Mecanismos de Rastreabilidade de Acessos à Internet (Junho 2008)

Stéphanas Schaden, Gilson Marques da Silva, *CTBC*

***Resumo*—Este artigo apresenta os mecanismos tecnológicos existentes para garantir a rastreabilidade das conexões utilizadas para acesso à Internet. São detalhados os principais tipos de conexão existentes e como elas funcionam. Finalmente, são apresentados os mecanismos que podem ser utilizados para garantir o não-repúdio dos acessos feitos através destas conexões.**

***Palavras-chave*—Acessos à Internet, Mecanismos de Rastreabilidade, Não-repúdio, Regulamentação**

I. Introdução

A Internet tem se tornado parte da vida das pessoas e das organizações a tal ponto que os principais sistemas, processos e serviços atuais usam algum recurso desta rede. Com o aumento exponencial da necessidade da utilização da Internet, esta rede também é cada vez mais acessível de diversos pontos geográficos e a partir de tipos de dispositivos diferentes. Essa maximização de recursos disponíveis para se conectar à Internet ocorre em virtude da demanda crescente das próprias pessoas e das organizações. Com isso, o acesso à Internet tem se massificado, não mais existindo limites geográficos ou do tipo de dispositivo utilizado, podendo ser ele um telefone fixo, aparelho celular ou outro.

Com o aumento da utilização da rede, conseqüentemente, o número de abusos cometidos na Internet também cresce. Estes abusos podem ser desde um simples SPAM a fraudes bancárias com prejuízos incalculáveis.

Desta forma, é necessário que existam mecanismos, tanto dos ISP's (*Internet Service Provider*), como das operadoras que fornecem a infra-estrutura para a conexão destes dispositivos à Internet, para que seja possível identificar o individuo ou organização que fez um determinado acesso.

Para que esta rastreabilidade exista, é necessário que haja uma identificação que vá além do usuário utilizado no acesso, pois é comum na Internet o furto e uso indevido de informações, incluindo usuários e senhas de conexões. Uma conexão pode ser originada com um determinado usuário e este pode não ser o responsável pelo acesso. Desta forma, é necessário identificar de qual dispositivo, linha telefônica ou ponto físico a conexão foi originada [1]. Este é atualmente um grande desafio para as operadoras de todo o mundo: como garantir a rastreabilidade dos acessos à Internet identificando a real origem da conexão.

Neste trabalho são apresentados mecanismos existentes que podem ser implementados nas principais tecnologias utilizadas para acesso à Internet. Dentre estas, são destacadas as principais: conexão dedicada, conexão discada, ADSL (*Asymmetric Digital Subscriber Line*), banda larga via televisão a cabo, GPRS (*General Packet Radio Service*), EDGE (*Enhanced Data Rates for GSM Evolution*) e 3G (*3rd Generation*).

Para estas tecnologias, são apresentadas medidas que geralmente são utilizadas pelas operadoras para identificar a conexão, bem como recursos que as operadoras ainda não implementam que podem ser utilizados para o processo da rastreabilidade.

II. Problema

O grande motivador da necessidade de rastreabilidade surge em virtude da massificação do acesso à Internet e conseqüentemente da elevação de práticas criminais, como furto de senhas bancárias, fraudes e pornografia infantil [2]. A partir do momento que estas ações começam a acontecer, não basta apenas que o acesso seja identificado pelo usuário da conexão. É necessário que exista um processo para garantir o não-repúdio do acesso, a fim de que estas informações possam ser utilizadas em processos legais ou em ações investigativas.

O grande problema é que as operadoras e ISP's não possuem processos adequados que garantam a identificação da conexão com os parâmetros necessários. A situação é tão crítica que muitas vezes a operadora ou ISP nem armazena as informações das conexões de acesso, ou quando armazena, não possui processos para garantir que estas informações não sejam corrompidas ou perdidas. E os principais motivadores destes problemas são a falta de regulamentação das atividades ilícitas cometidas na Internet bem como regulamentações para as operadoras e ISP's. Em virtude da demora neste processo de regulamentação [3] o resultado é o que se vê em grande parte das operadoras e ISP's do país: não existe a preocupação devida em se manter os dados das conexões de acesso.

Juntando todas estas dificuldades, existe um desafio: garantir o não-repúdio nas conexões. Como fazer isto? O que é possível fazer com os recursos existentes?

De fato, com as atuais regulamentações e recursos tecnológicos não é possível resolver todo o problema, porém existem diversos mecanismos que podem ser implementados, a fim de minimizar a falta de rastreabilidade.

III. Tipos de Protocolos e Fluxos de Tráfego Onde não Existe a Possibilidade de Garantir o Não-Repúdio

Existem alguns tipos de tráfego onde não existem formas de se garantir a rastreabilidade. Atualmente, dois terços do tráfego existente na Internet utilizam o protocolo TCP (*Transmission Control Protocol*) para transportar os dados [4]. Uma das características principais deste protocolo de transporte é a orientação à conexão. No protocolo TCP, para que uma comunicação aconteça é necessário que a origem e o destino primeiramente estabeleçam uma conexão antes do envio dos dados. Neste tipo de tráfego há como garantir o não-repúdio, pois, se há uma comunicação, previamente há o estabelecimento de conexão, e se há o estabelecimento de conexão o endereço IP de origem não pode ser falsificado, pois se for falsificado o tráfego não retornaria à origem.

