UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

MECANISMO FUNCIONAL ESCALÁVEL PARA CONTABILIZAÇÃO DE USO DE SERVIÇOS RESIDENCIAIS EM REDE DE ACESSO EM BANDA LARGA UTILIZANDO TECNOLOGIA ADSL

ANDRÉ GRUSZYNSKI

ORIENTADOR: RODRIGO PINTO LEMOS

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPGENE.DM-056/2008

BRASÍLIA/DF: AGOSTO - 2008

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

MECANISMO FUNCIONAL ESCALÁVEL PARA CONTABILIZAÇÃO DE USO DE SERVIÇOS RESIDENCIAIS EM REDE DE ACESSO EM BANDA LARGA UTILIZANDO TECNOLOGIA ADSL

ANDRÉ GRUSZYNSKI

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

APROVADA POR:

RODRIGO PINTO LEMOS, Dr., EEEC/UFG
(ORIENTADOR)

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

ALTAMIRO AMADEU SUSIN, Dr., DELET/UFRGS
(EXAMINADOR EXTERNO)

BRASÍLIA, 08 DE AGOSTO DE 2008.

FICHA CATALOGRÁFICA

GRUSZYNSKI, ANDRÉ
G892m MECANISMO FUNCIONAL ESCALÁVEL PARA CONTABILIZAÇÃO DE USO DE SERVIÇOS RESIDENCIAIS EM REDE DE ACESSO EM BANDA LARGA UTILIZANDO TECNOLOGIA ADSL / André Gruszynski.-- Brasília,2008
xxii, 160 p. : il. ; 297mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2008)
Dissertação de Mestrado – Universidade de Brasília, Faculdade de Tecnologia, Departamento de Engenharia Elétrica.
Orientador: Rodrigo Pinto Lemos
1. Contabilização 2. Banda Larga
3. ADSL 4. *Pay-per-use*
I. ENE/FT/UnB II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

GRUSZYNSKI, ANDRÉ (2008). Mecanismo funcional escalável para contabilização de uso de serviços residenciais em rede de acesso em banda larga utilizando tecnologia ADSL, Publicação PPGENE.DM-056/2008, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 160 p.

CESSÃO DE DIREITOS

NOME DO AUTOR: André Gruszynski

TÍTULO: Mecanismo funcional escalável para contabilização de uso de serviços residenciais em rede de acesso em banda larga utilizando tecnologia ADSL.

GRAU: Mestre ANO: 2008

André Gruszynski

SQSW 104, Bloco C, Apto 308

70670-403, Setor Sudoeste, Brasília, DF

DEDICATÓRIA

Ao meu filho Lucas.

À Aline, mãe do Lucas.

“O único lugar onde o sucesso vem antes do trabalho é no dicionário.”

-- Albert Einstein

AGRADECIMENTOS

Agradeço à Aline, minha esposa, pelo incondicional amor e inestimável apoio que recebi ao longo desta jornada. Ao Lucas, nosso filho, por me ensinar o verdadeiro espírito da curiosidade. Aos meus pais, Alexandre e Cecy, por sempre acreditarem na capacidade dos seus filhos de obterem êxito. À minha irmã Ana e ao meu cunhado Antônio, pelas inúmeras e valiosas sugestões. Ao meu irmão Cirilo, pelo exemplo de perseverança em seus objetivos e de amor às coisas que faz. Ao Emerson Baumgarten e à Loriza Andrade, meus companheiros: «quem tem amigos, nunca está só». Ao Marcelo Blanes e ao Carlos Campana Pinheiro, pelas importantes contribuições e filosóficas discussões. Ao Prof. Rodrigo Pinto Lemos, pela sua disposição e dedicação em me auxiliar a desbravar este assunto.

O meu sucesso é o nosso sucesso. Muito obrigado!

(Esta página foi intencionalmente deixada em branco.)

RESUMO

Este trabalho descreve um mecanismo cuja finalidade é fornecer informações que possibilitem realizar, de uma forma alternativa à tradicional, que é a de valor fixo e independente do consumo, a cobrança pelo consumo dos serviços de banda larga que utilizam tecnologia ADSL (*Asymmetric Digital Subscriber Line*). Duas grandezas são consideradas para fins de contabilização: a quantidade de tempo em que uma conexão esteve ativa e a quantidade de *bytes* trafegados durante esta conexão. Como requisito adicional, o mecanismo proposto deve ser ampliável de forma proporcional ao crescimento do número de acessos. Na primeira parte é apresentada a arquitetura habitual de uma rede de acesso em banda larga baseada em tecnologia ADSL, são discutidas as alternativas encontradas para realizar a coleta das informações de consumo e, ao final, é escolhida uma das alternativas. A opção escolhida é baseada no uso de um protocolo de autenticação, de autorização e de bilhetagem chamado RADIUS, motivo pelo qual esse assunto é explorado com profundidade. Essa investigação fundamenta o mecanismo que é proposto a seguir, constituído a partir dos elementos de uma rede de acesso ADSL tradicional, porém dispostos, implementados e configurados observando um conjunto de critérios e técnicas voltados à redução de oportunidades de perda de informações de consumo. Experimentos e provas de conceito foram elaborados e descritos com a finalidade de prover a validação prática de certos aspectos propostos. Um desses experimentos teve como objetivo descobrir, analisar e documentar a forma através da qual o elemento de rede NAS (*Network Access Server*) realiza a contabilização do tráfego em uma conexão, bem como determinar os eventos de comunicação que marcam o início e o fim da comunicação. Como resultado, a forma de contabilização das duas grandezas pelo NAS foi compreendida, validando os valores de consumo calculados pelos equipamentos e registrados em bilhetes através do protocolo RADIUS. Conclui-se que tal mecanismo constitui uma resposta satisfatória para o desejo, de algumas operadoras de telecomunicações, de possuir meios de efetuar a cobrança de serviços baseados em uma rede de acesso em banda larga ADSL, tendo em conta o tempo de utilização de uma conexão e a quantidade de *bytes* transferidos durante tal conexão.

PALAVRAS-CHAVE

Banda larga, ADSL, Utilização, Contabilização, *Pay-per-use*, AAA, RADIUS.

RÉSUMÉ

Cette dissertation décrit un mécanisme dont le but est de fournir des informations pour taxer d'une manière alternative à la traditionelle (valeur fixe, independent de la consommation), les services d'accès à l'Internet rapide ADSL (Assymetric Digital Subscriber Line). Deux variables sont considerées pour comptabiliser le coût: la durée temporelle pendant laquelle la connexion a restée active et la quantité d'octets échangés pendant ce temps. En plus, le mécanisme proposé doit être amplifiable d'une manière proportionelle à la croissance des accès concernés. La première partie de la dissertation présente l'architecture habituelle d'un réseau d'accès à l'Internet rapide en technologie ADSL et considère les alternatives aptes à saisir les données de consommation, concluant par choisir une de ces alternatives. L'option choisie fait usage d'un protocole d'authentication, d'autorisation et de taxation appelé RADIUS, et c'est la raison du traitement plus profond donné à ce thème. Cette étude est aussi la base du processus présenté à la suite, constitué à partir des éléments d'un réseau traditionnel ADSL. Toutefois disposés, implémentés e configurés selon un complexe de critères et de techniques ayant pour but de minimiser les chances de perte d'informations rélatives à la consommation. Des essais et des preuves de concept ont été amenés et décrits pour valider de façon pratique certaines des propositions présentées. Un de ces essais a eut l'objectif de découvrir, analyser et documenter la façon selon laquelle l'élement NAS (Network Access Server) du réseau comptabilise, dans une connexion, le transit des octets, et identifier les évènements de communication déterminant le début et la fin d'une connexion. La réussite de ces expérimentations, ayant comme résultat la comprehension des critères de comptabilisation des deux variables, a permis la validation des montants de consommation, calculés par les équipements et enregistrés en des billets par le protocole RADIUS. La dissertation et l'ensemble des essais reálisés permettent conclure que le mécanisme envisagé et proposé convient à certains opérateurs de télécommunications, qui désirent des moyens de se faire payer les services d'Internet rapide ADSL en utilisant comme critères de taxation la durée de la connexion et la quantité d'octets transités au cours de cette connexion.

MOTS-CLÉS

Large bande, ADSL, Utilisation, Comptabilisation, AAA, RADIUS, Payement par utilisation.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

(Esta página foi intencionalmente deixada em branco.)

LISTA DE SIGLAS

AAA	*Authentication, Authorization, Accounting*
AAAA	IPv6 *Address Record Type*
AAL5	*ATM Adaptation Layer 5*
ACK	*Acknowledged*
AC-Name	*Access Concentrator Name*
ADSL	*Asymmetric Digital Subscriber Line*
ADSL2+	*Asymmetric Digital Subscriber Line 2Plus*
ANATEL	Agência Nacional de Telecomunicações
ATM	*Asynchronous Transfer Mode*
ATU-C	*ADSL Transceiver Unit – Central*
ATU-R	*ADSL Transceiver Unit – Remote*
BRAS	*Broadband Remote Access Server*
CHAP	*Challenge Handshake Authentication Protocol*
CLI	*Command Line Interface*
CoA	*Change of Authorization*
CPU	*Central Processing Unit*
DNS	*Domain Name System*
DSL	*Digital Subscriber Line*
DSLAM	*Digital Subscriber Line Access Multiplexer*
GMT	*Greenwich Mean Time*
HDSL	*High-bit-rate Digital Subscriber Line*
HLB	Hora Legal Brasileira
HMAC	*Hash Message Authentication Code*
ICMP	*Internet Control Message Protocol*
IDC	*International Data Corporation*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
IPCP	*Internet Protocol Control Protocol*
IPv6	*Internet Protocol version 6*
ITU	*International Telecommunication Union*
ITU-T	*ITU Telecommunication Standardization Sector*

kbps	*kilobits* por segundo
LCP	*Link Control Protocol*
LMDS	*Local Multipoint Distribution Service*
MAC	*Media Access Control*
Mbps	*megabits* por segundo
MD5	*Message-Digest 5*
MMDS	*Multichannel Multipoint Distribution Service*
NAK	*Not acknowledged*
NAS	*Network Access Server*
NCP	*Network Control Protocol*
NMPEC	*Network Management Private Enterprise Code*
NTP	*Network Time Protocol*
ON	Observatório Nacional
OSI	*Open Systems Interconnection*
PADI	PPPoE *Active Discovery Initiation*
PADO	PPPoE *Active Discovery Offer*
PADR	PPPoE *Active Discovery Request*
PADT	PPPoE *Active Discovery Terminate*
PAP	*Password Authentication Protocol*
PC	*Personal Computer*
PDML	*Packet Details Markup Language*
PEN	*Private Enterprise Number*
PPP	*Point-to-Point Protocol*
PPPoA	*Point-to-Point Protocol over ATM*
PPPoE	*Point-to-Point Protocol over Ethernet*
PPPoED	*Point-to-Point Protocol over Ethernet Discovery*
PPPoEoA	*Point-to-Point Protocol over Ethernet over ATM*
PSI	Provedor de Serviços Internet
PVC	*Permanent Virtual Circuit*
RADIUS	*Remote Authentication Dial-in User Service*
RADSL	*Rate-Adaptive Digital Subscriber Line*
RFC	*Request For Comments*
SCTP	*Stream Control Transfer Protocol*
SDSL	*Symmetric Digital Subscriber Line*

SNMP	*Simple Network Management Protocol*
SNTP	*Simple Network Time Protocol*
STD	*Internet Official Protocol Standard*
TCP	*Transmission Control Protocol*
TCP/IP	*Transmission Control Protocol/Internet Procotol*
ToS	*Type of Service*
TV	Televisão
UDP	*User Datagram Protocol*
USB	*Universal Serial Bus*
VC	*Virtual Circuit*
VDSL	*Very-high-bit-rate Digital Subscriber Line*
VP	*Virtual Path*
VPN	*Virtual Private Network*
VSA	*Vendor-Specific Atribute*
WiFi	*Wireless Fidelity*
WiMAX	*Worldwide Interoperability for Microwave Access*
WLL	*Wireless Local Loop*
WWW	*World Wide Web*
xDSL	Família *Digital Subscriber Line*
XOR	*eXclusive-OR*

(Esta página foi intencionalmente deixada em branco.)

1 - INTRODUÇÃO

Neste trabalho pretende-se apresentar um mecanismo capaz de realizar a contabilização do uso de acessos em banda larga que utilizam tecnologia ADSL (*Asymmetric Digital Subscriber Line*), avaliando o tempo de conexão e a quantidade de *bytes* trafegados durante cada conexão.

A finalidade deste mecanismo é fornecer informações que possibilitem realizar a cobrança pelo uso dos serviços de banda larga de uma forma alternativa à forma tradicional, que é a de valor fixo e independente do consumo. Existe, portanto, a necessidade de que as informações de utilização providas representem com fidelidade o consumo do cliente.

É outro requisito que ele seja ampliável para acompanhar o crescimento do número de acessos em banda larga instalados, de forma gradual e sem necessidade de grandes modificações nos elementos envolvidos.

No decorrer deste trabalho serão apresentadas as alternativas encontradas para realizar a coleta das informações de consumo e, em função das características inerentes a essas alternativas, uma delas será escolhida e investigada com profundidade.

1.1 - CONTEXTUALIZAÇÃO

O título desta dissertação desperta diversos questionamentos. A seguir são apresentadas algumas perguntas e as respectivas respostas, visando a proporcionar um melhor entendimento do que será tratado neste trabalho.

1.1.1 - O que é um "mecanismo funcional"?

"Mecanismo", segundo o dicionário [PRIBERAM2007], é a "combinação de peças, montadas de modo a permitir um funcionamento conjunto". [ULTRAL2007] define como "os aspectos técnicos de fazer alguma coisa".

O senso comum sugere que "funcional" é algo que funciona. Complementa [PRIBERAM2007], que funcional é algo prático, que se usa facilmente, que está pronto para entrar em funcionamento.

Juntando os dois termos, "mecanismo funcional" pode ser definido como uma combinação de peças, montadas objetivando o funcionamento conjunto, de forma prática e de uso fácil.

1.1.2 - O que é "escalável"?

"Escalável" é um jargão técnico para estabelecer que um sistema pode funcionar tanto em uma estrutura pequena quanto em uma estrutura grande, mantendo, no pior dos casos, uma proporcionalidade entre a capacidade de atendimento e os recursos necessários para realizar este atendimento.

Segundo [SANTOS2004], "escalabilidade" é a capacidade de um sistema crescer para acomodar cargas maiores, onde a carga pode ser medida por diferentes unidades: quantidade de transações por intervalo de tempo, quantidade de usuários concorrentes, volume de dados a ser manipulado, etc.

Em geral existe uma expectativa de que quanto maior for a capacidade de atendimento maior será o resultado da relação entre a capacidade de atendimento e o volume de recursos necessários para este atendimento, trazendo o chamado "ganho de escala".

Assim, "escalável" é um atributo com duas características principais:

- Funciona de forma similar em ambientes de diferentes dimensões.

- Os recursos necessários para proporcionar o crescimento de capacidade de atendimento, no pior dos casos, acompanham de forma aproximadamente linear tal crescimento.

1.1.3 - O que é "contabilização"?

Contabilização vem de contabilizar, ou seja, de registrar apropriadamente uma determinada operação. No contexto desta dissertação, contabilização significa registrar corretamente informações referentes à utilização de um serviço.

1.1.4 - O que são "serviços residenciais"?

Para este trabalho, a expressão "serviços residenciais" refere-se ao conjunto de serviços de acesso à Internet provido por uma operadora de telecomunicações ao público formado exclusivamente por pessoas físicas.

1.1.5 - O que é "banda larga"?

Em recente pesquisa realizada pela IDC Brasil [IDC2007], o termo "banda larga" foi definido como qualquer conexão permanente com a Internet (*always on*) de velocidade igual ou superior a 128 kbps, tanto no sentido do assinante para a rede (*updload*) quanto no sentido da rede para o assinante (*download*). O mesmo estudo menciona como tecnologias de "banda larga" a TV a cabo, o ADSL, o xDSL (família *Digital Subscriber Line*), o WLL (*Wireless Local Loop)*, o LMDS (*Local Multipoint Distribution Service*), o MMDS (*Multichannel Multipoint Distribution Service*), o WiMAX (*Worldwide Interoperability for Microwave Access*), o acesso através de satélite e também as linhas dedicadas à Internet.

1.1.6 - O que é "ADSL"?

ADSL é uma tecnologia de acesso em banda larga que utiliza o par de cobre da linha telefônica convencional para transmitir dados em alta velocidade. Maiores detalhes poderão ser encontrados na seção 2.1.

1.1.7 - O que é "tempo"?

Dos conceitos da física o tempo permite ordenar eventos e, com o uso conjunto de coordenadas de espaço, ele possibilita a localização completa de tais eventos. Para este trabalho, estamos interessados no intervalo de tempo entre os eventos de estabelecimento e de término de uma determinada conexão à Internet, o qual denominaremos de "duração da conexão".

É apropriado, neste momento, explicar o conflito que existe entre a "conexão permanente" que faz parte da definição de um acesso em banda larga e o recém apresentado conceito de "duração da conexão".

De uma forma geral, o termo "conexão permanente" refere-se à disponibilidade habitual dos recursos físicos necessários para o estabelecimento de uma conexão lógica e que, em geral, está alocado unicamente a um cliente. No caso de um acesso ADSL, existe um conjunto de elementos físicos constituído por modems, uma linha física composta por um par de fios de cobre e outros equipamentos eletrônicos que resulta em um circuito permanente entre o usuário e o provedor do acesso ADSL.

O conceito de "duração da conexão", por outro lado, está relacionado com a comunicação lógica que é estabelecida usando um determinado circuito, seja ele permanente ou não. Para um acesso em banda larga usando tecnologia ADSL, em geral, a conexão lógica – também chamada de "sessão" –, está relacionada ao estabelecimento de um protocolo de comunicações chamado PPP (*Point-to-Point Protocol*) entre o equipamento do usuário e o equipamento da operadora de telecomunicações.

1.1.8 - O que é "volume"?

Volume refere-se à soma da quantidade de *bytes* trafegados em um enlace de dados em cada um dos dois sentidos: do cliente para a rede, chamado de tráfego de subida ou de *upload* e da rede para o cliente, conhecido por tráfego de descida ou de *download*.

1.1.9 - Que aspectos legais estão envolvidos no provimento de acesso à Internet utilizando banda larga baseada em tecnologia ADSL no Brasil?

Segundo [ANATEL], o provimento de conexão à Internet através de ADSL, bem como por acesso discado, radiofreqüência ou *cable* modem, deve estar associado a um serviço de telecomunicações devidamente regulamentado pela ANATEL (Agência Nacional de Telecomunicações).

Os serviços de telecomunicações que dão suporte ao provimento de conexão à Internet como o acesso ADSL só deverão ser explorados por empresas que possuam concessão, permissão ou autorização emitida pela ANATEL.

Para um indivíduo contratar um serviço de acesso à Internet através de ADSL, existe então a necessidade da contratação de dois serviços:

1. o de provimento de conexão à Internet, que é um serviço de valor adicionado fornecido por um provedor de serviços Internet (PSI) previamente habilitado pelo prestador de serviços de telecomunicações, e
2. o de acesso ADSL, fornecido pelo prestador de serviços de telecomunicações.

O uso da tecnologia ADSL para o provimento de acesso à Internet é regido pelo Regulamento do Serviço de Comunicação Multimídia ([REGSCM]), anexo à Resolução número 272, de 9 de agosto de 2001, da ANATEL ([RES272]).

1.1.10 - Qual o interesse em realizar cobrança por volume e tempo de utilização?

Segundo [KASHIF2004], o mercado de banda larga pode ser dividido em dois grandes grupos: o corporativo e o residencial. O mercado residencial pode ser usualmente dividido em três subgrupos: o de uso pesado, uso médio e uso leve.

Na análise conduzida por [KASHIF2004], o grupo de uso pesado é o principal consumidor de banda de conexão internacional e, como forma de minimizar o impacto causado pelo comportamento desse grupo, as operadoras podem introduzir mecanismos de cobrança baseados em tempo de conexão ou volume de dados trafegados. Alternativa proposta por

esse autor é a de ofertar pacotes de tempo de conexão ou de volume de transferência adicional como forma de obter receita complementar.

Figura 1.1: Página da Brasil Telecom na Internet para o produto Turbo Lite.
(Fonte: [MEGATURBO])

A cobrança baseada em tempo de conexão ou volume de tráfego abre também a possibilidade de criar pacotes de serviços com limitação de banda e tempo de conexão, dentro do conceito "pague pelo uso" (*pay-per-use*), visando a criar um serviço de preço mais baixo para atrair novos consumidores e popularizar a banda larga. Essas foram as

propostas do serviço da operadora de telecomunicações Brasil Telecom denominado "Turbo Lite", conforme [BRT2003] e [SANTIAGO2003].

A implementação do produto "Turbo Lite" na rede da operadora Brasil Telecom, porém, apresentou diversas dificuldades técnicas e operacionais. Após esforço em corrigir os problemas encontrados e superar a rejeição, por parte dos clientes, da introdução de uma técnica de controle de acesso conhecida como portal cativo (*captive portal*), a venda desse serviço foi interrompida. Apesar disso, o serviço consta ainda no portfólio da operadora Brasil Telecom, conforme se pode observar na Figura 1.1.

1.2 - DEFINIÇÃO DO PROBLEMA

Existem no mundo algumas operadoras de telecomunicações que oferecem serviços de acesso à Internet cobrados em razão do consumo. Exemplo é a empresa canadense *Rogers Communications Inc*, que, através do seu serviço "*Rogers Hi-Speed Internet*" ([ROGERS2008]), cobra o acesso à Internet em razão da quantidade de conteúdo originado e destinado ao computador do cliente.

A empresa americana *Time Warner Inc*., que fornece acesso à Internet através da sua estrutura de TV a cabo, realiza, desde junho de 2008, testes em pequena escala para a introdução da cobrança em função do consumo de recursos pelos seus clientes. Segundo [SVENSSON2008], uma das justificativas apresentadas pela empresa *Time Warner Inc.* para investir em uma estrutura de medição é que a metade dos recursos da estrutura de oferta do serviço é consumida por apenas 5% dos seus clientes e, assim, a adoção desse modelo de cobrança trará uma maneira mais justa de suporte ao investimento que é necessário realizar nessa estrutura.

Aponta [DVORAK2008] que, mesmo que mecanismos para realizar a medição do consumo de Internet ainda não estejam desenvolvidos, não existe maneira de o modelo de negócio onde o acesso do cliente é realizado sem quaisquer restrições durar muito mais tempo. Para ele, a Internet é considerada um recurso tal como a água e a energia elétrica, devendo, portanto, ser medida e cobrada da mesma maneira: pelo seu uso. Apresenta ainda

oito razões pelas quais o acesso à Internet deve ser medido e os benefícios que tal modelo de negócio traz.

A existência do interesse em realizar a cobrança de acordo com a utilização dos acessos à Internet, por parte das operadoras de telecomunicações, combinada com a inexistência de mecanismos desenvolvidos para realizar a medição do consumo estabelece o problema cuja solução este trabalho visa a tratar. Em especial, o empenho é determinar o consumo de serviços residenciais que são fornecidos através de acessos em banda larga que utilizam tecnologia ADSL.

Outro aspecto importante do problema é a chamada "escalabilidade" e a solução apresentada o tem em conta, pois a implementação do mecanismo deve acompanhar, de forma proporcional, o crescimento da quantidade de acessos ADSL na planta da operadora. Em outras palavras, a solução apresentada não deve impor a necessidade de grandes modificações na rede em função de crescimento de acessos ADSL, exceto pelos recursos necessários para proporcionar a capacidade suplementar necessária ao próprio sistema em decorrência do crescimento da rede.

1.3 - JUSTIFICATIVA E OBJETIVOS

A principal justificativa para o desenvolvimento deste trabalho é a existência do interesse, por parte de operadoras de telecomunicações, em cobrar acessos em banda larga de uma forma diferente da praticada atualmente, que é a de um valor fixo mensal, independente da utilização. Apesar de não ser um tema inédito, não foram encontrados muitos estudos nesta área específica, principalmente, em situações similares ao cenário brasileiro de provimento de conexões em banda larga utilizando tecnologia ADSL.

Entende-se que o resultado deste trabalho, ao ser adotado, poderá proporcionar ao cliente de um serviço de conexão à Internet através de banda larga a oportunidade de uma cobrança mais adequada ao seu perfil de uso.

O objetivo geral deste trabalho é, portanto, determinar um mecanismo destinado a viabilizar a cobrança pela utilização de acessos ADSL residenciais. Tal mecanismo permitiria a cobrança através da avaliação de duas grandezas relacionadas à utilização de

um acesso em banda larga ADSL: o tempo de duração da conexão e o consumo de banda, em termos de *bytes* trafegados. Adicionalmente, esse mecanismo deve ser passível de ampliação em sua capacidade, de forma a acompanhar o crescimento do número de acessos ADSL residenciais da operadora.

Constituem os objetivos específicos:

a) estudar a arquitetura usual de uma rede de acesso ADSL, para compreender as relações entre os seus elementos constituintes;
b) localizar e avaliar alternativas para a coleta de informações de utilização;
c) escolher uma alternativa e estudá-la com a profundidade necessária;
d) propor o mecanismo, fundamentado no estudo realizado;
e) elencar os principais parâmetros de configuração do mecanismo e introduzir estratégias buscando a melhoria do desempenho do sistema;
f) realizar os experimentos necessários para validar o mecanismo apresentado e as estratégias propostas.

1.4 - HIPÓTESES

A hipótese primária é que o problema possa ser resolvido através da utilização de um esquema de geração, transmissão e armazenamento de bilhetes que permita a contabilização das informações de utilização dos acessos ADSL.

Outra hipótese é que a solução encontrada possuirá capacidade de crescer, acompanhando o crescimento da rede de acesso ADSL da operadora.

1.5 - LIMITAÇÕES

Limitando-se, este trabalho, à apresentação de um mecanismo funcional que permita a realização da contabilização de utilização, por tempo ou por volume de tráfego transferido, de acessos em banda larga sobre tecnologia ADSL, não avalia ele, portanto, as situações relacionadas ao uso de outros tipos de acesso físico, como acessos WiFi ou por meio de TV a cabo, apesar de que, eventualmente, o seu resultado possa ser adaptado a tais situações.

Não versa também sobre o problema de identificação inequívoca do usuário do acesso ADSL, o qual, para todos os efeitos, é considerado resolvido. Informações sobre esse tópico podem ser obtidas em [HENZ2008].

Não aborda sistemas de mediação de dados, de faturamento, de geração de extratos de uso ou de portal de auto-aprovisionamento e de gerenciamento de serviços.

1.6 - ESTRUTURA DA DISSERTAÇÃO

O conteúdo deste trabalho divide-se em seis capítulos, que podem desta forma ser resumidos:

- Capítulo 1: neste capítulo é realizada a introdução ao objeto de pesquisa, apresentando o problema motivador do projeto, a justificativa para o seu desenvolvimento e as limitações envolvidas.
- Capítulo 2: nele é abordada a fundamentação teórica associada ao tema, apresentando a arquitetura habitual das redes de acesso em banda larga e detalhando os blocos funcionais envolvidos. São apresentadas também as alternativas avaliadas para a solução do problema.
- Capítulo 3: neste capítulo, são apresentados os conceitos de Autenticação, Autorização e Bilhetagem, as relações destes processos com uma conexão ADSL e detalhado o protocolo RADIUS.
- Capítulo 4: o capítulo 4 apresenta a solução proposta para realizar a contabilização por tempo e por volume de tráfego de acessos em banda larga residenciais baseados em tecnologia ADSL.
- Capítulo 5: nele são apresentados os experimentos realizados visando a consubstanciar a solução proposta no capítulo 4, bem como os resultados obtidos.
- Capítulo 6: no capítulo 6 são apresentadas as conclusões deste trabalho e as sugestões para trabalhos futuros nesta área.

2 - REFERENCIAL TEÓRICO

Neste capítulo é abordada a fundamentação teórica associada ao objeto de pesquisa, apresentando a arquitetura usual das redes de acesso em banda larga e detalhando os elementos funcionais envolvidos. São apresentadas também as alternativas avaliadas para a solução do problema.

2.1 - ARQUITETURA DE REDE DE ACESSO ADSL

Nesta parte são apresentados os principais elementos envolvidos no provimento de serviços baseados em acesso ADSL. Para uma melhor compreensão, os elementos foram divididos por ambientes: cliente, operadora e provedor de acesso à Internet, podendo serem vistos na Figura 2.1.

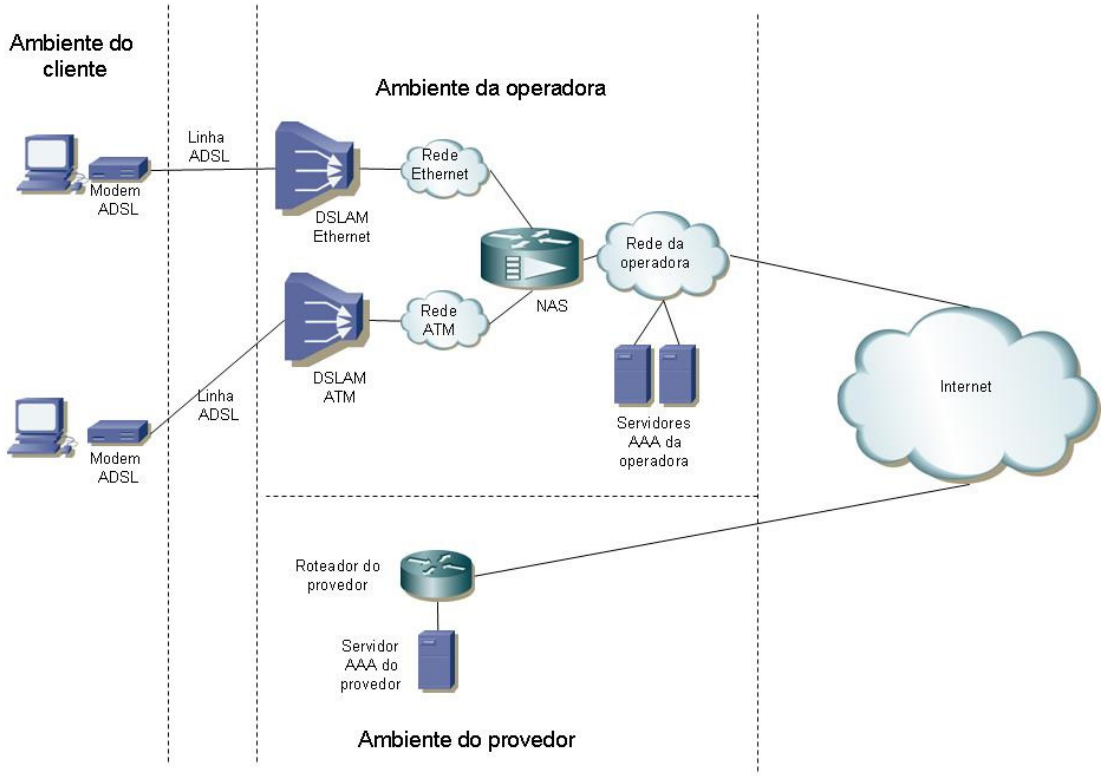

Figura 2.1: Elementos principais da arquitetura de rede ADSL

2.1.1 - Linha ADSL (*Asymmetric Digital Subscriber Line*)

A linha digital de assinante (*Digital Subscriber Line*, DSL) é uma tecnologia de modems que utiliza o par trançado das linhas telefônicas convencionais para transportar dados em banda larga.

O termo xDSL é utilizado para descrever uma família de formas de DSL, tais como ADSL, SDSL (*Symmetric Digital Subscriber Line*), HDSL (*High-bit-rate Digital Subscriber Line*), RADSL (*Rate-Adaptive Digital Subscriber Line*) e VDSL (*Very-high-bit-rate Digital Subscriber Line*). Todas essas formas possuem o mesmo objetivo: entregar acessos com elevada disponibilidade de banda a localidades dispersas com a menor necessidade de modificações na infra-estrutura das operadoras de telecomunicações.

Os serviços xDSL são sempre dedicados, ponto a ponto entre a central telefônica da operadora de telecomunicações e o ambiente do cliente, utilizando o par trançado convencional existente, também chamado de "última milha". O tipo de acesso xDSL que é objeto deste trabalho é o ADSL, que significa *Asymmetric Digital Subscriber Line*, ou Linha Digital do Assinante Assimétrica.

Como o próprio nome sugere, o acesso ADSL possui uma assimetria: ele permite uma banda maior para a transmissão de dados no sentido da rede para o assinante (*downstream*) do que a originada pelo assinante em direção à rede (*upstream*). Esta assimetria torna a utilização do ADSL ideal para o acesso à Internet, onde habitualmente a quantidade de dados destinada ao assinante é muito superior à originada por ele.

Com essa tecnologia, dependendo da qualidade da linha física (par trançado metálico), é possível atingir taxas até 8Mbps no sentido da rede para o assinante e até 640kbps do assinante para a rede, ampliando a capacidade de transmissão do acesso existente em mais de 50 vezes, sem realizar qualquer tipo de alteração física na estrutura de rede metálica. O padrão ADSL mais recente, chamado ADSL2+ pode alcançar até 24Mbps, dependendo principalmente do comprimento da rede metálica entre o equipamento da central telefônica e o do assinante.

2.1.2 - Modem ADSL

O modem ADSL é a denominação comum para o equipamento de linha digital do assinante assimétrica que é instalado no ambiente do cliente. As características técnicas e funcionais deste equipamento são definidas na norma [ITU992.1], a qual o denomina de ATU-R (*ADSL Transceiver Unit – Remote*).

Geralmente, o modem ADSL possui uma interface de rede *Ethernet* ou USB, através da qual é ligado ao computador do cliente, e uma interface analógica para conexão à linha telefônica.

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 NAS (*Network 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 2.2 apresenta as conexões lógicas para as duas possibilidades de operação.

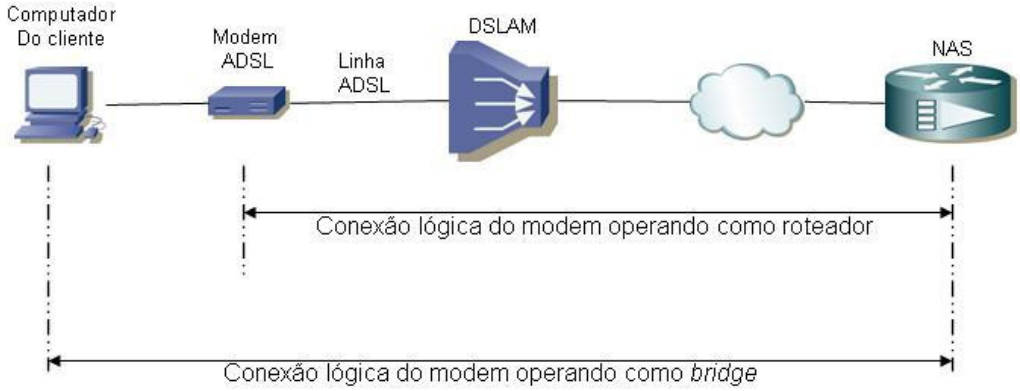

Figura 2.2: Conexões lógicas para as duas possibilidades de operação do modem ADSL

2.1.3 - DSLAM (*Digital Subscriber Line Access Multiplexer*)

O DSLAM (*Digital Subscriber Line Access Multiplexer*) é o equipamento que agrupa os modems ADSL, denominados ATU-C (*ADSL Transceiver Unit – Central*) pela norma [ITU992.1], no ambiente da operadora. A Figura 2.3 ilustra este conceito.

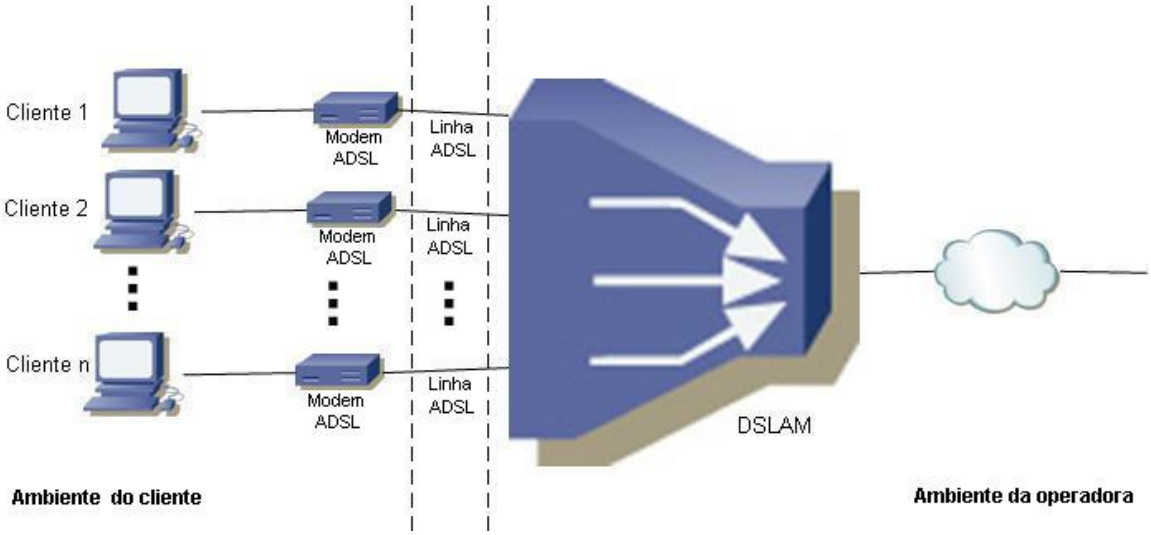

Figura 2.3: O DSLAM agrupa os modems do lado da operadora.

O DSLAM é geralmente modular, ou seja, composto de uma base (*chassis*) à qual podem ser adicionadas placas com certa quantidade de modems ATU-C. Assim, é possível ter configurações pequenas, com poucas portas de conexão, e configurações muito grandes, com centenas de portas, possibilitando à operadora atender às mais diversas demandas pelo serviço.

A Figura 2.4 apresenta dois modelos de DSLAMs fabricados pela *Huawei*, empresa chinesa fabricante também de diversos outros tipos de elementos de rede. O DSLAM da esquerda é o modelo 5303, com capacidade de até 144 portas. O DSLAM da direita é o modelo 5300, que pode atingir 672 portas.

Figura 2.4: Dois modelos de DSLAM fabricados pela *Huawei*

Existem basicamente dois tipos desse equipamento, o DSLAM ATM (*Asyncronous Transfer Mode*) e o DSLAM *Ethernet*. A diferença principal entre um e outro, e que determina a sua denominação, está relacionada com a sua interface de conexão ao NAS (*Network Access Server*): a do primeiro é ATM e a do segundo é *Ethernet*.

2.1.4 - NAS (*Network Access Server*)

O NAS (*Network Access Server*) é um tipo de equipamento de rede cuja finalidade, dentro de uma rede de acesso ADSL, é estabelecer a conexão lógica entre o modem (ou o computador do cliente) com a rede da operadora. É também conhecido por BRAS (*Broadband Remote Access Server*), por terminador e por agregador; todos esses termos são intercambiáveis entre si.

É comum estar dito na documentação relativa a esse tipo de equipamento que ele possui um lado voltado ao assinante e outro lado voltado à rede; o lado do assinante refere-se às interfaces utilizadas para conectar o NAS às redes ATM ou *Ethernet* onde se encontram os DSLAMs. O lado da rede, por sua vez, faz alusão à conexão com os demais elementos que compõem a rede de comunicação de dados da operadora de telecomunicações.

Figura 2.5: Agregadores das empresas *Juniper Networks* e *Cisco Systems*.

Existem agregadores de diversas capacidades, variando de poucas centenas de acessos a dezenas de milhares de acessos. O NAS apresentado na Figura 2.5, à esquerda, da fabricante *Juniper Networks*, é o modelo ERX 1440, que pode atender a cerca de 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 atestadas por [MIERCOM2004].

2.1.5 - Servidores AAA (*Authentication*, *Authorization*, *Accounting*)

Esses elementos e suas finalidades serão detalhados no capítulo 3, mas de uma forma sucinta, 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), 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.

2.2 - COLETA DE INFORMAÇÕES DE UTILIZAÇÃO

Para possibilitar a cobrança da utilização de um serviço é necessário coletar as informações sobre a utilização desse serviço por seu usuário. Uma das primeiras definições de um sistema de cobrança é a do local onde será feita a medição da grandeza pela qual o serviço será cobrado.

De acordo com [LITTLEJOHN2005], medir do lado mais próximo ao usuário permite um laço mais forte entre a autenticação e a contabilização. Ou, em outras palavras, tanto é mais fácil associar o usuário à informação de utilização do serviço quanto mais próxima desse usuário a medição for realizada. Por outro lado, estando a medição mais próxima do usuário, quanto mais usuários existirem maior deve ser o sistema que realiza a medição.

Considerando a arquitetura básica de uma rede ADSL apresentada anteriormente, a seguir são enumeradas formas de realizar a coleta de informações de utilização, mostrando os prós e contras de cada alternativa.

2.2.1 - SNMP (*Simple Network Management Protocol*)

O SNMP (*Simple Network Management Protocol*), segundo [RFC1157], é um protocolo simples, através do qual a informação de gerenciamento para um elemento de rede pode ser inspecionada ou ser alterada por usuários logicamente remotos.

Esse protocolo possui a vantagem de ser largamente suportado pelos elementos de rede, e pode ser utilizado para a coleta de informações de tráfego de interfaces correspondentes aos usuários do NAS, porém algumas características, que serão apresentadas a seguir, não o favorecem para fins de cobrança por tempo de uso ou por volume de tráfego.

A primeira característica é que, nos dados coletados através de SNMP, não existe vinculação direta entre uma identificação do usuário e a interface para a qual está sendo feita a coleta. Essa identificação e associação devem ser feitas por alguma outra forma externa ao SNMP, o que pode ocasionar um descasamento entre a informação de utilização e o real utilizador.

Outra característica é que cada interface do NAS possui um índice, que é a referência pela qual é feita a coleta de informações de utilização. Os índices de interface não são fixos, pois as interfaces de usuário no NAS são dinâmicas, criadas no momento do estabelecimento da conexão dos usuários e encerradas no momento da desconexão. Mesmo que uma seqüência de interfaces pudesse ser determinada, a reinicialização do NAS ou a substituição de um componente do equipamento poderia alterar a ordem das interfaces.

A quantidade de interfaces de usuários em um NAS é da ordem de dezenas de milhares. A coleta SNMP, em determinadas circunstâncias, pode ocasionar alto consumo de recursos do processador (CPU - *Central Processing Unit*) do elemento de rede, prejudicando seu funcionamento. Conforme [CISCOa, p. 1],

> "*Sob certas circunstâncias, o processo IP-SNMP pode consumir quase todos os recursos de CPU. Este processo pode prejudicar a execução de outros processos e causar um comportamento errático no equipamento. O sintoma mais óbvio é a perda de conexões TCP para o equipamento. A causa mais provável para este problema é o envio de uma grande quantidade de requisições SNMP para o equipamento em um curto período de tempo, o que causa a recuperação de grandes quantidades de dados.*"

Por fim, o SNMP apenas informa o tráfego em um canal ou enlace e este tráfego é sempre crescente, deixando para o sistema de contabilização a tarefa de alocar corretamente o consumo de recursos ao usuário e administrar o chamado "estouro de contadores".

A decorrência desse conjunto de características da utilização do SNMP para a contabilização de utilização é que seu uso para esta finalidade acaba por ser restrito a situações específicas, o que condiz com a constatação de [LITTLEJOHN2005] sobre a raridade de encontrar situações onde a medição de tráfego é feita através de SNMP.

Maiores informações sobre o protocolo SNMP podem ser obtidas em [RFC1157] e [PERKINS1997].

2.2.2 - NETFLOW

O *NetFlow* é uma ferramenta para a coleta de informações detalhadas de tráfego desenvolvida pela empresa *Cisco Systems*. Segundo [LITTLEJOHN2005], o protocolo *Netflow* tem sido adotado como um padrão *de facto* para a coleta de informações detalhadas de tráfego e vários outros fabricantes tem adicionado alguma forma de suporte *Netflow* em seus dispositivos. O *J-Flow*, por exemplo, é o protocolo desenvolvido pela empresa *Juniper Networks* para a mesma finalidade.

Nos dispositivos de rede que possuem suporte ao *Netflow*, é possível, então, realizar a coleta de informações sobre os fluxos IP. Fluxo, segundo [CISCOb], é uma seqüência unidirecional de pacotes que têm algumas propriedades comuns e que passam através de um dispositivo de rede. Essas propriedades comuns são: endereço IP e porta de origem, endereço IP e porta de destino, protocolo de camada 3 do modelo de referência OSI (*Open Systems Interconnection*) utilizado, *byte* ToS (*Type of Service*) e a interface lógica de entrada no equipamento.

Apesar do grau elevado de detalhamento que o *Netflow* possibilita obter sobre o tráfego, seu uso para contabilizar a utilização de serviços por um determinado usuário não se mostra adequado, pelas razões apresentadas a seguir.

O *Netflow* não possui nenhum componente de identificação de usuário, de forma que, em ambientes com endereçamento IP dinâmico – que é o caso do ADSL – , não existe maneira de associar um determinado fluxo a um usuário sem a utilização de alguma ferramenta adicional.

Por padrão, o *Netflow* consolida as informações de tráfego por intervalos de 15 minutos. Mesmo que uma ferramenta adicional seja implementada para permitir a associação entre fluxos e usuários, caso um mesmo endereço IP tenha sido utilizado por mais de um cliente final dentro deste intervalo de tempo, não há como determinar o volume de tráfego utilizado por cada um destes clientes.

