**UNIVERSIDADE DE BRASÍLIA**
**FACULDADE DE TECNOLOGIA**
**DEPARTAMENTO DE ENGENHARIA ELÉTRICA**

# USO DOS DADOS DE CONTABILIZAÇÃO DO RADIUS PARA FATURAMENTO E PARA GERAÇÃO DE INFORMAÇÕES GERENCIAIS E OPERACIONAIS DE SERVIÇOS EM BANDA LARGA

**DANTE JESUS RICHESKY DA SILVA**

**ORIENTADOR: RODRIGO PINTO LEMOS**

**DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA**

**PUBLICAÇÃO: PPGENE.DM-422/2010**

**BRASÍLIA / DF: JULHO - 2010**

**UNIVERSIDADE DE BRASÍLIA**
**FACULDADE DE TECNOLOGIA**
**DEPARTAMENTO DE ENGENHARIA ELÉTRICA**

# "USO DOS DADOS DE CONTABILIZAÇÃO DO RADIUS PARA FATURAMENTO E PARA GERAÇÃO DE INFORMAÇÕES GERENCIAIS E OPERACIONAIS DE SERVIÇOS EM BANDA LARGA"

**DANTE JESUS RICHESKY DA SILVA**

**DISSERTAÇÃO DE MESTRADO PROFISSIONALIZANTE SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE.**

APROVADA POR:

RODRIGO PINTO LEMOS, Dr., UFG
(ORIENTADOR)

PAULO HENRIQUE PORTELA DE CARVALHO, Dr., ENE/UNB
(EXAMINADOR INTERNO)

FLÁVIO ELIAS GOMES DE DEUS, Dr., ENE/UNB
(EXAMINADOR INTERNO)

**BRASÍLIA, 09 DE JULHO DE 2010.**

## FICHA CATALOGRÁFICA

Silva, Dante Jesus Richesky da.
S586u Uso dos Dados de Contabilização do RADIUS para Faturamento e para Geração de Informações Gerenciais e Operacionais de Serviços em Banda Larga / Dante Jesus Richesky da Silva. -- 2010.
xx, 136 p. : il. ; 30 cm.

Dissertação (mestrado) - Universidade de Brasília, Faculdade de Tecnologia, Departamento de Engenharia Elétrica, 2010.
Inclui bibliografia.
Orientação: Rodrigo Pinto Lemos.

1. Internet (Redes de computação). 2. Sistemas de comunicação em banda larga. I. Lemos, Rodrigo Pinto. II. Título.

CDU 004.738.5

## REFERÊNCIA BIBLIOGRÁFICA

SILVA, D. J. R. (2010). Uso dos Dados de Contabilização do RADIUS para Faturamento e para Geração de Informações Gerenciais e Operacionais de Serviços em Banda Larga. Dissertação de Mestrado, Publicação PPGENE.DM-422/2010, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 136p.

## CESSÃO DE DIREITOS

NOME DO AUTOR: Dante Jesus Richesky da Silva

TÍTULO: Uso dos Dados de Contabilização do RADIUS para Faturamento e para Geração de Informações Gerenciais e Operacionais de Serviços em Banda Larga.

GRAU: Mestre ANO: 2010



_____

Dante Jesus Richesky da Silva
Rua São Clemente, 114, Bloco 2 – Ap. 706 – Bairro Botafogo
CEP 22260-000 – Rio de Janeiro/RJ – Brasil

**DEDICATÓRIA**

*Á Nereida e ao Allan.*

**AGRADECIMENTOS**

Agradeço especialmente à Nereida e ao Allan, que além de cederem parte do nosso tempo de convivência durante o curso e o desenvolvimento do trabalho, incentivaram, apoiaram e compartilharam os esforços nesta e em muitas outras longas jornadas. Aos meus pais Dantes e Ivone, aos meus irmãos Dil Marcos e Lou Ane, que, mesmo de longe, sempre me apoiaram, me incentivaram e me deram forças.

Agradeço à Brasil Telecom pela iniciativa de realização de programa específico de mestrado e por propiciar o desenvolvimento deste trabalho. O agradecimento estende-se a Oi, que manteve o suporte a continuidade do curso e viabilizou a conclusão e utilização deste trabalho.

Aos meus amigos e colegas de equipe Daniel Sperb, Christianne Marques, Marcelo Veiga, Lilian Batista Nadu, Fabiana Nawate, Carlos Eduardo Carneiro, Marcela Ramalho, André Bonomi e Márcio Novaes, que ao longo do desenvolvimento do trabalho e durante o curso deram apoio e desenvolveram atividades que viabilizaram a sua conclusão.

Aos colegas Rogério Bley, Djair Brito, Marcos Daniel Vieira, Mauricio Veloso e Alberico Carvalho, todos meus superiores diretos durante o desenvolvimento do curso e do trabalho, pelo apoio e incentivo a sua conclusão com sucesso.

Ao André Gruszynski, que desempenhou a árdua atividade de co-orientar o desenvolvimento deste trabalho e auxiliou diretamente na evolução, sendo uma referência pelos conhecimentos na área.

Ao Prof. Rodrigo Lemos, pela disposição e dedicação em auxiliar neste trabalho, contribuindo e sendo presente, mesmo com a distância, no seu desenvolvimento.

Obrigado a todos vocês, que foram os impulsionadores e os viabilizadores do sucesso nesta jornada.

**RESUMO**

É notório e incontestável o crescimento da abrangência e o aumento da importância da Internet e do seu acesso em banda larga, que atualmente estão dentro dos objetivos de crescimento de vários países ao redor do mundo. Este crescimento gerou a necessidade de acessos remotos mais confiáveis em termos de disponibilidade, integridade e rastreabilidade, para que sua utilização comercial ou legal passasse a ser incontestável. Esta necessidade levou ao desenvolvimento de mecanismos de autenticação confiáveis, que disponibilizam dados importantes sobre os acessos realizados.

Este trabalho trata da utilização dos dados gerados pelos sistemas de autenticação para a finalidade de cobrança proporcional dos serviços. A utilização destes dados, especificamente para cobrança dos serviços prestados por uma operadora aos Provedores de Acesso à Internet, mostrou que esta utilização está longe de ser simples, apresentando resultados inconsistentes que permitiram cobrança apenas parcial dos serviços.

Neste trabalho foi desenvolvida uma metodologia para tratar estes dados, partindo da análise de amostras preliminares e do estudo de características técnicas e comportamentais dos três atores principais: cliente final, ISP e operadora, para tornar os dados mais confiáveis e permitir a cobrança correta dos serviços, inclusive na utilização simultânea de chaves de autenticação. O mecanismo desenvolvido para bloqueio de acessos indevidos por tentativas repetitivas também agregou uma interessante solução ao relacionamento com o usuário final, que auxilia a identificar o motivo da falha de acesso e facilita sua correção, reduzindo a necessidade de contato com a operadora ou com o ISP.

Conclui-se que as soluções desenvolvidas tornaram os dados mais confiáveis e permitiram a cobrança mais correta e abrangente dos serviços dos ISPs. Como resultados agregados, reduziu-se o volume de contatos dos usuários com a operadora, que em parte eram devidos à rejeição no processo de autenticação, e foram geradas informações significativas sobre o comportamento dos usuários para utilizações futuras.

**PALAVRAS CHAVES:**

Banda larga, ADSL, Contabilização, Faturamento, Página de Aviso, AAA, RADIUS.

**ABSTRACT**

It is clear and undeniable the growth in scope and importance of the Internet and the broadband solutions, that currently are the growth purpose in several countries around the world. The Internet widespread use creates the need for reliable remote access in terms of availability, integrity and traceability for its commercial use and greater relevance to become incontestable. This need has forced to the development of reliable authentication mechanisms, which provide important data about the accesses performed.

This work deals with the use of data generated by authentication systems for the purpose of proportional billing services. Using that data, specifically to billing services provided by a carrier to Internet Service Providers (ISPs), has showed that this use isn´t so easy, with several inconsistent results, that allowed only partial billing of services.

In this work is developed a methodology to process the data, starting in the analysis of preliminary results and the study of behavioral and technical characteristics of the three main actors, the end user, the ISP and the carrier, to turn the data more reliable and allow proper billing of the services, even when there is simultaneous use of access keys. The developed solutions have brought significant results for identification of users and to better control the use of the authentication and access keys. The mechanism designed to block unauthorized access also added an interesting solution to the relationship with the end user, because it helps to identify the reason for the failure of access and facilitate their correction, reducing the need to contact to the carrier or the ISP Call Centers.

The work development allows concluding that developed solutions have turned the data more reliable and have allowed the correct billing of services from ISPs as more accurately and comprehensively. As an aggregated results, reached also a reduction in the volume of users' contacts with the carrier’s call center, which in part were due to rejection in the authentication process, and were generated significant information about the behavior of users for future uses.

**KEYWORDS:**

Broadband, ADSL, Accounting, Billing, Warning Page, AAA, RADIUS.

**SUMÁRIO**

## LISTA DE FIGURAS

## LISTA DE TABELAS

## LISTA DE ACRÔNIMOS

| | |
|---|---|
| AAA | *Authentication, Authorization and Accounting* |
| ADSL | *Asymmetric Digital Subscriber Line* |
| ADSL2 | *Asymmetric Digital Subscriber Line 2* |
| ADSL2+ | *Asymmetric Digital Subscriber Line 2 Plus* |
| ANATEL | Agência Nacional de Telecomunicações |
| ANSI | *American National Standards Institute* |
| ATM | *Asynchronous Transfer Mode* |
| ATU-C | *ADSL Transceiver Unit - Central* |
| ATU-R | *ADSL Transceiver Unit - Remote* |
| BBS | *Bulletin Board System* |
| BMP | *Billing Mediation Plataform* |
| bps | *bits* por segundo |
| BRAS | *Broadband Remote Access Server* |
| CAP | *Carrier-less Amplitude/Phase* |
| CDR | *Call Detail Record* |
| CHAP | *Challenge-Handshake Authentication Protocol* |
| DHCP | *Dynamic Host Configuration Protocol* |
| DMT | *Discrete Multi-Tone* |
| DNS | *Domain Name System* |
| DSL | *Digital Subscriber Line* |
| DSLAM | *Digital Subscriber Line Access Multiplexer* |
| EHPT | *Ericsson Hewlett-Packard Telecommunications* |
| HTML | *HyperText Markup Language* |
| ETSI | *European Telecommunications Standarts Institute* |
| HP | *Hewlett-Packard* |
| GB | *Gigabyte* |
| HTTP | *Hypertext Transfer Protocol* |
| IETF | *Internet Engineering Task Force* |
| IP | *Internet Protocol* |

| | |
|---|---|
| I/O | *Input / Output* |
| ISP | *Internet Service Provider* |
| IBM | *International Business Machines* |
| ITU | *International Telecommunication Union* |
| kbps | *Kilobits* por segundo |
| LAN | *Local Area Network* |
| kHz | *Kilohertz* |
| LCP | *Link Control Protocol* |
| LES | Linhas em Serviço |
| LGT | Lei Geral de Telecomunicações |
| Mbps | *Megabits* por segundo |
| MD5 | *Message-Digest algorithm 5* |
| NAS | *Network Access Server* |
| MHz | *Megahertz* |
| NCP | *Network Control Protocol* |
| PAP | *Password Authentication Protocol* |
| PA | Posição de Atendimento |
| PGO | Plano Geral de Outorgas |
| PPP | *Point-to-Point Protocol* |
| PPPoA | *Point-to-Point Protocol over ATM* |
| PPPoE | *Point-to-Point Protocol over Ethernet* |
| PPPoEoA | *Point-to-Point Protocol over Ethernet over ATM* |
| PSI | Provedor de Serviços de Internet |
| QAM | *Quadrature Amplitude Modulation* |
| RADIUS | *Remote Authentication Dial-in User Service* |
| RAS | *Remote Access Server* |
| RFC | *Request for Comments* |
| RTPC | Rede de Telefônica Pública Comutada |
| SCI | Serviço de Conexão à Internet |
| SCM | Serviços de Comunicação Multimídia |
| SLDA | Serviço de Linha Dedicada Analógica |

| | |
|---|---|
| SVA | Serviço de Valor Adicionado |
| TAC | Termo de Ajuste de Conduta |
| TCP | *Transmission Control Protocol* |
| TCP/IP | *Transmission Control Protocol / Internet Protocol* |
| TMA | Tempo Médio de Atendimento |
| UDP | *User Datagram Protocol* |
| UF | Unidade da Federação |
| VPN | *Virtual Private Network* |
| WAN | *Wide Area Network* |
| WWW | *World Wide Web* |
| xDSL | Família DSL *(Digital Subscriber Line)* |

# 1 - INTRODUÇÃO

Ao longo dos últimos anos, a Internet vem deixando de ser uma ferramenta opcional, para se tornar, cada vez mais, uma necessidade. Uma quantidade significativa de serviços já é disponibilizada exclusivamente pelo acesso via Internet e, em muitos casos, embora não seja a opção exclusiva, é a mais rápida, mais fácil e de menor custo. A abrangência e a disponibilização de inúmeros serviços de significativa importância legal e financeira tornaram obrigatórias a segurança no acesso à Internet e a identificação de quem utilizou um recurso. O armazenamento e o processamento dos dados gerados pelos sistemas de controle de acesso passaram a ser a principal ferramenta para o conhecimento de quem efetivamente realizou uma atividade com o recurso em uma determinada data e hora.

No Brasil, em acordo recente de auto-regulamentação e TAC (Termo de Ajuste de Conduta) entre os principais Provedores de Acesso à Internet e operadoras de telecomunicações com o Ministério Público, foi fixado o prazo mínimo de 36 meses para armazenamento dos registros de acessos de usuários finais, para que estas informações possam ser utilizadas na identificação e responsabilização por transações ou por crimes realizados através da Internet. Quando trata-se de acesso remoto, estes registros são gerados pelos sistemas utilizados para autenticação de acesso dos usuários, que têm o papel principal de identificá-los e de gerar informações relativas ao histórico da conexão.

Neste novo cenário de crescimento da necessidade de controle da autenticação e da identificação de usuários que acessam a Internet, com a obrigatoriedade de armazenamento para utilização em questionamentos de finalidade legal, a qualidade e disponibilidade das informações dos registros de acesso tornaram-se preocupações em termos de investimento e custos, porém criaram algumas oportunidades de aprimorar as técnicas para a sua utilização, considerando o armazenamento por maior período e a consequente formação de massa crítica para a realização de pesquisas.

Os serviços de acesso á Internet são ferramentas essenciais e, como qualquer recurso, têm custos para sua disponibilização e utilização. A cobrança por estes serviços de

uma forma correta e proporcional ao seu uso, seja pela quantidade de usuários, por tempo ou por banda utilizada, é uma forma mais justa e universalizadora. Para que se possa cobrar pelos serviços de alguma destas formas é necessário que estes sejam medidos. Ao medir a utilização dos recursos, além das informações necessárias para a cobrança, muitas outras informações de comportamento de utilização dos recursos pelos clientes finais podem ser extraídas.

Este trabalho desenvolve o tema de uso das informações geradas pelos sistemas de AAA (*Authorization*, *Authentication* e *Accounting*), tratados na [RFC2903] e empregados para os diversos tipos de acesso remoto a redes, como fonte de informação para cobrança proporcional de serviços. Em particular a avaliação da qualidade e confiabilidade do uso das informações geradas pelo RADIUS (*Remote Authentication Dial In User Service*) tratado na [RFC2865] e sua contabilização, tratada na [RFC2866], amplamente utilizados para disponibilização de acesso à Internet pelas operadoras de telecomunicações e pelos Provedores de Serviços de Internet (PSI), também chamados no mercado de ISPs (*Internet Service Providers*), de provedores de acesso à Internet ou ainda, simplesmente de provedores.

Para abordar o tema, são analisadas as tecnologias de acesso à Internet de uso em massa, focando em serviços de banda larga sobre a rede de telefonia fixa (tecnologia xDSL) em ambientes de grande porte. Para este grupo de soluções de acesso, é proposta uma metodologia para melhora na qualidade dos dados gerados pelos sistemas de contabilização. São propostas também metodologias e soluções para o tratamento dos dados de forma a possibilitar o seu uso como fonte confiável de informações para o uso no faturamento proporcional de serviços e para embasar decisões gerenciais e técnicas, propiciando melhores escolhas no planejamento e na execução de manobras, implantações e definições de produtos e serviços.

Em cenários como os de uma pequena empresa ou de um pequeno ISP a utilização dos dados pode parecer simples, principalmente pelo número restrito de elementos envolvidos e pela utilização direta das ferramentas dos sistemas de AAA. Porém, em sistemas maiores, que são descentralizados ou que utilizam *proxys* e redirecionamento de

autenticação, esta utilização é dificultada pelo volume, pelas perdas na transmissão e pela necessidade de controle dos elementos envolvidos. Para sistemas de acesso à Internet utilizados em massa, a regulamentação de telecomunicações e o comportamento de alguns usuários finais também acrescentam pontos de dificuldades a serem tratados.

## 1.1 - CONTEXTUALIZAÇÃO

A prestação de serviços de acesso à Internet em par metálico utilizando tecnologia xDSL atinge atualmente um volume significativo de usuários finais no mundo todo. Esse volume e o seu crescimento levam à necessidade de criação de soluções específicas e mais robustas, escaláveis e confiáveis para o tratamento dos dados envolvidos e para a cobrança dos serviços. No Brasil, por questões regulatórias, o serviço de acesso à Internet não pode ser prestado diretamente ao usuário final pelas concessionárias de telecomunicações, por ser classificado como um SVA (Serviço de Valor Adicionado), vetado a este tipo de operadora de acordo com a LGT (Lei Geral de Telecomunicações).

Com a impossibilidade de prestação direta dos serviços pelas concessionárias, estes foram divididos em duas partes, sendo uma prestada aos ISPs e a outra, mais especificamente a referente ao serviço de conectividade ponto a ponto classificado como serviço de telecomunicações, prestada diretamente ao usuário final. O serviço de telecomunicações prestado aos ISPs, que é a disponibilização de infra-estrutura para conexão à Internet dos usuários finais, pode ser cobrado proporcionalmente a sua utilização, de acordo com os recursos alocados para cada cliente que tenha seu acesso permitido pelo provedor.

O crescimento da demanda pelos serviços de acesso em banda larga e o consequente aumento dos custos e da necessidade de investimentos a eles relacionados, somado ao cenário regulatório citado, levou a operadora pesquisada a decidir pela cobrança do serviço prestado aos ISPs a partir do ano de 2007. Para poder realizar a cobrança de forma proporcional a utilização média de recursos, passou a ser necessário medir a quantidade de *logins* de usuários finais que tiveram o acesso à Internet permitido

por cada ISP, considerando ainda a contabilização adicional no caso de uso por mais de 30 minutos de um mesmo *login* (nome de usuário) para mais de um acesso, tratada como uso simultâneo de *login*.

Para esta medição, são utilizados como base os dados gerados pelos sistemas de autenticação que, conforme abordado em [GRUSZYNSKI2008], geram informações confiáveis sobre a utilização dos recursos. Porém, a interpretação destas informações e o tratamento para sua contabilização são fatores determinantes para que os serviços sejam medidos e faturados de forma correta. A utilização direta dos dados, com o tratamento convencional de bilhetagem trouxe à tona uma série de dificuldades relacionadas às diferenças técnicas deste serviço em relação a outros serviços medidos da operadora.

A utilização dos sistemas de faturamento tradicionais da operadora facilitou o tratamento dos dados para viabilizar a identificação da existência de uso simultâneo e a segmentação por ISP e por estado, possibilitando gerar a cobrança correta de acordo com os impostos aplicados no local de prestação dos serviços. Porém estes sistemas não trataram corretamente a utilização simultânea de *logins*, que deve ser contabilizada quando as credenciais de acesso de um usuário são também utilizados por outro e não deve ser contabilizada quando o usuário, através de um mesmo acesso, gerar mais de uma autenticação (falso simultâneo).

O processamento dos dados de utilização gerados pelos sistemas de AAA da operadora, sem ter os tratamentos especiais relativos a algumas características técnicas do serviço e dos próprios dados, resultou em informações que continham algumas distorções, como, por exemplo, leituras maiores do que a base ativa (quantidade de usuários maior do que a possível, quando se contabilizava o uso simultâneo de *login*), contestações pelos provedores, que informavam que alguns *logins* relacionados como tendo o acesso permitido por eles não existiam ou estariam suspensos ou até desativados nas suas bases de dados. Em alguns casos de pequenos ISPs, foram constatadas ocorrências de quantidades medidas incompatíveis com a base de clientes do provedor, existindo até um caso isolado de medição de clientes quase três vezes superior aos *logins* ativos do ISP.

A necessidade de correção para tornar esta informação mais confiável forçou um estudo mais aprofundado dos sistemas envolvidos e uma investigação prévia das fontes de geração de distorções. Este estudo mostrou uma série de oportunidades de geração de informações que poderiam ser muito úteis para fins de definições gerenciais e operacionais, principalmente no desenvolvimento de produtos e serviços e também para a escolha dos melhores horários e datas para fazer manobras na rede.

Porém, nesta análise preliminar, ficou claro que o desenvolvimento das soluções para viabilizar a cobrança correta não seria simples, pois passaria por um estudo aprofundado dos sistemas de autenticação e autorização para entender como ocorriam acessos fora de padrões esperados, dos sistemas de geração de dados de contabilização, para ter a visão correta dos dados que estavam servindo de base para todo o processo e dos processos e sistemas envolvidos na geração da informação para o faturamento.

Além da complexidade técnica de abranger vários sistemas distintos, há também o fato dos sistemas envolvidos serem tratados por áreas distintas dentro da empresa. Por exemplo, os sistemas de AAA são desenvolvidos na Área de Planejamento de Redes e operados pela equipe do Centro de Gerência de Redes, os sistemas de mediação controlados pela área de Tecnologia da Informação e os sistemas de faturamento controlados e operados pela Área de Faturamento e Arrecadação da empresa.

## 1.2 - DEFINIÇÃO DO PROBLEMA

A medição dos serviços e a geração de dados para cobrança proporcional de serviços de acordo com seu uso foi inicialmente abordada em [GRUSZYNSKI2008], que desenvolveu uma solução escalável para contabilização dos serviços e a identificação dos usuários através de suas informações de acesso em ambientes de uso compartilhado de infra-estrutura também foi abordada anteriormente em [HENZ2008]. Porém, a utilização direta dos dados gerados pelos sistemas de contabilização do RADIUS sem um tratamento adequado mostrou-se não confiável, por apresentar resultados inconsistentes, como, por exemplo, leituras de usuários maiores do que o total de usuários cadastrados, ocorrência de

usuários informados pelos provedores como inexistentes, entre outros. Isto compromete os esforços para implantar a cobrança proporcional, tornando necessário o tratamento e a melhora da qualidade dos dados para viabilizar a solução de contabilização. Esse é um problema aberto, ao qual este trabalho se lança em busca da solução.

Pode-se então definir como problema principal a ser tratado, a existência de inconsistências nos resultados obtidos através os sistemas inicialmente desenvolvidos para o tratamento dos dados de AAA e para geração de informações utilizadas no faturamento de serviços de Banda Larga cobrados dos ISPs. Estas inconsistências comprometem a correta cobrança dos serviços e precisam ser corrigidas para torná-la mais precisa, aumentando a arrecadação e reduzindo a ocorrência de contestações pelos ISPs.

## 1.3 - OBJETIVOS

O objetivo principal deste trabalho é viabilizar a cobrança correta de serviços relacionados ao acesso Banda Larga em tecnologia ADSL dos ISPs, de acordo com a quantidade de clientes finais que tenham o acesso à Internet permitido por eles, utilizando como fonte os dados gerados pelos sistemas de autenticação baseados em RADIUS. O segundo objetivo é gerar informações sobre o comportamento dos clientes finais que possam ser confiavelmente utilizadas para tomadas de decisão, tanto comerciais como técnicas, e para definição de datas, horários e maneiras de realizar manobras de rede, como implantação e retiradas de serviços e alterações de *softwares* e equipamentos.

O trabalho se justifica pela importância de medir e cobrar corretamente pelos serviços prestados. A operadora pesquisada tem certificação em seus processos de faturamento e para cobrar este serviço precisa ter a certeza de que o faturamento está correto e corresponde à utilização de cada ISP. A cobrança traz resultados financeiros e a correta medição aumenta o faturamento e diminui as contestações e os desgastes com os clientes.

Outra justificativa é que, nas diversas manobras relacionadas à autenticação e à autorização de acesso, tanto da operadora como dos ISPs, ficou clara a necessidade de se ter mais informações sobre o comportamento real de uso dos clientes finais que pudessem direcionar as escolhas de datas, horários e maneiras que gerassem menores impactos para os clientes finais.

Adicionalmente, a cobrança pelos serviços, além dos resultados financeiros, faz com que o ISP tenha que aumentar seus controles sobre a autenticação e a autorização, melhorando a identificação dos clientes finais, necessária quando há algum tipo de investigação sobre atos praticados utilizando os recursos de acesso.

## 1.4 - METODOLOGIA DE TRABALHO

Para atingir os objetivos, inicialmente deve-se fazer uma análise aprofundada de todos os elementos envolvidos e uma pesquisa bibliográfica para o embasamento teórico necessário. Na sequência, deve ser feito um estudo da solução originalmente implantada, conhecendo toda a sua arquitetura e seu funcionamento. Com estas informações, devem ser analisados os dados preliminares para identificar as possíveis origens das distorções. A análise dos dados deve ser realizada através de indicadores que possibilitem a comparação antes e depois de ações corretivas ou da implantação de soluções para o problema.

Depois de identificadas as origens das distorções, devem ser analisadas as possíveis soluções, identificando as vantagens e desvantagens técnicas, comerciais, regulatórias e de relacionamento com os ISPs e com os clientes finais inerentes a cada uma, para que se possam escolher as melhores soluções a serem implantadas.

Com a definição das soluções, devem ser planejadas e executadas as implantações, seguindo os procedimentos da empresa, com as devidas autorizações, envolvimento e condução de algumas etapas pelas áreas responsáveis.

A hipótese primária a ser comprovada é de que é possível melhorar a qualidade dos dados para permitir a cobrança dos serviços dos ISPs referentes à utilização de todos os

seus clientes que fizerem conexões durante o período de medição de um mês. Outra hipótese a ser comprovada é de que é possível controlar o acesso com uso simultâneo de login e bloquear acesso indevido por *time out* sem prejudicar o acesso dos clientes que estão utilizando os serviços corretamente

Após a implantação das soluções, devem ser medidos os resultados a partir de indicadores apropriados, para que se possa ter a certeza se efetivamente obteve-se melhora da qualidade e da consistência das informações geradas e para comprovar ou não as hipóteses iniciais. A análise dos resultados obtidos e o conhecimento adquirido ao longo do desenvolvimento do trabalho devem levar as conclusões de sua validade e aplicabilidade e possibilitar ainda a indicação de trabalhos futuros.

## 1.5 - ESTRUTURA ORGANIZACIONAL DA DISSERTAÇÃO

Este trabalho está dividido em seis capítulos, estruturados da seguinte forma: No capítulo um, é apresentada a introdução ao tema, sua contextualização, a definição e delimitação do problema e a metodologia utilizada para o desenvolvimento do trabalho. No capítulo dois realiza-se uma revisão dos sistemas de acesso à Internet de interesse deste trabalho, principalmente tecnologias de acesso utilizando rede metálica, e dos sistemas de autenticação para acesso remoto. No capítulo três descreve-se o sistema inicialmente desenvolvido para geração de dados de contabilização e os resultados preliminares. No capítulo quatro, apresenta-se a solução técnica proposta para a correção dos sistemas e dos processos envolvidos, contemplando o detalhamento do projeto e das avaliações e metodologias de implantação das soluções. Já no capítulo cinco, são apresentados os resultados obtidos com a implantação das soluções; por fim, no capítulo seis, tecem-se as conclusões e as propostas de continuidade deste trabalho.

Adicionalmente, no final deste trabalho, há um apêndice com informações geradas no decorrer do seu desenvolvimento e que tem relevância para o uso gerencial e em programações de manutenções ou manobras que envolvem os sistemas de autenticação e autorização.

# 2 - REFERENCIAL TEÓRICO

Como referencial teórico, para melhor entendimento e para servir como base de conhecimento para o desenvolvimento do tema, dois assuntos principais são abordados neste capítulo. O primeiro deles é o acesso remoto, focando em suas tecnologias, principalmente as relacionadas à banda larga e nos aspectos regulatórios da prestação do serviço no Brasil. O segundo é o conhecimento dos sistemas de autenticação remotos, com suas características e soluções para atender as demandas técnicas, comerciais e regulatórias da prestação de serviços de acesso em banda larga.

## 2.1 - ACESSO REMOTO A REDES

O uso de acesso remoto às redes tem crescido rapidamente com a evolução das tecnologias e com a redução dos custos, tanto dos equipamentos e *softwares* de acesso como dos de uso dos clientes. Os equipamentos de uso doméstico têm cada vez maior capacidade de processamento e armazenamento e a disponibilização dos serviços para utilização remota impulsiona ainda mais a necessidade deste acesso.

No histórico das redes de computadores, a interligação de um ponto fora do ambiente da rede principal, por qualquer meio de acesso, pode ser classificado como um acesso remoto. Com a criação da rede Internet, os acessos remotos tornaram-se muito mais importantes e necessários para o desenvolvimento das atividades nos cenários de competitividade e globalização da economia que cresceram junto à evolução da rede.

A estrutura inicial da Internet comercial, formada pela interconexão de diversas redes distintas, já tinha o objetivo de permitir que usuários de uma rede pudessem acessar a informações de outras, ou da grande rede WWW (*World Wide Web*). Para chegar à rede Internet, o usuário precisava no mínimo ter o acesso a uma destas redes, o que era feito através de acesso remoto.

### 2.1.1 - Histórico do acesso à Internet

No histórico do crescimento da disseminação e da importância que a rede Internet alcançou atualmente, e também no que se vislumbra como seu futuro, o acesso remoto tem um papel extremamente importante.

Assim que a Internet passou a ser uma rede aberta com acesso comercial, surgiram os Provedores de Acesso à Internet, que foram os primeiros a tratar o acesso remoto à Internet como um negócio, onde o objetivo era a conexão de um usuário final a grande rede. Cada provedor passou a ser mais um nó desta rede, o que permite que um cliente conectado remotamente a ele tenha acesso à grande rede Internet.

O uso das redes das operadoras de telecomunicações, inicialmente para o acesso discado e posteriormente para conexão através de tecnologias de acesso em banda larga (xDSL, *Cable Modem*, Celulares etc.), também tornou o negócio extremamente atrativo para estas empresas.

Cabe destacar que as tecnologias de acesso remoto tratadas neste trabalho são utilizadas para conexão à Internet, embora parte da metodologia possa também ser utilizada para aplicação em acessos à redes privadas ou *intranets*.

### 2.1.2 - Tecnologias de acesso remoto à Internet em rede de par metálico

Desde a criação da rede Internet os acessos remotos tem evoluído rapidamente, muitas tecnologias são agregadas para facilitar este acesso. Dentro deste trabalho serão analisadas as tecnologias de acesso à Internet de uso doméstico, ou de uso em massa, que utilizam o par metálico das redes de telefonia fixa, como meio de transmissão.

Nas próximas seções são apresentadas as principais características técnicas e operacionais destas tecnologias de acesso, sendo mais detalhada a tecnologia ADSL, que é a tecnologia utilizada para os acessos em banda larga tratados dentro deste trabalho.

### 2.1.3 - Acesso discado (*Dial-up*)

O acesso de usuários remotos, principalmente de uso doméstico, iniciou no Brasil nos meados de 1995 com o surgimento dos primeiros ISPs, que baseavam a venda de seus serviços na conexão discada através de linhas telefônicas convencionais, com as chamadas atendidas em *modem*s externos ou equipamentos RAS para entroncamento digital, como mostrado na Figura 2.1.

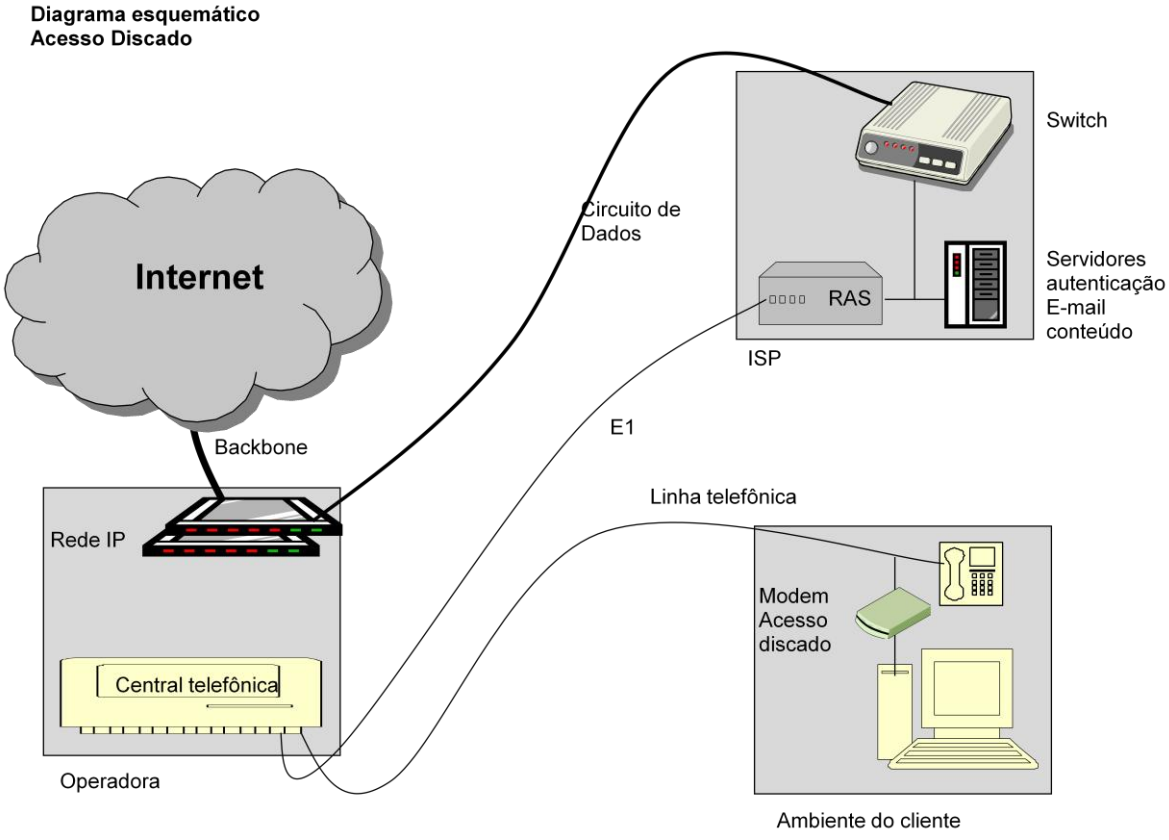



Figura 2.1: Diagrama esquemático do acesso discado convencional [DANTEa].

Embora seja a forma pioneira de acesso à Internet e ainda continue em uso, este sistema de conexão está perdendo cada vez mais seu espaço, principalmente devido à massificação dos acessos em banda larga nas suas diversas tecnologias. Os principais motivos que levam a substituição da tecnologia de acesso pelos usuários são a velocidade, que no acesso discado é normalmente limitada a 56 kbps (excluindo sistemas de compressão), e a diferença de ter a possibilidade de ficar conectado de forma permanente, visto que as tecnologias de banda larga normalmente disponibilizam a conexão em tempo integral (*always on).*

A conexão discada continua sendo a alternativa para os lugares onde ainda não há a disponibilidade de banda larga, para os casos onde o usuário tem pouco volume de utilização e para os casos em que o usuário aceita trafegar em baixas velocidades para ter menor custo ou para não ter custo fixo. É também a principal alternativa de acesso às redes que não estão conectadas à Internet, como BBS (*Bulletin Board System*), redes de pagamento e *intranets* de empresas.

A velocidade de acesso neste tipo de conexão sempre foi um ponto crítico, a evolução das tecnologias de *modem*s para conexão e os sistemas de compressão, como listado na Tabela 2.1, vêm melhorando a experiência do usuário neste sentido. Soluções como agregar mais de uma linha telefônica para conexão em um mesmo computador utilizando *softwares* específicos para esta finalidade e dobrando assim a capacidade e o uso de hardwares de compressão de dados são eficientes, porém acabam muitas vezes elevando o custo e, quando comparadas as soluções de banda larga, passam a não ser a melhor alternativa.

