LUIS HENRIQUE GIBELI

CONSTRUÇÃO DE *BASELINES* PARA GERÊNCIA DE SISTEMAS VOIP

CONSTRUCTION OF BASELINES FOR VOIP SYSTEMS MANAGEMENT

CAMPINAS
2012

UNIVERSIDADE ESTADUAL DE CAMPINAS
FACULDADE DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO

LUIS HENRIQUE GIBELI

CONSTRUÇÃO DE *BASELINES* PARA GERÊNCIA DE SISTEMAS VOIP

CONSTRUCTION OF BASELINES FOR VOIP SYSTEMS MANAGEMENT

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas para obtenção do título de Mestre em Engenharia Elétrica, na área de Telecomunicações e Telemática.

Master degree dissertation presented to the Electrical Engineering Graduation Program of the School of Electrical and Computer Engineering of the University of Campinas to obtain the M.Sc. degree in Electrical Engineering, in field of Telecommunications and Telematics.

Orientador: Prof. Dr. Leonardo de Souza Mendes

Co-Orientador: Prof. Dr. Gean Davis Breda

***Advisor: Associate Professor* Leonardo de Souza Mendes**
***Co-Advisor: Associate Professor* Gean Davis Breda**

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA DISSERTAÇÃO
DEFENDIDA PELO ALUNO, E ORIENTADA PELO PROF. DR.

LEONARDO DE SOUZA MENDES

CAMPINAS
2012

FICHA CATALOGRAFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA E ARQUITETURA - BAE - UNICAMP

G355c	Gibeli, Luis Henrique Construção de baselines para gerência de sistemas voip / Luis Henrique Gibeli. --Campinas, SP: [s.n.], 2012. Orientador: Leonardo de Souza Mendes Coorientador: Gean Davis Breda. Dissertação de Mestrado - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação. 1. Internet. 2. Redes de computadores. I. Mendes, Leonardo de Souza. II. Breda, Gean Davis. III. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. IV. Título.

Título em Inglês: Construction of baselines for voip systems management
Palavras-chave em Inglês: Internet, Networks of computers
Área de concentração: Telecomunicações e Telemática
Titulação: Mestre em Engenharia Elétrica
Banca examinadora: Rodolfo Miranda de Barros, Bruno Bogaz Zarpelão
Data da defesa: 28-08-2012
Programa de Pós Graduação: Engenharia Elétrica

COMISSÃO JULGADORA - TESE DE MESTRADO

Candidato: Luis Henrique Gibeli

Data da Defesa: 28 de agosto de 2012

Titulo da Tese: "Construção de Baselines para Gerência de Sistemas VoIP"

Prof. Dr. Leonardo de Souza Mendes (Presidente): _____

Prof. Dr. Rodolfo Miranda de Barros: _____

Dr. Bruno Bogaz Zarpelão: _____

Aos meus pais José Luis e Lucia Helena, meu irmão Luis Fernando e à minha namorada Mayara.

Agradecimentos

A Deus por tudo. Pela trajetória que segui em minha vida.

Aos meus pais José Luis e Lucia Helena que sempre me deram amor, apoio em minhas decisões e nunca mediram esforços para me ajudar em meus estudos. Ao meu irmão Luis Fernando pela parceria, carinho e momentos de descontração.

A minha namorada Mayara, pelo amor, carinho e compreensão. Obrigado por me incentivar nos momentos mais difíceis desta trajetória.

Ao meu orientador Prof. Leonardo, pelo suporte, pelo conhecimento passado e principalmente pela confiança depositada.

Ao meu co-orientador Prof. Gean, que me acompanhou desde o início deste trabalho, também agradeço pelo suporte, pelos ensinamentos, pelas revisões, discussões e pela confiança depositada.

Aos meus amigos pelos momentos de descontração, em especial agradeço Thiago Willian Capucin pelo companheirismo em todos estes anos de graduação e pós-graduação.

Ao colega Fábio Pessoa por ter colaborado na obtenção dos bilhetes de tarifação.

Aos administradores técnicos da Infovia Municipal de Pedreira: Claudinei, Mateus e Ricardo, que nos viabilizaram acesso e disponibilizaram todo o material necessário para o desenvolvimento deste trabalho.

Resumo

As modernas redes de comunicações são compostas pela interconexão de um grande número de redes heterogêneas, capazes de suportar múltiplos serviços e aplicações. Muitos destes serviços, como VoIP e videoconferência, são sensíveis a latência. Desta forma, a crescente demanda por este tipo de serviço através da Internet impõe o desenvolvimento de redes capazes de oferecer qualidade de serviço para suportá-los. Estas redes requerem ferramentas específicas de gerenciamento.

Quando uma chamada VoIP é realizada através da Internet, um bilhete de tarifação é gerado produzindo informações específicas desta chamada. Estes bilhetes são chamados de *IP Detail Records* (IPDR). O IPDR gerado em cada chamada VoIP contém informações relacionadas ao seu histórico. Estas informações, além de descreverem o que aconteceu com a chamada, oferecem informações valiosas a respeito do estado da rede. Assim, os IPDRs podem ser utilizados para estabelecer *baselines* do tráfego VoIP na rede.

Este trabalho apresenta um modelo de gerência de sistemas VoIP baseado no desenvolvimento de *baselines*. O objetivo do trabalho é introduzir uma nova abordagem que procura resgatar os conceito utilizados na telefonia pública comutada para ajudar a gerência VoIP. Um estudo de caso foi desenvolvido na Rede Metropolitana de Pedreira, interior de São Paulo, onde o tráfego de chamadas VoIP pôde ser analisado através dos *baselines* criados.

Palavras-chave: IPDR, Gerência de Rede, Rede Metropolitana de Acesso Aberto, VoIP.

Abstract

Modern communications networks are formed by the interconnection of an immense number of complex and heterogeneous networks, capable of supporting multiple services and applications. Many of these services, like VoIP or videoconferencing, are latency sensitive. Thus, the increasing demand for latency sensitive services through the Internet imposes the development of networks capable of delivering quality of service specific for dealing with synchronous. These networks require the use of specific management tools.

When a VoIP call occurs upon the Internet, a ticket (a file record) is generated to register information regarding that specific call. These files are called Internet Protocol Detail Record (IPDR). The IPDR, which is generated for every VoIP call, contain information related to the call's history. The full set of information in the IPDRs carries a very complete description of what happened to the call and can provide valuable information about the state of the network during the history of the call. Therefore, IPDRs can be used to establish baselines for the VoIP traffic within network.

This work presents a management VoIP system model based on development of a baseline. The target of this work is to introduce a new methodology based on concepts used in the Public Switched Telephone Network to help VoIP management. A case study was developed in the city Pedreira-SP, where the VoIP traffic could be managed through the baselines created.

Key-words: IPDR, Network Management, Open Access Metropolitan Network, VoIP.

Lista de Figuras

Lista de Tabelas

Glossário

ADSL	Asymmetric Digital Subscriber Line
AS	Autonomous System
ATA	Adaptador para Telefone Analógico
Bl-1	Baseline de uma semana
bl-3	Baseline de sábado, domingo e dias úteis
Bl-4	Baseline de quatro semanas
bl-7	Baseline de dias da semana
Bl-8	Baseline de oito semanas
BLGBA	Baseline Gerenciamento de Backbone Automático
CATV	Cable TV
CDR	Call Detail Record
CNAME	Canonical Name
CSV	Comma Separated Values
DNS	Domain Name Server
DSLAM	Digital Subscriber Line Access Multiplexer
FMS	Fraud Management System
FTTH	Fibre to the Home
GBA	Gerenciamento Automático de Backbone
HTTP	Hypertext Transfer Protocol
IAX	Inter-Asterisk Exchange
IBGE	Instituto Brasileiro de Geografia e Estatística
ID	Identifier
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPDR	IP Detail Record
IPFIX	IP Flow Information Export
ISP	Internet Service Provider
ITU	International Telecommunications Union
ITU-T	International Telecommunication Union-Telecommunication Standardization Sector
LAN	Local Area Network
LaRCom	Laboratório de Redes e Comunicações
MAN	Metropolitan Area Network
MIB	Management Information Base
MRTG	Multi Router Traffic Grapher
MySQL	Michael Widenius Structured Query Language
NAT	Network Address Transalation
NfSen	Netflow Sensor
NGN	Next Generation Network
P2P	Peer-to-Peer
PABX	Private Branch Exchange

POP	Point of Presence
POTS	Plain Old Telefone Services
PSTN	Public Switched Telephony Network
QoS	Quality of Service
RAS	Registration, Admission and Status
RMAA	Rede Metropolitana de Acesso Aberto
RR	Receiver Report
RRDT	Round Robin Database Tool
RTCP	Real-Time Control Protocol
RTP	Real-Time Transport Protocol
SCM	Serviço de Comunicação Multimídia
SDES	Source Description
SDH	Synchronous Digital Hierarchy
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SR	Sender Report
STCP	Stream Control Transmission Protocol
STFC	Sistema de Telefonia Fixo e Comutado
TCP	Transmission Control Protocol
TMN	Telecommunications Management Network
UA	User Agent
UAC	User Agent Client
UDP	User Datagram Protocol
UEL	Universidade Estadual de Londrina
URA	Unidade de Resposta Audível
VB6	Visual Basic 6
VoIP	Voice Over IP
WAN	Wide Area Network
WiMAX	Worldwide Interoperability for Microwave Access

Trabalhos Publicados pelo Autor

1. Gibeli, Luis Henrique; Mendes, Leonardo de Souza; Breda, Gean Davis. "*A New Methodology for IP Telephony Analysis Applied on Open Access MANs*", IWT International Workshop on Telecommunications, Rio de Janeiro – RJ, p. 209-213,May 3rd-6th 2011.
2. Gibeli, Luis Henrique; Breda, Gean Davis; Zarpelão, Bruno Bogaz; Miani, Rodrigo Sanches; Vieira, Liniquer Kavrokov; Mendes, Leonardo de Souza. "*VoIP Systems Management using Internet Protocol Detail Records*", The Fourth International Conference on Advances in Future Internet, Roma – Italia, p. 20-25, Aug 24th 2012.

Sumário

Capítulo 1

Introdução

A partir de meados da década de noventa, com a constante evolução das tecnologias de informação e comunicação, as redes de telecomunicações tornaram-se cada vez mais robustas, sendo capazes de suportar múltiplos serviços. Estes serviços fazem parte do conjunto heterogêneo de informações que podem ser transportados através da Internet e do TCP/IP, como, por exemplo, as chamadas telefônicas, vídeo sob demanda, jogos on-line, mensagens instantâneas entre outros [1].

As redes de telecomunicações são de vital importância para a sociedade atual, semelhante ao que ocorre com serviços como fornecimento de água e luz [2]. A interrupção em serviços de telecomunicações pode representar grandes perdas econômicas. Segundo um estudo realizado pela empresa PriceWaterhouseCoopers [3], entre fevereiro de 2011 à fevereiro de 2012, trinta e dois por cento das empresas brasileiras tiveram prejuízos devido à interrupção do serviço de telecomunicações. Dentre elas, 5% amargaram perdas superiores a US$ 100 milhões.

Nas empresas de telefonia, a transmissão de voz está migrando do modelo de telefonia clássica para redes IP, graças ao desenvolvimento da tecnologia VoIP [4][5]. No princípio de sua utilização, a tecnologia VoIP possuía baixa qualidade de serviço [5] e somente despertava interesse a um grupo específico de usuários. À medida que este sistema se tornou mais acessível e de melhor qualidade, sua utilização alcançou maiores proporções.

Dentre as qualidades da tecnologia VoIP, se destacam o baixo custo, a oferta de serviços que permitem mobilidade, fácil gerenciamento de contatos, transferência de chamadas, *voicemail,* entre outros. Porém, independente desses atributos, para que o VoIP se torne uma tecnologia viável e esteja dentro dos padrões aceitáveis, é necessário amplo investimento em qualidade de serviço (QoS) [6][7][8].

Uma solução para atender a demanda por QoS tem sido encontrada com a construção de redes de acesso que operam em banda larga [9]. Este tipo de infraestrutura, fornece um conjunto de serviços e funcionalidades, em ambiente seguro, de alta performance, proporcionando uma significativa redução dos custos de comunicação. Estas redes oferecem canais de comunicação de alta velocidade e são utilizadas para transmitir serviços multimídia, tais como: voz, dados e vídeo.

Como exemplo de infraestrutura de banda larga, podemos citar as Redes Metropolitanas de Acesso Aberto, as quais podem ser caracterizadas como sendo as vias públicas da informação. Elas se diferem das redes de comunicações atuais pelo conceito de universalidade. Através delas é possível transportar de maneira unificada os tráfegos de vídeo, voz e dados. Elas também atuam como um instrumento de inclusão social e digital para a população.

Uma possível solução para melhorar o comportamento do serviço VoIP é automatizar funções de gerenciamento com o intuito de mitigar a interrupção de serviços, otimizar a utilização dos recursos, reduzir custos e detectar falhas proativamente. Uma maneira de aprimorar e aperfeiçoar o gerenciamento do tráfego VoIP está na utilização de bilhetes chamados *IP Detail Record* (IPDR). O padrão do IPDR foi definido pelo *Telemanagement Forum* [8][10]. Os IPDRs são tíquetes gerados nos gateways de voz durante a geração de uma chamada VoIP, similarmente aos CDRs (*Call Detail Records*) que são gerados na telefonia convencional [10][11]. A função de um IPDR é fornecer informações detalhadas de todo o histórico de uma chamada. Dentro do bilhete IPDR é possível destacar algumas informações, tais como: tempo de duração da chamada, número de origem e destino, perfil de tarifação, identificação do usuário, data/hora de ocorrência da chamada, tronco de saída utilizado, status da chamada, dentre outros.

Neste trabalho será apresentado um modelo para construção de *baselines* que se baseia em informações presentes em uma base de dados composta pelos IPDRs, e tem como um dos principais objetivos auxiliar no gerenciamento do tráfego VoIP. Neste estudo, procuramos oferecer uma nova abordagem/metodologia que contribua para o aumento da qualidade de serviço nas redes TCP/IP através da caracterização do tráfego VoIP. Outra contribuição é estudo da viabilidade do uso do modelo proposto no processo de detecção de

falhas e comportamentos anômalos relacionados ao serviço VoIP dentro das redes metropolitanas.

Um fator que motivou este trabalho foi a falta de um modelo capaz de monitorar o sistema da telefonia IP, baseando-se nas características de chamadas telefônicas, e de gerar informações de gerência. Até onde pesquisamos, existe um número escasso de trabalhos que utilizam IPDR para monitoramento do ambiente de telefonia IP. Portanto, existe espaço para métodos que abordem a análise do comportamento da tecnologia VoIP e que traduzam este comportamento do ponto de vista de eventos que ocorrem na telefonia tradicional como chamada completada, congestionamento, não responde, discagem incorreta, assinante ocupado, etc.

1.1 – Trabalhos Relacionados

Durante a pesquisa bibliográfica realizada concluímos que existe um número limitado de trabalhos que utilizam os IPDRs para analisar tráfego telefônico IP. Uma explicação cabível se deve ao fato do IPDR possuir informações estratégicas relativas a tarifação, e as operadoras bem como os administradores de rede serem resistentes com relação a exposição do conteúdo destes bilhetes. Em [12], Tartarelli, et al., direcionaram a análise dos bilhetes para gerenciar o tráfego telefônico identificando problemas e observando o perfil de utilização. Ele analisou uma grande quantidade de logs e registrou todo o histórico para auxiliar outras operadoras que possuíam problemas semelhantes. Sistemas de gerenciamento de fraudes (*Fraud Management System* - FMS) foram construídos com base na análise de IPDRs por Ruiz-Agundez et al. [13] e Bihina Bella et al.[14]. Eles propuseram este sistema em redes NGN (*Next Generation Network*).

Outra possibilidade é utilizar os CDRs e IPDRs para realizar uma análise em relação aos aspectos sociais dos usuários. Em [15], Dasgupta et al., analisaram os CDRs para modelar o comportamento das chamadas de usuários que alternavam constantemente de operadoras. O objetivo dos autores neste caso era investigar a possibilidade de uma pessoa decidir mudar de operadora devido à influência de amigos que já haviam mudado. Além disso, eles propõem uma abordagem que visa identificar pessoas que apresentam um potencial maior para trocar de operadora com base em sua rede de contatos. Adicionalmente, IPDRs e CDRs podem ser utilizados em sistemas de detecção de falhas na

comunicação. No trabalho de Breda e Mendes [11] foi analisado o desempenho de algoritmos de tempo real e espaço amostral, proposto por Nunes [11], para detectar falhas através da análise de CDRs.

Com relação a trabalhos que abordaram a construção de *baselines*, Proença Junior [1], apresenta o modelo BLGBA para a criação de *baselines*. Neste caso, o autor realiza análises estatísticas em dados coletados das MIBs pertencentes aos agentes SMNP residentes nos equipamentos da rede da Universidade Estadual de Londrina – UEL. Além do modelo de criação de *baseline*, o autor implementa um sistema de alarmes multinível que avalia o *baseline* em relação ao movimento real, informando ao administrador da rede, o desvio significativo do comportamento da rede, caso necessário.

1.2 – Escopo e Organização da Dissertação

Este trabalho está organizado da seguinte maneira:

No Capítulo 1, Introdução, é apresentada uma visão geral sobre o modelo proposto, bem como os fatores motivadores. São também referenciados trabalhos de outros autores relacionados a este projeto.

No Capítulo 2, Seções Técnicas, são apresentados os principais conceitos e características de uma Rede Metropolitana de Acesso Aberto e citados alguns exemplos que foram implementados com sucesso no mundo. Também é feita uma revisão da literatura a respeito do VoIP e dos protocolos operantes nesta tecnologia.

No Capítulo 3, Bilhetes de Tarifação, estes são introduzidos e conceituados. Inicialmente são apresentados exemplos e em seguida é feita a leitura do bilhete a partir de seu formato original. Dentro do ambiente de desenvolvimento apresentamos o aplicativo de leitura. Posteriormente, definimos possíveis classificações para cada bilhete. O resultado da classificação gera os eventos que servem de matéria-prima para a geração de *baselines*.

No Capítulo 4, *Baselines*, definimos suas funções e apresentamos detalhes sobre a motivação para utilizá-los na gerência das redes, bem como a forma que eles são elaborados. Além de apresentar alguns exemplos, apresentamos algumas ferramentas comerciais utilizadas na gerência de redes.

No Capítulo 5, Estudo de caso desenvolvido, é descrito um estudo de caso realizado na cidade de Pedreira, interior do estado de São Paulo. São apresentados também os resultados deste trabalho e suas conclusões.

No Capítulo 6, Conclusões Finais e outras Considerações, são apresentadas as conclusões finais e sugestões para trabalhos futuros.

Capítulo 2

Seções Técnicas

Neste capítulo serão apresentados os principais conceitos de uma rede metropolitana de acesso aberto (RMAA), onde serão demonstradas suas características e o modelo em que sua estrutura é construída. Também serão apresentados, alguns serviços que podem ser explorados nas RMAAs, bem como as maneiras com que o município se beneficia com tais serviços, além de exemplos bem sucedidos deste tipo de abordagem no mundo. Adicionalmente, este capítulo aborda os conceitos que embasam a tecnologia VoIP bem como os protocolos responsáveis pelo seu funcionamento. Por fim, uma análise sobre as alternativas existentes de gerência de redes de telecomunicações também é apresentada nesta seção.

2.1 – Redes Metropolitanas de Acesso Aberto

2.1.1 – Definição

As redes metropolitanas de acesso aberto são infraestruturas que permitem a convergência de aplicações e serviços multimídia na rede de telecomunicações de um município [16]. Conteúdos multimídia, como videoconferências, imagens médicas, mensagens instantâneas, educação a distancia, entre outros, passam a se tornar mais acessíveis aos habitantes de um município que dispõe desta rede.

Uma diferença entre as redes de comunicações existentes e as redes metropolitanas de acesso aberto é que as RMAAs possuem um caráter universalizante e, por serem multi-serviço, permitem a distribuição de diversos conteúdos (voz, dados e imagem), que hoje são tratados e oferecidos de maneira separada pelas operadoras tradicionais, de forma simples e unificada [17]. Isto significa que ela é capaz de tratar igualmente todos os tipos de tráfegos baseados no TCP/IP. Ao invés de oferecer o acesso aos serviços como uma mercadoria, as

RMAAs consideram que isso seja a infraestrutura necessária para uma nova organização social.

O objetivo deste modelo de infraestrutura de comunicação é modernizar o município, diminuindo custos e incluindo munícipes no mundo digital. Desta forma, o acesso à Internet de forma comunitária se torna uma possibilidade assim como o oferecimento de serviços VoIP.

Segundo Graham [18], as redes metropolitanas de acesso aberto são parte de um ambiente de distribuição de informações que permite a inclusão digital e a universalização da informação. Mendes [17] definiu RMAA como uma rede de comunicação que serve de espinha dorsal para uma *intranet* pública da cidade, a qual está aberta para a municipalidade. Além disso, a RMAA deve ser capaz de comutar não apenas o tráfego local, como também permitir que seus usuários se conectem a Internet, utilizem POTS (*Plain Old Telefone Services*) e até mesmo soluções CATV (*Cable* TV). Neste contexto, a construção da RMAA passa a fazer parte da demanda de infraestrutura do município, tal qual a construção de ruas, avenidas, redes de água, esgoto ou da rede de energia elétrica.

Uma rede metropolitana de acesso aberto permite o emprego de sistemas integrados nas secretarias municipais gerando um impacto positivo tanto em termos de eficiência quanto em termos de redução de gastos. Um exemplo que podemos citar é o caso da Secretaria da Saúde do município de Campinas, onde com a implantação de um Sistema de Gestão de Materiais e Medicamentos o município conseguiu otimizar a quantidade de medicamento no estoque levando à diminuição na compra e no descarte de medicamentos vencidos [19]. Outra área de impacto é referente à redução de custos na telefonia, pois com a utilização do VoIP o custo por ligação é reduzido comparado com a telefonia convencional [20].

A Figura 2.1 apresenta uma representação genérica de uma Rede Metropolitana de Acesso Aberto, na qual é demonstrada a interligação dos prédios públicos do município. Neste exemplo, os principais prédios podem estar conectados ao *backbone* via fibra óptica ou através de enlaces de rádio.

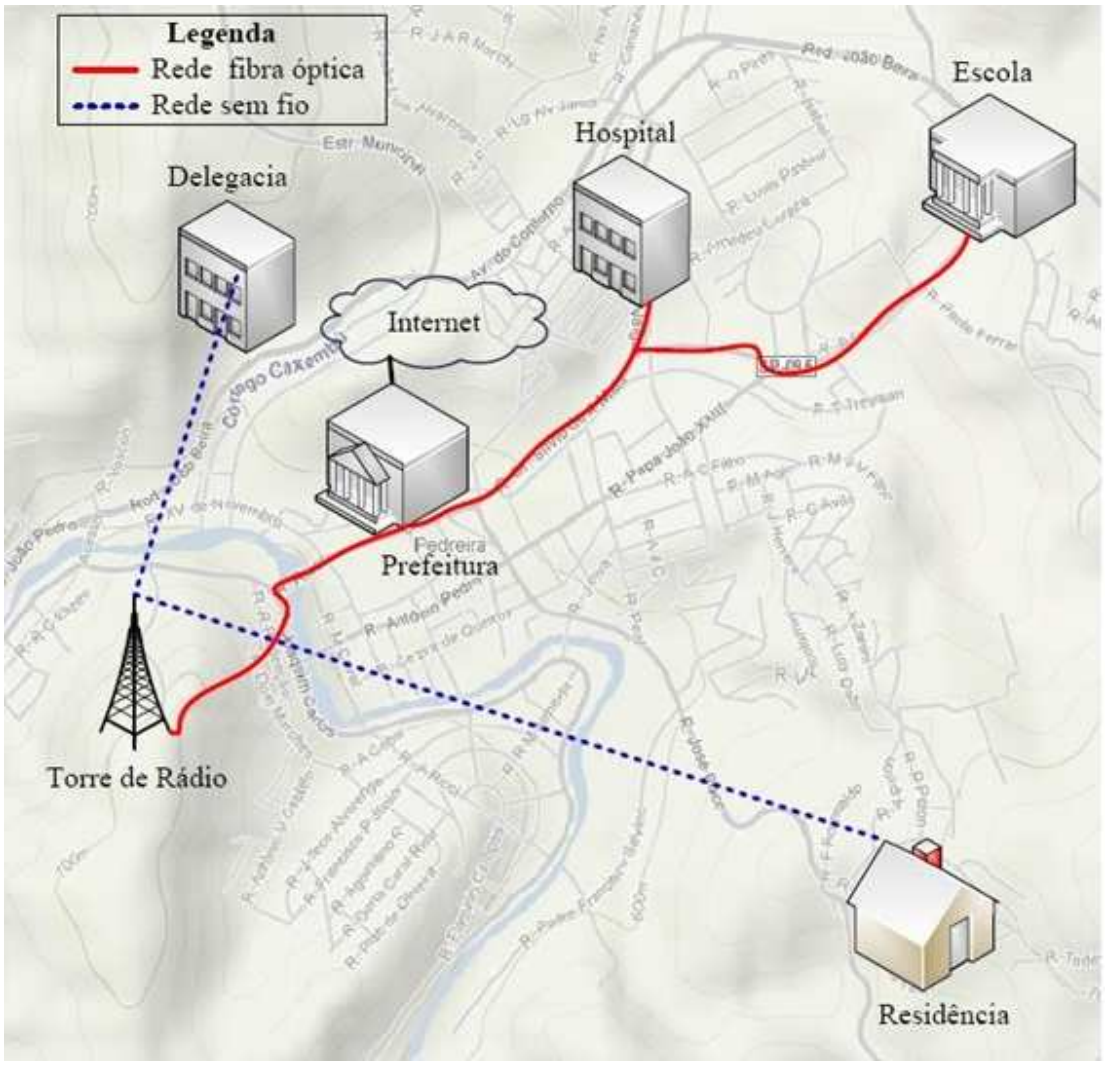


Figura 2.1 – Representação genérica de uma rede metropolitana de acesso aberto.

2.1.2 – Arquitetura Física

As redes metropolitanas de acesso aberto podem se basear em diversas tecnologias de rede, tais como: fibra óptica, redes sem fios, cabo coaxial e cabo de par trançado. Obviamente, a implementação completa da RMAA pode representar um investimento alto, o qual habitualmente não está disponível no orçamento da prefeitura. Uma alternativa que os municípios têm adotado é a execução do projeto de forma modular, ou seja, a implementação inicial da RMAA ocorre em pontos prioritários. Os projetos são configurados de maneira escalável na qual a arquitetura inicial é executada de forma

expansível prevendo a inclusão de novos pontos/nós com o uso de tecnologias mais econômicas como, por exemplo, redes sem fio IEEE 802.11.

Independente da tecnologia escolhida, podemos descrever a RMAA em três camadas: Camada de Acesso, Camada de Distribuição e Núcleo da Rede. Na Figura 2.2, apresentamos a arquitetura física conceitual de uma RMAA. O Núcleo da Rede, que geralmente é composto por um anel óptico redundante, forma a parte principal da rede. O núcleo garante que a RMAA irá suportar todo o tráfego da cidade, portanto, esta camada é capaz de transportar gigabits por segundo de informação além de prover confiabilidade e escalabilidade [17][21]. Além de transportar todo o volume de dados, o núcleo deve cuidar da interconexão da MAN com as redes de serviços públicos (Internet, rede de telefonia pública, empresas de distribuição de TV, etc) e também oferecer pontos de interligação com a Camada de Distribuição, chamados de Pontos de Presença (PoP – *Point of Presence*).

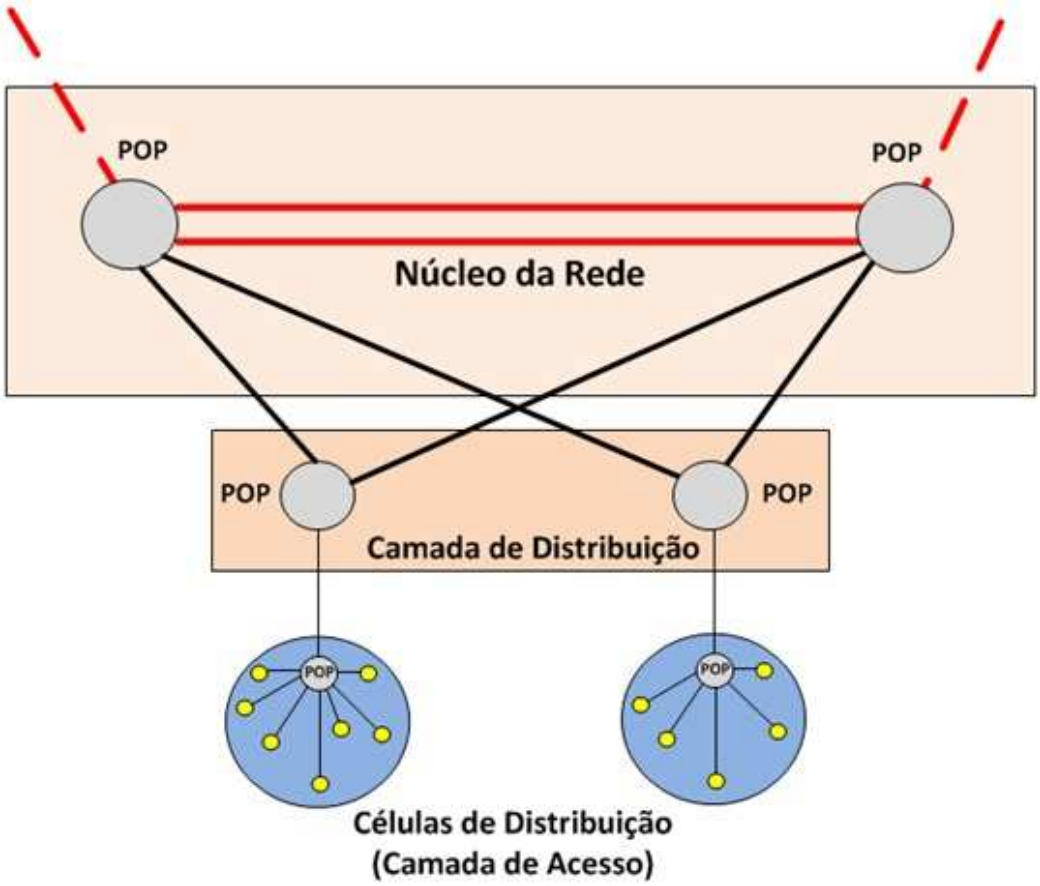


Figura 2.2 – Descrição física de uma RMAA.

A Camada de Distribuição é a camada que realiza a interface entre a camada de acesso e o núcleo. Ela é responsável por efetuar o roteamento e a filtragem de pacotes e determinar como os pacotes chegarão ao núcleo, se necessário. Uma vez que esta camada é composta por vários centros de distribuição ligados diretamente ao núcleo, ela deve ser capaz de lidar com centenas de megabits por segundo de dados. Esta camada também deve prover disponibilidade, qualidade de serviço, rápida recuperação em caso de indisponibilidades e balanceamento de carga [17][21]. Finalmente, a Camada de Acesso é responsável por manipular o ponto genérico de presença na RMAA. Estes pontos derivam dos POPs da camada superior formando células de distribuição. É nesta camada que pequenas empresas e as residências estão conectadas.

Do ponto de vista lógico, a RMAA é frequentemente construída sobre os protocolos Ethernet e TCP/IP que são definidos através do padrão IEEE802.3 e RFC793/RFC791 respectivamente. O padrão Ethernet está presente em soluções de fibra óptica, par trançado, cabo coaxial e *wireless.* Dentro das RMAAs, ele oferece uma variedade de soluções que permitem tratar diversas camadas que formam a infraestrutura física em um único e uniforme meio de acesso [17]. O protocolo responsável por escoar o tráfego entre as múltiplas redes públicas e privadas que podem conviver dentro da RMAA, e que permite também a troca de tráfego entre a rede da cidade e dos prestadores de serviços externos (telefonia pública, internet, etc) é o TCP/IP. Na verdade, o TCP/IP não se trata de um protocolo único, e sim de uma família de protocolos que trabalham juntos e interagem para garantir a comunicação de dados como encontramos, por exemplo, na Internet.

2.1.3 – Infraestrutura das RMAAs

Como dito anteriormente, a infraestrutura da RMAA é construída de forma modular visando, em sua proposta inicial, atender pontos prioritários. Posteriormente, a infraestrutura da RMAA de um município pode crescer e prover serviços adicionais à população.

A Figura 2.3 traz um exemplo de projeto conceitual de uma rede metropolitana de acesso aberto. Neste exemplo, o prédio da prefeitura funciona como a central de dados. Dentro de seu estabelecimento físico estão instalados os switches ópticos que operam no núcleo da rede, as interfaces com a telefonia móvel e convencional, e os servidores que

operam como gateway de voz. É também neste local que os *links* de Internet são concentrados. A partir do prédio da prefeitura saem as fibras ópticas que vão fornecer o meio físico do núcleo da rede na qual se conectarão as escolas e os hospitais.

