UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

PROPOSTA E IMPLEMENTAÇÃO DE ARQUITETURA PARA IDENTIFICAÇÃO FÍSICA E LÓGICA DE ACESSOS BANDA LARGA UTILIZANDO TECNOLOGIA ADSL

LEANDRO HENZ

ORIENTADOR: ANDERSON CLAYTON ALVES NASCIMENTO

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPGENE.DM - 057/2008

BRASÍLIA/DF: JULHO – 2008

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

PROPOSTA E IMPLEMENTAÇÃO DE ARQUITETURA PARA IDENTIFICAÇÃO FÍSICA E LÓGICA DE ACESSOS BANDA LARGA UTILIZANDO TECNOLOGIA ADSL

LEANDRO HENZ

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:

Anderson C A Nascimento

ANDERSON CLAYTON ALVES NASCIMENTO, Dr, ENE/UNB
(ORIENTADOR)

Flávio Elias

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

Rodrigo Pinto Lemos

RODRIGO PINTO LEMOS, Dr., UFG
(EXAMINADOR EXTERNO)

BRASÍLIA, 30 DE JULHO DE 2008.

FICHA CATALOGRÁFICA

HENZ, Leandro

Proposta e Implementação de Arquitetura para Identificação Física e Lógica de Acessos Banda Larga utilizando Tecnologia ADSL [Distrito Federal] 2008.

xx, 99p., 210 x 297 mm (ENE/FT/UnB, Mestre, Dissertação de Mestrado – Universidade de Brasília. Faculdade de Tecnologia.

Departamento de Engenharia Elétrica.

1. Banda Larga 2. ADSL

3. Autenticação 4. Protocolo PPPoE

I. ENE/FT/UNB II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

HENZ, LEANDRO (2008). Proposta e Implementação de Arquitetura para Identificação Física e Lógica de Acessos Banda Larga utilizando Tecnologia ADSL. Dissertação de Mestrado em Engenharia Elétrica, Publicação PPGENE.DM-057/2008, Departamento Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 99p.

CESSÃO DE DIREITOS

AUTOR: LEANDRO HENZ

TÍTULO: Proposta e Implementação de Arquitetura para Identificação Física e Lógica de Acessos Banda Larga utilizando Tecnologia ADSL.

GRAU: Mestre ANO: 2008

_____

Leandro Henz
Rodovia João Paulo, 764, apto 203A – João Paulo
Florianópolis – SC

DEDICATÓRIA

.

A Cynthia, minha esposa, maior incentivadora e fonte propulsora para que eu sempre busque crescimento pessoal e profissional.

A minha filha Laís que trouxe mais brilho e cor a minha vida.

Aos meus pais Adécio e Marlene que sempre me apoiaram em todos os momentos, são exemplos de vida e cuidaram da Laís quando Cynthia e eu precisamos.

Sem eles este trabalho não teria sido concluído.

AGRADECIMENTOS

Agradeço à Brasil Telecom pela iniciativa de formar uma turma de mestrandos e por ter patrocinado financeiramente este curso de mestrado.

Agradeço ao Dirval, Diretor de Engenharia e Operações da Brasil Telecom, que me incentivou, apoiou, acreditou e não me permitiu desistir, tornando este trabalho um sucesso.

Aos meus colegas Ana Luísa, Alexandre Piqueira, Angelita, André Gruszynski, Gustavo Brambila e Adriano Amaral que com muito companheirismo e humor tornaram os sábados de aula e os trabalhos em grupo menos desgastantes.

À Murilo Klock, grande conhecedor e estudioso de ADSL e participante ativo na realização deste trabalho. Foi um grande parceiro colaborando na realização do testes, implementação técnica e contribuições para o trabalho.

À Daniel Kratz, Wagner Rose e José Daniel que também contribuíram para a implementação deste trabalho na Brasil Telecom.

À André Gruszynski, grande estudioso e uma referência em processos de autenticação, autorização e bilhetagem. Sabe como ninguém todos os detalhes do protocolo RADIUS. Trouxe contribuições importantes ao trabalho.

Sem eles este trabalho não chegaria ao fim. Muito obrigado a todos vocês que foram fatores determinantes do meu sucesso.

.

RESUMO

O cenário de telecomunicações no Brasil e no mundo aponta nos últimos e para os próximos anos forte crescimento do segmento de Banda Larga.

No Planejamento estratégico de muitas operadoras de telecomunicações, o segmento de Banda Larga é vital porque disponibilizar acessos em banda larga aos seus clientes assegura: potencialização da receita por terminal, "blindagem" e manutenção do acesso de telefonia fixa e fidelização do cliente mediante previsões de aumento acirrado da concorrência.

Para combater a concorrência e potencializar a receita existe a necessidade de personalização e de customização dos serviços disponibilizados sobre Banda Larga.

Neste contexto, o trabalho é relevante, primeiramente, porque visa atender aspectos legais já que a metodologia desenvolvida possibilitará a identificação judicial expedida pela justiça para identificação de usuários que praticam atos ilícitos na Internet. Além disto, a vinculação entre a identificação física e lógica possibilitará a criação de novos serviços personalizados e customizados para as mais diferentes aplicações atendendo demanda de nichos específicos e possibilitando uma diferenciação dos serviços fornecidos entre os clientes e pela concorrência. Outro valor agregado deste processo é a detecção de fraude através da geração de bilhetes de autenticação cuja porta do DSLAM encontra-se vaga no inventário e, portanto, sem faturamento e a retro-alimentação do cadastro através das inconsistências entre a informação do inventário físico e informações lógicas dos bilhetes de autenticação.

A metodologia foi aplicada em DSLAMs de teste dos vários fabricantes existentes na planta da operadora pesquisada simulando as condições reais da planta e as topologias existentes. O resultado dos testes foi um sucesso e alcança os objetivos propostos. A implementação da metodologia está em andamento na planta ADSL, estando com 85% dos DSLAMs habilitados e 100% dos BRAS, com perspectiva de conclusão em setembro de 2008.

ABSTRACT

The telecommunications scenario in Brazil and abroad has been pointing towards a strong growth in the Broad Band segment in recent and in coming years.

This segment is vital to the telecommunication companies regarding increasing revenues per client, providing of POTS (plain old telephone service), market share protection, churn rate avoidance and customer fidelity in face of hard-pacing competitive environment. Aiming to reach these issues is necessary personalization and customization of broadband services.

This way, one of the goals of the present work is assure the compliance with legal issues, given that the methodology developed would allow court-issued identification of users who practice illicit acts on the Internet. In addition, the link between the physical and logical identification would allow the creation of new customized services for a variety of applications reaching the needs of specific market segments, allowing best performance against the competitors. Another issue is the detection of unauthorized authentication at the DSLAM (digital subscriber line access multiplexer). When it happens without appropriate billing it could be treated as a fraud indication, preventing and correcting inconsistencies between the information at the physical inventory and logical information from the authentication tickets.

The method was applied to DSLAMs from many different vendors in real work conditions within real facilities and the tests reached the proposed objectives. The process is in progress at the studied company's facilities with 85% of the DSLAMs and 100% of the BRAS (broadband remote access server) approved and the conclusion deadline is September 2008.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

TERMINOLOGIA

AAA	*Authentication, Authorization, Accounting*
AAL5	*ATM Adaptation Layer 5*
ADSL	*Asymmetric Digital Subscriber Line*
ADSL2+	*Asymmetric Digital Subscriber Line 2 plus*
AM	*Amplitude Modulation*
ANATEL	Agência Nacional de Telecomunicações
ANSI	*American National Standards Institute*
ASK	*Amplitude Shift Keying*
ATM	*Asynchronous Transfer Mode*
ATU	*ADSL Transmission Unit*
ATU-C	*Asymmetrical Terminal Unit – Central Office*
ATU-R	*Asymmetrical Terminal Unit – Remote*
BRAS	*Broadband Remote Access Server*
CAP	*Carrierless Amplitude and Phase*
CHAP	*Challenge Handshake Authentication Protocol*
CLEC	*Competitive Local Exchange Company*
CPE	*Customer Premise Equipment*

CRM	*Customer Relationship Management*
DFT	*Discrete Fourier Transform*
DHCP	*Dynamic Host Configuration Protocol*
DMT	*Discrete Multitone*
DNS	*Domain Name System*
DSL	*Digital Subscriber Line*
DSLAM	*Digital Subscriber Line Access Multiplexer*
ETSI	*European Technical Standard Institute*
FDM	*Frequency Division Multiplex*
FEC	*Forward Error Correction*
FUST	Fundo de Universalização dos Serviços de Telecomunicações
FM	*Frequency Modulation*
FTP	*File Transfer Protocol*
FTTx	*Fiber to the (H-House, B-building, etc)*
HDSL	*High-bit-rate Digital Subscriber Line*
HTTP	*Hypertext Transfer Protocol*
IDFT	*Inverse Discrete Fourier Transform*
IETF	*Internet Engineering Task Force*

IP	*Internet Protocol*
IPCP	*Internet Protocol Control Protocol*
IMS	*IP Multimedia Subsystem*
ISDN	*Integrated Service Digital Network*
ISP	*Internet Service Provider*
ITU	*International Telecommunication Union*
LCP	*Link Control Protocol*
LDAP	*Lightweight Directory Access Protocol*
MAC	*Media Access Control*
MPLS	*Multi-Protocol label Switching*
NAS	*Network Access Sever*
NAT	*Network Address Translator*
NCP	*Network Control Protocol*
OSI	*Open Systems Interconnection*
OSS	*Operaction Support System*
PADI	*PPPoE Active Discovery Initiation*
PADO	*PPPoE Active Discovery Offer*
PADT	*PPPoE Active Discovery Terminate*

PADR	*PPPoE Active Discovery Request*
PADS	*PPPoE Active Discovery Session-confirmation*
PAP	*Password Authentication Protocol*
PM	*Phase Modulation*
POTS	*Plain Old Telephony Services*
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*
PSK	*Phase Shift Keying*
PSTN	*Public Switched Telephone Network*
PVC	*Permanent Virtual Circuit*
QAM	*Quadrature Amplitude Modulation*
RADIUS	*Remote Authentication Dial In User Service*
RADSL	*Rate Adaptive DSL*
RFC	*Request For Comments*
SDH	*Synchronous Digital Hierarchy*
SDSL	*Symmetric Digital Subscriber line*

SHDSL	*Symmetric High-bit-rate Digital Subscriber Line*
SNR	*Signal-to-Noise Ratio*
SSH	*Security Shell*
TCP	*Transmission Control Protocol*
TDM	*Time Division Multiplex*
UDP	*User Datagram Protocol*
USB	*Universal Serial Bus*
VDSL	*Very-high-bit-rate Digital Subscriber Line*
VLAN	*Virtual Local Area Network*
VoIP	*Voice over IP*
VP	*Virtual Path*
VC	*Virtual Circuit*
VPN	*Virtual Private Network*
VSA	*Vendor-Specific Attribute*
WIMAX	*Worldwide Interoperability for Microwave Access*
WLL	*Wirelles Local Loop*
XDSL	*Família Digital Subscriber Line*
XML	*Extensible Markup Language*

1 INTRODUÇÃO

O cenário atual do mercado de telecomunicações vem apresentando nos últimos anos forte crescimento em serviços de comunicação de dados, sobretudo banda larga e serviços de tecnologia móvel.

No Brasil a taxa de crescimento de banda larga em 12 meses foi de 34% e no primeiro trimestre de 2008 registrou crescimento de 7,5%. A distribuição por tecnologia é constituída de: 75% acessos ADSL (*Asymmetric Digital Subscriber Line)*, 23% *cable* modem, 2% outros (FTTx (família *Fiber To The)*, satélite, WLL (*Wireless Local Loop*), etc.)[IDC].

Existe um forte apelo do governo em promover e incentivar o uso intensivo da Internet com programas que proporcionem a inclusão digital. A ANATEL (Agência Nacional de Telecomunicações), apoiada pelas operadoras de telecomunicações, utilizará recursos do FUST (Fundo de Universalização dos Serviços de Telecomunicações) para instalar serviço de Banda Larga em todas as escolas do país. Esta verba inicialmente estava destinada a outros setores [ANATEL].

A redução dos custos da tecnologia e da banda contratada de interconexão e também a redução do custo dos microcomputadores e *laptops*, inclusive com o incentivo de redução fiscal do governo corroboraram para o crescimento acentuado da Banda Larga no Brasil.

Não só o uso da Internet, mas também a criação de novos serviços como *VoIP*, *video-on-demand*, transmissão de vídeo em *broadcast*, jogos *on-line*, telemedicina, ensino a distância, monitoração e segurança à distância exigem acessos em velocidades cada vez maiores.

Outro ponto também bastante citado na literatura é a convergência das aplicações e redes para uma arquitetura de rede IP com a evolução para o IMS (*IP Multimedia Subsystem*) em desenvolvimento e padronização no momento [TR22.800].

Neste contexto, a tecnologia xDSL e mais especificamente o ADSL se tornaram uma excelente opção de Rede de Acesso para o atendimento da demanda por serviços de

Internet de alta velocidade, por utilizar a infra-estrutura já existente da rede de cabos das operadoras de telefonia, e permitir o tráfego simultâneo dos serviços de voz e dados sobre o mesmo par metálico. Portanto, o ADSL chegou para agregar valor à rede metálica legada que, segundo algumas previsões, já estaria com seus dias contados com o advento da fibra óptica. Isso fez com que essa rede ganhasse mais força como meio de acesso mais barato e viável, pois o alto custo com a implantação de uma rede óptica de acesso faz com que se adie sua implantação para a grande massa de consumidores. Para possibilitar a transmissão de dados e voz, o sistema utiliza FDM (*frequency division multiplexing*) a fim de dividir o espectro de freqüências em três partes: serviços de voz; *upload* e *download* de dados. O desempenho alcançado pelo ADSL está diretamente relacionado a um complexo e eficiente sistema de modulação, fazendo com que sua utilização ultrapasse os limites dos serviços de Internet proporcionando acessos com velocidade de *download* e *upload* cada vez maiores.

Na estratégia de muitas operadoras, uma das principais metas é disponibilizar acessos em banda larga aos seus clientes assegurando desta forma: potencialização da receita por terminal, "blindagem" e manutenção do acesso de telefonia fixa e fidelização do cliente ante previsões de aumento acirrado da concorrência.

A necessidade e criação de serviços de valor agregado, suportado por acessos em banda larga, formas diferenciadas de tarifação e fornecimento do serviço e convergência de serviços fixo-móvel também são necessárias para um diferencial competitivo.

Inicia-se uma fase intensiva de disponibilização de serviços personalizados e customizados para nichos específicos do mercado como: cobrança por uso, cobrança por banda contratada e excedente, banda garantida por aplicação, por exemplo: programas do tipo *peer-to-peer*, *triple-play* e *quadruple-play* [ROGERS].

Baseado neste cenário, o objetivo deste trabalho é analisar a forma mais eficaz, econômica e viável de implementação de uma metodologia que envolve implementação técnica, processos, sistemas e inventário para vinculação entre a identificação lógica e física dos acessos dos clientes de banda larga utilizando tecnologia ADSL.

Considera-se como premissa deste trabalho, que as operadoras de telecomunicações possuem um cadastro que indique a vinculação entre o cliente e a porta física do DSLAM ao qual este está conectado. Também, do ponto de vista de segurança, considera-se que as informações do bilhete de autenticação não sofrem manipulação e não são interceptadas, garantindo assim sua legitimidade.

O trabalho é relevante, primeiramente, porque visa atender aspectos legais já que a metodologia desenvolvida possibilita a identificação judicial expedida pela justiça para identificação de usuários que praticam atos ilícitos na Internet. Além disto, a vinculação entre a identificação física e lógica possibilita a criação de novos serviços personalizados e customizados para as mais diferentes aplicações atendendo demanda de nichos específicos e possibilitando uma diferenciação dos serviços fornecidos pela concorrência. Além dos objetivos principais é possível dois subprodutos deste processo: 1) a detecção de fraude através da geração de bilhetes de autenticação cuja porta do DSLAM encontra-se vaga no inventário e, portanto sem faturamento; 2) a retro-alimentação do cadastro através das inconsistências entre informação do inventário físico e informações lógicas dos bilhetes de autenticação.

Metodologicamente, o trabalho foi realizado adotando-se as seguintes etapas: a) análise dentro da empresa, na Diretoria de Engenharia e Operações, de um segmento com demanda crescente e que necessitasse de uma evolução técnica ou processual. Esta área foi a de Banda Larga, pois é um segmento estratégico da empresa porque além de uma forte expansão e aumento da receita associada, o ADSL é essencial para a "blindagem" dos terminais telefônicos da empresa estrategicamente vinculados (terminal + banda larga) garantindo assim a receita da assinatura básica e também retenção do cliente; b) dentro do segmento Banda Larga procurou-se identificar o que era necessário para o fornecimento de novos e variados serviços; c) pesquisa bibliográfica para identificar tecnicamente qual a melhor forma de implementar o vínculo entre a identificação física da porta do DSLAM onde o cliente está conectado e o bilhete de autenticação gerado a partir do uso do serviço pelo cliente; d) levantamento dos equipamentos (fabricante, modelo e versão de *software*), topologias de rede e características do serviço de banda Larga da operadora analisada; e) definição da solução técnica, aplicação de testes de laboratório e identificação dos

benefícios da implementação na operadora em questão; e) estudo dos processos vinculados ao tema, proposição de alteração e criação de novos procedimentos; f) análise dos sistemas de OSS (*Operation Support System*) utilizados pela operadora e proposição de adequações necessárias.

O trabalho encontra-se estruturado na seqüência a seguir descrita: no segundo capítulo é realizada uma descrição da tecnologia ADSL, aspectos de modulação, topologia e infra-estrutura da rede, princípios de funcionamento e processo de autenticação, autorização e bilhetagem. No terceiro capítulo é abordada a evolução histórica da rede ADSL da operadora pesquisada, planta atual, arquitetura, topologias e equipamentos existentes na operadora, os serviços ofertados e o processo de autenticação, autorização e bilhetagem. No quarto capítulo, abordam-se, as formas de implementação da vinculação entre a identificação física e lógica dos acessos ADSL do ponto de vista técnico, a definição da melhor alternativa, as adequações no sistema de inventário da operadora e a adoção das melhores práticas e processos de atualização do cadastro do inventário, garantindo-se que o cliente conectado numa determinada porta, de fato está conectado a mesma na estação. No capítulo cinco implementamos a metodologia sugerida e detalhada no capítulo anterior comprovando-se na prática os benefícios da identificação física e lógica dos clientes de acessos em banda larga. Por fim, no capítulo seis, apresentam-se as considerações finais, sugestões de trabalhos futuros e as conclusões sobre o estudo realizado.

2 A TECNOLOGIA xDSL

O objetivo deste capítulo é descrever a tecnologia xDSL (família *Digital Subscriber Line*), suas variações e aplicações, as técnicas de modulação empregadas, a codificação do canal, a arquitetura típica de uma rede ADSL e o processo de estabelecimento de uma conexão PPP (P*oint to Point Protocol*) passando pelo processo de autenticação do serviço banda larga. Este conjunto de informações formará a base conceitual para os próximos capítulos e para a fundamentação da solução técnica proposta nesta dissertação.

2.1 BREVE HISTÓRICO

Abaixo, segue em ordem cronológica e bem sucinta o histórico do ADSL desde seu surgimento até os dias atuais [GOLDEN]:

- 1985 – *Bell Labs* descobriu um novo modo de utilizar os tradicionais pares de cobre para suportar os novos serviços digitais;
- 1989 – Ano de concepção do ADSL;
- 1990 - Companhias telefônicas iniciaram a divulgação do ADSL como uma maneira de entrar no mercado de vídeo;
- 1995 – Companhias inovadoras vislumbraram o ADSL como um modo de oferecer acesso Internet de alta velocidade;
- Atualmente – ADSL é amplamente utilizado como tecnologia de acesso a serviços banda larga e no Brasil é predominante frente a outras tecnologias de banda larga.

2.2 TECNOLOGIA xDSL – VARIAÇÕES E APLICAÇÕES

A tecnologia DSL (*Digital Subscriber Line*) permite a utilização da infra-estrutura de acesso da rede de cabos já existente da rede telefônica convencional, para serviços de banda larga. Várias são as variações de xDSL (ver Tabela 2.1), mas a modalidade da tecnologia DSL que prevalece nas operadoras de telecomunicações é a ADSL e suas evoluções (ADSL2, ADSL2+), pois leva em consideração o fato de que as aplicações utilizadas pelos usuários exigem muito mais banda de *download (sentido Internet* – usuário*)* que *upload (*sentido usuário - *Internet).* A este fato, deve-se a tecnologia também ser denominada assimétrica. Desta forma vamos nos referir mais especificamente ao ADSL e suas evoluções a partir deste ponto.

Tabela 2.1: Variações da Tecnologia DSL

	2 ou 4 fios simétrico	**Dados e POTS compartilhado**	**Modulação**	**Taxa de Bit X Distância**
IDSL	2 fios simétrico	Não	2B1Q (4B3T)	160 kbps (2B+d+cabeçalho) até 5,5 km
HDSL	4 fios simétrico	Não	2B1Q ou CAP	1,544 Mbps até 3,6 km (784kbps por par)
SDSL	2 fios simétrico	Não	2B1Q ou CAP	64kbps a 2,3Mbps até 5,5km
ADSL	2 fios simétrico	Sim	DMT (Full Era ou G. Lite)	1,5Mbps/64kbps até 5,5km 6Mbps / 640 kbps até 2,7km
ADSL2 & ADSL2+	2 fios simétrico	Sim	DMT (Full Era ou G. Lite)	melhora taxa e alcance comparado ao DSL atingindo até 25Mbps
HDSL2	2 fios simétrico	Não	TC PAM	1,544 Mbps até 3,6 km
SHDSL	2 fios simétrico	Não	TC PAM	Até 2,32 Mbps
VDSL	2 fios simétrico	Sim	QM ou DMT	13Mbps, 26Mbps 52Mbps download para 1,4km, 0,9km e 0,3km respecivamente e 1,5Mbps a 26Mbps upload

Apesar de ser uma tecnologia mais acessível economicamente por utilizar a rede metálica de acesso já existente, como todas as outras tecnologias de transmissão de dados

em alta velocidade, essa também apresenta fatores limitantes que podem inviabilizar o atendimento a algumas regiões. Um dos fatores limitantes é à distância. A própria distância máxima permitida vai variar de acordo com os seguintes critérios:

- Bitola dos cabos;
- Tipo de isolamento;
- Existência de paralelos na rede
- Idade dos cabos;
- Qualidade das emendas e conexões

Na Figura 2.1, pode-se observar a limitação das tecnologias DSL conforme alcance:

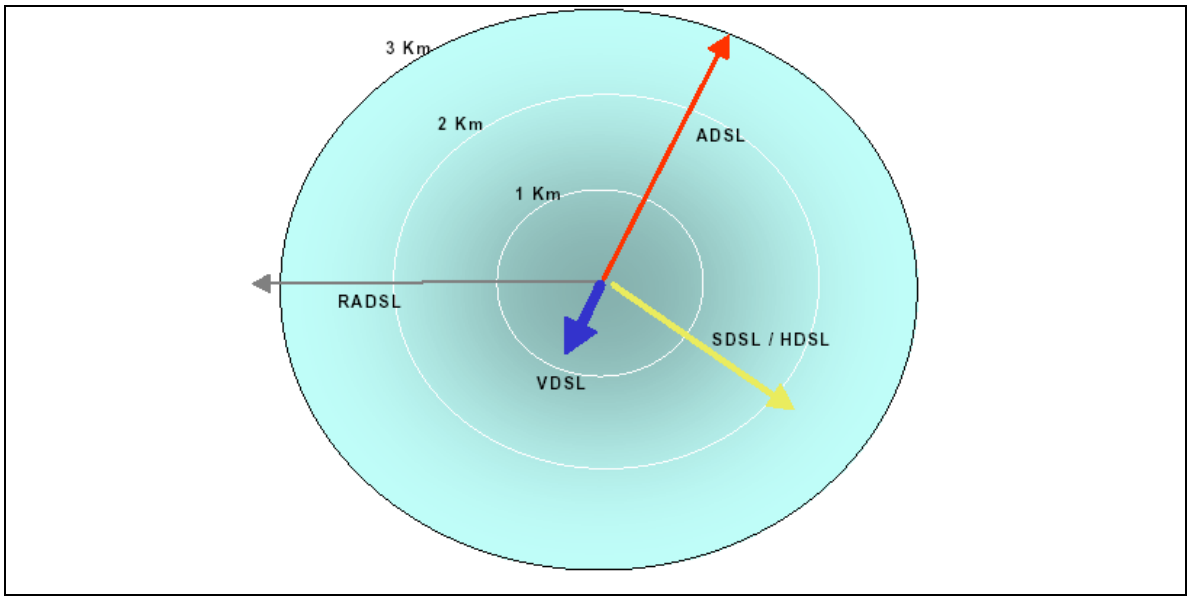

Figura 2.1: Raio de alcance das variações da tecnologia DSL conforme distância da central

Além disto, o máximo alcance vai depender da velocidade configurada no DSLAM (*Digital Subscriber Line Access Multiplexer)*.

2.3 TÉCNICAS DE MODULAÇÃO

Na tecnologia ADSL existem dois tipos de modulação: a modulação DMT (*Discrete Multitone*) e a modulação CAP (*Carrierless Amplitude and Phase*). Ambas são baseadas na modulação QAM (*Quadrature Amplitude and Phase Modulation*), onde cada símbolo é codificado com um par (amplitude, fase). Um exemplo do tipo de modulação 4-QAM está representado na Figura 2.2:

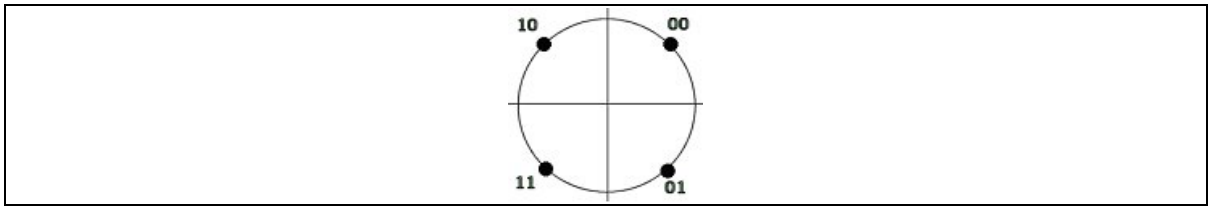

Figura 2.2: Modulação 4-QAM

A modulação DMT - que foi selecionada como padrão pela ANSI (*American National Standards Institute*) através da recomendação T1.413 e, posteriormente, pela ETSI (*European Telecommunications Standards Institute*), descreve uma técnica de modulação por multi-portadoras, na qual os dados são coletados e distribuídos sobre uma grande quantidade de sub-portadoras, com cada uma utilizando um tipo de modulação analógica QAM [ANSI T1.43]. Na modulação CAP, outra versão de modulação QAM, os dados modulam uma única portadora que depois é transmitida na linha telefônica. Antes da transmissão, a portadora é suprimida e, depois, é reconstruída na recepção.

Essas técnicas de modulação serão abordadas nesse capítulo.

2.3.1 O Espectro de freqüência

No sistema ADSL os sinais de voz e dados trafegam no mesmo par metálico mas não se misturam, devido ao fato de ocuparem em bandas de freqüência diferentes. O sistema telefônico utiliza a banda de 0 até 4 kHz, enquanto que o sistema ADSL trabalha na faixa de 25 kHz a 1,1 MHz, conforme Figura 2.3.

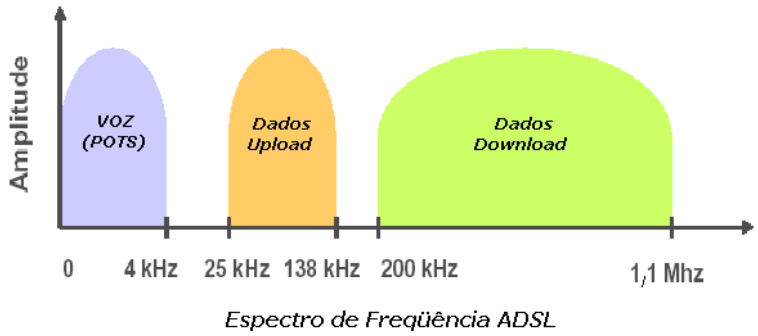

Figura 2.3: Sinal ADSL no domínio da freqüência

Para a transmissão do sinal, o ADSL utiliza a multiplexação por divisão na freqüência (FDM – *frequency division multiplexing*). Essa multiplexação é caracterizada por dividir o espectro de freqüências em várias "fatias" separadas, umas das outras, por "fatias de menores dimensões" de modo a possibilitar a utilização de filtros passa-faixa e assim isolar a banda desejada.