Para minimizar o efeito causado pelo intervalo de coleta padrão, existe a possibilidade de reduzir este intervalo de consolidação visando a melhorar o detalhamento das informações de utilização. Adotar essa redução, porém, provocará um maior consumo de recursos de processamento e de memória do NAS, bem como de todo o sistema de coleta e de processamento das informações.

No mesmo sentido, alerta [LITTLEJOHN2005] que o grau de detalhamento do *Netflow* impõe desafios significativos quando utilizado em redes grandes, em função do consumo de recursos no trabalho de agregação das informações de utilização coletadas.

Em função das situações apresentadas, a utilização do *Netflow* como ferramenta para obtenção de informações de utilização dos serviços baseados em ADSL é pouco recomendável.

Maiores informações sobre o *Netflow* podem ser obtidas em [CISCOc] e [RFC3954].

2.2.3 - CLI (*Command Line Interface*)

Segundo [AHN2006], a CLI (*Command Line Interface*) – interface de linha de comando – é um método para interagir com um sistema computacional onde o operador do sistema provê a entrada de comandos através da digitação desses comandos em um teclado e o sistema retorna o resultado através de texto em um monitor de computador.

O NAS possui um tipo de sistema operacional nele instalado, e, em geral, é possível coletar informações sobre acessos ativos de clientes realizando consultas através de sua interface de linha de comando.

Alguns desafios surgem, porém, na utilização dessa alternativa. Conexões de usuários são estabelecidas e encerradas sem aviso prévio. Assim, para determinar quais conexões são novas, quais já existiam e quais foram encerradas, é necessário comparar os resultados entre consultas.

Supondo que fosse possível, através de uma única consulta, recuperar todas as informações necessárias sobre um determinado acesso, e considerando que cada NAS possui dezenas de milhares de acessos, seriam necessárias dezenas de milhares de consultas para saber o estado das conexões. É necessário fazer isso para todas as conexões, pois não é possível saber antecipadamente quais conexões serão encerradas e porque, uma vez encerradas, todos os dados relativos a estas conexões são perdidos.

A interface de linha de comando foi criada para realizar a configuração e a manutenção do equipamento NAS e não para coletar estatísticas em volume elevado; em decorrência, a quantidade de recursos de processamento a ela alocados é habitualmente pequena e pode não dar vazão ao montante de dados envolvidos no processo de coleta.

Não se mostra, portanto, uma alternativa viável para realizar a coleta de informações de utilização.

2.2.4 - Utilização de *probes*

A *probe* é um elemento de rede destinado a monitorar o tráfego que por ele passar. Para avaliação do tráfego originado por usuários ADSL, deve ser inserida na conexão do NAS com a rede da operadora (*uplink*).

Uma vez que monitora fluxos de dados, essa alternativa para coleta de informações de consumo de serviços possui desafios similares ao uso do *Netflow*, porém com um grau a mais de complexidade: por razões de disponibilidade, habitualmente cada NAS possui pelo

menos duas conexões de *uplink* com a rede. Como cada conexão precisa ter a sua própria *probe* e o tráfego de, e para, um determinado cliente pode passar por qualquer uma das duas conexões, o resultado é um trabalho de consolidação de dados bastante complexo, e que deve ser feito para cada usuário.

A Figura 2.6 ilustra a situação descrita acima: enquanto um coletor *Netflow* busca informações em um só elemento (o NAS), o coletor de informações de *probes* deve fazer o mesmo para dois elementos e ainda realizar o trabalho de consolidação.
Considerando a complexidade da solução e o custo que se originaria na grande quantidade de equipamentos que precisaria ser adquirida para a sua implantação, o uso de *probes* não constitui alternativa atraente para a avaliação de consumo de serviços ADSL.

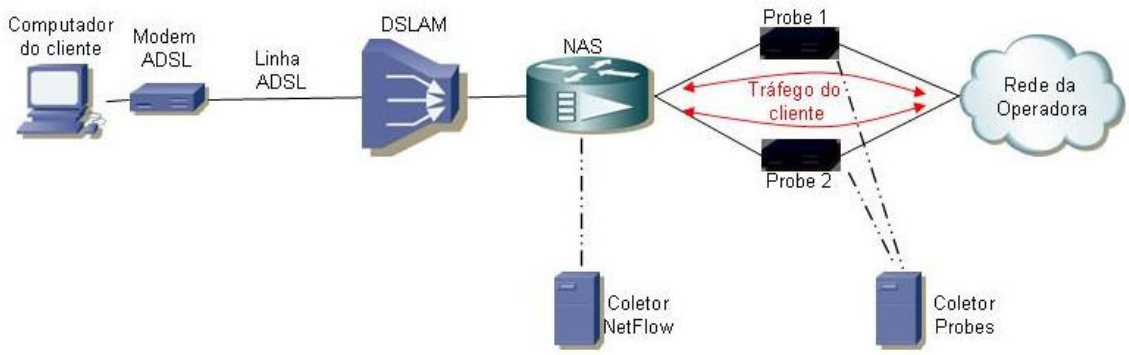

Figura 2.6: Diagrama de rede comparativo entre o uso de *Netflow* e de *Probes*.

2.2.5 - Servidores AAA

Conforme visto anteriormente, a arquitetura de rede para o serviço ADSL possui, como um de seus elementos constituintes, um conjunto de servidores AAA. No contexto desta dissertação, "AAA" ou "*Triple-A*" é a sigla em inglês para três palavras: *Authentication*, *Authorization*, *Accounting*, que, em português, são habitualmente traduzidas como "Autenticação", "Autorização" e "Contabilização", respectivamente.

Alternativamente, o termo *Accounting* pode também ser traduzido como "Bilhetagem", dado que o termo tradicional para o registro de utilização de um serviço de uma operadora

de telecomunicações é “bilhete”; ao longo deste texto, as duas formas - contabilização e bilhetagem - serão utilizadas de forma indistinta.

Estes servidores AAA utilizam o protocolo RADIUS (*Remote Authentication Dial-in User Service*) para realizar a autenticação, autorização e bilhetagem de acessos ADSL. Segundo [LITTLEJOHN2005], o uso do RADIUS para a contabilização de tráfego possui algumas vantagens, enumerando entre elas a simplicidade, o grande número de usuários do protocolo e a relação existente entre a autenticação e a bilhetagem.

Comenta esse mesmo autor que a principal desvantagem é que o RADIUS apresenta apenas o valor total do tráfego da conexão do usuário, porém, nas suas próprias palavras [LITTLEJOHN2005, p. 2]:

> “Se isso é tudo que você precisa, então RADIUS é bem apropriado para as suas necessidades”.

Alerta, porém, que o RADIUS pode não ser adequado para conexões de longa duração como as de sistemas em banda larga em função de alguns deles não tratarem adequadamente bilhetes intermediários.

Uma vez que a estrutura de AAA é inerente à arquitetura de banda larga, e consideradas as características descritas acima, a utilização dos servidores AAA para a obtenção das informações de utilização aparenta ser, dentre as localizadas, a alternativa mais promissora para realizar a contabilização de uso de serviços residenciais em rede de acesso em banda larga utilizando tecnologia ADSL. Pode-se concluir, porém, que é necessária a busca por soluções escaláveis que tirem proveito das medições disponibilizadas, bem como observar as condições apropriadas para a geração e o tratamento de bilhetes intermediários.

3 - OS TRÊS “A”S:

Ao longo deste capítulo, o conceito de cada um dos “A”s que compõem a sigla AAA – Autenticação, Autorização e Bilhetagem – será explorado, detalhando a sua importância e situando a sua utilização em uma rede de acesso em banda larga baseada em tecnologia ADSL. Em especial, diversos aspectos relacionados com a Autenticação e a Bilhetagem serão apresentados.

Neste capítulo também será examinado o protocolo de AAA chamado RADIUS, descrevendo as suas características relevantes, as suas diferentes mensagens, o conceito de atributos, o formato dos pacotes de dados e o seu funcionamento diante do uso de diferentes mecanismos de autenticação presentes na rede ADSL.

3.1 - O QUE É “AAA”?

Conforme apresentado no capítulo anterior, “AAA” é a sigla em inglês para *Authentication*, *Authorization*, *Accounting*, que podemos traduzir para a língua portuguesa por Autenticação, Autorização e Bilhetagem. Segundo [NAKHJIRI2005], autenticação, autorização e bilhetagem são três importantes blocos utilizados na construção de uma arquitetura que auxilia na proteção da rede de uma operadora de telecomunicações contra fraudes, ataques, gerenciamento inapropriado de recursos e perda de receita.

A enciclopédia eletrônica [WHATIS] apresenta AAA como sendo uma estrutura (*framework*) para, de forma inteligente, controlar o acesso a recursos computacionais, aplicando políticas, auditando a utilização e provendo a informação necessária para cobrar pelos serviços.

Assim, AAA consiste genericamente em um sistema que permite autenticar um usuário, autorizar a utilização de algum serviço por esse usuário após a autenticação e gerar um registro de utilização, para esse usuário, pelo uso de tal serviço. A seguir será apresentado cada um dos termos componentes da sigla AAA.

3.1.1 - O primeiro “A”: Autenticação

O senso comum sugere que algo é autêntico quando é aceito como verdade ou fato, por corresponder a um elemento que não é falso, tal como uma mera imitação. Autenticar, segundo o dicionário [FERREIRA2007], é o processo de reconhecer como verdadeiro.

A preocupação com a autenticidade é antiga. Na idade média, os documentos oficiais ingleses eram marcados com o uso do *“Great Seal of England”*, para que quem recebesse o documento pudesse reconhecê-lo como verdadeiro ou não. Tal selo era guardado por uma pessoa de confiança, que era o *Lord Chancellor* e, mais tarde, o *Lord Keeper of the Great Seal*. A cada novo rei, um novo selo era feito e o antigo, ao menos teoricamente, era destruído. Ainda hoje é assim com os Papas.

Naquela época, a mensagem poderia ser carregada por qualquer mensageiro, visto que a identidade do mensageiro não era considerada importante, apenas a do emissor do documento. O senhor local reconheceria o selo real que fecha (“sela”) a mensagem e isso bastaria para acreditar na autenticidade da mensagem e atender à solicitação real.

Atualmente, provar a autenticidade é ainda importante, envolvendo, porém desafios mais complexos que a mera apresentação de um selo real. O processo de autenticação é, conforme [NAKHJIRI2005], composto de dois atos: o de provar a autenticidade da informação que é enviada ou armazenada e o de provar a autenticidade da informação que está sendo recebida ou recuperada.

Um exemplo deste processo é o registro de firma em qualquer cartório. O interessado em realizar o registro informa seus dados de qualificação e apresenta, como forma de provar a autenticidade da informação enviada, um documento oficial de identidade. O notário, por sua vez, necessita comprovar que a informação recebida é verdadeira, o que é feito através da análise do documento oficial de identidade. Se tal documento é verdadeiro e corresponde ao interessado, a informação que é recebida é, por conseqüência, considerada verdadeira.

O exemplo acima também atende à definição de autenticação de [HASSEL2002], onde autenticação é o processo de verificação da identidade declarada por uma pessoa ou máquina.

A forma mais comum de autenticação em meio eletrônico é a combinação da utilização de uma identificação de usuário, também conhecida como "nome do usuário" ou *username* e de uma senha, cujo conhecimento significa para o sistema que o usuário efetivamente é quem alega ser, ou seja, é autêntico.

3.1.1.1 - Tipos de autenticação

A seguir são apresentados os tipos mais comuns de autenticação: autenticação de cliente, autenticação da mensagem e a autenticação mútua.

A autenticação de cliente – onde cliente, neste contexto, pode significar tanto um elemento de rede como um ser humano usuário de um serviço de rede – ocorre quando este cliente apresenta sua identidade, associada a um conjunto de credenciais, na expectativa de obter acesso a algum serviço de rede. Essas credenciais são, então, utilizadas pela rede para verificar se efetivamente pertencem ao cliente e, caso afirmativo, o acesso é permitido.

Enquanto a autenticação do cliente visa a garantir que os dois extremos da comunicação são legítimos, a autenticação da mensagem serve para identificar se a integridade de uma mensagem foi mantida entre a origem e o destino. Quando a autenticação da mensagem é realizada, o recebedor tem a certeza de que a informação nela contida foi originada por uma fonte confiável e não foi modificada ao longo do percurso.

A autenticação do cliente, apresentada anteriormente, é um processo unilateral, onde apenas um lado do canal de comunicações prova sua identidade ao outro. O cliente, naquele caso, confia na rede que está acessando. Existem situações onde os dois lados do canal de comunicações necessitam identificar-se um perante o outro e, nesse caso, ocorre a autenticação mútua, que pode ser feita de forma paralela ou uma após a outra.

3.1.1.2 - Modelos para troca de mensagens de autenticação

Nesta parte serão apresentados dois modelos para a troca de mensagens de autenticação: um modelo envolvendo duas partes e outro que envolve três diferentes entidades.

No modelo de autenticação envolvendo duas partes, duas entidades interagem através de uma linha direta de comunicações, ou seja, sem envolver algum nó intermediário no processo. Isso não significa que o meio de comunicação entre estas duas entidades deva ser privativo, mas apenas que não é necessário envolver nenhuma outra parte no processo de autenticação.

O exemplo mais comum desse modelo é a autenticação cliente-servidor, podendo ainda ser realizada apenas a autenticação do cliente ou utilizada a autenticação mútua. A Figura 3.1 representa como seria a situação onde o NAS possui uma base de dados interna de informações de clientes. Ao solicitar o estabelecimento do protocolo de enlace, o cliente final envia as suas credenciais para o NAS, que as verifica contra a sua base de dados interna, que contém as informações suficientes para realizar a autenticação.

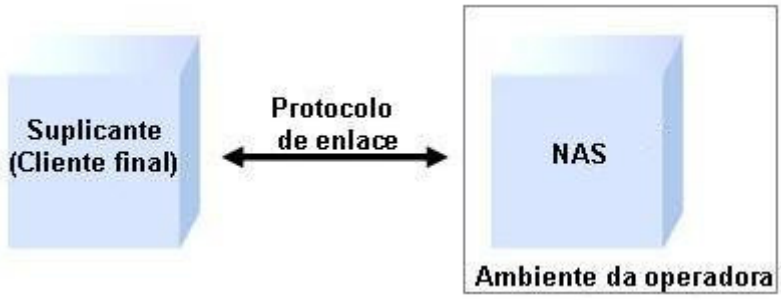

Figura 3.1: Autenticação envolvendo duas partes.

Administrar as informações de clientes em um ambiente com autenticação envolvendo duas partes pode ser uma tarefa factível para uma pequena quantidade de clientes, porém, à medida que a quantidade de clientes a autenticar aumenta, o modelo de autenticação envolvendo duas partes deixa de ser prático.

O principal ponto a observar é que o volume de informações de clientes que deve ser armazenado na parte que realiza a autenticação é diretamente proporcional ao número de

clientes envolvidos no processo de autenticação. Deve-se considerar também, que essas informações de clientes são muito dinâmicas: as pessoas compram e desistem de serviços, trocam de endereço – o que pode significar a troca de equipamento que realiza o atendimento – , alteram a sua identificação e a sua senha.

Para amenizar o trabalho imposto por esse dinamismo associado ao cliente, o modelo de autenticação envolvendo três partes pode ser utilizado. Nesse modelo, estão envolvidos no processo de autenticação o suplicante, o autenticador e o servidor de autenticação. A Figura 3.2 mostra estes elementos e suas relações.

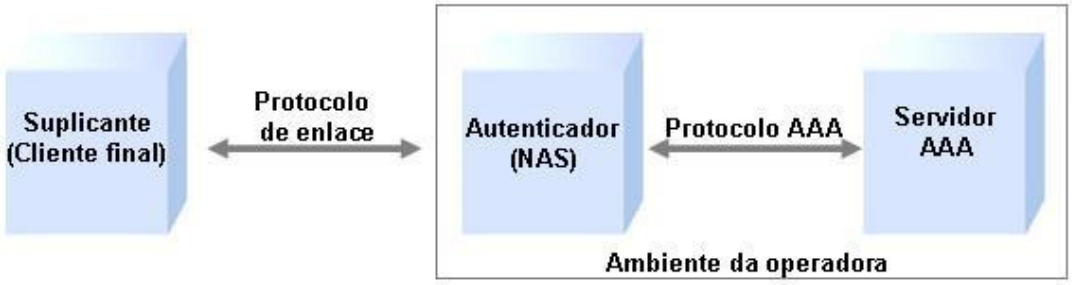

Figura 3.2: Autenticação envolvendo três partes.

O suplicante corresponde ao interessado em obter acesso à rede ou serviço; é o cliente final, que na arquitetura ADSL apresentada anteriormente corresponde ao modem, quando este é configurado para funcionar como roteador, ou ao computador do cliente, quando o modem é utilizado como *bridge*.

O autenticador é a entidade que interage com o usuário, todavia ele não possui autoridade para permitir ou não o acesso; na arquitetura do ADSL equivale ao NAS. O servidor de autenticação é quem, de fato, promove a validação das credenciais do suplicante e decide se o mesmo poderá, ou não, obter o acesso solicitado.

3.1.2 - O segundo "A": Autorização

Enquanto a autenticação é o processo responsável por identificar o usuário, a autorização trata do que o usuário previamente autenticado pode ou não pode fazer ou acessar.

Conforme [HASSEL2002], a autorização envolve utilizar um conjunto de regras ou modelos para decidir o que um usuário já autenticado pode realizar em um sistema. Esse autor exemplifica que a atribuição de um endereço IP fixo para um determinado cliente, em oposição ao fornecimento de um IP dinâmico, é uma decisão de autorização.

A enciclopédia eletrônica [WHATIS] define que autorização é o processo de aplicar políticas, determinando a que tipos ou qualidades de atividades, recursos ou serviços um determinado usuário possui acesso.

Autorização é definida por [NAKHJIRI2005] como o ato de determinar se um privilégio em particular pode ser fornecido ao portador de uma dada credencial – seja ele um usuário ou dispositivo. Esse privilégio pode ser o acesso a um recurso, como um enlace de comunicações, a um banco de dados, a um computador, ou a quaisquer outras coisas que pertençam a uma rede ou a um provedor de serviços.

A padronização dos procedimentos de autorização é feita por [RFC2904] e diversos exemplos de aplicações que envolvem autorização podem ser encontrados em [RFC2905]. Em [RFC2906], podem ser encontradas as características que protocolos de AAA devem possuir para terem a capacidade de realizar os processos de autorização.

3.1.3 - O terceiro "A": *Accounting* (Bilhetagem)

O termo "bilhetagem" está relacionado com o armazenamento de informações de utilização de um determinado serviço, visando à cobrança futura.

O processo de bilhetagem é o responsável por medir e documentar os recursos utilizados por um usuário durante seu acesso e é realizado, segundo [HASSEL2002], pelo registro das estatísticas de sessão e das informações de uso, podendo ainda ser utilizado para controle de autorização, cobrança, análise de tendências e planejamento de capacidade e utilização de recursos.

Aponta [NAKHJIRI2005] que o principal foco da bilhetagem é realizar a coleta de informações sobre o consumo de recursos em toda a rede ou em partes específicas da

mesma, e adiciona, além da possibilidade de realização de análise de tendência, duas aplicações para a bilhetagem: auditoria, pelo ato de verificar a correção de um extrato de uso ou a conformidade com uma determinada política de serviço ou de segurança e a alocação de custos, visando a atender ao crescente interesse em entender as estruturas de custo associadas aos serviços de telefonia e dados.

Afirma [RFC2975] que o campo do "Gerenciamento de Contabilização (Bilhetagem)" preocupa-se com a coleta de dados sobre consumo de recursos com os propósitos de análise de tendências e capacidade, alocação de custos, auditoria e cobrança. Alerta o mesmo autor que, considerando que não existem requerimentos uniformes de segurança e confiabilidade por parte das aplicações de contabilização, não é possível encontrar, em um único protocolo e conjunto de serviços de segurança, uma solução para todos os problemas.

3.1.3.1 - Conceitos e componentes da arquitetura de gerenciamento de bilhetagem

A arquitetura de gerenciamento de bilhetagem especifica as interações entre os dispositivos de rede, os servidores de contabilização e os eventuais servidores de faturamento, definindo também os procedimentos para a coleta dos dados de utilização. A seguir são apresentados os conceitos e componentes dessa arquitetura, conforme [RFC2975] e com complementos de [NAKHJIRI2005], oferecendo o termo em português e mantendo o termo original em língua inglesa para uma melhor compreensão.

A bilhetagem ou contabilização (*accounting*) é a coleta dos dados referentes ao consumo de um recurso com o propósito de realizar análise de capacidade e de tendência, alocação de custos, auditoria e faturamento. O gerenciamento de bilhetagem requer que o consumo de recursos seja medido, precificado, atribuído e comunicado entre as partes apropriadas.

O objetivo da bilhetagem de arquivo (*archival accounting*) é coletar todos os dados de bilhetes para reconstruir da melhor forma as entradas indisponíveis em decorrência de uma perda de dados e para arquivar e manter estes dados por um determinado período de tempo.

A bilhetagem intermediária (*interim accounting*) é um recurso para prover os dados parciais da utilização de um serviço até um determinado instante de tempo e que pode ser útil caso algum problema restrinja o envio ou a recepção do bilhete de fim de sessão.

A bilhetagem em tempo real (*real-time accounting*) envolve o processamento da informação sobre utilização de recursos dentro de uma determinada janela de tempo.

A precificação (*rating*) é a determinação do preço a ser cobrado pela utilização de um recurso, enquanto faturamento (*billing*) é o processo de preparar uma fatura. O faturamento traduz a utilização de um serviço em unidades monetárias, usando o resultado da precificação como base de conversão, levando em conta as condições tarifárias aplicáveis ao cliente.

A alocação de custos (*cost allocation*) é um método para atribuir parcelas do custo total de um serviço entre os diversos elementos necessários para o seu provimento.

Quando um processo de faturamento depende de informações de utilização de recursos ele é chamado de faturamento sensível ao uso (*usage sensitive billing*). Assim, a perda de informações de utilização pode traduzir-se diretamente em perda de receita. Os sistemas que são sensíveis ao uso podem requerer, também, que as informações sejam transmitidas e processadas com o menor atraso possível. A razão para isso é possibilitar a implementação de recursos de autorização e de minimização de fraudes, tal como limitar o uso simultâneo com a mesma credencial, verificar a disponibilidade de crédito para ativação da sessão ou, ainda, permitir mais de uma sessão por acesso físico. Serão apresentados mais adiante os modelos de processos de coleta de bilhetes. A adoção de um ou de outro modelo deverá considerar também, além das características de eficiência e consumo de recursos, a necessidade de processamento com baixo atraso.

Caso o processo de faturamento seja independente da utilização de recursos, ele é chamado de faturamento não sensível ao uso (*non-usage sensitive billing*) e, em teoria, toda a informação de utilização pode ser perdida sem afetar o processo de faturamento. Por outro lado, a perda de informação de utilização pode prejudicar os processos de auditoria e de análise de tendências e de capacidade, de forma que a perda destas informações não é,

normalmente, aceitável. A auditoria (*auditing*) é o ato de verificar a coerência entre um procedimento que é de fato executado e o procedimento recomendado.

O registro de sessão (*session record*) representa o resumo do consumo de recursos realizado por um usuário durante uma sessão. Esse registro pode ser composto pela agregação de dados de diversos elementos que participaram do provimento do serviço ao usuário.

Quando um protocolo é utilizado para conduzir os dados com o propósito de contabilização ele é denominado protocolo de bilhetagem (*accounting protocol*). Esse protocolo pode ser utilizado para realizar uma bilhetagem intra-domínio ou inter-domínio.

A bilhetagem intra-domínio (*intra-domain accounting*) é um processo que envolve a coleta de informações sobre o consumo de recursos dentro de um domínio administrativo para uso neste mesmo domínio. Na bilhetagem intra-domínio, os bilhetes e registros de sessão não cruzam as fronteiras administrativas. O conceito de domínio administrativo, neste caso, refere-se ao apresentado por [RFC1136].

A bilhetagem inter-domínio (*inter-domain accounting*) envolve a coleta de informações sobre o consumo de recursos dentro de um domínio administrativo para uso em outro domínio administrativo. Na bilhetagem inter-domínio, os bilhetes e registros de sessão tipicamente cruzam fronteiras administrativas. A Figura 3.3 apresenta esquematicamente os conceitos de billhetagem inter e intra-domínio.

O servidor de bilhetagem (*accounting server*) é a entidade que recebe ou busca os bilhetes dos dispositivos de rede. No processamento por ele realizado pode estar inclusa a verificação de duplicidade de bilhetes, a transformação em registros de sessão e também o encaminhamento desses registros para outros sistemas. O servidor de faturamento (*billing server*) é o elemento que recebe ou busca os registros de sessão e gera, conforme a precificação, as faturas para os clientes. Pode, eventualmente, executar funções relacionadas com a alocação de custos, a análise de tendências e o planejamento de capacidade.

Por vezes, entre o servidor de bilhetagem e o de faturamento é inserido um elemento denominado mediador, visando a realizar um pré-processamento da informação de utilização. Esse pré-processamento inclui, mas não está limitado a, realizar a coleta dos bilhetes em diversos servidores, identificar registros duplicados, validar, ordenar e filtrar bilhetes conforme alguma regra de negócio e correlacionar os registros com dados de outras fontes.

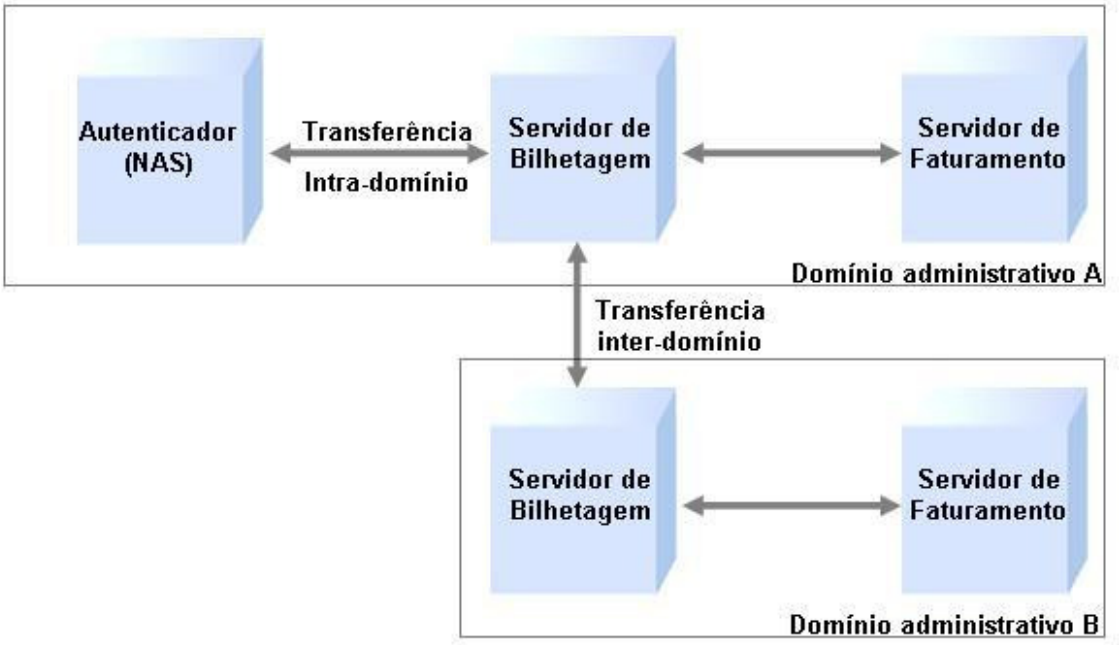

Figura 3.3: Bilhetagem inter-domínio e intra-domínio

3.1.3.2 - Modelos para a coleta de dados de utilização

Diversos modelos de coleta de dados foram, segundo [NAKHJIRI2005], desenvolvidos na indústria. Quatro desses modelos serão apresentados a seguir.

Modelo Consulta (*Polling model*)

No modelo Consulta, um servidor de bilhetagem obtém os dados de utilização através de consulta aos elementos de rede em intervalos de tempo regulares.

Esses intervalos devem, obrigatoriamente, ser menores do que o tempo necessário para encher o espaço de armazenamento temporário dos elementos de rede e devem ser também adequados levando em consideração as necessidades de atualização do sistema de cobrança.

Devido à característica de acumulação de dados em cada dispositivo, os dados são normalmente transferidos em lote, o que, segundo [RFC2975], resulta em um processo de transferência eficiente. Alerta, esse mesmo autor, que, quanto maior a quantidade de elementos, maior será o sistema, e quanto maior a quantidade de dados a coletar, maior será a banda necessária para transferir os dados de utilização.

Esse modelo possui a vantagem de não apresentar perda de dados em decorrência de falhas de rede, exceto na ocorrência de situações onde o tempo de falha é superior ao período necessário para encher o espaço de armazenamento temporário no elemento de rede. Por outro lado, caso o elemento de rede seja reiniciado e os dados de utilização não estejam armazenados em memória não volátil do próprio equipamento, tais dados serão perdidos.

Modelo “Disparado por evento” (*Event-driven model*)

Neste modelo, o elemento de rede encaminha os dados de utilização ao servidor de bilhetagem tão logo esses dados estejam disponíveis em função da ocorrência de um evento, tal como o início ou o fim de uma conexão.

Por essa característica, esse modelo apresenta a menor necessidade de memória, pois apenas os dados que ainda não foram transmitidos precisam ficar armazenados no elemento de rede. Permite também desenvolver sistemas com o menor atraso de processamento, o que habilita a utilização de técnicas anti-fraude, segundo [NAKHJIRI2005].

Por outro lado, ele apresenta uma eficiência de transmissão de dados inferior à do modelo Consulta. É também mais suscetível à perda de dados em situações de congestionamento ou de falha de rede, pois as informações de utilização são armazenadas no elemento de

rede por um curto período de tempo, e, passado este tempo, e independentemente do bilhete ter sido recebido ou não pelo servidor de bilhetagem, ele é descartado do elemento de rede.

Modelo "Consulta disparada por evento" (*Event-driven polling model*)

Neste modelo, o servidor de bilhetagem irá consultar o elemento de rede por dados de utilização apenas quando ocorre um evento. Esse evento pode ser o decurso de um determinado tempo ou o fato de haver sido atingido um determinado volume de dados, ou a conjunção de ambos.

A principal vantagem desse modelo é o aumento da eficiência de transmissão, por transferir lotes maiores de dados de utilização, e a característica de não ocorrer perda de dados em decorrência de falhas de rede. Por outro lado, caso uma memória não volátil não seja utilizada no elemento de rede, a perda de dados decorrente de uma reinicialização desse elemento é inevitável.

Utilização de bilhetagem intermediária (*Interim Accouting*)

Habitualmente são gerados bilhetes para os eventos de início e de fim de uma sessão. Como a maior parte das informações de consumo de recursos está presente apenas após o término da sessão, a perda do bilhete de início não é muito significativa – pode afetar controles de autorização – porém a perda do bilhete de fim de conexão resulta em perder toda a informação do consumo realizado.

A implementação de bilhetagem intermediária normalmente é feita para melhorar a confiabilidade do sistema de contabilização e pode ser aplicada a qualquer dos modelos de coleta de bilhetes. Ela consiste em encaminhar periodicamente dados referentes ao consumo de recursos da sessão, que podem ser utilizados para recuperar as informações da sessão – ao menos parcialmente –, caso o bilhete final seja perdido.

Enquanto o uso de bilhetagem intermediária pode limitar a perda de dados devido a problemas na rede ou pela reinicialização do elemento de rede, sua aplicação é limitada pelos recursos adicionais de banda, processamento e espaço de armazenamento de que ela necessita.

Em decorrência, segundo [RFC2975], a bilhetagem intermediária é implementada principalmente para evitar a perda de informações de sessões de longa duração e o intervalo entre os bilhetes intermediários é tipicamente ajustado para um valor superior à duração média das sessões. Adotado esse procedimento, a maior parte das sessões não irá gerar um bilhete intermediário e o consumo de recursos será moderado.

À medida que o intervalo entre bilhetes intermediários é ajustado para valores próximos ao da duração média de sessão, a quantidade de bilhetes gerada aumenta progressivamente. Se o intervalo for inferior ao da sessão média, a maior parte das sessões gerará pelo menos um bilhete adicional, o que resultará em um aumento significativo dos recursos consumidos para transporte, processamento e armazenamento dos bilhetes. Em caso de utilização, o valor para este intervalo deve ser cuidadosamente avaliado.

3.1.3.3 - Segurança e confiabilidade da bilhetagem

Alerta [NAKHJIRI2005] que a veracidade dos dados de utilização gerados pela operadora deve ser garantida, visto que a conseqüência de utilizar dados incorretos é, provavelmente, gerar faturas também incorretas. Lembra esse mesmo autor que os usuários podem verificar a veracidade das informações utilizadas para a emissão de faturas a partir de suas próprias medições ou através da utilização de uma auditoria independente.

A incorreção de dados de utilização pode ser provocada de forma não intencional, através de configuração inadequada de elementos de rede, ou por ação provocada intencionalmente, através, por exemplo, de modificação dos registros de utilização.

Em razão disso, medidas devem ser tomadas para que as configurações dos equipamentos estejam corretas e também para restringir o acesso não autorizado aos registros de utilização e aos elementos de rede e ainda para garantir que os registros foram originados

efetivamente pelos elementos de rede autorizados e não sofreram modificação entre a origem e o destino.

Adicionalmente, em situações em que o faturamento é sensível ao uso, ou em que os dados de utilização servem para realizar alocação de custos ou auditoria, a implementação de bilhetagem de arquivo é normalmente obrigatória, seja para o cumprimento de obrigações legais seja para atender a requisitos de ordem financeira.

Como nessas situações as eventuais falhas podem ocasionar perda de receita para a operadora, existe um incentivo para desenvolver um sistema de bilhetagem que seja tolerante a falhas. Tipicamente, conforme [RFC2975], tais falhas estão vinculadas à perda de pacotes, à indisponibilidade do servidor de bilhetagem, a defeitos de rede ou a reinicialização de equipamentos.

Perda de pacotes

A discussão em torno de perda de pacotes normalmente está vinculada à discussão sobre o protocolo de transporte utilizado, se é UDP (*User Datagram Protocol*), TCP (*Transmission Control Protocol*) ou SCTP (*Stream Control Transfer Protocol*), dadas as características próprias de cada um destes protocolos no que tange ao tratamento dado a situações nas quais pode ocorrer perda de pacotes.

Alerta [RFC2975] que o transporte baseado em UDP é freqüentemente utilizado em aplicações de bilhetagem e, de fato, como veremos mais adiante, o UDP é o protocolo utilizado para o transporte da bilhetagem do sistema ADSL.

Assim, deve-se avaliar o que pode ser feito, quando utilizado o protocolo UDP, para tornar menor o efeito causado pela perda de pacotes, enquanto maiores informações sobre os protocolos UDP, TCP e SCTP podem ser encontradas, respectivamente, em [RFC768], [RFC793] e [RFC4960].

O protocolo UDP não prevê retransmissão em caso de perda de pacotes. É possível, porém, implementar um mecanismo acima do UDP para realizar a retransmissão de informações

caso uma confirmação de recebimento dessas informações não volte ao emissor. Deve-se, porém, cuidar para que o tempo de espera pela confirmação seja superior ao tempo necessário para uma mensagem ir e voltar (*round-trip time*) somado ao tempo de processamento do lado receptor, de forma a evitar que uma retransmissão seja realizada antes que a transmissão com sucesso possa ser reconhecida.

É fato que as retransmissões não podem ser feitas indefinidamente, pois existem limitações de memória nos equipamentos e, em caso de situações de congestionamento, estas retransmissões provavelmente apenas tornarão pior a situação.

Assim, a situação particular de uma rede que envolva bilhetagem precisa ser analisada para definir qual a quantidade de retransmissões e o tempo entre elas que pode ser adotado, visando a uma solução de compromisso para a mitigação do problema.

Deve ser considerada, independente do protocolo de transporte utilizado, a possibilidade de ocorrência de registros duplicados em decorrência da utilização de retransmissões.

Indisponibilidade do servidor de bilhetagem

Caso o servidor de bilhetagem torne-se indisponível, a perda de dados de utilização é, possivelmente, inevitável. Em tal situação, é altamente desejável que um servidor secundário possa assumir imediatamente a função do servidor em condição de falha. Ter um ou mais servidores secundários reduz o risco de perda de informações.

Para sistemas que utilizam UDP como protocolo de transporte, a transmissão para servidor secundário pode ocorrer após uma quantidade de transmissões sem reconhecimento para o servidor primário e pode ser apropriado considerar valores diferentes para a quantidade máxima de retransmissões e o tempo entre elas. Deve ser avaliada a necessidade de tratamento para a ocorrência de registros do mesmo evento armazenados em diferentes servidores.

É importante levar em consideração que podem ocorrer falhas nos servidores de bilhetagem que não impeçam a recepção e reconhecimento dos pacotes de dados, mas que levem à perda de dados, tais como falta de conexão ao banco de dados ou falta de espaço em disco. Essas situações e as medidas para sua mitigação devem ser avaliadas, preferencialmente, antes da ativação do sistema.

Defeitos de rede

A ocorrência de defeitos na rede pode provocar a interrupção da comunicação entre os elementos de rede e o servidor de bilhetagem primário. Nessa hipótese, as informações de utilização deverão ser encaminhadas para o servidor secundário.

O projeto da rede deve considerar a disposição dos servidores de bilhetagem, primário e secundários, em pontos distintos da rede, visando a minimizar a oportunidade de ocorrência de falha que atinja a comunicação para todos os servidores simultaneamente.

A adoção de um armazenamento de informações de utilização em memória não volátil nos elementos de rede auxiliaria a minimizar os efeitos de falhas de rede impeditivas da comunicação com os servidores de bilhetagem; na prática, porém, os elementos de rede que fazem parte do sistema ADSL não possuem esta característica.

Reinicialização de equipamentos

Na ocorrência de uma reinicialização de equipamentos que concentram os acessos de clientes, todas as sessões ativas são encerradas sem a emissão de um bilhete de fim de sessão.

Quando essa reinicialização é decorrente de uma manutenção programada, a adoção de um procedimento que provoque o encerramento das sessões dos usuários antes da efetiva reinicialização irá produzir os bilhetes de final de sessão desses usuários, não prejudicando a contabilização de uso.

3.2 - MECANISMOS DE AUTENTICAÇÃO

O protocolo habitualmente utilizado para o estabelecimento de conexões lógicas sobre acessos ADSL é chamado PPP (*Point-to-Point Protocol*), ou protocolo ponto-a-ponto. Este protocolo foi concebido em 1989, através de [RFC1134]; a sua padronização atual é definida pelos documentos [RFC1661] e [RFC1662] e é reconhecida desde 2004 como um *Internet Official Protocol Standards* por [STD1], recebendo a numeração STD51.

Antes do desenvolvimento e popularização do protocolo PPP, diversos mecanismos de autenticação já haviam sido criados para a finalidade de prover controle de acesso a sistemas que dispunham de conexão através de linha discada. Por esse motivo, o PPP foi desenvolvido de forma a fazer uso desses mecanismos de autenticação.

Os principais mecanismos de autenticação de usuários de acessos ADSL são o PAP (*Password Authentication Protocol*) e o CHAP (*Challenge Handshake Authentication Protocol*). Para compreender como estes mecanismos de autenticação funcionam é importante conhecer o funcionamento básico do PPP e das suas variações presentes em uma arquitetura de rede ADSL.

3.2.1 - PPP (*Point-to-Point Protocol*)

O PPP, segundo [RFC1661], 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.

De forma complementar, [NAKHJIRI2005] apresenta o PPP como um protocolo utilizado para estabelecer o enlace de dados – camada 2 do modelo de referência OSI – entre um cliente e o seu nó de acesso à rede, promovendo principalmente o enquadramento dos dados, mas também fornecendo um conjunto de outros serviços.

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. 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. Maiores detalhes sobre esse protocolo e a comparação com outros protocolos de enlace podem ser obtidos em [RCF1661], [RFC1662], [HUNT1994] e [LEWIS1999].

3.2.2 - 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 3.4.

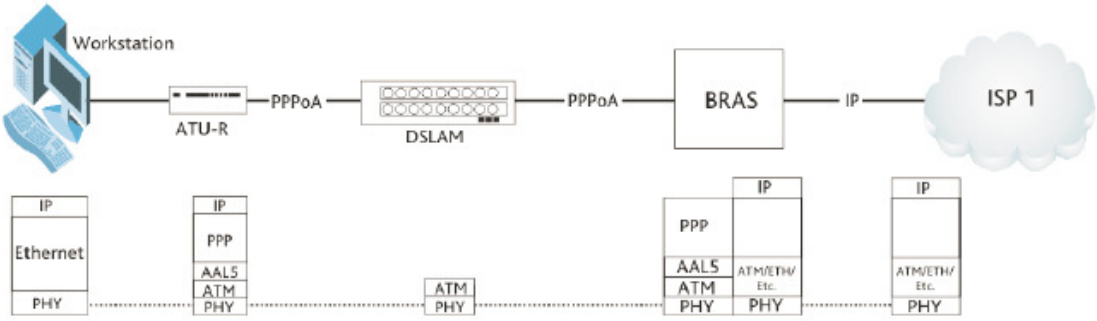

Figura 3.4: Pilhas de protocolos para o PPPoA (Fonte: [SPIRENT2002])

Informações detalhadas sobre o funcionamento do PPPoA podem ser obtidas em [RFC2364], e sobre o protocolo ATM podem ser obtidas em [SOARES1995].

3.2.3 - 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.

Detalhes deste protocolo podem ser obtidos em [RFC2516].

3.2.4 - 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 3.5.

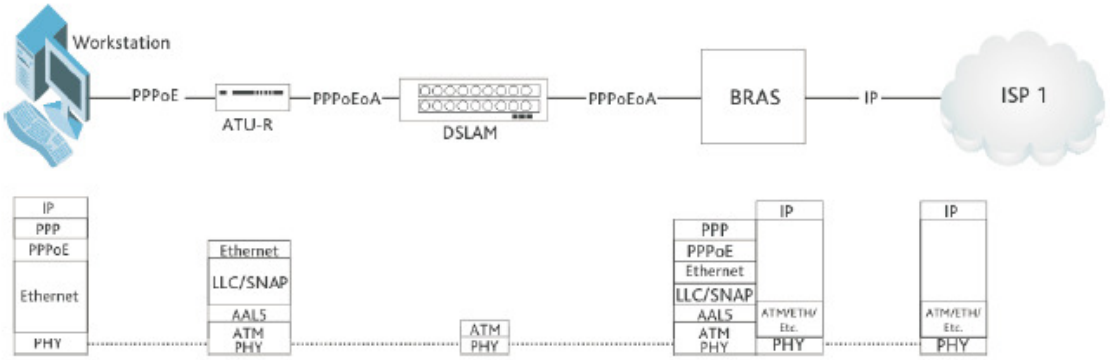

Figura 3.5: Pilhas de protocolos para o PPPoEoA (Fonte: [SPIRENT2002])

3.2.5 - Comparação entre os protocolos PPPoA, PPPoE e PPPoEoA

A utilização de um ou outro protocolo é, normalmente, transparente para o usuário comum. Usuários mais especializados, porém, perceberão que existem, de fato, diferenças na utilização.

Inicialmente, nas redes das operadoras de telecomunicações, existia apenas um tipo de DSLAM, o que utiliza a tecnologia ATM para a sua conexão com NAS. Naturalmente, o protocolo mais utilizado era o PPPoA.

Em determinada época a adoção de um *software* cliente PPPoE para o computador permitiu a utilização de modems ADSL bem mais simples e de custo significativamente mais baixo. Contudo, a utilização do PPPoE em acessos conectados a um DSLAM ATM, em razão do re-encapsulamento dos frames *Ethernet* em células ATM que é feito no equipamento, torna-se PPPoEoA. Nessa condição ocorre uma redução na largura de banda disponível para o cliente, situação a qual o usuário mais especializado consegue perceber através de comparação do desempenho do seu acesso com o de outros clientes que utilizem ou PPPoA ou PPPoE.

Atualmente, a disponibilidade de DSLAMs ATM no mercado é muito baixa. Com a implantação de novos acessos apenas em DSLAMs *Ethernet*, o uso do protocolo PPPoA não é mais possível, restando apenas a opção da utilização do protocolo PPPoE.

Independentemente do protocolo utilizado, é razoável considerar que a forma de contabilização de tráfego utilizada pelos contadores de uma interface lógica em um NAS não sofra variação em função do tipo de encapsulamento utilizado no caminho entre o cliente e o NAS (PPPoA, PPPoE ou ainda PPPoEoA), pois os cabeçalhos de cada tipo de encapsulamento intermediário são removidos antes de chegarem na interface lógica do NAS; ela é, funcionalmente, apenas uma interface PPP.

Apresenta [SPIRENT2002] um estudo comparativo entre os protocolos PPPoA, PPPoE e PPPoAoE. Uma metodologia para derivar a eficiência das diferentes pilhas de protocolos pode ser vista em [VANAKEN2003].

3.2.6 - Método de Autenticação PAP

Segundo [LEWIS1999], o PAP (*Password Authentication Protocol*) foi o primeiro protocolo de autenticação desenvolvido para o PPP. Complementa [NAKHJIRI2005], que o PAP é o método de autenticação mais básico utilizado com o PPP.