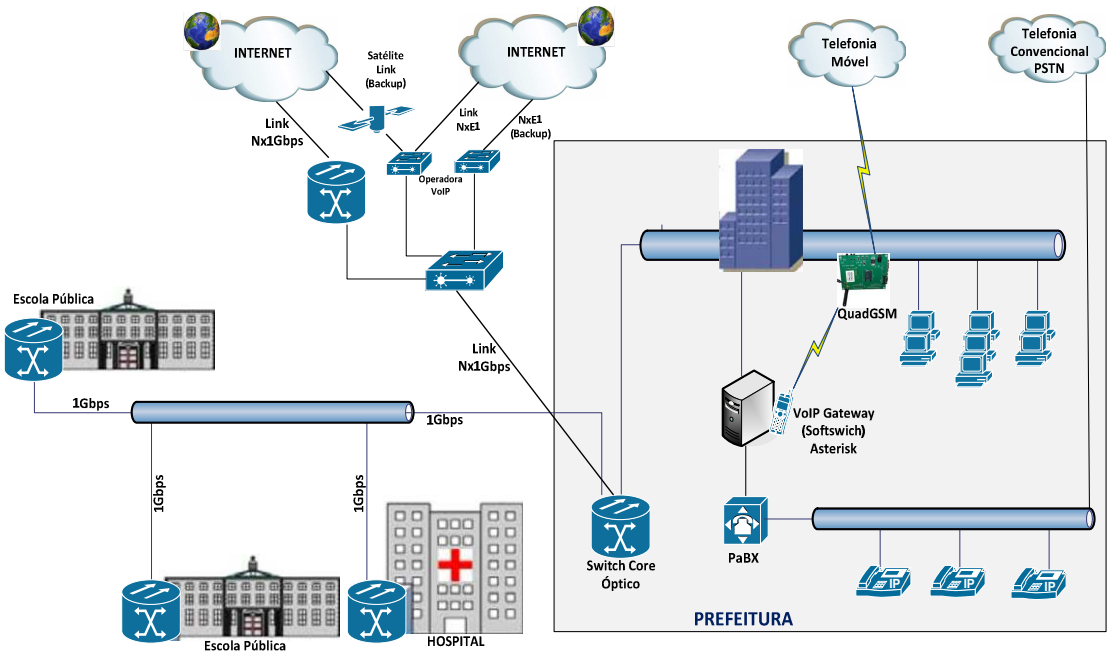


Figura 2.3 – Modelo conceitual de uma RMAA [17].

Para que a população esteja apta a usufruir dos serviços oferecidos, ela deve estar de alguma forma conectada à infraestrutura da RMAA. A abordagem mais simples adota um conjunto de células de rádio (sem fio) para cobrir a cidade. As células de rádio se enquadram na Camada de Acesso e se baseiam no padrão IEEE 802.11b/g. Este padrão oferece velocidade de 54 Mbps e opera na frequência não licenciada de 2,4GHz.

Para se conectar à Camada de Distribuição, as células de rádio utilizam cabo de par trançado ou enlaces de rádio. A Camada de Distribuição, por sua vez, pode se conectar ao núcleo da rede através de conexões ópticas ou até mesmo enlaces de rádio no padrão IEEE 802.11a que operam na frequência de 5,8GHz. Neste caso, opta-se por utilizar o padrão IEEE 802.11a pela velocidade alcançada de 108 Mbps e ausência de interferências.

Com intuito de melhorar a qualidade e o rendimento, as células de acesso são pequenas, com raio máximo de 100 metros, e podem concentrar até 60 pontos de acesso. Esta é uma das maneiras existentes nas quais os moradores podem ter acesso à RMAA e,

consequentemente, à Internet. A Figura 2.4 mostra o modelo de distribuição através de soluções de acesso sem fio.

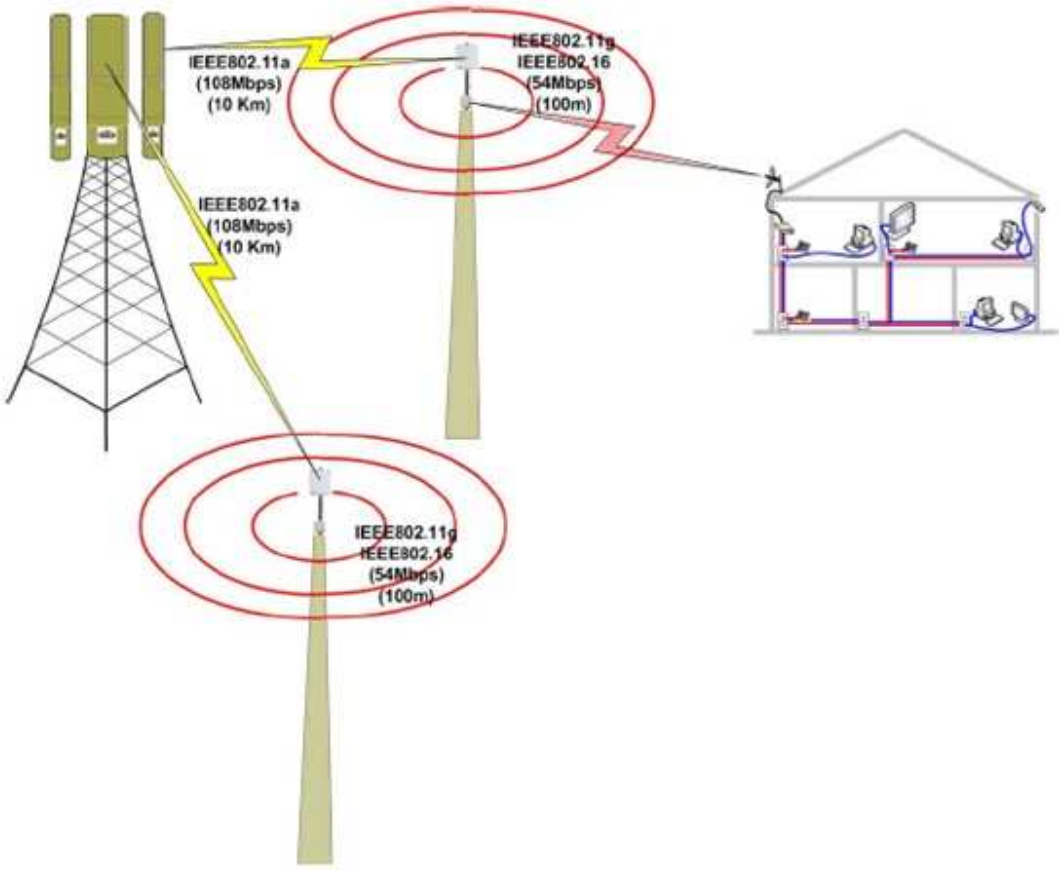


Figura 2.4 – Modelo de distribuição através de soluções sem fio [17].

Dependendo da situação, existem outras possíveis abordagens que podem substituir as células de rádio IEEE802.11b/g, tais como cabo de par trançado, tecnologia WiMAX definida no padrão IEEE 802.16 ou até fibra óptica (FTTH – *Fibre to the Home*). No cenário apresentado na Figura 2.5, os usuários se conectam à rede através de um switch DSLAM (*Digital Subscriber Line Access Multiplexer*) operando em modems ADSL2+ [17].

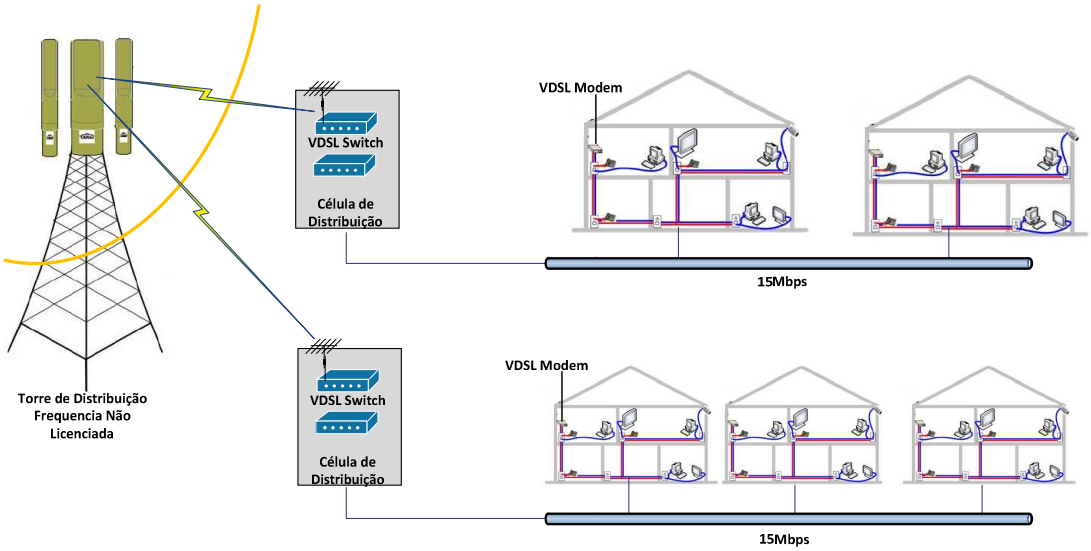


Figura 2.5 – Modelo de distribuição de acesso por modems VDSL nas RMAAs [17]

A Figura 2.6 apresenta o modelo de distribuição de acesso baseado no padrão WiMAX IEEE 802.16.

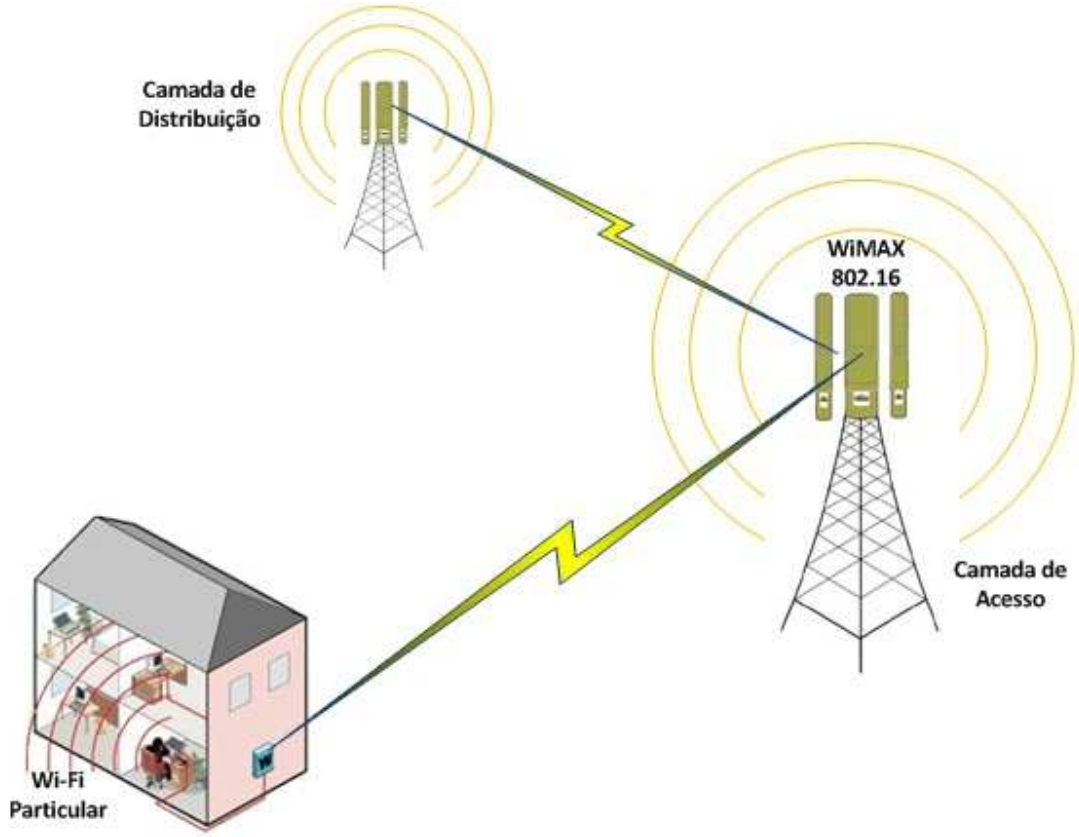


Figura 2.6 – Modelo de distribuição de acesso por células WiMAX.

A Figura 2.7 apresenta o modelo de distribuição de acesso por fibra óptica (FTTH).

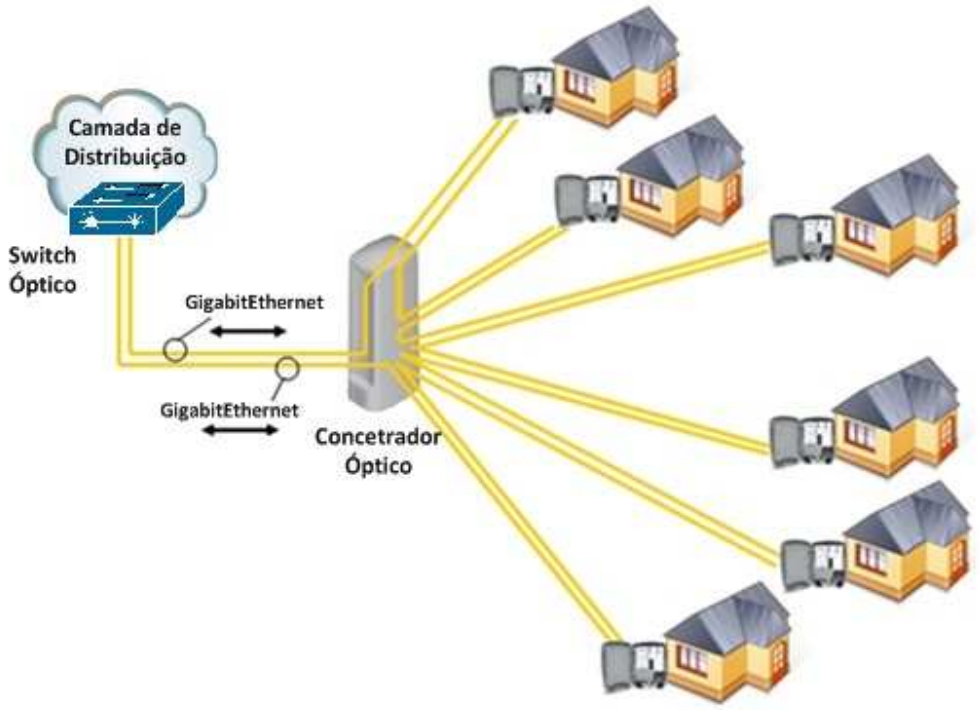


Figura 2.7 – Modelo de distribuição de acesso por FTTH.

2.1.4 – Exemplos de Redes Metropolitanas

Nesta seção, serão apresentados exemplos de implantações de redes metropolitanas de acesso aberto no mundo que obtiveram sucesso. A Tabela 2.1 demonstra alguns exemplos de cidades que adotaram o modelo de RMAA, e faz um paralelo entre tecnologia utilizada e as contribuições em cada situação, respectivamente.

Cidade	Tecnologia	Contribuições
Pedreira, Brasil	Híbrida – Fibra Óptica e sem fio	Interconexão de prédios públicos, distribuição de Internet para a população e VoIP corporativo.

Cidade	Tecnologia	Contribuições
Amsterdam, Holanda	Fibra Óptica	Desenvolvimento social e econômico, disponibilização de 20% da capacidade do backbone para a população através de *Fibre to the Home*.
Patras, Grécia	Híbrida – Fibra Óptica e sem fio	Interconexão de instituições de Educação, Pesquisa e Administração públicas.
Viena, Austria	Fibra Óptica	Disponibilização aos serviços de maneira igualitária à população.
Leiden, Holanda	Sem fio	Programa de distribuição de vídeo, servidores de jogos e VoIP.
Kutztown, Estados Unidos	Fibra Óptica	Fornecimento de conexões de fibra óptica de alta velocidade a residências, escolas, prédios públicos e privados.
Catalunha, Espanha	Fibra Óptica	Provisionamento de câmeras de segurança nas ruas, gerenciamento de tráfego, controle dos semáforos.
Granbury, Estados Unidos	Sem fio	Criação de uma rede que contempla a união de serviços de segurança pública (polícia, bombeiros e serviços de emergência) e da administração municipal.
Cheynne, Estados Unidos	Sem fio	Gerenciamento de controle de tráfego de trânsito.
Spokane, Estados Unidos	Sem fio	Aplicação de e-Government.
Wellington e Auckland, Nova Zelândia	Híbrida: Fibra Óptica e sem fio	Redução de custos com serviços de telecomunicações uma vez que os usuários (população) são os proprietários da rede.

Cidade	Tecnologia	Contribuições
Shangai, China	Híbrida – Fibra Óptica e sem fio	Aplicação de e-Government. Sistema de pagamento eletrônico, informatização de setores da educação e saúde.
Irlanda (94 cidades)	Híbrida – Fibra Óptica e cabo coaxial	Desenvolvimento social e econômico, distribuição de acesso a Internet à população.
Estocolmo, Suécia	Fibra Óptica	Desenvolvimento da infraestrutura óptica do município visando a ciência da informação, viabilização de acesso da população aos serviços dos provedores.

Tabela 2.1 – Redes Metropolitanas no mundo [22][23].

Um benefício herdado da implantação de uma rede metropolitana de acesso aberto é a possibilidade do município se tornar um provedor de serviços de comunicações, criando novas alternativas na captação de recursos [24]. Por ser uma rede que opera numa hierarquia baseada nos protocolos TCP/IP, conforme dito anteriormente, qualquer aplicação compatível com esse protocolo estará apta a utilizar a capilaridade e os recursos da rede metropolitana de acesso aberto. Os exemplos a seguir destacam implantações de rede metropolitanas que obtiveram sucesso no mundo.

2.1.4.1 Rede Metropolitana de Wellington e Auckland

A cidade de Wellington é a capital da Nova Zelândia, e até o final do ano de 2011, tinha aproximadamente 393 mil habitantes. O projeto de sua rede metropolitana de acesso aberto se iniciou em 1995 a partir de uma iniciativa do Conselho da Cidade de Wellington.

O objetivo dos idealizadores deste projeto foi construir uma infraestrutura avançada de telecomunicações que viabilizasse as empresas privadas e governamentais o acesso aos serviços de telecomunicações desejados [25]. Dez anos depois a rede se expandiu para a cidade de Auckland, que é a capital financeira do país.

A infraestrutura da rede de Wellington e Auckland foi construída de maneira híbrida, onde a maior parte da rede é composta por enlaces ópticos. Atualmente 548 prédios estão conectados à infraestrutura. A Figura 2.8 apresenta a RMAA de cada cidade, na qual as ramificações azuladas representam a capilaridade óptica e a grande mancha alaranjada demarca o perímetro da cidade.

Figura 2.8 – Rede metropolitana de Wellington e Auckland [25].

A Figura 2.9 demonstra o modelo de serviço oferecido. A ilustração representa do ponto de vista lógico como a rede está situada. Tanto as operadoras (ISP) quanto os usuários estão conectados à infraestrutura (representado pelo barramento em azul). Através da capacidade de transmissão da rede, os serviços providos pelas operadoras (destacados pela linha pontilhada) chegam aos usuários. Os serviços podem ser vídeo, dados, VoIP, áudio, telefonia convencional e móvel, entre outros. Dentro do grupo de usuários, os que possuem sistema autônomo (*Autonomous Systems* - ASs) podem estabelecer acordos de troca de tráfego de Internet com outros ASs.

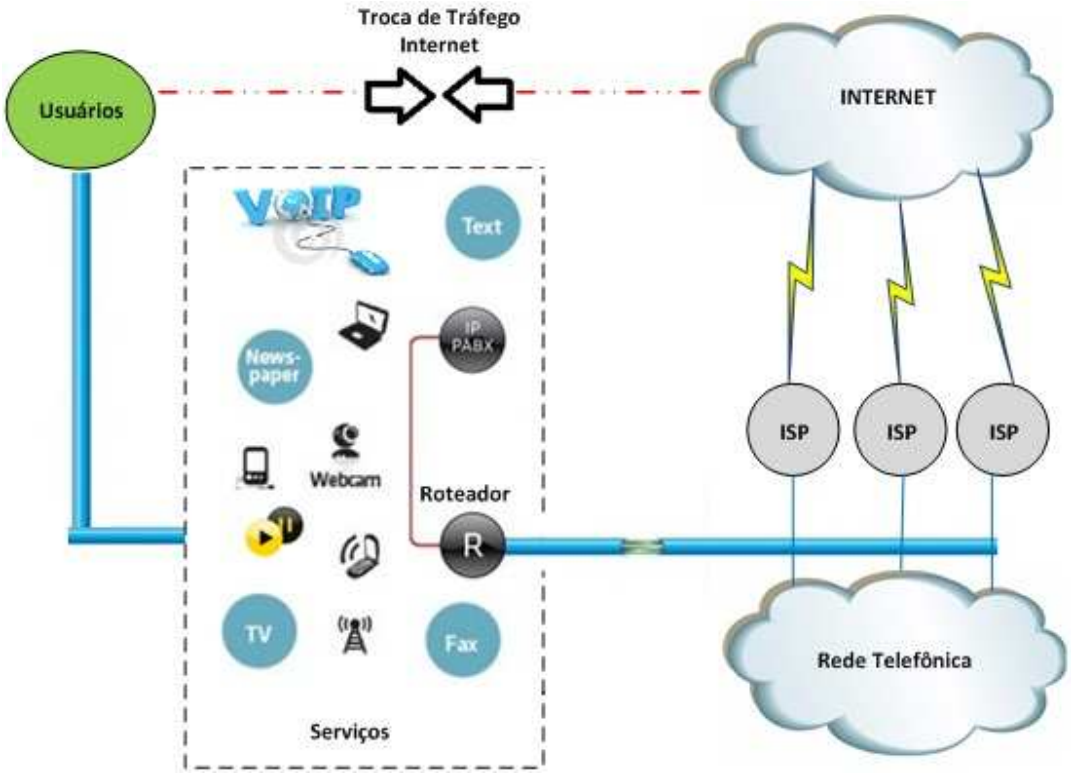


Figura 2.9 – Serviços oferecidos na RMAA de Wellington e Auckland.

Segundo os idealizadores deste projeto, o investimento trouxe benefícios econômicos à cidade e consequentemente aos seus cidadãos, uma vez que houve economia na contratação dos serviços oferecidos pelas operadoras.

Os serviços são comercializados através da Internet e podem atender diferentes públicos. Eles podem ser oferecidos tanto pelo setor privado quando público, e dentre os principais identificamos:

- LAN Pública: onde os usuários podem conectar suas residências diretamente a rede das operadoras através de uma rede Metro Ethernet;
- Troca de Tráfego Internet: empresas podem realizar troca de tráfego Internet sem precisar trafegar pela rede das operadoras;
- Bridge: oferece interconexão entre dois pontos localizados em cidades distintas através de uma conexão segura e privada;

- Harmonia: disponibiliza compartilhamento de vídeos e músicas que podem ser adquiridos sob demanda;
- WatchNET: disponibiliza um segmento dedicado para transporte de alta velocidade de imagens de câmeras de vigilância que atendem os principais pontos da cidade.

Outro serviço importante é chamado de CaféNET, no qual células sem fio são espalhadas por ambas cidades, e os usuários têm acesso à Internet efetuando pagamento via cartão de crédito ou de forma antecipada.

Uma vez que há competição entre os provedores de serviço, o custo dos serviços tende a diminuir beneficiando o usuário final. Um exemplo de concorrência ocorre no serviço VoIP, já que metade dos trinta e cinco provedores que estão interligados à rede metropolitana de Wellington e Auckland, oferece serviço telefônico IP.

2.1.4.2 Rede Metropolitana da Irlanda

A República da Irlanda é um país europeu com cerca de seis milhões de habitantes. As RMAAs irlandesas foram construídas em duas fases, após uma concessão exclusiva do governo irlandês. O projeto consistiu em criar redes metropolitanas em algumas cidades do país.

A fase inicial teve início no ano de 2004 e contemplou a criação de uma infraestrutura óptica que atendia vinte e oito cidades. Na segunda fase, a infraestrutura foi estendida a mais sessenta e seis municípios, abrangendo ao todo noventa e quatro cidades.

Este investimento impulsionou a indústria de telecomunicações irlandesa e popularizou a banda larga no país. Segundo [26], a RMAA estimulou a competição entre os provedores reduzindo com isso o custo dos serviços de telecomunicações.

A infraestrutura óptica disponibilizou acesso igualitário às operadoras incentivando a disputa por mercado. O acesso aberto trouxe à população contato com diferentes serviços que puderam ser oferecidos com custo reduzido, como por exemplo, acesso à Internet e telefonia VoIP. A Figura 2.10 apresenta as cidades contempladas no projeto.

Figura 2.10 – RMAAs da Irlanda [26].

2.2 – Tecnologia VoIP

Com o surgimento da Internet, cada vez mais universidades e instituições privadas investem em pesquisas buscando criar tecnologias que visam melhorar os serviços existentes. Dentro dessas melhorias surgiu a telefonia IP. A telefonia IP, também conhecida como VoIP (*Voice Over IP*), pode ser caracterizada como qualquer aplicação telefônica que opera sobre uma rede de comutação de pacotes de dados, que utiliza o protocolo IP (*Internet Protocol*) [27][28].

Segundo Darlington [29], desde o surgimento da Internet, companhias começaram a explorar a possibilidade de inserir tráfego de voz na rede de dados. O surgimento do VoIP se deu em 1995, e foi paulatinamente sendo difundido no mercado. A partir de 1998, empresas americanas realizaram os primeiros testes, e assim a tecnologia pôde ser aprimorada e novas aplicações foram surgindo. Desde 2005, a popularidade da telefonia IP está em constante crescimento. Segundo pesquisa realizada pelo grupo Teleco, no ano de 2007 existiam 700 mil assinantes VoIP no Brasil. Em 2009 este número era cerca de 2 milhões, mostrando um crescimento bastante acentuado em um período de dois anos.

O mercado da telefonia IP concentra-se em dois tipos de aplicações chaves. O primeiro consiste em redes privadas, geralmente em ambientes corporativos, que visam aproveitar a infraestrutura de rede existente (*intranet*), inserindo serviços de voz com tecnologia de telefonia IP. Dessa forma, gera-se economia para a corporação, pois ela centraliza a gerência dos sistemas (voz e dados) e economiza com a tarifação realizada pelas operadoras telefônicas [28]. O segundo modelo onde a telefonia IP é aplicada, consiste na utilização de dispositivos que são projetados para permitir o transporte de voz entre redes de telefonia convencional e a rede de dados [28]. Este tipo de aplicação tornou-se popular em grandes corporações que possuem escritórios distribuídos pelo mundo, pois com o uso do VoIP as ligações de longa distância ficaram significantemente mais baratas.

Para que o serviço VoIP possa operar, é necessário utilizar terminais apropriados que diferem bastante em complexidade dos telefones analógicos convencionais. A complexidade que existe é decorrente da quantidade de recursos suportados pelos terminais IP. Normalmente se utilizam os seguintes tipos de terminais IP:

- Computador: desde que ele tenha uma placa de som, microfone, auto falantes ou fones de ouvido, e um programa do tipo *softphone*, que possui todos os recursos de um terminal IP;
- Adaptador para Telefone Analógico (ATA): é um dispositivo cujo papel é operar como conversor de um terminal IP para um telefone analógico convencional. O ATA deve ser conectado tanto na rede IP quanto no telefone analógico convencional;
- Telefone IP: é um aparelho telefônico digital que possui todos os recursos necessários para suportar o serviço VoIP.

As conversações baseadas em telefonia IP podem ocorrer das seguintes formas [28][30]:

- De um terminal VoIP para outro: os usuários utilizam dispositivos que operam como terminais IP, como *smart phones* ou telefones IP para realizar as chamadas VoIP. Até mesmo computadores ou tablets podem ser utilizados com o auxilio de *softwares softphone,* conforme mencionado anteriormente. Neste tipo de conversação o usuário pode tanto discar o número VoIP de destino, quanto digitar o nome do destinatário. Neste caso a resolução do nome é feita por DNS (*Domain Name Server*);

- De um terminal VoIP para um terminal na PSTN (*Public Switched Telephony Network)*: os usuários realizam a chamada a partir de um terminal conectado à rede IP com destino a um número que está cadastrado na rede de telefonia convencional;

- De um terminal na PSTN a outro terminal na PSTN: neste caso, a utilização do VoIP se caracteriza pela presença de troncos IP no caminho entre a origem e o destino da conversação;

- De um terminal na PSTN para um terminal VoIP: o usurário VoIP recebe um número convencional de telefone para receber chamadas provenientes da rede pública. A chamada parte de um terminal cadastrado na telefonia convencional com destino a um terminal conectado à rede IP.

As Figuras 2.11, 2.12 e 2.13 apresentam as possíveis maneiras que conversas baseadas em telefonia IP podem ocorrer.

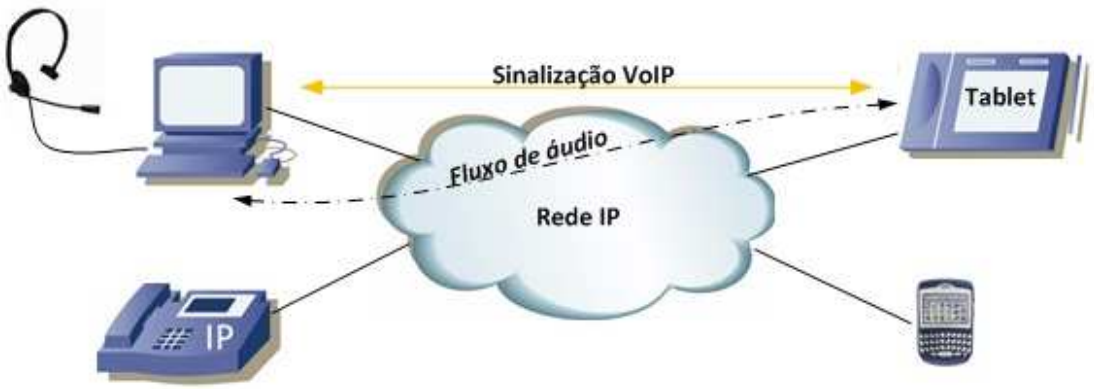


Figura 2.11 – Terminal VoIP para terminal VoIP.

Na Figura 2.12 dois novos elementos foram inseridos: os gateways de voz e de sinalização. O gateway de voz é responsável por repassar o fluxo de voz entre a rede IP e a PSTN. Suas principais funções caracterizam-se [31]:

- ✓ Codificação, decodificação e transcodificação da voz digital quando a transmissão de áudio na PSTN é analógica;
- ✓ Adaptação dos formatos digitais de áudio quando as codificações utilizadas na PSTN e na rede IP são diferentes;
- ✓ Transmissão e recepção de amostras de áudio presentes em datagramas IP;
- ✓ Encerramento das chamadas na PSTN.

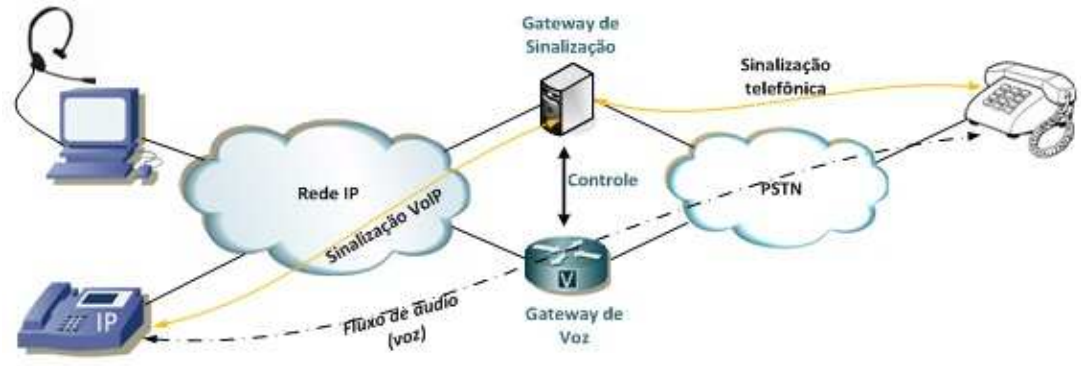


Figura 2.12 – Terminal VoIP para terminal PSTN ou vice-versa [32].

O gateway de sinalização, por sua vez, é responsável por controlar a geração das informações de sinalização presentes nas chamadas correntes efetuadas pelo gateway de voz. Suas principais funções caracterizam-se:

- ✓ Conversão da sinalização, traduzindo os tons de sinalização utilizados na telefonia convencional para sinalização VoIP;
- ✓ Geração de sinais nas linhas telefônicas, como tom de discagem ou ocupado [31].

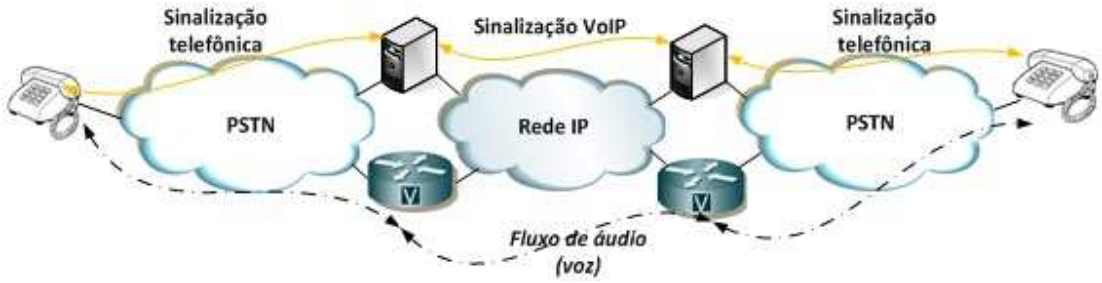


Figura 2.13 – Terminal PSTN para terminal PSTN.