2.3.2 A modulação CAP

A modulação CAP (*Carrierless Amplitude and Phase*) é baseada em uma modulação QAM, no qual o sinal varia em amplitude e fase, tornando-se um sistema composto entre o ASK (*Amplitude Shift Keying*) e PSK (*Phase Shift Keying*).

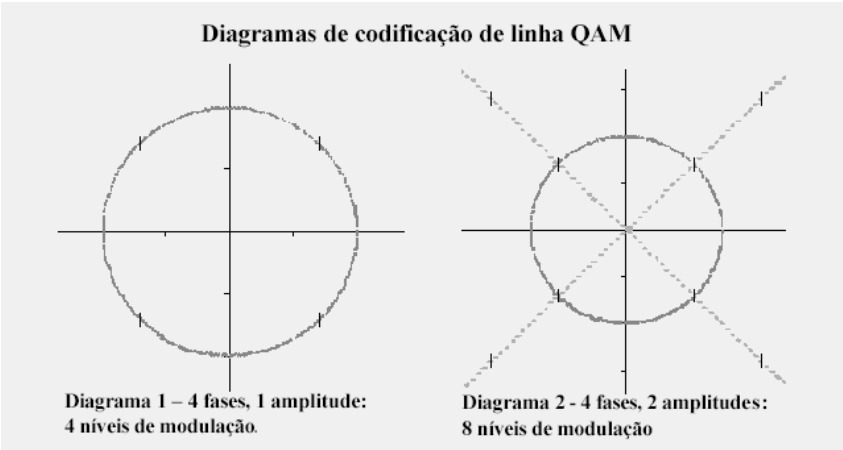

Figura 2.4: Diagramas de modulação QAM

Em um sinal ADSL, o número total de níveis modulados pode variar entre 4 e 1024 conforme as condições da linha.

Num sistema de modulação CAP só as bandas laterais transportam informação.

A modulação CAP divide a banda na linha telefônica em três canais. O primeiro, que ocupa a faixa até 4 kHz, é exclusivo para voz. O segundo é exclusivo para envio de dados do usuário para o servidor (*upstream*), e vai de 25 a 160 kHz. Já o terceiro canal, exclusivo para recepção de dados pelo usuário (*downstream*), começa em 240 kHz e vai até, no máximo, 1,5 MHz, conforme apresenta a Figura 2.5. Como os três canais são bem definidos e espaçados entre si, reduz-se a probabilidade de interferência entre canais [GINSBURG].

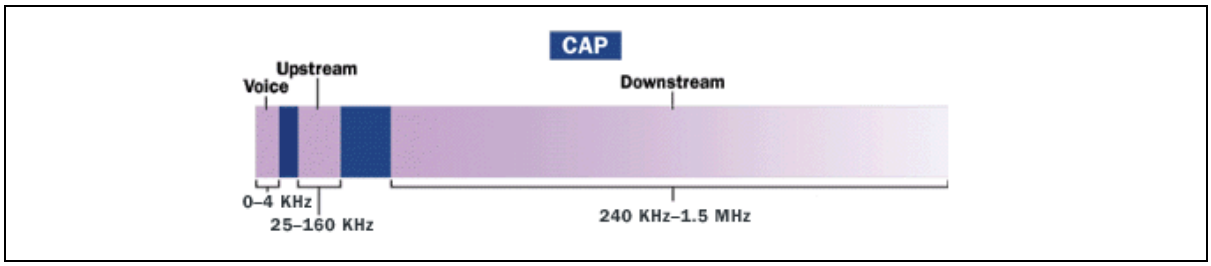

Figura 2.5: Separação dos canais na modulação CAP

Os diagramas das Figura 2.6 e 2.7 ilustram, respectivamente, o esquema básico de um transmissor e de um receptor CAP.

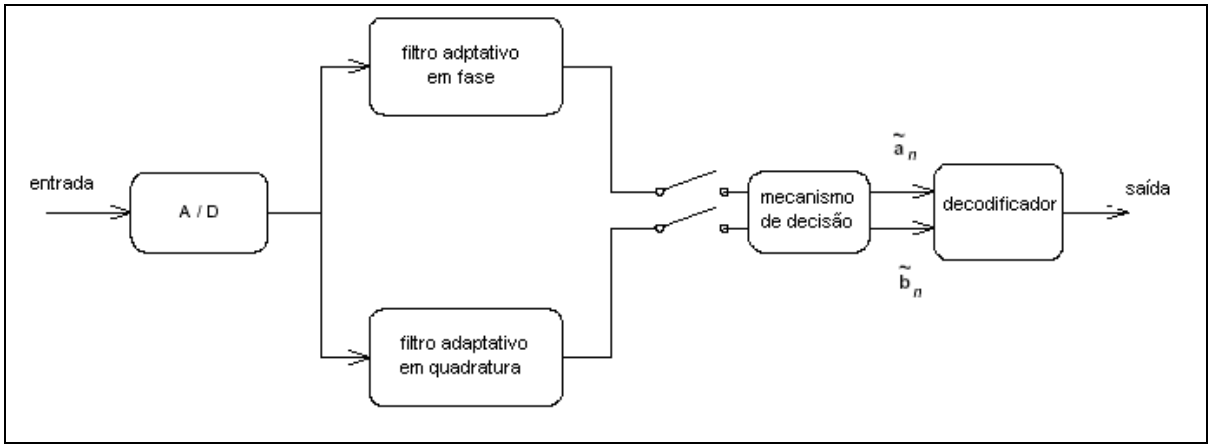

Figura 2.6: Esquema básico de um transmissor CAP

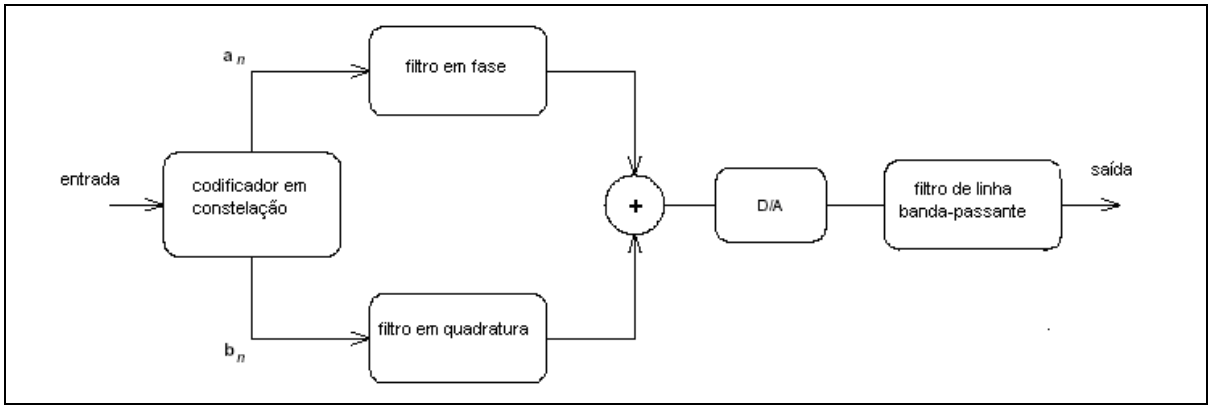

Figura 2.7: Esquema básico de um receptor CAP

2.3.3 A modulação DMT

A Modulação DMT (*Discrete Multi-Tone Modulation*) é um tipo de modulação multi-portadoras utilizada para transmissão em cabos. Nessa, o espectro de freqüência é dividido em sub-canais, cada qual com sua portadora, conforme a Figura 2.8.

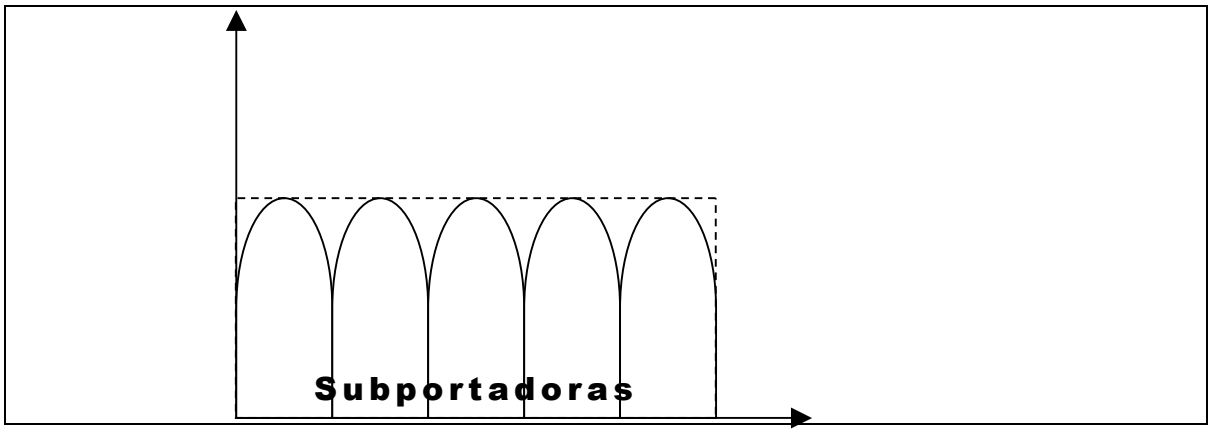

Figura 2.8: Divisão do espectro em várias portadoras.

Essa modulação utiliza:

- espectro de 0 a 4KHz para serviços de voz (telefonia convencional).
- espectro entre 26KHz e 1,1MHz para dados (banda larga).
- o espectro > 26KHz é dividido em 256 subcanais de 4Khz cada (24 canais para *upstream* e 222 para *downstream,* conforme Figura 2.9)
- baseado na qualidade de cada subcanal – aloca uma taxa de bits a cada um deles

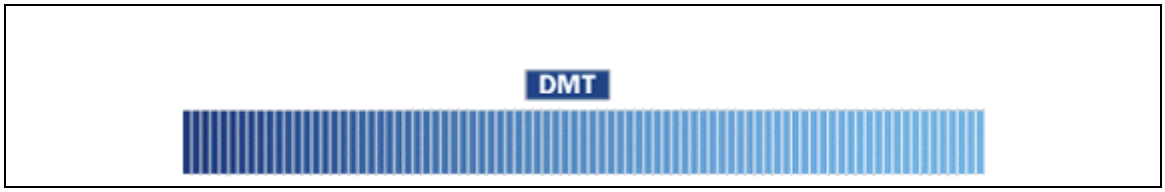

Figura 2.9: Faixa de downstream dividida em 222 portadoras na modulação DMT

As portadoras são moduladas em QAM, suportando de 0 a 15 bits de informação, tendo a variação de bits dependendo da qualidade da linha e do nível de ruído.

As portadoras são geradas a partir da utilização da Transformada Inversa Discreta de Fourier (IDFT - *Inverse Discrete Fourier Transform*), onde as subportadoras são ortogonais entre si, e, portanto não ocasionando interferências entre elas. Assim, não há a necessidade de banda de guarda para separá-las. De forma similar, o demodulador efetua a Transformada Discreta de Fourier (DFT – *Discrete Fourier Transform)* na recepção do sinal. A Figura 2.10 ilustra o esquema geral de um transmissor e receptor DMT.

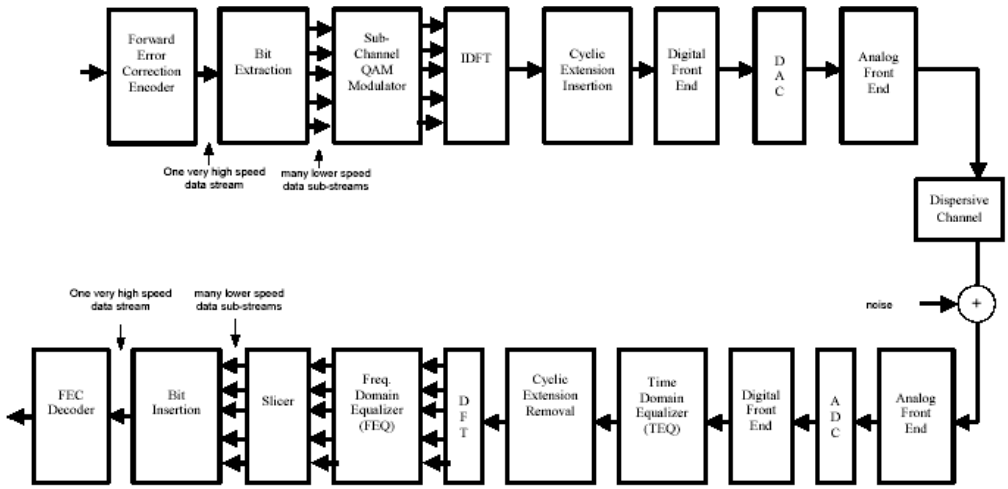

Figura 2.10: Diagrama de bloco geral de um sistema DMT

O transmissor constrói e envia símbolos DMT a uma taxa 1/T, onde T é o período do símbolo DMT. Os símbolos são modulados através de QAM.

Uma característica interessante do uso da modulação DMT é a possibilidade de transmitir em altas taxas de bits mesmo em canais sujeitos a ruídos como os cabos

telefônicos. Isso ocorre pelo fato do sistema alocar uma pequena quantidade de bits em cada portadora (no máximo 15), facilitando o transporte desses dados [ITU992.1].

Além disso, é possível se ajustar automaticamente quantidade de bits em cada portadora (carregamento de bits), reduzindo-se essa quantidade nas freqüências mais afetadas pelo ruído, ou mesmo, abandonando-as a fim de aumentar a relação sinal-ruído (SNR). Isso ocorre variando a dimensão da constelação QAM de cada portadora, em função da SNR, distribuindo a potência do sinal em suas diversas portadoras, de forma a tornar a transmissão mais eficiente possível. Dessa forma, dependendo da faixa de freqüência atingida pelo ruído e da intensidade deste, pode haver uma queda na taxa total de transmissão, em função do baixo carregamento de bits. A Figura 2.11 ilustra essa idéia [ITU992.1 e ITU992.2].

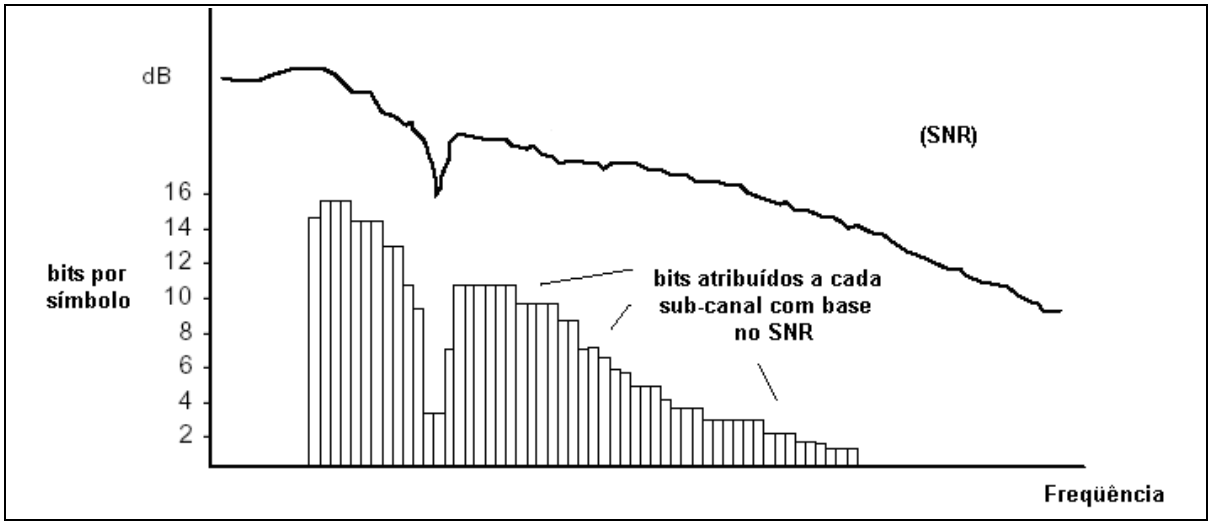

Figura 2.11: Carregamento de bits nas portadoras

Para executar essa operação de seleção dinâmica das portadoras, são trocados regularmente bits de controle entre DSLAM e o modem do cliente [MUNCINELLI].

2.3.4 CAP x DMT

A partir da quantidade de portadoras, já se tem a primeira diferenciação entre as modulações, visto que CAP é uma técnica de modulação com portadora simples que utiliza toda a largura de banda e a DMT é uma técnica de múltiplas portadoras que utiliza bandas

estreitas para cada uma delas. Segue um breve resumo com as principais diferenças entre as duas técnicas.

Equalização Adaptativa*:* essa é necessária para compensar a atenuação do sinal. Nessa o sistema aprende sobre as características da linha, através do envio e recepção de sinais sobre o canal. O sistema CAP necessita da equalização adaptativa em função das características do ruído variarem significativamente pelo espectro utilizado por essa técnica. O sistema DMT não necessita dessa equalização em função do sinal estar distribuído em pequenas bandas de freqüência (4 kHz cada), tornando-o mais imune ao ruído.

Consumo de Energia*:* em função da geração das múltiplas portadoras tornarem o circuito do DMT mais complexo, o mesmo consome mais energia do que o CAP.

Velocidade*:* em função das portadoras apresentarem poucos problemas de equalização e a possibilidade de adaptar as taxas em cada uma das portadoras para melhor aproveitar as características do canal, o sistema DMT apresenta vantagens na velocidade de transmissão quando comparado com o CAP.

Licença*:* o DMT é um sistema público, de padrão aberto através do ITU (*International Telecommunication Union*) e ANSI. Por outro lado, o CAP é de propriedade da *GLOBESPAN* [GLOBESPAN].

Assim, apesar da modulação CAP ser mais barata e ter o tempo de codificação menor, a modulação DMT é superior a ela nos seguintes pontos:

- Flexibilidade
- Maior imunidade ao ruído
- Capacidade de otimizar o ritmo de transmissão em incrementos menores: 32 kbps em DMT contra 340 kbps em CAP.

O sistema DMT é hoje o padrão previsto pelo ANSI desde 1994 e padronizado para o ADSL conforme normas G.992.1 e G.992.2 do ITU-T [ITU992.1, ITU992.2].

2.3.5 Codificação de canal

Trafegando nos cabos metálicos, o sinal ADSL enfrenta muitos problemas de ruído, principalmente na faixa superior do espectro de freqüência (próximo de 1,1 MHz), onde esses cabos apresentam alta atenuação. Dessa forma, são utilizados códigos para detecção e correção de erros através da correção de erro direta (FEC – *Forward error correction*). O código utilizado pelo ADSL é o *Trellis Code* (Código em Treliça).

O funcionamento deste método de detecção de erros consiste em permitir apenas um conjunto de transições entre estados. Se a mudança de estado não for permitida significa que houve erro na transmissão.

Esse código é utilizado em sistemas em que a largura de banda de transmissão é limitada (como é o caso do ADSL) e, embora exija um aumento do número de níveis de modulação, é bastante eficaz introduzindo um ganho de codificação significativo, conforme mostrado na Tabela 2.2.

Tabela 2.2: Ganho de Codificação utilizando Trellis Code

Número de estados *Da Treliça*	**Ganho de codificação (dB)**
2	1,1
4	3,54
8	4,01
16	4,44
32	5,13
64	5,33
128	5,33
256	5,51

É importante frisar que a utilização de técnicas FEC obriga a implementação de eletrônica mais avançada e portanto de maior custo para o DSLAM e o modem do cliente [GOLDEN].

2.4 TRANSMITINDO VOZ E DADOS SIMULTANEAMENTE

A Tecnologia ADSL possibilita a transmissão simultânea de dados e voz na mesma linha telefônica.

O assinante ao digitar seu usuário e senha de acesso à Internet, os dados serão passados à rede telefônica juntamente com a voz de quem está ao telefone pelos fios dos quadros/armários de interligação de sua residência, até o cabo de interligação que fica na central telefônica.

O sinal combinado de voz e dados entra num filtro denominado *splitter* que separa voz dos dados. A voz é encaminhada para a rede de comutação de circuitos da companhia telefônica (PSTN – *Public Switched Telephone Network*) e procede pelo seu caminho como de costume. Os dados são encaminhados para o DSLAM. No DSLAM há um modem ADSL que é identificado por um endereço chamado porta. Cada modem de assinante tem a sua porta correspondente no DSLAM.

No DSLAM concentram-se vários usuários e o sinal parte para a rede de transmissão de dados, que pode ser uma rede ATM ou Ethernet, através de um meio que tem capacidade para muitos usuários. Ligado a esta rede, há um sistema que identifica qual é o endereço de internet que será atribuído à interface de rede da máquina do usuário, podendo ser fixo ou não; porém somente após o processo de validação da autenticidade do usuário é que este endereço é liberado para que, assim se possa navegar na Internet.

A Figura 2.12 mostra o funcionamento do ADSL através da rede, utilizando os cabos de fios de cobre que permeiam toda área de atuação das operadoras de Telecomunicações.

Legenda:

Transmissão de voz

Transmissão de dados

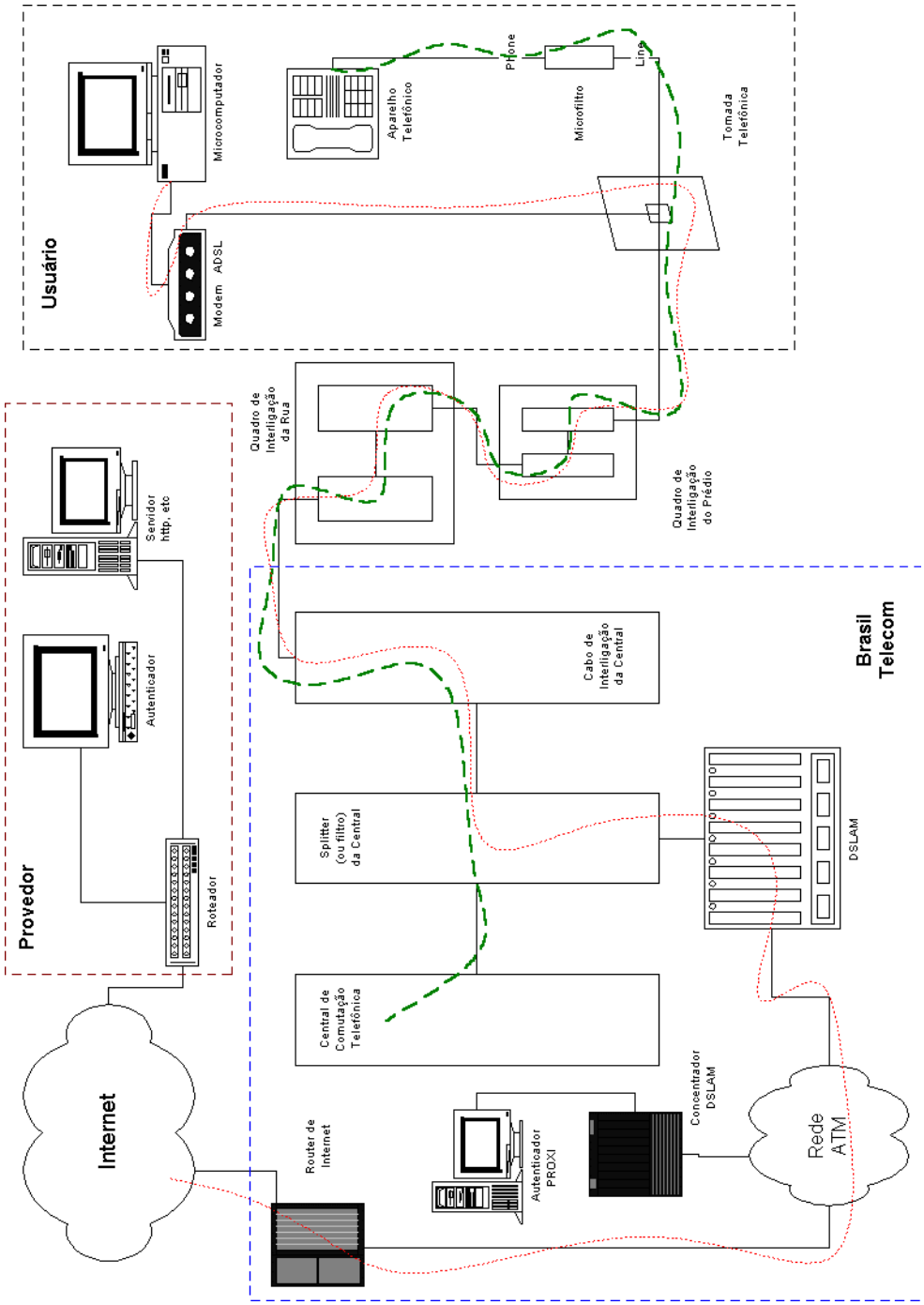

Figura 2.12: Funcionamento do ADSL – voz e dados trafegando simultaneamente no ambiente da Operadora e do cliente

2.4.1 Como voz e dados trafegam no mesmo par metálico

Os sinais de voz e dados não se misturam e trafegam no mesmo par metálico, devido ao fato de trabalhar em bandas de freqüências diferentes. O sistema telefônico trabalha numa banda de 1Hz a 4 kHz, enquanto o sistema ADSL centenas de portadoras para *downstream* e dezenas para *upstrea*m, todas com uma largura de banda de 4 kHz, sendo a primeira próxima a 11kHz e a última próxima a 1,1 MHz, conforme Figura 2.13.

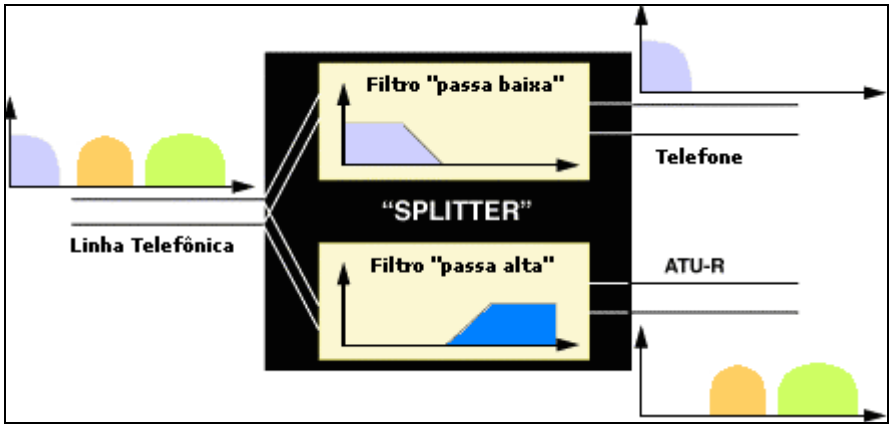

Figura 2.13: Distribuição de freqüências ADSL

Com a adição do processo de cancelamento de eco, o número de portadoras de *upstream* pode aumentar. Cada portadora pode levar de 0 a aproximadamente de 11 a 15 *bits*, dependendo da tecnologia fornecida pelo fabricante, conforme Figura 2.14.