Existem também várias aplicações usadas na Internet que utilizam o protocolo UDP (*User Datagram Protocol*) para transportar os dados. Uma das características deste protocolo é a não orientação à conexão. No UDP não é necessário que previamente haja estabelecimento de conexão. Em virtude das características de cada um dos protocolos de transporte mencionados e de características de outros utilizados nas redes de computadores, existem situações onde não é possível garantir o não-repúdio do tráfego gerado por um determinado acesso:

1) *Protocolos que utilizam o protocolo UDP como transporte e o tráfego é enviado apenas em um sentido.* Nesta categoria existem vários protocolos que enviam tráfego e não esperam resposta do destino informando que os dados enviados foram recebidos. Exemplos de protocolos que possuem esta característica são *syslog* e *trap's* SNMP (*Simple Network Management Protocol*). Visto que estes protocolos são unidirecionais, não há como se garantir o não-repúdio, pois como não houve necessidade da origem estabelecer uma conexão com o destino, este tráfego pode ter sido gerado com o endereço IP falsificado.
2) *Tráfego onde não há troca de informações entre a origem e o destino, podendo ele ser transportado pelo protocolo UDP ou TCP.* Exemplo deste tipo de tráfego são os ataques de negação de serviço com endereços IP falsificados.
3) *NAT (Network Address Translation)* [5]. Este é um grande ofensor do processo de rastreabilidade na Internet é uma prática utilizada pela maioria das empresas e inclusive por alguns serviços oferecidos pelas próprias operadoras. O NAT é um mecanismo de tradução de endereços IP e é bastante utilizado pelos clientes das operadoras em virtude destes clientes receberem uma gama limitada de endereços públicos e também em virtude do custo que as operadoras cobram pelo número de endereços públicos fornecidos. Outro motivo para utilização do NAT é que, com o IPv4 *(Internet Protocol version 4)* o número máximo de endereços possíveis não atenderia a todos os dispositivos existentes no planeta que necessitam de se comunicar com a Internet. Desta forma, geralmente, o tráfego interno das empresas antes de ser enviado para a Internet passa por um elemento da rede que faz a tradução do endereço interno para um endereço público. O grande problema desta prática é que não há como garantir o não-repúdio do tráfego que foi processado pelo NAT, visto que o tráfego gerado pelos endereços da rede interna geralmente são encaminhados para a Internet com o mesmo endereço público. O que as operadoras devem fazer é garantir que os serviços oferecidos por ela possuam rastreabilidade, mesmo que o cliente não garanta o mesmo na sua rede interna. Porém, o que se percebe é que às vezes as próprias operadoras vendem serviços fornecendo endereços privados para o cliente, a exemplo de serviços móveis, como GPRS, EDGE e 3G. Se os clientes não possuem mecanismos para fazer a rastreabilidade em sua rede, a operadora de todas as formas deve garantir a sua parte.

IV. Principais Tipos de Acesso à Internet e Mecanismos Para garantir a Rastreabilidade Nestes Acessos

A. Acesso Dedicado

Este é um tipo de acesso bastante utilizado por médias e grandes empresas, onde o meio de acesso à Internet é dedicado do cliente até a operadora. Geralmente, neste tipo de acesso, o cliente possui um *link* dedicado até a infra-estrutura da operadora. Neste tipo de acesso, uma faixa de endereços IP é reservada no *backbone* da operadora e alocada diretamente para o cliente. Enquanto a faixa de endereços estiver configurada adequadamente no *backbone* existe a garantia que qualquer acesso feito a partir destes endereços foi originado através do meio físico dedicado, salvo as situações detalhadas no item três.

Neste tipo de acesso, o essencial para que a operadora garanta que um determinado acesso foi originado de um determinado cliente é uma base cadastral confiável com a alocação dos endereços IP. Geralmente, o maior problema é que as operadoras não mantêm o histórico destas alocações, possuindo cadastro apenas do que está em funcionamento, de forma que se houver a necessidade de verificação de alocação de um determinado IP há uma semana ou há cinco anos esta informação não existe. O grande motivo de se manter o histórico da alocação dos endereços IP é que um endereço que hoje está sendo utilizado por um determinado cliente pode ter sido utilizado há uma semana por outro e se o incidente foi de uma semana atrás o responsável não é o cliente atual. De uma forma geral, para todos os tipos de acesso, a operadora deve possuir um cadastro confiável e com histórico de alocação dos endereços para que exista sucesso no processo de rastreabilidade.

B. Conexão Discada/ISDN (Integrated Services Digital Network)

Este é um tipo de conexão à Internet bastante utilizado por

usuários residenciais que possuem renda baixa e geralmente neste tipo de acesso as conexões são feitas em períodos noturnos em virtude do baixo custo do acesso neste horário.

Este acesso também é utilizado em algumas empresas para transmitir informações de aplicações de missão crítica em situações de quedas generalizadas nos mecanismos padrões de comunicação. Neste tipo de acesso o cliente possui um modem (modulador/demulador) e os dados são transmitidos pela linha telefônica até um equipamento concentrador de acesso da operadora que é conhecido como RAS (*Remote Access Server*). Neste tipo de tecnologia, a velocidade de transmissão é baixa, geralmente chegando ao máximo de 56kbits/s e quando o canal está sendo utilizado pelo modem não é possível estabelecer comunicação de voz [6]. Neste modelo, a topologia de acesso à Internet acontece conforme exibido na figura 1.

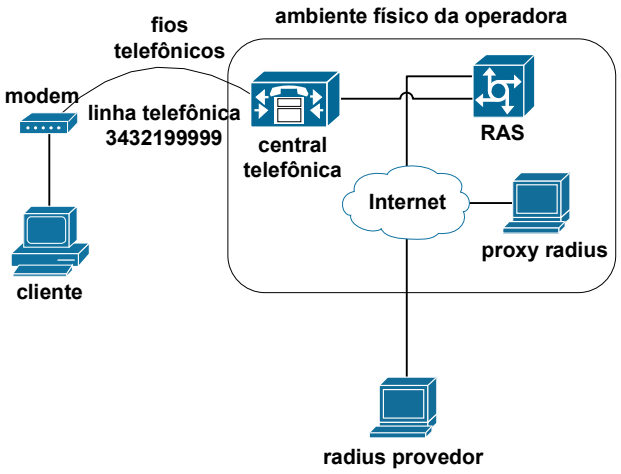

Fig. 1. Topologia de acesso à Internet através de conexão discada.

