

Figura 79 - Aspersor estático.
Fonte: Casos de Casa (2009).

4.3 ASPERSÃO GIRATÓRIA

A aspersão giratória funciona como os estáticos, mas abrangem uma área maior. São os mais numerosos entre os portáteis e outros.

Figura 80 - Aspersor giratório.
Fonte: Casos de Casa (2009).

4.4 ASPERSÃO OSCILANTE

São os mais versáteis dentre todos os irrigadores. Nele, o fluxo de água provoca a movimentação de um braço cheio de furos, não em círculo, mas em meia lua.

Figura 81 - Aspersor oscilante.
Fonte: Casos de Casa (2009).

4.5 GOTEJAMENTO SIMPLES

Trata-se de uma mangueira ou conduíte com pequenos furos colocados próximo ao caule dos arbustos, de modo a umedecer continuamente as raízes. A vantagem de se utilizar a irrigação por gotejamento é, basicamente, o controle. Esse método de irrigação é preciso e econômico.

Figura 82 - Sistema de gotejamento por mangueira.
Fonte: G1 (2013).

4.6 GOTEJAMENTO AUTOMÁTICO

O sistema é o mesmo, mas tudo é controlado por um sistema eletrônico, podendo adicionar também a liberação de fertilizantes na quantidade certa e tempo de uso pré-determinados pelo produtor.

Figura 83 - Sistema de gotejamento automático.
Fonte: Casos de Casa (2009).

4.7 PIVÔ CENTRAL

O sistema consiste por uma tubulação metálica onde são instalados os aspersores. A tubulação recebe a água do ponto do pivô, que se apoia em torres metálicas triangulares, mantém-se a uma elevação pré-fixa do solo (2,70 ou 3,70 de altura livre sob a estrutura) sendo suspensa por torres equipadas com rodas pneumáticas do tipo trator.

Figura 84 - Irrigação por pivô central.
Fonte: http://www.gruposervplan.com.br (2011).

4.8 IRRIGAÇÃO POR SULCOS

Um método que consiste na distribuição de água através de pequenos canais, paralela às fileiras das plantas. Tem menor custo fixo e operacional, e consome menos energia que os métodos por aspersão, mas tem a desvantagem da baixa eficiência que é em torno de 30% a 40%.

1 Figura 85 - Irrigação por sulcos
2 Fonte: AGEITEC (2011)

4.9 *BROWSER*

Trata-se de um programa de computador desenvolvido para interagir com documentos virtuais da internet, conhecido como página da web e é capaz de processar diversas linguagens. O browser é responsável pela comunicação com os servidores (ACECO-TI, 2003).

4.10 SISTEMA HYPERTERMINAL

É um aplicativo do *Windows* utilizado para estabelecer ligação com o sistema hiperterminal, também influência no suporte de instalação, ainda que possa não ser automaticamente instalado (ACECO-TI, 2003).

5 DESENVOLVIMENTO

Nessa etapa do trabalho, o foco é a análise, avaliação das características e aspectos técnicos com maior profundidade, conhecer o sistema de monitoramento (NET WATCH) a sua configuração, ferramentas e equipamentos que vão ser usadas para a montagem do projeto.

5.1 DIAGRAMA DE BLOCO

A figura 9 representa o diagrama de blocos do projeto do Sistema de Irrigação Controlado via CLP.

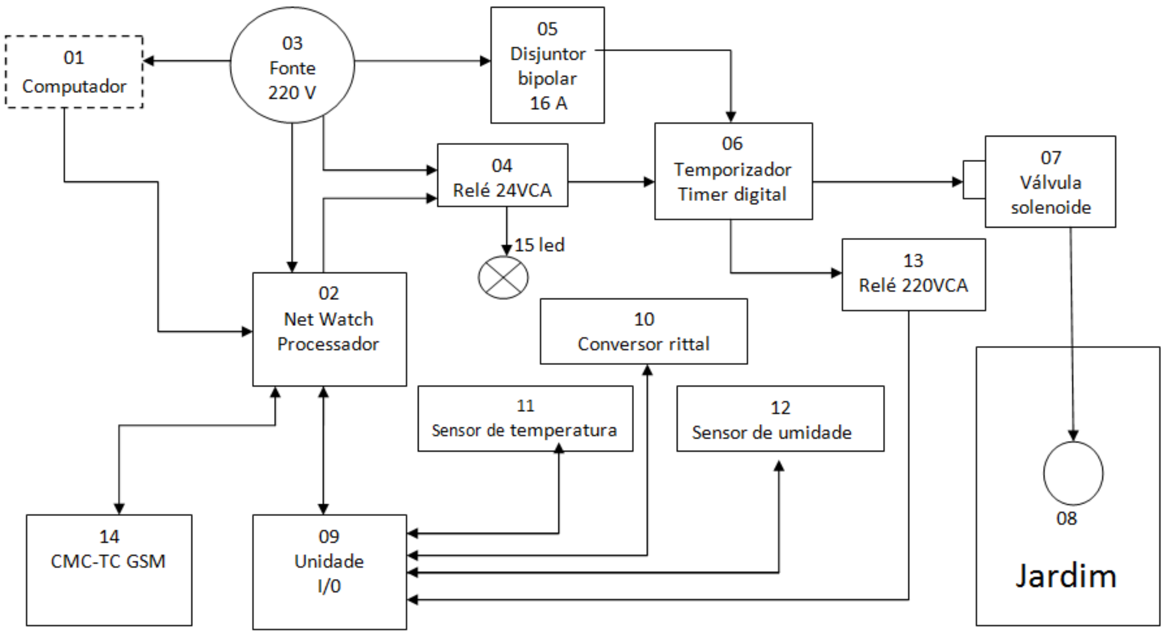


Figura 86 - Diagrama de blocos do Projeto.
Fonte: Autores.

Os seguintes componentes estão representados no diagrama de blocos do projeto:

1) Computador: é utilizado para configurações e parametrizações do *Net Watch*;
2) Net Watch: processa os dados recebidos pela a unidade I/O, unidade GSM e energizar o relé 24 VCA de acordo com o comando nele configurado;
3) Fonte 220V: alimenta o computador, *Net Watch*, unidade GSM, temporizador e solenoide;
4) Relé 24VCA: Ao alimentar a bobina com 24VCA o mesmo fica responsável por energizar o temporizador;
5) Disjuntor bipolar 16 A: *by-pass* do sistema de automação;
6) Temporizador digital: atua pela programação de tempo de trabalho da válvula solenoide;
7) Válvula solenoide: responsável pelo fluxo de água;
8) Jardim: protótipo do projeto;
9) Unidade I/O: monitoramento de alarmes;

10) Conversor Rittal 580: monitora a energização da bobina da válvula solenoide;
11) Sensor de temperatura: faz a leitura da temperatura ambiente;
12) Sensor de umidade: faz a leitura da umidade relativa do ar;
13) Relé 220V: relé que monitora a energização da bobina da válvula solenoide;
14) CMC-TC GSM: envia SMS para os números cadastrados na unidade GSM.

5.2 UNIDADE PROCESSADORA (CMC-TC).

O CMC–TC é uma unidade processadora que, após receber os dados captados por sensores definidos, processa-os, e permite obter, remotamente, via rede, os status de cada uma das operações.

O CLP CMC TC é fabricado pela empresa alemã Rittal Gmbh (figura 10).

Figura 87 - CMC_TC (Computer Multi Control – Top Concept).
Fonte: RITTAL GMBH (2004, p.30).

Sua função é receber os dados das entradas, processá-los de acordo com a sua programação, e enviar via rede os dados da situação. Os dados de alarme e status são trocados com a rede, via protocolo TCP/IP.

A programação do equipamento é feita via hyperterminal e através de cabo serial com conexão RJ 11 diretamente na Unidade de Processamento.

A linguagem de programação desta unidade é baseada em Java e possui entradas digitais e analógicas ampliando ainda mais sua utilização para controles mais precisos. A unidade de aquisição de dados é um modulo conectada a unidade central de processamento (CMC-TC) conectado via cabo ethernet cat-5 padrão 10/100 conectorizados

5.3 PARÂMETROS DO CMC-TC

Representação dos parâmetros da unidade processadora, unidade I/O e unidade GSM.

5.3.1 Unidade Processadora CMC-TC

A unidade de processamento de forma é à base do Sistema CMC-TC. Esta unidade é necessária para cada aplicativo do monitoramento. A seguir estão descritos seus parâmetros e para que servem.

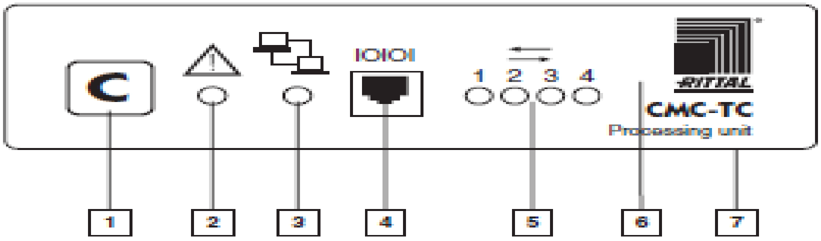


Figura 88 - Painel frontal da unidade processadora CMC-TC.
Fonte: RITTAL GMBH (2004, p.30)

No painel estão instalados os componentes a seguir.

1) Tecla Controle: É usada para reconhecer a detecção do sistema.
2) Alarme de led: Sinaliza alterações ou configuração.
3) *Link* / Tráfego: O led sinaliza que levou os estado da rede 10 *BaseT interface.*
4) RS 232 RJ 11: Para a programação através da PC interface serial.
5) Canais de *LEDs*: Estes *LEDs* indicam o estado das unidades de sensores.
6) Alarme acústico: Dispositivo de sinalização integrado para a UP.
7) Dispositivo de montagem: Para a fixação com nylon velcro.