Tabela 2.1: Tecnologias de acesso discado e taxas de transmissão

| **Tecnologia de conexão para acesso discado** | **Taxa de transmissão** | |
|---|---|---|
| *Modem* 110 *baud* | 110 | bps |
| *Modem* 300 (300 *baud*) (Bell 103 or V.21) | 300 | bps |
| *Modem* 1.200 (600 *baud*) (Bell 212A or V.22) | 1.2 | kbps |
| *Modem* 2.400 (600 *baud*) (V.22bis) | 2.4 | kbps |
| *Modem* 2.400 (1.200 *baud*) (V.26bis) | 2.4 | kbps |
| *Modem* 4.800 (1.600 *baud*) (V.27ter) | 4.8 | kbps |
| *Modem* 9.600 (2.400 *baud*) (V.32) | 9.6 | kbps |
| *Modem* 14.4 (2.400 *baud*) (V.32bis) | 14.4 | kbps |
| *Modem* 28.8 (3.200 *baud*) (V.34) | 28.8 | kbps |
| *Modem* 33.6 (3.429 *baud*) (V.34) | 33.6 | kbps |
| *Modem* 56k (8.000/3429 *baud*) (V.90) | 33.6 a 56 | kbps |
| *Modem* 56k (8.000/8.000 *baud*) (V.92) | 48 a 56 | kbps |
| Compressão por hardware (variável) (V.90/V.42bis) | 56 a 220 | kbps |
| Compressão por hardware (variável) (V.92/V.44) | 56 a 320 | kbps |
| Compressão do servidor para web (variável) (Netscape ISP) | 100 a 1.000 | kbps |

Nesta solução, a necessidade de autenticação e controle de acesso fica somente a cargo do ISP, visto que a chamada é atendida em seu equipamento. Os processos de autenticação e de autorização são realizados utilizando a comunicação direta entre o equipamento de acesso do usuário final e os sistemas de AAA no próprio ISP.

O crescimento da demanda e a necessidade de capilaridade para o atendimento em outros municípios com ligação local, fizeram com que os ISPs passassem a ter filiais em outras localidades. Estas filiais podiam ser interligadas por uma rede privada ou ter sua própria conexão com a Internet. Porém, a manutenção de operações com muitas filiais gera grandes custos e passou a ser um limitante para o acesso em municípios menores.

A solução inicial desenvolvida para que os ISPs não necessitassem ter filiais em cada município foi a instalação de equipamentos em uma modalidade desenvolvida em [DANTEb], que ficou conhecida no mercado como *housing*, ou seja, os equipamentos dos ISPs instalados dentro dos prédios onde estão as centrais das telefônicas das operadoras, como visto na Figura 2.2.

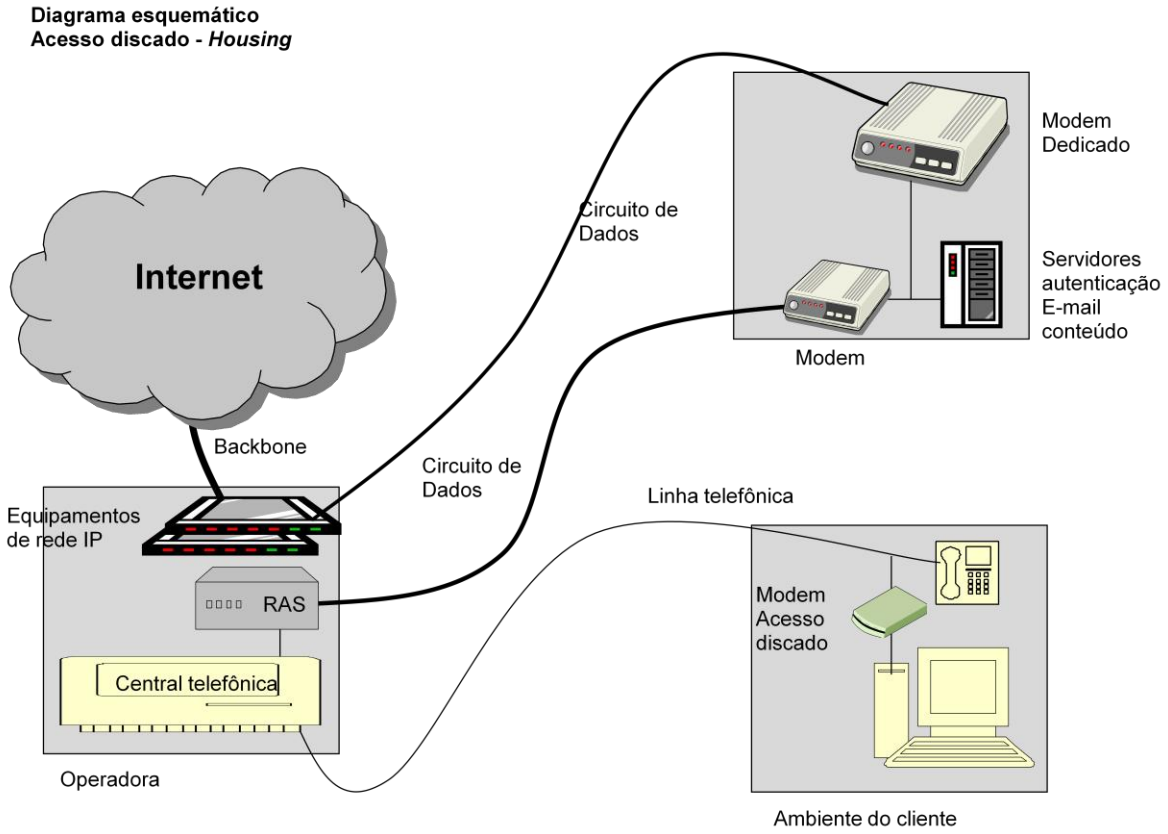



Figura 2.2: Diagrama esquemático do acesso discado em *Housing*

Porém, a oferta de solução de hospedagem do equipamento tem algumas dificuldades operacionais, como o acesso de terceiros ao ambiente da operadora e a ociosidade de portas, principalmente porque os equipamentos utilizados operavam com troncos digitais (E1s), disponibilizando no mínimo o equivalente a 30 linhas de acesso, sendo que a necessidade do ISP em localidades menores era de apenas algumas portas. Como evolução natural, as operadoras começaram a disponibilizar sistemas de acesso discado em equipamentos próprios, com a possibilidade de o ISP contratar somente a quantidade de portas que julgasse necessário. Esta modalidade foi disponibilizada no mercado brasileiro com o nome comercial de Dialnet e tem seu diagrama esquemático mostrado na Figura 2.3.

Neste modelo, como o equipamento que atende a chamada é da operadora, o redirecionamento do pacote de autenticação e autorização se torna necessário, já que a requisição de acesso deve ser encaminhada para o ISP que é escolhido de acordo número discado pelo cliente final ou com domínio que compõe o *login* deste cliente.

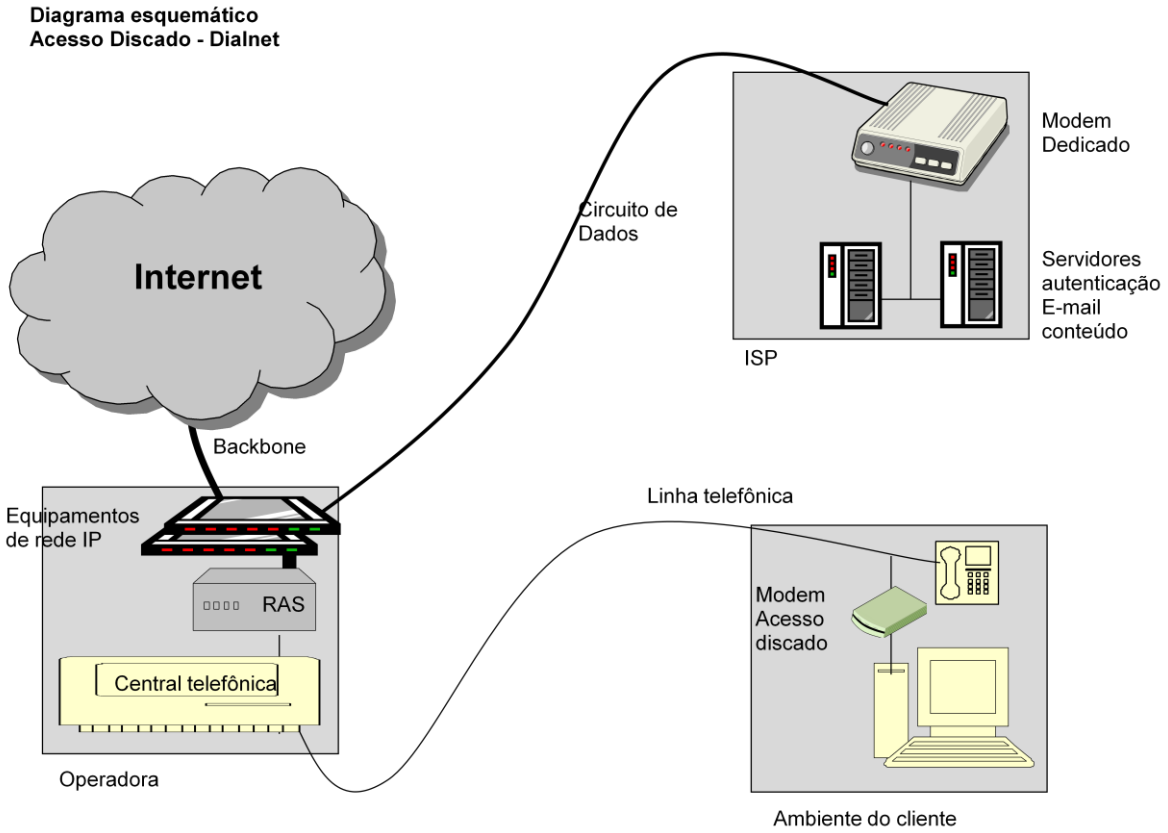



Figura 2.3: Diagrama esquemático do acesso discado utilizando portas Dialnet [DANTEa]

A solução de acesso com *Dialnet* utiliza equipamentos de propriedade da operadora para fazer a conexão com o equipamento do usuário final, neste caso, fazendo uma analogia aos sistemas de banda larga, quando a saída para a Internet do acesso *Dialnet* também é provida pela operadora, resulta em uma solução de redirecionamento da autenticação e autorização, semelhante à adotada nos sistemas de acesso banda larga ADSL que serão vistos a seguir.

### 2.1.4 - Acesso em banda larga utilizando par metálico

A utilização do par metálico para conexão dedicada iniciou-se com *modem*s analógicos que atingiam apenas baixas velocidades. Esta conexão ficou conhecida no mercado como Serviço de Linha Dedicada Analógica (SLDA) e alcançava velocidades semelhantes àquelas das conexões discadas, porém, com a vantagem de ser uma conexão dedicada e com custo menor do que pagar pela ligação telefônica da conexão discada durante longos períodos de utilização.

Para alcançar maiores taxas de transmissão é necessário utilizar melhor a banda disponível no meio de acesso. As novas tecnologias de acesso utilizando par metálico passaram então a ocupar faixas de frequências superiores às alocadas para comunicação de voz. As soluções desenvolvidas podem inclusive utilizar as faixas de freqüência separadamente, o que permite o uso do par para transporte de voz convencional concomitantemente ao uso para transmissão de dados.

#### 2.1.4.1 - Tecnologia DSL

A tecnologia denominada DSL (*Digital Subscriber Line)* é formada por um grupo de soluções técnicas implantadas para melhor utilização do par metálico. Está baseada principalmente na utilização das frequências acima da faixa dedicada para comunicação de voz, que é formada pelos primeiros 4 kHz, e no uso de técnicas de modulação DMT *(Discrete Multi-Tone)* e CAP *(Carrier-less Amplitude/Phase)*, para maior proteção em relação ao ruído.

A modulação DMT, definida como padrão pela ANSI (*American National Standards Institute*) na recomendação T1.413 e pela ETSI (*European Telecommunications Standarts Institute*), é uma técnica de modulação onde os dados transmitidos são distribuídos em diversas portadoras que utilizam individualmente a modulação analógica QAM (*Quadrature Amplitude Modulation*). A modulação CAP utiliza outra versão de modulação QAM, na qual os dados modulam apenas uma portadora, que depois é

transmitida na linha telefônica. Antes da transmissão, a portadora é suprimida e, depois, é reconstruída na recepção.

### 2.1.4.2 - Tecnologia ADSL

A tecnologia ADSL (*Asymmetric Digital Subscriber Line*) utiliza a linha telefônica convencional (analógica) para transportar dados em frequência diferente da utilizada pela comunicação de voz, que tipicamente é de 0 a 4 kHz. As frequências utilizadas para *upstream* (envio de dados do cliente remoto para a rede) e *downstream* (recepção de dados vindos da rede para o cliente remoto) são divididas conforme representado a seguir:

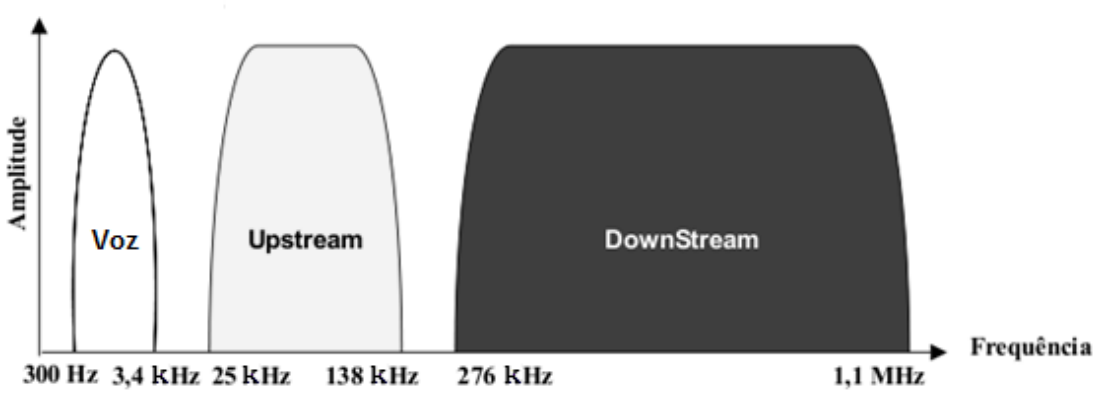



Figura 2.4: Uso do domínio Frequência pelo ADSL

Para a separação das faixas de frequências utilizadas para dados e para voz, é recomendado o uso de um filtro, conhecido no mercado pelo nome *splitter*. É um elemento passivo que permite a passagem apenas das frequências necessárias para cada uma de suas saídas, evitando a interferência das transmissões de voz e de dados nos equipamentos subsequentes que não as utilizam.

A Figura 2.5 a seguir mostra a conexão esquemática dos equipamentos da conexão ADSL. Nesta figura, pode ser observada a utilização da infra-estrutura da operadora para quase toda a prestação do serviço. Nesta modalidade o ISP fica encarregado apenas do processo de autenticação, utilizado para controlar a permissão do acesso dos clientes finais à Internet.

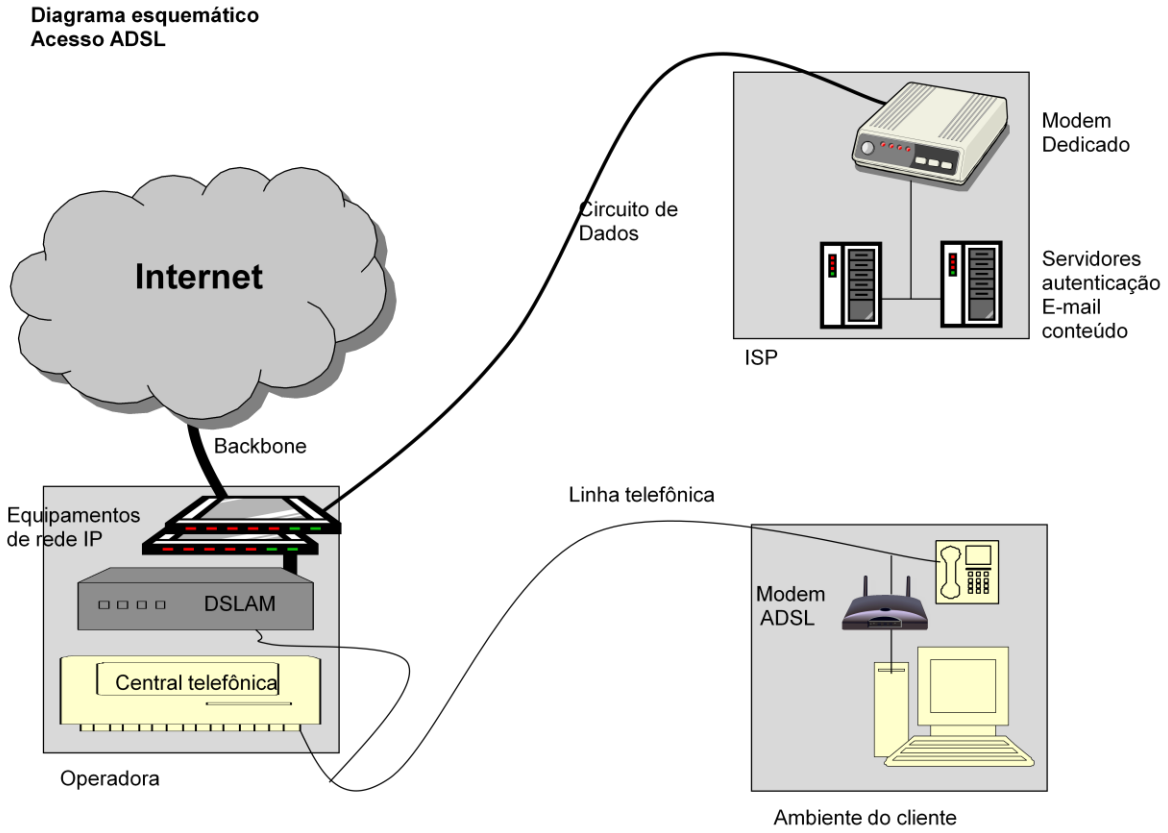



Figura 2.5: Diagrama esquemático de conexão ADSL

Pelo diagrama, partindo do cliente em relação à rede Internet, após a estação de trabalho, há a conexão desta com o *modem*, que por sua vez é conectado ao par metálico. Este par metálico está conectado dentro do ambiente da central telefônica da operadora a uma porta de um DSLAM (*Digital Subscriber Line Access Multiplexer*), que também está conectado a rede IP da operadora. Não há a necessidade de uma conexão física entre o

sistema e o ISP, já que a saída para Internet ocorre pela autorização da conexão lógica do cliente à rede IP da operadora, que por sua vez está conectada à rede Internet. Desta forma, na maioria dos casos, a conexão do provedor é somente com a rede Internet e a comunicação de mensagens de autenticação e contabilização ocorre exclusivamente sobre esta rede, conforme pode ser visto na Figura 2.6.

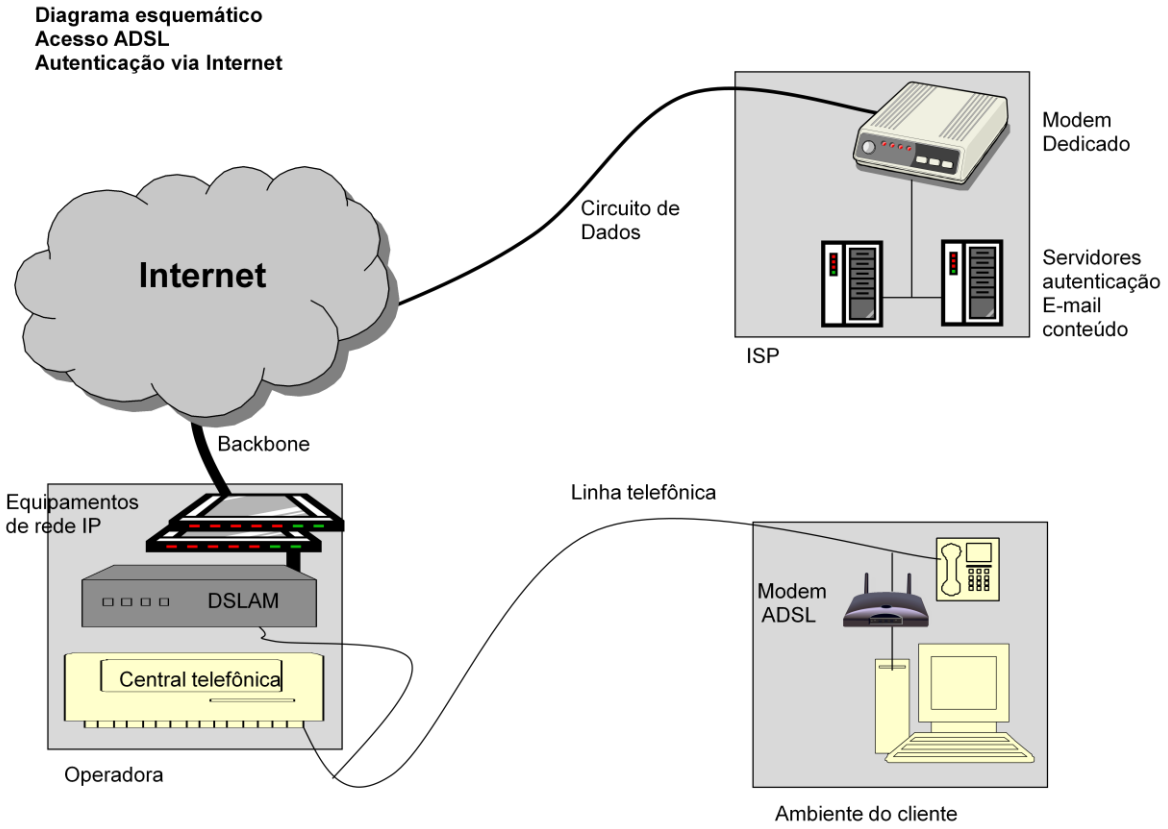



Figura 2.6: Diagrama esquemático da conexão ADSL com autenticação no ISP via Internet

Desde a sua criação, a tecnologia ADSL vem sofrendo evoluções que permitem cada vez maior disponibilidade de banda e menor sensibilidade ao ruído, além de utilização de frequências mais altas sobre o par metálico. As principais mudanças estão relacionadas com as taxas máximas atingidas para *upstream* e *downstream*, conforme descrito na Tabela

2.2, que mostra o nome de mercado das tecnologias, as normas que as definem e as suas taxas máximas.

Tabela 2.2: Padrões do ADSL (Fontes: ANSI e ITU listadas na tabela)

| Nome no mercado | ANSI/ITU | Taxa máxima downstream | Taxa máxima upstream |
|---|---|---|---|
| ADSL | ANSI T1.413-1998 *Issue* 2 | 8 Mbps | 1 Mbps |
| ADSL - G.DMT | ITU G.992.1 | 12 Mbps | 1,3 Mbps |
| ADSL linha convencional (POTS) | ITU G.992.1 | 12 Mbps | 1,3 Mbps |
| ADSL Linha digital (ISDN) - IDSL | ITU G.992.1 | 12 Mbps | 1,8 Mbps |
| ADSL Lite (G.Lite) | ITU G.992.2 | 1,5 Mbps | 512 Kbps |
| ADSL2 | ITU G.992.3/4 e G.992.3 anexo J | 12 Mbps | 1 Mbps |
| RE-ADSL | ITU G.992.3 anexo L | 5 Mbps | 1 Mbps |
| ADSL2+ | ITU G.992.5 | 24 Mbps | 1 Mbps |
| ADSL2+M | ITU G.992.5 anexo M | 24 Mbps | 3,5 Mbps |

O crescente interesse pela velocidade no acesso, principalmente no *download* realizado pelos usuários finais, pressiona os fornecedores de serviços a utilizar de tecnologias que permitam maiores bandas. Considerando que em termos de custos dos equipamentos praticamente não há variação, o fato de ter maior capacidade de transmissão fez com que o ADSL2+ passasse a ser quase um padrão para novas instalações de soluções xDSL (família *Digital Subscriber Line*) de massa no Brasil. Consequentemente, algumas operadoras retiraram das suas listas de equipamentos homologados aqueles baseados na tecnologia ADSL definida na [ITUG992.1], ficando homologados apenas os compatíveis com a tecnologia descrita na [ITUG992.5].

Para alcançar maiores taxas de transmissão, a tecnologia ADSL2+ apresenta uma maior ocupação no domínio da frequência conforme visto na Figura 2.7, utilizando frequências mais altas que o ADSL original.

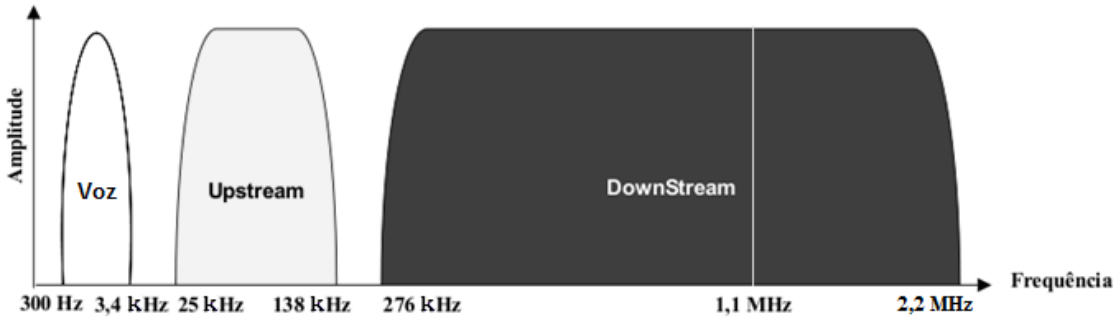



Figura 2.7: ADSL2+ no domínio da frequência

Na Figura 2.7, pode-se notar que a faixa de frequência ocupada para *downstream*, que no ADSL e no ADSL2 vai até a frequência de 1,104 MHz, no caso do ADSL2+ ocupa até os 2,208 MHz. O uso de uma banda maior proporciona taxas de *downstream* maiores, porém, como o foco da tecnologia é o acesso assimétrico, no ADSL2+ não se alterou a faixa de frequências do upstream, o que ocorreu apenas na tecnologia descrita no Anexo M da [ITUG992.5], que modificou a divisão entre as frequências de *upstream* e *downstream* para os 276 kHz, conforme visto na Tabela 2.3.

Tabela 2.3: Frequências e taxas das principais tecnologias de ADSL

| TIPO | Definido em | início do Upstream | Divisão Upstream / Downstream | Final do Downstream | Taxa de upload atingida | Taxa de download atingida |
|---|---|---|---|---|---|---|
| ADSL 1 | G.992.1 | 25 kHz | 138 kHz | 1.1 MHz | 1 Mbps | 8 Mbps |
| ADSL 2 | G.992.3 | 25 kHz | 138 kHz | 1.1 MHz | 1 Mbps | 12 Mbps |
| ADSL 2+ | G.992.5 | 25 kHz | 138 kHz | 2.2 MHz | 1 Mbps | 24 Mbps |
| ADSL 2+M | G.992.5 An. M | 25 kHz | 276 kHz | 2.2 MHz | 3,5 Mbps | 24 Mbps |

### 2.1.5 - Principais elementos da rede de acesso ADSL

A rede que permite a comunicação de um cliente utilizando a tecnologia ADSL é composta de vários elementos conectados fisicamente. Conforme representado na Figura

2.8, os principais elementos, partindo do ambiente do cliente, são o seu terminal de acesso (normalmente um computador, mas pode ser notebook, celular etc.), o seu *modem*, a sua linha telefônica, o DSLAM onde a linha telefônica é conectada fisicamente, o NAS, que está conectado fisicamente aos DSLAMs e a rede IP do provedor o serviço, que por sua vez possui elementos que comunicam com a rede acessada (por exemplo o roteador representado na figura).

O NAS também é responsável por completar a conexão lógica com o equipamento do cliente e pela comunicação com os sistemas de autenticação para permitir o acesso do cliente a rede acessada, que tipicamente é a rede Internet, mas poderia ser uma rede privada (*intranet*).

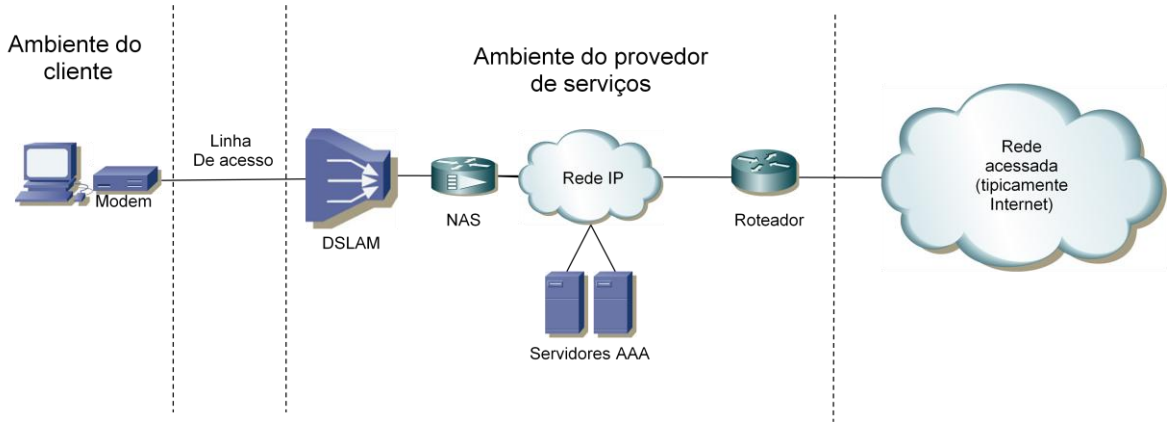



Figura 2.8: Principais elementos da rede ADSL – adaptado de [GRUSZYNSKI2008]

Cada um dos elementos citados é indispensável no processo de acesso à rede. A indisponibilidade ou falha dos equipamentos, ou dos *softwares* destes equipamentos, pode interferir na qualidade e disponibilidade da conexão, tornando então todos os elementos críticos também quando se trata o objetivo de medir os serviços. Para poder tratar corretamente as dificuldades que podem ocorrer na medição dos serviços devido à interferência dos elementos, cabe detalhar um pouco as suas características de funcionamento.

2.1.5.1 - Computador do usuário final

O computador do usuário final e sua rede interna são elementos muito importantes na análise do sistema de acesso, visto que alterações nos aplicativos do computador do cliente podem impactar o processo de autenticação e de acesso, ainda mais quando associados ao comportamento e conhecimento deste cliente, que muitas vezes, principalmente em casos de uso doméstico, não tem muita experiência na área tecnológica.

Muitos aplicativos são desenvolvidos para o acesso ou para o uso remoto através da conexão com a rede Internet, sendo necessária a conexão ativa para seu funcionamento. Neste trabalho são analisados principalmente aqueles que têm impacto direto na percepção do cliente de que sua conexão está funcionando, destacando o sistema operacional, principalmente devido aos seus controles de rede e sistema de resolução de nomes DNS (*Domain Name System*), o discador (quando usado), o navegador e outros aplicativos que utilizam serviços remotos na Internet, como correio eletrônico (*e-mail*), *softwares* de bate-papo *on-line (chat*) etc.

**Sistema Operacional**

O Sistema operacional, além de ser o ambiente de trabalho no qual todas as aplicações são sobrepostas também é quem faz os controles dos dispositivos de entrada e saída (I/O) do equipamento. Os dispositivos e sistemas de controle de rede são componentes críticos no acesso à Internet, sendo assim, além do *hardware* de acesso, os seus *drivers* e a sua interação com o sistema operacional também são indispensáveis para a operação. O sistema operacional faz também o controle da rede TCP/IP no equipamento e é nele que são configurados os parâmetros deste acesso. Na configuração da rede TCP/IP devem ser destacadas as configurações de endereçamento IP do equipamento e de endereço IP dos servidores de DNS, que são significativas para este trabalho.

Normalmente a configuração padrão (*default*) de acesso é ter os endereços do equipamento e do servidor de DNS atribuídos remotamente, ou seja, um equipamento externo informará via DHCP estes endereços. A mudança destes parâmetros deve ocorrer

somente em aplicações específicas, onde o endereço do equipamento deve permanecer fixo perante a rede, principalmente porque os sistemas de acesso remoto providos pelos ISPs e operadoras são compartilhados e exigem justamente o contrário, pois precisam que o endereço IP possa ser utilizado por vários equipamentos ao longo do tempo para o melhor aproveitamento destes recursos.

Cabe ressaltar que, em topologias de acesso utilizando *gateways* de saída, como no caso da utilização de *modem* como *router,* que será detalhada adiante, quem recebe o endereço IP de acesso remoto é este dispositivo, ficando a rede interna independente deste endereçamento. Nesta situação, a configuração do protocolo TCP/IP no Sistema Operacional deve ser realizada para a conexão com esta rede, podendo ser com endereços IP fixos ou dinâmicos, independente das características do acesso remoto. No caso de *modem* utilizado como *router,* existem configurações distintas para LAN (*Local Area Network*), que é a rede interna onde o computador, *modem* e demais equipamentos locais estão conectados e WAN (*Wide Area Network*), que é a rede de acesso remoto, na qual o *modem* se conecta através da rede de telefônica.

No terminal de acesso (normalmente o computador do cliente final) a definição do endereço servidor de DNS determina apenas se este será procurado em um endereço IP fixo ou se este endereço será atribuído remotamente. Porém, sabendo-se que o endereço do servidor de DNS pode ser alterado e que já existem iniciativas de redirecionamento com fins publicitários, deve ser considerado também que o uso de um endereço de servidor de DNS fixo e escolhido pelo cliente pode passar a ser mais comum. Desta forma, soluções que sejam baseadas em alteração no servidor de DNS podem estar mais sujeitas a falhas, ou pelo menos não serem tão abrangentes.

Deve também ser considerado que toda a cadeia de resolução de nomes, desde o sistema operacional até os servidores raiz, trabalha com *caches* e em esquema de hierarquia, ou seja, quando um servidor de nomes não tem a informação do endereço IP de um determinado domínio, ele questiona a sua instância superior e assim sucessivamente. Porém, em cada um destes servidores pode já haver a informação de endereçamento ou do caminho para buscar este endereçamento, não sendo necessário chegar até o topo da

hierarquia. Embora este sistema de consulta seja mais eficiente e rápido, também incorre na necessidade de atualização da informação quando há alguma alteração. Devido a esta característica, uma alteração de endereçamento executada pode demorar a ser refletida em toda rede, dependendo do tempo de retenção da informação nos *caches* da sequência de servidores.

## Discador

Uma das formas de conexão à Internet utilizando *modem* ADSL é a sua configuração apenas como *bridge*. Neste caso, o *modem* faz o seu papel de modulador/demodulador e fica transparente a conexão lógica da rede. Para esta opção é necessário que o computador ou dispositivo de acesso do cliente tenha um aplicativo capaz de estabelecer a conexão lógica com o NAS (*Network Access Server*). Este aplicativo é conhecido no mercado de telecomunicações como Discador ADSL e é desenvolvido e fornecido por algumas empresas especializadas diretamente para os integradores, que montam um *kit* de acesso para ser entregue junto ao *modem*.

Na operadora pesquisada o *software* aplicativo certificado para ser integrado aos *modem*s para que estes possam ser considerados homologados é produzido pela empresa Lightcomm e pode ser reconhecido nas formas presentes na Figura 2.9 que apresenta as telas de abertura do discador original e Novo Discador Turbo.


Tela inicial do
Discador Turbo Lightcomm

Tela inicial do Novo
Discador Turbo Lightcomm

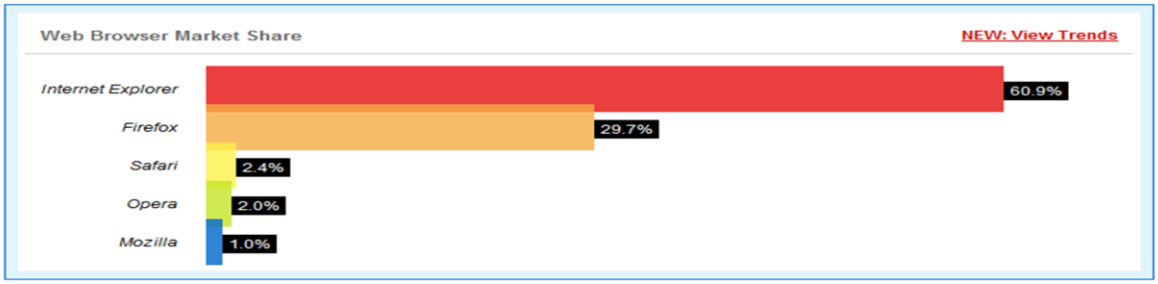
Figura 2.9: Telas do Discador Turbo e do Novo Discador Turbo [LIGHTCOMM]

**Navegador**

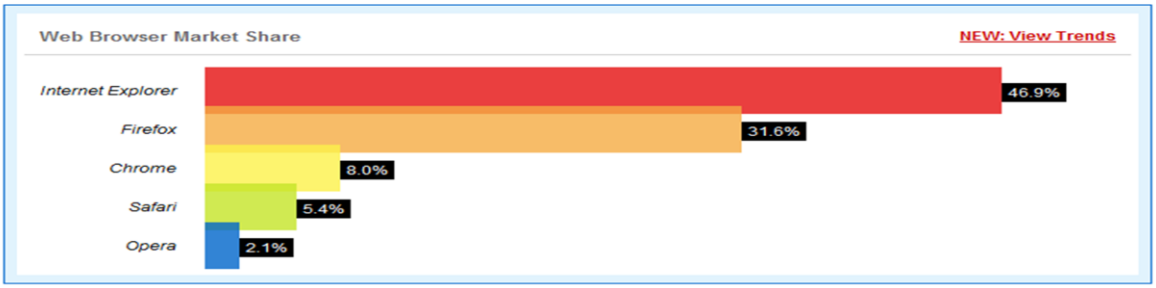
A forma mais comum de utilização e, para muitos, o objetivo principal do acesso à Internet é a navegação nas inúmeras páginas disponibilizadas na rede, que atualmente possuem uma quantidade enorme de serviços que são prestados utilizando como interface o navegador. O navegadores tiveram, assim como os demais elementos, uma história de grande evolução desde o início da Internet, recebendo uma série evoluções e programação e de aplicativos adicionais (*plug-ins*) que permitem maior interatividade e a interpretação de linguagens de programação, como Java, Flash, DirectX etc.