O modem é ligado ao computador do usuário e à linha telefônica. A linha telefônica termina na central telefônica da operadora e a central possui uma ligação com o RAS que faz a demodulação dos dados enviados pelo modem do usuário. O RAS possui as configurações dos endereços IP que são alocados para os usuários que estabelecem as conexões, bem como os endereços dos servidores que farão o gerenciamento da autenticação dos acessos. Geralmente, o processo acontece da seguinte forma: O usuário especifica um número telefônico de conexão, um usuário e uma senha para se conectar. Estes dados são enviados pela linha telefônica até a central da operadora e a central verifica qual é o número telefônico solicitado para ser feito a conexão e por sua vez faz o encaminhamento da chamada através deste número para o RAS. Este equipamento recebe a chamada e faz o processo de negociação com o modem do usuário. Se esta primeira fase ocorreu corretamente o RAS verifica para qual equipamento ele deve encaminhar a autenticação a fim de validar o acesso. Os dados geralmente são enviados para um equipamento radius da operadora chamado de proxy radius e este faz o repasse da autenticação para o radius do provedor de acesso. Se o proxy radius da operadora receber confirmação de sucesso do radius do provedor ele informa ao RAS que a autenticação ocorreu com êxito. A partir deste momento a conexão é estabelecida, o RAS aloca e disponibiliza um endereço IP para o usuário e gera um bilhete de *start* da conexão e o envia para o proxy radius. O proxy radius grava estas informações em uma base de dados e faz o repasse deste bilhete para o radius do provedor que também grava este bilhete em uma base de dados. Quando acontecer o processo de desconexão, o fluxo será o mesmo do processo de conexão, porém, o RAS gerará um bilhete de *stop* e não um bilhete de *start*. Neste tipo de acesso é possível garantir o não-repúdio da conexão, desde que vários itens sejam observados.

Quando a conexão está sendo estabelecida, a central telefônica verifica qual é o número telefônico de origem utilizado na chamada. É possível fazer com que a central repasse este número conhecido também como CLI (*Caller Line Identification*) para o RAS. Além disso, outra prática importante é configurar a central de forma que, mesmo que a linha telefônica utilizada na conexão possua o serviço para não identificar o número de origem da chamada (anti-bina), o número telefônico deve ser repassado para o RAS. O RAS por sua vez deve ser configurado para enviar o CLI para o equipamento que fará o gerenciamento das autenticações (geralmente, o servidor proxy radius da operadora). Se a central telefônica e o RAS possuírem estas configurações e as mantiverem de forma adequada, os bilhetes das conexões originadas através deste tipo de acesso terão a informação do número telefônico utilizado. Abaixo são detalhados os bilhetes de conexão do cliente proprietário da linha 3432199999 exibido na figura 1.

Tue May 27 12:10:33 2008
User-Name = "usuariofictício"
NAS-IP-Address = 200.170.XXX.228
Acct-Status-Type = Start
Acct-Session-Id = "341073148"
Calling-Station-Id = "**3432199999**"
Framed-IP-Address = 200.233.XXX.222

Tue May 27 12:16:04 2008
User-Name = "usuariofictício"
NAS-IP-Address = 200.170.XXX.228
Acct-Status-Type = Stop
Acct-Session-Id = "341073148"
Calling-Station-Id = "**3432199999**"
Framed-IP-Address = 200.233.XXX.222

Para que os bilhetes possuam confiabilidade de data e hora é necessário que tanto os equipamentos que geram os bilhetes das conexões quanto os servidores radius que recebem estes bilhetes possuam mecanismos para manter seus relógios sincronizados através do protocolo NTP (*Network Time Protocol*) [7] e que possuam configurações para manter as zonas de tempo reais em que os equipamentos se encontram.

Através dos bilhetes da conexão é possível verificar exatamente o dia, a hora, o minuto e o segundo que a conexão foi iniciada e finalizada, o endereço IP utilizado, bem como o usuário e o número telefônico.

A tecnologia ISDN funciona de forma similar à conexão discada. A diferença é que a linha telefônica passa a oferecer uma banda de 128kbits/s, visto que os dados são transmitidos

de forma digital e multiplexados. Para o estabelecimento da conexão o processo funciona da mesma forma que a conexão discada.

Para a correta identificação da pessoa física ou jurídica que utilizou uma conexão discada ou uma conexão ISDN é necessário que o cadastro da operadora com as informações dos números telefônicos associados às pessoas físicas ou jurídicas seja confiável, pois o processo tecnológico pode ter sido feito corretamente e o número telefônico utilizado na chamada identificado corretamente, porém, se o cadastro da operadora aponta o nome de uma pessoa errada para o número telefônico, todo o processo pode ser comprometido.

C. *Conexão Banda Larga ADSL*

Este é atualmente o tipo de acesso banda larga à Internet com maior volume de usuários [8] devido à alta taxa de transmissão que se consegue na linha telefônica, ao custo acessível à grande parte da população além da linha telefônica não ficar ocupada quando a conexão está estabelecida. E também neste tipo de acesso está o maior desafio das operadoras para garantir o não-repúdio.

Diferentemente da conexão discada, mesmo utilizando-se a linha telefônica, o tráfego de acesso à Internet não passa pela central da operadora, visto que não se trata de uma chamada telefônica. Desta forma, não é possível fazer com que o número telefônico seja enviado nos bilhetes da conexão.

O funcionamento da rede ADSL acontece conforme exibido na figura 2.

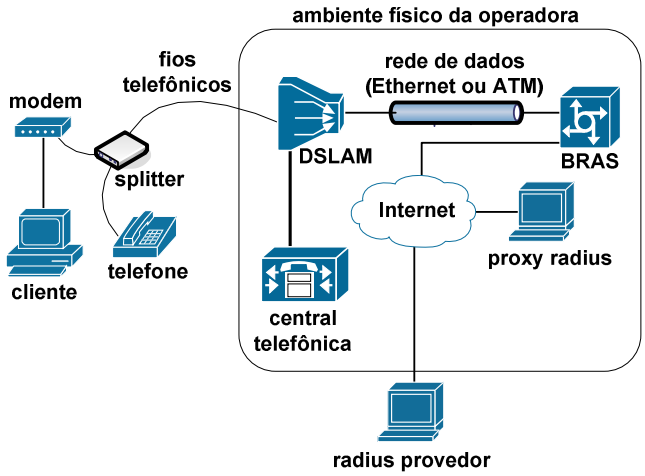

Fig. 2. Topologia de acesso à Internet através de conexão ADSL.