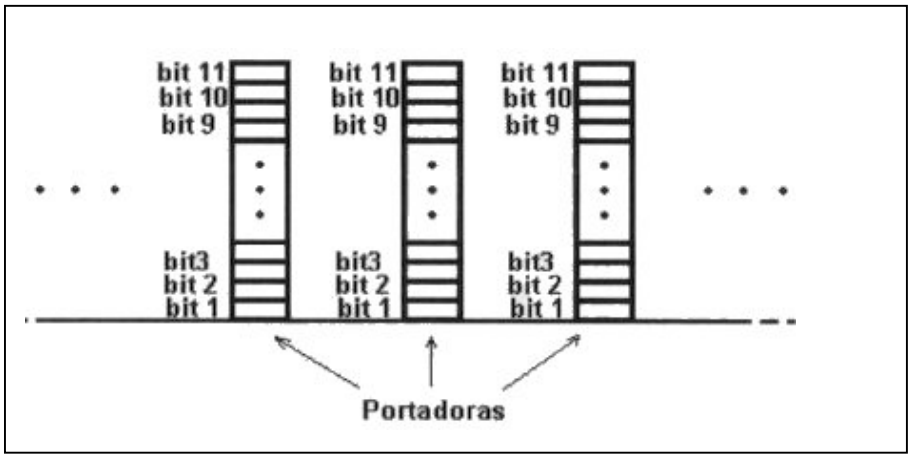

Figura 2.14: Representação da quantidade de bits por portadora transportados no espectro de freqüência do ADSL

2.5 ARQUITETURA DE UMA REDE ADSL

Neste item descreveremos os principais elementos que compõem a rede ADSL possibilitando o provimento de serviços Banda Larga. A figura 2.15 apresenta uma visão simplificada destes elementos.

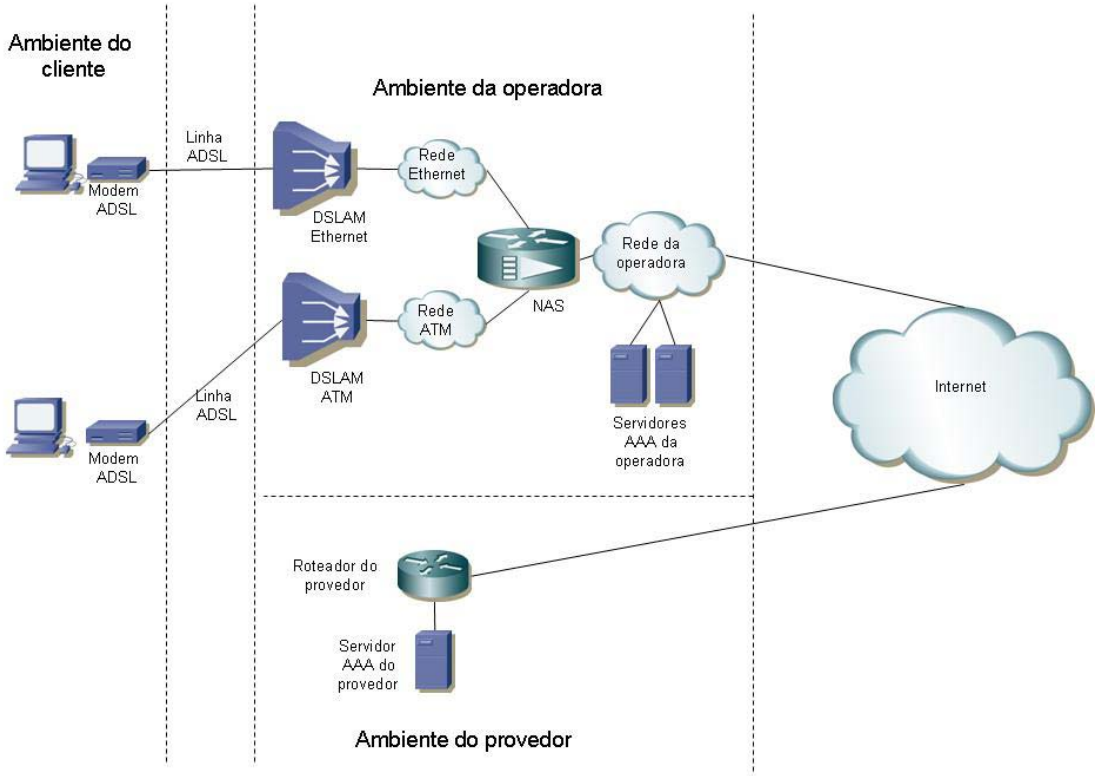

Figura 2.15: Elementos principais da arquitetura de rede ADSL (Fonte:[GRUSZYNSKI,2008])

Na Figura 2.16, está representado, de forma simplificada, o esquemático de uma instalação da última milha de um acesso ADSL. Descreveremos os elementos de rede e suas funções.

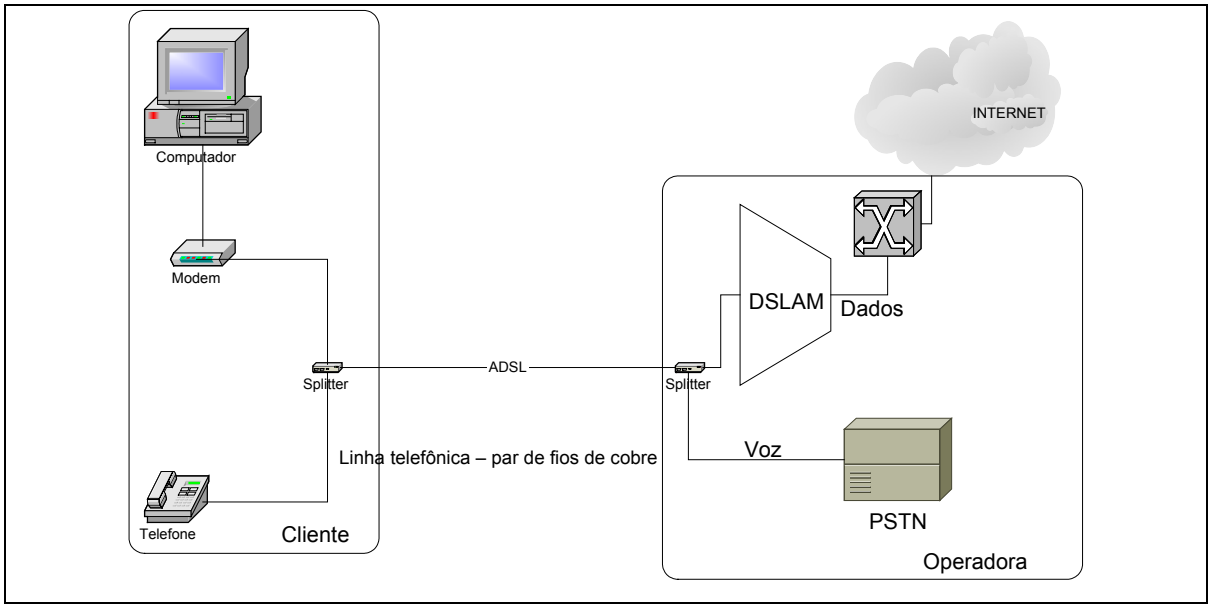

Figura 2.16: Esquema básico de uma instalação de um acesso ADSL

2.5.1 Modem ADSL

O modem ADSL de assinante, também conhecido como CPE (*Customer Premise Equipment*) pode ser do tipo interno ao computador (na forma de placas) e externo, com conexão ethernet ou USB, podendo também acumular as funções de roteador.

As características técnicas e funcionais deste equipamento são definidas na norma [ITU992.1], a qual o denomina de ATU-R (*ADSL Transceiver Unit – Remote*).

Este equipamento pode operar basicamente de duas formas: como roteador ou como *bridge*. Quando funciona como roteador, o modem possui recursos internos para estabelecer a conexão lógica com o BRAS (*Broadband Remote Access Server*). Quando funciona como *bridge*, os recursos necessários para o estabelecimento de uma conexão lógica devem estar instalados no computador do cliente. A Figura 2.17 apresenta as conexões lógicas para as duas possibilidades de operação. A Figura 2.18 mostra painel frontal e traseira de um moem ADSL comercializado no Brasil.

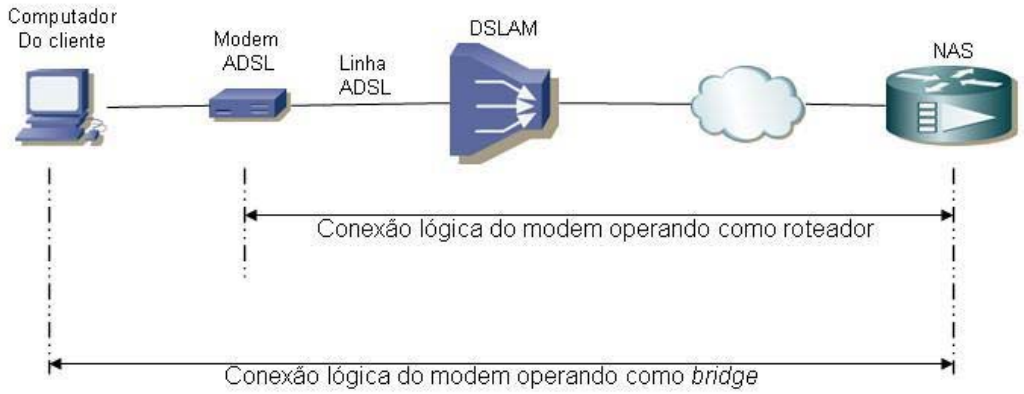

Figura 2.17: Conexões lógicas para as duas possibilidades de operação do modem ADSL (Fonte: [GRUSZYNSKI,2008])

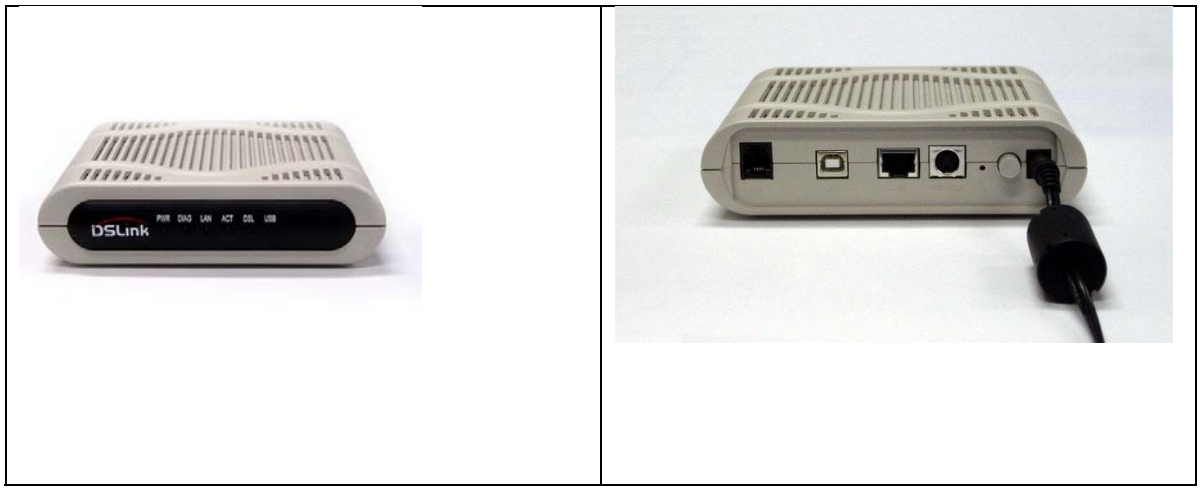

Figura 2.18: Modem ADSL DSLink 200U/E funciona em modo Bridge ou Router com conexão USB ou ethernet com o microcomputador do assinante

2.5.2 Splitters

O par trançado da linha ADSL chega à central telefônica e necessita ser dividido e filtrado, sendo que uma parte vai para comutação telefônica comum (POTS) (freqüências de 0 a 4 kHz) e a outra vai para o DSLAM (de 20 kHz a 1,1 MHz).

Existe também o *splitter* que é localizado na instalação do assinante, também denominado micro-filtro, dividindo e filtrando o sinal que vai em direção ao modem do assinante (de 20 kHz e 1,1 MHz) e que vai para o aparelho de telefone (freqüências de 0 a 4 kHz).

2.5.3 DSLAM

O DSLAM (*Digital Subscriber Line Access Multiplexer*), também definido como ATU-C (*ADSL Termination Unit – Central Office*) pela norma [ITU992.1], pode ser definido como sendo um dispositivo que contém o chassis onde estão os modems DSL do lado da central, agregando os mesmos na conexão ATM/ETH que proverá o acesso ao *backbone internet*. É um equipamento que está localizado no ambiente da operadora, e é onde os pares metálicos são conectados aos modems ADSL, após a divisão no *splitter* (que será abordado na seqüência).

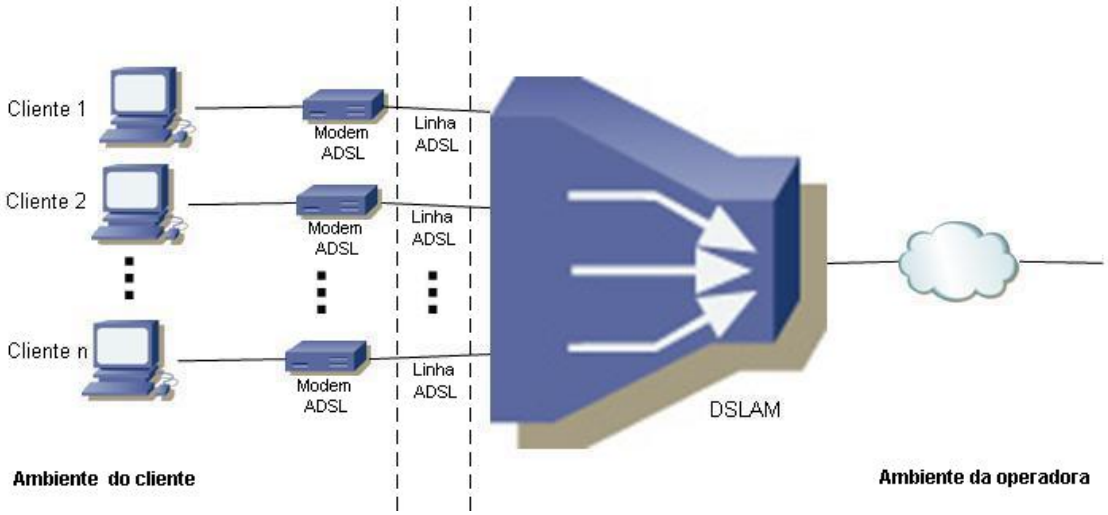

Figura 2.19: O DSLAM agrupa os modems do lado da operadora (Fonte: [GRUSZYNSKI,2008])

Existem basicamente dois tipos desse equipamento, o DSLAM ATM (*Asyncronous Transfer Mode*) e o DSLAM *Ethernet*. A diferença principal entre um e outro, é que o DSLAM ATM está conectado ao BRAS (*Broadband Remote Access Server*) utilizando interface ATM e o DSLAM Ethernet está conectado ao BRAS utilizando interface

Ethernet. Atualmente praticamente todos os novos DSLAMs implantados nas redes das operadoras são Ethernet devido ao maior número de serviços possíveis, maior facilidade em configurar tais serviços e custo bastante reduzido.

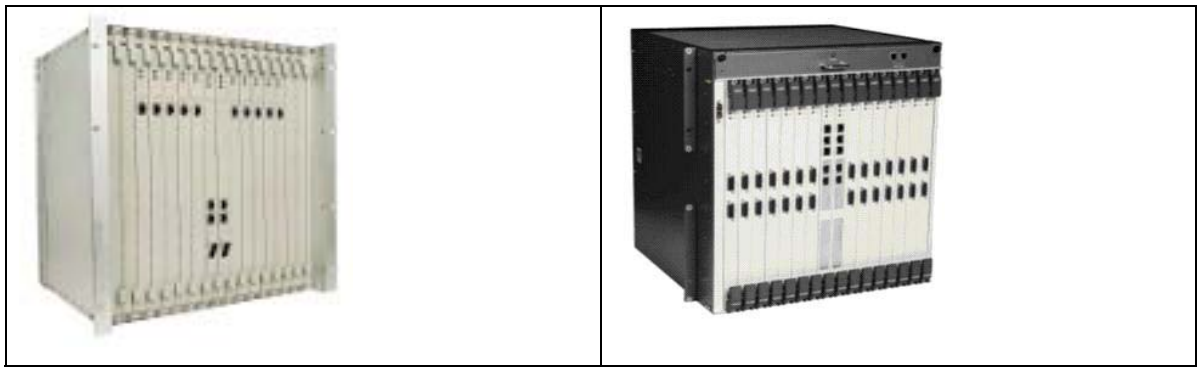

Figura 2.20: DSLAM ATM Huawei MA5100 e DSLAM ETH Huawei MA5600 (Fontes: [HUAWEIa, HUAWEib])

Na Figura 2.20 são mostrados os DSLAMs da Huawei, modelos MA5100 e MA5600, respectivamente DSLAMs ATM e Ethernet com capacidade de até 448 assinantes.

Na figura 2.21 estão representados os equipamentos de agregação utilizados no núcleo da rede de Dados para transporte do ADSL ao *backbone* IP.

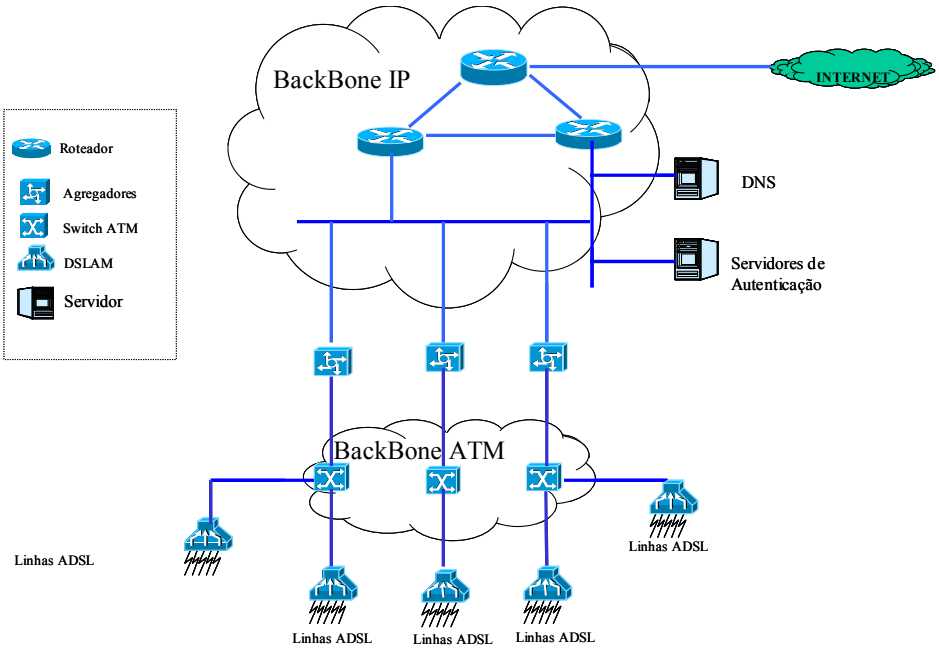

Figura 2.21: Diagrama Simplificado da Rede de Transporte e Agregação do ADSL.

2.5.4 Switches ATM

Switches ATM são equipamentos capazes de agrupar um conjunto de DSLAM ao BRAS também denominado ao longo deste trabalho de Agregador ou Terminador.

Ele é composto dentre outras, de placas com interfaces de 155Mbps, 34Mbps e 2Mbps que por sua vez possuem portas ATM. É através destas portas que os DSLAMs são interligados por meio de fibras.

2.5.5 Switches IP

A idéia é a mesma dos Switches ATM, ou seja, concentrar dentre outros todas as terminações dos DSLAMs, sendo que neste caso, os switches IP concentram DSLAMs Ethernet. A ligação entre estes switches e os DSLAMs também é feita via fibra, porém em vez de PVCs (*Permanent Virtual Circuit*) utilizam-se de VLANs (*Virtual Local Area Network*).

2.5.6 BRAS (Broadband Remote Access Server)

Pode-se definir o BRAS como equipamento responsável por agregar ou terminar conexões vindas de um ou mais DSLAMs instalados na planta. Estes equipamentos são os responsáveis também por terminar a sessão PPP (*Point to Point Protocol*) do assinante e designar um endereço IP válido ao mesmo para utilização do serviço. Nesta dissertação quando surgir as designações NAS, Agregador ou Terminador estamos nos referindo a este equipamento, também conhecido por estas expressões.

Dentre seus serviços, exemplificamos alguns:

- Terminador de sessão PPP;
- Serviços de AAA (*Authentication, Authorization, Accounting)*;
- Terminador de túneis;

- Serviços de VPN (*Virtual Private Network*);
- Serviços de MPLS (*Multi-Protocol Label Switching*);
- Alocação de IP (*Internet Protocol*) para o assinante;

Uma vez que o usuário é autenticado através de servidores RADIUS (*Remote Authentication Dial In User Service*), a negociação do IPCP toma lugar e o endereço IP (sempre válido) é designado para o modem ou micro do cliente (dependendo da origem da sessão PPP).

Figura 2.22: Agregadores das empresas Juniper Networks e Cisco Systems (Fontes: [CISCOa; JUNIPERb]).

O BRAS apresentado na Figura 2.22, à esquerda, da fabricante *Juniper Networks*, é o modelo ERX 1440, que pode atender até 48.000 acessos simultâneos. O da direita é o modelo 10008, da empresa *Cisco Systems*, cuja capacidade é de 61.500 conexões simultâneas. Estas capacidades foram verificadas por [MIERCOM].

2.5.7 Servidores AAA (Authentication, Authorization, Accounting)

Conforme [GRUSZYNSKI,2008] os servidores AAA (*Authentication*, *Authorization*, *Accounting*) são os elementos de rede que decidem se a conexão lógica de um cliente ADSL pode, ou não, ser estabelecida e registram os eventos de conexão e desconexão.

No Brasil, por determinação da Agência Nacional de Telecomunicações (ANATEL), o uso do ADSL para provimento de acesso a Internet é regido pelo Regulamento do Serviço de Comunicação Multimídia [REGSCM]. Este regulamento determina que uma

conexão ADSL à Internet da operadora não pode ser fornecida sem a utilização de um provedor de serviços Internet. Assim, para que uma conexão possa ser estabelecida, os servidores AAA da operadora consultam os servidores AAA do provedor do cliente, em busca de informações que permitam a decisão de aceitar a conexão ou declinar da solicitação.

2.6 ESTABELECENDO UMA CONEXÃO

Neste item descreve-se como é estabelecida uma conexão lógica sobre acessos ADSL, descrevendo os protocolos habitualmente utilizados e de suas variações presentes em uma arquitetura de rede ADSL. O objetivo desta seção é descrever o protocolo PPP (*Point to Point Protocol*) que é usualmente empregado atualmente. A importância de conhecer como o PPP funciona será base teórica importante para o entendimento da implementação técnica sugerida nesta dissertação.

2.6.1 Protocolo PPP (Point to Point Protocol)

O protocolo PPP é definido pelos documentos [RFC1661, RFC1662, STD1]. Segundo [RFC1661], PPP é um protocolo que provê um método padronizado para transportar datagramas multiprotocolos sobre enlaces ponto-a-ponto, sendo composto por três componentes principais: um método para encapsular os datagramas multiprotocolos, um protocolo de controle do enlace (LCP – *Link Control Protocol*), que é utilizado para estabelecer, configurar e testar a conexão, e uma família de protocolos de controle de rede (NCP – *Network Control Protocol*), que é utilizada para estabelecer e configurar diferentes protocolos de camada de rede.

Segundo [GRUSZYNSKI,2008] são três as principais fases do estabelecimento de uma conexão PPP:

- Fase LCP: nesta fase, além de negociados os parâmetros do enlace, tais como tamanho máximo do quadro e velocidade do enlace, é ajustado o mecanismo de

autenticação que será utilizado durante a próxima fase. Este mecanismo pode ser PAP (*Password Authentication Protocol*) ou CHAP (*Challenge handshake Authentication Protocol*). Uma fase adicional pode ser utilizada para certificar-se sobre a qualidade de linha com o objetivo de verificar a viabilidade de, posteriormente, estabelecer os protocolos de rede.

- Fase de autenticação: esta fase foi criada para que o mecanismo de autenticação negociado da fase anterior seja utilizado. O ponto de terminação do PPP pode autenticar o suplicante diretamente (modelo de suas partes) ou funcionar como um agente intermediário, passando as credenciais de autenticação para um servidor de AAA (modelo de três partes). Note-se que, na arquitetura convencional de acesso ADSL, somente o lado da rede realiza a autenticação, mas o PPP possui suporte para a realização de autenticação mútua.

- Fase NCP: nesta fase os parâmetros da camada de rede, tais como a compressão de cabeçalho e o protocolo de rede, são negociados. O protocolo IPCP *(Internet Protocol Control Protocol)*, definido em [RFC1332], é o NCP para estabelecer e configurar o protocolo IP sobre o PPP.

O padrão do PPP [RFC1661] especifica que a fase de autenticação é opcional, mas, caso seja desejada, a implementação deve requerer o uso da autenticação durante a fase LCP. Caso a autenticação deva ser realizada – que é a condição normal em uma rede ADSL –, a mudança da fase de autenticação para a fase NCP somente pode ocorrer caso a autenticação seja bem-sucedida; caso contrário deverá interromper o estabelecimento do enlace.

Uma vez completadas as três fases, o enlace PPP é estabelecido.

A seguir descreveremos as variações do PPP, apontadas por [GRUSZYNSKI,2008], e que dependem basicamente da arquitetura de Rede ADSL empregada. O protocolo PPPoE (*Point to Point Protocol over Ethernet*) será descrito com maior nível de detalhe, pois é no estabelecimento do PPPoE que é inserida a identificação do *slot* e porta física do DSLAM por onde esta conexão lógica é estabelecida.

2.6.1.1 PPPoA (Point-to-Point Protocol over ATM)

O PPPoA é uma variação do protocolo PPP, definida pela [RFC2364], que é utilizada para estabelecer a conexão entre o modem ADSL do cliente (ATU-R) e o NAS. Nesta variação o PPP considera a camada AAL5 (*ATM Adaptation Layer 5)* como um enlace ponto-a-ponto, situação que pode ser observada nas pilhas de protocolos constantes na Figura 2.23.

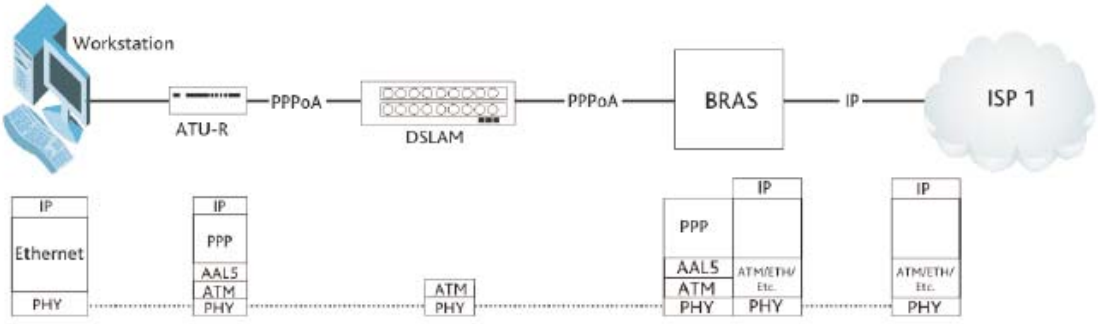

Figura 2.23: Pilhas de protocolos para o PPPoA (Fonte: [SPIRENT])

Informações detalhadas sobre o funcionamento do PPPoA podem ser obtidas em [RFC2364].

2.6.1.2 PPPoEoA (Point-to-Point Protocol over Ethernet over ATM)

Todo acesso ADSL que utiliza o protocolo PPPoE, quando conectado a um DSLAM cuja conexão com a rede seja feita utilizando tecnologia ATM é, por definição, um acesso PPPoEoA, visto que o protocolo PPPoE é re-encapsulado em células ATM para o transporte entre o DSLAM e o NAS. Esse fenômeno pode ser observado nas pilhas de protocolos representadas na Figura 2.24.