A história dos navegadores teve como um dos seus primeiros representantes o Mosaic, no início da década de noventa, porém foi o Netscape que assumiu o mercado em 1995 quando a Internet começou a ter destaque no Brasil. A partir do ano de 1995 em diante, iniciou-se uma batalha de navegadores com o lançamento pela Microsoft do Internet Explorer, distribuído de forma gratuita, que no final da década assumiu a liderança isolada. Porém, outros navegadores foram lançados depois e começaram a conquistar a preferência de uso, ou por terem mais flexibilidade ou por não estarem vinculados apenas ao sistema operacional Windows. Entre eles o Firefox, que tem crescido seu *share* e já atingiu 35% do mercado, como pode ser visto na Figura 2.10, que mostra o *share* dos navegadores de abril de 2010, de acordo com o *site* [W3COUNTER].

Há uma importância adicional no navegador utilizado pelo cliente, principalmente por ele ser a principal interface dele com a Internet e de ser a principal forma de comunicação entre ele e a rede em que ele está se conectando. Qualquer solução de comunicação desenvolvida deve considerar que sua apresentação deve ocorrer pelo menos nos cinco principais navegadores citados. Na Figura 2.10 pode-se também notar que o Chrome, navegador lançado pelo Google, em abril de 2010 ocupa a terceira posição no *ranking* e que o Firefox também teve crescimento expressivo no período, com redução significativa na preferência pelo Internet Explorer.




*Market Share* de Navegadores em julho de 2008




*Market Share* de navegadores em abril de 2010

Figura 2.10: *Share* de navegadores em julho/2008 e abril/2010 [W3COUNTER]

**Outros aplicativos que utilizam o acesso remoto**

Além do navegador, muitas vezes os usuários finais se conectam à Internet para utilizar outros serviços, como correio eletrônico (*e-mail*), aplicativos para conversa *on-line* (*chat*) ou outros. Há uma preocupação neste caso, pois o uso da comunicação pelo navegador pode não ser eficiente se o cliente simplesmente não utilizá-lo, principalmente porque estes aplicativos não têm a finalidade de apresentar conteúdo diretamente, dificultando então o seu uso para comunicação direta (*on-line*).

### 2.1.5.2 - *Modem* ADSL

O *modem* (*modulator/demodulator*) é o equipamento que permite a comunicação utilizando a tecnologia DSL que fica no lado do usuário e que fecha a comunicação com

outro elemento modulador/demodulador, tipicamente presente no DSLAM (*Digital Subscriber Line Access Multiplexer*), que fica no lado do fornecedor do serviço.

O *modem* ADSL tem suas características técnicas e operacionais definidas na [ITUG992.1], a qual o denomina de ATU-R (*ADSL Transceiver Unit – Remote*) e define suas características principais. Complementarmente, as características dos *modems* que utilizam a tecnologia ADSL2 estão definidas na [ITUG992.3] e dos que utilizam a tecnologia ADSL2+ na [ITUG992.5].

Um ponto importante em relação à utilização do *modem* ADSL é que ele normalmente permite duas configurações distintas: como roteador (*router)* ou como *bridge*. No uso como roteador, o próprio *modem* tem a função de encaminhar as credenciais de acesso no processo de autenticação, recebe o endereço IP remoto da conexão ADSL e funciona como roteador para o restante da rede. Na configuração como *bridge*, o *modem* atua como uma ponte para os demais elementos da rede, a conexão lógica é feita normalmente entre o computador remoto e o NAS (*Network Access Server)*, sendo necessário então que este computador tenha um *software* para esta finalidade. Este *software*, embora não tenha nada a ver com acesso discado, é normalmente denominado "discador" da conexão ADSL. A Figura 2.11 ilustra as formas de conexões lógicas utilizadas no acesso ADSL.

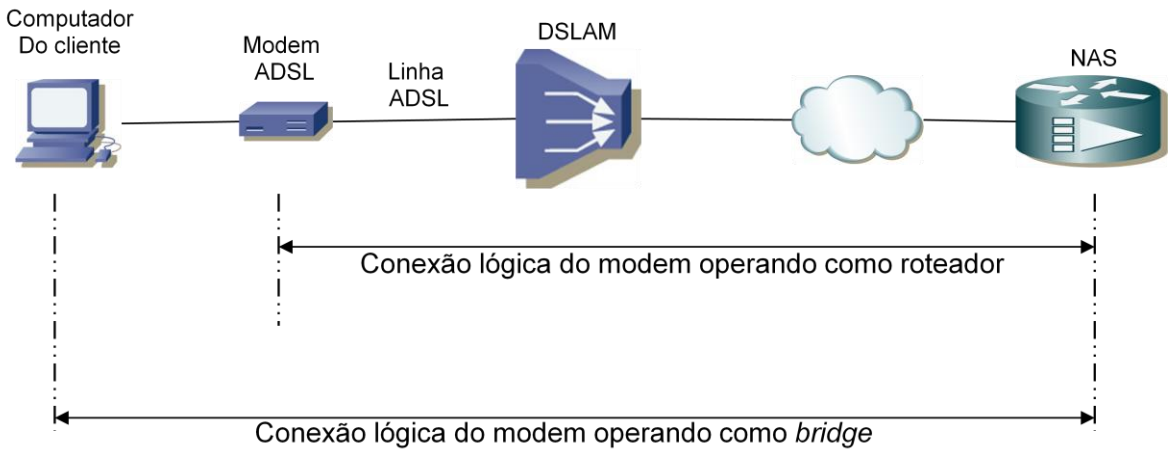



Figura 2.11: Conexões lógicas: *modem* ADSL como *router* ou *bridge* [GRUSZYNSKI2008]

É importante destacar que, na maioria das instalações domésticas é utilizado também um filtro de linha que permite a separação das frequências que são destinadas ao *modem* e ao aparelho de telefone convencional. Este elemento, embora passivo e muitas vezes não analisado, é peça importante dentro da conexão, seu mau funcionamento pode, além de interromper a conectividade, torná-la intermitente ou reduzir sua qualidade. Embora a utilização do filtro seja recomendada pelas operadoras, muitas vezes ele não é utilizado na instalação, principalmente quando o aparelho de telefone é *wireless*, já que este acaba filtrando o sinal que é transmitido ao *handset* e, normalmente, não deixa passar ruídos fora da faixa de freqüência utilizada para voz que sejam perceptíveis ao usuário final.

As operadoras de telecomunicações normalmente têm processos de homologação ou certificação dos *modem*s para a recomendação de utilização em suas redes. Nesta homologação, além dos testes de características de conectividade, são ajustados os parâmetros de funcionamento, customizadas as configurações e, quando necessário, adaptado o discador para que o conjunto funcione de forma correta. Outro ponto importante, considerando ser uma utilização em massa e que portanto tem volume de usuários finais significativos, é que o uso de *modems* homologados facilita a preparação dos atendentes dos *Call Centers*, tanto da operadora como dos ISPs, para que eles possam disponibilizar suporte à sua configuração.

Para as análises deste trabalho serão considerados os *modems* homologados pela operadora pesquisada, que estão listados na Tabela 2.4 e com imagens na Figura 2.12. Embora outros *modem*s possam ser utilizados, a grande maioria dos clientes finais opta por pela aquisição dos *modems* homologados, que são distribuídos com o *kit* de acesso (filtros, cabos e *software* discador) específico para uso com a operadora. Os próprios ISPs preferem distribuir este tipo de *modem* quando fazem campanhas comerciais que incluam o seu fornecimento.

Tabela 2.4: Lista de *modem*s certificados pela Brasil Telecom [BTSA]

| Fornecedor | Modelo | Interface | Modo Operação | Certificação |
|---|---|---|---|---|
| D-Link | D-Link DSL 500B | Ethernet | Router/Bridge | Vigente |
| DSLink | DSLink 260E | Ethernet | Router/Bridge | Vigente |
| Intelbrás | GKM 1200e | Ethernet | Router/Bridge | Vigente |
| Siemens | Siemens SpeedStream 4200 | Ethernet | Router/Bridge | Vigente |
| Thomson | Thomson Speed Touch 510v6 | Ethernet | Router/Bridge | Vigente |

Estes *modem*s, representados na da Figura 2.12, são os mais utilizados atualmente em acessos ADSL da operadora pesquisada e podem ser facilmente reconhecidos nas instalações dos acessos residenciais, nas empresas e nas demais organizações que utilizam produtos de tecnologia ADSL para seu acesso à Internet.


Figura 2.12: *Modem*s certificados pela Brasil Telecom (fonte: sites dos fabricantes)

### 2.1.5.3 - DSLAM

O equipamento DSLAM (*Digital Subscriber Line Access Multiplexer*) faz o papel do *modem* para receber as conexões de uma forma agrupada no lado do prestador de serviços, como pode ser visto na Figura 2.13. Este equipamento é tratado na [ITUG992.1], onde é denominado ATU-C (*ADSL Tranceiver Unit – Central*).

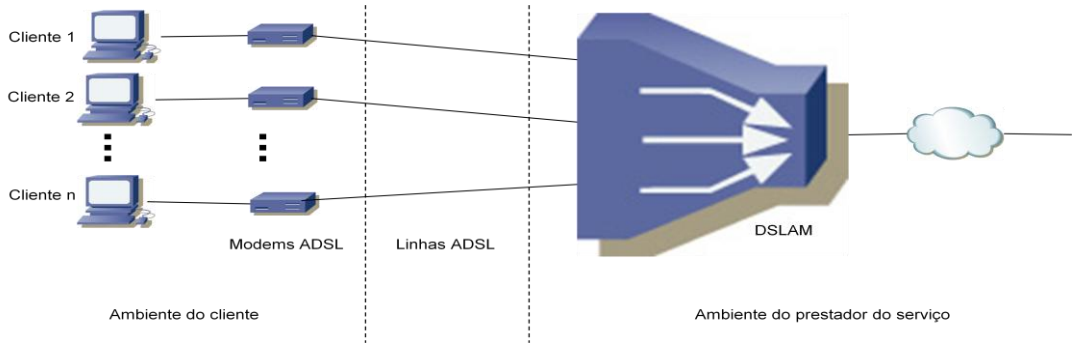



Figura 2.13: Agrupamento de conexões com o DSLAM [GRUSZYNSKI2008]

Atualmente existem diversos modelos destes equipamentos fornecidos por vários fabricantes, principalmente em função do aumento significativo na concorrência entre eles nos últimos anos. Na operadora pesquisada, apenas para exemplificar quanto a modelos e quantidades, segundo [HENZ2008] em 2008 estavam ativos os equipamentos listados na Tabela 2.5. O quadro permite uma noção de volumes comparados com a disponibilização de portas, embora as quantidades, marcas e modelos sejam dinâmicos.

Tabela 2.5: Quantidades de DSLAMs e portas em 2008 na Brasil Telecom [HENZ2008]

| | FABRICANTE | MODELO | TOTAL | TOTAL DE PORTAS |
|---|---|---|---|---|
| DSLAMs ATM | ALCATEL | 7300 ASAM | 926 | 178.254 |
| | CISCO | 6120 | 109 | 12.984 |
| | INOVIA | | 88 | 17.403 |
| | LUCENT | STINGER | 644 | 440.581 |
| | HUAWEI | MA5100 - MA5103 - MA5105 | 2.726 | 459.270 |
| | Total | | | 1.108.492 |

| | FABRICANTE | MODELO | TOTAL | TOTAL DE PORTAS |
|---|---|---|---|---|
| DSLAMs Ethernet | HUAWEI | MA5100 - MA5300 - MA5600 | 1.824 | 514.151 |
| | ERICSSON | HM 130 | 462 | 89.297 |
| | UTSTARTCOM | B820 - B1000 | 1.955 | 494.592 |
| | SIEMENS | HiX5635 | 263 | 102.484 |
| | Total | | | 1.200.524 |

| | | | | |
|---|---|---|---|---|
| DSLAMs | Total | | | 2.309.016 |

#### 2.1.5.4 - NAS

O NAS (*Network Access Servers*), também denominado BRAS (*Broadband Remote Access Server*), conforme visto na Figura 2.11, é o equipamento responsável por estabelecer a conexão lógica com o equipamento do cliente. Este equipamento é conhecido como agregador ou terminador, pela sua característica de ser o ponto de terminação da rede de acesso, formada dos DSLAMs até os equipamentos dos usuários finais e de conexão à rede de comunicação de dados da operadora ou prestador do serviço.

No início da instalação das redes de conexão para ADSL, muitas delas foram implantadas utilizando ATM (*Asynchronous Transfer Mode)* para conexão dos DSLAMs com os NAS. Porém no processo de evolução das redes e com o crescimento dos volumes, a tecnologia Ethernet passou a ser a mais largamente utilizada. Mesmo assim, em muitas redes ainda é comum ter os dois tipos de redes operando simultaneamente, embora em segmentos de rede distintos.

A utilização de ATM ou Ethernet na conexão do DSLAM com o NAS tem interferência significativa no processo de conexão do usuário final, principalmente porque o enlace é fechado entre o equipamento do cliente e o NAS utilizando o PPP (*Point-to-Point Protocol*) nesta conexão lógica, e este protocolo precisa ser escolhido de acordo com a rede onde o DSLAM está conectado, podendo então ser PPPoA (*Point-to-Point Protocol over ATM*), PPPoE (*Point-to-Point Protocol over Ethernet*) ou ainda PPPoEoA (*Point-to-Point Protocol over Ethernet over ATM*).

Na configuração dos parâmetros de acesso, seja no *modem* ou no discador, esta informação é muito importante. A conexão do cliente só será completada se este parâmetro for definido de acordo com a tecnologia de rede utilizada.

Como exemplos de agregadores utilizados na rede da operadora pesquisada, os equipamentos na Figura 2.14, modelo ERX 1440, com capacidade de atender até 48.000 acessos simultâneos e o equipamento da Cisco Systems, modelo 10008, com capacidade de 61.500 acessos simultâneos [MIERCOM].


Figura 2.14: Exemplos de NAS (BRAS) (Fontes: [JUNIPER] e [CISCO])

Para efeitos de análise quanto à quantidade de equipamentos afetados em casos de manobras que necessitem de configuração nos agregadores, no primeiro semestre de 2008, segundo [HENZ2008], havia 63 equipamentos BRAS ativos na operadora pesquisada, conforme listado na Tabela 2.6.

Tabela 2.6: Quantidade e modelos de BRAS ativos no 1º semestre de 2008 [HENZ2008].

| FABRICANTE | MODELO | TOTAL | TOTAL DE PORTAS |
|---|---|---|---|
| CISCO | 10008 | 43 | 1.579.127 |
| JUNIPER | ERX | 19 | 729.889 |
| Total | | 63 | 2.309.016 |

### 2.1.6 - Aspectos legais do uso de ISP para o acesso à Internet

Conforme citado no capítulo 1, no Brasil, de acordo com a atual regulamentação, o serviço de acesso à Internet não pode ser prestado diretamente ao usuário final pelas concessionárias. Esta restrição deve-se a dois fatores distintos da regulamentação, que associados tornam obrigatório, no caso das concessionárias, que o serviço seja prestado por um ISP, que faz a autenticação e determina a permissão do acesso à Internet de um usuário final.

O primeiro fator está na Norma 4, publicada em 1995 pela [ANATEL], que tem as seguintes definições:

> a. “Internet: nome genérico que designa o conjunto de redes, os meios de transmissão e comutação, roteadores, equipamentos e protocolos necessários à comunicação entre computadores, bem como o "*software*" e os dados contidos nestes computadores”;
>
> b. “Serviço de Valor Adicionado: serviço que acrescenta a uma rede preexistente de um serviço de telecomunicações, meios ou recursos que criam novas utilidades específicas, ou novas atividades produtivas, relacionadas com o acesso, armazenamento, movimentação e recuperação de informações”;
>
> c. “Serviço de Conexão à Internet (SCI): nome genérico que designa Serviço de Valor Adicionado que possibilita o acesso à Internet a Usuários e Provedores de Serviços de Informações.”

Por estas definições, o serviço de acesso à Internet foi classificado como um SVA (Serviço de valor Adicionado), embora esta definição tenha acontecido em 1995, quando no Brasil ainda se estava na fase inicial da disponibilização dos serviços de conexão à Internet, o que leva a crer que toda a norma foi baseada na conexão à Internet utilizando o acesso discado via RTPC (Rede de Telefonia Pública Comutada).

O segundo fator está na [LGT] (Lei Geral de Telecomunicações), Lei Nº 9472, de 16 de julho de 1997, que no seu artigo 61 define que:

> “Art. 61. Serviço de valor adicionado é a atividade que acrescenta, a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde,

> novas utilidades relacionadas ao acesso, armazenamento, apresentação, movimentação ou recuperação de informações.
>
> § 1º Serviço de valor adicionado não constitui serviço de telecomunicações, classificando-se seu provedor como usuário do serviço de telecomunicações que lhe dá suporte, com os direitos e deveres inerentes a essa condição.
>
> § 2° É assegurado aos interessados o uso das redes de serviços de telecomunicações para prestação de serviços de valor adicionado, cabendo à Agência, para assegurar esse direito, regular os condicionamentos, assim como o relacionamento entre aqueles e as prestadoras de serviço de telecomunicações."

Adicionalmente, o Artigo 86 da mesma lei, inclui a seguinte limitação:

> "Art. 86. A concessão somente poderá ser outorgada a empresa constituída segundo as leis brasileiras, com sede e administração no País, criada para explorar exclusivamente os serviços de telecomunicações objeto da concessão."

A associação dos pontos expostos acima levou a conclusão de que as empresas Concessionárias de Serviços Públicos de Telecomunicações não pudessem prestar os SVA (Serviço de valor Adicionado), entre os quais ficou classificado o SCI (Serviço de Conexão à Internet). Esta conclusão direcionou também as soluções técnicas necessárias para que este serviço seja então prestado por um ISP (*Internet Service Provider*) ou que tenha a sua permissão para a liberação deste acesso.

### 2.1.7 - Histórico de implantação do acesso ADSL na Operadora

Na operadora pesquisada, a oferta de soluções de acesso à Internet utilizando tecnologia ADSL teve sua história iniciada no ano de 1999, com o lançamento do projeto piloto, que foi lançado apenas em duas localidades, em Curitiba-PR e Brasília-DF. Nesta fase do projeto ainda não havia a disponibilização comercial. Este período, além de ser o marco do início da disponibilização dos serviços em tecnologia ADSL, foi utilizado para fazer os primeiros ajustes na rede e nos sistemas da operadora. O lançamento comercial foi somente em junho de 2000, quando, embora continuasse apenas nas duas localidades, atingiu a marca de 10.500 acessos.

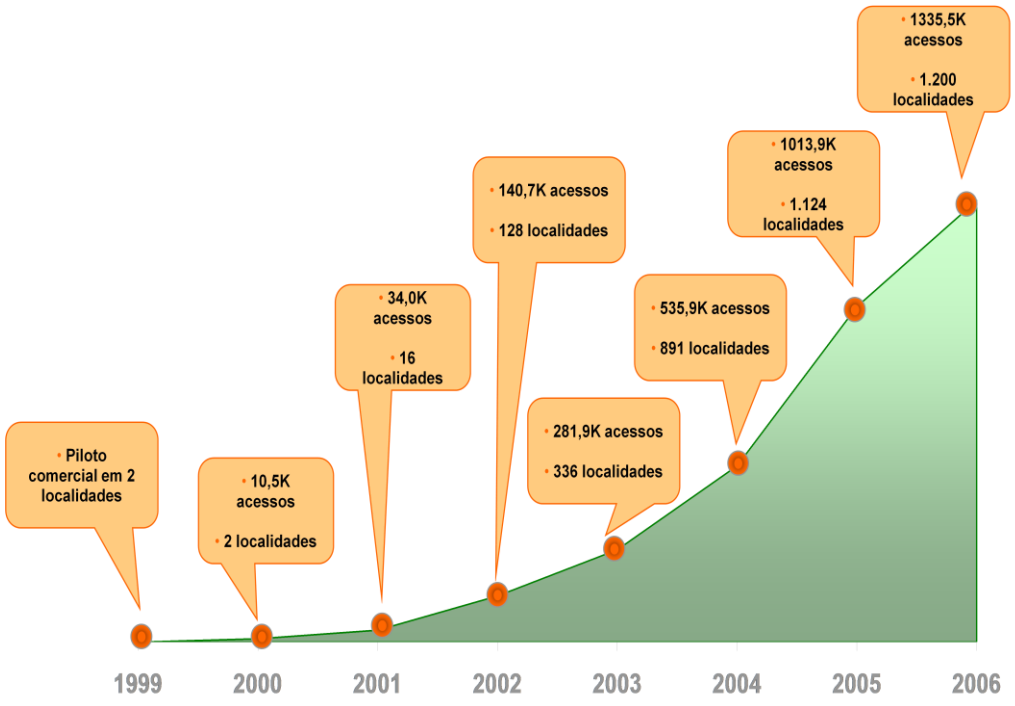



Figura 2.15: Evolução da planta de acessos ADSL na rede da Brasil Telecom [DANTEc]

A Figura 2.15 mostra a evolução do crescimento dos acessos ADSL até 2006, ano em que a quantidade de clientes de ADSL superou a quantidade de clientes que se conectavam via acesso discado de terminais distintos, como pode ser visto na Figura 2.16.

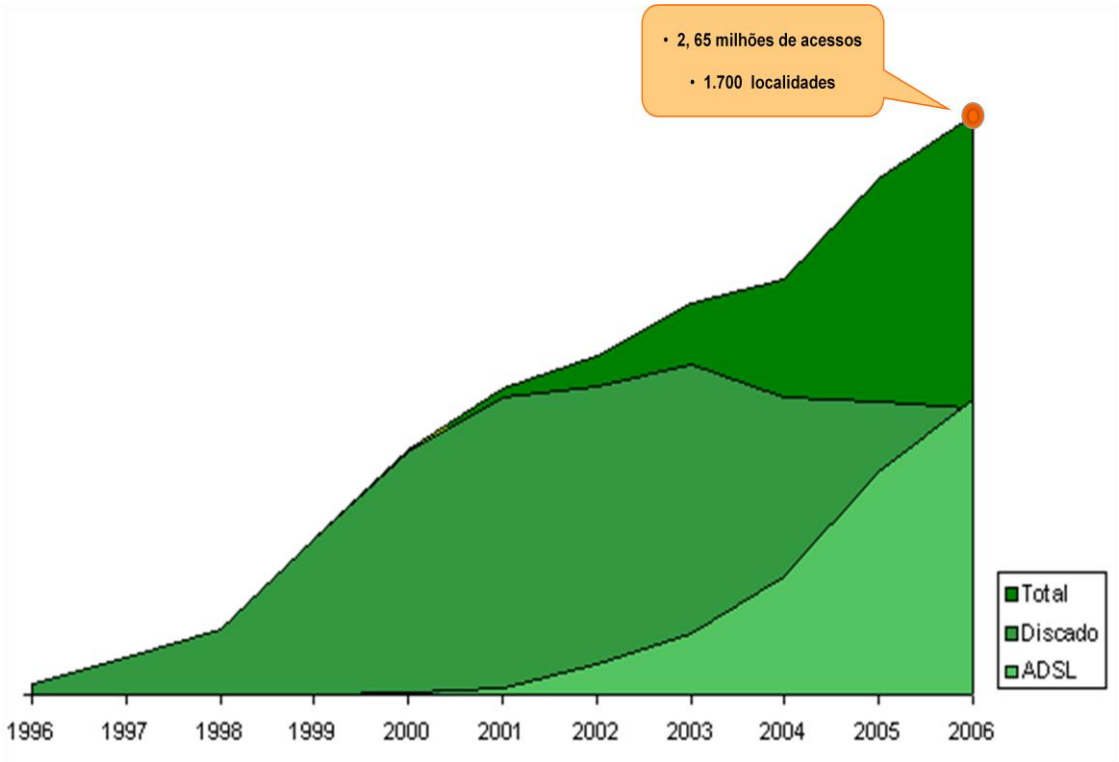



Figura 2.16: Evolução dos acessos discado e banda larga ADSL [DANTEc]

No final do primeiro trimestre de 2010, a Brasil Telecom S/A publicou em seu site de relacionamento com investidores [BTSAa], dentro de seus relatórios de informações de resultados, que havia atingido a marca de 1958 mil acessos ADSL, com uma penetração ADSL/LES (Linhas com ADSL sobre a quantidade total de Linhas Em Serviço) de 25,6%.

## 2.2 - SISTEMAS DE AUTENTICAÇÃO REMOTA

O termo “compartilhamento”, de acordo com o [DICIONÁRIO], significa “tomar parte em”, ou “participar de”, desta forma, o compartilhamento de infra-estruturas, no acesso remoto às redes indica que um usuário final pode participar do uso de uma infra-estrutura para acessar uma rede. Isto significa que, pelo menos em parte do tempo, este usuário final estará utilizando o recurso. Como este uso não é dedicado, se não houvesse um processo de identificação e autorização de acesso o uso da infra-estrutura não seria controlado, causando dificuldades de dimensionamento e de reconhecimento dos usuários. No processo normal de utilização dos recursos, convencionalmente o usuário final deve informar suas credenciais de acesso para que seja autenticado e receba a permissão de utilização do recurso e do acesso a rede.

A utilização dos recursos e das redes pode ser contabilizada com a finalidade de cobrança pelos serviços ou simplesmente para identificação do usuário final que acessou a rede em uma data e hora específica, para fins de auditoria e segurança.

A utilização dos recursos de acesso remoto de forma compartilhada e controlada pressupõe então três processos básicos: a autenticação, a autorização e a contabilização. Estes processos são conhecidos também pelo acrônimo AAA (*Authentication, Authorization and Accounting*) e compõe os sistemas principais de identificação dos usuários finais que utilizam os recursos e acessam remotamente uma rede.

Em sistemas simples, com volumes de acesso não expressivos e com os servidores e equipamentos de acesso no mesmo ambiente, como os sistemas utilizados nos pequenos ISPs ou em acessos remotos à intranet de pequenas empresas, a instalação direta de um servidor RADIUS normalmente já é o suficiente para resolver os problemas de AAA. Porém, a evolução dos meios de acesso e a massificação de sua utilização, principalmente com a finalidade de acesso à Internet, geraram a necessidade de consolidação das infra-estruturas de autenticação. Para tratar grandes volumes de usuários distribuídos geograficamente que conectam-se às redes várias vezes ao dia, os sistemas de AAA precisam ter robustez e serem escaláveis e confiáveis [GRUSZYNSKI2008].

### 2.2.1 - Autenticação, Autorização e Contabilização (*AAA*)

Os três "As", ou no inglês "*Triple-A*" são utilizados para descrever o conjunto de sistemas que são essenciais para o controle do acesso remoto, podendo estar presentes em sistemas centralizados ou distribuídos, em um ou diversos servidores e sistemas. Detalhando um pouco mais, cada um dos "As" tem uma finalidade específica conforme descrito a seguir.

#### 2.2.1.1 - Authentication (Autenticação)

O primeiro A, relativo à autenticação, é a parte do sistema que é responsável pela identificação do usuário, ou seja, determina pelos parâmetros recebidos se o usuário tem as credenciais corretas e pode ser "reconhecido". Esta etapa normalmente é considerada necessária para que se possa passar às demais.

A principal confrontação neste caso é a apresentação de códigos de acesso e senhas que sejam pré-cadastrados e aceitos como a sendo a correta identificação do usuário, como, por exemplo, a informação de seu "nome de usuário", de seu número de telefone ou a localidade de origem de sua conexão (que podem estar inclusos na requisição) e sua senha. Há também a possibilidade da autenticação ser através de parâmetros técnicos, como identificação sistêmica da porta física do equipamento de acesso ou outro parâmetro que possa ser associado a um determinado usuário.

No acesso remoto, o processo de autenticação envolve troca de mensagens entre os elementos envolvidos, que segundo [NAKHJIRI2005] pode ser implantada em dois modelos, um com duas e outro com três partes envolvidas

No modelo com duas partes, as características são semelhantes ao modelo cliente-servidor, embora em alguns casos a autenticação seja mútua, na maioria das vezes é feita apenas a autenticação do cliente. No caso de autenticação em sistemas ADSL, para utilização deste modelo é necessário que o NAS tenha uma base de dados de informações dos usuários finais para a autenticação. A Figura 2.17 mostra o funcionamento neste caso,

onde o cliente envia suas credenciais diretamente para o NAS, que faz o papel de autenticação sem a dependência de outros elementos.


Figura 2.17: Modelo de autenticação com apenas duas partes

Um modelo de duas partes pode ser a solução para o caso de pequenas quantidades de agregadores e de usuários finais, porém é pouco prático para volumes maiores, uma vez que as alterações das credenciais dos usuários finais precisam ser feitas diretamente nas bases dos NAS envolvidos. Quanto maior a quantidade de clientes e de agregadores envolvidos, maior é a complexidade para sua operação, já que envolve uma grande quantidade de entrada e saída de usuários finais (cadastros e exclusões de *logins*) e alterações de senhas, que precisam ser feitas na base de dados do agregador responsável pela conexão do cliente afetado.

Em um sistema completo de uma grande operadora, conforme pode ser visto em [BTSAa] para operadora pesquisada, são milhões de usuários finais. Estes usuários finais são conectados a alguns milhares de DSLAM, conforme visto Tabela 2.5, que são conectados a dezenas de agregadores, conforme visto na

Tabela 2.6, com os processos de autenticação centralizados em algumas unidades de conjuntos de servidores de AAA, conforme [GRUSZYNSKI2008].

Para que o problema seja reduzido, o caminho é ter a autenticação centralizada, ou concentrada em um terceiro elemento, que facilita o processo de armazenamento e alteração das credencias dos usuários finais, deixando de ser necessária a presença de informações dos clientes finais nos agregadores. Neste caso utiliza-se um modelo de três

partes, conforme visto na Figura 2.18, que representa os três elementos básicos e a forma da comunicação entre eles.


Figura 2.18: Modelo de autenticação com três partes

Cabe ainda ressaltar que, mesmo em um modelo onde há o redirecionamento da autenticação para um ambiente externo, como no caso de autenticação feita em um ISP, permanece o modelo de três elementos, visto que os servidores no ISP também são classificados como o mesmo elemento "Servidor AAA", como observado na Figura 2.19.

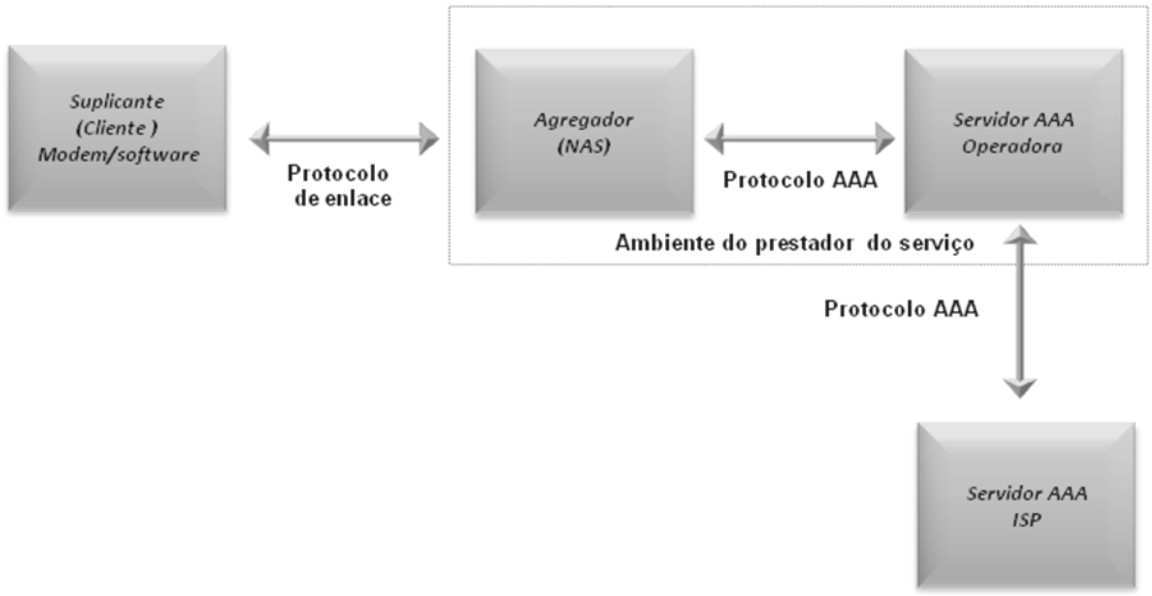



Figura 2.19: Modelo de autenticação com redirecionamento da autenticação

Estando validadas as credenciais, o cliente já está autenticado, porém a simples autenticação não é o suficiente para que o acesso seja liberado. A autenticação do cliente normalmente é fator necessário para que na etapa seguinte ele seja autorizado a acessar a rede, o que é feito pelo sistema de autorização conforme será visto a seguir.

#### 2.2.1.2 - *Authorization* (Autorização)

O Segundo A, relativo à autorização, é a parte do sistema responsável pela liberação do acesso do usuário à rede. Esta etapa está associada à permissão do usuário e atribuição de seu endereço de comunicação com o restante da rede (normalmente endereço IP). Nesta etapa podem ser adicionados atributos para direcioná-lo à conexão de maneiras diferenciadas.

É importante destacar que nos casos onde a Requisição de Acesso é redirecionada para um ISP, este passa ser o responsável pela permissão, que ocorre através da resposta que pode ser um aceite (*Access-Accept*) ou uma rejeição (*Access-Reject*). Neste caso a autorização de acesso é realizada, de acordo com resposta recebida e com parâmetros pré-estabelecidos, pela operadora.

É correto interpretar que o processo de autorização deva ocorrer depois da autenticação e seja feito apenas para os casos de êxito na validação das credenciais. Porém, na prática, isto pode não acontecer. Os parâmetros adotados para o tratamento da autorização podem ser modificados para que, caso não seja devolvida uma resposta positiva na autenticação, o cliente seja tratado de forma diferente, ou seja, pode ser autorizado a acessar a rede ou até autorizado apenas a acessar uma rede de “boas vindas” ou de oferta de serviços. O tratamento de volumes elevados de usuários finais, as dificuldades de fazer o atendimento individual de troca de senhas ou de *logins* e os casos de possíveis falhas nos sistemas de autenticação, ou da comunicação entre eles, também podem ser fatores críticos na decisão do que fazer no caso de não ter uma resposta positiva à requisição de autenticação.

Conforme levantamento interno da operadora, alguns ISPs adotam políticas diferentes do padrão para o caso de erro de *login* ou de senha. Por exemplo, foi constatado que provedores permitiam o acesso de um *login* que existia em sua base, mesmo que a senha encaminhada não estivesse correta. Este tipo de política é significativo para o desenvolvimento deste trabalho, visto que a cobrança de serviços baseada nos dados de AAA depende de confiabilidade destes dados, sendo necessário tratamento especial para estes casos.

#### 2.2.1.3 - *Accounting* (Contabilização)

O terceiro A, relativo à contabilização, está associado ao tratamento e armazenamento de dados sobre a utilização dos serviços, principalmente data e hora de início e fim e quais os recursos que foram alocados.

Na área de telecomunicações o termo utilizado para descrever a contabilização muitas vezes é a bilhetagem, visto que o grupo ou linha de informações sobre uma conexão é chamado de bilhete. O bilhete contém as informações de início e fim das conexões, recursos utilizados e dados de identificação do usuário. Mais específicamente no tratamento de bilhetagem dos sistemas de autenticação baseados em RADIUS, de acordo com [HASSEL], o que é armazenado é o registro das informações estatísticas da sessão e das informações de uso, podendo ser utilizado com diversas finalidades, entre elas a cobrança pelos serviços, o controle das autorizações e a análise do uso e das tendências de uso dos recursos para possibilitar melhor planejamento.

O armazenamento das informações de uso de recursos também tem grande importância para a identificação de usuários que estavam utilizando determinado recurso compartilhado no momento que este recurso foi utilizado para realizar atividades que necessitem ser investigadas. Esta utilização é comum para identificação de usuários que cometem crimes na Internet. Outro ponto, destacado por [NAKHJIRI2005] é a possibilidade de auditoria para verificar se as utilizações estão dentro dos limites da política de serviço e se o extrato de utilização corresponde corretamente ao uso.

## 2.3 - ARQUITETURA AAA - ELEMENTOS BÁSICOS

O acesso remoto a uma rede tem como atores principais o Cliente (quem está acessando de forma remota a rede) e o provedor do serviço, que normalmente é uma operadora de serviços de telecomunicações. Na Figura 2.20 estes elementos básicos de cada um destes atores estão representados em um modelo onde a autenticação ocorre na rede da própria operadora.