O usuário gera tráfego de voz através do telefone ou de dados através do modem e estes informações são enviadas na linha telefônica em freqüências diferentes. Na operadora, existe um *splitter*, que fica geralmente instalado fisicamente no DSLAM (*Digital Subscriber Line Access Multiplexer*) que faz o processo de separação da freqüência da voz da freqüência dos dados. A voz é encaminhada para a central telefônica e os dados são enviados internamente para o DSLAM processá-los. Os dados processados pelo DSLAM são encaminhados para a rede até chegarem no BRAS (*Broadband Remote Access Server*). O BRAS é o equipamento concentrador dos acessos e o responsável por fazer todo o controle dos acessos ADSL, como alocação dos endereços IP para as conexões, gerenciamento do processo de autenticação e é responsável também por fazer o roteamento de todo o tráfego dos clientes ADSL que serão enviados para a Internet. Quando o usuário ADSL envia sua solicitação de autenticação e esta autenticação chega ao BRAS, a partir deste momento o processo de autenticação ocorre exatamente igual ao processo descrito para a conexão discada.

Geralmente, a maioria dos acessos ADSL é originada de redes com tecnologia *Ethernet*, porém, grande parte das operadoras ainda possuem uma parcela da sua rede funcionando com tecnologia ATM (*Asynchronous Transfer Mode*) e ainda utilizam esta estrutura para oferecer serviços.

A seguir serão detalhados os dois tipos de tecnologia e o que geralmente é enviado nos bilhetes de conexão em cada uma delas.

ADSL sobre ATM

A tecnologia ATM é uma tecnologia de comunicação de dados que foi criada em meados de 1980 com a estratégia principal de poder ser utilizada para transportar vídeo e áudio em tempo real além dos dados convencionais [9]. Diferente da tecnologia *Ethernet* onde os dados são enviados em pacotes de tamanhos variáveis, na tecnologia ATM os dados são encapsulados em células de tamanho fixo de 53 *bytes* e em virtude da padronização do tamanho das células a transmissão acontece com um comportamento padronizado, sendo mais fácil de ser processada pelos equipamentos em virtude da não necessidade de utilização de buffers de tamanhos variados.

Neste tipo de tecnologia existe um conceito também muito importante que é o circuito virtual, onde é estabelecido um canal virtual de uma porta A até uma ponta B da rede. Para implementar estes circuitos virtuais a tecnologia faz uso de dois parâmetros:

VP (Virtual Path): É o caminho virtual criado entre dois equipamentos na rede ATM. O caminho virtual é identificado através do parâmetro VPI (*Virtual Path Identifier*) e para este campo são reservados 8 bits, podendo-se chegar a 12, dependendo da implementação da rede.

VC (Virtual Circuit): É o canal virtual que será utilizado para comunicação entre dois equipamentos na rede. O canal virtual utilizará o VP para se comunicar com o outro equipamento. O circuito virtual é identificado através do parâmetro VCI (*Virtual Circuit Identifier*) e para este campo são reservados 16 bits.

Com estes parâmetros é possível estabelecer 4096 ou 256 caminhos virtuais em uma infra-estrutura de rede ATM e 65535 circuitos virtuais em cada caminho virtual, de acordo com as combinações máximas dos bits reservados na célula ATM [10].

Em virtude do conceito de circuito virtual, as redes ATM das operadoras podem ser configuradas com estes parâmetros para identificar unicamente o assinante na rede. Para que isso aconteça, a operadora deve configurar cada caminho virtual entre o DSLAM e o BRAS com um VPI único e cada porta de assinante do DSLAM com um VCI único. A configuração dos VPI's e VCI's executada no DSLAM deve ser refletida no BRAS visto que se trata de caminhos virtuais e circuitos virtuais entre dois elementos da rede. Com a rede configurada

seguindo este modelo quando um usuário solicitar uma conexão na rede ADSL os dados deste cliente chegarão no DSLAM e este iniciará o estabelecimento do circuito virtual até o BRAS. O circuito virtual será estabelecido com identificação única na rede conforme exibido na figura 3.

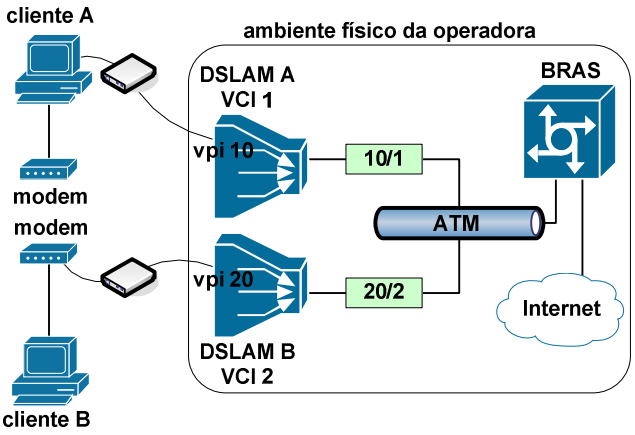

Fig. 3. Topologia de acesso à Internet através de conexão ADSL utilizando infra-estrutura de rede ATM.

Com esta topologia, basta apenas configurar o BRAS para que ele envie nos bilhetes de conexão a informação do VPI/VCI que o assinante utilizou. O bilhete a seguir mostra as informações de conexão do cliente "A" exibido na figura 3. Foi utilizado o caminho virtual com identificação 1 e o circuito virtual com identificação 10 entre o DSLAM e o BRAS:

Mon Jun 9 10:58:21 2008
Acct-Status-Type = Start
User-Name = "usuariofictício"
Framed-IP-Address = 189.41.XXX.254
NAS-Port-Id = "atm 2/0.:**1.10**"

De posse destas informações, basta que a operadora possua um cadastro confiável com as combinações dos VPI's e VCI's relacionando-os com a linha telefônica dos assinantes.