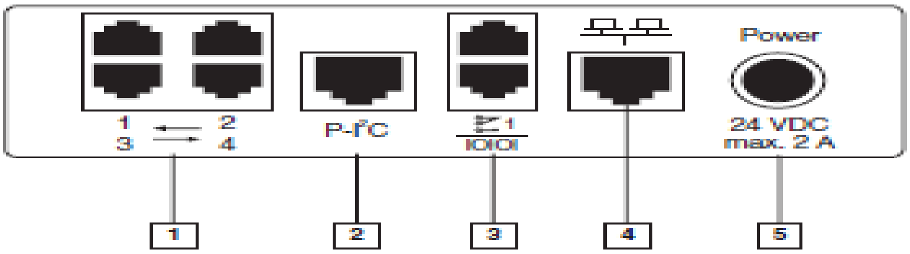


Figura 89 - Painel traseiro da unidade processadora CMC-TC.
Fonte: RITTAL GMBH (2004, p.30).

No painel traseiro consta uma série de componentes.

3 Entradas para sensor: Até quatro unidades de sensor pode ser ligado ao UP.
4 Bus I2C: Até duas extensões 7200.520 unidades pode ser ligado através da alimentação Bus I2C
5 Alarme de relé RJ 12/RS 232: Transição de contato do alarme UP para relé
6 Ethernet 10BaseT: *Interface Ethernet* a IEEE 802.3 10BaseT via *half-duplex* de 10 Mbit / s.
7 Fonte de alimentação: A tensão nominal para o UP é de 24 VDC

5.3.2 Unidade I/O

A unidade de I / O tem quatro entradas e saídas universais. Os sensores e atuadores listados abaixo podem ser operados aqui. A interface para o utilizador rede é via o UP (unidade de processamento), que é sempre requerida para operar o sistema.

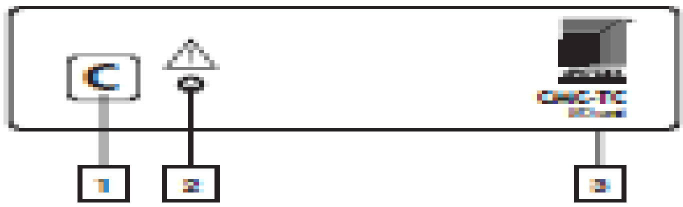


Figura 90 - Painel frontal da unidade de sensor I/O.
Fonte: RITTAL GMBH (2004, p.30).

1. Tecla Controle: Para a detecção / set-up dos sensores / atuadores.
2. Alarme *LED*: Sinais de alarmes ou alterações de configuração.
3. Fixação de montagem.

Figura 91 - Painel traseiro da unidade de sensor I/O
Fonte: RITTAL GMBH (2004, p.30)

1. Quatro entradas para sensores /atuadores.
2. RJ 45, conexão com PU via cabo de conexão.

5.3.3 Unidade GSM CMC-TC

A unidade GSM CMC-TC serve para monitorar e avisar de algum alarme acorrido, mandando um aviso no E-MAIL ou via SMS.

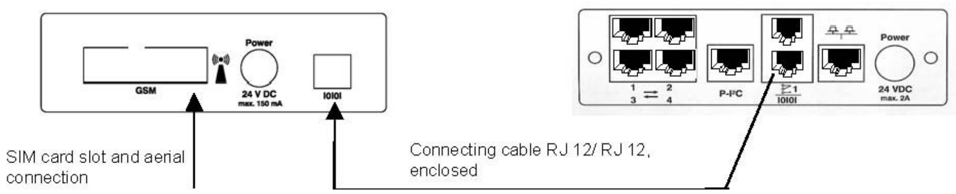


Figura 92 - Conexão da unidade GSM e unidade processadora CMC-TC.
Fonte: ACECO TI (2003, p.12)

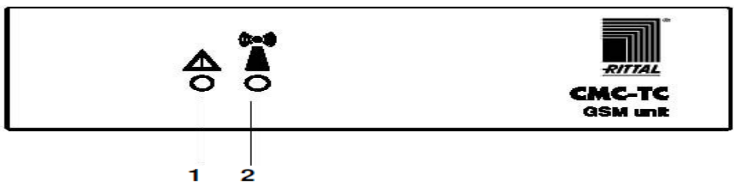


Figura 93 - painel frontal da unidade GSM
Fonte: ACECO TI (2003, p.12)

1. *LED* duplo vermelho / verde: Este *LED* é controlado via comandos AT através de *software* na PU e indica o status de funcionamento da unidade GSM:

O *LED* fica vermelho durante a inicialização da unidade GSM, posteriormente indica baixa qualidade de sinal.

O *LED* fica laranja durante o envio de SMS.

O *LED* fica verde após a inicialização do GSM e indica que esta operacional.

2. *LED* verde da antena Este *LED* é controlado diretamente pelo módulo GSM e indica seu status.

Apagado: Indica que o GSM está desligado ou desconectado do sistema de transmissão.

Piscando lento: O GSM está conectado do sistema de transmissão. Piscando rápido: Indica transmissão de dados.

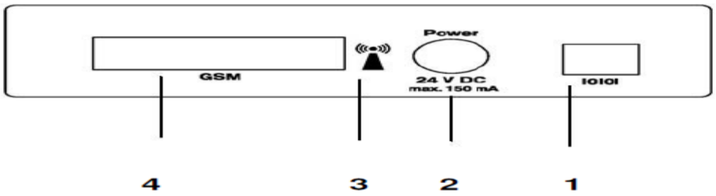


Figura 94 - Painel traseiro da unidade GSM
Fonte: ACECO TI (2003, p.12).

1. O CMC-TC GSM é conectado a UP através da interface RS232 utilizando um cabo com conectores RJ12. Este cabo alimenta a unidade com +24 VDC e também é responsável pelo tráfego de dados entre a unidade e a UP.
2. A conexão de alimentação de 24 VDC 150 mA é reserva para futuras ampliações do sistema CMC-TC.
3. Símbolo da conexão da antena para o GSM.
4. *Slot* SIM *card* com conexão para antena.

5.4 COMPONENTES UTILIZADOS NO PROJETO

Representação dos componentes e equipamentos utilizados no projeto e protótipo do jardim.

5.4.1 Válvula Solenoíde

Válvula solenoide com tensão de 220V, quando energizada faz a liberação da água ou de qualquer fluido.

Figura 95 - Válvula solenoide
Fonte: Autor

5.4.2 Relé

Utilizado um relé (*Finder)* para energizar a válvula solenoide, sua descrição:
Tensão de bobina 24VCA
Corrente 7A

Tensão de saída 220 V

Figura 96 - Relé (Finder)
Fonte: Autor

5.4.3 Irrigador, Aspersor Oscilante.

A válvula de regulagem de fluxo integral pode ser ajustável para atender todos os formatos de gramados e canteiros de flores.

Figura 97 - Aspersor oscilante
Fonte: Autor

5.4.4 Sensor de Temperatura

O sensor assume a função de uma temperatura monitorar e contém um identificador de modo que seja detectada automaticamente e definido pelo sistema CMC-TC. É ligado em uma unidade de sensor através do cabo de ligação.
Configuração: sensor analógico, Rittal 7320.500 termístor do tipo NTC 10kohm a 25ºC com variação de +/- 3% e range de temperatura de +5ºC a +45 ºC.

Figura 98 - Sensor de temperatura
Fonte: Autor

5.4.5 Sensor de Umidade

O sensor mede a umidade relativa do ar e a converte em um sinal de freqüência. Ele contém um identificador de modo que é automaticamente detectado e configurado pelo CMC-TC . Fonte de alimentação e avaliação de dados é através da unidade de sensor de E / S usando a conexão cabo.

Configuração: sensor analógico, Rittal 7320.510. Tipo 50khz a 76% de umidade e range de 10% a 90% de umidade.

Figura 99 - Sensor de umidade
Fonte: Autor

5.4.6 Cabo de Conexão RJ 11/ 12.

O cabo de conexão RJ 12 permite a saída do relé de alarme da unidade de processamento. O cabo de conexão RJ 11 facilita conexão com a tomada CMC em conjunto com o módulo de entrada digital. O cabo está equipado com uma tomada RJ 11/12 conectado numa extremidade. A outra extremidade está aberta, comprimento do cabo 5 m.

Figura 100 - Cabo de conexão RJ 11/12.
Fonte: RITTAL GMBH (2004, p.30)

5.4.7 Configuração do CLP

As parametrizações dos sensores e demais componentes do sistema foram baseados nos equipamentos à venda no mercado e serão apresentados no teste de funcionamento.

Abaixo seguem os procedimentos utilizados para a configuração do CLP.

Para iniciar a comunicação entre CLP e um computador, utilizou-se uma conexão via RS-232. No computador, *via hyperterminal*, foi criada uma conexão de nome “cmc” conforme figura 24.

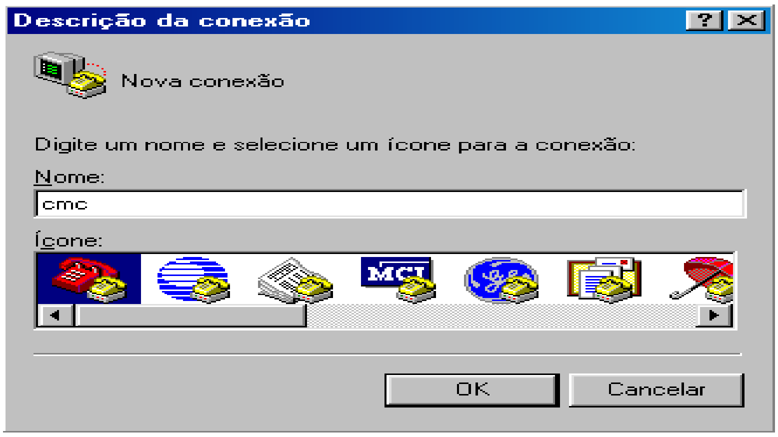


Figura 101 – Tela de nova conexão no hiperterminal
Fonte: Autor

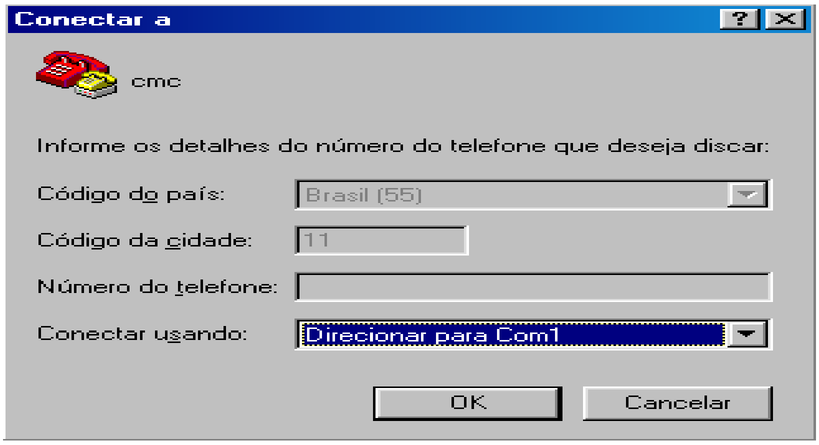


Figura 102 - Nova conexão via Hyperterminal.
Fonte: Autor.