O PAP foi definido por [RFC1334], e proporciona um método simples para estabelecer a identidade de um lado da conexão após o estabelecimento inicial do enlace, utilizando uma negociação de duas vias.

Após o estabelecimento inicial do enlace, as credenciais do cliente (nome do usuário e senha) são repetidamente enviadas pelo suplicante ao autenticador, até que ou a autenticação ocorra ou o enlace seja desfeito. Caso a autenticação ocorra, o PPP passa para a fase seguinte (NCP) e a conexão é estabelecida. Nenhuma nova autenticação será realizada enquanto o enlace estiver em operação.

Note-se que as credenciais do usuário são encaminhadas no enlace PPP sem qualquer tipo de proteção ou de criptografia, proporcionando, portanto, oportunidade para um potencial problema de segurança caso o enlace seja alvo de interceptação. Um método que oferece um grau melhor de segurança é o CHAP, que será apresentado a seguir.

3.2.7 - Método de Autenticação CHAP

Segundo [HASSEL2002], o CHAP (*Challenge Handshake Authentication Protocol*) é baseado na premissa que a senha de um cliente nunca deve ser enviada em qualquer pacote através da rede.

O CHAP é utilizado para, periodicamente, verificar a identidade do cliente utilizando uma negociação de três vias. A verificação inicial é realizada no estabelecimento do enlace, e pode ser repetida a qualquer tempo após ele ter sido ativado.

A negociação é realizada nesta seqüência:

- Na fase de autenticação, o autenticador envia um "desafio" (*challenge*) ao cliente. Este desafio consiste em uma seqüência de octetos, que muda a cada vez que um desafio é enviado a um cliente.
- O cliente responde ao desafio com o resultado de uma manipulação matemática (*hash*) irreversível de uma combinação entre a senha e o desafio. Para essa manipulação matemática, um algoritmo negociado durante a fase LCP é utilizado. Habitualmente o algoritmo MD5, proposto em [RFC1321], é utilizado.
- O autenticador compara esta resposta do cliente com o resultado esperado da manipulação matemática por ele executada. Caso os valores coincidam, a autenticação foi realizada com sucesso e o PPP passa para a fase NCP; caso contrário, a conexão deve ser terminada.
- Em intervalos aleatórios, o autenticador envia um novo desafio ao cliente e repete os três passos acima.

Caso um esquema de autenticação de três partes seja utilizado, o autenticador deverá enviar a resposta do cliente ao desafio e o próprio desafio ao servidor de autenticação para que esse último possa, a partir da senha do cliente, à qual o servidor deve ter acesso, realizar a manipulação matemática e a comparação dos resultados.

O protocolo CHAP, tal como o PAP, foi definido por [RFC1334]. Sua padronização final, porém, é apresentada em [RFC1994].

3.3 - O PROTOCOLO RADIUS

O RADIUS (*Remote Authentication Dial-in User Service*), conforme [HASSEL2002], tal como a maioria dos produtos inovadores, foi construído a partir de uma necessidade: 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. A descrição completa desta necessidade e também da origem do protocolo RADIUS podem ser obtidas em [INTERLINK].

O protocolo RADIUS foi definido originalmente em janeiro de 1997, através do documento [RFC2058] e hoje está padronizado através da [RFC2865] e da [RFC2866]. É amplamente adotado como protocolo de autenticação em redes de acesso usando tecnologia ADSL, entre outras aplicações.

3.3.1 - Características do protocolo RADIUS

As especificações do protocolo RADIUS determinam suas principais características, que a seguir serão apresentadas, conforme [RFC2865] e [RFC2866].

3.3.1.1 - Modelo Cliente-Servidor

O cliente RADIUS é responsável por passar, ao servidor RADIUS designado em sua configuração, as credenciais de acesso do usuário final, na forma de requisições, e aguardar a resposta desse servidor, atuando conforme a resposta recebida.

O servidor RADIUS, por sua vez, é responsável por receber e processar as requisições de autenticação originadas pelo cliente, retornando as informações de configuração necessárias para o cliente RADIUS entregar o serviço ao usuário.

É importante notar, conforme apresenta [NAKHJIRI2005], que no contexto RADIUS o cliente RADIUS é o elemento que atua como cliente na troca de mensagens RADIUS, e que o usuário ou o dispositivo de rede que busca estabelecer a conexão não é o elemento cliente nesta discussão. Habitualmente, um NAS (*Network Access Server*) funciona como o

cliente RADIUS e o usuário ou o dispositivo de rede pode ser referido como “cliente final” ou “suplicante” para distinguir de forma mais clara o papel de cada elemento.

Para os processos de bilhetagem, vale o mesmo princípio: o cliente envia ao servidor uma Requisição de Bilhetagem e o servidor a recebe e a processa adequadamente. Os aspectos gerais da bilhetagem serão abordados neste capítulo e os particulares serão tratados no capítulo 4.

Por fim, é importante ressaltar que um servidor RADIUS pode também atuar como um cliente RADIUS quando ele consultar outro servidor RADIUS para fins de autenticação, autorização ou bilhetagem. A essa situação damos o nome de consulta “*Proxy*”.

3.3.1.2 – Segurança

As transações entre o cliente e o servidor RADIUS são autenticadas através do uso de uma senha compartilhada conhecida como *shared secret*, que nunca é enviada através da rede. Adicionalmente, qualquer senha é enviada criptografada entre o cliente e o servidor, o que elimina a possibilidade de alguém, monitorando uma rede insegura, determinar a senha de um usuário.

Alerta [HASSEL2002], porém, que a segurança pode ser um obstáculo em algumas implementações. Em situações onde múltiplas consultas *Proxy* são utilizadas, todos os servidores envolvidos necessitarão ver todos os dados constantes na requisição RADIUS para que possam processá-la adequadamente, o que pode não ser uma condição aceitável de segurança.

Adicionalmente, diversas vulnerabilidades do protocolo RADIUS, originadas no próprio protocolo ou causáveis por uma implementação pouco cuidadosa do lado cliente, foram elencadas por [HILL2001]; não é escopo deste trabalho, porém, detalhá-las.

3.3.1.3 - Mecanismos flexíveis de autenticação e bilhetagem

O protocolo RADIUS não define a implementação do cliente ou do servidor, mas a troca de mensagens entre eles. Dessa forma, uma implementação do servidor RADIUS pode

suportar diferentes métodos de autenticação para validar as credenciais de um cliente final. O requisito essencial é que ele receba as informações de identificação do cliente final (por exemplo: nome do usuário e senha).

3.3.1.4 - Protocolo extensível

O protocolo RADIUS transporta informação na forma de atributos. Existindo a necessidade de incorporar alguma nova informação na comunicação entre o cliente e o servidor, novos atributos podem ser adicionados ao RADIUS sem alterar as implementações existentes do protocolo.

3.3.2 - Tipos de mensagens RADIUS

O protocolo RADIUS possui um conjunto de mensagens para permitir a comunicação entre um cliente e um servidor. A base do protocolo RADIUS, definida por [RFC2865] e [RFC2866], consiste em oito mensagens. Outras seis mensagens são propostas por [RFC5176].

Aponta [NAKHJIRI2005] que as especificações que incluem novos tipos de mensagens RADIUS, tal como [RFC5176], são consideradas como informativas e não como adições ao padrão RADIUS, em decorrência da necessidade de compatibilidade entre o grande número de sistemas RADIUS existentes e em operação e dos potenciais problemas que essas novas mensagens podem trazer a tais sistemas.

A seguir essas mensagens serão descritas de forma sucinta, iniciando pelas oito mensagens do protocolo base (de 3.3.2.1 a 3.3.2.7) e seguindo com as seis propostas por [RFC5176] (de 3.3.2.8 a 3.3.2.11). São também apresentados os nomes das mensagens em idioma inglês, por serem os registrados nas referências consultadas.

3.3.2.1 - Requisição de Acesso (*Access-Request*)

Esta mensagem é gerada pelo cliente RADIUS e dirigida ao servidor RADIUS para transportar a solicitação de acesso do usuário final.

3.3.2.2 - Requisição de Desafio (*Access-Challenge*)

Esta mensagem é gerada pelo servidor RADIUS e destinada ao cliente RADIUS e é utilizada para questionar o cliente RADIUS ou o usuário final sobre alguma coisa ou realizar algum tipo de negociação.

3.3.2.3 - Acesso Permitido (*Access-Accept*)

Esta mensagem é gerada pelo servidor RADIUS e destinada ao cliente RADIUS e é utilizada para indicar que a solicitação de acesso realizada pelo usuário final foi aceita.

3.3.2.4 - Acesso Rejeitado (*Access-Reject*)

Esta mensagem é gerada pelo servidor RADIUS e destinada ao cliente RADIUS e é utilizada para indicar que a solicitação de acesso realizada pelo usuário final foi rejeitada.

3.3.2.5 - Requisição de Bilhetagem (*Accounting-Request*)

Esta mensagem é gerada pelo cliente RADIUS e dirigida ao servidor RADIUS para transportar as informações correntes da conexão ou do serviço fornecido ao usuário final.

3.3.2.6 - Bilhetagem Aceita (*Accounting-Response*)

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

3.3.2.7 - Estado do Servidor (*Status-Server*) e Estado do Cliente (*Status-Client*)

Estas mensagens são consideradas experimentais por [RFC2865], que não menciona as finalidades previstas para elas. O nome a elas dado sugere que foram criadas para averiguar o estado de funcionamento do servidor e do cliente RADIUS, respectivamente. Uma forma prática de utilização para a mensagem Estado do Servidor é proposta por

[DEKOK2008], que também apresenta uma sugestão para a potencial utilização da mensagem Estado do Cliente.

3.3.2.8 - Requisição de Desconexão (*Disconnect-Request*)

Esta mensagem é enviada pelo servidor RADIUS ao cliente RADIUS para solicitar o encerramento de uma sessão de um usuário final e descartar todo o contexto relacionado com essa sessão, ou seja, desalocar todos os recursos utilizados para ativar a sessão do usuário no cliente RADIUS.

3.3.2.9 - Desconexão Aceita (*Disconnect-ACK*) e Desconexão não Aceita (*Disconnect-NAK*)

O cliente RADIUS responde a uma mensagem Requisição de Desconexão com uma mensagem Desconexão Aceita se foi possível encerrar a sessão do usuário e descartar o contexto desta sessão. Caso não tenha sido possível encerrar a sessão e desalocar os recursos por ela ocupados, a mensagem retornada ao servidor RADIUS será do tipo Desconexão não Aceita.

3.3.2.10 - Requisição de Mudança de Autorização (*CoA-Request*)

A mensagem Requisição de Mudança de Autorização serve para alterar características de uma sessão de um usuário final. Segundo [RFC5176], a utilização típica para esta mensagem é solicitar a alteração de filtros de dados associados à sessão do usuário.

3.3.2.11 - Mudança de Autorização Aceita (*CoA-ACK*) e Mudança de Autorização não Aceita (*CoA-NAK*)

Caso tenha sido possível realizar a alteração de autorização solicitada através de uma mensagem Requisição de Mudança de Autorização, o cliente RADIUS responde ao servidor com uma mensagem Mudança de Autorização Aceita, caso contrário, responde com uma mensagem Mudança de Autorização não Aceita.

3.3.3 - Atributos RADIUS

O atributo é a maneira de transportar uma informação em uma mensagem do protocolo RADIUS. Os atributos podem carregar informações específicas de autenticação, autorização e bilhetagem, além de detalhes de configuração necessários para o estabelecimento de uma conexão.

Quando um cliente RADIUS solicita a um servidor a permissão para o estabelecimento de uma conexão utilizando uma mensagem Requisição de Acesso, as credenciais de acesso de um cliente final, entre outras informações, são transportadas na forma de atributos. Nesse exemplo, os atributos utilizados são, geralmente, *User-Name* para a identificação do cliente final e *Password* para a senha.

Dentro de uma mensagem RADIUS, um atributo é sempre um tripleto formado pelos campos tipo, tamanho e valor e seu formato pode ser visto na Figura 3.6. A descrição dos campos é apresentada na Tabela 3.1.

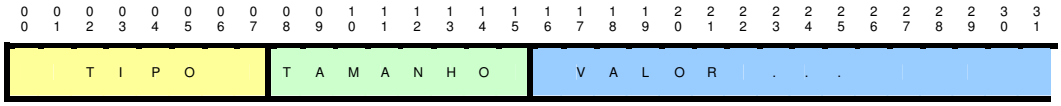

Figura 3.6: Formato do atributo RADIUS

Tabela 3.1: Descrição dos campos do atributo RADIUS

Campo	Tamanho	Descrição
Tipo	1 *byte*	É o tipo do atributo, conforme [RFC2865] e [RFC2866].
Tamanho	1 *byte*	Indica o tamanho total do atributo, incluindo os 2 *bytes* dos campos Tipo e Tamanho.
Valor	Variável	Contém a informação a ser transportada, limitada a 253 *bytes*.

Os documentos [RFC2865] e [RFC2866] definem cerca de 40 diferentes tipos de atributos. Na Tabela 3.2 são apresentados alguns atributos que habitualmente estão presentes em sistemas ADSL como o da operadora Brasil Telecom.

Tabela 3.2: 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 3.2. 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.

O subcampo Identificador tem o tamanho de quatro *bytes* e recebe a identificação designada ao fabricante, chamada de PEN (*Private Enterprise Number*), conforme originalmente definido em [RFC1700] e, atualmente, em [RFC3232]. O autor [HASSEL2002] refere-se a este identificador como *Network Management Private Enterprise Code* (NMPEC).

Os demais subcampos são caracterizados de acordo com o descrito na Tabela 3.3 e são similares aos campos descritos para os atributos convencionais, conforme Tabela 3.1.

Tabela 3.3: Descrição dos subcampos para um VSA

Campo	Tamanho	Descrição
Identificador	4 *bytes*	Contém o código que identifica o fabricante (PEN)
Tipo	1 *byte*	É o tipo do atributo, cujo significado é particular ao fabricante do equipamento.
Tamanho	1 *byte*	Indica o tamanho total do atributo, incluindo os 6 *bytes* dos campos Identificador, Tipo e Tamanho.
Valor	Variável	Contém a informação a ser transportada, deve possuir pelo menos um *byte* e é limitado a 247 *bytes*.

3.3.4 - O Pacote RADIUS

O RADIUS utiliza o protocolo de transporte UDP, definido em [RFC768], para enviar as mensagens trocadas entre cliente e servidor e, segundo [RFC2865], exatamente um pacote RADIUS é encapsulado no campo de dados do UDP.

O pacote RADIUS segue o formato apresentado na Figura 3.7, e a descrição sucinta dos campos pode ser vista na Tabela 3.4. A descrição detalhada dos campos é apresentada na seqüência.

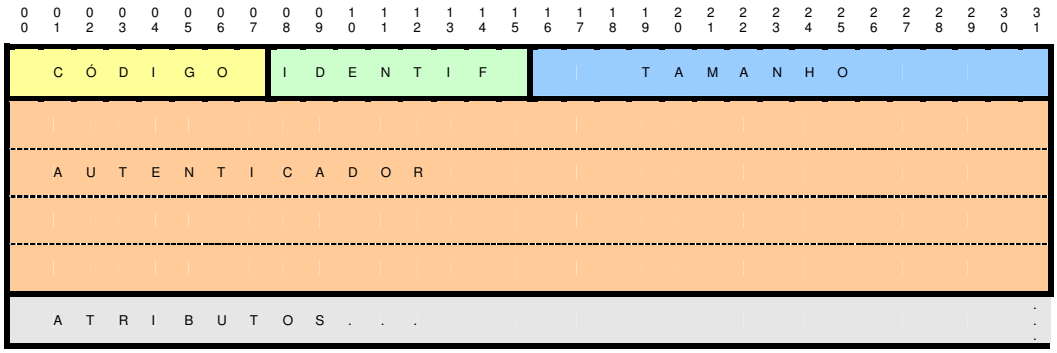

Figura 3.7: Formato do pacote RADIUS

Tabela 3.4: Descrição dos campos do pacote RADIUS

Campo	Tamanho	Descrição
Código	1 *byte*	Indica o tipo de mensagem
Identificador	1 *byte*	Utilizado para diferenciar mensagens com mesma origem e destino e casar respostas com as suas respectivas requisições.
Tamanho	2 *bytes*	Indica o tamanho total da mensagem, incluindo todos os campos.
Autenticador	16 *bytes*	Utilizado para autenticar a resposta de um servidor RADIUS.
Atributos	Variável	Atributos, no formato apresentado na Figura 3.6.

3.3.4.1 - Campo Código

O campo Código possui um *byte* de tamanho e identifica o tipo de mensagem RADIUS que determinado pacote transporta. Os códigos referentes às mensagens apresentadas na seção 3.3.2 são apresentados na tabela Tabela 3.5. O código 255 é definido como "reservado" por [RFC2865].

Tabela 3.5: Valores para o campo código

Código	Mensagem
1	Requisição de Acesso (*Access-Request*)
2	Acesso Permitido (*Access-Accept*)
3	Acesso Rejeitado (*Access-Reject*)
4	Requisição de Bilhetagem (*Accounting-Request*)
5	Bilhetagem Aceita (*Accounting-Response*)
11	Requisição de Desafio (*Access-Challenge*)
12	Estado do Servidor (*Status-Server*)
13	Estado do Cliente (*Status-Client*)
40	Requisição de Desconexão (*Disconnect-Request*)
41	Desconexão Aceita (*Disconnect-ACK*)
42	Desconexão não Aceita (*Disconnect-NAK*)
43	Requisição de Mudança de Autorização (*CoA-Request*)
44	Mudança de Autorização Aceita (*CoA-ACK*)
45	Mudança de Autorização não Aceita (*CoA-NAK*)

3.3.4.2 - Campo Identificador

O Identificador é um número entre 0 e 255 cuja presença no pacote RADIUS visa a auxiliar no casamento entre uma requisição e sua resposta.

Através deste mecanismo, um cliente RADIUS que envia uma requisição com o campo Identificador com um valor *id*, a partir do endereço IP *a.b.c.d* e porta de origem UDP *udpport*, assumirá que uma mensagem recebida no IP *a.b.c.d*, porta UDP *udpport* e com o campo Identificador com valor *id* é a resposta à sua requisição.

Adicionalmente, o servidor RADIUS utiliza o Identificador para detectar o recebimento de uma requisição duplicada, caso esta requisição possua o mesmo endereço IP e porta UDP de origem de outra que tenha sido recebida dentro de um determinado período tempo.

Assim, caso um servidor RADIUS receba, dentro de um intervalo de tempo, mais de um pacote RADIUS com mesmo endereço IP, mesma porta UDP de origem e mesmo valor para o campo Identificador, ele poderá processar apenas o primeiro pacote recebido e ignorar os demais. Não existe em [RFC2865] uma sugestão para o intervalo de tempo, mas é razoável conceber que, para que este mecanismo de detecção de pacotes duplicados funcione adequadamente, o intervalo deva ser no máximo o tempo de processamento máximo de um pacote para uma implementação de servidor RADIUS.

3.3.4.3 - Campo Tamanho

Este campo ocupa dois *bytes* e indica o tamanho total da mensagem RADIUS, incluindo, então, o espaço ocupado pelos campos Código, Identificador, Tamanho, Autenticador e Atributos. O tamanho mínimo de uma mensagem é vinte *bytes*, considerando a situação em que nenhum atributo é enviado e que o campo Autenticador ocupa 16 *bytes*. O tamanho máximo, definido por [RFC2865], é 4096 *bytes*.

3.3.4.4 - Campo Autenticador

Este campo ocupa dezesseis *bytes* e possui finalidades e formas de geração, conforme o tipo de mensagem RADIUS que é transmitida, que serão discutidas a seguir.

Campo Autenticador em mensagens Requisição de Acesso

Em mensagens do tipo Requisição de Acesso o campo Autenticador é chamado de Autenticador da Requisição (*Request Authenticator*) e é utilizado fundamentalmente para alimentar o mecanismo utilizado para criptografar e decriptografar a senha do cliente final, quando esta está presente na mensagem. Este mecanismo de criptografia é chamado, conforme [RFC2865], de algoritmo de ocultação de senha (*password hiding algorithm*), e será apresentado na seção 3.3.5.

Nesse tipo de mensagem este campo deve ser preenchido pelo cliente RADIUS com um valor não previsível (randômico). Por não ser gerado pelo cliente nem verificado pelo servidor com base em algum tipo de senha, este campo, por si, não provê a possibilidade de verificação de integridade da Requisição de Acesso.

Segundo [NAKHJIRI2005], a única exigência para o campo autenticador da requisição é que ele possua unicidade global e temporal, de forma que um mesmo NAS possa interagir com diferentes servidores RADIUS e que ataques do tipo repetição (*replay attacks*) sejam evitados. A não observância dessas características na implementação do cliente RADIUS pode levar à ocorrência de problemas de segurança, conforme [RFC2865].

É apropriado ressaltar que, para a verificação de integridade de uma mensagem Requisição de Acesso, [RFC2869] propõe a utilização de um atributo específico, chamado de *Message-Autenticator*, onde a função HMAC-MD5 elaborada por [RFC2104] é aplicada sobre a concatenação dos campos Tipo, Identificador, Tamanho, Autenticador e Atributos, utilizando a senha compartilhada como chave. Por incluir os atributos no cálculo, o valor a ser utilizado para o próprio atributo *Message-Autenticator* no processo de cálculo é uma seqüência de 16 *bytes* de valor zero.

Dessa forma, o servidor RADIUS poderia, ao receber uma Requisição de Acesso com o atributo *Message-Autenticator*, realizar o mesmo processo de cálculo utilizado pelo cliente RADIUS e, caso o valor calculado pelo servidor coincida com o valor do atributo presente na requisição, a requisição é considerada íntegra. Caso contrário, existe a certeza que a requisição foi adulterada, devendo ser descartada pelo servidor.

Campo Autenticador em mensagens Requisição de Bilhetagem (*Accounting-Request*), Requisição de Desconexão (*Disconnect-Request*) e Requisição de Mudança de Autorização (*CoA-Request*)

Nesses tipos de mensagem, o campo Autenticador também é chamado de Autenticador da Requisição, porém contém o *hash* MD5 calculado sobre a concatenação dos campos Código, Identificador, Tamanho, 16 *bytes* de valor 0, Atributos, incluindo também na concatenação a senha compartilhada.

Afirma [RFC2866] que a forma de geração do Autenticador da Requisição para uma mensagem do tipo Requisição de Acesso e para uma do tipo Requisição de Bilhetagem é diferente, pois, nesta última, o atributo correspondente à senha do usuário final não está presente.

Campo Autenticador em mensagens Acesso Permitido (*Access-Accept*), Acesso Rejeitado (*Access-Reject*), Requisição de Desafio (*Access-Challenge*), Bilhetagem Aceita (*Accounting Response*), Desconexão Aceita (*Disconnect-ACK*), Desconexão não Aceita (*Disconnect-NAK*), Mudança de Autorização Aceita (*CoA-ACK*) e Mudança de Autorização não Aceita (*CoA-NAK*)

Nessas mensagens o campo Autenticador passa a ser chamado de Autenticador da Resposta (*Response Authenticator*). Ele deve ser preenchido pelo servidor RADIUS com o resultado da operação *hash* MD5 realizada sobre a concatenação dos campos Código, Identificador, Tamanho, o Autenticador da Requisição (para a qual esta resposta foi elaborada), Atributos e, por fim, a senha compartilhada.

O cliente RADIUS que recebe a mensagem deve efetuar o mesmo procedimento de cálculo (*hash* MD5) para decidir por aceitar a resposta caso o resultado coincida ou por descartar tal resposta, caso contrário.

Percebe-se, então, a importância da senha compartilhada. Segundo [RFC2865], a senha compartilhada deve ser tal como uma senha bem escolhida, possuindo pelo menos 16 caracteres e sendo de difícil adivinhação, o que deve ser suficiente para prover proteção contra ataques de busca exaustiva. Alerta [NAKHJIRI2005] que muitos administradores utilizam a mesma senha compartilhada para todos os NAS para evitar as complicações de

manter uma senha por elemento de rede e que, ao contornar este problema de escala, abrem oportunidade para falhas de segurança.

3.3.4.5 - Campo Atributos

O campo Atributos é de tamanho variável e contém uma lista de zero ou mais atributos, no formato descrito na seção 3.3.3.

3.3.5 - Algoritmo de ocultação de senha

O algoritmo de ocultação de senha (*password hiding algorithm*) é um mecanismo utilizado como medida de segurança para que, em mensagens de Requisição de Acesso, a senha do cliente final não seja transmitida tal qual foi digitada ou configurada.

Esse mecanismo, desenvolvido por [KAUFMAN1995] e adotado por [RFC2865], utiliza três dados de entrada: a senha compartilhada entre o cliente e o servidor RADIUS, o valor aleatório criado para o campo Autenticador do pacote RADIUS de Requisição de Acesso e a senha do cliente final. O resultado, chamado de "senha oculta", será atribuído ao atributo *Password* da mensagem de Requisição de Acesso.

De posse dos três dados de entrada, inicialmente a senha do cliente final é dividida em blocos de 16 *bytes*. Caso o bloco final não possua 16 *bytes*, é completado com *bytes* de valor 0xFF (base hexadecimal) até atingir os 16 *bytes*. Cada bloco de 16 *bytes* denomina-se p_i .

A seguir a senha compartilhada (SC) e o Autenticador da Requisição (AR) são concatenados e, sobre este resultado, é calculado o *hash* MD5. É feita, então, uma operação lógica XOR bit-a-bit entre o primeiro bloco de 16 *bytes* da senha do usuário final e o *hash* MD5, cujo resultado chamar-se-á c_1. Podemos representar esta operação da seguinte maneira:

$$c_1 = p_1 \text{ XOR } MD5(SC+AR) \qquad (3.1)$$

Caso exista um segundo bloco p_2, a operação a seguir deverá ser realizada:

$$c_2 = p_2 \text{ XOR } MD5(SC+c_1) \quad (3.2)$$

Para cada bloco de 16 *bytes* p_i, executa-se, então, a seguinte operação:

$$c_i = p_i \text{ XOR } MD5(SC+c_{i-1}) \quad (3.3)$$

Onde o valor de c_0 corresponde ao valor do Autenticador da Requisição.

A senha oculta é o resultado da concatenação seqüencial dos blocos cifrados c_i calculados pelas operações acima.

Ao receber a mensagem de Requisição de Acesso, o servidor RADIUS executa o processo inverso para obter a senha do usuário final na forma original.

3.3.6 - Funcionamento do protocolo RADIUS

Nesta seção será descrito o funcionamento básico do protocolo RADIUS, partindo de uma composição simples e passando para as situações comumente encontradas em redes de operadoras de telecomunicações como a da Brasil Telecom.

A seção 3.2.1 deste trabalho versou sobre o protocolo PPP, que é o protocolo utilizado para estabelecer o acesso dos usuários de serviços ADSL ao elemento de terminação na rede da operadora de telecomunicações, o NAS. Na seqüência, dois métodos de autenticação foram apresentados: o PAP (*Password Authentication Protocol*) e o CHAP (*Challenge Handshake Authentication Protocol*).

Será discutido a seguir como o protocolo RADIUS é utilizado com cada um destes métodos de autenticação.

3.3.6.1 - Funcionamento da autenticação com PAP

O cliente final possui credenciais de acesso, habitualmente conhecidas como nome do usuário e senha, que são inseridas na configuração do dispositivo que iniciará o estabelecimento da sessão PPP. As trocas de mensagens que serão apresentadas a seguir podem ser acompanhadas através da Figura 3.8.

Durante a fase de autenticação, o NAS recebe essas credenciais do usuário final e gera e encaminha uma mensagem Requisição de Acesso para o servidor RADIUS. Para essa requisição foi criado um Autenticador da Requisição que, em conjunto com a senha compartilhada entre o NAS e o servidor RADIUS, foi utilizado para ocultar a senha do cliente final através do mecanismo apresentado na seção 3.3.5.

Uma vez encaminhada a mensagem de Requisição de Acesso, o NAS aguarda uma resposta. Caso não receba uma resposta dentro de um período pré-determinado, ele pode retransmitir a mensagem, seja para o mesmo servidor RADIUS, seja para outro, conforme sua configuração.

O servidor RADIUS, ao receber a mensagem de Requisição de Acesso, verifica sua origem com base no endereço IP utilizado para enviá-la. Caso esse endereço IP esteja em sua configuração como origem válida e possua uma senha compartilhada associada, ele processa o pacote para recuperar os atributos presentes na mensagem. Caso contrário, o servidor deve descartar a requisição.

Com base no Autenticador da Requisição e na senha compartilhada que o servidor possui com o NAS, o servidor RADIUS recupera a senha do cliente final e utiliza o nome do usuário como chave de busca para localizar o cliente final em uma base de dados.

Se o usuário for encontrado na base de dados e a senha correspondente, lá registrada, coincidir com a senha contida na Requisição de Acesso, o servidor RADIUS responde encaminhando ao NAS uma mensagem de Acesso Permitido. Pressupõe-se, em tal situação, que as condições de autorização eventualmente presentes foram validadas.

Caso o usuário não seja encontrado ou a senha não coincida, ou, ainda, alguma outra condição de autorização não seja preenchida, o servidor RADIUS responde ao NAS com uma mensagem de Acesso Rejeitado.

Percebe-se que a condição de não coincidência de senha pode ocorrer porque a senha registrada na base de dados é diferente da configurada pelo cliente final ou porque a senha compartilhada configurada no NAS é diferente da configurada no servidor, ou, ainda, devido a ambas as possibilidades.

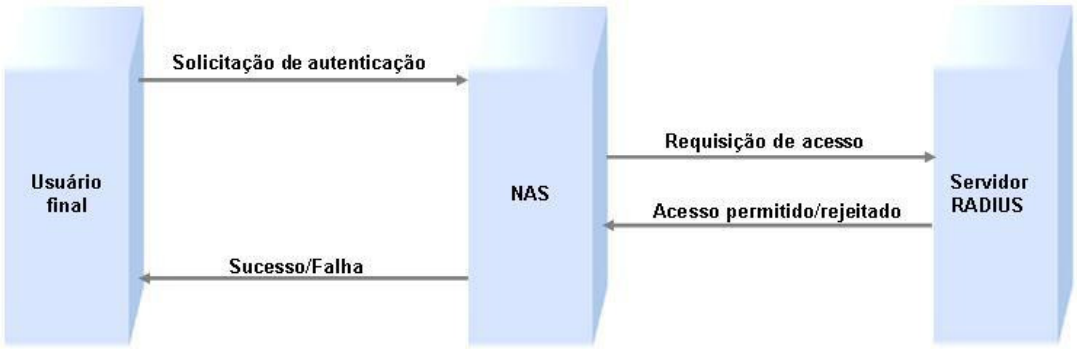

Figura 3.8: Operação PAP

De posse da resposta do servidor RADIUS, o NAS prossegue no estabelecimento da conexão PPP, conforme apresentado na seção 3.2.1, ou finaliza a negociação negando a conexão, situação na qual o cliente final poderá reiniciar o processo PPP, conforme estiver configurado.

3.3.6.2 - Funcionamento da autenticação com CHAP

Quando o NAS e o cliente final negociarem a utilização de CHAP durante a fase de autenticação do PPP, o NAS criará um valor de 16 *bytes*, chamado de CHAP *Challenge* (desafio) que será enviado ao usuário final, em conjunto com um identificador da operação CHAP, denominado CHAP *Id*, de tamanho 1 *byte*. As trocas de mensagens que são apresentadas nesta seção podem ser acompanhadas através da Figura 3.9.

O usuário final responderá ao NAS com seu nome do usuário e o resultado de uma operação MD5, feita para a concatenação do CHAP *Id* com a sua senha (chamada nesta operação de *secret*) e com o CHAP *Challenge*, conforme abaixo:

$$\text{Resposta} = \text{MD5}(\text{CHAP } Id, secret, \text{CHAP } Challenge) \quad (3.4)$$

De posse dessa resposta, o NAS criará uma mensagem de Requisição de Acesso, incluindo nela também o CHAP *Challenge* e o nome do usuário. Caso o CHAP *Challenge* coincida com o Autenticador da Requisição, não é necessário enviar o primeiro na forma de um atributo. O CHAP *Id* e a resposta ao desafio são concatenados e enviados no atributo chamado *CHAP-Password.*

O servidor, ao receber a requisição, identificará a presença do atributo *CHAP-Password*, o que indicará que se trata de uma requisição CHAP.

Da mesma forma que no processamento de uma requisição com PAP, o servidor buscará em sua base de dados pelo nome do usuário. Para o CHAP, porém, ele necessita recuperar a senha armazenada e realizar a mesma operação feita pelo NAS (equação 3.4) para posteriormente comparar com o valor presente na Requisição de Acesso para o atributo *CHAP-Password*, excluído deste último o *byte* inicial referente ao CHAP-*Id*.

Caso a comparação indique coincidência, o servidor RADIUS responderá com uma mensagem Acesso Permitido, caso contrário, com Acesso Rejeitado.

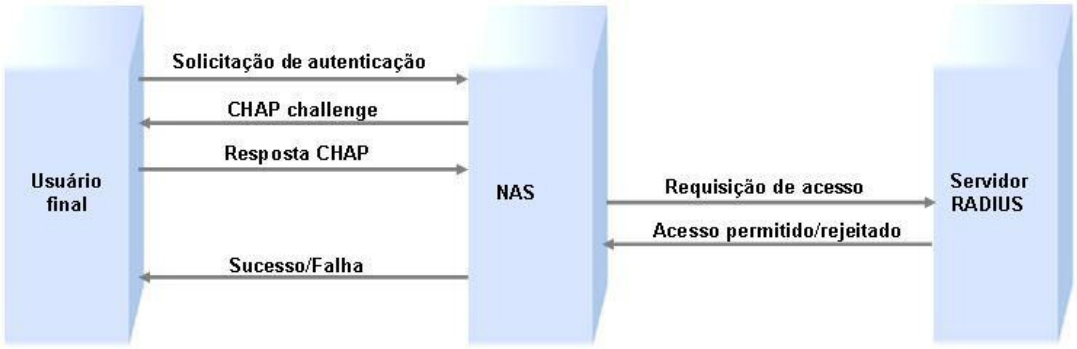

Figura 3.9: Operação CHAP

Conforme a resposta recebida do servidor RADIUS, o NAS prossegue no estabelecimento da conexão PPP, segundo apresentado na seção 3.2.1, ou encerra a negociação. Nessa última situação o cliente final poderá reiniciar ou não o processo PPP, a seu critério. A Figura 3.9 sumariza a operação CHAP.

3.3.6.3 - Funcionamento da bilhetagem

Uma vez estabelecida a conexão PPP, o NAS envia ao servidor RADIUS uma mensagem do tipo Requisição de Bilhetagem, contendo um conjunto de informações representativas da conexão. O servidor RADIUS, por sua vez, processa a Requisição de Bilhetagem e envia ao NAS uma mensagem Bilhetagem Aceita.

Caso o NAS não receba a confirmação de que o servidor recebeu e processou a Requisição de Bilhetagem ele pode, conforme sua configuração, reenviar a Requisição de Bilhetagem ao servidor.

A Figura 3.10 representa a situação descrita acima. Não está indicado nessa figura, contudo, que quando do encerramento da conexão PPP, uma seqüencia de mensagens de Requisição de Bilhetagem e Bilhetagem Aceita irá ocorrer para efetuar o transporte de informações relativas à conexão.

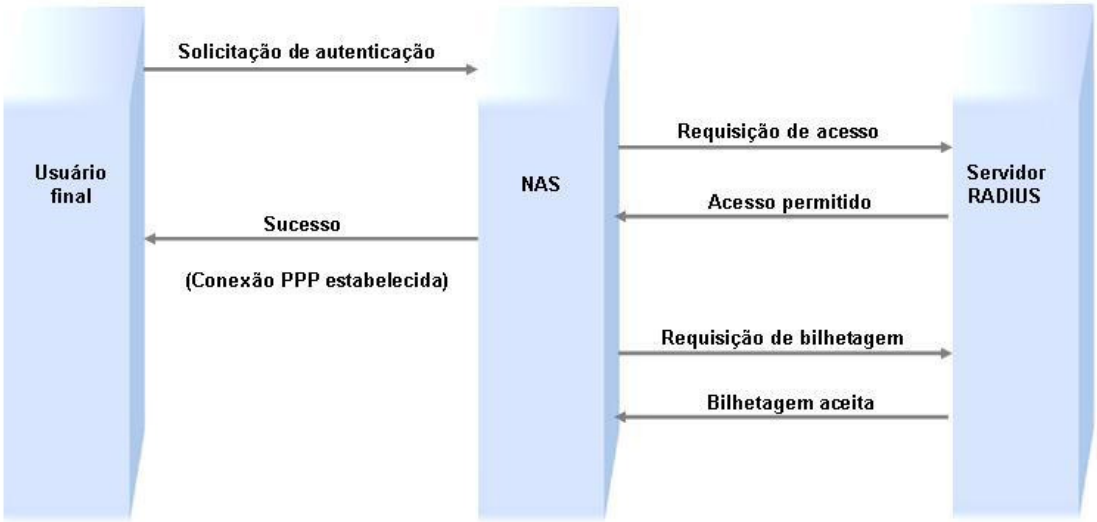

Figura 3.10: Funcionamento da bilhetagem

3.3.6.4 - Funcionamento da autenticação através do Provedor de Serviços Internet

Quando a autenticação deva ser feita através de um provedor de serviços Internet, o servidor RADIUS da operadora recriará a mensagem de Requisição de Acesso que recebeu do NAS e encaminhará essa nova Requisição de Acesso para o servidor RADIUS do provedor.

Conforme a resposta recebida do servidor RADIUS do provedor para esta requisição, o servidor RADIUS da operadora encaminhará como resposta ao NAS uma mensagem de Acesso Permitido ou de Acesso Rejeitado.

A Figura 3.11 apresenta o funcionamento da autenticação utilizando um provedor de serviços Internet, que é uma operação de autenticação inter-domínio, pelo fato de as mensagens relacionadas com a operação cruzarem as fronteiras de diferentes domínios administrativos. O conceito de domínio administrativo, nesse caso, refere-se ao apresentado por [RFC1136].

Também, nessa situação, os mecanismos de retransmissão de requisições do protocolo RADIUS podem ser utilizados.

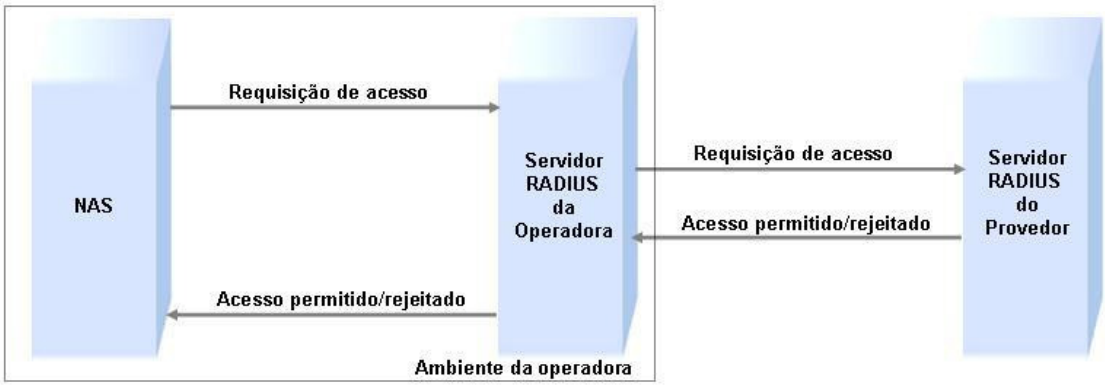

Figura 3.11: Autenticação inter-domínio.

3.3.6.5 - Diagrama completo

A Figura 3.12 apresenta as transações RADIUS usualmente ocorrentes durante uma conexão PPP entre o cliente final e o NAS. Não estão indicados os eventos de retransmissão de requisições, que podem estar presentes, mas, de forma proposital, algumas situações foram nela representadas.São elas:

- O processo de autenticação representado é PAP. Poderia ter sido CHAP, sem prejuízo das demais operações representadas. O único requisito para o uso do CHAP é que o servidor RADIUS do provedor trate a requisição CHAP adequadamente.

- O envio da mensagem de Acesso Permitido ao NAS pelo RADIUS da operadora só é feito após o recebimento da mensagem Acesso Permitido do servidor RADIUS do provedor. O acesso só é concedido ao usuário final depois de autenticado pelo provedor de serviços Internet.

- As mensagens de Bilhetagem Aceita são enviadas ao NAS antes do recebimento de mensagem similar oriunda do RADIUS do provedor, para demonstrar que o processo de armazenamento do bilhete pela operadora e o envio desse bilhete ao provedor podem ser feitos de forma dissociada.

- A mensagem de bilhetagem intermediária não é enviada ao provedor. É uma condição que pode ser programada, caso exista interesse do provedor em receber também esta mensagem.

- A conexão foi encerrada por solicitação do usuário final. Poderia ter sido encerrada por qualquer de outras razões previstas pelo protocolo PPP.

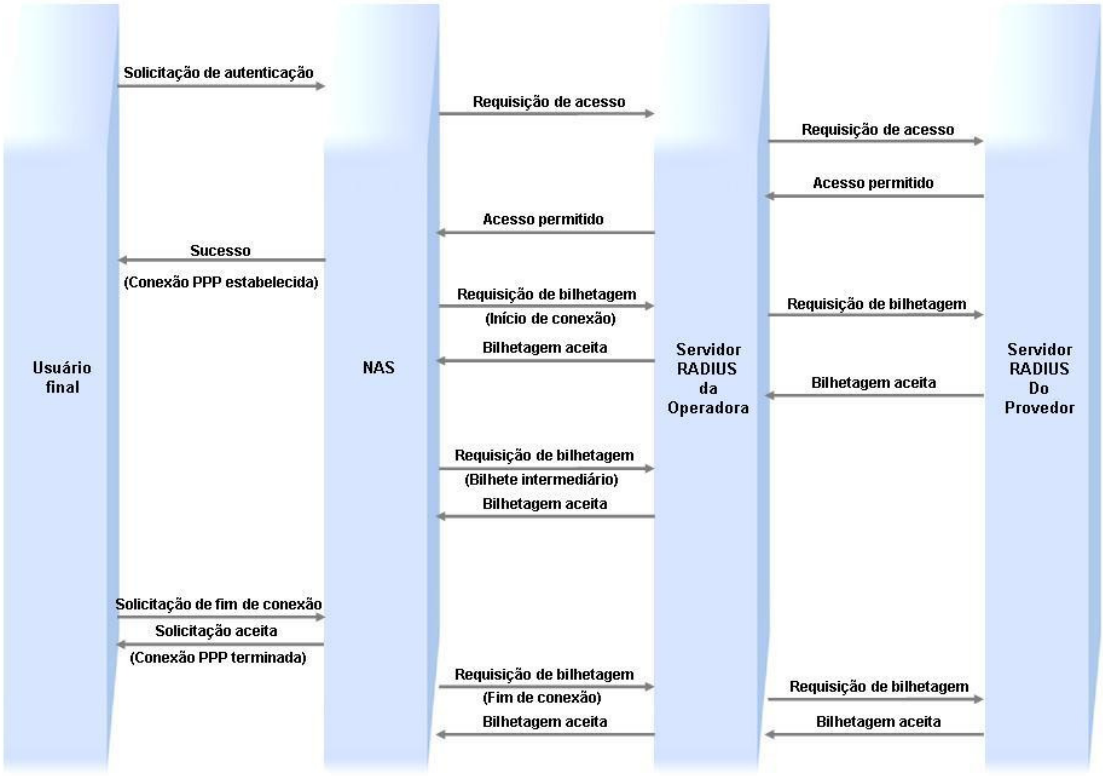

Figura 3.12: Diagrama de transações RADIUS

(Esta página foi intencionalmente deixada em branco.)

4 - SISTEMA PROPOSTO

4.1 - INTRODUÇÃO

Neste capítulo será apresentada a proposição de um sistema básico para realizar a contabilização de utilização por tempo e volume de dados trafegados de acessos ADSL, baseado na utilização do protocolo RADIUS.

Serão apresentados também os parâmetros de configuração relevantes ao tema e estratégias para o tratamento de requisições de autenticação, autorização e bilhetagem, visando à melhoria de desempenho de um sistema RADIUS utilizado em numa rede de acesso ADSL.

4.2 - OS PROCESSOS AAA

Cada sistema que implementa processos de autenticação, de autorização e de bilhetagem, realiza essa implementação de sua maneira particular, conforme os requisitos apresentados em especificações de serviço e nas normas pertinentes ao próprio sistema. A seguir serão apresentados os processos de autenticação, autorização e bilhetagem, na forma em que são habitualmente estabelecidos em uma rede de acesso ADSL.

4.2.1 - O processo de autenticação RADIUS

O tipo de autenticação existente nos serviços residenciais ADSL é uma autenticação do cliente. Esse cliente 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 utilizado 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. O NAS recebe as credenciais e as envia ao servidor RADIUS da operadora, que por sua vez, as encaminha ao servidor RADIUS do provedor de serviços Internet.

A operadora não possui registro destas credenciais, não sendo possível, então, com base nelas, associar a conexão PPP, estabelecida por esse cliente final, a qualquer um dos clientes da operadora.

Existe a hipótese da ocorrência de uma alteração significativa na regulamentação pertinente à oferta do serviço de banda larga através de tecnologia ADSL. Essa hipótese versa sobre a não obrigatoriedade da utilização de um provedor de acesso à Internet para que a conexão do usuário final seja estabelecida. Em tal hipótese, o problema ainda assim persistiria, pois apenas uma parcela das credenciais (a correspondente ao conjunto de clientes que desejam a autenticação realizada pela própria operadora) seria de conhecimento da operadora.