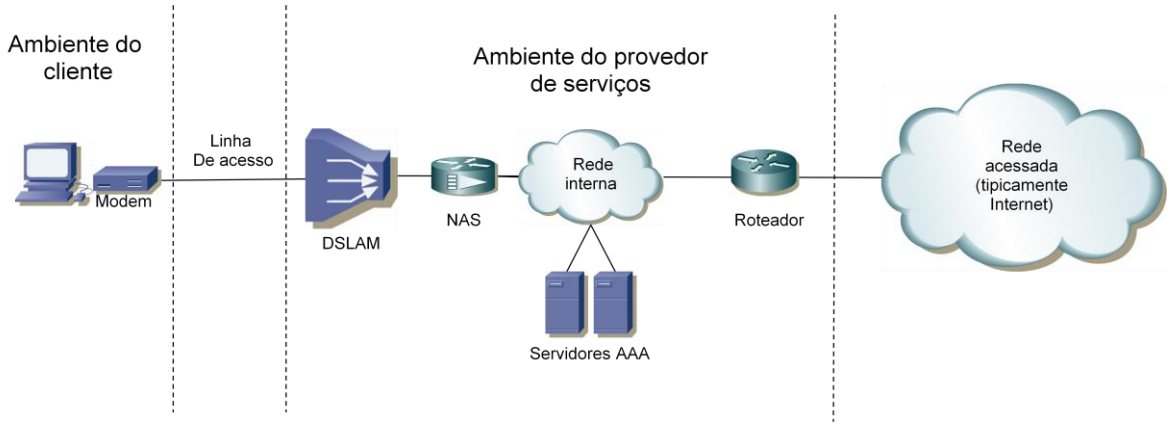



Figura 2.20: Elementos básicos – diagrama de blocos adaptado de [GRUSZYNSKI2008]

Nas operadoras de telecomunicações os volumes de autenticação são extremamente altos, necessitando de utilização de arquiteturas mais robustas para suportar os volumes de requisições. Neste caso é necessário ter mais de um servidor de autenticação operando em paralelo com distribuição da carga.

Um aspecto importante da atual regulamentação brasileira é que as concessionárias de serviços de telecomunicações não podem prestar SVAs, conforme detalhado anteriormente. Devido a este motivo, já no início de suas ofertas de produtos baseados em solução ADSL, as operadoras concessionárias desenvolveram soluções que possibilitam o redirecionamento da autenticação aos ISPs, para que estes sejam os responsáveis pelo processo de permissão do acesso à Internet, mesmo que a conexão física à rede seja

provida pela operadora, caso em que o ISP deve pagar à operadora pelos recursos de rede e infra-estrutura utilizados pelos seus clientes.

A Figura 2.21 mostra o diagrama de conexões em uma operadora de telecomunicações onde há o redirecionamento da autenticação para um ISP remoto. Pode ser constatado que, na solução exemplificada as requisições e respostas de autenticação e bilhetagem trafegam pela própria rede Internet, não sendo obrigatória uma conexão direta entre as redes da operadora e do ISP.

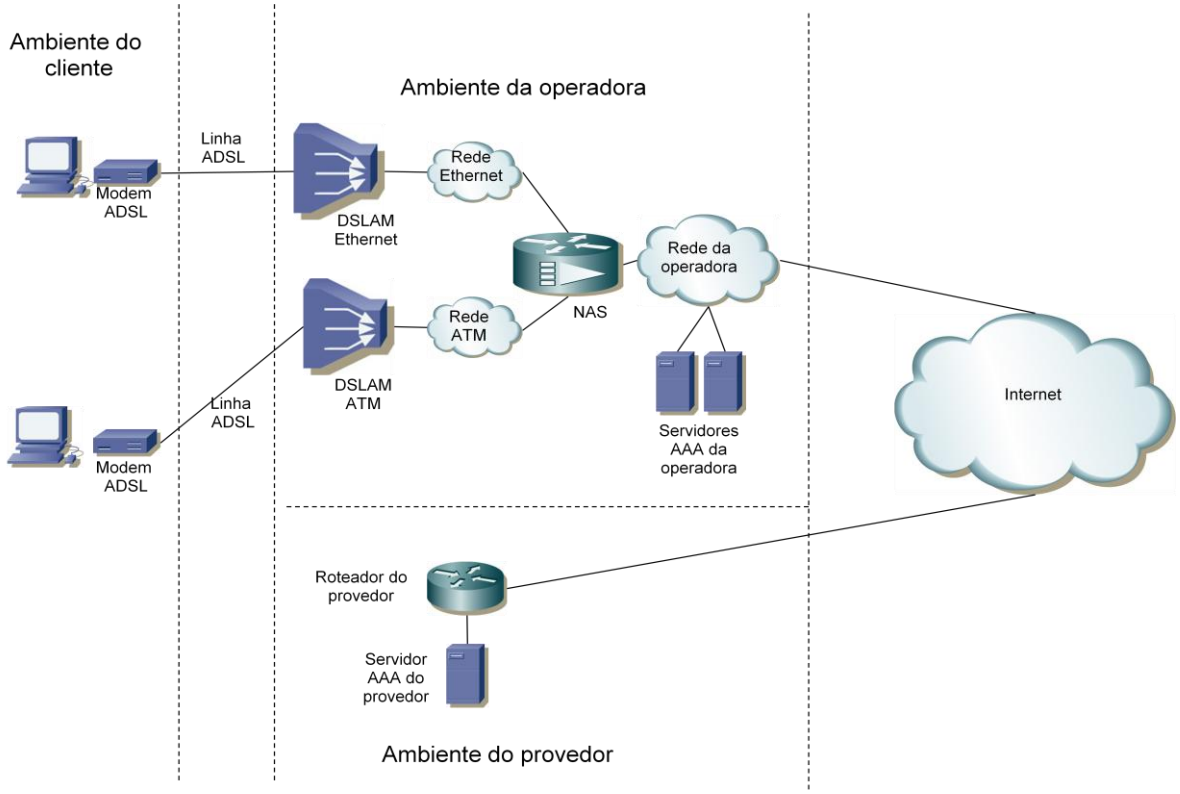



Figura 2.21: Sistema de AAA - autenticação por ISP remoto [GRUSZYNSKI2008]

## 2.4 - COMUNICAÇÃO ENTRE OS ELEMENTOS NO PROCESSO DE AUTENTICAÇÃO

Para o estabelecimento das conexões lógicas entre o equipamento no ambiente do cliente (*modem* ou computador) e o NAS, no ambiente da operadora, ambos vistos na Figura 2.21, é utilizado o protocolo PPP (*Point-to-Point Protocol*), definido inicialmente na [RFC1134] e padronizado posteriormente nas [RFC1661] e [RFC1662].

De acordo com a [RFC1661], o PPP é um protocolo que fornece um método padrão para o transporte de datagramas multiprotocolos sobre enlaces ponto a ponto. O PPP [e composto por três componentes principais:

a) Um método de encapsulamento de datagramas multiprotocolo;

b) Um protocolo de controle do enlace, ou LCP (*Link Control Protocol*) para estabelecer, configurar e testar a conexão do enlace; e

c) Uma família de protocolos de controle de rede NCP (*Network Control Protocol*), que é utilizado para estabelecer e configurar diferentes protocolos de camada de rede.

A Figura 2.21 representa a existência de duas redes distintas para comunicação entre os equipamentos DSLAM e os agregadores (NAS), baseadas em Ethernet e em ATM, que de fato ainda são comumente utilizadas pelas operadoras, embora as redes ATM estejam sendo gradualmente substituídas por redes Ethernet. A utilização destas redes leva à necessidade de uso de variações do protocolo PPP, que são o PPPoA (*Point-to-Point Protocol over ATM*), tratado na [RFC2364], o PPPoE (*Point-to-Point Protocol over Ethernet*), tratado na [RFC2516] e ainda o PPPoEoA (*Point-to-point Protocol over Ethernet over ATM*), utilizado para conexão de acessos ADSL utilizando o protocolo PPPoE em redes onde o DSLAM está conectado ao NAS através de uma rede ATM. Neste caso, é feito um re-encapsulamento do protocolo PPPoE nas células ATM, o que pode solucionar a compatibilidade, mas reduz o desempenho da conexão.

## 2.5 - MÉTODOS DE AUTENTICAÇÃO EM ENLACES PPP

Em conexões ADSL os principais métodos de autenticação são o PAP (P*assword Authentication Protocol*), definido na [RFC1334] e o CHAP (*Challenge-Handshake Authentication Protocol*), também definido na [RFC1334], porém padronizado na [RFC1334].

No PAP, assim que estabelecido o enlace PPP entre o suplicante e o usuário final, o conjunto *login* e a senha passa a ser encaminhado de maneira repetitiva do suplicante para o autenticador, até que se tenha uma resposta positiva (autenticação) ou que o enlace seja interrompido. A questão principal neste método é que há o efetivo envio da senha através do enlace, o que o torna mais suscetível a falhas de segurança do que a solução utilizando CHAP. No CHAP, ao invés do suplicante encaminhar a senha, o autenticador envia uma sequência de octetos, chamada de *challenge* (desafio). Este desafio é tratado matematicamente no suplicante para formar uma combinação entre a senha e o *challenge*, que é encaminhada como resposta ao autenticador.

## 2.6 - PROCESSOS DE AUTENTICAÇÃO COM *MODEM* COMO *BRIDGE* E COMO *ROUTER*

Conforme visto na seção 2.1.5.2, o *modem* do usuário final pode ser utilizado como *bridge*, onde, para efeitos do protocolo PPP ele é apenas uma "ponte" entre o equipamento que acessará a rede e o NAS, ou como *router*, onde ele fecha o enlace PPP diretamente com o NAS. A seguir, desenvolve-se uma análise mais detalhada sobre o processo de autenticação em cada um destes casos.

### 2.6.1 - Autenticação com *modem* como *bridge*

No caso de *modem* utilizado como *bridge*, é necessário um aplicativo, o "discador", que é utilizado para o encaminhamento do nome de usuário (*login*) e da senha para o NAS. O enlace PPP entre o equipamento do usuário final e o NAS só é formado pelo acionamento do discador, ou seja, mesmo com o *modem* e equipamento ligados, nenhuma comunicação relativa a autenticação é iniciada antes da utilização do aplicativo.

Todas as configurações quanto ao envio do *login* e da senha para o NAS são feitas no aplicativo e no próprio computador do usuário, sendo possível que:

a) O aplicativo discador pode ser iniciado manualmente ou automaticamente quando o computador é inicializado.

b) O aplicativo pode conter o *login* e a senha armazenados ou pode exigir que sejam digitados a cada conexão

c) Ao ser desfeita a conexão por perda de comunicação o aplicativo pode tentar a re-conexão automaticamente ou aguardar pela ação do usuário

Estas possibilidades são muito importantes quando se avalia ações que envolvem o processo de autenticação, pois influenciam diretamente na percepção do usuário quando há alguma mudança no processo.

### 2.6.2 - Autenticação com *modem* como *router*

Na configuração de *modem* como *router*, cada vez mais usado pelo crescente uso de redes domésticas, o enlace PPP é estabelecido entre o *modem* e o NAS, normalmente logo após o equipamento ser ligado.

Neste tipo de configuração, o *login* e a senha devem ser cadastrados pelo cliente diretamente no *modem*, onde também são feitas todas as configurações para o seu envio ao NAS. Esta configuração torna mais prático o seu uso no dia a dia, uma vez que, quando

ligado, o *modem* encaminha o *login* e a senha ao NAS logo após o início do estabelecimento do enlace PPP, sem a necessidade de qualquer intervenção do usuário.

Embora torne mais prático o uso no dia a dia, a sua configuração inicial é mais complexa para usuários que não têm habilidades mais avançadas na área de informática, pois exige conhecimento adicional nesta área para que se consiga fazer o acesso ao *modem* e alterar a sua configuração.

Nos *modem*s ADSL mais antigos, havia a necessidade de conexão de um cabo serial e uso de um aplicativo especifico para configuração, porém atualmente esta tarefa é um pouco mais simples, a configuração é feita através do navegador do usuário. Para esta configuração o usuário precisa identificar o endereço IP de seu *modem* dentro da sua rede, sendo que este endereço deve ser digitado diretamente no navegador para ter acesso à tela de configuração. O acesso às configurações do *modem* normalmente é protegido por um conjunto específico de *login* e senha, normalmente informado no manual de equipamento.

Esta complexidade de configuração, muitas vezes, implica no usuário solicitar um suporte técnico para configuração e torna a mudança de senha uma atividade quase inacessível para alguns usuários.

Um ponto importante é que com o *login* e a senha cadastrados no *modem*, caso este conjunto não seja aceito pelo servidor de autenticação e a resposta não retorne (*time out*), ou a resposta seja um *reject* (permissão negada), a configuração padrão é que o *modem* continue repetidamente reencaminhando as credenciais ao NAS. Este comportamento tem algumas implicações adicionais no sistema de autenticação, como sobrecarga por tentativas repetitivas ou até falhas de autorização, como no caso de tratamento diferenciado para o *time out*.

## 2.7 - O RADIUS

O RADIUS (*Remote Authentication Dial In User Service*) é um protocolo tratado na [RFC2865], definido nela como sendo desenvolvido para a realização de autenticação,

autorização e encaminhamento de informações de configuração entre uma rede de acesso compartilhada, que deseja autenticar as suas ligações, e um servidor de autenticação.

De acordo com a definição na [RFC2865], o RADIUS opera no modelo cliente/servidor, onde o NAS opera como cliente do servidor RADIUS. O NAS, como cliente, é responsável por encaminhar as informações do usuário final e tomar a ação de acordo com a resposta recebida. Por sua vez, o Servidor RADIUS é responsável por receber a requisição de acesso do usuário, autenticar e devolver as informações de configuração necessárias para que o cliente (NAS) entregue o serviço ao usuário. A [RFC2685] destaca ainda que um servidor RADIUS pode agir também como *proxy*, neste caso sendo cliente de outros servidores RADIUS ou de servidores de autenticação de outros tipos.

De fato, a utilização de sistemas centralizados de autenticação pressupõe a sua comunicação com os diversos equipamentos e sistemas remotos que suportam a disponibilização dos serviços para cada meio de acesso. Para tal, há uma necessidade de se ter um protocolo que padronize esta comunicação e permita a interoperabilidade dos servidores e sistemas de autenticação com outros sistemas de autenticação e com seus usuários finais. Segundo [HASSEL2002], o RADIUS foi construído a partir da necessidade de se ter um método de autenticação, autorização e bilhetagem para usuários que necessitavam de acesso a recursos heterogêneos.

### 2.7.1 - Uso do UDP no RADIUS

O RADIUS utiliza UDP (*User Datagram Protocol*) como protocolo de comunicação para autorização, autenticação e contabilização [RFC2865]. Este protocolo tem a característica básica de não garantir a entrega dos pacotes [STEVENS1994]. Neste caso, as informações transportadas entre os sistemas podem não chegar ao destino, sem necessariamente comprometer o funcionamento ou acesso, mas podendo comprometer a contabilização, principalmente porque a informação de bilhetagem pode não chegar ao servidor que fará a sua contabilização. A própria [RFC2865] indica que a escolha do

protocolo UDP é constantemente questionada, mas justifica os motivos de sua escolha pelos motivos listados a seguir:

a) O UDP facilita a utilização de servidores alternativos de autenticação, visto que o controle de reenvio fica em camada superior à de transporte;

b) O RADIUS não tem a necessidade de uma resposta instantânea. O cliente pode esperar alguns segundos para ter seu acesso estabelecido, o que permite que caso a resposta a requisição não chegue rapidamente, outra solicitação possa ser encaminhada imediatamente ao servidor secundário. Os tempos de espera pela resposta do TCP não são compatíveis com esta necessidade. Este protocolo leva em conta o tempo de ida e volta dos pacotes e pode exigir a retransmissão antes da resposta e por isso demorar até alguns minutos em vez de poucos segundos;

c) O UDP não depende de sincronização e independe dos tempos de rede, o que facilita sua utilização em redes heterogêneas e que sofrem alterações de usuários finais e servidores constantemente;

d) O uso do UDP simplifica a implantação dos servidores, visto que o processamento com ele é muito mais leve do que se utilizando o protocolo TCP, o que possibilita a utilização de equipamentos e sistemas menos robustos.

Na realidade, quando se analisa sistemas de AAA, os problemas relacionados ao transporte através de protocolo UDP estão normalmente ligados à contabilização, principalmente quando se deseja medir a utilização de recursos com a finalidade de faturamento. Nestes casos, a perda de pacotes pode representar perda de receita ou erro de contabilização do uso de uma franquia, podendo ser mais crítico se o pacote perdido levar a conclusão de que a conexão permanece ativa.

### 2.7.2 - Segurança na comunicação usando protocolo RADIUS

Como se trata de um protocolo para o tratamento de autenticação e autorização, há uma preocupação adicional quanto à segurança. Algumas medidas de aumento de segurança fazem parte do padrão do protocolo, conforme visto a seguir.

As comunicações entre o cliente e o servidor RADIUS são autenticadas através de uma senha compartilhada, denominada *shared secret*, que não é encaminhada pela rede nas transações de autenticação. Qualquer solicitação ou resposta só é processada pelo destino se autenticada através desta senha.

Qualquer outra senha, quando enviada através da rede, é criptografada entre o cliente e o servidor utilizando uma combinação matemática (*hash*) entre a senha encaminhada, a senha secreta (*shared secret*) de conhecimento do cliente e do servidor e o campo Autenticador, presente na requisição de acesso e composto por um número aleatório, conforme descrito na [RFC2865]. Em operações com o servidor RADIUS atuando como *proxy*, este passa a ser cliente de outro servidor de autenticação. Neste caso também é necessária a definição de uma senha "*shared secret"* para esta comunicação.

### 2.7.3 - Mensagens do protocolo RADIUS (*packets*)

As comunicações do protocolo RADIUS são padronizadas em um conjunto de mensagens (*packets*) que são trocadas entre os elementos clientes e servidores. A [RFC2865] descreve oito mensagens principais, que serão detalhadas a seguir. Estas mensagens são identificadas dentro do pacote encaminhado no campo *Code*, que pode ser identificado na Figura 2.22 que representa a forma em que o *packet* é transmitido. Os campos são transmitidos da esquerda para direita.

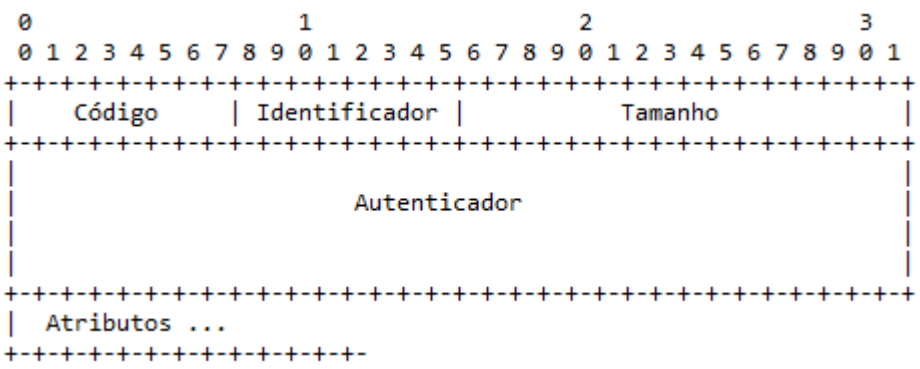



Figura 2.22: Formato do pacote (*packet*) do RADIUS adaptada da [RFC2865]

A mensagem encaminhada tem sempre o formato descrito na Figura 2.22 e a informação do campo código é quem determina a sua função e seu encaminhamento. A [RFC2865] define que, de acordo com este campo, as mensagens têm as finalidades descritas na Tabela 2.7.

Tabela 2.7: Tipos de mensagens do RADIUS adaptada da [RFC2865]

| Code | Tipo de mensagem | Função |
|---|---|---|
| 1 | *Access-Request* | Requisição de acesso |
| 2 | *Access-Accept* | Acesso permitido |
| 3 | *Access-Reject* | Acesso rejeitado |
| 4 | *Accounting-Request* | Requisição de bilhetagem |
| 5 | *Accounting-Response* | Requisição de bilhetagem aceita |
| 11 | *Access-Challenge* | Desafio de acesso |
| 12 | *Status-Server (experimental)* | Status do Servidor (não definida) |
| 13 | *Status-Client (experimental)* | Status do cliente (não definida) |
| 255 | *Reserved* | Reservado |

A seguir estão detalhadas cada uma das mensagens e suas funções, além do elemento responsável pela sua geração e encaminhamento.

***Access-Request* - Requisição de Acesso**

A mensagem de requisição de acesso é gerada pelo cliente RADIUS, que tipicamente é o NAS ou um *proxy*, e encaminhada ao servidor RADIUS. Esta mensagem transporta a solicitação de acesso do usuário.

***Access-Accept* - Acesso Permitido**

A mensagem de Acesso Permitido é gerada pelo servidor RADIUS e encaminhada ao cliente RADIUS (*NAS ou proxy*). Esta mensagem é utilizada para informar que a solicitação de acesso foi aceita e contém também informações sobre a configuração de autorização do acesso do usuário.

***Access-Reject* - Acesso Rejeitado**

A mensagem de acesso rejeitado é gerada pelo servidor RADIUS e enviada ao cliente RADIUS. Ela é utilizada para indicar que a solicitação de acesso realizada pelo usuário final foi rejeitada. Se o cliente RADIUS for um *proxy server* ele poderá interpretar e modificar esta mensagem de acordos com suas políticas de autorização, antes de encaminhar ao cliente RADIUS que processará a autorização do usuário final.

***Accounting-Request* - Requisição de Bilhetagem**

A mensagem de requisição de bilhetagem é gerada pelo cliente RADIUS (NAS ou *proxy*) e enviada ao servidor RADIUS de Bilhetagem (*RADIUS Accounting Server*). Esta mensagem transporta as informações correntes da conexão ou de serviço fornecido ao usuário.

***Accounting-Response* – Requisição de Bilhetagem Aceita**

A mensagem de requisição de bilhetagem aceita é gerada pelo servidor RADIUS e enviada ao cliente RADIUS. Esta mensagem é utilizada para indicar que a solicitação de bilhetagem foi recebida pelo servidor.

***Access-Challenge* - Requisição de Desafio**

A mensagem de requisição de desafio é gerada pelo servidor RADIUS e enviada ao cliente RADIUS (NAS ou *proxy*). Esta mensagem é utilizada para questionar o cliente ou o usuário final.

***Status-Server* – Requisição de informação de Estado do Servidor**

Embora esteja definida na [RFC2865], o documento não definiu as finalidades previstas para esta mensagem. Pelo seu nome, pode ser interpretado que seu objetivo é solicitar informações sobe o estado de funcionamento do servidor RADIUS.

Ainda na condição de documento preliminar (*draft*), [DEKOK] propõe no IETF (*Internet Engineering Task Force*) uma padronização para o uso da Requisição de Estado de servidor, justamente para verificação do estado de funcionamento, porém este documento ainda está em fase de elaboração e aprovação, embora já disponível para consulta e comentários na Internet.

***Status-Client* – Requisição de informação de Estado do Cliente**

Embora também esteja definida na [RFC2865], o documento não definiu as finalidades previstas para esta mensagem. Pelo seu nome, pode ser interpretado que seu objetivo é solicitar informações sobre o estado de funcionamento do Cliente RADIUS.

Adicionalmente, a [RFC3575], posteriormente atualizada na [RFC5176], listou os documentos de referência das principais mensagens do RADIUS, possibilitando a consulta mais aprofundada caso necessário, esta lista é apresentada na Tabela 2.8.

Tabela 2.8: Lista de mensagens do RADIUS adaptada da [RFC3575]

| *Code* | Mensagem | *Code* | Mensagem |
|---|---|---|---|
| 1 | *Access-Request* | 27 | *NAS-Reboot-Response* |
| 2 | *Access-Accept* | 28 | *Reserved* |
| 3 | *Access-Reject* | 29 | *Next-Passcode* |
| 4 | *Accounting-Request* | 30 | *New-Pin* |
| 5 | *Accounting-Response* | 31 | *Terminate-Session* |
| 6 | *Accounting-Status* | 32 | *Password-Expired* |
| 7 | *Password-Request* | 33 | *Event-Request* |
| 8 | *Password-Ack* | 34 | *Event-Response* |
| 9 | *Password-Reject* | 40 | *Disconnect-Request* |
| 10 | *Accounting-Message* | 41 | *Disconnect-ACK* |
| 11 | *Access-Challenge* | 42 | *Disconnect-NAK* |
| 12 | *Status-Server (experimental)* | 43 | *CoA-Request* |
| 13 | *Status-Client (experimental)* | 44 | *CoA-ACK* |
| 21 | *Resource-Free-Request* | 45 | *CoA-NAK* |
| 22 | *Resource-Free-Response* | 50 | *IP-Address-Allocate* |
| 23 | *Resource-Query-Request* | 51 | *IP-Address-Release* |
| 24 | *Resource-Query-Response* | 250-253 | Experimental |
| 25 | *Alternate-Resource-Reclaim-Request* | 254 | Reservada |
| 26 | *NAS-Reboot-Request* | 255 | Reservada |

### 2.7.4 - Atributos do RADIUS

Para transportar as informações dentro de suas mensagens, o RADIUS utiliza atributos que, de acordo com o seu tipo, contêm dados utilizados para os objetivos de autenticação, autorização e contabilização. As informações de autorização contêm também os detalhes de configuração necessários para o estabelecimento da conexão.

Todas as informações, como o *login* e senha, informação de porta física e equipamentos utilizados, dentre outras, são encaminhadas em formato de atributos dentro do pacote RADIUS. Um atributo é um conjunto de três campos que são encaminhados

sequencialmente no pacote. Estes campos trazem as informações de tipo, tamanho e valor do atributo, conforme descrito a seguir. Cabe ressaltar que a ordem em que os diferentes tipos de atributos são enviados no pacote não é relevante, desde que suas especificações os acompanhem corretamente.

**Campo Tipo**

O campo tipo é composto por um *byte* e determina o tipo ou função do atributo. A Tabela 2.9 mostra a lista de atributos definidos na [RFC2865], de acordo com este campo.

Tabela 2.9: Atributos do RADIUS adaptada da [RFC2865]

| Número do Atributo | Nome do Atributo |
|---|---|
| 1 | *User-Name* |
| 2 | *User-Password* |
| 3 | *CHAP-Password* |
| 4 | *NAS-IP-Address* |
| 5 | *NAS-Port* |
| 6 | *Service-Type* |
| 7 | *Framed-Protocol* |
| 8 | *Framed-IP-Address* |
| 9 | *Framed-IP-Netmask* |
| 10 | *Framed-Routing* |
| 11 | *Filter-Id* |
| 12 | *Framed-MTU* |
| 13 | *Framed-Compression* |
| 14 | *Login-IP-Host* |
| 15 | *Login-Service* |
| 16 | *Login-TCP-Port* |
| 17 | *Reply-Message* |
| 19 | *Callback-Number* |
| 20 | *Callback-Id* |
| 22 | *Framed-Route* |
| 23 | *Framed-IPX-Network* |

| Número do Atributo | Nome do Atributo |
|---|---|
| 24 | *State* |
| 25 | *Class* |
| 26 | *Vendor-Specific* |
| 27 | *Session-Timeout* |
| 28 | *Idle-Timeout* |
| 29 | *Termination-Action* |
| 30 | *Called-Station-Id* |
| 31 | *Calling-Station-Id* |
| 32 | *NAS-Identifier* |
| 33 | *Proxy-State* |
| 34 | *Login-LAT-Service* |
| 35 | *Login-LAT-Node* |
| 36 | *Login-LAT-Group* |
| 37 | *Framed-AppleTalk-Link* |
| 38 | *Framed-AppleTalk-Network* |
| 39 | *Framed-AppleTalk-Zone* |
| 40-59 | *Reserved for accounting* |
| 60 | *CHAP-Challenge* |
| 61 | *NAS-Port-Type* |
| 62 | *Port-Limit* |
| 63 | *Login-LAT-Port* |

**Campo Comprimento**

O campo comprimento também é formado por um byte e é utilizado para indicar o tamanho total do atributo, incluindo os três campos que o formam. É importante destacar que no processo de autenticação, se um *Access-Request* tiver o campo comprimento de qualquer um dos seus atributos errado, terá como resposta um *Access-Reject*. Uma resposta do servidor com o comprimento de qualquer atributo errado é tratada pelo NAS como um *Access-Reject* ou descartada silenciosamente, ou seja, descartada sem aviso aos demais elementos.

**Campo Valor**

O campo valor tem comprimento variável, o que mostra a importância do campo comprimento para correta leitura dos atributos. Este campo tem as informações específicas do atributo e pode ter dados em cinco formatos diferentes, conforme apresentado na Tabela 2.10.

Tabela 2.10: Formatos do campo valor dos atributos do RADIUS adaptado da [RFC2865]

| Formato | Descrição |
|---|---|
| texto | Tamanho entre 1 e 253 bytes, contendo texto em UTF-8 codificado. Caso o texto tenha comprimento zero, o atributo inteiro deve ser omitido. |
| string | Varia entre 1 e 253 bytes com dados em binário. Caso a string tenha comprimento zero, o atributo inteiro deve ser omitido. |
| endereço | Tamanho de 32 bits, com os bits mais significativos transmitidos primeiro. |
| inteiro | Tamanho de 32 bits, com os bits mais significativos transmitidos primeiro. |
| tempo | Tamanho de 32 bits, com os bits mais significativos transmitidos primeiro. Contém o número de segundos desde o 00:00:00 UTC, 01 de janeiro de 1970. |

### 2.7.5 - Processo de autenticação de acessos ADSL no RADIUS

Os processos de autenticação utilizando RADIUS podem ser desde os mais simples, com duas partes e credenciais trafegando diretamente na rede, até modelos mais complexos, com três partes e redirecionamento da autenticação (*proxy*).

Conforme visto anteriormente, o protocolo de comunicação utilizado para estabelecer os enlaces das conexões ADSL é o PPP, com suas variações PPPoE, PPPoA e PPPoEoA. O processo de autenticação no RADIUS é disparado pelo início da conexão, ou seja, no estabelecimento do enlace PPP.

Conforme já apresentado, existem dois métodos de autenticação normalmente utilizados sobre comunicações PPP, o PAP e o CHAP. Nos dois casos, o usuário final possui para sua autenticação pelo menos duas informações, o seu nome de usuário (*login*) e a sua senha, também denominadas credenciais. Outras informações podem ser utilizadas para autenticação, como informações de porta ou de equipamento utilizado.

Para melhor entendimento, a seguir é descrito o funcionamento deste processo desde nos modelos mais simples até nos modelos atualmente utilizados nas operadoras, que envolvem redirecionamento a um ISP.

#### 2.7.5.1 - Processo de autenticação utilizando PAP

Quando utilizado o processo de autenticação PAP, este ocorre seguindo o diagrama da Figura 2.23. Neste processo o nome de usuário (*login*) e a senha do usuário são trafegados entre os elementos nas mensagens encaminhadas entre eles.

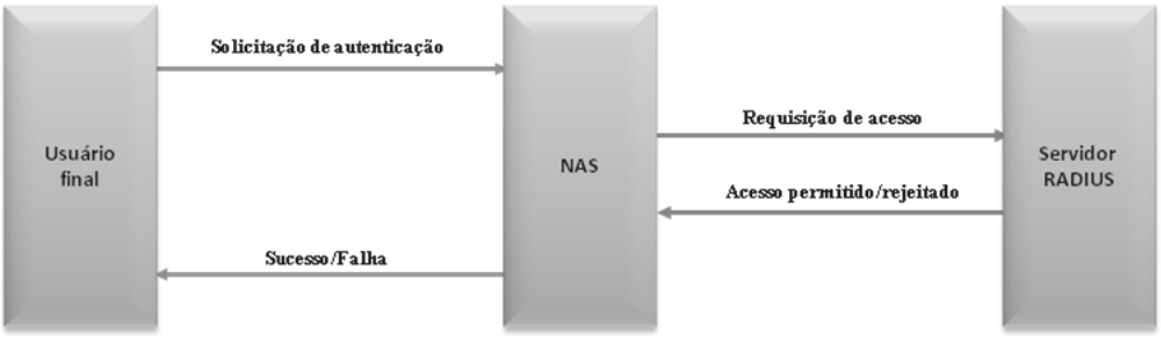



Figura 2.23: Fluxo das mensagens em autenticação usando PAP

No início do estabelecimento do enlace PPP entre o equipamento do usuário final e o NAS, há o envio da solicitação de autenticação com as informações de *login* e senha, com as quais o NAS gera a mensagem de Requisição de Acesso (*Access-Request)*, que é encaminhada por ele ao servidor de autenticação RADIUS.

Após encaminhar o *Access-Request*, o NAS fica aguardando a resposta de acordo com o tempo pré-configurado e, caso não receba uma resposta no período previsto, ele retransmite a mensagem para o mesmo servidor ou para outro(s), caso haja esta previsão em sua configuração.

Quando a mensagem de Requisição de Acesso chega ao servidor RADIUS, ele verifica em sua base se o endereço IP de origem (do NAS) consta como válido. Sendo o endereço válido, ele utiliza a senha compartilhada (*shared secret*) cadastrada para recuperar as informações recebidas na mensagem. Com a recuperação da senha do usuário final, o servidor busca o nome do usuário em sua base de dados para fazer a comparação das credenciais.

Primeiro o servidor RADIUS verifica a existência do nome de usuário, caso exista, verifica se a senha recebida na requisição é idêntica àquela cadastrada na sua base. Caso as verificações sejam positivas, o servidor responde ao NAS com a mensagem de Acesso permitido (*Access-Accept*) que, além da informação de autorização, contém informações para a disponibilização da conexão. Caso contrário, é encaminhada a resposta de Acesso

negado (*Access-Reject*). Com esta resposta, o NAS pode prosseguir com o estabelecimento da conexão PPP do usuário final à rede ou encerrar a negociação. Caso a negociação seja encerrada, o equipamento do usuário final interpreta como acesso rejeitado e pode reiniciar o processo de solicitação de acesso novamente.

### 2.7.5.2 - Processo de autenticação CHAP

Quando utilizado o CHAP, o processo ocorre seguindo o diagrama da Figura 2.24. O processo de utilização do CHAP é iniciado quando a solicitação de autenticação encaminhada pelo equipamento do usuário final é respondida pelo NAS com a indicação de utilização de CHAP através do envio de um *CHAP-Challenge* (desafio).

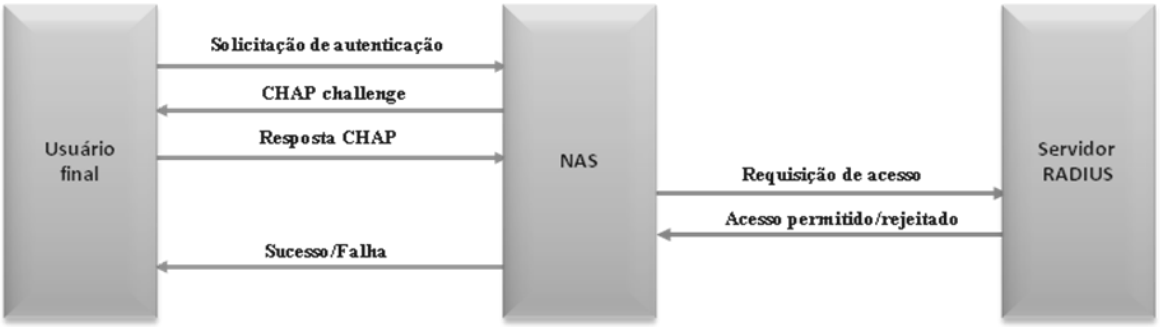



Figura 2.24: Fluxo das mensagens em autenticação usando CHAP

O *CHAP-Challenge* é uma mensagem que contém um campo com 16 bytes em conjunto com o *CHAP-Id*, que é o identificador da operação de autenticação CHAP com tamanho de um byte.

A Resposta CHAP, encaminhada pelo usuário final é formada pelo *login* (nome de usuário) e o resultado da operação MD5 (*Message-Digest algorithm* 5), que é um algoritmo de criptografia (*hash*) de 128 bits unidirecional, desenvolvido pela RSA Data

Security, Inc., descrito na [RFC1321], realizada com o CHAP-Id, a senha (chamada de *secret* na fórmula original) e o CHAP-*Challenge*, conforme descrito na fórmula a seguir:

$$\text{Resposta CHAP} = \text{MD5}(\text{CHAP-}Id, secret, \text{CHAP-}Challenge) \qquad (2.1)$$

Ao receber a Resposta CHAP, o NAS cria a Requisição de Acesso (*Access-request*), incluindo o *login* e o CHAP-*Challenge*. O CHAP-*Id* e a Resposta CHAP são concatenados e encaminhados como atributo do tipo 3, CHAP-Password.

A requisição de acesso é encaminhada pelo NAS ao servidor RADIUS que, ao recebê-la, identifica a presença do atributo CHAP-*Password* e a trata então como uma requisição CHAP.

O processo de autenticação ocorre a partir da busca pelo *login* (nome de usuário) e pela senha na base de dados do servidor RADIUS. Porém na autenticação CHAP o servidor precisa fazer a mesma operação MD5, descrita na Equação 2.1 para poder comparar o resultado com o valor recebido na Requisição de Acesso, no atributo *CHAP-Password*, excluindo o byte inicial que é referente ao *CHAP-Id*. A partir desta comparação, caso o resultado seja idêntico, o servidor responderá com a mensagem de Acesso Permitido (*Access-accept*), caso contrário responderá com Acesso Rejeitado (*Access-Reject*).

A resposta do servidor é então encaminhada de volta ao NAS, que pode prosseguir com o estabelecimento da conexão PPP do usuário final à rede ou encerrar a negociação. Caso a negociação seja encerrada, o equipamento do usuário final interpreta como acesso rejeitado e pode reiniciar o processo de solicitação de acesso novamente.