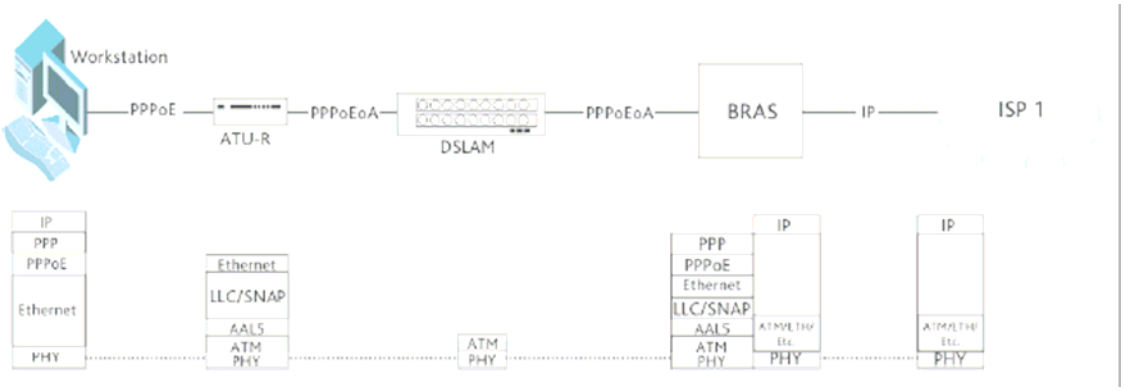

Figura 2.24: Pilhas de protocolos para o PPPoEoA (Fonte: [SPIRENT])

2.6.1.3 PPPoE (Point-to-Point Protocol over Ethernet)

O PPPoE é um protocolo definido por [RFC2516] para estabelecer e encapsular sessões ponto-a-ponto entre clientes e agregadores de tráfego de forma a transportá-las através de uma rede *Ethernet* real ou emulada. O principal apelo da utilização do PPPoE é possibilitar a utilização de recursos providos pelo PPP, tais como autenticação e controle de serviços por usuário, sobre redes *Ethernet*, que não são, por concepção, redes orientadas à conexão.

O PPPoE é composto de duas fases: descoberta e PPP. O estágio da descoberta é composto de quatro fases: inicialização, oferta, requisição e confirmação. Completadas estas quatro fases, o cliente e o BRAS conhecem o PPPoE SESSION_ID e seus respectivos endereços MAC e juntos estabelecem uma sessão PPPoE única.

- PADI (*PPPoE Active Discovery Initiation*)

Na fase de inicialização o cliente (*host*) que pode ser o micro-computador ou o modem ADSL, dependendo da configuração do modem envia um pacote PADI (*PPPoE Active Discovery Initiation*). Este pacote contém um TAG indicando o serviço que o host está requerindo e TAGs adicionais.

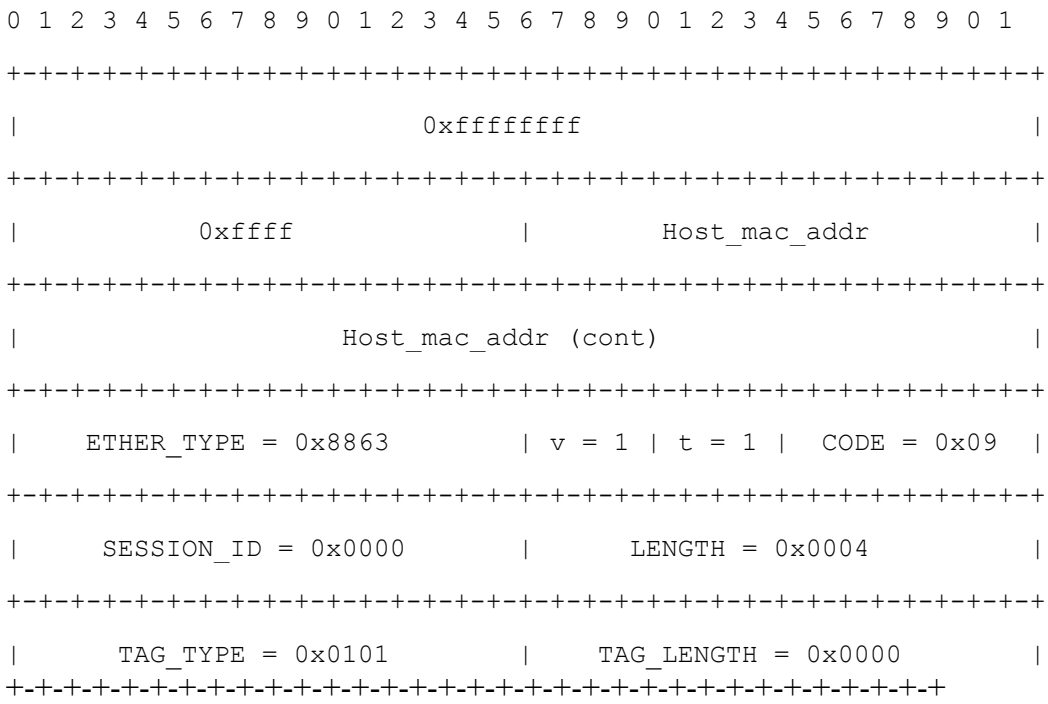

Figura 2.25: Formato de um pacote PADI [RFC2516]

- PADO (*PPPoE Active Discovery Offer*)

Quando um BRAS recebe um pacote do tipo PADI do *host* que ele pode servir, este envia um PADO. O PADO contém o nome do BRAS, um *service-name* TAG idêntico ao enviado pelo *host* no PADI e outros indicando outros serviços que o BRS oferece.

- PADR (*PPPoE Active Discovery Request)*

O *host* tendo recebido um pacote do tipo PADO envia ao BRAS um pacote do tipo PADR. Este pacote contém o endereço de destino do BRAS um TAG (*TAG_TYPE Service-Name*) indicando o serviço requerido pelo *host.*

- PADS (*PPPoE Active Discovery Session-Confirmation)*

Quando o BRAS recebe um pacote do tipo PADR este se inicia para iniciar a sessão PPP descrita na sessão anterior. É gerado um único SESSION_ID e é encaminhado ao host um pacote do tipo PADS. Este pacote contém um TAG indicando o serviço sob o qual o BRAS aceitou a sessão PPPoE e TAGs adicionais.

- PADT (*PPPoE Active Discovery Terminate)*

Este pacote pode ser enviado a qualquer tempo, tanto pelo host quanto pelo BRAS indicando o término da sessão PPPoE. A partir do recebimento de um pacote PADT nenhum envio de tráfego PPP é permitido utilizando esta sessão PPP.

- TAG_TYPES e TAG_VALES

No Apêndice A, da RFC2516, são definidos os tipos de TAGs existentes para uso. Para este trabalho o interesse está no uso da TAG x105 *Vendor Especific*. Nesta TAG são passadas informações proprietárias dos fabricantes (*vendors*) [RFC1700]. É neste atributo, do pacote PADI do protocolo PPPoE que está inserida a informação do DSLAM, *slot* e porta que permitirá o vínculo entre a identificação lógica da conexão e a informação física da porta permitindo o vínculo e conseqüentemente a identificação do cliente da operadora que originou a conexão [TR101].

2.6.2 Processo de autenticação, autorização e bilhetagem utilizando protocolo RADIUS (Remote Authentication Dial-in User Service)

Durante a fase LCP de estabelecimento de uma conexão PPP é realizada a etapa de autenticação. O RADIUS, protocolo amplamente utilizado atualmente para esta finalidade, surgiu da necessidade de se ter um método de autenticação, autorização e bilhetagem para usuários que necessitavam de acesso a recursos computacionais heterogêneos no Estado da Califórnia, nos Estados Unidos da América. O protocolo está padronizado através da [RFC2865] e da [RFC2866]. Segue descrição dos três processos utilizando o protocolo RADIUS, com base no trabalho desenvolvido por [GRUSZYNSKI, 2008].

2.6.2.1 O processo de autenticação RADIUS

Conforme [GRUSZYNSKI,2008], o tipo de autenticação existente nos serviços residenciais ADSL é uma autenticação do cliente, onde ele utiliza uma identificação de usuário e uma senha, que o autenticarão junto ao provedor de serviços Internet.

Quando um cliente adquire o serviço de um provedor de Internet ele registra, junto a esse provedor, um nome do usuário e uma senha. Ele utilizará este nome de usuário em

combinação com o domínio do seu provedor para formar uma identificação no formato nomedousuário@dominiodoprovedor.

O modelo de troca de mensagens de autenticação é o modelo envolvendo três partes: a identificação e a senha do cliente final são configuradas no modem ou no computador desse para estabelecer a conexão PPP.

Um pacote *Access-Request* (Solicitação de Acesso) é criado pelo cliente RADIUS (BRAS) com informações para esta autenticação. Quando o servidor de autenticação (*RADIUS*) da operadora recebe o *Access-Request* vindo do BRAS, este verifica o domínio e baseado num arquivo interno, este verifica a qual endereço IP o domínio se refere e então o envia pelo *backbone* IP da operadora até a Internet onde será alcançado o provedor e este fará o processo de verificação de *login* e senha do cliente e o autorizará ou não enviando ao *RADIUS* da operadora, respectivamente, o *Access-Accept* (autorização para utilização do serviço) ou o *Access-Reject* (negação para utilização do serviço).

Como fazer esta associação entre a conexão PPP e o cliente da operadora? A proposta é utilizar uma combinação entre alguns dos atributos constantes na requisição de acesso: o *NAS-Identifier* e o *NAS-Port-Id* para DSLAMs ATM; *NAS-Identifier* e *Cisco-AVPair* para DSLAMs Ethernet e BRAS CISCO; e *NAS-Identifier* e *Calling-Station-Id* para DSLAMs Ethernet e BRAS JUNIPER.

O *NAS-Identifier* é o atributo que contém o nome designado utilizado pelo BRAS para enviar a requisição de acesso. O atributo *NAS-Port-Id* é uma representação lógica da conexão ATM até a porta física do DSLAM ATM utilizada para iniciar a conexão PPP; corresponde à identificação do PVC (*Permanent Virtual Circuit*) ATM na interface do BRAS. Os atributos *Cisco-AVPair* e *Calling-Station-Id* são atributos encaminhados pelos BRAS CISCO e JUNIPER respectivamente, contendo a representação da porta física do DSLAM utilizada para iniciar a conexão PPP, para o caso de o usuário final estar conectado através de um DSLAM *Ethernet [CISCOb; JUNIPERa; JUNIPERb]*.

De posse da combinação dos atributos mencionados, presentes na mensagem de Requisição de Acesso (*Access-Request*), é possível consultar uma base de dados e recuperar a informação de qual cliente da operadora está vinculado à sessão PPP que está para iniciar.

2.6.2.2 O processo de autorização RADIUS

A consulta a uma base de dados utilizada para identificar o cliente da operadora pode servir para recuperar dados de autorização. Alguns exemplos de decisões de autorização são: se este cliente pode ter mais de uma sessão PPP no mesmo acesso, se deve receber um determinado endereço IP fixo, se o acesso deve ter algum tratamento diferenciado, ou, ainda, se a sessão deve ser bloqueada em decorrência de falta de pagamento.

2.6.2.3 O processo de bilhetagem RADIUS

A coleta de informações de consumo de acessos ADSL residenciais visa a atender a uma necessidade de serviços cujo faturamento é sensível ao uso, ou seja, o valor a ser cobrado do cliente final possui vínculo com a informação de quanto do serviço de conexão foi consumido ao longo de um ciclo de utilização. Para cada conexão estabelecida, um bilhete de autenticação RADIUS é gerado e armazenado em uma base de dados contendo todos os atributos RADIUS.

2.6.2.4 Atributos RADIUS

Os documentos [RFC2865] e [RFC2866] definem cerca de 40 diferentes tipos de atributos. Na Tabela 2.3 são apresentados alguns atributos que habitualmente estão presentes em sistemas ADSL.

Tabela 2.3: Alguns atributos RADIUS

Tipo	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*
11	*Filter-Id*
22	*Framed-Route*
25	*Class*
26	*Vendor-Specific*
27	*Session-Timeout*
28	*Idle-Timeout*
32	*NAS-Identifier*
61	*NAS-Port-Type*

O protocolo RADIUS permite também aos fabricantes de equipamentos criarem atributos para configurar ou habilitar recursos não padronizados em seus equipamentos: esses atributos são chamados de VSA (*Vendor-Specific Atribute*), ou de atributos específicos de um fabricante.

Para implementar um atributo específico, é utilizado o atributo padrão de número 26 (*Vendor-Specific*) da Tabela 2.3. O campo Valor do atributo é dividido em quatro subcampos: identificador, tipo, tamanho e valor, que, respectivamente, servem para identificar o fabricante, o número do atributo específico designado pelo fabricante, o tamanho total do VSA e o valor do atributo.

3 TECNOLOGIA ADSL NA OPERADORA PESQUISADA

Este capítulo tem por objetivo descrever de forma abrangente e detalhada a evolução do uso da tecnologia ADSL na operadora pesquisada, a arquitetura de Rede ADSL, principais topologias de acesso empregadas, as modalidades de serviço Banda Larga utilizando ADSL comercializadas e uma visão do processo de aprovisionamento e inventário de portas ADSL.

3.1 BREVE HISTÓRICO

A operadora em análise iniciou a instalação de equipamentos ADSL em 1999 nas cidades de Curitiba e Brasília. Os primeiros DSLAMs instalados na rede utilizavam utilizam protocolo ATM e eram de fabricação LUCENT. Os DSLAMs eram interconectados com o *backbone* ATM através de interfaces de 155Mbps e os switches ATM do fabricante CISCO. Estes switches, por sua vez, eram interconectados com equipamentos BRAS também CISCO. Os CPEs instalados nas residências dos clientes eram do fabricante CISCO e quando o serviço entrou em regime comercial os CPEs eram do fabricante 3COM, nos modelos (interno e externo, sendo os últimos do tipo modem *bridge* ou modem *router*). Os CPEs eram de propriedade da Brasil Telecom alugados aos clientes por um valor fixo mensal.

Em 2001, o serviço se expandiu para quase todas as capitais onde a operadora atua e DSLAMs do fabricante ALCATEL foram instalados em vários estados. A operadora criou novas modalidades de serviço e passou a oferecer a possibilidade de compra do CPE pelo cliente.

Durante todo este período a instalação do serviço era precedida de uma qualificação de linha devido às limitações de distância entre o DSLAM e o CPE, inerentes a tecnologia ADSL e já citadas no capítulo 2.

Em 2002 após aprimoramento da identificação das áreas onde era possível a comercialização do serviço e também com os esforços para tornar a configuração do CPE mais fácil e semi-automática, a operadora passou a adotar o modelo de auto-instalação.

Em 2003 devido ao avanço tecnológico, redução dos custos e congelamento das Redes ATM foram adquiridos e instalados os primeiros DSLAMs Ethernet que se conectavam aos switches Ethernet via fibra ou utilizavam conversores *Fast-Ethernet* para E1 utilizando a rede de transporte SDH (*Synchronous Digital Hierarchy*) para se conectar aos *switches*. Mais a frente placas *Fast-ethernet* foram adquiridas nos equipamentos SDH possibilitando a conexão sem o uso de conversores.

Atualmente todos os novos DSLAMs utilizam protocolo Ethernet e gradativamente os DSLAMs ATM estão sendo substituídos.

Durante este ínterim foram adquiridos os primeiros BRAS da Juniper (ERX) [JUNIPERb] e em seguida começou a substituição de agregadores CISCO modelo 6400 por equipamentos Juniper modelo ERX ou CISCO da família 10000 [CISCOb].

Juntamente com os Agregadores da Juniper, foi adquirida uma solução de portal cativo (*captive portal*) para permitir o lançamento do serviço Turbo, nome comercial para o serviço de acesso a internet utilizando acesso ADSL da operadora, na modalidade *Lite*. Esta modalidade previa a cobrança de uma tarifa fixa mensal adicionada de um valor por Megabyte de *download* realizado no mês. Esta solução de portal acarretou uma mudança cultural nas clientes visto que uma segunda autenticação se fazia necessária. O portal foi implantado em meados de 2004 e além do aspecto cultural citado acima, mostrou-se extremamente instável e não escalável resultando na decisão de suspendê-lo em meados de 2005.

Neste terceiro trimestre de 2008 uma nova topologia de rede de transporte será experimentada com o entroncamento dos DSLAMs na rede Metro-Ethernet que a operadora iniciou ativação em 2007 e continua ao longo deste ano.

3.2 PLANTA ATUAL

Atualmente a operadora possui uma planta de 2,3 milhões de portas em Acesso Banda Larga do tipo ADSL, ADSL2 e ADSL2+. Deste total de portas 80% estão comercializadas.

Na planta da Brasil Telecom estão instalados e em funcionamento DSLAMs de sete fabricantes, divididos conforme as Tabelas 3.1 e 3.2:

- DSLAM ATM

Tabela 3.1: Quantidade de DSLAMs ATM e quantidade de portas

FABRICANTE	MODELO	TOTAL DSLAMs	TOTAL PORTAS
ALCATEL	7300 ASAM	926	178.254
CISCO	6120	109	12.984
INOVIA		88	17.403
LUCENT	STINGER	644	440.581
HUAWEI	MA 5100, MA5103 e MA5105	2.726	459.270
TOTAL		**4.493**	**1.108.492**

- DSLAM Ethernet

Tabela 3.2: Quantidade de DSLAMs Ethernet e quantidade de portas

FABRICANTE	MODELO	TOTAL DSLAMs	TOTAL PORTAS
HUAWEI	MA5100, MA5300 e MA5600	1.824	514.151
ERICSSON	HM 130	462	89.297
UTSTARCOM	B820 e B1000	1.955	494.592
SIEMENS	HiX5635	263	102.484
TOTAL		**4.504**	**1.200.524**

Na planta, estão instalados e em funcionamento Agregadores de dois fabricantes, apresentados na Tabela 3.3:

Tabela 3.3 Quantidade de BRASs e quantidade de portas

FABRICANTE	MODELO	TOTAL BRASs	TOTAL PORTAS
CISCO	10008	43	1.579.127
JUNIPER	ERX	19	729.889
TOTAL		**62**	**2.309.016**

3.3 ARQUITETURA DA REDE ADSL DA OPERADORA PESQUISADA

Neste item iremos descrever as características da arquitetura da rede ADSL. Um diagrama de rede pode ser visto na Figura 3.1.

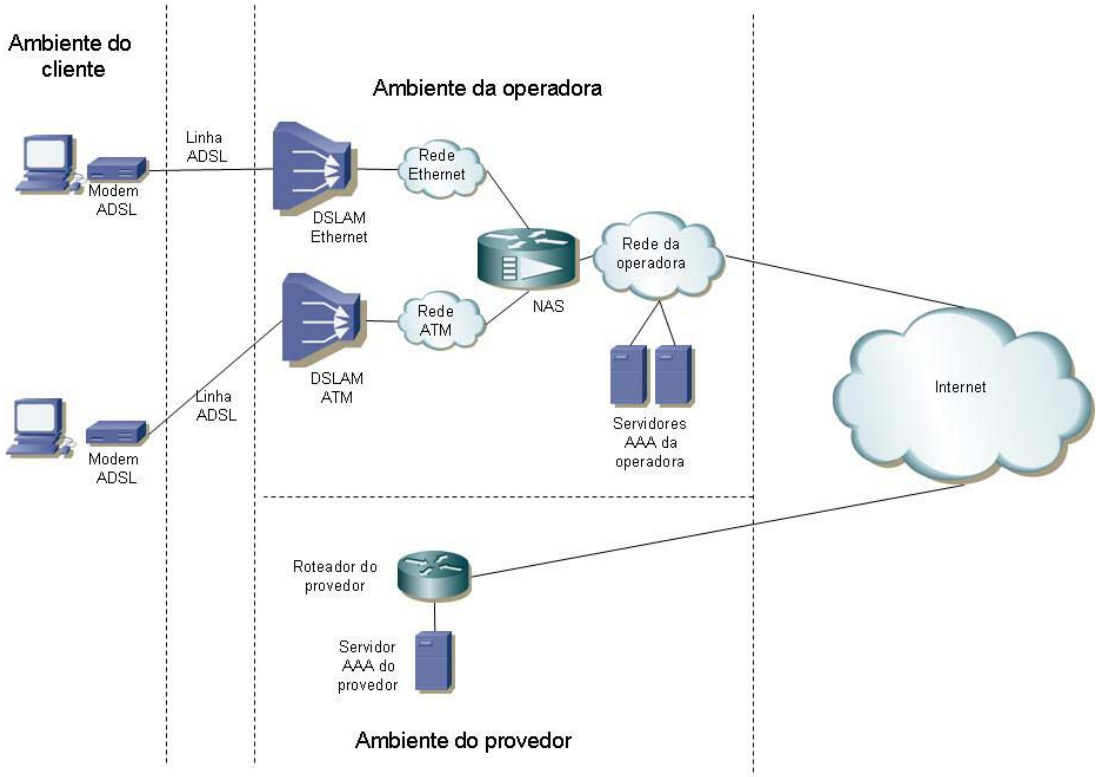

Figura 3.1: Arquitetura da Rede ADSL da operadora analisada. (Fonte: [GRUSZYNSKI, 2008])

Como já citado anteriormente, a rede de acesso ADSL da Brasil Telecom é constituída tanto de DSLAMs ATM quanto de DSLAMs Ethernet. Os DSLAMs ATM são entroncados nos switches de agregação através de interfaces de 2Mbps, 34Mbps ou 155Mbps dependendo da quantidade de DSLAMs e quantidade de portas que estão interconectadas nesta interface. Tanto em DSLAMs ATM quanto Ethernet, o nível de cascata é bastante significativo. Algumas variações de topologia, bem como, cascateamento, podem ser visualizadas nas figuras abaixo.

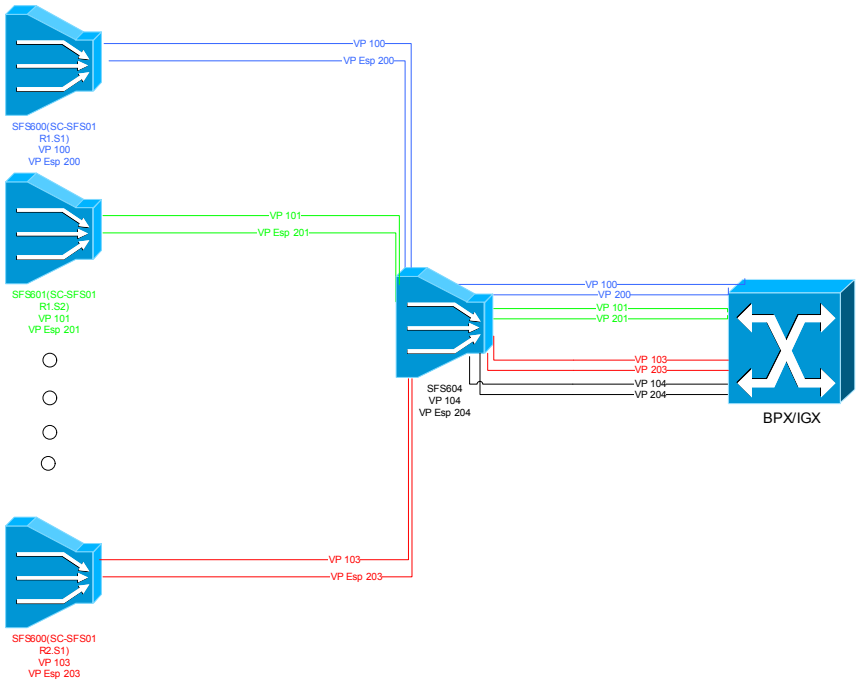

Figura 3.2: n DSLAMs cascateados num DSLAM concentrador

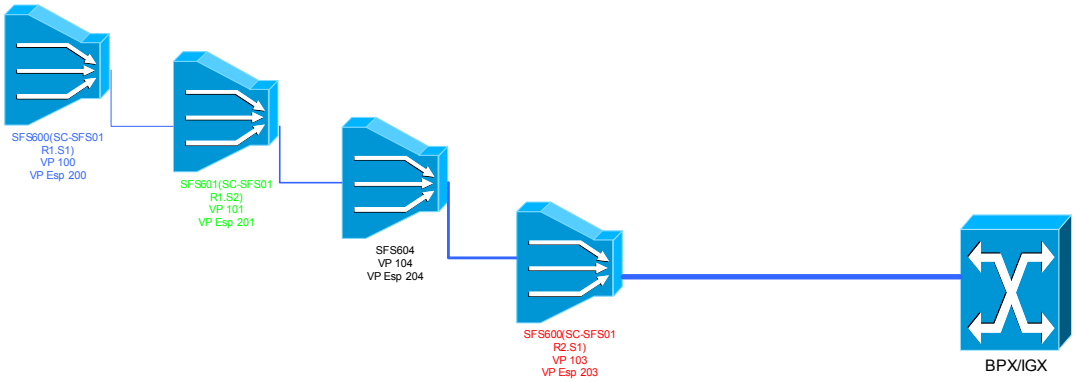

Figura 3.3: n DSLAMs cascateados um após outro formando quatro níveis de cascata

O cascateamento de DSLAMs, apesar de otimizar recursos traz alguns impactos operacionais dificultando o *trouble-shooting* em casos de falha.

Além disto, o número de fabricantes e modelos de DSLAMs também é muito elevado. Dentro de uma mesma cascata, é normal existir DSLAMs de fabricantes diferentes. Do ponto de vista de Operação e Manutenção envolvendo treinamento da equipe, necessidade de sobressalentes (*spare parts*) de cada fabricante e modelo esta não é uma situação desejável. Esta situação tornou a análise da implementação técnica bastante trabalhosa, pois foi necessário identificar os modelos de informação DSLAM, *slot* e porta em cada cenário.

Para DSLAMs ATM, a operadora adota configuração de VP *Switching* (comutação de *Virtual Path*) sendo configurado entre o DSLAM e o BRAS um VP para cada DSLAM e um VC para cada porta física. Entretanto, esta regra nem sempre é respeitada chegando a casos extremos de num mesmo *slot*, parte das portas com um VP terminando num BRAS e parte das portas com outro VP terminando no mesmo ou em outro BRAS, conforme Figura 3.4.

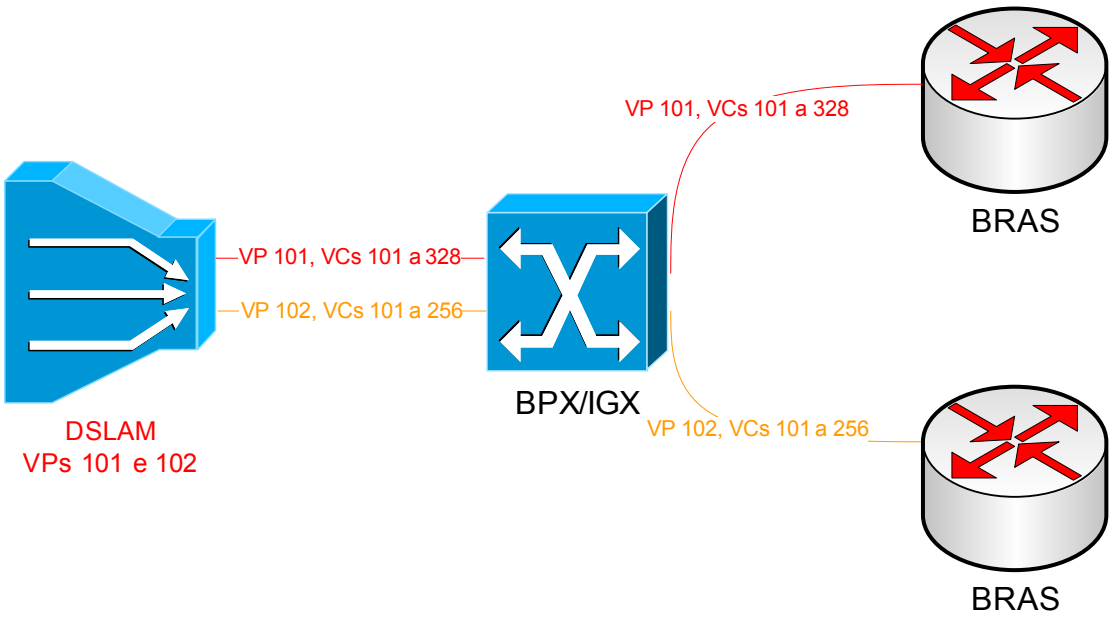

Figura *3.4: um DSLAM com dois VPs configurados terminando em BRAS distintos.*

Para DSLAMs Ethernet, a operadora adota a configuração de duas VLANs por DSLAM (ver Figura 3.5) sendo a primeira para transportar logicamente o serviço na modalidade residencial e a segunda para transportar o serviço na modalidade empresarial. Da forma como é aprovisionado, a distinção do tráfego e por conseqüência dos bilhetes de autenticação dentro de uma mesma VLAN só é possível através do *MAC Address* e implica necessariamente do cliente estar conectado no momento da pesquisa. Esta situação torna o trabalho de identificação dos clientes trabalhosa e demorada, sendo este um dos principais motivadores para este trabalho de dissertação.