Após a criação da conexão, direcionamos a porta de comunicação para "Com1" e a velocidade máxima de comunicação da porta para 9600 bits por segundo conforme figura 26.

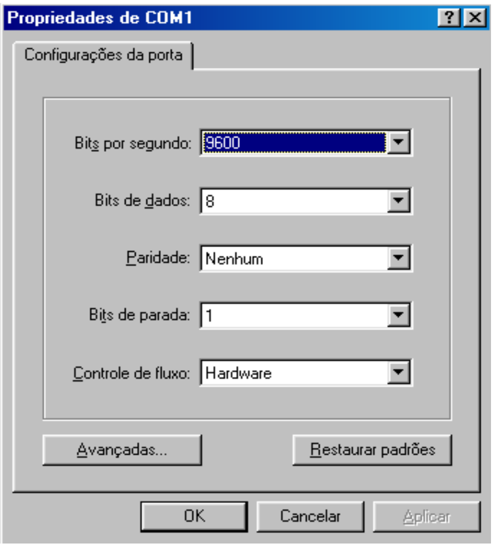


Figura 103 - Configuração da porta COM1
Fonte: Autor

Após a correta configuração da porta, para maior segurança, foi criado um usuário e senha para acesso da conexão. Como o sistema depende de um computador remoto para supervisão, foi necessário configurar o sistema de gerenciamento de usuários via *ethernet* conforme figura 27 e 28.

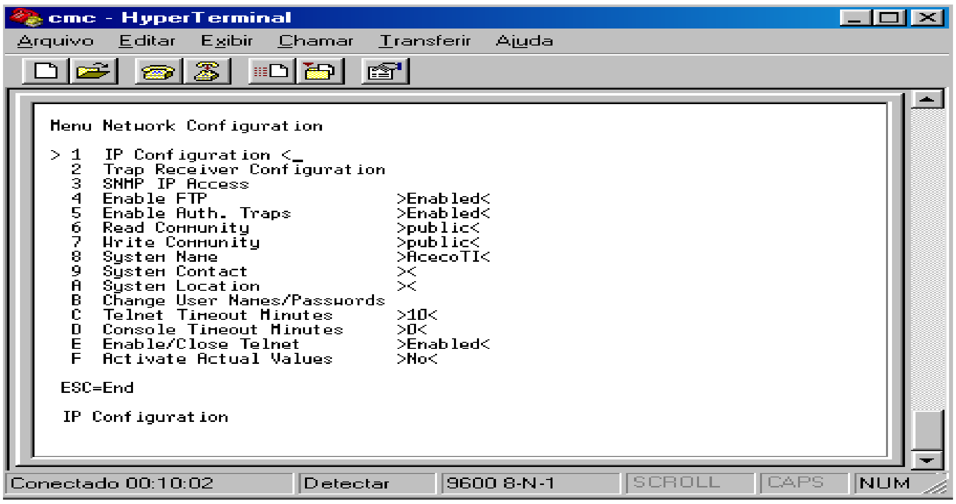


Figura 104 - Configuração de rede
Fonte: Autor

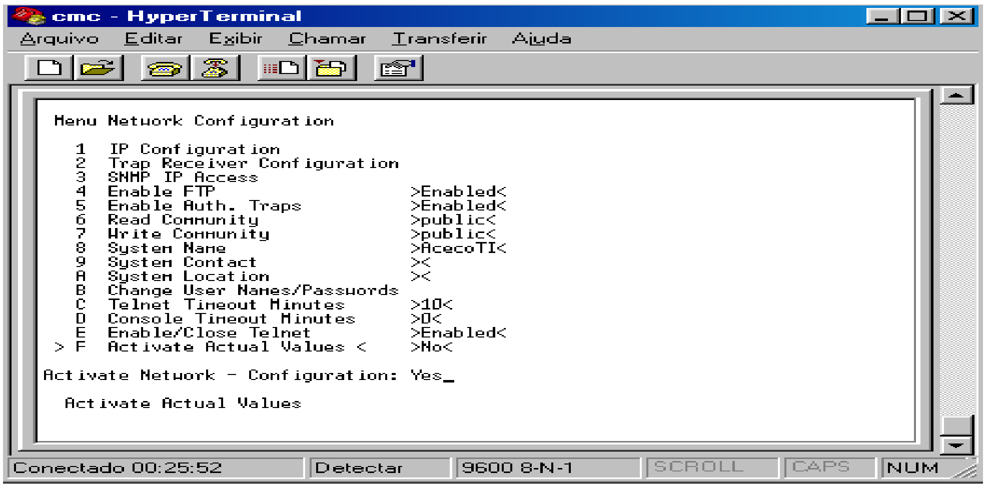


Figura 105 - Configuração de conta
Fonte: Autor

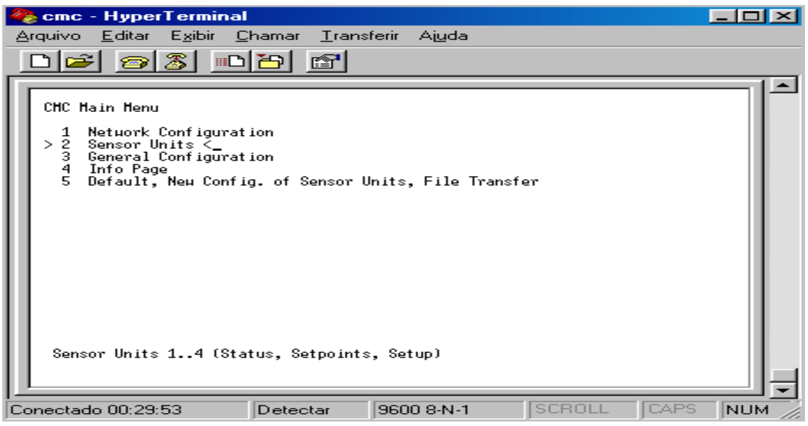


Figura 106 - Configuração dos sensores
Fonte: Autor

3

Na configuração "*Sensor Units*", pode-se visualizar os módulos conectados na unidade de processamento e até mesmo mudar configurações de cada sensor.
Estas configurações, também podem ser alteradas no próprio software e via Browser.

Depois de criado um usuário, através do IP 10.10.5.1 pode acessar tanto a área de configurações como o supervisório do sistema.

Após os passos apresentados acima, foram realizadas as parametrizações de software, lógica de atuação:

Quando a temperatura ambiente atingir 28ºC será indicado no supervisório "alarme de temperatura"; atuando automaticamente o temporizador, que por sua vez só energizara a válvula solenoide após o tempo nele programado, que ira irrigar o gramado até que a temperatura seja reduzida. Da mesma forma, o sensor de umidade relativa do ar ao indicar que a umidade está muito baixa a irrigação será atuada até que a umidade se torne estável. Em caso de chuva, onde não existe a necessidade de irrigação; o sensor de umidade impedirá que a válvula abra; em função de que quando esta chovendo a umidade relativa do ar é alta.

Para a simulação do sistema de irrigação, foi construída uma replica de um gramado em uma caixa de madeira, no formato de 800x800mm. Com um sistema de filtragem da água para que o excesso seja escoado para um ralo qualquer sem vazamento. Será utilizada uma mangueira de jardim para a interligação entre uma torneira e o nosso irrigador.

Desta forma, quando o CLP atuar, uma de suas saídas digitais energizara um rele de 24VCA (*Finder*) alimentando assim uma válvula solenoide em 220V que liberara água para o irrigador.

5.5 MONTANDO O PAINEL DE AUTOMAÇÃO

Primeiramente foi comprado um painel de MDF 800x800mm.

Foi colocado um trilho DIM no centro do painel para a fixação dos componentes.

Figura 107 - Trilho DIM
Fonte: Autor

Foi fixado temporizador digital.

Figura 108 - Timer digital
Fonte: Autor

Foi fixado disjuntor bifásico de 16 A, relé *finder* com bobina de 24VCA

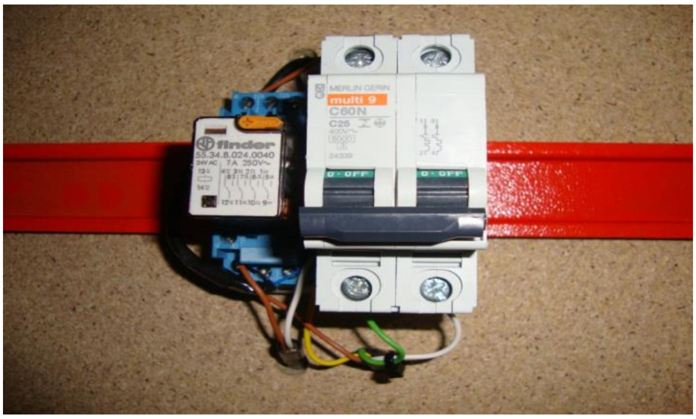


Figura 109- Relé e disjuntor
Fonte: Autor

Foi fixado Led, para alertar quando o sistema entrar em alarme.

Figura 110- led
Fonte: Autor

Foi fixada a unidade processadora CLP (CMC- TC).