2.7.5.3 - Autenticação com RADIUS como *proxy* (redirecionamento ao ISP)

Conforme descrito anteriormente, o RADIUS pode ser utilizado como *proxy* para o encaminhamento das mensagens a outro servidor que faz a autenticação. Esta solução é utilizada nos casos onde a requisição de acesso deve ser redirecionada para um ISP que faz a autenticação, o que ocorre nas concessionárias por motivos regulatórios, conforme já relatado. O processo de encaminhamento da solicitação ocorre conforme ilustrado na Figura 2.25.


Figura 2.25: Fluxo das mensagens em autenticação com redirecionamento ao ISP.

O processo de autenticação entre o NAS e o usuário final ocorre da forma já descrita, exceto pelo servidor RADIUS *proxy* (da operadora) precisar receber a resposta do servidor RADIUS remoto (do ISP) para dar continuidade em sua comunicação com o NAS. Neste processo, o servidor RADIUS da operadora recria a mensagem de Requisição de Acesso que recebeu do NAS e a encaminha ao servidor RADIUS do ISP, de acordo com a forma de comunicação entre eles prevista.

Na operadora pesquisada a comunicação entre o seu servidor RADIUS e os servidores RADIUS dos ISPs é feita utilizando o método PAP com o compartilhamento de uma senha *shared secret* e a lista de permissões de endereços IP cadastrada nos dois lados.

No servidor RADIUS do ISP, o processamento da autenticação ocorre de maneira idêntica à descrita para autenticação PAP na seção 2.7.5.1. Após o processamento, a resposta do servidor RADIUS remoto é encaminhada ao servidor RADIUS da operadora, que encaminha a mensagem de permissão ou de rejeição ao NAS.

Conforme [GRUSZYNSKI2008], a autenticação usando um ISP é considerada uma operação inter-domínio, pelo fato das mensagens relacionadas com a operação cruzarem as fronteiras de diferentes domínios administrativos. O conceito de domínio administrativo refere-se ao apresentado na [RFC1136].

### 2.7.6 - Contabilização do RADIUS (*Accounting*)

O processo de contabilização ou bilhetagem no RADIUS é disparado em dois momentos, o de início da conexão, após estabelecida a conexão PPP, e no final da conexão, após desfeito o enlace PPP com o usuário final. A Figura 2.26 ilustra o fluxo destas mensagens em uma configuração multi-domínio, considerando o redirecionamento da autenticação a um ISP.

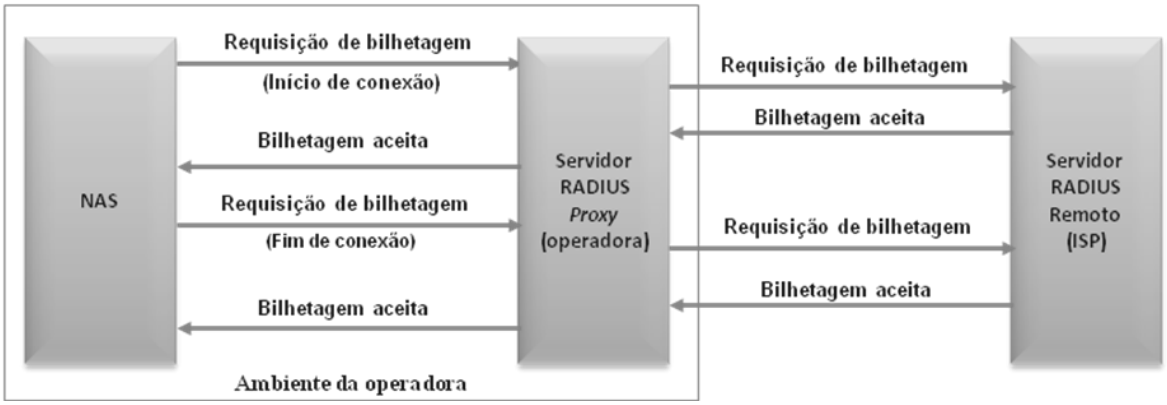



Figura 2.26: Fluxo das mensagens de contabilização com multi-domínio.

O fluxo das mensagens de contabilização inicia-se pelo encaminhamento de uma Requisição de Bilhetagem pelo NAS ao servidor RADIUS. Esta mensagem tem várias informações sobre a conexão, como endereço IP, porta etc. O servidor RADIUS processa esta mensagem armazenando as informações, se programado para isto, e responde ao NAS com uma resposta de Bilhetagem Aceita (*Accounting-Response*). Caso o NAS não receba a mensagem de Bilhetagem Aceita ele normalmente reencaminha a Requisição de Bilhetagem, embora este reenvio seja configurável e possa ser suprimido.

Cabe ressaltar que o uso do servidor RADIUS como *proxy* não impede que ele também processe as requisições de bilhetagem, embora ele deva, conforme visto na Figura 2.26, reencaminhar a Requisição de Bilhetagem ao servidor RADIUS remoto e aguardar a resposta de Bilhetagem Aceita antes de responder ao NAS.

Quando a sessão é interrompida, seja porque o usuário desligou seu *modem* ou encerrou sua conexão através do discador ou por alguma falha no percurso que desfaça o enlace PPP, é gerado pelo NAS uma nova Requisição de Bilhetagem, desta vez com informações completas sobre toda a sessão encerrada, como nome de usuário, data e hora de início e fim da conexão, bits trafegados etc. Esta requisição é então encaminhada ao servidor RADIUS, que a processa e responde novamente ao NAS com a mensagem de Bilhetagem Aceita. De fato as informações necessárias para bilhetagem só estarão completas com o recebimento desta requisição, conforme pode ser visto na Figura 2.28.

As informações da mensagem de Requisição de Bilhetagem do final da sessão são então transformadas em um bilhete para contabilização no RADIUS. Este bilhete é comumente chamado de Bilhete de *Stop*, por ser gerado somente após a finalização da sessão, ou Bilhete RADIUS, por ser de fato o que é armazenado para a contabilização no RADIUS. Todos os processos de contabilização e de faturamento que utilizam dados de conexão ocorrem a partir do processamento destes bilhetes.

### 2.7.7 - O Bilhete RADIUS

Conforme descrito anteriormente, existem dois tipos principais de bilhetes de contabilização que podem ser armazenados e processados com a finalidade de medir a utilização de recursos, são eles o bilhete Requisição de Contabilização gerado no início da conexão (*start*) e o bilhete de Requisição de Contabilização gerado no término da conexão (*stop*). A Figura 2.27, mostra um exemplo fictício de bilhete de requisição relativo a conexão (*start*), com os principais dados retirados de um bilhete real.

```
Sun oct 04 11:35:06 GMT-03:00 2009
        Acct-Status-Type = Start
        User-Name = "usuario@isp.com.br"
        Event-Timestamp = 1254666906
        Acct-Delay-Time = 0
        Acct-Session-Id = "erx atm 0/0.107221:107.221:0298263122"
        NAS-IP-Address = 200.101.129.33
        Class = "PAENRAS01_PR_OK_DEF_CLF_0"
        Service-Type = Framed-User
        Framed-Protocol = PPP
        Framed-Compression = None
        Unisphere-PPPoE-Description = "pppoe 00:00:00:00:00:00"
        Framed-IP-Address = 200.138.98.238
        Framed-IP-Netmask = 255.255.255.255
        Calling-Station-Id = "#CTAME706#ERX<=> CTAME501 10/2#107#221"
        Connect-Info = "speed:UBR"
        NAS-Port-Type = xDSL
        NAS-Port = 7012573
        NAS-Port-Id = "atm 0/0.107221:107.221"
        Acct-Authentic = RADIUS
        NAS-Identifier = "CTAME706"
```

Figura 2.27: Exemplo fictício de Bilhete RADIUS de início de conexão (*start*)

Na Figura 2.27 são mostrados os campos de um bilhete RADIUS com informações do início da conexão, o que pode ser identificado pelo atributo *Acct-status-Type = start*. Neste bilhete, entre outras informações, podem ser identificados o nome do usuário (*User-Name*), data e hora da conexão, através do *Event-Timestamp*, porta através do *NAS-Port*. Porém este bilhete só informa dados do início, visto que as informações finais só estarão disponíveis no término da conexão.

Já na Figura 2.28, é mostrado um bilhete fictício de desconexão (*stop*) da mesma conexão, com as informações completas da sessão. Esse bilhete é gerado pelo NAS e enviado para o servidor de bilhetagem como *Accounting-Request*, utilizando o protocolo RADIUS. Este bilhete, gerado no término da conexão, pode ser identificado pelo atributo *Acct-status-Type = stop*. Além das informações já citadas para o bilhete de *start*, também podem ser ressaltadas as informações de volumes de pacotes trafegados, a duração da sessão e a causa de desconexão.

```
Sun oct 04 14:44:05 GMT-03:00 2009
        Acct-Status-Type = Stop
        User-Name = "usuario@isp.com.br"
        Event-Timestamp = 1254678245
        Acct-Delay-Time = 0
        Acct-Session-Id = "erx atm 0/0.107221:107.221:0298263122"
        NAS-IP-Address = 200.101.129.33
        Class = "PAENRAS01_PR_OK_DEF_CLF_0"
        Service-Type = Framed-User
        Framed-Protocol = PPP
        Framed-Compression = None
        Unisphere-PPPoE-Description = "pppoe 00:00:00:00:00:00"
        Framed-IP-Address = 200.138.98.238
        Framed-IP-Netmask = 255.255.255.255
        Unisphere-Ingress-Policy-Name = "de_usuario"
        Unisphere-Egress-Policy-Name = "para_usuario_RATE"
        Calling-Station-Id = "#CTAME706#ERX<=> CTAME501 10/2#107#221"
        Acct-Input-Gigawords = 0
        Acct-Input-Octets = 12015
        Acct-Output-Gigawords = 0
        Acct-Output-Octets = 18055
        Unisphere-Input-Gigapackets = 0
        Acct-Input-Packets = 20
        Unisphere-Output-Gigapackets = 0
        Acct-Output-Packets = 70
        NAS-Port-Type = xDSL
        NAS-Port = 7012573
        NAS-Port-Id = "atm 0/0.107221:107.221"
        Acct-Authentic = RADIUS
        Acct-Session-Time = 11339
        Acct-Terminate-Cause = User-Request
        NAS-Identifier = "CTAME706"
```

Figura 2.28: Exemplo fictício de Bilhete RADIUS de final da conexão (*stop*)

Segundo [GRUSZYNSKI2008], uma Requisição de Bilhetagem pode ter todos os atributos RADIUS que possam ser utilizados em uma mensagem de Requisição de Acesso

ou de Acesso Permitido, exceto os atributos *User-Password, CHAP-Password, Reply-Message* e *State*. Ele adiciona que existem mais três regras básicas relacionadas com a presença de atributos na mensagem de Requisição de Bilhetagem:

a) De acordo com a [RFC2866], a Requisição de Bilhetagem deve conter pelo menos um dos dois atributos *NAS-IP-Address* ou *NAS-Identifier*, podendo ter os dois. Percebe-se, examinando os bilhetes armazenados nos servidores RADIUS da plataforma ADSL da operadora, que normalmente ambos os atributos estão presentes.

b) A Requisição de Bilhetagem deve conter também pelo menos um de dois atributos de identificação da interface de conexão do usuário: *NAS-Port* ou *NAS-Port-Type*. Nos bilhetes armazenados nos sistemas da operadora pesquisada normalmente ambos os atributos estão presentes. A [RFC2869] introduziu um novo atributo, chamado *NAS-Port-Id*, cujo objetivo é fornecer uma descrição da interface de conexão. A presença deste último atributo na mensagem de Requisição de Bilhetagem não é obrigatória.

c) O endereço IP contido no atributo *Framed-IP-Address* deve corresponder efetivamente ao endereço atribuído ao usuário final. Este critério é muito importante em termos de segurança para identificação de atos realizados utilizando a conexão à rede.

### 2.7.8 - *Policies* do RADIUS

No processo de autenticação e autorização o RADIUS baseia-se em um conjunto de *policies* (políticas) que são pré-estabelecidas para o tratamento das requisições e de como elas devem ser respondidas. Estas políticas são programadas como condições que quando presentes levam a um tratamento diferenciado.

Assim, as requisições vindas de diferentes equipamentos, domínios, regiões ou outro parâmetro presente na informação da requisição podem ser tratadas de maneiras

diferenciadas quanto à autenticação e quanto aos atributos adicionados à resposta para configuração do acesso à rede na autorização.

Entre as inúmeras *policies,* normalmente configuradas nos sistemas de autenticação e autorização, cabe destacar a política de autorização de acesso por *time out.* Esta *policy* tem como objetivo definir como deve ser tratado pelo NAS ou pelo Servidor RADIUS *relay*, a inexistência da resposta para a mensagem *Access-Request.* Esta definição prévia tem importância muito significativa nos sistemas que trabalham com grandes volumes de requisições.

Conforme já explanado, por motivos regulatórios as autenticações e consequentemente as permissões de acesso à Internet dos clientes finais são redirecionadas aos ISPs pelas concessionárias. Isto reflete em ser decisão do ISP se um determinado cliente final que ele não conseguiu autenticar corretamente deve ou não ter o acesso concedido.

Considerando os volumes de clientes finais atendidos, principalmente no caso de ISPs de grande porte, há uma preocupação adicional de qual será o resultado se, por alguns minutos, o servidor de autenticação estiver inativo. Uma falha, mesmo que por curto intervalo de tempo, pode significar um volume enorme de clientes sem acesso, o que reflete no congestionamento dos *Call Centers* de atendimento e na consequente insatisfação dos clientes finais. Por este motivo, muitas vezes os ISPs que têm grandes volumes solicitam à concessionária que, para as Requisições de Acesso de clientes finais que utilizam os seus domínios, caso estas não sejam respondidas por eles (*time out*), sejam consideradas como aceitas no RADIUS *relay,* que desta forma responde ao NAS com um *Access-accept*.

Embora do ponto de vista operacional a condição seja justificável, há uma falha de segurança nesta concessão de acesso, uma vez que o cliente final que tiver com *login* inválido, senha inválida ou até bloqueado por falta de pagamento ou outro motivo no ISP, poderá vir a ter acesso aos recursos de rede caso sua requisição não seja respondida, o que pode ocorrer em caso de congestionamento, principalmente por ser uma comunicação UDP.

No RADIUS do provedor, também podem ser implantadas *policies* específicas para tratamento diferenciado de clientes finais, o que possibilita ao ISP responder de acordo com sua conveniência tanto casos autenticados com *Access-Reject* ao invés de *Access-Accept*, como casos não autenticados com *Access-Accept* ao invés de *Access-Reject*, sem nenhum controle adicional do RADIUS *relay*. Este ponto é muito importante para análise comportamental dos clientes finais, visto que informações de brechas de acesso circulam muito rapidamente na rede Internet.

Cabe citar que, pelas *policies* configuradas em seu servidor de autenticação, um ISP pode, por exemplo, permitir o acesso de todos os clientes finais que chegarem ao seu RADIUS (*Accept-all*), de todos os clientes finais que têm o nome de usuário cadastrado na sua base de dados ou ainda todos aqueles que estiverem na base de dados e não estiverem inadimplentes, independentemente da confirmação de sua senha. Todas estas possibilidades devem ser averiguadas quando há comportamento anômalo nas concessões de acesso feitas por um ISP, para que se destine o correto tratamento.

# 3 - ANÁLISE DA SOLUÇÃO EXISTENTE E DOS DADOS PRELIMINARES

Neste capítulo há uma descrição da solução originalmente implantada na Brasil Telecom para o tratamento dos dados de AAA e uma análise dos dados gerados, mostrando os resultados obtidos das leituras e comparando-os com outros dados para identificar os desvios e os possíveis problemas em relação à qualidade dos mesmos para fins de faturamento dos serviços.

## 3.1 - SOLUÇÃO DE GERAÇÃO, TRATAMENTO E ARMAZENAMENTO DOS DADOS

O objetivo principal do sistema originalmente implantado para o tratamento dos bilhetes gerados pelos sistemas de AAA é a cobrança dos serviços de acesso remoto pelo seu uso. Na Brasil Telecom, assim como nas demais empresas de telecomunicações, os sistemas de geração da informação de bilhetagem (geração dos bilhetes RADIUS ou bilhetes de STOP) são complexos, principalmente pelo volume e pela descentralização e utilização em *cluster*, além da obrigatoriedade de redirecionamento da autenticação aos ISPs, por ser uma concessionária. Nesta empresa, o desenvolvimento e implantação dos sistemas de coleta e armazenamento de dados de autenticação de ADSL para finalidade de cobrança de serviços dos ISPs foi iniciado ao longo do ano de 2006.

O sistema desenvolvido usa como base de informação os dados de bilhetagem gerados pelos sistemas de autenticação, que são formados por três conjuntos de servidores RADIUS. Estes servidores são configurados como primários ou secundários em todos os agregadores da rede da empresa e fazem também a comunicação com sistemas externos, como o redirecionamento da autenticação para os ISPs.

Este conjunto de servidores é o responsável pela autenticação dos produtos de acesso ADSL de uso residencial ou pessoa física, que até outubro de 2009 eram comercializados somente com o nome comercial “Turbo” e atualmente são comercializados também com a marca “Oi Velox”.

Conforme já visto, o processo de bilhetagem RADIUS pode ser gerado pelas informações contidas nas Requisições de Bilhetagem de *Start* e de *Stop*, sendo que as Requisições de Bilhetagem do final da sessão (*stop*) é que contém todas as informações necessárias para contabilização da sessão, pois possuem, além das informações já constantes no bilhete de *start*, a duração (informação exata de horário de início e fim) e *bits* trafegados até o final da sessão.

Os bilhetes de contabilização do RADIUS contêm grande quantidade de informações trazidas em seus atributos sobre as características da conexão e sobre os recursos utilizados. Nem todas estas informações são necessárias para a finalidade de contabilização e de cobrança de serviços por sua utilização. Considerando as finalidades de identificação do usuário, estudo de perfis de utilização e medição dos serviços para cobrança pela utilização, apenas alguns dos campos de informação do bilhete são necessários e, por se tratarem sempre de volumes muito elevados de bilhetes, a solução tem como segunda fase, após a geração e coleta dos dados, um sistema para o processamento dos bilhetes originais e gravação de novos bilhetes, resumidos com as informações necessárias, que passam a ser os bilhetes utilizados no restante do processo.

Para esta filtragem inicial e também para a retirada dos bilhetes duplicados ou nulos, foi adotada a utilização dos sistemas de mediação da operadora, os mesmos que são utilizados para tratamento dos bilhetes de telefonia, chamados de CDRs (*Call Detail Record*), que são dimensionados para tratar grandes volumes de dados. Assim, no fluxo definido para o seu tratamento inicial, os bilhetes de *stop* são gerados pelos sistemas de *accounting* do RADIUS e depois são coletados pelo sistema de mediação, que faz a filtragem, retira bilhetes duplicados e prepara novos bilhetes resumidos e formatados para o envio aos sistemas de faturamento.


Figura 3.1: Fluxo de tratamento dos bilhetes do RADIUS

Na Figura 3.1 é representado o fluxo que inicia na geração dos dados, que são os bilhetes de contabilização do final das conexões *(stop)*, ou bilhetes de *accounting* do RADIUS, seguido pela sua coleta e preparação no sistema de mediação (MDS) e posteriormente pelo envio ao sistema de faturamento (SFA). Estes sistemas são descritos a seguir.

### 3.1.1 - Sistema de mediação da operadora (MDS)

O sistema de mediação, adotado para o tratamento inicial (preparação) dos bilhetes de contabilização do RADIUS, é utilizado na operadora para fazer a centralização, compatibilização e a padronização de toda a bilhetagem das chamadas efetuadas e recebidas pela operadora para que possam ter o formato que é aceito no processamento nos sistemas de faturamento.

O sistema utilizado na operadora para finalidade de mediação é o BMP (*Billing Mediation Plataform*), desenvolvido pela EHPT (*Ericsson Hewlett-Packard Telecommunications*), que é um sistema de grande porte que utiliza como plataforma os servidores *Superdome*, fabricados pela HP (*Hewlett-Packard)*, instalados nos *Data Centers* de Porto Alegre (RS) e Curitiba (PR). Este sistema processa atualmente mais de 200 milhões de CDRs *(Call Detail Record)* por dia e foi implantado no projeto de convergência da empresa, como sistema principal para centralização e compatibilização da bilhetagem gerada pelas diversas plataformas.

O MDS prepara os bilhetes de contabilização do RADIUS para terem um dos formatos aceitos pelo sistema de faturamento SFA, conforme visto na Figura 3.2, com uma série de campos de informações, para onde são transcritas as informações dos atributos dos bilhetes de *accounting* originais do RADIUS.

```
Fixed   Id                              *       1       ascii           '1'
Field   IDdoIPDR                        *       6       ascii   R/'0' '0'
Field   DataEvento                      *       8       ascii   R/'0' '0'
Field   HoraEvento                      *       6       ascii   R/'0' '0'
Field   DuracaoDoEvento_h               *       3       ascii   R/'0' '0'
Field   DuracaoDoEvento_m               *       2       ascii   R/'0' '0'
Field   DuracaoDoEvento_s               *       2       ascii   R/'0' '0'
Field   DataFinalDoEvento               *       8       ascii   R/'0' '0'
Field   HoraFinalDoEvento               *       6       ascii   R/'0' '0'
Field   ElementoDeColeta                *       30      ascii   L/' ' ' '
Field   ElementoDeRedeUtilizado         *       30      ascii   L/' ' ' '
Field   InterfaceFisica                 *       16      ascii   L/' ' ' '
Field   PortaDeServico                  *       10      ascii   L/' ' ' '
Field   TipoDeServico                   *       4       ascii   R/'0' '0'
Field   ClasseDeTarifacao               *       4       ascii   R/'0' '0'
Field   ClasseDoServico                 *       4       ascii   R/'0' '0'
Field   IPCliente                       *       32      ascii   L/' ' ' '
Field   IdentificacaoDoCliente          *       60      ascii   L/' ' ' '
Field   IdentificacaoDeUsuario          *       60      ascii   L/' ' ' '
Field   TelefoneDoCliente               *       15      ascii   R/'0' '0'
Field   TelefoneDoUsuario               *       15      ascii   R/'0' '0'
Field   BytesDeUpload                   *       20      ascii   R/'0' '0'
Field   BytesDeDownload                 *       20      ascii   R/'0' '0'
Field   BandaUtilizada                  *       15      ascii   R/'0' '0'
Field   BandaExtraUtilizada             *       15      ascii   R/'0' '0'
Field   QoS                             *       15      ascii   L/' ' ' '
Field   Protocolo                       *       15      ascii   L/' ' ' '
Field   ArquivoDeConteudo               *       160     ascii   L/' ' ' '
Field   TipoDeConteudo                  *       20      ascii   L/' ' ' '
Field   ValorTarifado                   *       10      ascii   R/'0' '0'
Field   RecursoUtilizado                *       10      ascii   R/'0' '0'
Field   EmailDeOrigem                   *       80      ascii   L/' ' ' '
Field   EmailDeDestino                  *       80      ascii   L/' ' ' '
Field   NumeroDeMensagens               *       6       ascii   R/'0' '0'
Field   Reserva                         *       88      ascii   L/' ' ' '
Field   Reserva                         *       87      ascii   L/' ' ' '
Field   Reserva                         *       12      ascii   R/'0' '0'
Field   Reserva                         *       12      ascii   R/'0' '0'
Field   StatusDoBilhete                 *       2       ascii   R/'0' '0'
Field   SequencialDeFatiamento          *       4       ascii   R/'0' '0'
Field   IDDoBilheteOriginalDeFatiamento *       15      ascii   R/'0' '0'
Field   Filial                          *       15      ascii   L/' ' ' '
Fixed   *                               *       1       bin     0x0a
```

Figura 3.2: Campos escolhidos para o tratamento de faturamento

Na Figura 3.2 estão informados todos os campos presentes nos bilhetes que são recriados pelo MDS com as informações do bilhete de *accounting* do RADIUS. Nesta figura estão destacados com um retângulo os campos reserva, que podem ser utilizados

para adição de informação, e sublinhado o campo de informação da PortaDeServiço, ambos são referenciados no desenvolvimento da solução neste trabalho.

### 3.1.2 - Sistema de faturamento (SFA)

O sistema de faturamento utilizado na empresa é o SFA (Sistema de Faturamento e Arrecadação), que opera sobre a plataforma *Mainframe* da IBM (*International Business Machines*). Este sistema é o responsável por fazer todo o tratamento dos bilhetes e das regras de negócio dos serviços implantados, fazendo a interface com os sistemas MDS (mediação), SAC (Sistema de Atendimento a Clientes), SAF (Sistema de Apoio ao Faturamento) e do CRM (*Custom Relationship Manager*) Clarify.

O sistema SFA é utilizado na operadora para o faturamento de serviços prestados para os clientes que tem serviços contratados com valor fixo mensal, que tem seus serviços e valores mensais cadastrados nos sistemas SAC e Clarify, e também para o faturamento dos serviços medidos, que são inicialmente consolidados pela mediação (MDS) e depois processados no SFA para geração dos arquivos que são encaminhados para impressão de faturas e notas fiscais de serviços.

### 3.1.3 - Solução de medição e faturamento

A solução completa usa então os sistemas RADIUS, MDS e SFA, sendo que no processo final de faturamento dos serviços, existe a necessidade de separar o faturamento por filiais, atendendo a correta alocação de impostos para cada UF (Unidade da Federação).

Assim, os bilhetes gerados pelo RADIUS e preparados pelo MDS seguem um fluxo de distribuição por UF no SFA, gerando a contabilização e o faturamento em cada estado.

O diagrama da Figura 3.3 a seguir mostra a sequência de servidores e sistemas envolvidos na geração dos relatórios de faturamento.

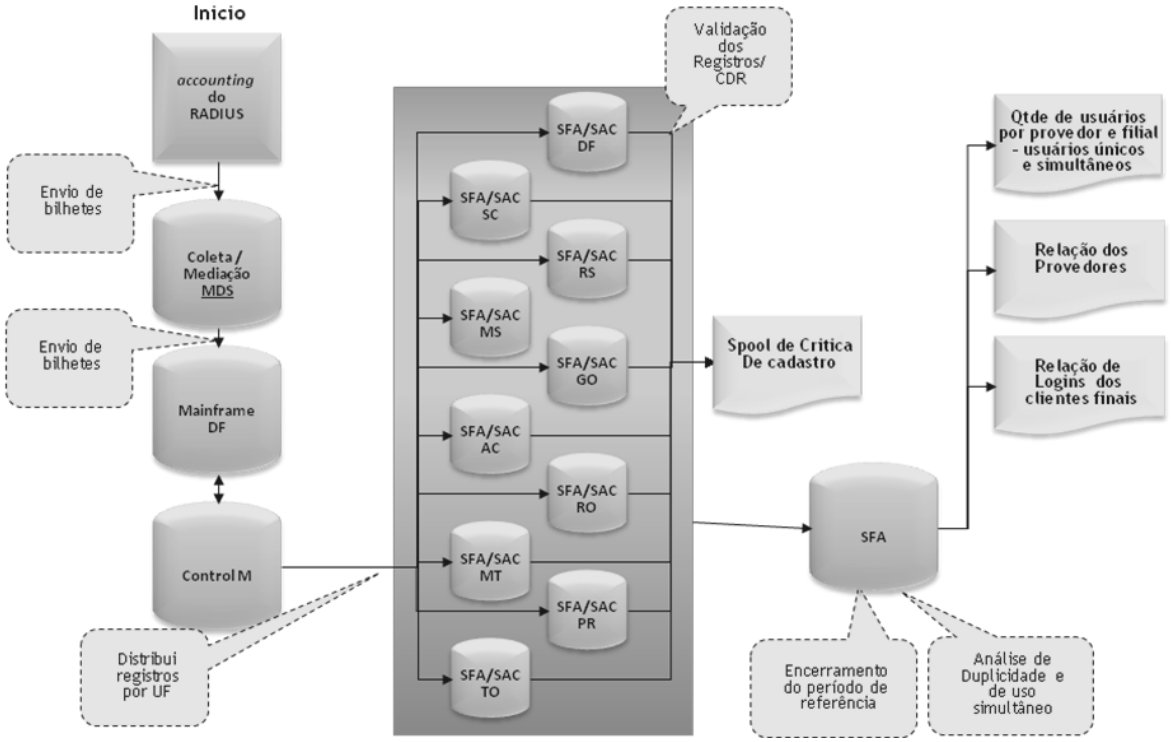



Figura 3.3: Macro Fluxo – Geração de relatórios de faturamento [OIa]

Na Figura 3.3, adaptada da apresentação interna da área de faturamento da empresa [OIa], pode ser identificado o fluxo dos dados na solução de tratamento para o faturamento, que inicia no canto superior esquerdo, pela geração de bilhetes nos sistemas de AAA. Os dados de contabilização do RADIUS são inicialmente armazenados em uma base de dados volátil (retenção de três meses), identificada no diagrama como "*accounting* do RADIUS". Dessa base de dados são coletados pelo MDS os arquivos sequenciais de bilhetes de *stop* com suas informações completas. O MDS filtra os bilhetes, associando os domínios aos ISPs e aos seus números de serviço, de acordo com uma tabela de conversão e, na sequência encaminha ao *Mainframe*. Aí, a ferramenta *Control M* sequencia o envio

ao sistema de faturamento SFA de cada filial. O SFA gera então os relatórios que podem ser utilizados para o faturamento de cada provedor.

A solução inicial de faturamento dos serviços foi concebida para não gerar a fatura de maneira automática. O objetivo inicial era ter apenas a geração de três relatórios, que possibilitam o faturamento manual, listados a seguir:

a) arqlogin: resumo por ISP com usuários (lista de usuários que tiveram o acesso permitido e uso simultâneo se houver).

b) arqdetal: bilhetes com autenticações (lista de bilhetes no período que permite a identificação e comprovação dos usos simultâneos)

c) arqprove: resumo de ISPs (nome dos provedores que permitiram o acesso de clientes em uma determinada UF)

## 3.2 - AMOSTRAGEM INICIAL

Para que se pudesse avaliar a qualidade dos dados no desenvolvimento inicial, foram analisadas as amostragens tomadas no segundo semestre de 2007. Essas informações já estavam sendo utilizadas para cobrança de serviços, apesar de uma parte significativa dos acessos não estarem sendo contabilizados, uma vez que os resultados das medições informavam um número baixo de usuários em relação ao volume total de acessos em serviço. Adotando a premissa de que os agregadores e os NAS não “criam” bilhetes, havia a certeza de que a cobrança realizada seria sempre inferior ao número real de usuários finais que tiveram o acesso permitido por um ISP.

## 3.3 - QUALIDADE DOS DADOS

Para medir a qualidade dos dados, com o objetivo de ter parâmetros para mensurar os resultados dentro deste trabalho e para o próprio acompanhamento dos resultados na empresa, foram criados alguns indicadores descritos a seguir:

a) **Percentual de usuários medidos em relação à base** – Neste indicador é considerada a proporção entre o total de usuários finais medidos, inclusive aqueles medidos como acesso simultâneo, e o total da base de usuários finais ativos nos produtos ADSL de uso residencial. O objetivo deste indicador é medir a eficiência nos sistemas de medição, identificando a fração da base que está sendo medida.

b) **Percentual de usuários únicos em relação aos usuários medidos –** Neste indicador é considerada a proporção entre o total de usuários finais únicos, sem considerar o uso simultâneo, ou seja, apenas a contagem dos *logins* distintos, e o total da base de usuários finais medidos (com simultâneos). O objetivo deste indicador é medir a quantidade de usuários simultâneos medidos, principalmente para avaliar o impacto deste tipo de acesso em relação à eficiência das medições e do próprio faturamento dos serviços dos provedores de acesso, que normalmente cobram apenas pela disponibilização de um *login*, não medindo o seu uso simultâneo.

c) **Percentual de usuários únicos em relação à base –** Neste indicador é considerado o total de usuários finais únicos, sem considerar o uso simultâneo, em relação à base de usuários finais ativos nos produtos ADSL de uso residencial. O objetivo inicial deste indicador era ter a visibilidade da quantidade que está sendo faturada por provedor, visto que na maioria dos casos o provedor cobra pela disponibilização do *login*. Porém este indicador teve também a característica de medir a eficiência da cobrança dos serviços da operadora durante o período de correções, já que neste período a cobrança se restringiu aos usuários únicos.

## 3.4 - ANÁLISE DA QUALIDADE DOS DADOS OBTIDOS

Com base nos indicadores criados e nas informações técnicas e operacionais dos serviços, foi possível analisar os resultados obtidos nos relatórios das primeiras medições e ter informações sobre a sua qualidade. A seguir analisam-se estes dados preliminares de acordo com os indicadores desenvolvidos.

Nos primeiros meses os relatórios gerados pelo sistema de faturamento apresentaram como resultados informações de que o total de usuários medidos, considerando os usos simultâneos, era entre 15% a 20% maior do que a base instalada. Ou seja, as leituras mostravam contagens de usuários únicos somados aos usos simultâneos maiores do que o total possível, que seria a base total de acessos ADSL de uso residencial ativos (em uso) na planta da operadora.

Assim, para que se pudesse fazer uma análise melhor dos dados, efetuou-se o reprocessamento manual dos bilhetes para verificar os casos onde houve repetição dos atributos (considerados falsos simultâneos). As análises realizadas a seguir utilizaram a base de dados gerada no segundo semestre de 2008 e processada manualmente.

### 3.4.1 - Percentual de usuários finais medidos em relação à base

A primeira informação que se busca em relação à eficiência das leituras e, consequentemente, da qualidade do faturamento gerado por elas, é a quantidade total de clientes finais sobre os quais se poderia emitir o faturamento, ou seja, a contagem de clientes únicos e suas utilizações simultâneas, se existirem.

O gráfico apresentado na Figura 3.4 a seguir mostra o resultado obtido para o indicador de total de usuários finais medidos em relação à base total ativa de acessos ADSL instalados para clientes residenciais. Os dados utilizados são os gerados pelo reprocessamento manual dos bilhetes, com a retirada dos casos onde houve repetição dos atributos (considerados falsos simultâneos). Os percentuais nos meses 11 e 12 apresentam

significativa melhora devido à correção do cadastro de domínios de provedores pequenos que não estavam corretamente cadastrados.

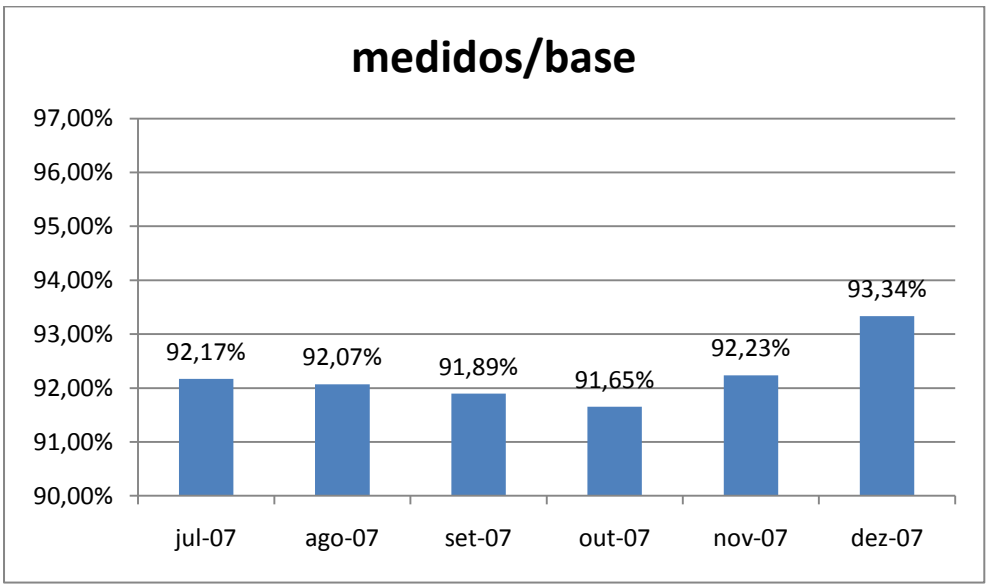



Figura 3.4: Gráfico usuários medidos / base ativa residencial – julho a dezembro de 2007

Mesmo com as correções dos domínios, após a retirada das duplicidades o percentual de usuários finais medidos ficou pequeno em relação às expectativas, indicando falta de eficiência no sistema inicial de medição e contabilização, visto que o objetivo deve ser o faturamento do máximo possível de clientes e as quantidades medidas ficaram significativamente abaixo da base total ativa de acessos ADSL instalados para clientes residenciais.

Uma questão importante a ser considerada é que a geração da mensagem de Requisição de Bilhetagem utilizada no processo de *accounting* é somente a de final de sessão (bilhete de *stop*). Isto está associado à ação de desconexão do usuário final, que também só existe se houver uma conexão original, para posterior desconexão. Desta forma, se um usuário permanece conectado durante todo o mês, ou se ele passa o mês sem se

conectar, não há uma comunicação com o RADIUS, o que leva a inexistência de bilhetes de *accounting* deste usuário no período.

Para os casos onde o usuário permanece conectado, uma solução para a identificação seria a utilização de um mecanismo de verificação da existência da conexão, ou seja, configurar os sistemas (BRAS) para que eles gerem requisições de bilhetagem intermediária para obter a resposta se a conexão está ativa.