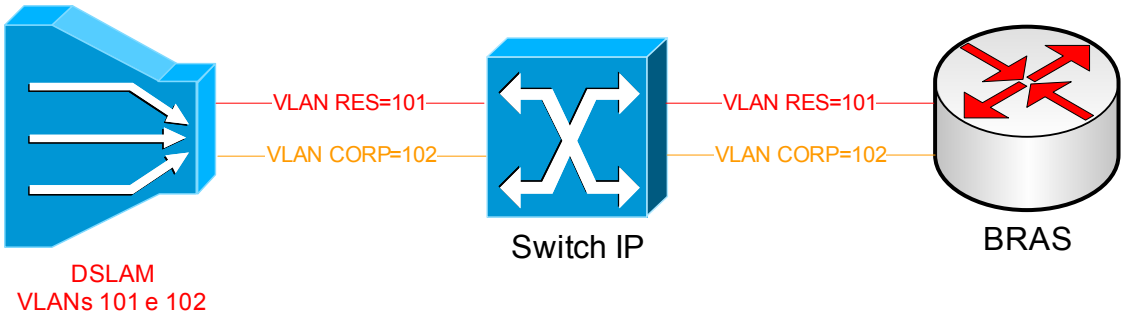

Figura 3.5: DSLAM Ethernet com configuração típica - 2 VLANs configuradas

A situação vivenciada ao longo da elaboração deste trabalho foi a constatação de DSLAMs de mesmo fabricante e modelo, porém com várias versões de *software*. Para permitir a padronização da rede e simplificação da implementação técnica sugerida nesta dissertação está em andamento a execução de janelas de manutenção para substituição de todas as versões de *software* existentes pela última versão disponível e esta versão foi objeto de testes de implementação do PPPoE TAG.

Além do objetivo principal deste trabalho de estabelecer o vínculo físico e lógico dos acessos em banda larga utilizando rede ADSL, foi possível: inventário completo de DSLAMs e portas, identificação e homogeneização das versões de *software* em uso na operadora, inserção de DSLAMs que não estavam cadastrados na gerência.

Com relação aos equipamentos BRAS também foi necessário substituir a versão de *software* existentes por versões que suportassem o PPPoE TAG.

3.4 MODALIDADE DE SERVIÇOS

Neste item propõe-se apresentar o portfólio de produtos Banda Larga da Brasil Telecom utilizando acessos ADSL. A operadora comercializa atualmente três modalidades de serviço utilizando tecnologia ADSL: Turbo Residencial, IP Profissional e IP Turbo. Apesar de apresentar variações que atendem segmentos de clientes distintos, as modalidades são muito limitadas no que diz respeito ao perfil de uso dos clientes, ou seja, não são capazes de nenhuma distinção na camada de aplicação. É visível a demanda por serviços cada vez mais personalizados e para que as operadoras possam atender as necessidades dos clientes a implementação técnica proposta neste trabalho é premissa básica.

3.4.1 Turbo Residencial

Turbo Residencial é um serviço de telecomunicações que disponibiliza no ambiente do cliente acesso rápido à Internet, com velocidades de 256kbps a 8Mbps, através do uso de modems ADSL/ADSL2+. Através deste serviço o cliente tem duas comunicações simultâneas, ou seja, conexão de voz convencional e conexão à Internet simultaneamente.

Algumas características básicas do Internet Turbo ADSL:

- Necessidade de um Provedor de acesso a Internet;
- Necessita de uma linha telefônica da Brasil Telecom;
- Permite formação de rede interna com até 03 equipamentos (LAN);
- Endereçamento DHCP (*Dynamic Host Configuration Protocol*);
- IP Dinâmico;

O Turbo Residencial foi desenvolvido para suprir todas as necessidades do seu público alvo, sendo o foco principal o acesso rápido à Internet, considerando a utilização de navegação HTTP como objetivo.

Não estão previstas algumas aplicações nesta modalidade de serviço, tais como:

- *Telnet* entrante;
- *FTP* entrante;
- *HTTP* entrante;
- *Web Server*;
- *Mail Server*;
- *FTP Server*;

O controle sobre os serviços disponíveis ou não, é feito via lista de acesso configurada nos agregadores.

Além disso, outra característica importante do serviço é a atribuição de endereço IP, que neste caso se caracteriza por ser dinâmico e atribuído pelo Agregador, como um DHCP.

3.4.2 IP Profissional

IP Profissional também conhecido com Turbo Empresas é um serviço que disponibiliza no ambiente do cliente acesso rápido à Internet, com velocidades de 256kbps até 8Mbps, através do uso de modems ADSL. Através deste serviço o cliente tem duas comunicações simultâneas, ou seja, conexão de voz convencional e conexão à Internet, característico da tecnologia.

Características básicas do IP Profissional:

- Necessita de uma linha telefônica da operadora;
- Permite ilimitado número de sessões simultâneas;

- Permite formação de rede interna com até 20 equipamentos (LAN);
- Endereçamento IP atribuído às credenciais de usuário e senha, fornecidos pela base LDAP (*Lightweight Directory Access Protocol*), que na Brasil Telecom é a plataforma da Novell denominada *eDirectory*, onde são criadas e armazenadas as contas dos clientes IP Profissional da Brasil Telecom;

Os serviços adicionais que podem ser utilizados são:

- Formação de Redes Privativas Virtuais (VPN);
- *Firewall* (serviço adicional);
- *Telnet*;
- FTP entrante;
- HTTP entrante;
- *Web Server* (serviço adicional);
- *Mail Server* (serviço adicional);
- *FTP Server* (serviço adicional);
- Vídeo conferência (serviço adicional);

Estes serviços adicionais dependerão exclusivamente do *software* do cliente.

O controle de liberação de serviços é também feito via lista de acesso.

Entretanto, uma das características mais importantes é quanto à atribuição de endereço IP, que neste caso são IPs fixos por cliente e não mais atribuído pelo Agregador.

3.4.3 IP Turbo

Categoria de serviço que usa o serviço IP Profissional para simular um IP dedicado e, portanto tem todas as funcionalidades deste, porém, no IP Turbo o cliente recebe um bloco de oito endereços IPs fixos e válidos além do endereço de autenticação.

Algumas características básicas:

- A rota com os oito IPs cedidos aos clientes é passada ao servidor RADIUS nos atributos contidos na mensagem de Acesso Permitido, com base, nas informações recuperadas da base LDAP;
- Custo bem mais baixo que um IP dedicado;

A lista de acesso para este serviço é a mesma do IP Profissional

3.4 PROCESSO DE AUTENTICAÇÃO, AUTORIZAÇÃO E BILHETAGEM (AAA) DA OPERADORA

Será descrito neste item a topologia e formas de autenticação empregadas na operadora em discussão.

3.4.1 Processo de Autenticação por Proxy

Devido à regulamentação da ANATEL (órgão regulador de Telecomunicações do Brasil) [REGSCM], as operadoras com concessão para prestar serviços de telecomunicações (Brasil Telecom, Oi, Telefônica, Embratel), estão impossibilitadas de efetuar a autenticação dos usuários. Esta atribuição de autenticação é desempenhada pelos Provedores de Serviço Internet (ISP). Desta forma, cada usuário banda larga precisa contratar o acesso Banda Larga das empresas que possuem concessão, permissão ou autorização da ANATEL e um Provedor de Serviços de Internet (ISP) para o processo de autenticação validando ou não suas credenciais de usuário e senha.

Atualmente, as Operadoras e os Provedores de Acesso a Internet utilizam o protocolo RADIUS que é o padrão da indústria para AAA (*Authentication, Accounting e Authorization*). O protocolo RADIUS já foi apresentado no capítulo anterior.

Na figura 3.6 segue a seqüência do processo de autenticação desde a origem, que pode ser o microcomputador do cliente ou o CPE, dependendo da forma de configuração do modem (*bridge* ou *router*) até a chegada no Servidor RADIUS do Provedor e posteriormente seu retorno.

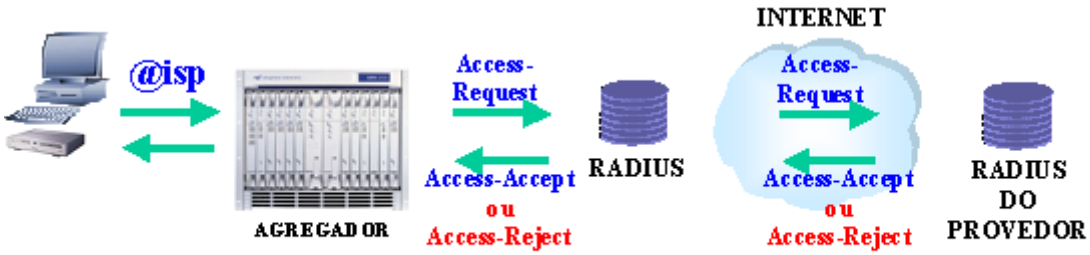

Figura 3.6: Processo de Autenticação do Serviço ADSL na operadora pesquisada

Outra abordagem para representar o processo de autenticação é exibida na figura 3.7, onde estão representados os agregadores e os servidores de autenticação da operadora e dos Provedores. Atualmente mais de 200 Provedores de Acesso Internet são conveniados.

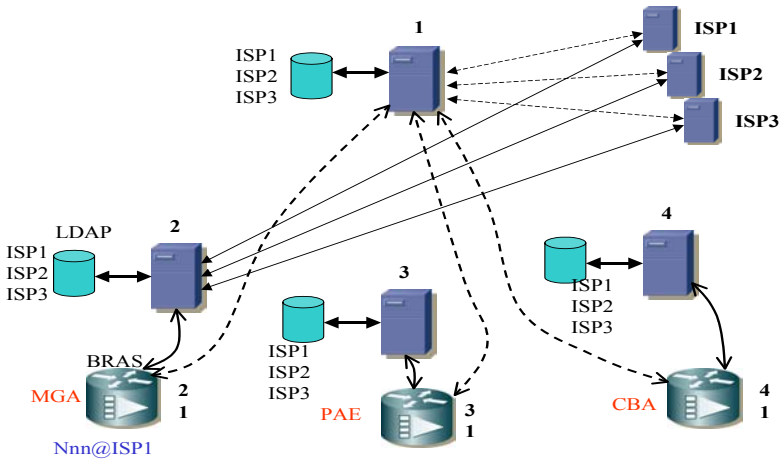

Figura 3.7: Representação simplificada da topologia de rede e processo de autenticação.

Com base na Figura 3.7 vamos descrever o processo de autenticação de um cliente com *username* **Nnn** e cujo Provedor é denominado **ISP1**.

Supondo um cliente Nnn@ISP1 de Maringá (MGA), queira realizar o *login* na rede ADSL, tendo contratado os serviços do provedor "ISP1". Para isso o BRAS, onde termina este cliente, consulta uma tabela interna, pré-configurada, dos servidores de autenticação disponíveis (no caso **2** e **1**) seguindo a ordem de prioridade configurada e solicita a autenticação do cliente ao servidor **2** (que é o 1.o da lista de prioridades).

O servidor **2** direciona a requisição do cliente para o servidor de autenticação do "ISP1" e requisita para o referido provedor "ISP1" a autenticação do cliente "Nnn", servindo de *proxy* entre o cliente e o provedor.

No caso de falha do servidor **2**, o BRAS utiliza a segunda opção de servidores, que no caso seria o servidor **1**, que passaria a ser consultado em substituição ao servidor **2**, garantindo assim a alta disponibilidade no caso de falha do servidor regional.

Para as outras regiões o sistema é similar, com a regionalização demonstrada na figura 3.6 com servidores em Curitiba, Porto Alegre e Brasília.

3.4.2 Processo de Autenticação Local

O processo de autenticação local é utilizado para serviços em Banda Larga, enquadrados no segmento Empresarial/corporativo denominados: IP Turbo e IP Profissional, apresentado na Figura 3.8

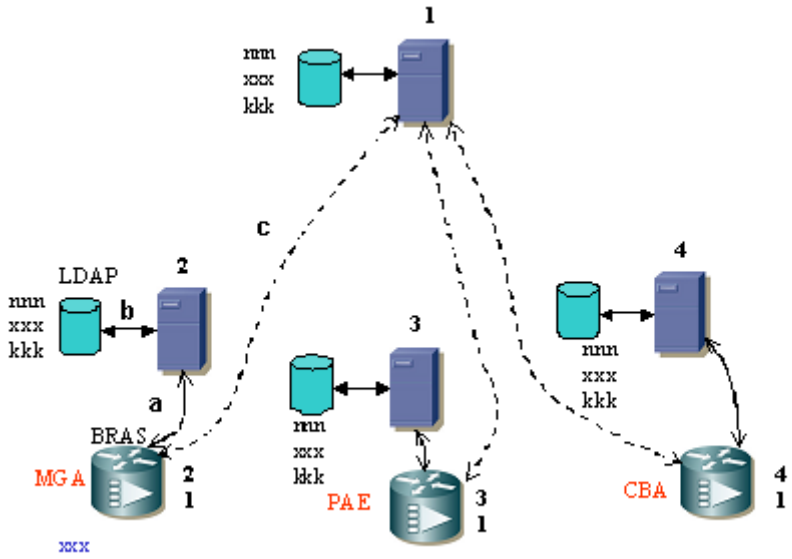

Figura 3.8: Representação simplificada da topologia de rede e processo de autenticação local.

Supondo um cliente "xxx" de Maringá (MGA) realizando o *login* na rede para utilizar um serviço IP Turbo cuja autenticação por um provedor não é requerida. Para isso, o BRAS onde termina este cliente, consulta uma tabela interna pré-configurada dos servidores de autenticação disponíveis (no caso **2** e **1**) seguindo a ordem de prioridade e solicita a autenticação do cliente ao servidor **2** (que é o 1.o da lista de prioridades) (caminho a).

O servidor **2** consulta a base de dados LDAP local para obter os parâmetros associados ao perfil do cliente e realiza a autenticação do cliente "xxx" (caminho b).

No caso de falha do servidor **2**, ou do LDAP a ele associado, o BRAS utiliza a segunda opção de servidores, que no caso seria o servidor **1**, que passaria a ser consultado em substituição ao servidor **2**, garantindo assim a alta disponibilidade no caso de falha do servidor regional (caminho c).

3.4.3 Processo de Bilhetagem

O processo de bilhetagem será executado para todos os serviços, independentemente do tipo de cobrança a que está sujeito. Os pacotes com as informações para bilhetagem são enviados pelo BRAS ao servidor de autenticação que executou a autenticação do usuário. Este servidor irá encaminhar os bilhetes a um dos servidores de Bilhetagem (**A** ou **B**) da Brasil Telecom e também ao sistema de bilhetagem do provedor onde o usuário foi autenticado, se for o caso. Na Figura 3.9 é apresentado o diagrama desta arquitetura.

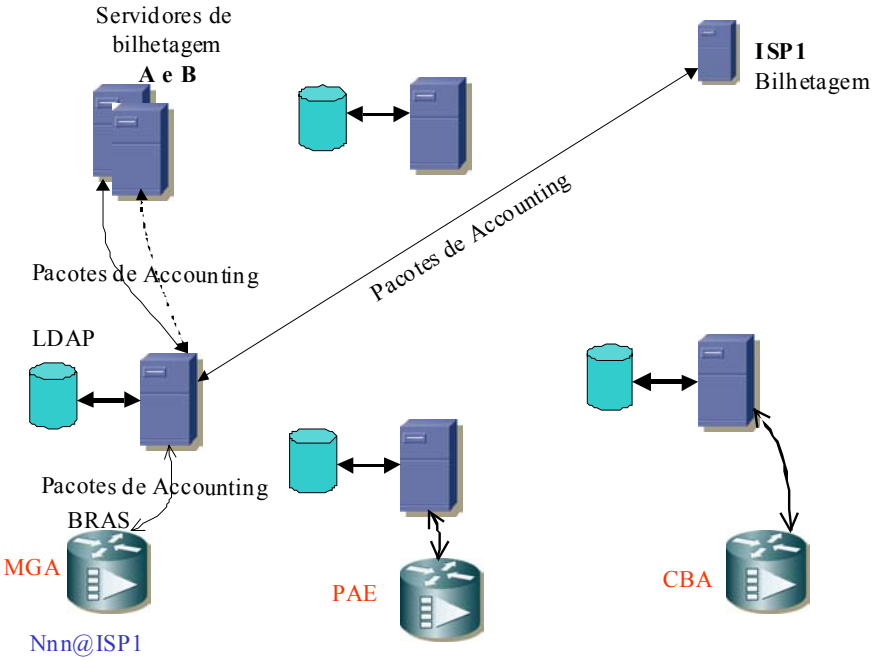

Figura 3.9 – Topologia de Rede simplificada e o processo de bilhetagem

3.4.4 Parâmetros do bilhete de autenticação RADIUS

Os parâmetros de um bilhete de autenticação RADIUS são apresentados, quando a origem é um Agregador Cisco nas Figuras 3.10 e 3.11 e quando a origem é um Agregador Juniper as Figuras 3.12. e 3.13.

Bilhete START CISCO 10K - DSLAM ATM	
Acct-Session-Id	"7/0/0/140.167_00B3D857"
Cisco-AVPair	"client-mac-address 000f.3dfd.1c83"
Framed-Protocol	PPP
Framed-IP-Address	201.35.217.160
User-Name	"flaviopegoraro@terra.com.br"
Ascend-Connect-Progress	LAN-session-is-up
Cisco-AVPair	"connect-progress LAN Ses Up"
Acct-Authentic	RADIUS
Acct-Status-Type	Start
NAS-Port-Type	Virtual
NAS-Port	1888223399
NAS-Port-Id	"7/0/0/140.167"
Connect-Info	"PPPoE"
Class	"PAENRAS01_SC_OK_DEF_CLF"
Service-Type	Framed-User
NAS-IP-Address	201.14.143.254
Acct-Delay-Time	0

Figura 3.10: Bilhete de Autenticação RADIUS considerando DSLAM ATM e BRAS Cisco 10K

Bilhete START CISCO 10K - DSLAM ETH	
Acct-Session-Id	"1/1/0/1110_0000985B"
Cisco-AVPair	"client-mac-address 0013.468d.a727"
Framed-Protocol	PPP
Framed-IP-Address	201.35.255.107
User-Name	"primor@ps5.com.br"
Ascend-Connect-Progress	LAN-session-is-up
Cisco-AVPair	"connect-progress LAN Ses Up"
Acct-Authentic	RADIUS
Acct-Status-Type	Start
NAS-Port-Type	Ethernet
NAS-Port	402654294
NAS-Port-Id	"1/1/0/1110"
Class	"PAENRAS01_SC_OK_DEF_CLF"
Service-Type	Framed-User
NAS-IP-Address	201.35.252.254
Acct-Delay-Time	0

Figura 3.11: Bilhete de Autenticação RADIUS considerando DSLAM Ethernet e Agregador Cisco 10K sem o PPPoE TAG habilitado

Bilhete START JUNIPER ERX - DSLAM ATM	
Acct-Status-Type	Start
User-Name	"cspconpa@terra.com.br"
Event-Timestamp	1149750000
Acct-Delay-Time	0
NAS-Identifier	"PAEMT706"
Acct-Session-Id	"erx atm 4/0.100154:100.154:016273
NAS-IP-Address	200.180.128.227
Class	"PAENRAS01_RS_OK_DEF_CLF"
Service-Type	Framed-User
Framed-Protocol	PPP
Framed-Compression	None
Framed-IP-Address	200.180.177.5
Framed-IP-Netmask	255.255.255.255
Calling-Station-Id	"#PAEMT706#ERX<> PAEMET501 5
Connect-Info	"speed:UBR"
NAS-Port-Type	xDSL
NAS-Port	1080295578
NAS-Port-Id	"atm 4/0.100154:100.154"
Acct-Authentic	RADIUS

Figura 3.12: Bilhete de Autenticação RADIUS considerando DSLAM ATM e Agregador Juniper sem PPPoE habilitado

Bilhete START JUNIPER ERX - DSLAM ETH	
Acct-Status-Type	Start
User-Name	"aninha19687@superig.com.br"
Event-Timestamp	1149750003
Acct-Delay-Time	0
NAS-Identifier	"CTAME706"
Acct-Session-Id	"erx gigabitEthernet 8/0.2620:2620:0183977921"
NAS-IP-Address	200.101.129.33
Class	"CTANRAS01_PR_OK_DEF_CLF"
Service-Type	Framed-User
Framed-Protocol	PPP
Framed-Compression	None
Unisphere-PPPoE-Description	"pppoe 00:13:a3:53:16:31"
Framed-IP-Address	200.103.145.14
Framed-IP-Netmask	255.255.255.255
Calling-Station-Id	"#CTAME706#E80#2620"
NAS-Port-Type	Ethernet
NAS-Port	2147486268
NAS-Port-Id	"gigabitEthernet 8/0.2620:2620"
Acct-Authentic	RADIUS

Figura 3.13: Bilhete de Autenticação RADIUS considerando DSLAM Ethernet e Agregador Juniper sem PPPoE TAG habilitado

É neste ponto específico da autenticação que entraremos com mais detalhes nos próximos capítulos, pois a contribuição desta dissertação de mestrado está na implementação técnica e adequação das Redes Banda Larga das Operadoras para o enriquecimento de informações nos bilhetes de autenticação possibilitando o vínculo entre o acesso físico e lógico ADSL.

3.5 PROCESSO DE VERIFICAÇÃO DE DISPONIBILIDADE E INSTALAÇÃO DO SERVIÇO

Neste item será descrito o processo de verificação de disponibilidade de porta:

- Índices chaves:
  - O terminal telefônico do cliente determina a estação e o armário de distribuição que atendem o cliente;
  - Velocidade que o cliente deseja:
    - ✓ até 1,5Mbps pode ser ADSL;
    - ✓ entre 2 e 8Mbps somente portas marcadas no inventário com tecnologia: ADSL2+
  - modalidade de serviço:
    - ✓ Turbo
    - ✓ IP Profissional
    - ✓ IP Turbo

No cruzamento do sistema de CRM (*Customer Relationship Management*) e o sistema de inventário de ADSL pode ser respondido:

- Viável

- Inviável – sem porta disponível

- Inviável – rede não apta. Esta resposta significa que à distância entre o cliente e a estação telefônica onde está instalado o DSLAM é maior que a permitida para prestação do serviço com qualidade. Na operadora pesquisada considera-se prestação de serviço com qualidade quando a atenuação upload e download é menor que 55dBs e a relação sinal ruído upload e download é maior que 15dBs.

4 SOLUÇÃO TÉCNICA PROPOSTA E PROCESSOS ASSOCIADOS

Este capítulo se destina a descrever as possibilidades pesquisadas para solucionar a problemática da falta de vínculo entre a identificação física da porta onde o cliente ADSL está conectado e a informação lógica dos bilhetes de autenticação, do ponto de vista técnico e de processos. Foram estudadas quatro formas de solução do problema, as quais são apresentadas e comparadas entre si, justificando-se a adoção de uma das técnicas.

A solução técnica proposta é detalhada e as fases para implementação da solução numa empresa de Telecomunicações são apresentadas.

Ainda neste capítulo, serão descritos os benefícios esperados com esta solução técnica.

4.1 SOLUÇÕES TÉCNICAS POSSÍVEIS

Neste item estão descritas quatro possíveis soluções para solucionar o problema. As quatro soluções foram assim denominadas:

- Vinculação do usuário e senha com porta física do DSLAM;
- Vinculação do endereço MAC com porta física do DSLAM;
- Dupla autenticação
- Inserção da porta física do DSLAM no bilhete de autenticação RADIUS.

4.1.1 Vinculação do usuário e senha com porta física do DSLAM

Uma das possíveis formas de vinculação física e lógica seria armazenar no sistema de inventário de portas ADSL ou numa nova base de dados às informações de porta física do DSLAM, contrato do terminal telefônico do cliente, usuário e senha de autenticação do cliente junto ao Provedor de Acesso Internet.

A fragilidade deste método reside na impossibilidade legal da Operadora de Telecomunicações de efetuar a autenticação. Desta forma, qualquer usuário do serviço Banda Larga pode trocar seu usuário e/ou senha junto aos Provedores de Internet, ou até mesmo trocar de provedor, que o serviço continuará funcionando e a Operadora perde a possibilidade de vínculo.

As Operadoras, para permitir a venda do serviço Banda Larga ao maior número de clientes possível, faz parcerias e credencia um número elevado de provedores. Por sua vez, não existe nenhuma exigência legal do Provedor de Internet informar as credencias de usuário e senha de qualquer um dos seus clientes, inclusive sendo esta uma informação confidencial. Por todos estes motivos, esta alternativa está descartada. Outro forte agravante é que a atualização da base de dados deveria ser realizada em tempo real porque enquanto a atualização não é processada, bilhetes de autenticação não terão o vínculo com o cadastro físico da Operadora.

4.1.2 Vinculação do endereço MAC com porta física do DSLAM

Outra forma possível de vinculação física e lógica seria armazenar no inventário de portas ADSL ou numa nova base de dados às informações de porta física do DSLAM, contrato do terminal telefônico do cliente e o Endereço MAC (*MAC Address)* do equipamento do cliente utilizado para originar a solicitação da requisição de autenticação.

O endereço MAC é o endereço físico da estação, ou melhor, da interface de rede. É um endereço de 48 bits, representado em hexadecimal. O protocolo é responsável pelo controle de acesso de cada estação à rede Ethernet utilizado na camada 2 (Enlace) do Modelo OSI (*Open Systems Interconnection*). Os três primeiros octetos são destinados à identificação do fabricante, os três posteriores são fornecidos pelo fabricante. É um endereço único, i.e., não existem, em todo o mundo, duas placas com o mesmo endereço.

A fragilidade deste método reside no fato de que o serviço não deixará de funcionar se o cliente trocar de modem ou microcomputador e não comunicar a Operadora. Uma

mudança de configuração do modem do modo *bridge* para *router* e vice-versa também quebraria o vínculo.

Operacionalmente este método também é muito complexo porque o cliente desconhece a informação do endereço MAC. Relembrando conforme descrito no capítulo 2, se o cliente utiliza um modem em modo *router*, a conexão PPP é estabelecida entre o modem e o BRAS e, conseqüentemente, o Endereço MAC informado no bilhete de autenticação será o do próprio modem. Se o cliente estiver utilizando uma conexão de Internet com modem em modo *bridge*, o Endereço MAC será o do microcomputador onde está instalado o *software* de estabelecimento da conexão, também conhecido como discador. Da mesma forma que a solução anterior, a atualização da base de dados deve ser realizada em tempo real porque enquanto a atualização não é processada, bilhetes de autenticação não terão o vínculo com o cadastro físico da operadora.

4.1.3 Dupla autenticação

No passado, devido o lançamento de uma modalidade denominada Turbo Lite, a Brasil Telecom implantou uma solução de portal cativo (*captive portal*) adquirindo uma plataforma SDX da Juniper Networks e servidores LDAP para armazenamento de um usuário e senha definido pela operadora. Neste processo, após a autenticação do Provedor de Internet, o cliente é direcionado a uma página da operadora, denominada Portal, onde era solicitado um segundo usuário e senha. Somente após esta segunda autenticação o cliente tinha o serviço liberado. Além de não ser escalável, esta solução se mostrou muito ruim do ponto de vista da experiência do cliente. O nível de insatisfação por necessitar de uma segunda autenticação era elevado. Por exemplo, para um cliente acessar seus e-mails num *software* de e-mail, por exemplo: *Outlook*, era necessário primeiramente abrir um *browser*, digitar o *login* e senha da operadora e somente após esta segunda autenticação o cliente passava a ter acesso a novas mensagens na sua caixa de correio.

Pelos motivos acima descritos esta implementação técnica também não é uma abordagem recomendada.

4.1.4 Inserção da porta física do DSLAM no bilhete de autenticação RADIUS

Para explicar a forma de inserção da porta física do DSLAM no bilhete de autenticação RADIUS é necessário separar os dois diferentes tipos de DSLAM: ATM e Ethernet.