Uma proposta para fazer a associação entre a conexão PPP e o cliente da operadora é utilizar uma combinação entre alguns dos atributos constantes na Requisição de Acesso: o *NAS-IP-Address* ou o *NAS-Identifier*, com o *NAS-Port* ou o *NAS-Port-Id*.

O *NAS-Identifier* é o atributo que contém o nome designado ao equipamento, enquanto o *NAS-IP-Address* corresponde ao endereço IP utilizado pelo NAS para enviar a Requisição de Acesso. A vantagem em utilizar o *NAS-Identifier* é que o endereço IP do equipamento poderia ser alterado sem, no entanto, provocar a alteração na identificação do acesso.

O atributo *NAS-Port* recebe um valor do tipo inteiro que representa a conexão lógica entre o NAS e a porta física de um acesso de cliente no DSLAM ATM; corresponde à identificação do PVC (*Permanent Virtual Circuit*) ATM na interface do NAS.

Nas implementações observadas, o atributo *NAS-Port-Id*, por sua vez, recebe a representação da porta física de um acesso de cliente no DSLAM *Ethernet* quando é utilizada a forma de identificação proposta na recomendação [TR101], chamada “PPPoE

Intermediate Agent". Tal recomendação estabelece, contudo, que um atributo VSA sob o PEN designado ao *DSL Forum* (PEN 3561) seja utilizado para transmitir a informação de porta física; este atributo é o *Agent-Circuit-Id*, cujo campo Tipo é 1. Para as ponderações aqui apresentadas, vamos considerar que seja utilizado o *NAS-Port-Id*.

De posse da combinação entre *NAS-Identifier* e *NAS-Port* ou entre *NAS-Identifier* e *NAS-Port-Id*, presentes na mensagem de Requisição de Acesso, 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. Para saber qual das duas combinações deve ser utilizada para efetuar tal consulta, é necessário reconhecer, por algum outro atributo, qual é o tipo do acesso – o *NAS-Port-Type* seria um candidato a examinar. Existe, entretanto, uma solução bastante trivial: quando a técnica de identificação implementada é a PPPoE *Intermediate Agent* e o acesso é oriundo de DSLAM *Ethernet*, o valor correspondente ao que seria o VP (*Virtual Path*) ATM na representação do atributo *NAS-Port*, para este acesso, é igual a zero.

4.2.2 - 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 o estabelecimento da sessão deve ser negado em decorrência de falta de pagamento.

4.2.3 - 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.

O RADIUS utiliza o modelo de coleta de informações de utilização “disparado por evento”. Tão logo a informação de utilização esteja disponível, o NAS envia ao servidor RADIUS uma mensagem do tipo Requisição de Bilhetagem contendo tal informação. Apesar das vantagens que esse modelo de coleta apresenta, ele é mais suscetível à perda de dados em situações de congestionamento ou de falha de rede e, portanto, alguns cuidados devem ser tomados para minimizar as oportunidades de perda.

Uma das formas de minimizar o efeito da perda de informações de utilização é a chamada bilhetagem intermediária. Os equipamentos NAS utilizados pela operadora possibilitam a habilitação de bilhetagem intermediária, porém há de se determinar qual o valor mais adequado para o intervalo entre bilhetes, baseado na duração média das conexões ADSL. Uma maneira de realizar a avaliação da duração média da sessão será apresentada no capítulo 5.

A bilhetagem intermediária pode ser utilizada para tratar outra situação: a das conexões que iniciaram dentro de um ciclo de medição cujo final ultrapassa o dia do faturamento daquele ciclo de utilização.

Pelo fato do RADIUS utilizar o modelo de coleta de informações “disparado por evento”, apenas o evento de final de conexão irá gerar um bilhete com os totalizadores de utilização. Supondo-se que uma conexão inicie no penúltimo dia do mês civil, que é o ciclo habitual de utilização que é avaliado, e termine depois do dia 10 do mês civil subseqüente, se o faturamento foi fechado no dia 9, os dados de utilização desta conexão não estavam disponíveis e o consumo dos dois últimos dias do ciclo anterior não constará na fatura.

Para evitar esse problema, um intervalo de geração de bilhetagem intermediária apropriado poderia ser calculado no momento do estabelecimento da conexão e enviado ao NAS na mensagem de Acesso Permitido, de forma que um bilhete com a utilização parcial seja emitido em um instante próximo ao fim do ciclo de utilização, caso a conexão do cliente dure até tal momento.

Caso a identificação do cliente da operadora venha a ser realizada no momento da autenticação, é possível habilitar, ou não, a geração de bilhetes intermediários por conexão, com base no serviço contratado pelo cliente.

Dessa forma, é possível ter bilhetagem intermediária apenas para os clientes cujo serviço contratado é sensível ao uso. Ainda mais, é possível ajustar o tempo entre bilhetes para cada um destes clientes, conforme seu histórico de duração de sessões.

Outros critérios adicionais podem ser utilizados para definir a ativação, ou não, da bilhetagem intermediária, bem como o tempo entre os bilhetes. Um desses critérios pode ser o NAS no qual este usuário se conecta. Caso um NAS apresente um histórico de mensagens de bilhetagem sem resposta – estatística que pode ser coletada no NAS –, o servidor RADIUS pode ajustar (para as novas conexões) um tempo menor entre a emissão de bilhetes, visando a minimizar os efeitos da possível perda em decorrência de problemas de rede.

Com tal ajuste granular da bilhetagem intermediária, é possível chegar a uma solução de compromisso entre os benefícios da geração dos bilhetes e o consumo de recursos de banda, de processamento e de espaço de armazenagem despendidos pela sua geração.

4.3 - SEGURANÇA E CONFIABILIDADE DA BILHETAGEM

Foram apresentadas no capítulo 3 algumas preocupações relacionadas com a segurança e a confiabilidade da bilhetagem, que podem ser resumidas a uma frase: os dados de utilização devem refletir o uso do cliente e devem chegar ao servidor de bilhetagem.

A avaliação da veracidade dos dados de utilização será realizada com base em testes e apresentada no capítulo 5. Aqui será discutida a segunda parte da questão, que é a transferência dos dados de utilização entre o NAS e o servidor RADIUS.

Já se sabe que o protocolo RADIUS utiliza como transporte o protocolo UDP, e que este último não prevê retransmissão de pacotes em caso de perda. Diante disso, resta apenas procurar maneiras de minimizar os efeitos da eventual perda de mensagens. Uma delas é o uso de bilhetagem intermediária, discutido anteriormente. Outra é utilizar o mecanismo de retransmissão de mensagens previsto no protocolo RADIUS.

Sempre que um cliente RADIUS envia uma mensagem de bilhetagem a um servidor, ele aguarda uma resposta indicando o recebimento e processamento (mensagem de Bilhetagem Aceita). Caso essa resposta não seja recebida pelo cliente RADIUS dentro de um intervalo de tempo pré-determinado, o protocolo RADIUS prevê a possibilidade de retransmissão da mensagem.

O cuidado principal no ajuste de retransmissões é que o tempo de espera do cliente RADIUS pela confirmação do recebimento da mensagem pelo servidor seja superior ao tempo necessário para que a mensagem de bilhetagem não só chegue ao servidor, como seja processada, e volte ao cliente a mensagem de confirmação. Caso o tempo seja inferior, o cliente poderá gerar a retransmissão de uma mensagem que já está em processamento ou ainda cuja confirmação ainda não chegou. Nesse caso, ocorre apenas o consumo desnecessário de recursos de rede e de servidor.

Os NAS permitem um conjunto de configurações relacionado ao uso de servidores RADIUS. Essas configurações envolvem a adição de mais de um servidor RADIUS, a quantidade de retransmissões, o tempo de espera pela confirmação de recebimento, a ordem de utilização dos servidores configurados e ainda a ação a realizar caso o NAS perceba que um destes servidores não está operacional. Em geral, é possível dissociar dos servidores de bilhetagem os servidores de autenticação e autorização. De forma restrita, alguns NAS permitem também determinar algumas condições especiais para a geração, ou não, de bilhetes.

Vimos que os efeitos de perda de pacotes, da indisponibilidade do servidor de bilhetagem e de defeitos de rede podem ser reduzidos mediante o uso de um servidor de bilhetagem secundário.

Tal servidor secundário deve estar instalado, preferencialmente, em ambiente fisicamente distinto do ambiente do servidor primário, para evitar que situações ambientais (incêndio, queda de energia, problemas de rede, por exemplo) afetem ambos os servidores. Esta situação está representada na Figura 4.1.

Enquanto a autenticação é feita para todas as conexões em fase de estabelecimento – e muitas das autenticações não têm sucesso – , a bilhetagem é feita apenas para conexões que efetivamente foram estabelecidas.

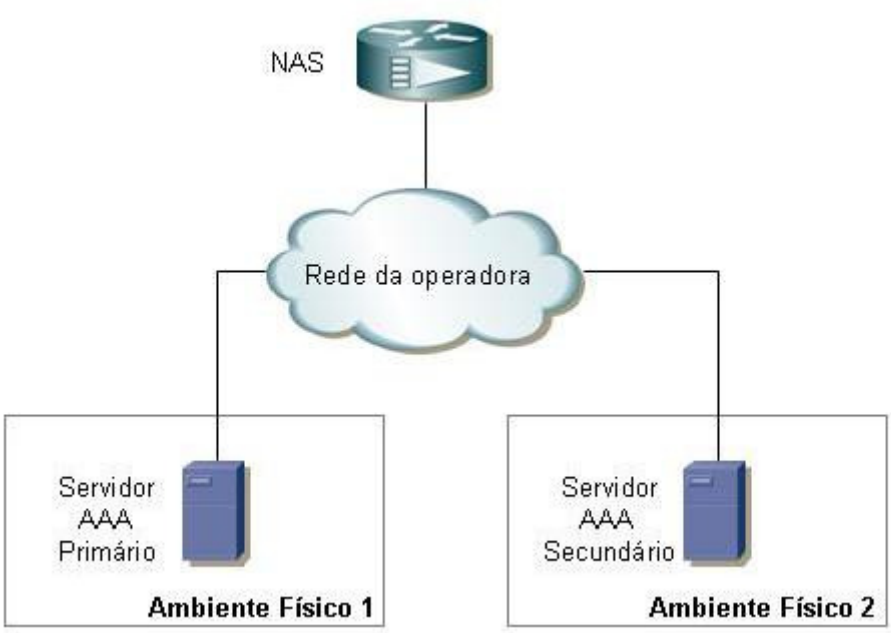

Figura 4.1: Servidores AAA instalados em ambientes distintos.

Outro fator a considerar visando a minimizar a perda de bilhetes é o comportamento do modem ADSL quando ele está configurado como roteador. Nessa condição o modem, ao ser ligado, procura estabelecer uma conexão PPP e, tão logo uma conexão PPP é terminada, o modem reinicia o seu processo PPP visando a re-estabelecer a conexão. Caso as credenciais utilizadas para a conexão não permitam a autenticação do cliente final, o resultado é uma rajada de pedidos de autenticação que só terminará com o desligamento do modem ou com a correção das credenciais.

Eventos que resultam em não autenticação de clientes finais de forma massiva, tais como o bloqueio financeiro de um grande número de usuários, ou a indisponibilidade temporária de servidores de autenticação de provedores de serviços Internet, podem provocar a sobrecarga dos servidores RADIUS da operadora.

Assim, a segregação da função de bilhetagem das funções de autenticação e autorização também melhora a disponibilidade da plataforma para o recebimento dos bilhetes, pois assim os fenômenos relacionados com a autenticação não afetarão os processos de bilhetagem. Esta situação está representada na Figura 4.2.

Na adoção da segregação das funções de autenticação e autorização da função de bilhetagem, deve-se ter em consideração que informações contidas nos bilhetes podem ser necessárias para a tomada de decisões de autorização, devendo, nesses casos, tais informações serem disponibilizadas, pelo servidor de bilhetagem, ao servidor responsável pela autorização.

Por fim, a situação de reinicialização não programada de um NAS com conexões PPP ativas resulta na perda dos bilhetes de encerramento destas conexões. Para essa situação deve ser utilizada a "bilhetagem de arquivo", vista na seção 3.1.3.1, aproveitando os bilhetes intermediários disponíveis e a mensagem que o NAS, ao reinicializar, envia ao servidor de bilhetagem indicando a sua reinicialização.

Quando a reinicialização é programada, é possível forçar a desconexão dos usuários previamente, o que resultará na geração dos bilhetes de encerramento correspondentes.
Com base nessa análise, a topologia básica para reduzir os efeitos de falhas de rede no registro de bilhetes contempla a segregação de servidores para realizar as funções de autenticação/autorização e bilhetagem, bem como a duplicação de tais recursos em ambientes geograficamente distintos.

Figura 4.2: Segregação de funções de Autenticação e Bilhetagem

Em geral o elemento de rede que é desenvolvido para o ambiente de telecomunicações possui uma série de recursos intrínsecos para aumentar a sua disponibilidade. Em razão dessa característica, o elo mais fraco passa a ser o ponto de interconexão entre os elementos de rede. Assim, para reduzir ainda mais a oportunidade de que falhas de rede prejudiquem a comunicação entre os elementos que a compõem, é interessante dotar de dupla conectividade todos os elementos envolvidos.

Com base nessas duas considerações, temos como resultado o modelo básico que é proposto na Figura 4.3: segregação de funções para os servidores, servidores primários e secundários em ambientes geograficamente distintos e estabelecimento de dupla conectividade entre os elementos envolvidos. Esse modelo básico pode ser replicado para acompanhar o crescimento da rede ADSL, traduzido no aumento de elementos NAS decorrente da ampliação de portas de acesso.

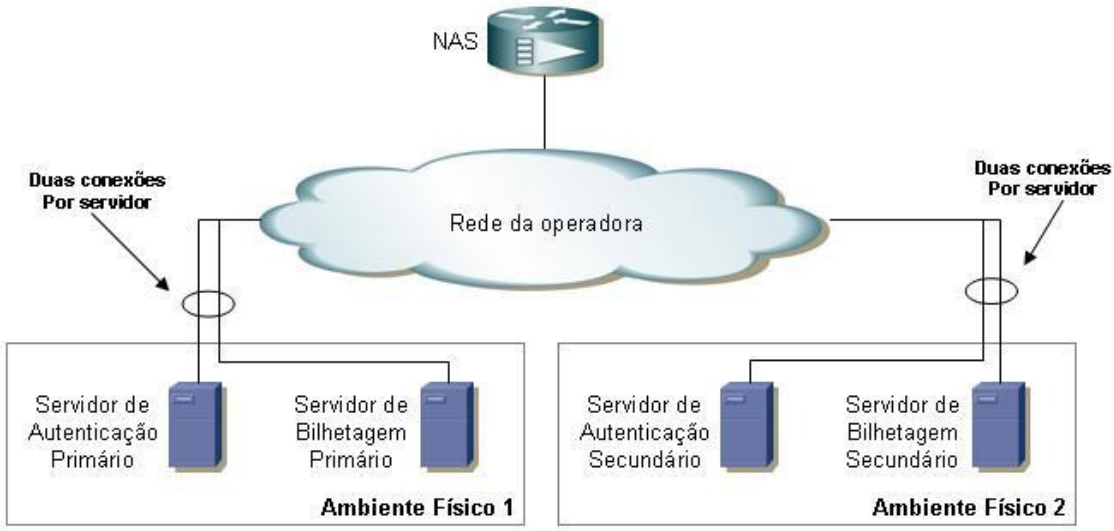

Figura 4.3: Modelo básico de um ambiente AAA para rede ADSL.

Caso a operadora possua atuação em mais de uma área geográfica, os conjuntos de servidores podem ser distribuídos entre os pontos principais – em termos de disponibilidade de infra-estrutura em cada área geográfica –, configurando os NAS de cada uma dessas regiões para utilizar o conjunto de servidores da sua região como primários e o de outra região como secundários. O único cuidado nesse arranjo é que os servidores devem ser capazes de suportar a carga conjunta das regiões envolvidas.

4.4 - O BILHETE RADIUS

O bilhete RADIUS, que será examinado a seguir, é a forma de registro de utilização de um serviço ADSL. Esse registro de utilização é gerado pelo NAS e enviado, utilizando o protocolo RADIUS, até o servidor de bilhetagem.

O bilhete pode ser armazenado de diversas maneiras, como se verá adiante. Para possibilitar um melhor entendimento, os bilhetes (ou trechos de um bilhete) serão apresentados sempre no formato criado por [LIVINGSTON].

Nesse formato, o registro inicia com a informação de data e hora (carimbo de tempo ou *timestamp*) e é seguido por uma lista de pares atributo-valor, um abaixo do outro, conforme a Figura 4.4.

```
Sat Nov 03 08:00:13 GMT-03:00 2007
        Acct-Status-Type = Stop
        User-Name = "clientefinal@provedor.com.br"
        Event-Timestamp = 1194087596
        Acct-Delay-Time = 18
        Acct-Session-Id = "erx GigabitEthernet 3/0.1620:1620:0179077986"
        NAS-IP-Address = 200.215.97.250
        Class = "PAENRAS01_SC_OK_DEF_CLF_0"
        Service-Type = Framed-User
        Framed-Protocol = PPP
        Framed-Compression = None
        Unisphere-PPPoE-Description = "pppoe 00:15:e9:28:db:2f"
        Framed-IP-Address = 201.25.207.3
        Framed-IP-Netmask = 255.255.255.255
        Unisphere-Ingress-Policy-Name = "de_usuario"
        Unisphere-Egress-Policy-Name = "para_usuario_RATE"
        Calling-Station-Id = "#JVECE701#E30#1620"
        Acct-Input-Gigawords = 0
        Acct-Input-Octets = 20010
        Acct-Output-Gigawords = 0
        Acct-Output-Octets = 13029
        Unisphere-Input-Gigapackets = 0
        Acct-Input-Packets = 20
        Unisphere-Output-Gigapackets = 0
        Acct-Output-Packets = 70
        NAS-Port-Type = Ethernet
        NAS-Port = 805307988
        NAS-Port-Id = "GigabitEthernet 3/0.1620:1620"
        Acct-Authentic = RADIUS
        Acct-Session-Time = 21073
        Acct-Terminate-Cause = User-Request
        NAS-Identifier = "JVECE701"
```

Figura 4.4: Bilhete RADIUS no formato proposto por [LIVINGSTON]

O tipo de mensagem RADIUS que envia as informações de utilização dos serviços do NAS ao servidor de bilhetagem é Requisição de Bilhetagem. Uma vez recebida e processada pelo servidor, este último envia ao NAS o reconhecimento da requisição, através de uma mensagem Bilhetagem Aceita. Caso não tenha sido possível processar a requisição, nada deve ser enviado ao NAS.

Uma Requisição de Bilhetagem pode ter todos os atributos RADIUS que possam ser utilizados em uma mensagem de Requisição de Acesso ou de Acesso Permitido, exceto um pequeno grupo de atributos composto por *User-Password*, *CHAP-Password*, *Reply-Message* e *State*.

Existem mais três regras básicas relacionadas com a presença de atributos na mensagem de Requisição de Bilhetagem.

A primeira é que, segundo [HASSEL2002] os atributos *NAS-IP-Address* e *NAS-Identifier* são mutuamente exclusivos, ou seja, apenas um deles pode estar presente na Requisição de Bilhetagem. Afirma [RFC2866], porém que: "*An Accounting-Request MUST contain either a NAS-IP-Address or a NAS-Identifier (or both)*", ou seja, que, em uma Requisição de Bilhetagem, pelo menos um desses dois atributos, *NAS-IP-Address* ou *NAS-Identifier* deve estar presente. Percebe-se, examinando os bilhetes armazenados nos servidores RADIUS da plataforma ADSL, que habitualmente ambos os atributos estão presentes.

A segunda regra é que a mensagem deve conter pelo menos um de dois atributos relacionados com a interface de conexão do usuário: *NAS-Port* ou *NAS-Port-Type*; habitualmente, ambos os atributos estão presentes. [RFC2869] introduz um novo atributo, chamado *NAS-Port-Id*, cujo objetivo é fornecer uma descrição da interface de conexão. A presença desse último atributo na mensagem de Requisição de Bilhetagem não é obrigatória.

Por fim, a terceira regra é que o endereço IP contido no atributo *Framed-IP-Address* corresponda efetivamente ao endereço atribuído ao cliente final.

4.5 - ATRIBUTOS ESPECÍFICOS PARA BILHETAGEM

Existe um conjunto de atributos específicos para o processo de bilhetagem, e alguns desses atributos, apresentados a seguir, devem ser tidos em conta para a correta interpretação de um bilhete. Esses atributos serão utilizados, em conjunto, para o cômputo da utilização dos serviços ADSL por tempo de utilização e por volume de tráfego.

4.5.1 - *Acct-Status-Type*

O NAS possui capacidade para geração de bilhetes como resultado do início de uma conexão, de uma desconexão, ou, ainda, de uma avaliação intermediária da conexão, conforme configuração.

Nos bilhetes, cada uma dessas três situações é identificada pelo valor do atributo *Accounting-Status-Type*. Se o valor for *Start*, o bilhete possui informações sobre o início de uma conexão. Para a avaliação intermediária e para o final de uma conexão, os valores são, respectivamente, *Interim-Update* e *Stop*. Esse atributo pode conter ainda o valor *Accounting-On*, que indica a reinicialização de um NAS.

O bilhete da Figura 4.4 é um bilhete de fim de conexão, pois o valor para o seu atributo *Accounting-Status-Type* é *Stop*.

4.5.2 - *Acct-Delay-Type*

O valor desse atributo indica o tempo em segundos que o NAS levou para conseguir enviar com sucesso o bilhete, sem contar o tempo de trânsito da mensagem de Requisição de Bilhetagem. Um valor maior que zero indica, portanto, que se trata de um bilhete que ou sofreu retransmissão ou foi enviado para um servidor alternativo.

O bilhete da Figura 4.4 é um bilhete que foi recuperado de um servidor secundário; de fato, o valor para o seu atributo *Acct-Delay-Type* é 18, o que corresponde ao valor de espera de 18 segundos ajustado no NAS para realizar uma nova tentativa de envio.

Subtraindo do valor do carimbo de tempo do bilhete o valor deste atributo, é possível chegar ao momento da ocorrência do evento informado pelo bilhete, desprezado o tempo de trânsito da Requisição de Bilhetagem.

Sua ausência no bilhete – esse atributo não possui presença obrigatória – é equivalente a sua presença com valor 0.

4.5.3 - *Acct-Input-Octets*

Sua presença no bilhete indica a quantidade de *bytes* que passaram através da interface associada ao cliente, no sentido do cliente para o NAS. Deve ser utilizado em conjunto com o atributo *Acct-Input-Gigawords* para calcular o tráfego total de entrada no NAS que é oriundo do cliente.

4.5.4 - *Acct-Output-Octets*

Sua presença no bilhete indica a quantidade de *bytes* que passaram através da interface associada ao cliente, no sentido do NAS para o cliente. Deve ser utilizado em conjunto com o atributo *Acct-Output-Gigawords* para calcular o tráfego total de saída do NAS em direção ao cliente.

4.5.5 - *Acct-Session-Id*

Este atributo é utilizado para identificar uma sessão de forma única, de maneira que os bilhetes de início e fim de conexão, bem como os bilhetes intermediários, possam ser correlacionados. Bilhetes com o mesmo *Acct-Session-Id* correspondem à mesma conexão.
Segundo [HASSEL2002], porém, muitos clientes RADIUS tendem a não enviar o atributo *Acct-Session-Id* com valores únicos. Em razão disto, seria necessário examinar a regra de formação deste atributo para verificar as condições nas quais um mesmo valor poderá ser reutilizado. No entanto é possível reduzir os efeitos causados pela reutilização de valores para *Acct-Session-Id* através da combinação desse atributo com outros atributos presentes no bilhete, tais como *User-Name*, *NAS-IP-Address, Framed-IP-Address* e *NAS-Port-Id* para realizar a conciliação entre bilhetes de uma mesma conexão.

4.5.6 - *Acct-Session-Time*

Este atributo indica em segundos o tempo durante o qual um usuário final esteve conectado ao NAS. Sua presença no bilhete, porém, não é obrigatória, e será alvo de exame no capítulo 5.

4.5.7 - *Acct-Input-Packets*

Sua presença no bilhete indica a quantidade de pacotes que passaram através da interface associada ao cliente, no sentido do cliente para o NAS.

4.5.8 - *Acct-Output-Packets*

Sua presença no bilhete indica a quantidade de pacotes que passaram através da interface associada ao cliente, no sentido do NAS para o cliente.

4.5.9 - *Acct-Input-Gigawords*

Sua presença no bilhete indica a quantidade de vezes que o contador de *bytes* do atributo *Acct-Input-Octets* ultrapassou seu valor máximo de 4.294.967.296.

4.5.10 - *Acct-Output-Gigawords*

Sua presença no bilhete indica a quantidade de vezes que o contador de *bytes* do atributo *Acct-Output-Octets* ultrapassou seu valor máximo de 4.294.967.296.

4.5.11 - *Event-Timestamp*

Este atributo indica o instante de tempo em que ocorreu o evento que originou o bilhete. O valor desse atributo corresponde ao número de segundos decorridos desde o início do dia 1º de janeiro de 1970, considerando o fuso horário de Greenwich (GMT), até o momento de ocorrência do evento.

O início do dia 1º de janeiro de 1970 foi o momento escolhido como a referência, ou *epoch*, para as medidas de tempo para diversos sistemas computacionais. Consta que a escolha não foi aleatória, pois esta data, segundo [IET2001], corresponde ao dia do nascimento do sistema operacional UNIX.

Considerando que o atributo *Event-Timestamp* é do tipo inteiro, de 32 bits, ele é capaz de descrever, em segundos, o tempo decorrido de forma inequívoca até o dia 19 de janeiro de 2038, às 03h 14m 07s, no fuso GMT, totalizando 2.147.483.647 segundos transcorridos desde 1º de janeiro de 1970 (considerando que esse contador poderia representar uma quantidade de tempo anterior ao marco inicial, com sinal negativo). Aponta [IET2001] que pequenas diferenças de tempo, da ordem de alguns segundos, poderão ser encontradas quando da avaliação de datas baseadas nesse tipo de contabilização de tempo, em razão dos ajustes do tipo *leap second* que vêm sendo realizados desde 1972 na referência de tempo civil e que podem não ser tratadas corretamente pelos sistemas computacionais. Até próximo ao ano de 2038, portanto, nenhuma adequação se faz necessária nos sistemas e no tratamento deste atributo.

4.6 - AVALIAÇÃO DA DURAÇÃO DE UMA CONEXÃO

Existem pelo menos três maneiras de avaliar a duração de uma sessão, apresentadas e discutidas a seguir.

A primeira utiliza uma informação que não está relacionada diretamente com a conexão do usuário, que é o carimbo de tempo do bilhete. Este carimbo de tempo, que é a informação de data e hora que precede os diversos atributos contidos em um bilhete, indica o momento que o bilhete foi processado e gravado pelo servidor de bilhetagem.
Apesar do desejo de que as informações de início e fim de conexão estejam imediatamente disponíveis no servidor de bilhetagem, não existe garantia de que não tenha ocorrido um atraso significativo entre o evento que gerou o bilhete e o momento da recepção e processamento deste bilhete pelo servidor de bilhetagem.

Não existindo uma melhor alternativa, a utilização dessa técnica para determinar o tempo de conexão (T_C) pode, de forma simplificada, ser representada na equação a seguir:

$$T_C = (CT_{stop} - CT_{start}) - ADT_{stop} + ADT_{start} \quad (4.1)$$

Onde: CT_{stop} corresponde ao carimbo de tempo do bilhete de fim de conexão;
CT_{start} é o carimbo de tempo do bilhete de início de conexão;
ADT_{stop} é o valor do atributo *Acct-Delay-Time* no bilhete de fim de conexão e
ADT_{start} é o valor do atributo *Acct-Delay-Time* no bilhete de início de conexão.

Perceba o leitor que a subtração entre os selos de tempo resultará em um valor relacionado a uma quantidade de tempo, que deve ser convertido em segundos para que o restante da equação seja avaliado. O tempo de trânsito do bilhete, entre o NAS e o servidor de bilhetagem, nessa técnica, não é considerado.

A segunda técnica para determinar a duração de uma conexão é a que utiliza os valores do atributo *Event-Timestamp* dos bilhetes de início e fim de conexão. Nessa técnica, o tempo de conexão T_C é calculado através da equação 4.2:

$$T_C = (ET_{stop} - ET_{start}) \quad (4.2)$$

Onde: ET_{start} é o valor do atributo *Event-Timestamp* do bilhete de início de conexão.
ET_{stop} é o valor do atributo *Event-Timestamp* do bilhete de fim de conexão.

Essa segunda técnica para avaliar a duração da sessão apresenta uma vantagem significativa frente à primeira: em decorrência de o valor do atributo *Event-Timestamp* representar o momento real dos eventos de início e de fim de conexão, o tempo de trânsito, o de atraso por retransmissão e o de processamento não influenciam no valor obtido para o tempo de conexão, considerando a operação normal de todos os equipamentos envolvidos.

A terceira forma de obter o tempo de conexão é utilizar o valor do atributo *Acct-Session-Time*. Este atributo, quando presente, informa o tempo de conexão em quantidade de segundos, conforme a equação 4.3:

$$T_C = AST \quad (4.3)$$

Onde: AST é o valor do atributo *Acct-Session-Time* encontrado no bilhete de fim de conexão.

A principal vantagem dessa última técnica frente às demais é que, não sendo necessário avaliar o conteúdo do bilhete de início de conexão, não é necessário localizar tal bilhete, o que representa um ganho de tempo de processamento nas situações onde não existe bilhetagem intermediária. Tal como a segunda técnica, os tempos de trânsito, de atraso por retransmissão, e de processamento não influenciam no valor obtido para o tempo de conexão.

4.7 - AVALIAÇÃO DO VOLUME DE TRÁFEGO DE UMA CONEXÃO

A avaliação do volume de tráfego de uma conexão pode ser realizada pelo conteúdo dos atributos *Acct-Input-Octets*, *Acct-Output-Octets*, *Acct-Input-Gigawords* e *Acct-Output-Gigawords*.

O tráfego total de entrada (TT_E) no NAS é calculado conforme a equação abaixo:

$$TT_E = \textit{Acct-Input-Gigawords} \times 4.294.967.296 + \textit{Acct-Input-Octets} \qquad (4.4)$$

O tráfego total de saída (TT_S) do NAS ao cliente é, de forma similar, calculado conforme a equação 4.5 abaixo:

$$TT_S = \textit{Acct-Output-Gigawords} \times 4.294.967.296 + \textit{Acct-Output-Octets} \qquad (4.5)$$

O tráfego total (TT) do cliente em uma determinada sessão é avaliado pela soma entre os valores calculados de tráfego total de entrada e tráfego total de saída, de acordo com a equação 4.6.

$$TT = TT_E + TT_S \qquad (4.6)$$

Segundo [JUNIPER], os contadores de tráfego dos agregadores da série ERX refletidos nos atributos *Acct-Input-Octets* e *Acct-Output-Octets* incluem todo tráfego de uma sessão PPP desde o reconhecimento da autenticação PAP ou CHAP até o seu encerramento, excluindo os pacotes do PPP de requisição de término de sessão, de reconhecimento de final de sessão e os eventuais *paddings* inseridos pelo PPPoE em pacotes de controle e de dados.

Assim, os contadores incluem todo o tráfego de controle (IPCP) e de dados (IP) das camadas superiores, os pacotes de *keepalive* do PPP (LCP *echo-request* e *echo-response*), as demais negociações do LCP após a autenticação, e a retransmissão de tráfego PAP ou CHAP.

Os contadores de pacotes dos agregadores da série ERX, que originam os valores dos atributos *Acct-Input-Packets* e *Acct-Output-Packets* contabilizam, entretanto, apenas os pacotes das camadas superiores, ou seja, apenas os do tráfego IP.

Em decorrência desse fato, cabe ressaltar que a avaliação do tamanho médio dos pacotes de dados a partir dos atributos *Acct-Input-Octets* e *Acct-Output-Octets* e *Acct-Input-Packets* e *Acct-Output-Packets* fornecerá apenas um valor aproximado, superior ao real.

4.8 - SINCRONISMO DE RELÓGIO

Em qualquer das três alternativas apresentadas para a avaliação do tempo de conexão, é necessário que a base de tempo dos elementos envolvidos seja a mesma, para que os registros de tempo dos eventos de conexão e desconexão expressem corretamente o momento da ocorrência tais eventos e possam ser correlacionados.

Alerta [SILVA2006] que a falta de sincronismo de relógio pode causar danos para a empresa, principalmente se ela realiza transações comerciais que estejam vinculadas ao parâmetro tempo.

Assim, a oferta de um serviço baseado no consumo de um recurso exige a possibilidade de fornecer ao cliente desse serviço um extrato detalhado da sua utilização. Em decorrência disso, mais do que sincronizados entre si, os elementos de rede – especialmente os NAS e os servidores RADIUS – devem estar sincronizados com a chamada "Hora Legal Brasileira" (HLB).

A Hora Legal Brasileira é a referência legal de tempo no Brasil e é gerada, mantida e distribuída pela Divisão do Serviço da Hora do Observatório Nacional (ON). As

operadoras de telecomunicações, pela natureza dos serviços por elas prestados, já possuem, dentro das suas instalações, equipamentos de referência de tempo sincronizados com a HLB.

Dada a existência dessa estrutura de referência de tempo, é necessário apenas configurar os elementos de rede para que eles, através do protocolo NTP (*Network Time Protocol*), proposto por [RFC1305] ou do protocolo SNTP (*Simple Network Time Protocol*), formalizado por [RFC4330], atualizem seus relógios internos.

4.9 - FUSOS HORÁRIOS E HORÁRIO DE VERÃO

A Brasil Telecom possui oferta de serviços ADSL em uma região geográfica que, até 23 de junho de 2008, abrangia três fusos horários no horário normal e, habitualmente, quatro fusos quando instituído o chamado "horário de verão". Cabe mencionar que, por força da lei [LEI11.662], o Estado do Acre passou a integrar o terceiro fuso-horário nacional e o quarto fuso-horário brasileiro foi extinto, de forma que o cenário de análise mais provável passa a ser constituído por dois fusos-horários em horário normal e três quando instituído o "horário de verão".

Em 2007/2008, as unidades da federação em que foi adotado o horário de verão foram: Rio Grande do Sul, Santa Catarina, Paraná, São Paulo, Rio de Janeiro, Espírito Santo, Minas Gerais, Goiás, Mato Grosso, Mato Grosso do Sul e Distrito Federal.

Quando entra em vigor o horário de verão, os relógios são adiantados em uma hora nos Estados onde foi imposto. Findo o período do horário de verão, os relógios são atrasados em uma hora.

Essa adição de uma hora nos relógios aumenta, de uma forma virtual, uma hora de conexão nos registros das conexões que estiverem estabelecidas imediatamente antes da troca de horário. De uma forma similar, a volta ao horário normal reduz em uma hora o tempo das conexões ativas no momento da mudança, podendo causar ainda o efeito "volta no tempo" onde o registro de término de conexão precede o de início.

Existe também a situação em que o acesso físico de um cliente final está em uma unidade da federação e o NAS está em outra. Na hipótese de essas unidades federativas estarem em fusos diferentes, o registro feito pelo NAS será diferente do horário real da conexão.

Para contornar os problemas acima evidenciados, a solução mais apropriada é que todos os NAS e os servidores envolvidos operem configurados em um mesmo fuso, e que este fuso seja imutável, ou seja, não sofra alteração em decorrência do horário de verão. A sugestão é que seja adotado o fuso conhecido como GMT-3 (*Greenwich Mean Time,* atraso de 3 horas), que é o fuso que geograficamente corresponde à capital do país, Brasília.

Ao adotar essa proposta, caberá ao sistema de faturamento, que possui as informações de localização geográfica do cliente, realizar a adequação do horário nos extratos de utilização e calcular adequadamente os efeitos da troca de horário para as conexões que estão estabelecidas no momento da troca de horário.

4.10 - CONFIGURAÇÕES RADIUS GENÉRICAS

Com base no funcionamento da rede de acesso ADSL, algumas regras gerais devem ser adotadas para o funcionamento apropriado da proposta aqui apresentada. Essas regras serão apresentadas a seguir.

4.10.1 - Ajuste de tempo de espera (*timeout*)

Conforme mencionado anteriormente, o cliente RADIUS, uma vez tendo enviado uma mensagem ao servidor, aguarda, por um período de tempo determinado, configurável, uma resposta deste último. O cliente RADIUS, depois de expirado esse tempo, pode realizar a retransmissão da mensagem ou desistir da requisição.

A determinação do valor apropriado para esse tempo de espera deve ser feita com base na soma dos tempos de trânsito da mensagem entre o NAS e o servidor, de processamento da mensagem e de trânsito da resposta entre o servidor e o NAS. Como simplificação, o

tempo de trânsito no sentido NAS-servidor pode ser considerado o mesmo que o tempo entre servidor-NAS.

O tempo de processamento da mensagem habitualmente depende do que é necessário fazer para realizar a autenticação e autorização ou o registro da bilhetagem.

No cenário envolvendo a presença de provedores de serviço Internet para realizar a autenticação e a consulta a uma base de dados interna para realizar a autorização do cliente final, os tempos para realizar estas consultas devem ser cuidadosamente considerados.

Deve ser prevista a consulta a mais de um servidor do provedor de serviços Internet, e, de forma similar, a consulta à base de dados interna deve ser realizada em servidor alternativo em caso de indisponibilidade do servidor primário.

Como aproximação inicial, podemos considerar que o tempo de espera To_{NAS} a ser configurado no NAS pode ser determinado pela equação 4.7:

$$To_{NAS} = 2 \times (T_{tran} + To_{psi} + To_{bi}) + T_{proc} \qquad (4.7)$$

Onde: T_{tran} é o tempo de trânsito entre NAS e servidor RADIUS

To_{psi} é o tempo de espera por uma resposta do servidor RADIUS do provedor de serviços Internet.

To_{bi} é o tempo de espera por uma resposta da base de dados de autorização

T_{proc} é o tempo de processamento da requisição, excluídos os demais tempos.

Os valores usuais para uma primeira aproximação de To_{NAS} são: T_{tran} = 0,5s , To_{psi} = 3s , To_{bi} = 3s e T_{proc} = 1s, o que resulta em 14 segundos.

Os ajustes nos parâmetros devem ser feitos com base nas particularidades da rede e dos serviços oferecidos, levando em conta também outras variáveis, como a introdução de atrasos por parte dos provedores de acesso a Internet nas mensagens de Acesso Rejeitado e a necessidade de consultar mais de uma base de dados de autorização.

É importante ainda ressaltar que a determinação desse valor de tempo de espera é também o resultado de uma solução de compromisso; ao aumentar o valor, é razoável conceber que,

nas situações de falha, ocorra um enfileiramento de mensagens no NAS. Ao reduzir, retransmissões de requisições podem ser feitas pelo NAS enquanto a solicitação original ainda está em processamento pelo servidor RADIUS.

4.10.2 - Ajuste de quantidade de retransmissões

A finalidade da retransmissão é minimizar os efeitos da perda de pacotes em função de falhas na rede de pequena duração.

Em uma rede de operadora de telecomunicações, habitualmente, todos os elementos envolvidos no provimento de um serviço e que estão dentro do ambiente da operadora, são construídos visando a possuir alta disponibilidade. Em geral, os enlaces de comunicação de dados são redundantes e a ocorrência de falhas de comunicação é rara.

Em tal cenário a retransmissão traz benefícios. Um servidor RADIUS que já esteja processando uma mensagem com prazo de processamento prestes a vencer, ao receber a retransmissão pode ampliar o tempo de processamento da mensagem original, quando o normal seria retomar o processamento desde o início.

Situações de sobrecarga que ocorram com o servidor RADIUS selecionado para receber a mensagem não melhoram com o recebimento de mais mensagens. Um servidor em falha, entretanto, não voltará a atender a requisições apenas por receber mais requisições. Em tais situações, não só não existe benefício com o uso de retransmissão como o problema pode piorar.
Em geral, os NAS possibilitam a configuração de, pelo menos, até quatro servidores RADIUS. Propõe-se então, que a retransmissão seja sempre desativada, e, para mitigar a oportunidade de falha na recepção das mensagens RADIUS, em especial as requisições de bilhetagem, a configuração seja feita apontando para quatro servidores.

Caso a estrutura de AAA disponha de apenas dois servidores, a configuração de dois endereços IP nas interfaces de rede do servidor pode emular a composição com quatro servidores; é importante apenas que as mensagens sejam enviadas alternadamente para cada servidor.

4.10.3 - Utilização de balanceamento de carga

O comportamento normal de um NAS é enviar as mensagens para os servidores RADIUS na ordem em que estes foram configurados. Assim, o NAS sempre enviará a mensagem para o primeiro servidor configurado, e, caso dele não receba resposta, enviará para o segundo e assim por diante.

Apesar da praticidade que este comportamento traz para os procedimentos de verificação de problemas – o técnico sempre sabe para onde será enviada a requisição –, ele não favorece o funcionamento da rede em duas situações: em caso de falha de um servidor e se as requisições dos diversos NAS de uma rede não forem bem distribuídas pelos servidores RADIUS em função da ocupação desigual de recursos desses NAS.

Na primeira situação, o NAS continuará enviando a mensagem para o servidor em falha, problema que é agravado se este servidor for o primeiro da lista, pois o NAS não receberá resposta para 100% das requisições e terá de realizar nova transmissão. Tal situação ocasionará o enfileiramento de requisições RADIUS no NAS, o que diminuirá o seu desempenho e, por conseqüência, reduzirá a qualidade do serviço prestado.

Para a segunda situação, é senso comum que, pelo fato de o protocolo RADIUS utilizar como transporte o UDP, quanto mais perto do NAS o servidor estiver, melhor, razão pela qual em geral os servidores são designados aos NAS seguindo um critério de proximidade lógica na rede.

Esse critério de distribuição de carga pode resultar em conjuntos de servidores com carga bem superior à de outros, conforme a quantidade de NAS instalados por área geográfica.

Os elementos NAS, em geral, podem ser configurados para que distribuam as mensagens RADIUS entre os servidores disponíveis, realizando o envio aos servidores de forma balanceada.

Adotar esse tipo de configuração resulta em uma melhor distribuição de carga entre todos os servidores, o que melhora o aproveitamento da estrutura disponível. A falha de um dos servidores de um grupo de quatro servidores configurado nos NAS significará que apenas

25% das requisições não terão atendimento no primeiro envio, contra 100% de perda caso a falha atinja o primeiro servidor da configuração tradicional.

4.10.4 - Utilização de *server deadtime*

Alguns NAS possuem uma função chamada de *server deadtime*, cujo objetivo é, durante um determinado período de tempo, evitar que o NAS envie mensagens RADIUS a um servidor que foi identificado como indisponível.

O recurso é interessante por minimizar o envio de mensagens a um servidor com problemas, porém a principal questão é quais são os critérios utilizados pelo NAS para determinar a indisponibilidade de um servidor RADIUS.

Os NAS da empresa *Cisco Systems* podem configurar dois critérios: o tempo decorrido desde o recebimento da última resposta do servidor RADIUS e a quantidade global de mensagens retransmitidas sem resposta (autenticação e bilhetagem). Para o uso desse último critério, porém, o uso de retransmissões deve estar habilitado.

Já os equipamentos da *Juniper Networks* utilizam como critério de determinação da falha de um servidor a não recepção de uma única resposta a uma mensagem RADIUS, o que pode causar a determinação prematura da indisponibilidade de um servidor.

Assim, a utilização ou não do recurso de *server deadtime* deve ser avaliada conforme os recursos de configuração disponíveis e testes do efetivo comportamento desse recurso no ambiente da operadora.

4.10.5 - Utilização de faixa estendida de portas UDP de origem

Foi mencionado anteriormente que a mensagem do protocolo RADIUS possui um campo chamado identificador, cujo valor pode estar entre 0 e 255 e que esse campo, em conjunto com o endereço IP e a porta UDP de origem, é utilizado para a detecção de mensagens duplicadas no servidor RADIUS.

Quando o NAS utiliza somente uma porta UDP para originar as requisições RADIUS, apenas 256 diferentes requisições podem estar em andamento em um dado instante. Caso o número de requisições em andamento ultrapasse esse valor, as requisições subseqüentes poderão utilizar identificadores que já estão em uso, o que será interpretado pelo servidor RADIUS como uma requisição duplicada. Por outro lado, caso ocorra tal reuso indevido de identificadores, as respostas enviadas pelo servidor também poderão ser incorretamente tratadas pelo NAS, gerando uma situação em que a resposta fornecida não coincide com a requisição.

Os NAS geralmente possuem algum tipo de configuração para habilitar o uso de portas UDP extras para as requisições, de forma a não ocorrer o problema.

4.10.6 - Habilitação dos atributos envolvendo *gigawords*

Os atributos *gigawords* (*Acct-Input-Gigawords* e *Acct-Output-Gigawords*) foram introduzidos por [RFC2869] como uma ampliação do protocolo RADIUS e envolvem a utilização de contadores adicionais nos equipamentos NAS.

Por essa razão, em alguns tipos de NAS a utilização desse recurso deve ser habilitada explicitamente na sua configuração.

4.11 - OUTRAS SUGESTÕES DE CONFIGURAÇÃO

A seguir serão apresentadas outras sugestões de configurações para os NAS e implementações nos servidores RADIUS, visando à redução de carga e à melhoria de desempenho da plataforma de autenticação e bilhetagem.