Outra possibilidade a ser analisada é a de ocorrência de perda de bilhetes de contabilização, visto que o processo de contabilização não precisa obrigatoriamente ocorrer para que a conexão exista. Para que uma conexão exista é necessário que uma Requisição de Acesso (*Access-Request*) chegue aos sistemas de autenticação e que a resposta de Acesso Permitido (*Access-Accept)* chegue ao agregador, não tendo influência do processo de bilhetagem, que ocorre após o término da conexão, já que utiliza o bilhete gerado no final da sessão (*stop*).

A requisição de *Accounting-Request*, que é gerada pelo NAS no final da sessão, trafega até o servidor de *accounting* do RADIUS utilizando transporte UDP, o qual não fornece garantia de entrega. Se a entrega não for confirmada por uma resposta de Bilhetagem Aceita (*Accounting-Response*), é encaminhada nova Requisição de Bilhetagem, porém, após um número pré-configurado de tentativas, o NAS deixa de enviar a Requisição de Bilhetagem, possibilitando, neste caso, que a conexão não seja corretamente contabilizada.

Uma alternativa para dimensionar a perda real seria uma comparação direta entre a quantidade de mensagens de *Access-Accept* e quantidade de bilhetes de *stop* por período, o que poderia identificar o volume desta perda. Porém esta perda está associada à configuração de tentativas de reenvio das Requisições de Bilhetagem e ao congestionamento na rede e nos equipamentos envolvidos, o que tende a tornar a medição muito variável para cada sistema.

### 3.4.2 - Percentual de usuários únicos em relação aos usuários medidos

O gráfico apresentado na Figura 3.5, a seguir, mostra o resultado obtido para o indicador de total de usuários únicos em relação ao total de usuários medidos (com simultâneos). Este indicador é muito importante para os ISPs, visto que o faturamento de seus serviços normalmente é por usuário único e todo o uso simultâneo pode ser uma despesa adicional, já que nos contratos com as operadoras está prevista a cobrança de usuários nestas condições.

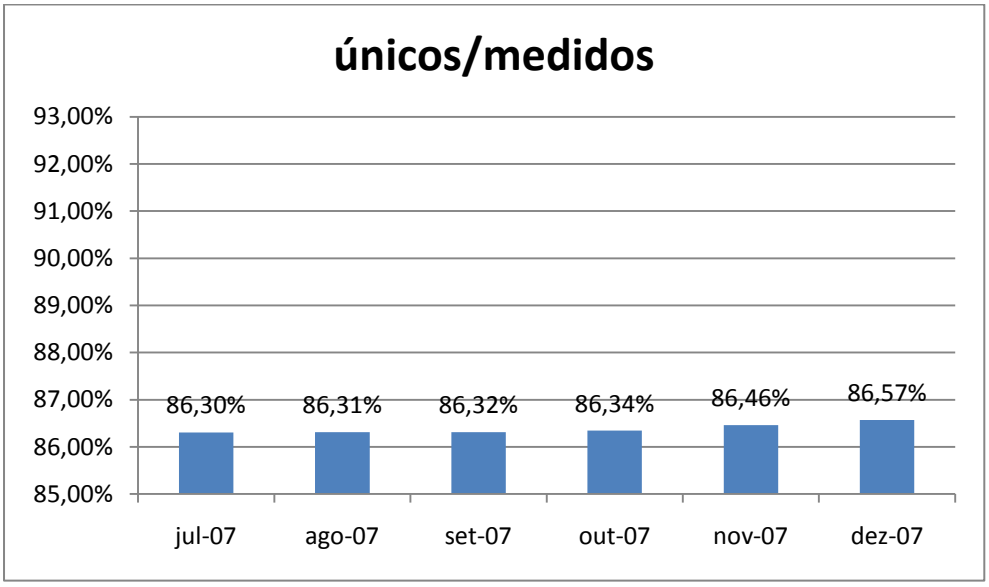



Figura 3.5: Gráfico usuários únicos / usuários medidos – julho a dezembro de 2007

A percentagem neste indicador mostra o descontrole visível do uso simultâneo de *logins* nos principais provedores. Os volumes de usuários finais únicos na ordem de 86% dos medidos indicam a ocorrência de uso simultâneo em 14% dos aproximadamente 1,4 milhões de usuários medidos, ou seja, cerca de 180 mil usuários utilizando *logins* de outros clientes. A ocorrência deste volume fica muito acima das expectativas, já que o provedor normalmente cobra um valor fixo mensal para disponibilização de acesso vinculado a um *login* e permitir uso simultâneo significa deixar de cobrar de um usuário.

Dentro do processo de investigação dos motivos para se ter um volume exagerado de usuários com o mesmo *login*, foram identificadas através da análise dos dados, das informações recebidas dos ISPs e da área técnica da empresa responsável pela implantação e manutenção dos acessos ADSL, as seguintes possibilidades:

a) Simples divulgação de usuários pelos seus *logins* e senhas para amigos e conhecidos.

b) Disseminação de *logins* e senhas na Internet, pelo próprio usuário ou por terceiros.

c) Uso de *logins* e senhas "padrão" pelos técnicos que instalam o serviço ADSL para o usuário final.

Com a continuidade do processo investigativo, em uma análise mais detalhada dos *logins* por provedor, foram identificados exemplos das três ocorrências, sendo os casos mais graves os relatados nas letras "b" e "c".

Os casos isolados de uso do mesmo *login* por mais de 100 usuários simultâneos, quando pesquisados junto aos clientes finais e ISPs, foram na sua maioria identificados como sendo de divulgação na Internet de *logins* e senhas válidos ou da informação de que um determinado provedor não estava controlando corretamente a autenticação. Após a notificação, na maioria dos casos, os próprios ISPs fizeram ações corretivas de bloqueio e de contato com o cliente final para que este alterasse seu *login* ou sua senha.

Em menor volume, alguns casos foram identificados como a utilização por técnicos de *logins* e senhas que eles tinham a informação de ser válidos. Como na experiência destes técnicos eles sabiam que determinados ISPs não controlavam o seu uso simultâneo, acabavam usando em quase todos os clientes finais por eles configurados, seja por facilidade de não ter que perguntar ao cliente o *login* e senha corretos ou, aliados ao cliente final, para evitar o pagamento dos serviços a um ISP.

### 3.4.3 - Percentual de clientes únicos em relação à base

O gráfico apresentado na Figura 3.6, a seguir, mostra o resultado obtido para o indicador de total de usuários únicos em relação à base total ativa de acessos ADSL instalados para clientes residenciais:

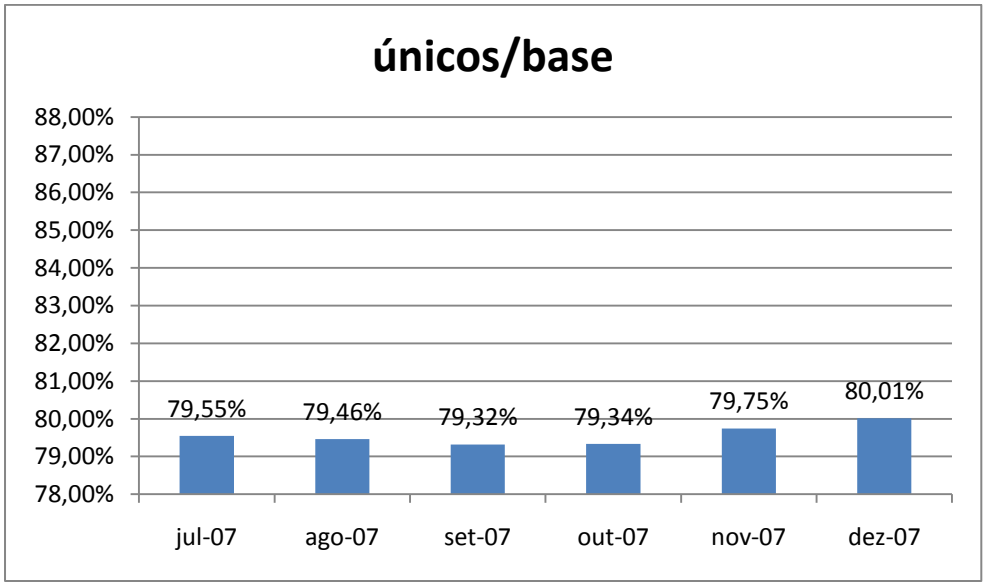



Figura 3.6: Gráfico usuários únicos / base ativa residencial – julho a dezembro de 2007

Quanto maior for este indicador, maior é a eficiência dos sistemas de autenticação da operadora e dos provedores juntos, ou seja, a maior quantidade de clientes finais pagantes aos provedores. O resultado deste indicador para toda a base da operadora indica o comportamento médio dos clientes finais, associado às ações corretivas ou punitivas implantadas pela operadora ou pelos ISPs em relação ao uso simultâneo. Este indicador utilizado sobre a base de um ISP específico mostra a sua eficiência em controlar o uso simultâneo, que está associada a sua receita, visto que o uso simultâneo dificilmente é cobrado pelo provedor e pode ser cobrado pela operadora.

Além disso, este indicador e os seus resultados foram utilizados para acompanhar mês a mês a evolução obtida com a implantação das correções e das soluções propostas controle da autenticação, para que se tenham cada vez maiores quantidades de usuários sendo autenticados com seus *logins* e senhas próprios. Quanto maior este indicador, mais eficiente está o conjunto em relação à identificação correta dos clientes finais.

Este indicador também teve grande importância para a operadora durante o desenvolvimento das soluções, principalmente porque, devido à consciência da ineficiência da medição dos usuários simultâneos no início da cobrança pelos serviços, todo faturamento foi baseado exclusivamente nos usuários únicos medidos durante todo o ano de 2007 e parte do ano de 2008.

### 3.4.4 - Contestações

Ainda nos primeiros meses de prestação dos serviços, muitos dos provedores indicaram presença de nomes de usuários desconhecidos, ou seja, que não estavam presentes na sua base de clientes, ou na sua base de *logins*, mesmo entre os inativos.

A análise de amostragem de bilhetes evidenciou que havia a autorização por *time out* para vários casos. Estes casos foram interpretados junto aos ISPs como sendo relativos às seguintes ocorrências:

a) Usuários com nome de *login* escrito errado, por exemplo usando o *login* nomedeuuario@isp.com.br, enquanto na base do ISP estava cadastrado com o *login* “nomedeusuario@isp.com.br”.

b) Usuários com senhas erradas ou bloqueados por falta de pagamento e que permaneciam com acesso

c) Usuários que já estiveram na base do provedor, porém não tem mais contrato de serviços e o *login* foi excluído da base o provedor.

Considerando que havia a necessidade de manter ativa a *policy* de *time out* para alguns provedores, principalmente para os que têm volume muito grande de clientes, ficou evidenciado que ainda havia um problema a ser resolvido, visto que todas as ocorrências de contestação da amostragem foram identificadas como acessos permitidos por *time out*.

Como medida inicial, a operadora passou a aceitar todas as contestações onde os bilhetes traziam a informação de que permissão de acesso havia sido por *time out*, até que se tivesse uma solução para o problema ou uma forma de reduzir este tipo de ocorrência.

Outro ponto que gerou preocupação foi o volume de clientes que tiveram o acesso permitido mesmo estando com sua senha errada, principalmente porque a eliminação da política de acesso por *time out* resultaria em rejeição na próxima requisição de acesso do cliente, embora este cliente estivesse adimplente na operadora e no provedor.

Além dos problemas de contabilização, também foi identificado o grande desconforto de muitos clientes nesta situação. Muitos deles não sabiam da falha em sua autenticação e, como tinham seu acesso permitido somente quando acontecia um *time out*, eram obrigados a aguardar por até vários minutos depois de ligarem os seus *modems* para que pudessem acessar a Internet.

# 4 - PROPOSTA DE SOLUÇÃO TÉCNICA PARA OS SISTEMAS E PROCESSOS

Uma vez identificados os problemas encontrados na base, neste capítulo propõe-se uma solução técnica para que os dados se tornem suficientemente confiáveis para o uso nos processos de faturamento e como fonte de informação gerencial.

## 4.1 - CORREÇÕES PROCESSUAIS

As primeiras análises dos dados levaram à constatação de que os domínios de alguns ISPs não estavam corretamente cadastrados nos sistemas. Isto ficou evidente no relatório de provedores medidos por UF, o que resultou na indicação de algumas correções preliminares no cadastro dos sistemas, na configuração e no processo de autenticação dos provedores. Estas medidas foram rapidamente implantadas e, a seguir procede-se ao seu detalhamento.

### 4.1.1 - Correções do cadastro dos domínios dos ISPs nos sistemas

O domínio, também chamado de *realm*, é utilizado no processo de redirecionamento da autenticação para um ISP conforme visto no Capítulo 2. Em princípio considera-se que apenas os usuários finais que têm em seu *login* o domínio de um ISP devam ser a ele contabilizados. Porém é normal que um ISP utilize mais de um domínio, como, por exemplo, “isp.com” e “isp.com.br” e, por razões distintas, até acrescentar ou mudar seus domínios ao longo de sua operação.

Qualquer alteração ou utilização de novos domínios deve ser corretamente cadastrada nos sistemas de tratamento da medição dos usuários, sob pena de não serem contabilizados, já que a alocação final é de usuários finais por domínio.

No caso específico da solução adotada na operadora, considerando a utilização do SFA, há ainda a necessidade da associação do bilhete a um número de serviço, que é o número de serviço do provedor em uma determinada filial (semelhante a um número de acesso de telefonia ou de dados), que este sistema utiliza como referencia para associação dos clientes medidos e do uso simultâneo.

Para que esta associação ocorra corretamente é necessário que seja cadastrada uma tabela de conversão de domínios em "números de serviço" no MDS, para que esse possa adicionar esta informação nos bilhetes por ele gerados, resultando no processamento do bilhete para o ISP associado ao "número de serviço" no SFA.

A primeira correção implantada, a partir da constatação de irregularidades e identificação de domínios não associados a terminais, foi a correção da tabela de associação no MDS e respectiva adequação a números de serviço no SFA, que ocorreu já nos primeiros três meses do início da medição e cobrança dos serviços.

### 4.1.2 - Redução do uso da política de liberação de acesso por *time out*

Devido à questão regulatória já comentada, as concessionárias de telecomunicações de telefonia fixa têm que reencaminhar a autenticação do usuário para um ISP, que faz esta atividade e responde para a operadora com um *Access-Accept* ou *Access-Reject*. Historicamente a ausência de resposta do ISP, era interpretada pelos sistemas da operadora como *time out*, porém, pela *policy* pré-configurada, era convertida em *Access-Accept* pelo RADIUS, que encaminhava esta respostas como autorização de acesso para o NAS, que por sua vez liberava o cliente final para o uso dos serviços. O principal motivo desta configuração era que uma falha em um servidor de autenticação de um ISP gerava um volume muito grande de chamados dos usuários reclamando de não conseguir navegar na Internet.

O resultado prático desta política foi o surgimento de um volume significativo de usuários finais que acessavam com *logins* ou senhas inválidos, apenas devido a insistência

de retransmissão feita por *modem*s com *login* e senha configurados (modo *router*) e que automaticamente ficavam reenviando a requisição de autenticação, até que em um momento a resposta não retornava aos servidores da operadora, liberando o acesso com um *accept* por *time out*.

Como o tratamento da autenticação é de responsabilidade do provedor, por aspectos regulatórios, a escolha se a falta de resposta deve ocasionar uma permissão de acesso ou uma solicitação de retransmissão é também de responsabilidade dos ISPs. Assim, embora a escolha seja do ISP, a operadora passou a indicar a adoção preferencial da segunda alternativa, evitando-se a permissão de acesso à rede sem a devida identificação do cliente final.

A grande maioria dos ISPs aderiu a proposta e solicitou a retirada da *policy* de autorização por *time out* de seus domínios nos sistemas da operadora, principalmente por motivos econômicos, já que os clientes finais autorizados em um determinado domínio são cobrados do ISP responsável pelas requisições autorizadas nele. Esta implantação, embora processual e relativamente simples, resultou em redução significativa de usos indevidos e de contestação de usuários pelos próprios ISPs.

Porém, os ISPs com grandes quantidades de clientes optaram por não solicitar a mudança da política de tratamento do *time out*, alegando que, se fosse alterada, qualquer pequena falha nos seus servidores de autenticação ou na comunicação destes servidores com a rede da operadora causaria volume extremamente alto de usuários finais sem autenticação e consequentemente sem acesso. Além de ser uma experiência indesejada para o cliente, isto teria impacto direto no aumento de reclamações feitas nos *Call Centers* da operadora ou do provedor em volumes não suportados pelos atendimentos normais das empresas. A falta de viabilidade de retirada da política forçou a desenvolvimento de outra solução para evitar o acesso indevido, que será vista na seção 4.3.

## 4.2 - SOLUÇÃO PARA EVITAR O USO SIMULTÂNEO DE *LOGIN* E SENHA

Há grande preocupação em identificar clientes que possam ter utilizado um recurso para fins ilícitos. Porém, em muitos casos, os responsáveis pela autenticação não dispõem de configurações adequadas para impedir a utilização de um mesmo *login* e senha por mais de um cliente. Esta falha de configuração possibilita a utilização, autorizada ou não, de *login* e da senha de um usuário por outros, dificultando a cobrança pelos serviços e a identificação quando necessária.

A tarefa de impedir a conexão simultânea não é tão simples quanto parece. Alguns modelos de *modems*, quando utilizados como *bridge,* permitem que um usuário que tenha mais de um equipamento em sua residência possa fazer mais de uma conexão, neste caso utilizando o mesmo recurso de acesso (mesma conexão ADSL), o que deve ser permitido. Outro ponto é que ao se desconectar e se reconectar, a mensagem de Requisição de Bilhetagem (*Accounting-Request*), gerada pelo NAS no final da sessão, pode não chegar ao RADIUS do ISP. A ausência deste bilhete resulta na interpretação pelo servidor remoto de que o *login* ainda está em uso. Esta ocorrência, caso não seja tratada corretamente, pode causar a recusa de acesso para um cliente que o está solicitando e tem direito ao seu uso.

Por estes motivos, foi desenvolvida a primeira parte da solução, que é um sistema de identificação do uso simultâneo e de diferenciação do "falso simultâneo". A solução foi idealizada para que o ISP possa identificar se uma Requisição de Acesso (*Access-Request*) recebida que contém em seus atributos um *login* que já está em uso é do mesmo cliente final ou se é de outro tentando utilizá-lo.

### 4.2.1 - Desenvolvimento da solução de identificação de uso simultâneo

Como base para o desenvolvimento da solução, foi considerado que somente conexões com o mesmo *login* e partindo de portas físicas com identificações diferentes devem ser tratadas como uso simultâneo. Os casos com solicitação com mesmo *login* e

provenientes de mesma porta física, devem ser considerados como uso normal, mesmo que esta utilização se sobreponha a outra no mesmo período.

Para isto escolheram-se atributos do RADIUS com as informações de porta para permitir a diferenciação dos acessos físicos utilizados pelos clientes finais. Conforme visto no capítulo 2, seção 2.7.7 -, os campos NAS-Port e NAS-Port-Type estão presentes em todos os bilhetes de contabilização da operadora. Entretanto, o campo NAS-Port-Id não está obrigatoriamente presente.

Três alternativas foram avaliadas inicialmente: utilizar a metodologia de identificação desenvolvida por [HENZ2008], somar os campos NAS-Port e Nas-Port-Id e formar uma nova string que seria utilizada para identificar melhor a porta física ou utilizar apenas o campo NAS-PORT, com vantagens de simplicidade operacional.

Por questões de prazos, a alternativa de utilizar o campo de identificação desenvolvido por [HENZ2008] não pôde ser utilizada, visto que a sua implantação ainda estava em andamento na empresa e não contemplaria grande parte dos bilhetes.

A alternativa de soma dos campos, embora agregasse um pouco mais de segurança, teria necessidade de alteração na programação da construção dos bilhetes no MDS, com aumento da necessidade de maior processamento, e também na programação utilizada para controle de simultaneidade nos ISPs, esta considerada mais complexa caso adotada.

A alternativa de utilizar apenas a informação do Nas-Port, mesmo com a possibilidade de haver coincidência de numeração deste campo para portas distintas, foi considerada a melhor por questões de prazo e de complexidade. A possível duplicidade de numeração levaria apenas a não considerar uma conexão como simultânea, por ser tratada como sendo da mesma porta, porém a contabilização neste caso seria sempre menor.

Para que o campo NAS-Port pudesse ser processado em toda a sequência de sistemas envolvidos, foi necessário selecionar os campos a serem utilizados dentro do bilhete resumido, que é gerado pelo MDS e posteriormente encaminhado para o sistema de faturamento (SFA). Observando a Figura 3.2, pode ser constatado que este bilhete tem um campo específico para identificação da porta de serviço (sublinhada na figura). Porém, este

campo tem tamanho limitado a 10 caracteres, inferior ao existente na identificação da porta de serviço de alguns DSLAMs, o que prejudicaria o seu uso.

Na mesma figura pode ser identificada também a existência de campos de reserva para futuras utilizações. Destes, o primeiro tem tamanho limitado a 88 caracteres, o que permite a inserção dos atributos de NAS-Port ou até dos campos NAS-Port-Id somados caso necessário, embora a escolha inicial tenha sido de utilizar somente o campo NAS-Port, o que poderia ser alterado caso necessário no futuro, permitindo maior precisão na eliminação de uso simultâneo. Assim, o primeiro campos dos identificados na figura como reservadoss foi selecionado para utilização e passou a ser identificado como campo Porta-do-Cliente.

No sistema SFA, as conexões sobrepostas de um mesmo *login* são tratadas como se fossem chamadas telefônicas simultâneas. Este sistema, pelo seu porte, consegue processar os milhares de bilhetes, verificando se no seu período de utilização existiam outras conexões em andamento e utilizando o mesmo *login*. Caso não exista esta conexão é contabilizada normalmente. Caso exista, compara o campo PORTA DO CLIENTE e, se for diferente, marca esta conexão como válida para cobrança, se for igual, descarta da contabilização.

O sistema SFA permite ainda criar um limite mínimo de coexistência de conexões simultâneas para que elas sejam contabilizadas. Este limite pode ser uma segurança redundante para evitar que conexões reiniciadas pelo mesmo cliente final sejam contabilizadas, embora elas devam ser descartadas por serem geradas com mesma identificação de porta.

Como critério de cobrança, no término do período de contabilização, no caso configurado para um mês, o sistema SFA identifica os picos de utilização simultânea, acrescentando no relatório de uso uma contagem de simultâneos do *login*, sempre que esta situação ocorrer. Esta marcação permite que sejam cobrados os usos simultâneos, tanto na geração manual como numa possível geração automática da fatura.

### 4.2.2 - Notificação aos ISPs da cobrança dos usuários simultâneos

No relacionamento comercial entre a operadora pesquisada e os ISPs, os contratos já previam que a autorização de usuários simultâneos com mesmo *login* era passível de cobrança. Porém, na fase inicial da cobrança dos serviços, antes da implantação da solução citada na seção anterior, a contabilização destes usuários era duvidosa e os volumes significativos.

Com a implantação da solução, o passo seguinte foi o envio de notificação formal aos ISPs do início da cobrança prevista em contrato, informando o prazo de 90 dias para que os ISPs retomassem seus controles e passassem a não permitir, ou pelo menos passassem a cobrar o uso simultâneo de *login*, possibilitando que os provedores fossem cobrados apenas por clientes finais que pagam a eles pelos serviços.

Nesta notificação foi descrito também que todo o controle de uso simultâneo no lado da operadora é feito baseado na conexão utilizando mesmo *login*, porém com NAS-Port diferente. Qualquer conexão com o mesmo *login* e mesmo NAS-Port não é considerada como acesso simultâneo e é descartada da contabilização.

Esta comunicação e o início efetivo da cobrança, aliados à implantação da solução na rede da operadora e às implantações de controles pelos principais ISPs, possibilitou uma redução significativa do uso simultâneo de *logins*, conforme será apresentado no capítulo cinco, onde são descritos os resultados obtidos.

## 4.3 - PÁGINA DE AVISO DE FALHA DE AUTENTICAÇÃO

Considerando o problema que permaneceu pela impossibilidade de retirada da *policy de time out* para os grandes ISPs e a consequente brecha de permissão de acesso de clientes finais sem a devida autenticação (liberados por *time out*) ainda permanecia um problema em aberto.

O principal problema da permissão de acesso por *time out* ocorre quando um cliente final que não deveria ser ter o acesso concedido acaba recebendo a permissão de acesso por que não houve a resposta do ISP, que neste caso deveria ser um *Access-Reject*. Numa situação onde o servidor RADIUS está indisponível, seja por falha do servidor ou da sua comunicação com a rede da operadora, esta situação pode até ser aceita, visto que a grande maioria dos clientes finais autorizados é regular. O caso mais grave, então, é aquele no qual um conjunto de *login* e senha, que recebe normalmente respostas de *Accept-Reject*, recebe em uma determinada tentativa a resposta de *Access-Accept*. Esta situação pode ocorrer após muitas tentativas consecutivas, caso comum quando o cliente final utiliza seu *modem* configurado como *router*, o qual encaminha Requisições de Acesso de maneira repetitiva e automática.

Desta forma, a solução idealizada teve como um dos seus objetivos o bloqueio das tentativas repetitivas, evitando que o acesso por *time out* ocorresse de forma tão facilitada, possibilitando então a geração de dados mais confiáveis de faturamento e redução drástica de *logins* não reconhecidos pelos ISPs.

O objetivo técnico, aliado a idealização de um sistema que avisasse ao cliente que sua conexão não estava sendo permitida pelo provedor, com muitos benefícios mapeados para este aviso, possibilitou a criação da parte mais importante da solução proposta por este trabalho, que é a Página de Aviso de Falha de Autenticação. Esta solução consiste em um mecanismo que reconhece se a solicitação do cliente não foi aceita (o ISP respondeu com um *reject*) ou se o domínio informado pelo cliente não existe. Exclusivamente, em um destes dois casos, em vez de liberar o seu acesso à Internet, o redireciona para uma VPN, onde qualquer requisição de visualização de página em seu navegador resulta na apresentação uma página de aviso na sua tentativa de navegação. Esta solução é detalhada nas próximas seções.

### 4.3.1 - Objetivos

No desenho da solução, dois objetivos foram colocados para a Página de aviso de Falha de Autenticação. O primeiro, já citado, e desejado para melhora dos dados de faturamento, foi o objetivo de extinguir acessos de clientes não autenticados pelos ISPs que ocorriam devido a permissões indevidas por *time out*.

O segundo, considerado de grande importância nos objetivos de relacionamento com o cliente final pela empresa, foi a viabilização de um aviso ao cliente final de que sua conexão estava funcionando corretamente, porém ele não havia sido autenticado e não teve seu acesso "autorizado" pelo seu ISP. Esta comunicação, com certeza, permitiria a redução do tempo de atendimento nos *Call Centers* da Operadora e dos ISPs, visto que o cliente, ao ligar para o atendimento, já informaria a ocorrência da página, o que facilitaria para que o atendente direcionasse seu atendimento para a correção de *login* e senha ou liberação do acesso no ISP.

A redução do tempo de atendimento e o direcionamento correto da solução para o cliente final, além de reduzir custos de *Call Center* para operadora e para o ISP, permitem que o cliente seja mais bem atendido, melhorando sua experiência quanto à qualidade de atendimento.

No decorrer do desenvolvimento da solução foi adicionado ainda um terceiro objetivo, que é a redução da necessidade de processamento nos servidores RADIUS e nos agregadores, que passariam a receber um volume muito menor de requisições, visto que, após a exibição da Página de Aviso, os *modems* em modo *router* não ficariam encaminhando novas requisições, por considerarem já estar conectados.

### 4.3.2 - Especificação funcional

A especificação funcional é o documento que indica qual deve ser a resposta funcional esperada da solução, ou seja, qual o comportamento que deve ter a solução de acordo com os cenários identificados.

A específicação funcional da Página de Aviso de Falha de Autenticação prevê a apresentação de uma página de aviso para os casos onde não houve a autorização de acesso do cliente final. Esta negativa pode ocorrer por motivos distintos, o que levou a considerar que a necessidade de redirecionamento da conexão, e consequente exposição da página, deveria ser tratada de acordo com os grupos de possíveis respostas às Requisições de Autorização, conforme listado a seguir:

a) No caso de resposta positiva do ISP (*Access-Accept*), a conexão é aceita normalmente, sendo liberado o acesso à Internet

b) No caso de resposta negativa pelo ISP (*Access-Reject*), a página deve apresentada ao cliente final para qualquer endereço eletrônico que ele tente acessar através de seu navegador.

c) No caso do domínio utilizado não estar cadastrado como um dos domínios de redirecionamento da autenticação, a página deve apresentada ao cliente para qualquer endereço que ele tente acessar através de seu navegador.

d) No caso de *time out* na espera pela resposta do ISP, deve haver um parâmetro ajustável para a apresentação ou não da página. Inicialmente, para o caso de ausência de resposta (*time out*), deve ser considerado que não houve a autenticação e encaminhada uma resposta negativa ao NAS (*Access-Reject*), que a reencaminha ao *modem* ou discador do cliente. Com esta resposta o *modem* pode encaminhar nova Requisição de Acesso ou o cliente pode solicitar a conexão pelo discador.

Os parâmetros para especificação funcional foram desenvolvidos neste trabalho, porém o documento formal da empresa foi desenvolvido dentro da área responsável pelo desenvolvimento de produtos, seguindo as recomendações aqui expostas.

### 4.3.3 - Processo de escolha da solução

A partir da especificação funcional foram viabilizadas as análises das possíveis alternativas de soluções para seu desenvolvimento. Esta análise teve a participação das áreas de Planejamento, Projeto de Comunicação de Dados e Arquitetura de Soluções de TI da empresa. Dentro do processo de escolha foi analisado todo o fluxo de encaminhamento de informações dos sistemas de conexão da rede de acesso Banda Larga e dos sistemas de autenticação envolvidos. Entre as soluções avaliadas ficaram duas possíveis, a utilização de um *Captive Portal* e a solução de manter o fluxo de autenticação normal para os usuários finais que receberem como resposta *Access-Accept,* tratando de forma diferenciada somente os casos que receberam resposta *Access-Reject* ou sem resposta (*time out).*

A solução de *Captive Portal* consiste na utilização de um sistema que força o cliente a acessar uma página inicial web, normalmente utilizada com o objetivo de fazer a autenticação antes de liberar o seu acesso à Internet. A adoção desta solução levaria os clientes obrigatoriamente a uma segunda autenticação. Neste caso todos os clientes finais, ao digitarem qualquer endereço no seu navegador, já seriam interceptados pelo sistema e redirecionados para uma página que solicitaria uma nova autenticação. Esta solução exigiria investimentos em sistemas robustos para tratar todas as conexões de usuários finais, além da dificuldade operacional, já que todos os usuários finais teriam que acessar o navegador obrigatoriamente antes de fazer qualquer outra atividade na rede. Além destes pontos, o histórico de dificuldades que a empresa teve em uma tentativa anterior de utilização deste tipo de solução, a deixaram comparativamente em desvantagem de custo e complexidade em relação a outra solução proposta.

A segunda solução avaliada foi a de efetivamente aceitar a conexão do cliente, para os casos que devem apresentar a tela de aviso, porém redirecionando os casos previstos nas letras “b” e “c” da especificação funcional, para uma VPN específica em vez de liberar seu acesso à rede Internet.

Desta forma, o cliente que teve como resposta um *Access-Reject* ou que teve sua solicitação rejeitada por domínio inexistente, tem a sua resposta modificada para *Access-*

*Accept*, porém os parâmetros de resposta fazem com que ele seja direcionado à VPN, passando a ser atendido por um servidor de DNS modificado. Este servidor de DNS tem como característica a devolução de uma resposta única com o IP do servidor onde a página de aviso está armazenada, fazendo com que qualquer requisição seja sempre respondida com a apresentação da página de aviso pelo navegador.

A segunda alternativa foi escolhida, principalmente devido a menor complexidade para o usuário final, embora ela também tenha custo menor, visto que os clientes finais tratados por ela correspondem somente aos casos onde é necessária a apresentação da tela, exigindo equipamentos menos robustos para sua implantação.

## 4.4 - ARQUITETURA E FUNCIONAMENTO

A partir da definição da escolha da solução, partiu-se então para o detalhamento de sua arquitetura e de seu funcionamento. Para melhor entendimento, a solução implantada é baseada na interceptação da resposta encaminhada pelo RADIUS do ISP através do RADIUS da operadora. Este substitui a resposta do ISP caso ela seja um *Access-Reject* ou caso o domínio utilizado na Requisição de Acesso recebida do NAS não conste na lista de redirecionamento do RADIUS da operadora. Nestes dois casos, o cliente final receberá uma confirmação positiva na autenticação, porém ele será autorizado a entrar somente em uma rede privada. A Figura 4.1 ilustra o funcionamento da solução.

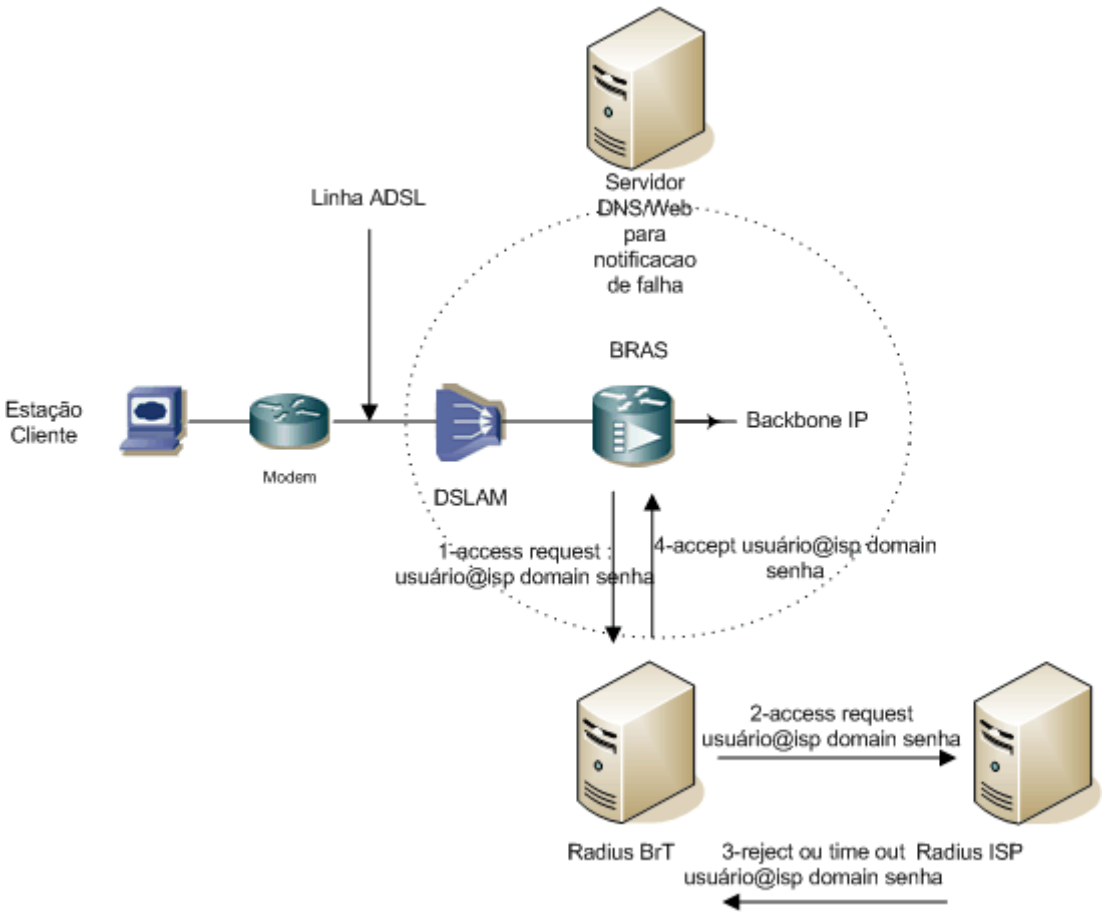



Figura 4.1: Diagrama de implantação da solução [BTSAc].

**Detalhamento do funcionamento**

a) O usuário banda larga inicia processo de estabelecimento de sessão PPP e inicia o processo de requisição de acesso;

b) O BRAS (NAS) encaminha Requisição de Acesso para o Servidor RADIUS da operadora;

c) O Servidor RADIUS da operadora reencaminha a Requisição de Acesso para o Servidor RADIUS do ISP, de acordo com o domínio que compõe o nome do usuário (*login*). Caso o domínio não exista na tabela, procede-se como descrito na alínea "f" a seguir;

d) O servidor RADIUS do ISP responde com *Access-Accept*, *Access-Reject* ou não responde (*time out*);

e) Para as solicitações autorizadas (resposta *Access-Accept* recebida do RADIUS do ISP), é mantido o procedimento normal;

f) Para as solicitações rejeitadas (resposta *Access-Reject* recebida do RADIUS do ISP) ou que tiverem apontando para um domínio inexistente, o servidor RADIUS da operadora responde, com parâmetros específicos para que o cliente receba a autorização, porém seja redirecionado para o acesso a uma rede privada que tem o *default gateway* direcionado para o servidor DNS/Web da solução. Este servidor está configurado para redirecionar todas as requisições HTTP para o endereço IP do próprio equipamento, que possui um Servidor Web (*HTML Server*) configurado para apresentar a página de aviso pré-definida.