4.1.4.1 DSLAM ATM

Inicialmente será abordada a forma de implementação da configuração lógica dos PVCs no *backbone* de Dados. Independente de um DSLAM estar diretamente ligado num switch ATM ou fazer parte de uma cascata de DSLAMs, cada DSLAM terá um ou mais *Virtual Paths* (VPs) de saída, sendo na maioria das vezes um VP. Este VP chega até o Switch ATM e do Switch ATM até o BRAS ocorre invariavelmente uma comutação do VP, chegando ao destino (BRAS) com um VP diferente daquele que foi configurado na saída do DSLAM. Já o *Virtual Circuit* (VC) é geralmente padronizado com o fabricante e modelo do DSLAM, mas independente desta facilidade, este VC de cada porta é o mesmo desde a saída do DSLAM até a entrada no BRAS. Esta informação é importante quando for detalhado mais à frente, o desenvolvimento de uma rotina de varredura e obtenção do VC de 1.108.492 portas de DSLAM ATM em funcionamento na operadora pesquisada. Para a obtenção do(s) VP(s) dos 4.493 DSLAMs ATM foi necessário levantamento em cada um dos Agregadores e suas respectivas interfaces e subinterfaces, conforme apresentado na Figura 4.1.

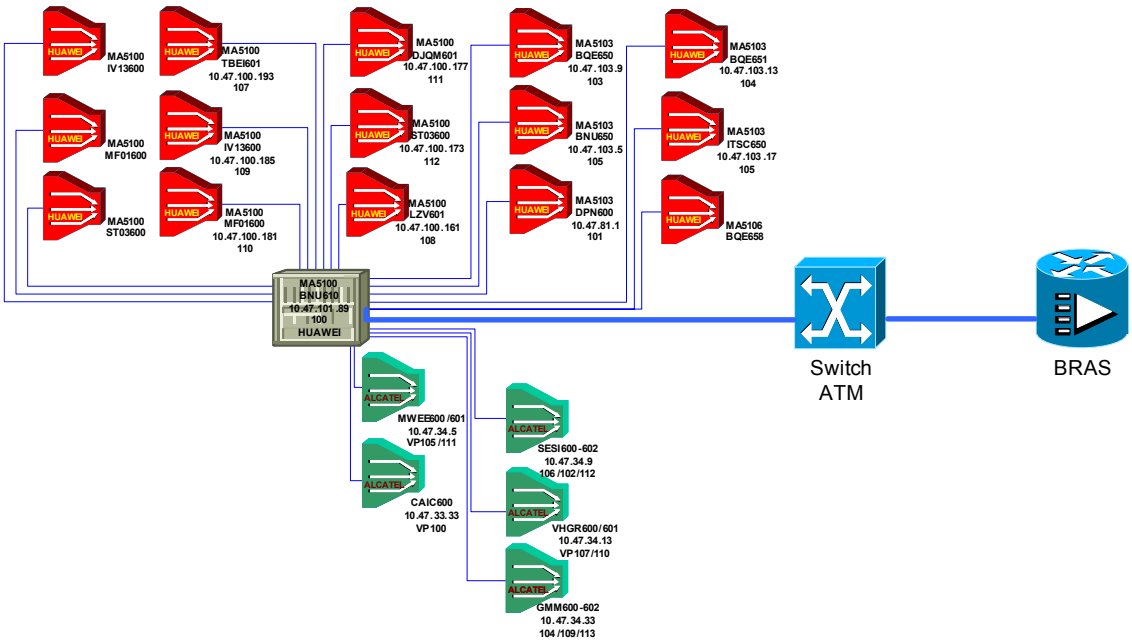

Figura 4.1: Exemplo de Topologia da Rede ADSL utilizando DSLAMs ATM

- ✓ A informação de DSLAM, placa e porta contida na conexão PPPoA é inserida no Bilhete de Autenticação no atributo *NAS-Port*. Este atributo é do tipo inteiro sendo uma representação numérica da porta física, denominada de "formato D". No atributo *NAS-Port-id* a informação aparece em forma de texto. O formato é visualizado nos testes descritos no capítulo 5.

Também é necessário neste caso identificar um atributo no Bilhete RADIUS referente a qual BRAS estamos nos referindo. Esta informação está presente no atributo *NAS-Identifier* onde é exibido o endereço IP do Agregador na rede IP da operadora.

4.1.4.2 DSLAM Ethernet

Similar ao que foi dito para os DSLAMs ATM será descrita a forma de implementação da configuração lógica das VLANs no *backbone* de Dados Ethernet. Independente de um DSLAM estar diretamente ligado a um switch Ethernet ou fazer parte de uma cascata de DSLAMs, cada DSLAM terá duas VLANs de saída, sendo uma para os clientes com modalidade de serviço Residencial e uma para os clientes com modalidade de

serviço IP Profissional ou IP Turbo. Esta VLAN chega até o Switch Ethernet e deste até o BRAS. Não existe repetição de VLAN num mesmo switch ou Agregador, apresentado na Figura 4.2.

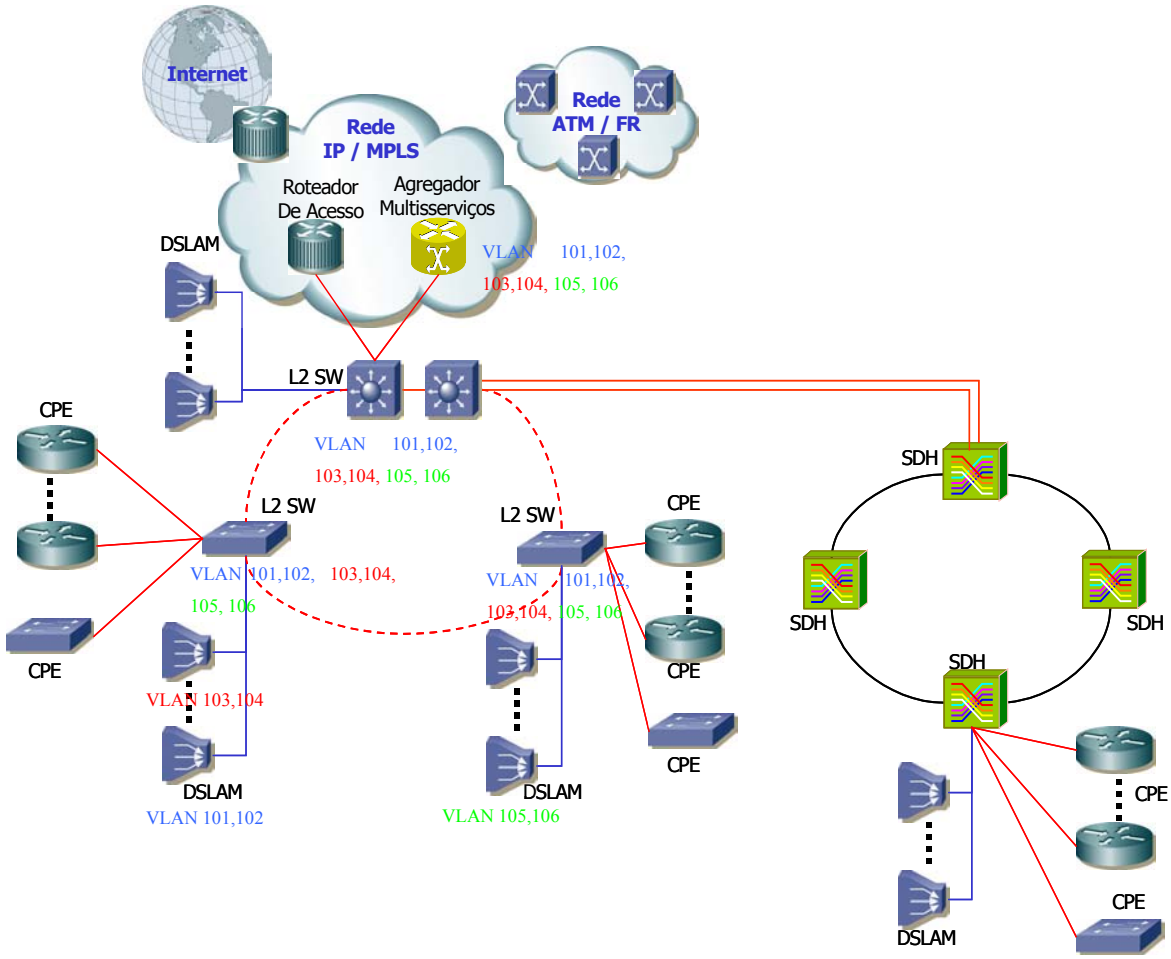

Figura 4.2: Topologia da Rede ADSL e Backbone de Dados utilizando DSLAMs Ethernet

Antes da implementação técnica proposta neste trabalho, não havia nenhum atributo no bilhete RADIUS (Figura 4.3) que permitisse identificar o DSLAM, *slot* e porta associada a uma determinada conexão. Somente era conhecida a VLAN, permitindo-se identificar o DSLAM, porém não ao usuário. Neste cenário, o processo de identificação do usuário é dificultado e depende da premissa que o usuário esteja conectado no momento da pesquisa, caso contrário, continua não sendo possível a identificação.

```
Fri Aug 24 07:45:05 GMT-03:00 2008
   Acct-Session-Id = 7/0/0/101.132_01A4EAD3
   Framed-Protocol = PPP
   Framed-IP-Address = 200.138.202.25
   User-Name = SCOS21583630@ae.sc
   Ascend-Connect-Progress = 60
   Cisco-AVPair2 = connect-progress=LAN Ses Up
   Acct-Authentic = RADIUS
   Acct-Status-Type = Start
   NAS-Port-Type = Virtual
   NAS-Port = 1885667460
   NAS-Port-Id = 7/0/0/101.132
   Class = PAENRAS01_SC_OK_EMP_CLT_0
   Service-Type = Framed-User
   NAS-IP-Address = 201.14.143.254
   Acct-Delay-Time = 0
   NAS-Identifier = BNUT3702
   Brt-ServiceId = EMP
   Brt-NasArea = SC
   Brt-AuthServer = PAENRAS01
   Brt-AuthResult = OK
   Brt-Hauss = CLT
   Brt-Acct-Start-Time = 2007/08/24 07:45:05
```

Figura 4.3: Bilhete RADIUS tipo Start antes da habilitação do PPPoE TAG nos DSLAMs e Agregadores

Para a arquitetura composta por DSLAMs Ethernet, a proposta consiste em configurar um conjunto de comandos nos DSLAMs e BRAS (Agregadores) fazendo com que a informação de DSLAM, *slot* e porta seja inserida pelo DSLAM, no pacote PADI, durante a fase de estabelecimento do PPPoE dentro do processo de conexão PPP. Esta informação estará contida no campo *TAG_Value* e o campo *TAG_TYPE* é denominado conforme a [RFC2516, RFC1700] no Apêndice A de 0x0105 (*Vendor Specific)*. Maiores detalhes do estabelecimento da conexão PPPoE e PPP foram abordados no capítulo 2.

Como esta opção depende única e exclusivamente de informações existentes na Operadora e a vinculação entre a porta física do DSLAM no qual o cliente está conectado e o bilhete de autenticação torna-se possível, esta é a melhor solução técnica dentre as estudadas e escolhida para implementação na rede ADSL da operadora em análise.

No próximo item descreveremos as etapas desenvolvidas para alcançar os objetivos de implementação técnica na rede ADSL.

4.2 A IMPORTÂNCIA DO INVENTÁRIO DA REDE ADSL DAS OPERADORAS

Uma das grandes deficiências operacionais das empresas de Telecomunicações reside em possuir um cadastro de equipamentos e facilidades incompleto e não consistente. A Rede ADSL, pela grande quantidade de elementos de rede e também de portas, eleva ainda mais a dificuldade de manter o cadastro o mais confiável possível. Além disso, as atualizações no sistema de inventário devem ocorrer quase que simultaneamente à alteração, inclusão ou deleção na rede ADSL.

Sendo o objetivo principal deste trabalho a vinculação física e lógica de acessos ADSL, consideramos como premissa que o cadastro de portas tenha alta confiabilidade. Sempre que a informação de qual cliente está conectado fisicamente a uma determinada porta estiver incorreto, conseqüentemente sua vinculação a conexão lógica não estará correta.

Num cenário de customização de serviços, as operadoras devem investir de forma intensiva na correção e manutenção do cadastro. Um dos subprodutos desta dissertação é a criação de um processo que cruza a informação de porta física de bilhetes de autenticação gerados com o status do sistema de inventário. Constatando que a porta informada não está ativa gera-se um relatório de inconsistências às equipes de campo que devem identificar os terminais e corrigir o cadastro.

Com a implementação técnica proposta, foram solicitadas à TI da operadora pesquisada melhorias no sistema de Inventário ADSL (denominado Objectel), visando automatizar algumas rotinas, melhorar o controle e iniciar um processo anti-fraude.

4.3 FASES DA IMPLEMENTAÇÃO TÉCNICA

Definida a melhor forma para alcançar os objetivos propostos, faz-se necessário descrever as fases necessárias para comprovação da hipótese. Tratar-se-á de DSLAMs ATM e Ethernet sempre separadamente, pois cada um tem suas particularidades.

Serão descritos a seguir, quatro processos desenvolvidos com o objetivo de operacionalizar a implementação na rede ADSL: Processo para DSLAMs ATM, Processo para DSLAM Ethernet, Processo para Agregadores e Processo de Mudança.

4.3.1 Processo para DSLAMs ATM

O Fluxograma apresentado na Figura 4.4 exemplifica as atividades e seqüência de passos utilizados para vinculação física e lógica envolvendo DSLAMs ATM.

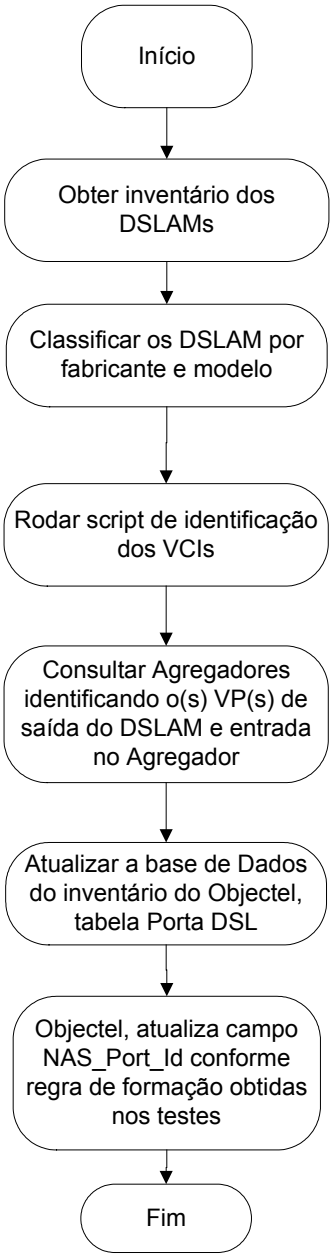

Figura 4.4: Fluxograma de atividades da implementação técnica em DSLAMs ATM

Utilizando como fontes de pesquisa o sistema de Inventário Objectel e a gerência dos DSLAMs dos vários fabricantes, foram relacionados todos os DSLAMs ATM da planta por fabricante e modelo, determinando-se a agregação em BRAS Cisco ou Juniper.

Para cada combinação de fabricante e modelo de DSLAM e BRAS foram colhidos bilhetes de autenticação para verificar a lei de formação do atributo *NAS-Port-Id*. O detalhamento dos testes e definição do formato do atributo será escopo do próximo capítulo.

Para identificar os VCIs de mais de 1 milhão de portas foi desenvolvido um *robô* (programa destinado a repetir uma atividade indefinidamente) para executar a varredura da rede de DSLAM ATM da operadora. Este *robô* coleta a informação das portas de assinantes no sistema de inventário, verifica quais são novas e parte para a identificação dos VCI das mesmas. Para tanto, o mesmo possui acesso aos *gateways* de acesso aos DSLAM (um para cada fabricante).

De forma geral, o *robô* segue as seguintes etapas:

1. Busca no inventário portas a serem verificadas;
2. Verifica o DSLAM ao qual as portas pertencem;
3. Acessa o *gateway* do fabricante via SSH (*Security Shell*) a partir da rede corporativa;
4. Acessa o DSLAM via SSH a partir da rede corporativa;
5. Recupera as informações dos VCI através de comandos específicos para cada fabricante/modelo;
6. Grava a informação na base de dados do inventário.

Para a obtenção do(s) VP(s) de cada DSLAM foi analisado manualmente a configuração de todos os equipamentos BRAS verificando e identificando em qual interface, sub-interface o DSLAM está configurado e qual(is) VP(s) foram atribuídos ao DSLAM.

4.3.2 Processo para DSLAMs Ethernet

O Fluxograma apresentado na Figura 4.5 exemplifica as atividades e seqüência de passos utilizados para vinculação física e lógica envolvendo DSLAMs Ethernet.

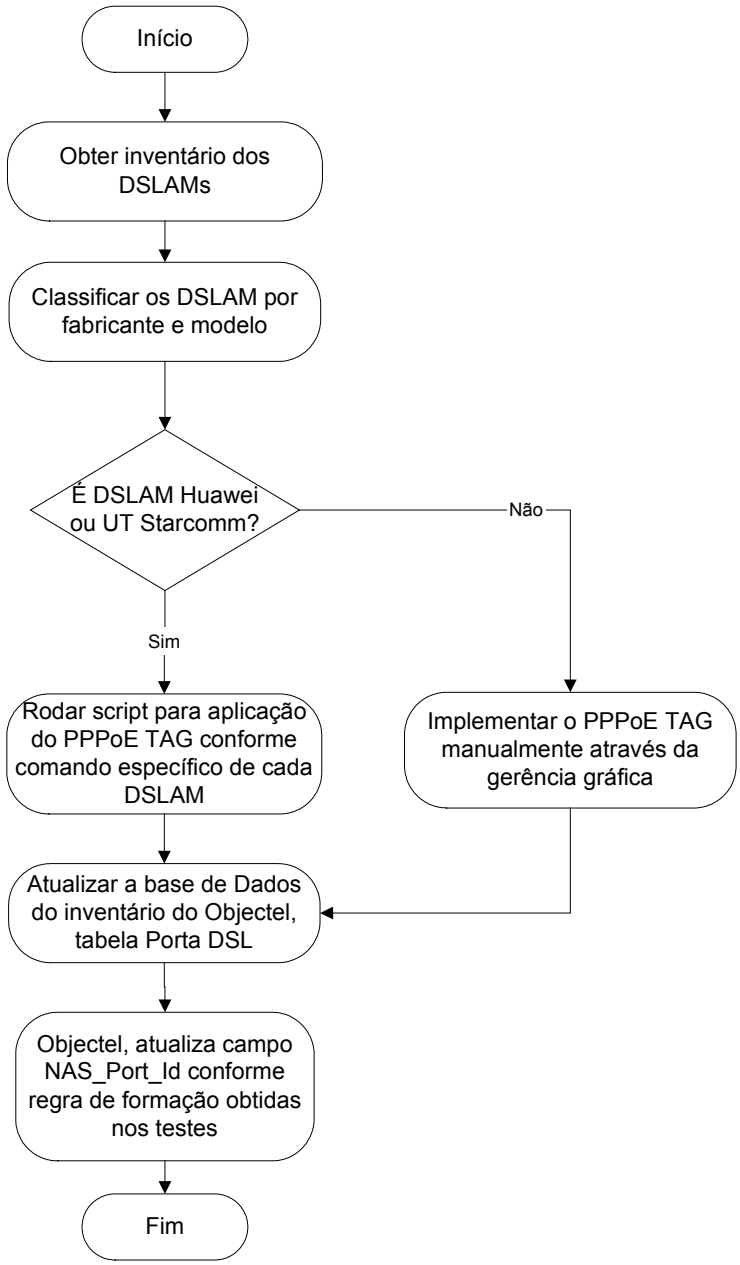

Figura 4.5: Fluxograma de atividades da implementação técnica em DSLAMs Ethernet

Para cada fabricante e modelo de DSLAM foram obtidas as versões de *software* que suportam a inserção do TAG e o procedimento com os comandos necessários para habilitação desta funcionalidade.

4.3.2.1 DSLAMs Huawei

Na planta da operadora analisada a maior quantidade de equipamentos é do fabricante Huawei, existindo o mesmo nos modelos: MA5100, MA5300 e MA5600. Os DSLAMs MA5300 não fazem parte do escopo deste trabalho, pois estão em processo de substituição por equipamentos MA5600 com previsão de conclusão até outubro/2008. Segue na Tabela 4.1 a relação de comandos e a versão de *software* necessária. A aplicação destes comandos é realizada remotamente via SSH.

Tabela 4.1: Versão de Software e Comandos para habilitar o TAG no DSLAM Huawei[HUAWEIa, HUAWEIb]

Modelo	Versão de *Software*	Comandos
MA5100	MA5100V200R005B05D063	ESRT613#***conf t*** ESRT613(config)#***int lan 0/15*** ESRT613(config-if-lan-0/15)#***pitp switch pmode***
MA5600	MA5600V300R002B02D230	PSPR605(config)#***pitp enable pmode***

4.3.2.2 DSLAM UTSTARCOM

UTSTARCOM é o segundo maior fabricante na planta da Brasil Telecom. Existem dois modelos diferentes B820 e B1000. Ambos possuem o mesmo comando e o mesmo formato de saída. Segue na Tabela 4.2 a relação de comandos e versão de *software* necessária. A aplicação destes comandos é realizada remotamente via SSH.

Tabela 4.2: Versão de Software e Comandos para habilitar o TAG no DSLAM UTSTARCOM [UTSTARCOMa, UTSTARCOMb]

Modelo	Versão de *Software*	Comandos
B820	Qualquer	ITBI603#**node-id 999** ITBI603(IPADSL3A-10)#**pppoe-agent enable** ITBI603(IPADSL3A-10)#dsl**-line-customized-agent-circuit-id "ITBI603 atm $shelf/$slot/$port:$vpi.$vci** ITBI603(IPADSL3A-10)#**dsl-line-agent-circuit-id-format customized**
B1000	Qualquer	Idem

4.3.2.3 Implementação em DSLAMs Huawei e UTSTARCOM

Para implantação dos comandos em DSLAMs Huawei e UTSTARCOM executados via SSH, foi desenvolvido um *robô* (programa destinado a repetir uma atividade indefinidamente) para executar a aplicação do *PPPoE TAG* nos DSLAM Ethernet.

Este *robô* coleta a informação dos DSLAMs Ethernet no inventário da rede, verifica quais são novos e parte para a aplicação do *PPPoE TAG* nos mesmos. É executada conectividade via SSH aos *gateways* de acesso aos DSLAM (um para cada fabricante).

De forma geral, o *robô* segue as seguintes etapas:

1. Busca no inventário os DSLAM;
2. Acessa o *gateway* do fabricante;
3. Acessa o DSLAM;
4. Aplica a identificação *PPPoE TAG* através de comandos específicos;
5. Grava a informação na base de dados do inventário.

4.3.2.4 DSLAM SIEMENS

A configuração necessária para habilitar o TAG nos DSLAMs SIEMENS é realizada via gerência gráfica. A gerência SIEMENS permite ao operador definir um formato de saída dentre alguns formatos possíveis. Habilita-se o *DHCP Relay Agent* com parâmetro *relay agent option = PPPoE both,* vinculam-se as VLANs de saída do DSLAM ao DHCP *Relay Agent* e as portas do DSLAM a VLAN de saída. Desta forma o DSLAM SIEMENS passa a externar a informação do TAG inserindo-o no processo de estabelecimento do PPPoE.

4.3.2.5 DSLAM ERICSSON

Toda intervenção nos DSLAMs ERICSSSON é feita via gerência. Na gerência de DSLAMs Ericsson é possível atribuir o TAG ao serviço, neste caso o *profile*, desde que nenhum cliente esteja ativo neste *profile*. Em resumo, foi necessário criar novos *profiles* inserindo o serviço DHCP opção 82 denominado de *Circuit ID – Costumer Number* que carrega a informação do equipamento, *slot* e porta.

4.3.3 Processo para Agregadores

O Fluxograma apresentado na Figura 4.6 exemplifica as atividades e seqüência de passos utilizados para vinculação física e lógica envolvendo Agregadores.

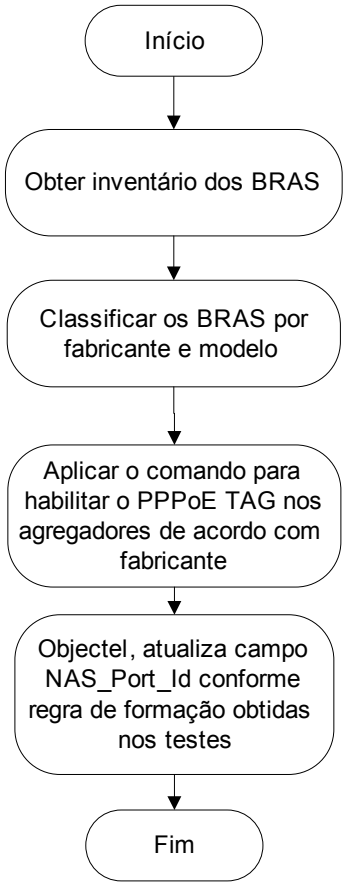

Figura 4.6: Fluxograma de atividades da implementação técnica nos Agregadores

Para cada fabricante de Agregador foram obtidas as versões de *software* que suportam a inserção do TAG e o procedimento com os comandos necessários para habilitação desta funcionalidade.

4.3.3.1 Agregador CISCO

A versão de software recomendada para habilitar o PPPoE TAG do BRAS CISCO 10008 é **12.0**. Para habilitar o PPPoE TAG no Agregador CISCO 10008, deve-se executar, em cada um dos elementos, os seguintes comandos em cada elemento de rede, conforme Figura 4.7:

bba-group pppoe <profile do serviço>

vendor-tag circuit-id service

vendor-tag strip

Onde <*profile do serviço*> equivale ao serviço, residencial, empresarial, etc.

Figura 4.7: Comandos para habilitar o PPPoE TAG no agregador CISCO

4.3.3.2 Agregador JUNIPER

A versão de software recomendada para habilitar o PPPoE TAG do BRAS JUNIPER é **8.0.4**. Para habilitar o PPPoE TAG no Agregador JUNIPER deve ser configurada a opção "*pppoe remote-circuit-id*" em cada Interface VLAN dos DSLAMs através do seguintes comandos, representados aqui na Figura 4.8:

```
GNALE700#conf t
GNALE700(config)#interface gigabitEthernet 10/0.1720
GNALE700(config-if)#pppoe remote-circuit-id
```

Figura 4.8: Comandos para habilitar o PPPoE TAG no agregador JUNIPER

A configuração da Interface VLAN do DSLAM fica conforme figura 4.9:

```
GNALE700#show conf interface gigabitEthernet 10/0.1720
! Configuration script being generated on TUE JUL 22 2008 16:24:17 GMT-3
! Juniper Edge Routing Switch ERX-1440
! Version: 8.0.4 release-0.0 [BuildId 8402] (November 8, 2007  15:50)
! Copyright (c) 1999-2007 Juniper Networks, Inc.  All rights reserved.
!
! Commands displayed are limited to those available at privilege level 10
!
! NOTE:  This script represents only a subset of the full system configuration.
interface gigabitEthernet 10/0.1720
!
 vlan id 1720
 ip description VLAN_ADSL_NQACTO604_RESIDENCIAL
 pppoe
 pppoe auto-configure
 pppoe remote-circuit-id
 pppoe profile any residencialPPPoE
```

Figura 4.9: Padrão de Configuração da Interface após habilitar PPPoE TAG

O segundo passo da configuração é sobrescrever o parâmetro *Calling-station-id* com a informação do DSLAM no pacote RADIUS, através do seguintes comandos, apresentados na Figura 4.10:

```
GNALE700#conf t
GNALE700(config)#radius override calling-station-id remote-circuit-id
```

Figura 4.10: Seqüência de Configuração do parâmetro Calling-station-Id

4.3.4 Processo de Mudança e atualização de inventário em caso de expansão, remanejamento, otimização e migração de DSLAMs na Rede.