Figura 111- Unidade processadora CMC-TC
Fonte: Autor

Foi fixada a unidade I/O.

Figura 112 - Unidade I/O
Fonte: Autor

Foi fixada a unidade GSM Unit CMC-TC.

Figura 113 - Unidade GSM unit
Fonte: Autor

Apresentando painel de automação finalizado

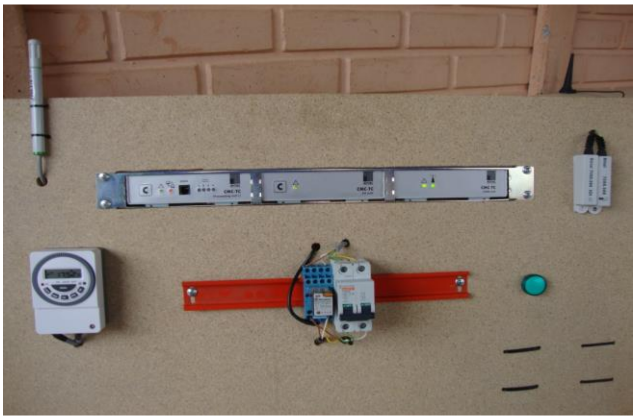


Figura 114 - Painel finalizado
Fonte: Autor

5.6 MONTAGEM DO JARDIM

Foi construída uma caixa 800x800mm para o protótipo do jardim

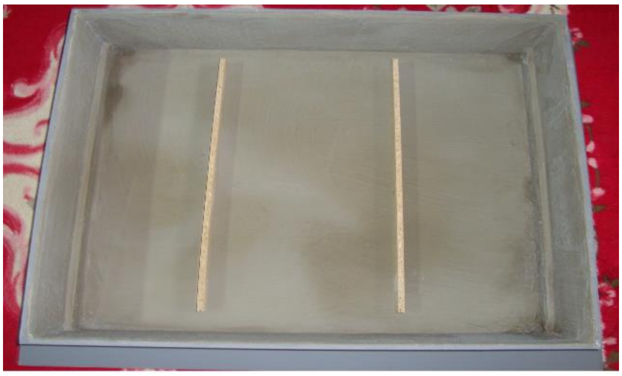


Figura 115 – Caixa
Fonte: Autor.

Foi elaborado um fundo falso para o dreno da água lançada pelo irrigador

Figura 116 - Fundo falso da caixa
Fonte: Autor

Aplicado grama artificial em cima do fundo falso

Figura 117 - Grama artificial
Fonte: Autor

Realizando acabamento final do jardim com flores artificiais, pedras e irrigador de aspersão.

Figura 118 - Acabamento final do jardim
Fonte: Autor

6.7 SISTEMA SUPERVISÓRIO

Apresentamos a seguir, as telas de status do sistema supervisório que pode ser acessado via *Software* ou *via web*.

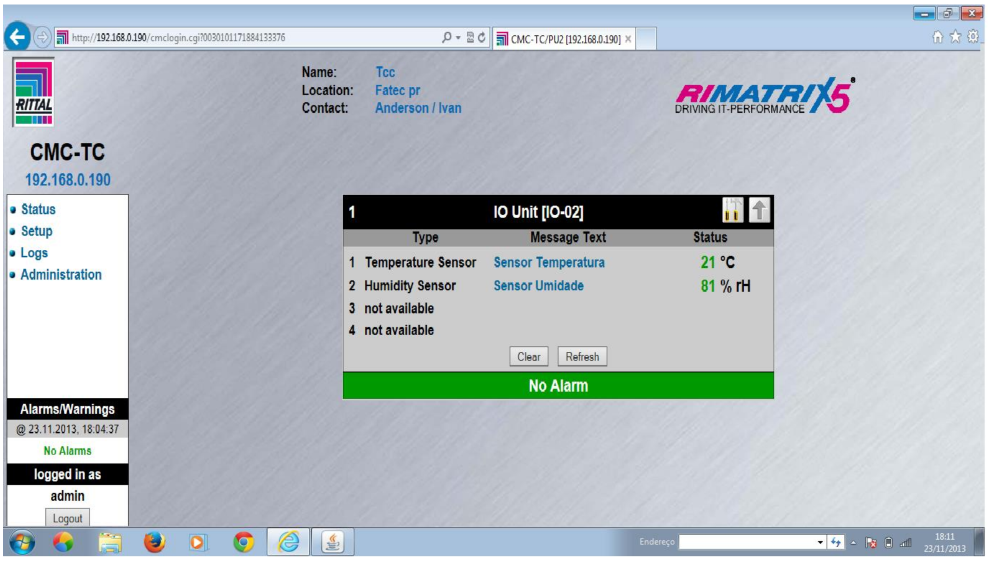


Figura 119 - Status sistema normal via web
Fonte: Autor

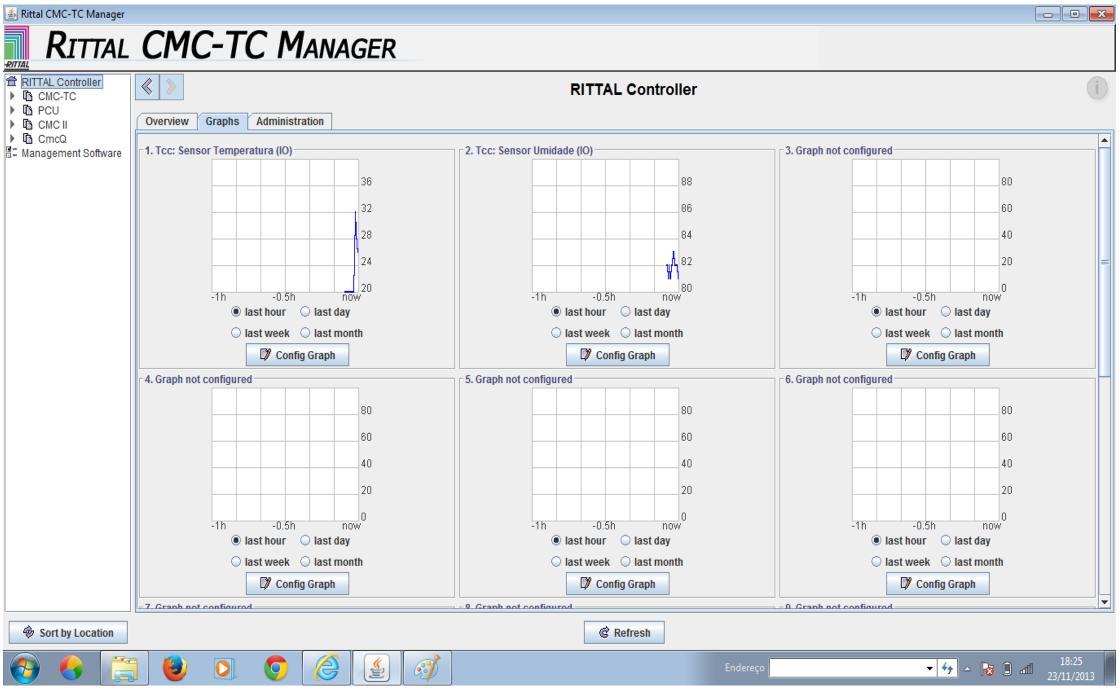


Figura 120 - Status sistema normal via software (CMC - TC)
Fonte: Autor.

Na tela abaixo temos o ícone Graph, permite configurar gráficos em horas, dia e semana, basta clicar em Configuração Grafh, selecionar o Sistema interessado, em seguida o sensor. Desta forma podemos fazer comparativos em relação aos períodos supervisionados pelo *software*.

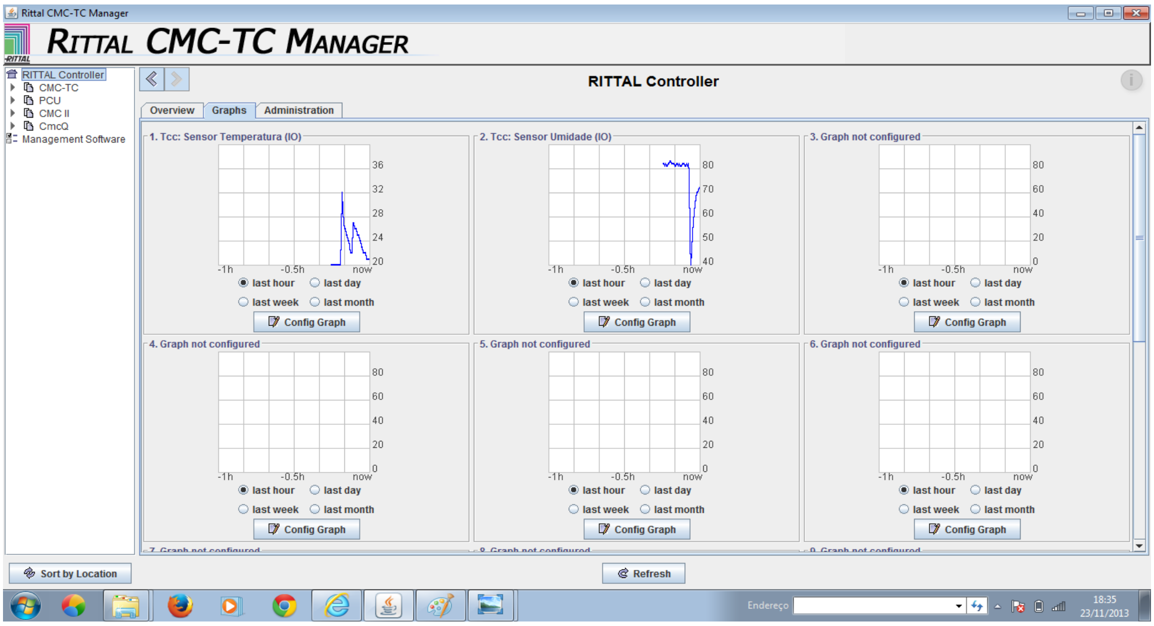


Figura 121 Tela de gráficos
Fonte: Autor

A seguir são apresentadas telas informando status de alarme de temperatura e outra de umidade relativa do ar *via browser*.