4.11.1 - Tempo de espera pela autenticação no PPP

Sempre que o sistema operacional do NAS permitir que seja configurado, o tempo de espera pela autenticação no PPP deve ser ajustado para um valor compatível com o tempo

necessário para realizar o envio da requisição de autenticação inicial e suas eventuais retransmissões, levando em conta o tempo de espera ajustado.

4.11.2 - *PPPoE Throttling*

O *PPPoE Throttling* é um recurso disponível nos NAS do fabricante *Cisco Systems* e foi criado para minimizar os efeitos de requisições repetidas e contínuas realizadas por um equipamento cliente para iniciar uma sessão PPPoE.

Esse recurso restringe, com base no endereço MAC (*Media Access Control*) ou VC (*Virtual Circuit*) de origem da conexão, a quantidade de requisições que pode ser realizada em um determinado período de tempo, bloqueando as solicitações dessa origem por outro período de tempo, caso tal quantidade tenha sido excedida.

Com o uso desse recurso, conexões PPPoE cujo processo de autenticação não obteve sucesso podem ser bloqueadas por um determinado tempo, reduzindo, por conseqüência, a carga na plataforma de autenticação e bilhetagem.

4.11.3 - Autenticação e segregação de usuários inválidos

Diversos nomes de usuário, que não possuem vinculação com provedores de serviços Internet, são utilizados diariamente na configuração de modems de clientes finais. Em geral, estes nomes de usuário (tais como “admin”, “root”, “administrador”, “teste”, “usuário” entre diversos outros) são fruto ou da configuração padrão de fábrica dos modems ou mesmo de tentativas de fraudar o sistema de autenticação e obter o acesso à Internet sem o uso de uma credencial válida.

Esses clientes não conseguem utilizar os serviços ADSL em decorrência de credenciais de autenticação inválidas, porém seus modems ficam continuamente procurando estabelecer uma conexão PPP, o que envolve o processo de autenticação.

Uma maneira de tratar este problema é o servidor RADIUS, ao perceber a utilização de uma destas credenciais, não executar seu fluxo normal de autenticação e imediatamente

responder ao pedido com uma mensagem de Acesso Rejeitado. Um pequeno atraso pode ser introduzido antes do envio da resposta para evitar que o modem tente estabelecer outra sessão imediatamente.

Outra ação do servidor RADIUS é retornar ao cliente uma mensagem de Acesso Permitido, porém com parâmetros (enviados através de atributos da mensagem) para estabelecer a conexão PPP dentro de uma rede privada e restrita. Essa segunda proposição segrega a conexão do cliente final em uma rede sem conectividade exterior e faz com que as requisições de autenticação desse acesso cessem, reduzindo a carga no servidor de autenticação e bilhetagem.

Uma evolução dessa alternativa é introduzir um sistema de notificação via WWW ao usuário, indicando a falha na autenticação e sugerindo procedimentos de correção. Um limite de duração de conexão pode ser aplicado para que a conexão seja encerrada automaticamente depois de decorrido um intervalo de tempo.

4.11.4 - Implementação de "lista negra" dinâmica

É razoável conceber que uma consulta do tipo *proxy*, feita a um provedor de serviços Internet, que resulte em Acesso Rejeitado, receberá a mesma resposta se a mesma consulta – mesmo nome de usuário e mesma senha – for feita alguns instantes de tempo depois. Essa mesma concepção pode ser aplicada para as requisições de acesso que resultem em consulta a uma base de dados local cujo resultado também seja Acesso Rejeitado.
Para reduzir a carga aplicada aos servidores *proxy* e de base de dados local, a proposta é armazenar em memória, por um intervalo de tempo de duração aleatória, as credenciais de acesso utilizadas nas autenticações que resultaram em Acesso Rejeitado.

O servidor RADIUS, ao receber uma Requisição de Acesso, verificaria em memória a presença das credenciais de acesso, e, encontrando-as, finalizaria o processo imediatamente, enviando uma mensagem de Acesso Rejeitado. Um atraso de tempo poderia ser introduzido antes do envio da mensagem de rejeição.

Existem algumas evidências, obtidas pela observação de registros de falhas de autenticação da plataforma AAA da Brasil Telecom, de que são poucos os acessos que produzem as autenticações repetidamente em falha e que tais tentativas ocorrem de forma quase simultânea. A utilização de intervalo de tempo de duração aleatória para o armazenamento das credenciais em memória visa a reduzir a incidência de picos de consultas *proxy* de autenticação, pela não expiração simultânea das entradas em memória.

4.11.5 - Conformação de bilhetes

Foi dito anteriormente que o bilhete RADIUS é um registro cujas informações foram originadas pelo NAS. É razoável conceber que, pela flexibilidade do protocolo, um fabricante de NAS implemente de forma diferente de outro fabricante o preenchimento de alguns atributos, a disposição dos atributos na mensagem e também a utilização de atributos opcionais.

O servidor de bilhetagem pode ajustar o bilhete que será gravado para que os bilhetes oriundos de equipamentos NAS de distintos fabricantes possuam um registro similar, de forma a reduzir a quantidade de regras de verificação necessárias no sistema de faturamento.

4.11.6 - Adição de informações complementares nos bilhetes

Pela concepção do protocolo RADIUS, os processos de autenticação e bilhetagem são dissociados, ou seja, não existe manutenção de estado entre os dois eventos. A única exceção a essa regra é o atributo *Class*. Esse atributo, no processo de bilhetagem, conserva o valor retornado ao NAS pelo servidor RADIUS no processo de autenticação. Pode, então, ser utilizado para registrar no bilhete algumas informações pertinentes ao processo de autenticação, tais como a identificação do servidor que realizou a autenticação, o tipo de serviço autorizado, o resultado do processo de autenticação, a área de localização geográfica do cliente, etc.

Novos atributos podem ser adicionados ao bilhete para registrar o resultado de operações realizadas sobre os valores de atributos existentes. Como exemplo temos o valor de

consolidação dos dados relacionados ao volume de *bytes* trafegados em uma conexão, o valor do atributo *Event-Timestamp* convertido para um formato de data e hora, um valor que represente o fuso horário da região onde está o cliente e a tarifa vigente no momento da conexão. São inúmeras as possibilidades de utilização dessa técnica.

4.12 - RESUMO DA PROPOSIÇÃO

O mecanismo objeto deste trabalho é composto pelos mesmos elementos tradicionais de uma rede de acesso em banda larga que utiliza a tecnologia ADSL, dispostos, implementados e configurados, porém, observando um conjunto de critérios e técnicas que visam a reduzir a oportunidade de perda de informações de bilhetagem. Todos os elementos são, pois, importantes para que o mecanismo funcione adequadamente. Uma especial atenção, contudo, é dada ao NAS e aos servidores de autenticação, autorização e bilhetagem.

O cenário brasileiro para a oferta de acessos ADSL por uma operadora de telecomunicações possui um grau adicional de complexidade, ao ser imposta a necessidade de um organismo externo – o provedor de serviços Internet – para que o serviço possa ser fornecido ao cliente final. Essa exigência, de caráter regulatório, cria a dissociação entre a credencial de acesso utilizada nos processos de autenticação – que é do provedor – e a linha ADSL – que faz parte da estrutura da operadora de telecomunicações.

Em tal cenário, cujos aspectos foram apresentados na seção 4.2.1, a operadora de telecomunicações não possui qualquer controle sobre o funcionamento das credenciais de acesso utilizadas pelos clientes. Em decorrência, a operadora não tem conhecimento dos eventuais bloqueios, cancelamentos ou trocas de senha de acesso que venham a ser aplicados às credenciais de acesso dos clientes, com a ciência e o aceite deles ou sem. A operadora também não pode contar com a absoluta disponibilidade dos sistemas AAA dos provedores de serviços Internet.

Assim, a adoção de uma combinação de soluções que venham a reduzir o impacto causado pela indisponibilidade de sistemas de AAA de provedores ou, por exemplo, de bloqueio de

clientes por razões financeiras e de forma massiva por parte de um grande provedor, é extremamente importante para que a disponibilidade da plataforma AAA da operadora não seja afetada.

Para resguardar, então a plataforma AAA da operadora de telecomunicações contra situações ou fenômenos que ocorram foram do seu domínio administrativo, sobre os quais, por conseqüência, ela não possui qualquer controle, é mandatória a adoção de técnicas e recursos como os apresentados nas seções 4.10.4, 4.10.5, 4.11.2, 4.11.3 e 4.11.4. No capítulo 5, é possível apreciar os resultados práticos da implementação dessas técnicas e recursos.

Visando a reduzir a oportunidade de perda de informações de utilização dos acessos e viabilizar o crescimento em escala do sistema, a adoção das medidas propostas na seção 4.3, em especial as relativas à segregação das funções de autenticação e autorização da função de bilhetagem em servidores distintos e a disposição de servidores primários e secundários em localidades geográficas distintas é essencial. A adoção de servidores com conexão redundante auxilia a melhorar a disponibilidade da plataforma e é recomendável.

O uso de bilhetagem intermediária deve ser analisado quando da implementação da cobrança por tempo ou por tráfego, pois a sua importância, os critérios de aplicação e o valor do intervalo de tempo entre os bilhetes dependem basicamente do comportamento do cliente na utilização do serviço. Uma técnica para a determinação do intervalo de bilhetagem intermediária, com base nas recomendações e considerações apresentadas na seção 4.2.3 é apresentada nas seções 5.3.2 e 5.4.2.

A aplicação da combinação de algumas outras medidas, como as apresentadas nas seções 4.10.1, 4.10.2, 4.10.3 e 4.11.1, é também recomendável, pois auxilia a reduzir a oportunidade de perda das informações de utilização das conexões. Em especial, o adequado cálculo do tempo de espera combinado com a adoção de balanceamento de carga proporciona uma distribuição das requisições de autenticação e de bilhetagem, absorvendo mais facilmente a ocorrência de picos de requisições e diminuindo a oportunidade da ocorrência de sobrecarga em um servidor AAA específico.

Para que um bilhete RADIUS seja útil para a realização da cobrança por tempo ou volume de dados trafegados, as informações nele constantes devem ser suficientes e confiáveis. Suficientes, no sentido de que os atributos específicos para a bilhetagem, vistos na seção 4.5, aliados a atributos que possibilitem a identificação do serviço utilizado e também do cliente devem estar presentes no bilhete. Confiáveis, no sentido de que devem refletir o consumo de forma fiel.

A questão da presença ou não dos atributos necessários no bilhete, bem com da fidelidade entre o consumo e o registro efetuado será alvo de abordagem no capítulo 5, nas seções 5.3.1 e 5.4.1. O problema da associação entre o bilhete e o cliente da operadora não constitui escopo deste trabalho, porém seu princípio de solução foi apresentado na seção 4.2.1.

Estando presentes no bilhete os atributos necessários, a avaliação da duração de uma sessão pode ser realizada por qualquer das três alternativas apresentadas na seção 4.6, sendo altamente recomendável, pela sua simplicidade e economia de recursos de processamento, a adoção da terceira forma apresentada – uso do atributo *Acct-Session-Time* – sempre que for possível. Para garantir que o carimbo de tempo do bilhete reflita efetivamente o momento da ocorrência do evento de conexão ou do evento de desconexão, a adoção do sincronismo de relógio, proposto na seção 4.8, em conjunto com a utilização de fuso horário fixo, proposta na seção 4.9, deve ser realizada.

A avaliação do volume de tráfego de uma conexão deve ser realizada através das equações 4.4, 4.5 e 4.6, propostas na seção 4.7, não devendo ser esquecida a habilitação dos atributos envolvendo *gigawords*, conforme exposto na seção 4.10.6. Adicionalmente, as operações matemáticas necessárias para consolidar o valor de consumo podem ser realizadas no momento da recepção da Requisição de Bilhetagem pelos correspondentes servidores. Utilizando técnicas de adição de informações complementares (seção 4.11.6) e de conformação de bilhetes (seção 4.11.5), tal valor de consumo pode ser adicionado ao bilhete, facilitando o processamento posterior por sistemas de faturamento, de extrato de uso, e de controle de quota, entre outros.

(Esta página foi intencionalmente deixada em branco.)

5 - EXPERIMENTOS

Nos capítulos anteriores foi apresentado o embasamento teórico sobre o qual foi elaborada e descrita uma proposta de um mecanismo de contabilização de uso de serviços residenciais em rede de acesso em banda larga utilizando tecnologia ADSL. Todos os pontos dessa proposta possuem suporte direto no embasamento teórico. Alguns experimentos, não obstante, foram realizados com a finalidade de consolidar as idéias apresentadas.

Neste capítulo serão descritos os objetivos dos experimentos realizados, a maneira como o foram e os resultados obtidos.

5.1 - AMBIENTES DE TESTES

Para a realização dos experimentos foram utilizadas duas estruturas básicas, a seguir descritas.

5.1.1 - Ambiente de laboratório

É um ambiente controlado que foi utilizado para a realização de testes preliminares de configuração dos NAS e de alterações a serem realizadas na plataforma AAA RADIUS. Toda alteração de configuração necessária para a realização dos experimentos no ambiente de produção foi previamente avaliada no ambiente de laboratório.

5.1.2 - Ambiente de produção

Neste ambiente foram realizados os todos os experimentos e coletados os resultados. Com o objetivo de verificar o adequado funcionamento dos sistemas envolvidos, foram utilizados acessos ADSL da rede de produção da operadora, dentro das condições normais de configuração e de utilização, sem qualquer preparo especial. As modificações na plataforma RADIUS foram, uma vez homologadas em ambiente de laboratório, realizadas nos servidores de produção seguindo os procedimentos padronizados para esse tipo de atividade. Para os experimentos envolvendo o uso de conexões ADSL, foram utilizadas credenciais de acesso especialmente criadas através de uma estrutura simulada de um

provedor de serviços Internet, de forma a capturar mais facilmente os bilhetes correspondentes.

5.2 - PARÂMETROS MEDIDOS

Alguns dos experimentos realizados visaram a obter como resultado a avaliação ou a comparação de uma ou mais grandezas, que são a seguir apresentadas acompanhadas de breve definição.

O tempo de conexão é o intervalo de tempo, em geral avaliado em segundos, durante o qual o usuário final ficou conectado, medido entre o início da conexão PPP e o momento do encerramento desta conexão.

Considera-se o resultado da soma, em *bytes*, do tráfego de entrada e de saída do computador do cliente como o volume de tráfego de uma conexão. Eventualmente, pode-se considerar o tráfego em apenas um dos sentidos, situação na qual tal sentido deve estar explicitamente definido.

A duração média de sessão é o valor do somatório das durações de cada conexão de um conjunto de conexões, conforme informado nos bilhetes referentes a essas conexões, dividido pelo tamanho do conjunto.

O tamanho médio do bilhete é o valor do somatório do espaço de armazenamento ocupado por um conjunto de bilhetes de determinado tipo, dividido pela quantidade de bilhetes de tal tipo constantes no arquivo. Habitualmente, estamos interessados no tamanho médio dos bilhetes de início e de fim de conexão.

A quantidade de requisições de autenticação e bilhetagem por unidade de tempo, geradas ou recebidas por um equipamento ou servidor é denominada de carga AAA ou volume de requisições AAA. Em geral, é uma informação útil para o dimensionamento de servidores, que também permite comparar diferentes situações, tais como as existentes em alguns dos experimentos apresentados a seguir.

5.3 - DESCRIÇÃO DOS EXPERIMENTOS

Nesta parte serão descritos os experimentos realizados, detalhando-os de forma a que possam ser compreendidos e repetidos conforme a conveniência dos interessados. Os códigos dos programas desenvolvidos e os detalhes das alterações dos sistemas de AAA, contudo, não serão apresentados, por se tratarem de propriedade intelectual.

5.3.1 - Determinação do tempo de conexão e do volume de dados trafegados

O objetivo deste experimento é verificar se o consumo de duas grandezas, objetivamente o tempo de utilização e a quantidade de dados trafegados em uma conexão ADSL, percebido pelo usuário, possui correlação com os valores constantes nos bilhetes RADIUS para essa conexão. O experimento consiste em simular o ambiente e o comportamento do usuário final, utilizando apenas recursos a que ele normalmente tem acesso.

Este experimento foi realizado em duas partes. A primeira parte foi realizada buscando determinar a forma de contabilização de tráfego utilizada pelos dois tipos de NAS disponíveis (*Cisco* 10008 e *Juniper* ERX 1440). A segunda parte procurando verificar o adequado funcionamento dos contadores envolvidos em conexões cujo tráfego e duração não foram previamente determinados.

Neste experimento foram utilizados inicialmente dois acessos ADSL, um direcionado para um NAS do fabricante *Cisco Systems* e outro para um NAS do fabricante *Juniper Networks*. Para esses dois acessos, nenhuma configuração especial foi realizada, tendo sido deixada a configuração padronizada pela Brasil Telecom para um acesso de perfil residencial. Os dois acessos foram disponibilizados a partir do mesmo DSLAM, modelo 5103 do fabricante *Huawei*, conectado aos NAS através de uma rede ATM. Ambos os NAS estavam instalados no mesmo ambiente físico, e o acesso lógico entre eles e o DSLAM foi realizado através do mesmo caminho na rede ATM, exceto apenas pelo trecho final – conexão entre a rede ATM e cada um dos NAS –, que, necessariamente, foi diferente.

Posteriormente, em função de situação que será detalhada na seção 5.4.1, um acesso ADSL adicional foi utilizado. Esse acesso, fisicamente vinculado ao mesmo DSLAM dos outros dois, foi terminado logicamente em outros equipamentos NAS *Juniper* ERX 1440, com a finalidade de verificar o comportamento dos contadores de tráfego em outras versões do sistema operacional do equipamento.

Inicialmente, apenas um modem ADSL modelo "SpeedStream 5200", fabricado pela empresa *Siemens*, foi utilizado de forma alternada, nos dois acessos. O modem foi configurado para operar no modo *bridge* e nenhuma alteração de configuração foi feita quando da troca de um acesso ADSL para o outro. Posteriormente um segundo modem, modelo "827" do fabricante *Cisco Systems*, também foi utilizado nos testes, com a finalidade de verificar se alguma diferença relacionada ao modem poderia ser percebida nas medições.

Para as duas partes do experimento foram utilizados computadores do tipo PC, com sistema operacional *Linux*, distribuição *Debian Etch*, sem qualquer otimização ou configuração especial, exceto a instalação das atualizações propostas pelo próprio sistema operacional. Nesses computadores foram instalados e configurados o suporte ao protocolo PPPoE e o *software* de captura de pacotes *Wireshark* ([WIRESHARK]).

Para promover tráfego no acesso ADSL, quando da execução da segunda parte do experimento, foram utilizados os programa *Wget* ([WGET], *iPerf* ([IPERF]) e *JPerf* ([JPERF]). A utilização do *JPerf* exigiu a atualização da instalação da linguagem *Java,* pré-instalada, para a sua versão mais recente.

As mesmas credenciais de acesso foram utilizadas em todos os testes realizados, e foram determinadas de forma a permitir a fácil localização, nos servidores de bilhetagem, dos bilhetes correspondentes às conexões de teste.

Foi realizado, para a primeira parte do experimento, um conjunto de conexões com duração de apenas o tempo necessário para estabelecer, trafegar uns poucos pacotes de dados para, logo em seguida, encerrar a conexão. O tráfego dessas conexões foi coletado com o uso do *software Wireshark* para possibilitar a análise dos critérios de contabilização de tráfego e de tempo que são refletidos nos bilhetes RADIUS, por cada um dos tipos de NAS.

Na segunda parte do experimento, conexões de duração e de tráfego não previamente determinados foram geradas a partir do computador PC. Essas conexões foram monitoradas com o uso do *software Wireshark*. Para cada conexão, o resultado da coleta, exportado em arquivo no formato PDML (*Packet Details Markup Language*), foi submetido a um programa desenvolvido por este autor, que, utilizando os critérios de contabilização descobertos através da primeira parte deste experimento, contabilizava os valores de utilização para comparação com os encontrados no bilhete RADIUS correspondente.

Nas duas partes do experimento foi observado se todos os atributos necessários para a contabilização de tempo e tráfego estavam presentes nos bilhetes correspondentes às conexões realizadas.

5.3.2 - Determinação do intervalo para a geração de bilhetes intermediários

Conhecer o valor aproximado do tempo médio de conexão é útil para determinar o intervalo de tempo entre a geração de bilhetes intermediários, conforme foi apresentado na seção 3.1.3.2. Mais do que isso, dada uma amostra de bilhetes, é possível estimar o acréscimo de bilhetes que ocorrerá ao optar-se por um determinado valor para o tal intervalo.

O objetivo deste experimento é, portanto, realizar, através da utilização do atributo *Acct-Session-Time* de um conjunto de bilhetes RADIUS que possuem o atributo *Accounting-Status-Type* com valor *Stop*, a avaliação do tempo médio de conexão e, também, estimar, para alguns intervalos de geração, o acréscimo na quantidade de bilhetes. Este experimento, porém, não pretende realizar um tratamento estatístico dos dados desse conjunto de bilhetes, mas sim apresentar um modo de extrair as informações necessárias para efetuar o processamento de determinada amostra de bilhetes.

A amostra selecionada para esta avaliação corresponde aos bilhetes recebidos pelo servidor de bilhetagem durante um período de 24 horas, divididos em 24 diferentes arquivos. Nenhum critério estatístico foi utilizado para selecionar a amostra. Deve-se ter em mente

também que nenhuma amostra de bilhetes disponível hoje seria, de fato, válida para determinação do valor de intervalo de bilhetagem intermediária; no momento em que existir uma alteração no modelo de cobrança dos serviços, como, por exemplo, que a cobrança do serviço seja realizada levando em conta o tempo de conexão, os hábitos de consumo do serviço certamente mudarão.

Para efetuar o processamento foi criado um programa destinado a ler os bilhetes de cada arquivo e identificar, para cada bilhete, a presença do atributo *Accounting-Status-Type* com valor *Stop*. Uma vez encontrado um bilhete de fim de conexão, o valor do atributo *Acct-Session-Time* era extraído e gravado em outro arquivo, chamado "arquivo de tempos". Para cada arquivo de bilhetes processado foi gerado um "arquivo de tempos".

Outro programa foi criado para ler todos os "arquivos de tempos" e contar a quantidade de ocorrências encontradas de cada valor de duração de conexão, produzindo como saída outro arquivo contendo tais informações.

Com o uso de um *software* de planilha eletrônica, foi realizada uma tentativa de consolidação das informações de duração das conexões e, também, a realização de simulações para estimar a quantidade de bilhetes que seria registrada para diferentes intervalos de geração de bilhetes intermediários. Tal tentativa, porém, foi frustrada pelo grande volume de dados envolvido, sendo adotada uma solução alternativa.

Foi criado, então, um terceiro programa, cujo objetivo é ler o arquivo de saída do segundo programa, calcular a média das durações de conexão e realizar as simulações visando a obter a quantidade de bilhetes que seriam criados para determinados intervalos de tempo adotados para a geração de bilhetes intermediários.

5.3.3 - Determinação do tamanho médio do bilhete

O tamanho médio do bilhete é uma informação utilizada para estimar o espaço em disco necessário para o armazenamento dos bilhetes de utilização dos acessos em banda larga que utilizam tecnologia ADSL. É importante conhecer, separadamente, os valores dos tamanhos médios para o bilhete de início de conexão e o de fim de conexão, pois, no caso da utilização de bilhetagem intermediária, o espaço ocupado pelos bilhetes adicionais poderá ser estimado com base no tamanho do bilhete de fim de conexão.

Os arquivos de bilhetes selecionados para este experimento são os mesmos utilizados no experimento anterior, descrito na seção 5.3.2 e, da mesma forma, o objetivo principal é apresentar um método para realizar a avaliação e não realizar uma análise estatística do conjunto de dados selecionado ou, ainda, selecionar um conjunto com base em critérios estatísticos.

Para determinar o tamanho médio de cada tipo de bilhete foi desenvolvido um programa que processa um conjunto de arquivos de bilhetes. Para cada arquivo o programa identifica, através da análise do valor do atributo *Accounting-Status-Type*, o tipo de cada bilhete e computa o seu tamanho. Com base no tipo, o programa incrementa um contador de ocorrências e soma o tamanho a um acumulador apropriado. Após o processamento de cada arquivo são apresentados, separados por tipo, os valores correspondentes à quantidade encontrada de bilhetes e ao tamanho médio do registro. Com a finalidade de verificar o processamento adequado de todos os bilhetes contidos em cada arquivo, o programa também apresenta os valores para o tamanho do arquivo de bilhetes e o somatório dos tamanhos dos bilhetes processados.

5.3.4 - Avaliação dos benefícios da implementação de Lista Negra dinâmica

O objetivo deste experimento é verificar a existência de benefícios na implementação do mecanismo proposto na seção 4.11.4, procurando mensurar, em termos de carga AAA direcionada aos provedores de serviços Internet, caso existam, os ganhos desta implementação.

Para essa verificação, foi implementado um código adicional para o tratamento de requisições do tipo Requisição de Acesso nos servidores RADIUS. Neste código, cada requisição recebida, antes de ser direcionada ao provedor de serviços Internet correspondente, é submetida a uma verificação: a combinação de nome do usuário e senha é procurada em uma estrutura de memória *cache* e o envio ao provedor é feito somente se tal combinação não estiver contida neste *cache*.

Caso a consulta ao provedor resulte em uma mensagem Acesso Rejeitado, a combinação de nome do usuário e senha é inserida no *cache*. As entradas no *cache* expiram em um

tempo randômico, dentro de um intervalo configurável, de forma que depois de algum tempo uma nova consulta ao provedor, com a mesma credencial, poderá ser realizada.

As informações sobre as consultas recebidas e as redirecionadas ao provedor foram coletadas através da interface gráfica do servidor RADIUS.

5.3.5 - Avaliação dos benefícios da implantação da autenticação e segregação de usuários inválidos

O objetivo deste experimento é verificar a existência de benefícios na implementação da segregação de usuários em falha ou inválidos, proposta em 4.11.3, procurando mensurar os ganhos dessa implementação, em termos de carga AAA, caso existam. Os resultados do experimento foram coletados através da interface gráfica do servidor RADIUS.

Para essa verificação, foi implementado um código para o tratamento de requisições do tipo Requisição de Acesso nos servidores RADIUS apenas para um nome de usuário inválido, conhecido como "-f". Nesse código, cada requisição recebida é respondida com uma mensagem Acesso Permitido, na qual são enviados, ao NAS, atributos que indicam que esse usuário deve ser inserido em uma VPN (*Virtual Private Network*) pré-configurada no NAS.

5.3.6 - Avaliação dos benefícios de utilização de *PPPoE Throttling*

O objetivo deste experimento é verificar a existência de benefícios na implementação da configuração do recurso *PPPoE Throtling*, proposta na seção 4.11.2, procurando mensurar, em termos de consultas AAA, caso existam, os ganhos desta implementação.

Os parâmetros configurados nos NAS do fabricante *Cisco Systems* foram:

bba-group pppoe <nome do bba-group>
sessions per-mac throttle 5 60 120

O comando faz com que o NAS ignore as tentativas de conexão por um período de 120 segundos, se a partir um cliente, identificado através do seu *MAC-Address*, forem realizadas cinco tentativas de estabelecimento de conexão PPPoE, tendo elas sucesso ou não, durante um período de 60 segundos.

O comportamento previsto para o comando foi testado em ambiente de laboratório e, uma vez certificado o seu correto funcionamento, foi realizada a avaliação no ambiente de produção, cujos resultados foram coletados através da interface gráfica dos servidores RADIUS.

5.3.7 - Verificação de configuração da utilização de *gigawords*

Foi realizada a verificação de todos os NAS da Brasil Telecom, visando a verificar se os requisitos para a utilização dos atributos *Acct-Input-Gigawords* e *Acct-Output-Gigawords* estavam presentes em cada um dos equipamentos.

Para os equipamentos do fabricante *Cisco Systems*, a verificação consistiu em reconhecer a ausência, na sua configuração, do comando "*no aaa accounting gigawords*". Para os equipamentos do fabricante *Juniper*, os comandos de configuração "*radius include input-gigawords disable*" e "*radius include output-gigawords disable*" não devem estar presentes.

5.3.8 - Adição de informações complementares nos bilhetes

Este experimento visa a verificar a viabilidade da utilização do atributo *Class* para o transporte de informações do processo de autenticação e autorização para o processo de bilhetagem.

Para a realização deste teste, o código do servidor RADIUS responsável pelos processos de autenticação foi modificado para incluir, na resposta de Acesso Permitido, o atributo *Class* com algumas informações, que foram concatenadas utilizando o caractere "_" como separador.

No servidor de bilhetagem, o código foi adaptado para, uma vez percebendo a existência do atributo *Class*, desfazer a concatenação e inserir os valores individuais em atributos de significado local. Para compor esses atributos de significado local foi realizado o cadastro de um "*Private Enterprise Number*" junto ao órgão responsável, que atribuiu o número

24776 à Brasil Telecom. No dicionário de atributos dos servidores RADIUS os atributos locais foram criados na estrutura de VSAs, utilizando o PEN da Brasil Telecom como "*vendor-id*".

A avaliação dos resultados se deu através da realização de testes de conexão e a posterior análise dos bilhetes relativos a estas conexões.

5.3.9 - Conformação de bilhetes

O objetivo deste experimento é verificar a viabilidade da realização de conformação de bilhetes, proposta na seção 4.11.5, ou seja, adicionar ou reescrever informações para que os bilhetes possuam um formato pré-definido e conhecido. O resultado é avaliado através da analise de bilhetes de conexões de teste antes e depois de ativar o código proposto nesta seção.

Para esse experimento foi realizada uma alteração no código do servidor RADIUS de bilhetagem para adicionar ou reescrever o atributo *NAS-IP-Address* presente na mensagem de Requisição de Bilhetagem com um valor selecionado em uma tabela com base no valor do atributo *NAS-IP-Address*.

5.4 - RESULTADOS OBTIDOS

A seguir, os resultados dos experimentos descritos na seção 5.3 serão apresentados. Sempre que adequado, as informações relevantes serão dispostas em figuras ou tabelas, com o objetivo de enriquecer a explanação.

5.4.1 - Determinação do tempo de conexão e do volume de dados trafegados

Conforme exposto na seção 5.3.1, este experimento foi dividido em duas partes. Na primeira parte, o objetivo foi determinar a forma pela qual o tempo de conexão e o tráfego são contabilizados em cada um dos dois NAS utilizados na planta da Brasil Telecom. Com o objetivo de verificar a validade da forma encontrada na primeira parte em situações de tráfego e de duração de conexão não previamente determinados, a segunda parte do experimento foi realizada.

Na primeira parte do experimento foram realizadas diversas conexões de duração curta, com tráfego na ordem de 25 a 30 pacotes de dados. Cada conexão foi monitorada com o uso do *software Wireshark* e o correspondente bilhete foi coletado após seu término.

A Figura 5.1 é uma cópia de tela do *software Wireshark* que corresponde a uma conexão realizada com o NAS *Cisco* 10008. Nesta conexão foram trafegados 28 pacotes de dados. A primeira coluna representa o número do pacote, que é atribuído na ordem em que foi capturado pelo programa. A segunda coluna representa a diferença de tempo, em segundos, relativa ao momento do recebimento do primeiro pacote capturado e a terceira coluna o tempo relativo, também em segundos, ao pacote imediatamente anterior. A quarta coluna corresponde ao tamanho do quadro *Ethernet* e a quinta coluna apresenta o somatório dos tamanhos dos quadros até a linha em análise. A quinta e a sexta coluna correspondem, respectivamente, à origem e ao destino do pacote. A sétima coluna indica o protocolo identificado e a oitava coluna apresenta informações adicionais sobre o conteúdo do pacote.

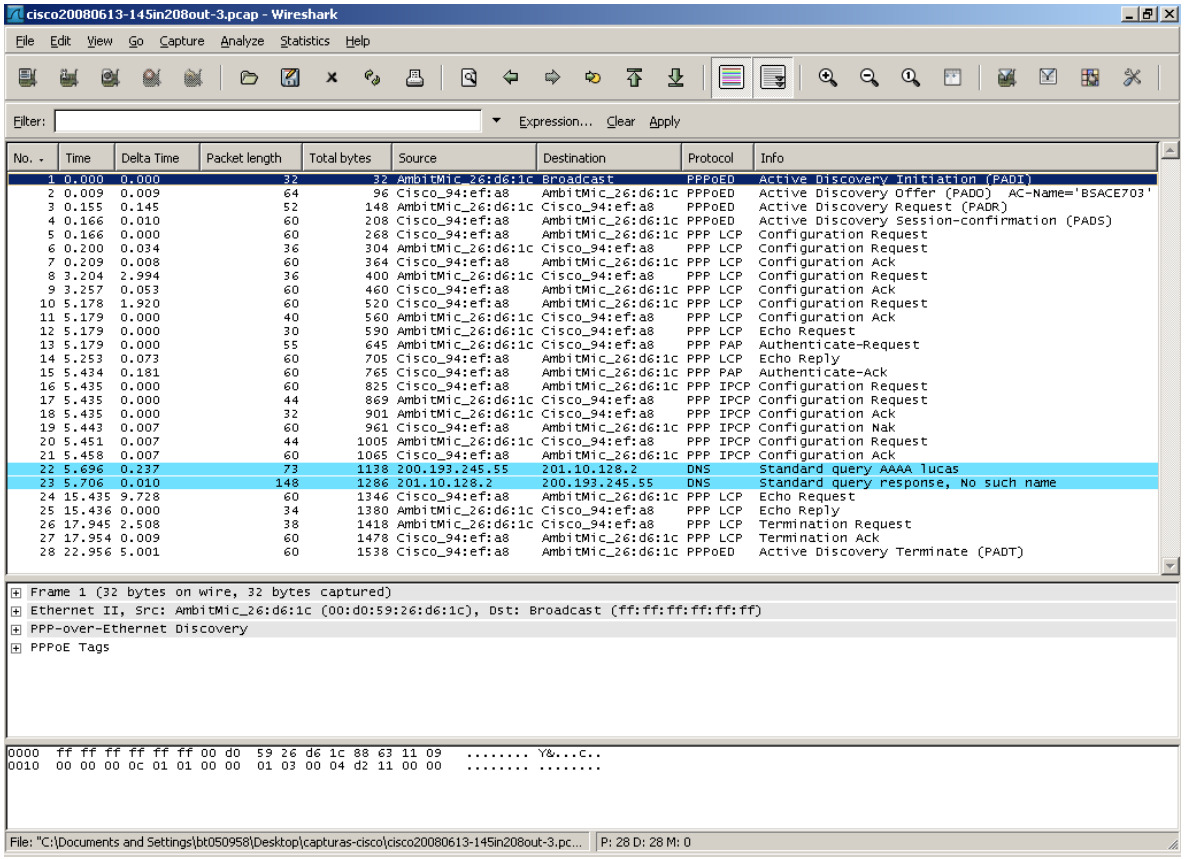

Figura 5.1: Captura de tráfego para uma conexão PPPoE com o NAS *Cisco* 10008

```
Fri Jun 13 20:40:26 GMT-03:00 2008
        Cisco-AVPair = "client-mac-address=00d0.5926.d61c"
        Framed-Protocol = PPP
        Framed-IP-Address = 200.193.245.55
        User-Name = "agski@wireshark.com.br"
        PreSession-Time = 5
        Acct-Session-Time = 13
        Acct-Input-Octets = 145
        Acct-Output-Octets = 208
        Pre-Input-Octets = 97
        Pre-Output-Octets = 89
        Acct-Input-Packets = 6
        Acct-Output-Packets = 6
        Pre-Input-Packets = 5
        Pre-Output-Packets = 6
        Acct-Status-Type = Stop
        Acct-Delay-Time = 0
        NAS-Identifier = "BSACE703"
        Brt-Acct-Start-Time = "2008/06/13 20:40:13"
        Brt-Acct-Stop-Time = "2008/06/13 20:40:26"
```

Figura 5.2: Bilhete correspondente à captura de tráfego representada Figura 5.1.

O bilhete correspondente a esta conexão pode ser visto na Figura 5.2. Nesse bilhete, buscando uma melhor clareza, foram suprimidos alguns atributos que não estão relacionados com o experimento.

O tráfego capturado, mostrado na Figura 5.1, representa uma conexão PPPoE integral, o que inclui o estabelecimento da sessão PPPoE (pacotes de 1 a 4), o estabelecimento da conexão PPP (pacotes de 5 a 21), o tráfego de dados IP (pacotes 22 e 23), uma ocorrência de *keepalive* do PPP originada pelo NAS (pacotes 24 e 25), a solicitação de finalização do PPP (pacote 26), a confirmação de finalização da sessão PPP (pacote 27) e o encerramento da sessão PPPoE (pacote 28). Para a análise do tráfego, as informações da captura foram convertidas na Tabela 5.1.

Percebe-se que os contadores apresentados no bilhete da Figura 5.2 não possuem uma relação clara com os dados apresentados na Tabela 5.1; isso ocorre principalmente porque as informações de tamanho obtidas pelo programa de captura referem-se ao tamanho do quadro *Ethernet* e não ao tamanho do pacote correspondente à sessão PPP. Adicionalmente, os pacotes correspondentes ao processo de estabelecimento (pacotes de 1 a 4) e de finalização (pacote 28) da sessão PPPoE não devem participar da contabilização, pois não são visíveis aos contadores da interface lógica PPP no NAS.

Devido a isso, os pacotes correspondentes ao protocolo PPPoED (*Point-to-Point Protocol over Ethernet Discovery*) devem ser suprimidos da análise e uma pequena correção deve

ser aplicada ao tamanho dos demais pacotes, retirando-se o valor do tamanho do cabeçalho do quadro *Ethernet* (14 *bytes*) e o valor do introduzido pela sessão PPPoE (8 *bytes*), descontado deste último o que corresponde ao cabeçalho do PPP (2 *bytes*), que deve permanecer, visto que a conexão entre o cliente e o NAS utiliza o protocolo PPP. Assim, devem ser descontados 20 *bytes* do valor presente na coluna "Tamanho".

Tabela 5.1: Dados da captura da Figura 5.1

No.	Tempo	D Tempo	Tamanho	Acumulado	Origem	Destino	Protocolo	Informação adicional
1	0,000	0,000	32	32	AmbitMic_26:d6:1c	Broadcast	PPPoED	Active Discovery Initiation (PADI)
2	0,009	0,009	64	96	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPPoED	Active Discovery Offer (PADO)
3	0,155	0,145	52	148	AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPPoED	Active Discovery Request (PADR)
4	0,166	0,010	60	208	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPPoED	Active Discovery Session-confirmation (PADS)
5	0,166	0,000	60	268	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Configuration Request
6	0,200	0,034	36	304	AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Configuration Request
7	0,209	0,008	60	364	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Configuration Ack
8	3,204	2,994	36	400	AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Configuration Request
9	3,257	0,053	60	460	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Configuration Ack
10	5,178	1,920	60	520	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Configuration Request
11	5,179	0,000	40	560	AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Configuration Ack
12	5,179	0,000	30	590	AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Echo Request
13	5,179	0,000	55	645	AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP PAP	Authenticate-Request
14	5,253	0,073	60	705	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Echo Reply
15	5,434	0,181	60	765	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP PAP	Authenticate-Ack
16	5,435	0,000	60	825	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP IPCP	Configuration Request
17	5,435	0,000	44	869	AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP IPCP	Configuration Request
18	5,435	0,000	32	901	AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP IPCP	Configuration Ack
19	5,443	0,007	60	961	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP IPCP	Configuration Nak
20	5,451	0,007	44	1005	AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP IPCP	Configuration Request
21	5,458	0,007	60	1065	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP IPCP	Configuration Ack
22	5,696	0,237	73	1138	200.193.245.55	201.10.128.2	DNS	Standard query AAAA lucas
23	5,706	0,010	148	1286	201.10.128.2	200.193.245.55	DNS	Standard query response, No such name
24	15,435	9,728	60	1346	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Echo Request
25	15,436	0,000	34	1380	AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Echo Reply
26	17,945	2,508	38	1418	AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Termination Request
27	17,954	0,009	60	1478	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Termination Ack
28	22,956	5,001	60	1538	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPPoED	Active Discovery Terminate (PADT)

O resultado dessa subtração pode ser observado na Tabela 5.2. Nessa tabela, foram suprimidos os pacotes correspondentes ao protocolo PPPoED e a coluna Tamanho foi dividida em duas, correspondendo ao tráfego em cada sentido, entrada e saída, sob o ponto de vista do NAS. Na última linha, para as colunas "Tamanho Entrada" e "Tamanho Saída", é apresentado o valor corresponde à soma dos valores presentes em cada coluna.

A Tabela 5.3 compara os valores totais das colunas "Tamanho Entrada" e "Tamanho Saída" da Tabela 5.2 com os valores de tráfego que constam no bilhete da Figura 5.2.

Enquanto o total de tráfego de entrada está coerente, percebe-se a existência de uma grande diferença na avaliação do tráfego de saída.

A investigação desta diferença foi iniciada pela análise dos dados da captura da Figura 5.1. Na Figura 5.3 é apresentado o conteúdo do pacote de número 5, que é o primeiro pacote de saída do NAS para o computador PC utilizado no teste. Observando as informações apresentadas, percebe-se que existe uma diferença entre o valor informado para o tamanho do conteúdo do pacote e o tamanho do pacote capturado, apresentados, respectivamente, como 20 e 40.

Tabela 5.2: Dados da captura da Figura 5.1 com tamanho de pacote ajustado

No.	Tempo	D Tempo	Tamanho Entrada	Tamanho Saída	Origem	Destino	Protocolo	Informação adicional
5	0,166	0,000		40	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Configuration Request
6	0,200	0,034	16		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Configuration Request
7	0,209	0,008		40	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Configuration Ack
8	3,204	2,994	16		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Configuration Request
9	3,257	0,053		40	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Configuration Ack
10	5,178	1,920		40	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Configuration Request
11	5,179	0,000	20		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Configuration Ack
12	5,179	0,000	10		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Echo Request
13	5,179	0,000	35		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP PAP	Authenticate-Request
14	5,253	0,073		40	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Echo Reply
15	5,434	0,181		40	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP PAP	Authenticate-Ack
16	5,435	0,000		40	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP IPCP	Configuration Request
17	5,435	0,000	24		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP IPCP	Configuration Request
18	5,435	0,000	12		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP IPCP	Configuration Ack
19	5,443	0,007		40	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP IPCP	Configuration Nak
20	5,451	0,007	24		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP IPCP	Configuration Request
21	5,458	0,007		40	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP IPCP	Configuration Ack
22	5,696	0,237	53		200.193.245.55	201.10.128.2	DNS	Standard query AAAA lucas
23	5,706	0,010		128	201.10.128.2	200.193.245.55	DNS	Standard query response, No such name
24	15,435	9,728		40	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Echo Request
25	15,436	0,000	14		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Echo Reply
26	17,945	2,508	18		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Termination Request
27	17,954	0,009		40	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Termination Ack
		Total:	242	568				

Tabela 5.3: Comparação entre os dados da captura e os dados do bilhete RADIUS

	Input	*Output*	Origem da Informação
Pre-Octets	97	89	Bilhete
Acct-Octets	145	208	
Soma	242	297	
Tamanho obtido	242	568	Captura
Diferença	0	257	

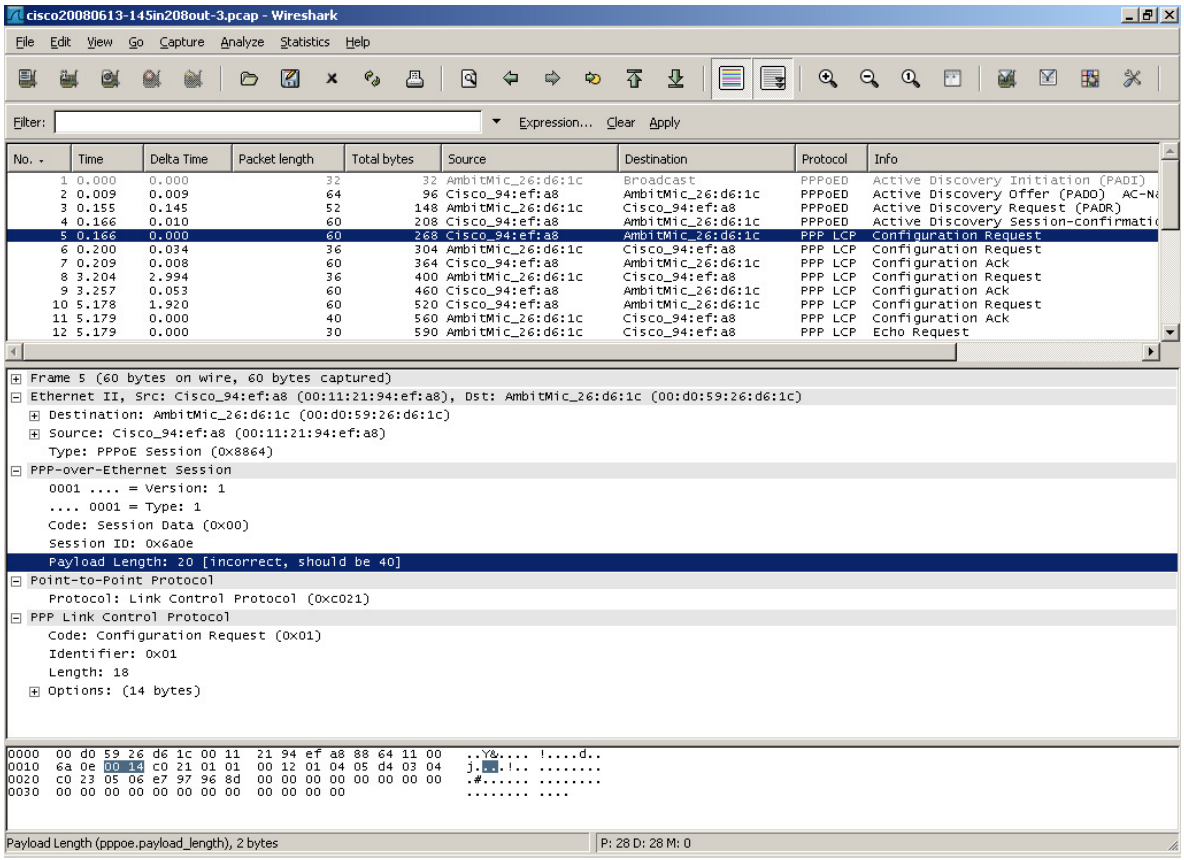

Figura 5.3: Análise do pacote número 5 da captura da Figura 5.1.