Na Figura 2.13 as chamadas tradicionais podem ser transportadas dentro da rede IP das operadoras. A intenção de transportar pacotes de voz sobre a rede de dados tem obtido sucesso por apresentar diversas vantagens:

- O uso da telefonia IP é mais viável financeiramente do que a telefonia convencional [28][29][30][33];
- Flexibilidade, pois diferentes tipos de tráfego são convergidos na mesma rede;
- O VoIP permite que organizações integrem seus serviços (telefone, fax, e-mail, etc) em uma única plataforma;
- O sistema VoIP pode promover práticas de trabalho flexíveis, ou seja, funcionários remotos ou terceirizados podem ser identificados quando estão conectados na rede local da empresa;

- Criação de novas classes de serviços, vídeo conferência, tele-serviços, *call centers*, etc.

Por utilizar a rede de dados, os serviços VoIP seguem o modelo de melhor esforço (*best effort*) do protocolo IP. Na Internet, frequentemente não há rotas fixas para os pacotes pertencentes a uma determinada conversação. Com isso, pacotes da mesma sessão podem percorrer caminhos diferentes, que nem sempre são os mais adequados para atender os níveis de qualidade exigidos na transmissão de voz. O VoIP, portanto, apresenta dificuldades para atingir um nível de qualidade de serviço semelhante ao da telefonia convencional e para manter a estabilidade da qualidade durante a chamada. Outro desafio é oferecer uma disponibilidade similar a da rede telefônica convencional, superior a 99,999% [28].

Dentre as desvantagens apresentadas pela tecnologia VoIP em comparação com a telefonia convencional, podem ser destacadas [30]:

- Confiabilidade, uma vez que a disponibilidade da rede da operadora VoIP pode afetar a estabilidade do VoIP;
- No ambiente doméstico a desconfiança é relacionada com a garantia de serviços críticos, como ligações de emergência, uma vez que o telefone IP é dependente da energia elétrica;
- Garantia de privacidade, já que a telefonia IP herda todas as vulnerabilidades da rede IP, interferindo na segurança da informação;
- Rapidez, segundo [31], o tempo de geração de tom de discagem, alerta de chamada, e desconexão são superiores na telefonia VoIP.

Operacionalmente, o VoIP é suportado por um conjunto de protocolos que são responsáveis pelo estabelecimento das chamadas IP, transporte de mídia, manutenção do serviço, entre outros. Estes protocolos serão abordados nos tópicos seguintes.

2.2.1 – Protocolos de Transporte de Mídia

Conforme mencionado anteriormente, frequentemente na rede de dados o tráfego de pacotes não possui um caminho pré-definido, uma vez que o envio dos mesmos não obedece a uma rota fixa, variando de acordo com a disponibilidade e fluxo das rotas na rede. Além disso, não há reserva de recursos para as aplicações VoIP caso esteja sendo seguido o modelo de melhor esforço. Consequentemente, a instabilidade da rede afeta diretamente o desempenho das aplicações como o VoIP que opera em tempo-real. Visando otimizar a transmissão dos dados oriundos de aplicações de tempo-real, surgiram protocolos como o RTP e o RTCP [34].

2.2.1.1 – *Real-Time Transport Protocol* (RTP)

O protocolo RTP (*Real-time Transport Protocol*) foi definido pela RFC 3550 e sua principal função é gerenciar a transmissão de dados de aplicações de tempo-real como o VoIP.

Em conjunto com o protocolo UDP (*User Datagram Protocol*), o RTP oferece as funcionalidades necessárias para o transporte de mídia em tempo real. O UDP é preferido, pois o TCP poderia acrescentar um atraso incompatível com aplicações de tempo-real por causa de seus mecanismos de controle de congestionamento e controle de fluxo. Estão atreladas ao RTP funcionalidades como identificação do tipo de dado transportado, número da sequência, indicação de tempo de amostragem (*timestamping*) e monitoramento de entrega de pacotes.

O RTP é caracterizado também por encapsular os dados de mídia, mas não garante qualidade de serviço e não fornece mecanismos para certificar que o dado será entregue, e quando entregue chegará ao destino na ordem esperada. Porém, o número de sequência incluído no cabeçalho do RTP permite que os pacotes sejam reordenados no destino na sequência correta.

2.2.1.2 – *Real-Time Control Protocol* (RTCP)

O RTCP (*Real-Time Control Protocol*) é um protocolo complementar ao RTP responsável por coletar estatísticas e prover informações de controle durante a transmissão de fluxos RTP.

Do mesmo modo que o RTP, o RTCP é tipicamente usado sobre o UDP que por sua vez deve multiplexar os pacotes de mídia e de controle utilizando números diferentes de portas lógicas [34].

Dentre as principais funções do RTCP caracterizam-se:

- Fornecer *feedback* aos participantes da sessão referente a qualidade de serviço na distribuição da mídia. O conteúdo passado aos participantes informa a quantidade de pacotes que foram transmitidos, pacotes perdidos, atrasos, *jitter*, entre outros;
- Rastrear os participantes da sessão. O RTCP identifica a origem de uma sessão RTP através de um identificador persistente chamado de nome canônico ou CNAME. Se a aplicação for reiniciada, o identificador CNAME que pertence ao originador da sessão é solicitado pelo receptor para rastrear a sessão perdida. Assim, a sessão pode ser mantida. O CNAME também pode ser utilizado para sincronizar a transmissão de mídia de um participante que utiliza múltiplas sessões RTP para transferência dos dados;
- Fornecer subsídios para que os participantes da sessão possam calcular a taxa de envio de pacotes. É através das mensagens RTCP que cada participante conhece o número de terminais se comunicando via RTP;
- Transporta informações de controle de sessão, como por exemplo, informações do participante que devem ser exibidas na interface do usuário.

Os pacotes RTCP são responsáveis por transportar várias informações de controle e podem ser dos seguintes tipos:

- SR (*Sender Report*): utilizado para gerar estatísticas da transmissão e recepção de participantes que são transmissores ativos em uma sessão;

- RR (*Receiver Report*): utilizado para gerar estatísticas da recepção dos participantes que não são transmissores ativos em uma sessão;
- SDES (*Source Description*): itens de descrição de origem, incluindo o CNAME;
- BYE: indica o final da participação de uma aplicação em uma sessão;
- APP: utilizado em funções específicas de aplicação.

2.2.2 – Protocolos de Sinalização

Diferentemente do transporte de mídia, existem diversos padrões de protocolos de sinalização. Na tecnologia VoIP, os protocolos de sinalização devem especificar a operação dos seguintes itens:

- Codificação da voz;
- Configuração da chamada;
- Modo de autenticação.

Além dos itens acima citados, os protocolos de sinalização são responsáveis por estabelecer, controlar, gerenciar e encerrar as chamadas. Nas próximas seções serão apresentados os três protocolos de sinalização mais utilizados em chamadas que envolvem VoIP.

2.2.2.1 – H.323

O H.323 é uma recomendação da *International Telecommunication Union-Telecommunication Standardization Sector* (ITU-T) para especificar a comunicação multimídia baseada em redes de comutação de pacotes. Além disso, estabelece padrões para codificação e decodificação de fluxos de áudio e vídeo. Ele foi desenvolvido antes do surgimento do VoIP, porém ainda é muito utilizado na telefonia IP mesmo com o surgimento do *Session Initiation Protocol* (SIP).

A adoção do padrão H.323 para aplicações multimídia em redes traz uma série de benefícios, entre os quais se destacam [32]:

- Independência da rede;
- Interoperabilidade de equipamentos e aplicações;
- Independência da plataforma;
- Representação padronizada de mídia;
- Interoperabilidade entre redes (ex: LAN e PSTN);
- Suporte a gerenciamento de largura de banda;
- Suporte a conferências multiponto;
- Suporte a *multicast*.

A recomendação H.323 engloba várias outras recomendações da ITU-T, como o H.225.0, H.245, Q.931 e RAS (*Registration, Admission and Status*). O H.225.0 é responsável pelo registro, admissão, controle e sinalização das chamadas. O H.245 é utilizado para troca de mensagens que contém as características suportadas pelos terminais (ex.: codecs, taxa de transmissão tolerável, etc). O Q.931 é responsável pela sinalização que estabelece e encerra uma chamada estabelecida com base no padrão H.323. Já o RAS é responsável pela troca de informações entre terminais e *gatekeeper*, além dos já apresentados RTP e RTCP.

O padrão H.323 especifica quatro tipos de componentes, que juntos possibilitam a comunicação multimídia. São eles:

- Terminal: pode ser um computador pessoal ou um equipamento executando uma aplicação H.323, que prevê comunicação em tempo real. Todos os terminais devem suportar voz;
- Gateway: são elementos que tem como função prover a comunicação dos terminais H.323 com outros terminais que utilizam padrões diferentes;
- *Gatekeeper*: elemento de caráter opcional, é usado para controle de admissão e resolução de endereços. Também são responsáveis pelo gerenciamento da largura de banda em conferências H.323;
- MCU: responsável por administrar conferências multipontos. Manipula as negociações entre os terminais para determinar a capacidade comum entre eles de processamento de áudio e vídeo. Seu uso também é opcional.

A Figura 2.14 ilustra um exemplo típico de sistema H.323.

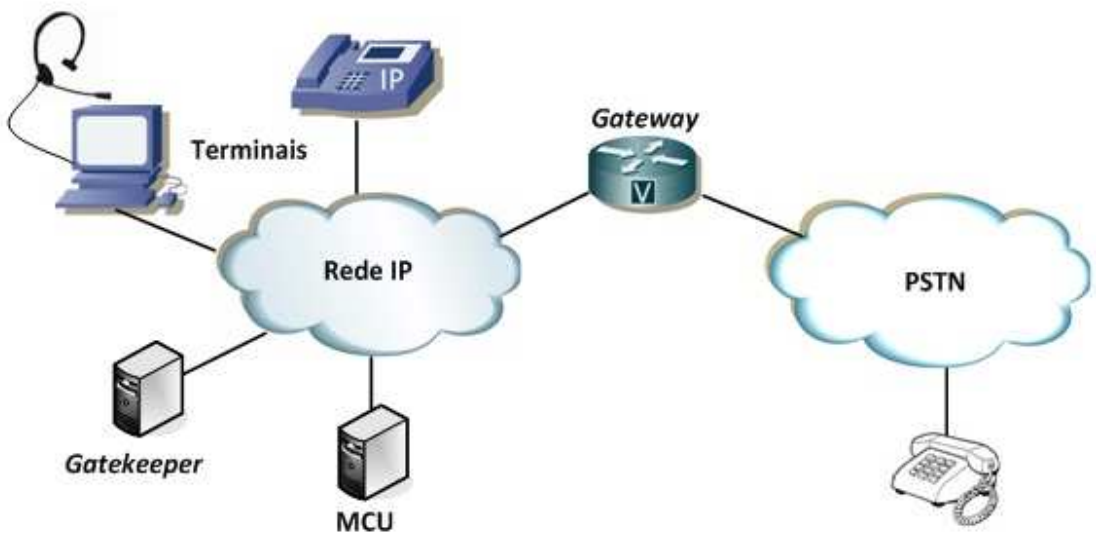


Figura 2.14 - Componentes de um sistema H.323.

2.2.2.2 – *Session Initiation Protocol* (SIP)

O SIP (*Session Initiation Protocol*) é um protocolo da camada de aplicação, que utiliza sintaxe baseada em texto, similar ao HTTP (*Hypertext Transfer Protocol*), para estabelecer e gerenciar sessões multimídia. Ele foi definido pela *Internet Engineering Task Force* (IETF) através da RFC 3261, e atualmente é considerado o grande pilar que sustenta o VoIP. Isso se deve a sua simplicidade e flexibilidade para introduzir novos serviços.

O SIP opera em conjunto com outros protocolos como o RTP/RTCP, responsáveis pelo transporte de mídia, e o SDP (*Session Description Protocol*), cuja função é descrever sessões multimídia.

A Figura 2.15 mostra a representação lógica de um sistema baseado no protocolo SIP.

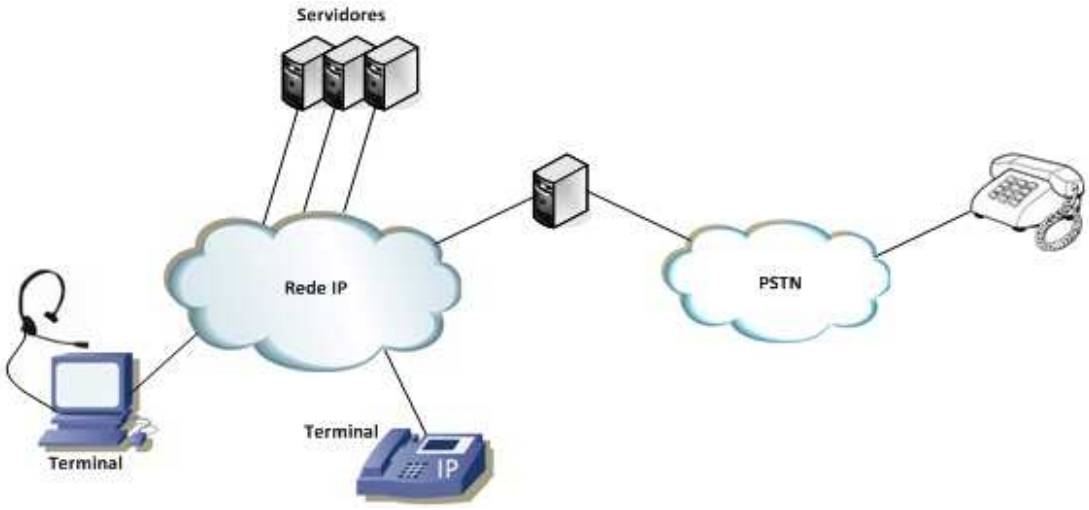


Figura 2.15 - Componentes de um sistema SIP

Como pode ser observado, este modelo é composto somente por terminais ou servidores. O terminal, também chamado de agente do usuário (UA – *User Agent*), pode operar como cliente (UAC – *User Agent Client*), quando ele solicita o inicio da sessão SIP, ou como servidor (UAS – *User Agent Server*), quando ele responde a solicitação de outro UAC. O servidor, por sua vez, pode intermediar chamadas, traduzir nomes conhecidos em endereços roteáveis, rotear mensagens de sinalização e solicitações de redirecionamento entre terminais [35].

Dentro de uma rede IP, os servidores são caracterizados de três maneiras:

- Servidor Proxy: roteia mensagens de requisição de maneira que elas sejam encaminhadas para um elemento mais próximo do destino. Ele interpreta e, se necessário, reescreve partes específicas e essenciais das mensagens de requisição antes das mesmas serem encaminhadas. Também é útil para fins de bilhetagem e na execução de políticas de segurança;
- Servidor de Redirecionamento: responde ao pedido do agente do usuário (terminal) fornecendo resolução de nomes e informando a localização a qual o usuário poderá ser encontrado;
- Servidor de Registro: registra a localização atualizada dos usuários e repassa esta informação ao servidor de redirecionamento.

As mensagens trocadas no SIP são baseadas em requisições e respostas. Abaixo são destacados os tipos de requisições e suas respectivas descrições:

- INVITE: É a primeira mensagem enviada por um usuário que deseja convidar outro a estabelecer uma sessão multimídia. Esta mensagem contém informações que descrevem parâmetros de mídia que este terminal pretende utilizar. Estas informações são formatadas através do protocolo SDP (*Session Description Protocol*);

- ACK: É uma mensagem de reconhecimento enviada pelo transmissor para confirmar ao receptor que sua mensagem de confirmação foi recebida com sucesso. O ACK representa o conceito de *three-way handshake* utilizado também nas sessões TCP;

- OPTIONS: Realiza diversas consultas ao servidor, dentre elas quais são os tipos de mídia suportados pelo receptor antes do estabelecimento da chamada;

- BYE: Independentemente do sentido, esta mensagem é usada para encerrar a sessão a qualquer instante da chamada;

- CANCEL: É utilizada para cancelar transações pendentes. O CANCEL identifica a chamada através das informações contidas no cabeçalho SIP;

- REGISTER: Os usuários enviam solicitações REGISTER para informar o servidor de registro sobre sua localização.

As respostas são definidas em seis categorias e são identificadas por códigos de três dígitos:

- 1xx - pedido recebido, continuando a processar o pedido;
- 2xx - a ação foi recebida, entendida e aceita com sucesso;
- 3xx - uma ação adicional deve ser tomada para completar o pedido;
- 4xx - o pedido contém sintaxe inválida e não pode ser processado;

- 5xx - erro de servidor;
- 6xx - falha global.

A Figura 2.16 apresenta sequencialmente as mensagens SIP que são trocadas entre dois terminais durante a inicialização e término de uma sessão SIP [35].

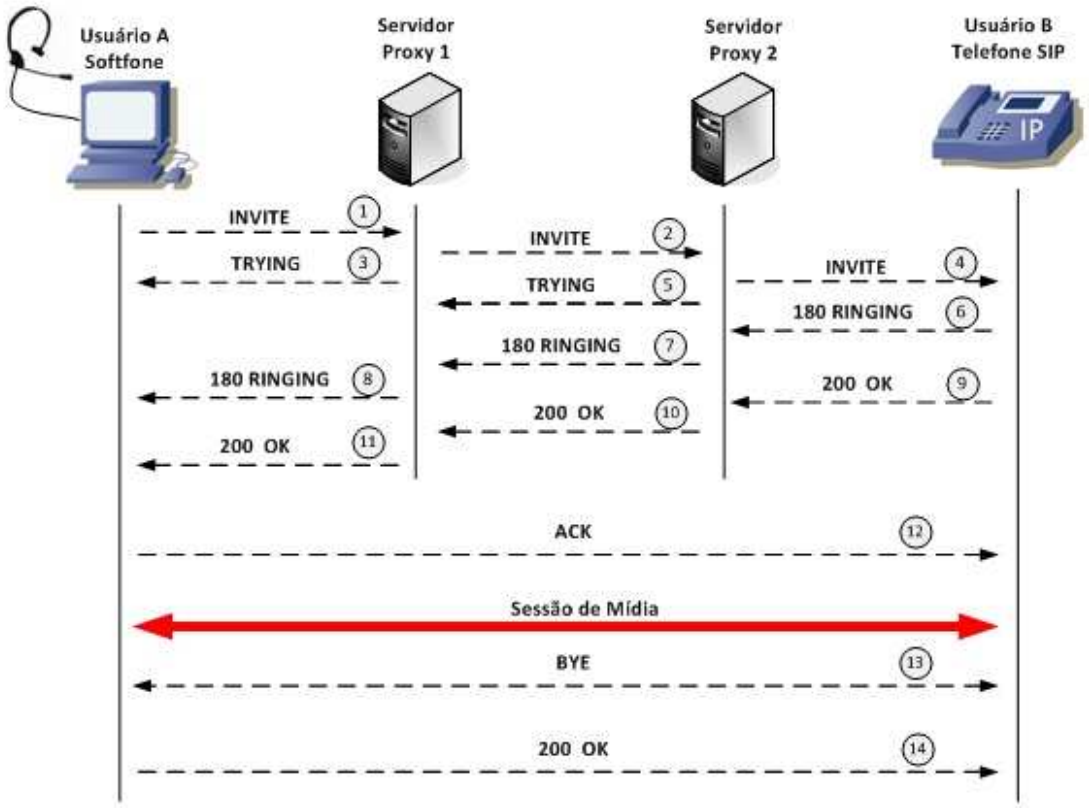


Figura 2.16 - Mensagens SIP.

A mensagem INVITE, contém informações do formato da mídia, do originador da chamada, endereço de origem e destino. O Usuário A recebe uma resposta informacional chamada de TRYING (100) do servidor proxy. Esta mensagem indica que o INVITE foi recebido pelo servidor e ele está trabalhando para encaminhá-lo ao destino. Fazendo uma analogia com as mensagens utilizadas na PSTN, esta mensagem se assemelha a mensagem Q.931, "Procedendo Chamada" (*Call Proceeding*).

Quando a mensagem chega ao ponto remoto, o telefone toca e uma mensagem do tipo RINGING (180) é enviada pelo terminal de destino ao terminal de origem. Quando

esta mensagem chega ao telefone de origem, a informação é passada ao usuário através de um tom musical ou uma mensagem no display do aparelho telefônico. Já na PSTN, esta mensagem é conhecida como Q.931 "Alertando" (*Alerting*). No instante em que o Usuário B atende a ligação, uma mensagem 200 OK é enviada ao Usuário A indicando que a chamada foi atendida. Neste momento, o Usuário B descreve, através do SDP, os parâmetros da chamada que ele deseja estabelecer. Neste ponto caracteriza-se o modelo de oferta e resposta de mensagens SDP.

Finalmente, o Usuário A envia uma confirmação ACK ao Usuário B, confirmando o recebimento da mensagem 200 OK. Este mensagem ACK pode carregar os últimos ajustes com relação aos parâmetros de tipos de mídia sugeridos pelo telefone remoto.

Após o estabelecimento da chamada, a mídia é transmitida entre as estações através do RTP, com o auxílio do RTCP. A próxima e última mensagem de sinalização é o BYE, utilizada por qualquer uma das partes envolvidas na sessão para encerrar a chamada. Como todas as mensagens dependem do UDP, o qual é um protocolo não orientado a conexão, nenhuma ação é tomada após o BYE.

A Tabela 2.2 apresenta uma comparação entre os sinais SIP e PSTN [28].

SIP	PSTN
TRYING	Q.931 CALL PROCEEDING
RINGING	Q.931 ALERTING
ACK	Q.931 CONNECT
INVITE	Q.931 CONNECT

Tabela 2.2 – Comparação entre mensagens SIP e PSTN [33].

Além dos protocolos que foram descritos anteriormente, dentro da Seção 2.2.2, existem outros que complementam o SIP e são conhecidos como protocolos de controle de *gateway*. Com o intuito de simplificar o trabalho dos *gateways,* eles separam as funções lógicas (sinalização, tratamento de mídia) que são desempenhadas pelos *gateways*. Os principais protocolos de controle de gateway de mídia são o MGCP (*Midia Gateway Controller Protocol*) e o Megaco/H.248 [35].

2.2.2.3 – IAX (*Inter-Asterisk Exchange*)

O Asterisk é uma ferramenta que incorpora os serviços disponibilizados em PABXs comerciais de telefonia convencional e possui flexibilidade permitindo a adição de mais serviços utilizando a tecnologia VoIP. O Asterisk suporta diversas aplicações como [36]:

- PABX: realiza controle de encaminhamento de chamadas entre terminais IP e convencionais;
- Gateway de voz: responsável por repassar o fluxo de voz entre a rede IP e a PSTN;
- *Voicemail:* integra aplicações *voicemail* através de um sistema de mensagem unificada, que encaminha mensagens de voz via email;
- URA (Unidade de Resposta Audível): tecnologia muito utilizada em *call centers* que permite detectar voz e sinais telefônicos no decorrer de uma chamada telefônica. Pode ser capaz de responder e interagir com o usuário através de mensagens de áudio pré-gravadas;
- Áudio conferência: suporta múltiplos terminais conectados simultaneamente na mesma chamada telefônica;
- Distribuição automática de chamadas: tecnologia utilizada em *call centers* que oferece inteligência na distribuição das chamadas entrantes.

Visando intercomunicar servidores Asterisk, a empresa Digium desenvolveu o protocolo Inter-Asterisk Exchange (IAX). Atualmente ele se encontra em sua segunda versão, denominada IAX2. O IAX2 foi especificado através da RFC 5456 com a categoria de informacional, indicando que ele ainda não foi padronizado.

O IAX2 é um protocolo *peer-to-peer* (P2P), responsável por controlar, registrar as localizações dos servidores, criar, modificar e terminar sessões multimídia.

O IAX2 opera de maneira semelhante ao protocolo SIP, exceto que no IAX2, o RTP e o fluxo de sinalização utilizam a mesma porta UDP: 4569. Com isso facilita a administração do NAT (*Network Address Transalation*) nos firewalls, e elimina-se a necessidade de outros protocolos operarem através do NAT. Outra característica importante

é que este protocolo permite o agrupamento de múltiplas sessões, de forma que eles sejam representados por meio de um único cabeçalho, reduzindo assim o consumo de banda.

O IAX2 é um protocolo autossuficiente, ou seja, ele combina funções de controle e transporte de mídia. Portanto, dentro de um ambiente VoIP, o IAX2 pode ser empregado ao invés do SIP ou H.323.

2.2.3 – Gerenciamento do VoIP

O VoIP é uma aplicação de tempo-real e, portanto, é sensível a latência. Segundo as considerações feitas em [34], em uma rede de dados, o desempenho de aplicações como o VoIP pode ser prejudicado por fatores como largura de banda, perda de pacotes, *jitter* e eco. Também podemos ter atrasos originados no processamento, empacotamento, enfileiramento e na serialização dos pacotes. Segundo definição da ITU-T, Qualidade de Serviço (QoS) é o efeito coletivo de diversos fatores de desempenho em um sistema, que determina o grau de satisfação de um usuário de serviços de telecomunicações.

Um dos meios para se alcançar qualidade nos serviços é a adoção de práticas de gerência de redes. O objetivo da gerência de redes é proporcionar o aproveitamento efetivo dos recursos disponíveis, o mapeamento da ocorrência de anomalias e problemas, a resolução destes problemas e a aplicação de medidas preventivas para minimizar o impacto dos problemas. Nas redes convergentes, como as RMAAs, os critérios de gerenciamento aplicados no tráfego de voz são, geralmente, os mesmos que são aplicados no tráfego de dados. Desta maneira, o monitoramento de recursos envolvidos diretamente na comunicação VoIP é mascarado e muitas vezes ofuscado. Por exemplo, nas RMAAs, os critérios de gerenciamento não levam em conta se o tráfego monitorado envolve aplicações de tempo real. A não ser através das reclamações dos usuários, os administradores não têm visibilidade do fluxo das chamadas VoIP e da qualidade com a qual elas estão sendo efetuadas.

Como o tráfego VoIP não recebe um tratamento dedicado de gerência dentro das redes convergentes, serão apresentados entre as Seções 2.2.3.1 a 2.2.3.3 os principais protocolos e padrões de gerência de redes utilizados atualmente. Será apresentada também uma nova alternativa de gerência VoIP, que faz parte da proposta deste trabalho: a utilização de IPDRs.

2.2.3.1 – *Simple Network Management Protocol* (SNMP)

O SNMP (*Simple Network Management Protocol*) é um protocolo de gerência definido no nível de aplicação, e é utilizado para obter e alterar informações de dispositivos ou agentes espalhados em uma rede baseada no TCP/IP [37]. Sua especificação foi definida no documento RFC 1157. No SNMP, os dados sobre os equipamentos são obtidos através de requisições de um gerente a um ou mais agentes utilizando os serviços do protocolo UDP para enviar e receber suas mensagens através da rede. O gerenciamento de uma rede convergente através do SNMP permite o acompanhamento simples e em tempo real do status dos elementos da rede, podendo ser utilizado para gerenciar diferentes tipos de sistemas. Este gerenciamento é conhecido como Modelo de Gerenciamento SNMP [38].

O modelo de operação do SNMP é baseado em dois elementos: o agente e o gerente. Cada equipamento gerenciado é visto como um conjunto de objetos que trazem informações sobre o estado atual do equipamento. Estas informações ficam a disposição do gerente, que pode consultar ou alterar o estado destes objetos enviando mensagens ao agente presente no elemento monitorado. Os objetos gerenciados são organizados dentro de uma base de dados de gerenciamento chamada de MIB (*Management Information Base*) definidos pela RFC 1213. A MIB fornece informações gerais de gerenciamento sobre um determinado equipamento da rede como: quantidade de pacotes transmitidos, utilização da interface, consumo de CPU e memória do equipamento, entre outros. Em outras palavras, todo recurso (objeto) de um equipamento que precisa ser monitorado pelo SNMP precisa estar armazenado dentro da MIB.

Através do SNMP é possível coletar diversas informações que têm atendido até os dias de hoje os gerentes de redes. No entanto, não existe dentro das MIBs padronizadas, objetos específicos que tratem o tráfego VoIP. Portanto, informações específicas do VoIP como chamadas com falha, chamadas com sucesso, congestionamento, assinante ocupado, não estão disponíveis no SNMP.

A Figura 2.17 apresenta um exemplo de relatório que pode ser obtido facilmente através do modelo de gerência VoIP orientado a IPDR. Esta figura apresenta a quantidade de chamadas realizadas com sucesso no dia 30 de setembro de 2009, comparada com um *baseline* de oito semanas.

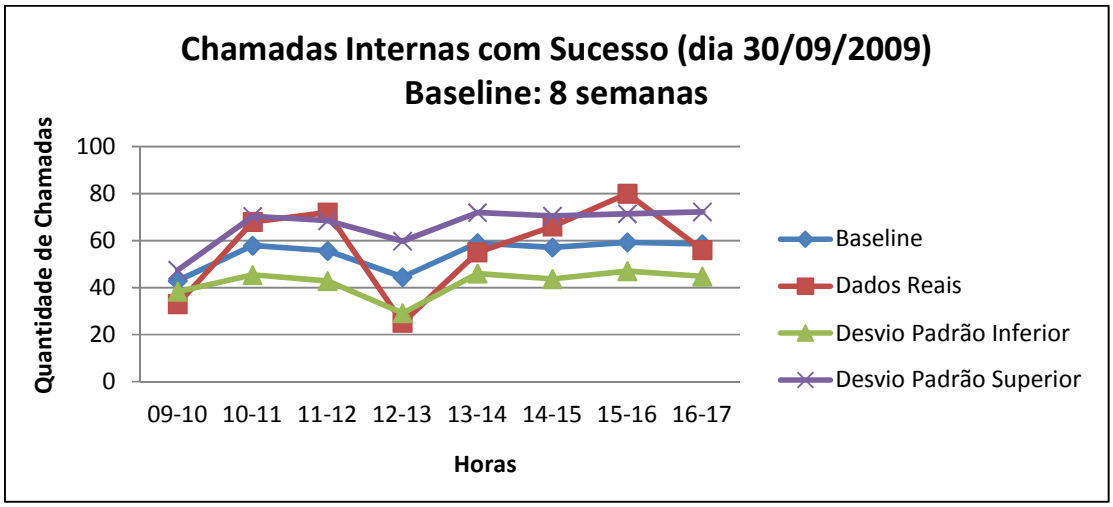


Figura 2.17 – Baseline de quantidade de chamadas com sucesso no dia 30/09/2009.

2.2.3.2 – IP *Flow Information Export* (IPFIX)

Em uma rede de dados, é importante que se possa realizar inspeções sobre os fluxos de pacotes que trafegam pelos elementos da rede. Com este propósito, o IETF, através da RFC 5101, desenvolveu o IPFIX para padronizar a maneira de coletar e exportar os dados sobre fluxos de pacotes em uma rede IP. O IPFIX foi uma padronização do protocolo NetFlow proprietário da Cisco.

A arquitetura do IPFIX é composta por três processos [39]:

- Processo de Medição (MP – *Measurement Process*);
- Processo de Exportação (EP - *Export Process*);
- Processo de Coleta (CP - *Collecting Process*).

O Processo de Medição é responsável por gerar o registro de fluxo. As informações que alimentam o processo de medição podem ser originadas, por exemplo, por uma interface de um elemento da rede. Dentre as funções desempenhadas pelo processo de medição caracterizam-se captura do cabeçalho dos pacotes, *timestamping*, amostragem, classificação e manutenção do registro de fluxo. O fluxo de dados fica armazenado na memória cache dos equipamentos IPFIX. Um dispositivo que hospeda um ou mais

processos de exportação é chamado dispositivo IPFIX. Como exemplo deste tipo de dispositivo, podemos destacar roteadores, switches multicamadas ou qualquer servidor com sistema operacional capaz de realizar funções de encaminhamento de pacotes e suportar o protocolo IPFIX.

O Processo de Exportação é responsável por enviar através de mensagens IPFIX o registro de fluxo para o Processo de Coleta. O Processo de Coleta por sua vez recebe o registro de fluxo enviado pelo Processo de Exportação. Ele é capaz de processar e armazenar o registro de fluxo. Denomina-se como Coletor um dispositivo que hospeda um ou mais processo de coleta. Como exemplo deste tipo de dispositivo, podemos destacar uma estação/servidor que hospeda um banco de dados para que os registros de fluxo sejam armazenados.

A Figura 2.18 apresenta a modelo da arquitetura do IPFIX:

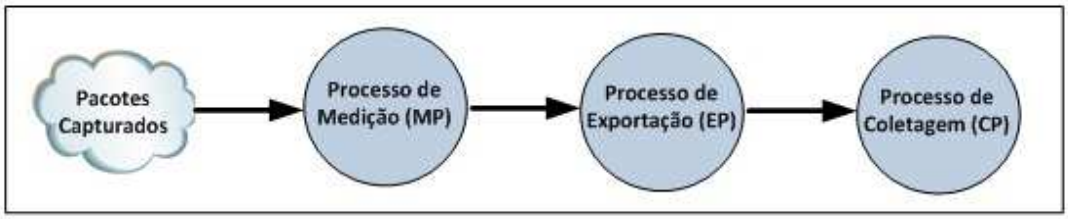


Figura 2.18 - Arquitetura IPFIX.

A troca de informações entre o Processo de Exportação e o Processo de Coleta é realizada por meio de mensagens IPFIX, as quais são baseadas em *templates* que especificam a estrutura e semântica das informações transmitidas. Elas são encapsuladas na camada de transporte pelos protocolos TCP, UDP e STCP (*Stream Control Transmission Protocol*). Adicionalmente, as mensagens IPFIX são compostas por um cabeçalho e um ou mais grupos de armazenamento. O cabeçalho IPFIX é formado por 16 bytes distribuídos em campos como: número da versão, tamanho da mensagem, *timestamp*, número de sequência e identificação de domínio de observação. A identificação de domínio de observação determina de onde o fluxo foi observado, pois um pacote pode pertencer somente a um domínio de observação. Geralmente o envio de dados através do IPFIX deve ser habilitado no núcleo da rede, em equipamentos que tratam os pacotes na camada de rede (camada 3 do modelo OSI).