A página a ser apresentada no navegador do cliente final, pela definição da especificação funcional, deve informar que ao acesso ADSL está funcionando normalmente, porém a navegação está limitada porque não houve "autorização" de acesso pelo seu ISP, indicando ao cliente que ele revise o *login* e a senha que está utilizando e, caso estejam corretos, entre em contato com seu respectivo ISP.

### 4.4.1 - Configuração nos sistemas

Para o funcionamento da solução, o equipamento servidor de DNS e HTML (Web) foi instalado no *Data Center* da operadora e conectado a uma rede privada. Para o acesso a esta rede, além da configuração de uma VPN específica, também foi necessário configurar faixas adicionais de endereços IP (neste caso endereços de uma rede privada) em todos os BRAS da rede, para que estes endereços IP possam ser designados aos clientes finais forem conectados à VPN.

A partir da implantação desta VPN, os servidores RADIUS tiveram *policies* configuradas para que pudessem promover o redirecionamento e para refletirem o tratamento previsto na especificação funcional. Com estas configurações, os servidores passaram a encaminhar a resposta de Acesso Permitido (*Access-Accept*) para os casos clientes finais que se enquadram nas condições previamente definidas (domínio inexistente ou *Access-Reject* do ISP), encaminhando também ao NAS os atributos de configuração específicos que determinam que estes clientes finais recebam endereçamento IP e acesso somente para este segmento de rede.

### 4.4.2 - Página apresentada ao cliente

A página a ser apresentada para o cliente, de acordo com a especificação funcional, deve informar a cliente final que a sua conexão ADSL está funcionando corretamente, contudo não houve a autorização de acesso à Internet pelo seu ISP. A Figura 4.2 representa a tela que foi desenvolvida na implantação original como parte deste trabalho. Esta página, durante o período de junho de 2008 até julho de 2009, foi a apresentada no navegador dos clientes finais que foram direcionados para a solução.


Figura 4.2: Página de aviso de falha de autenticação implantada em 2008

Cabe ressaltar que, dentro do processo de publicação de qualquer tipo de comunicação ao cliente dentro da operadora, são necessários vários passos de aprovação. Como a página foi desenvolvida dentro deste trabalho, seu texto teve que ser previamente aprovado pelas áreas jurídica, regulatória e de desenvolvimento de produtos, posteriormente seus arquivos em HTML tiveram que ser encaminhados a uma das empresas de comunicação contratada e, finalmente, à área de comunicação e marketing para sua aprovação.

Após todo o processo de aprovação, os arquivos e as figuras que formam a página a ser apresentada foram gravados diretamente no servidor DNS/WEB, representado no topo da Figura 4.1.

Com a fusão das empresas Oi e Brasil Telecom, a nova marca adotada pela empresa passou a ser somente Oi, que foi vinculada a todos os serviços da operadora. Para compatibilização com a nova marca, em julho de 2009 a tela foi alterada, ficando com o formato apresentado na Figura 4.3 a seguir:

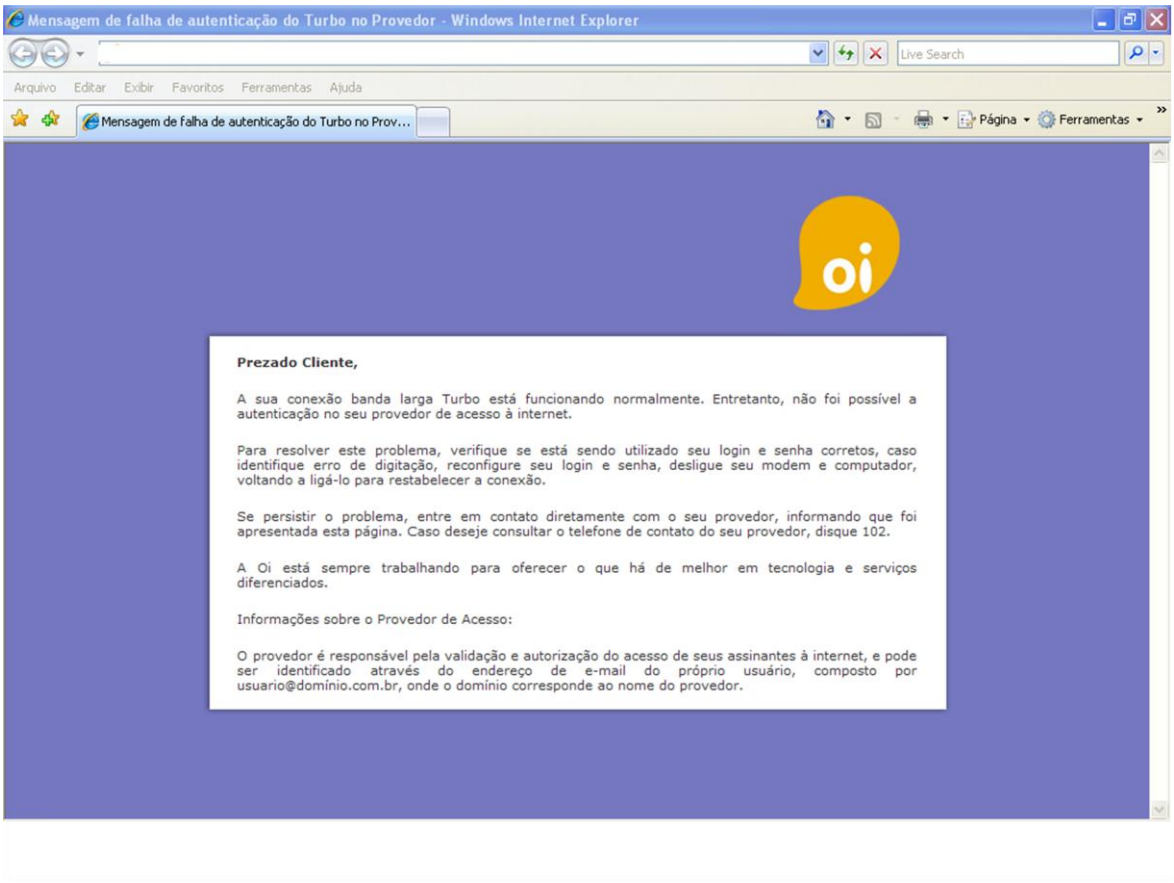



Figura 4.3: Página de aviso de falha de autenticação alterada em julho de 2009

### 4.4.3 - Implantação

A solução de conectividade em banda larga ADSL da operadora atende atualmente quase dois milhões de clientes finais de acessos residenciais, sendo que na época da implantação já eram aproximadamente um milhão e meio de clientes. Para evitar impactos

desastrosos na operação, visto que potencialmente este volume de usuários finais poderia ter a apresentação da página em seu navegador, caso estivesse no critério de redirecionamento, ou caso houvesse alguma falha na implantação, todo processo foi cuidadosamente programado e planejado, com o envolvimento das áreas de planejamento técnico, de operações e de atendimento da empresa.

#### 4.4.3.1 - Solução de implantação gradual

Se todos os processos de autenticação estivessem funcionando corretamente, a implantação da página, após o desenvolvimento e os testes realizados, seria simples. Porém pelos resultados das análises do Capítulo 3, já havia a informação da existência de um grande volume de clientes finais que estavam com *logins* ou senhas errados e conseguiam seu acesso exclusivamente pela permissão de acesso concedida por *time out*. Havia também a informação repassada pelos ISPs em relação a contatos feitos com clientes finais nesta situação, relatando que muitos deles nem sabiam desta falha, ao contrário, reclamavam o fato de demorarem para que pudessem acessar a Internet depois de ligarem o *modem*.

Outro ponto a ser considerado é que, paralelamente à implantação da solução pela operadora, alguns dos ISPs estavam também implantando seus controles contra uso simultâneo, já que haviam sido notificados dos volumes e da possibilidade da cobrança por usuários que poderiam estar utilizando credenciais de terceiros e não pagando diretamente ao ISP. Este ponto foi considerado como um desafio adicional, visto que o "bloqueio" do usuário simultâneo, inicialmente podia ser disfarçado pela permissão de acesso concedida por *time out*, ou seja, muitos dos usuários que teriam seus acessos negados estavam ainda obtendo o acesso por *time out* antes da implantação da solução.

A implantação em uma única fase do sistema poderia ter resultados indesejados, pois, muito provavelmente, os volumes de chamadas nos *Call Centers* de atendimento, tanto da operadora quanto dos ISPs, seriam muito superiores a capacidade de atendimento, o que geraria grande insatisfação nos usuários finais.

A solução desenvolvida para contornar a dificuldade foi o escalonamento da ativação, dividindo a implantação geograficamente e por domínios dos ISPs, através da aplicação gradual das regras nos servidores RADIUS da operadora.

Todas as manobras foram agendadas e acompanhadas junto à operação de *Call Center* da operadora que só liberava a nova ativação quando o volume de chamadas voltava a se estabilizar. Para esta implantação, o cronograma utilizado foi o descrito na Tabela 4.1, que contemplou datas específicas de implantação dos lotes, que foram separados por domínios e por regiões.

Tabela 4.1: Cronograma de implantação da Página de Aviso de Falha de Autenticação

| Data | Locais e domínios de aplicação |
|---|---|
| 23/06/2008 | Curitiba - Teste piloto - Ativado o sistema somente para o domínio do ig.com.br e somente para a cidade de Curitiba. |
| 24/06/2008 | Curitiba – Todos os demais domínios, com exceção do domínio brturbo.com.br (maior base) |
| 25/06/2008 | Interior do Paraná - Todos os domínios com exceção do brturbo.com.br (maior base). |
| 26/06/2008 | Porto Alegre - Todos os domínios com exceção do brturbo.com.br (maior base). |
| 30/06/2008 | Interior do Rio Grande do Sul - Todos os domínios com exceção do brturbo.com.br (maior base). |
| 01/07/2008 | Florianópolis - Todos os domínios com exceção do brturbo.com.br (maior base) |
| 02/07/2008 | Interior de Santa Catarina - Todos os domínios com exceção do brturbo.com.br (maior base). |
| 07/07/2008 | Goiás e Tocantins - Todos os domínios, inclusive brturbo.com.br. |
| 08/07/2008 | Mato Grosso, Mato Grosso do Sul, Rondônia e Acre - Todos os domínios, inclusive brturbo.com.br |
| 09/07/2008 | Distrito Federal - Todos os domínios, inclusive brturbo.com.br. |
| 14/07/2008 | Rio Grande do Sul e Santa Catarina – somente o domínio brturbo.com.br |
| 15/07/2008 | Paraná – somente o domínio brturbo.com.br |

#### 4.4.3.2 - Principais dificuldades na implantação

Conforme foi previsto, as principais dificuldades da implantação foram relativas às diversas ocorrências de problemas de configuração dos equipamentos dos clientes finais. Com a apresentação da tela, muitos clientes finais, seguindo a orientação, faziam os primeiros testes e, na sequência, entravam, em contato com o provedor, que nem sempre conseguia resolver o problema na primeira tentativa. Entre os principais problemas de configuração podem ser destacados:

a) *login* errado – a composição do *login* do usuário final é o se "nome de usuário", seguido pela "@" e o domínio do ISP que ele utiliza (ex. nomedeusuario@isp.com.br). Quando a falha é um erro somente na parte "nome de usuário" ele é facilmente detectado pelos atendentes dos ISPs. Porém em muitas vezes o erro estava no domínio do provedor, o que nem sempre era conferido pelo atendente ou pelo usuário final. A única solução encontrada foi instruir os ISP a aumentar a recomendação de conferência deste item, principalmente nos casos onde a falha permanecia após as conferências normais.

b) Mais de uma configuração de acesso no *modem* utilizado como *router* – Em alguns casos o *modem* do cliente apresentava mais de uma linha de configuração, sendo uma com o *login* e senha corretos e outra com informações não válidas. Esta situação demorou a ser diagnosticada, pois a simples conferência da linha correta não indicava a presença de erros. Somente após algumas ocorrências é que foi diagnosticado que esta possibilidade existia, sendo constatada principalmente em *modem*s Dlink. Após a constatação, passou a fazer parte das recomendações aos ISPs, para que também orientassem seu atendimento a verificar esta possibilidade no tratamento dos casos onde havia recorrência de reclamação de algum cliente.

c) Configuração dos computadores dos usuários finais – A apresentação da Página de Aviso, como resposta a uma consulta de DNS pelo navegador do cliente, em alguns casos resultava em uma informação que ficava armazenada no *cache* de DNS do computador do usuário final e, mesmo depois de corrigido, o resultado para a mesma requisição era a apresentação da Página de Aviso, que ficava armazenada

para a apresentação *off-line* no equipamento. Para evitar esta ocorrência, a solução adotada foi de sempre indicar que, após a correção, o usuário final deveria reiniciar seu computador. Porém em alguns casos, mesmo após a reinicialização, permanecia o mesmo resultado. Nestes casos, a solução encontrada foi a execução do comando *ipconfig*/*dnsflush*, através da linha de comando do sistema operacional.

## 4.5 - RESUMO DAS SOLUÇÕES IMPLANTADAS E SUA CRONOLOGIA

As soluções implantadas, correção de domínios no sistema de mediação (MDS), correção dos números de serviço para cobrança no sistema de faturamento (SFA), eliminação da autenticação por *time out* na maioria dos provedores, alteração funcional para diferenciação do uso simultâneo, notificação dos provedores quanto ao uso simultâneo e de sua cobrança e a implantação da página de aviso de falha de autenticação foram todas executadas até outubro de 2008. Os resultados foram medidos e comprovados no primeiro semestre de 2009 e estão apresentados no próximo capítulo.

# 5 - RESULTADOS OBTIDOS

Após todas as implantações, ocorridas principalmente no segundo semestre de 2008, os dados puderam ser reavaliados para comprovação dos resultados, embora de forma prática os resultados já tivessem sido transportados para o aumento do faturamento no serviço e melhoras no atendimento e relacionamento com os ISPs. Neste capítulo apresenta-se a análise dos principais resultados obtidos e indicações de outras possíveis melhorias.

## 5.1 - ANÁLISE DOS DADOS APÓS AS IMPLANTAÇÕES

Para analisar os resultados obtidos após a aplicação das correções e implantação das soluções técnicas, foram utilizados principalmente os indicadores anteriormente criados para o acompanhamento do projeto, e os resultados obtidos puderam ser validados conforme descrito a seguir:

### 5.1.1 - Percentual de usuários medidos em relação à base

A quantidade de usuários medidos em relação à base teve aumento significativo, passando de 91,65% na pior leitura, vista em outubro de 2007, na seção 3.4.1, para 96,67% na melhor leitura em abril de 2009, conforme pode ser visto no gráfico apresentado na Figura 5.1 a seguir.

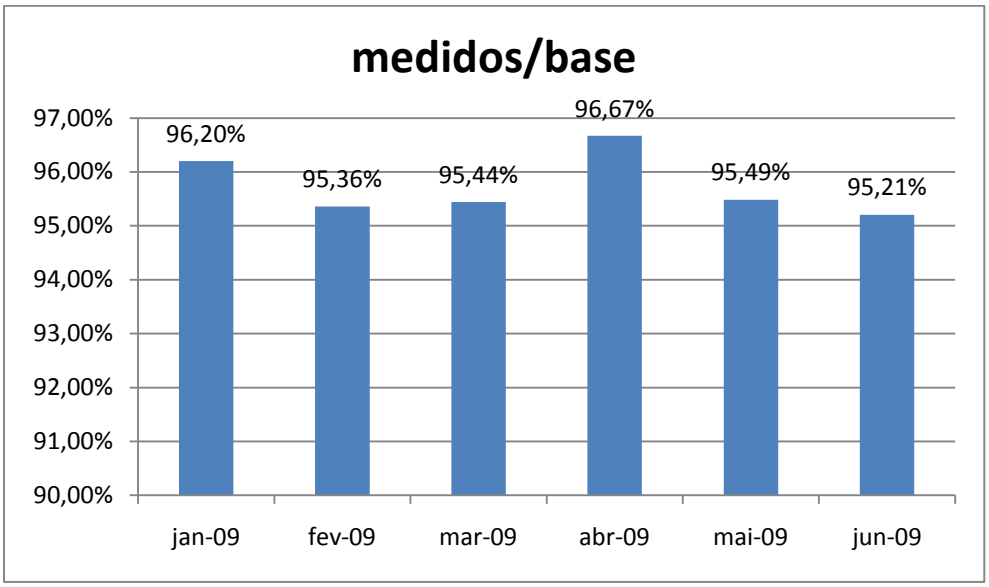



Figura 5.1: Gráfico de usuários medidos / base ativa residencial – janeiro a junho de 2009

Estas leituras comprovam que as soluções implantadas deram o resultado esperado, aumentando a quantidade de clientes medidos que passou a ficar em um patamar superior a 95% da base total ativa de acessos ADSL instalados para clientes residenciais.

Conforme era esperado, mesmo com a implantação das soluções, ainda permaneceu uma diferença entre o total de clientes medidos e a base ativa, embora menor que a constatada nas medições preliminares. Esta diferença não deve ser considerada uma ineficiência no sistema de medição, visto que está relacionada ou à ausência de utilização ou à falta da necessidade de autenticação, o que ocorre respectivamente nos casos de usuários que não se conectam ou que permanecem conectados no mês todo.

Conforme constatado nas análises constantes no Apêndice A, seção A.3, durante o período de amostragem de seis meses, mais de 3% dos clientes fizeram conexões com duração superior a 30 dias. O crescente uso de redes domésticas, tanto cabeadas como *wireless*, tem modificado o comportamento dos clientes finais. Nos casos onde o cliente final tem uma rede doméstica, o seu *modem* normalmente é configurado como *router* e fica ligado, sendo desligado muito esporadicamente ou quando há falta de energia elétrica. Este

cenário indica que se torna mais importante a utilização de bilhetagem intermediária, não desenvolvida neste trabalho, mas indicada como sugestão para futuros trabalhos.

Há carência de material sobre este assunto, o que dificulta a comparação deste resultado com outras operadoras e provedores de serviços, principalmente porque o modelo de cobrança separada dos serviços do ISP e impossibilidade da operadora concessionária prestar o serviços ao cliente final, que ocorre no Brasil, não é comum em outros países.

### 5.1.2 - Percentual de usuários únicos em relação aos usuários medidos

A quantidade de usuários únicos em relação ao total de usuários medidos teve aumento significativo, passando de 86,30% na pior leitura, em julho de 2007, conforme visto na seção 3.4.2, para 91,14% na melhor leitura em maio de 2009, conforme pode ser visto no gráfico apresentado na Figura 5.2 a seguir.

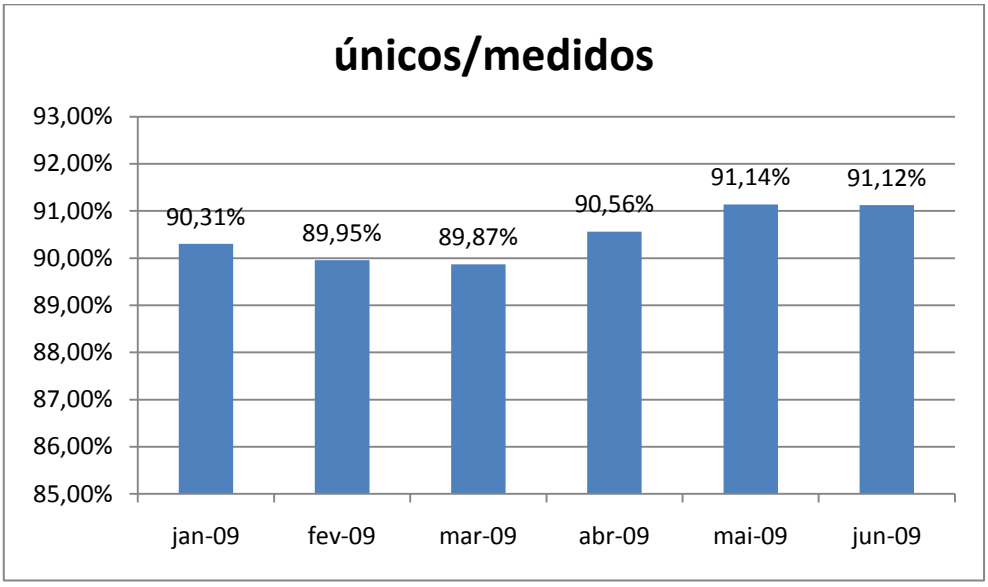



Figura 5.2: Gráfico de usuários únicos / usuários medidos – janeiro a junho de 2009

Neste indicador, os resultados obtidos foram mais surpreendentes, as ações de correção e a página de aviso reduziram significativamente a ocorrência de uso simultâneo.

Mesmo assim, alguns ISPs mantiveram por sua escolha a decisão de não controlar a autenticação de acessos simultâneos com um mesmo *login*, mesmo com a informação de que isto representa riscos de segurança e maior dificuldade de controle, principalmente por limitações técnicas e de investimento. Nestes casos, considerou-se que não cabiam mais ações técnicas do lado da operadora, já que era uma escolha do ISP. A solução implantada foi a exclusão dos descontos no caso de uso simultâneo de *login*, como forma a coibir esta prática. Esta solução comercial foi implantada no final de 2009 e ainda não foi medida, não fazendo parte deste trabalho, embora tenha sido adotada em sua consequência.

### 5.1.3 - Percentual de usuários únicos em relação á base ativa de clientes

A quantidade de usuários únicos em relação à base total ativa de acessos ADSL instalados para clientes residenciais teve aumento significativo, passando de 71,32% na pior leitura, em setembro de 2007, conforme visto na seção 3.4.3, para 87,55% na melhor leitura, em abril de 2009, conforme pode ser visto no gráfico apresentado na Figura 5.3 a seguir:

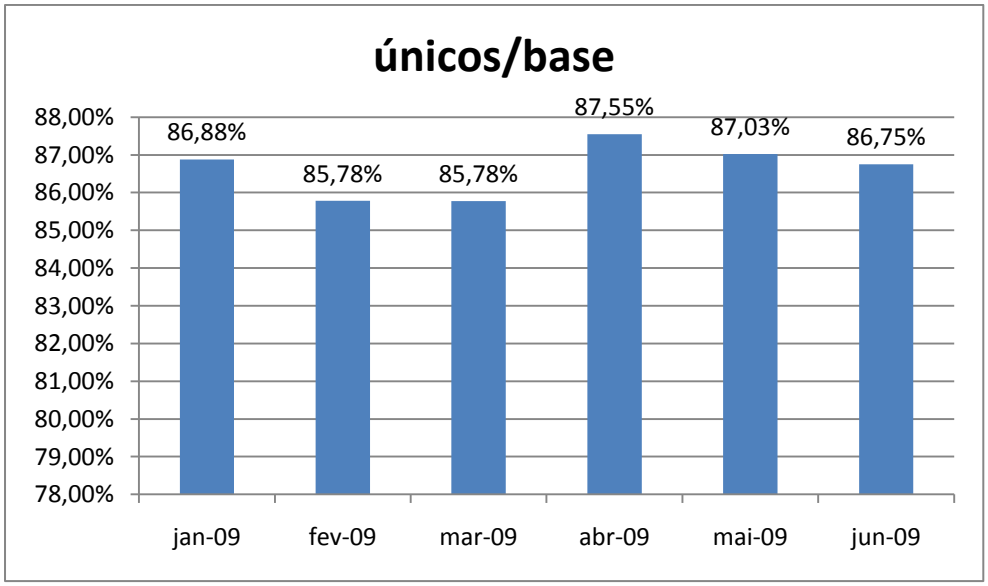



Figura 5.3: Gráfico usuários únicos / base ativa residencial – janeiro a junho de 2009

Como consequência da redução de ocorrência de acessos simultâneos utilizando o mesmo *login*, este indicador também teve melhoras significativas. O indicador continua sendo adotado como a referência de maior eficiência e melhor qualidade no serviço e medição de utilização, tanto pela operadora como pelos ISPs.

## 5.2 - RESULTADOS DA PÁGINA DE AVISO DE FALHA DE AUTENTICAÇÃO

A implantação da Página de Aviso de Falha de Autenticação trouxe benefícios significativos na qualidade e confiabilidade dos dados para efeitos de faturamento, sendo que praticamente extinguiu a ocorrência de acessos de usuários sem a devida autenticação por um ISP. Além desta melhoria, que ficou comprovada na redução de contestações e nos resultados dos indicadores (embora sobreposta às demais correções), alguns resultados agregados e muito positivos foram obtidos também no relacionamento com os usuários, que podem ser comprovados através da redução da necessidade de contato do usuário com o *Call Center* de atendimento da operadora. A melhora neste relacionamento já era esperada e, após anunciada, passou também a ser um dos objetivos principais do projeto durante seu desenvolvimento e sua implantação. Os resultados obtidos podem ser reconhecidos mais facilmente na análise dos indicadores de atendimento da própria área de atendimento de *Call Center* da operadora, descritos a seguir.

### 5.2.1 - Redução do volume de atendimento (quantidade de chamadas)

Como resultado da implantação da página de aviso, após as oscilações do período de implantação, houve uma redução significativa na quantidade de chamados atendidos no *Call Center* de suporte da operadora.

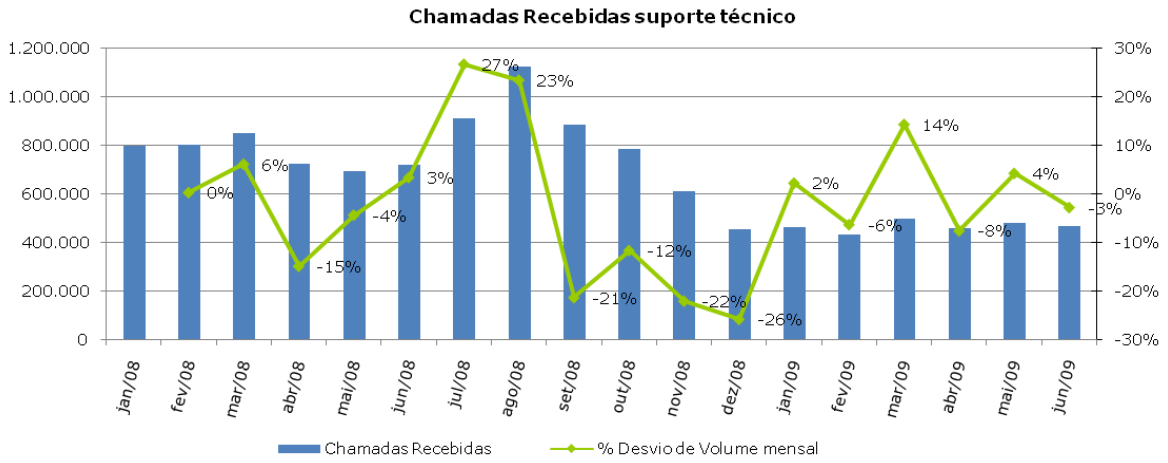



Figura 5.4: Gráfico de atendimentos - Comparativo 1º sem 2008 x 1º sem 2009 [BTCC]

O gráfico da Figura 5.4 apresenta o volume mensal de chamadas entrantes no *Call Center* de atendimento de suporte do produto de acesso ADSL da operadora (produto Turbo). Nas barras as "Chamadas Recebidas", de acordo com a graduação na coluna da esquerda, e na linha "Desvio de Volume Mensal", comparando sempre com o mês anterior e de acordo com a graduação na coluna da direita.

No gráfico, é visível a redução do volume de chamadas entrantes que iniciou-se a partir de setembro de 2008. A redução foi acompanhada e qualificada na área de atendimento de Call Center nos meses seguintes a implementação da Página de Aviso de Falha de Autenticação, que ocorreu no mês de Julho de 2008. Segundo a [BTCC], parte da redução, equivalente a 10% das chamadas recebidas, teve como motivador principal a informação ao cliente no ato da navegação sobre o erro na autenticação e orientação para conferir o *login* e a senha utilizados e, somente caso ele considerasse que estavam corretas, ligar para seu ISP para identificar o motivo de não ter sido autenticado.

Porém, observando o gráfico, há um forte crescimento nas chamadas nos meses de julho e agosto. No mês de julho este crescimento foi devido em parte ao processo de implantação da Página de Aviso de Falha de Autenticação e parte ao bloqueio de uso simultâneo de *logins* implantado no mesmo período por dois grandes ISPs.

Nos meses seguintes (agosto, setembro e outubro), segundo informações da [BTCC], ocorreram problemas sistêmicos e de redes que mascararam a perceptível redução de chamadas pelo motivo de falha de autenticação. Segundo a própria [BTCC], o impacto seria muito maior se não houvesse a Página, principalmente pelo fato de ter havido a retirada de serviços de um provedor com grande volume de usuários finais.

A [BTCC] complementou que especificamente no mês de agosto de 2008, após a conclusão da implantação da página, houveram as seguintes ocorrências:

a) Falhas temporárias de rede, principalmente no estado de Santa Catarina, com impacto em aproximadamente 500.000 clientes;

b) Retirada dos serviços de um provedor por rescisão de seu contrato devido a inadimplência, afetando aproximadamente 85.000 clientes finais. Muitos clientes entraram em contato com o *Call Center* de reparo. Esta retirada foi realizada em etapas utilizando o modelo de divisão em lotes por letra inicial do *login*;

c) Falha no cadastro de clientes que optaram por ficar sem provedor. Esta opção foi possível devido a liminar em vigência na época no estado do Paraná, porém foram necessários vários ajustes sistêmicos para permitir o cadastro nos sistemas da operadora.

Os impactos citados fizeram com que a redução de volumetria só fosse perceptível a partir de dezembro de 2008, quando o volume médio mensal passou a ser na ordem de 450.000 chamadas, significativamente menor do que o volume mensal médio de 750.000 do período anterior a implantação da solução. Cabe ressaltar que somente a redução equivalente a 10% das chamadas foi atribuída a implantação da página de aviso, equivalente a aproximadamente 80.000 chamadas mensais.

Apenas como referencial, usando um custo estimado de uma PA (Posição de Atendimento) de *Call Center* como sendo R$ 6.000,00 mensais e considerando uma estimativa de TMA (Tempo Médio de Atendimento) de 400 segundos para o suporte técnico, pode-se estimar o custo médio de um atendimento como sendo na ordem de R$

3,50 por chamada. Utilizando este referencial, pode-se estimar que a redução de custo gerada pela solução foi em torno de R$ 280.000,00 mensais. Cabe ressaltar que os valores são estimados, não sendo informações oficiais da empresa. Adicionalmente, deve-se considerar que a solução também reduziu o TMA (Tempo Médio de Atendimento), visto que muitas chamadas passaram a ser resolvidas mais rapidamente, por haver a informação de que a falha nestas solicitações é exclusivamente devida à falta da autenticação, embora não afete a estimativa que foi feita com base no TMA anterior a implantação da solução.

# 6 - CONCLUSÕES E RECOMENDAÇÕES

Neste capítulo são apresentadas as conclusões e indicados temas para desenvolvimentos em trabalhos futuros.

## 6.1 - CONCLUSÕES GERAIS

Neste trabalho foi tratado o uso das informações geradas pelos sistemas de AAA do RADIUS para a finalidade de cobrança de serviços. Mais especificamente, a geração de informações mais consistentes e confiáveis sobre o uso dos serviços pelos clientes finais que tiveram o acesso permitido pelos provedores de acesso à Internet, para que possa ser cobrado do ISP a sua parte da prestação do serviço.

O principal problema abordado está relacionado ao fato dos resultados preliminares, obtidos com a utilização direta dos dados de contabilização do RADIUS e dos sistemas de mediação e faturamento da operadora, mostraram inconsistências nas informações geradas, principalmente quando incluídos os usos simultâneos de *logins*. Outro problema que precisou ser tratado foi relacionado às discrepâncias identificadas entre os *logins* cadastrados em alguns provedores e os identificados como autenticados ou tendo acesso permitido por eles.

Inicialmente foram feitas algumas correções de cadastro e notificações para que os provedores corrigissem seus processos de autenticação. Estas correções melhoraram um pouco os resultados obtidos, mas, ficou claro que ainda existiam problemas em aberto e que havia a necessidade de desenvolver um trabalho mais completo, utilizando uma metodologia apropriada, para que se chegasse a soluções que possibilitassem medir e cobrar corretamente pelos serviços prestados aos ISPs.

O desenvolvimento do trabalho teve as etapas iniciais de análise aprofundada de todos os elementos envolvidos, pesquisa bibliográfica para o embasamento teórico, estudo da solução originalmente implantada (sua arquitetura e seu funcionamento). Esta etapa foi seguida de uma análise das bases de dados gerados pelos sistemas de AAA e dos resultados pós o processamento no sistema original, onde identificaram-se as origens das distorções e criaram-se indicadores que possibilitaram a comparação dos resultados antes e depois de ações corretivas e da implantação de soluções para o problema.

Depois de adquiridos os conhecimentos e identificadas as origens dos problemas, foram analisadas as possíveis soluções e as vantagens e desvantagens de cada uma. Baseando-se nestas informações, foram utilizados métodos objetivos de escolha e selecionadas as soluções que melhor atendiam os objetivos.

Desta forma, foram desenvolvidas e implantadas as soluções de correções de processo e cadastro, alteração do sistema para identificação da porta física utilizada pelo cliente final para possibilitar o controle efetivo de uso simultâneo de *login* e implantação de um sistema que elimina os acessos indevidos por tentativas repetitivas de autenticação, desde que todos os agregadores da rede estejam com as configurações corretas para a alocação de endereços privados e redirecionamento para VPN.

Pelos resultados obtidos e apresentados no capítulo 5, conclui-se que as soluções desenvolvidas alcançaram o objetivo de tornar as informações mais confiáveis e permitirem a cobrança dos serviços dos ISPs com mais eficiência, viabilizando a inclusão da cobrança do uso simultâneo de *logins*, aumentando a receita e reduzindo as contestações.

Além disso, a cobrança mais objetiva dos serviços relacionados à autenticação e liberação do acesso dos clientes finais, forçou os provedores a terem mais controle sobre a sua base de clientes e suas autenticações, o que melhorou significativamente a capacidade de identificação de clientes finais quando necessária para fins técnicos ou legais.

Adicionalmente, alcançou-se também uma redução do volume de contatos dos usuários com a operadora, que em parte eram devidos à resposta negativa pelo ISP no

processo de autenticação. Esta redução ocorreu pela melhora nos processos de autenticação dos provedores e principalmente pela ferramenta implantada para o aviso de falha de autenticação, que proporciona ao cliente uma informação de que seu acesso ADSL está funcionando corretamente, porém ele não foi "autorizado" pelo provedor a acessar a Internet.

Esta solução, após o período de implantação que exigiu a correção de credenciais de muitos clientes finais, passou a ser uma ferramenta de auxilio aos atendentes dos *Call Centers*, tanto da operadora quanto do provedor. Segundo o relato informal dos responsáveis pela área de atendimento de alguns ISPs, quando há a informação pelo cliente final de que ele está visualizando a Página de Aviso, há a eliminação de vários passos do *script*, o que permite ir direto ao ponto de correção de *login* ou senha, reduzindo o TMA e as experiências negativas para os clientes finais.

Outro ponto significativo deste trabalho foi a geração de diversas informações sobre o comportamento de uso dos clientes finais que são resultados de processamentos manuais das bases de dados de bilhetes de contabilização. Este conjunto de informações comportamentais de uso dos clientes finais atinge o objetivo de ser base para decisões gerenciais e técnicas que propiciem as melhores escolhas no planejamento e execução de manobras, principalmente para reduzir os impactos aos clientes finais. As informações foram usadas ao longo do trabalho para seu desenvolvimento, em manobras que ocorreram ao longo do seu período de implantação e são atualmente utilizadas para diversos fins na operadora.

Como resultados futuros, espera-se que as informações de perfil e de comportamento dos usuários sejam largamente utilizadas na operadora e em outras empresas que disponibilizam acesso à Internet de forma massiva. O conhecimento destes comportamentos e perfis permite a escolha de horários de manobras por região e por tipo de serviço, além de permitir o desenvolvimento de produtos e soluções direcionadas ao público que as utiliza.

Espera-se também que as soluções de controle de acesso simultâneo, bloqueio de acessos indevidos concedidos por *time out* e de melhorias no processo de geração de

informações sejam implantadas em outras empresas, visto que a metodologia pode ser utilizada em operadoras e prestadores de serviços que tenham sistemas de AAA com redirecionamento da autenticação e que precisem medir ou cobrar pelos acessos permitidos pelos responsáveis pela autenticação.

## 6.2 - SUGESTÕES PARA TRABALHOS FUTUROS

Durante o desenvolvimento do trabalho, muitas novas idéias surgem, porém nem todas podem ser incorporadas, sob pena de fugir do seu foco e torná-lo extenso e menos objetivo. Dentre as idéias que surgiram, duas principais são expostas a seguir como sugestões para trabalhos futuros.

A primeira é que, conforme visto no Apêndice A, seção A.3, um dos problemas em relação a não se medir quantidades mais próximas a 100% da base ativa é o fato dos clientes poderem ficar conectados durante todo o mês, sem gerar uma desconexão e, consequentemente, sem gerar um bilhete de *accounting* dentro do mês, ficando fora da contabilização. De acordo com os resultados obtidos na seção A.3, mais de 3% dos clientes fizeram conexões de mais de trinta dias. Adicionalmente, a tendência é de crescimento destas ocorrências, devido ao aumento do uso de redes domésticas e consequentemente do uso de *modems* configurados em modo *router*.