Juntamente com este cadastro, a operadora deve possuir um processo de gerenciamento de mudanças que garanta que qualquer modificação na estrutura da rede ADSL que interfira nas identificações seja refletida na base de cadastro.

ADSL sobre Ethernet

Este tipo de infra-estrutura é a mais utilizada hoje em dia em virtude da tecnologia *Ethernet* ter se tornado de fato a tecnologia padrão para comunicação em redes locais [11]. É neste tipo de arquitetura de rede também que existem os principais problemas de garantia do não-repúdio dos acessos, pois, diferentemente da rede ATM, onde existe o conceito do canal virtual estabelecido da origem ao destino, na rede *Ethernet* todos os elementos estão compartilhando a transferência dos dados no mesmo segmento.

A maioria das operadoras possui infra-estrutura para prover o serviço de ADSL utilizando o conceito de VLAN (*Virtual Local Area Network*), definido pelo padrão IEEE 802.1Q [12]. Com a utilização de VLAN's é possível segmentar a rede e assim diminuir o volume de *broadcasts*, limitando-o ao segmento de cada VLAN. A figura 4 mostra como fica implementado este modelo.

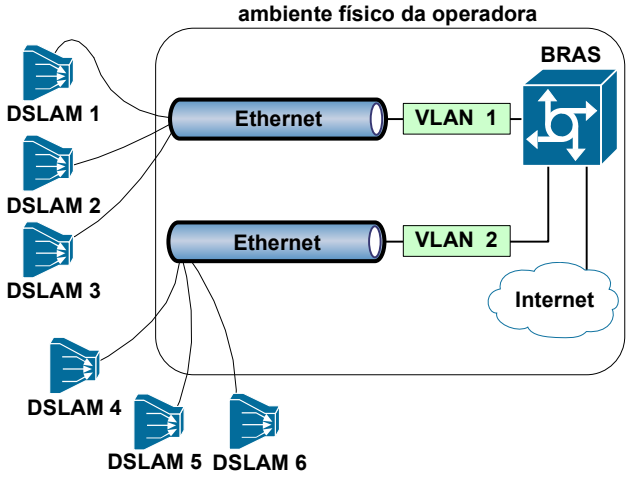

Fig. 4. Segmentação da infra-estrutura de rede ADSL com tecnologia Ethernet utilizando VLAN.

Quando a rede da operadora está segmentada utilizando VLAN's os quadros *Ethernet* gerados pelo usuário, antes de saírem do DSLAM recebem uma marcação com a identificação da VLAN configurada no DSLAM. Esta identificação é chamada de *tag*. O funcionamento acontece conforme mostrado na figura 5.

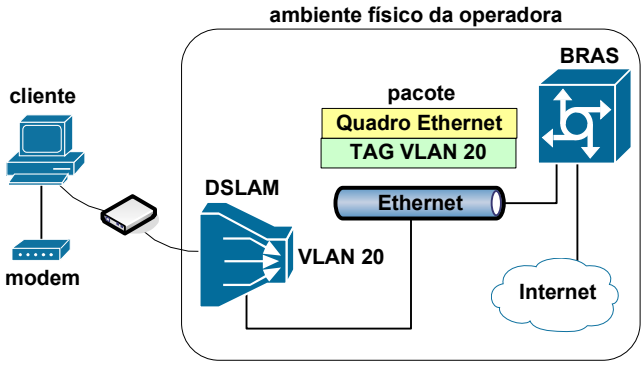

Fig. 5. Marcação do quadro Ethernet com o "*tag*" de id 20.

A seguir é exibido o bilhete da conexão do cliente da figura 5.

Mon Mar 31 08:55:05 2008
Acct-Status-Type = Start
User-Name = "usuario@provedorficticio.com.br"
Acct-Session-Id = "0647440354"
Framed-IP-Address = 189.15.XXX.23
NAS-Port-Id = "GigabitEthernet 4/1/0.**20**"

No bilhete, o BRAS gerou as seguintes informações:
Data: dia, hora, minuto e segundo da conexão
Acct-Status-Type: Tipo da conexão
User-Name: Usuário utilizado na conexão
Acct-Session-Id: Identificador único da conexão gerado para cada par de conexões na rede (*start e stop*)
Framed-IP-Address: Endereço IP utilizado na conexão
NAS-Port-Id: Informações da interface física e lógica onde foi estabelecida a conexão. No exemplo do bilhete anterior a

conexão foi recebida pela interface física GigabitEthernet4/1/0 e interface lógica VLAN 20.

Com as informações do bilhete é possível saber apenas qual segmento da rede foi utilizado.

Para resolver este problema existem duas soluções tecnológicas que podem ser utilizadas:

1) Utilização do padrão estabelecido pelo IEEE denominado 802.1ad (Provider Bridge), conhecido como QinQ [13].
2) Utilização da funcionalidade proposta do DSL Fórum 2004-71 denominada "PPPoE Remote Circuit ID" [14].

Ambas as tecnologias resolvem o problema do não-repúdio desde que itens sejam observados em cada uma delas. Este artigo focará a primeira opção visto que é o modelo que mais se aproxima de um "circuito virtual" único para o assinante.

O QinQ funciona da seguinte forma: No DSLAM é definida uma VLAN (denominada *outer)* na interface que o liga até a rede de dados e para cada porta de assinante é definida uma VLAN única (denominada *inner)*. Com estas configurações, quando um quadro *Ethernet* é recebido da linha telefônica do cliente na porta do DSLAM é adicionado o *tag* da VLAN *inner* no quadro *Ethernet* e quando este quadro for sair da porta física do DSLAM que o liga à rede de dados é adicionada a VLAN *outer*, de forma que quando os quadros *Ethernet* chegarem ao BRAS eles cheguem com a VLAN *inner* e a VLAN *outer*. Com esse duplo *tag* é possível fazer a identificação física do assinante na rede *Ethernet*, visto que, cada DSLAM será identificado com uma VLAN única e cada assinante de cada DSLAM também será identificado com uma VLAN única.