Dentre os pontos positivos do IPFIX podemos destacar a flexibilidade, a utilização de *templates*, não ser exclusivo de um único fabricante, economizar banda ao enviar o fluxo de pacotes coletados, entre outros. Como ponto negativo, podemos destacar a necessidade de uma grande quantidade de dados para a geração de relatórios mais fundamentados. Ou seja, como o IPFIX gera estatísticas com base na análise de um fluxo de pacotes coletado, para que haja uma maior coerência de resultados, teoricamente, é necessário que os períodos das coletas sejam grandes. Outro ponto desfavorável é que o consumo de recursos dos dispositivos IPFIX é proporcional ao tamanho do período de coleta.

O IPFIX pode gerar estatísticas do consumo de banda por usuário, por aplicação, por protocolo, por URL, também pode analisar a latência das conexões e de chamadas VoIP, memória de equipamentos, quantidade de ataques, etc. No entanto, percebe-se que este protocolo atua na monitoração da rede pelo ponto de vista do tráfego de dados em geral, tratando igualmente os diferentes tipos de tráfego. No caso do VoIP, os tipos de análise que ele desempenha são uteis, porém não contemplam os resultados que buscamos. Em outras palavras, o IPFIX não trata informações específicas do VoIP.

2.2.3.3 – TMN

Uma das características encontradas em sistemas de telecomunicações é a heterogeneidade das redes e de equipamentos. No final da década de oitenta, a *ITU (International Telecommunications Union)* [40] criou um conceito básico visando padronizar a gerência das redes de telecomunicações, denominado Rede de Gerência de Telecomunicações *(TMN – Telecommunications Management Network).*

A TMN foi desenvolvida com o objetivo de gerenciar redes, serviços e equipamentos heterogêneos, operando sobre equipamentos e tecnologias de diversos fabricantes que possuem funções de gerência. A TMN oferece uma arquitetura básica, que permite a integração entre os sistemas de gerência e os equipamentos de telecomunicações através de modelos genéricos de gerência, criando padrões para administradores e fabricantes.

Os princípios básicos da TMN baseiam-se em recomendações. A seguir é apresentada a lista de recomendações da série M.3000:

- M.3010 – *Principles for a TMN;*
- M.3020 – *TMN Interface Specification Methodology;*
- M.3100 – *Generic Network Information Model;*
- M.3180 – *Catalogue of TMN Management Information;*
- M.3200 – *TMN Management Services;*
- M.3300 – *TMN Management Capabilities Presented at the "F" Interface;*
- M.3400 – *TMN Management Functions.*

A TMN considera as redes e os serviços de telecomunicações como sendo um conjunto de sistemas cooperativos e os gerencia de forma harmônica e integrada. A interação entre as redes de telecomunicações e a TMN ocorre em vários pontos e é realizada por interfaces padronizadas, podendo até dispor de parte da rede de telecomunicações para realizar suas funções.

Existem diversos tipos de redes, serviços e elementos que podem seguir o padrão de gerenciamento TMN, dentre eles podemos citar:

- Redes públicas e privadas, redes de telefonia fixa e móvel, redes privativas de voz, e redes inteligentes;
- Elementos de transmissão (multiplexadores, roteadores, switches, controladores wireless, equipamentos SDH, *cross-connects*);
- Sistemas de transmissão analógicos e digitais baseados em cabos coaxiais, fibras ópticas, rádio e enlace de satélites;
- Mainframes, controladoras remotas, servidores;
- Redes locais, metropolitanas e de longa distância (LAN, MAN e WAN);
- Redes de comutações por circuitos e pacotes;
- A própria TMN;
- Serviços de suporte e tele-serviços.

A estrutura funcional tem por objetivo subdividir funcionalmente a gerência em níveis ou camadas que restringem as atividades de cada uma delas, porém possibilitando a comunicação direta de camadas não adjacentes. A hierarquia é apresentada na Figura 2.19.

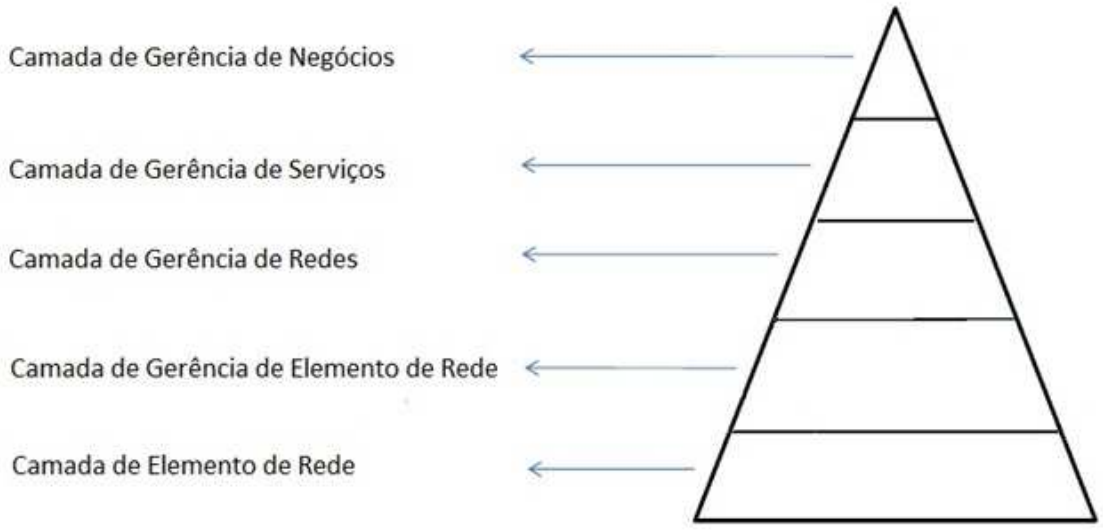


Figura 2.19 – Hierarquia de Camadas de Gerência [41][42].

A seguir, temos o detalhamento do escopo de cada camada:

- Camada de Elemento de Rede – Corresponde a entidades (software ou hardware) que necessitam efetivamente de monitoração e/ou controle. Eles devem possuir agentes que coletem informações relacionadas ao desempenho do equipamento, utilização de recursos, alarmes, dados de tráfego, e fornecê-las ao sistema de gerência;
- Camada de Gerência de Elemento de Rede – É responsável pelo gerenciamento dos elementos de rede, coordenando e controlando os mesmos, possibilitando manutenção preventiva;
- Camada de Gerência de Rede – Realiza o gerenciamento da rede suportada pela camada inferior, fornecendo uma visão geral para a operadora de telecomunicações no que se refere à conectividade e rotas;
- Camada de Gerência de Serviços – Responsável pelo relacionamento com o cliente, provisionamento de serviços, abertura e fechamento de contas, resoluções de reclamações dos clientes, inclusive relacionadas à tarifação;
- Camada de Gerência de Negócio – Responsável pela gerência do empreendimento, envolvendo todos os aspectos de prestação de serviços, possibilitando entre outras funções o gerenciamento de administração, organização e manutenção.

De forma a englobar todas as funções necessárias ao gerenciamento de uma rede de telecomunicações (planejamento, instalação, operação, manutenção e provisionamento), são identificadas cinco áreas funcionais de caráter gerencial:

- Gerência de Desempenho – responsável por avaliar e relatar o comportamento dos equipamentos de telecomunicações e a eficiência da rede;
- Gerência de Falhas – responsável por detectar, isolar e corrigir operações anormais na rede de telecomunicações;
- Gerência de Configuração – habilita o administrador a criar e/ou modificar recursos físicos e lógicos da rede de telecomunicações;
- Gerência de Contabilização – provê um conjunto de funções que possibilitam a determinação do custo associado ao uso da rede de telecomunicações;
- Gerência de Segurança – criação e controle de mecanismos e políticas de segurança.

O modelo de gerenciamento de redes de telecomunicações TMN é aplicado para padronizar a gerência de diversos tipos de redes, inclusive redes TCP/IP. Na prática, ferramentas/protocolos de gerência utilizadas hoje (IPFIX, MRTG, agentes SNMP, etc) interagem na Camada de Elemento de Rede que pertence à estrutura funcional da TMN. Assim, podemos dizer, do ponto de vista da monitoração dos serviços VoIP, que esta funcionalidade resulta nas limitações das ferramentas existentes.

2.2.3.4 – Modelo de Gerência VoIP Orientado a Bilhetes de Tarifação

Nas seções anteriores, foram apresentados e discutidos os métodos e protocolos mais utilizados atualmente na monitoração e gerência das redes de telecomunicações. Notamos que no caso do SNMP, dentro da base de informação de gerenciamento padrão MIB II (RFC 1213), ainda não existem objetos específicos capazes de tratar de forma específica o serviço VoIP. Já no IPFIX, o protocolo gera diversos tipos de estatísticas inclusive para o VoIP, porém não de forma específica. Além disso, no IPFIX grandes quantidades de pacotes devem ser coletadas para que as estatísticas sejam mais assertivas.

Acreditamos que é importante desenvolver mecanismos de gerência capazes de coletar dados específicos das chamadas VoIP e de avaliar a qualidade do serviço com base nestes dados.

Um fator que contribuiu para o avanço deste estudo é a ausência de um modelo capaz de monitorar e gerenciar o sistema telefônico VoIP a partir de características das chamadas, assim como ocorre na telefonia convencional.

Neste trabalho, propomos o aperfeiçoamento do gerenciamento de tráfego VoIP por meio da construção de *baselines* que utilizam bilhetes de tarifação gerados durante as

chamadas telefônicas IP. Em outras palavras, procuramos criar novos métodos capazes de explorar características comuns entre as chamadas realizadas na telefonia VoIP e na telefonia convencional.

Com base no método proposto, visamos traduzir o comportamento das chamadas VoIP a partir de eventos que também ocorrem na telefonia convencional, tais como: chamada completada, congestionamento de canal, discagem incorreta, entre outros.

Capítulo 3

Bilhetes de Tarifação

Toda chamada telefônica gera informações que são registradas em forma de bilhetes de tarifação. O bilhete de tarifação é responsável por armazenar estes dados, ou seja, registrar de forma detalhada todas as informações provenientes de uma ligação telefônica.

Dentro do sistema de telefonia clássica, os bilhetes de tarifação são chamados de *Call Detail Records* ou CDRs, enquanto nos sistemas de telefonia IP eles são denominados de *IP Detail Records* ou IPDRs.

Não existe uma normatização específica que regulamente a criação do CDR e/ou IPDR. Cada fabricante cria o formato do bilhete conforme lhe aprouver, desde que o bilhete possua os campos essenciais definidos pelo *Telemanagement Forum*. Logicamente, algumas informações se tornam obrigatórias, uma vez que o bilhete de tarifação deve permitir a bilhetagem das chamadas. Sendo assim, informações sobre o número de origem e destino, tempos de conversação são encontrados em todos os bilhetes, na maioria das vezes com denominações diferentes.

Outra informação importante, é que no cenário atual existem poucas publicações disponíveis sobre o tema. A escassez de trabalhos pode estar relacionada à dificuldade de acesso aos dados registrados nos bilhetes. O sigilo ocorre não somente por parte dos fabricantes de equipamentos, que concentram informações de criação e conteúdo dos bilhetes, como também por parte dos provedores, devido ao relacionamento entre estas informações e a receita da empresa.

3.1 – *IP Detail Records*

O IPDR foi discutido e padronizado pelo *Telemanagement Forum* [8][10] e representa o tíquete gerado durante uma chamada VoIP. O *Telemanagement Forum* é um fórum global sem fins lucrativo formado por mais de novecentos membros (companhias), onde sua direção é feita por um conselho formado por executivos sênior de operadoras.

Como mencionamos anteriormente, as operadoras de telecomunicações tarifam seus clientes através das informações contidas nos IPDRs. Apesar da sua utilização inicial, as informações contidas nos IPDRs também podem ser utilizadas no gerenciamento do volume de tráfego de chamadas, definição do perfil de usuário, dimensionamento do sistema e até mesmo como uma ferramenta de *debugging* [36].

A criação de um bilhete IPDR tem início após uma tentativa de chamada. A tentativa de uma chamada começa quando um usuário de um telefone disca para outro telefone e/ou serviço. A partir deste evento, mesmo que a chamada não seja atendida ou mesmo estabelecida, todas as informações relativas à chamada são armazenadas em um registro. Registro este que se transformará em um IPDR/CDR quando a chamada for finalizada.

Dentre as informações disponíveis nos IPDRs temos, tempo de duração, número de origem e destino, perfil de tarifação, ID do usuário, data/hora de ocorrência, tronco de saída utilizado, status da chamada, dentre outros. A Figura 3.1 apresenta o fluxograma completo de criação de um IPDR.

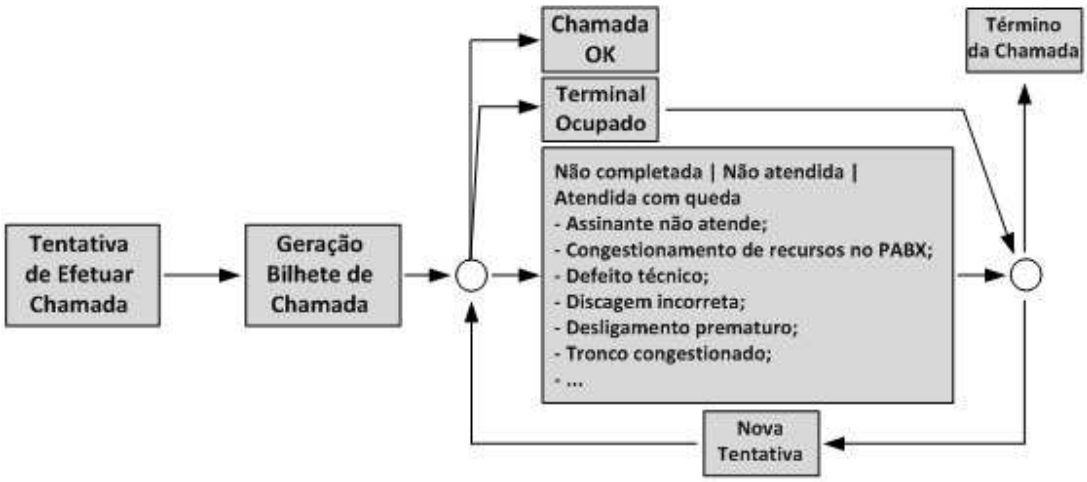


Figura 3.1 - Fluxograma completo de criação do IPDR.

O bilhete IPDR é capaz de registrar os usuários e todos os componentes envolvidos em uma chamada. Em outras palavras, o bilhete IPDR tem a função de caracterizar, de forma completa, todas as ligações telefônicas em um sistema de telefonia. Conforme

apresentado em [41], existem cinco atributos básicos que um IPDR deve conter, ou seja, ele deve ser capaz de responder os seguintes questionamentos:

- "Quem?" – Identificação dos participantes de origem e destino;
- "Quando?" – Fornecer o tempo referente ao início e fim das transações, tempo necessário para originar e completar a chamada, tempo de requisição de conexão, tempo e duração da conexão, etc. Para facilitar a troca de informação, os valores devem ser ordenados a partir do valor mais significativo conforme especificado pela norma ISO 8601;
- "Onde?" – Informar para onde a chamada foi enviada e os elementos envolvidos;
- "Por quê?" – O que aconteceu com a chamada, se ela foi completada com sucesso, se foi interrompida, se a rede estava congestionada, etc;
- "O quê?" – Informar se a ligação que está sendo feita é livre de tarifação, tarifação normal, pré-paga, etc.

A utilização da tecnologia VoIP é relativamente recente no Brasil e ainda não há uma regulamentação específica para este serviço. A normatização técnica dos serviços de voz existentes não especifica a tecnologia utilizada, mas sim o tipo de serviço a ser prestado pelos servidores. A prestação de serviços se divide em STFC (Sistema de Telefonia Fixo e Comutado), o qual possui uma regulamentação estruturada e representa o serviço público de voz, e o SCM (Serviço de Comunicação Multimídia), que possui uma regulamentação mais livre e é prestado como parte dos serviços multimídia [41].

À medida que a tecnologia VoIP ganha espaço no contexto nacional, aumenta a necessidade de estudos relacionados à gerência deste serviço em redes IP.

3.2 – Leitura dos Bilhetes IPDR

O formato dos bilhetes IPDR pode variar entre os diferentes tipos de plataformas existentes. Dentre as plataformas conhecidas, uma das mais utilizadas é a *Asterisk,* devido à sua versão gratuita disponível e por possuir código fonte aberto. Os dados dos bilhetes IPDR nesta plataforma são dispostos de maneira contínua e os valores são separados por vírgula ou CSV (*comma separated values*).

O procedimento de leitura tem início na disposição das informações de maneira ordenada, ou seja, as informações são traduzidas em um formato de tabela, onde as linhas correspondem aos bilhetes e as colunas aos valores respectivos que compõem cada um destes. Através desta organização é possível efetuar as análises sobre os dados. Na Figura 3.2 é possível visualizar uma amostra de como as informações estão no seu estado original.

```
('2008-12-02 21:14:25','\"5519170190100\" <5519170190100>',
'5519170190100','01992954307','from-internal','SIP/1301-b6a168b0','SIP/701-
0821b970','Dial','SIP/701/00171992954307|300|',18,6,'ANSWERED',3,'','','')
```

Figura 3.2 – Dados de um IPDR em seu estado original.

Na seção subsequente será apresentado o formato dos bilhetes e alguns exemplos.

3.2.1 – Formato dos Bilhetes

Na plataforma *Asterisk*, por padrão, os bilhetes IPDR possuem dezoito campos que são ordenados conforme mostra a Figura 3.3. Porém, os administradores do sistema têm a possibilidade de reordená-los e até customizá-los de forma mais conveniente [36]. A Tabela 3.1 apresenta o nome dos campos do bilhete IPDR e suas respectivas descrições.

```
<accountcode>,<src>,<dst>,<dcontext>,<clid>,<channel>,<dstchannel>,<lastapp>,
\<lastadata>,<start>,<answer>,<end>,<duration>,<billsec>,<disposition>, \
 <amaflags>[,<uniqueid>][,<userfield>]
```

Figura 3.3 – Ordenação dos campos do bilhete IPDR.

Campo	Exemplo de Valor	Descrição
Accountcode	12345	Identificação de conta. Este campo é definido pelo usuário e é vazio por padrão.
Src	12565551212	Número da identificação do chamador (número de origem). Valor configurado automaticamente.

Campo	Exemplo de Valor	Descrição
Dst	102	Extensão de destino para a chamada (número de destino). Valor configurado automaticamente.
Dcontext	Chamadas Internas	Contexto de destino para a chamada. Tipos de chamadas são atrelados a um contexto que é usado para fins de bilhetagem, roteamento da chamada, etc. Valor configurado automaticamente.
Clid	"Usuário A" <12565551212>	Identificação completa do chamador, incluindo seu nome de registro. Valor configurado automaticamente.
Channel	SIP/0004F2040808-a1bc23ef	Canal utilizado pelo telefone chamador. Valor configurado automaticamente.
Dstchannel	SIP/0004F2046969-9786b0b0	Canal utilizado pelo telefone chamado. Valor configurado automaticamente.
Lastapp	Dial	Última aplicação de plano de discagem executada. Valor configurado automaticamente.
Lastdata	SIP/0004F2046969, 30,tT	Argumentos passados para o campo "Lastapp". Valor configurado automaticamente.
Start	2010-10-26 12:00:00	Horário de início da chamada. Valor configurado automaticamente.
Answer	2010-10-26 12:00:15	Horário que a chamada obteve resposta. Valor configurado automaticamente.
End	2010-10-26 12:03:15	Horário de encerramento da chamada. Valor configurado automaticamente.
Duration	195	Valor em segundos do tempo entre o início e término da chamada. Valor configurado automaticamente.

Campo	Exemplo de Valor	Descrição
Billsec	180	Valor em segundos do tempo entre o instante que a chamada obteve resposta e seu término. Valor diretamente relacionado ao processo de cobrança. Valor configurado automaticamente.
Disposition	ANSWERED	Indica o que aconteceu com a chamada. Por padrão, pode ser *NO ANSWER, FAILED, BUSY, ANSWERED ou UNKNOWN.*
Amaflags	DOCUMENTATION	Representa um flag do tipo *Automatic Message Accounting* (AMA) que é associado com a chamada. Pode ser *OMIT, BILLING, DOCUMENTATION, or UNKNOWN.*
Userfield	PerMinuteCharge:0.02	Campo atrelado a usuários específicos que recebem tarifações particulares. Campo vazio por padrão.
Uniqueid	1288112400.1	Representa uma identificação única para o canal utilizado pelo chamador. Valor configurado automaticamente.

Tabela 3.1 – Campos do bilhete IPDR.

3.2.2 – Exemplo de Bilhetes IPDR

A seguir, serão apresentados dois exemplos de bilhetes IPDR onde os campos separados por vírgula são ordenados conforme mostrado na Figura 3.4. No primeiro exemplo, um usuário faz uma ligação para a sua caixa de mensagens de voz (*voicemail*). Podemos observar, através das informações registradas no bilhete, que o segundo e o terceiro campo representam o número de origem e o de destino, respectivamente. Portanto, é possível concluir que o número do ramal de origem é "2565551212" e o de destino corresponde à extensão "*98", número este que foi configurado no gateway de voz para verificar o recurso do *voicemail*. Na Figura 3.4 é possível visualizar o IPDR gerado nesta chamada:

"""Console"" 2565551212>","2565551212","*98","UserServices","Console/dsp","",
"VoiceMailMain","@shifteight.org","2010-08-16 01:08:44","2010-08-16 01:08:44",
"2010-08-16 01:08:53","9","9","ANSWERED","DOCUMENTATION","",
"1281935324.0","",0

Figura 3.4 – IPDR gerado no primeiro exemplo

No segundo exemplo, o usuário cujo ramal é “2565551212” realiza uma chamada SIP para o ramal de destino “101”. Através do IPDR mostrado na Figura 3.5, é possível verificar que a chamada foi iniciada as “01h16min10seg”, e atendida pelo destino as “01h16min16seg”. O campo “01h16min29seg” representa o momento em que a chamada foi encerrada. O próximo campo do bilhete cujo valor é “19” representa o tempo de duração da chamada em segundos.

"""Console"" <2565551212>","2565551212","101","LocalSets","Console/dsp",
"SIP/0000FFFF0002-00000000","Dial","SIP/0000FFFF0002","2010-08-16
01:16:10","2010-08-16 01:16:16","2010-08-16 01:16:29","19","13","ANSWERED",
"DOCUMENTATION","","1281935770.2","",2

Figura 3.5 – IPDR gerado no segundo exemplo.

3.3 – Ambiente de Desenvolvimento

Outra contribuição deste trabalho foi o desenvolvimento do aplicativo de leitura e classificação de bilhetes utilizando a linguagem VB6 [43], orientada a banco de dados na ferramenta MS-Access 2003 [44].

O MS-Access é um gerenciador de banco de dados, capaz de criar programas que controlam uma base de dados e que permitem atualizar estas informações. Suas funções pré-estabelecidas compreendem fazer consultas, emitir relatórios, fazer comparações de informações, criar e concatenar tabelas, criar índices e formulários, etc.

A especificação do equipamento utilizado na construção do ambiente inclui um computador com processador Intel Core 2 Duo E7400 2.80GHz, barramento de 1066MHz, disco rígido de 250GB, memória cachê de 3MB e sistema operacional Windows XP.

Com a disponibilidade de um ambiente específico e de conhecimentos em programação surge um cenário ideal para exploração das informações contidas nos bilhetes IPDR.

3.3.1 – Aplicativo de Leitura de Bilhetes

O aplicativo de leitura foi desenvolvido para realizar a leitura de um bilhete independente do fabricante do equipamento. Basicamente, o programa lê o arquivo original dos IPDRs extraídos em formato CSV, identifica o início e o fim de cada bilhete e os classifica. A Figura 3.6 ilustra um trecho da base de dados original contendo alguns bilhetes.

('2008-12-02 21:13:59','\"1301\" <1301>','1301','1017','from-internal','SIP/1301-b6a1a500','SIP/1017-0821b970','Dial','SIP/1017||tr',9,0,'NO ANSWER',3,"","",),('2008-12-02 21:14:25','\"5500170190100\" <5500170190100>','5519170190100','01135600954307','from-internal','SIP/1301-b6a168b0','SIP/701- 0821b970','Dial','SIP/701/00171992954307|300|',18,6,'ANSWERED',3,"","",),('2008-12-02 21:14:43','\"5519170190100\" <5519170190100>','5519170190100','01602954307','from-internal','SIP/1301-b6a168b0','SIP/701-0821b970','Dial','SIP/701/00171992954307|300|',0,0,'NO ANSWER',3,"","",)
,('2008-12-02 22:19:40','\"1301\" <1301>','1301','01590954307','from-internal','SIP/1301-b6a5cf18','SIP/701-b6a768a0','Dial','SIP/701/00171992954307|300|Tt',104,90,'ANSWERED',3,"","",),('2008-12-02 22:21:24','\"1301\" <1301>','1301','01992954307','from-internal','SIP/1301-b6a5cf18','SIP/701-b6a768a0','Dial','SIP/701/00171911154307|300|Tt',0,0,'NO ANSWER',3,"","",),('2008-12-02 23:50:43','\"5588203090100\" <55172030901...)

Figura 3.6 – Exemplo da base de dados original dos IPDRs

Após a leitura, o programa identifica e imprime cada campo de maneira organizada em uma tabela chamada de “Tabela IPDR Completa” conforme ilustra a Figura 3.7.

O primeiro campo, nomeado “N° IPDR”, contém um número sequencial que indica a ordem a ser seguida na leitura do bilhete. O campo “Dst” representa o número do destino, o qual em alguns casos foi apresentado com o valor “X”, a fim de garantir a privacidade

dos dados, uma vez que os valores originais correspondem a números da telefonia convencional provavelmente ativos.

A “Tabela IPDR Completa” original possui todos os campos apresentados na Tabela 3.1 da Seção 3.2.1. Entretanto, para que a tabela se adaptasse ao espaço disponível da página, alguns campos menos relevantes foram omitidos da Figura 3.7. Estes campos estão representados da seguinte forma: “(...)”.

Nº IPDR	Calldate	Time	Clid	Src	Dst	Dcontext	Channel	(...)	Duration	Billsec	Disposition
1	02/12/2009	21:13:59	"1301" <1301>	1301	1017	from-internal	SIP/1301-b6a1a500	...	9	0	NO ANSWER
2	02/12/2009	21:14:25	"5519170190100"	5519170190100	X	from-internal	SIP/1301-b6a168b0	...	18	6	ANSWERED
3	02/12/2009	21:14:43	"5519170190100"	5519170190100	X	from-internal	SIP/1301-b6a168b0	...	0	0	NO ANSWER
4	02/12/2009	21:23:06	"Pedreira 1116" <	1116	X	from-sip-ext	SIP/10.19.4.5-b6a0f	...	11	11	ANSWERED
5	02/12/2009	21:23:30	"Pedreira 1116" <	1116	X	from-sip-ext	SIP/10.19.4.5-b6a28	...	5	5	ANSWERED
6	02/12/2009	21:51:10	"1301" <1301>	1301	1017	from-internal	SIP/1301-b6a17f10	...	18	0	NO ANSWER
7	02/12/2009	21:52:42	"1301" <1301>	1301	X	from-internal	SIP/1301-b6a2f128	...	25	8	ANSWERED
8	02/12/2009	21:53:07	"1301" <1301>	1301	X	from-internal	SIP/1301-b6a2f128	...	0	0	NO ANSWER
9	02/12/2009	21:55:17	"1301" <1301>	1301	X	from-internal	SIP/1301-b6a17f10	...	30	19	ANSWERED
10	02/12/2009	21:55:47	"1301" <1301>	1301	X	from-internal	SIP/1301-b6a17f10	...	0	0	NO ANSWER
11	02/12/2009	22:03:14	"1301" <1301>	1301	201	from-internal	SIP/1301-b6a2f128	...	29	17	ANSWERED
12	02/12/2009	22:03:43	"1301" <1301>	1301	201	from-internal	SIP/1301-b6a2f128	...	0	0	NO ANSWER
13	02/12/2009	22:19:40	"1301" <1301>	1301	X	from-internal	SIP/1301-b6a5cf18	...	104	90	ANSWERED
14	02/12/2009	22:21:24	"1301" <1301>	1301	X	from-internal	SIP/1301-b6a5cf18	...	0	0	NO ANSWER
15	02/12/2009	22:15:32	"1116" <1116>	1116	X	from-internal	SIP/1116-b6a5b988	...	352	335	ANSWERED
16	02/12/2009	22:21:24	"1116" <1116>	1116	X	from-internal	SIP/1116-b6a5b988	...	0	0	NO ANSWER
17	02/12/2009	22:22:49	"3266" <3266>	3266	X	from-internal	SIP/1301-b6a7bda8	...	21	9	ANSWERED
18	02/12/2009	22:23:10	"3266" <3266>	3266	X	from-internal	SIP/1301-b6a7bda8	...	0	0	NO ANSWER
19	02/12/2009	22:44:20	"3266" <3266>	3266	X	from-internal	SIP/1301-082578d8	...	86	71	ANSWERED
20	02/12/2009	22:45:46	"3266" <3266>	3266	X	from-internal	SIP/1301-082578d8	...	0	0	NO ANSWER
21	02/12/2009	22:47:59	"3266" <3266>	3266	X	from-internal	SIP/1301-b6a5e4a8	...	154	135	ANSWERED
22	02/12/2009	22:50:33	"3266" <3266>	3266	X	from-internal	SIP/1301-b6a5e4a8	...	0	0	NO ANSWER
23	02/12/2009	22:57:05	"1001" <1001>	1001	1301	from-internal	SIP/1001-b6a5b988	...	46	41	ANSWERED
24	02/12/2009	22:57:51	"1001" <1001>	1001	1301	from-internal	SIP/1001-b6a5b988	...	0	0	NO ANSWER

Figura 3.7 – Tabela IPDR Completa.

Outra contribuição do trabalho que desenvolvemos é a classificação apresentada na próxima seção. Esta classificação gerou uma taxonomia para bilhetes IPDRs. Na próxima seção entraremos em mais detalhes em relação à classificação criada para os IPDRs.

3.4 – Classificação dos Bilhetes

Após a leitura e organização dos bilhetes, é necessário classificá-los. Classificar um IPDR significa descrever o que aconteceu com a chamada, ou seja, cria-se uma taxonomia para os bilhetes de tarifação. A palavra taxonomia deriva-se do idioma grego e no princípio foi utilizada como classificação de organismos vivos. Posteriormente a palavra abrangeu um contexto maior sendo aplicada a classificações diversas.

A taxonomia dos bilhetes varia de sistema para sistema, ou seja, para telefonia celular existem eventos que são diferentes da telefonia fixa e do VoIP. Como exemplo, em um sistema VoIP não é possível identificar problemas numa determinada central à frente, pois em uma rede IP os pacotes de dados podem seguir caminhos diferentes para alcançar um mesmo destino. Apesar de tudo, sempre existem eventos comuns entre diferentes sistemas, tais como: chamada completada, rede congestionada, linha ocupada, discagem incorreta, e etc.

Os IPDRs são submetidos a uma classificação, a qual é feita em função das informações contidas no bilhete e a partir de critérios pré-estabelecidos. Os critérios definem quais campos do IPDR devem estar relacionados em cada evento. Os critérios são organizados em uma tabela denominada "Tabela de Sobreposição" como mostra a Figura 3.8. Esta tabela se comporta como uma máscara que é sobreposta à "Tabela IPDR Completa", conforme exemplificada na Figura 3.7, no item anterior.

Tabela IPDR Completa

	Calldate	Time	Clid	Src	Dst	Dcontext	Channel	(...)	Duration	Billsec	Disposition
	02/12/2009	21:13:59	"1301" <1301>	1301	1017	from-internal	SIP/1301-b6a1a50(	...	9	0	NO ANSWER
	02/12/2009	21:14:25	"551917019015	5519170190100	X	from-internal	SIP/1301-b6a168b(	...	18	6	ANSWERED
	02/12/2009	21:14:43	"551917019015	5519170190100	X	from-internal	SIP/1301-b6a168b(	...	0	0	NO ANSWER
	Classificação										
	CELI-A		"1301" <1301>		1017	from-internal					ANSWERED
	02/12/2009	21:53:07	"1301" <1301>	1301	X	from-internal	SIP/1301-b6a2f128	...	0	0	NO ANSWER
	02/12/2009	21:55:17	"1301" <1301>	1301	X	from-internal	SIP/1301-b6a17f10	...	30	19	ANSWERED
	02/12/2009	21:55:47	"1301" <1301>	1301	X	from-internal	SIP/1301-b6a17f10	...	0	0	NO ANSWER
	02/12/2009	22:03:14	"1301" <1301>	1301	201	from-internal	SIP/1301-b6a2f128	...	29	17	ANSWERED
	CNEI-A		"1301" <1301>		X	from-internal	SIP/1301-b6a5cf18				NO ANSWER
	02/12/2009	22:15:32	"1116" <1116>	1116	X	from-internal	SIP/1116-b6a5b988	...	352	335	ANSWERED
	02/12/2009	22:21:24	"1116" <1116>	1116	X	from-internal	SIP/1116-b6a5b988	...	0	0	NO ANSWER
	02/12/2009	22:22:49	"3266" <3266>	3266	X	from-internal	SIP/1301-b6a7bda8	...	21	9	ANSWERED
	02/12/2009	22:23:10	"3266" <3266>	3266	X	from-internal	SIP/1301-b6a7bda8	...	0	0	NO ANSWER
	02/12/2009	22:44:20	"3266" <3266>	3266	X	from-internal	SIP/1301-082578d8	...	86	71	ANSWERED
	02/12/2009	22:45:46	"3266" <3266>	3266	X	from-internal	SIP/1301-082578d8	...	0	0	NO ANSWER
	02/12/2009	22:47:59	"3266" <3266>	3266	X	from-internal	SIP/1301-b6a5e4a8	...	154	135	ANSWERED

Tabela de Sobreposição

Figura 3.8 – Tabela de Sobreposição

O aplicativo utiliza este mecanismo para relacionar o valor dos campos em cada IPDR, e para cada combinação de relacionamento, associar a um tipo de classificação ou evento ao bilhete.