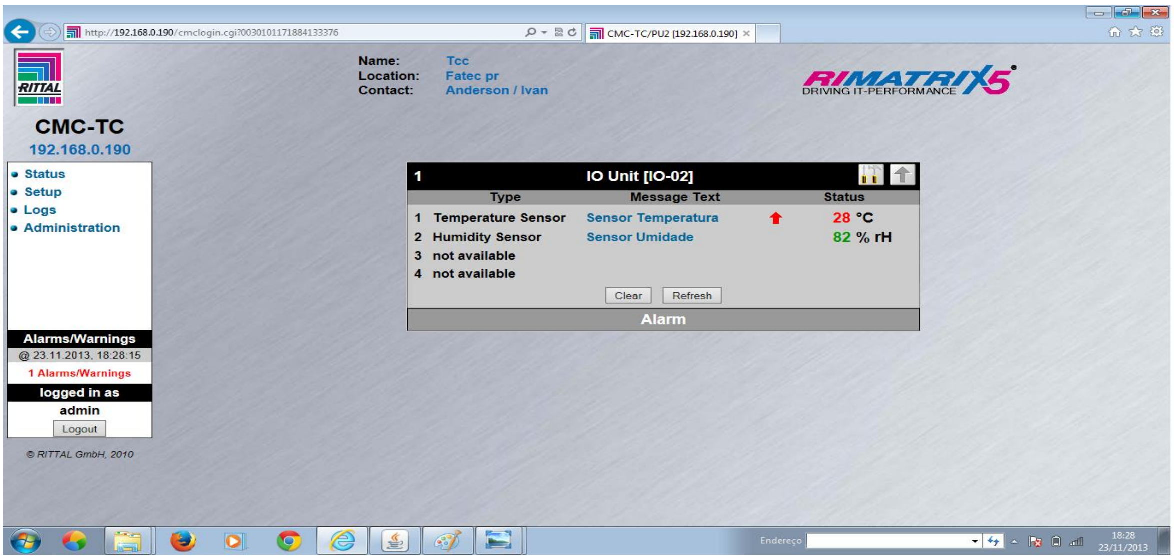


Figura 122 - Status alarme de temperatura via web
Fonte: Autor

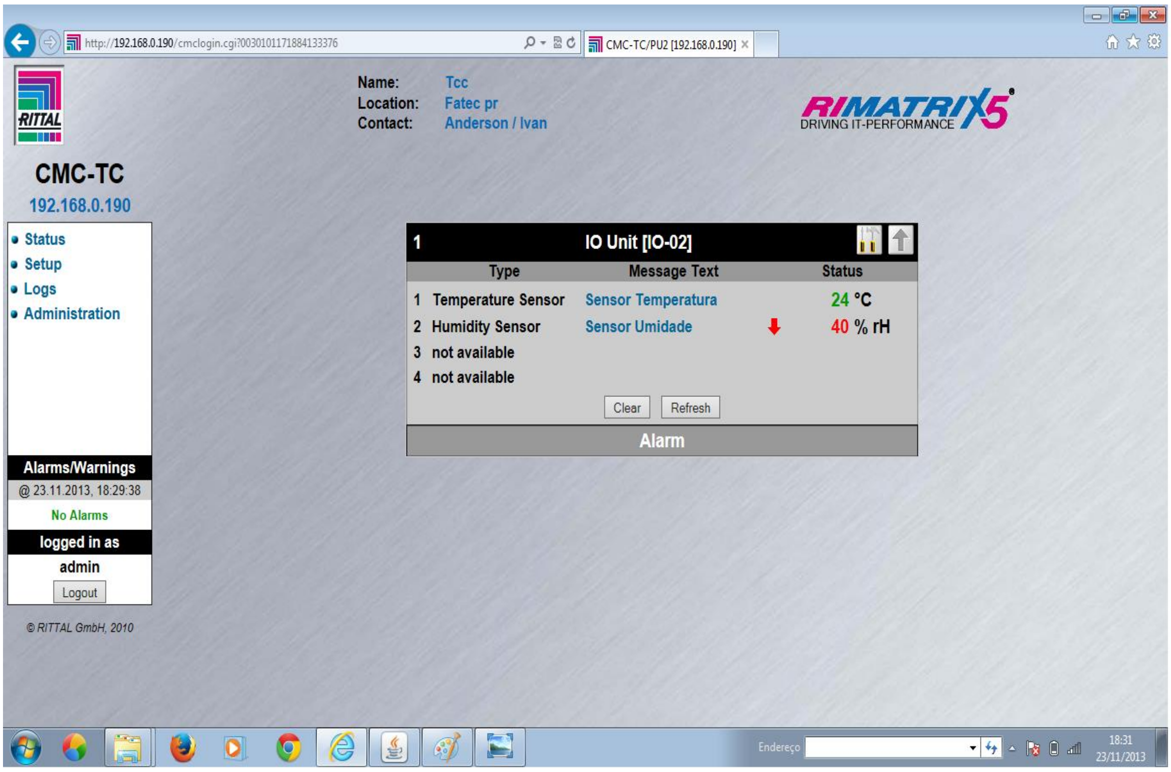


Figura 123 - Status alarme de umidade relativa do ar via web
Fonte: Autor

O sistema ainda oferece a opção de visualização conforme apresentado nas figuras 47 e 48.

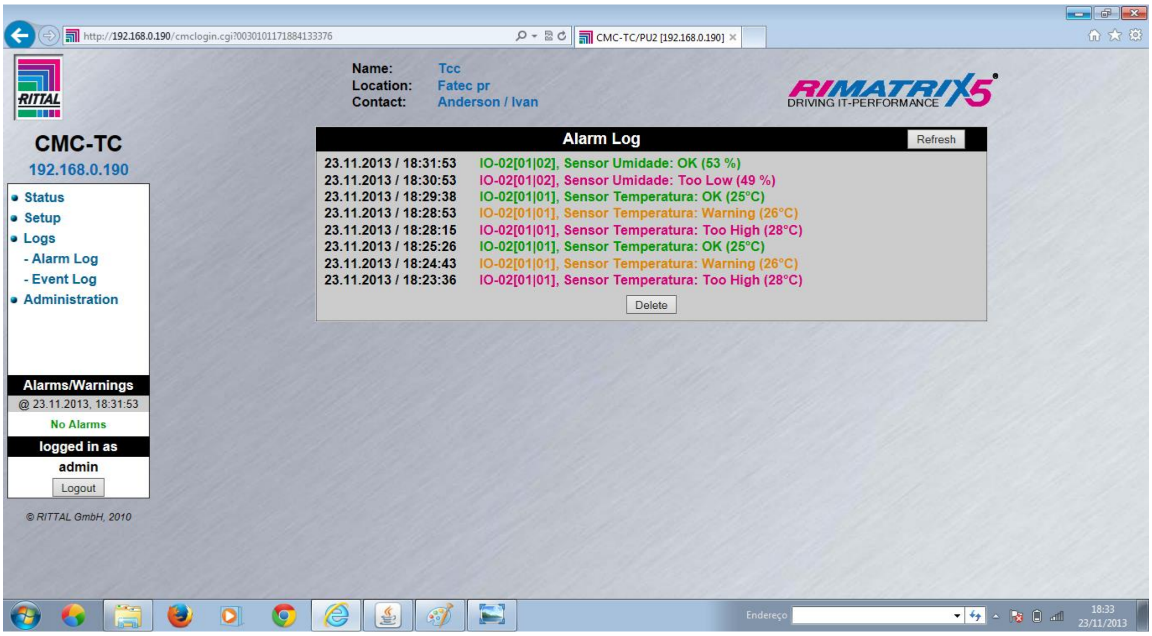


Figura 124 - Status de alarme via web
Fonte: do Autor

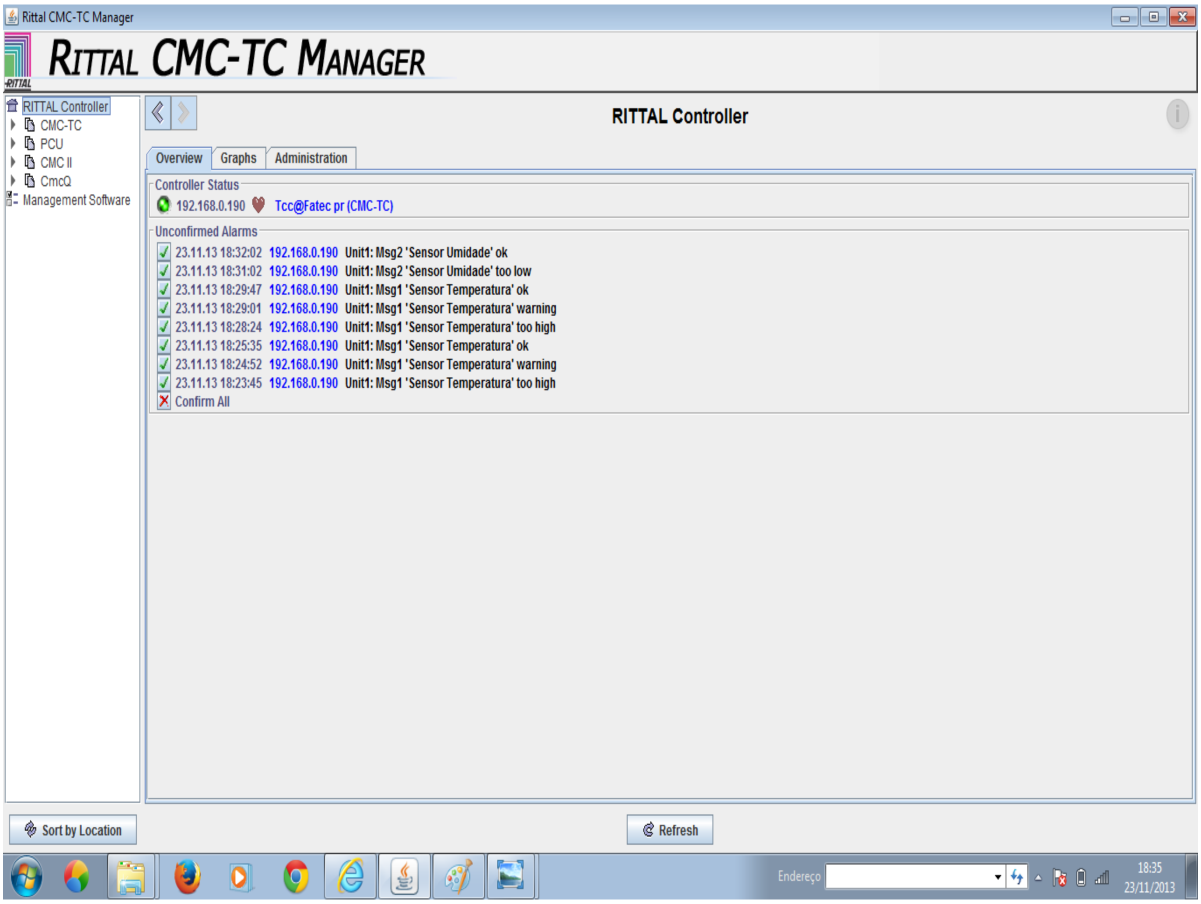


Figura 125 - Status de alarme via software
Fonte: Autor

6 CONCLUSÕES E RECOMENDAÇÕES

Como conclusões do projeto, podem ser destacadas as seguintes.