Na definição do padrão IEEE 802.1Q, são reservados 12 *bits* para serem utilizados como identificador da VLAN. Desta forma, é possível identificar 4096 assinantes por DSLAM e 4096 DSLAM's na rede, perfazendo uma possibilidade máxima de identificação de 16.777.216 assinantes na rede.

Caso a operadora possua um volume de assinantes maior que 16.777.216, alternativas na topologia podem ser desenhadas para duplicar ou triplicar este número.

A figura 6 mostra uma conexão ADSL sendo originada a partir de uma infra-estrutura com configuração de QinQ.

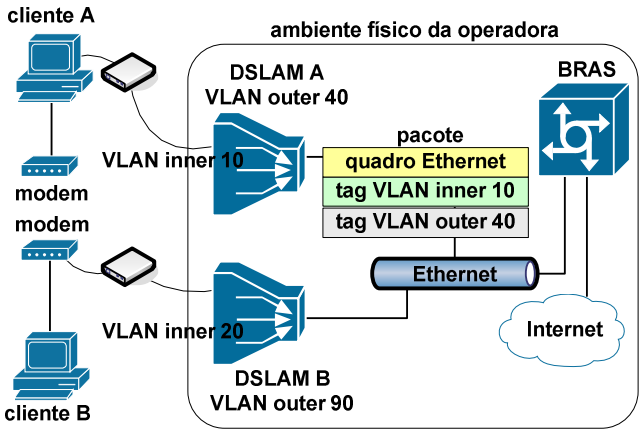

Fig. 6. Topologia de acesso à Internet através de conexão ADSL utilizando infra-estrutura de rede com configuração de QinQ.

O bilhete a seguir mostra as informações da conexão do cliente "A" exibido na figura 6. O cliente se conectou utilizando o usuário "usuario@provedorficticio.com.br" e a conexão ADSL foi estabelecida com origem do DSLAM com identificação 40 e pela porta do DSLAM com identificação 10.

Mon Mar 31 08:55:05 2008
Acct-Status-Type = Start
User-Name = "usuario@provedorficticio.com.br"
Acct-Session-Id = "0647440354"
Framed-IP-Address = 189.15.XXX.23
NAS-Port-Id = "GigabitEthernet 4/1/0.**40:10**"

De posse destas informações, se a operadora possuir um cadastro confiável com as combinações dos *tags* das VLAN's, relacionando-os com as linhas telefônicas dos assinantes é possível garantir qual linha telefônica foi utilizada por uma determinada conexão.

O grande dificultador deste tipo de implementação nas operadoras deve-se em virtude da necessidade de reconfiguração de toda a rede, esforço este, que, geralmente não é empregado em virtude do custo e também da não regulamentação no processo de rastreabilidade.

D. Internet via Cabo

Este é um tipo de acesso à Internet onde é utilizada a infra-estrutura de televisão a cabo para transportar dados. O processo é similar à transmissão de dados na rede ADSL, em virtude dos canais de televisão serem transmitidos em uma determinada freqüência e os dados em outra.

Na infra-estrutura da operadora existe um equipamento chamado CMTS (*Cable Modem Termination System*) que é responsável por receber os dados enviados por rádio freqüência através do cabo de televisão e transmiti-los para a rede de dados e vice-versa [15]. O CMTS atua como se fosse o DSLAM da rede ADSL visto que ele é o elemento da rede que recebe os sinais analógicos da rede de televisão e os converte em sinais digitais para que possam ser enviados para a Internet. Existem CMTS's que terminam a sessão do modem, fazendo o papel do BRAS da rede ADSL e existem CMTS's que atuam apenas como *bridge*, sendo necessário outro equipamento da rede para terminar a sessão do usuário.

De acordo com o padrão DOCSIS (*Data Over Cable Service Interface Specification*) [16], que é definido pelo ITU-T (*International Telecomunications Union Telecomunications Standardization Sector*) para especificar os padrões de operação e comunicação de dados sobre as redes de televisão a cabo, o parâmetro que ainda é utilizado para aceitar ou não um dispositivo na rede é o endereço físico do modem.

Cada modem possui um endereço MAC (*Media Access Control*) único. Para que este modem funcione na rede é necessário que o MAC seja permitido nos equipamentos que compõem a infra-estrutura.

O mecanismo existente nas redes de dados sobre televisão a cabo para garantia da rastreabilidade dos acessos é o conceito já mencionado nas redes ADSL conhecido como QinQ, porém, com uma implementação um pouco diferente da rede ADSL, visto que diferente do DSLAM, no CMTS não existe uma porta física para cada assinante. Existe uma ligação única onde o tráfego de todos os assinantes é recebido. Para que seja possível implementar o QinQ os CMTS's modernos

possuem um recurso para associar o tráfego originado de um modem a uma determinada VLAN, considerada a VLAN *inner* ou VLAN do assinante. Quando o tráfego for encaminhado pela interface de dados do CMTS é então adicionada a VLAN *outer*, de forma que a diferenciação do modelo de funcionamento do QinQ, comparado à rede ADSL, é que a VLAN do assinante não é mais associada a uma porta física, mas é feita ao endereço MAC do modem. Para que este modelo de topologia funcione, é necessário que o terminador da sessão esteja configurado com os parâmetros adequados de QinQ, seguindo o mesmo modelo da rede ADSL.

O funcionamento da rede neste modelo de topologia acontece conforme a figura 7.