Ao classificar uma chamada há uma rotulação do bilhete correspondente, o que reflete as informações relativas ao histórico da chamada. É possível criar um grande número de eventos para classificar os bilhetes. Cada evento pode ser dividido em subeventos, os quais são subdivisões que refletem as particularidades de cada evento.

Um campo do IPDR de extrema relevância na criação da taxonomia é o campo "disposition" que se refere ao status da chamada. Este campo reflete tipicamente quatro situações:

- ANSWERED: Para chamadas que foram realizadas com sucesso;
- NO ANSWER: Quando o destino não pôde ser encontrado;
- TO: Quando o terminal remoto encontrava-se ocupado;
- FAILED: Quando ocorreu algum tipo de falha durante a geração da chamada.

O campo "disposition" é conhecido na telefonia tradicional como "final de seleção" e indica o que aconteceu com as chamadas que saíram do PABX e foram encaminhadas para frente. Pode indicar também as chamadas que entraram no PABX. Esta informação é de suma importância na classificação dos bilhetes.

Logicamente, o campo "final de seleção" não é o único a ser considerado na taxonomia dos bilhetes. A maioria dos campos possui informações importantes e devem ser considerados na criação de eventos e subeventos relativo aos IPDRs.

A Tabela 3.2 apresenta a taxonomia criada para descrever os possíveis históricos das chamadas.

Evento	Descrição
CELE	Indica as chamadas estabelecidas Local => Externa
CELI-A	Indica as chamadas estabelecidas Local => Interna (contexto de chamada A)
CELI-A1	Indica as chamadas estabelecidas localmente entre ramais
CELI-A1.1	Indica as chamadas estabelecidas localmente e foram encerradas subitamente
CELI-A1.2	Indica as chamadas estabelecidas localmente com uso de música de espera
CELI-A1.3	Indica as chamadas estabelecidas localmente com transferência de ramal
CELI-A1.4	Indica as chamadas estabelecidas localmente com geração de mensagem de voz
CNEE	Indica as chamadas externas não estabelecidas
CNEI-A	Indica as chamadas internas não estabelecidas (contexto de chamada A)
CNEI-A1	Indica as chamadas internas não estabelecidas, pois não houve resposta do destino
CNEI-A2	Indica as chamadas internas não estabelecidas devido ao tronco/circuito congestionado

Evento	Descrição
TO	Indica as chamadas que o telefone de destino está ocupado
FCE-A	Ocorrência de falha ao executar uma chamada externa (contexto de chamada A)
FCE-A1	FCE-A devido à discagem incorreta
FCE-A2	FCE-A devido a congestionamento do canal com ausência de sinal/mensagem de retorno
FCE-A3	FCE-A devido a congestionamento do canal com presença de mensagem de retorno
FCE-A4	FCE-A devido a congestionamento do canal com presença de sinal de retorno
FCE-A5	FCE-A durante a geração do IPDR
CELI-B	Indica as chamadas estabelecidas Local => Interna (contexto de chamada B)
CELI-B1	Indica as chamadas estabelecidas localmente entre ramais
CELI-B1.1	Indica as chamadas estabelecidas localmente e foram encerradas subitamente
CELI-B1.2	Indica as chamadas estabelecidas localmente com uso de música de espera
CELI-B1.3	Indica as chamadas estabelecidas localmente com transferência de ramal
CELI-B1.4	Indica as chamadas estabelecidas localmente com geração de mensagem de voz
CELI-C	Indica as chamadas estabelecidas Local => Interna (contexto de chamada C)
CELI-C1	Indica as chamadas estabelecidas localmente entre ramais
CELI-C1.1	Indica as chamadas estabelecidas localmente e foram encerradas subitamente
CELI-C1.2	Indica as chamadas estabelecidas localmente com uso de música de espera
CELI-C1.3	Indica as chamadas estabelecidas localmente com transferência de ramal
CELI-C1.4	Indica as chamadas estabelecidas localmente com geração de mensagem de voz
(...)	(...)
CELI-n	Indica as chamadas estabelecidas Local => Interna (contexto de chamada n)
CELI-n1	Indica as chamadas estabelecidas localmente entre ramais (contexto de chamada n)
CELI-n1.i	Onde i (i=1→∞) representa os subeventos do contexto de chamada n

Tabela 3.2 – Classificação dos IPDRs.

No servidor Asterisk do qual foi retirada a base de dados dos IPDRs, existem configurados cinco contextos de destino para chamadas (Dcontext). O contexto de destino serve para atrelar um grupo de chamada a um perfil, o qual é utilizado para fins de bilhetagem, roteamento, entre outros.

Para cada tipo de contexto (A, B, C, ..., n), foram criadas classificações conforme mostra a Tabela 3.2. Como os contextos podem ser criados de acordo com o interesse dos administradores, a classificação foi representada de forma genérica, onde *n* representa o contexto genérico e *i* (*i*=1→∞) seus subeventos.

A taxonomia proposta, apresentada na Tabela 3.2, tem como uma das suas maiores vantagens a apresentação de informações detalhadas sobre o que aconteceu de fato com a chamada. Por exemplo, se um usuário, por alguma razão, não foi capaz de telefonar para outro usuário, de acordo com a classificação padrão dos IPDRs, a chamada receberia o status de falha. Neste caso, o campo "disposition" estaria preenchido com o valor *FAILED*. Entretanto, existem inúmeros motivos que podem ter ocasionado o insucesso desta ligação, como por exemplo: terminal desligado, canal congestionado, falha de protocolo, etc.

Este trabalho propõe classificações específicas para cada tipo de terminação da chamada, o que vai além de uma simples chamada com *status* OK ou não. Utilizando a classificação padrão, o administrador, ao analisar o gerenciamento de um sistema VoIP, teria ciência somente do sintoma e não da causa raiz do problema. Considerando as novas terminologias propostas, foram criados subeventos os quais indicam não somente a falha em si, como também, o(s) motivo(s) que as originaram.

Uma vez classificados, os bilhetes IPDRs estão prontos para serem usados na construção dos *baselines*.

Capítulo 4

Baselines

Devido ao crescimento das demandas por serviços de telecomunicações e a existência de diferentes plataformas e variedade de protocolos, as redes de comunicação estão se tornando cada vez maiores e mais complexas. Neste cenário, confiar o gerenciamento de redes somente à habilidade e experiência de um operador humano não é a melhor alternativa. Desse modo, torna-se cada vez mais necessária a automatização do gerenciamento das redes, a fim de aperfeiçoar a utilização dos recursos, reduzir custos, e evitar indisponibilidades dos serviços.

Um modelo simples, mas fundamental, de auxílio à gerência de redes está na construção de *baselines,* os quais monitoram o comportamento normal do tráfego em um segmento [1][45]. O *baseline* também pode ser utilizado em gerenciamentos de projetos ou de sistemas em geral. Neste caso, eles operam como ferramenta que possibilita o acompanhamento de projetos permitindo compararmos o atual estado com o que foi previsto durante o planejamento inicial.

Neste trabalho, os *baselines* serão utilizados como uma ferramenta no gerenciamento do serviço VoIP. Nesta seção serão apresentados os conceitos que envolvem os *baselines*, os benefícios que eles agregam para a gerência do VoIP e o modelo adotado neste trabalho para sua criação. Este capítulo também apresenta um estudo sobre as principais ferramentas existentes para auxiliar o gerenciamento de redes.

4.1 – Definição

O *baseline* pode ser utilizado em diferentes disciplinas, como economia, medicina, matemática, topografia, gerência de redes, entre outros [46]. Basicamente, ele atua como um instrumento que estabelece o padrão de comportamento de um conjundo de dados. Depois do estabelecimento de um *baseline* inicial, toda alteração do padrão será registrada como um diferencial até o próximo *baseline* ser definido.

Segundo [1], o *baseline* de um segmento de rede pode ser definido como sendo o conjunto básico de informações que retratam o perfil do tráfego neste segmento. Estes perfis são definidos através de limiares máximos e mínimos do comportamento estatístico da rede pela unidade de tempo.

De acordo com a explicação apresentada em [47], *baseline* é o processo de estudo da rede em intervalos de tempo definidos, que tem como objetivo garantir que a rede esteja operando conforme o esperado. Com base em sua análise, além de identificar problemas recorrentes e prever o comportamento futuro da rede, o administrador pode tomar decisões precisas na escolha de critérios para geração de alarmes.

Em outras palavras, o *baseline* fornece subsídios para que o administrador de uma rede tome decisões mais assertivas. Através deste modelo é possível detectar anomalias e eventuais problemas com mais facilidade, podendo antecipar soluções, antes mesmo que o evento aconteça.

O estabelecimento ou previsão do que seria o comportamento natural do tráfego da rede, em um segmento ou em um de seus componentes, como servidores, *switches*, roteadores e gateways de voz, é uma função básica, porém fundamental, para auxiliar os gerentes de rede [48][49].

Dispor de *baselines* durante a rotina de gestão da rede auxilia o administrador a identificar limitações e controlar recursos sensíveis como o VoIP, por exemplo, que por ser uma aplicação em tempo-real, não suporta retransmissão ou congestionamentos de rede. Outra função deste aplicativo está na mensuração da utilização dos recursos, possibilitando ao administrador ter o conhecimento real da capacidade da rede, o que permite prever expansão da mesma quando houver necessidade.

Uma maneira de compreender o papel do *baseline,* apresentada em [47] é ilustrada conforme a Figura 4.1.

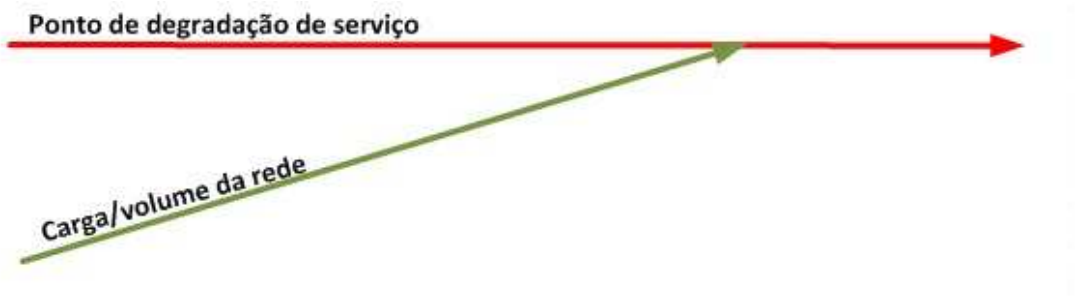


Figura 4.1 – Diagrama representativo de *baselines.*

A linha vermelha, ponto de degradação de serviço, representa a capacidade máxima suportada pelos elementos ou segmentos da rede, este valor é determinado através da especificação do fabricante com relação ao comportamento dos *hardwares* e *softwares* envolvidos. A linha verde, carga da rede, representa a progressão natural do volume de dados na rede no dia a dia. No caso de um sistema telefônico IP, representaria o volume de chamadas VoIP. Assim, o *baseline* pode ajudar a determinar os itens destacados a seguir, e com isso, contribuir para tomada de decisão de quando, onde e como investir o orçamento em melhorias na infraestrutura da rede.

- Em que ponto da linha verde a rede se encontra;
- Com qual velocidade a linha verde evolui;
- Estimar em qual instante as duas linhas se encontrarão.

Conforme mencionado em [1][47][49], o uso do *baseline* proporciona vantagens relacionadas à gerência de performance, obtidas com base no conhecimento prévio da quantidade máxima e mínima de tráfego em um segmento ao longo do dia. Sendo assim é possível estabelecer alarmes, gerando controles mais efetivos e funcionais da rede, uma vez que o critério de geração de alarme se adapta ao *baseline* que respeita as variações do tráfego ao longo do dia. O mesmo não aconteceria com a utilização de limites, os quais são programados apenas baseados na experiência do administrador de rede.

Com relação à gerência de segurança, o *baseline* pode prover também informações relacionadas à análise do comportamento de usuários. Este mecanismo é utilizado pelas operadoras de cartão de crédito e bancos para mapear o padrão/perfil de consumo dos

clientes. Muitas vezes por exemplo, os clientes são informados pelos administradores do sistema quanto ocorre uma movimentação financeira atípica em suas contas bancárias.

O perfil de utilização de usuários está diretamente relacionado ao conhecimento antecipado do volume de dados em um segmento na rede. Estas informações podem ajudar a detectar comportamentos anômalos, aspectos intrusivos colaborando com a estabilidade da rede.

4.2 – Ferramentas

Atualmente, independente do tamanho da rede, é muito comum a utilização de ferramentas que auxiliem o gerenciamento. Estas ferramentas podem ser proprietárias ou *softwares* livres. Dentre as de uso aberto é possível destacar o MRTG (*Multi Router Traffic Grapher*) [50], o NfSen (*Netflow Sensor*) [51] e o Cacti [52].

Estas ferramentas geram gráficos através de análises estatísticas geradas a partir da leitura de contadores. Estes contadores são colhidos das MIBs pertencentes aos agentes SNMP em elementos da rede. As estatísticas são calculadas com base na média dos objetos SNMP lidos ao longo de um determinado período, sobre um segmento ou objeto específico.

O MRTG consiste em um script desenvolvido em Perl, que utiliza o SNMP para leitura dos dados, e um programa em Linguagem C para geração dos gráficos que representam o comportamento do tráfego em um segmento monitorado. Esta ferramenta não se limita somente em monitorar o tráfego, como também permite monitorar qualquer variável SNMP.

Como o MRTG guarda o histórico dos dados de maneira consolidada, além de analisar o dia corrente, ele permite gerar gráficos retroativos em escalas semanais, mensais e até anuais. Os gráficos no MRTG são visualizados via web, como pode ser observado na Figura 4.2.

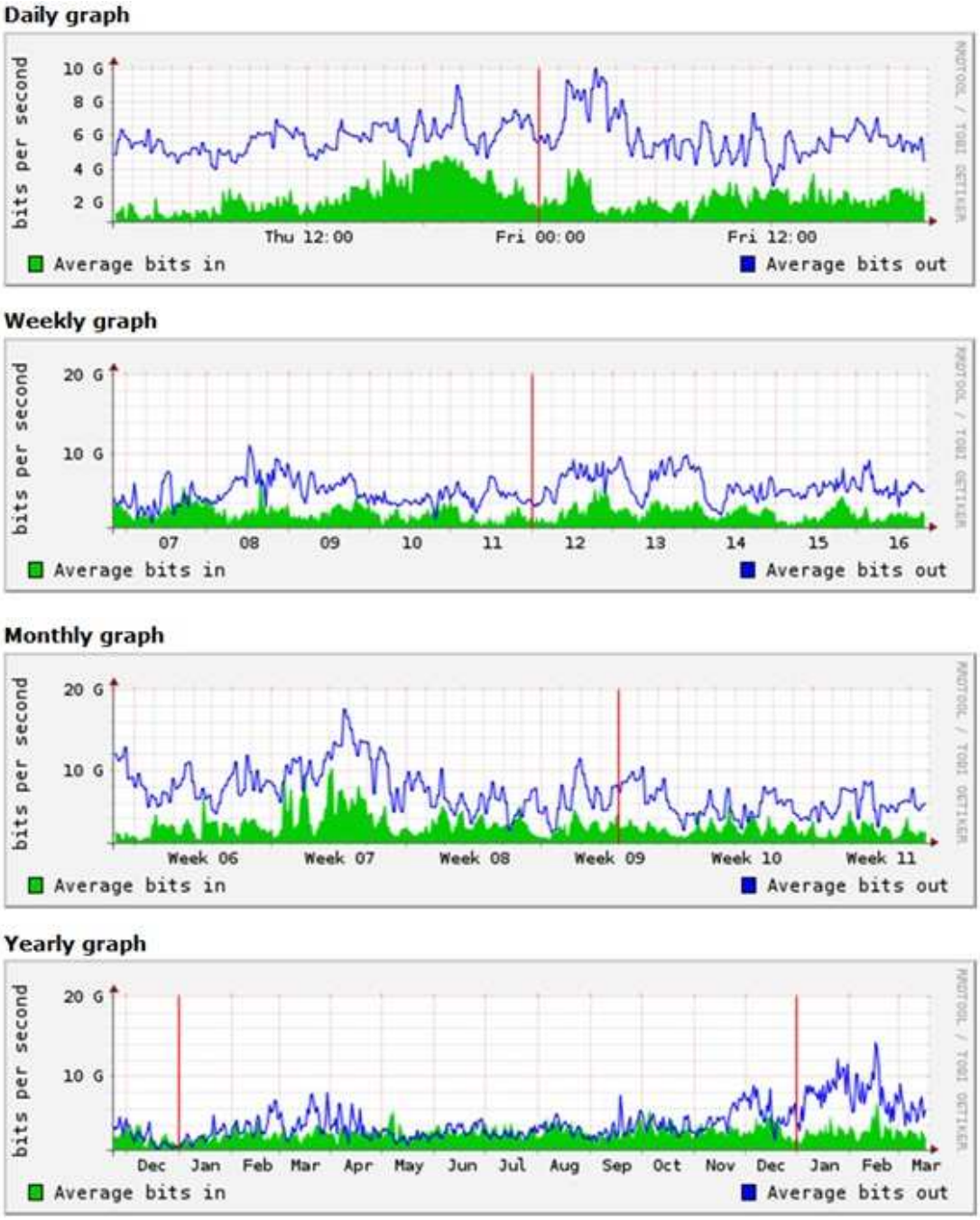


Figura 4.2 – Análise diária, semanal, mensal e anual MRTG [50].

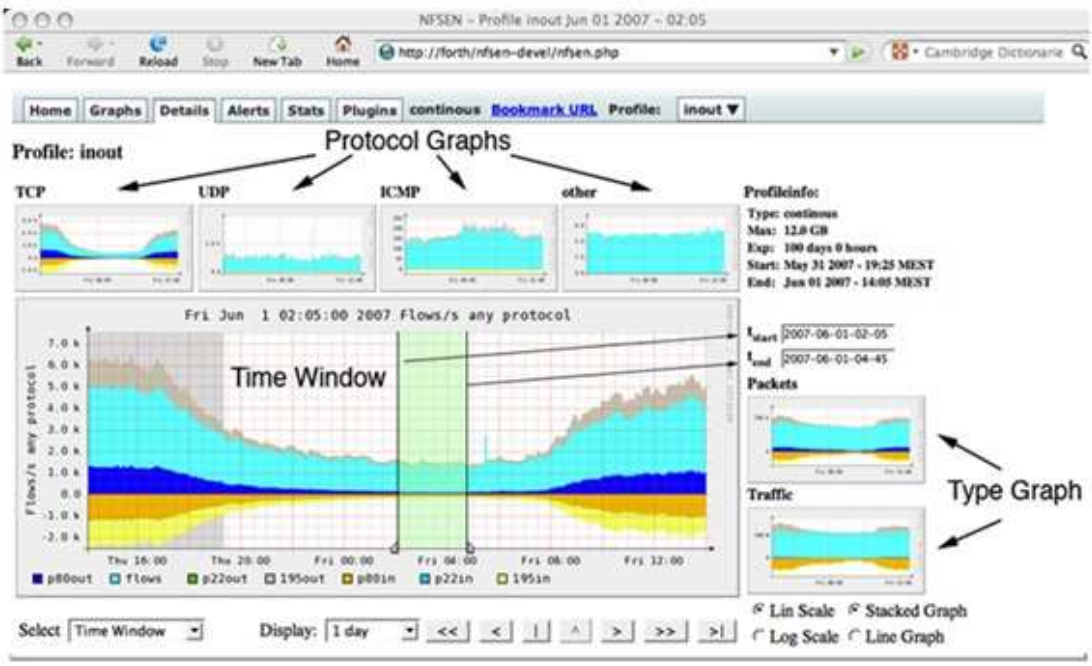
O NfSen é uma aplicação gráfica baseada em web, que retrata de maneira visual os dados coletados via ferramenta *nfdump* [51]. O *nfdump* é uma ferramenta que coleta e processa os dados gerados pela ferramenta NetFlow (antecessora ao IPFIX). Como características do NfSen, podemos destacar:

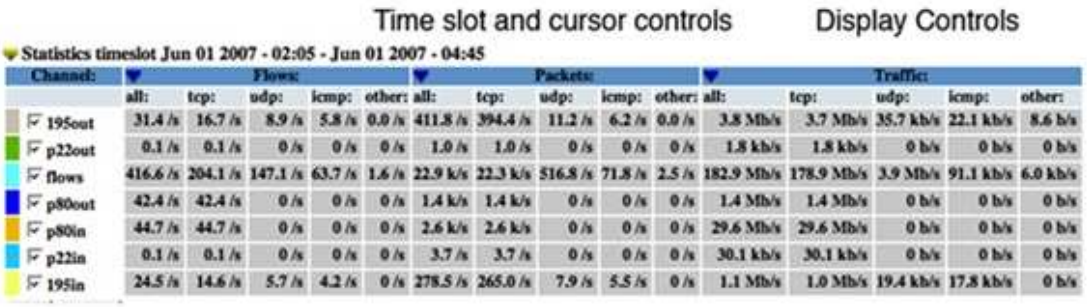
- Exibe os dados do NetFlow: Fluxo de dados, pacotes, protocolos, etc;
- Fácil navegação através dos dados do NetFlow;
- Processa o dados do NetFlow dentro de um intervalo de tempo especificado;
- Criação de perfis contínuos;
- Define alertas com base em várias condições.

Em linhas gerais, o NfSen se destaca pela sua navegabilidade e pelos serviços oferecidos, tais como: criação de filtros nomeados, verificação direta do responsável pelo endereço IP, criação de perfis de gerenciamento e geração de alertas em casos de comportamento anormal.

Para geração dos alertas, primeiramente é definido um filtro. As condições para geração do alerta são baseadas no número total de pacotes/bytes resultantes desse filtro. A quantidade total de pacotes/bytes pode ser comparada ao valor absoluto ou à média de valores em um período de tempo. Quando a condição é violada, uma ação pode ser executada. Nesta ferramenta, a ação mais utilizada é o envio de um email reportando o tipo ou código da violação.

A Figura 4.3 apresenta a interface do NfSen.





Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
195out	31.4 /s	16.7 /s	8.9 /s	5.8 /s	0.0 /s	411.8 /s	394.4 /s	11.2 /s	6.2 /s	0.0 /s	3.8 Mb/s	3.7 Mb/s	35.7 kb/s	22.1 kb/s	8.6 b/s
p22out	0.1 /s	0.1 /s	0 /s	0 /s	0 /s	1.0 /s	1.0 /s	0 /s	0 /s	0 /s	1.8 kb/s	1.8 kb/s	0 b/s	0 b/s	0 b/s
flows	416.6 /s	204.1 /s	147.1 /s	63.7 /s	1.6 /s	22.9 k/s	22.3 k/s	516.8 /s	71.8 /s	2.5 /s	182.9 Mb/s	178.9 Mb/s	3.9 Mb/s	91.1 kb/s	6.0 kb/s
p80out	42.4 /s	42.4 /s	0 /s	0 /s	0 /s	1.4 k/s	1.4 k/s	0 /s	0 /s	0 /s	1.4 Mb/s	1.4 Mb/s	0 b/s	0 b/s	0 b/s
p80in	44.7 /s	44.7 /s	0 /s	0 /s	0 /s	2.6 k/s	2.6 k/s	0 /s	0 /s	0 /s	29.6 Mb/s	29.6 Mb/s	0 b/s	0 b/s	0 b/s
p22in	0.1 /s	0.1 /s	0 /s	0 /s	0 /s	3.7 /s	3.7 /s	0 /s	0 /s	0 /s	30.1 kb/s	30.1 kb/s	0 b/s	0 b/s	0 b/s
195in	24.5 /s	14.6 /s	5.7 /s	4.2 /s	0 /s	278.5 /s	265.0 /s	7.9 /s	5.5 /s	0 /s	1.1 Mb/s	1.0 Mb/s	19.4 kb/s	17.8 kb/s	0 b/s

Figura 4.3 – Interface de gerência NfSen [51].

O Cacti é uma solução gráfica completa que foi projetada para aproveitar o poder de armazenamento de dados e as funcionalidades gráficas da ferramenta RRDT (*Round Robin Database Tool*) [51]. A ferramenta RRD ou base de dados *round-robin* foi desenvolvida para armazenar séries de dados de qualquer tipo, tais como temperatura, CPU, quantidade de bytes, e pode ser integrada com diversas linguagens de programação.

Neste caso, os dados são armazenados em uma base MySQL via RRDT e a manipulação e criação dos gráficos fica sob responsabilidade do Cacti. Outra característica desta ferramenta é que ela suporta o SNMP, podendo ser usada para a criação de gráficos, assim como no MRTG.

A Figura 4.4 demonstra um modelo de gráfico gerado pelo Cacti.

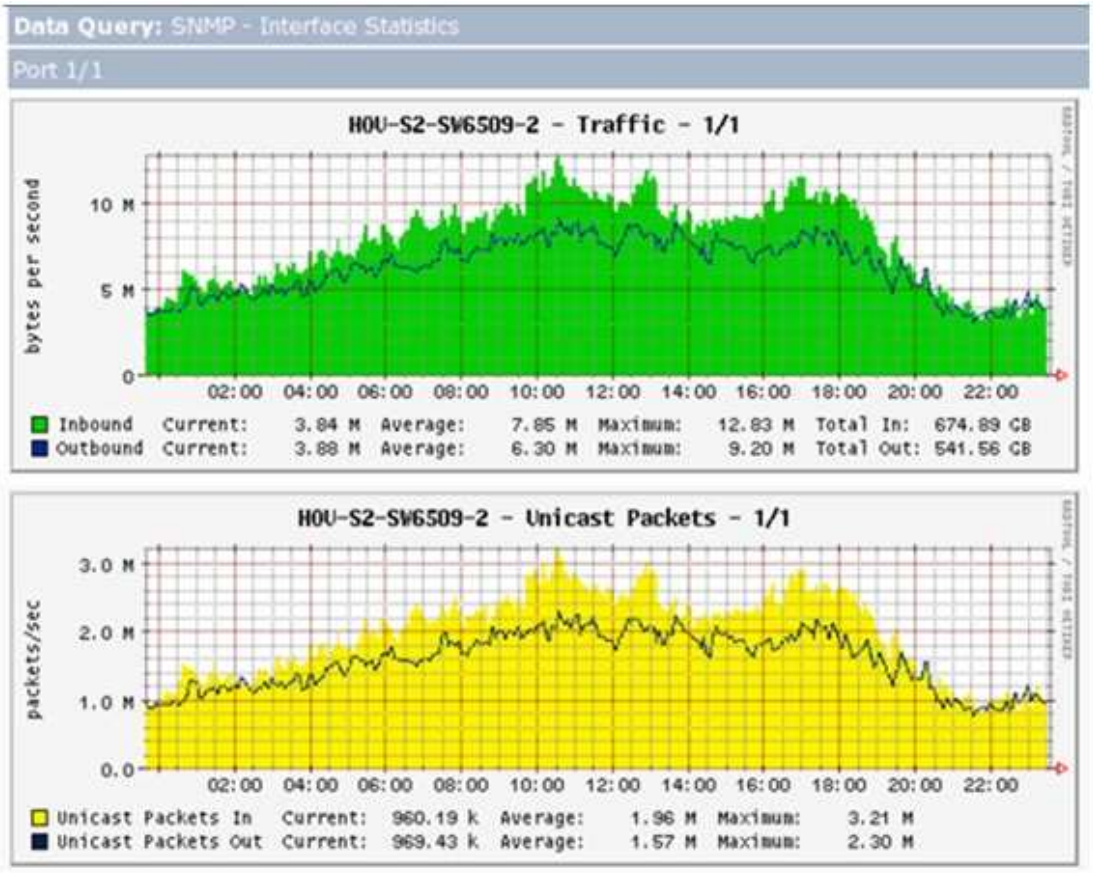


Figura 4.4 – Interface de gerência Cacti [52].

Comparando as funcionalidades de cada ferramenta, constata-se que elas são muito parecidas do ponto de vista da geração dos gráficos, pois nos três casos, os gráficos são gerados com análises estatísticas baseadas em médias por período de tempo. Outra semelhança é que nos três casos, a forma de monitoração independe do tipo de serviço. Ou seja, o tráfego VoIP, por exemplo, é gerenciado da mesma maneira que os outros tipos de tráfego.

Por ser gerada a partir de médias, a utilização destas ferramentas causa limitações ao administrador durante a detecção e solução de problemas, uma vez que sua interpretação correta depende do conhecimento empírico adquirido pelo administrador no dia a dia do seu trabalho [1]. Isto se torna um agravante do ponto de vista de qualidade da monitoração, pois em [49], os autores já afirmavam que quanto maior a quantidade de segmentos, maior a complexidade no processo de administração da rede, considerando a grande quantidade de gráficos a serem analisados.

Verifica-se nas Figuras 4.2 a 4.4 que os gráficos demonstram informações sobre o volume médio de tráfego que entra e sai de um elemento. Esta informação sozinha não fornece um recurso adicional que possa ser utilizado como fundamento na tomada de decisão, frente a problemas que possam estar ocorrendo ou já tenham ocorrido. Neste caso, o uso de *baselines* pode proporcionar um benefício, justamente por fornecer uma estimativa do que seria o comportamento natural do objeto ou segmento analisado.

A Seção 4.3 demonstra que o uso de *baseline* complementa a análise de dados de monitoração e serve de fundamento para a análise dos resultados.

4.3 – Exemplos de *Baselines*

Proença Junior [1] apresentou um modelo de *baseline* chamado *Baseline* GBA (BLGBA) com o objetivo de prever a expectativa do tráfego e de outras variáveis que compusessem seu perfil básico, de acordo com padrões requeridos pelo administrador da rede. O desenvolvimento do modelo BLGBA foi realizado com o uso da ferramenta GBA (Gerenciamento Automático de *Backbone*) que utiliza o protocolo SNMP.

Os *baselines* foram gerados a partir da análise de alguns segmentos específicos da rede. Proença Junior estabeleceu *baselines* através de dados históricos de doze semanas que foram coletados das MIBs pertencentes aos agentes SNMP residentes em equipamentos principalmente da rede da Universidade Estadual de Londrina (UEL). Neste trabalho, o autor criou dois formatos de *baseline*, *bl-7* e *bl-3*. O *bl-7 gera* sete arquivos, um para cada dia da semana, e o *bl-3 gera* três arquivos, um para os dias da semana e um para o sábado e outro para o domingo.

A Figura 4.5 demonstra exemplos de *baselines* apresentados em [1] para os dias 08 e 09 de abril de 2005. A parte verde (movimento real) representa a leitura dos bits de entrada e a linha azul representa o *baseline* gerado para o modelo *bl-3*. A parte vermelha representa uma situação de alarme definida pelo autor.

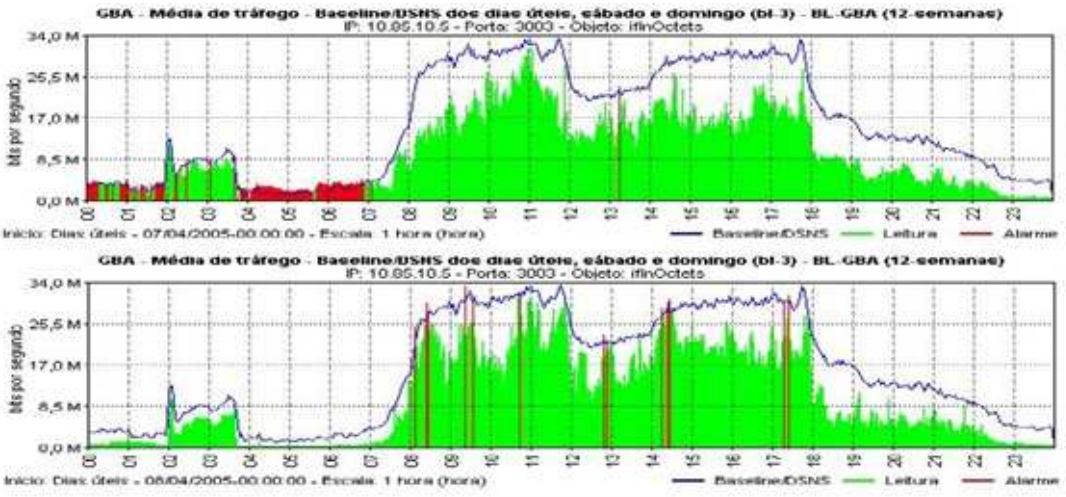


Figura 4.5 – BLGBA (bl-3).

A Figura 4.6 ilustra *baselines* apresentados em [1] para os dias 08 e 09 de abril de 2005 no modelo *bl-7*.