O processo entre a criação, montagem e a programação do CLP, ocorreu com alguns problemas:

Foi encontrada incompatibilidade de tensão na bobina da válvula solenoide ocasionando a queima da bobina. Realizado pesquisa e compra de nova válvula para substituição.

Encontrado dificuldade na montagem do protótipo do jardim, tais como, vedação da caixa 800x800mm e sistema de drenagem para o escoamento da água acumulada.

O projeto apresenta limitações, pois o CLP pode acionar somente uma válvula solenoide, porém o sistema de irrigação pode ser ampliado após a válvula solenoide, realizando a ramificação da tubulação de água.

Por outro lado, o projeto de pesquisa permiitu que os integrantes da equipe se familiarizassem com a realidade das dificuldades entre a teoria e sua implementação prática.

BIBLIOGRAFIA REFERENCIADA E CONSULTADA

ACECO TI. *Data Center Netwatch* – **Manual do Usuário**.17p

ACECO TI. Procedimento para instalação – **Manual do Usuário**. São Paulo, 2003. 09p.

ACECO TI. Sistema de Monitoração *Netwatch* - **Unidade GSM CMC TC.** São Paulo, 2003. 12p.

AGEITEC. Irrigação - **Sistema de irrigação por sulco**. Disponível em: <http://www.agencia.cnptia.embrapa.br/gestor/cenoura/arvore/CONT000gnhp6ryj02wx5ok0edacxlwt4ys1a.html#> Acesso em: 21/09/2013.

ALIEXPRESS. Brasil - **Aspersão Oscilando de Jardim**. Disponível em <http://pt.aliexpress.com/w/wholesale-oscillating-garden-sprinkler.html> Acesso em: 10/09/2013.

CASOS DE CASA. **Conheça alguns tipos de irrigação.** Publicado em: 2009 Disponível em: <http://www.casosdecasa.com.br/index.php/reforma-e-construcao/> Acesso em: 28/09/2013.

CODESVASF, Brasil - **Histórico da irrigação no Brasil** - Publicado em: 29/03/2010 às 15h15min. Disponível em: <http://www.codevasf.gov.br/programas_acoes/irrigacao/historico-da-irrigacao-no-brasil > Acesso em: 20/09/2013.

EBAH -**Tipo de irrigação** - Disponível em: <http://www.ebah.com.br/content/ABAAABUOwAA/tipos-irrigacao> Acesso em: 11/09/2013.

G1. **Sistema de gotejamento por mangueira**. Publicado em: 25/08/2013 às 14h21. Disponível em: <http://g1.globo.com/al/alagoas/noticia/2013/08/sistema-de-irrigacao-por-gotejamento-e-adotado-no-agreste-de-alagoas.html>.

GARDENA. Irrigação – **História da empresa gardena**. Disponível em: <http://www.gardena.com/br/about-gardena/> Publicado em: 2011 - Acesso em 23/09/2013.

GRAMADINHO VERDE - **Irrigação correta garante vitalidade do jardim e economia de água** - Disponível em: <http://www.gramadinhoverde.com.br/2011/09/irrigacao-correta-garante-vitalidade-do-jardim-e-economia-de-agua-conheca-sistemas> Acesso em: 18/09/2013.

IRRICOMRIO, Sistema de irrigação - **A maneira mais eficiente para você** - Disponível em: <www.irricomrio.com.br/desenho_para_instalacao.htm> Acesso em 28/09/2013.

IRRIGMASTER. Irrigação - **Inteligente e fácil modo para ter uma Paisagem Bonita** - Disponível em: <www.irrigmaster.com.br> Publicado em: 2005 - Acesso em 28/09/2013.

JARDIM DE FLORES - Disponível em: <www.jardimdeflores.com.br/JARDINAGEM>

RAIN BIRD RJ. História da Irrigação - **Manual de Projeto de Irrigação** – Disponível em: <http://www.rainbirdrj.com.br/arquivos/pdf/tecnico/Manual%20Projetos%20de%20Irrigacao.pdf> acesso em 25/09/2013. 75p.

RITTAL GMBH. CMC Top Concept - **Unidade CMC TC.** São Paulo, 2004. 30p

RITTAL, Manual do Usuário - **CMC Top Concept - Unidade** Disponível em: <http://www.eversystem.com.br/trial/pdf/softamb/1.1>..Acesso em: 28/09/2013.

RITTAL. Download de software - **Rittal PMC UPS-Software**. Publicado em: 06/09/2013 às 01h54min Disponível em: < http://www.rittal.com/brazil/services_support/downloads/index.shtml> Acesso em 10/10/2013.

RS. Amidata S.A - **Automação e controle de processo** - Disponível em: <http://pt.rs-online.com/web/p/termistores/0172186/> Acesso em: 25/09/2013.

UNESP. Irriga terra - **Automação de sistemas de irrigação**. Disponível em: <http://www.agr.feis.unesp.br/curso2.htm> Acesso em 23/09/2013.

WIKIPÉDIA. Irrigação - **Métodos de irrigação**. Publicado em: 06/09/2013 às 01h54min Disponível em: <http://pt.wikipedia.org/wiki/Irriga%C3%A7%C3%A3o.> Acesso em 10/10/2013.

O PAPEL DA RADIOTERAPIA NO TRATAMENTO DO CÂNCER DE COLO DE ÚTERO

RADIOTHERAPY CARRIES IN THE TREATMENT OF CANCER OF THE UTERINE CERVIX

Andrielly Voss Carvalho[19]
Emely de Moura Rosa[20]
Ana Paula Christakis Costa (Orientador)[21]
Daniele de Lemos (Co-orientador)[22]

ROSA, Emely de Moura; CARVALHO, Andrielly Voss; LEMOS, Daniele de; COSTA, Ana Paula Christakis (Orientador). **O Papel da Radioterapia no Tratamento do Câncer de Colo de Útero***.* Revista Tecnológica da FATEC-PR, v.1, n.4, p. 186 - 193, jan./dez., 2013.

RESUMO:

O câncer de colo do útero é uma das neoplasias mais comuns entre as mulheres. Como é um câncer que tem um crescimento lento e normalmente é diagnosticada nas fases mais evasivas, a neoplasia traz um grande índice de óbitos entre as mulheres. Quanto aos fatores de risco para o seu surgimento pode-se destacar o início precoce da atividade sexual, múltiplos parceiros e o uso de contraceptivos orais. O HPV também está associado à neoplasia, e pode ser detectado somente através de exames ginecológicos. O câncer do colo do útero é uma patologia cuja radioterapia constitui um dos tratamentos mais importantes. É possível fazer uma análise para o tratamento radioterápico utilizando o estadiamento do tumor como instrumento. Com este estudo, pudemos concluir que, como o câncer no colo do útero é diagnosticado na maioria das vezes em estágios mais avançados, o tratamento é feito de forma paliativa. Para cada estágio a radioterapia vai desenvolver um papel diferente e em alguns casos levar até a cura do carcinoma. Concluímos também que o tratamento de Alta taxa de dose (HDR) tem vantagens ao de Baixa taxa de dose (LDR). A radioterapia desenvolve um papel fundamental no tratamento do câncer do colo do útero, porem mesmo com todos os benefícios obtidos através do tratamento radioterápico, não se pode deixar de dar atenção aos fatores que podem gerar o câncer e recomendar às mulheres que façam sempre os exames recomendados a fim de evitar tal patologia.

Palavras-chave: Câncer. Colo de útero. Radioterapia. Tratamentos. Estadiamento.

***ABSTRACT*:**

[19] Andrielly Voss Carvalho é formanda de 2013 no Curso Superior de Tecnologia em Radiologia Médica, da Faculdade CBES - Colégio Brasileiro de Estudos Sistêmicos.
[20] Emely de Moura Rosa é formanda de 2013 no Curso Superior de Tecnologia em Radiologia Médica, da Faculdade CBES - Colégio Brasileiro de Estudos Sistêmicos.
[21] Ana Paula Christakis Costa é docente, pesquisadora e orientadora de Trabalho de Conclusão de Curso (TCC) no Curso Superior de Tecnologia em Radiologia Médica, da Faculdade CBES - Colégio Brasileiro de Estudos Sistêmicos.
[22] Daniele de Lemos é docente, pesquisadora e co-orientadora de Trabalho de Conclusão de Curso (TCC) no Curso Superior de Tecnologia em Radiologia Médica, da Faculdade CBES - Colégio Brasileiro de Estudos Sistêmicos.