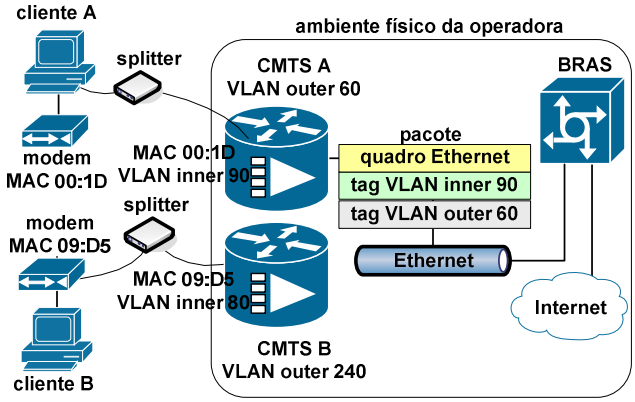

Fig. 7. Topologia de acesso à Internet através de infra-estrutura com CMTS atuando como *bridge*, onde o cliente "A" com MAC 00:1D é associado no CMTS à VLAN 90 e é utilizado a VLAN 60 para identificar o CMTS.

Quando o CMTS está terminando a sessão do usuário, e funcionando como roteador, o parâmetro existente para garantir a rastreabilidade dos acessos é o endereço MAC do modem. Para que isto aconteça é necessário que CMTS suporte o mecanismo de envio do endereço MAC do modem nos bilhetes de conexão.

O grande dificultador da implementação de rastreabilidade nas infra-estruturas de dados sobre as redes de televisão a cabo são os equipamentos legados. Geralmente, estes equipamentos não suportam recursos como QinQ, geração de bilhetes de conexão ou envio do MAC do modem nos bilhetes.

Para que a rastreabilidade nestas redes seja garantida é necessário que se utilize equipamentos modernos e uma topologia de rede projetada com o propósito de garantia da rastreabilidade dos acessos.

E. GPRS, EDGE e 3G

Segundo a corporação Google, o futuro da Internet é a mobilidade [17], e a cada dia a utilização de dispositivos móveis para conexão a esta rede tem aumentado. E com a evolução destas tecnologias, principalmente a 3G que oferece alta taxa de transmissão, chegando geralmente a uma possibilidade de velocidade de *downstream* de 7.2 Mbits/s, é necessária uma atenção especial das operadoras para estas tecnologias. É possível que o maior desafio de garantia da rastreabilidade dos acessos seja nestas tecnologias móveis. A dificuldade não está muitas vezes no processo de identificação, pois é possível garantir qual SIM *card* (*Subscriber Identity Module card*) foi utilizado na conexão, visto que cada *chip* possui uma identificação única. Porém, diferentemente das linhas telefônicas, onde a conexão é originada através de um meio físico, nestas tecnologias o acesso pode ser originado de qualquer região onde o sinal do serviço seja oferecido.

Desta forma, a rastreabilidade dos acessos nas redes *GPRS*, *EDGE* e *3G* se limita até o número do *chip* utilizado na conexão, não podendo garantir que um determinado acesso foi feito a partir de um determinado ponto físico. Com a informação do identificador do *chip* a operadora deve possuir uma base de cadastro confiável com a associação do número do chip à pessoa que o comprou e ao número telefônico associado ao *chip* para que se tenha a informação da pessoa responsável pelo *chip* utilizado na conexão.

Nestas redes, quando um dispositivo estabelece uma conexão de dados à Internet, existe um elemento da rede chamado de GGSN (*Gateway GPRS Support Node*) que faz todo o processo de bilhetagem do tráfego. Sobre o ponto de vista do aspecto da rastreabilidade, não existe diferença destas tecnologias móveis (GPRS, EDGE e 3G), haja vista, que os bilhetes das conexões em qualquer uma delas possuem as mesmas informações. A seguir é apresentado um bilhete gerado de uma conexão GPRS:

servedIMSI = **7243401000XX924**
servedMSISDN = 55349992XX13
chargingID = 3493264162
accessPointNameNI = XXXX.br
servedPDPAddress = 172.28.XX.252
recordClosureTime = 2008-06-09 15:01:35-03:00
recordOpeningTime = 2008-06-09 15:00:49-03:00

Nas redes GPRS, EDGE e 3G não é gerado um bilhete assim que o dispositivo inicia a conexão. Existe apenas um bilhete que é gerado no término da conexão e este contém todas as informações necessárias.

De acordo com as informações apresentadas no bilhete anteriormente os seguintes parâmetros podem ser utilizados no processo de rastreabilidade:

servedIMSI: Contém a informação do identificador único do SIM *card* utilizado na conexão. Este é o parâmetro principal do processo de rastreabilidade, visto que este número está eletronicamente gravado no *chip*.

servedMSISDN: número do telefone programado na operadora que está associado ao SIM *card* utilizado.

chargingID: identificador único gerado para identificar a conexão nos bilhetes.

accessPointNameNI: identificador da APN (*Access Point Name*), que é o domínio utilizado pelo dispositivo na conexão para receber as configurações devidas da operadora.

servedPDPAddress: endereço IP recebido pelo dispositivo e utilizado para fazer o acesso à Internet.

RecordClosureTime: dia, mês, ano, minuto, segundo e zona de tempo que a conexão foi finalizada.

recordOpeningTime: dia, mês, ano, minuto, segundo e zona de tempo que a conexão foi iniciada.

De posse destes parâmetros se a operadora possuir um cadastro da associação dos números dos SIM *cards* e números telefônicos com os clientes que compraram o serviço, é

possível saber qual é o cliente responsável pelo SIM *card* utilizado em uma determinada conexão, porém, existem dois grandes problemas nas redes destas tecnologias:

O primeiro problema é que nas topologias de rede GPRS, EDGE e 3G implementadas nas operadoras a rede IP oferecida aos dispositivos é uma rede com endereços privados e quando o tráfego dos dispositivos é destinado à Internet, existe um elemento da rede, que faz a tradução dos endereços de origem para endereços públicos utilizando os mecanismos de NAT. Conforme já mencionado, não é possível garantir rastreabilidade de acessos com tradução dos endereços utilizando NAT. Mesmo que a operadora possua logs de todas as traduções feitas, existe a possibilidade de dois dispositivos acessarem o mesmo endereço na Internet simultaneamente.