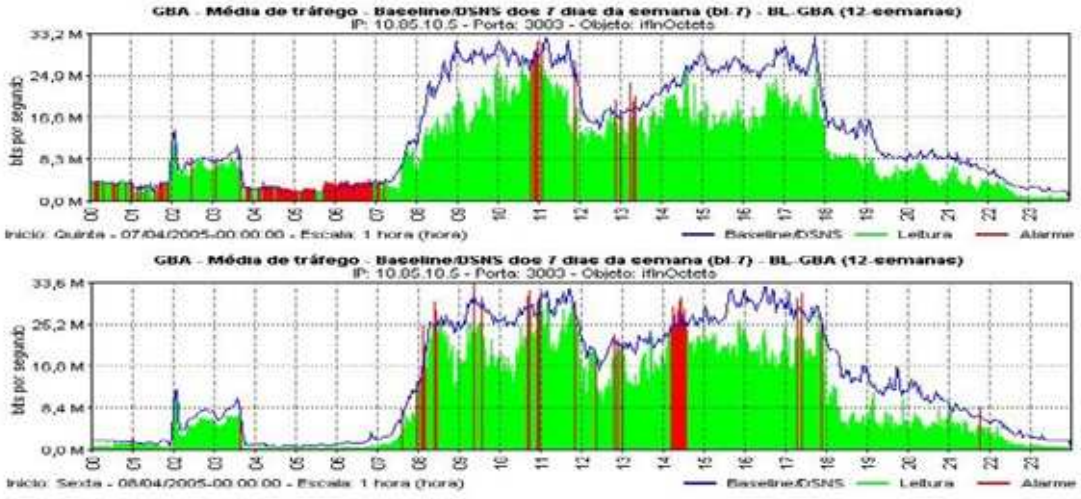


Figura 4.6 – BLGBA (bl-7).

Zarpelão [53] propôs um modelo de detecção de anomalias em redes de computadores baseado em três níveis de análise. O comportamento dinâmico do tráfego de rede foi uma das dificuldades em seu trabalho. Logo, foi necessário ter o domínio do padrão de operação da rede para que fosse possível gerar conclusões em relação a sua saúde em caso de anomalia. Para isso, o autor utilizou o modelo BLGBA proposto por Proença Junior [1] para caracterizar o tráfego e gerar *baselines*. Neste caso, se ao invés de utilizar

um modelo baseado em *baseline*, o sistema de detecção de anomalias fosse baseado no resultado de uma das ferramentas apresentadas na seção anterior, os resultados poderiam não ser coerentes com o comportamento natural da rede.

4.4 – Elaboração dos *Baselines*

Conforme descrito anteriormente, este trabalho propõe a construção de *baselines* relativos às chamadas VoIP, utilizando o conteúdo dos IPDRs gerados dentro de uma rede metropolitana. A Figura 4.7 representa o processo de geração dos *baselines* nas MANs.

O início se dá quando um usuário faz uma tentativa de realizar uma chamada VoIP. Esta chamada é processada e em seguida um IPDR é gerado. O IPDR por sua vez é armazenado em uma base de dados. Os bilhetes são então extraídos, organizados e classificados em função da taxonomia proposta. Uma vez que os bilhetes estão classificados, eles podem ser utilizados para criar os *baselines*.

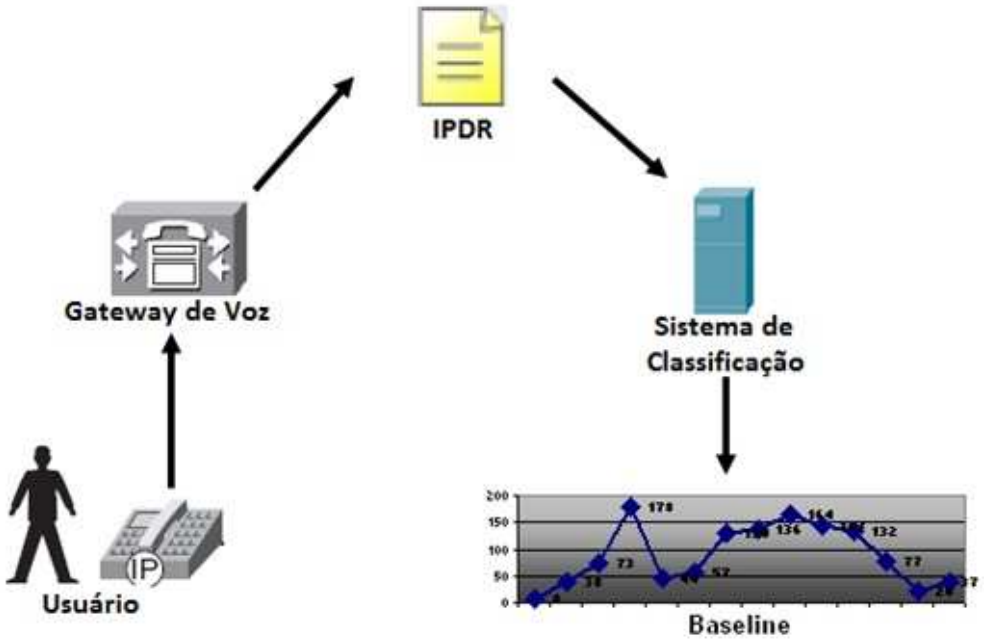


Figura 4.7 – Modelo de criação dos *baselines.*

Para a elaboração dos *baselines,* são necessários alguns passos. No primeiro passo, os IPDRs são coletados no PABX VoIP. Logo após, eles são organizados num relatório mensal. A organização é realizada pelo aplicativo de leitura que gera a Tabela IPDR Completa, conforme apresentada no terceiro capítulo.

A segunda etapa envolve a geração de relatórios estatísticos. Esta tarefa é desempenhada pelo sistema de classificação, o qual analisa, classifica cada IPDR, e gera estatísticas das chamadas. Durante a classificação, cada chamada é associada a um evento específico, onde os eventos servirão para a geração das estatísticas.

O último estágio é responsável pela construção dos *baselines* e também é realizado pelo sistema de classificação. Neste passo, os eventos são contabilizados, e, para cada um deles, um *baseline* é gerado. A geração dos baselines em si é feita a partir da média aritmética da quantidade de cada evento em cada horário do dia.

Dessa maneira é possível obter, por exemplo, informações como o número de chamadas internas estabelecidas com sucesso a cada hora, ou o número de chamadas externas realizadas durante o mês que utilizaram o tronco de uma operadora específica. Além disso, os baselines podem refletir os diversos comportamentos da rede, tais como: congestionamento, chamadas completadas, transferências, chamadas ocupadas, falhas diversas em diversos recursos físicos (ramais, troncos, centrais PABX, gateways, etc), ramais inoperantes, erros de discagem, falhas de sinalização, dentre outros.

A elaboração dos *baselines* com base nos IPDRs pode ser feita de acordo com o interesse do administrador da rede. No processo de criação dos *baselines,* três tipos de informações podem ser utilizadas, são elas: os eventos, o momento e os dispositivos da rede.

- Eventos (classificação): CELI-A1, CELI-A1.1, CELI-A1.2, CELI-A1.3, CELI-A1.4, CELI-B1, CELI-B1.1, CELI-B1.2, CELI-B1.3, CELI-B1.4, CELI-C1, CELI-C1.1, CELI-C1.2, CELI-C1.3, CELI-C1.4, CELI-D1, CELI-D1.1, CELI-D1.2, CELI-D1.3, CELI-D1.4, CELI-D1.5, CELI-D1.6, CELI-E1, CELI-E1.1, CELI-E1.2, CELI-E1.3, CELI-E1.4, CNEI-A1, CNEI-A2, CNEI-B1, TO, FCE-A1, FCE-A2, FCE-A3, FCE-A4, FCE-A5, FCI-A1, FCI-A2, FCI-A3, FCI-A4 e FCI-A5;

- Momento: segundo, segundos, minuto, minutos, hora, horas, dia, dias, mês, meses, ano, anos, ano bissexto, etc;
- Dispositivo: telefone IP, telefone convencional com adaptador ATA, computador, softfone, terminais móveis, gateways, etc.

A Figura 4.8 retrata a granularidade existente no processo de elaboração dos *baselines*.

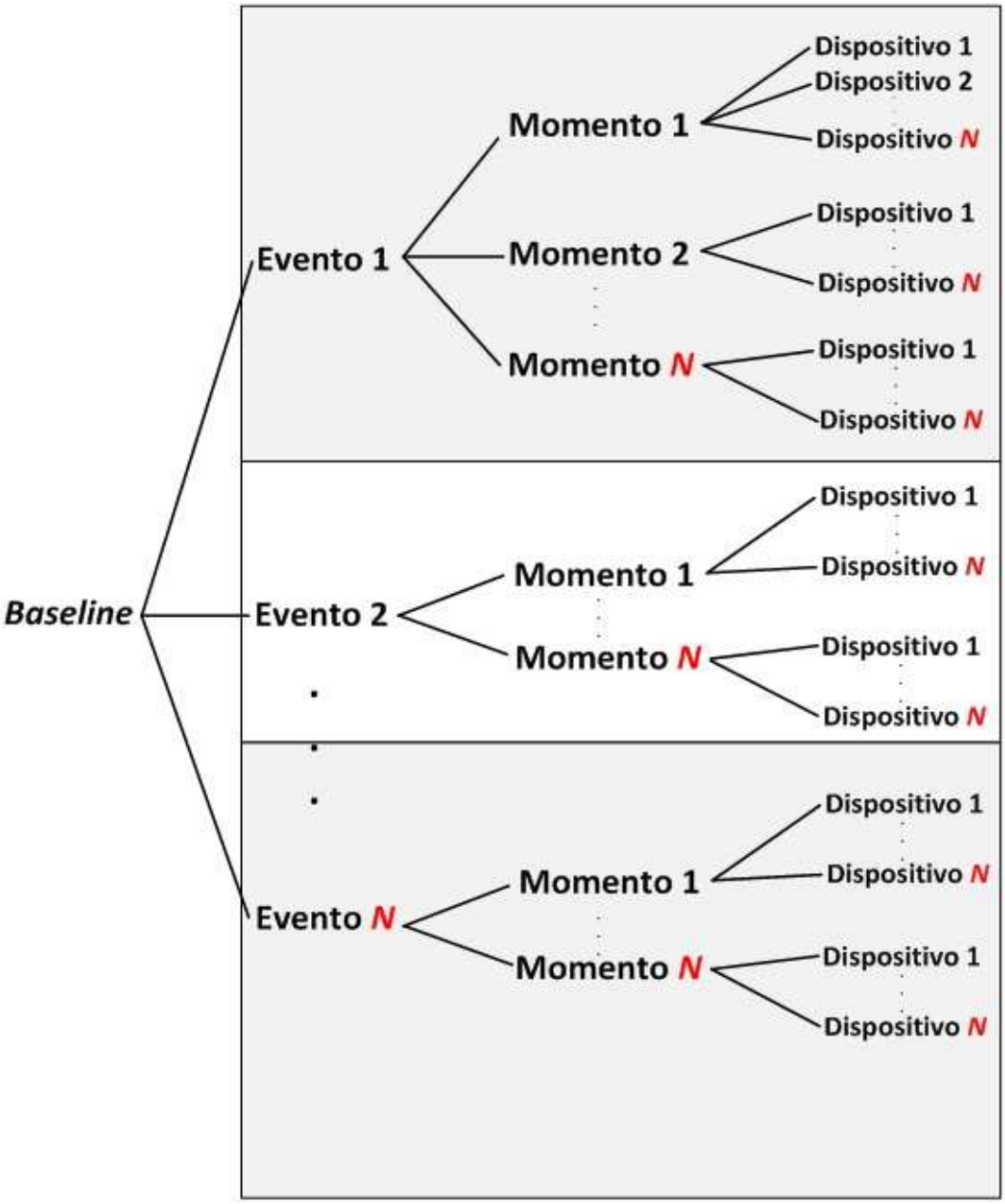


Figura 4.8 – Elaboração dos *baselines*.

Para a criação dos baselines, o sistema que classifica e organiza as chamadas gera uma matriz *H* com dimensões *N*x*M*, onde *N*=24 representa o número de horas no dia e *M* representa o número de dias analisado. Em cada linha da matriz é possível obter a estatística dos eventos ocorrentes em um horário específico para cada dia, já as colunas representam as estatísticas diária deste evento. A matriz é definida em (1).

$$H = \begin{pmatrix} h_{1,1} & \cdots & h_{1,M} \\ \vdots & \vdots & \vdots \\ h_{N,1} & \cdots & h_{N,M} \end{pmatrix} \quad (1)$$

O baseline é representado conforme a matriz *B* com as dimensões *N*x1, como é definido em (2).

$$B = \begin{pmatrix} b_{1,1} \\ \vdots \\ b_{N,1} \end{pmatrix} \quad (2)$$

O valor do elemento $b_{x,1}$ é calculado através da média aritmética da linha *H* de acordo com (3).

$$b_{x,1} = \frac{1}{m} \sum_{i=1}^{m} h_{x,i} \quad (3)$$

A metodologia de criação de *baselines* apresentada será utilizada no estudo de caso comentado no próximo capítulo.

Capítulo 5

Estudo de caso desenvolvido

Neste capítulo, apresentamos um estudo de caso aplicado à cidade de Pedreira. Pedreira é um município do estado de São Paulo situado a 33 quilômetros da cidade de Campinas e 130 quilômetros da capital. De acordo com o Censo Demográfico do IBGE de 2010, a população total do município é de 41.549 habitantes. Além do forte comércio de cerâmica e porcelana, o município se destaca por possuir uma rede metropolitana de acesso aberto [54].

O projeto de criação da Rede Metropolitana de Acesso Aberto de Pedreira é resultado da parceria entre o LaRCom-Unicamp (Laboratório de Redes de Comunicações) e a prefeitura da cidade. Os estudos para a implantação da rede iniciaram-se em 2005 e sua inauguração se deu em junho de 2007. Atualmente, a RMAA de Pedreira é uma rede híbrida, formada por conexões de fibra óptica e enlaces de rádio. O intuito inicial de sua construção foi interligar diversos pontos (secretarias, prefeitura, escolas e hospitais) tanto no centro quanto em regiões mais afastadas da cidade. Os serviços atualmente disponibilizados e que trafegam na RMAA são: acesso à Internet, voz sobre IP (VoIP), dados, email e câmeras IP de segurança pública. A Figura 5.1 ilustra a RMAA de Pedreira.

De acordo com a Figura 5.1, o *backbone* da rede (representado em vermelho) é composto por ramos de fibra óptica com capacidade 1Gbps que abordam os principais pontos da administração pública municipal. Os pontos mais afastados se interligam a infraestrutura do *backbone* através de enlaces de rádio (representados em laranja) utilizando a frequência de 5,8GHz. Outro componente importante de RMAA de Pedreira são as células de acesso. As células de acesso são redes sem fio que utilizam frequência de 2,4GHz, cuja principal função é conectar os usuários da RMAA.

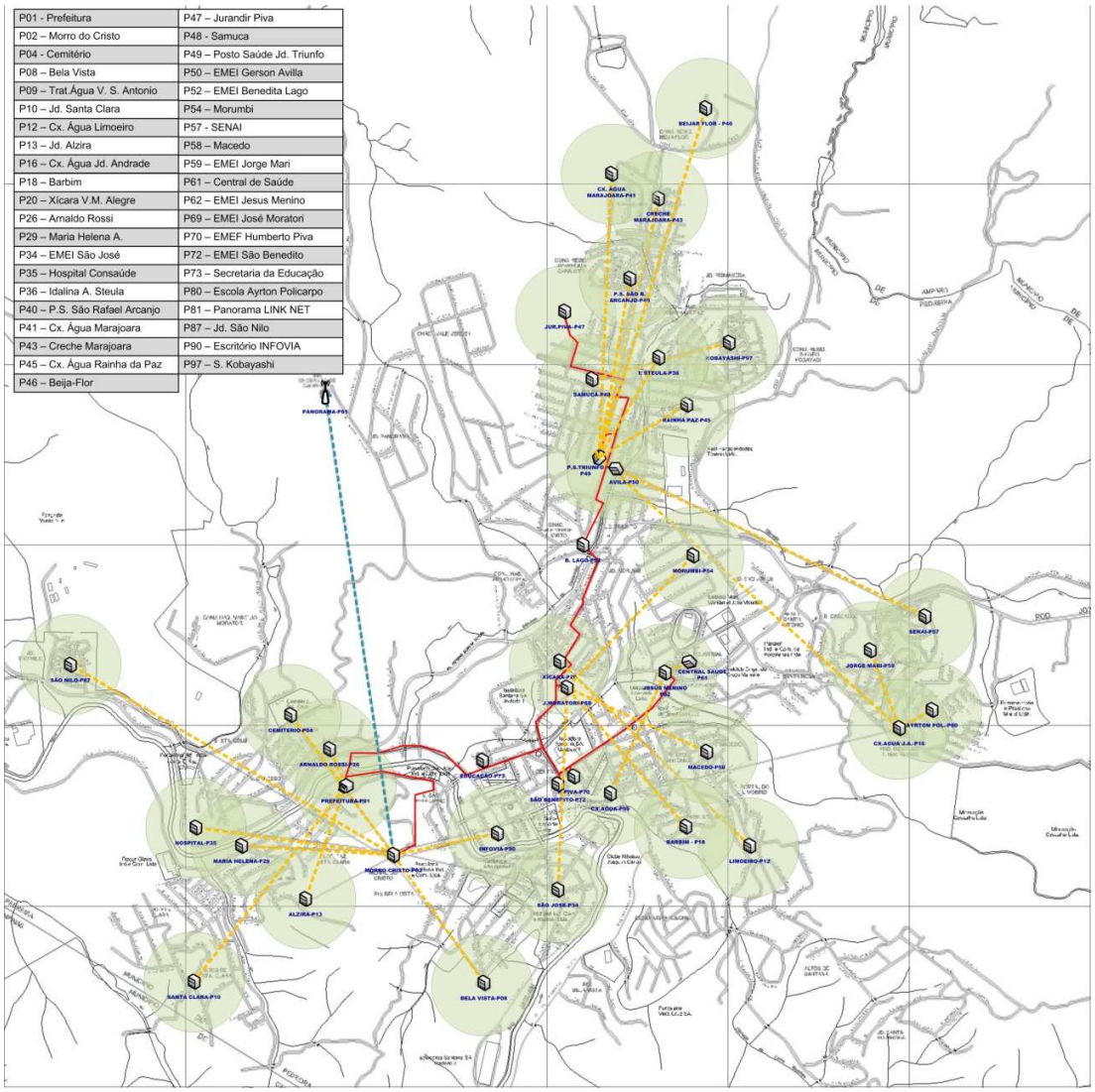


Figura 5.1 – RMAA de Pedreira.

Um dos serviços disponibilizados na RMAA de Pedreira é a telefonia VoIP corporativa. Conforme dito anteriormente, o principal objetivo da implementação do sistema VoIP nas RMAAs é a redução do custo nas ligações, uma vez que o tráfego de voz é transportado sobre a rede de dados já existente.

A Prefeitura Municipal de Pedreira adotou a tecnologia VoIP para interligar os prédios públicos. A configuração da rede de Telefonia IP da prefeitura segue a estrutura mostrada na Figura 5.2. Os componentes apresentados na Figura 5.2 foram explicados no segundo capítulo deste trabalho.

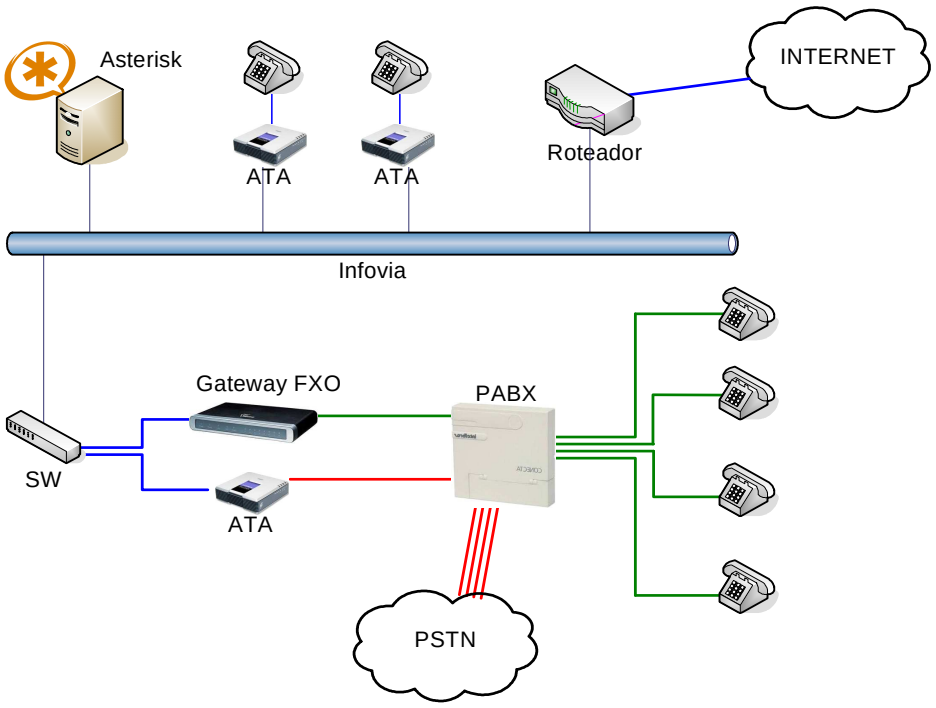


Figura 5.2 - Estrutura VoIP para Pedreira.

5.1 – Modelo de Criação do *Baseline*

A necessidade de aprimorar a qualidade de serviço, a possibilidade do desenvolvimento de novos métodos de gerência do VoIP e a disponibilidade da base de dados de bilhetes de tarifação gerados na RMAA de Pedreira, foram os fatores motivadores deste estudo de caso.

A base de dados dos IPDRs utilizada para a geração dos *baselines* é relativa às chamadas realizadas entre agosto e dezembro de 2009.

O modelo proposto neste trabalho foi utilizado para efetuar análises estatísticas sobre os valores coletados da base de dados IPDR de Pedreira, respeitando as informações exatas de cada bilhete, segundo a segundo, durante todo o dia. A ideia principal é que o *baseline* deverá preservar as características do tráfego de chamadas VoIP, levando em conta as variações temporais ao longo do dia.

Pelo fato de não haver expediente regular nos finais de semana em Pedreira, considerou-se a criação de três tipos de *baselines*. O primeiro é chamado de ***Bl-1*** e considera a média aritmética dos IPDRs gerados nos dias úteis de uma semana. O segundo é chamado de ***Bl-4*** e considera a média aritmética dos IPDRs gerados nos dias úteis de

quatro semanas. Por fim no terceiro, chamado ***Bl-8*****,** a média aritmética é calculada com base nos bilhetes gerados nos dias úteis em oito semanas. Os três tipos de *baselines* adotaram como horário de coleta entre 09:00 de 17:00 horas.

A opção em não considerar os finais de semana e horários fora do expediente de trabalho na geração de *baselines*, foi realizada com a intenção de minimizar a margem de erro no resultado final apresentado. Proença Junior [1] havia chegado a essa mesma conclusão, comprovando que a discrepância entre o tráfego gerado em um dia útil e os finais de semana tende a ser muito significativa. No caso da Rede Metropolitana de Acesso Aberto de Pedreira, a diferença chega a ser muito grande, conforme pode ser observado nas Figuras 5.3 e 5.4. Neste caso, foi analisado o comportamento médio das chamadas efetuadas entre 03 de agosto a 28 de setembro de 2009.

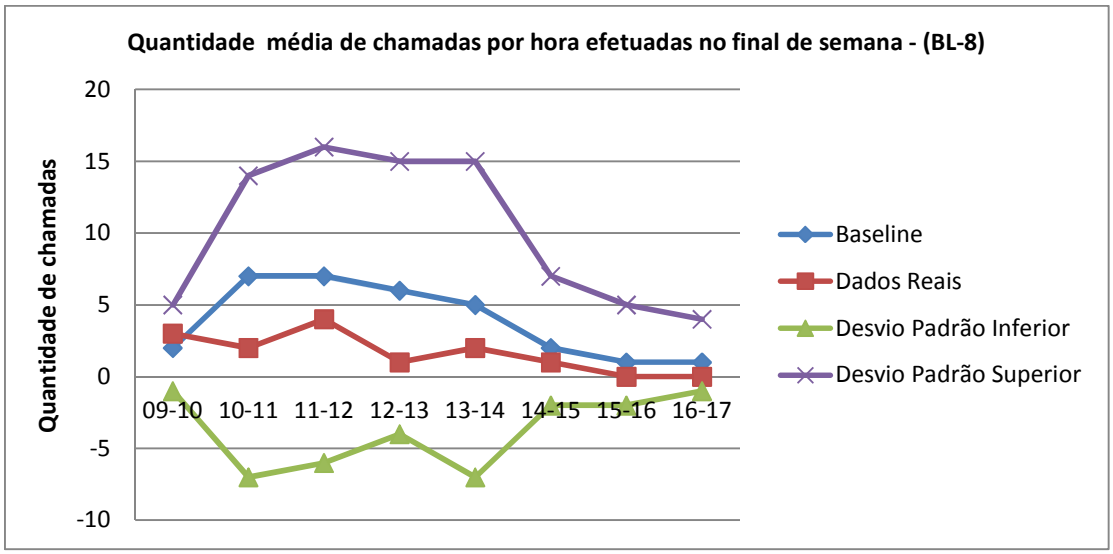


Figura 5.3 – Quantidade média de chamadas por hora no final de semana.

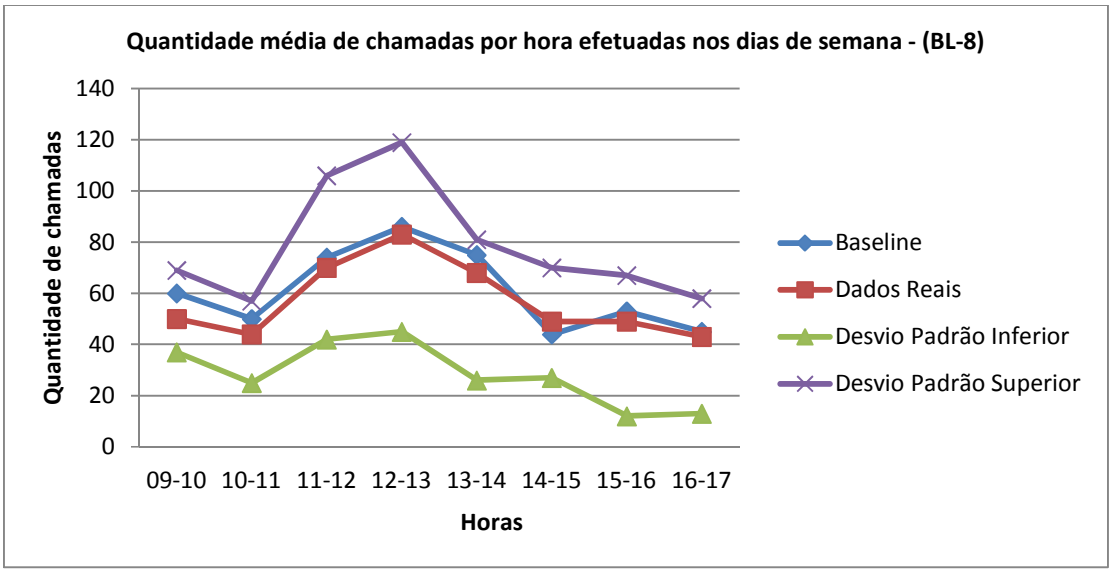


Figura 5.4 – Quantidade média de chamadas por hora nos dias de semana.

Para a definição do algoritmo de cálculo do *baseline* foi adotada a média aritmética dos dados coletados. Poderíamos ter escolhido outros modelos estatísticos como moda, mediana, porém optamos pela média por ser a mais utilizada em nosso dia-a-dia e por acreditarmos que seria um modelo relevante ao nosso experimento. No entanto não foram feitos testes analíticos com outros modelos.

Além do *Baseline*, todos gráficos apresentam outras três curvas: Dados Reais, Desvio Padrão Inferior e Desvio Padrão Superior. A curva "Dados Reais" informa a quantidade de eventos ocorridos efetivamente durante o dia. Ela indica o volume de chamadas diárias correspondente a uma determinada classificação ou evento.

Para obter os dados que compõem as curvas "Desvio Padrão Inferior e Superior", primeiramente foi preciso calcular o desvio padrão $s_{x,1}$ para cada $b_{x,1}$ calculado em (3). Desta forma, para cada matriz B, teremos uma matriz S com dimensões $Nx1$, conforme apresentado em (4), com os desvios padrões calculados de acordo com (5):

$$S = \begin{pmatrix} s_{1,1} \\ \vdots \\ s_{N,1} \end{pmatrix} \tag{4}$$

$$s_{x,1} = \sqrt{\frac{1}{M-1}} \sum_{i=1}^{M} (h_{x,i} - b_{x,1})^2 \tag{5}$$

Após criar a matriz *S*, podemos utilizá-la para criar matrizes *U* e *L*, que contém o desvio padrão superior e o desvio padrão inferior, respectivamente, conforme em (6) e (7). As duas matrizes tem dimensões *Nx1*. Os elementos destas matrizes são calculados conforme apresentado em (8) e (9), onde *w* é um peso determinado pelo administrador da rede para alterar a sensibilidade do mecanismo de geração de alarmes.

$$U = \begin{pmatrix} u_{1,1} \\ \vdots \\ u_{N,1} \end{pmatrix} \tag{6}$$

$$L = \begin{pmatrix} l_{1,1} \\ \vdots \\ l_{N,1} \end{pmatrix} \tag{7}$$

$$u_{x,1} = b_{x,1} + w.s_{x,1} \tag{8}$$

$$l_{x,1} = b_{x,1} - w.s_{x,1} \tag{9}$$

Assim, quando o dado real for maior que $u_{x,1}$ ou menor que $l_{x,1}$, um desvio de comportamento será caracterizado.

5.2 – Desvio de Comportamento

Poder comparar o comportamento do tráfego real com seu *baseline* traz a possibilidade de interpretar melhor o perfil do tráfego VoIP e identificar anormalidades em seu comportamento natural.

Segundo Zarpelão [53], anomalias em redes de computadores são desvios súbitos e acentuados que ocorreram no tráfego em consequência de diversas situações como defeitos em softwares, uso abusivo de recursos da rede, falhas em equipamentos, erros de configurações e ataques.

Através dos diversos testes analíticos executados neste trabalho, podemos notar desvios no comportamento do tráfego VoIP de Pedreira. Um desvio de comportamento é detectado quando o valor do tráfego real ultrapassa o limiar inferior e/ou superior do

gráfico. Ou seja, a curva "Dados Reais" excede o delimitado pela curva "Desvio Padrão Inferior" e/ou "Desvio Padrão Superior".

Dependendo do tipo do evento e do dia analisado, a quantidade de desvios de comportamento pode variar. Um desvio no comportamento de um determinado evento nem sempre significa um problema na rede. Em outras palavras, nem sempre um alarme deve ser enviado ao administrador da rede.

Em cada evento analisado, informações como quantidade de desvios no mês, média de desvios por dia, tempo médio entre os desvios e o volume de desvios por faixa de horário puderam ser contabilizadas. Estas informações foram consolidadas em tabelas e serão apresentadas em conjunto com os *baselines*.

5.3 – Resultados

Os testes visando a validação do modelo proposto foram realizados utilizando o fator de multiplicação do desvio padrão (w) igual a 1 e 2. A criação dos *baselines* conforme mencionado foi feita de três maneiras, ***Bl-1***, ***Bl-4*** *e* ***Bl-8***. Em ***Bl-1***, o período de coleta dos IPDRs foi feito entre 22-set-2009 à 28-set-2009. Já em ***Bl-4***, a coleta foi realizada entre 31-ago-2009 à 28-set-2009. Por fim, em ***Bl-8***, a coleta foi feita entre 03-ago-2009 à 28-set-2009. Nos gráficos que serão apresentados a seguir, o *baseline* gerado foi comparado com os dados reais referente ao dia 29-set-2009. Como a quantidade de possibilidades para geração de *baselines* é extensa, decidimos apresentar os que tiveram maior destaque.

As Figuras 5.5, 5.6 e 5.7 mostram os *baselines* ***Bl-1***, ***Bl-4*** *e* ***Bl-8*** de chamadas internas realizadas com sucesso (CELI-A) com w=1.