Tabela 5.4: Dados da captura Figura 5.1 com tamanho de pacote de saída ajustado

No.	Tempo	D Tempo	Tamanho Entrada	Tamanho Saída	Origem	Destino	Protocolo	Informação adicional
5	0,166	0,000		20	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Configuration Request
6	0,200	0,034	16		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Configuration Request
7	0,209	0,008		16	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Configuration Ack
8	3,204	2,994	16		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Configuration Request
9	3,257	0,053		16	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Configuration Ack
10	5,178	1,920		20	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Configuration Request
11	5,179	0,000	20		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Configuration Ack
12	5,179	0,000	10		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Echo Request
13	5,179	0,000	35		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP PAP	Authenticate-Request
14	5,253	0,073		10	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Echo Reply
15	5,434	0,181		7	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP PAP	Authenticate-Ack
16	5,435	0,000		12	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP IPCP	Configuration Request
17	5,435	0,000	24		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP IPCP	Configuration Request
18	5,435	0,000	12		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP IPCP	Configuration Ack
19	5,443	0,007		24	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP IPCP	Configuration Nak
20	5,451	0,007	24		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP IPCP	Configuration Request
21	5,458	0,007		24	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP IPCP	Configuration Ack
22	5,696	0,237	53		200.193.245.55	201.10.128.2	DNS	Standard query AAAA lucas
23	5,706	0,010		128	201.10.128.2	200.193.245.55	DNS	Standard query response, No such name
24	15,435	9,728		14	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Echo Request
25	15,436	0,000	14		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Echo Reply
26	17,945	2,508	18		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Termination Request
27	17,954	0,009		6	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Termination Ack
		Total:	242	297				

Tal fenômeno ocorreu para todos os pacotes originados no NAS. A partir das informações obtidas através do programa de captura, os dados da coluna “Tamanho Saída” da Tabela 5.2 foram corrigidos e são apresentados na Tabela 5.4.

A comparação entre o resultado da captura ajustado na Tabela 5.4 e os dados do bilhete da Figura 5.1 é apresentada na Tabela 5.5. Percebe-se agora uma coerência entre o resultado da captura e os valores obtidos no bilhete RADIUS, o que indica que a relação entre o tráfego do cliente e os contadores do NAS foi encontrada.

Tabela 5.5: Nova comparação entre os dados da captura e os dados do bilhete RADIUS

	Input	*Output*	Origem da Informação
Pre-Octets	97	89	Bilhete
Acct-Octets	145	208	
Soma	242	297	
Tamanho obtido	242	297	Captura
Diferença	0	0	

Cabe, ainda, determinar em que momentos inicia e termina a contagem de tráfego apresentada nos bilhetes RADIUS para cada um dos sentidos. A partir das informações de tamanho dos pacotes e dos valores parciais constantes no bilhete RADIUS é possível determinar esses momentos, que estão indicados na Tabela 5.6.

Pelo apresentado na Tabela 5.6, o momento que determina o início da conexão é o envio da mensagem de reconhecimento de autenticação (*Authenticate Ack*) do NAS para o cliente e o do final de conexão é o envio do reconhecimento do final de conexão (*Termination Ack*), também do NAS para o cliente. De posse dessas informações sobre os momentos de início e de fim de conexão, podemos determinar, com base nos dados da coluna “Tempo” da tabela, a duração da conexão. As linhas relevantes da tabela foram utilizadas para construir a Tabela 5.7.

Observa-se que os tempos obtidos através do *software* de captura refletem o momento de chegada dos pacotes na interface *Ethernet* no computador cliente. É razoável conceber que o tempo de trânsito dos pacotes que determinam o início e fim da conexão sejam muito similares, pois são de mesmo tamanho (60 *bytes* no quadro *Ethernet*, conforme Tabela 5.1). Assim, a diferença de tempo entre o instante de tempo do início da conexão e o de final de conexão será a mesma, vista pelo NAS ou pelo computador cliente.

Tabela 5.6: Determinação do início e término da contagem de tráfego

No.	Tempo	D Tempo	Tamanho Entrada	Tamanho Saída	Origem	Destino	Protocolo	Informação adicional
5	0,166	0,000		20	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Configuration Request
6	0,200	0,034	16		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Configuration Request
7	0,209	0,008		16	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Configuration Ack
8	3,204	2,994	16		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Configuration Request
9	3,257	0,053		16	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Configuration Ack
10	5,178	1,920		20	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Configuration Request
11	5,179	0,000	20		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Configuration Ack
12	5,179	0,000	10		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Echo Request
13	5,179	0,000	35		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP PAP	Authenticate-Request
14	5,253	0,073		10	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Echo Reply
15	5,434	0,181		7	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP PAP	Authenticate-Ack
		Sub-total:	97	89				INÍCIO DA CONEXÃO
16	5,435	0,000		12	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP IPCP	Configuration Request
17	5,435	0,000	24		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP IPCP	Configuration Request
18	5,435	0,000	12		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP IPCP	Configuration Ack
19	5,443	0,007		24	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP IPCP	Configuration Nak
20	5,451	0,007	24		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP IPCP	Configuration Request
21	5,458	0,007		24	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP IPCP	Configuration Ack
22	5,696	0,237	53		200.193.245.55	201.10.128.2	DNS	Standard query AAAA lucas
23	5,706	0,010		128	201.10.128.2	200.193.245.55	DNS	Standard query response, No such name
24	15,435	9,728		14	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Echo Request
25	15,436	0,000	14		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Echo Reply
26	17,945	2,508	18		AmbitMic_26:d6:1c	Cisco_94:ef:a8	PPP LCP	Termination Request
27	17,954	0,009		6	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Termination Ack
		Sub-total:	145	208				FIM DA CONEXÃO

Tabela 5.7: Determinação da duração da conexão

No.	Tempo	D Tempo	Tamanho Entrada	Tamanho Saída	Origem	Destino	Protocolo	Informação adicional
15	5,434	0		7	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP PAP	Authenticate-Ack
27	17,954	12,520		6	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Termination Ack
	Total	12,520						

A conexão em análise durou, de acordo com os dados apresentados na Tabela 5.7, o equivalente a 12,520 segundos. Considerando que o valor do atributo *Acct-Session-Time* do bilhete RADIUS é sempre dado em segundos, fazendo o arredondamento do valor obtido pelo processo de captura, obtêm-se 13 segundos, que coincide com o valor presente no bilhete RADIUS da Figura 5.2.

No bilhete da Figura 5.2 existe também o atributo *PreSession-Time*, com valor igual a 5 segundos. De forma análoga à utilizada para determinar a duração da conexão, podemos

avaliar o tempo despendido em estabelecer a conexão, o que é feito através da Tabela 5.8. O valor obtido, arredondado para segundos, é 5 segundos, o que coincide com o valor presente no atributo *PreSession-Time*.

Tabela 5.8: Determinação da duração do estabelecimento da conexão

No.	Tempo	D Tempo	Tamanho Entrada	Tamanho Saída	Origem	Destino	Protocolo	Informação adicional
5	0,166	0		20	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP LCP	Configuration Request
15	5,434	5,268		7	Cisco_94:ef:a8	AmbitMic_26:d6:1c	PPP PAP	Authenticate-Ack
	Total	5,268						

Foi descoberto também, a partir de outros arquivos de captura, que os pacotes contendo mensagens de controle do protocolo PPP (solicitações *LCP Echo Request* e as respectivas respostas *LCP Echo Response*) não são contabilizados pelo NAS quando a mensagem *LCP Echo Request* é gerada pelo equipamento da extremidade do cliente.

Como resultado desta análise, temos na Tabela 5.9 as regras para o cálculo da duração de conexão e do consumo de tráfego para o NAS *Cisco* 10008.

Tabela 5.9: Regras de contabilização para o *Cisco* 10008

No.	Descrição da regra
1	A conexão inicia com o reconhecimento da autenticação (emissão da mensagem *"Authenticate Ack"* pelo NAS).
2	A conexão termina com o reconhecimento do final de conexão (emissão da mensagem *"Termination Ack"* pelo NAS).
3	A contagem de tráfego de entrada no NAS baseia-se no tamanho do pacote PPP recebido, contando os eventuais *bytes* de *padding* inseridos no pacote.
4	A contagem de tráfego de saída do NAS leva em conta apenas o conteúdo líquido do pacote PPP, não incluindo os eventuais *bytes* de *padding* que forem inseridos no pacote.
5	A contagem de tráfego não considera os pacotes contendo as mensagens de controle *LCP Echo Request* originadas pela terminação do lado do cliente e as respectivas *LCP Echo Response* geradas pelo NAS.

Não foi aqui descrita a análise para a contabilização da quantidade de pacotes trafegados, porém, nos testes realizados, a contagem de pacotes do processo de captura sempre coincidiu com os números apresentados nos bilhetes RADIUS para os atributos *Acct-Input-Packets* e *Acct-Output-Packets.*

Esse processo de análise foi repetido com igual resultado em diversas rodadas de avaliação de conexões de curta duração e, com base nos resultados obtidos, um programa foi desenvolvido para processar os arquivos de captura do *software Wireshark* exportados para o formato PDML. A Figura 5.4 apresenta o resultado para o arquivo correspondente à Figura 5.1.

```
Processamento do arquivo: cisco20080613-145in208out-3.pdml.xml
Encontrados 28 pacotes
Processados 23 do protocolo PPP
-----------------------------------
Pre-Input-Octets    = 97
Pre-Output-Octets   = 89
Pre-Total-Octets    = 186
-----------------------------------
Pre-Input-Packets   = 5
Pre-Output-Packets  = 6
Pre-Total-Packets   = 11
-----------------------------------
Acct-Input-Octets   = 145
Acct-Output-Octets  = 208
Acct-Total-Octets   = 353
-----------------------------------
Acct-Input-Packets  = 6
Acct-Output-Packets = 6
Acct-Total-Packets  = 12
-----------------------------------
Duração: 12.519754 segundos
-----------------------------------
```

Figura 5.4: Saída do programa de análise para o arquivo PDML da captura da Figura 5.1.

O procedimento descrito acima para o equipamento *Cisco* 10008 foi, então, realizado utilizando a conexão ADSL cuja terminação lógica era feita em um NAS *Juniper* ERX 1440. A análise das capturas de pacotes de conexões, porém, indicou diferenças significativas entre a contabilização realizada conforme a descrição apresentada na seção 4.7 e os valores encontrados nos bilhetes RADIUS correspondentes. Algumas formas de contabilização alternativas foram pesquisadas, porém nenhum padrão consistente foi encontrado.

Como uma possível explicação para as divergências encontradas era a presença de algum defeito de *software*, particular à versão instalada no NAS, um novo conjunto de testes foi realizado utilizando outro acesso ADSL, conectado logicamente a outro NAS do mesmo modelo, cuja versão de sistema operacional instalado era mais recente. Os resultados obtidos, apesar de diferentes dos anteriores, foram igualmente insatisfatórios, por não seguirem a descrição do fabricante e não possuírem um padrão identificável.

Como os equipamentos NAS utilizados nos dois testes possuem versões de *software* relativamente antigas e que não possuem mais total suporte por parte do fabricante, a possibilidade de realizar um terceiro conjunto de testes, desta vez utilizando um NAS com sistema operacional em versão recente, foi avaliada. Foi localizado um equipamento em outra cidade que possuía as características necessárias, e a conexão lógica do acesso ADSL foi, então, transferida para esse outro equipamento.

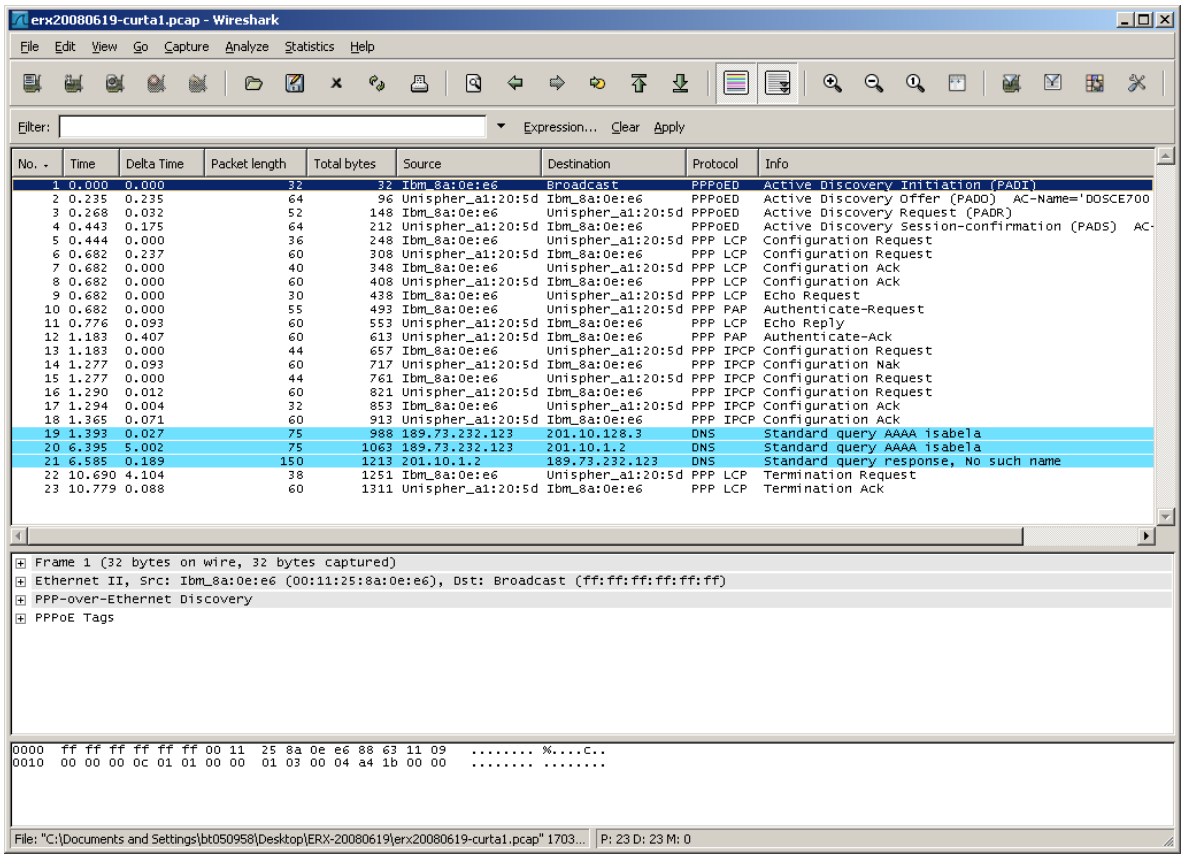

Figura 5.5: Captura de tráfego para uma conexão PPPoE com o NAS *Juniper* ERX 1440

Um novo conjunto de capturas foi realizado, e a análise foi conduzida de forma similar à realizada para o equipamento *Cisco* 10008. A Figura 5.5 apresenta a tela do *software Wireshark*, cuja apresentação dos dados é similar à da Figura 5.1, que corresponde a uma conexão realizada com o NAS *Juniper* ERX 1440. Nesta conexão, foram trafegados 23 pacotes de dados.

O bilhete correspondente a esta conexão pode ser visto na Figura 5.6. Nesse bilhete, não estão apresentados os atributos RADIUS não relacionados com o experimento, havendo os atributos sido reordenados para a uma seqüência similar à dos presentes na Figura 5.2.

O tráfego capturado, mostrado na Figura 5.5, representa uma conexão PPPoE integral, o que inclui o estabelecimento da sessão PPPoE (pacotes de 1 a 4), o estabelecimento da conexão PPP (pacotes de 5 a 18), o tráfego de dados IP (pacotes 19 a 21), a solicitação de finalização do PPP (pacote 22) e a confirmação de finalização da sessão PPP (pacote 23). Cabe ressaltar que, em nenhuma das capturas realizadas com os NAS do fabricante *Juniper*, o pacote correspondente ao encerramento da sessão PPPoE – equivalente ao

pacote 28 da Figura 5.1 – foi recebido pela estação cliente. Trata-se, porém, de mera constatação, pois tal comportamento não prejudica a análise.

```
Thu Jun 19 18:08:39 GMT-03:00 2008
        Unisphere-PPPoE-Description = "pppoe 00:11:25:8a:0e:e6"
        Acct-Status-Type = Stop
        User-Name = "agski@wireshark.com.br"
        Acct-Delay-Time = 0
        Framed-Protocol = PPP
        Framed-IP-Address = 189.73.232.123
        Acct-Input-Gigawords = 0
        Acct-Input-Octets = 170
        Acct-Output-Gigawords = 0
        Acct-Output-Octets = 190
        Unisphere-Input-Gigapackets = 0
        Acct-Input-Packets = 2
        Unisphere-Output-Gigapackets = 0
        Acct-Output-Packets = 1
        Acct-Session-Time = 10
        NAS-Identifier = "DOSCE700"
        Brt-Acct-Start-Time = "2008/06/19 17:58:33"
        Brt-Acct-Stop-Time = "2008/06/19 17:58:43"
```

Figura 5.6: Bilhete correspondente à captura de tráfego representada na Figura 5.5.

Para a análise do tráfego, as informações da captura apresentada na Figura 5.5 foram convertidas na Tabela 5.10 abaixo:

Tabela 5.10: Dados da captura da Figura 5.5

No.	Tempo	D Tempo	Tamanho	Acumulado	Origem	Destino	Protocolo	Informação adicional
1	0,000	0,000	32	32	Ibm_8a:0e:e6	Broadcast	PPPoED	Active Discovery Initiation (PADI)
2	0,235	0,235	64	96	Unispher_a1:20:5d	Ibm_8a:0e:e6	PPPoED	Active Discovery Offer (PADO)
3	0,268	0,032	52	148	Ibm_8a:0e:e6	Unispher_a1:20:5d	PPPoED	Active Discovery Request (PADR)
4	0,443	0,175	64	212	Unispher_a1:20:5d	Ibm_8a:0e:e6	PPPoED	Active Discovery Session-confirmation (PADS)
5	0,444	0,000	36	248	Ibm_8a:0e:e6	Unispher_a1:20:5d	PPP LCP	Configuration Request
6	0,682	0,237	60	308	Unispher_a1:20:5d	Ibm_8a:0e:e6	PPP LCP	Configuration Request
7	0,682	0,000	40	348	Ibm_8a:0e:e6	Unispher_a1:20:5d	PPP LCP	Configuration Ack
8	0,682	0,000	60	408	Unispher_a1:20:5d	Ibm_8a:0e:e6	PPP LCP	Configuration Ack
9	0,682	0,000	30	438	Ibm_8a:0e:e6	Unispher_a1:20:5d	PPP LCP	Echo Request
10	0,682	0,000	55	493	Ibm_8a:0e:e6	Unispher_a1:20:5d	PPP PAP	Authenticate-Request
11	0,776	0,093	60	553	Unispher_a1:20:5d	Ibm_8a:0e:e6	PPP LCP	Echo Reply
12	1,183	0,407	60	613	Unispher_a1:20:5d	Ibm_8a:0e:e6	PPP PAP	Authenticate-Ack
13	1,183	0,000	44	657	Ibm_8a:0e:e6	Unispher_a1:20:5d	PPP IPCP	Configuration Request
14	1,277	0,093	60	717	Unispher_a1:20:5d	Ibm_8a:0e:e6	PPP IPCP	Configuration Nak
15	1,277	0,000	44	761	Ibm_8a:0e:e6	Unispher_a1:20:5d	PPP IPCP	Configuration Request
16	1,290	0,012	60	821	Unispher_a1:20:5d	Ibm_8a:0e:e6	PPP IPCP	Configuration Request
17	1,294	0,004	32	853	Ibm_8a:0e:e6	Unispher_a1:20:5d	PPP IPCP	Configuration Ack
18	1,365	0,071	60	913	Unispher_a1:20:5d	Ibm_8a:0e:e6	PPP IPCP	Configuration Ack
19	1,393	0,027	75	988	189.73.232.123	201.10.128.3	DNS	Standard query AAAA Isabela
20	6,395	5,002	75	1063	189.73.232.123	201.10.1.2	DNS	Standard query AAAA Isabela
21	6,585	0,189	150	1213	201.10.1.2	189.73.232.123	DNS	Standard query response, No such name
22	11,.690	4,104	38	1251	Ibm_8a:0e:e6	Unispher_a1:20:5d	PPP LCP	Termination Request
23	10,779	0,088	60	1311	Unispher_a1:20:5d	Ibm_8a:0e:e6	PPP LCP	Termination Ack

Tal como na outra análise, em decorrência de a informação de tamanho (coluna 4) estar relacionada com o quadro *Ethernet*, percebe-se que os contadores apresentados no bilhete da Figura 5.6 não possuem uma relação clara com os dados apresentados na Tabela 5.10. Assim, o mesmo procedimento utilizado para gerar a Tabela 5.2 foi utilizado para criar Tabela 5.11, segmentando o tráfego de entrada e de saída, ajustando o tamanho do pacote e excluindo os pacotes relacionados com o estabelecimento da sessão PPPoE. Como era esperado, pela descrição da seção 4.7, que apenas os pacotes posteriores ao de reconhecimento da autenticação (mensagem *"Authentication Ack"*) e anteriores aos das mensagens de final de conexão PPP (mensagens *"Termination Request"* e *"Termination ACK"*) fossem contabilizados nos contadores de tráfego, só os pacotes nessas condições foram apresentados na Tabela 5.11. Nessa tabela, a última linha mostra o resultado do somatório dos valores das colunas "Tamanho Entrada" e "Tamanho Saída".

Tabela 5.11: Dados da captura da Figura 5.5 com tamanho de pacote ajustado

No.	Tempo	D Tempo	Tamanho Entrada	Tamanho Saída	Origem	Destino	Protocolo	Informação adicional
13	1,183	0,000	24		Ibm_8a:0e:e6	Unispher_a1:20:5d	PPP IPCP	Configuration Request
14	1,277	0,093		40	Unispher_a1:20:5d	Ibm_8a:0e:e6	PPP IPCP	Configuration Nak
15	1,277	0,000	24		Ibm_8a:0e:e6	Unispher_a1:20:5d	PPP IPCP	Configuration Request
16	1,290	0,012		40	Unispher_a1:20:5d	Ibm_8a:0e:e6	PPP IPCP	Configuration Request
17	1,294	0,004	12		Ibm_8a:0e:e6	Unispher_a1:20:5d	PPP IPCP	Configuration Ack
18	1,365	0,071		40	Unispher_a1:20:5d	Ibm_8a:0e:e6	PPP IPCP	Configuration Ack
19	1,393	0,027	55		189.73.232.123	201.10.128.3	DNS	Standard query AAAA Isabela
20	6,395	5,002	55		189.73.232.123	201.10.1.2	DNS	Standard query AAAA Isabela
21	6,585	0,189		130	201.10.1.2	189.73.232.123	DNS	Standard query response, No such name
		Total:	170	250				

Percebe-se um primeiro resultado, que é a convergência do valor do totalizador de tráfego de entrada (valor total da coluna "Tamanho Entrada") para o valor apresentado no bilhete da Figura 5.6, no atributo *Acct-Input-Octets*. O valor correspondente ao tráfego de saída, porém, necessitava de uma melhor investigação.

Essa investigação seguiu o mesmo caminho e obteve o mesmo resultado da investigação conduzida para a situação similar encontrada na análise de tráfego realizada para o NAS do fabricante *Cisco*. Naquela foi detectado que os contadores de tráfego de saída consideravam apenas o tamanho da mensagem e não o valor integral do pacote PPP. A Tabela 5.12 apresenta os dados dos pacotes da Tabela 5.11, com os valores do tráfego de saída considerando apenas o tamanho das mensagens.

Percebe-se agora que os valores obtidos pela análise do tráfego capturado correspondem aos valores dos contadores de tráfego encontrados no bilhete, sugerindo que as regras de avaliação de tráfego para o equipamento do fabricante *Juniper* foram descobertas.

Tabela 5.12: Dados da captura da Figura 5.5 com tamanho de pacote de saída ajustado

No.	Tempo	D Tempo	Tamanho Entrada	Tamanho Saída	Origem	Destino	Protocolo	Informação adicional
13	1,183	0,000	24		Ibm_8a:0e:e6	Unispher_a1:20:5d	PPP IPCP	Configuration Request
14	1,277	0,093		24	Unispher_a1:20:5d	Ibm_8a:0e:e6	PPP IPCP	Configuration Nak
15	1,277	0,000	24		Ibm_8a:0e:e6	Unispher_a1:20:5d	PPP IPCP	Configuration Request
16	1,290	0,012		12	Unispher_a1:20:5d	Ibm_8a:0e:e6	PPP IPCP	Configuration Request
17	1,294	0,004	12		Ibm_8a:0e:e6	Unispher_a1:20:5d	PPP IPCP	Configuration Ack
18	1,365	0,071		24	Unispher_a1:20:5d	Ibm_8a:0e:e6	PPP IPCP	Configuration Ack
19	1,393	0,027	55		189.73.232.123	201.10.128.3	DNS	Standard query AAAA Isabela
20	6,395	5,002	55		189.73.232.123	201.10.1.2	DNS	Standard query AAAA Isabela
21	6,585	0,189		130	201.10.1.2	189.73.232.123	DNS	Standard query response, No such name
		Total;	170	190				

Confirmados, então, os momentos de início e fim de conexão, podemos determinar, com base nos dados da coluna “Tempo” da Tabela 5.10, a duração da conexão. As linhas relevantes dessa tabela foram utilizadas para construir a Tabela 5.13.

Tabela 5.13: Determinação da duração da conexão para o NAS *Juniper* ERX

No.	Tempo	D Tempo	Tamanho	Acumulado	Origem	Destino	Protocolo	Informação adicional
12	1,183	0	60	613	Unispher_a1:20:5d	Ibm_8a:0e:e6	PPP PAP	Authenticate-Ack
23	10,779	9,569	60	1311	Unispher_a1:20:5d	Ibm_8a:0e:e6	PPP LCP	Termination Ack
	Total	9,569						

As mesmas considerações aplicadas ao NAS *Cisco* 10008 podem ser utilizadas para esta situação, de maneira que a conexão em análise durou, de acordo com os dados apresentados na Tabela 5.13, o equivalente a 9,569 segundos, donde, pelo mesmo critério de arrendondamento aplicado anteriormente, chega-se ao valor de 10 segundos, que coincide com o número presente no bilhete RADIUS da Figura 5.6 para o atributo *Acct-Session-Time*.

Foi constatado, nos testes com o NAS *Juniper* ERX, que os pacotes contendo mensagens de controle do protocolo PPP (solicitações *LCP Echo Request* e as respectivas respostas *LCP Echo Response*) são, ao contrário do que ocorre no NAS *Cisco* 10008, contabilizados pelo NAS quando a mensagem *“LCP Echo Request”* é gerada pelo equipamento da extremidade do cliente.

A quantidade de pacotes trafegados, em todos os testes realizados com o NAS *Juniper* ERX para a determinação do método de contabilização, coincidiu com os números apresentados nos bilhetes RADIUS para os atributos *Acct-Input-Packets* e *Acct-Output-Packets*, considerando os critérios apontados na seção 4.7.

Esse processo de análise foi repetido com igual resultado em diversas rodadas de avaliação de conexões de curta duração e, com base nos resultados obtidos, o programa desenvolvido quando da análise dos critérios de contabilização de tráfego do NAS *Cisco* 10008 foi adaptado para processar os arquivos de captura, em formato PDML, obtidos para o NAS *Juniper* ERX. A Figura 5.7 apresenta o resultado para o arquivo correspondente à captura representada na Figura 5.5.

```
Processamento do arquivo: erx20080619-curta1.pdml.xml
Encontrados 23 pacotes
Processados 19 do protocolo PPP
-------------------------------------
Acct-Input-Octets   = 170
Acct-Output-Octets  = 190
Acct-Total-Octets   = 360
-------------------------------------
Acct-Input-Packets  = 2
Acct-Output-Packets = 1
Acct-Total-Packets  = 3
-------------------------------------
Início: 1.183740000
Fim: 10.779203000
Duração: 9.595463 segundos
-------------------------------------
```

Figura 5.7: Saída do programa de análise para o arquivo PDML da captura da Figura 5.5.

Como resultado dessa análise, temos, na Tabela 5.14 as regras para o cálculo da duração de conexão e do consumo de tráfego para o NAS *Juniper* ERX.

Tabela 5.14: Regras de contabilização para o NAS *Juniper* ERX

No.	Descrição da regra
1	A conexão inicia com o reconhecimento da autenticação (emissão da mensagem *"Authenticate Ack"* pelo NAS).
2	A conexão termina com o reconhecimento do final de conexão (emissão da mensagem *"Termination Ack"* pelo NAS).
3	A contagem de tráfego de entrada no NAS baseia-se no tamanho do pacote PPP recebido, contando os eventuais *bytes* de *padding* inseridos no pacote.
4	A contagem de tráfego de saída do NAS leva em conta apenas o conteúdo líquido do pacote PPP, não incluindo os eventuais *bytes* de *padding* que forem inseridos no pacote.
5	A contagem de tráfego considera os pacotes contendo as mensagens de controle *LCP Echo Request* originadas pela terminação do lado do cliente e as respectivas *LCP Echo Response* geradas pelo NAS.

A segunda parte do experimento consistiu em realizar capturas de tráfego em conexões com duração e tráfego não previamente determinados e comparar o resultado fornecido pelo programa de contabilização de trafego desenvolvido por este autor com os valores disponíveis nos bilhetes correspondentes.

As primeiras comparações demonstraram a necessidade de revisitar a análise da avaliação do tráfego de saída feita para os dois tipos de NAS, pois existia uma diferença bastante grande entre o valor do bilhete e o valor calculado pelo programa. Para o tráfego de entrada no NAS, independentemente do modelo, o valor apontado era sempre coincidente com o do bilhete.

Como, em todas as conexões, o número de pacotes analisados pelo programa sempre coincidiu com o número de pacotes apontados no bilhete, e o número obtido pelo programa era, na maioria das vezes, menor do que o valor que o bilhete apresentava, a suspeita recaiu sobre o método de cálculo do tamanho do pacote PPP.

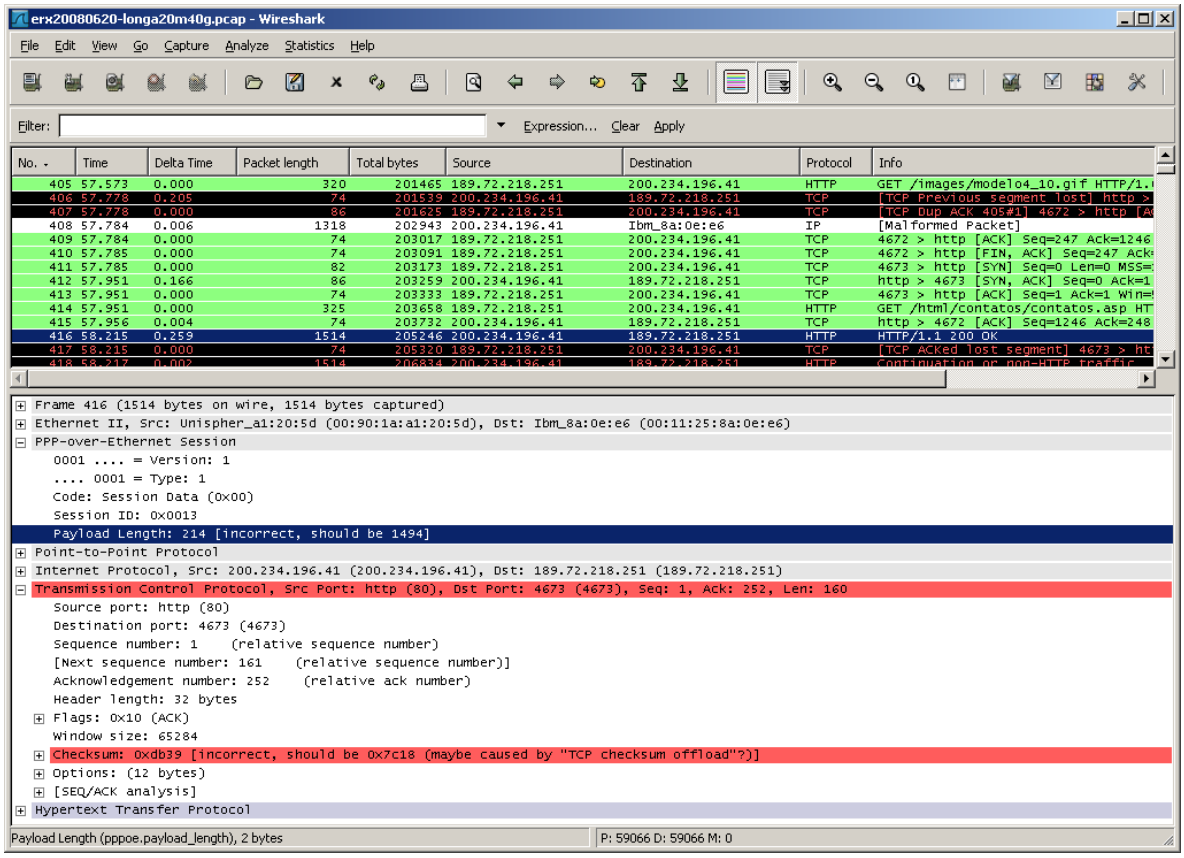

Figura 5.8: Tela do programa *Wireshark* para uma conexão de maior duração.

Analisando uma captura de maior duração através do *software Wireshark*, foi possível verificar que, durante uma conexão, são registrados diversos pacotes que apresentam algum tipo de má formação ou erro de *checksum*, como pode ser apreciado na Figura 5.8. Nessa figura podemos ver as duas situações: para o quadro de número 408, o *Wireshark* aponta a existência de má formação do pacote IP e, para o quadro 416, cuja análise está parcialmente aberta na parte inferior da figura, indica a ocorrência de erro de *checksum*.

O tamanho indicado no pacote PPP para o conteúdo do quadro número 416, (linha destacada em azul, *Payload length*) é 214 *bytes* quando deveria ser, segundo a análise do *Wireshark*, 1494 *bytes*. De fato, na parte inferior da Figura 5.9, podemos verificar que efetivamente tal quadro tem tamanho 1514 *bytes*: trata-se da transcrição da parte final do quadro *Ethernet*, e, na última linha, que inicia pelo índice 05E0, há 10 posições ocupadas. Por aritmética simples, em base hexadecimal, temos que a última posição corresponde a 0E0A, que, uma vez convertido para base decimal, chega ao número 1514.

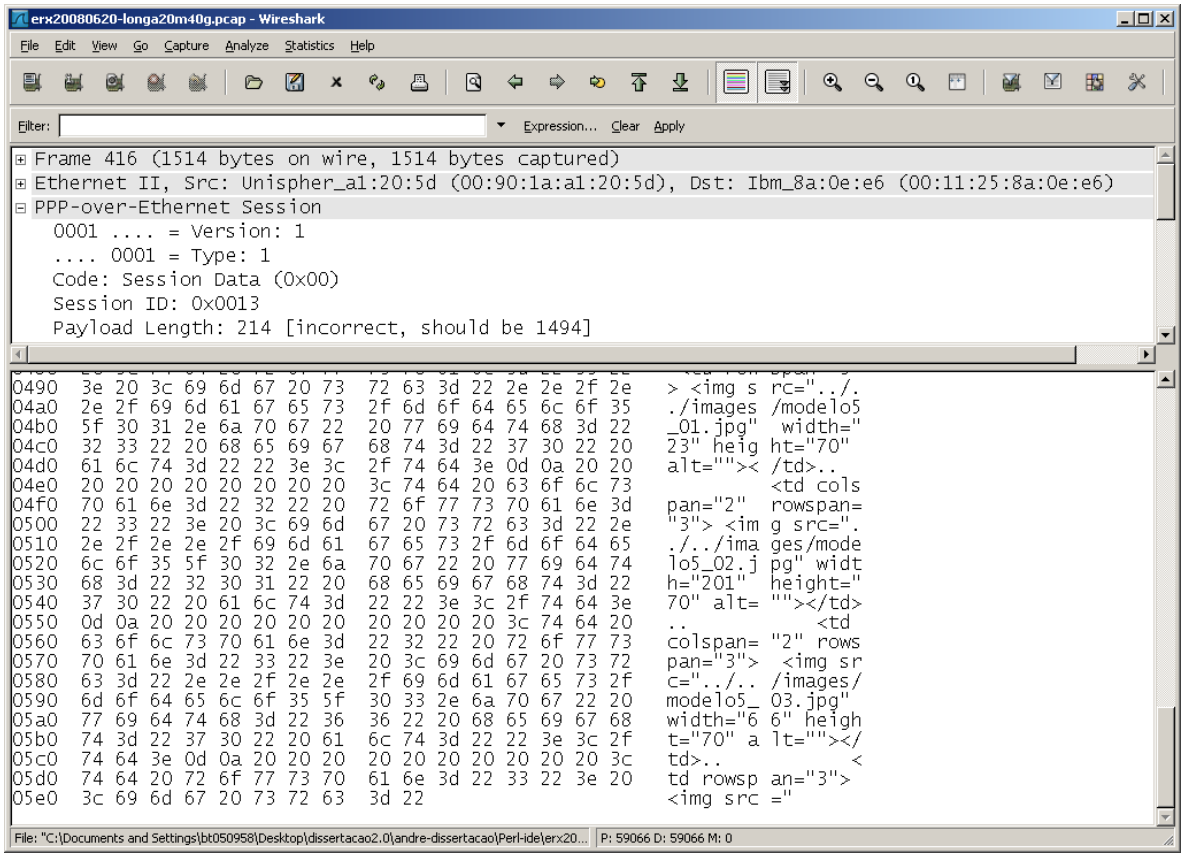

Figura 5.9: Tela do programa *Wireshark* para o quadro 416.

Assim, os 1494 *bytes* indicados pelo *Wireshark* para o tamanho do pacote PPP efetivamente correspondem ao tamanho do quadro capturado, 1514 *bytes*, menos os 20 *bytes* de cabeçalhos introduzidos pelo quadro *Ethernet* e pela sessão PPPoE.

Observando a transcrição do pacote 416 dessa captura, da posição final para a inicial, facilmente conclui-se que a diferença entre o tamanho apresentado para o pacote PPP e o seu tamanho efetivo não se origina em preenchimento (*padding*) feito pelos processos do NAS que implementam o protocolo PPPoE, devendo, então, esse pacote ser contabilizado com tamanho 1494 *bytes* e não 214 *bytes*.

Diante dessas considerações, o programa de análise de arquivos de captura foi modificado para apenas considerar a existência de preenchimento em pacotes de controle do PPP (LCP, IPCP, PAP), utilizando nessas situações o valor reportado para o conteúdo do PPP pelo encapsulamento imediatamente superior, que nos testes realizados corresponde ao PPPoE. Nas demais situações, o tamanho do pacote PPP é obtido pela subtração de 20 *bytes* do valor do quadro *Ethernet* capturado.

Uma vez ajustado o programa de análise de arquivos de captura, foi ele aplicado aos arquivos de captura disponíveis, obtendo-se coincidência entre os valores apresentados para o tráfego nos bilhetes e as informações providas pelo do programa.

Por outro lado, a avaliação do tempo de conexão, através da utilização do programa de análise de captura, revelou uma situação especial. Em função da configuração de autorização RADIUS utilizada para alguns dos testes, algumas conexões foram encerradas depois de decorrido o prazo estipulado através do atributo *Session-Timeout*. Nesse caso, o NAS *Cisco* 10008 não realizou a solicitação de final de conexão PPP através do envio de uma mensagem *"Terminate Request"*, mas encerrou a sessão PPPoE através de um pacote *"PPP Active Discovery Terminate"*, como pode ser visto na Figura 5.10; essa figura corresponde à tela do programa *Wireshark* para uma conexão que durou 3.600 segundos, de acordo com o bilhete da Figura 5.11.

Como o programa de análise de captura não processa os pacotes não encapsulados em PPPoE – o pacote *PPP Active Discovery Terminate* é um exemplo desse caso –, o programa utiliza o carimbo de tempo do último quadro recebido com tal encapsulamento

para estimar o momento de final de conexão. Assim, como pode ser visto na Figura 5.12, o programa indicou que a sessão durou um pouco menos do que o constante no bilhete da Figura 5.11.

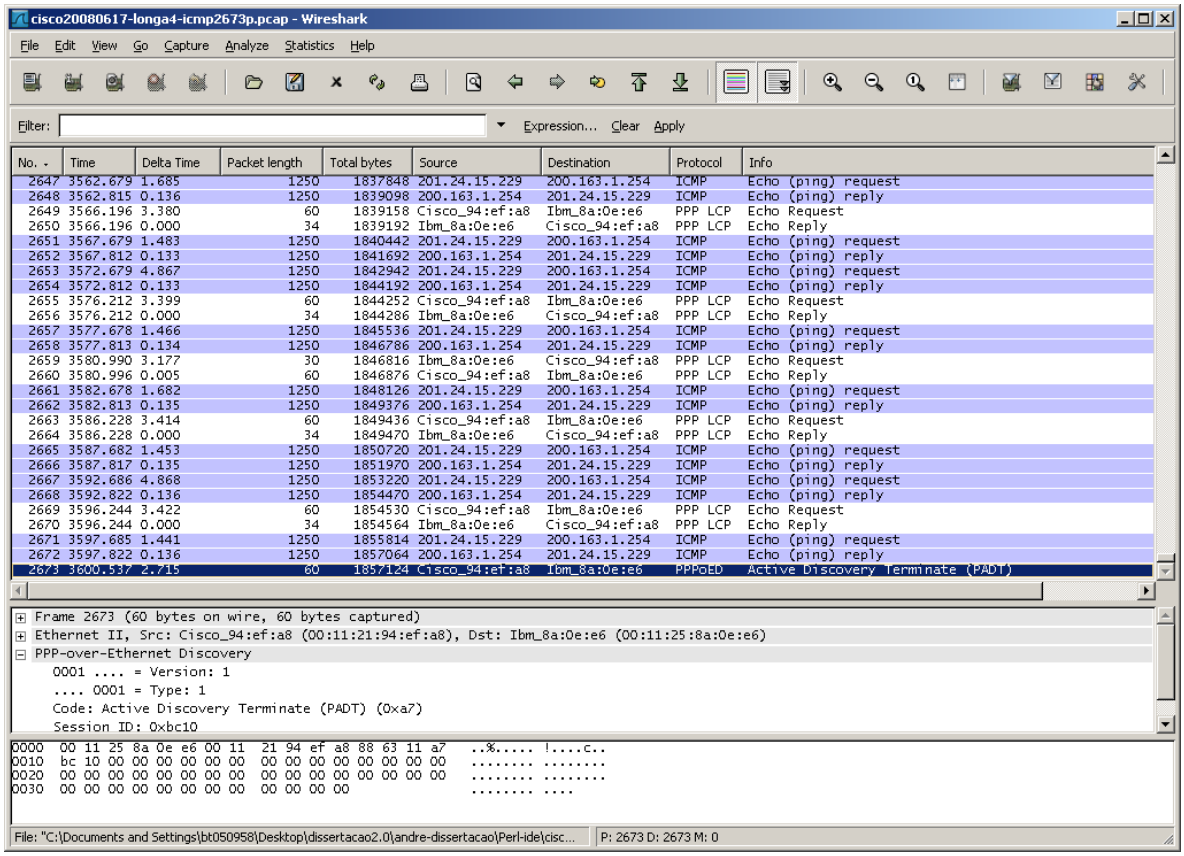

Figura 5.10: Tela do programa *Wireshark* apresentando o encerramento de conexão por solicitação do NAS *Cisco* 10008.

```
Tue Jun 17 17:33:39 GMT-03:00 2008
        Cisco-AVPair = "client-mac-address=0011.258a.0ee6"
        Framed-Protocol = PPP
        Framed-IP-Address = 201.24.15.229
        User-Name = "agski@wireshark.com.br"
        PreSession-Time = 0
        Acct-Session-Time = 3600
        Acct-Input-Octets = 893765
        Acct-Output-Octets = 891146
        Pre-Input-Octets = 81
        Pre-Output-Octets = 53
        Acct-Input-Packets = 1152
        Acct-Output-Packets = 1150
        Pre-Input-Packets = 4
        Pre-Output-Packets = 4
        Acct-Terminate-Cause = Session-Timeout
        Disconnect-Cause = 100
        Acct-Status-Type = Stop
        Acct-Delay-Time = 0
        NAS-Identifier = "BSACE703"
        Brt-Acct-Start-Time = "2008/06/17 16:33:39"
        Brt-Acct-Stop-Time = "2008/06/17 17:33:39"
```

Figura 5.11: Bilhete para a conexão apresentada na Figura 5.10.

```
Processamento do arquivo: cisco20080617-longa4-icmp2892-3600-parte1.pdml.xml
Encontrados 2673 pacotes
Processados 2668 do protocolo PPP
Encontrados 2310 que não são Echo Request ou Reply
-------------------------------------
Pre-Input-Octets    = 81
Pre-Output-Octets   = 53
Pre-Total-Octets    = 134
-------------------------------------
Pre-Input-Packets   = 4
Pre-Output-Packets  = 4
Pre-Total-Packets   = 8
-------------------------------------
Acct-Input-Octets   = 893765
Acct-Output-Octets  = 891146
Acct-Total-Octets   = 1784911
-------------------------------------
Acct-Input-Packets  = 1152
Acct-Output-Packets = 1150
Acct-Total-Packets  = 2302
-------------------------------------
Início: 0.351056000
Fim: 3597.822683000
Duração: 3597.471627 segundos
-------------------------------------
```

Figura 5.12: Saída do programa de captura para a conexão apresentada na Figura 5.10.