Cancer of the cervix is one of the most common malignancies among women. How is cancer that has a slow growth and is usually diagnosed in later stages fugitive, neoplasia carries a high rate of deaths among women. Regarding risk factors for its emergence can highlight the early onset of sexual activity, multiple partners and use of oral contraceptives. HPV is also associated with cancer, and can be detected only through gynecological exams. Cancer of the cervix is a disease whose radiation is one of the most important treatments. You can do an analysis for radiotherapy using tumor staging as a tool. With this study, we concluded that, like cancer of the cervix is most often diagnosed in advanced stages, treatment is done in a palliative. For stages radiotherapy will develop a different role and in some cases lead to a cure for cancer. We also conclude that the treatment of high dose rate (HDR) has the advantages of low dose rate (LDR). Radiotherapy carries a key role in the treatment of cancer of the cervix, but even with all the benefits provided by the radiotherapy, one can not fail to give attention to factors that may cause cancer and advised women to always make the exams recommended to avoid such pathology.

Keywords: *Cancer. Uterine cervix. Radiotherapy. Treatments. Staging.*

1 INTRODUÇÃO

O câncer é uma doença que se origina de uma célula com defeito que se multiplica, dando origem a outras células defeituosas, que vão invadir e destruir tecidos próximos e distantes podendo levar à morte. Há diversos tipos de câncer e nas mulheres, os mais freqüentes são o câncer de mama e o câncer de colo do útero (ONCOGUIA, 2008).

SASSE, em 2008, afirma que o câncer de colo do útero costuma apresentar crescimento lento. Durante vários anos, as células da superfície do colo do útero se tornam anormais. No início, estas anormalidades ainda não se caracterizam como um câncer e são denominadas displasias. Porém algumas dessas alterações ou displasias podem dar início a uma série de alterações que podem levar ao aparecimento do câncer de colo de útero.

As possíveis abordagens terapêuticas para o câncer de colo de útero incluem a cirurgia e a radioterapia. Portanto, procura-se por meio desse estudo mostrar a importância da radioterapia no tratamento do câncer do colo do útero, tendo o embasamento teórico para justificá-la.

1.1 OBJETIVOS

Os objetivos do trabalho são os seguintes:

- Mostrar o papel do tratamento radioterápico no câncer de colo de útero;
- Entender como o câncer de colo de útero se desenvolve e o estadiamento do carcinoma;
- Identificar as formas utilizadas para o tratamento do câncer do colo do útero de acordo com seu estágio;
- Analisar como o tratamento de radioterapia é desenvolvido.

2 MÉTODOLOGIA

O projeto de pesquisa foi realizado através de um estudo qualitativo de cunho bibliográfico sobre o papel da radioterapia no tratamento do câncer do colo do útero, abordando em quais estágios do câncer a radioterapia é utilizada.

Para o desenvolvimento do trabalho foi selecionado dentre a temática abordada, referências de livros, artigos e periódicos, com publicações entre o ano de 1998 à 2009.

3 REVISÃO BIBLIOGRÁFICA

A seguir estão apresentados os resultados do estudo e análise da literatura pertinente ao tema da pesquisa realizada.

3.1 SISTEMA REPRODUTOR FEMININO

O sistema reprodutor feminino inclui: os ovários, que reproduzem os óvulos; as tubas uterinas, que transportam e protegem os óvulos; o útero, que provê um meio adequado para o desenvolvimento do embrião; e a vagina, que serve como receptáculo dos espermatozóides (SLEUTJES, 2004).

3.2 CÂNCER DO COLO DO ÚTERO

O câncer no colo de útero é a segunda neoplasia mais comum em mulheres, sendo responsável pela morte de 230 mil mulheres por ano, no mundo todo. A doença é diagnosticada muito mais freqüentemente nas fases evasivas e, nos estágios mais avançados, de difícil tratamento e de pior prognóstico, o que justifica proporcionalmente um maior índice de óbitos (INCA 2008).

As mulheres que iniciam a atividade sexual são potencialmente suscetíveis ao desenvolvimento da doença, com o início precoce da atividade sexual, a multiplicidade do parceiro e o uso de contraceptivos orais que favorecem o surgimento do câncer no colo do útero.

O HPV, que também é um dos fatores que levam ao câncer do colo do útero, normalmente se apresenta com lesões microscópicas que só podem ser diagnosticadas através do exame de Papanicolau ou a Colposcopia. Os estágios iniciais do HPV podem ser tratados, impedindo que o paciente tenha maiores complicações no futuro (RAMOS, 2009).

Oncoguia (2008), diz que o quadro clínico de pacientes com câncer de colo de útero pode não apresentar nenhum sintoma. Nesses casos, chamados assintomáticos, o tumor é detectado no exame ginecológico periódico. Algumas pacientes apresentam quadros de sangramento vaginal intermitente, secreção vaginal de odor fétido e dor abdominal associada com queixas urinárias ou intestinais, nos casos mais avançados da doença. Um sintoma comum é o sangramento fora do período menstrual, principalmente depois da relação sexual, porém esse sintoma aparece em fase mais adiantada do tumor.

3.3 PREVENÇÃO DO CÂNCER DE COLO DO ÚTERO

A prevenção primária pode ser realizada através do uso de preservativos durante a relação sexual. A prática do sexo seguro é uma das formas de evitar o contágio pelo HPV, vírus com papel importante no desenvolvimento do câncer.

A prevenção do câncer de útero é feita com o conhecimento dos sinais de alerta pela mulher, com exames ginecológicos anuais e com o tratamento das doenças que possibilitam o desenvolvimento do câncer.

3.4 TRATAMENTOS

Ress (2000), diz que diferentes tipos de câncer são tratados de maneiras muito diversas. A radioterapia e a quimioterapia são capazes de destruir os cânceres, deixando os tecidos vizinhos normais completamente intactos. No entanto, alguns cânceres não respondem bem à radioterapia ou às drogas e são melhor tratados com a cirurgia. Outros são de remoção cirúrgica difícil ou impossível, mas podem responder bem ao tratamento.

Segundo Canary e Almeida (1998), o câncer do colo do útero é de expressiva significação, e como é uma patologia cuja radioterapia constitui um dos tratamentos mais importantes, é possível fazer uma análise da radioterapia e dos métodos usados para o seu tratamento utilizando o tumor como o instrumento desta analise.

A radioterapia tem papel fundamental no tratamento paliativo e curativo do câncer de colo do útero, mas apesar dos benefícios nesses tratamentos, pode-se evitar o mesmo se a paciente estiver atenta aos meios de prevenção (ABRANTES; NOVAES & VIÉGAS, 2001).

3.5 RADIOTERAPIA EXTERNA

Na Radioterapia externa, uma grande máquina direciona radiação à pélvis ou outros tecidos nos quais o câncer se espalhou. O tratamento, geralmente, é realizado em hospital ou clínica. A paciente pode receber radioterapia externa 5 dias por semana por várias semanas, possibilitando a redução do tumor no colo do e útero melhorando as condições locais para a braquiterapia.

Na maioria das clínicas e hospitais do Brasil é utilizada a telecobaltoterapia, com fonte de Cobalto 60 que usa energia média de feixe de 1,25 MeV. Com isso há um aumento da dosagem em estruturas superficiais, quando a região a ser tratada é profunda, como o câncer de colo de útero. O uso de aceleradores lineares de alta energia vem sendo cada vez mais comum, mas a vantagem se dá pelo fato de poupar estruturas sadias de doses desnecessárias.

Segundo Abrantes; Novaes & Viégas (2001), usa-se um arranjo de quatro campos de irradiação de forma que a dose é concentrada no colo e paramétrios e diminuída da bexiga e no reto. O campo é traçado por meio de num aparelho simulador de raios X, onde são obtidas radiografias da pelve em AP e Perfil. O colo do útero é identificado com um clip radiopaco e o tamanho do campo a ser irradiado vai variar de acordo com o estágio e a extensão do tumor.

É muito importante que o paciente seja colocado em posição de tratamento e que seja possível a reprodução da mesma durante os dias do tratamento. Para demarcar a área a ser irradiada podem ser utilizados:

Tinta: tintura de fucsina, de difícil remoção, porém temporária. Alguns pacientes podem apresentar alergia.

Tatuagem: Utiliza-se nanquim ou similar e agulha hipodérmica para pigmentar a pele. Difícil de localizar, dolorosa e definitiva. A vantagem é que se necessário retomar o tratamento após alguns anos utiliza-se campos próximos ao tratado.

Molde plástico: placa acrílica maleável e moldável, após ser aquecida em água. Os campos de tratamento são demarcados no molde, garante a imobilização do paciente (ABRANTES; NOVAES & VIÉGAS, 2001).

3.6 BRAQUITERAPIA

A Braquiterapia é uma forma de radioterapia onde a fonte encontra-se em contato com a paciente, em cavidade pré-existente, neste caso cavidade uterina, ou também pela inserção de agulhas hipodérmicas, porém este último método é menos utilizado. Um tubo fino é colocado dentro da vagina. Uma substância radioativa é carregada para dentro do tubo. O aplicador é fixo a um sistema de fixação localizado fora da paciente, para impedir que o mesmo saia da posição de tratamento.

A paciente pode precisar permanecer no hospital enquanto a fonte radioativa estiver colocada (até 3 dias) ou a sessão de tratamento pode durar alguns minutos e pode-se ir para casa depois. Depois que a substância radioativa for removida, nenhuma radiação é deixada no corpo. A braquiterapia pode ser repetida duas ou mais vezes por várias semanas (ABRANTES; NOVAES & VIÉGAS 2001).

A braquiterapia permite uma alta dose de radiação no volume do tumor sem que haja sobredosagem em estruturas vizinhas. Da acordo com o distanciamento da fonte há uma queda rápida da dose recebida (ABRANTES; NOVAES & VIÉGAS, 2001).

Pode ser realizada a braquiterapia por baixa taxa de dose (LDR) ou por alta taxa de dose (HDR). As vantagens quanto à proteção radiológica tem feito com que os tratamentos de alta taxa de dose sejam preferíveis aos de baixa taxa de dose. Na braquiterapia de alta taxa de dose utilizam-se taxas de dose superiores a 1200 cGy/h, com tempo de tratamento de 20 a 30 min em 3 ou 4 frações. A paciente receberá maior dose de irradiação, porem ficará menos tempo imobilizada, e o tratamento será ambulatorial. Como a taxa de dose é alta, o tratamento é realizado por controle remoto para evitar riscos de exposição à equipe técnica.