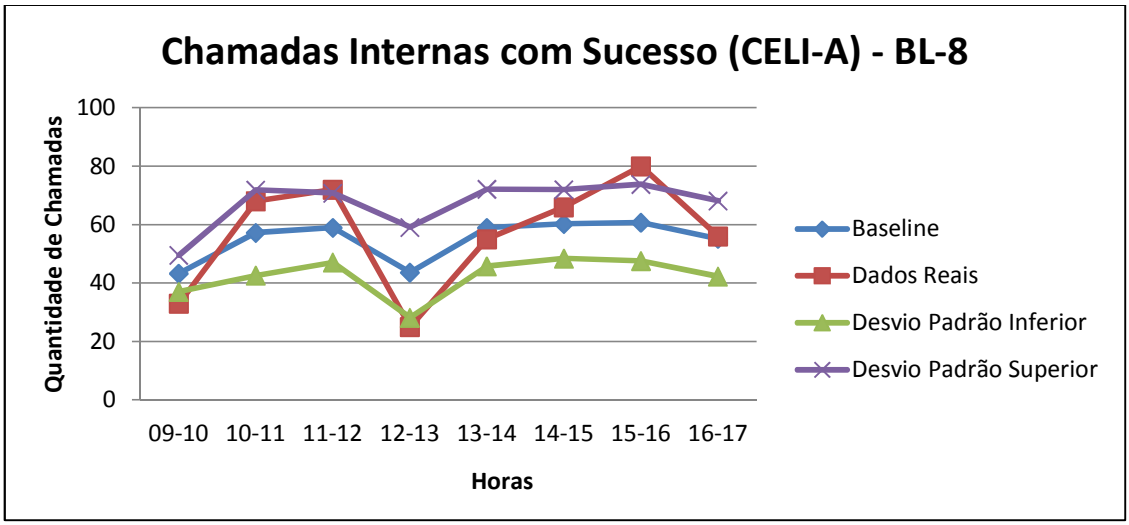


Figura 5.5 – *Baseline* Chamadas Internas com Sucesso (CELI-A) com *w*=1 – ***Bl-8.***

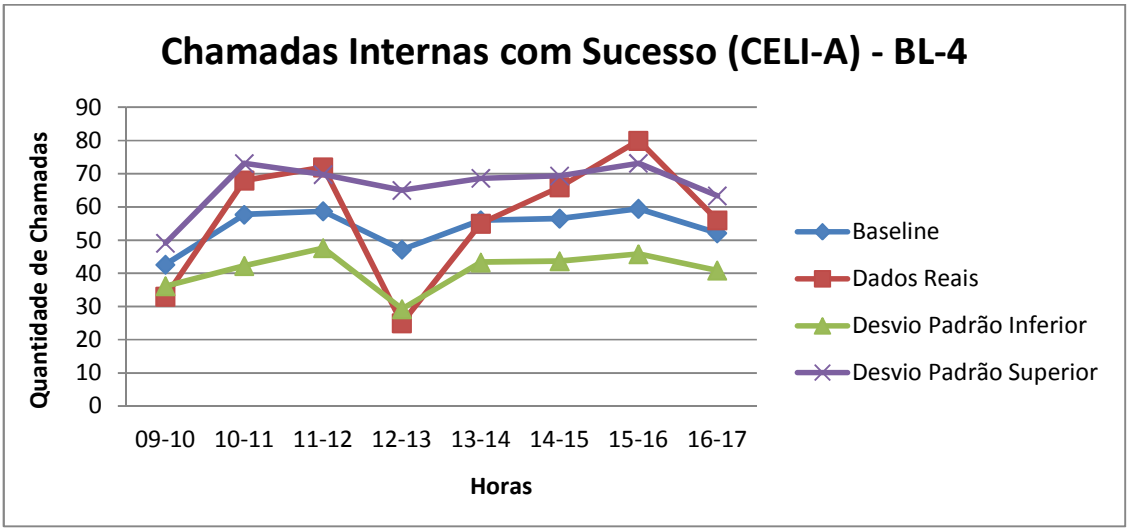


Figura 5.6 – *Baseline* Chamadas Internas com Sucesso (CELI-A) com *w*=1 – ***Bl-4.***

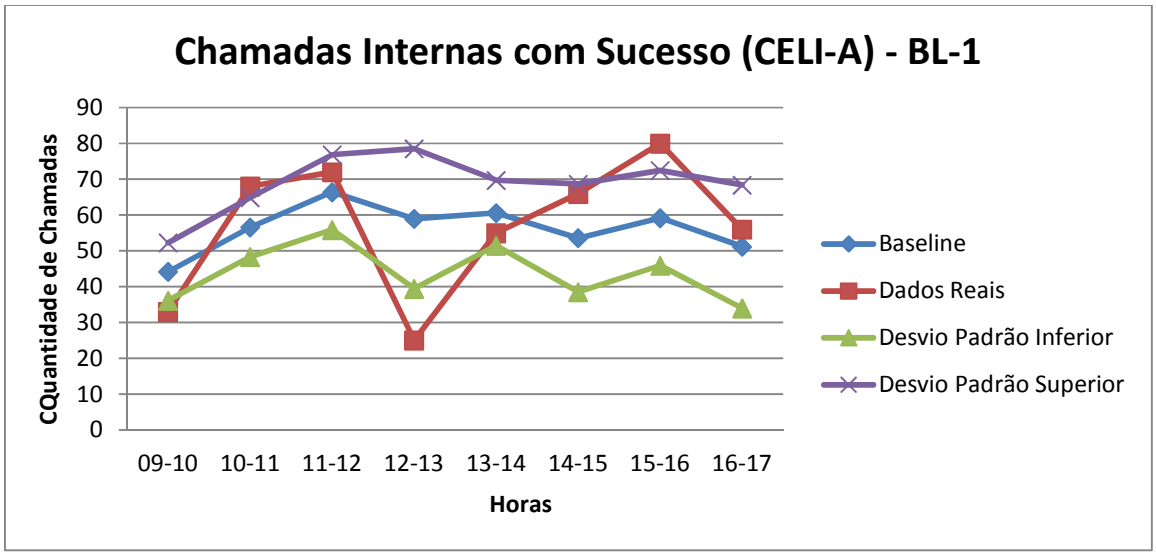


Figura 5.7 – *Baseline* Chamadas Internas com Sucesso (CELI-A) com *w*=1 – ***Bl-1.***

Neste exemplo, a quantidade de chamadas internas com sucesso geradas no dia 29-set-2009 foi comparada entre os três modelos de *baselines*. Em relação ao *baseline* de oito semanas (***Bl-8***), nota-se que entre as 09:00 e 15:00 horas os dados permaneceram dentro dos limites estabelecidos pelo desvio padrão. Entre 15:00 e 16:00 horas é possível notar que o dado real ultrapassou o limiar representado pelo desvio padrão superior. No caso do *baseline* de quatro semanas (***Bl-4***), entre 12:00 e 13:00 horas, o dado real apresentou um valor menor que o definido pelo desvio padrão inferior. Entre 15:00 e 16:00 horas, percebe-se que o valor do dado real superou o limiar estabelecido pelo desvio padrão superior. No *baseline* de uma semana (***Bl-1***), o comportamento do tráfego é semelhante ao apresentado em ***BL-4,*** exceto entre 11:00 e 12:00 horas, e entre 12:00 e 13:00 horas. Nestes horários, a curva "Dados Reais" está mais afastada das curvas "Desvio Padrão Superior" e "Desvio Padrão Inferior".

A mesma análise que embasou a geração das Figuras 5.5, 5.6 e 5.7 foi repetida durante trinta dias entre 29-set e 29-out-2009 com intuito de criar estatísticas para à quantidade de desvios de comportamento do tráfego em relação ao estimado por seu *baseline*. A Tabela 5.1 consolida algumas informações sobre os alarmes gerados durante o período analisado para cada modelo de *baseline*.

	BL-8	***BL-4***	***BL-1***
Quantidade de alarmes no mês	66	69	71
Média de alarmes por dia	3	3,1	3,22
Tempo médio entre alarmes	1 alarme a cada 2 horas e 36 min	1 alarme a cada 2 horas e 34 min	1 alarme a cada 2 horas e 29 min

Tabela 5.1 – Alarmes gerados para *baselines* de chamadas CELI-A com *w*=1.

A Tabela 5.2 relaciona a quantidade de alarmes gerados com *w*=1 por faixa de horário para cada *baseline* observado.

	Quantidade de alarmes por faixa de horário					
	BL-8		***BL-4***		***BL-1***	
Horas	**Quantidade**	**%**	**Quantidade**	**%**	**Quantidade**	**%**
09-10	4	6,06	4	5,80	4	5,63
10-11	6	9,09	6	8,70	6	8,45
11-12	14	21,21	14	20,29	14	19,72
12-13	7	10,61	8	11,59	9	12,68
13-14	3	4,55	4	5,80	4	5,63
14-15	5	7,58	5	7,25	6	8,45
15-16	21	31,82	22	31,88	22	30,99
16-17	6	9,09	6	8,70	6	8,45

Tabela 5.2 – Alarmes gerados por faixa de horário para *baselines* de chamadas CELI-A com *w*=1.

Este resultado compara cada modelo de *baseline* referente à quantidade de alarmes gerados no mês analisado. Através da Tabela 5.1 é possível notar que em *baselines* formados em um período menor (ex: ***Bl-1***), acontecem alarmes com maior frequência em relação à frequência de alarmes gerados em *baselines* formados em um período maior (ex: ***Bl-8*** e ***Bl-4***). A Tabela 5.2 apresenta a quantidade de alarmes em cada faixa de horário analisado. Podemos perceber que entre 15:00 e 16:00 horas ocorrem a maior concentração de alarmes. Independente do modelo de *baseline* adotado, esse volume de alarmes representa aproximadamente 31% dos alarmes do mês.

Os mesmos *baselines* gerados nas Figuras 5.5, 5.6 e 5.7 são novamente apresentados nas Figuras 5.8, 5.9 e 5.10. Porém, neste caso, o *baseline* foi comparado com os dados reais coletados nos dias 02-out-2009, 14-out-2009 e 20-out-2009.

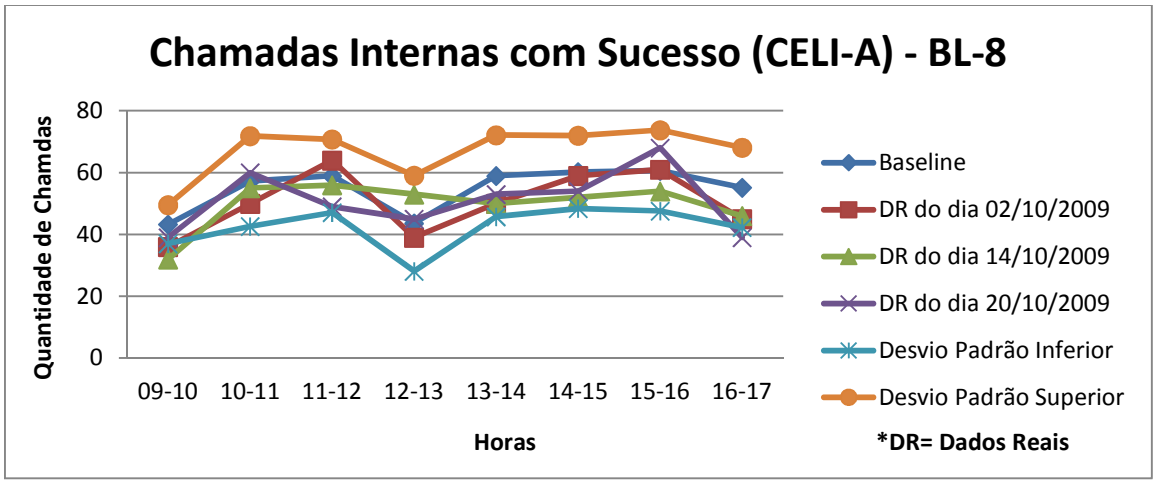


Figura 5.8 – *Baseline n°2* Chamadas Internas com Sucesso (CELI-A) com *w*=1 – ***Bl-8.***

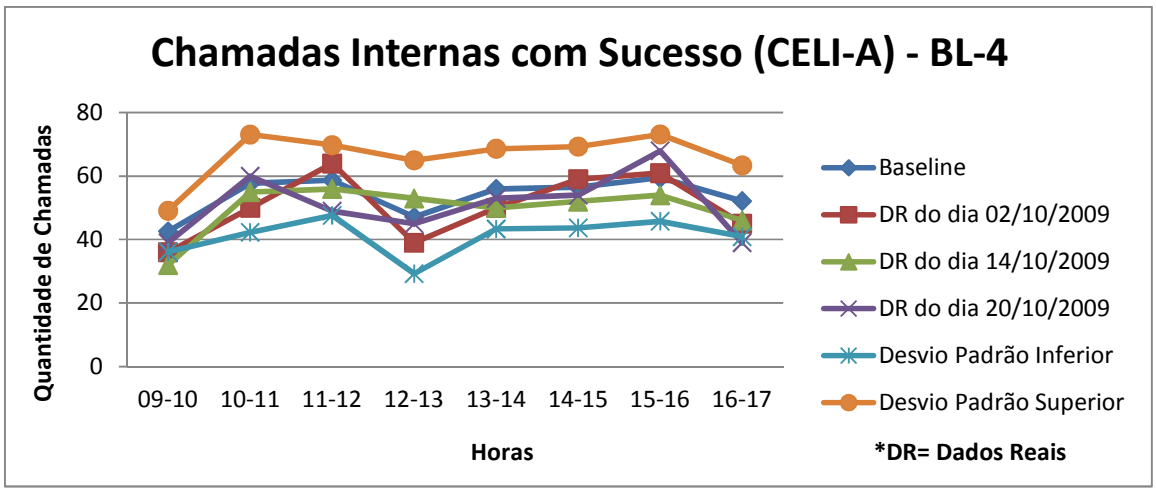


Figura 5.9 – *Baseline n°2* Chamadas Internas com Sucesso (CELI-A) com *w*=1 – ***Bl-4.***

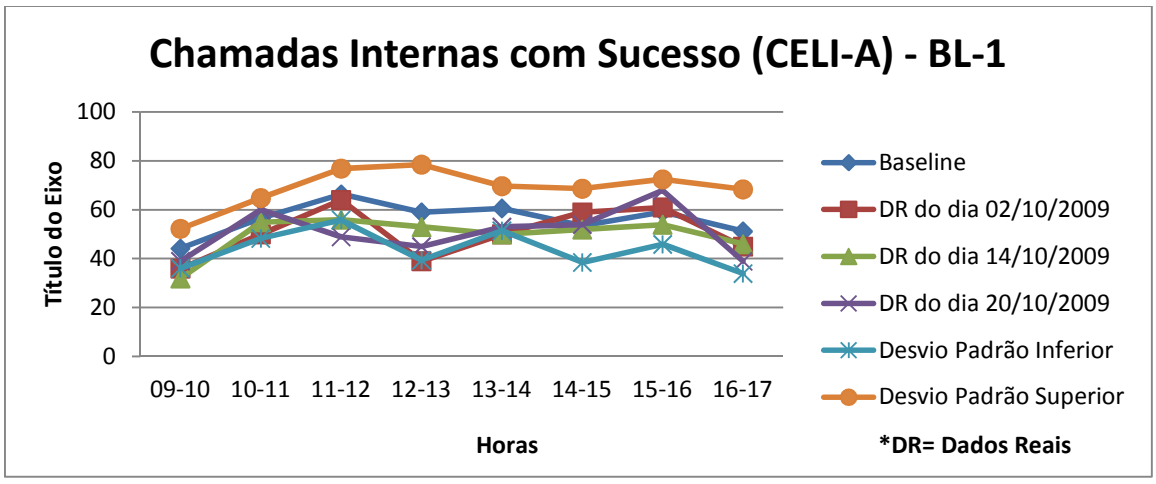


Figura 5.10 – *Baseline n°2* Chamadas Internas com Sucesso (CELI-A) com *w*=1 – ***Bl-1.***

Neste exemplo, nas Figuras 5.8, 5.9 e 5.10 a quantidade de chamadas internas com sucesso geradas nos dias 02-out-2009, 14-out-2009 e 20-out-2009 foram comparadas entre os três modelos de *baselines*. Em relação aos três tipos de *baselines*, nota-se que os dados reais permaneceram dentro dos limites estabelecidos pelo desvio padrão. É possível observar que nestes dias não ocorreram desvios no comportamento no sistema VoIP.

As Figuras 5.11, 5.12 e 5.13 mostram os *baselines* ***Bl-1***, ***Bl-4*** *e* ***Bl-8*** de chamadas internas realizadas com sucesso (CELI-A) com *w*=2.

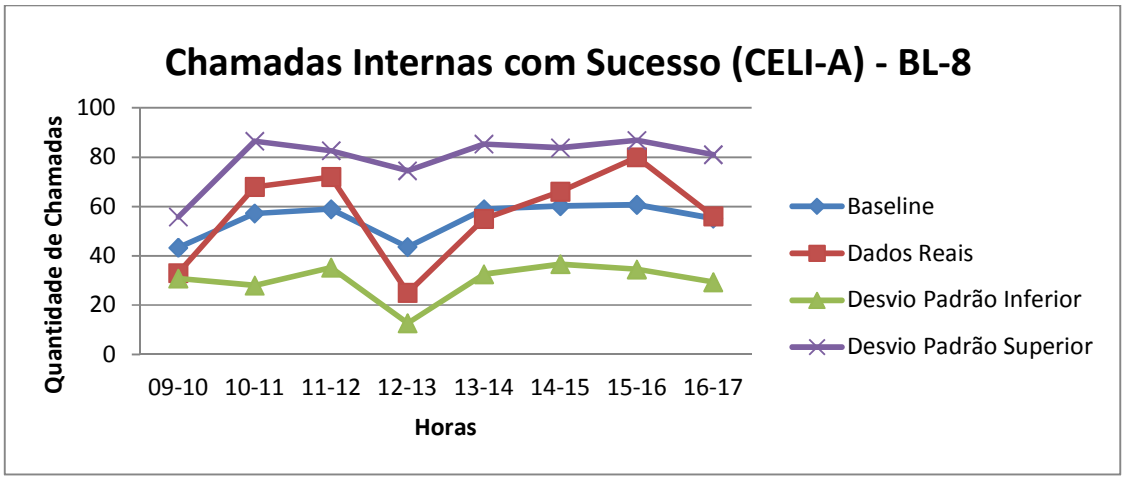


Figura 5.11 – *Baseline* Chamadas Internas com Sucesso (CELI-A) com *w*=2 – ***Bl-8.***

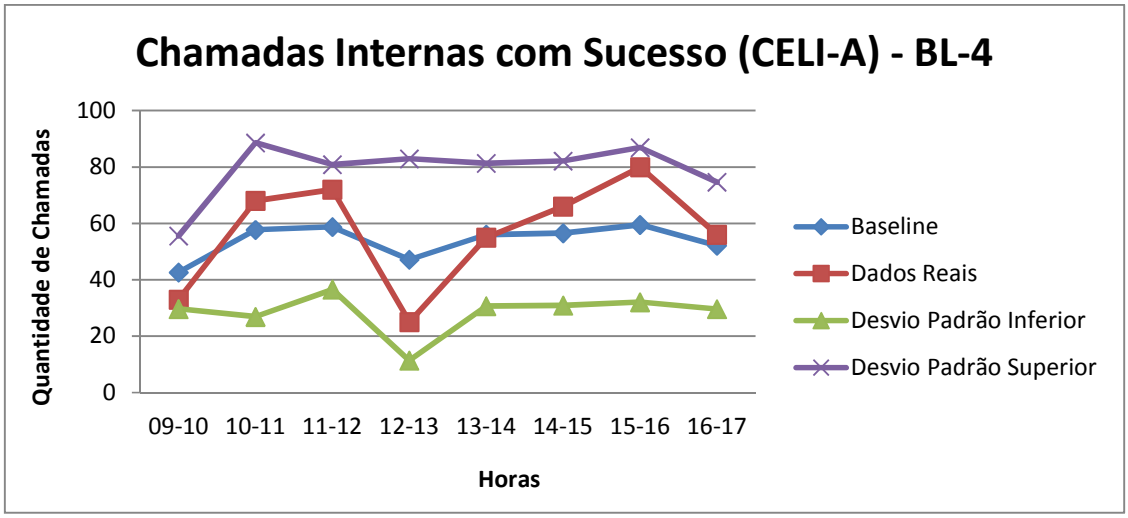


Figura 5.12 – *Baseline* Chamadas Internas com Sucesso (CELI-A) com *w*=2 – ***Bl-4.***

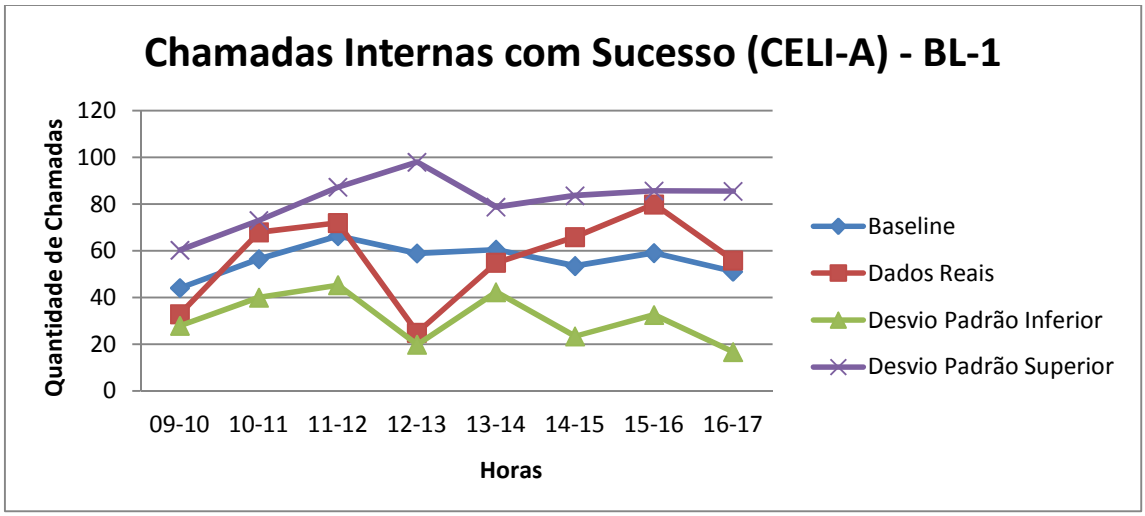


Figura 5.13 – *Baseline* Chamadas Internas com Sucesso (CELI-A) com *w*=2 – ***Bl-1.***

Neste exemplo, a quantidade de chamadas internas com sucesso geradas no dia 29-set-2009 foi comparada entre os três modelos de *baselines* considerando o multiplicador do desvio padrão (*w*) igual a dois. Analisando o *baseline* de oito semanas (***Bl-8***) nota-se que durante todo o período analisado, os dados permaneceram dentro dos limites estabelecidos pelo desvio padrão. No caso do *baseline* de quatro semanas (***Bl-4***), o comportamento é o mesmo. No caso do *baseline* de uma semana (***Bl-1***) é apresentado um comportamento semelhante à ***Bl-8*** e ***Bl-4***, exceto entre 12:00 e 13:00 horas onde os dados reais estão mais próximos do estabelecido pelo desvio padrão inferior.

A Tabela 5.3 consolida as informações sobre os alarmes gerados durante o período analisado para cada modelo de *baseline* considerando *w*=2.

	BL-8	***BL-4***	***BL-1***
Quantidade de alarmes no mês	20	21	24
Média de alarmes por dia	0,9	0,95	1,09
Tempo médio entre alarmes	1 alarme a cada 8 horas e 48 min	1 alarme a cada 8 horas e 25 min	1 alarme a cada 7 horas e 20 min

Tabela 5.3 – Alarmes gerados para *baselines* de chamadas CELI-A com *w*=2.

A Tabela 5.4 relaciona a quantidade de alarmes gerados com *w*=2 por faixa de horário para cada *baseline* observado.

	Número de alarmes por faixa de horário					
	BL-8		***BL-4***		***BL-1***	
Horas	**Quantidade**	**%**	**Quantidade**	**%**	**Quantidade**	**%**
09-10	0	0	0	0,00	1	4,17
10-11	1	5	1	4,76	1	4,17
11-12	1	5	1	4,76	2	8,33
12-13	7	35	7	33,33	7	29,17
13-14	1	5	2	9,52	2	8,33
14-15	0	0	0	0,00	0	0,00
15-16	10	50	10	47,62	10	41,67
16-17	0	0	0	0,00	1	4,17

Tabela 5.4 – Alarmes gerados por faixa de horário para *baselines* de chamadas CELI-A com *w*=2.

As Figuras 5.14, 5.15 e 5.16 apresentam os *baselines* ***Bl-1***, ***Bl-4*** *e* ***Bl-8*** das chamadas internas realizadas com falha (FCI-A) com *w*=1.

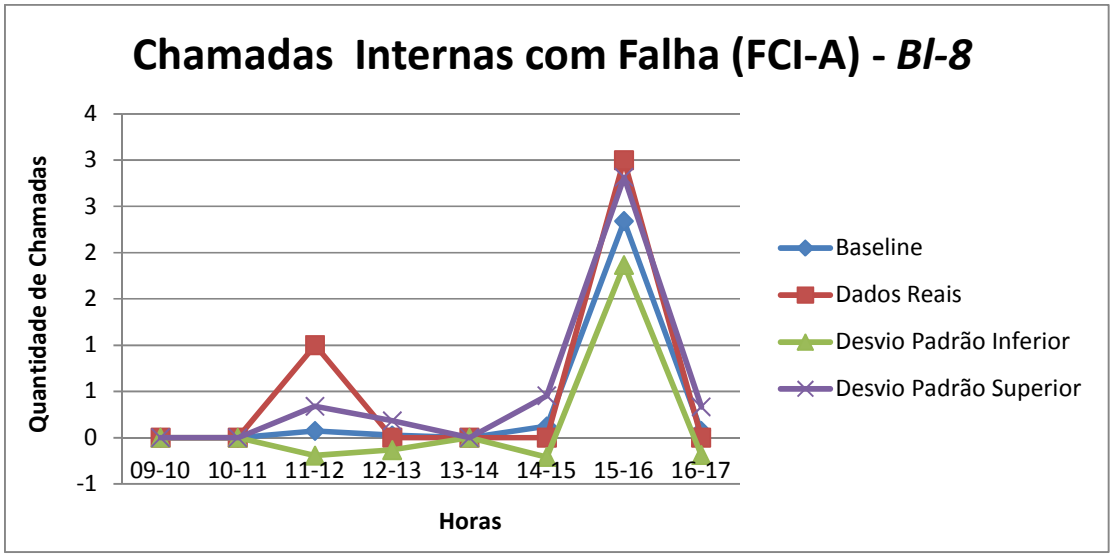


Figura 5.14 – *Baseline* Chamadas Internas com Falha (FCI-A) com *w*=1 – ***Bl-8.***

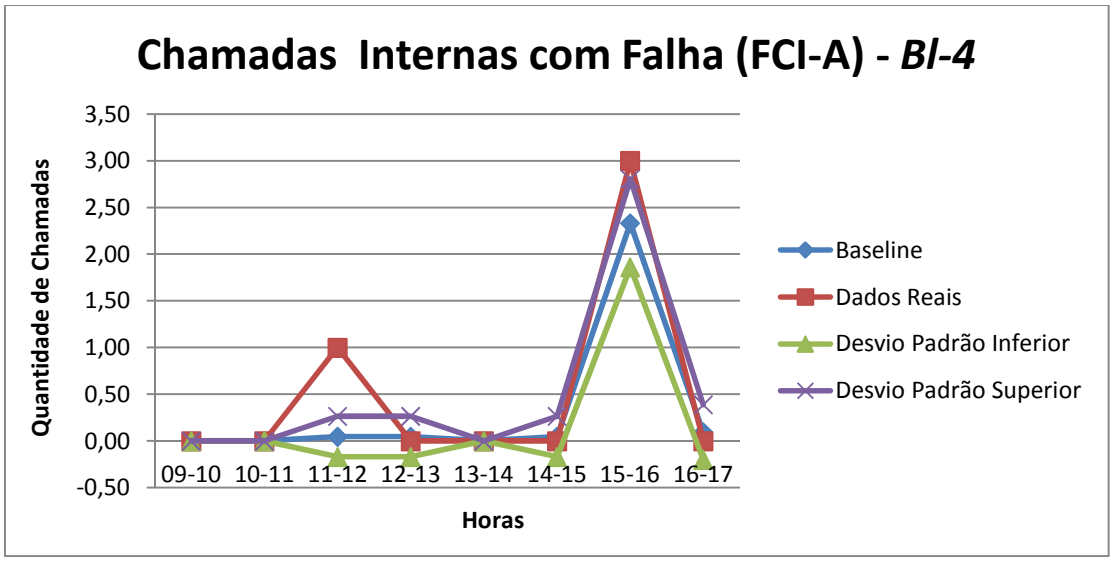


Figura 5.15 – *Baseline* Chamadas Internas com Falha (FCI-A) com *w*=1 – ***Bl-4.***

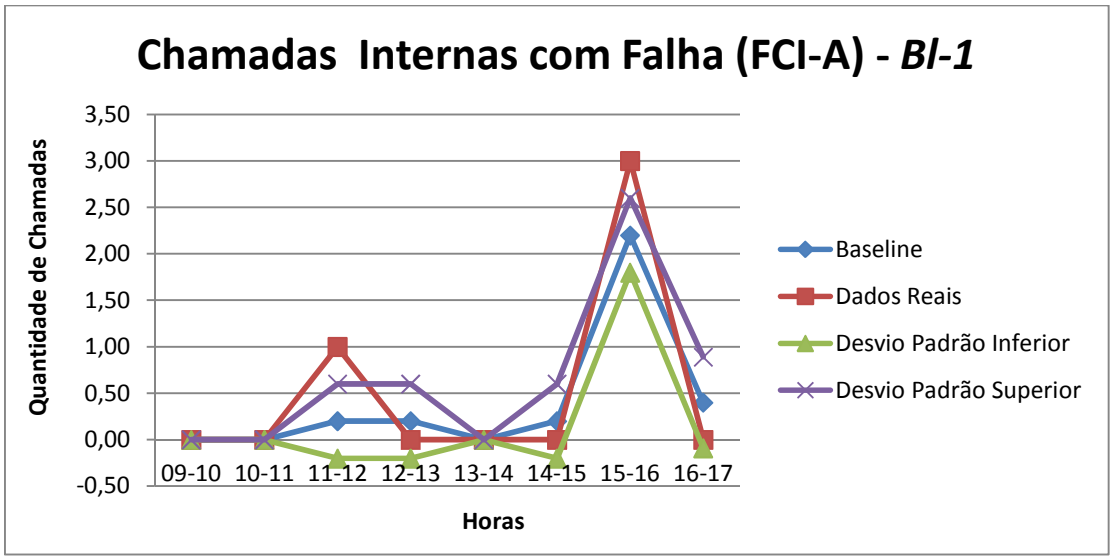


Figura 5.16 – *Baseline* Chamadas Internas com Falha (FCI-A) com *w*=1 – ***Bl-1.***

Neste exemplo, foram gerados três *baselines* analisando as chamadas internas geradas com falha. Nos três modelos de *baseline* (***Bl-8***, ***Bl-4*** e ***Bl-1***), as curvas seguem a mesma tendência. Adicionalmente, percebe-se que existem chamadas com falha entre 11:00 e 12:00 horas e entre 15:00 e 16:00 horas. Nos três casos, entre 11:00 e 12:00 horas, o valor real de chamadas no dia 29-set-2009 superou o definido pelo desvio padrão superior. Nos *baselines* ***Bl-8*** e ***Bl-4***, entre 15:00 e 16:00 horas a quantidade de chamadas com falha

foi equivalente ao estabelecido pelo desvio padrão superior. No caso do ***Bl-1***, entre 15:00 e 16:00 horas este valor foi levemente superior.

A Tabela 5.5 apresenta de maneira consolidada os alarmes gerados durante o período analisado para cada modelo de *baseline* com *w*=1.

	BL-8	***BL-4***	***BL-1***
Quantidade de alarmes no mês	21	21	24
Média de alarmes por dia	0,91	0,91	1,04
Tempo médio entre alarmes	1 alarme a cada 8 horas e 14 min	1 alarme a cada 8 horas e 14 min	1 alarme a cada 7 horas e 41 min

Tabela 5.5 – Alarmes gerados para *baselines* de chamadas FCI-A com *w*=1.

A Tabela 5.6 apresenta uma relação entre a quantidade de alarmes gerados com *w*=1 por faixa de horário para cada *baseline* observado.

	Número de alarmes por faixa de horário					
	BL-8		***BL-4***		***BL-1***	
Horas	**Quantidade**	**%**	**Quantidade**	**%**	**Quantidade**	**%**
09-10	0	0,00	0	0,00	0	0,00
10-11	1	4,76	1	4,76	1	4,17
11-12	5	23,81	5	23,81	6	25,00
12-13	1	4,76	1	4,76	1	4,17
13-14	1	4,76	1	4,76	1	4,17
14-15	2	9,52	2	9,52	3	12,50
15-16	11	52,38	11	52,38	12	50,00
16-17	0	0,00	0	0,00	0	0,00

Tabela 5.6 – Alarmes gerados por faixa de horário para *baselines* de chamadas FCI-A com *w*=1.

Este resultado compara cada modelo de *baseline* referente à quantidade de alarmes (FCI-A) gerados entre 29-set à 29-out-2009. Através da Tabela 5.5 pode-se observar que a quantidade de alarmes gerados para *baselines* ***Bl-8*** e ***Bl-4*** foi semelhante. Já em ***Bl-1***, a quantidade de alarmes foi superior. A Tabela 5.6 indica que a ocorrência dos alarmes gerados durante o mês, seguiu a mesma tendência do dia 29-set-2009 conforme os *baselines* exibidos nas Figuras 5.14, 5.15 e 5.16. Ou seja, a maior concentração de alarmes ocorre entre 15-16 horas (aproximadamente 50%) seguido por 11-12 horas. (aproximadamente 24%).

As Figuras 5.17, 5.18 e 5.19 apresentam os *baselines* ***(Bl-8, Bl-4 e Bl-)*** gerados para chamadas externas efetuadas com falha em 29-set-2009.