Desta forma, para que o processo de rastreabilidade funcione nestas redes o primeiro passo a ser seguido pelas operadoras é desenhar uma topologia de rede que os dispositivos recebam endereços IP públicos, como já acontece hoje para os acessos discados e ADSL.

O segundo problema é que as operadoras, em virtude da necessidade de venda dos serviços, estão comercializando acessos através de *chips* pré-pago pré-programados, onde não existe a necessidade do comprador do serviço ir fisicamente até um ponto de venda e fazer um cadastro com as informações pessoais. Várias operadoras já estão vendendo *chips* para acesso à Internet através destas tecnologias em bancas de revistas, supermercados e outros pontos de venda, bastando apenas que o usuário assim que comprar o *chip* ligue no atendimento da operadora e informe alguns dados pessoais, não havendo necessidade de comprovantes de documentações. Neste caso, qualquer um pode informar números falsos de documentos pessoais.

Este é um problema crítico, pois, tecnologias como 3G oferecem alta taxa de transmissão [18] e com isso, estes acessos passam a ser utilizados em atos ilícitos na Internet.

É necessário que a operadora venda os serviços, porém, com os recursos mínimos para que seja possível garantir rastreabilidade nos acessos feitos através destas tecnologias.

V. Resultados e Contribuições da Pesquisa

Este artigo traz ao conhecimento da sociedade, operadoras de telecomunicações, provedores de serviço, órgãos investigativos e policiais, mecanismos tecnológicos que existem e que podem ser adotados para garantia de rastreabilidade nos acessos à Internet.

É fato, que em investigações, mesmo que a operadora faça a identificação correta dos acessos, estes dados devem ser parte do processo e não as únicas informações utilizadas.

De uma forma geral, este trabalho produz uma documentação que até então era inexistente no tema, focando os tipos de acesso à Internet mais utilizados no país.

VI. Conclusão

O principal motivo da falta de implementação dos recursos tecnológicos existentes para garantia da rastreabilidade nos acessos, deve-se à falta de regulamentação no país, haja vista que, sem regulamentação, as equipes de segurança da informação não conseguem justificar o custo gerado para modificar toda a rede e mantê-la com os parâmetros de rastreabilidade adequados.

Para que estes recursos possam realmente ser aplicados é necessário que o governo brasileiro crie regulamentações adequadas tanto para as operadoras de telecomunicações quanto para os provedores de serviço, pois sem a regulamentação, a situação das redes das operadoras de telecomunicações do país continuará como está hoje: sem mecanismos que garantam a rastreabilidade dos acessos.

Referências

[1] CLAYTON, R., *The Limits of Traceability*, 2001. Disponível em <http://www.cl.cam.ac.uk/~rnc1/The_Limits_of_Traceability.html>. Acesso em Junho de 2008.

[2] O GLOBO ONLINE; *Tentativas de fraudes na Internet têm alta de 8% em 2007*, 2008. Disponível em <http://www.nic.br/imprensa/clipping/2008/midia019.htm>. Acesso em Junho de 2008.

[3] CERQUEIRA, T., *A Regulamentação da Internet no Brasil*, 2004. Disponível em <http://www.apriori.com.br/cgi/for/viewtopic.php?f=22&t=88>. Acesso em Junho de 2008.

[4] CAIDA –Cooperative Association for Internet Data Analysis; *Passive Network Monitors*, 2008. Disponível em <http://www.caida.org/data/realtime/passive/?monitor=miami&row=timescales&col=sources&sources=proto&graphs_sing=ts&counters_sing=bits&timescales=672>. Acesso em Junho de 2008.

[5] EGEVANG, K., et al. *The IP Network Address Translator (NAT)*. RFC 1631, 1994. Disponível em <http://www.ietf.org/rfc/rfc1631.txt>. Acesso em Junho de 2008.

[6] ENGLE, M., *Internet Connections: A Librarian's Guide to Dial-up Access and Use*: ALA Editions, 2000.

[7] MILLS, D e LINKABIT, M., *Network Time Protocol (NTP)*. RFC 958, 1985. Disponível em <http://www.ietf.org/rfc/rfc958.txt>. Acesso em Junho de 2008.

[8] Capacity, TelCap Ltd, v.8, n.8, p. 83, jun. 2008.

[9] PERROS, H., *An Introduction to ATM Networks. 1. ed:* Wiley, 2001.

[10] RUSSEL, T., *Telecommunications Protocols. 2. ed*: McGraw-Hill Professional Publishing, 1999.

[11] KUROSE, J. e ROSS, K., *Redes de Computadores e a Internet: Uma Abordagem Top-Down. 3. ed:* Pearson Education, 2005.

[12] IEEE; *802.1Q – Virtual LANs*, 2006. Disponível em <http://www.ieee802.org/1/pages/802.1Q.html>. Acesso em Junho de 2008.

[13] IEEE; *802.1ad – Provider Bridges*, 2006. Disponível em < http://www.ieee802.org/1/pages/802.1ad.html>. Acesso em Junho de 2008.

[14] CISCO SYSTEMS; *PPPoE Circuit-Id Tag Processing*, 2005. Disponível em <http://www.cisco.com/en/US/docs/ios/12_4t/12_4t4/htecidtg.html>. Acesso em Junho de 2008.

[15] OLSSON, A., *Understanding Changing Telecommunications: Building a Successful Telecom Business. 1. ed:* Wiley, 2004.

[16] DOCSIS - Resource Information for Cable Operators; *DOCSIS: Data Over Cable Service Interface Specifications*. Disponível em <http://docsis.org>. Acesso em Junho de 2008.

[17] PLANTÃO INFO; *Futuro da Internet é mobilidade, diz Google*, 2007. Disponível em <http://info.abril.com.br/aberto/infonews/102007/26102007-12.shl>. Acesso em Junho de 2008.

[18] STUDIES, A, CRANDALL, R e ALLEMAN, J., *Broadband: Should We Regulate High-Speed Internet Access?*: American Enterprise Institute Press, 2003.