Este problema pode ser resolvido com a implantação de uma solução de envio de bilhetagem intermediária, que pode indicar se uma conexão permanece ativa durante o intervalo de medição e desta forma permitir a cobrança do serviço relativo a esta conexão.

Fica então a sugestão para desenvolvimento futuro desta ferramenta, que basicamente é a configuração nos sistemas envolvidos para que gerem uma Requisição de Contabilização intermediária quando um cliente permanece conectado acima de um período de tempo pré-estabelecido. Desta forma, mesmo quando não há uma conexão ou desconexão, haverá um bilhete para contabilização da utilização.

Um ponto impactante desta bilhetagem intermediária é que ele gera uma carga adicional aos sistemas e aumenta a necessidade de armazenamento, principalmente porque há uma limitação em alguns equipamentos onde, ao habilitar bilhetagens intermediárias, fazem estas requisições em períodos máximos de 24 horas, gerando no mínimo um bilhete a mais por dia por acesso ativo.

O desenvolvimento desta solução, análise de impactos positivos e negativos, custos e possibilidades de aumento de receita podem ser tema de um trabalho futuro, alavancado pelo crescimento da ocorrência de conexões com mais de 30 dias de duração, que ocorre pela migração de clientes para o uso de *modem* em modo *router* associado ao crescimento do uso de redes domésticas de computadores.

Outra questão que permanece em aberto é o fato ainda haver a dependência de um processo manual para a emissão da fatura de serviços para os provedores. Embora as soluções implantadas durante este trabalho tenham melhorado significativamente o processo de geração da informação para possibilitar o faturamento, não fez parte do escopo a automatização do processo de emissão de faturas, que deve ser feita diretamente nos sistemas de faturamento, que tem interface com os sistemas de impressão.

Na solução atual, o Sistema de Faturamento (SFA) é utilizado apenas para o processamento de relatórios, que são analisados e estruturados manualmente. As quantidades de clientes medidas por provedor são lançadas em uma planilha eletrônica que calcula os valores líquidos com descontos por quantidade, quando aplicáveis, e insere os impostos por UF. Estes valores são encaminhados para emissão de faturas *on-line* (nome utilizado na empresa para a fatura solicitada manualmente), uma para cada UF.

A sugestão de trabalho futuro, já que foram vencidas as etapas de gerar informações confiáveis, inclui a adequação dos sistemas para que a atividade feita manualmente, de inclusão de descontos e calculo do valor liquido relatórios com valores de cobrança e a viabilização da impressão das faturas pelos sistemas já utilizados na operadora.

## REFERÊNCIAS BIBLIOGRÁFICAS


[ANATEL] Anatel, **NORMA 004/95, Uso de Meios da Rede Pública de Telecomunicações Para Acesso à Internet**, Disponível em http://www.anatel.gov.br/Portal/verificaDocumentos/documento.asp?numeroPublicacao=10283&assuntoPublicacao=Norma%20MC%20n%BA%20004/1995&caminhoRel=Cidadao-Biblioteca-Acervo%20 Documental&filtro=1&documentoPath=biblioteca/Normas/Normas_MC/norma_004_95.htm. Consulta em 02 de junho de 2010.

[ANDERSSON] Andersson, et al. ***Protected EAP Protocol (PEAP)***, IETF 2004. Disponível em <http://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-01>. Consulta em 03 de junho de 2010.

[AWK] Free *Software* Foundation, ***Gawk: Effective AWK programming.*** Junho, 2010. Disponível em < http://www.gnu.org/*software*/gawk/manual/>. Consulta em 14 de junho de 2010.

[BTCC] Brasil Telecom Call Center, **Apresentação interna sobre os resultados após a implantação da Página de Aviso de Falha de Autenticação**, Documento de uso interno. Abril, 2010.

[BTSAa] Brasil Telecom S.A., **Lista de *modem*s Certificados**, disponível em <http://www.novaoi.com.br/portal/site/NovaOi/menuitem.69086a042c45d97e30197402f26d02a0/?vgnextoid=c80b20e427260210VgnVCM10000021d0200aRCRD&STATE=22%7CSC%7CSanta%20Catarina>. Consulta em 01 de maio de 2010.

[BTSAb] Brasil Telecom S.A., **Site de Relacionamento com Investidores**, disponível em <http://www.brasiltelecom.com.br/ri/>. Consulta em 23 de maio de 2010.

[BTSAc] Brasil Telecom S.A., **Especificação Técnica: ADSL Falha de Autenticação de Provedores**, Documento interno da Gerência de Infra-estrutura de TI.

[DANTEa] Richesky, Dante, **Projeto de atendimento de Provedores de acesso nas Centrais Telefônicas (*Housing*).** CRT - Companhia Riograndense de Telecomunicações, documento de interno da empresa, 2000.

[DANTEb] Richesky, Dante, **Apresentação sobre evolução tecnológica do acesso à Internet.** Brasil Telecom S/A, documento de interno da empresa, 2007.

[DANTEc] Richesky, Dante, **Apresentação Evolução da Internet.** Brasil Telecom. Exibida na Câmara dos Deputados, setembro, 2009

[DEKOK] DEKOK, Alan, ***Use of Status-Server Packets in the Remote Authentication Dial In User Service* (RADIUS) *Protocol*,** Maio, 2010**.** Disponível em <http://tools.ietf.org/html/draft-ietf-radext-status-server-09>. Consulta em 04 de junho 2010.

[DICIONÁRIO] **Dicionário de Português**, Disponível em <HTTP:// www.dicionariodeportugues.com.br>. Consulta em 03 de junho de 2010.

[FUNK] Funk, Paul and Simon Blake-Wilson. **EAP *Tunneled* TLS *Authentication Protocol* (EAP-TTL).** IETF. 2004. Disponível em <http://tools.ietf.org/html/draft-funk-eap-ttls-v1-01>. Acesso em 04 de dezembro de 2009.

[GRUSZYNSKI2008] Gruszynski, André, **Mecanismo funcional escalável para contabilização de uso de serviços residenciais em rede de acesso em banda larga utilizando tecnologia ADSL**, Publicação PPGENE.DM-056/2008. Departamento de Engenharia Elétrica. Universidade de Brasília, DF, 2008.

[HASSEL2002] Hassel, Jonathan, **RADIUS**. O´Reilly & Associates, 2002

[HENZ2008] Henz, Leandro, **Proposta e Implementação de Arquitetura para Identificação Física e Lógica de Acessos Banda Larga utilizando tecnologia ADSL**, Publicação PPGENE.DM-057/2008. Departamento de Engenharia Elétrica. Universidade de Brasília, DF, 2008.

[ITUG992.1] ITU Recommendation G.992.1, ***Asymmetric Digital Subscriber Line* (ADSL) *transceivers***, ITU, Junho/1999. Disponível em: <http:// www.itu.int/rec/T-REC-G.992.1-199907-I/en>. Consulta em 04 de junho de 2010.

[ITUG992.3] ITU Recommendation G.992.3, ***Asymmetric digital subscriber line transceivers* 2 (ADSL2),** ITU, Abril/2009. Disponível em: <http://www.itu.int/rec/T-REC-G.992.3-200904-P/en>. Consulta em 04 de junho 2010.

[ITUG992.5] ITU Recommendation G.992.5, ***Asymmetric digital subscriber line (ADSL) transceivers - Extended bandwidth*** **ADSL2 (ADSL2plus),** ITU. Janeiro/2009. Disponível em: <http:// www.itu.int/rec/T-REC-G.992.5-200901-P/en>. Consulta em 04 de junho de 2010.

[JOSHUAHILL] Joshua Hill, ***An Analysis of the*** **RADIUS** ***Authentication Protocol***, infogard Laboratories, 2001. Disponível em http://www.untruth.org/~josh/security/RADIUS/RADIUS-auth. html>. Consulta em 02 de dezembro de 2009.

[LGT] Presidência da República, Casa Civil, **Lei 8.472 de 16 de julho de 1997, Lei Geral de Telecomunicações**, Disponível em <http://www.planalto.gov.br/ccivil/leis/L9472.htm>. Consulta em 03 de junho de 2010.

[MIERCOM] Miercom, ***Lab Testing Summary Report: Edge Routers Cisco Systems and Juniper Networks***. Outubro, 2004. Disponível em <www.**miercom**.com/dl.html?fid=20041015&type=report>. Consulta em 29 de maio de 2010.

[NAKHJIRI2005] Nakhjiri, Madjid & Nakhjiri, Mahsa, **AAA and Network Security for mobile Access - RADIUS, Diameter, EAP, PKI and IP Mobility**, Wiley, 2005.

[Oi] Oi. **Apresentação interna sobre o processo de faturamento do Turbo Provider**, Desenvolvida pela área de faturamento da empresa, fevereiro, 2010.

[RFC1134] PERKINS, D., ***The Point-to-Point Protocol: A Proposal for Multi-Protocol Transmission of Datagrams Over Point-to-****Point Links****,*** IETF, RFC 1134, Novembro/1989. Disponível em <http://www.ietf.org/rfc/ rfc1134.txt>. Consulta em 02 de dezembro de 2009.

[RFC1136] Hares, S. & Katz D., ***Administrative Domains and Routing Domains - A Model for Routing in the Internet***, RFC 1136, Dezembro, 1989. Disponível em <http://tools.ietf.org/rfc/ rfc1136.txt>. Consulta em 05 de junho de 2010.

[RFC1321] Rivest, R., ***The MD5 Message-Digest Algorithm,*** **RFC 1321**, Abril, 1992. Disponivel em <http://tools.ietf.org/rfc/rfc1321.txt>. Consulta em 05 de junho de 2010.

[RFC1334] LLOYD, B. & Simpson, W., ***PPP Authentication Protocols***, IETF - RFC 1334. Outubro/1992. Disponível em < http://tools. ietf.org /html/rfc1334>. Consulta em 02 de dezembro de 2009.

[RFC1661] SIMPSON, W., ***The Point-to-Point Protocol (PPP)***, IETF - RFC 1661. Julho/1994. Disponível em < http://www.apps.ietf.org/ rfc/rfc1661.html>. Consulta em 02 de dezembro de 2009

[RFC1662] SIMPSON, W., ***PPP in HDLC-like Framing***. RFC1662. Julho/1994. Disponível em <http://www.apps.ietf.org/rfc/ rfc1662.html>. Consulta em 02 de dezembro de 2009.

[RFC1994] SIMPSON, W., ***PPP Challenge Handshake Authentication Protocol (CHAP)***. RFC 1994, Agosto, 1996. Disponível em < http://www.ietf.org/rfc/rfc1994.txt>. Consulta em 01 de dezembro de 2009

[RFC2176] Aboba & Simon, ***PPP EAP-TLS Authentication Protocol***. RFC 2716, Outubro, 1999. Disponível em <http://www.ietf.org/ rfc/rfc2716.txt>. Consulta em 01 de dezembro de 2009

[RFC2284] Blunk & Vollbrecht, ***PPP Extensible Authentication Protocol (EAP),*** RFC 2284, Março,1998. Disponível em < http://www.faqs.org/rfcs/rfc2284.html>. Consulta em 01 de dezembro de 2009

[RFC2364] GROSS, G. et al, ***PPP Over AAL5***, IETF - RFC 2364. <http://www.ietf.org/rfc/rfc2364.txt>. Julho/1998. Consulta em 05 de dezembro de 2009

[RFC2516] MAMAKOS, L. et al, ***A Method for Transmitting PPP Over Ethernet (PPPoE)***. RFC 2516. <http://www.ietf.org/ rfc/rfc2516.txt>. Fevereiro, 1999. Consulta em 04 de dezembro de 2009

[RFC2865] Rigney, et al. ***Remote Authentication Dial In User Service* (RADIUS).** RFC 2865, Junho, 2000. Disponível em < http://www.ietf.org/rfc/rfc2865.txt>. Consulta em 07 de setembro de 2007.

[RFC2866] Rigney, C., **RADIUS *Accounting*.** RFC 2866, Junho, 2000. Disponível em < http://www.ietf.org/rfc/rfc2866.txt>. Consulta em 07 de setembro de 2007.

[RFC2869] Rigney C., Willats W. e Calhoun P., ***RADIUS Extensions.*** RFC 2869. Junho, 2000. Disponível em <http://www.ietf.org/ rfc/ rfc2869.txt>. Acesso em 06 de junho de 2010.

[RFC2882] Mitton, D., ***Network Access Servers Requirements: Extended RADIUS Practices***, RFC 2882, Julho, 2000. Disponível em <http:// www.ietf.org/rfc/rfc2882.txt>. Consulta em 04 de abril de 2010.

[RFC2903] de Laat, et al, ***Generic AAA Architecture*.** RFC 2903. Agosto, 2000. Disponível em < http://www.ietf.org/rfc/ rfc2903.txt>. Acesso em 03 de abril de 2010.

[RFC3575] Aboba, B., **IANA *Considerations for* RADIUS**, RFC 3575, julho, 2003. Disponível em <http://tools.ietf.org/rfc/rfc3575.txt>. Consulta em 07 de junho de 2010.

[RFC3576] Chiba, et al., ***Dynamic Authorization Extensions to Remote Authentication Dial In User Service* (RADIUS)**, RFC 3576, Julho, 2003. Consulta em 07 de junho de 2010.

[RFC3579] Aboba & Calhoun, **RADIUS (*Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol* (EAP).** RFC 3579, setembro, 2003.

[RFC3580] Congdon, et al., **IEEE 802.1X *Remote Authentication Dial In User Service (RADIUS) Usage Guidelines.*** RFC 3580. Setembro, 2003. Consulta em 01 de junho de 2010.

[RFC5176] Chiba, et al, ***Dynamic Authorization Extensions to Remote Authentication Dial In User Service* (RADIUS).** RFC 5176, janeiro, 2008. Disponível em < http://tools.ietf.org/html/rfc5176>. Consulta em 07 de junho de 2010.

[STEVENS1994] Stevens, W. Richard, **TCP/IP *Illustrated Volume 1: The Protocols*.** Addison-Wesley, 1994.

[W3COUNTER] W3Counter**, *Global Web Stats***, Disponível em <HTTP:// http://www.w3counter.com>. Consulta em 30 de maio de 2010.

# APÊNDICE A – INFORMAÇÕES PARA USO GERENCIAL E OPERACIONAL

Dentre os objetivos iniciais deste trabalho estava prevista a utilização dos dados, após o seu tratamento e as implantações planejadas, para geração de informações gerenciais sobre o comportamento dos clientes finais que pudessem ser confiavelmente utilizadas para tomadas de decisão, tanto comerciais como técnicas, além do uso em manobras como retiradas de serviços, alterações de equipamentos e implantações. Neste apêndice há um detalhamento dos dados tratados e as informações obtidas para estas finalidades.

## A.1. Dados e avaliação de perfil de utilização

Os dados utilizados para fazer as análises comportamentais foram os coletados no período de 01 de janeiro a 30 de julho de 2009, já com todas as correções e implantações finalizadas. As análises neste trabalho estão relacionadas aos comportamentos de autenticação não fazendo parte do escopo análises de picos de utilização dos sistemas e dos equipamentos.

Nestas análises foram usados os dados já filtrados pelos sistemas de Mediação, que eliminam bilhetes duplicados e informações não necessárias, mesmo assim, os dados de bilhetagem de cada mês têm normalmente mais de 15 GB quando somadas todas as UFs. Ao todo foram processados mais de 100 GB, utilizando scripts e programas desenvolvidos em linguagem de programação [AWK], que processa dados armazenados em arquivos texto.

## A.2. Horários de autenticação

É relevante quando se pretende fazer algum tipo de manobra em sistemas de autenticação, entender o comportamento dos clientes em relação aos horários de pico em suas tentativas de acesso, ou seja, os horários onde os sistemas afetados teriam os maiores

e os menores volumes de requisições, para que se possa fazer as manobras com menor impacto ou com maior abrangência, de acordo com a necessidade.

Para este objetivo, os dados de autenticações dos seis meses de conexão foram processados para verificar o número de autenticações realizadas dentro de cada intervalo de uma hora do dia. O resultado gerou a informação das médias percentuais de autenticações por hora apresentadas no gráfico da Figura A.1 a seguir.

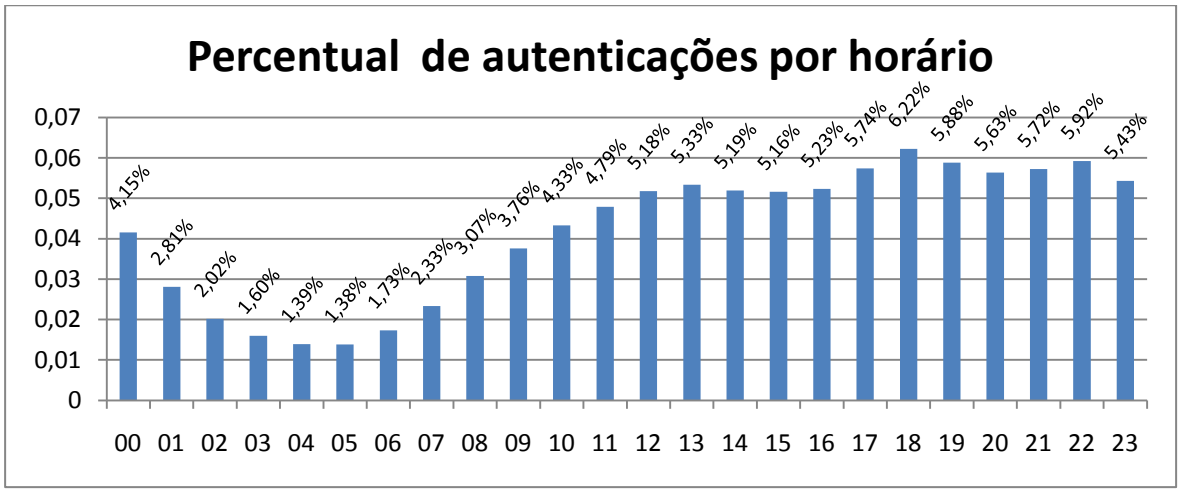



Figura A.1 - Percentual médio de autenticações nos intervalos de uma hora ao longo do dia

## A.3. Tempo de permanência conectado

Outra informação muito importante quando se pretende medir a quantidade de clientes autenticados e a ocorrência de autenticação, ou seja, se os clientes que utilizaram o serviço tiveram a necessidade de autenticação no período da medição. Para verificar esta informação, foram processados os dados de autenticação dos seis meses, verificando em todos os bilhetes de *stop* qual o tempo total da conexão. Para cada *login* foi utilizado então o tempo máximo de conexão no período, para verificar a quantidade de clientes que tiveram como tempo máximo de conexão os períodos listados. Esta análise resultou nos gráficos da Figura A.2 que mostra os percentuais de clientes que fizeram somente

conexões com duração máxima de até 30 dias e da Figura A.3 que mostra a distribuição em períodos maiores, divididos em intervalos de duração de 10 dias.

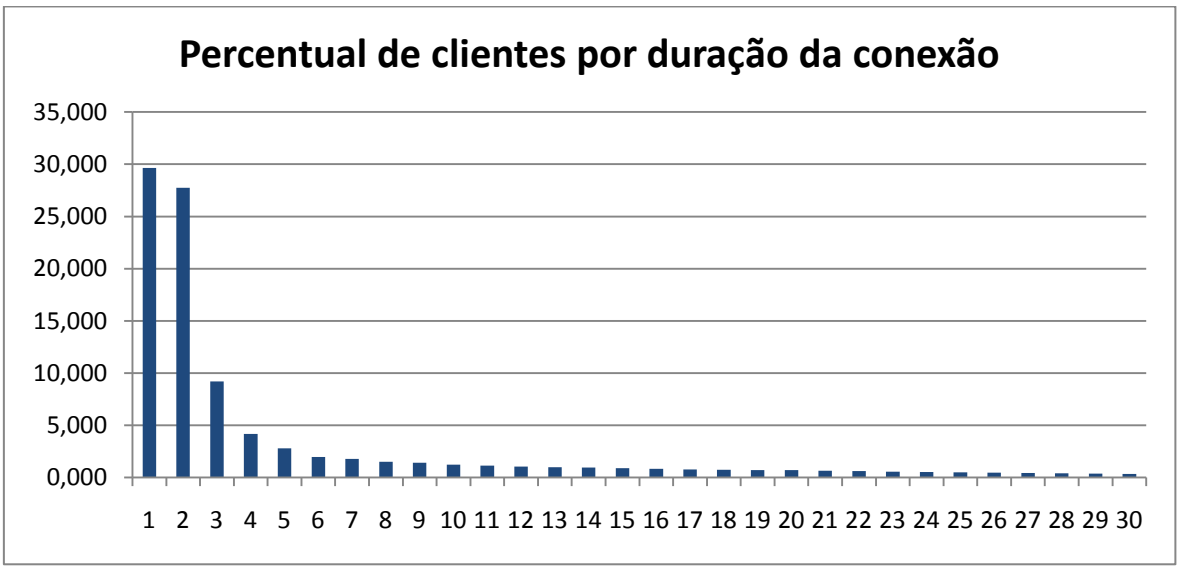



Figura A.2 - Percentuais de clientes com duração de conexão máxima de 30 dias

Na Figura A.2, pode ser verificado que a maior parte dos usuários fez somente conexões com duração menor do que 48 horas (57,41%), sendo que entre estes 29,65% fizeram somente conexões com duração menor do que 24 horas.

Um ponto relevante é que uma grande parte dos usuários já faz conexões de mais de 24 horas, o que deve ser considerado na avaliação de soluções de medição baseadas em bilhetagens intermediárias para conexões superiores a este período.

Para a solução de medição com períodos de apuração de um mês, a informação mais importante é a de quantos usuários da base fazem conexões com duração superior a este período, para isso é necessário verifica quais *logins* que fizeram conexões de 31 dias ou mais e verificar qual é o seu percentual em relação ao total de *logins* que fizeram conexão no período de seis meses.

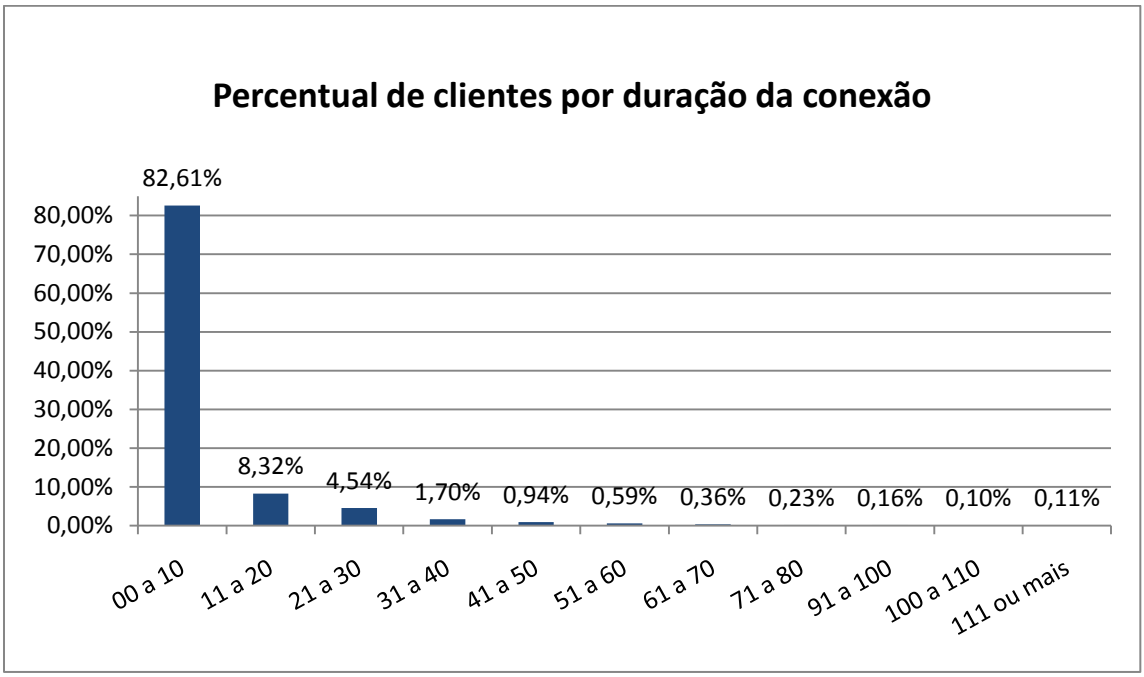



Figura A.3 - Percentuais de clientes por duração de conexão máxima

Na Figura A.3 pode ser verificado que 3,26% dos clientes fizeram conexões que duraram mais do que 30 dias, ou seja, em uma medição mensal pode não ter sido gerado um bilhete de *stop*, levando a ausência de registro para contabilização.

## A.4. Autenticações por dia da semana e do mês

Quando se pretende fazer qualquer tipo de manobra deve ser estudado além da hora qual é a melhor data para execução. Dois fatores são importantes, a quantidade de requisições que ocorrem no período da manobra ou após a interrupção de um serviço e os reflexos que a manobra ou a interrupção geram nos *Call Centers* de atendimento da operadora ou do ISP.

Para efeitos de análise diária, foi considerado o número de conexões iniciados em cada dia do período de medição. Os gráficos dos meses de janeiro e fevereiro, apresentados na Figura A.4, mostram que o número de conexões tem um comportamento previsível,

com menor quantidade de autenticações nos sábados, domingo e feriados e picos de autenticações nas segundas-feiras.

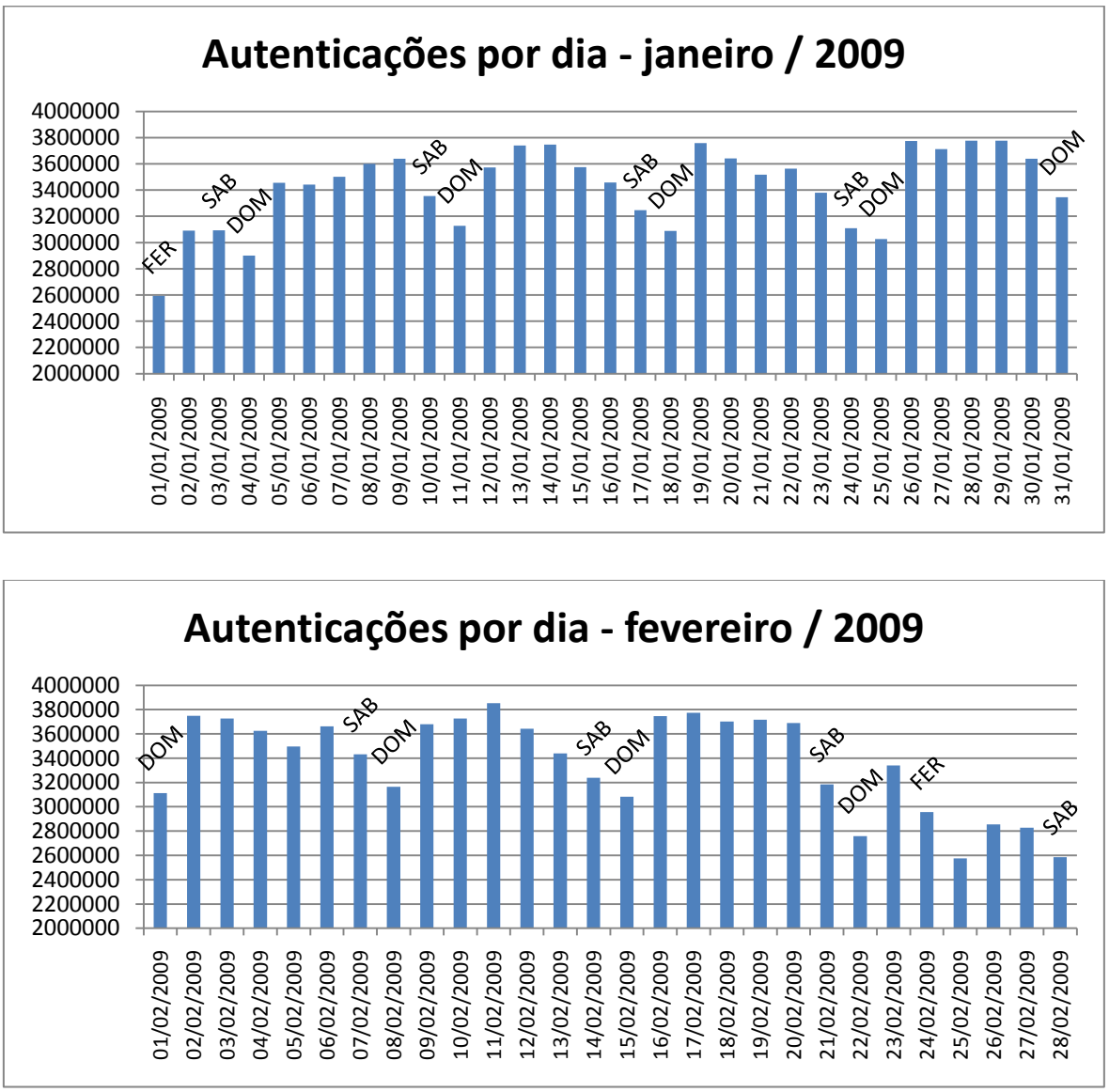



Figura A.4 – Quantidades de autenticações bem sucedidas por dia do mês

Na Figura A.4 observa-se que no dia 01 de janeiro de 2009, feriado nacional, ocorreram 2,5 milhões de autenticações, chegando ao máximo até 3,1 milhões durante o

feriado prolongado. Nas semanas seguintes o comportamento típico foi de entre 3,6 e quatro milhões de autenticações nos dias de semana e aproximadamente 3,3 milhões nos sábados e 3 milhões nos domingos. Os picos próximos a 4 milhões foram registrados todos nas segundas-feiras. O comportamento só foi alterado novamente na semana do feriado de carnaval, tendo 2,6 milhões de autenticações na quarta-feira de cinzas.

É importante considerar que manobras realizadas nos fins de semana e feriados podem ser indicadas se a interrupção não significar indisponibilidade posterior, uma vez que sempre após os domingos e feriados são registrados picos de autenticações, que podem ser somadas a chamadas nos *call centers* que os clientes deixam para fazer em dia útil, sendo represadas nos finais de semanas e acumuladas nas segundas-feiras.

## A.5. Manobras divididas por lotes

Muitas manobras podem significar interrupção ou até podem ser relacionadas a retirada de serviços, como ocorre no caso de rescisão contratual entre o ISP e a operadora. Para estes casos a indicação é de divisão por lotes para minimizar o impacto de relacionamento com o cliente final, já que este precisa entrar com contato com a operadora ou com o ISP para fazer sua regularização.

Uma das formas encontradas para fazer esta divisão foi o uso de lotes baseados na letra inicial do *login*, Neste caso o volume de clientes afetados é dividido em lotes que são formados por *logins* iniciados por grupos de caracteres, com o objetivo de limitar a quantidade atingida em cada manobra.

Normalmente, quando a ação envolve apenas um provedor, os lotes são formados tendo por base a listagem de clientes finais medidos para o provedor. Porém, em alguns casos as manobras atingem mais de um ISP, sendo necessário ter uma visão da distribuição média.

Para ter esta visão foram analisados os *logins* utilizados para conexão no período de seis meses avaliado, considerando cada nome como apenas uma ocorrência, para levantar a

distribuição média da base. A  Figura A.5 mostra o resultado desta distribuição, detalhada na Tabela A.1.

Tabela A.1 - Distribuição percentual de *logins* pelo seu primeiro caractere

| Letra inicial do *login* | Percentual |
|---|---|
| a | 10,19474% |
| m | 10,13033% |
| c | 7,61374% |
| j | 7,55261% |
| r | 7,16838% |
| l | 6,55781% |
| s | 5,74523% |
| e | 5,70824% |
| d | 5,17649% |
| f | 4,16147% |
| g | 3,97688% |
| p | 3,92776% |
| v | 3,31034% |
| t | 2,97452% |
| n | 2,89203% |
| b | 2,68936% |
| i | 2,41041% |
| w | 1,56553% |
| h | 1,54260% |
| k | 1,52647% |
| o | 1,26168% |
| z | 0,63387% |
| u | 0,27747% |

| Letra inicial do *login* | Percentual |
|---|---|
| y | 0,15892% |
| x | 0,12879% |
| q | 0,10911% |
| 4 | 0,06056% |
| 1 | 0,05437% |
| A | 0,04109% |
| J | 0,04068% |
| M | 0,03865% |
| R | 0,03718% |
| L | 0,02936% |
| E | 0,02760% |
| C | 0,02692% |
| D | 0,02428% |
| S | 0,02383% |
| F | 0,01832% |
| P | 0,01811% |
| 3 | 0,01780% |
| V | 0,01552% |
| G | 0,01512% |
| B | 0,01257% |
| I | 0,01141% |
| N | 0,01095% |
| T | 0,01039% |

| Letra inicial do *login* | Percentual |
|---|---|
| 2 | 0,00986% |
| K | 0,00912% |
| 9 | 0,00860% |
| 0 | 0,00682% |
| W | 0,00680% |
| H | 0,00661% |
| O | 0,00468% |
| 6 | 0,00431% |
| 5 | 0,00325% |
| 7 | 0,00279% |
| 8 | 0,00272% |
| Z | 0,00234% |
| U | 0,00070% |
| X | 0,00046% |
| Q | 0,00042% |
| _ | 0,00037% |
| Y | 0,00036% |
| . | 0,00019% |
| ~ | 0,00004% |
| \ | 0,00004% |
| - | 0,00003% |
| + | 0,00002% |

Quando se planeja a execução de manobras na rede, há sempre o objetivo de reduzir ao máximo o impacto negativo para o cliente final. Desta forma, a escolha da melhor data, horário e grupos (lotes) afetados em cada manobra são extremamente relevantes neste objetivo.

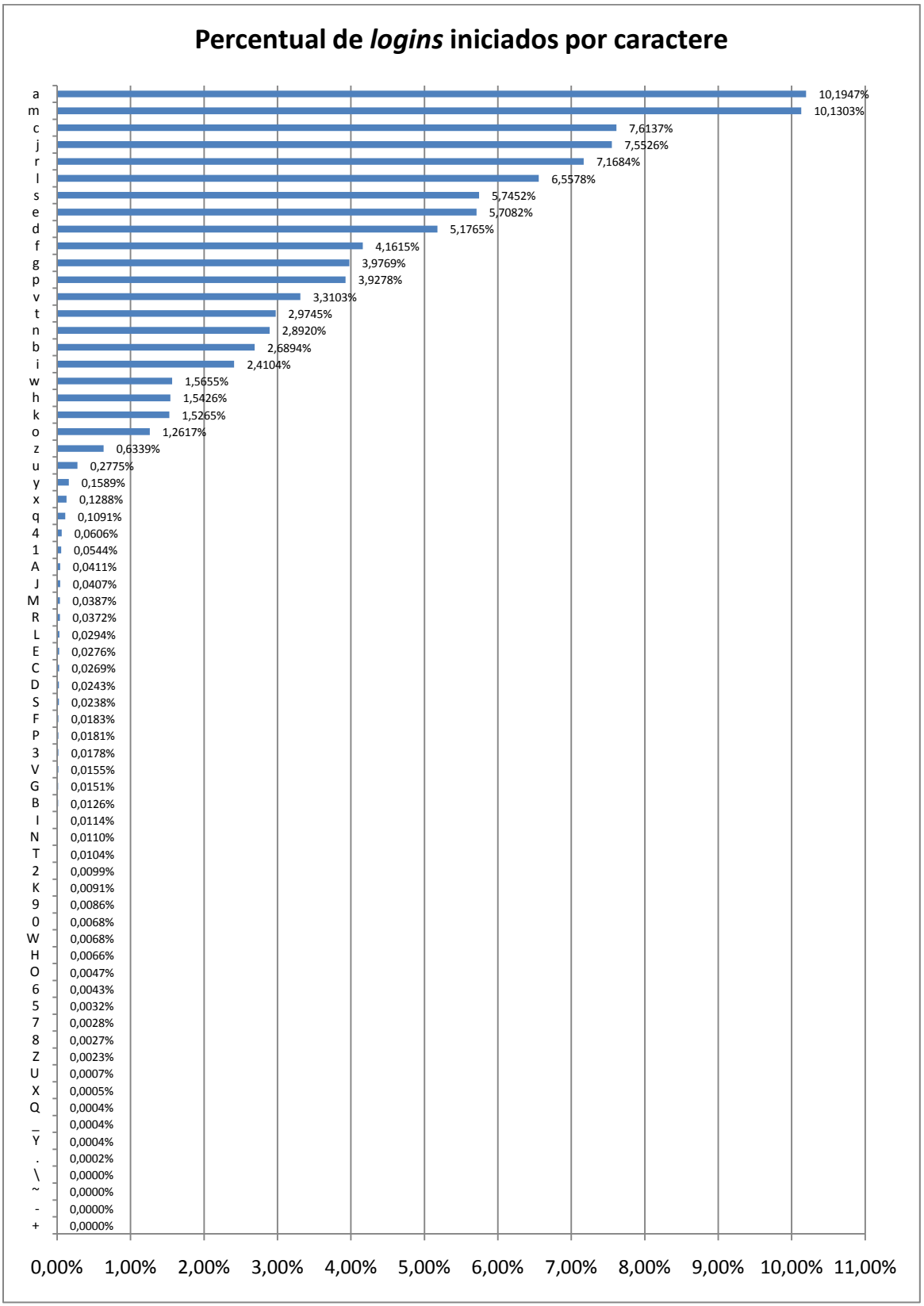



Figura A.5 – Distribuição percentual de *logins* pelo seu primeiro caractere