O tratamento não utiliza anestesia e não há internação da paciente. Iniciado o tratamento o técnico deve acompanhar a paciente a fim de garantir seu bem estar, e necessitando, o tratamento pode ser interrompido. A braquiterapia por baixa taxa de dose (LDR) também pode ser utilizada no término da radioterapia externa, mas esta técnica de tratamento necessita de anestesia e internação da paciente por um período de até 72 horas.

3.7 ESTADIAMENTO DO CARCINOMA

Segundo a Quadro 1, o câncer de colo de útero é influenciado por vários fatores que se relacionam com o tumor, incluindo estágio, tamanho da lesão, invasão tumoral, estatus dos linfonodos, invasão do espaço linfovascular, tipo histológico e grau de diferenciação tumoral (SALVAJOLI, 1999).

Estágio 0	carcinoma *in situ*
Estágio I	carcinoma limitado ao colo uterino **IA:** carcinoma pré-clínico (visto somente pela microscopia) **- IA1:** invasão estromal mínima: 3 x5 mm. - **IA2:** invasão de até 5x7mm de largura. **IB:** dimensões superiores a IA2. - **IB1:** tumores com diâmetros de até 4cm. **- IB2:** tumores com diâmetros maiores que 4cm.

Estágio II	tumor além do colo, mas que não atinge a parede pélvica. Comprometimento da vagina até no máximo o 1/3 médio **IIA**: sem comprometimento evidente de paramétrio (apenas vagina). **IIB:** com comprometimento evidente de paramétrio.
Estágio III	tumor no 1/3 inferior da vagina ou até a parede pélvica. Todos os casos com uretero-hidronefrose ou exclusão renal. **IIIA:** não há extensão à parede pélvica (só da vagina). **IIIB:** extensão à parede pélvica e/ou uretero-hidronefrose ou exclusão renal.
Estágio IV	tumor além da pelve verdadeira ou na mucosa da bexiga ou do reto. **IVA:** envolvimento órgãos adjacentes, como reto e bexiga. **IVB:** envolvimento de órgãos distantes.

Quadro 1 – Estágios: Câncer de Colo de Útero.
Fonte: Salvajoli (1999).

3.8 TRATAMENTOS

Salvajoli (1999) relata que estágios IB - IIA são tratados tanto pela cirurgia quanto pela radioterapia, já os estágios IIB - IVA tratam-se principalmente com a radioterapia, e o IVB, que já é um estágio bem mais avançado, trata-se pela radioterapia ou quimioterapia de forma paliativa. Afirma também, que para o estágio IA a opção de se usar a radioterapia é variável e o uso da radioterapia externa é desnecessário.

A maioria das pacientes de países desenvolvidos apresenta o câncer do colo nos estágios IB e IIA, sendo tratadas pela radioterapia ou cirurgia radical e estima-se uma sobrevida entre 70 e 90%. Escolhe-se a radioterapia como tratamento nestes estágios quando o tumor ultrapassa os 4 cm, pode ser usada em qualquer paciente e evita os riscos de qualquer procedimento cirúrgico radical. Recomenda-se a irradiação pélvica com megavoltagem na dose de 45 Gy em 25 frações diárias de 1,8 Gy, seguida da braquiterapia.

Nos estadios IIB – III e IV o tratamento deve ser radioterápico, e estima-se uma taxa de sobrevida de 65% dos pacientes. A irradiação pélvica é na dose de 45 Gy em 25 frações seguidos da braquiterapia. Para o estadio IVA com envolvimento da bexiga e/ou reto, mas sem extensão para a parede pélvica, pode ser realizada a exenteração pélvica que após o tratamento radioterápico primário pode chegar à possibilidade de cura, porém com taxas de complicações. A radioterapia é feita com irradiação externa da pelve na dose de 45 a 50,4Gy em 25 ou 28 frações, em caso que permitam a utilização da braquiterapia está é recomendável.

No estadio IVB, que já é um estadio bem mais avançado, trata-se pela radioterapia ou quimioterapia de forma paliativa, pois o câncer é raramente curável.

Como a enfermidade está num estadio mais avançado e não é possível a cirurgia, nos estadios IIIA e IIIB trata-se com a radioterapia exclusiva, porém a resposta quanto à cura é pobre. Usa-se um tratamento de baixa dose com duas inserções de 20Gy em 48h com intervalos de 15 dias. No IIIA e no IIIB duas inserções de baixa dose de 20Gy com intervalos quinzenais ou quatro inserções de alta dose de 6Gy com intervalos semanais.

Nos estadios IA1 e IA2 a opção de se usar a radioterapia é variável, usa-se para pacientes sem condições cirúrgicas por doenças associadas. Devem ser tratadas com irradiação intracavitaria, e o uso da radioterapia externa é desnecessário.

3.9 EFEITOS COLATERAIS

Os efeitos colaterais da radioterapia dependem principalmente da quantidade de radiação e a parte do corpo tratada. A radiação no abdômen e da pélvis pode causar náusea, vômito, diarréia ou problemas urinários. A paciente pode perder os pêlos na área genital. A pele na área tratada pode ficar vermelha, seca e sensível. A paciente também pode ter secura, coceira ou queimação na vagina. O médico pode aconselhar à paciente a só ter relações sexuais depois que o tratamento com radioterapia terminar (FONTES, 2009).

3.10 DISCUSSÕES E CONCLUSÕES

Como o câncer no colo do útero é diagnosticado na maioria das vezes em estágios mais avançados o tratamento é feito de forma paliativa com a finalidade de dar um conforto à paciente, nesta fase tão difícil de sua vida.

Nos estágios IB e IIA as pacientes têm uma taxa de sobrevida alta quando submetidas ao tratamento radioterápico, já no estágio IIB a taxa de sobrevida tem uma queda de aproximadamente 15%. Apesar das pacientes receberem a mesma quantidade de dose neste estágio, há um comprometimento do paramétrio, o que leva a esta queda na sobrevida das pacientes.

No estágio IVA o tratamento radioterápico, após a exenteração pélvica, pode trazer à cura do câncer, porém com taxas complicações. O que não ocorre no estágio IVB, em que os tratamentos radioterápicos são realizados de forma paliativa, pois a chance da cura é quase nula.

No estágio IA1 e IA2 o tratamento radioterápico é realizado pela braquiterapia, mas somente em pacientes que não tenham condições cirúrgicas. A braquiterapia é aconselhada nestes casos, pois como se trata de tumor em fase inicial, a distribuição da dose de radiação se concentra no volume tumoral e não acarreta em doses altas em estruturas sadias.

Os estágios IIIA e IIIB, em que o carcinoma está mais avançado, recomendam-se a radioterapia, porém com um resultado não tão satisfatório.

Quando necessária, a braquiterapia por HDR tem vantagens em relação ao LDR. No HDR a radiação liberada num intervalo de tempo mais curto, o que possibilita que a paciente retorne para casa sem necessidade de internamento.

Por fim, concluí-se através desta pesquisa que a radioterapia tem um papel fundamental no tratamento do câncer do colo do útero, e que em alguns casos pode levar a cura completa do mesmo.

Mas, apesar de todos os benefícios obtidos através do tratamento radioterápico, não se pode deixar de dar atenção aos fatores que podem gerar o câncer e recomendar às mulheres que façam sempre os exames recomendados a fim de evitar tal patologia.

BIBLIOGRAFIA CONSULTADA E REFERÊNCIADA

ABRANTES, M.A.P, NOVAES, P.E.R.S , VIÉGAS, C.M.P. **Câncer de Colo Uterino.** 2001 Disponível em: http://www.inca.gov.br/pqrt/download/tec_int/cap1_p1.pdf. [02 abr. 2010]

CANARY, P.C , ALMEIDA, C.E, **Revista Brasileira de Cancerologia.** Vol. 44, n°2 Abr/Mai/Jun Rio de Janeiro 1998.

FONTES, H.A.F, **Copacabana Runners,** 2009. Disponível em: www.copacabanarunners.net/cancer cervical-tratamento.html. [13 abr. 2010].
INCA, (2008). **Instituto Nacional de Câncer**. Disponível em: www.inca.gov.br. [09 abr. 2010].

ONCOGUIA, (2008). **Câncer do Colo do Útero.** Disponível em: http://www.oncoguia.com.br/site/interna.php?cat=12&id=100&menu=2. [27 jun. 2009]

RAMOS. S.P, **gineco.com.br.** Disponível em: http://www.gineco.com.br/hpvum.htm [11/ abr. 2010]

RESS. Gareth J. Ministério da Saúde, **Controle do Câncer de Colo de Útero.** 1ª ed, Brasília - 2000.

SALVAJOLI, J.V;. **Radioterapia em Oncologia.** Edição única. Rio de Janeiro. Medsi,1999, 709-738.

SLEUTJES, L, **Anatomia Humana,** Podemos Ser Práticos E Ir Direto Ao Assunto**,** São Paulo, 2004.

REVISTA TECNOLÓGICA DA FATEC-PR

Publicação Anual da Faculdade de Tecnologia de Curitiba – FATEC-PR

Aceitam-se permutas com outros periódicos.

Para obter exemplares da revista, basta acessar o site *www.fatecpr.edu.br* e clicar no *link* da Revista Tecnológica da FATEC-PR e fazer o download do arquivo PDF correspondente e imprimir.

Revista Tecnológica da FATEC-PR
Faculdade de Tecnologia de Curitiba – Fatec-Pr
Mantenedora: Escola Tecnológica de Curitiba S/C Ltda.
Rua Itacolomi, 450 – Portão
CEP: 81070-150 - Curitiba-Pr
Telefone: 3246-7722 - Fax: 3248-0246
http://www.fatecpr.edu.br
e-mail: secretaria@fatecpr.edu.br