Cabe o alerta, portanto, de que quando uma conexão for encerrada de maneira abrupta, ou seja, quando a interrupção da comunicação ocorrer sem a troca de mensagens prevista na definição do protocolo PPP, possivelmente existirá uma diferença na avaliação de duração de conexão quando conduzida de forma isolada pelas partes participantes do enlace.

O mecanismo utilizado para a verificação do estado ativo de um enlace PPP, chamado habitualmente de *ppp keepalive*, pode ser implementado de diversas maneiras, razão pela qual é difícil mapear quais seriam as possíveis diferenças de tempo em função das muitas combinações possíveis de extremos de um enlace PPP. Em geral, porém, essa diferença de tempo estará relacionada com a quantidade de pacotes de *LCP Echo Request* sem resposta *LCP Echo Reply*, que uma implementação aguardará antes de considerar que o enlace está indisponível e, também, o tempo entre as emissões desses pacotes *LCP Echo Request*.

Nesse experimento, a utilização de um ou outro modem ADSL não introduziu modificações perceptíveis no estabelecimento e na manutenção da conexão nem alterações na forma de contabilização do consumo. Os atributos necessários para o adequado registro do consumo das conexões realizadas para este experimento foram sempre encontrados nos bilhetes; destaca-se, porém, a ausência dos atributos *gigawords* (ver seção 5.4.7) nos registros produzidos pelo NAS *Cisco* 10008.

5.4.2 – Determinação do intervalo para a geração de bilhetes intermediários

Uma vez executados os programas desenvolvidos para este experimento, obteve-se um arquivo de saída com os valores de duração de conexões em segundos. Esse arquivo possui 130.747 linhas, sendo o menor valor de tempo encontrado igual a 0 segundo e o maior valor 16.710.714 segundos, o que equivale a pouco mais de 193 dias. A quantidade de bilhetes analisada foi 4.780.658 bilhetes, para igual número de conexões.

As tentativas em produzir uma apresentação das informações com base nos dados do arquivo de durações de conexões em segundos foram infrutíferas, devido ao grande volume de dados. O programa foi, então, modificado para apresentar os dados de duração de conexão acumulados por minuto e por hora, visando a condensar as informações para fins de apresentação. A tabela e as figuras apresentadas nesta seção foram produzidas com base nesses dois novos arquivos de saída.

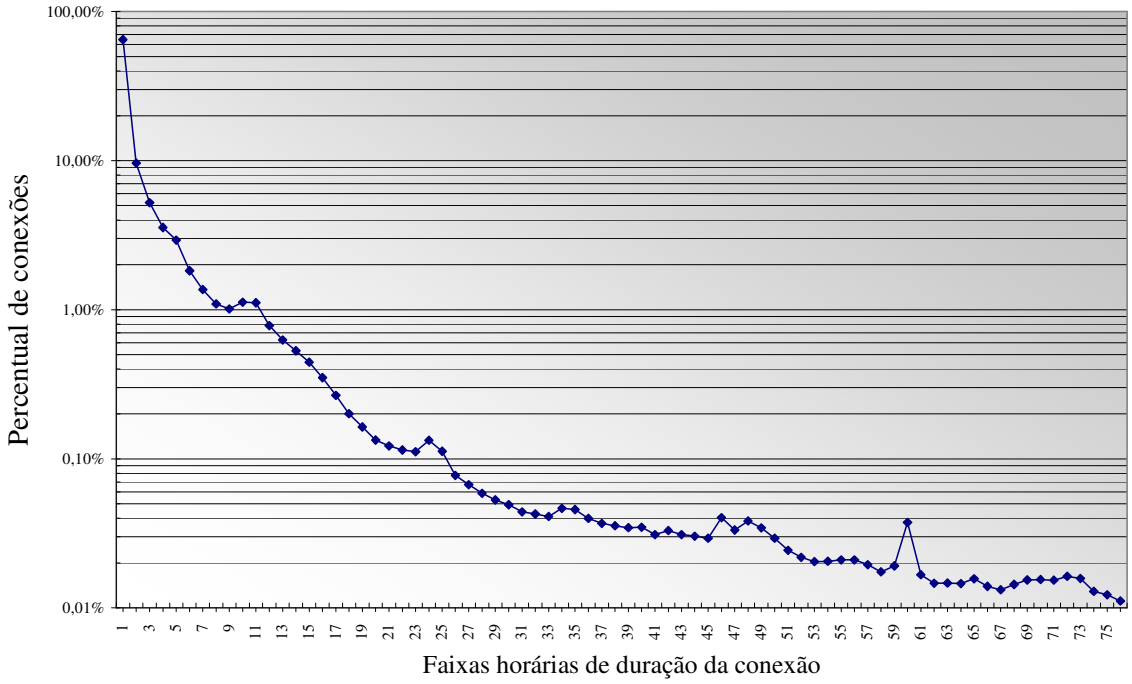

Figura 5.13: Percentual de conexões por faixas de duração

A Figura 5.13 apresenta o percentual de conexões por faixa horária de duração, ou seja, o primeiro ponto corresponde a 64,76% do total de conexões, que tiveram duração entre 0 e

3599 segundos, ou, em outras palavras, conexões de duração inferior a uma hora. O segundo ponto representa 9,63% das conexões, com duração entre 3600 e 7199 segundos e assim sucessivamente. Essa figura, assim como a Tabela 5.15, abrange 99,22% das conexões analisadas; a contribuição individual de cada faixa horária acima de 76 horas é da ordem de 0,1% ou menor, razão pela qual não foi apresentada.

Tabela 5.15: Quantidade e percentual de conexões por faixas de duração

Faixa horária	Quantidade de conexões	Percentual individual	Percentual acumulado	Faixa horária	Quantidade de conexões	Percentual individual	Percentual acumulado
1	3095777	64,756%	64,76%	39	1649	0,034%	98,40%
2	460208	9,626%	74,38%	40	1662	0,035%	98,44%
3	249854	5,226%	79,61%	41	1481	0,031%	98,47%
4	170235	3,561%	83,17%	42	1577	0,033%	98,50%
5	140269	2,934%	86,10%	43	1483	0,031%	98,53%
6	87338	1,827%	87,93%	44	1446	0,030%	98,56%
7	65443	1,369%	89,30%	45	1403	0,029%	98,59%
8	52254	1,093%	90,39%	46	1928	0,040%	98,63%
9	48347	1,011%	91,40%	47	1593	0,033%	98,67%
10	53710	1,123%	92,53%	48	1831	0,038%	98,71%
11	53168	1,112%	93,64%	49	1648	0,034%	98,74%
12	37413	0,783%	94,42%	50	1401	0,029%	98,77%
13	29952	0,627%	95,05%	51	1165	0,024%	98,79%
14	25370	0,531%	95,58%	52	1043	0,022%	98,82%
15	21249	0,444%	96,02%	53	976	0,020%	98,84%
16	16734	0,350%	96,37%	54	983	0,021%	98,86%
17	12755	0,267%	96,64%	55	1005	0,021%	98,88%
18	9611	0,201%	96,84%	56	1005	0,021%	98,90%
19	7821	0,164%	97,01%	57	931	0,019%	98,92%
20	6380	0,133%	97,14%	58	835	0,017%	98,94%
21	5834	0,122%	97,26%	59	916	0,019%	98,96%
22	5476	0,115%	97,38%	60	1787	0,037%	98,99%
23	5331	0,112%	97,49%	61	799	0,017%	99,01%
24	6366	0,133%	97,62%	62	700	0,015%	99,02%
25	5367	0,112%	97,73%	63	702	0,015%	99,04%
26	3698	0,077%	97,81%	64	695	0,015%	99,05%
27	3204	0,067%	97,88%	65	749	0,016%	99,07%
28	2807	0,059%	97,94%	66	668	0,014%	99,08%
29	2536	0,053%	97,99%	67	632	0,013%	99,10%
30	2350	0,049%	98,04%	68	688	0,014%	99,11%
31	2107	0,044%	98,08%	69	737	0,015%	99,13%
32	2042	0,043%	98,12%	70	741	0,015%	99,14%
33	1960	0,041%	98,17%	71	735	0,015%	99,16%
34	2224	0,047%	98,21%	72	779	0,016%	99,17%
35	2181	0,046%	98,26%	73	754	0,016%	99,19%
36	1906	0,040%	98,30%	74	617	0,013%	99,20%
37	1761	0,037%	98,33%	75	586	0,012%	99,21%
38	1703	0,036%	98,37%	76	532	0,011%	99,22%

O valor calculado pelo programa para a média aritmética dos tempos de duração de conexão foi 14510 segundos, o equivalente a 241,83 minutos. Observando o arquivo de saída em segundos, constatou-se que cerca de 50% das conexões duraram entre 0 e 1068 segundos (17,8 minutos), que 30% das conexões duraram entre 1069 e 11120 segundos (185,3 minutos), e que 20% duraram entre 11121 e 16.710.714 segundos. Aproximadamente 83,7% das conexões duraram 242 minutos ou menos. Um pouco mais de 97,5% das conexões duraram menos que 84600 segundos, o equivalente a 24 horas; por conseqüência, um pouco menos de 2,5% das conexões ultrapassaram um dia de duração.

Essa análise, realizada sobre o arquivo de saída do correspondente programa, pode ser acompanhada, de forma complementar, através do gráfico da Figura 5.14. Esse gráfico apresenta o percentual de conexões avaliadas, acumulado por faixa horária de duração das conexões em horas; assim, a primeira coluna representa o percentual de conexões que duraram até uma hora, a segunda coluna mostra o percentual de conexões que duraram até duas horas e assim sucessivamente. O gráfico apresenta as conexões até 76 horas de duração, razão pela qual o percentual final atingido não é 100%, mas, aproximadamente, 99,2%.

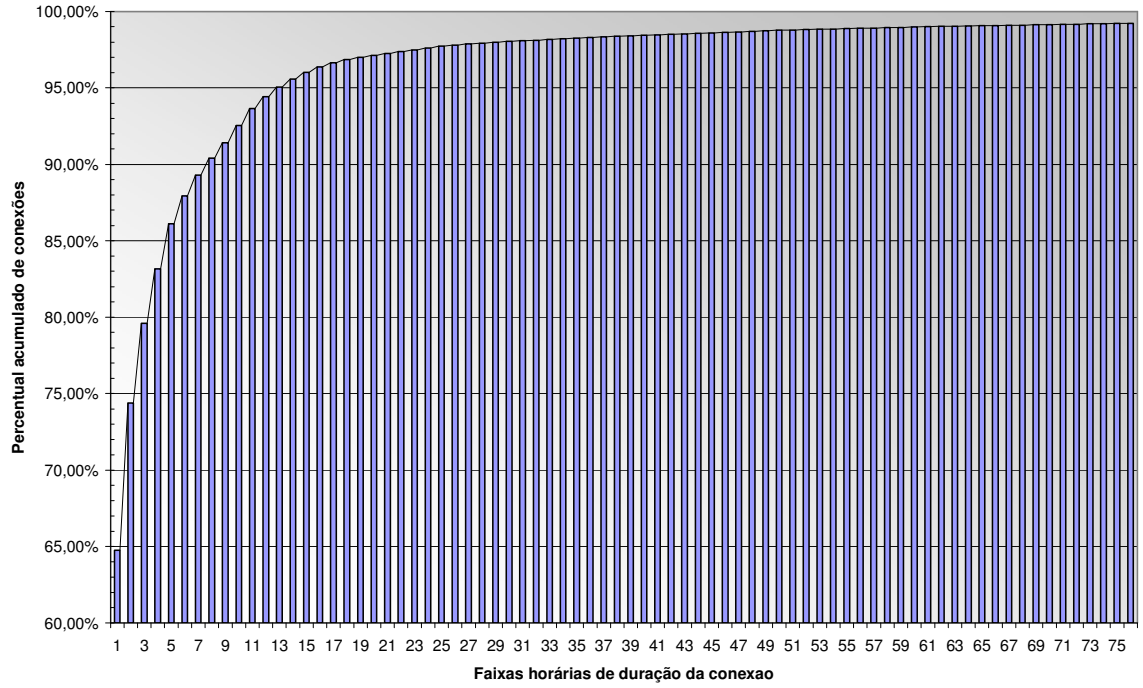

Figura 5.14: Percentual acumulado de conexões por faixas de duração

Com base nas informações de duração de conexão foram realizadas 288 simulações de intervalo de geração de bilhetes intermediários, iniciando com um intervalo de 5 minutos e realizando o acréscimo, a cada nova simulação, de 5 minutos até completar 1440 minutos, que é o equivalente a 24 horas. O intervalo de 24 horas é o maior intervalo configurável para a bilhetagem intermediária para os equipamentos do fabricante *Juniper Networks*, razão pela qual esse limite superior foi escolhido para as simulações.

Nessas simulações, foi considerado que cada conexão sempre gera pelo menos dois bilhetes: um de início e outro de fim de conexão; assim, considerando as 4.780.658 conexões avaliadas e a geração de bilhetes intermediários desabilitada (intervalo de bilhetagem intermediária infinito), a menor quantidade de bilhetes produzidos pelas conexões em análise é 9.561.316 bilhetes.

A Tabela 5.16 apresenta alguns dos valores obtidos nas simulações, com ênfase para a linha relativa a 245 minutos, que corresponde a um possível valor a ser adotado para o intervalo de geração de bilhetes intermediários, de acordo com o critério proposto na seção 4.2.3. Considerando que a análise foi conduzida sobre uma amostra de bilhetes recebidos em um dia, cabe destacar que os valores da coluna "quantidade estimada de bilhetes" são valores diários. O gráfico da Figura 5.15 sintetiza o resultado das simulações, apresentando o percentual de acréscimo de bilhetes para os diferentes valores de intervalo de bilhetagem intermediária; o ponto em destaque corresponde ao resultado obtido para o valor de intervalo de 245 minutos.

Assim, considerando a amostra utilizada para o estudo como válida, observa-se que, com a adoção do valor 245 minutos, ocorrerá um acréscimo da ordem de 40% nos bilhetes recebidos, para o qual os servidores de bilhetagem deverão estar adequadamente dimensionados.

Para realizar o cálculo do adicional de carga AAA no sistema, é conveniente considerar a situação dita "de pior caso", que é a que ocorrerá no horário de pico. Podemos estabelecer qual é o horário de pico a partir avaliação da quantidade de bilhetes recebida por hora ao longo de um dia. A Tabela 5.18 possui a informação da quantidade de bilhetes encontrados por arquivo para a amostra utilizada neste experimento. Cada arquivo contém os bilhetes recebidos no intervalo de uma hora, o que leva à conclusão que a faixa horária de maior movimento é a correspondente à linha 18 da tabela.

Nesse arquivo foram encontrados 633.675 bilhetes, o que equivale à pouco mais de 176 requisições por segundo, considerando uma distribuição homogênea dos bilhetes ao longo do tempo. Aplicando o percentual de acréscimo de 40% sobre a carga AAA calculada para o horário de pico, chega-se a conclusão que o conjunto de servidores de bilhetagem deverá ter a capacidade de processar, no mínimo, cerca de 250 requisições de bilhetagem por segundo para absorver a carga decorrente da ativação da bilhetagem intermediária com um intervalo de 245 minutos.

Também deverão ser avaliados os aspectos de dimensionamento inerentes ao processamento e armazenamento desses bilhetes pelos sistemas de mediação e de faturamento antes da ativação da bilhetagem intermediária, através de um estudo para verificar os benefícios de tal ativação frente aos custos envolvidos.

É importante ressaltar que a análise realizada não considerou a situação de acréscimo de acessos na rede; tal situação pode ser adicionada ao processo de análise através da aplicação de um fator multiplicativo correspondente ao percentual de crescimento da rede.

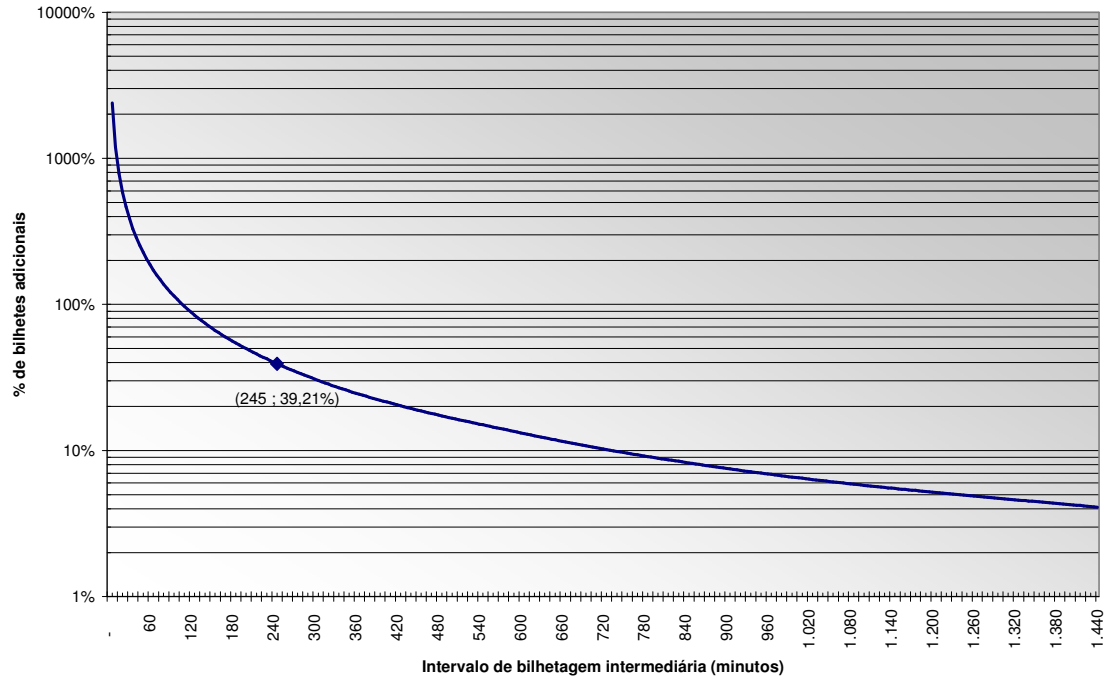

Figura 5.15: Percentual de bilhetes adicionais para diferentes intervalos

Tabela 5.16: Alguns resultados das simulações de bilhetagem intermediária

Intervalo em minutos	Quantidade estimada de bilhetes	% acréscimo de bilhetes	Intervalo em minutos	Quantidade estimada de bilhetes	% acréscimo de bilhetes
5	238.819.053	2397,76%	480	11.233.729	17,49%
10	123.279.882	1189,36%	540	11.011.082	15,16%
15	84.887.499	787,82%	600	10.825.031	13,22%
20	65.696.007	587,10%	660	10.668.882	11,58%
25	54.201.722	466,89%	720	10.541.122	10,25%
30	46.547.967	386,84%	780	10.439.251	9,18%
35	41.076.638	329,61%	840	10.354.867	8,30%
40	36.982.032	286,79%	900	10.282.561	7,54%
45	33.822.426	253,74%	960	10.221.868	6,91%
50	31.260.987	226,95%	1.020	10.170.875	6,38%
55	29.194.596	205,34%	1.080	10.127.530	5,92%
60	27.453.388	187,13%	1.140	10.090.167	5,53%
120	18.004.665	88,31%	1.200	10.056.884	5,18%
240	13.400.456	40,15%	1.260	10.028.109	4,88%
245	13.310.151	39,21%	1.320	10.001.596	4,60%
300	12.509.537	30,83%	1.380	9.977.444	4,35%
360	11.920.274	24,67%	1.440	9.951.705	4,08%
420	11.524.570	20,53%	∞	9.561.316	0,00%

5.4.3 - Determinação do tamanho médio do bilhete

A apresentação dos resultados do experimento foi dividida em duas tabelas, com a finalidade de facilitar a análise. A Tabela 5.17 apresenta, para cada um dos 24 arquivos processados, o tamanho do arquivo e a soma dos tamanhos de todos os bilhetes identificados no arquivo (Tamanho Total). Exibe também a soma dos tamanhos dos bilhetes de início de conexão (Tamanho Início), a soma dos tamanhos dos bilhetes de final de conexão (Tamanho Final) e a soma dos tamanhos dos bilhetes intermediários (Tamanho Intermediário) que foram encontrados em cada arquivo. Todos os valores de tamanho nesta seção estão apresentados em *bytes*.

Nas últimas duas linhas da Tabela 5.17 são mostrados, respectivamente, os valores equivalentes à soma dos valores de cada coluna e o percentual de cada uma frente aos valores totais. Ao encontrar o mesmo valor para os somatórios das colunas “Tamanho Arquivo” e “Tamanho Total” tem-se a certeza de que todos os bilhetes foram analisados.

Tabela 5.17: Espaço ocupado pelos bilhetes analisados

No.	Tamanho Arquivo	Tamanho Total	Tamanho Início	Tamanho Final	Tamanho Intermediário
0	326.943.798	326.943.798	75.600.505	250.596.641	746.652
1	228.422.129	228.422.129	57.911.676	170.125.830	384.623
2	167.988.012	167.988.012	48.967.766	118.689.463	330.783
3	137.763.878	137.763.878	44.579.441	92.922.045	262.392
4	125.807.808	125.807.808	43.565.488	82.074.381	167.939
5	130.867.511	130.867.511	47.833.490	82.806.755	227.266
6	172.599.359	172.599.359	68.810.706	103.321.974	466.679
7	277.750.375	277.750.375	134.721.126	141.966.030	1.063.219
8	398.325.930	398.325.930	201.221.351	195.071.737	2.032.842
9	447.040.062	447.040.062	202.586.639	242.065.321	2.388.102
10	494.191.464	494.191.464	211.197.475	280.409.216	2.584.773
11	547.338.530	547.338.530	218.947.980	325.784.771	2.605.779
12	624.458.335	624.458.335	252.193.169	369.570.005	2.695.161
13	623.375.565	623.375.565	238.347.469	382.643.621	2.384.475
14	578.765.263	578.765.263	214.521.156	362.208.379	2.035.728
15	540.457.589	540.457.589	199.997.219	338.566.085	1.894.285
16	554.009.180	554.009.180	204.754.913	347.226.280	2.027.987
17	630.092.764	630.092.764	222.752.494	405.053.277	2.286.993
18	711.058.182	711.058.182	252.832.944	455.424.478	2.800.760
19	656.654.636	656.654.636	243.454.971	410.669.999	2.529.666
20	589.863.957	589.863.957	216.334.283	371.248.318	2.281.356
21	548.057.402	548.057.402	187.005.647	358.987.352	2.064.403
22	505.260.190	505.260.190	155.342.882	347.967.614	1.949.694
23	451.511.489	451.511.489	121.867.941	328.146.605	1.496.943
Total:	10.468.603.408	10.468.603.408	3.865.348.731	6.563.546.177	39.708.500
%	100%	100%	36,92%	62,70%	0,38%

A presença de bilhetes intermediários não era esperada, mas como essa presença não afeta a análise em curso, sua origem não foi objeto de investigação. Por não ter sido feito um exame quanto ao seu conteúdo, os valores de tamanho apresentados para os bilhetes intermediários não devem ser tomados como válidos; foram apresentados apenas para fins de verificação de consistência dos demais resultados obtidos neste experimento.

Na Tabela 5.18, para cada arquivo analisado foi destacada a quantidade de bilhetes total, de início e fim de conexão, bem como a quantidade de bilhetes intermediários encontrada. Nas três últimas colunas são expostas as médias calculadas para os tamanhos dos bilhetes de início de conexão, de fim de conexão e também para os bilhetes intermediários encontrados. Nas últimas duas linhas apresenta-se os totais obtidos para as quatro primeiras colunas e o valor médio para as três últimas; os valores médios foram arredondados para o valor inteiro mais próximo.

Lembrando que os bilhetes analisados correspondem aos bilhetes recebidos em um intervalo de 24 horas, percebe-se, pelos valores totais e percentuais calculados, que a taxa de admissão de conexões na rede é da mesma ordem de grandeza que a taxa de encerramento de conexões. Esse comportamento está dentro do esperado para a amostra de conexões utilizada, na qual 97,5% das conexões duraram menos de 24 horas, conforme apresentado na seção 5.4.2.

De posse dos valores médios apresentados na Tabela 5.18 para os tamanhos de cada tipo de bilhete, é possível estimar a quantidade de espaço em disco que seria ocupada na adoção do valor 245 minutos para o intervalo de bilhetagem intermediária, o que é feito com o auxílio da Tabela 5.19. Para realizar a estimativa, adota-se, para o do bilhete intermediário, o mesmo tamanho médio do bilhete de fim de conexão e, para obter a quantidade de bilhetes deste tipo, subtrai-se do valor total de bilhetes obtido na Tabela 5.16 para o intervalo 245 minutos a quantidade de bilhetes de início e de fim de conexão utilizada nos cálculos da seção 5.4.2.

Tabela 5.18: Quantidade e tamanho médio de bilhetes por tipo

No.	Quantidade Total	Quantidade Início	Quantidade Final	Quantidade Intermediário	Tam. Médio Início	Tam. Médio Final	Tam. Médio Intermediário
0	271.353	90.180	181.173	599	838	1.383	1.247
1	192.368	68.997	123.371	308	839	1.379	1.249
2	144.715	58.296	86.419	265	840	1.373	1.248
3	121.012	53.063	67.949	211	840	1.368	1.244
4	112.078	51.837	60.241	135	840	1.362	1.244
5	117.667	56.915	60.752	183	840	1.363	1.242
6	157.553	82.048	75.505	376	839	1.368	1.241
7	265.209	161.096	104.113	858	836	1.364	1.239
8	383.902	240.509	143.393	1.639	837	1.360	1.240
9	419.411	242.107	177.304	1.922	837	1.365	1.243
10	457.920	252.689	205.231	2.081	836	1.366	1.242
11	500.266	262.424	237.842	2.099	834	1.370	1.241
12	572.974	302.749	270.225	2.171	833	1.368	1.241
13	565.595	286.262	279.333	1.920	833	1.370	1.242
14	522.514	257.908	264.606	1.641	832	1.369	1.241
15	486.758	239.652	247.106	1.520	835	1.370	1.246
16	498.277	245.148	253.129	1.626	835	1.372	1.247
17	561.347	266.489	294.858	1.836	836	1.374	1.246
18	633.675	302.266	331.409	2.248	836	1.374	1.246
19	590.353	291.598	298.755	2.030	835	1.375	1.246
20	528.820	259.166	269.654	1.827	835	1.377	1.249
21	484.039	223.935	260.104	1.653	835	1.380	1.249
22	436.876	185.422	251.454	1.562	838	1.384	1.248
23	381.806	145.074	236.732	1.199	840	1.386	1.248
Total:	9.406.488	4.625.830	4.780.658	31.909	837	1.372	1.245
%		49,18%	50,82%	0,34%			

Obtém-se, assim, a estimativa de ocupação de espaço em disco de 15,7 *Gigabytes* por dia na hipótese da adoção do valor 245 minutos para o intervalo de bilhetagem intermediária, enquanto o comportamento de conexão analisado for repetitivo ao longo do tempo. É importante ressaltar que essa estimativa não levou em conta o acréscimo de acessos na rede, situação que pode ser facilmente considerada, como recomendado anteriormente, através da aplicação de um fator multiplicativo.

Tabela 5.19: Estimativa de ocupação de espaço de armazenamento

Tipo de bilhete	Quantidade	Tamanho médio	Tamanho Total
Início de conexão	4.780.658	837	4.001.410.746
Fim de conexão	4.780.658	1372	6.559.062.776
Intermediário	3.748.835	1372	5.143.401.620
Total	13.310.151	-	15.703.875.142

5.4.4 - Avaliação dos benefícios da implementação de Lista Negra dinâmica

A avaliação dos benefícios da implantação da implantação de Lista Negra dinâmica foi realizada com o auxílio da Figura 5.16 e da Figura 5.17, que são cópias de telas do programa de gerenciamento de um determinado servidor RADIUS da planta da Brasil Telecom durante a ativação do recurso em uma parte do ambiente de produção.

Para a Figura 5.16 e a Figura 5.17 deve-se considerar que a linha azul corresponde a quantidade de requisições de acesso recebidas do NAS ou encaminhadas pelo servidor ao provedor de acesso à Internet, a linha vermelha corresponde à quantidade de respostas de Acesso Rejeitado encaminhadas ao NAS ou recebidas pelo servidor do provedor e a linha verde, por fim, corresponde à quantidade de respostas de Acesso Permitido enviadas ao NAS ou recebidas do provedor, respectivamente.

No entorno da amostra de número 120, a lista negra dinâmica foi habilitada para o servidor. Percebe-se na Figura 5.16, a existência de um período de acomodação no comportamento entre os NAS e Servidor RADIUS, representado por uma variação nas quantidades de requisições recebidas e respostas fornecidas entre as amostras de números 120 e 150, aproximadamente, que equivale a um intervalo de tempo de três minutos.

Na Figura 5.17, nota-se uma acentuada queda nas requisições que são encaminhadas aos provedores de acesso à Internet, de 130 para apenas 30 requisições por segundo, aproximadamente, o que representa uma queda de quase 77% na quantidade de requisições encaminhadas aos provedores. Como resultado imediato, ocorre uma redução no tráfego gerado pelo servidor RADIUS e uma diminuição no tempo de processamento das requisições, visto que apenas as consultas que não possuem entrada no *cache* são submetidas aos provedores.

Essa diminuição no tempo de processamento das requisições pode ser vista de outra maneira: apesar de não poder ser quantificada de forma exata, aumenta-se a capacidade de processamento disponível no servidor RADIUS da operadora. E, como a requisição cuja resposta é baseada na informação em *cache* não é enviada aos servidores de autenticação dos provedores, isso também representa uma redução no consumo de recursos nos sistemas dos provedores. Percebeu-se uma redução de mais de 25% na quantidade de requisições enviadas aos provedores que ficaram sem resposta

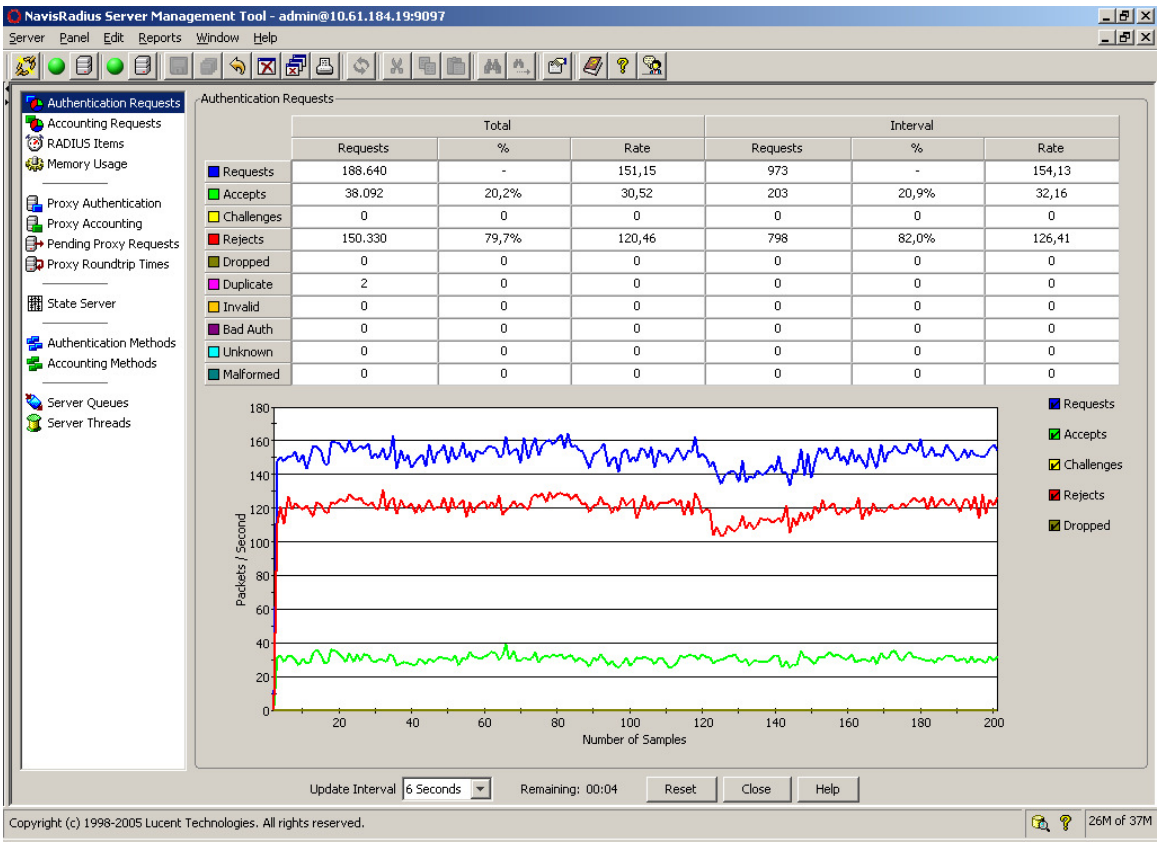

Figura 5.16: Requisições de autenticação recebidas por um servidor RADIUS, durante a implementação do recurso lista negra dinâmica.

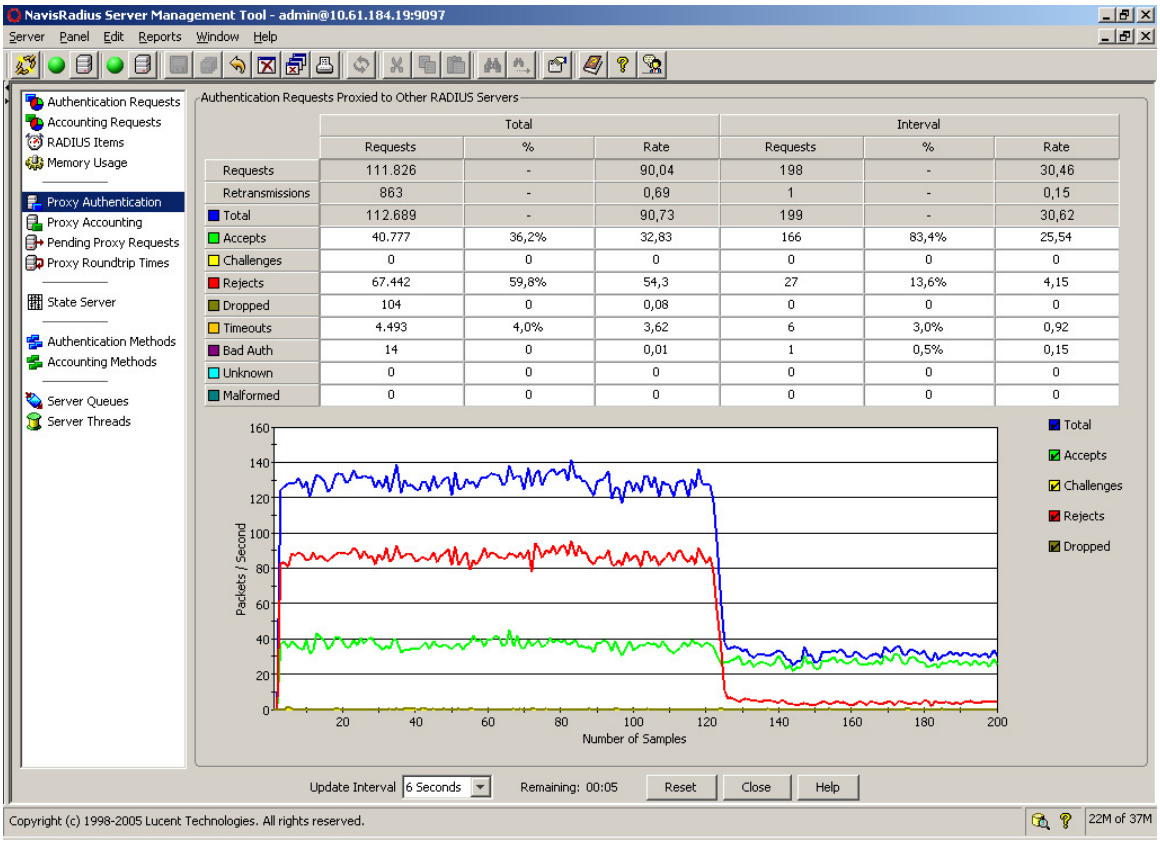

Figura 5.17: Redução na quantidade de requisições de autenticação encaminhadas aos provedores de serviço Internet, decorrente de implementação de lista negra dinâmica.

5.4.5 - Avaliação dos benefícios da implantação da autenticação e da segregação de usuários inválidos

A avaliação dos benefícios da implantação da autenticação e da segregação de usuários inválidos foi realizada com o auxílio da Figura 5.18, que é a cópia da tela do programa de gerenciamento de determinado servidor RADIUS da planta da Brasil Telecom durante a ativação do recurso em uma parte do ambiente de produção.

O gráfico presente na Figura 5.18 exibe a quantidade de Requisições de Acesso (linha azul), a de respostas Acesso Permitido (linha verde) e a de respostas Acesso Rejeitado (linha vermelha) que foram tratadas, por segundo, por um servidor de autenticação em um determinado período de tempo. Esse período corresponde a 50 minutos (200 amostras, uma a cada 15 segundos), intervalo de tempo no qual foi ativada e acompanhada a autenticação e a segregação do usuário "-f" em 20 elementos NAS dos fabricantes *Cisco* e *Juniper*.

Desprezado o *overshoot* inicial, que é decorrente da acomodação dos contadores de requisições após a reativação do *software* RADIUS, pode-se estimar que a quantidade de requisições recebidas esteja próxima a 170 requisições por segundo, das quais cerca de 35 são respondidas com a mensagem Acesso Permitido e as demais, aproximadamente 135, com a mensagem Acesso Rejeitado.

A partir da amostra de número 20 foi iniciado o processo de configuração do recurso de autenticação e segregação para o usuário –f, o qual foi encerrado no instante correspondente a amostra de número 80. Percebe-se que, durante o processo de configuração, a quantidade de requisições de autenticação que é recebida pelo servidor RADIUS é gradualmente reduzida, mantendo-se, contudo, a mesma taxa de admissão de clientes na rede (mensagens Acesso Permitido emitidas). Isso sugere que tal redução deve-se particularmente à configuração realizada e não à variação na quantidade de clientes procurando acesso à rede.

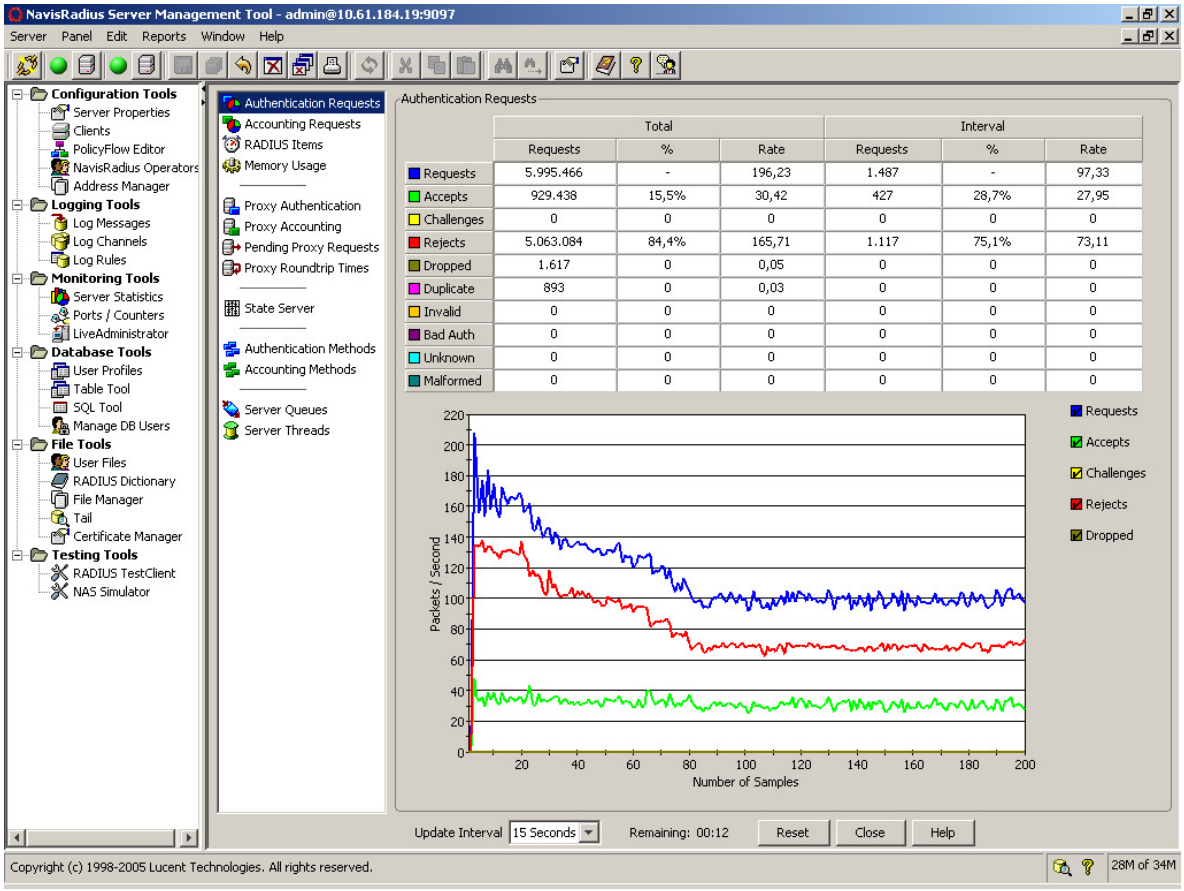

Figura 5.18: Redução da quantidade de requisições de autenticação decorrente de implementação da autenticação e da segregação de usuários inválidos

Da amostra 80 até o final do período representado não ocorre nenhuma outra grande alteração no volume de requisições recebidas pelo servidor, que permaneceu em torno de 100 por segundo, ou nos tipos de resposta emitidas pelo servidor RADIUS.

A partir dessas informações pode-se concluir que aproximadamente 41% das requisições de autenticação recebidas pelo servidor analisado eram oriundas de tentativas de autenticação do usuário inválido "-f" e que, com a adoção da técnica de autenticação e segregação de usuários inválidos, a carga apresentada pelos NAS a esse servidor foi substancialmente reduzida.

5.4.6 - Avaliação dos benefícios de utilização de *PPPoE Throttling*

A avaliação dos benefícios da implantação do recurso *PPPoE Throttling* foi realizada com o auxílio da Figura 5.19, que é a cópia da tela do programa de gerenciamento de determinado servidor RADIUS da planta da Brasil Telecom durante a avaliação realizada do recurso no ambiente de produção.

O gráfico presente na Figura 5.19 representa a quantidade por segundo de Requisições de Acesso (linha azul), de respostas Acesso Permitido (linha verde) e de mensagens Acesso Rejeitado (linha vermelha) tratadas pelo servidor de autenticação em um determinado período de tempo. Esse período corresponde a 50 minutos, intervalo de tempo no qual foi realizada a implementação do comando em 19 NAS do fabricante *Cisco*.

No início do período, a quantidade de Requisições de Acesso tem picos de cerca de 180 requisições por segundo. À medida que o comando foi implementado nos equipamentos envolvidos no teste, a quantidade de requisições foi sendo reduzida. Em alguns equipamentos, os com maior quantidade de clientes PPPoE, a aplicação do comando resultou em queda mais significativa da quantidade de requisições por unidade de tempo.