Como já foi mencionado no item 4.2 é fundamental para que haja vinculação física e lógica dos acessos em Banda larga utilizando acessos ADSL de forma correta, que o cadastro de portas da operadora se mantenha confiável e atualizado no tempo. Desta forma, o processo de mudança foi definido e difundido na empresa. Toda mudança envolvendo alteração física ou lógica na rede ADSL deve ter ao final do processo uma atividade de atualização cadastral. O processo de mudança só é dado como concluído quando são refletidas no cadastro todas as alterações executadas na rede. Na figura 4.11 segue um fluxograma do Processo de Mudança na operadora analisada.

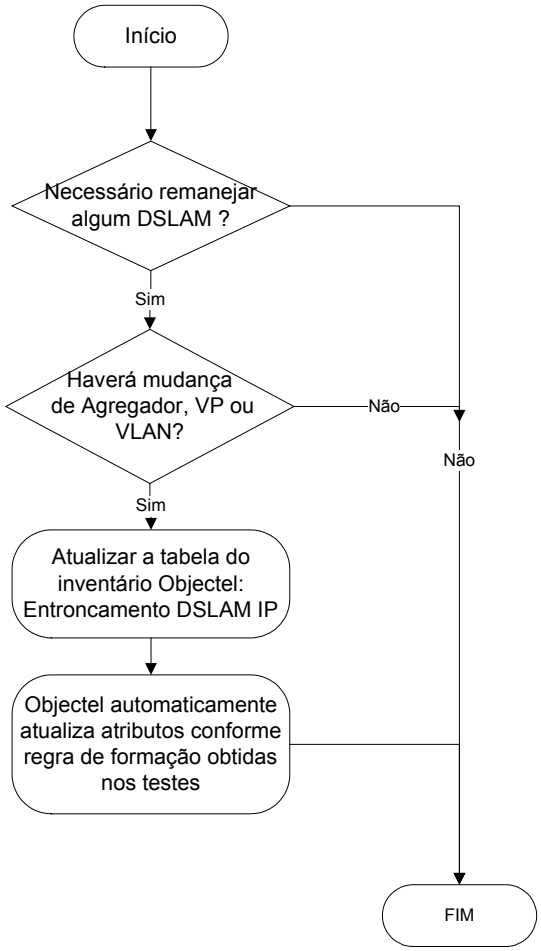

Figura 4.11: Fluxograma do Processo de Mudança na operadora pesquisada

4.4 BENEFÍCIOS ESPERADOS

Com a implementação técnica sugerida, discutida e defendida neste capítulo, além dos processos de atualização cadastral necessários no processo de mudança, as operadoras de Telecomunicações, terão os seguintes ganhos:

1. Jurídico/Legal: Responder a todos os pedidos de identificação judicial expedidos pela justiça solicitando quebra de sigilo de usuários Internet que praticam atos ilícitos. Atualmente somente são passíveis de identificação os usuários conectados em DSLAM ATM ou os usuários conectados em DSLAMs Ethernet que permanecem conectados na Internet no momento de recebimento

do ofício da justiça e pesquisa no servidor de autenticação da operadora. Além de permanecer conectado não pode ter havido por parte do usuário alteração da máquina de origem do ataque pois esta é a única chave existente.

Atualmente a operadora analisada deixa de responder em média 100 pedidos por mês. O número de solicitações de identificação judicial aumenta a cada ano, num ritmo bastante intenso e as operadoras precisam definir mecanismos mais eficazes e automáticos de responder a demanda, sob pena de aumento de funcionários e multas por descumprimento. O Senador Eduardo Azeredo é relator de uma proposta na Assembléia Legislativa, já aprovada pelas comissões de Educação, Ciência e Tecnologia, Constituição e Justiça e de Assuntos Econômicos, para coibir e punir delitos de informática que prevê a modificação e a ampliação de cinco leis brasileiras: Código Penal, Código Penal Militar, Lei de Repressão Uniforme, Lei Afonso Arinos e Estatuto da Criança e Adolescente [SENADO]. Este projeto de lei determina multas e sanções pesadas por descumprimento de identificações judiciais. Enquanto as operadoras não implantarem mecanismo como o sugerido neste trabalho, estarão descumprindo o acima exposto.

2. Financeiro/Processual – realizar o cruzamento de bilhetes de autenticação RADIUS com o cadastro do inventário físico de portas identificando a geração de bilhetes em portas ADSL com status diferente de Ativa. Esta ação poderá identificar ativações fraudulentas de ADSL permitindo a regularização da situação com incremento de receita. Outro efeito colateral obtido desta ação é a possibilidade de atualização cadastral. Quando houver um bilhete de autenticação positivo e a porta informada está diferente de ativa no cadastro, verificar-se-á que se trata de registro incorreto no sistema de inventário permitindo assim sua correção e depuração, conforme Figura 4.12.

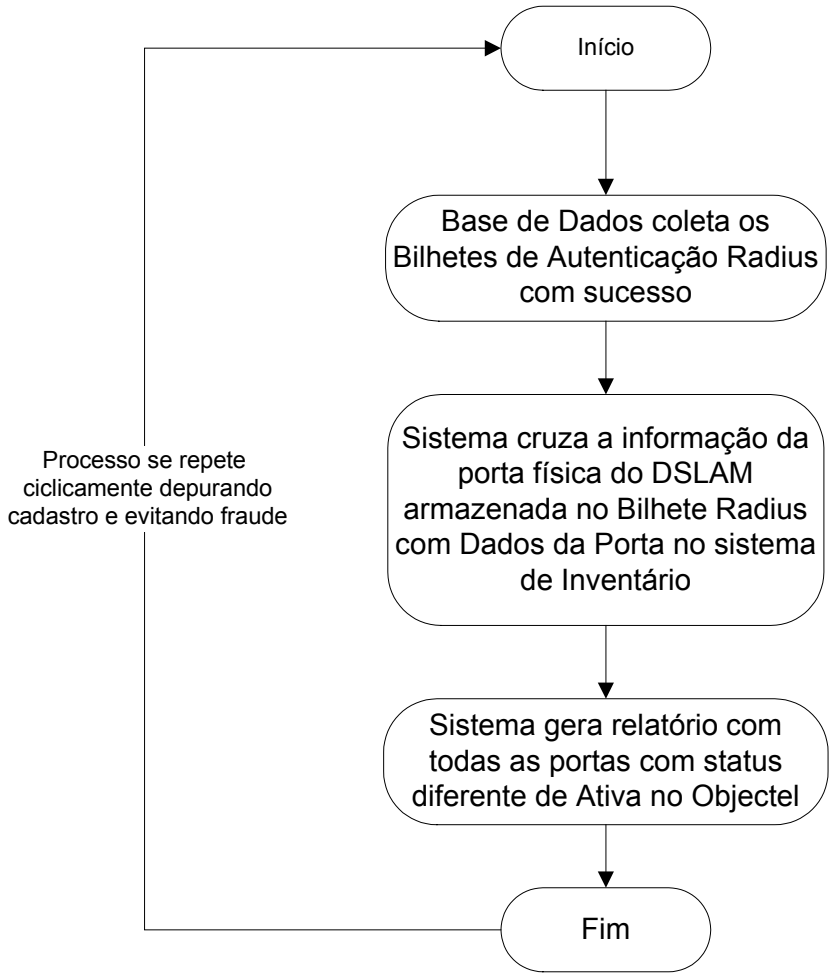

Figura 4.12: Fluxograma do Processo de Reconciliação do Cadastro

3.1 Marketing/Comercial – lançamento de serviços e planos de tarifação personalizados ou adequados a determinados nichos de mercado, como, por exemplo: cobrança por tempo de uso, garantia de banda ou privilégio para determinadas aplicações, cobrança por banda utilizada;

3.2 Marketing/Comercial – será possível armazenar o *login* de autenticação dos clientes que utilizam tecnologia ADSL, que na maioria das vezes é o próprio e-mail do cliente, e com isto promover ações de marketing como envio de *mailings* ou até mesmo encaminhar e-mail para aviso de interrupções programadas do serviço.

4 Retenção – um número significativo de clientes entra em contato com o *Call Center* solicitando o cancelamento do serviço ADSL informando que nunca conseguiu completar o processo de auto-instalação do CPE e não utilizou o serviço. Com a implementação proposta nesta dissertação de mestrado será possível identificar se a porta que o cliente estava conectado gerou bilhetes de autenticação com sucesso ou não e qual a duração.

5 IMPLEMENTAÇÃO TÉCNICA: TESTES REALIZADOS, DIFICULDADES E ESTÁGIO DE IMPLEMENTAÇÃO

Este capítulo tem por objetivo apresentar todas as atividades desenvolvidas com equipamentos de testes, bem como, os testes realizados na planta "viva" da operadora em análise, apresentando seus resultados e o estágio atual da implementação técnica proposta. Aqui são utilizados todos os conceitos discutidos ao longo desta dissertação e aplicada à implementação técnica sugerida no capítulo 4. As dificuldades encontradas também serão aqui abordadas.

5.1 INVENTÁRIO DOS DSLAMs ATM

Conforme mencionado no capítulo 4, para obtenção dos VCIs correspondentes a 1.108.492 portas de DSLAMs ATM em funcionamento na operadora foi desenvolvido um robô que executa *scripts* que permitem a conexão em cada um dos DSLAMs remotamente através de uma sessão *telnet* ou SSH nos *gateways* de cada gerência, a partir da rede do Centro de Gerência da operadora.

Para cada fabricante e modelo de DSLAM foi identificada à seqüência de comandos necessária, bem como, o formato de saída das informações nos DSLAMs, para a obtenção da associação *slot* e porta com o seu respectivo VCI, que pelas características de implementação na operadora se mantêm os mesmos dentro da Rede ATM e no Agregador.

Na Figura 5.1 é possível observar o robô se conectando ao DSLAM ADRCE601 e após uma seqüência de comandos específica para os DSLAMs Huawei MA5100 podem-se verificar todos os VPIs e VCIs configurados na placa controladora e os respectivos *slot*/porta equivalentes.

```
Huawei MA5100 Multi-service Access Module.
  Copyright(C) 1998-2004 by Huawei Technologies Co., Ltd.

>>User name:xxx
>>User password:

ADRCE601>enable

ADRCE601#configure terminal

ADRCE601(config)#scroll
  Screen output automatic scrolling

ADRCE601(config)#show pvc 0/7
{ groupindex<K>|vlan<K>|<cr> }:

Command:
        show pvc 0/7
-------------------------------------------------------------------------------
 CONN  CAST ============ SRC =============  ============ DST ============= MNGE
 INDX  TYPE SERV F/S /P    VPI  VCI    CTTR  SERV F/S /P    VPI  VCI    CTTR STAT
-------------------------------------------------------------------------------
    0  p2p  ima  0/7 /2    14   100       2  sar  *         *    *         2 up
    1  p2p  ima  0/7 /2    14   101       2  adl  0/0 /0    1    32        2 up
    2  p2p  ima  0/7 /2    14   103       2  adl  0/0 /2    1    32        2 up
    3  p2p  ima  0/7 /2    14   104       2  adl  0/0 /3    1    32        2 up
    4  p2p  ima  0/7 /2    14   105       2  adl  0/0 /4    1    32        2 up
    5  p2p  ima  0/7 /2    14   106       2  adl  0/0 /5    1    32        2 up
    6  p2p  ima  0/7 /2    14   107       2  adl  0/0 /6    1    32        2 up
    7  p2p  ima  0/7 /2    14   108       2  adl  0/0 /7    1    32        2 up
    8  p2p  ima  0/7 /2    14   109       2  adl  0/0 /8    1    32        2 up
    9  p2p  ima  0/7 /2    14   110       2  adl  0/0 /9    1    32        2 up
   10  p2p  ima  0/7 /2    14   111       2  adl  0/0 /10   1    32        2 up
   11  p2p  ima  0/7 /2    14   112       2  adl  0/0 /11   1    32        2 up
   12  p2p  ima  0/7 /2    14   113       2  adl  0/0 /12   1    32        2 up
   13  p2p  ima  0/7 /2    14   114       2  adl  0/0 /13   1    32        2 up
   14  p2p  ima  0/7 /2    14   115       2  adl  0/0 /14   1    32        2 up
   15  p2p  ima  0/7 /2    14   116       2  adl  0/0 /15   1    32        2 up
   16  p2p  ima  0/7 /2    14   117       2  adl  0/0 /16   1    32        2 up
   17  p2p  ima  0/7 /2    14   118       2  adl  0/0 /17   1    32        2 up
   18  p2p  ima  0/7 /2    14   119       2  adl  0/0 /18   1    32        2 up
   19  p2p  ima  0/7 /2    14   120       2  adl  0/0 /19   1    32        2 up
   20  p2p  ima  0/7 /2    14   121       2  adl  0/0 /20   1    32        2 up
   21  p2p  ima  0/7 /2    14   122       2  adl  0/0 /21   1    32        2 up
   22  p2p  ima  0/7 /2    14   123       2  adl  0/0 /22   1    32        2 up
   23  p2p  ima  0/7 /2    14   124       2  adl  0/0 /23   1    32        2 up
   24  p2p  ima  0/7 /2    14   126       2  adl  0/0 /25   1    32        2 up
   25  p2p  ima  0/7 /2    14   127       2  adl  0/0 /26   1    32        2 up
   26  p2p  ima  0/7 /2    14   128       2  adl  0/0 /27   1    32        2 up
```

Figura 5.1: Formato de saída dos dados do DSLAM Huawei 5100

Para a obtenção do Agregador, interface, sub-interface e VP de entrada referente a um determinado DSLAM foi realizado levantamento individual em cada um dos sessenta e dois (62) Agregadores e 4.493 DSLAMs em operação na planta.

5.2 PADRÃO DE INFORMAÇÃO DO ATRIBUTO NAS_Port_Id EM DSLAMs ATM

A primeira conclusão que se chega, quando são realizados testes é de que o formato da informação do DSLAM, *slot* e porta contidos no atributo *NAS-Port-Id* do bilhete *RADIUS* independe da topologia de rede entre um DSLAM e de seu(s) respectivo(s) Agregador(es). Não importa se o DSLAM é cascateado a outro DSLAM ou não, se está ligado via fibra óptica ou utilizando qualquer rede de transporte. Esta é uma consideração importante que simplifica a definição dos cenários futuros de teste.

Uma segunda conclusão é de que o formato do conteúdo do atributo *NAS-Port_Id* é o mesmo para os vários fabricantes de DSLAM ATM.

A única diferença de formato ocorreu em função do fabricante do Agregador. Desta forma, foram identificados dois formatos de conteúdo do atributo, sendo um para BRAS CISCO e outro para BRAS JUNIPER.

5.2.1 BRAS CISCO 10008

O padrão *NAS_Port_Id* para DSLAMs terminando em agregador *CISCO* é:

<Interface_BRAS>/<Sub_Interface_BRAS>/<porta_BRAS>/<VPI_DSLAM>.<VCI_DSLAM>

A equivalência entre BRAS, Interface, Sub-Interface, Porta e VPI para se determinar qual é o DSLAM, está disponível no sistema de Inventário da operadora, numa tabela denominada: Entroncamento do DSLAM com IP. Esta tabela foi validada e corrigida a partir da verificação da configuração de todos os Agregadores em operação.

Na Figura 5.2 é exibido um Bilhete RADIUS do tipo *start* que é gerado após processo de autenticação e autoriza um determinado cliente a utilizar o serviço de Banda Larga em acesso ADSL com origem em BRAS CISCO.

```
Fri Aug 24 11:27:35 GMT-03:00 2007
        Acct-Session-Id = "7/0/1/115.187_1572AD5E"
        Framed-Protocol = PPP
        Framed-IP-Address = 201.41.44.63
        User-Name = "CROS26899952"
        Ascend-Connect-Progress = 60
        Cisco-AVPair = "connect-progress=LAN Ses Up"
        Acct-Authentic = RADIUS
        Acct-Status-Type = Start
        NAS-Port-Type = Virtual
        NAS-Port = 1903362235
        NAS-Port-Id = "7/0/1/115.187"
        Class = "PAENRAS01_RS_OK_EMP_CLT_0"
        Service-Type = Framed-User
        NAS-IP-Address = 201.14.221.254
        Acct-Delay-Time = 0
        NAS-Identifier = "CSLCE701"
        Brt-ServiceId = "EMP"
        Brt-NasArea = "RS"
        Brt-AuthServer = "PAENRAS01"
        Brt-AuthResult = "OK"
        Brt-Hauss = "CLT"
        Brt-Acct-Start-Time = "2007/08/24 11:27:35"
```

Figura 5.2: Exemplo de Bilhete RADIUS tipo Start com terminação em BRAS CISCO 10008

Do Bilhete são extraídas as informações: *NAS_Port_Id*: 7/0/1/115.187 e *NAS-Identifier*: 201.14.221.254 que corresponde ao BRAS: CSLCE701

Do formato do atributo *NAS-Port-Id*, tem-se a seguinte Tabela 5.1:

Tabela 5.1: Formato do Atributo NAS-Port_Id - Agregador CISCO

Interface BRAS	Sub-Interface BRAS	Porta BRAS	VPI	VCI
7	0	1	115	187

Da Tabela de Equivalência:

CSLCE701-7/0/1 VPI: 115 corresponde ao DSLAM: CSLCE607

VCI: 187 corresponde ao *slot*/porta: CSLCE607-24/03

5.2.2 BRAS ERX

O padrão *NAS_Port_Id* para DSLAMs terminando em agregador JUNIPER é:

atm <*Interface_BRAS*>/<*porta_BRAS*>.<*VPI_DSLAM*><*VCI_DSLAM*>:<*VPI_DSLAM*><*VCI_DSLAM*>

Na Figura 5.3 é exibido um Bilhete RADIUS do tipo *start* que é gerado após processo de autenticação e autoriza um determinado cliente a utilizar o serviço de Banda Larga em acesso ADSL, com origem em BRAS JUNIPER.

```
Fri Aug 24 00:00:18 GMT-03:00 2007
      Acct-Status-Type = Start
      User-Name = "SCOS55315318@ipt.sc"
      Acct-Session-Id = "erx atm 0/2.107129:107.129:0542051153"
      NAS-IP-Address = 200.138.224.254
      Class = "PAENRAS01_SC_OK_EMP_CLT_0"
      Service-Type = Framed-User
      Framed-Protocol = PPP
      Framed-IP-Address = 201.3.244.85
      NAS-Port-Type = xDSL
      NAS-Port = 40566913
      NAS-Port-Id = "atm 0/2.107129:107.129"
      Acct-Authentic = RADIUS
      NAS-Identifier = "FNSCE701"
      Brt-ServiceId = "EMP"
      Brt-NasArea = "SC"
      Brt-AuthServer = "PAENRAS01"
      Brt-AuthResult = "OK"
      Brt-Hauss = "CLT"
      Brt-Acct-Start-Time = "2007/08/24 00:00:19"
```

Figura 5.3: Exemplo de Bilhete RADIUS tipo Start com terminação em BRAS Juniper ERX

Do Bilhete são extraídas as informações: *NAS_Port_Id*: atm 0/2.107129:107.129 *NAS-IP-Address*: 200.138.224.254 que corresponde ao BRAS: FNSCE70Do formato do atributo *NAS-Port-Id*, tem-se a Tabela 5.2:

Tabela 5.2: Formato do Atributo NAS-Port_Id - Agregador JUNIPER

Interface BRAS	Porta BRAS	VPI	VCI
0	2	107	129

Da Tabela de Equivalência:

FNSCE701-0/2 VPI: 107 corresponde ao DSLAM: BRES601

VCI: 129 corresponde ao *slot*/porta: BRES601-01/29

Em resumo, a lei de formação, em se tratando de DSLAMs ATM, independe do DSLAM. A tabela 5.3 resume a lei de formação obtida.

Tabela 5.3: Lei de formação do atributo NAS-Port-Id para DSLAMs ATM

BRAS	Formato
CISCO	"**<interface>/<subinterface>/<porta>/<VPI>.<VCI>**"
JUNIPER	"**atm <interface>/<porta>.<VPIVCI>:<VPI>.<VCI>**"

5.3 IMPLEMENTAÇÃO DO PPPoE TAG NOS DSLAMS ETHERNET

Foi estudada a documentação dos DSLAMs dos vários fabricantes existentes na operadora em análise e identificados os comandos necessários para habilitação do parâmetro PPPoE TAG nos DSLAMs. Em alguns casos específicos foi necessário o envolvimento do fabricante para fornecer uma versão de *software* que suportasse a implementação da funcionalidade.

Da mesma forma que para os DSLAMs ATM, a execução de testes considerando várias topologias existentes na planta da operadora comprovaram que a inserção do TAG no PPPoE independe da arquitetura de rede.

Utilizando como fontes de pesquisa o sistema de Inventário Objectel, a base de dados existente no Centro de Gerência e a gerência dos DSLAMs dos vários fabricantes, foram relacionados todos os DSLAMs Ethernet da planta por fabricante e modelo e determinando a agregação em BRAS Cisco ou Juniper, também com suas respectivas versões de *software*. A Tabela 5.4 apresenta como estava a distribuição de DSLAMs Ethernet e BRAS em 01/04/2008, onde IOS OK significa que possui a funcionalidade PPPoE TAG e IOS Nok não suporta, sendo necessário executar uma atividade de *upgrade* de *software*.

Tabela 5.4: Distribuição de DSLAMs Ethernet e BRAS em 01/04/2008 – 91,6% versão de software já atualizada para suportar o PPPoE TAG

Modelo Agregador	Modelo DSLAM	Portas ADSL
Cisco 10K (Versão IOS OK)	ERICSSON	76.413
Cisco 10K (Versão IOS OK)	HUAWEI MA5100V200R002B01D058	14.160
Cisco 10K (Versão IOS OK)	HUAWEI MA5100V200R002B01D058	448
Cisco 10K (Versão IOS OK)	HUAWEI MA5100V200R005B03D052	39.165
Cisco 10K (Versão IOS OK)	HUAWEI MA5100V200R005B03D052	1.216
Cisco 10K (Versão IOS OK)	HUAWEI MA5100V200R005B05D063	3.104
Cisco 10K (Versão IOS OK)	HUAWEI MA5100V200R005B05D063	384
Cisco 10K (Versão IOS OK)	HUAWEI MA5300	22.742
Cisco 10K (Versão IOS OK)	HUAWEI MA5600	363.649
Cisco 10K (Versão IOS OK)	UTSTARCOM	420.250
Cisco 10K (Versão IOS OK)	SIEMENS	79.730
Cisco 10K (Versão IOS Nok)	ERICSSON	3.921
Cisco 10K (Versão IOS Nok)	HUAWEI	0
Cisco 10K (Versão IOS Nok)	HUAWEI MA5100V200R002B01D058	2.496
Cisco 10K (Versão IOS Nok)	HUAWEI MA5100V200R005B03D052	4.384
Cisco 10K (Versão IOS Nok)	HUAWEI MA5100V200R005B03D052	416
Cisco 10K (Versão IOS Nok)	HUAWEI MA5300	1.037
Cisco 10K (Versão IOS Nok)	HUAWEI MA5600	6.271
Cisco 10K (Versão IOS Nok)	UTSTARCOM	43.488
ERX (Versão IOS Nok)	ERICSSON	8.795
ERX (Versão IOS Nok)	HUAWEI MA5100V200R002B01D058	2.720
ERX (Versão IOS Nok)	HUAWEI MA5100V200R005B03D052	5.152
ERX (Versão IOS Nok)	HUAWEI MA5100V200R005B05D063	1.440
ERX (Versão IOS Nok)	HUAWEI MA5300	576
ERX (Versão IOS Nok)	HUAWEI MA5600	640
ERX (Versão IOS Nok)	UTSTARCOM	10.872
ERX (Versão IOS Nok)	SIEMENS	1.225
		1.114.694

Partiu-se então para realização de testes considerando as combinações de DSLAM e BRAS existentes na planta. Através dos testes foi possível constatar, que diferentemente dos DSLAMs ATM, o formato da informação varia de fabricante para fabricante, todavia

num mesmo fabricante o formato independe do modelo do DSLAM. Em relação ao BRAS, a diferenciação não está no formato, mas sim, em qual atributo do bilhete a informação é inserida.

Após testes, considerando a combinação de fabricantes de DSLAM e BRAS e as versões de *software* recomendadas, foi possível constatar o correto funcionamento do serviço Banda larga utilizando tecnologia ADSL.

O detalhamento dos testes e definição do formato dos atributos estão descritos nos itens a seguir.

5.4 PADRÃO DE INFORMAÇÃO DOS ATRIBUTOS CISCO-AVPair E Calling-Station-Id EM DSLAMs ETHERNET

Cada fabricante possui um padrão específico para informar o DSLAM, *slot* e porta respectivos a uma determinada conexão. Descreve-se abaixo o formato encontrado nos DSLAMs em operação na planta ADSL da operadora.

5.4.1 DSLAM ERICSSON

O formato do atributo *CISCO-AVPair* e *Calling-Station-Id* para BRAS CISCO e JUNIPER respectivamente quando o DSLAM em questão é do fabricante ERICSSON [ERICSSON] é:

<DSLAM>.<slot>.<porta>

Onde:

DSLAM = nome do DSLAM na gerência;

slot = número do *slot* onde está inserida a placa de assinante;

porta = número da porta onde está o assinante está conectado;

Na Figura 5.4 é exibido um Bilhete de Autenticação RADIUS do tipo *start* de um DSLAM ERICSSON e Agregador CISCO.

```
Thu Mar 27 16:09:31 GMT-03:00 2008
        Acct-Session-Id = "1/1/0/666_026EDFD0"
        Cisco-AVPair = "client-mac-address=fe00.0118.0005"
        Cisco-Policy-Up = "BEST-EFFORT"
        Framed-Protocol = PPP
        Framed-IP-Address = 201.89.208.133
        User-Name = "testeturbo"
        Ascend-Connect-Progress = 60
        Cisco-AVPair = "connect-progress=LAN Ses Up"
        Acct-Authentic = RADIUS
        Acct-Status-Type = Start
        NAS-Port-Type = Ethernet
        Cisco-AVPair = "circuit-id-tag=CTAME682.6.1"
        NAS-Port = 402653850
        NAS-Port-Id = "1/1/0/666"
        Class = "CTANRAS01_PR_OK_LOC_CLT_0"
        Service-Type = Framed-User
        NAS-IP-Address = 201.25.179.254
        Acct-Delay-Time = 0
        NAS-Identifier = "CTAME700"
        Brt-ServiceId = "LOC"
        Brt-NasArea = "PR"
        Brt-AuthServer = "CTANRAS01"
        Brt-AuthResult = "OK"
        Brt-Hauss = "CLT"
        Brt-Acct-Start-Time = "2008/03/27 16:09:31"
```

Figura 5.4: Exemplo de Bilhete RADIUS tipo Start envolvendo DSLAM ERICSSON e BRAS CISCO 10008

5.4.2 DSLAM UTSTARCOM B820 e B1000

O formato do atributo *CISCO-AVPair* e *Calling-Station-Id* para BRAS CISCO e JUNIPER respectivamente quando o DSLAM em questão é do fabricante UTSTARCOM [UTSTARCOMa, UTSTARCOMb] é:

<DSLAM> *atm* ***<shelf>/<slot>/<porta>:<VPI>.<VCI>***

Onde:

DSLAM = nome do DSLAM na gerência;

shelf = *sempre igual a 1;*

slot = número do *slot* onde está inserida a placa de assinante;

porta = número da porta onde está o assinante está conectado;

VPI = *virtual path interface*. Conexão ATM entre o DSLAM e o modem do assinante;

VCI = *virtual circuit interface*. Conexão ATM entre o DSLAM e o modem do assinante;

Os campos VPI e VCI são atribuídos, na operadora analisada, da seguinte forma:

VPI = 0 e VCI = 35 para todos os estados, exceto RS;

VPI = 1 e VCI = 32 para o RS;

Na Figura 5.5 é exibido um Bilhete de Autenticação RADIUS do tipo *start* de um DSLAM UTSTARCOM e Agregador CISCO.

```
Fri Mar 28 09:32:45 GMT-03:00 2008
        Acct-Session-Id = "1/1/0/3060_0272D696"
        Cisco-AVPair = "client-mac-address=001d.6a08.7fe7"
        Cisco-Policy-Up = "BEST-EFFORT"
        Framed-Protocol = PPP
        Framed-IP-Address = 201.3.108.220
        User-Name = "testeturbo"
        Ascend-Connect-Progress = 60
        Cisco-AVPair = "connect-progress=LAN Ses Up"
        Acct-Authentic = RADIUS
        Acct-Status-Type = Start
        NAS-Port-Type = Ethernet
        Cisco-AVPair = "circuit-id-tag=CTAME999 atm 1/6/2:0.35"
        NAS-Port = 402656244
        NAS-Port-Id = "1/1/0/3060"
        Class = "CTANRAS01_PR_OK_LOC_CLT_0"
        Service-Type = Framed-User
        NAS-IP-Address = 201.25.179.254
        Acct-Delay-Time = 0
        NAS-Identifier = "CTAME700"
        Brt-ServiceId = "LOC"
        Brt-NasArea = "PR"
        Brt-AuthServer = "CTANRAS01"
        Brt-AuthResult = "OK"
        Brt-Hauss = "CLT"
        Brt-Acct-Start-Time = "2008/03/28 09:32:45"
```

Figura 5.5: Exemplo de Bilhete RADIUS tipo Start envolvendo DSLAM UTSTARCOM e BRAS CISCO 10008

5.4.3 DSLAMs MA5100, MA5600 HUAWEI

O formato do atributo *CISCO-AVPair* e *Calling-Station-Id* para BRAS CISCO e JUNIPER respectivamente quando o DSLAM em questão é do fabricante HUAWEI [HUAWEIa, HUAWEIb]é:

***<DSLAM>** atm 0>/<**slot**>/0/<**porta**>:<VPI>.<VCI>*

Onde:

DSLAM = nome do DSLAM na gerência;

slot = número do *slot* onde está inserida a placa de assinante;

porta = número da porta onde está o assinante está conectado;

VPI = *virtual path interface*. Conexão ATM entre o DSLAM e o modem do assinante;

VCI = *virtual circuit interface*. Conexão ATM entre o DSLAM e o modem do assinante;

Para demonstrar o formato citado acima, o tráfego de uma conexão foi coletado e utilizando um software de captura de pacotes denominado Wireshark [WIRESHARK], pode-se verificar na Figura 5.6 a fase de *Discovery* do PPPoE e a inserção do TAG VALUE *Vendor Specific* pelo DSLAM no pacote PADI.