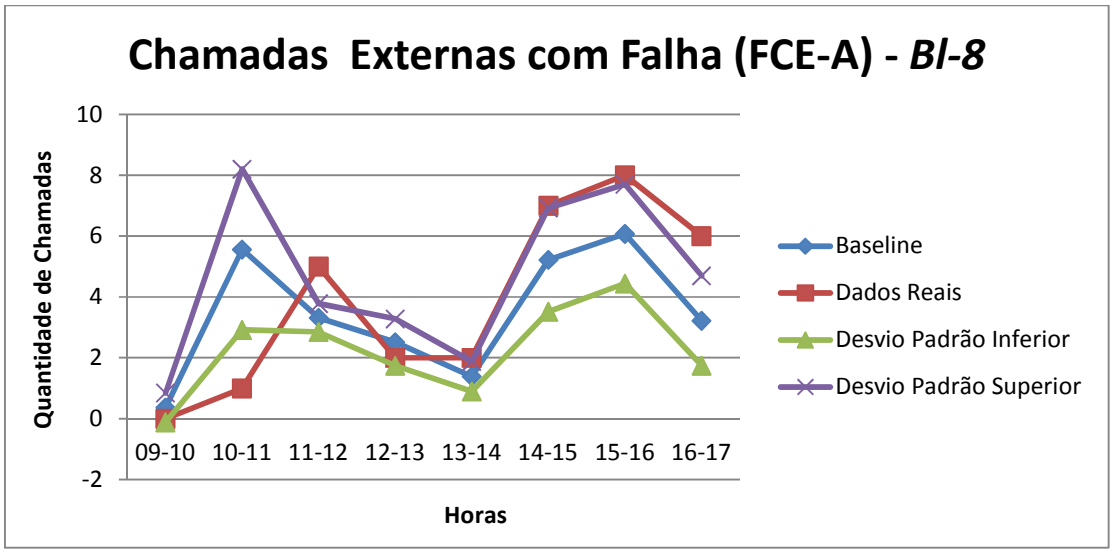


Figura 5.17 – *Baseline* Chamadas Externas com Falha (FCE-A) com *w*=1 – ***Bl-8.***

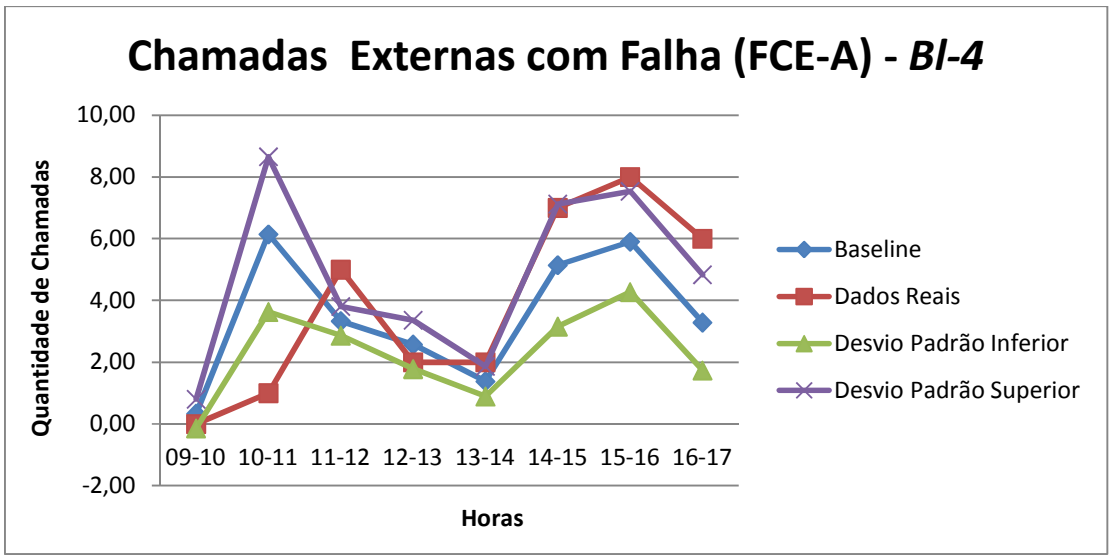


Figura 5.18 – *Baseline* Chamadas Externas com Falha (FCE-A) com *w*=1 – ***Bl-4.***

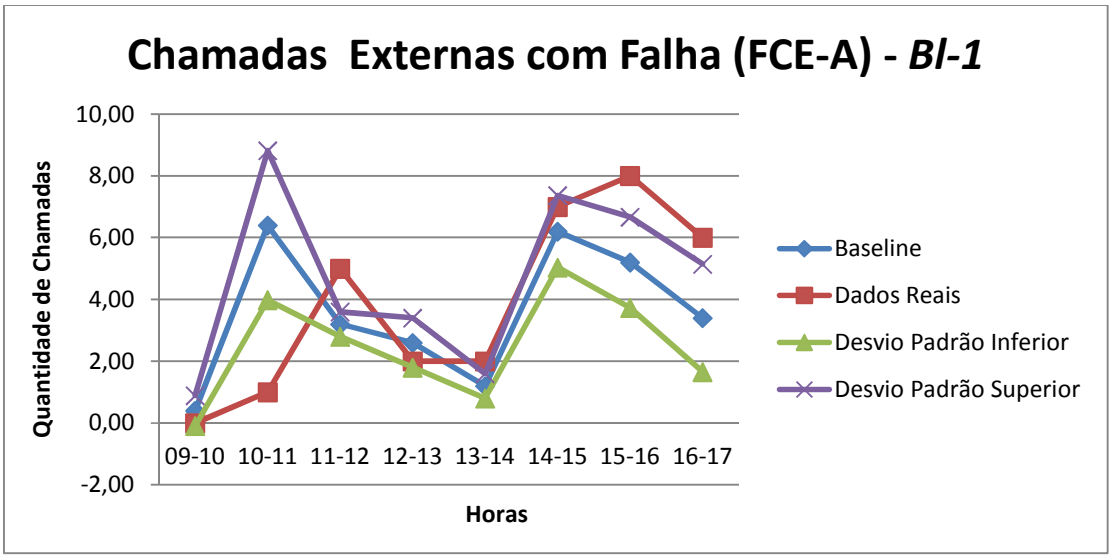


Figura 5.19 – *Baseline* Chamadas Externas com Falha (FCE-A) com *w*=1 – ***Bl-1.***

Neste exemplo é possível notar que as curvas seguem a mesma tendência. No período da manhã, entre 10:00 e 11:00 horas percebe-se que a quantidade de chamadas externas realizadas com falha foi inferior ao estabelecido no desvio padrão inferior. Nota-se também que entre 11:00 e 12:00 horas e após as 14 horas a quantidade de chamadas externas com falha foi maior que o definido pelo desvio padrão superior.

A Tabela 5.7 relaciona a quantidade de alarmes gerados com *w*=1 por faixa de horário para cada *baseline* de chamadas externas com falha.

	BL-8	***BL-4***	***BL-1***
Quantidade de alarmes no mês	32	33	36
Média de alarmes por dia	1,39	1,43	1,56
Tempo médio entre alarmes	1 alarme a cada 5 horas e 45 min	1 alarme a cada 5 horas e 35 min	1 alarme a cada 5 horas e 7 min

Tabela 5.7 – Alarmes gerados para *baselines* de chamadas FCE-A com *w*=1.

A Tabela 5.8 apresenta uma relação entre a quantidade de alarmes gerados com *w*=1 por faixa de horário para cada *baseline* observado.

	Número de alarmes por faixa de horário					
	BL-8		***BL-4***		***BL-1***	
Horas	**Quantidade**	**%**	**Quantidade**	**%**	**Quantidade**	**%**
09-10	3	9,38	3	9,09	3	8,33
10-11	7	21,88	7	21,21	7	19,44
11-12	9	28,13	9	27,27	9	25,00
12-13	1	3,13	2	6,06	2	5,56
13-14	1	3,13	1	3,03	2	5,56
14-15	1	3,13	1	3,03	2	5,56
15-16	6	18,75	6	18,18	6	16,67
16-17	4	12,50	4	12,12	5	13,89

Tabela 5.8 – Alarmes gerados por faixa de horário para *baselines* de chamadas FCE-A com w=1.

Este resultado realiza uma comparação entre cada modelo de *baseline* referente à quantidade de alarmes (FCE-A) gerados entre 29-set à 29-out-2009. Através da Tabela 5.7 é possível observar que a quantidade de alarmes gerados em ***Bl-1*** é levemente superior em relação à ***Bl-4*** e ***Bl-8***. Através da Tabela 5.8 é possível observar que, nos três casos, aproximadamente 20% dos alarmes são gerados entre 11:00 e 12:00 horas. Outros 19% acontecem entre 15:00 e 16:00 horas.

As Figuras 5.20, 5.21 e 5.22 apresentam os *baselines* ***(Bl-8, Bl-4 e Bl-1)*** gerados para chamadas realizadas com tempo de duração superior a trinta minutos em 29-set-2009.

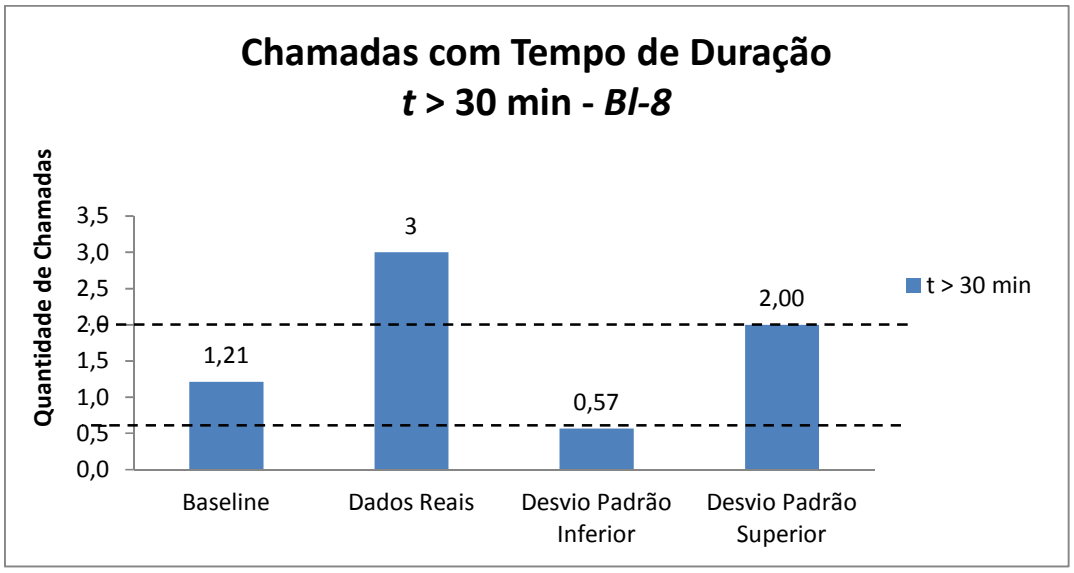


Figura 5.20 – *Baseline* Chamadas com Tempo de Duração *t*>30min – ***Bl-8.***

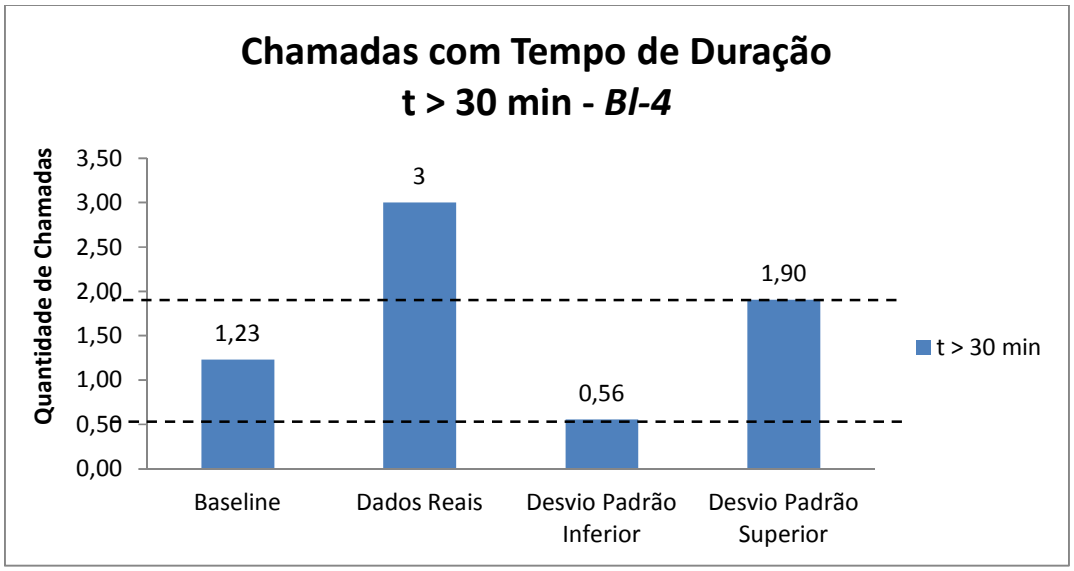


Figura 5.21 – *Baseline* Chamadas com Tempo de Duração *t*>30min – ***Bl-4.***

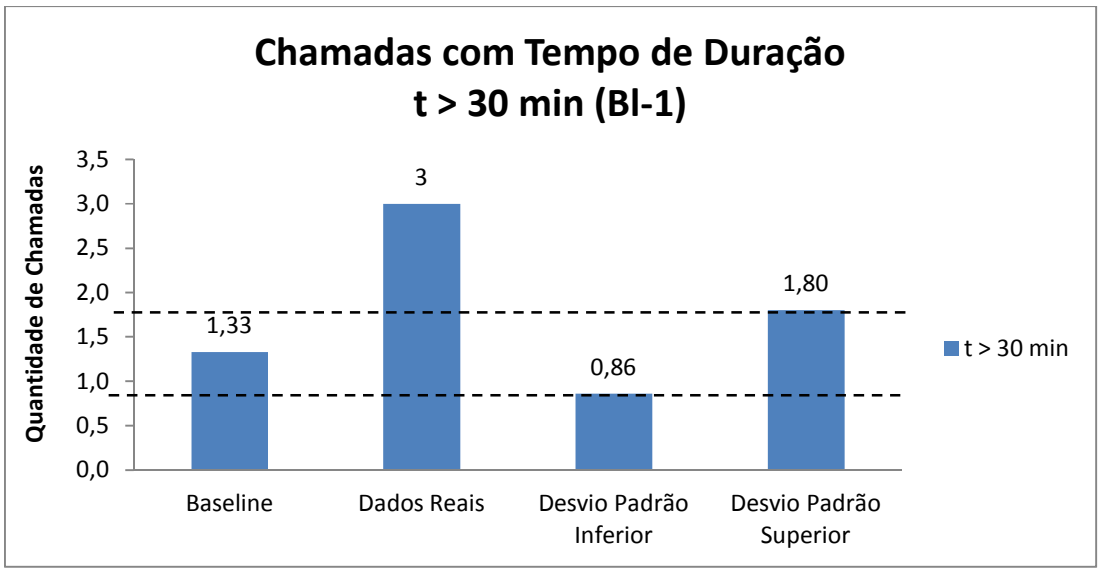


Figura 5.22 – *Baseline* Chamadas com Tempo de Duração *t*>30min – ***Bl-1.***

Neste exemplo, foram gerados três *baselines* analisando as chamadas efetuadas no dia 29-set-2009 que tiveram duração superior a trinta minutos. Através dos resultados é possível observar que nos três casos (***Bl-8***, ***Bl-4*** e ***Bl-1***) os dados reais ultrapassaram o definido pelo desvio padrão superior. Neste caso ocorreram três chamadas que duraram mais que trinta minutos, e o *baseline* previa em média um volume de chamadas 50% inferior.

A Tabela 5.9 apresenta de forma consolidada a quantidade de alarmes gerados nos *baselines* de chamadas com duração superior a 30 minutos realizadas com sucesso.

	BL-8	***BL-4***	***BL-1***
Quantidade de alarmes no mês	4	4	4
Média de alarmes por dia	0,17	0,17	0,17
Tempo médio entre alarmes	1 alarme a cada 47 horas e 4 min	1 alarme a cada 47 horas e 4 min	1 alarme a cada 47 horas e 4 min

Tabela 5.9 – Alarmes gerados por faixa de horário para *baselines* de chamadas com tempo de duração superior a trinta minutos e com w=1.

Algumas conclusões sobre os resultados apresentados nesta seção:

1. Os *baselines* apresentados nas Figuras 5.5, 5.6 e 5.7 apresentam uma informação interessante ao administrador da rede, pois retratam as chamadas internas que foram completadas. Isto significa que ao exceder o desvio padrão superior, este desvio de comportamento não deve ser interpretado como um alarme, pois ele indica que o sistema suportou uma quantidade maior de chamadas simultâneas. Por outro lado, ao exceder o limiar inferior, deve-se estabelecer um ponto de atenção, pois a quantidade de chamadas com sucesso diminuiu a um nível abaixo do padrão considerado normal. Neste caso pode ser considerada uma situação de alarme.
2. Com base nos *baselines* e nas informações apresentadas na Tabela 5.2 é possível identificar, dia 29-set-2009, momentos de maior tráfego VoIP na rede: entre 11:00 e 12:00 horas e 15:00 e 16:00 horas. Através dos *baselines* de chamadas CELI-A foi possível perceber que os dados reais superaram o estabelecido pelo *baseline*. No entanto, com base nos *baselines* apresentados nas Figuras 5.8, 5.9 e 5.10, podemos inferir que o comportamento do dia 29-set-2009 é atípico, uma vez que o mesmo relatório foi extraído de outros dias, e o volume de chamadas permaneceu dentro do estabelecido pelo desvio padrão. Esta informação pode ser interessante para fins de planejamento, pois se ao prorrogar esta análise a um período mais longo, observar-se que este comportamento se mantém, isto nos leva a crer que a demanda está aumentando e a rede está crescendo.
3. Tanto nos *baselines* apresentados nas Figuras 5.11, 5.12 e 5.13, quanto nas Tabelas 5.3 e 5.4, a sensibilidade do mecanismo de geração de alarme foi reduzida, uma vez

que o fator de multiplicação dobrou em relação a *w*=1. Gozar desta possibilidade pode ser interessante para o administrador de rede, já que isso lhe permite diminuir a quantidade de alarmes, caso ele considere a quantidade de alarmes gerados para *w*=1 exagerada. Através do modelo de resultado proposto, podemos notar também que os horários com maior concentração de alarmes são semelhantes a *w*=1. Isto indica que estes horários merecem maior atenção do administrador da rede.

4. Os *baselines* apresentados nas Figuras 5.14, 5.15 e 5.16 demonstram que a maior concentração de chamadas com falha ocorreu entre 11:00 e 12:00 horas e entre 15:00 e 16:00 horas. De acordo com o *baseline* de chamadas internas com sucesso (CELI-A) verificamos que esta faixa de horário imprime os horários de maior movimento na rede VoIP de Pedreira. Este comportamento pode ser natural, já que o aumento da concorrência pelos recursos da rede tende a aumentar a probabilidade de ocorrência de falhas.
5. Os dados apresentados na Tabela 5.6 reafirmam que os horários entre 11:00 e 12:00 horas e 15:00 e 16:00 horas merecem maior atenção por parte da gerência de rede, pois há uma reincidência de chamadas internas com falha. Ou seja, se o *baseline* mostra que em média existem muitas falhas num determinado horário, o administrador tem em mãos uma situação que deve ser investigada. Neste tipo de abordagem os *baselines* também se mostraram úteis.
6. Através das Figuras 5.17, 5.18 e 5.19, podemos identificar os desvios de comportamento do tráfego ao longo do dia. Ao exceder o limiar inferior, este desvio não deve ser interpretado como um alarme, já que a quantidade de chamadas externas com falha diminuiu a um nível abaixo do padrão esperado. Por outro lado, quando o limiar superior é excedido, deve-se estabelecer um ponto de atenção, pois a quantidade de chamadas superou o considerado normal. Este tipo de dado pode ajudar o administrador da rede a identificar problemas na rede das operadoras mesmo sem gerenciá-las. Através das Tabelas 5.7 e 5.8 é possível perceber que a distribuição dos alarmes ao longo do dia difere-se um pouco das chamadas internas (FCI-A) e externas (FCE-A).
7. Através dos resultados apresentados nas Figuras 5.20, 5.21 e 5.22 é possível definir o perfil de utilização da rede e dos usuários. Esta informação pode ser útil ao

administrador na detecção de uso abusivo dos recursos da rede ou até mesmo de ataques. A Tabela 5.9 mostra que entre 29-set e 29-out-2009 apenas quatro alarmes foram identificados. Esta estatística pode ser utilizada para a geração de *baselines* da quantidade de alarmes identificados no mês.

Capítulo 6

Conclusões Finais e outras Considerações

Neste trabalho, apresentamos uma nova abordagem para gerência de sistemas VoIP através da construção de *baselines*. Os *baselines* são criados a partir de uma base de dados composta por bilhetes de tarifação chamados IPDRs. A construção dos *baselines* visa caracterizar o tráfego VoIP em redes IP. Uma das vantagens deste modelo é que ele resgata os conceitos da telefonia tradicional dentro do mundo IP. O modelo proposto foi aplicado em uma rede metropolitana que se encontra em produção. As principais contribuições obtidas deste trabalho foram:

- Introdução do conceito de IPDR na construção de *baselines* no cenário da telefonia VoIP. Conforme pesquisamos, não existem trabalhos similares nos meios acadêmicos;
- Desenvolvimento do aplicativo para leitura de bilhetes, que interpretou a base de dados de IPDRs bruta e a transformou em uma interface amigável;
- A classificação dos bilhetes, através da classificação de eventos, gerou uma taxonomia para bilhetes IPDRs;
- Desenvolvimento do modelo de criação de *baselines* que agregam grande valor à gerência de redes e detecção de problemas;
- A base dados coletada constitui um banco de informações históricas e vão continuar disponíveis para trabalhos futuros;
- O trabalho de pesquisa realizado demonstra a importância da caracterização do tráfego para a gerência de sistemas VoIP.

Com relação aos resultados, o primeiro ponto abordado foi a geração do *baseline* de chamadas efetuadas com sucesso. Neste caso, notamos que no dia 29 de setembro de 2009,

algumas vezes no dia, a quantidade de chamadas realizadas ultrapassou o estimado tanto pelo desvio padrão superior quanto inferior. A fim de comprovar se aquele era um comportamento anormal, o *baseline* foi repetido em outros dias do mês seguinte, e em todos os casos testados, os dados reais não ultrapassaram o estabelecido pelo *baseline*. Com isso, concluímos como atípico o comportamento do tráfego CELI-A no dia 29-set-2009. Foram gerados também, *baselines* para as chamadas internas com falha (FCI-A), chamadas externas com falha (FCE-A) e chamadas que duraram mais que trinta minutos.

Os *baselines* caracterizam o tráfego telefônico IP, gerando uma "assinatura" do comportamento dos elementos do sistema. Esta "assinatura" pode ser comparada com o comportamento atual dos elementos, de forma que seja possível inferir se existe algum problema que esteja afetando o desempenho da rede. Apesar de utilizarmos dados de uma Rede Metropolitana, esta metodologia pode ser aplicada a qualquer tipo de rede desde que esta possua bilhetes IPDR. Indo um pouco mais além, chegamos à conclusão que esta metodologia pode ser aplicada a qualquer rede desde que esta possua logs, bilhetes, suporte a SNMP, ou seja, registros que retratem um ou mais eventos sobre os elementos do sistema.

A classificação dos IPDRs proporcionou uma vasta gama de possibilidades na criação dos *baselines*. Através dela podemos mapear o comportamento de situações específicas tais como: o número de chamadas interurbanas realizadas em um determinado setor ou o número de chamadas internacionais originadas de um ramal específico. Este exemplo pode ser utilizado para ajudar na detecção de fraudes na rede e também na obtenção do perfil de consumo dos usuários.

Outro resultado que julgamos relevante é que o modelo proposto trata a gerência sobre os sistemas VoIP do ponto de vista dos eventos de telefonia convencional. A tecnologia VoIP é uma aplicação que opera sobre o protocolo TCP/IP, ou seja, sobre uma rede de pacotes. A gerência sobre este modelo de redes está estruturada sobre objetos SNMP e retratam alguns tipos de comportamenteos relacionados aos pacotes. A gerência que estamos propondo trata a tecnologia VoIP do ponto de vista de uma ligação telefônica tradicional (Rede de Telefonia Pública Comutada- RTPC), ou seja, com todos os desfechos que uma ligação telefônica pode ter. Isto é extremamente relevante, pois é uma mudança na maneira de "olharmos" para gerência VoIP.

Esta nova abordagem demonstrou ser muito útil e promissora, pois permitiu a caracterização do tráfego com base em informações que até então eram subutilizadas, que é o caso dos IPDRs. A criação e análise dos *baselines* complementaram a gerência da rede atribuindo otimização e agilidade a este processo. Os *baselines* gerados a partir dos IPDRs demonstraram que a metodologia criada agrega eficiência na gestão de uma rede VoIP, podendo ser utilizada na detecção de problemas. Através desta metodologia é possível desenvolver percepções mais assertivas em relação ao que está acontecendo na rede VoIP. Isto possibilita agilidade na tomada de decisões.

6.1 – Sugestões para Trabalhos Futuros

Como sugestão para trabalhos futuros:

- Utilização de outros modelos estatísticos (ex: moda, mediana), bem como outros modelos de dispersão estatística (ex: variância) para criação dos *baselines*;
- Criar e testar outros modelos de detecção de alarmes baseados em modelos Estocásticos e Redes Neurais artificiais.

Referências Bibliográficas

[1] M. L. Proença Junior, “Baseline Aplicado a Gerência de Redes”, tese de doutorado, Faculdade de Engenharia Elétrica e de Computação, Universidade Estadual de Campinas, 2005.

[2] Magalhães I.L, Pinheiro W. B., “Gerênciamento de Serviços de TI na prática” – Novatec.

[3] http://www.pwc.com.br/pt/publicacoes/index.jhtml , 2011.

[4] N. M. Markovich and U. R. Krieger, “Statistical analysis and modeling of Skype VoIP flows” Computer Communications, v. 33, p. S11-S21, 2010.

[5] B. Xi, H. Chen, W. S. Cleveland, and Thomas Telkamp, “Statistical analysis and modeling of Internet VoIP traffic for network engineering” Electronic Journal of Statistics, v. 4, p. 58-116, 2010.

[6] S. Karapantazis, F. Pavlidou, “VoIP: A comprehensive survey on a promising technology”, Computer Networks, v. 53, n. 12, p. 2050-2090, 2009.

[7] N. Blefari-Melazzi, J. N. Daigle and M. Feminella, “Efficient and stateless deployment of VoIP services” Computer Networks, v. 53, n. 5, p. 706-726, 2009.

[8] http://www.tmforum.org/ipdr

[9] O. Dabbebi, R. Badonnel, O. Festor, “Automated runtime risk management for voice over IP networks and services”. Network Operations and Management Symposium (NOMS), 2010 IEEE , p.57-64, 2010.

[10] TM Forum – TM Forum IPDR Program, http://www.tmforum.org/BestPracticesStandards/IPDR/4501/Home.html, 2011.

[11] G. Breda, L. Mendes, *Failures Detection in Voice Communication Systems*, *In: GLOBECOM 2006*. December 2006. San Francisco/CA, USA.

[12] S. Tartarelli, N. Heureuse, S. Niccolini, "Lessons learned on the usage of call logs for security and management in IP telephony," Communications Magazine, IEEE , vol.48, no.12, pp.76-82, December 2010.

[13] I. Ruiz-Agundez, Y. Penya, P. Garcia-Bringas, “Fraud Detection for Voice over IP Services on Next-Generation Networks”, editors: P. Samarati, M. Tunstall, J. Posegga, K. Markantonakis, D. Sauveron, Information Security Theory and Practices: Security

and Privacy of Pervasive Systems and Smart Devices, Lectures Notes on Computer Science, Springer Berlin / Heidelberg, v. 6033, p. 199-212, 2010.

[14] M.A. Bihina Bella, J.H.P. Eloff, M.S. Olivier, "A fraud management system architecture for next-generation networks", Forensic Science International, Volume 185, Issues 1-3, 2009, Pages 51-58.

[15] Dasgupta, K. and Singh, R. and Viswanathan, B. and Chakraborty, D. and Mukherjea, S. and Nanavati, A.A. and Joshi, A., "Social ties and their relevance to churn in mobile telecom networks", Proceedings of the 11th international conference on Extending database technology: Advances in database technology, p. 668-677, 2008.

[16] F. M. Pires, L. Mendes "Proposta de uma Arquitetura Híbrida e Hierárquica de Rede de Sensores/Atuadores para Aplicação em Cenários Metropolitanos", dissertação de mestrado, Faculdade de Engenharia Elétrica e de Computação, Universidade Estadual de Campinas, 2010.

[17] L. S. Mendes, M. L. Bottoli and G. D. Breda, "Digital cities and Open MANs: a new communications paradigm", Latin America Transactions, IEEE (Revista IEEE America Latina) , vol.8, no.4, p.394-402, 2010.

[18] Graham II JW. *Authenticating Public Access networking*, SIGUCCS'02, 20–23 November 2002, Providence, Rhode Island, USA.

[19] http://2009.campinas.sp.gov.br/saude/sistemas/sig2m.htm

[20] http://www.chooseyourvoip.com/articles/cost-advantages-of-voip/

[21] Hucaby D. Ciscopress.com - CCNP Switch 642-813 – Official Certification Guide – 251-253.

[22] Miani R. S., "Aplicação de métricas à análise de segurança em Redes Metropolitanas de Acesso Aberto", dissertação de mestrado, Faculdade de Engenharia Elétrica e de Computação, Universidade Estadual de Campinas, 2009.

[23] Bouras C., Gkamas A., Papagiannopoulos J., Theophilopous G., Tsiatsos T., "Broadband municipal optical network in Greece: A suitable business model" – Elsevier – 2009.

[24] Mendes, L., Inocêncio, A., Panhan, A., and Tilli, M. (2008). Bringing together digital cities and open access mans. *The 2008 Networking and Electronic Commerce Research Conference*, 1.

[25] http://origin.citylink.co.nz/

[26] http://www.enet.ie/

[27] T. Porter, B. Baskin, L. Chaffin, M. Cross, J. Kanclirz Jr, A. Rosela, C. Shim, A. Zmolek "Pratical VoIP Security", Sygress Publishing 2006.

[28] *Voice Over 802.11* – Frank Ohrtman, 2003.

[29] Darlington, R., "A Guide to Voice over Internet Protocol", Julho 2005, http://www.rogerdarlington.me.uk/VoIP.html

[30] Yoshioka S., "Protocolos para Telefonia IP", Julho 2003.

[31] http://www.teleco.com.br/tutoriais/tutorialtelefoniaip/pagina_2.asp

[32] H.323, *"Packet Based Multimedia Communications Systems"* - International Telecommunication Union Telecommunication Standardization Sector ITU-T - novembro de 2000.

[33] Garcia, M. E, "Método de Análise de Tráfegos VoIP Sobrepostos", dissertação de mestrado, Faculdade de Engenharia Elétrica e de Computação, Universidade Estadual de Campinas, 2009.

[34] RFC3550 – "*Real-Time Transport Protocol*" – 2003 - http://www.ietf.org/rfc/rfc3550.txt

[35] RFC3261 – "*Session Initiation Protocol*" – 2002 - http://www.ietf.org/rfc/rfc3261.txt

[36] Meggelen J.V, Smith J., Madsen L. *Asterisk: O Futuro da Telefonia*. Alta Books, 2005.

[37] RFC1157 – "*Simple Network Management Protocol*" – 1990 - http://www.faqs.org/rfcs/rfc1157.html

[38] Murray P., Stalvig P., "SNMP: Simplified" – F5 Networks – 2008.

[39] Trammell B., Boschi E., Zurich ETH, "*An Introduction to IP Flow Information Export (IPFIX)"* – IETF Standard Update – 2008.

[40] International Telecommunication Union, "The Status of Voice Over Internet Protocol (VoIP) Worldwide"- 2007.

[41] Breda G.D., "Detecção de Falhas em Redes de Comunicações", tese de doutorado, Faculdade de Engenharia Elétrica e de Computação, Universidade Estadual de Campinas, 2008.

[42] Barreto C., Soares O. F., "TMN Telecommunication Management Network" – trabalho de pós graduação, Universidade Católica de Salvador, 1999.

[43] Winemiller, E., Roff, J.T., Heyman, B., Groom, R., "Visual Basic 6 Database", Macmillan Computer Publishhing, 1998.

[44] [Sitio com dados da ferramenta Microsoft Access]: http://www.microsoft.com/en/us/default.aspx

[45] M. L. Proença Junior, C. Coppelmans, M. Botolli, and L. S. Mendes, "Security and reliability in information systems and networks: Baseline to help with network management". In Ascenso, J., Vasiu, L., Belo, C. and Saramago, M. (eds), e-Business and Telecommunication Networks, Springer, Netherlands, 2006.

[46] H. Hajji, "*Baselining network traffic and online faults detection*", Communications, IEEE International Conference 2003.

[47] Technical Support and Documentation, "*Baseline Process Best Practices White Paper*" – 2005 – Cisco Systems.

[48] Thottan M., Ji C., "Proactive Anomaly Detection Using Distributed Intelligent Agents" – IEEE – 1998.

[49] Ho L. L., Cavuto D. J, Papavassiliou S., Zawadzki A. G., "*Adaptive and Automated Detection of Service Anomalies in Transaction-Oriented WAN's: Network Analysis, Algorithms, Implementation, and Deployment*" – IEEE Journals Vol.18 – 2000.

[50] MRTG - *The Multi Router Traffic Grapher*, disponível no endereço: http://oss.oetiker.ch/mrtg/doc/mrtg.en.html - 2012.

[51] NfSen – *Netflow Sensor*, disponível no endereço: http://nfsen.sourceforge.net/#mozTocId376385 – 2011.

[52] Cacti, disponível no endereço: http://www.cacti.net/ - 2011.

[53] B. B. Zarpelão, "Detecção de Anomalias em Redes de Computadores", tese de doutorado, Faculdade de Engenharia Elétrica e de Computação, Universidade Estadual de Campinas, 2010.

[54] http://www.pedreira.sp.gov.br/ing/index.php