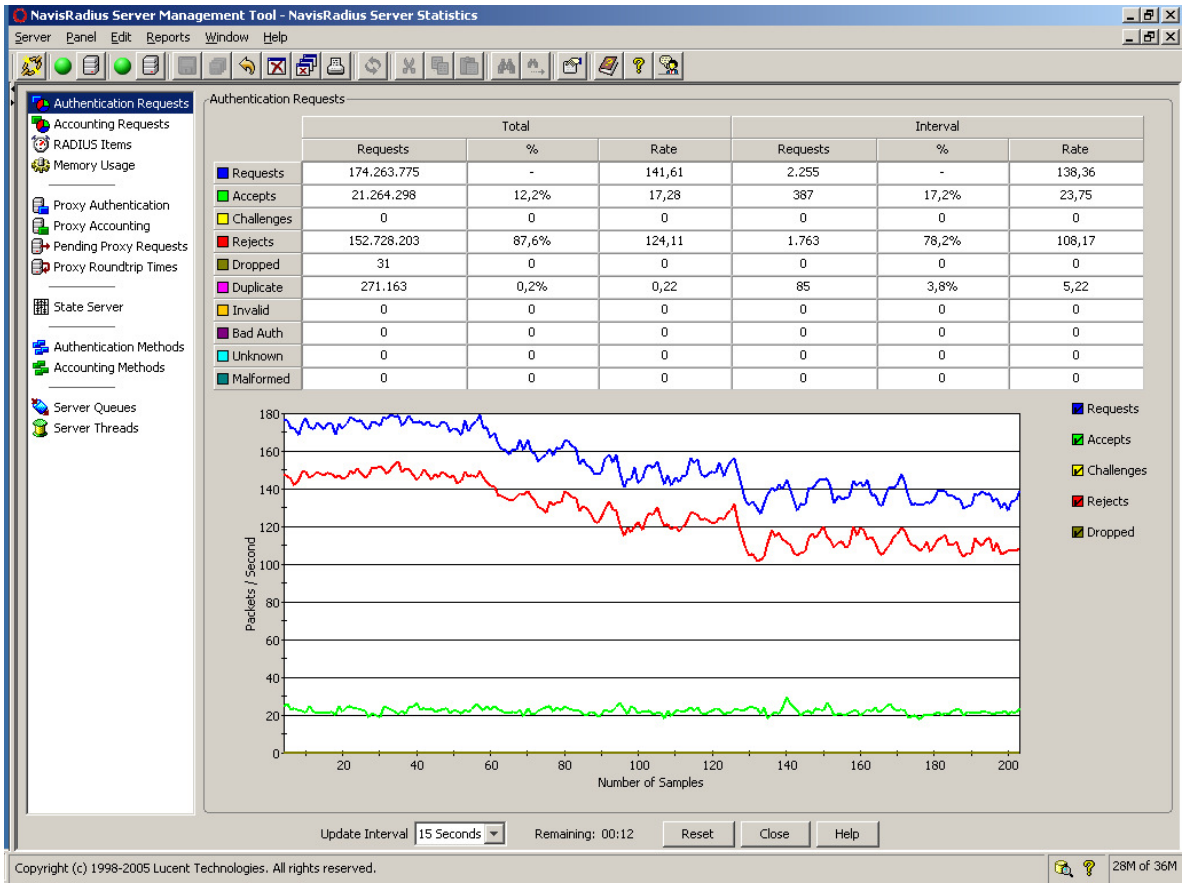

Figura 5.19: Redução na quantidade de requisições de autenticação decorrente de implementação de PPPoE Throttling

Ao final da implementação os picos de requisições chegaram a 140 requisições por segundo, uma diferença de 40 requisições por unidade de tempo, ou, de outra forma, aproximadamente 22% menos requisições do que no início da avaliação. Pela análise gráfica também se verifica que, durante o período avaliado, a quantidade de requisições que recebeu resposta Acesso Permitido permanece razoavelmente constante, indicando que a queda nas requisições de autenticação deveu-se principalmente à implementação do comando e não a uma variação significativa da taxa de usuários procurando obter acesso à rede.

5.4.7 - Verificação de configuração da utilização de *gigawords*

A verificação demonstrou que todos os NAS *Cisco* 10008 presentes na planta da Brasil Telecom estão com a geração dos atributos *gigawords* desativada, enquanto todos os NAS *Juniper* ERX estão com o recurso ativado.

A ativação do recurso no NAS *Cisco* 10008 necessita, após a implementação do comando *aaa accounting gigawords* em sua configuração, a reinicialização do equipamento, de forma que tal configuração apenas poderá ser realizada em uma manutenção programada e com indisponibilidade do serviço durante o tempo necessário para a completa inicialização do equipamento.

5.4.8 - Adição de informações complementares nos bilhetes

O experimento consistiu em programar os servidores de autenticação da Brasil Telecom para, nas mensagens RADIUS de Acesso Permitido, adicionar o atributo *Class* com as informações da Tabela 5.20, que estão disponíveis apenas durante o processo de autenticação e autorização RADIUS, e verificar a sua chegada sem alterações no processo de bilhetagem. Cabe ressaltar que o significado das informações da Tabela 5.20 não é, para este experimento, importante; de fato, algumas dessas informações sequer são válidas ou possuem aplicação imediata, mas foram inseridas para demonstrar o potencial de utilização do recurso.

Tabela 5.20: Informações adicionadas ao atributo *Class*

Descrição
Identificador do servidor RADIUS que realizou a autenticação
Identificador da filial da Brasil Telecom onde o NAS está instalado
Resultado do processo de autenticação
Identificador do grupo de autorização utilizado ao estabelecer o acesso
Identificador para controle de acessos simultâneos
Identificador de pacote de serviços contratado pelo cliente

Adicionalmente, os servidores RADIUS de bilhetagem foram programados para recuperar o atributo *Class*, separar as informações e inseri-las em atributos VSA com o identificador (PEN ou *vendor-id*) atribuído à Brasil Telecom pelo IANA.

A Figura 5.20 mostra a tela do *software NavisRadius Server Management Tool* através do qual o PEN da Brasil Telecom foi inserido no dicionário RADIUS (veja a penúltima linha da coluna "*Vendors"*). A Figura 5.21 apresenta o registro dos atributos no dicionário do servidor RADIUS; a associação entre cada atributo e a correspondente informação pode ser vista na Tabela 5.21.

Tabela 5.21: Atributos RADIUS inseridos no dicionário.

Nome do atributo	Descrição
Brt-AuthServer	Identificador do servidor RADIUS que realizou a autenticação
Brt-NasArea	Identificador da filial da Brasil Telecom onde o NAS está instalado
Brt-AuthResult	Resultado do processo de autenticação
Brt-Service-Id	Identificador do grupo de autorização utilizado ao estabelecer o acesso
Brt-Hauss	Identificador para controle de acessos simultâneos
Brt-PackageId	Identificador de pacote de serviços contratado pelo cliente

A implementação foi realizada com sucesso e, na Figura 5.22, pode ser visto um bilhete contendo os atributos *Class* e os atributos internos à Brasil Telecom; tal como em outras figuras similares, nesse bilhete atributos não relacionados com o experimento foram removidos para facilitar a compreensão. O atributo *Brt-PackageId* não foi utilizado no experimento, apesar de constar no atributo *Class*.

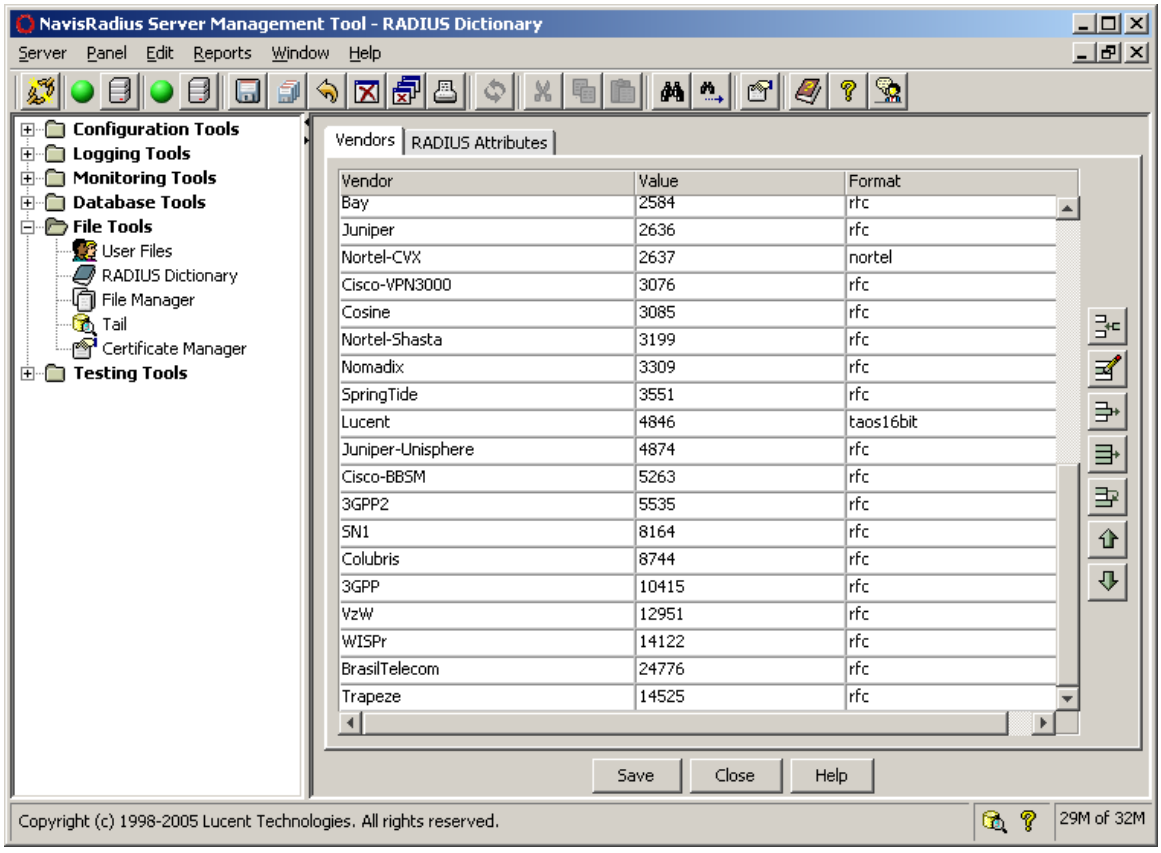

Figura 5.20: Dicionário RADIUS, apresentando o registro do PEN da Brasil Telecom

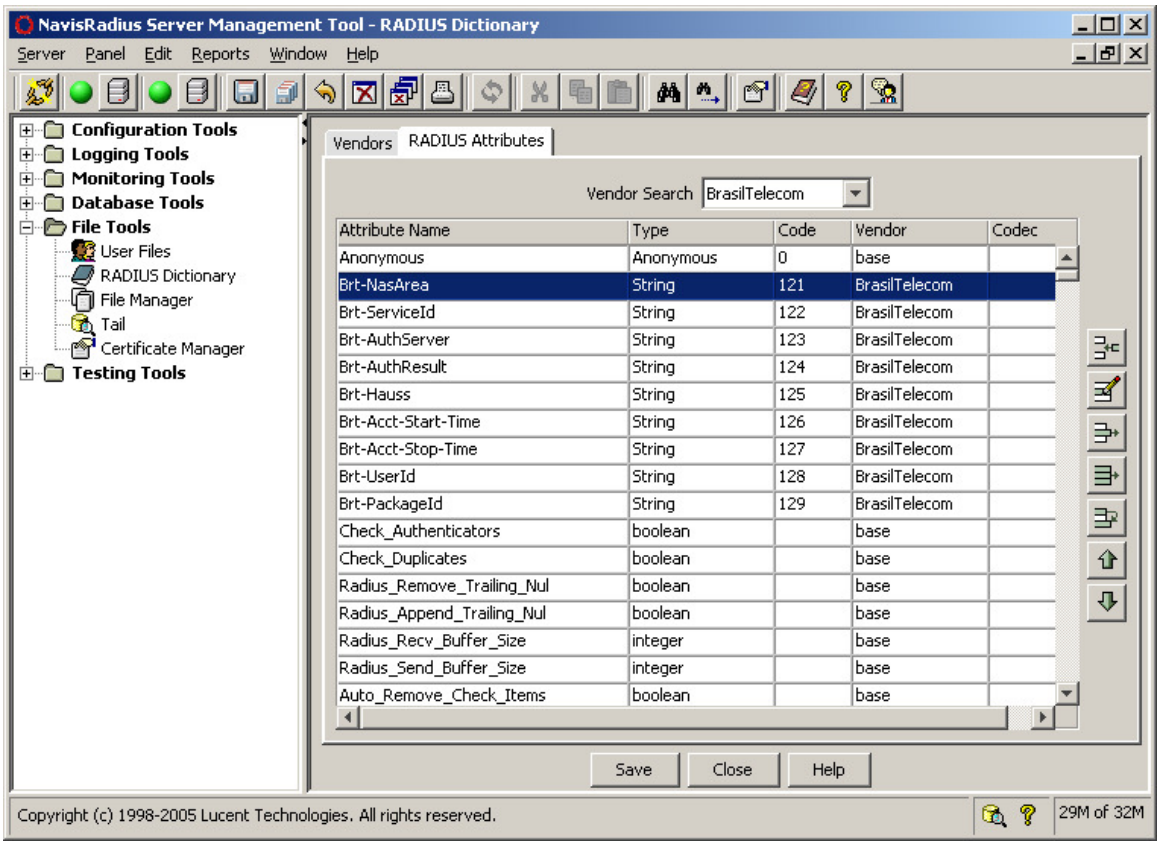

Figura 5.21: Dicionário RADIUS, apresentando os atributos registrados sob o PEN da Brasil Telecom

```
Tue Jun 17 17:33:39 GMT-03:00 2008
        Framed-Protocol = PPP
        Framed-IP-Address = 201.24.15.229
        User-Name = "agski@wireshark.com.br"
        Acct-Status-Type = Stop
        Class = "CTANRAM01_DF_PO_DEF_CLF_0"
        Brt-AuthServer = "CTANRAM01"
        Brt-NasArea = "DF"
        Brt-AuthResult = "PO"
        Brt-ServiceId = "DEF"
        Brt-Hauss = "CLF"
        Brt-Acct-Start-Time = "2008/06/17 16:33:39"
        Brt-Acct-Stop-Time = "2008/06/17 17:33:39"
```

Figura 5.22: Bilhete apresentando atributos internos à Brasil Telecom

Diante dos bons resultados obtidos neste experimento, não só esses atributos foram adicionados ao sistema em produção como também outros foram criados para outras finalidades. De volta à Figura 5.21, pode-se observar três atributos que não constam na Tabela 5.21; são eles: *Brt-UserId*, *BrT-Acct-Start-Time* e *BrT-Stop-Time*. Esses novos atributos não estão relacionados com o conteúdo do atributo *Class*, mas são utilizados para apresentar informações adicionais visando a facilitar a análise de bilhetes por outros sistemas e por seres humanos.

O atributo *Brt-UserId* recebe o resultado da concatenação da identificação do cliente com informações de identificação do NAS e é utilizado na integração da plataforma AAA com um sistema de mediação. Os atributos *BrT-Acct-Start-Time* e *BrT-Acct-Stop-Time* indicam o momento de recepção do bilhete de início de conexão e o do bilhete de fim de conexão, respectivamente.

No bilhete de início de conexão, apenas o atributo *BrT-Acct-Start-Time* está presente e o seu valor indica o momento do recebimento do pacote no servidor de bilhetagem. No bilhete de fim de conexão, ambos estão presentes, mas há uma pequena diferença: o atributo *BrT-Acct-Stop-Time* indica o momento no qual o bilhete foi recebido e o atributo *BrT-Acct-Start-Time* é calculado em função do momento de chegada do bilhete menos o tempo de duração da conexão, que é dado pelo atributo *Acct-Session-Time*.

5.4.9 - Conformação de bilhetes

Neste experimento, a função do servidor RADIUS responsável pelo registro do bilhete em arquivo foi precedida de um conjunto de funções para consultar um arquivo de configuração, com base no conteúdo do atributo *NAS-IP-Address*, e recuperar um valor para substituir o do atributo *NAS-Identifier* ou, ainda, adicioná-lo caso não esteja presente na mensagem de Requisição de Bilhetagem.

A Figura 5.23 mostra um bilhete antes da ativação do código e a Figura 5.24 mostra um bilhete após a ativação. Nessas duas figuras, alguns atributos não relacionados com o experimento foram removidos para proporcionar maior clareza, bem como os valores dos campos *User-Name* foram alterados para preservar a privacidade dos clientes. Percebe-se que o bilhete da Figura 5.23 não possui o atributo *NAS-Identifier*, enquanto o da figura Figura 5.24 o inclui. O experimento demonstra, portanto, a existência da capacidade de reescrever as informações presentes nos bilhetes, de forma a gravar os bilhetes recebidos pelos servidores de bilhetagem em um formato pré-definido e independente da plataforma NAS.

```
Sun Jun 22 16:44:00 GMT-03:00 2008
        Framed-Protocol = PPP
        Framed-IP-Address = 201.2.11.176
        User-Name = "user@globo.com"
        Acct-Status-Type = Stop
        Class = "BSANRAS01_DF_OK_DEF_CLF_0"
        NAS-IP-Address = 201.34.54.254
        Brt-ServiceId = "DEF"
        Brt-NasArea = "DF"
        Brt-AuthServer = "CTANRAM01"
        Brt-AuthResult = "OK"
        Brt-Hauss = "CLF"
        Brt-Acct-Start-Time = "2008/06/22 16:22:38"
        Brt-Acct-Stop-Time = "2008/06/22 16:43:39"
```

Figura 5.23: Bilhete de uma conexão recebido antes da ativação do código.

```
Sun Jun 22 16:46:10 GMT-03:00 2008
        Framed-Protocol = PPP
        Framed-IP-Address = 189.72.154.214
        User-Name = "user@terra.com.br"
        Acct-Status-Type = Stop
        Class = "BSANRAS01_DF_OK_DEF_CLF_0"
        NAS-IP-Address = 201.34.54.254
        NAS-Identifier = "BSACE702"
        Brt-ServiceId = "DEF"
        Brt-NasArea = "DF"
        Brt-AuthServer = "CTANRAM01"
        Brt-AuthResult = "OK"
        Brt-Hauss = "CLF"
        Brt-Acct-Start-Time = "2008/06/22 13:25:32"
        Brt-Acct-Stop-Time = "2008/06/22 16:45:47"
```

Figura 5.24: Bilhete de uma conexão recebido depois da ativação do código.

6 - CONSIDERAÇÕES FINAIS

Neste capítulo serão apresentadas as conclusões decorrentes do trabalho de pesquisa realizado, bem como as recomendações e sugestões para trabalhos futuros neste mesmo tema ou em assuntos correlatos.

6.1 - CONCLUSÃO

No capítulo inicial, o elemento motivador da pesquisa foi caracterizado como sendo o interesse de operadoras de telecomunicações em possuir um mecanismo que lhes possibilitasse efetuar a contabilização do uso efetivo de acessos em banda larga que utilizem tecnologia ADSL, porquanto uma vez que tal uso, por acesso, fosse adequadamente evidenciado, a operadora poderia efetuar a cobrança com base nas informações de consumo.

Duas características foram elencadas para tal mecanismo: o consumo seria determinado em função de duas grandezas e deveria poder crescer de forma proporcional ao incremento da quantidade de acessos em banda larga ADSL. As duas grandezas que seriam avaliadas para representar o consumo eram o intervalo de tempo em que um acesso permanecesse logicamente conectado à rede da operadora e a soma da quantidade de *bytes* transferidos nos dois sentidos da comunicação, denominada “volume de dados trafegados”.

Conciliando a necessidade gerada pelo interesse de operadoras de telecomunicações com as características apropriadas ao mecanismo desejado, foram constituídas duas hipóteses: a hipótese principal, na qual foi feita a suposição de que um esquema de geração, transmissão e armazenamento de bilhetes permitiria a contabilização do consumo de acessos em banda larga ADSL e uma conjectura secundária, na qual a solução encontrada possuiria condições de crescer acompanhando o aumento da rede de acesso em banda larga ADSL.

A seguir, no capítulo 2, foi apresentada a fundamentação teórica necessária para caracterizar a rede de acesso em banda larga ADSL para a qual o mecanismo de contabilização de uso foi proposto, mostrando seus elementos essenciais e evidenciando as

suas inter-relações. Nessa mesma oportunidade, foram destacadas formas para a obtenção das informações de utilização de acessos em banda larga, avaliando, para cada uma delas, a viabilidade da sua aplicação para a finalidade pretendida.

Das maneiras de contabilizar o uso, tanto por tempo de conexão quanto por volume de tráfego, uma salientou-se dentre as apresentadas; a que envolvia os processos de autenticação, de autorização e de bilhetagem existentes nas redes de acesso em banda larga ADSL, razão pela qual foi conduzido, no capítulo 3, um estudo conceitual sobre esses processos e seus pontos de contato com a rede em apreço. Ainda no capítulo 3 especial atenção foi destinada ao estudo do protocolo RADIUS, por ser este o protocolo utilizado para as funções de autenticação, de autorização e de bilhetagem em uma rede de acesso em banda larga que utiliza tecnologia ADSL.

No capítulo 4, à luz dos conhecimentos adquiridos no desenvolvimento dos capítulos anteriores, foi proposto o mecanismo de contabilização de uso, utilizando o protocolo RADIUS como peça fundamental. Inicialmente, os processos de autenticação, de autorização e de bilhetagem foram inseridos no contexto de uma rede de acesso ADSL, considerando o cenário brasileiro para o provimento deste tipo de serviço. Após, foram abordados os aspectos relacionados com a segurança e a confiabilidade do processo de bilhetagem. A forma de registro da utilização – o bilhete – foi, então, examinada e os campos específicos para a contabilização de uso – os atributos – foram analisados.

Dando prosseguimento à proposição, foram apresentadas as formas de realizar a avaliação da duração e do volume de tráfego de uma conexão, a partir dos valores constantes nos bilhetes que representam as conexões em banda larga ADSL. Foi destacada também a importância do sincronismo de relógio dos elementos componentes da rede ADSL com a chamada “Hora Legal Brasileira” e sugerido o tratamento a ser dado para a situação na qual a rede de acesso ADSL abrange localidades geográficas que estão em diferentes fusos horários ou sujeitas à ocorrência da mudança de horário conhecida como “horário de verão”.

Com base no funcionamento do protocolo RADIUS em uma rede de acesso em banda larga ADSL, foram apresentadas as considerações a serem adotadas quando da configuração de seus parâmetros básicos, tais como o tempo de espera e a quantidade de retransmissões, e

também para as demais características habituais encontradas nas implementações de tal protocolo, como, por exemplo, a utilização de balanceamento de carga. Outras configurações e técnicas menos evidentes, entretanto não menos importantes, foram descritas em seguida, das quais se destacaram as técnicas "autenticação e segregação de usuários inválidos" e a "lista negra dinâmica", ambas desenvolvidas por este autor.

O modelo básico de um ambiente de autenticação, de autorização e de bilhetagem, proposto na seção 4.3 e apresentado, de forma esquemática, na Figura 4.3, aliada às demais técnicas apresentadas no capítulo 4, permitiram conceber que a solução encontrada possuía a capacidade de acompanhar o crescimento da rede de acesso ADSL da operadora, o que confirmou a hipótese secundária apresentada no início do trabalho. Ao final do capítulo 4 foi apresentada a síntese da proposição, concatenando todos os aspectos expostos ao longo desse capítulo.

Com a finalidade de consubstanciar a proposta descrita no capítulo 4 foram elaborados e executados alguns experimentos, que tiveram suas descrições e resultados aduzidos no capítulo 5.

O principal experimento realizado foi o que versa sobre a determinação do tempo de conexão e do volume de dados trafegados. Nesse experimento, a forma pela qual os equipamentos responsáveis pela conexão dos acessos ADSL contabilizam a utilização de tais acessos foi descoberta, analisada e descrita. A cabal compreensão da forma de contabilização dos recursos utilizados, aliada à proposição constante no capítulo 4, confirmou a hipótese principal deste trabalho: um esquema de geração, transmissão e armazenamento de bilhetes permite a contabilização do consumo de acessos em banda larga ADSL.

É apropriado destacar que a utilização do esquema de bilhetes proposto habilita a operadora a realizar a contabilização de quaisquer acessos em banda larga ADSL que utilizem a forma de conexão e tenham o funcionamento conforme descrito nos capítulos 2 e 3. Dessa forma, um serviço destinado ao mercado empresarial que possua implementação similar ao serviço residencial objeto deste trabalho pode, perfeitamente, ter seu uso contabilizado usando esse mesmo mecanismo.

Dentre as diversas dificuldades enfrentadas na elaboração e na condução do experimento, destacou-se a pouca disponibilidade de documentação dos fabricantes dos equipamentos acerca do funcionamento dos contadores de utilização e da formação dos valores apresentados nos bilhetes de conexão. As consultas sobre o assunto, encaminhadas aos representantes dos fabricantes envolvidos, não receberam respostas esclarecedoras.

Neste mesmo experimento, percebeu-se a necessidade da aferição da maneira de contabilização de uso, não apenas para diferentes equipamentos, mas para cada diferente versão de um mesmo sistema operacional que se pretendesse instalar no ambiente de produção. Durante a execução do experimento, para um determinado tipo de equipamento e em duas oportunidades, foi verificada a inconsistência entre os valores apontados nos bilhetes e os correspondentes volumes de tráfego efetivamente cursados. Em ambos os casos os equipamentos em avaliação utilizavam versões de sistema operacional mais antigas.

Cabe ressaltar que a técnica elaborada para a determinação da forma de contabilização dos equipamentos avaliados no experimento, que utiliza recursos comuns e programas de domínio público, pode ser aplicada a outros equipamentos de mesma finalidade e função.

Notou-se que existe uma dissimilitude entre as formas de contabilização do volume de tráfego dos equipamentos avaliados, relacionada com um tipo específico de fluxo de mensagens de controle da conexão PPP. Entende-se, todavia, que ela não mereça tratamento especial em virtude de tal tráfego de controle não ser significativo, em especial quando comparado com o tráfego principal da conexão.

Os resultados da aplicação das técnicas desenvolvidas em outros dois experimentos – o de determinação do intervalo para a geração de bilhetagem intermediária e o de determinação do tamanho médio do bilhete –, servem para fundamentar decisões relativas ao dimensionamento de servidores de bilhetagem. Ambos os experimentos foram realizados com a utilização de dados reais de uma rede de acesso ADSL e seus resultados também podem ser utilizados para o dimensionamento de sistemas que sucedem o sistema de bilhetagem, tais como o de mediação e o de faturamento.

No tema “determinação do intervalo de bilhetagem intermediária”, é interessante notar que existe um certo senso comum de que a escolha de um intervalo de 15 minutos seria

apropriada para, em caso de perda do bilhete de fim de conexão, "não perder muito". Este valor foi o escolhido em 2004 – o critério utilizado é desconhecido – para o intervalo de geração de bilhetagem intermediária da implementação do produto Turbo Lite. Se tal configuração ainda estivesse ativa hoje, para todos os acessos e considerado o perfil de duração de conexão amostrado, ela provocaria a geração de 787,82% mais bilhetes do que o número atual. Comprova-se que, nesse assunto, "senso comum" não necessariamente significa "bom senso"; é preciso realizar uma análise criteriosa da situação e não aceitar valores de forma acrítica.

Como resultado complementar, os dois experimentos demonstraram a necessidade de tomar cuidado com as operações matemáticas que são realizadas com os dados originados nos bilhetes; com a quantidade de bilhetes de um só dia, cerca de 9,5 milhões, já foi necessário utilizar, nos programas desenvolvidos, técnicas de adição utilizando variáveis do tipo inteiro com tamanho arbitrário.

É oportuno destacar que os programas desenvolvidos para os dois experimentos podem ser utilizados para promover outras avaliações, como, por exemplo, apresentar o volume de tráfego total para um determinado provedor ou avaliar conexões de curta duração, mediante a adição de outros critérios de seleção baseados nos valores de atributos e outras ações a serem realizadas com o conteúdo dos bilhetes.

Outros experimentos tiveram por objetivo verificar os benefícios na adoção de duas técnicas propostas pelo autor para melhorar o desempenho dos sistemas de autenticação, de autorização e de bilhetagem, a saber, "lista negra dinâmica" e "autenticação e segregação de usuários inválidos".

A implantação da técnica denominada "lista negra dinâmica" teve como resultado uma redução de cerca de 77% nas consultas RADIUS de autenticação direcionadas aos provedores. Como conseqüência dessa redução, verificou-se também uma queda da ordem de 25% nas consultas RADIUS que não recebem resposta do provedor; atribui-se esta melhora na qualidade das respostas dos provedores ao desafogo proporcionado aos seus servidores e ao da operadora pela adoção da técnica. Dado o resultado positivo, a técnica foi incorporada, em caráter permanente, ao código de produção dos servidores RADIUS da operadora.

O experimento que versa sobre a "autenticação e segregação de usuários inválidos" demonstrou a existência de benefícios na implementação dessa técnica. No experimento realizado, a sua adoção provocou a expressiva redução de 41% nas requisições de autenticação recebidas pelo servidor, situação que, vista de outro modo, produziu uma ampliação virtual de capacidade do servidor na ordem de 70%. Essa técnica também foi incorporada ao código de produção dos servidores RADIUS da operadora.

O recurso *PPPoE Throttling*, objeto de um dos experimentos, também trouxe ganhos ao sistema de autenticação, de autorização e de bilhetagem. Durante a realização dos testes com o recurso, observou-se uma redução de aproximadamente 22% na quantidade de requisições de acesso recebida pelo servidor RADIUS. Percebido o benefício, sem a ocorrência de efeitos colaterais, a configuração proposta neste trabalho foi, então, adicionada à configuração padrão daquele tipo de equipamento.

O experimento cujo objetivo era verificar a adequação da configuração dos equipamentos para a geração dos atributos denominados *gigawords* ressaltou a necessidade de ajustar a configuração de alguns equipamentos previamente à adoção do mecanismo proposto. A análise dessa configuração específica não foi escolhida ao acaso: trata-se de uma configuração que, para tornar-se ativa em um dos equipamentos analisados, exige reinicialização de tal equipamento. Cabe observar que esse tipo de procedimento, para ser efetuado, segue um complexo ritual para ser efetuado em função da quantidade de clientes envolvidos.

Encerrando o capítulo 5, os experimentos relacionados com a adição de informações complementares e a conformação de bilhetes demonstraram a existência da possibilidade de adição, nos bilhetes, de informações que estão disponíveis apenas no processo de autenticação, bem como a capacidade de modificar a forma de apresentação de informações que estejam presentes nas requisições de bilhetagem. Destaca-se que os códigos utilizados nos testes foram, mediante pequenas alterações, anexados ao sistema RADIUS de produção da operadora; as informações complementares têm sido largamente utilizadas nos processos de solução de problemas de conexão e também para o atendimento de solicitações judiciais de identificação de usuários.

Conclui-se, por conseguinte, que o mecanismo apresentado constitui uma resposta satisfatória para o desejo, de algumas operadoras de telecomunicações, de possuir meios de efetuar a cobrança de serviços baseados em uma rede de acesso em banda larga ADSL, tendo em conta o tempo de utilização de uma conexão e a quantidade de *bytes* transferidos durante tal conexão. Como resultado essencial, o emprego do mecanismo e das técnicas desenvolvidas nesta dissertação torna viável a criação de serviços de acesso em banda larga ADSL, cuja cobrança pelo uso pode ser efetivada com transparência e retidão.

6.2 - SUGESTÕES PARA TRABALHOS FUTUROS

Uma elaborada análise de todos os dados disponibilizados pelos equipamentos de agregação de acessos ADSL nos bilhetes de conexão não foi realizada em virtude das limitações impostas pelo escopo deste trabalho. Ficou evidente, contudo, para este autor, que outras informações relacionadas ao serviço ADSL e a qualidade da sua prestação podem ser extraídas ou derivadas do processamento de tais dados. Uma vez que exista interesse de operadoras de telecomunicação no assunto, aparenta ser promissora a realização de uma análise objetivando a construção de um sistema de informações operacionais e gerenciais sobre o serviço de acesso em banda larga ADSL, tendo os bilhetes de conexão como fonte primária de dados.

Uma preocupação inerente a qualquer sistema que trabalhe com registros de uso de serviços é que esses registros cheguem íntegros ao ponto de coleta e de processamento. Com o uso do protocolo RADIUS não é diferente. Assim, um assunto que pode ser explorado de forma bastante aprofundada, apesar de não ser inédito, é a criação de técnicas ou de mecanismos que possam ser utilizados para montar uma estrutura de transporte confiável para o protocolo RADIUS.

Por fim, este trabalho estabeleceu um mecanismo para a contabilização da utilização de acessos em banda larga ADSL. Tal mecanismo foi baseado na capacidade dos equipamentos NAS para gerar bilhetes com dados de utilização; disponibilizados, estes últimos, nos servidores de bilhetagem, devem ser coletados por um sistema de mediação,

processados e entregues a um sistema de faturamento para a emissão da fatura do serviço. Trata-se, evidentemente, de um serviço do tipo pós-pago.

Um possível desdobramento lógico deste trabalho poderia dar-se através da realização de um estudo e da proposição de um sistema de cobrança de serviços de acesso em banda larga ADSL para a oferta do serviço na modalidade pré-pago. Tal sistema poderia ser resultado da adaptação do mecanismo proposto nesta dissertação para um trabalho em estrutura de *hot billing*. *Hot billing* é conceituado como uma abordagem de autenticação, de autorização e de bilhetagem onde o NAS e o servidor AAA comunicam-se regularmente, seja em uma freqüência pré-determinada, seja quando uma informação relevante surge em qualquer dos dois elementos. Por vezes, *hot billing* é considerado como sendo um sistema habitual de geração de bilhetes, operando, porém, com a emissão de informações de consumo em "quase-tempo-real".

Foi apresentado que o protocolo RADIUS possui suporte à geração de mensagens de controle pelo lado servidor (Requisição de Desconexão e Mudança de Autorização) e que existe, dentro de certos limites, a capacidade de geração de bilhetes intermediários. Esses dois elementos poderiam, porventura, ser suficientes para a composição de um sistema de *hot billing*. Os principais desafios estariam em endereçar adequadamente as dificuldades inerentes à geração, transporte e processamento de grandes volumes de bilhetes e em fazer bom uso dos reduzidos recursos de comunicação entre os servidores RADIUS e seus clientes.

REFERÊNCIAS BIBLIOGRÁFICAS

[AHN2006] AHN, Sehyun. **Hybrid User Interfaces: Design Guidelines and Implementation Examples**. Massachusetts Institute of Technology. 2006.

[ANATEL] ANATEL. **Espaço do Cidadão: Internet**. 2007. Disponível em <http://www.anatel.gov.br/Portal/exibirPortalInternet.do?exibirPortalInternetRodape=true>. Acesso em: 28 jun. 2008.

[BRT2003] BRASIL TELECOM. **Relatório Anual 2003**. Brasil Telecom. 2003. Disponível em <http://www.mzweb.com.br/brasiltelecom/web/arquivos/relatorioanual2003/portugues/capacidade4.htm>. Acesso em: 28 jun. 2008.

[CISCOa] CISCO SYSTEMS. **SNMP: Frequently Asked Questions About IOS Software**. Disponível em <http://www.cisco.com/application/pdf/paws/26010/faq-snmpios.pdf>. Acesso em: 25 jun. 2008.

[CISCOb] _____. **NetFlow Services Solution Guide**. Disponível em <http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/netflsol/nfwhite.pdf>.

[CISCOc] _____. **Introduction to Cisco IOS NetFlow - A Technical Overview**. Disponível em <http://www.cisco.com/application/pdf/en/us/guest/products/ps6601/c1244/cdccont_0900aecd80406232.pdf>.

[DEKOK2008] DEKOK, Alan. **Use of Status-Server Packets in the Remote Authentication Dial In User Service (RADIUS) Protocol** Disponível em <http://www.ietf.org/internet-drafts/draft-ietf-radext-status-server-00.txt>. 17 jun. 2008. Acesso em: 25 jun. 2008.

[DVORAK2008] DVORAK, John C. **Eight Reasons Your Web Connection Should Be Metered**. PC Magazine. Junho de 2008. Disponível em <http://www.pcmag.com/article2/0,2817,2319449,00.asp>. Acesso em: 25 jun. 2008.

[FERREIRA2007] FERREIRA, Aurélio Buarque de Holanda. **Novo Dicionário Aurélio da Língua Portuguesa**. Dicionário eletrônico, Versão 5.11. Editora Positivo. 2007.

[HASSEL2002] HASSEL, Jonathan. **RADIUS**. O'Reilly & Associates. 2002.

[HENZ2008] HENZ, Leandro. **Proposta e implementação de arquitetura para identificação física e lógica de acessos banda larga utilizando tecnologia ADSL.** Publicação PPGENE.DM-057/2008. Departamento Engenharia Elétrica, Universidade de Brasília, Brasília, DF. 2008.

[HILL2001] HILL, Joshua. **An analysis of the RADIUS Authentication Protocol**. InfoGard Laboratories. 2001. Disponível em: <http://www.untruth.org/~josh/security/radius/radius-auth.html> Acesso em: 25 jun. 2008.

[HUNT1994] HUNT, Craig. **TCP/IP Network Administration**. O'Reilly & Associates. 1994.

[IDC2007] IDC Brasil. **Barômetro Cisco da Banda Larga – 1º semestre de 2007**. Disponível em <http://www.cisco.com/web/BR/barometro2007/>. Acesso em: 25 jun. 2008.

[IET2001] INSTITUTION OF ENGINEERING AND TECHNOLOGY. **Potential problem dates for computers from 2000-2100AD**. Janeiro/2001.

[INTERLINK] INTERKINK NETWORKS. **History of the RADIUS Server**. Application note. Disponível em <http://www.interlinknetworks.com/app_notes/History%20of%20RADIUS.pdf>. Acesso em: 08 ago. 2007.

[IPERF] **Iperf - The TCP/UDP Bandwidth Measurement Tool**. Disponível em <http://dast.nlanr.net/Projects/Iperf/>. Acesso em: 26 jun. 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: 28 jun. 2008.

[JPERF] **Jperf: Graphical frontend for IPERF written in Java** Disponível em <http://code.google.com/p/xjperf/downloads/ list>. Acesso em: 26 jun. 2008.

[JUNIPER] 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 jun. 2008.

[KASHIF2004] KASHIF, N., Broos, R. **DSL for Emerging Countries**. Alcatel Telecommunications Review. Alcatel. 2004.

[KAUFMAN1995] KAUFMAN, C.; Perlman, R.; Speciner, M., **Network Security: Private Communications in a Public World**. Prentice Hall. 1995.

[LEI11.662] **Lei Nº 11.662, de 24 abril de 2008**. Diário Oficial da União. 25 de abril de 2008. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11662.htm>. Acesso em: 28 jun. 2008.

[LEWIS1999] LEWIS, Chris. **Cisco TCP/IP: Routing Professional Reference**. McGraw-Hill. 1999. 2a ed.

[LITTLEJOHN2005] LITTLEJOHN, Kevin. **Traffic Counting Methods**. Obsidian. 2005. Disponível em <http://www.obsidian.com.au/jet/manuals/Whitepaper_accounting.pdf>. Acesso em: 25 jun. 2008.

[LIVINGSTON] LIVINGSTON ENTERPRISES. **RADIUS Accounting**. Disponível em <ftp://ftp.portmasters.com/pub/portmasters/radius/Accounting>. Acesso em: 10 dez. 2007.

[MEGATURBO] BRASIL TELECOM. Disponível em <http://www.megaturbo.com/>. Acesso em: 15 set. 2007.

[MIERCOM2004] MIERCON. **Edge Routers: Lab Testing Summary Report**. Outubro/2004.

[NAKHJIRI2005] NAKHJIRI, Madjid; Nakhjiri, Mahsa. **AAA and Network Security for Mobile Access: RADIUS, DIAMETER, EAP, PKI and IP Mobility**. John Wiley & Sons Ltd. 2005.

[PERKINS1997] PERKINS, David; McGinnis, Evan. **Understanding SNMP MIBs**. Prentice Hall. 1997.

[PRIBERAM2007] PRIBERAM. **Dicionário de Língua Portuguesa Online**. Disponível em <http://www.priberam.pt/dlpo/dlpo.aspx>. Acesso em: 15 set. 2007.

[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.

[RFC1134] PERKINS, D. **The Point-to-Point Protocol: A Proposal for Multi-Protocol Transmission of Datagrams Over Point-to-Point Links**. IETF. RFC 1134. Novembro/1989.

[RFC1136] HARES, S.; Katz, D. **Administrative Domains and Routing Domains: A Model for Routing in the Internet**. IETF. RFC 1136. Dezembro/1989.

[RFC1157] CASE, J. et al. **A Simple Network Management Protocol (SNMP)**. IETF. RFC 1157. Maio/1990.

[RFC1305] MILLS, David. **Network Time Protocol (Version 3) Specification, Implementation and Analysis**. IETF. RFC 1305. Março/1992.

[RFC1321] RIVEST, R. **The MD5 Message-Digest Algorithm**. IETF. RFC 1321. Abril/1992.

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

[RFC1334] LLOYD, B.; Simpson, W. **PPP Authentication Protocols**. IETF. RFC 1334. Outubro/1992.

[RFC1661] SIMPSON, W. (Ed.) **The Point-to-Point Protocol (PPP)**. IETF. RFC 1661. Julho/1994.

[RFC1662] SIMPSON, W. (Ed.) **PPP in HDLC-like Framing**. IETF. RFC 1662. Julho/1994.

[RFC1700] REYNOLDS, J.; Postel, J. **Assigned Numbers**. IETF. RFC 1700. Outubro/1994.

[RFC1994] SIMPSON, W. **PPP Challenge Handshake Authentication Protocol (CHAP)**. IETF. RFC 1994. Agosto/1996.

[RFC2058] RIGNEY, C. et al. **Remote Authentication Dial In User Service (RADIUS)**. IETF. RFC 2058. Janeiro/1997.

[RFC2104] KRAWCZYK, H.; Bellare, M.; Canetti, R. **HMAC: Keyed-Hashing for Message Authentication**. IETF. RFC 2104. Fevereiro/1997.

[RFC2364] GROSS, G. et al. **PPP Over AAL5**. IETF. RFC 2364. Julho/1998.

[RFC2516] MAMAKOS, L. et al. **A Method for Transmitting PPP Over Ethernet (PPPoE)**. IETF. RFC 2516. Fevereiro/1999.

[RFC2865] RIGNEY, C. et al. **Remote Authentication Dial In User Service (RADIUS)**. IETF. RFC 2865. Junho/2000.

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

[RFC2869] RIGNEY, C.; Willats, W.; Calhoun, P. **RADIUS Extensions**. IETF. RFC 2869. Junho/2000.

[RFC2904] VOLLBRECHT, J. et al. **AAA Authorization Framework**, IETF, RFC 2904, Agosto/2000.

[RFC2905] VOLLBRECHT, J. et al. **AAA Authorization Application Examples**. IETF, RFC 2905, Agosto/2000.

[RCF2906] FARRELL, S. et al. **AAA Authorization Requirements**. IETF. RFC 2906. Agosto/2000.

[RFC2975] ABOBA, B.; Arkko, J.; Harrington, D. **Introduction to Accounting Management**. IETF. RFC 2975. Outubro/2000.

[RFC3232] REYNOLDS, J. (Ed.) **Assigned Numbers: RFC 1700 is Replaced by an On-line Database**. IETF. RFC 3232. Janeiro/2002.

[RFC3954] CLAISE, B. (Ed.) **Cisco Systems NetFlow Services Export Version 9**. IETF. RFC 3954. Outubro/2004.

[RFC4330] MILLS. David. **Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 ans OSI**. IETF. RFC 4330. Janeiro/2006.

[RFC4960] STEWART, R. (Ed.) **Stream Control Transmission Protocol**. IETF. RFC 4960. Setembro/2007.

[RFC5176] CHIBA, M. et al. **Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)**. IETF. RFC 5176. Janeiro/2008.

[RFC768] POSTEL, J. **User Datagram Protocol**. IETF. RFC 768. Agosto/1980.

[RFC793] POSTEL, J. **Transmission Control Protocol**. IETF. RFC 793. Setembro/1981.

[ROGERS2008] ROGERS COMMUNICATIONS INC. **Rogers Hi-Speed Internet**. Disponível em <http://www.hispeed.rogers.com/bband/content/keepingpace/index.html>. Acesso em: 14 jun. 2008.

[SANTIAGO2003] SANTIAGO, Edmond. **Inclusão Social Turbo Vídeo: Banda larga, instrumento de viabilização de inclusão digital**. Notas de apresentação. 2003. Disponível em: <http://webthes.senado.gov.br/silo/palestra/CCS20030602-Edmond.pdf>. Acesso em: 27 jun. 2008.

[SANTOS2004] SANTOS, Rafael Lopes. **Aspectos de Uma Arquitetura Para Suporte à Prototipação de Aplicações Sensíveis ao Contexto**. Universidade Católica de Pelotas. 2004.

[SILVA2006] SILVA, Ivan M. **ReSinc/HLB: Rede de Sincronismo à Hora Legal Brasileira – Manual Técnico – Versão 3.0**. Observatório Nacional, Divisão Serviço da Hora. Outubro/2006.

[SOARES1995] SOARES, Luiz F. G.; Lemos, Guido; Colcher, Sérgio. **Das LANs MANs e WANs às Redes ATM**. 2ª. Ed. Campus. 1995.

[SPIRENT2002] 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.

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

[SVENSSON2008] SVENSSON, Peter. **Time Warner tries out metered Internet access**. Associated Press. 2 jun. 2008. Disponível em: <http://www.msnbc.msn.com/id/24936796/>. Acesso em: 14 jun. 2008.

[TR101] DSL FORUM. **TR-101: Migration to Ethernet-Based DSL Aggregation.** DSL Forum. Architecture and Transport Working Group. Abril/2006.

[ULTRAL2007] ULTRALÍNGUA. **Dicionário Online Ultralíngua**. Disponível em <http://www.ultralingua.com/onlinedictionary/>. Acesso em: 27 jun. 2008.

[VANAKEN2003] VAN AKEN, Dirk; Peckelbeen, Sascha. **Encapsulation Overhead(s) in ADSL Access Networks**. Thomson. Junho/2003. Disponível em <http://www.oplnk.net/files/White Paper_EncapsOverheads.pdf>. Acesso em: 14 jun. 2008.

[WGET] **GNU Wget**. Disponível em <http://www.gnu.org/ software/wget/> Acesso em: 21 jun. 2008.

[WHATIS] **What is authentication, authorization and accounting?**. Disponível em <http://searchsecurity.techtarget.com/s Definition/0,,sid14_gci514544,00.html>. Acesso em: 27 jun. 2008.

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