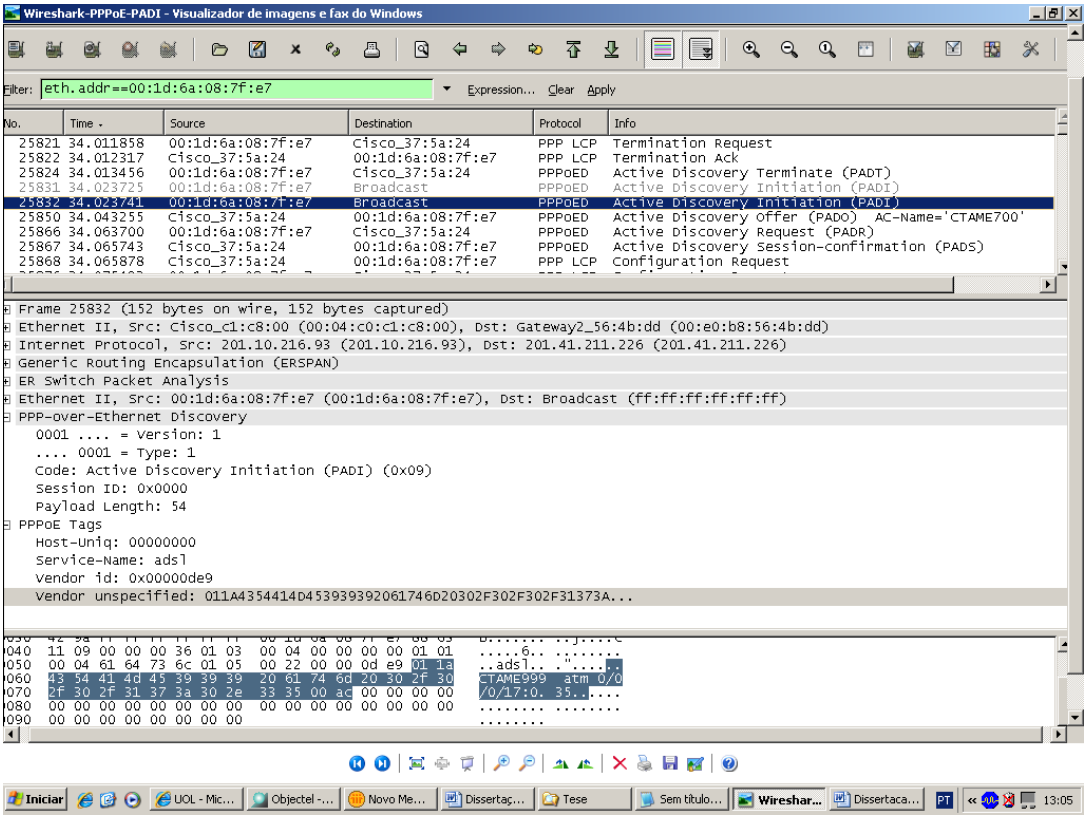

Figura 5.6: Captura de tráfego para uma conexão PPPoE com DSLAM HUAWEI5100 com função PPPoE TAG habilitada

Na Figura 5.7 é exibido um Bilhete de Autenticação RADIUS do tipo *start* de um DSLAM HUAWEI e Agregador CISCO.

```
Thu Mar 27 08:44:13 GMT-03:00 2008
        Acct-Session-Id = "1/1/0/3110_04BC39A2"
        Cisco-AVPair = "client-mac-address=0012.01bb.47d1"
        Cisco-Policy-Up = "BEST-EFFORT"
        Framed-Protocol = PPP
        Framed-IP-Address = 189.11.107.165
        User-Name = "testeturbo"
        Ascend-Connect-Progress = 60
        Cisco-AVPair = "connect-progress=LAN Ses Up"
        Acct-Authentic = RADIUS
        Acct-Status-Type = Start
        NAS-Port-Type = Ethernet
        Cisco-AVPair = "circuit-id-tag=CTAOR663 atm 0/9/0/30:0.35"
        NAS-Port = 402656294
        NAS-Port-Id = "1/1/0/3110"
        Class = "CTANRAS01_PR_OK_LOC_CLT_0"
        Service-Type = Framed-User
        NAS-IP-Address = 201.41.168.254
        Acct-Delay-Time = 0
        NAS-Identifier = "CTAJE701"
        Brt-ServiceId = "LOC"
        Brt-NasArea = "PR"
        Brt-AuthServer = "CTANRAS01"
        Brt-AuthResult = "OK"
        Brt-Hauss = "CLT"
        Brt-Acct-Start-Time = "2008/03/27 08:44:13"
```

Figura 5.7: Exemplo de Bilhete RADIUS tipo Start envolvendo DSLAM HUAWEI e BRAS CISCO 10008

5.4.4 DSLAM HiX5635 SIEMENS

O formato do atributo *CISCO-AVPair* e *Calling-Station-Id* para BRAS CISCO e JUNIPER respectivamente quando o DSLAM em questão é do fabricante SIEMENS [SIEMENS] é:

<DSLAM> *atm* ***<slot>/<porta>:<VPI>.<VCI>***

Onde:

DSLAM = nome do DSLAM na gerência;

slot = número do *slot* onde está inserida a placa de assinante;

porta = número da porta onde está o assinante está conectado;

VPI = *virtual path interface*. Conexão ATM entre o DSLAM e o modem do assinante;

VCI = *virtual circuit interface*. Conexão ATM entre o DSLAM e o modem do assinante;

Os campos VPI e VCI são atribuídos na Brasil Telecom da seguinte forma:

VPI = 0 e VCI = 35 para todos os estados, exceto RS;

VPI = 1 e VCI = 32 para o RS;

Na Figura 5.8 é exibido um Bilhete de Autenticação RADIUS do tipo *start* de um DSLAM SIEMENS e Agregador CISCO.

```
Tue Apr 01 16:31:57 GMT-03:00 2008
        Acct-Session-Id = "1/1/0/3630_028ECCF2"
        Cisco-AVPair = "client-mac-address=0013.469d.39e7"
        Cisco-Policy-Up = "BEST-EFFORT"
        Framed-Protocol = PPP
        Framed-IP-Address = 201.66.126.118
        User-Name = "cfcgaribaldi@onda.com.br"
        Ascend-Connect-Progress = 60
        Cisco-AVPair = "connect-progress=LAN Ses Up"
        Acct-Authentic = RADIUS
        Acct-Status-Type = Start
        NAS-Port-Type = Ethernet
        Cisco-AVPair = "circuit-id-tag=CTAB1690 atm 01/72:0.35"
        NAS-Port = 402656814
        NAS-Port-Id = "1/1/0/3630"
        Class = "CTANRAS01_PR_OK_DEF_CLF_0"
        Service-Type = Framed-User
        NAS-IP-Address = 201.25.179.254
        Acct-Delay-Time = 0
        NAS-Identifier = "CTAME700"
        Brt-ServiceId = "DEF"
        Brt-NasArea = "PR"
        Brt-AuthServer = "CTANRAS01"
        Brt-AuthResult = "OK"
        Brt-Hauss = "CLF"
        Brt-Acct-Start-Time = "2008/04/01 16:31:57"
```

Figura 5.8: Exemplo de Bilhete RADIUS tipo Start envolvendo DSLAM SIEMENS e BRAS CISCO 10008

Em resumo, a Tabela 5.5 apresenta o formato de saída da informação DSLAM, *slot* e porta em DSLAMs Ethernet.

Tabela 5.5: Lei de formação do atributo CISCO-AVPair (CISCO) e Calling-Station-Id (JUNIPER)

DSLAM	Formato
ERICSSON	***<DSLAM>.<slot>.<porta>***
UTSTARCOM	***<DSLAM>*** *atm* ***<shelf>/<slot>/<porta>:<VPI>.<VCI>***
HUAWEI	***<DSLAM>*** *atm 0>/<slot>/0/<porta>:<VPI>.<VCI>*
SIEMENS	***<DSLAM>*** *atm* ***<slot>/<porta>:<VPI>.<VCI>***

5.5 DIFICULDADES ENCONTRADAS

Há três anos a operadora pesquisada vem discutindo uma forma de identificar logicamente seus clientes. Vários fatores foram se somando para que a empresa demorasse tanto tempo para conseguir êxito, mesmo sendo tão importante para a empresa esta implementação. O Portal, mesmo não tendo este objetivo inicial frustrou as expectativas e teve de ser retirado da planta.

Dentre as maiores dificuldades encontradas para concluir este trabalho destaca-se a enorme quantidade de elementos de rede e portas envolvidas. Toda vez se que se pensava em começar uma solução técnica possível, os profissionais envolvidos se questionavam: e se o *hardware* de determinado DSLAM não for compatível? E se tivermos de trocar a versão de *software* de todos ou de algum fabricante em específico? Serão anos de atualização. E teremos orçamento para isto? Desta forma, a primeira grande dificuldade são as dificuldades que se colocavam antes mesmo delas existirem.

Sem dúvida, a quantidade de elementos de rede atrasou em muito a conclusão da implementação técnica, entretanto não foi a maior dificuldade.

A segunda dificuldade evidente estava associada à diversidade de fabricantes, modelos e versões de *software* de DSLAM e BRAS. São 8 (oito) fabricantes de DSLAM

com 13 (treze) modelos diferentes. São 2 (dois) fabricantes de BRAS e 3 (três) modelos diferentes. Felizmente uma dificuldade que parecia existir, mas não faz efeito sobre a implementação técnica sugerida são os cascateamentos de DSLAM. Existem DSLAMs de um fabricante cascateado em outro. Existem cascatas com mais de quarenta DSLAMs. Nesse aspecto a preocupação somente existiu até que os primeiros testes foram concluídos.

Iniciando pelo DSLAMs ATM, partiu-se da premissa de que existia uma regra de formação entre o *slot* e porta física com o VCI por fabricante. No início da implantação da rede esta premissa era verdadeira, mas com a modificação da planta e o envelhecimento dos DSLAMs, algumas situações diferentes foram encontradas: DSLAMs com mais de em VP; DSLAMs com placas diferentes contendo quantidade de portas variadas, DSLAMs com *slot*s vagos sem obedecer a uma seqüência lógica. Estes fatores exigiram que fosse desenvolvido o robô mencionado anteriormente para obter a equivalência *slot*/porta/VCI. Foi gasto praticamente 1 ano até concluir este levantamento, haja visto, que o robô levava semanas para pesquisar mais de 1 milhão de portas. Outro agravante é de que a planta é dinâmica. De um processamento para outro informações eram modificadas tornando necessário um trabalho investigativo para verificar porque a equivalência havia mudado.

Em relação aos DSLAMs Ethernet o desafio era maior pois não havia nos bilhetes de autenticação a informação do DSLAM, *slot* e porta. A opção de habilitar o PPPoE TAG teve que ser estudada em cada um dos fabricantes, identificando qual versão de *software* suportava os comandos, qual seria o formato de saída, onde esta informação seria inserida no bilhete. Com surpresa deparou-se com uma grande quantidade de versões de *software* na planta, principalmente nos DSLAMs Huawei. Os novos DSLAMs eram implantados com versões atualizadas de *software*, entretanto nenhum trabalho era realizado na planta em operação. Mais de uma versão suportava o comando para habilitar o PPPoE TAG mas com respostas distintas nos testes. Definiu-se a versão mais atual como padrão e se iniciou um trabalho de execução de upgrade de *software* em janelas de manutenção programadas. Este trabalho é de longa duração, ainda não foi concluído.

Este trabalho investigativo também propiciou a descoberta de uma quantidade significativa de DSLAMs que não estavam configurados no Sistema de Gerência e

conseqüentemente não executavam backup e não externavam alarmes de falha. Este trabalho também contribuiu para melhoria geral da rede ADSL.

O DSLAM UTSTARCOM [UTSTARCOMa, UTSTARCOMb], embora implemente o PPPoE TAG, não apresentava nenhuma menção sobre o assunto na sua documentação. Foi necessário envolvimento da fábrica no Japão para identificar como externar o nome do DSLAM no TAG. Interrogando o equipamento, não está disponível o comando executado.

Seguindo a documentação do BRAS JUNIPER, a informação do TAG não é externada. São necessários passos adicionais do que está contido na documentação, sendo também necessário envolvimento do fabricante.

Para os DSLAM ERICSSON [ERICSSON], onde todos os comandos são executados utilizando a gerência gráfica foi necessário o desenvolvimento de uma rotina que extraiu as configurações das portas num arquivo XML (*Extensible Markup Language*), as informações foram tratadas e gravadas novamente na gerência e nos DSLAMs. Demoramos vários dias para definir este processo porque a partir de uma quantidade pequena de portas ADSL a rotina parava e não era possível prosseguir sem a reinicialização da gerência. Depois de vários dias de análise concluiu-se que o arquivo de *syslog* da gerência estava definido em 2 (dois) kbytes, espaço insuficiente para a quantidade de atividades que estavam sendo executadas.

A maior dificuldade e totalmente imprevista, foi a incompatibilidade de alguns DSLAMs com determinados modems ADSL. Depois que havíamos realizado teste com todos os DSLAMs e Agregadores utilizando um modem ADSL com resultados positivos, ou seja, a informação de DSLAM, *slot* e porta estava presente, partiu-se para implementação em massa na planta. No segundo dia de implementação surgiram várias reclamações de clientes que exigiram retornar a situação original desabilitando a funcionalidade nos DSLAMs onde já havia sido habilitado o comando. Foi necessário interagir com HUAWEI e UTSTARCOM, tecnologias onde a incompatibilidade foi identificada, enviando os *logs* do estabelecimento do protocolo PPPoE e sessão PPP. A HUAWEI já encaminhou novo *software* corrigindo a incompatibilidade e o mesmo já foi amplamente inserido nos

DSLAMs não identificando novas falhas e a UTSTARCOM trabalha na análise dos *logs* até a conclusão desta dissertação de mestrado.

5.6 ANÁLISE DOS RESULTADOS

Em virtude dos testes já realizados e descritos nas seções anteriores deste capítulo, inclusive com a implantação em larga escala nos equipamentos em funcionamento na Rede ADSL da operadora estudada, constata-se que os resultados esperados foram alcançados e a vinculação entre a identificação física da porta ADSL que atende um determinado cliente e a identificação lógica do bilhete de autenticação torna-se possível e é realidade. Desta forma, o objetivo deste trabalho de dissertação de mestrado foi plenamente alcançado, propiciando a operadora pesquisada novas oportunidades de criação de serviços e o atendimento da exigência legal de identificação de quebra de sigilo.

5.7 ESTÁGIO DE IMPLEMENTAÇÃO

Neste item é apresentado um quadro que exemplifica o estágio de implementação e conseqüentemente o grau de identificação física e lógica, considerando como data base 25/07/2008.

Tabela 5.6: Estágio atual de Implementação da solução técnica proposta

Elemento de Rede	Situação	Comentário
DSLAM ATM	100% concluído	
DSLAM HUAWEI Ethernet	53% concluído	Necessário executar 15 janelas de manutenção para atualização de software. Previsão de dois meses para conclusão.
DSLAM SIEMENS	100% concluído	
DSLAM UTSTARCOM	100% concluído	
DSLAM ERICSSON	97% concluído	Restam substituir o *profile* de 12 DSLAMs. Previsão de uma semana para conclusão.
BRAS CISCO	100% concluído	Existem dois BRAS que não estão na última versão de software mas na versão atual também externalizam o TAG.
BRAS JUNIPER	30% concluído	Todos os BRAS que possuem DSLAM Ethernet conectado já estão versão correta e com o TAG habilitado. Não existe necessidade de alteração de software dos demais BRAS.

6 CONCLUSÕES

Este capítulo trata das conclusões obtidas a partir da pesquisa realizada, e finalmente oferece propostas e sugestões de trabalhos futuros que podem ser desencadeados a partir da metodologia proposta.

Como já mencionado anteriormente, no Planejamento estratégico de muitas operadoras de telecomunicações, o segmento de Banda Larga é vital porque disponibilizar acessos em banda larga aos seus clientes assegura: potencialização da receita por terminal, "blindagem" e manutenção do acesso de telefonia fixa e fidelização do cliente mediante previsões de aumento acirrado da concorrência.

Para combater a concorrência e potencializar a receita com serviços de valor agregado, existe a necessidade de personalização e de customização dos serviços disponibilizados sobre Banda Larga e a oferta de planos de tarifas diferenciados.

Neste contexto, nada mais apropriado e até porque não dizer primordial, o desenvolvimento desta pesquisa, primeiramente, porque visa atender aspectos legais já que a metodologia desenvolvida possibilitará a identificação judicial expedida pela justiça para identificação de usuários que praticam atos ilícitos na Internet. Em segundo lugar, mas não menos importante, a implementação da metodologia proposta possibilitará a criação de novos serviços para as mais diferentes aplicações, atendendo demanda de nichos específicos e possibilitando uma diferenciação dos serviços fornecidos pela concorrência.

A conclusão deste trabalho é um anseio da operadora desde 2005. Vários foram os fatores que impossibilitaram seu desenvolvimento, mas, sobretudo, as dificuldades face ao volume de trabalho dado o tamanho da planta ADSL (2,3 milhões de portas), a diversidade de CPEs, DSLAMs e Agregadores empregada e a capilaridade existente com mais de 9.000 DSLAMs atendendo mais de 1.500 localidades.

Outro valor agregado deste trabalho é a de detecção de fraude através da geração de bilhetes de autenticação cuja porta do DSLAM encontra-se vaga no inventário e, portanto, sem faturamento para a companhia e a retro-alimentação do cadastro através das

inconsistências entre a informação do inventário físico e informações lógicas dos bilhetes de autenticação.

A metodologia foi aplicada em DSLAMs de teste dos vários fabricantes existentes na planta da operadora, simulando as condições reais da planta e as topologias existentes na operadora. Pela abrangência e diversidade da planta, esta metodologia pode ser aplicada a qualquer operadora respeitando-se apenas particularidades existentes entre as mesmas. O resultado dos testes foi um sucesso e alcança os objetivos propostos.

A implementação da metodologia está em andamento na planta ADSL da operadora com perspectiva de conclusão nos próximos três meses.

Esta dissertação de mestrado pode ser utilizada como referência teórica para outras dissertações relacionadas a Banda Larga. Também vislumbra-se a partir deste trabalho, o desenvolvimento de pesquisas nos seguintes temas:

- Análise e desenvolvimento da integração entre o Inventário físico de portas ADSL com o servidor de autenticação, em tempo real, adequando a arquitetura de rede ADSL para enriquecer o bilhete de autenticação com o contrato do terminal telefônico do acesso físico;

- Análise e desenvolvimento da integração entre o sistema de Inventário físico de portas ADSL, o servidor de autenticação e plataformas de *Police Server* ermitindo desenvolvimento de novos serviços;

- Análise da evolução do processo de autenticação e vínculo físico e lógico frente a novos cenários de substituição da topologia de rede ADSL para um modelo utilizando protocolo DHCP;

- Análise e desenvolvimento de um comparativo de custos entre a solução atual utilizando-se Agregadores frente a novas tendências de utilização de DHCP Server.

7 REFERÊNCIAS BILBLIOGRÁFICAS

[ANATEL] ANATEL. **"Espaço do Cidadão: Internet"**. Disponível em <http://www.anatel.gov.br/Portal/exibirPortalInternet.do?exibirPortalInternetRodape=true>. Acesso em: 28 jun. 2008.

[ANSI T1.413] ***ANSI T1.513 - Network and Customer Installation Interfaces – Asymmetric Digital Subscriber Line (ADSL) Metallic Interface***. Norma do American National Standards Institute, 1998.

[CISCOa] CISCO. **"*Cisco 10008 Router Hardware Installation Guide*"**. Disponível em <http://www.cisco.com/en/US/docs/routers/10000/10008/install_and_upgrade/hardware_installation/guide/8-hig.html>. Acesso em: 25 jul. 2008.

[CISCOb] CISCO. **"*PPPoE RADIUS Port Identification*"**. Disponível em <http://www.cisco.com/en/US/docs/ios/12_1t/12_1t5/feature/guide/dtppprad.html>. Acesso em: 25 jul. 2008.

[DICIONÁRIO] DICIONÁRIO PORTUGUÊS. Disponível em <HTTP://www.dicionariodeportugues.com>.

[ERICSSON] Manual "***DSLAM Ethernet DSL Access***", versão 2.0, 2004.

[MUNCINELLI] MUNCINELLI G.. "**Aplicação do Método das Linhas de Transmissão (TLM) no Estudo de Distúrbios Não Contínuos em Linhas Digitais Assimétricas de Assinante (ADSL)"**. Dissertação de Mestrado. Universidade Tecnológica Federal do Paraná, 2006.

[GINSBURG] GINSBURG, David. **"*Implementing ADSL*"**. Massachusetts: Addison Wesley Longman Inc., 1999.

[GLOBESPAN] GLOBESPAN - ***Spectral Compatibility of Digital Subscriber Line (DSL) Systems***. Página da WEB, IEC - International Engineering Consortium, Web ProForum Tutorials, http://www.iec.org.

[GOLDEN] GOLDEN, P.; Dedicie H,; Jacobsen K. S.; **"*Fundamentals of DSL Technology*"**, 2004.

[GRUSZYNSKI] GRUSZYNSKI, A.; "**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. Tese de Mestrado em Engenharia Elétrica. Universidade de Brasília, Brasília, DF, 2008

[HUAWEIa] Manual ***"DSLAM MA5600 - SmartAX MA5600 Command Help(V3.10)***",2005

[HUAWEIb] Manual "***DSLAM MA5100 - SmartAX MA5100 (MA5103) Command Help"***, 2005

[IDC] IDC Brasil. **"Barômetro Cisco da Banda Larga – 1º trimestre 2008"**. Disponível em <http://www.cisco.com/web/BR/barometro/barometro.html>. Acesso em: 25 jul. 2008.

[ITU992.1] "***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>. Acesso em: 20 jun.2008.

[ITU992.2] "***G.9992.2: Splitterless asymmetric digital subscriber line (ADSL) transceivers***". ITU, 1999. Disponível em: <http://www.itu.int/rec/T-REC-G.992.2-199907-I/en>. Acesso em: 20 jun. 2008.

[JUNIPERa] JUNIPER NETWORKS. **"*JUNOSe™ Internet Software for E-series™ Routing Platforms Link Layer Configuration Guide*"**. Disponível em <http://www.juniper.net/techpubs/software/erx/junose80/swconfig-link/html/title-swconfig-link.html>. Acesso em: 25 jul. 2008.

[JUNIPERb] JUNIPER NETWORKS. **"*ERX Modeule Guide*"**. Disponível em http://www.juniper.net/techpubs/hardware/e-series.html. Acesso em: 25 jul. 2008.

[MIERCOM] MIERCOM. **"*Edge Routers: Lab Testing Summary Report*"**. Outubro, 2004.

[REGSCM] ANATEL. "**Regulamento do Serviço de Comunicação Multimídia"**. Anexo à Resolução número 272. ANATEL, 2001.

[RES272] _____. **"Resolução No 272"**. ANATEL. 9 de agosto de 2001.

[RFC1332] MCGREGOR, G. **"*The PPP Internet Protocol Control Protocol (IPCP)*"**. IETF. RFC 1332, 1992.

[RFC1661] SIMPSON, W. (Ed.) **"*The Point-to-Point Protocol (PPP)*"**. IETF. RFC1661, 1994.

[RFC1662] SIMPSON, W. (Ed.) **"*The Point-to-Point Protocol (PPP) in HDLC Framing*"**. IETF. RFC1662, 1994.

[RFC1700] POSTEL, J.; Reynolds, J. **"*Assigned Numbers*"**. IETF. RFC 1700, 1994.

[RFC2364] GROSS, G. et al. **"*PPP Over AAL5*"**. IETF. RFC 2516, 1998.

[RFC2516] MAMALOS, L. et al. **"*A Method for Transmitting PPP Over Ethernet (PPPoE)*"**. IETF. RFC2516, 1999.

[RFC2865] RIGNEY, C. et al. **"*Remote Authentication Dial In User Service (RADIUS)*"**. IETF. RFC2865, 2000.

[RFC2866] RIGNEY, C. **"*RADIUS Accounting*"**. IETF RFC 2866, 2000.

[ROGERS] ROGERS COMMUNICATIONS INC. **"*Rogers Hi-Speed Internet*"**. Disponível em <http://www.hispeed.rogers.com/bband/content/keepingpace/index.html>. Acesso em: 14 jun. 2008.

[SENADO] SENADO. **"Projeto Lei Substitutivo (ao PLS 76/2000, PLS137/2000 e PLC 89/2003)."** Disponível em <http://www.senado.gov.br/comunica/agencia/pags/01.html>. Acesso em 30 jul. 2008.

[SIEMENS] Manual "***DSLAM Siemens - User Manual SURPASS hiX 5635",*** R2.0M UMN:CLI, 2006.

[SPIRENT] SPIRENT COMMUNICATIONS. **"*Broadband Access Architectures: Point-to-Point Protocol Comes of Age*"**. 2002. Disponível em <http://www.spirentcom.com/documents/595.pdf>. Acesso em: 14 jun. 2008.

[STARR] STARR, T.; Sorbara, M.; Cioffi, J.M.;Silverman, P.J.; "***DSL Advances*"**, 2003

[STD1] REYNOLDS, J.; Ginoza, S. **"*Internet Official Protocol Standards*"**. IETF. STD 1, 2004.

[TR101] COHEN, A.; Shrum, E.; "***Migration to Ethernet-Based DSL Aggregation***". DSL Forum. TR101, 2006.

[TR22.800] FRANK, R. "***IP Multimedia Subsystem (IMS) subscription and access scenarios*"*.*** 3GPP TR22.800, 2003

[UTSTARCOMa] Manual "***DSLAM UTSTARCOM B820 - AN-2000 IB Release 2.1 Command Line Interface (CLI) User Manual"***, 2003.

[UTSTARCOMb] Manual "***DSLAM UTSTARCOM B1000 - IAN8K B1000 IP DSLAM - Release 3.2.2 - CLI Reference Guide"***, 2007.

[WIRESHARK] **"*Wireshark Network Protocol Analyser*"** Disponível em <http://www.wireshark.org>. Acesso em: 21 jul. 2008.